TALLINN UNIVERSITY OF TECHNOLOGY
SCHOOL OF INFORMATION TECHNOLOGIES

EFFECTIVENESS OF RED TEAM TACTICS, TECHNIQUES AND PROCEDURES IN THE CONTEXT OF LOCKED SHIELDS

MASTER THESIS

Student: Marcin Mateusz Badora

Student code: 223592IVCM

Supervisor: Rain Ottis PhD (TalTech)
Bernhard Lippe MSc (NATO CCDCOE)

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

PUNASE MEESKONNA TAKTIKA, TEHNIKATE JA PROTSEDUURIDE TÕHUSUS LOCKED SHIELDS ÕPPUSE KONTEKSTIS

MAGISTRITÖÖ

Autor: Marcin Mateusz Badora

Üliõpilaskood: 223592IVCM

Juhendaja: dr. Rain Ottis (TalTech)
mag. Bernhard Lippe (NATO CCDCOE)

Tallinn 2026

Contents

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Marcin Mateusz Badora

20.05.2026

Statement on the Use of Artificial Intelligence in Manuscript Preparation

During the drafting and editing stages of this thesis, AI-assisted language processing tools were employed to enhance the stylistic consistency, syntactical precision, and linguistic flow of the text. The author maintains full responsibility for the intellectual integrity of the work. All ideas, research methodologies, results and conclusions presented herein are the original work of the author and the use of these tools was strictly limited to the optimization of the English-language expression.

Abstract

The increasing sophistication of Tactics, Techniques and Procedures (TTPs) poses a significant challenge to the security of critical infrastructure. While understanding these attack vectors is vital for developing robust defences, the empirical analysis of real-world cyber-attacks is fundamentally constrained by the sensitive and classified nature of breach data, rendering large-scale, real-time analysis of actual incidents becomes nearly impossible.

To address this gap, this research utilizes the NATO CCDCOE Locked Shields (LS) cyber defence exercises as a high-fidelity simulation environment to evaluate the effectiveness of attack TTPs and identify significant correlations across diverse system architectures and attack effectiveness. This study conducts an evaluation of the LS 2024 exercise, leveraging the largest known recorded dataset of successful attacks performed against multiple competing Blue Teams (BT). The research employs a granular analysis of "attack dimensions" (alternative name for TTPs) in relation to targeted environments, workstation configurations and assigned mission objectives. To facilitate the interpretation of these complex variables, a Business Intelligence (BI) reporting was developed for the tracking and visualization patterns of attack properties. This framework allows for the systematic assessment of attack success rates and damage levels across different exercise phases and defensive postures represented by BTs.

Furthermore, the study contextualizes these findings within established cybersecurity frameworks including MITRE ATT&CK, the Diamond Model and the Lockheed Martin Cyber Kill Chain, to ensure alignment with industry-standard taxonomies in the reasoning process. By analysing the encounters between Red Team (RT) manoeuvres and BT responses, this research provides a quantitative assessment of offensive effectiveness. The primary contribution of this work is the provision of analysis on a large-scale, structured dataset of simulated attack events, which supplements existing literature on TTPs and offers a scalable methodology for evaluating the resilience of critical infrastructure against evolving cyber threats.

This thesis is written in English and is 63 pages long, including 6 chapters, 25 figures and 0 table.

Keywords: Red Team, Blue Team, TTPs, MITRE ATT&CK, Cyber Exercise, Locked Shields, Critical Infrastructure, Cybersecurity, Business Intelligence, Attack Dimensions

Lühikokkuvõte

Rünnakutaktika, -meetodite ja -protseduuride (TTP) üha suurem keerukus kujutab endast olulist väljakutset kriitilise infrastruktuuri turvalisusele. Kuigi nende rünnakuvektorite mõistmine on tugeva kaitse väljatöötamiseks hädavajalik, piirab reaalmaailma küberrünnakute empiirilist analüüsi oluliselt rikkumisandmete tundlik ja salastatud iseloom, mis muudab tegelike intsidentide ulatusliku reaalajas analüüsi peaaegu võimatuks.

Selle lünga täitmiseks kasutab käesolev uurimus NATO CCDCOE Locked Shields (LS) küberkaitseõppusi kui kõrge täpsusega simulatsioonikeskkonda, et hinnata rünnakute TTP-de tõhusust ja tuvastada olulisi seoseid erinevate süsteemiarhitektuuride ja rünnakute tõhususe vahel. Käesolevas uuringus hinnatakse LS 2024 õppust, kasutades ära suurimat teadaolevat registreeritud andmekogumit edukate rünnakute kohta, mis on sooritatud mitme konkureeriva sinise meeskonna (Blue Team, BT) vastu. Uuringus kasutatakse „rünnakumõõtmete" (TTP-de alternatiivne nimetus) detailset analüüsi seoses sihtkeskkondade, tööjaamade konfiguratsioonide ja määratud missiooni eesmärkidega. Nende keeruliste muutujate tõlgendamise hõlbustamiseks töötati välja ärianalüüsi (BI) aruandlus rünnakute omaduste jälgimiseks ja visualiseerimiseks. See raamistik võimaldab süstemaatiliselt hinnata rünnakute edukust ja kahju taset erinevates harjutuse faasides ja BT-de esindatud kaitsepositsioonides.

Lisaks asetab uuring need tulemused konteksti väljakujunenud küberjulgeoleku raamistikesse, sealhulgas MITRE ATT&CK, Diamond Model ja Lockheed Martin Cyber Kill Chain, et tagada järelduste tegemisel kooskõla tööstusharu standarditega. Analüüsides Red Teami (RT) manöövrite ja BT vastuste kokkupõrkeid, pakub käesolev uurimus ründe tõhususe kvantitatiivset hinnangut. Selle töö peamine panus on analüüsi pakkumine simuleeritud rünnakute sündmuste ulatusliku ja struktureeritud andmekogumi kohta, mis täiendab olemasolevat kirjandust TTP-de kohta ja pakub skaleeritavat metoodikat kriitilise infrastruktuuri vastupidavuse hindamiseks arenevate küberohtude suhtes.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 63 leheküljel, 6 peatükki, 25 joonist, 0 tabelit.

Keywords: Red Team, Blue Team, TTP-d, MITRE ATT&CK, Küberharjutused, Locked Shields, Kriitiline infrastruktuur, Küberturvalisus, Äriandmete analüüs (BI), Rünnakumõõdikud

List of Abbreviations

BT – Blue Team

BI – Business Intelligence

CKC - Lockheed Martin's Cyber Kill Chain

CTI - Cyber Threat Intelligence

CI – Critical Infrastructure

DDoS - Distributed Denial-of-Service

ENISA – European Union Agency for Cybersecurity

EXCON - Exercise Control

GT – Green Team

KPI – Key Performance Indicators

LLM - Large language model

LS – Locked Shields

MISP - Malware Information Sharing Platform

MITRE ATT&CK - The Adversarial Tactics, Techniques, and Common Knowledge

NATO CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence

OT – Operational Technology

PRISMA - Preferred Reporting Items for Systematic Reviews and Meta-Analysis

ROE - Rules of engagement

RT – Red Team

SDO - STIX Domain Objects

STIX - Structured Threat Information Expression

TAXII - Trusted Automated Exchange of Intelligence Information

TTP - Tactics, Techniques and Procedures

TTTP - Tools and Tactics, Techniques and Procedures

YT – Yellow Team

Author’s contribution

The author's contribution is a novel analysis revealing the effectiveness of attacks performed by RT against varying defence configurations in a unified infrastructure multiple instances of the same targets. The developed analysis model provides insight into the attack’s effectiveness against different segments of Critical Infrastructure (CI) measured in succeeding attacks. The infrastructure discussed in this context includes both Information Technology (IT) and Operational Technology (OT) assets within a single environment. This work provides insight into both types of CI’s OT and IT attack events showing effectiveness of those multiple attack vectors.

The complementing aspects of the attack effectiveness measurement include the network-level attack layer as well as success rates of endpoints’ infections. All these components are integrated into the LS environment simulating a state-like organisation (see the network map presented on Figure 5). This setting provides a broad area for conducting, capturing, handling and mitigating multiple attack types. Presented analysis highlights attack effectiveness in each segment of attacked infrastructure which provides a highly realistic measurement of environment protection and adversarial offensive capabilities.

1 Introduction

1.1 Motivation

The desire and motivation behind this study stems from the need to enhance cybersecurity capabilities in the face of increasingly sophisticated and dynamic threats, particularly in the context of national defence and security. The tensions all around the globe are rising and number of cyberattacks is growing. Recent state only highlights the importance of cyber resilience in context of Critical Infrastructure (CI) [1]. Building an active capability to enhance the threat resilience landscape combined with an activate identification and mitigation of known system's weaknesses supplements the defensive as well as offensive security posture in recent state of affairs. The safety of continuous operations with available and usable infrastructure, particularly in unstable external geopolitical environment, may be supported by more advanced mitigation capabilities and threat recognition. This study aims to improve risk recognition, tracking and mitigation of potential exploitation arising from successful adversary tactics and techniques.

Collecting and showcasing linkages of close to real-life threats and ways they materialise in cyberspace may bring significant benefits for training and building expertise among cybersecurity professionals in landscape of deteriorating threats. More expertise leads to better security posture and ability to react. The universe where different threats are converged is LS exercise during which significant number of security specialists engage to concurrently shape and rule landscape of cyberattacks. The scale of mentioned event makes it the biggest known live-fire cyber exercise more than 40 international BTs from different countries defend the artificial CI against attacks from an opposing RT. The RT members are targeting the systems with notable number of attacks. The attackers are simulating complex, real-world scenarios by using realistic cyberattacks designs inspired by actual cyber conflicts [2].

The RT simulates a nation level threat actor. The RT's workflow is determined by the exercise execution plan which divides the campaign into different phases (where the final phase includes destruction and disruption of the systems as a unique element of RT operation) [3]. The collection of data representing executed attacks in each of phases enables research and recreation of the infrastructure's snapshot under attack. Event-driven data is being captured during active phase of attacks within the exercise environment and stored for ongoing analysis during and after exercises execution. The collected data can be used to

better understand Key Performance Indicators (KPI) and serve as a foundation for further analytical case studies.

The assessment of collected outcomes and registered properties of the attacks may provide valuable support for enhancing the overall security posture in the information processing industry. Furthermore, the evaluation of data may cover a wide range of detailed research problems driven by the scale of the event and number of attacks performed and should be investigated diligently.

Notably, the review of relevant successful attacks can provide significant value and has the potential to be applied in real-life scenarios, contributing to the mitigation of threats [4]. This contribution may potentially serve as a valuable entry point for further study and ultimately enhance the outcomes of cyber exercises representing a valuable part of the academic study contribution in RT effectiveness. Research addressing simulation and deployment of vulnerable solution for RT is already well established [5].

1.2 Problem Statement

The fundamental challenge in modern cybersecurity lies in the ability of BTs to fortify defensive postures within protected environments while being continuously challenged by an adversary. While the conceptual problem addressed in this thesis is contextualized within the scope of simulated LS exercises, the conclusions have potential applicability to broader cybersecurity operations. Although LS is a BT-focused exercise, the attacks performed provide a vital means of evaluating RT performance.

The objectives and observations derived from this research are intended to be applicable to RT decision-making scenarios where represented threat is similar to simulated one in LS and provide more realising utilization of findings with MITRE ATT&CK and AI capabilities [6, 7]. As a simulated event, Locked Shields provides a controlled, safe digital space that allows participants to practice and improve responses without real-world consequences. The 2024 edition of this annual exercise offered a unique opportunity for BTs to sharpen their defensive capabilities, providing a training experience which structure is detailed further in Chapter 2.

A significant complication in evaluating cyber defence is the complexity of tracking the TTTPs (Tactics, Techniques, Tools and Procedures) of Advanced Persistent Threats (APTs). Accurately mapping the specific tools used during an execution is a difficult task without direct adversarial insight or specific "fingerprint-like" patterns left in payloads. Given the limitation that tools cannot be easily tracked, this study assumes that only the behaviours and decision-making processes of the adversary expressed in attack tendencies, such as selected objectives will be considered [8]. Therefore, to avoid misconception, whenever the acronym "TTP" is used in this thesis, attention is drawn specifically to Tactics, Techniques and Procedures, omitting the "Tools" component.

To address this complexity, the analysis in this thesis attempts to correlate attack occurrences with specific TTPs at the identified attack level, following the attack registration process and detecting TTPs as a measurement of effectiveness KPI. The approach for studying attack patterns relies on recording detailed information regarding attack properties: the type of attack, the objective, the targeted infrastructure, the ID of the affected machine and the overall success of the attack campaign. These identified characteristics of a compromise may be tracked via KPIs specific to each BT, specifically measuring how many

attacks bypassed defences and which specific attack properties were the most successful in this subgroup.

These characteristics may be described by their associated TTPs, their targeted system groups or other effective evaluation metrics. Attacks with higher success rates serve as a credible source for reasoning why they bypassed applied defences. The modelling for this evaluation, using the collected dataset, will be conducted in accordance with industry best practices, such as the cross-referenced with existing MITRE framework and will be reviewed within this thesis to process attack characteristics in a systematic way [9].

The objective of this research is to conduct an assessment of an in-depth attack simulation and to build a comparative structure of evaluations to identify RT performance. The measurement of attack performance is well established in academic research for providing possible best practices for describing a mission [10]. A key focus is to assess the effectiveness of attacks imposed by adversary in withstanding of defences measured by the rate of successful breaches.

Effective defence requires a thorough understanding of real-world threat landscapes. Currently, a gap exists in the independent assessment of how the threat profile of a specific adversary interacts with various defence strategies within critical infrastructure. The Locked Shields exercise addresses this problem statement through highly complex simulations of RT attacks, designed to behave as state-sponsored APT actors. This simulated environment serves a dual purpose: it provides a setting for BTs to practice countering adversary attack campaigns and offers a framework for large-scale data collection, as detailed in Chapter 2. While the simulation's precision is limited by the extent to which real-world incidents are being used by the RT for threat profiling, the recorded data of introduced attacks remains highly valuable. This study addresses the research gap by analysing recorded data to evaluate the effectiveness of RT actions against the LS-protected systems shown in Figure 5.

The importance of this research is supported by existing literature, which notes: “Knowing the techniques, tactics and procedures of your adversaries in cyberspace can be a key to success, as it is often deemed that ‘the offense has the upper hand’” [11]. This thesis demonstrates the value of describing attack properties, such as TTPs, and shows how visualizing attack patterns against different defenders can build foundational outcomes. Furthermore, while recent studies have covered complementary cases of traditional

vulnerability scanning and penetration testing during red teaming, they conclude that "future research should delve into the optimal methodologies, cost-effective approaches and long-term impact of red teaming on cybersecurity" [12] , which aligns with the TTP analysis presented in this research.

The need for measuring the effectiveness of RT activities has been observed since 2004 [13]. To improve tracking, researchers recommend examining industry-wide indicators such as TTPs and Cyber Threat Information storages [14]. Finally, following attempts to combine the MITRE ATT&CK framework with red teaming exercises [15], this work provides a methodology for MITRE ATT&CK mapping (combining Scenario, Tools and Tactics with Behavioural Analysis) for the post-mortem analysis of continuous defence improvements. The outcomes highlight the potential for further automation through attack descriptions, tamper-proof data integrity and artificial intelligence examination, all of which will be challenged alongside the research questions in this assessment.

1.3 Research Questions

This section outlines the research questions that steer the focus throughout this thesis. A review of the existing literature revealed a gap in knowledge regarding cybersecurity operations. This chapter details the specific question formulated to address the gap in systematic evaluation of attacks across multiple defence scenarios, along with the recognition of the key pattern of success in outcomes created.

In this context the questions are focusing on evidence and results the attacks, threats and TTPs have on attacked systems and context in which they were possessed.

The evaluation of the research gap expressed in problem statement and Chapter 2 was formulated as a consecutive set of sub questions. The questions aim to answer whether the gap can be filled using the data generated in the LS exercise.

- RQ1: What are the most relevant cyber threat cycles for Critical Infrastructure (CI) sector?
- RQ2: How can threat cycles be linked to attacks happening during LS?
- RQ3: How effectively did the LS Red Team execute the attacks identified in the previous questions?

RQ: 3.1

- Were there differences of the identified attacks within one BT?

RQ 3.2:

- Were there differences of the identified attacks between different BTs?

RQ 3.3:

- Is available data enough to address sub question 3.1 and 3.2?

1.4 Novelty

The primary contribution of this thesis lies in the evaluation of TTPs (within a potential MITRE context [7]) to determine attack effectiveness. This study utilizes cyber exercises to demonstrate the applicability of the TTPs (and potentially MITRE framework) in understanding the effectiveness of adversaries, such as APTs (RT in LS context), by identifying unique TTPs as recognizable patterns of attack success. A fundamental goal of this work is to establish a necessary research context that provides a foundation for understanding successful attack patterns within the studied IT/OT systems.

This context enables a structured analysis and validation of successful attack datasets within identical environments, allowing for precise comparisons and direct answers to the defined research questions. Critically, the analysis of datasets from live-fire events, such as Locked Shields, which involve APT-level of attacks, can reveal compromise patterns applicable to specific categories of researched infrastructure and their respective sectors.

These patterns closely mirror real-world scenarios, as the outcomes should address similar threat levels and represent various severity levels across diverse defence setups (refer to the LS design in Chapter 2). This work distinguishes itself from prior, non-RT-focused research, which focused on evaluating TTP effectiveness relying solely on single point detection [16] (for more related work focus on Chapter 2).

The novelty of this research lies in the evaluation of live-fire scenarios through an extensive analysis of Blue Team (BT) defence activities and their performance during live attack exercises, specifically regarding the relevance of TTPs within a Red Teaming (RT) campaign. As no prior research has systematically linked attack techniques to threats across multiple concurrent BT defence approaches. This study demonstrates the maturity and effectiveness of existing attacks. By examining how different BTs defended against specific

attacks during various campaign stages, this research showcases the resilience properties associated with certain attacks and the effectiveness of attack strategies against BTs.

This research addresses the identified gap by evaluating the success rate of different TTPs measured via LS-defined characteristics and propose transposing them into the public known metrics such MITRE-defined TTP framework. To the extent that the available data permits, visualized analytics will be presented for specific infrastructure types in form of aggregates and charts. This process itself serves as a novelty in demonstrating RT effectiveness as aggregates by infrastructure type across numerous identical instances is out of ordinary for latest research. This approach enables a nuanced understanding of not only whether specific TTPs succeeded, but also the specific phase of the campaign in which that success occurred.

Finally, this research addresses a lack of existing analysis regarding datasets that record multiple simultaneous attacks targeting mirrored infrastructure instances from a unified RT perspective which could serve as research source collected from real incidents. While the data is designed to mimic real-world infrastructure in LS environment, as closely as possible despite being an artificial environment, the scope of this study enables a deeper evaluation of TTP usability and effectiveness across varying defence regimes for simulated APT and its capability, that has not been established in prior research.

2 Related work

2.1 Emerging Cybersecurity Threats in the Public Sector

In order to describe the emerging cybersecurity threats in public sector a definition of threat and risk needs to be establish. For this thesis we will use definition provided by NIST Special Publication 800-30.

Threat is “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.” [17]. Risk on the other hand is “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” [17].

The expanding digital footprint of the public sector and critical infrastructure has converged with a significant escalation in sophisticated cyber threats. Critical sector entities are now consistently targeted by persistent and adaptive threat actors who exploit a combination of technical weaknesses in systems and inherited vulnerabilities within organizational dependencies [18]. Based on historically faced cyberattacks, typically aligned with major events, research has been conducted to collect best practices for overseeing these attack conditions.

European Union Agency for Cybersecurity (ENISA) has attempted to define incidents originating from regular cyber incidents, specifically large-scale incidents and cyber crises [19]. Following this approach, recent classifications summarize the threat landscape [20] with updates presenting the 2024 landscape [21]. This report identifies ransomware as a primary threat requiring significant caution, followed by malware and social engineering. Furthermore, the report details threats targeting data and availability, including denial-of-service (DoS) attacks and highlights information manipulation as a significant concern. The 2024 forecasts also identify emerging trends such as "Living Off

Trusted Sites" (LOTS), where threat actors use trusted cloud services and legitimate platforms like Slack and Telegram to disguise Command and Control (C2) communications [21] and the advancement of "Living Off the Land" (LOTL) techniques to evade detection [21].

Research focusing on the public sector using the MITRE ATT&CK framework has identified tactics that demonstrate adversarial behaviour, drawing on INTERPOL findings from 2020. INTERPOL reported a significant shift in cybercriminal targets from individuals to major corporations, governments and critical infrastructure, driven by the rapid deployment of remote systems to support work-from-home requirements [22].

Within the public sector, critical infrastructure systems are often interdependent. This interconnectedness means that threat cycles can be co-dependent across different sectors, facilitating broader compromises. Analysis of US critical infrastructure has demonstrated this reliance, specifically between water and wastewater systems, communication, emergency services and both food and agriculture systems [23]. This interdependence is also evident at the EU level, where the European Directive on the protection of critical infrastructure establishes a framework for identifying and protecting these interconnected systems to enhance security [24].

The European Repository of Cyber Incidents (EuRepoC) reports that since 2024, state institutions and political systems have been the most common targets [25]. The EuRepoC dashboard (Figure 1) provides a data-driven overview of the strategic targeting of critical infrastructure, recording 830 incidents across CI and state organizations, representing 43.61% of registered attacks. From January 1, 2024, to March 17, 2025, civil service and administration was the most targeted component. Similarly, the IC3 report highlights the scale of successful penetrations, noting that 14 of 16 critical infrastructure sectors experienced at least one ransomware attack in 2023 [26].

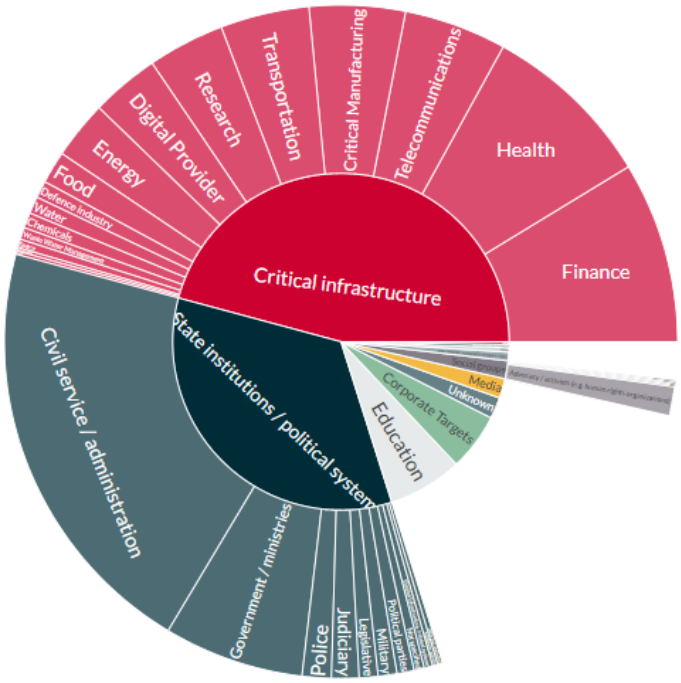

Figure 1. EuRepoC Dashboard presenting most common sector of cyberattacks [27]

Furthermore, CISA alerted owners of OT assets to strengthen defences against rising ransomware threats, noting that the connection between OT and IT networks makes them lucrative targets [52, 53]. The failure of CI affects not only financial aspects but also four key dimensions: safety, mission, business and security [28]. Regarding infrastructure types, Supervisory Control and Data Acquisition (SCADA) systems face distinct attack vectors while sharing generic properties with Industrial Control Systems (ICS) and OT infrastructure [29]. Research utilizing the Conpot honeypot to simulate industrial protocols (Modbus, S7comm, BACnet) shows that adversaries express notable interest in these targets through high volumes of attack attempts [30].

The SANS Survey (2023) aligns with ENISA's findings, identifying phishing, correspondence takeover, ransomware, malware and zero-day attacks as the top five threats [31]. Among the most damaging attacks, ransomware targeting heavy industry, information services and government infrastructure remains a primary concern, where hijacked data is held for ransom [32]. Additionally, Distributed Denial-of-Service (DDoS) attacks against vital infrastructure servers often serve as a distraction for more intrusive actions. Notable real-world campaigns include NotPetya and Ryuk [33]. Furthermore, compromised public-facing web platforms allow adversaries to inject malicious content and manipulate

information [19] [20], a trend noted in the Australian Signals Directorate's review of critical infrastructure [34]. Finally, nation-state actors or their proxies are increasingly targeting Industrial Control Systems serving as the backbone of energy, transport, water and utilize complex supply chain attacks, as exemplified by the SolarWinds breach [35] [36] [37].

2.2 The Attack Lifecycle and Threat Cycle

The attack lifecycle can be observed at the operational level when an attack begins or based on a threat profile's definition and the circumstances in which a specific attack is expected based on Cyber Threat Intelligence (CTI) prediction [37]. Multiple attempts to launch an attack may be performed. The probability and statistical approach are applicable to any events in a defined space, even if perceived as random [38]. The attack environment, the mission's thoughtfulness and the threat profile provide qualitative factors that affect the statistical likelihood of successive occurrences of attack [38] [39].

The scope of defacement attacks defined as the modification or destruction of critical data reveals a presence of an adversary and verify situational awareness of BTs and recognition of IOCs BT can monitor. In contrast, actions such as data exfiltration represent broader tactics, involving the extraction of sensitive information which can lead to lateral movement and expanded access. This access can be secured by RT to establish a long-term presence, followed by privilege escalation (e.g. gaining root-level access) for espionage and code execution. These tactics and techniques showcase how a threat can be systematized into a repeating cycle. To precisely define a threat cycle, a set of attack instructions must be summarized into a record of activities leading to an objective. Threat design considers the weaknesses of target infrastructure and possible access paths, where combined with correct targeting, vulnerability recognitions, functional communication monitoring and capturing secrets designed with mature assessment together satisfy a STRIDE, PASTA or CVSS threat modelling methods [40] [41].

Latest research proves successful approaches in semi-automated detection of incidents if complemented by human-cognition together with indicators of compromise [42]. Of course, the element of polymorphic threat acts a significant role in threat's detection, its precision and recall of the actual estimate [43]. The most utilized long term threat cycle prediction methods are performed by the subject matter experts supported with its judgments for proactive forecasting of threats [44] [45]. Defence measures implemented for incident

response and short-term predictive modelling within the protected infrastructure are driven by alerting and detection heatmaps. [45]. The definition of the detection mechanisms may be performed both based on risk assessment or correct threat cycle definition combined with ability to recognize the phase of incident in response lifecycle [46]. The "threat cycle" refers to the overall process of threat materialization, including actors, vectors and repetitive action for threat classification, its order and intensity [40]. The definition of a threat cycle is a model that traces the evolution and adoption of threats over time based on data-driven research [41]. In the context of above definition an assessment of the polymorphic malware in threat cycle detection context is essential to understand limitation and recent challenges. The polymorphic threat express properties of change with every replication [47]. As most detection systems are signature-based the polymorphic activities are invisible for unknown signatures thanks to technics as dynamic encryption schemas, code obfuscation or code insertions [48]. The latest research is showing success rate of detection between 68.75% to 81.25% [49]. Figure 2 represents an example of a threat cycle and a forecast of its developments [41].

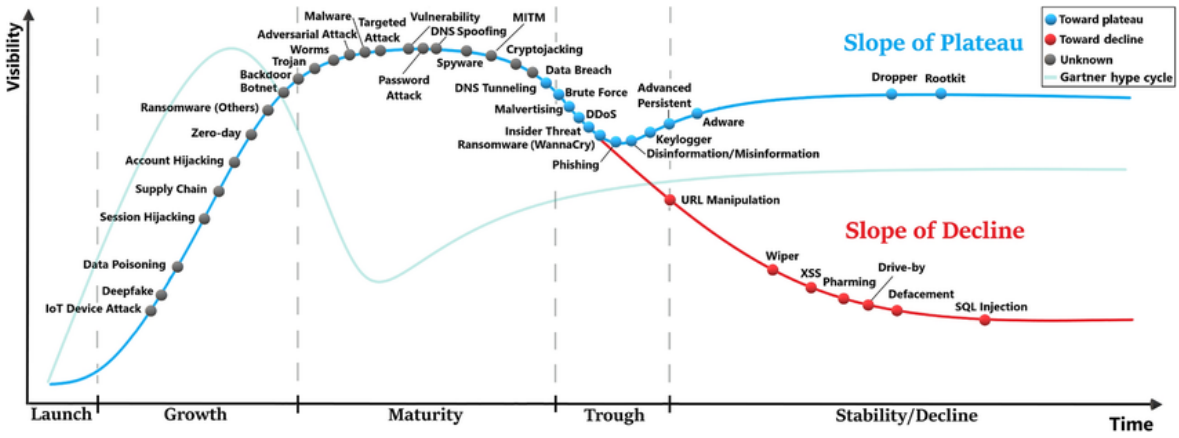

Figure 2. Example of threat cycle and general Gartner hype cycle comparison [41]

2.3 Tactics, Techniques and Procedures (TTPs)

To precisely define a threat cycle, attack instructions must be aggregated into a procedure level, where the order of techniques and tactics defines a single procedure. In formal recording, the MITRE ATT&CK framework defines potential TTPs applicable to any scenario. A threat may have a general objective, but its achievement is divided into sections addressing specific tactics. For example:

- *"Phase 1: Reconnaissance (TA0043)*
    - *Objective: Gather information about the target organization's infrastructure, systems and personnel.*
        - *MITRE Tactics: Reconnaissance.*
        - *MITRE Techniques:*
            - *T1589 - Domain Collection: Identify public-facing web domains, DNS records, and associated subdomains. (Vector: Passive OSINT)*
            - *T1590 - Active Reconnaissance: Utilize network scanning tools (Nmap, Shodan) to identify open ports, services, and ICS devices. (Vector: Network Scanning)*
            - *T1587 - Develop Capabilities: Identify vulnerabilities on web applications and ICS systems by leveraging public vulnerability databases (NVD, Exploit-DB). (Vector: Vulnerability Research)*
            - *T1189 - Drive-by Compromise: Identify publicly accessible web servers with vulnerabilities to serve malware to visiting users. (Vector: Web Application Exploitation)*
    - *Indicators of Compromise (IOCs): Anomalous DNS requests, increased network scanning activity, probing of ICS protocols (Modbus, DNP3).* [50]*".*

TTPs serve as the foundation for describing and grouping incidents, revealing the broader context of the threat cycle. While the primary objective is the "tactic," the "technique" describes the specific action. Furthermore, the tools used to implement a technique may be identified, though this is not explicitly mandatory in the MITRE ATT&CK framework. Techniques are implemented as a sequence of procedures.

When investigating attack frameworks, three industry-recognized solutions are prominent: the MITRE ATT&CK framework [51], Lockheed Martin's Cyber Kill Chain (CKC) [52] and the Diamond Model [53]. A comparative study from the 2022 IEEE International Symposium on Systems Engineering reviewed the dilemma of selecting suitable frameworks [54]. The findings suggest that MITRE ATT&CK is the most appropriate choice for cyberoperation (like for example Locked Shields) due to its comprehensive knowledge base and support for building attack chains [54]. The MITRE ATT&CK framework structures tactics and techniques in the form of a matrix, systematizing unique elements to facilitate visual analysis [50]. Furthermore, the MITRE ATT&CK Navigator exists to enable the efficient browsing of multiple TTPs and to assist in more streamlined attack planning [55].

In contrast, the Lockheed Martin CKC adopts a defence-oriented perspective, emphasizing the steps an attacker takes to compromise a system. While it provides a typical explanation of phases, it often lacks unique identifiers for mitigating modern threats. Its primary strength is a human-centric approach, but it has faced criticism for its difficulty in tracking modern, non-standardized adversary actions [54]. The Diamond Model takes a mathematical approach using clustering, classification and game theory [54]. While useful, its complexity makes it difficult to apply in real-world scenarios compared to the actionable, enumerated approach of MITRE ATT&CK [56] [50].

For building a repository of data, the STIX (Structured Threat Information Expression) format is used to exchange CTI. This serialization creates STIX Domain Objects (SDO) describing adversarial actions and their relationships [57]. Example SDO represented in JSON format on Figure 3 [57].

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:23.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the financial services sector."
}
```


Figure 3. MITRE's STIX Domain Objects record

MITRE ATT&CK Collections are built from these objects, with reference properties shared in a sharable form as shown below on Figure 4 [58].

```
{
 "id": "x-mitre-collection--402e24b4-436e-4936-b19b-2038648f489",
"type": "x-mitre-collection",
"spec_version": "2.1",
"x_mitre_attack_spec_version": "2.1.0",
"name": "Enterprise ATT&CK",
"x_mitre_version": "6.2",
"description": "Version 6.2 of the Enterprise ATT&CK dataset",
"created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"created": "2018-10-17T00:14:20.652Z",
"modified": "2019-10-11T19:30:42.406Z",
"object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
],
"x_mitre_contents": [
    {
        "object_ref": "attack-pattern--01a5a209-b94c-450b-b7f9-946497d91055",
        "object_modified": "2019-07-17T20:04:40.297Z"
    },
    {
        "object_ref": "relationship--0024d82d-97ea-4dc5-81a1-8738862e1f3b",
        "object_modified": "2019-04-24T23:59:16.298Z"
    },
    {
        "object_ref": "intrusion-set--090242d7-73fc-4738-af68-20162f7a5aae",
        "object_modified": "2019-03-22T14:21:19.419Z"
    }
```


Figure 4. MITRE Collections built from ATT&CK objects

The repository of objects in line with MITRE ATT&CK guideline is called “ATT&CK Data Model (ADM) and is a TypeScript library that provides a structured way to interact with MITRE ATT&CK datasets. It uses Zod schemas, TypeScript types and ES6 classes to create a type-safe, object-oriented interface for navigating the ATT&CK data model. This

library is designed to parse, validate and serialize STIX 2.1 formatted content, making it easy to work with ATT&CK-related data in a programmatic and intuitive way.” [59].

The exchange of structured CTI is also possible thanks to Trusted Automated Exchange of Intelligence Information (TAXII). TAXII utilizes all previously described components and brings [59] “an application protocol for exchanging CTI over HTTPS. The ATT&CK TAXII server provides API access to the ATT&CK STIX knowledge base.”

2.4 Cyber Defence Exercises and Locked Shields

The foundation of Locked Shields (LS) was launched in 2010 by the CCDCOE in Tallinn, Estonia as the "Baltic Cyber Shield" [3] [60]. The primary goal is to enable cybersecurity experts to enhance their skills in defending national IT systems. LS represents the largest state-of-the-art example of cyber resilience exercises, where competing BTs must secure pre-built networks of fictional organizations [61]. The infrastructure serves as a playground where the effectiveness of defensive strategies is measured. For example, the 2024 exercise involved 6,866 virtualized systems where they were subject to over 10000 objectives real-time attacks, involving more than 4,000 participants [62] from more than 40 nations. [63]

The deployed infrastructure serves as a battlefield where the RT attempts to simulate APT in cyber warfare to compromise defender systems. The network setup includes various "Special Systems" simulating Critical Infrastructure such as 5G, satellite, air defence, gas and electricity networks. The environment allows the RT to execute missions aiming to reach the centre of the BTs' controlled environments. A fundamental design requirement of the LS is the implementation of a 'vulnerable-by-design' architecture, which enables participants to operate within exploitable systems across multiple attack vectors.

The exercise involves several key roles inspired by ISACA standards [64] [65] [66] [67]:

- Red Team (RT): Simulates an adversary, planning TTP-based campaigns to exploit vulnerabilities and maximize damage within the Rules of Engagement (ROE). RT task is to provide an adversarial pressure defined as a constant (or incrementally growing) aggregate of successful attacks achieved within each phase of the LS exercises.

- Blue Team (BT): Protects dedicated, equal segments of infrastructure and applies countermeasures.
- White Team (WT): Coordinates the exercise, simulating the User Simulation Team (UST) and the Legal Team.
- Yellow Team (YT): Tracks situation awareness in entire environment.
- Green Team (GT): Maintains the infrastructure and ensures high-quality automation [68].

The LS 2024 exercise focused on attacks that reflect genuine real-world threats in simulated environment. The EXPO tool is the central system used by all teams (RT, BT, GT, WT, YT) to coordinate the exercise, track attacks and present scores [GT leader sourced]. The RT uses EXPO to structure and describe attacks, while the GT uses it for operational awareness.

The infrastructure evaluated in LS 2024 is divided into subdomains representing a fictional state-like organization: BAF (Armed Forces), BEG (Energy Group) and BGP (Banking Sector). The attack layers are categorized as:

- Web (WEB): Web interfaces.
- Network (NET): Attacks against "Special Systems" or Critical Infrastructure (CI).
- Client Side (CS): Attacks against user workstations and endpoints.

On the Figure 5 we can see segments of network and machines deployed within those segments. Each segment is called a “Special System” and is simulating different type of CI. It is worth noting that systems designed for LS execution are intended to have architecture flaws implemented to enable a more dynamic training experience for BTs

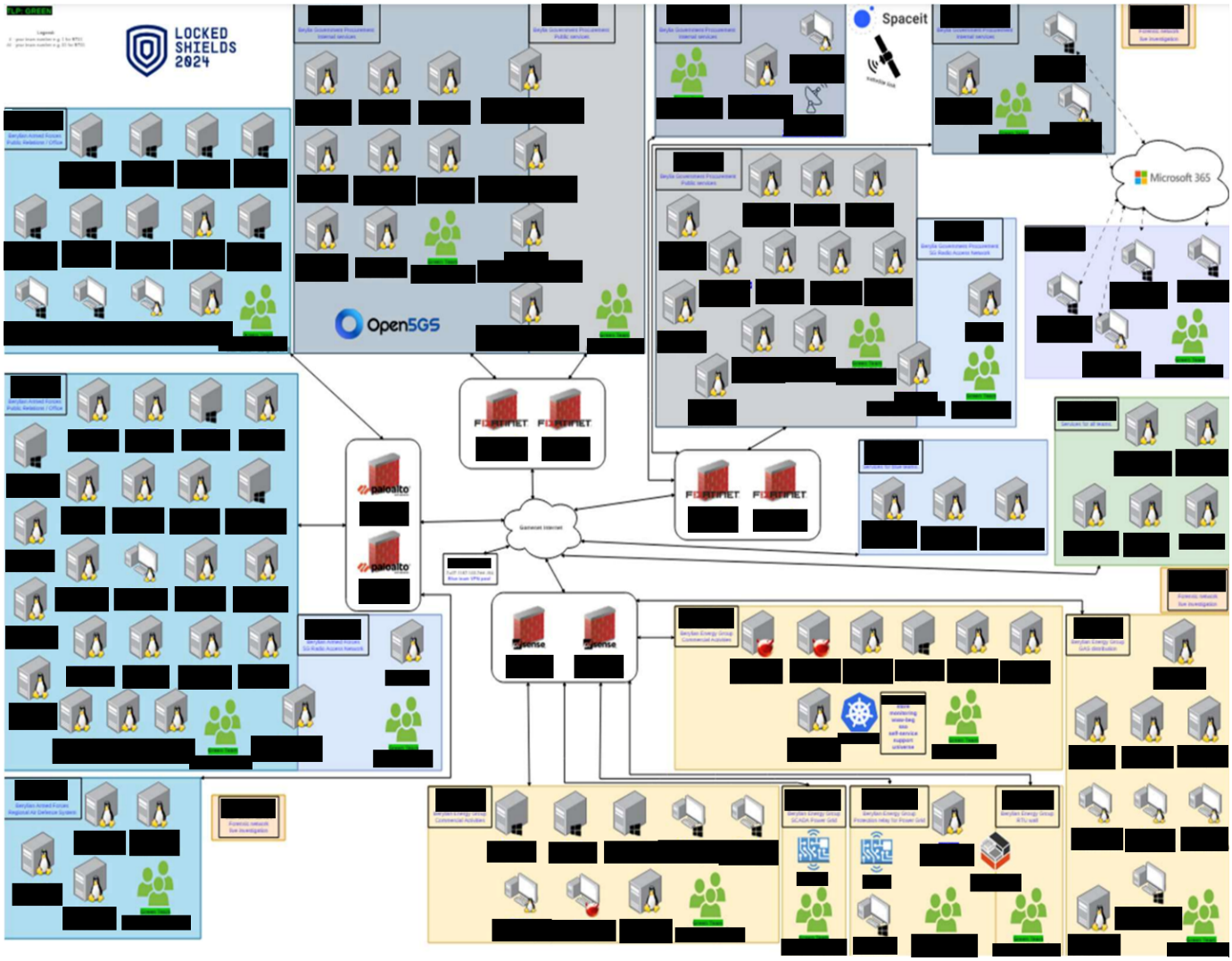

Figure 5. Network map of Locked Shields 2024 [63]

3 Methodology

3.1 Research Design and Strategy

This research employs a systematic methodology guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, followed by a snowballing approach. The aim is to evaluate existing literature on the relationship between relevant threat cycles for public sector domains and Locked Shields exercises. The review includes studies published between 2014 and 2025, focusing on cyber exercises, the MITRE ATT&CK framework, TTPs, threat cycles and critical infrastructure.

The systematic search utilized databases such as Elicit, ResearchGate, Google Scholar and ScienceDirect. Out of 95 identified articles, 35 met the inclusion criteria, demonstrating support for cyber exercise and TTPs analytics in offensive cyber capabilities context. For the remaining sources, a snowballing strategy was utilized to ensure transparency and context consistency.

This research aims to identify the factors influencing attack effectiveness and, consequently, the RT performance in executing threats. Using the attacks performed during the LS 2024 exercise as a foundation, this study provides a comprehensive evaluation of the RT against multiple defences within a system designed to be vulnerable. The study examines the BT efforts to defend against all threat types, including zero-day attacks, within a secure, simulated environment that simulates CI.

3.2 Data Sources and EXPO System

The primary data source is the LS 2024 dataset, provided by NATO CCDCOE‘s representatives. The correctness of dataset was approved by NATO CCDCOE. The research focuses on the EXPO system, the central coordination tool for all participants. EXPO facilitates user communication, scoring and operational awareness.

The collected EXPO dataset export consists of two .json files:

- File with a description of all performed attacks (see Figure 7).

- File with a set of data addressing attack types based on an objective and short description of actions “attack dimension” (see Figure 6).

EXPO is used for BTs to communicate with Exercise Control (EXCON) which serves as function coordinating the flow of exercises during execution time. The EXPO is also a generic system serving as a core of communication between participating parties as the secondary duty. The BT can communicate with its users assigned within the UST. Within the same time RT places information about the attacks to EXPO during each phase. All features combined creates a complex tool designed for exercise coordination.

The following findings about the way exercises are build and function were collected by author during participation as UST member in LS 2024 and later evaluated with support and verification during cooperation process with NATO CCDCOE’s representatives as an addition to dataset design discussions itself. During processing the dataset and conducting research a significant limitation was identified that the EXPO system reports phase of an attack but lacks the sequential context or the precise TTP-level description in details required for multidimensional analysis of combine technique and tactic. The information about the attack's function is present, however presented “attack dimesion” description does not explicitly describe the hierarchy of TTPs (described in more detailed in limitation section).

The detailed event logs from EXPO facilitate threat intelligence recognition and the monitoring of offensive execution. By analysing TTP effectiveness across different system categories (NET, WEB, CS) and IT/OT infrastructures, we can refine targeting strategies to maximize campaign success rates and identify the most resilient infrastructure types.

Below an example of EXPO recorded attack detail’s structure in json format entry, describing attack dimension, is shown:

```
{"_id":{"$oid":"21xxxxxxxxxxxxxx1"},
"expo_id":"AD-NETWORK-IPV4IPV6_DIRECT",
"name":"IPv4/IPv6 direct",
"description":"Direct IPv4 or IPV6 access to the target was possible from the
attacker's machine located in SINET",
"type":"network",
"categories":["Attacks_NET"],
"objectives":["hijack_bgp"], "__v":0}
```


Figure 6. Record of RT's attack details structure in EXPO

That is followed by the entry describing started and successfully completed attacks with its all know properties:


```
{
    "_id": "21xxxxxxxxxxxxxx1",
    "expo_id": "ATAC-N-P0-ws1_baf-compromise",
    "status": "STARTED",
    "category": "Attacks_CS",
    "phase": "0",
    "attack_dimensions": []
  }
```


Figure 7. Record of a RT attack event in EXPO

As it may be noticed, outside of information where attack is targeted, which phase it occurred no specific TTP identifier is given. All analytics needs to be based on the attack dimension's description providing summarized insight what happened. The BI model

derivate from mentioned json files' structure looks as on Figure 8 (Appendix 2 also contains model visualising both EXPO and MITRE defined data)

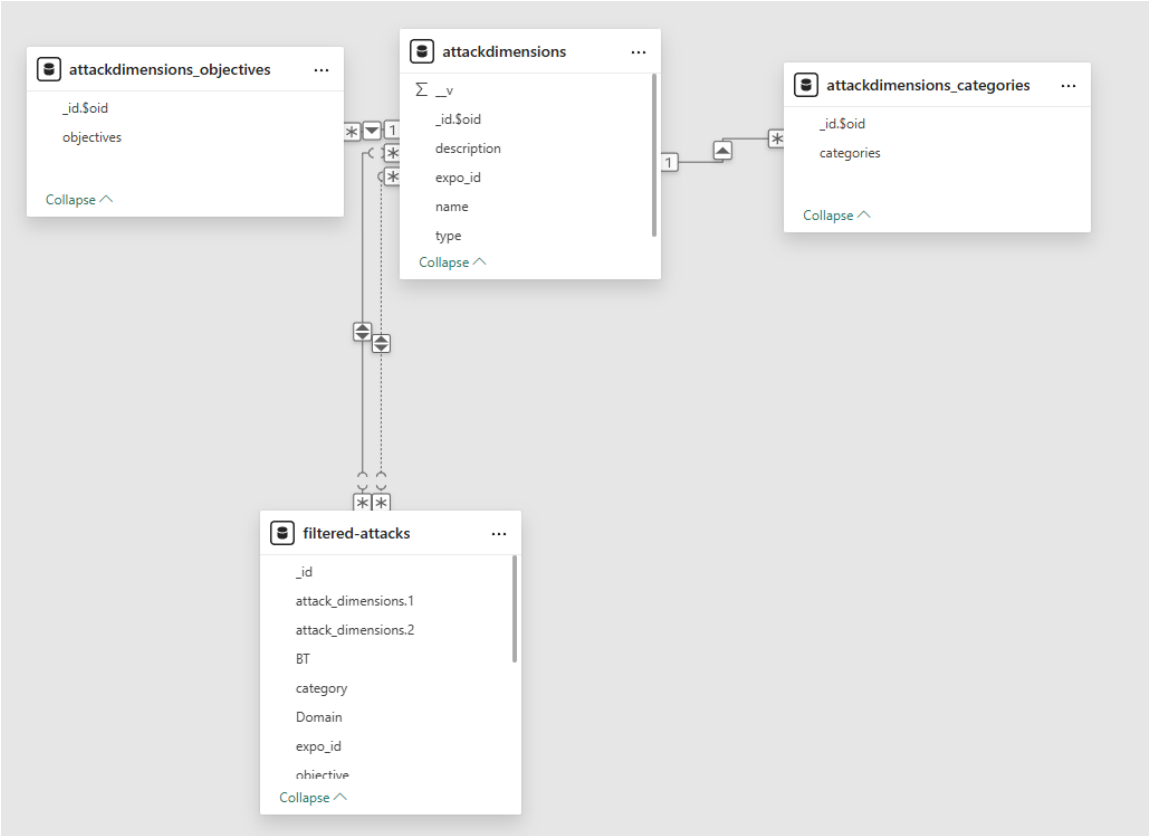

Figure 8. The core of EXPO data model

3.3 Data Engineering and Business Intelligence

The limitation of available data and its possible substitution in the context of threats will be evaluated. During consultations with GT's representatives, numerous data structures were analysed to identify the most detailed way to describe TTPs in LS24 from existing sources. The design of LS was possibly the best reflection of a close to real-world execution of adversarial activities, excluding real APT missions. Existing LS assets provided multiple datasets, supplying comprehensive logging, monitoring and tracking duties. Within the existing setup, multiple solutions such as Kafka, Malware Information Sharing Platform (MISP) and Cobalt Strike were evaluated and considered for the extraction of high TTP-relevance data with GT's representative concluding that EXPO will be the most suitable dataset for analysis of TTPs.

The methodology involves performing data engineering and data processing actions on raw datasets in order to enable querying and aggregating dataset. Once the data might be visualized and research may be performed on effectiveness of attack the goal is provide analysis addressing research question. Followed by possible addressing of existing identified limitations. Ideal outcome would provide the EXPO "attack dimensions" data as multidimensional construct similar to the MITRE ATT&CK framework to enable comparing capabilities between threats captured as STIX objects. The EXPO system and the MITRE framework both provide a solid foundation for analysing attack data, but the new Business Intelligence (BI) capabilities created in this research will enable a more detailed understanding of the relationships between EXPO information on different components of infrastructure, especially if each attack could be described by unique tactic and technique. Even if LS is fully simulated environment the simulated APT creates real threat to simulated infrastructure which may potentially share some patterns with real APT and in future effectiveness of LS RT may be assessed also by comparisons on existing non-simulated TTPs.

The research plan involves an ex post facto examination of data relationships, qualitative occurrences and the effectiveness of target compromises. To achieve this, BI visualizing reporting outcomes will be crafted, utilizing the described data structure to emphasize data meanings defining TTPs uniquely. The BI report, presenting different dataset perspectives, will be prepared and its outcomes presenting EXPO data will be presented in Chapter 4 to provide better insight into effectiveness and answer the research questions. (The diagram for the BI data model is visible in Appendix 2).

3.4 Data Processing and Augmentation

3.4.1 Manual Anonymization of EXPO dataset

Given the specificity of the dataset and the fragility of the processed information, a decision was made to anonymize the BT affiliations. The "expo_id" field, which originally stored the BT number, was modified to include a random letter corresponding to each BT to protect the identity of the participating teams and prevent breaches of confidentiality. The process of anonymization was performed with usage of regular expressions and manually verified to ensure the relationships between different components were preserved.

Moreover, this allows for the assessment of whether attacks correspond well to the CI and whether the simulation of these threats is a valid approximation of real-world scenarios without mentioning origin of participating BTs.

3.4.2 LLM-based Translation

To bridge the gap between generic EXPO attack dimensions and precise MITRE ATT&CK nomenclature, this research explores the use of Large Language Models (LLMs). The experiment was conducted using the Llama 3.3 70B model in quantization Q4_K_M with 70.6 billion parameters as a dense baseline for inference to generate a translation matrix via text input/output [69]. The LLM was equipped with TTP context, loaded with a Knowledge Base (KB) consisting of MITRE's techniques and tactics (version 16.1) [50] [72]. The process involved:

- using XLSX files from the official MITRE repository as raw data input for the script (see Appendix 3 and 4).
- using scripts to query the LLM to complement EXPO attack descriptions with specific MITRE tactics and techniques.
- performing backwards analysis via regular expressions and textual analysis of the output to ensure the validity of the proposed correlations.

The LLM output can be seen in Appendix 5. This approach aims to demonstrate how a structured, AI-augmented approach can enrich the EXPO dataset, providing the granularity needed to correlate simulated attacks on specific technique/tactic level. Additionally, it is worth noting that BI built in the course of this thesis if fully compatible both with EXPO's attack dimension and MITRE's TTPs. Results will also address if EXPO dataset is rich in attack context to extend to describe TTP in a unique manner.

4 Analysis

Building upon the principles of data engineering, the processing steps developed in Chapter 4 transform the collected dataset to enable the reporting of attack properties gathered in EXPO. Data analysis has become an essential tool for businesses, organizations and individuals to make informed decisions and to more precisely monitor progress and identify weaknesses [70].

The same principle applies to RTs and the tracking of attack effectiveness. Evaluating attacks subjects RTs to the same decision-driven data analysis as other industrial entities, albeit within an offensive context. This process is critical, as it provides valuable insights by learning from registered attacks to identify the factors and parameters that support successful attack execution. The structural complexity of cyber exercises, such as LS, and the high volume of attacks performed necessitate the dynamic visualization of progressing events. Monitoring recent resilience posture and the time constraints regarding its erosion are vital factors for evaluating RT effectiveness and planning escalation [71].

Given these circumstances, the following chapter presents a data-driven evaluation of applied attack techniques. This process acknowledges the constantly growing set of possible offenses that must be converted into actionable intelligence, necessitating the dynamic visualization of ongoing changes during the simulation of RT attacks. Aggregated visual reporting helps answer research questions concerning LS infrastructure and RT by enabling the tracking of the condition of specific BTs and attack advancement during and after the mission execution process. This information provides situational awareness and highlights the techniques that most effectively target specific system types for particular BTs or groups of BTs within the LS environment. Furthermore, tracking effectiveness and drawing conclusions regarding TTP successes results in more descriptive TTP attack chains. When integrated with the dynamic analysis of attack patterns, system categories, phases and specific BT builds, these descriptive TTPs provide continuous insight into the RT's mission state and advancement, potentially correlating specific TTPs with BTs that were unable to defend against them.

The following section utilizes Power BI visualizations to present answers to the stated research questions. Power BI facilitates the creation of interactive and dynamic BI reports, enabling the effective analysis and visualization of large-scale datasets. In this study, EXPO

attack records serve as the foundation for constructing an attack success registry, which encapsulates the granular details of the attack process. This reporting framework supports data-driven decision-making and provides insights into the various attack phases executed during the Locked Shields exercises. Furthermore, this reporting method assists in identifying trends, patterns and correlations within the data. The findings from the TTP comparison are evaluated in this chapter using the BI dashboards developed for this analysis. Technical implementation details, such as DAX formulas and Power Query transformations, together with created data model diagram are provided in Appendices 1 and 2.

4.1 Attacks performance against BT's infrastructure

The fundamental metric for quantifying the performance of attacks against established defences is the success rate achieved by the RT on specific BT infrastructures during the exercise. This success rate illustrates the progressive erosion of defences and the increasing exposure to adversary activities throughout the exercise phases. Given that the entry point of the exercise provides identical infrastructure for each BT and the initial attack path of the RT in Phase 1 is standardized, the defensive methodology further shapes the RT's campaign posture and the CI's resilience; therefore, any variation in the effectiveness of these techniques is directly attributable to the specific BTs, provided that performance between BTs varies.

Figure 9 illustrates the breakdown of completed attacks following the final exercise phase. The success rate ranges from 5.8% to 44.9%, despite the RT executes identical objectives and missions on the same infrastructure for every BT. This disparity implies that the primary variable is the BT's defensive design and incident response strategy. Consequently, identifying patterns within the most effective TTPs (specifically those that cause the greatest impact on BTs) is a critical focus of this analysis. A successful attack is defined by the compromise of the targeted system and the achievement of the RT objective (the objective structure is illustrated in Figure 13). As demonstrated in the datasets shown below (Figures 11 to 12), the degree of unmitigated vulnerability and exposure across all maintained systems represents the ultimate measure of RT success relative to BT resilience under successful attack. Moreover, the distribution of attack success according to the described measure provides a primary KPI for analysing RT effectiveness.

Blue Team	Successful attacks	%Success rate
D	339	44,90%
I	338	44,77%
R	246	32,58%
K	206	27,28%
H	183	24,24%
C	162	21,46%
G	144	19,10%
B	143	18,94%
E	128	16,95%
M	126	16,69%
L	121	16,05%
A	121	16,03%
F	119	15,76%
Q	108	14,30%
O	92	12,19%
P	70	9,28%
J	55	7,28%
N	44	5,83%

Figure 9. Attack success rate per BT

Figure 10 below expands the previously analysed dataset by the category of attacked systems. The context of the affected systems provides additional information regarding RT effectiveness toward different technologies defended by various BTs. In this view, it can be observed that there is a spike in the attack success rate for certain BTs. The highest success rates were observed within the CS category for teams D and I, respectively (73.17% and 64.02%), while the most resilient team maintained 16.46% within this category. For the special systems in the NET category, the RT's most effective attacks secured approximately 40.50% of successful attacks, in comparison to the least successful campaign, which was 7.44%. Moreover, in the WEB category, the most effective RT campaign resulted in 42.77% of successful attacks in comparison to the least successful one, at a rate of 2.34% (for teams I and N, respectively).

Blue Team	Category	Successful attacks	%Success rate
A	Attacks_CS	25	15,24%
A	Attacks_NET	17	14,05%
A	Attacks_WEB	79	16,81%
B	Attacks_CS	53	32,32%
B	Attacks_NET	18	14,88%
B	Attacks_WEB	72	15,32%
C	Attacks_CS	43	26,22%
C	Attacks_NET	22	18,18%
C	Attacks_WEB	97	20,64%
D	Attacks_CS	120	73,17%
D	Attacks_NET	49	40,50%
D	Attacks_WEB	170	36,17%
E	Attacks_CS	40	24,39%
E	Attacks_NET	10	8,26%
E	Attacks_WEB	78	16,60%
F	Attacks_CS	34	20,73%
F	Attacks_NET	9	7,44%
F	Attacks_WEB	76	16,17%
G	Attacks_CS	41	25,00%
G	Attacks_NET	22	18,18%
G	Attacks_WEB	81	17,27%
H	Attacks_CS	51	31,10%
H	Attacks_NET	13	10,74%
H	Attacks_WEB	119	25,32%
I	Attacks_CS	105	64,02%
I	Attacks_NET	32	26,45%
I	Attacks_WEB	201	42,77%
J	Attacks_CS	22	13,41%
J	Attacks_NET	9	7,44%
J	Attacks_WEB	24	5,11%
K	Attacks_CS	38	23,17%
K	Attacks_NET	25	20,66%
K	Attacks_WEB	143	30,43%
L	Attacks_CS	27	16,46%
L	Attacks_NET	15	12,40%
L	Attacks_WEB	79	16,84%
M	Attacks_CS	45	27,44%
M	Attacks_NET	21	17,36%
M	Attacks_WEB	60	12,77%
N	Attacks_CS	23	14,02%
N	Attacks_NET	10	8,26%
N	Attacks_WEB	11	2,34%
O	Attacks_CS	15	9,15%
O	Attacks_NET	10	8,26%
O	Attacks_WEB	67	14,26%
P	Attacks_CS	28	17,07%
P	Attacks_NET	8	6,61%
P	Attacks_WEB	34	7,25%
Q	Attacks_CS	17	10,37%
Q	Attacks_NET	14	11,57%
Q	Attacks_WEB	77	16,38%
R	Attacks_CS	50	30,49%
R	Attacks_NET	25	20,66%
R	Attacks_WEB	171	36,38%

Figure 10. Attack success rate based on system category type

The BI capability to visualize the state of applied defences, its erosion and the types of attacks performed during LS for selected BTs is presented in the following section. This analysis focuses on phase constraints and the status of attacks during execution phases, utilizing the attack success rate as a KPI to track performance over time.

Aggregating attack dimensions by BT enables an evaluation of whether RT performance against a specific BT is due to a well-designed attack or a deficiency in the implemented defences. If a high number of successful attacks within a specific dimension is distributed equally across various BTs, it ensures that the RT attack was objectively effective.

The primary objective of Figure 11 is to demonstrate which system type was most frequently compromised. The presented view aggregates the progress of four attack phases and represents their final stages. An additional feature of this view is the ability to switch between started, under-review and successfully completed attacks, all aggregated and summarized by LS phase. This functionality is useful for real-time analysis during data loading, allowing mission control to track open attack classes or teams, which can be adjusted to align with mission objectives. Additionally, the temporal phase can be layered and accumulated onto the measured attributes and subsequent behaviours.

An aggregate screening of all BT engagements reveals that web-based systems constitute the most penetrated attack layer, accounting for 59.7% of all successfully completed attacks. This occurred within a setting where each subsequent phase represented a steady number of completed attacks. Given the various defence setups and the nonlinear performance across different system categories within the BT responsibility, the WEB category emerges as the primary exposure layer for conducting red teaming engagements.

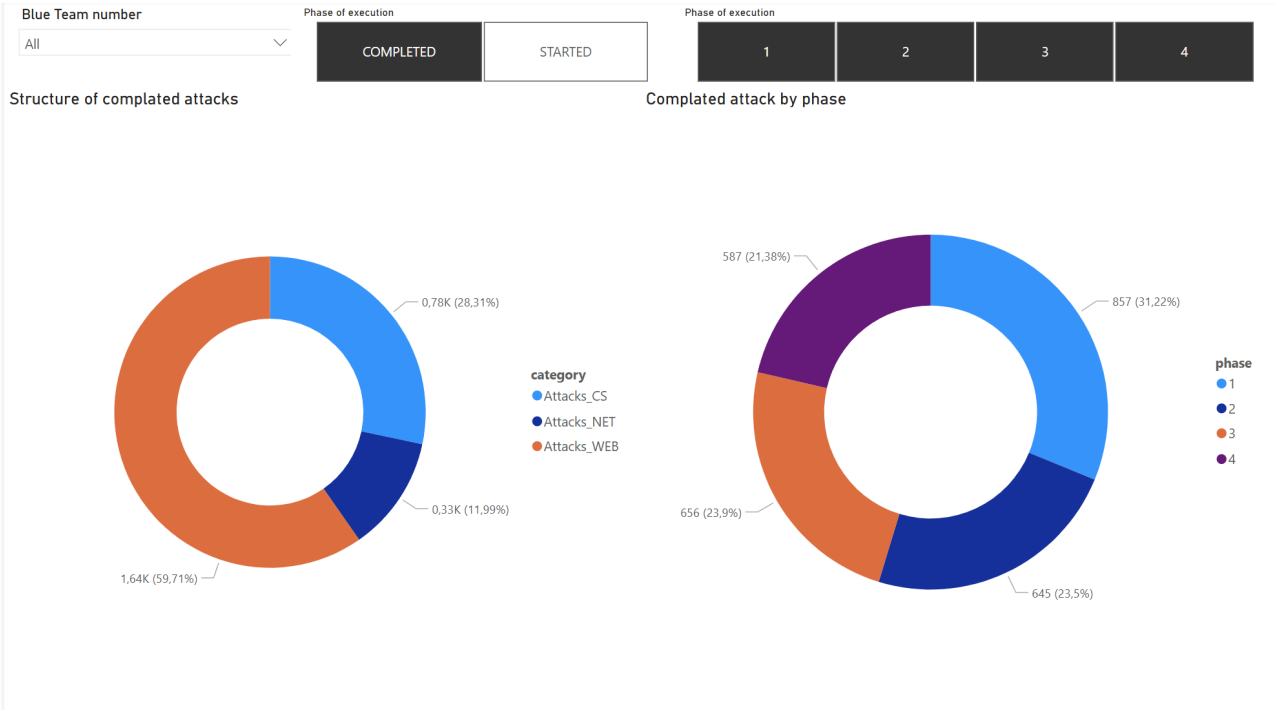

Figure 11 Completed attack structure by system categories.

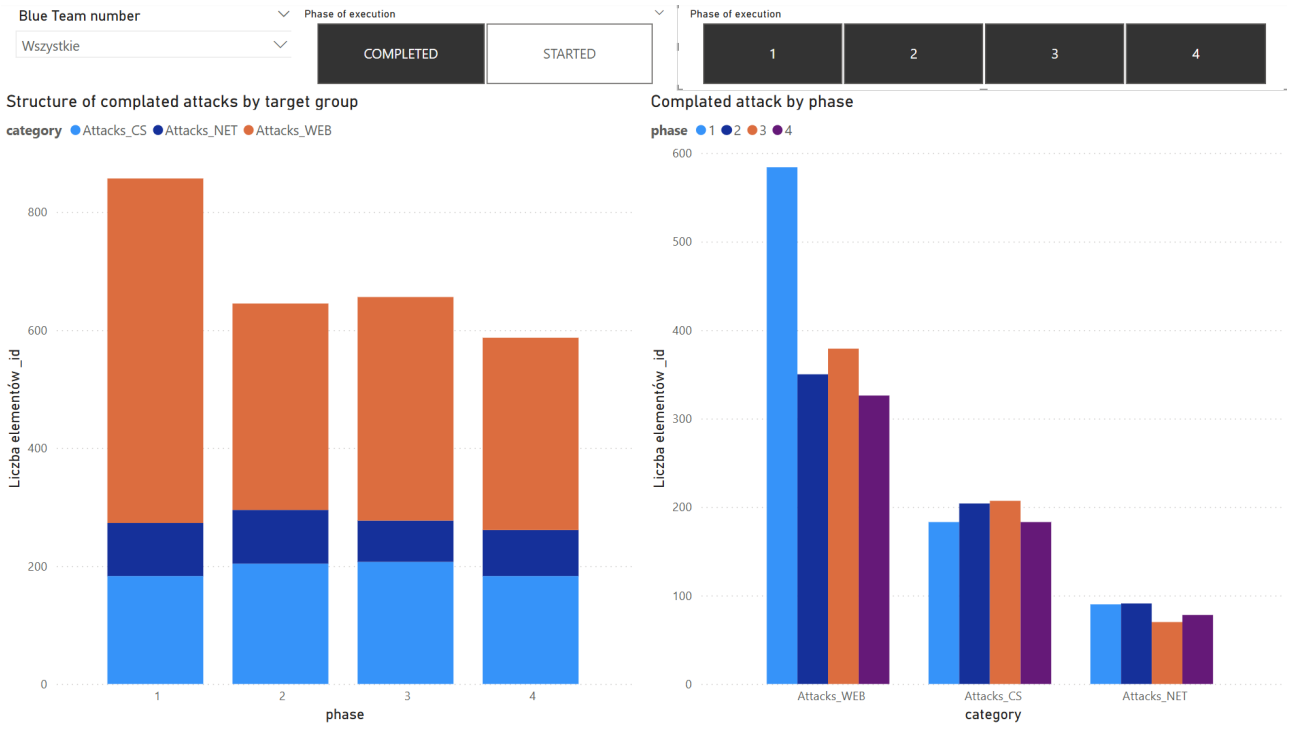

Figure 12. Attack success behaviour in between LS phases

The primary objective of Figure 12 is to compare subsystem categories and attack completion statuses across the exercise phases. A significant aspect of this analysis is the structure of successful attacks in each phase with respect to the targeted system categories.

On the right side of Figure 12, the visualization reports changes in attack success rates for each LS phase per system category. Notably, during phase 1 (specifically regarding web targets) volume of successful attacks exceed the average number of attacks per phase. This represents a clear discrepancy in the distribution of successful attacks that is not observed in other phases or other system categories.

The previous finding indicates that web targets were particularly susceptible to breaches during initial contact with the RT. As shown on the left side of Figure 12, the evaluation of successful attacks across combined system categories also reveals a spike in success during Phase 1 compared to subsequent phases. This implies that the TTPs initially selected for web systems were highly effective within the LS environment and encountered undefended systems during Phase 1. Data from subsequent phases, measured as a cumulative number of completed attacks, presents a stable or slightly declining trend, demonstrating the ability of BTs to harden systems against utilized TTPs and withstand the RT campaign on average without total collapse.

Notably, the significant change between phases was observed only for WEB targets between the first and second phases. The rate of successful completion does not fluctuate significantly across different target types or in later phases. The consistent number of RT breaches throughout all phases for CS and NET systems demonstrates consistent TTP effectiveness, proving that well-planned missions and selected TTPs leave defenders with little opportunity for rapid threat remediation.

The significant number of attacks targeting WEB systems during the initial phase suggests that the RT utilized the exploitation of public-facing web applications as an initial attack layer to potentially reach critical systems. Similarly, from an objective perspective and according to the RoE, the RT defines the targeted layer of the attacks. The outcomes of completed attacks can be reviewed through the structure of the affected workstations by the RT. EXPO records the objective of every specific attack and precisely identifies the targeted machine. The combination of these two factors: the objective and the domain of the targeted system, reveals the priority structure of RT operations.

This priority structure is illustrated in Figure 13. As shown in Figure 13, 15.88% of attacks focused on target compromise, 18.11% on data theft, followed by 19.89% on access elevation and 23.86% on defacement intended to cause damage to the BTs.

In total, 53.88% of the RT engagement focused on securing system access and collecting essential secrets or increasing access levels. This occurs before the mission transitions into more advanced threats to potentially collect valuable information or access to ease long-term presence. Consequently, more than half of the total successful RT engagement is related to espionage.

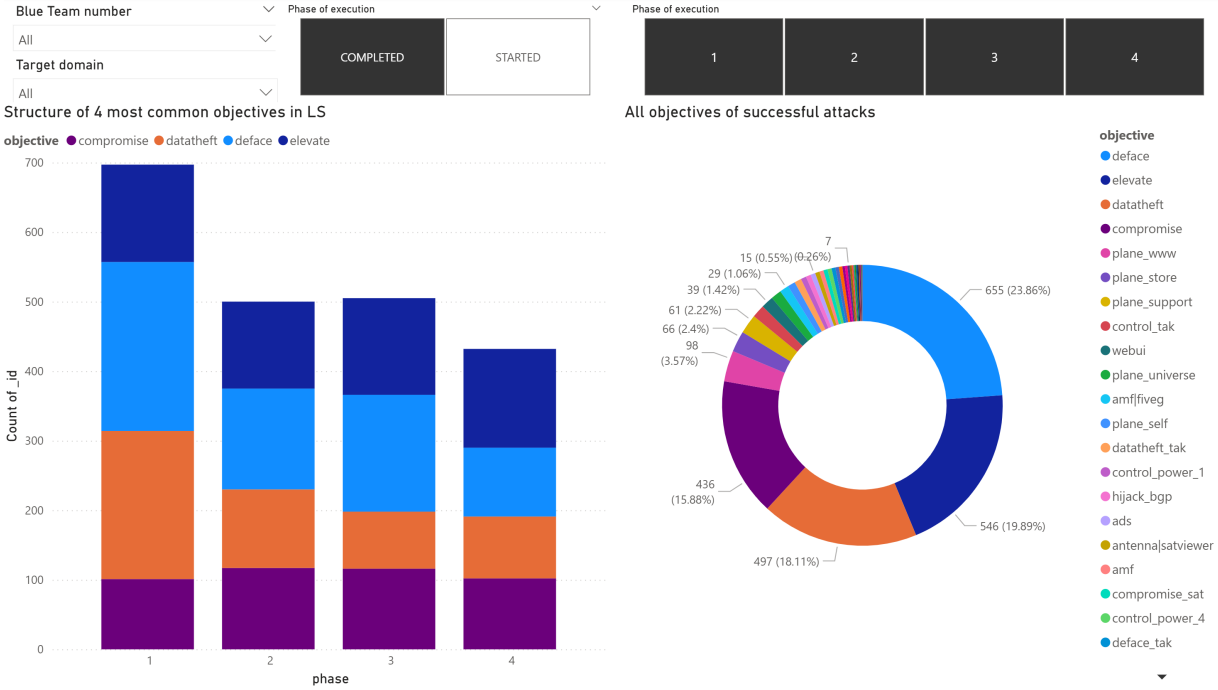

Figure 13. Completed objectives of performed attack compared its changes in time.

Notably, despite the spike in successful attacks during Phase 1, the proportional distribution of the four most common objectives remains consistent across all phases. This indicates that the RT successfully executed its mission, continuing operations without suspending actions upon the achievement of specific objectives during the LS. This provides the RT with a strategic advantage, as operations can transition toward stealthier activities, maintaining the flexibility required to execute more sophisticated attack vectors and threats.

Unlike the APT-focused analysis, the objective-oriented data in EXPO provides only a high-level description of less common objectives; expanding the scope of this research would require the integration of more granular data sources detailing specific RT attack

sequences. Furthermore, because the objectives utilized at this stage are closely tied to the specific LS scenario and environmental parameters, a comprehensive analysis of their success cannot be achieved through data-driven analysis alone.

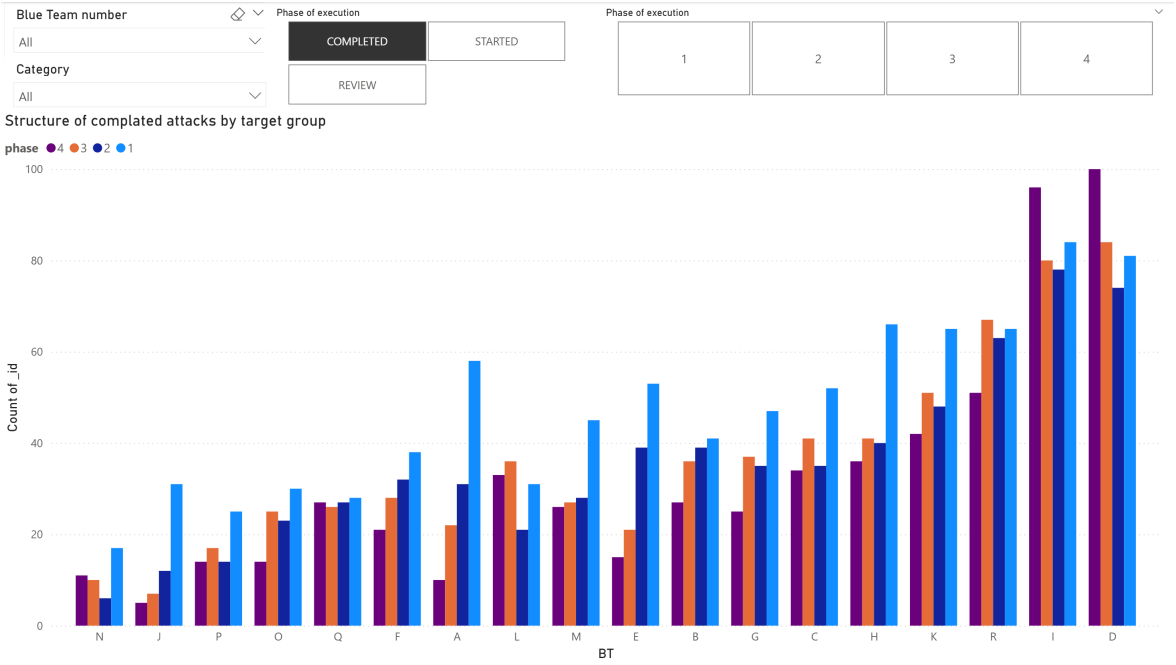

Figure 14. Overall BTs' performance over passing phases of LS (system categories combined)

Building upon the insights into RT effectiveness, the stable penetration rate, and successful espionage throughout the LS exercises, a review of BT system performance across consecutive phases reveals the most effective compromise patterns utilized by the RT. The two worst-performing BTs were unable to effectively mitigate the initial offensive, allowing the adversary's presence to expand. In contrast, the remaining teams experienced their highest number of breaches during Phase 1, subsequently adapting to incoming threats in later phases.

The detailed behaviour of BT defences across all systems is illustrated in Figure 14. This figure suggests that the TTPs utilized during the initial phase were most effective across 14 of the 18 analysed teams.

Conversely, Figure 15 presents the same analysis with a specific focus on CS systems; from this perspective, the identified trend is less pronounced. For the most heavily impacted team and seven others, the adversary's presence expanded with each subsequent phase, regardless of the effectiveness of the overall defence strategy. It is evident that for teams B, I and D, the RT was able to execute more complex attack schemas and leverage the full

potential of various TTPs, benefiting from low monitoring capabilities or stealthy manoeuvres. Those RT action's characteristic went unnoticed for BTs (B, I and R) presenting a significant risk for those BTs and elevating number of successful attacks.

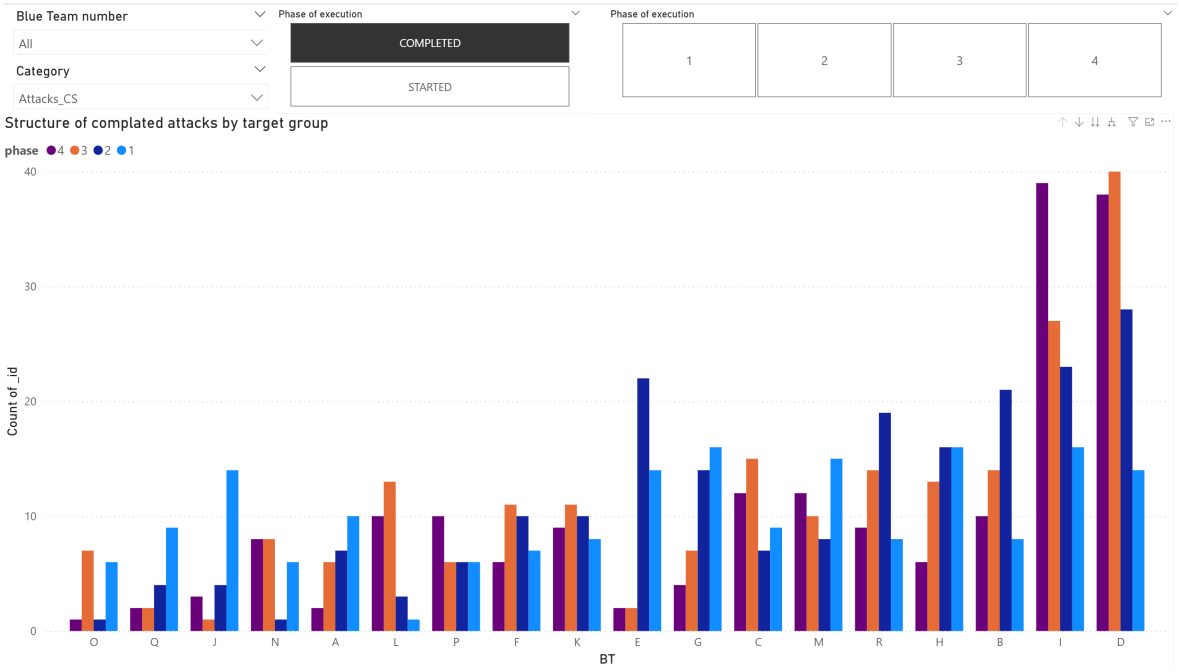

Figure 15. Overall BTs' performance over passing phases of LS (CS systems)

Figure 16 presents the attack data for the NET system category. The most heavily compromised BTs were D, I and R, which recorded the highest number of successful breaches. Within this category, the number of successful attacks exhibited a moderate distribution for specific BTs, demonstrating the effectiveness of these TTPs. Assuming standardized attack intensity across all phases and teams, exploits targeting NET systems appear to provide stable effectiveness, with a potentially high penetration rate if the defensive strategy allows for attack expansion at the BT level. This provides valuable training experience, as the RT utilized tactics and techniques capable of significant system compromise when defensive strategies were incoherent. Simultaneously, this maintained continuous attack pressure and constant incident handling demands for BTs that did not exhibit higher-than-average exposure.

Figure 17 serves as the final component of the analysis initiated with Figure 14. In this instance, however, the infection count exhibits significant variance, showing up to a twelve-fold difference between best and worst performing BTs. Furthermore, it is observable that Phase 1 was highly successful against WEB targets across most BTs, which

subsequently prompted improvements in their defences from phase to phase following that campaign (Figure 12 also display that trend).

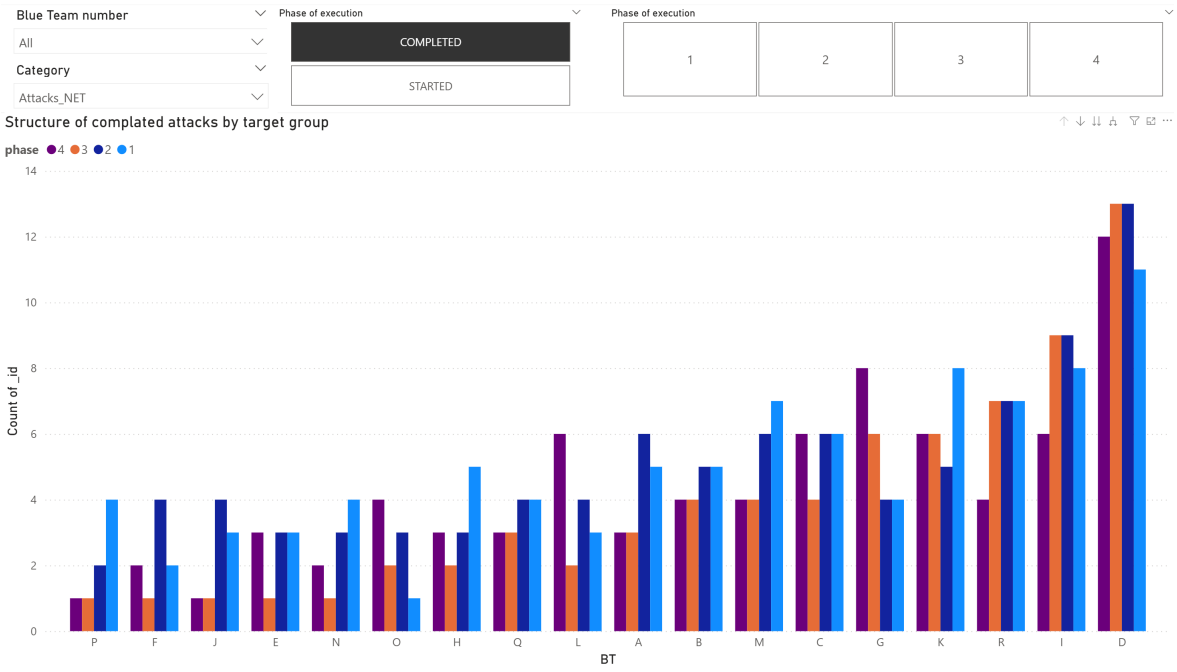

Figure 16. Overall BTs' performance over passing phases of LS (NET systems)

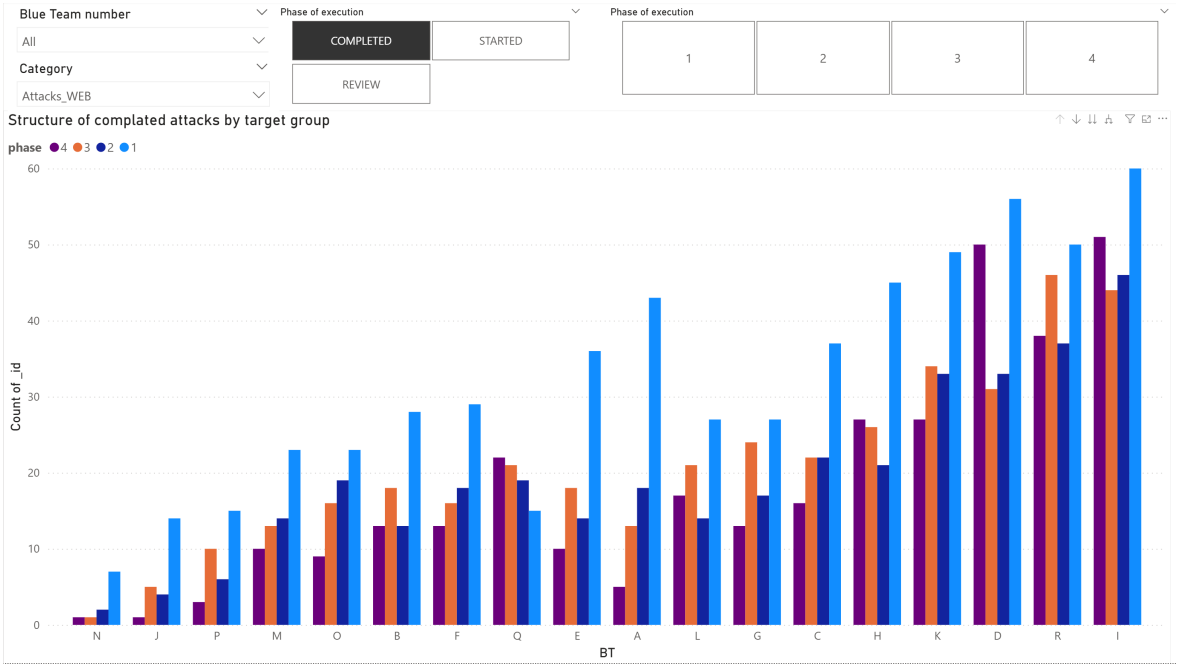

Figure 17. Overall BTs' performance over passing phases of LS (WEB systems)

In conclusion, TTPs attacking WEB targets in Phase 1 were more effective than average, as were the attacks targeting BTs D, R and I. The most effective defences against these attacks were observed in BTs N, J and P, where the RT's TTPs were successfully

countered. In instances where the same TTPs were applied to different targets during the initial phase, the broader RT campaign implies that these effective attacks are capable of breaching both mature and average BTs. Nevertheless, robust target protection can still respond successfully even to these highly potent attack techniques, providing a reduction in the number of successful attacks and demonstrating that well-implemented defences can significantly impede attack propagation.

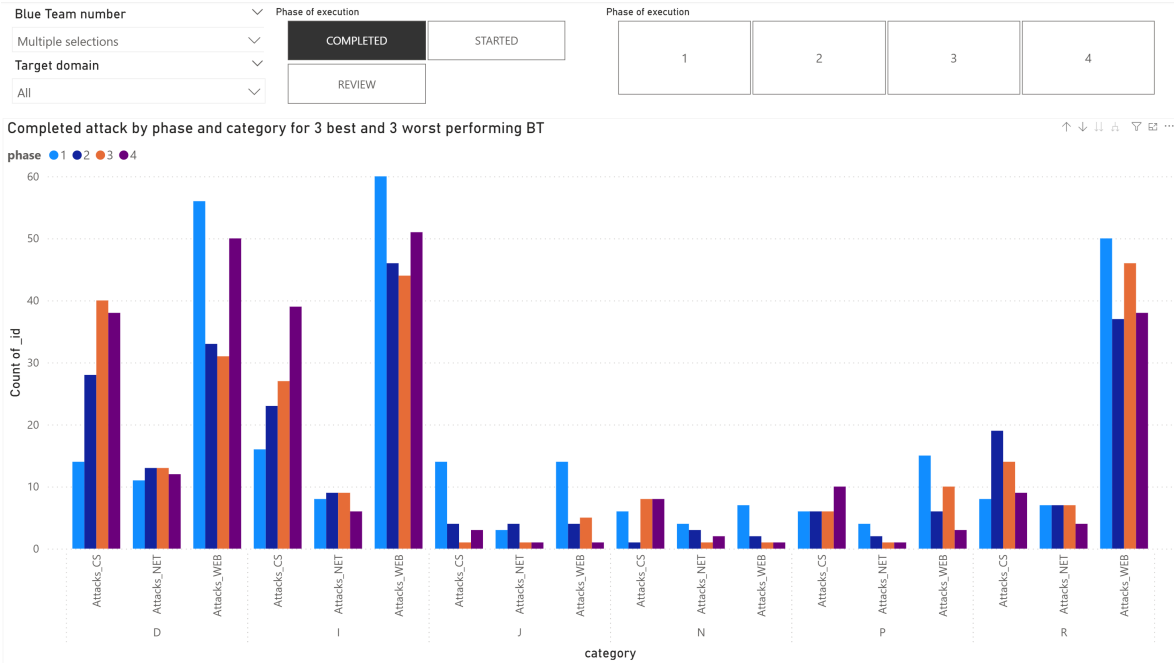

Figure 18. Overall BTs' performance over passing phases of LS for best and worst performing BTs

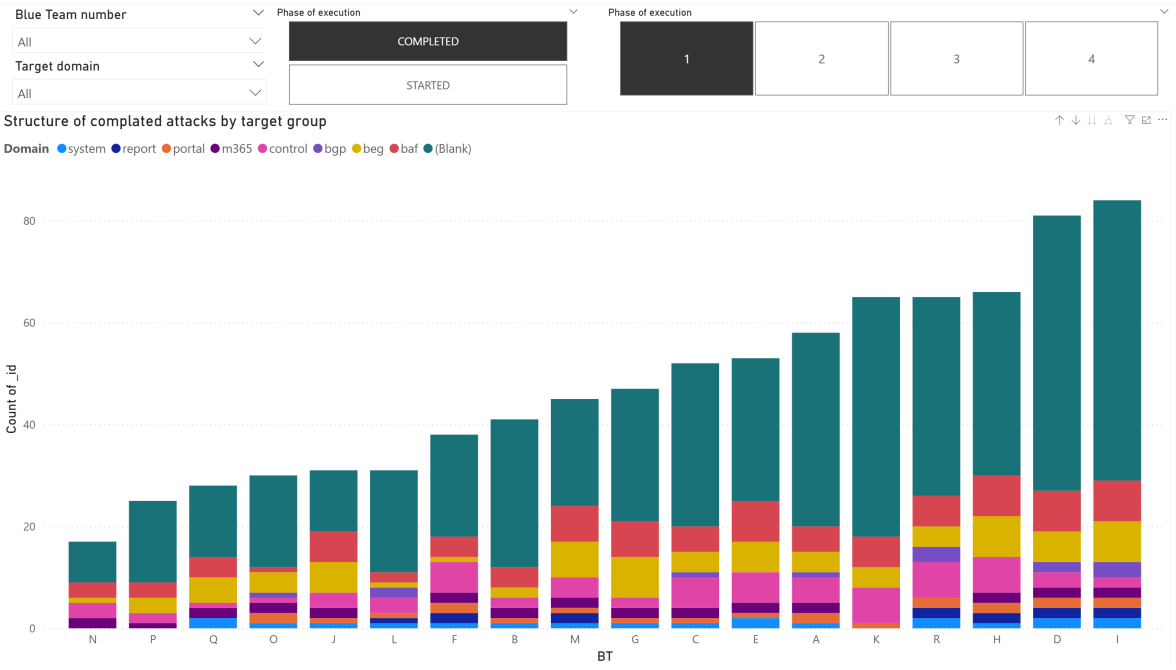

Figure 19. Attack's domains for targeted BT's machines

Figure 18 illustrates the BT response derived from the conclusions in Figures 14–17, demonstrating how the success of RT missions may vary on the same infrastructure under different defence strategies. The preceding reasoning reveals that identifying the most effective TTPs for target groups requires a clear classification of the attack domain. Unfortunately, the quality of EXPO data in this field is insufficient to forecast attack effectiveness within specific system types. However, such knowledge would facilitate the correlation of threat cycles with attacks on specialized systems and the identification of the most effective RT engagements. Figure 19 displays the records of targeted domains across all participating BTs. Despite clarity of dataset majority of attack don't specify clear objective.

4.2 Red Team TTP's evaluation in performed set of attacks

Section 4.2 will complement findings collected in section 4.1. As the KPI of successful attacks are known and EXPO data link attack dimensions to the attacks themselves it enables a deterministic comparison of the most successful and reliable attack dimensions identified in this chapter. While these following charts provide comprehensive insights, the following figures specifically illustrate the importance of successful attacks, represented by the size of squares arranged in a hierarchical structure. Each primary square denotes a specific EXPO attack dimension, which is further subdivided into sub-squares representing individual teams where applicable.

Beyond tracking attacks by type and affected environment, the system facilitates the observation of cumulative behaviours by enabling the comparison of targeted system groups across all execution phases. This allows for a consolidated analysis of completed attacks, objectives, subsystems and their associated attack dimensions. The report provides continuous visualization of both the most successful attacks and the most secure environments. Within the LS24 context, "AD-NETWORK FQDN_DIRECT" emerged as the most successful attack for 16 out of 18 BTs following the fourth phase of the exercise. The EXPO description for this specific attack is: "Service was accessed via FQDN from the attacker's machine located in SINET."

This description, however, highlights a significant limitation in the collected dataset and its subsequent analytical constraints. Enriching the dataset with more detailed descriptions would facilitate more meaningful analytical findings and significantly streamline the classification process if it would define technique RT to gain such access.

Two primary sources of highly effective attacks were identified. First involves infections executed by the RT during the initial phase of LS, specifically targeting WEB category systems.

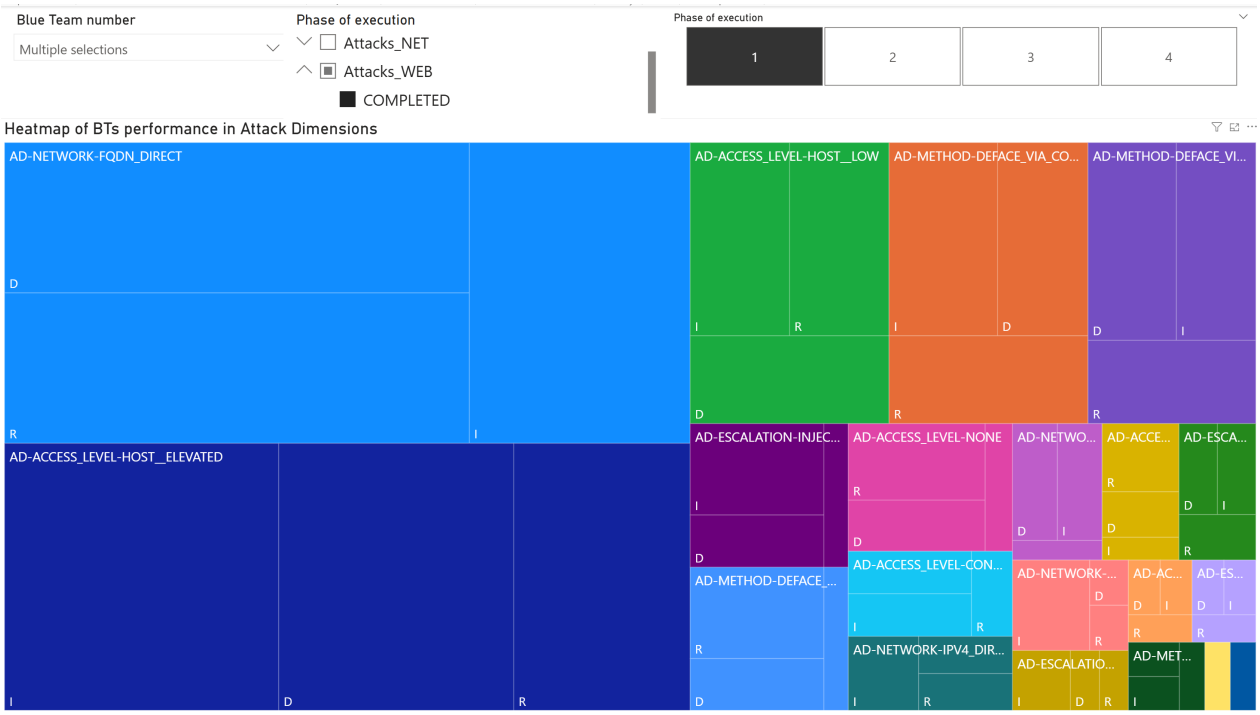

Figure 20. Attack dimensions used by RT in phase one of LS on WEB targets for the most infected BTs.

Figure 20 illustrates the structure of attack dimensions assigned to attacks on the D, I and R teams representing applicable dimensions. Notably, the five most common attack dimensions are identical to those presented in Figure 21. While Figure 21 employs the same analytical concept, it encompasses all participating BTs. These results align with previous findings indicating that all attacks targeting WEB systems during phase one were highly vulnerable and attack dimensions proved to be efficient consistently across majority of BTs. Notably, phase one represents the period of maximum infrastructural homogeneity among the BTs, as the RT is in the early stages of capturing the initial objectives.

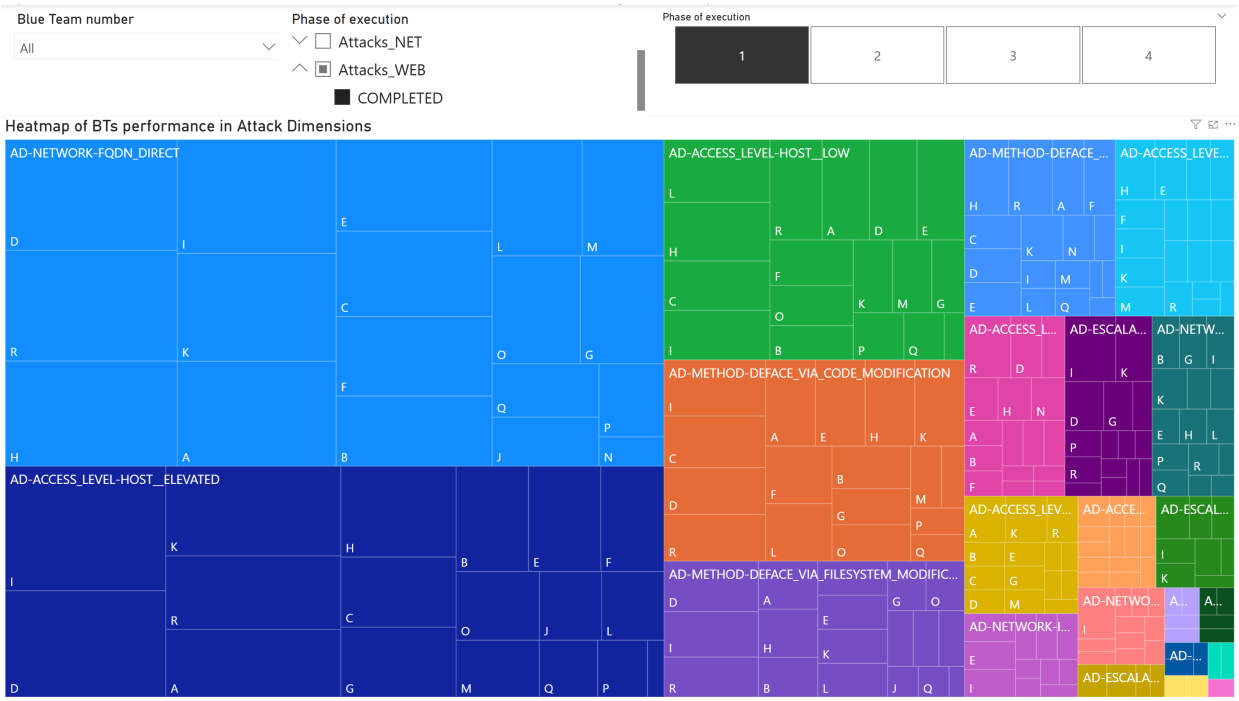

Figure 21. Attack dimensions used by RT in phase one of LS on WEB targets for all BTs.

The top 5 most successful attack dimensions were:

- AD-NETWORK-FQDN_DIRECT
    - Service was accessed via FQDN from the attacker's machine located in SINET
- AD-ACCESS_LEVEL-HOST__ELEVATED
    - The attacker had a elevated host level access on the target.
- AD-ACCESS_LEVEL-HOST__LOW
    - The attacker had a unelevated host level access on the target.
- AD-METHOD-DEFACE_VIA_CODE_MODIFICATION
    - The target was defaced via application code modification.
- AD-METHOD-DEFACE_VIA_FILESYSTEM_MODIFICATION
    - The target was defaced via changing file on disk.

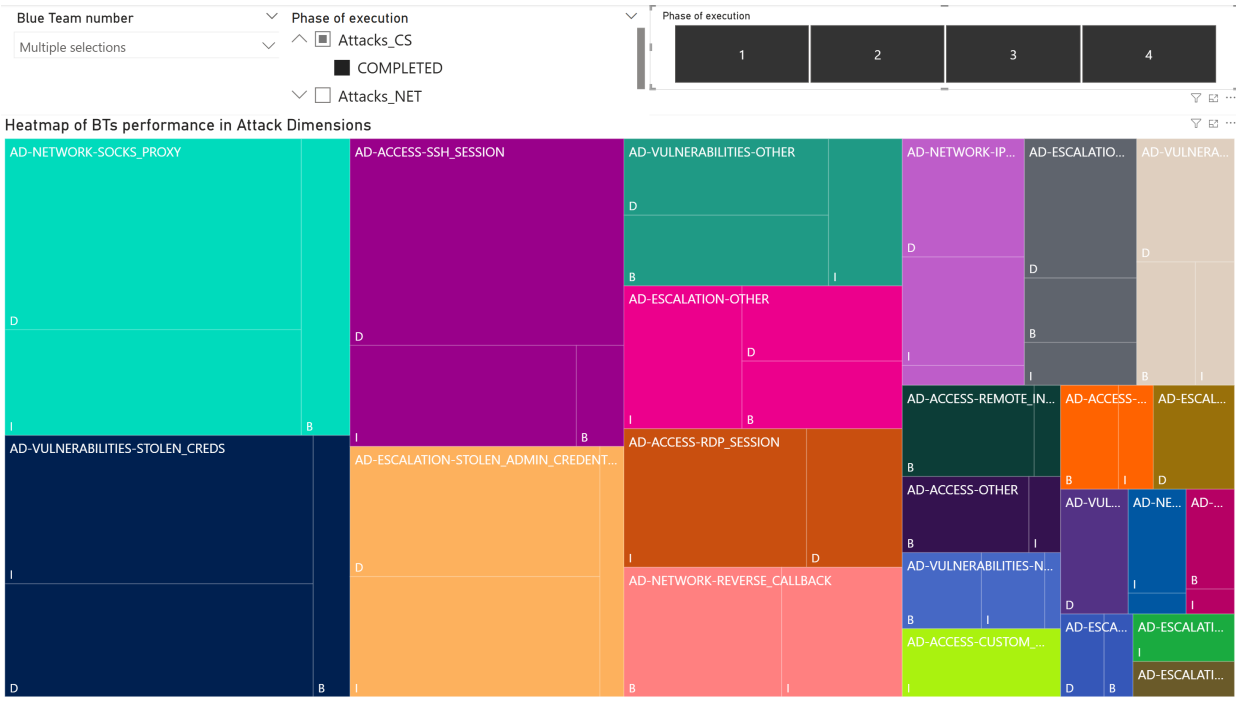

Figure 22. Attack dimensions referring to attack performed on client system for most infected BTs.

The second potential source of highly effective attacks identified consists of attacks on CS targeting BTs B, I and D. The effectiveness of these attacks was notably higher than that observed in the remaining BTs within the LS. Figure 22 provides a heatmap illustrating the attack dimensions for these specific teams, specifically for the subset of succeeded attacks corresponding to their CS.

The Top 5 most successful properties were:

- AD-NETWORK-SOCKS_PROXY
    - The attacker's machine located in SINET was able to connect to the target using a reverse SOCKS proxy located within target network.
- AD-VULNERABILITIES-STOLEN_CREDS
    - Previously stolen credentials were used to establish access to the target machine.
- AD-ACCESS-SSH_SESSION
    - SSH session was established to the target machine.

- AD-ESCALATION-STOLEN_ADMIN_CREDENTIALS
    - Previously stolen credentials were used to escalate privileges on the target machine.
- AD-VULNERABILITIES-OTHER

    Other vulnerabilities were used to establish access to the target machine.

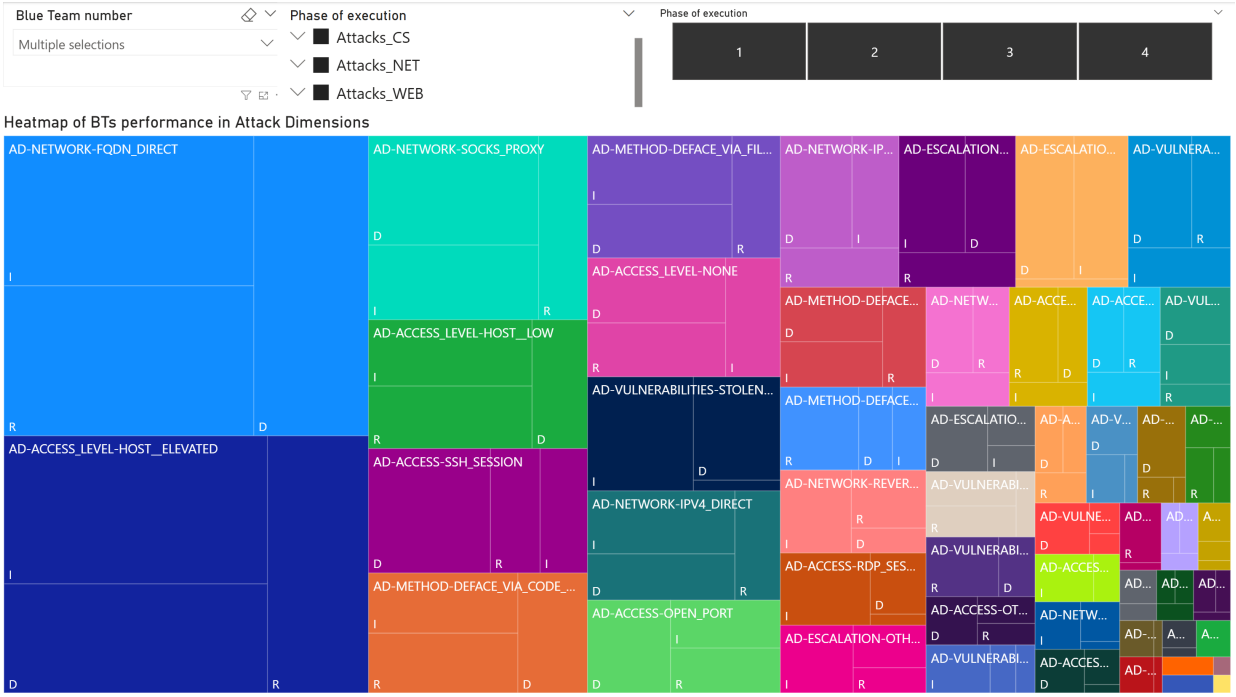

Figure 23. Attack dimensions referring to attack performed on the most infected BTs

Figure 23 presents an alternative aggregation of the EXPO data. By consolidating all system categories for the worst performing BT (I, D and R), this view facilitates the identification of the most successful attack dimensions within that group. The primary set of high-performing attack's dimensions included:

- AD-NETWORK-FQDN_DIRECT
    - Service was accessed via FQDN from the attacker's machine located in SINET
- AD-ACCESS_LEVEL-HOST__ELEVATED
    - The attacker had an elevated host level access on the target.

- AD-NETWORK-SOCKS_PROXY
    - The attacker's machine located in SINET was able to connect to the target using a reverse SOCKS proxy located within target network.
- AD-ACCESS_LEVEL-HOST__LOW
    - The attacker had a unelevated host level access on the target.
- AD-METHOD-DEFACE_VIA_CODE_MODIFICATION
    - The target was defaced via application code modification.

The distribution of attack dimensions within this group is more uniform than in previous assessments. Unlike earlier findings, no single dimension or small subset of dimensions reaches the 50% threshold within this subgroup of BTs. To substantiate these claims, an assessment of the targeted domains would be beneficial, as the threat landscape varies significantly depending on the domain of the system. However, the current implementation of EXPO lacks this information for certain attack activities, as illustrated in Figure 19. It fails to provide the RT operational context for the executed attacks (as discussed in detail in Section 4.3.1).

4.3 EXPO defined event vs STIX defined object in TTP context

This section presents two distinct methodological approaches designed to bridge the gap between the EXPO-defined event model and the MITRE STIX framework. The first approach, detailed in Section 4.3.1, describes a manual, human-led process to establish a baseline of description pairs or identify limitation. The second approach, detailed in Section 4.3.2, investigates an automated, AI-driven approximation utilizing a LLM. Together, these methods facilitate an evaluation of the effectiveness of translating attack dimensions into a standardized, actionable format.

4.3.1 The translation matrix of EXPO to STIX for purpose of this research

Figure 24 presents an event description that illustrates a potential collision between the EXPO-defined model and the MITRE-defined model. This example demonstrates how a unique attack dimension from EXPO can be represented by an entirely different set of TTPs within the MITRE framework. Limitation section also describes problem of contextualization of EXPO's "attack dimensions" for correct and relevant presentation.

Attack dimension	Description	Corresponding tactic	Corresponding technique	Corresponding procedures
AD-NETWORK-IPV4IPV6_DIRECT	Direct IPv4 or IPV6 access to the target was possible from the attacker's machine located in SINET	TA0008	T1021.001 (Sub technique T1563.002)	S0366
AD-NETWORK-IPV4IPV6_DIRECT	Direct IPv4or IPV6 access to the target was possible from the attacker's machine located in SINET	TA0109	T1071.001	C0028

Figure 24. Example of multiple TTP bundle description of EXPO defined attack activity.

Translating EXPO attack dimensions into the MITRE ATT&CK framework poses a significant challenge to maintaining contextual integrity. This limitation stems not only from approximation errors or collisions but also from a potential lack of shared operational context. Since the implementation of a TTP (e.g. direct IP access) is highly contingent upon the specific RT workflow, as evidenced by the LS24 exercise and historical attacks such as WannaCry, the direct mapping may fail to capture the true nature of the activity. Consequently, without in-depth knowledge of the underlying RT processes, mapping EXPO dimensions to more granular MITRE TTPs without recorded operational context risks a fundamental loss of the information required for accurate classification. Nevertheless, a manual assessment was conducted to verify that analysing attack descriptions at both the

tactic and technique levels is feasible within an LS environment and would enhance the clarity of future analyses with result presented on Figure 24.

4.3.2 The Llama 3.3 (LLM) generated unification matrix for attack description

In Appendix 5, the task of describing attack dimensions was assigned to an LLM, which was requested to "Match the best MITRE ATT&CK Technique ID for an event from EXPO." The requirement was to return only one technique and provide the reasoning why it was the best-suited one. Appendix 5 contains the resulting output (SHA1 hashed for transparency - Appendix 5).

The objective was to determine if an LLM could replicate the complex human mapping process through a structured computational approach. This approach consisted of three stages. The first, Context Provision, involved the LLM being provided with the IDs of tactics and techniques with their corresponding descriptions (Appendices 3 and 4), alongside the extensive technical context of the MITRE TTP hierarchy, ensuring the model was contextualized with the necessary nomenclature and structural logic of the STIX framework. This was followed by a query generation and assignment step, where a series of structured queries were generated, each describing a specific EXPO attack dimension for the previously contextualized model. The model was tasked with analysing these descriptions and assigning the most relevant TTP identifiers. Once the assignment was complete, data extraction via regular expressions followed to parse the response. This allowed the research to programmatically identify, isolate and extract the specific TTP numbers assigned by the model to each dimension.

Unfortunately, the outcomes of the LLM queries support the existence of constraints caused by the low level of contextualization in the existing descriptions (results in Appendix 5), resulting in the occurrence of T1437.001 more than 15 times across the unique attack dimensions (where EXPO defines 85 unique descriptions). Furthermore, the TA0001 tactic was selected more than 10 times within the 85 unique attack dimensions. The LLM output and the Figure 24 outcome correspond fully with each other. A detailed discussion of this problem follows in Chapter 5.

5 Limitations and future work

A fundamental design requirement of the LS is the implementation of a 'vulnerable-by-design' architecture, which enables participants to operate within exploitable systems across multiple attack vectors. This stands in contrast to the configuration of standard CI systems. While this study provides significant insights into the LS attack structure, a methodological limitation exists regarding the assessment of the infrastructure's technical resilience, understood as the integrated metric of usability, availability and defence capabilities. The LS does not measure the performance of BT defences resulting from system outages or the intentional misconfiguration of systems by defenders. Specifically, the RT's operational involvement and attack progression may be artificially constrained in such scenarios, as the RT may be unable to execute subsequent attack campaigns if targets become unreachable due to cascading corruption or BT-initiated configuration changes. In such scenarios, the reported effectiveness of the RT may be lowered in recent research, resulting in a reduced number of successful breaches and a lower total success rate of attacks. Such behaviour would not solely reflect a successful BT defence but rather an inability of the RT to engage with a degraded or unusable attack surface. The processed EXPO datasets used in this research do not correlate registered outages or the lack of usability recorded during the LS, as those data were not disclosed for this research by the CDCCOE. Therefore, while the existing results provide a clear view of RT attack dimensions, frequency and objectives within the scope of successful attacks, they may still underrepresent the true capability of the RT if system availability were not compromised and the system remained usable. Furthermore, in a live simulation environment, it is difficult for adversary to perform an unbiased assessment to distinguish whether an interruption in the attack sequence resulted from a successful defensive intervention by the BT or from a systemic failure caused by cascading events of configuration changes, without exercise-level awareness provided by other teams monitoring this aspect during the exercises. Future correlation of these data could potentially provide further support for the evaluation of RT effectiveness.

Another limitation concerns the level of detail used for describing attack engagement. As established in Chapter 4, industry standards (such as the MITRE STIX format) define the creation of TTPs and the scope of information they carry to allow for a systematic approach to describing tactics and techniques. This approach involves a high degree of complexity, often encompassing hundreds of entries, whereas the EXPO attack dimensions provide only

85. Comparing this systematic approach with the limitations of the 2024 EXPO dataset, it is evident that the granularity of the dataset is insufficient for multidimensional TTP analysis at both the tactic and technique levels. The limited descriptions and the single-layered nature of the attributes available for mapping EXPO's unique attack dimensions to TTP groups make such a mapping impossible without approximation.

This limitation further deepens the concern because contextual information is missing from the RT regarding how each attack dimension should be interpreted within the specific LS environment. For example, while AD-NETWORK-SOCKS_PROXY, the 2025 Poland Wiper Attack (C0063) and Cardinal RAT (S0348) usage all involve SOCKS proxy usage, they may not utilize the same procedures or share the same objectives and target profiling. This example demonstrates that without contextual elements, it is difficult to assess whether these techniques share the same underlying procedure, presenting a significant challenge to building a unique classification even if common element is described and defined.

Regarding the evaluation of a reporting approach like MITRE ATT&CK, if we assume a valuable translation of attack descriptions into the STIX objects defined by MITRE is possible (as demonstrated by the prototype dataset and translation matrix presented in subsection 4.3.1) then a redesigned EXPO could collect much more detailed events from future Locked Shields exercises. This would aim to present a more specific threat landscape within IT/OT contexts and measure detailed TTPs, allowing for the tracking of RT performance within a newly defined KPI regime.

The 2024 data capture setup inherently creates a limitation, as one attack dimension may not uniquely apply to a single tactic or technique within the vast space of the MITRE syntax. This is not a design flaw, EXPO was designed primarily from the BT's perspective, focusing on monitoring, communication and assessment. The design focused on monitoring infrastructure, ownership and the measurement of successful attacks, without providing deep insight into the specific tactics behind the executed offenses. However, this research creates a new analytical contribution by demonstrating the potential for this tool to perform these advanced functions in the future.

In the LS 2024 setup, each attack contains only a short, limited description of the event from the RT perspective, which is a highly generalized view. There is no strict correlation between the defined attack dimensions in EXPO and the TTPs established by MITRE. This

results in an expansion of the potential event space, where a single attack dimension may correspond to multiple potential TTPs rather than a unique one (as shown in Chapter 4) and enforce approximation. On the unique level, without detailed report for each attacked environment, missed IOCs related to attack, specific TTP and malware samples a unique threat intelligence based solely on EXPO records cannot be performed in automated manner with high precision yet.

6 Conclusion

The primary objective of this research was to evaluate the effectiveness of RT operations within complex environments. To establish a foundation for this evaluation, the research first analysed the real-world threat landscape to understand how threat maturity is expressed and to identify emerging threats. Subsequently, this analysis provided a basis for characterizing threats, systematising attack patterns, and leveraging existing research on threat cycles. This initial step was essential for assessing available data sources capable of providing a comprehensive and clear evaluation of RT effectiveness.

An investigation of the academic background revealed no meaningful existing datasets to drive such an analysis. However, the LS 2024 exercise proved to be a unique and necessary simulation environment for this research. The integration of attack monitoring capabilities during the LS 2024 execution allowed for a novel evaluation of RT performance. Through the analysis of this dataset, it was determined that attack maturity can be measured by the number of successful attacks occurring on the same CI across multiple defence variants and BT-influenced counteraction scenarios. This finding directed the analysis toward specific system categories and the special systems representing CI within the deployed LS environment.

Specifically, by observing the volume, success rates and various attack dimensions used against these special systems, it became possible to define the maturity of the adversarial pressure being simulated by the RT within existing threat cycle measures. Building upon this framework, the research utilised the EXPO data model and developed BI reporting to demonstrate how attack properties (attack dimensions) can be evaluated in relation to simplified TTP descriptions across different infrastructure segments. As the RT carried out attacks against the CI, the resulting data provided the foundation for analysing the defensive behaviours exhibited by various BTs in response. The results revealed that TTPs (as attack dimensions) may be a decisive factor for attack effectiveness because notably, 5 out of 85 defined attack dimensions presented in Figure 21 accounted for more than half of all successful attacks. Specifically, among successful attacks, certain dominant attack dimensions were observed within both the scope of the CS and the broader CI infrastructure (as seen in Figure 22 and Figure 23).

The data also showed that initial contact with an adversary on WEB systems results in higher infectiousness than in later phases. Furthermore, BT defence strategies deeply affect RT effectiveness, as evidenced by the effectiveness distribution presented in Figures 11 and 12, where the distribution of successful attacks varies significantly across different teams and timeframes (Figure 15). By integrating raw data from EXPO with BI reporting, it was demonstrated that RT attack tracking can be performed in real-time, helping to better orchestrate adversary missions and enable potential BT collaboration in future LS iterations.

Despite these findings, certain limitations of the current setup were identified. While the EXPO data model was detailed enough to provide a record of successful attacks and familiarise participants with the attack context, it did not provide information regarding system usability or infrastructure outages. It also showed a limited ability to track the full granularity of RT actions, specifically regarding the depth of dimensional analysis in the context of TTPs and the scope of the remaining attack surface available after each phase.

Furthermore, the dataset did not focus on the formal recording of TTPs themselves, as the RTs utilised TTPs in an unrecorded manner without a defined requirement to register simulated threats within EXPO per unique TTP. To address these gaps, future work should focus on the integration and redesign of these components of the EXPO tool. Specifically, integrating MITRE TAXII server capabilities with EXPO's exercise datasets could present a significant opportunity for future BT cooperation. Such an integration would allow for the combination of the strengths and weaknesses of multiple BTs and the evaluation of attack effectiveness; specifically, it would determine if attacks can achieve higher success rates against TTPs that multiple BTs fail to recognise, or if effectiveness decreases due to BT knowledge sharing.

Conclusion per RQ1:

Answering the question “What are the most relevant cyber threat cycles for critical infrastructure (CI) sector?” is possible by addressing the public incident repositories and finding the most targeted infrastructure. In the European Union since 2024 the most targeted infrastructure was a combination of state institutions and political system infrastructure. The critical infrastructure represented 43.6% of all performed and reported attacks [25]. The most relevant threats for critical domains identified from those incidents were threats focusing on ransomware, distributed DDoS, public-facing web platforms defacement and supply chain

attacks, which gain indirect access to public sector networks by compromising trusted third-party vendors.

Conclusion per RQ2:

To answer the research question, 'How can threat cycles be linked to attacks happening during LS?', the analysed dataset provided records of performed attacks and 'attack dimensions' within the simulated LS environment. Each attack provided a brief context of the activities taken to complete a successful attack. Processing this dataset provided information on attack practices, BT resilience levels, and the overall success of the attack campaign.

The attack distribution in Phase 1 for the WEB segment is visible in Figure 21, which, when viewed alongside the number of completed attacks in Figure 18, confirms that the threat established by the RT aligns with the threat cycle defined in Figure 2 as “mature” as defence gap was easily exploitable by RT. Moreover, the developed BI tool provided insights into each phase, both separately and cumulatively, for each CI segment and BT, visualizing the constant pressure applied by the RT in any scenario. The dataset allows for the profiling of attacks based on their effectiveness and the benchmarking of attacks across various defences. The threat cycles may further correlate threat cycles with attacks based on the depth of description to evaluate effectiveness. Furthermore, mapping attack descriptions to specific TTPs could place them into the context of emerging threat cycles for chosen infrastructures, assuming the LS simulation outcomes could remain relevant to real-world threats which can be addressed in the future work.

Conclusion per RQ3:

To address the research question “How effectively did the LS Red Team execute the attacks identified in the previous questions?” the measurement of RT attack success rates is analysed in Figure 9, 'Attack success rate per BT.' This metric serves as a critical indicator of the operational difficulty encountered by the RT and the varying levels of defensive maturity among the participating BTs. The data reveals a significant distribution of performance, reflecting a heterogeneous landscape of defensive capabilities. Notably, the analysis of the upper quartile (representing the most mature defences) indicates that even these sophisticated teams were susceptible to successful compromises across all phases. This suggests that the simulated APT-level pressure was sufficient to expose vulnerabilities in

protected CI, thereby fulfilling the pedagogical objective of the exercise. Conversely, the lower quartile experienced a success rate of attack at nearly 50% level, demonstrating the RT's ability to exploit fundamental defensive gaps.

The same is applicable to the Figure 10 “Attack success rate based on system category type” where the above observations are distributed across all system categories present in the LS. Ultimately, these results demonstrate that while the RT was able to achieve its objectives and conduct measurable damages across all environments the intensity of those attacks remained calibrated to the participating BTs. This preserved the training characteristics of the LS by avoiding the total neutralization of the systems before the final phase arrived, proving the high effectiveness of the RT for the 2024 execution.

Conclusion per RQ3.1

To address the research question “Were there differences in the identified attacks within a single BT?” the analysis reveals that variations occurred at the level of specific BT assets, such as protected system categories. For instance, the varying resilience demonstrated by BT 'I' was evident when comparing the CS category, which had a 64,02% of undefended attacks, to the NET category, which had 26,45% undefended attacks. More detailed statistics regarding success rates and their distribution across all BTs at the end of phase 4 are provided in Figure 10 “Attack success rate based on system category type”.

Conclusion per RQ3.2:

To address the research question, 'Were there differences in the identified attacks between different BTs?', the results indicate that significant variations occurred across the various BTs. Specifically, an analysis of effective attack patterns shows that teams 'O' and 'Q' struggled most with WEB-based attacks, whereas BTs 'J' and 'N' experienced the highest success rates against CS systems. The success rates of RT actions are summarized in Figure 9, 'Attack success rate per BT,' which provides an aggregate sum of successful attacks for each BT at the conclusion of Phase 4.

In relation to attacks on specific special systems following the initial phase of LS, as illustrated in Figure 19, 'Attack domains for targeted BT machines,' the

distribution and volume of recorded attacks demonstrate that the RT's achievement of initial objectives countering varying defensive strategies creates different states of defended infrastructure. This resulted in a unique level of adversary presence within the infrastructure of each BT. These findings support the conclusion that while each BT received a distinct level of training experience through RT interaction, the RT was simultaneously capable of successfully targeting all system categories. For a more detailed view of the propagation and frequency of attack dimensions focused on espionage refer to the properties in Figure 21, 'Attack dimensions used by RT in phase one of LS on WEB targets for all BTs,' which illustrates the propagation of each attack dimension across all successful attacks as well as per individual BT after the initial phase was finalised.

Conclusion per RQ3.3:

Regarding the research question “Is the available data sufficient to address sub-questions 3.1 and 3.2?” the answer is affirmative. The dataset provided a sufficient volume of data to perform an analysis of sub-questions 3.2 and 3.3. However, during the research process, certain limitations were identified, specifically the need for greater granularity in dimensional analysis (with the ability to introduce more abstract layers) and more detailed documentation of attack records to achieve more precise research outcomes. Nonetheless, the current dataset establishes the foundation for developing reporting capabilities for tracking attack effectiveness, serving as a significant subject for future work regarding more descriptive TTPs.".

6.1 Future work

Future research should focus on studies that support the structural description of cyberattack missions in controlled environments where extensive monitoring is available. Future work on the processed dataset could focus on unifying naming conventions for describing attacks and improving data quality by eliminating missing information regarding attack objectives and domains in EXPO. A potential direction for modifying the EXPO dataset is the migration to the MITRE STIX standard, facilitated by LLM correlation with existing data or via manual rule creation to add more detail to the processed data. Additionally, focus could be placed on collecting more detailed information regarding

attacks at the individual RT member level. The implementation of MITRE ATTCK properties into EXPO could support a deterministic description of events in STIX format, providing additional functionality for information exchange through TAXII to support potential future collective BTs cooperation. Moreover, the ability to trace back executed actions could enable the RT to generate and visualize precise TTP chains, providing a deeper understanding of how specific TTPs of successful attacks contribute to effectiveness against specific BT defences or vulnerabilities during the mission.

References

[1] V. Zubok and A. Davydiuk, “Analytical Review of the Resilience of Ukraine’s Critical Energy Infrastructure to Cyber Threats in Times of War,” in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, 2023.

[2] M. Smeets, “The role of military cyber exercises: A case study of locked shields,” in *2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon)*, Tallinn, 2022.

[3] NATO CCDCOE, “Locked Shields,” NATO Coperative Cyber Defence Centre of Excellence, [Online]. Available: https://ccdcoe.org/exercises/locked-shields/. [Accessed 2025 03 03].

[4] Y. Kwon, W. Wang, J. Jung, K. H. Lee and R. Perdisci, “C2SR: Cybercrime Scene Reconstruction for Post-mortem Forensic Analysis,” in *Network and Distributed Systems Security (NDSS) Symposium 2021*, virtual, 2021.

[5] A. Luik, *THE DESIGN AND IMPLEMENTATION OF AUTOMATED VULNERABILITY APPLICATION FRAMEWORK,* Tallinn: TALLINN UNIVERSITY OF TECHNOLOGY, 2018.

[6] D. Ganguli, L. Lovitt, J. Kernion, A. Askell, Y. Bai, S. Kadavath, B. Mann, E. Perez, N. Schiefer, K. Ndousse, A. Jones, S. Bowman, A. Chen, T. Conerly and N. DasSarma, “Red Teaming Language Models to Reduce Harms: Methods, Scaling Behaviors, and Lessons Learned,” Cornell University, 2022.

[7] B. Al-Sada, “Threat Profiles Analysis Based on MITRE ATT&CK Knowledge Base,” *PQDT - Global,* p. 149, 2024.

[8] D. Selmanaj, Adversary Emulation with MITRE ATT&CK: Bridging the Gap Between the Red and Blue Teams, O'Reilly Media, Inc, 2024.

[9] S. M. Z. U. Rashid, I. Montasir and A. Haq, “Risk-Based MITRE TTP Scoring for Proactive Cyber Threat Prioritization and Response,” in *2025 14th International Conference on Software and Computer Applications (ICSCA 2025)*, Kuala Lumpur, Malaysia, 2025.

[10] A. Kott, “To Improve Cyber Resilience, Measure It,” in *IEEE Computer, 54(2), Feb.2021,* , 2021.

[11] P. Brangetto, E. Çalişkan and H. Rõigas, “Cyber Red Teaming. Organisational, technical and legal implications in a military context.,” NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), Tallinn, 2015.

[12] M. Singirikonda, “Evaluating the Effectiveness of Red Teaming in Identifying Vulnerabilities,” *Journal of Cyber Security Technology,* vol. 1, p. 8, 2023.

[13] S. Kraemer, P. Carayon and R. Duggan, “Red Team Performance for Improved Computer Security,” *Human Factors and Ergonomics Society Annual Meeting Proceedings,* vol. 48, 2004.

[14] C. Johnson, L. Badger and D. Waltermire, “NIST Special Publication 800-150; Guide to Cyber Threat Information Sharing,” U.S. Department of Commerce; National Institute of Standards and Technology, 2016.

[15] S. Yulianto, B. Soewito, F. L. Gaol and A. Kurniawan, “Enhancing Cybersecurity Resilience through Advanced Red Teaming Exercises and MITRE ATT&CK

Framework Integration: A Paradigm Shift in Cybersecurity Assessment," *Cyber Security and Applications,* vol. 2, no. 2772-9184, p. 100077, 2024.

[16] X. Shen, Z. Li, G. Burleigh, L. Wang and Y. Chen, "Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: AnAnalysis of EDR Performance in Real-World Environments," *ASIA CCS '24, July 1–5, 2024, Singapore, Singapore,* 01-05 07 2024.

[17] National Institute of Standards and Technology, "NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Gaithersburg, MD, 2012.

[18] S. Krishnapriya and S. Singh, "A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques,," *Computers, Materials and Continua,* vol. 80, no. 2, pp. 2675-2719, 2024.

[19] ENISA, "BEST PRACTICES FOR CYBER CRISIS MANAGEMENT," ENISA, 2024.

[20] ENISA, "ENISA THREAT LANDSCAPE 2022," ENISA, 2022.

[21] ENISA, "European Unioin Agency For Cybersecurity Threat Landscape," ENISA, October 2024. [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape. [Accessed 17 March 2025].

[22] M. F. A. E. Rob, M. A. Islam, S. Gondi and O. Mansour, "The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector," *Issues in Information System,* vol. 25, no. 3, pp. 62-80, 2024.

[23] M. Roshanaei, "Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies," *Journal of Computer and Communications,* vol. 9, pp. 80-102, 2021.

[24] *COUNCIL DIRECTIVE 2008/114/EC,* 2008.

[25] P. D. S. Harnisch, D. K. Zettl-Schabath, K. Schuck, L. Prof. Matthias C. Kettemann, M. Müller, r. A. Bendiek, J. Bund, C. Borrett, E. Neuber and M. Kerttunen, "European Repository of Cyber Incidents," Coordination Group for Cyber Foreign Policy at the German Foreign Office and by the Danish Ministry of Foreign Affairs, 2025.

[26] Center, Internet Crime Complaint, "Federal Bureau of Investigation Internet Crime Report 2023," ic3, 2023.

[27] European Repository of Cyber Incidents, "European Repository of Cyber Incidents," European Repository of Cyber Incidents, [Online]. Available: https://eurepoc.eu/dashboard/. [Accessed 01 04 2025].

[28] W. Hurst, M. Merabti and P. Fergus, "A Survey of Critical Infrastructure Security," in *8th International Conference on Critical Infrastructure Protection (ICCIP)*, Arlington, United States, 2016.

[29] N. d'Ambrosio, G. Capodagli, G. Perrone and S. P. Romano, "SCASS: Breaking into SCADA Systems Security," *Computers & Science,* vol. 151, p. 104315, 2025.

[30] M. Mesbah, M. S. Elsayed and A. D. A. M. Jurcut, "Analysis of ICS and SCADA Systems Attacks Using Honeypots," *Future Internet,* vol. 15, no. 7, 2023.

[31] L. Crognale, "SANS 2024 Top Attacks and Threats Report," SANS Institute, 2024.

[32] European Union Agency for Cybersecurity (ENISA), "ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS," 2022.

[33] M. Benmalek, “Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges,” *Internet of Things and Cyber-Physical Systems,* vol. 4, pp. 186-202, 2024.

[34] Australian Government - Australian Signals Directorate, “Annual Cyber Threat Report 2023-2024,” ASD, 2024.

[35] DRAGO, “2025 OT Cybersecurity Report 8th Annual Year in Review,” DRAGOS, 2025.

[36] G. Anisa and F. Widianingsih, “SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age,” *Electronic Integrated Computer Algorithm Journal,* vol. 2, pp. 47-52, 2024.

[37] P. Santos, A. Rafael, M. J. C. S. Reis, C. Serodio and F. Branco, “A Systematic Review of Cyber Threat Intelligance: The Effectiveness of Technologies, Strategies, and Collaborations in Combat Modern Threats.,” *Sensors,* vol. 25, no. 14, p. 4272, 2025.

[38] K. H. Teigen and G. Keren, “Are random venets perceived as rare? On the relationship between perceived randomness and outcome probability.,” *Memory & Cognition,* vol. 48, pp. 299-313, 2020.

[39] S. R. Muller, “An Analysis of the Design of the Cybersecuirty Maturity Model Certification (CMMC) and Its Direct Effect on Supply Chain Management,” in *Real-world solutions for diversity, strategic change, and organizational developement: perspectives in healthcare, education, bussines, and technology*, IGI Global, 2023, pp. 220-238.

[40] A. Konev, A. Shelupanov, M. Kataev and V. A. a. A. Nabieva, “A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats,” *Symmetry 2022,* vol. 14, no. 3, p. 549, 2022.

[41] Z. Almahmoud, P. D. Yoo, O. Alhussein, I. Farhat and E. Damiani, “A holistic and proactive approach to forecasting cyber threats,” *Scientific Reports,* vol. 13, no. 1, p. 8049, 2023.

[42] M. Asiri, A. Arunasalam, N. Saxena and Z. B. Celik, “Frontline responders: Rethinking indicators of compromise for industrial control systems security,” *Computers & Security,* vol. 154, p. 104421, 2025.

[43] S. Bolen, “Medium,” Medium Corporation, 29 07 2025. [Online]. Available: https://medium.com/@scottbolen/polymorphic-ransomware-2-0-a6c5cf232057. [Accessed 01 12 2025].

[44] S. Colabianchi, F. Costantino, F. Nonino and G. Palombi, “Transforming threats into opportunities The role of human factors in enhancing cybersecurity.,” *Journal of Innovation & Knowledge,* vol. 10, no. 3, p. 100695, 2025.

[45] M. Ammi and Y. M. Jama, “Cyber Threat Hunting Case Study using MISP,” *Journal of Internet Services and Information Security,* vol. 13, no. 2, pp. 1-29, 2023.

[46] C. Ojo, E. A. Osoko, J. N. Okolo and M. Jaji, “Incident response; A structured model from detection to containment and recovery,” *Word Journal of Advanced Research and Reviews,* vol. 24, no. 1, pp. 1401-1407, 2024.

[47] Y. Ye, T. LI, D. Adjeroh and S. S. Iyengar, “A Survey on Malware Detection Using Data Mining Techniques,” *ACM Computing Surveys,* vol. 50, no. 3, pp. 1-35, 2017.

[48] J. Alrzini and D. Pennington, “A review of polymorphic malwar detection techniques,” *International Journal of Advanced Research in Engineering and Technology (IJARET),* vol. 11, no. 12, pp. 1238-1247, 2020.

[49] M. S. Avhankar, J. Pawar and V. Kumbhar, “A Comprehensive Survey on Polymorphic Malware Analysis: Challenges, Techniques and Future Directions,” *Communications on Applied Nonlinear Analysis,* vol. 32, no. 9, pp. 2765-2776, 2025.

[50] MITRE, “MITRE ATT&CK Enterprise Matrix,” MITRE, [Online]. Available: https://attack.mitre.org/matrices/enterprise/. [Accessed 02 04 2025].

[51] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, “MITRE ATT&CK: Design and Philosophy,” The MITRE Corporation, McLean, VA, 2018.

[52] Lockheed Martin, “GAINING THE ADVANTAGE. Applying Cyber Kill Chain Methodology to Network Defense”.

[53] S. Caltagirone, A. Pendergast and C. Betz, “The Diamond Model of Intrusion Analysis,” 2013.

[54] N. Naik, P. Jenkins, P. Grace and J. Song, “Comparing Attack Models for IT Systems: Lockheed Martin’s Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model,” in *TT&CK Framework and Diamond Model z*, Vienna, Austria, 2022.

[55] MITRE, “MITRE ATT&CK Navigator,” [Online]. Available: https://mitre-attack.github.io/attack-navigator/. [Accessed 02 04 2025].

[56] MITRE ATTCK Github Community, “MITRE ATT&CK Data Model,” 6 3 2025. [Online]. Available: https://github.com/mitre-attack/attack-data-model. [Accessed 20 04 2025].

[57] G. Darelli, “Cyber Threat Intelligence and how is leveraged inside Cyberkit4SME – Part 2,” cyberkit4sme, 25 05 2023. [Online]. Available: https://cyberkit4sme.eu/news/cyber-threat-intelligence-and-how-is-leveraged-inside-cyberkit4sme-part-2/. [Accessed 02 04 2025].

[58] I. Tuson, “Collections and Collection Indexes,” 14 10 2021. [Online]. Available: https://github.com/center-for-threat-informed-defense/attack-workbench-frontend/blob/main/docs/collections.md. [Accessed 02 04 2025].

[59] MITRE ATTCK Github Community, “TAXII 2.1 API User Guide,” 18 04 2024. [Online]. Available: https://github.com/mitre-attack/attack-workbench-taxii-server/blob/main/docs/USAGE.md. [Accessed 20 04 2025].

[60] CCDCOE, “Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report,” CCDCOE, Tallinn, 2010.

[61] E. NATO Cooperative Cyber Defence Center of Excellence Tallinn, “CCDCOE,” [Online]. Available: https://ccdcoe.org/uploads/2018/10/LS14_After_Action_Report_Executive_Summary.pdf. [Accessed 03 03 2025].

[62] NATO CDDCOE, “World´s most advanced cyber defence exercise kicks off in Tallinn,” NATO CDDCOE, 24 04 2024. [Online]. Available: https://ccdcoe.org/news/2024/worlds-most-advanced-cyber-defence-exercise-kicks-off-in-tallinn/. [Accessed 18 05 2026].

[63] NATO CCDCOE TALLINN, “After Action Report LS 2024,” Tallinn, 2024.

[64] V. Mani, CISA, CISM and S. S. B. Belt, “Strengthening Cybersecurity with Red Team Engagements,” *ISACA Journal,* vol. 1, 2022.

[65] M. Pihelgas, “Design and Implementation of an Availability Scoring System for Cyber Defence Exercises,” in *14th International Conference on Cyber Warfare and Security (ICCWS 2019)*, Stellenbosch, South Africa, 2019.

[66] T. Sonets, *IMPROVING USER SIMULATION TEAM WORKFLOW IN THE CONTEXT OF CYBER DEFENSE EXERCISE,* Tallinn: TALLINN UNIVERSITY OF TECHNOLOGY, 2016.

[67] S. Mases, K. Maennel and A. Brilingaite, “Trends and chellanges for balanced scoring in cybersecurity exercises: A case study on the example of Locked Schields,” *Frontiers in Education,* vol. 7, p. 958405, 2022.

[68] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic and X. Bellekens, “A Review of Cyber-Ranges and Test-Beds: Current and Future Trends,” *Sensors,* vol. 20, no. 24, pp. 1-36 (7148), 2020.

[69] Llama Team, AI @ Meta, “The Llama 3 Herd of Models,” arXiv.

[70] F. HakemZadeh and D. M. Rousseau, “Evidence-based decision-making is a social endeavor.,” *Behavioral Science & Policy,* vol. 10, no. 1, pp. 27-33, 2024.

[71] SecurityScorecard, “Cyber Conflict and the Erosion of Trust. Introducing the Cyber Resilience Scorecard. Safeguarding Trust, Economy, and Society,” World Economic Forum Annual Meeting 2024, Davos, 2024.

[72] D. Schlette, P. Empl, M. Caselli, T. Schreck and G. Pernul, “Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors,” in *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2024.

Appendices

Appendix 1 -DAX and M queries building business intelligence data model

##Object name is followed by code

```
attackdimensions_categories



let

    Źródło = Table.FromColumns({Lines.FromBinary(File.Contents("D:\Zabrac\DataSources\attackdimensionsannonimized.json"),
null, null)}),

    #"Przekształcono kolumnę" = Table.TransformColumns(Źródło, {"Column1", Json.Document}),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekształcono kolumnę", "Column1", {"_id", "expo_id",
"name", "description", "type", "categories", "objectives", "__v"}, {"_id", "expo_id", "name", "description", "type",
"categories", "objectives", "__v"}),

    #"Rozwinięty element _id" = Table.ExpandRecordColumn(#"Rozwinięty element Column1", "_id", {"$oid"}, {"_id.$oid"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element _id",{{"_id.$oid", type text}, {"expo_id", type
text}, {"name", type text}, {"description", type text}, {"type", type text}, {"categories", type any}, {"objectives", type
any}, {"__v", Int64.Type}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"categories", each Text.Combine(List.Transform(_,
Text.From), "["), type text}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Wyodrębnione wartości",{"objectives"}),

    #"Podzielono kolumnę według ogranicznika" = Table.ExpandListColumn(Table.TransformColumns(#"Usunięto kolumny",
{{"categories", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "categories"),

    #"Usunięto kolumny1" = Table.RemoveColumns(#"Podzielono kolumnę według ogranicznika",{"expo_id", "name",
"description", "type", "__v"})

in

    #"Usunięto kolumny1"



attackdimensions_objectives



let

    Źródło = Table.FromColumns({Lines.FromBinary(File.Contents("D:\Zabrac\DataSources\attackdimensionsannonimized.json"),
null, null)}),

    #"Przekształcono kolumnę" = Table.TransformColumns(Źródło, {"Column1", Json.Document}),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekształcono kolumnę", "Column1", {"_id", "expo_id",
"name", "description", "type", "categories", "objectives", "__v"}, {"_id", "expo_id", "name", "description", "type",
"categories", "objectives", "__v"}),

    #"Rozwinięty element _id" = Table.ExpandRecordColumn(#"Rozwinięty element Column1", "_id", {"$oid"}, {"_id.$oid"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element _id",{{"_id.$oid", type text}, {"expo_id", type
text}, {"name", type text}, {"description", type text}, {"type", type text}, {"categories", type any}, {"objectives", type
any}, {"__v", Int64.Type}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"categories", each Text.Combine(List.Transform(_,
Text.From), "["), type text}),

    #"Wyodrębnione wartości1" = Table.TransformColumns(#"Wyodrębnione wartości", {"objectives", each
Text.Combine(List.Transform(_, Text.From), "["), type text}),
```

```
    #"Podzielono kolumnę według ogranicznika" = Table.ExpandListColumn(Table.TransformColumns(#"Wyodrębnione wartości1",
{{"objectives", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "objectives"),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Podzielono kolumnę według ogranicznika",{"expo_id", "name", "description",
"type", "categories", "__v"})

in

    #"Usunięto kolumny"



attackdimensions



let

    Źródło = Table.FromColumns({Lines.FromBinary(File.Contents("D:\Zabrac\DataSources\attackdimensionsannonimized.json"),
null, null)}),

    #"Przekształcono kolumnę" = Table.TransformColumns(Źródło, {"Column1", Json.Document}),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekształcono kolumnę", "Column1", {"_id", "expo_id",
"name", "description", "type", "categories", "objectives", "__v"}, {"_id", "expo_id", "name", "description", "type",
"categories", "objectives", "__v"}),

    #"Rozwinięty element _id" = Table.ExpandRecordColumn(#"Rozwinięty element Column1", "_id", {"$oid"}, {"_id.$oid"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element _id",{{"_id.$oid", type text}, {"expo_id", type
text}, {"name", type text}, {"description", type text}, {"type", type text}, {"categories", type any}, {"objectives", type
any}, {"__v", Int64.Type}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"categories", each Text.Combine(List.Transform(_,
Text.From), "["), type text}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Wyodrębnione wartości",{"objectives", "categories"})

in

    #"Usunięto kolumny"



STIX Enterprise Techniques



let

    Source = Excel.Workbook(File.Contents("D:\Zabrac\DataSources\STIX\enterprise-attack-v16.1.xlsx"), null, true),

    techniques_Sheet = Source{[Item="techniques",Kind="Sheet"]}[Data],

    #"Promoted Headers" = Table.PromoteHeaders(techniques_Sheet, [PromoteAllScalars=true]),

    #"Changed Type" = Table.TransformColumnTypes(#"Promoted Headers",{{"ID", type text}, {"STIX ID", type text}, {"name",
type text}, {"description", type text}, {"url", type text}, {"created", type date}, {"last modified", type date},
{"domain", type text}, {"version", type text}, {"tactics", type text}, {"detection", type text}, {"platforms", type text},
{"data sources", type text}, {"is sub-technique", type logical}, {"sub-technique of", type text}, {"defenses bypassed",
type text}, {"contributors", type text}, {"permissions required", type text}, {"supports remote", type logical}, {"system
requirements", type text}, {"impact type", type text}, {"effective permissions", type text}, {"relationship citations",
type text}})

in

    #"Changed Type"



STIX Enterprise Tactics



let
```

```
    Source = Excel.Workbook(File.Contents("D:\Zabrac\DataSources\STIX\enterprise-attack-v16.1.xlsx"), null, true),

    tactics_Sheet = Source{[Item="tactics",Kind="Sheet"]}[Data],

    #"Promoted Headers" = Table.PromoteHeaders(tactics_Sheet, [PromoteAllScalars=true]),

    #"Changed Type" = Table.TransformColumnTypes(#"Promoted Headers",{{"ID", type text}, {"STIX ID", type text}, {"name",
type text}, {"description", type text}, {"url", type text}, {"created", type date}, {"last modified", type date},
{"domain", type text}, {"version", type text}})

in

    #"Changed Type"



STIX ICS Techniques



let

    Source = Excel.Workbook(File.Contents("D:\Zabrac\DataSources\STIX\ics-attack-v16.1.xlsx"), null, true),

    techniques_Sheet = Source{[Item="techniques",Kind="Sheet"]}[Data],

    #"Promoted Headers" = Table.PromoteHeaders(techniques_Sheet, [PromoteAllScalars=true])

in

    #"Promoted Headers"



STIX ICS Tactics



let

    Source = Excel.Workbook(File.Contents("D:\Zabrac\DataSources\STIX\ics-attack-v16.1.xlsx"), null, true),

    tactics_Sheet = Source{[Item="tactics",Kind="Sheet"]}[Data],

    #"Promoted Headers" = Table.PromoteHeaders(tactics_Sheet, [PromoteAllScalars=true]),

    #"Changed Type" = Table.TransformColumnTypes(#"Promoted Headers",{{"ID", type text}, {"STIX ID", type text}, {"name",
type text}, {"description", type text}, {"url", type text}, {"created", type date}, {"last modified", type date},
{"domain", type text}, {"version", type text}})

in

    #"Changed Type"



STIX Mobile Techniques



let

    Source = Excel.Workbook(File.Contents("D:\Zabrac\DataSources\STIX\mobile-attack-v16.1.xlsx"), null, true),

    techniques_Sheet = Source{[Item="techniques",Kind="Sheet"]}[Data],

    #"Promoted Headers" = Table.PromoteHeaders(techniques_Sheet, [PromoteAllScalars=true])

in

    #"Promoted Headers"



STIX Mobile Tactics
```

```
let

    Source = Excel.Workbook(File.Contents("D:\Zabrac\DataSources\STIX\mobile-attack-v16.1.xlsx"), null, true),

    tactics_Sheet = Source{[Item="tactics",Kind="Sheet"]}[Data],

    #"Promoted Headers" = Table.PromoteHeaders(tactics_Sheet, [PromoteAllScalars=true]),

    #"Changed Type" = Table.TransformColumnTypes(#"Promoted Headers",{{"ID", type text}, {"STIX ID", type text}, {"name",
type text}, {"description", type text}, {"url", type text}, {"created", type date}, {"last modified", type date},
{"domain", type text}, {"version", type text}})

in

    #"Changed Type"
```

STIX Techniques

```
let

    Source = Table.Combine({#"STIX Enterprise Techniques", #"STIX ICS Techniques", #"STIX Mobile Techniques"}),

    #"Zmieniono kolejność kolumn" = Table.ReorderColumns(Source,{"ID", "STIX ID", "name", "description", "url", "created",
"last modified", "domain", "version", "tactics", "tactic type", "detection", "platforms", "data sources", "is sub-
technique", "sub-technique of", "defenses bypassed", "contributors", "permissions required", "supports remote", "system
requirements", "impact type", "effective permissions", "relationship citations", "MTC ID"})

in

    #"Zmieniono kolejność kolumn"
```

STIX Tactics

```
let

    Source = Table.Combine({#"STIX Enterprise Tactics", #"STIX ICS Tactics", #"STIX Mobile Tactics"})

in

    Source
```

filtered-attacks

```
let

    Źródło = Json.Document(File.Contents("D:\Zabrac\DataSources\filtered-attacksannonimized.json")),

    #"Przekonwertowane na tabelę" = Table.FromList(Źródło, Splitter.SplitByNothing(), null, null, ExtraValues.Error),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekonwertowane na tabelę", "Column1", {"_id", "expo_id",
"status", "category", "phase", "attack_dimensions"}, {"_id", "expo_id", "status", "category", "phase",
"attack_dimensions"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element Column1",{{"_id", type text}, {"expo_id", type
text}, {"status", type text}, {"category", type text}, {"phase", type text}, {"attack_dimensions", type any}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"attack_dimensions", each
Text.Combine(List.Transform(_, Text.From), "["), type text}),
```

```
    #"Podzielono kolumnę według ogranicznika" = Table.SplitColumn(#"Wyodrębnione wartości", "attack_dimensions",
Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), {"attack_dimensions.1", "attack_dimensions.2",
"attack_dimensions.3"}),

    #"Zmieniono typ1" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika",{{"attack_dimensions.1", type
text}, {"attack_dimensions.2", type text}}),

    #"Podzielono kolumnę według ogranicznika1" = Table.ExpandListColumn(Table.TransformColumns(#"Zmieniono typ1",
{{"attack_dimensions.2", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "attack_dimensions.2"),

    #"Zmieniono typ2" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika1",{{"attack_dimensions.2",
type text}}),

    #"Zduplikowano kolumnę" = Table.DuplicateColumn(#"Zmieniono typ2", "expo_id", "expo_id – kopia"),

    #"Zmieniono kolejność kolumn" = Table.ReorderColumns(#"Zduplikowano kolumnę",{"_id", "expo_id", "expo_id – kopia",
"status", "category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn" = Table.RenameColumns(#"Zmieniono kolejność kolumn",{{"expo_id – kopia", "BT"}}),

    #"Podział kolumny według pozycji" = Table.SplitColumn(#"Zmieniono nazwy kolumn", "BT",
Splitter.SplitTextByPositions({5, 6}), {"BT.1", "BT.2"}),

    #"Zmieniono typ3" = Table.TransformColumnTypes(#"Podział kolumny według pozycji",{{"BT.1", type text}, {"BT.2", type
text}}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Zmieniono typ3",{"BT.2"}),

    #"Zmieniono nazwy kolumn1" = Table.RenameColumns(#"Usunięto kolumny",{{"BT.1", "BT"}}),

    #"Duplicated Column" = Table.DuplicateColumn(#"Zmieniono nazwy kolumn1", "expo_id", "expo_id - Copy"),

    #"Reordered Columns" = Table.ReorderColumns(#"Duplicated Column",{"_id", "expo_id", "expo_id - Copy", "BT", "status",
"category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Duplicated Column1" = Table.DuplicateColumn(#"Reordered Columns", "expo_id - Copy", "expo_id - Copy - Copy"),

    #"Split Column by Delimiter" = Table.SplitColumn(#"Duplicated Column1", "expo_id - Copy",
Splitter.SplitTextByDelimiter(":", QuoteStyle.None), {"expo_id - Copy.1", "expo_id - Copy.2"}),

    #"Changed Type" = Table.TransformColumnTypes(#"Split Column by Delimiter",{{"expo_id - Copy.1", type text}, {"expo_id
- Copy.2", type text}}),

    #"Removed Columns" = Table.RemoveColumns(#"Changed Type",{"expo_id - Copy.2"}),

    #"Split Column by Delimiter1" = Table.SplitColumn(#"Removed Columns", "expo_id - Copy.1",
Splitter.SplitTextByDelimiter("-", QuoteStyle.Csv), {"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id - Copy.1.3",
"expo_id - Copy.1.4", "expo_id - Copy.1.5"}),

    #"Changed Type1" = Table.TransformColumnTypes(#"Split Column by Delimiter1",{{"expo_id - Copy.1.1", type text},
{"expo_id - Copy.1.2", type text}, {"expo_id - Copy.1.3", type text}, {"expo_id - Copy.1.4", type text}, {"expo_id -
Copy.1.5", type text}}),

    #"Removed Columns1" = Table.RemoveColumns(#"Changed Type1",{"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id -
Copy.1.3"}),

    #"Renamed Columns" = Table.RenameColumns(#"Removed Columns1",{{"expo_id - Copy.1.5", "objective"}}),

    #"Split Column by Delimiter2" = Table.SplitColumn(#"Renamed Columns", "expo_id - Copy.1.4",
Splitter.SplitTextByDelimiter("_", QuoteStyle.Csv), {"expo_id - Copy.1.4.1", "expo_id - Copy.1.4.2"}),

    #"Changed Type2" = Table.TransformColumnTypes(#"Split Column by Delimiter2",{{"expo_id - Copy.1.4.1", type text},
{"expo_id - Copy.1.4.2", type text}}),

    #"Renamed Columns1" = Table.RenameColumns(#"Changed Type2",{{"expo_id - Copy.1.4.1", "Workstation"}, {"expo_id -
Copy.1.4.2", "Domain"}}),

    #"Removed Columns2" = Table.RemoveColumns(#"Renamed Columns1",{"expo_id - Copy - Copy"}),

    #"Wstawiono scaloną kolumnę" = Table.AddColumn(#"Removed Columns2", "Scalone", each
Text.Combine({[attack_dimensions.3], " & ", [attack_dimensions.1], " & ", [attack_dimensions.2]}), type text),

    #"Zmieniono nazwy kolumn2" = Table.RenameColumns(#"Wstawiono scaloną kolumnę",{{"Scalone", "Dimensions combined"}}),

    #"Zamieniono wartość" = Table.ReplaceValue(#"Zmieniono nazwy kolumn2"," &  & ",null,Replacer.ReplaceValue,{"Dimensions
combined"})
```

```
in

    #"Zamieniono wartość"



filtered-attacks STIX



let

    Źródło = Json.Document(File.Contents("D:\Zabrac\DataSources\filtered-attacksannonimized.json")),

    #"Przekonwertowane na tabelę" = Table.FromList(Źródło, Splitter.SplitByNothing(), null, null, ExtraValues.Error),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekonwertowane na tabelę", "Column1", {"_id", "expo_id",
"status", "category", "phase", "attack_dimensions"}, {"_id", "expo_id", "status", "category", "phase",
"attack_dimensions"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element Column1",{{"_id", type text}, {"expo_id", type
text}, {"status", type text}, {"category", type text}, {"phase", type text}, {"attack_dimensions", type any}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"attack_dimensions", each
Text.Combine(List.Transform(_, Text.From), "["), type text}),

    #"Podzielono kolumnę według ogranicznika" = Table.SplitColumn(#"Wyodrębnione wartości", "attack_dimensions",
Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), {"attack_dimensions.1", "attack_dimensions.2",
"attack_dimensions.3"}),

    #"Zmieniono typ1" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika",{{"attack_dimensions.1", type
text}, {"attack_dimensions.2", type text}}),

    #"Podzielono kolumnę według ogranicznika1" = Table.ExpandListColumn(Table.TransformColumns(#"Zmieniono typ1",
{{"attack_dimensions.2", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "attack_dimensions.2"),

    #"Zmieniono typ2" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika1",{{"attack_dimensions.2",
type text}}),

    #"Zduplikowano kolumnę" = Table.DuplicateColumn(#"Zmieniono typ2", "expo_id", "expo_id – kopia"),

    #"Zmieniono kolejność kolumn" = Table.ReorderColumns(#"Zduplikowano kolumnę",{"_id", "expo_id", "expo_id – kopia",
"status", "category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn" = Table.RenameColumns(#"Zmieniono kolejność kolumn",{{"expo_id – kopia", "BT"}}),

    #"Podział kolumny według pozycji" = Table.SplitColumn(#"Zmieniono nazwy kolumn", "BT",
Splitter.SplitTextByPositions({5, 6}), {"BT.1", "BT.2"}),

    #"Zmieniono typ3" = Table.TransformColumnTypes(#"Podział kolumny według pozycji",{{"BT.1", type text}, {"BT.2", type
text}}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Zmieniono typ3",{"BT.2"}),

    #"Zmieniono nazwy kolumn1" = Table.RenameColumns(#"Usunięto kolumny",{{"BT.1", "BT"}}),

    #"Duplicated Column" = Table.DuplicateColumn(#"Zmieniono nazwy kolumn1", "expo_id", "expo_id - Copy"),

    #"Reordered Columns" = Table.ReorderColumns(#"Duplicated Column",{"_id", "expo_id", "expo_id - Copy", "BT", "status",
"category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Duplicated Column1" = Table.DuplicateColumn(#"Reordered Columns", "expo_id - Copy", "expo_id - Copy - Copy"),

    #"Split Column by Delimiter" = Table.SplitColumn(#"Duplicated Column1", "expo_id - Copy",
Splitter.SplitTextByDelimiter(":", QuoteStyle.None), {"expo_id - Copy.1", "expo_id - Copy.2"}),

    #"Changed Type" = Table.TransformColumnTypes(#"Split Column by Delimiter",{{"expo_id - Copy.1", type text}, {"expo_id
- Copy.2", type text}}),

    #"Removed Columns" = Table.RemoveColumns(#"Changed Type",{"expo_id - Copy.2"}),

    #"Split Column by Delimiter1" = Table.SplitColumn(#"Removed Columns", "expo_id - Copy.1",
Splitter.SplitTextByDelimiter("-", QuoteStyle.Csv), {"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id - Copy.1.3",
"expo_id - Copy.1.4", "expo_id - Copy.1.5"}),
```

```
    #"Changed Type1" = Table.TransformColumnTypes(#"Split Column by Delimiter1",{{"expo_id - Copy.1.1", type text},
{"expo_id - Copy.1.2", type text}, {"expo_id - Copy.1.3", type text}, {"expo_id - Copy.1.4", type text}, {"expo_id -
Copy.1.5", type text}}),

    #"Removed Columns1" = Table.RemoveColumns(#"Changed Type1",{"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id -
Copy.1.3"}),

    #"Renamed Columns" = Table.RenameColumns(#"Removed Columns1",{{"expo_id - Copy.1.5", "objective"}}),

    #"Split Column by Delimiter2" = Table.SplitColumn(#"Renamed Columns", "expo_id - Copy.1.4",
Splitter.SplitTextByDelimiter("_", QuoteStyle.Csv), {"expo_id - Copy.1.4.1", "expo_id - Copy.1.4.2"}),

    #"Changed Type2" = Table.TransformColumnTypes(#"Split Column by Delimiter2",{{"expo_id - Copy.1.4.1", type text},
{"expo_id - Copy.1.4.2", type text}}),

    #"Renamed Columns1" = Table.RenameColumns(#"Changed Type2",{{"expo_id - Copy.1.4.1", "Workstation"}, {"expo_id -
Copy.1.4.2", "Domain"}}),

    #"Removed Columns2" = Table.RemoveColumns(#"Renamed Columns1",{"expo_id - Copy - Copy"}),

    #"Wstawiono scaloną kolumnę" = Table.AddColumn(#"Removed Columns2", "Scalone", each
Text.Combine({[attack_dimensions.3], " & ", [attack_dimensions.1], " & ", [attack_dimensions.2]}), type text),

    #"Zmieniono nazwy kolumn2" = Table.RenameColumns(#"Wstawiono scaloną kolumnę",{{"Scalone", "Dimensions combined"}}),

    #"Zamieniono wartość" = Table.ReplaceValue(#"Zmieniono nazwy kolumn2"," &  & ",null,Replacer.ReplaceValue,{"Dimensions
combined"}),

    #"Scalone zapdefaceania" = Table.NestedJoin(#"Zamieniono wartość", {"attack_dimensions.3"}, #"tactics LLM",
{"Column1.event_id"}, "tactics LLM", JoinKind.LeftOuter),

    #"Rozwinięty element tactics LLM" = Table.ExpandTableColumn(#"Scalone zapytania", "tactics LLM",
{"Column1.regex_matches_summary_descriptive"}, {"tactics LLM.Column1.regex_matches_summary_descriptive"}),

    #"Zmieniono kolejność kolumn1" = Table.ReorderColumns(#"Rozwinięty element tactics LLM",{"_id", "expo_id",
"Workstation", "Domain", "objective", "BT", "status", "category", "phase", "tactics
LLM.Column1.regex_matches_summary_descriptive", "attack_dimensions.3", "attack_dimensions.1", "attack_dimensions.2",
"Dimensions combined"}),

    #"Scalone zapytania1" = Table.NestedJoin(#"Zmieniono kolejność kolumn1", {"attack_dimensions.1"}, #"tactics LLM",
{"Column1.event_id"}, "tactics LLM", JoinKind.LeftOuter),

    #"Rozwinięty element tactics LLM1" = Table.ExpandTableColumn(#"Scalone zapytania1", "tactics LLM",
{"Column1.regex_matches_summary_descriptive"}, {"tactics LLM.Column1.regex_matches_summary_descriptive.1"}),

    #"Zmieniono kolejność kolumn2" = Table.ReorderColumns(#"Rozwinięty element tactics LLM1",{"_id", "expo_id",
"Workstation", "Domain", "objective", "BT", "status", "category", "phase", "tactics
LLM.Column1.regex_matches_summary_descriptive", "attack_dimensions.3", "tactics
LLM.Column1.regex_matches_summary_descriptive.1", "attack_dimensions.1", "attack_dimensions.2", "Dimensions combined"}),

    #"Scalone zapytania2" = Table.NestedJoin(#"Zmieniono kolejność kolumn2", {"attack_dimensions.2"}, #"tactics LLM",
{"Column1.event_id"}, "tactics LLM", JoinKind.LeftOuter),

    #"Rozwinięty element tactics LLM2" = Table.ExpandTableColumn(#"Scalone zapytania2", "tactics LLM",
{"Column1.regex_matches_summary_descriptive"}, {"tactics LLM.Column1.regex_matches_summary_descriptive.2"}),

    #"Zmieniono kolejność kolumn3" = Table.ReorderColumns(#"Rozwinięty element tactics LLM2",{"_id", "expo_id",
"Workstation", "Domain", "objective", "BT", "status", "category", "phase", "tactics
LLM.Column1.regex_matches_summary_descriptive", "attack_dimensions.3", "tactics
LLM.Column1.regex_matches_summary_descriptive.1", "attack_dimensions.1", "tactics
LLM.Column1.regex_matches_summary_descriptive.2", "attack_dimensions.2", "Dimensions combined"}),

    #"Posortowano wiersze" = Table.Sort(#"Zmieniono kolejność kolumn3",{{"attack_dimensions.3", Order.Descending}}),

    #"Wstawiono scaloną kolumnę1" = Table.AddColumn(#"Posortowano wiersze", "Scalone", each Text.Combine({[tactics
LLM.Column1.regex_matches_summary_descriptive], " & ", [tactics LLM.Column1.regex_matches_summary_descriptive.1], " & ",
[tactics LLM.Column1.regex_matches_summary_descriptive.2]}), type text),

    #"Zmieniono nazwy kolumn3" = Table.RenameColumns(#"Wstawiono scaloną kolumnę1",{{"Scalone", "Tactics combined"}}),

    #"Scalone zapytania3" = Table.NestedJoin(#"Zmieniono nazwy kolumn3", {"attack_dimensions.3"}, #"techniques LLM",
{"Column1.event_id"}, "techniques LLM", JoinKind.LeftOuter),

    #"Rozwinięty element techniques LLM" = Table.ExpandTableColumn(#"Scalone zapytania3", "techniques LLM",
{"Column1.regex_matches_summary_descriptive"}, {"techniques LLM.Column1.regex_matches_summary_descriptive"}),

    #"Zmieniono kolejność kolumn4" = Table.ReorderColumns(#"Rozwinięty element techniques LLM",{"_id", "expo_id",
"Workstation", "Domain", "objective", "BT", "status", "category", "phase", "tactics
LLM.Column1.regex_matches_summary_descriptive", "techniques LLM.Column1.regex_matches_summary_descriptive",
```

```
"attack_dimensions.3", "tactics LLM.Column1.regex_matches_summary_descriptive.1", "attack_dimensions.1", "tactics
LLM.Column1.regex_matches_summary_descriptive.2", "attack_dimensions.2", "Dimensions combined", "Tactics combined"}),

    #"Merged Queries" = Table.NestedJoin(#"Zmieniono kolejność kolumn4", {"attack_dimensions.1"}, #"techniques LLM",
{"Column1.event_id"}, "techniques LLM", JoinKind.LeftOuter),

    #"Expanded techniques LLM" = Table.ExpandTableColumn(#"Merged Queries", "techniques LLM",
{"Column1.regex_matches_summary_descriptive"}, {"Column1.regex_matches_summary_descriptive"}),

    #"Reordered Columns1" = Table.ReorderColumns(#"Expanded techniques LLM",{"_id", "expo_id", "Workstation", "Domain",
"objective", "BT", "status", "category", "phase", "tactics LLM.Column1.regex_matches_summary_descriptive", "techniques
LLM.Column1.regex_matches_summary_descriptive", "attack_dimensions.3", "tactics
LLM.Column1.regex_matches_summary_descriptive.1", "Column1.regex_matches_summary_descriptive", "attack_dimensions.1",
"tactics LLM.Column1.regex_matches_summary_descriptive.2", "attack_dimensions.2", "Dimensions combined", "Tactics
combined"}),

    #"Merged Queries1" = Table.NestedJoin(#"Reordered Columns1", {"attack_dimensions.2"}, #"techniques LLM",
{"Column1.event_id"}, "techniques LLM", JoinKind.LeftOuter),

    #"Expanded techniques LLM1" = Table.ExpandTableColumn(#"Merged Queries1", "techniques LLM",
{"Column1.regex_matches_summary_descriptive"}, {"techniques LLM.Column1.regex_matches_summary_descriptive.1"}),

    #"Reordered Columns2" = Table.ReorderColumns(#"Expanded techniques LLM1",{"_id", "expo_id", "Workstation", "Domain",
"objective", "BT", "status", "category", "phase", "tactics LLM.Column1.regex_matches_summary_descriptive", "techniques
LLM.Column1.regex_matches_summary_descriptive", "attack_dimensions.3", "tactics
LLM.Column1.regex_matches_summary_descriptive.1", "Column1.regex_matches_summary_descriptive", "attack_dimensions.1",
"tactics LLM.Column1.regex_matches_summary_descriptive.2", "techniques LLM.Column1.regex_matches_summary_descriptive.1",
"attack_dimensions.2", "Dimensions combined", "Tactics combined"}),

    #"Inserted Merged Column" = Table.AddColumn(#"Reordered Columns2", "Merged", each Text.Combine({[techniques
LLM.Column1.regex_matches_summary_descriptive], " & ", [Column1.regex_matches_summary_descriptive], " & ", [techniques
LLM.Column1.regex_matches_summary_descriptive.1]}), type text)

in

    #"Inserted Merged Column"



filtered-attacks dimenssion 1



let

    Źródło = Json.Document(File.Contents("D:\Zabrac\DataSources\filtered-attacksannonimized.json")),

    #"Przekonwertowane na tabelę" = Table.FromList(Źródło, Splitter.SplitByNothing(), null, null, ExtraValues.Error),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekonwertowane na tabelę", "Column1", {"_id", "expo_id",
"status", "category", "phase", "attack_dimensions"}, {"_id", "expo_id", "status", "category", "phase",
"attack_dimensions"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element Column1",{{"_id", type text}, {"expo_id", type
text}, {"status", type text}, {"category", type text}, {"phase", type text}, {"attack_dimensions", type any}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"attack_dimensions", each
Text.Combine(List.Transform(_, Text.From), ["]), type text}),

    #"Podzielono kolumnę według ogranicznika" = Table.SplitColumn(#"Wyodrębnione wartości", "attack_dimensions",
Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), {"attack_dimensions.1", "attack_dimensions.2",
"attack_dimensions.3"}),

    #"Zmieniono typ1" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika",{{"attack_dimensions.1", type
text}, {"attack_dimensions.2", type text}}),

    #"Podzielono kolumnę według ogranicznika1" = Table.ExpandListColumn(Table.TransformColumns(#"Zmieniono typ1",
{{"attack_dimensions.2", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "attack_dimensions.2"),

    #"Zmieniono typ2" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika1",{{"attack_dimensions.2",
type text}}),

    #"Zduplikowano kolumnę" = Table.DuplicateColumn(#"Zmieniono typ2", "expo_id", "expo_id – kopia"),

    #"Zmieniono kolejność kolumn" = Table.ReorderColumns(#"Zduplikowano kolumnę",{"_id", "expo_id", "expo_id – kopia",
"status", "category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn" = Table.RenameColumns(#"Zmieniono kolejność kolumn",{{"expo_id – kopia", "BT"}}),
```

```
    #"Podział kolumny według pozycji" = Table.SplitColumn(#"Zmieniono nazwy kolumn", "BT",
Splitter.SplitTextByPositions({5, 6}), {"BT.1", "BT.2"}),

    #"Zmieniono typ3" = Table.TransformColumnTypes(#"Podział kolumny według pozycji",{{"BT.1", type text}, {"BT.2", type
text}}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Zmieniono typ3",{"BT.2"}),

    #"Zmieniono nazwy kolumn1" = Table.RenameColumns(#"Usunięto kolumny",{{"BT.1", "BT"}}),

    #"Duplicated Column" = Table.DuplicateColumn(#"Zmieniono nazwy kolumn1", "expo_id", "expo_id - Copy"),

    #"Reordered Columns" = Table.ReorderColumns(#"Duplicated Column",{"_id", "expo_id", "expo_id - Copy", "BT", "status",
"category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Duplicated Column1" = Table.DuplicateColumn(#"Reordered Columns", "expo_id - Copy", "expo_id - Copy - Copy"),

    #"Split Column by Delimiter" = Table.SplitColumn(#"Duplicated Column1", "expo_id - Copy",
Splitter.SplitTextByDelimiter(":", QuoteStyle.None), {"expo_id - Copy.1", "expo_id - Copy.2"}),

    #"Changed Type" = Table.TransformColumnTypes(#"Split Column by Delimiter",{{"expo_id - Copy.1", type text}, {"expo_id
- Copy.2", type text}}),

    #"Removed Columns" = Table.RemoveColumns(#"Changed Type",{"expo_id - Copy.2"}),

    #"Split Column by Delimiter1" = Table.SplitColumn(#"Removed Columns", "expo_id - Copy.1",
Splitter.SplitTextByDelimiter("-", QuoteStyle.Csv), {"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id - Copy.1.3",
"expo_id - Copy.1.4", "expo_id - Copy.1.5"}),

    #"Changed Type1" = Table.TransformColumnTypes(#"Split Column by Delimiter1",{{"expo_id - Copy.1.1", type text},
{"expo_id - Copy.1.2", type text}, {"expo_id - Copy.1.3", type text}, {"expo_id - Copy.1.4", type text}, {"expo_id -
Copy.1.5", type text}}),

    #"Removed Columns1" = Table.RemoveColumns(#"Changed Type1",{"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id -
Copy.1.3"}),

    #"Renamed Columns" = Table.RenameColumns(#"Removed Columns1",{{"expo_id - Copy.1.5", "objective"}}),

    #"Split Column by Delimiter2" = Table.SplitColumn(#"Renamed Columns", "expo_id - Copy.1.4",
Splitter.SplitTextByDelimiter("_", QuoteStyle.Csv), {"expo_id - Copy.1.4.1", "expo_id - Copy.1.4.2"}),

    #"Changed Type2" = Table.TransformColumnTypes(#"Split Column by Delimiter2",{{"expo_id - Copy.1.4.1", type text},
{"expo_id - Copy.1.4.2", type text}}),

    #"Renamed Columns1" = Table.RenameColumns(#"Changed Type2",{{"expo_id - Copy.1.4.1", "Workstation"}, {"expo_id -
Copy.1.4.2", "Domain"}}),

    #"Removed Columns2" = Table.RemoveColumns(#"Renamed Columns1",{"expo_id - Copy - Copy", "attack_dimensions.3",
"attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn2" = Table.RenameColumns(#"Removed Columns2",{{"attack_dimensions.1", "attack_dimensions"}})

in

    #"Zmieniono nazwy kolumn2"



filtered-attacks dimenssion 2



let

    Źródło = Json.Document(File.Contents("D:\Zabrac\DataSources\filtered-attacksannonimized.json")),

    #"Przekonwertowane na tabelę" = Table.FromList(Źródło, Splitter.SplitByNothing(), null, null, ExtraValues.Error),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekonwertowane na tabelę", "Column1", {"_id", "expo_id",
"status", "category", "phase", "attack_dimensions"}, {"_id", "expo_id", "status", "category", "phase",
"attack_dimensions"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element Column1",{{"_id", type text}, {"expo_id", type
text}, {"status", type text}, {"category", type text}, {"phase", type text}, {"attack_dimensions", type any}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"attack_dimensions", each
Text.Combine(List.Transform(_, Text.From), [""]), type text}),
```

```
    #"Podzielono kolumnę według ogranicznika" = Table.SplitColumn(#"Wyodrębnione wartości", "attack_dimensions",
Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), {"attack_dimensions.1", "attack_dimensions.2",
"attack_dimensions.3"}),

    #"Zmieniono typ1" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika",{{"attack_dimensions.1", type
text}, {"attack_dimensions.2", type text}}),

    #"Podzielono kolumnę według ogranicznika1" = Table.ExpandListColumn(Table.TransformColumns(#"Zmieniono typ1",
{{"attack_dimensions.2", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "attack_dimensions.2"),

    #"Zmieniono typ2" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika1",{{"attack_dimensions.2",
type text}}),

    #"Zduplikowano kolumnę" = Table.DuplicateColumn(#"Zmieniono typ2", "expo_id", "expo_id – kopia"),

    #"Zmieniono kolejność kolumn" = Table.ReorderColumns(#"Zduplikowano kolumnę",{"_id", "expo_id", "expo_id – kopia",
"status", "category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn" = Table.RenameColumns(#"Zmieniono kolejność kolumn",{{"expo_id – kopia", "BT"}}),

    #"Podział kolumny według pozycji" = Table.SplitColumn(#"Zmieniono nazwy kolumn", "BT",
Splitter.SplitTextByPositions({5, 6}), {"BT.1", "BT.2"}),

    #"Zmieniono typ3" = Table.TransformColumnTypes(#"Podział kolumny według pozycji",{{"BT.1", type text}, {"BT.2", type
text}}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Zmieniono typ3",{"BT.2"}),

    #"Zmieniono nazwy kolumn1" = Table.RenameColumns(#"Usunięto kolumny",{{"BT.1", "BT"}}),

    #"Duplicated Column" = Table.DuplicateColumn(#"Zmieniono nazwy kolumn1", "expo_id", "expo_id - Copy"),

    #"Reordered Columns" = Table.ReorderColumns(#"Duplicated Column",{"_id", "expo_id", "expo_id - Copy", "BT", "status",
"category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Duplicated Column1" = Table.DuplicateColumn(#"Reordered Columns", "expo_id - Copy", "expo_id - Copy - Copy"),

    #"Split Column by Delimiter" = Table.SplitColumn(#"Duplicated Column1", "expo_id - Copy",
Splitter.SplitTextByDelimiter(":", QuoteStyle.None), {"expo_id - Copy.1", "expo_id - Copy.2"}),

    #"Changed Type" = Table.TransformColumnTypes(#"Split Column by Delimiter",{{"expo_id - Copy.1", type text}, {"expo_id
- Copy.2", type text}}),

    #"Removed Columns" = Table.RemoveColumns(#"Changed Type",{"expo_id - Copy.2"}),

    #"Split Column by Delimiter1" = Table.SplitColumn(#"Removed Columns", "expo_id - Copy.1",
Splitter.SplitTextByDelimiter("-", QuoteStyle.Csv), {"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id - Copy.1.3",
"expo_id - Copy.1.4", "expo_id - Copy.1.5"}),

    #"Changed Type1" = Table.TransformColumnTypes(#"Split Column by Delimiter1",{{"expo_id - Copy.1.1", type text},
{"expo_id - Copy.1.2", type text}, {"expo_id - Copy.1.3", type text}, {"expo_id - Copy.1.4", type text}, {"expo_id -
Copy.1.5", type text}}),

    #"Removed Columns1" = Table.RemoveColumns(#"Changed Type1",{"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id -
Copy.1.3"}),

    #"Renamed Columns" = Table.RenameColumns(#"Removed Columns1",{{"expo_id - Copy.1.5", "objective"}}),

    #"Split Column by Delimiter2" = Table.SplitColumn(#"Renamed Columns", "expo_id - Copy.1.4",
Splitter.SplitTextByDelimiter("_", QuoteStyle.Csv), {"expo_id - Copy.1.4.1", "expo_id - Copy.1.4.2"}),

    #"Changed Type2" = Table.TransformColumnTypes(#"Split Column by Delimiter2",{{"expo_id - Copy.1.4.1", type text},
{"expo_id - Copy.1.4.2", type text}}),

    #"Renamed Columns1" = Table.RenameColumns(#"Changed Type2",{{"expo_id - Copy.1.4.1", "Workstation"}, {"expo_id -
Copy.1.4.2", "Domain"}}),

    #"Removed Columns2" = Table.RemoveColumns(#"Renamed Columns1",{"expo_id - Copy - Copy", "attack_dimensions.3",
"attack_dimensions.1"}),

    #"Zmieniono nazwy kolumn2" = Table.RenameColumns(#"Removed Columns2",{{"attack_dimensions.2", "attack_dimensions"}})

in

    #"Zmieniono nazwy kolumn2"
```

filtered-attacks dimenssion 3

```
let

    Źródło = Json.Document(File.Contents("D:\Zabrac\DataSources\filtered-attacksannonimized.json")),

    #"Przekonwertowane na tabelę" = Table.FromList(Źródło, Splitter.SplitByNothing(), null, null, ExtraValues.Error),

    #"Rozwinięty element Column1" = Table.ExpandRecordColumn(#"Przekonwertowane na tabelę", "Column1", {"_id", "expo_id",
"status", "category", "phase", "attack_dimensions"}, {"_id", "expo_id", "status", "category", "phase",
"attack_dimensions"}),

    #"Zmieniono typ" = Table.TransformColumnTypes(#"Rozwinięty element Column1",{{"_id", type text}, {"expo_id", type
text}, {"status", type text}, {"category", type text}, {"phase", type text}, {"attack_dimensions", type any}}),

    #"Wyodrębnione wartości" = Table.TransformColumns(#"Zmieniono typ", {"attack_dimensions", each
Text.Combine(List.Transform(_, Text.From), "["), type text}),

    #"Podzielono kolumnę według ogranicznika" = Table.SplitColumn(#"Wyodrębnione wartości", "attack_dimensions",
Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), {"attack_dimensions.1", "attack_dimensions.2",
"attack_dimensions.3"}),

    #"Zmieniono typ1" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika",{{"attack_dimensions.1", type
text}, {"attack_dimensions.2", type text}}),

    #"Podzielono kolumnę według ogranicznika1" = Table.ExpandListColumn(Table.TransformColumns(#"Zmieniono typ1",
{{"attack_dimensions.2", Splitter.SplitTextByDelimiter("[", QuoteStyle.Csv), let itemType = (type nullable text) meta
[Serialized.Text = true] in type {itemType}}}), "attack_dimensions.2"),

    #"Zmieniono typ2" = Table.TransformColumnTypes(#"Podzielono kolumnę według ogranicznika1",{{"attack_dimensions.2",
type text}}),

    #"Zduplikowano kolumnę" = Table.DuplicateColumn(#"Zmieniono typ2", "expo_id", "expo_id – kopia"),

    #"Zmieniono kolejność kolumn" = Table.ReorderColumns(#"Zduplikowano kolumnę",{"_id", "expo_id", "expo_id – kopia",
"status", "category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn" = Table.RenameColumns(#"Zmieniono kolejność kolumn",{{"expo_id – kopia", "BT"}}),

    #"Podział kolumny według pozycji" = Table.SplitColumn(#"Zmieniono nazwy kolumn", "BT",
Splitter.SplitTextByPositions({5, 6}), {"BT.1", "BT.2"}),

    #"Zmieniono typ3" = Table.TransformColumnTypes(#"Podział kolumny według pozycji",{{"BT.1", type text}, {"BT.2", type
text}}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Zmieniono typ3",{"BT.2"}),

    #"Zmieniono nazwy kolumn1" = Table.RenameColumns(#"Usunięto kolumny",{{"BT.1", "BT"}}),

    #"Duplicated Column" = Table.DuplicateColumn(#"Zmieniono nazwy kolumn1", "expo_id", "expo_id - Copy"),

    #"Reordered Columns" = Table.ReorderColumns(#"Duplicated Column",{"_id", "expo_id", "expo_id - Copy", "BT", "status",
"category", "phase", "attack_dimensions.1", "attack_dimensions.2"}),

    #"Duplicated Column1" = Table.DuplicateColumn(#"Reordered Columns", "expo_id - Copy", "expo_id - Copy - Copy"),

    #"Split Column by Delimiter" = Table.SplitColumn(#"Duplicated Column1", "expo_id - Copy",
Splitter.SplitTextByDelimiter(":", QuoteStyle.None), {"expo_id - Copy.1", "expo_id - Copy.2"}),

    #"Changed Type" = Table.TransformColumnTypes(#"Split Column by Delimiter",{{"expo_id - Copy.1", type text}, {"expo_id
- Copy.2", type text}}),

    #"Removed Columns" = Table.RemoveColumns(#"Changed Type",{"expo_id - Copy.2"}),

    #"Split Column by Delimiter1" = Table.SplitColumn(#"Removed Columns", "expo_id - Copy.1",
Splitter.SplitTextByDelimiter("-", QuoteStyle.Csv), {"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id - Copy.1.3",
"expo_id - Copy.1.4", "expo_id - Copy.1.5"}),

    #"Changed Type1" = Table.TransformColumnTypes(#"Split Column by Delimiter1",{{"expo_id - Copy.1.1", type text},
{"expo_id - Copy.1.2", type text}, {"expo_id - Copy.1.3", type text}, {"expo_id - Copy.1.4", type text}, {"expo_id -
Copy.1.5", type text}}),

    #"Removed Columns1" = Table.RemoveColumns(#"Changed Type1",{"expo_id - Copy.1.1", "expo_id - Copy.1.2", "expo_id -
Copy.1.3"}),

    #"Renamed Columns" = Table.RenameColumns(#"Removed Columns1",{{"expo_id - Copy.1.5", "objective"}}),
```

```
    #"Split Column by Delimiter2" = Table.SplitColumn(#"Renamed Columns", "expo_id - Copy.1.4",
Splitter.SplitTextByDelimiter("_", QuoteStyle.Csv), {"expo_id - Copy.1.4.1", "expo_id - Copy.1.4.2"}),

    #"Changed Type2" = Table.TransformColumnTypes(#"Split Column by Delimiter2",{{"expo_id - Copy.1.4.1", type text},
{"expo_id - Copy.1.4.2", type text}}),

    #"Renamed Columns1" = Table.RenameColumns(#"Changed Type2",{{"expo_id - Copy.1.4.1", "Workstation"}, {"expo_id -
Copy.1.4.2", "Domain"}}),

    #"Removed Columns2" = Table.RemoveColumns(#"Renamed Columns1",{"expo_id - Copy - Copy", "attack_dimensions.1",
"attack_dimensions.2"}),

    #"Zmieniono nazwy kolumn2" = Table.RenameColumns(#"Removed Columns2",{{"attack_dimensions.3", "attack_dimensions"}})

in

    #"Zmieniono nazwy kolumn2"



filtered-attacks dimenssion appended



let

    Źródło = Table.Combine({#"filtered-attacks dimenssion 1", #"filtered-attacks dimenssion 2", #"filtered-attacks
dimenssion 3"}),

    #"Scalone zapytania" = Table.NestedJoin(Źródło, {"attack_dimensions"}, #"tactics LLM", {"Column1.event_id"}, "tactics
LLM", JoinKind.LeftOuter),

    #"Rozwinięty element tactics LLM" = Table.ExpandTableColumn(#"Scalone zapytania", "tactics LLM",
{"Column1.regex_matches_summary_descriptive"}, {"tactics LLM.Column1.regex_matches_summary_descriptive"}),

    #"Zmieniono nazwy kolumn" = Table.RenameColumns(#"Rozwinięty element tactics LLM",{{"tactics
LLM.Column1.regex_matches_summary_descriptive", "Tactic"}}),

    #"Scalone zapytania1" = Table.NestedJoin(#"Zmieniono nazwy kolumn", {"attack_dimensions"}, #"techniques LLM",
{"Column1.event_id"}, "techniques LLM", JoinKind.LeftOuter),

    #"Rozwinięty element techniques LLM" = Table.ExpandTableColumn(#"Scalone zapytania1", "techniques LLM",
{"Column1.regex_matches_summary_descriptive"}, {"techniques LLM.Column1.regex_matches_summary_descriptive"})

in

    #"Rozwinięty element techniques LLM"



tactics LLM



let

    Źródło = Table.FromColumns({Lines.FromBinary(File.Contents("D:\Zabrac\DataSources\tactics LLM.json"), null, null)}),

    #"Przekształcono kolumnę" = Table.TransformColumns(Źródło, {"Column1", Json.Document}),

    #"Rozwinięty element Column2" = Table.ExpandRecordColumn(#"Przekształcono kolumnę", "Column1", {"prompt", "event_id",
"event_description", "summary_json", "summary_descriptive", "regex_matches_summary_json",
"regex_matches_summary_descriptive"}, {"Column1.prompt", "Column1.event_id", "Column1.event_description",
"Column1.summary_json", "Column1.summary_descriptive", "Column1.regex_matches_summary_json",
"Column1.regex_matches_summary_descriptive"}),

    #"Usunięto pierwsze wiersze1" = Table.Skip(#"Rozwinięty element Column2",1),

    #"Rozwinięty element Column1.summary_json" = Table.ExpandRecordColumn(#"Usunięto pierwsze wiersze1",
"Column1.summary_json", {"summary"}, {"Column1.summary_json.summary"}),

    #"Rozwinięty element Column1.summary_descriptive" = Table.ExpandRecordColumn(#"Rozwinięty element
Column1.summary_json", "Column1.summary_descriptive", {"summary"}, {"Column1.summary_descriptive.summary"}),

    #"Rozwinięty element Column1.regex_matches_summary_json" = Table.ExpandListColumn(#"Rozwinięty element
Column1.summary_descriptive", "Column1.regex_matches_summary_json"),
```

```
    #"Rozwinięty element Column1.regex_matches_summary_descriptive" = Table.ExpandListColumn(#"Rozwinięty element
Column1.regex_matches_summary_json", "Column1.regex_matches_summary_descriptive"),

    #"Przefiltrowano wiersze" = Table.SelectRows(#"Rozwinięty element Column1.regex_matches_summary_descriptive", each
([Column1.regex_matches_summary_descriptive] <> null)),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Przefiltrowano wiersze",{"Column1.prompt"})

in

    #"Usunięto kolumny"



techniques LLM



let

    Źródło = Table.FromColumns({Lines.FromBinary(File.Contents("D:\Zabrac\DataSources\techniques LLM.json"), null,
null)}),

    #"Przekształcono kolumnę" = Table.TransformColumns(Źródło, {"Column1", Json.Document}),

    #"Rozwinięty element Column2" = Table.ExpandRecordColumn(#"Przekształcono kolumnę", "Column1", {"prompt", "event_id",
"event_description", "summary_json", "summary_descriptive", "regex_matches_summary_json",
"regex_matches_summary_descriptive"}, {"Column1.prompt", "Column1.event_id", "Column1.event_description",
"Column1.summary_json", "Column1.summary_descriptive", "Column1.regex_matches_summary_json",
"Column1.regex_matches_summary_descriptive"}),

    #"Usunięto kolumny" = Table.RemoveColumns(#"Rozwinięty element Column2",{"Column1.prompt"}),

    #"Usunięto pierwsze wiersze1" = Table.Skip(#"Usunięto kolumny",1),

    #"Rozwinięty element Column1.regex_matches_summary_json" = Table.ExpandListColumn(#"Usunięto pierwsze wiersze1",
"Column1.regex_matches_summary_json"),

    #"Rozwinięty element Column1.regex_matches_summary_descriptive" = Table.ExpandListColumn(#"Rozwinięty element
Column1.regex_matches_summary_json", "Column1.regex_matches_summary_descriptive"),

    #"Przefiltrowano wiersze" = Table.SelectRows(#"Rozwinięty element Column1.regex_matches_summary_descriptive", each
([Column1.regex_matches_summary_descriptive] <> null))

in

    #"Przefiltrowano wiersze"
```

Appendix 2 - Complete Research Design Model

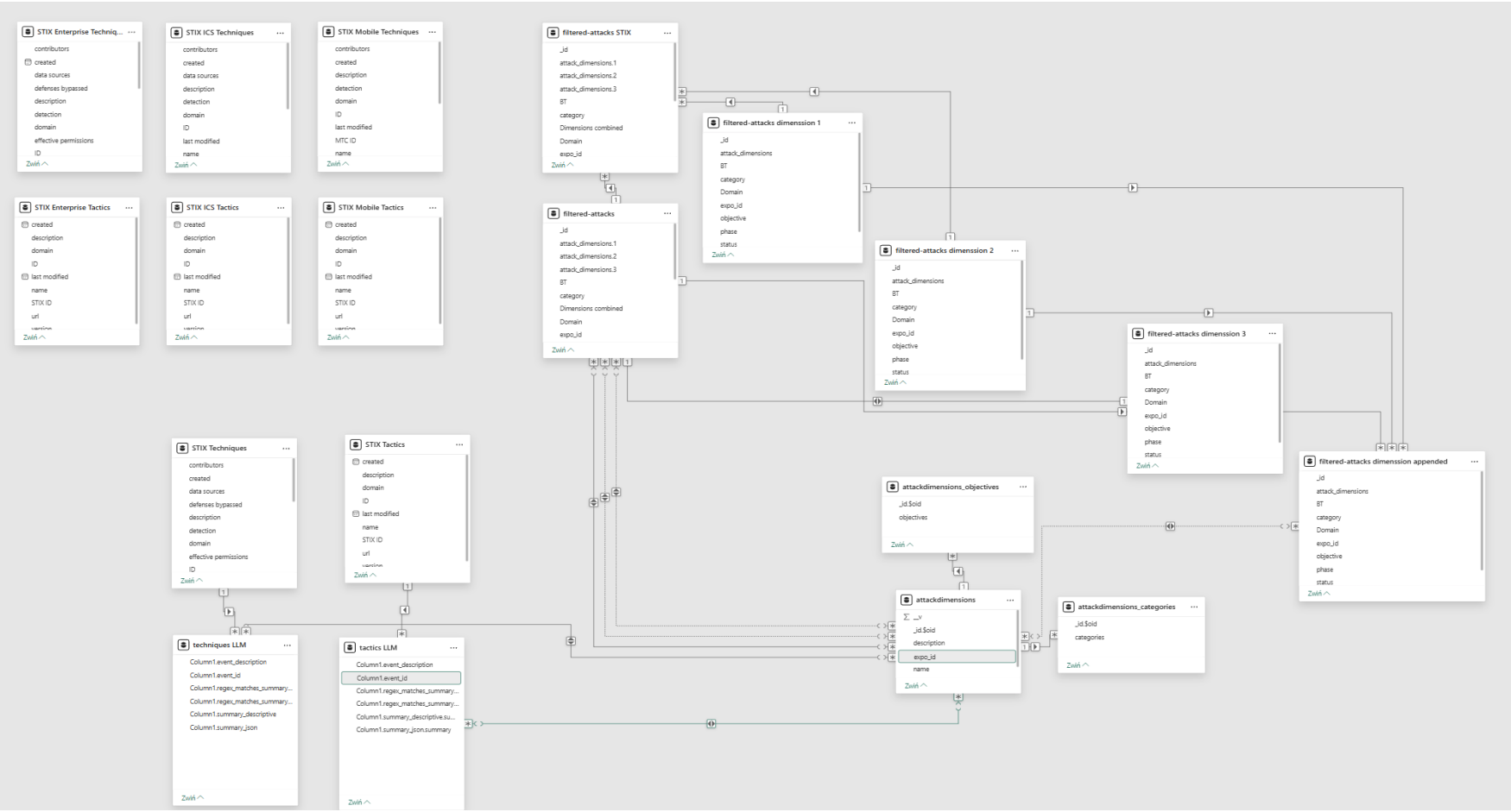

Figure 25. PowerBI for measuring attack success in existing setup

Appendix 3 - LLM_script_for_Tactics_Structure.py

```
import logging
import csv
import pandas as pd
from pydantic import BaseModel
import ollama
import re
import json



logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)

MODEL_NAME = 'llama3.3:70b'



class Tactic(BaseModel):
    identifier: str
    description: str



def read_csv_file(csv_file_path: str) -> str:
    """Read CSV file as raw string."""
    try:
        with open(csv_file_path, 'r', encoding='utf-8') as f:
            reader = csv.reader(f)
            return '\n'.join([','.join(row) for row in reader])

    except FileNotFoundError:
        logger.exception("CSV file not found")
        raise


def extract_Tactic_ids(text: str):
    """
    Extract MITRE Tactic IDs like:
    TA0004
    TA0041
    """
    pattern = r"TA\d{4}"
    return re.findall(pattern, text)



class OllamaSession:
    """
    Maintains conversation history between requests.
    """

    def __init__(self, model: str):
        self.model = model
        self.messages = []
```

```
    def add_system_message(self, content: str):
        self.messages.append({
            'role': 'system',
            'content': content
        })

    def chat(self, prompt: str) -> str:
        """
        Send prompt while preserving full history.
        """

        # Add user message
        self.messages.append({
            'role': 'user',
            'content': prompt
        })

        response = ollama.chat(
            model=self.model,
            messages=self.messages
        )

        if 'message' not in response:
            raise ValueError("No message in Ollama response")

        assistant_message = response['message']['content']

        # Store assistant reply in history
        self.messages.append({
            'role': 'assistant',
            'content': assistant_message
        })

        return assistant_message


def process_event(session: OllamaSession, event_id, event_description):

    prompt = f"""
Match the best MITRE ATT&CK Tactic ID for this event.

Event:
{event_description}

Rules:
- Return ONLY ONE Tactic ID
- First line = Tactic ID
- Second line = reasoning
- Use only IDs from previously provided STIX data
"""

    response = session.chat(prompt)

    print("\n------------------------")
    print(f"EVENT ID: {event_id}")
    print(response)

    matches = extract_Tactic_ids(response)
```

```
    data = {
        'event_id': event_id,
        'event_description': event_description,
        'response': response,
        'matched_ids': matches
    }

    try:
        with open('output_with_related_summary_Tactics.json', 'a',
encoding='utf-8') as f:
            json.dump(data, f, ensure_ascii=False)
            f.write('\n')

    except Exception:
        logger.exception("Failed writing output file")
        raise



def main():



    csv_data = read_csv_file('Tactics.csv')


    session = OllamaSession(MODEL_NAME)

    initial_prompt = f"""
You are provided with a MITRE ATT&CK / STIX Tactics database.

Rules:
- Remember all Tactic IDs and descriptions
- Never modify Tactic IDs
- Use ONLY Tactics from this dataset
- Keep mappings consistent across future requests

CSV DATA:
{csv_data}
"""

    session.add_system_message(initial_prompt)

    logger.info("STIX database loaded into conversation memory")


    events = pd.read_csv(
        'events.csv',
        delimiter=';',
        usecols=[0, 1],
        names=['event_id', 'description']
    )


    for _, row in events.iterrows():

        event_id = row['event_id']
        event_description = row['description']
```

```
        process_event(
            session,
            event_id,
            event_description
        )


if __name__ == "__main__":
    main()
```

Appendix 4 - LLM_script_for_Techniques_Structure.py

```
import logging
import csv
import pandas as pd
from pydantic import BaseModel
import ollama
import re
import json



logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)

MODEL_NAME = 'llama3.3:70b'


class Technique(BaseModel):
    identifier: str
    description: str



def read_csv_file(csv_file_path: str) -> str:
    """Read CSV file as raw string."""
    try:
        with open(csv_file_path, 'r', encoding='utf-8') as f:
            reader = csv.reader(f)
            return '\n'.join([','.join(row) for row in reader])

    except FileNotFoundError:
        logger.exception("CSV file not found")
        raise


def extract_technique_ids(text: str):
    """
    Extract MITRE technique IDs like:
    T1059
    T1566
    """
    pattern = r"T\d{4}"
    return re.findall(pattern, text)



class OllamaSession:
    """
    Maintains conversation history between requests.
    """

    def __init__(self, model: str):
        self.model = model
        self.messages = []

    def add_system_message(self, content: str):
        self.messages.append({
            'role': 'system',
```

```
            'content': content
        })

    def chat(self, prompt: str) -> str:
        """
        Send prompt while preserving full history.
        """

        # Add user message
        self.messages.append({
            'role': 'user',
            'content': prompt
        })

        response = ollama.chat(
            model=self.model,
            messages=self.messages
        )

        if 'message' not in response:
            raise ValueError("No message in Ollama response")

        assistant_message = response['message']['content']

        # Store assistant reply in history
        self.messages.append({
            'role': 'assistant',
            'content': assistant_message
        })

        return assistant_message



def process_event(session: OllamaSession, event_id, event_description):

    prompt = f"""
Match the best MITRE ATT&CK technique ID for this event.

Event:
{event_description}

Rules:
- Return ONLY ONE technique ID
- First line = technique ID
- Second line = reasoning
- Use only IDs from previously provided STIX data
"""

    response = session.chat(prompt)

    print("\n------------------------")
    print(f"EVENT ID: {event_id}")
    print(response)

    matches = extract_technique_ids(response)

    data = {
```

```
        'event_id': event_id,
        'event_description': event_description,
        'response': response,
        'matched_ids': matches
    }

    try:
        with open('output_with_related_summary_techniques.json', 'a',
encoding='utf-8') as f:
            json.dump(data, f, ensure_ascii=False)
            f.write('\n')

    except Exception:
        logger.exception("Failed writing output file")
        raise




def main():



    csv_data = read_csv_file('Techniques.csv')


    session = OllamaSession(MODEL_NAME)

    # Initial context
    initial_prompt = f"""
You are provided with a MITRE ATT&CK / STIX techniques database.

Rules:
- Remember all technique IDs and descriptions
- Never modify technique IDs
- Use ONLY techniques from this dataset
- Keep mappings consistent across future requests

CSV DATA:
{csv_data}
"""

    session.add_system_message(initial_prompt)

    logger.info("STIX database loaded into conversation memory")



    events = pd.read_csv(
        'events.csv',
        delimiter=';',
        usecols=[0, 1],
        names=['event_id', 'description']
    )


    for _, row in events.iterrows():

        event_id = row['event_id']
```

```
        event_description = row['description']

        process_event(
            session,
            event_id,
            event_description
        )


if __name__ == "__main__":
    main()
```

Appendix 5 - LLM's output

9a8ef8a1cf9ff509e1bf448d8b28e9b07c3bc384 is SHA1 hash of output_with_related_summary_Tactics.json

cc4fee4905186c11d1c7f2b9c9df354d36dbbce6 is SHA1 hash of output_with_related_summary_techniques.json

Appendix 6 – Proposed translation matrix of LLM's output and corresponding attack dimensions

Attack dimension	description	Corresponding tactic	Corresponding technique	Tactic LLM reasoning	Technique LLM reasoning
AD-NETWORK-IPV4IPV6_DIRECT	Direct IPv4 or IPV6 access to the target was possible from the attacker's machine located in SINET	TA0001	T1512	The event describes direct IPv4 or IPv6 access to the target from the attacker's machine, which suggests an initial entry point into the network, aligning with the Initial Access tactic.	The event involves leveraging a device's cameras to gather information, which matches the description of the T1512 technique, "Camera Capture", where an adversary uses a device's camera to capture images or video recordings.
AD-NETWORK-FQDN_DIRECT	Service was accessed via FQDN from the attacker's machine located in SINET	TA0008	T1437.001	The event mentions that a service was accessed via FQDN from the attacker's machine, which indicates lateral movement within a network, matching the description of Tactic ID TA0008: Lateral Movement.	The event describes direct IPv4 or IPV6 access, which suggests that the attacker is using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic, as described in T1437.001.
AD-NETWORK-IPV4_DIRECT	Direct IPv4 access to the target was possible from the attacker's machine located in SINET	TA0001	T1437.001	The event describes direct IPv4 access to the target from the attacker's machine, which suggests an initial entry point into the network, aligning with the "Initial Access" tactic.	The event describes direct IPv4 or IPV6 access, which suggests that the attacker is using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic, as described in T1437.001.
AD-NETWORK-IPV6_DIRECT	Direct IPv6 access to the target was possible from the attacker's machine located in SINET	TA0001	T1437.001	The event describes the attacker gaining initial access to the target through direct IPv6 access, which aligns with the Initial Access tactic. This tactic involves using various entry vectors to gain an initial foothold within a network, and in this case, the direct IPv6 access from the attacker's machine serves as the entry vector.	The event describes a service being accessed via FQDN, which matches the description of using application layer protocols associated with web protocols traffic to avoid detection/network filtering, as described in technique T1437.001.
AD-NETWORK-REVERSE_CALLBACK	The attacker's machine located in SINET was able to connect to the target using a reverse callback from the target machine.	TA0011	T1437.001	(Command and Control) The event describes a reverse callback connection from the target machine to the attacker's machine, which is indicative of command and control (C2) communication, allowing the attacker to control and send commands to the compromised system.	The event describes a service being accessed via FQDN, which matches the description of using application layer protocols associated with web protocols traffic to avoid detection/network filtering, as described in technique T1437.001.
AD-NETWORK-SOCKS_PROXY	The attacker's machine located in SINET was able to connect to the target using a reverse SOCKS proxy located within target network.	TA0008	T1437.001	The attacker's use of a reverse SOCKS proxy to connect to the target from their machine located in SINET indicates an attempt to move laterally within the network, which aligns with the Lateral Movement tactic.	The event mentions "Direct IPv4 access" which implies communication over a network, and the location of the attacker's machine is mentioned as SINET, suggesting a web-based or network-based attack, which aligns with using application layer protocols to blend in with existing traffic, as described by T1437.001.
AD-NETWORK-FIREWALL_PORT_FORWARD	The attacker's machine located in SINET was able to connect to the target using a reverse port forward from the target machine.	TA0008	T1437.001	The attacker's ability to connect to the target machine using a reverse port forward indicates lateral movement within the network, which aligns with the Lateral Movement tactic. This tactic involves techniques used by an adversary to enter and control remote systems on a network, often to gain access to additional resources or to move closer to their ultimate objective. The use of a reverse port forward in this context facilitates the attacker's ability to navigate through the network, making TA0008 (Lateral Movement) the most appropriate tactic ID for this event.	The event mentions "Direct IPv4 access" which implies communication over a network, and the location of the attacker's machine is mentioned as SINET, suggesting a web-based or network-based attack, which aligns with using application layer protocols to blend in with existing traffic, as described by T1437.001.
AD-NETWORK-PIVOT_THROUGH_EXISTING_ACCESS	The attacker's machine located in SINET was able to connect to the target using a reverse callback from previously compromised machine and pivoting through it.	TA0008	T1437.001	The attacker's action of connecting to the target using a reverse callback from a previously compromised machine and pivoting through it is an example of Lateral Movement, which is represented by the Tactic ID TA0008. This tactic involves techniques that enable an adversary to access and control remote systems on a network, often by exploiting existing connections or credentials.	The event mentions direct IPv6 access, which suggests that the attacker is using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic, allowing them to communicate with the target machine. This matches the description of T1437.001, which involves communicating using application layer protocols to blend in with existing traffic.
AD-NETWORK-OTHER	Other network attack vectors	TA0042	T1437.001	This event is related to "other network attack vectors", which implies that the adversary is trying to establish resources or infrastructure to support their operations, such as exploiting weaknesses in networks or systems, which aligns with the Resource Development tactic.	The event mentions direct IPv6 access, which suggests that the attacker is using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic, allowing them to communicate with the target machine. This matches the description of T1437.001, which involves communicating using application layer protocols to blend in with existing traffic.
AD-ACCESS-WEBSHELL	Webshell was used to establish access to the target machine.	TA0001	T1437.001	The use of a webshell to establish access to the target machine aligns with the Initial Access tactic, which involves techniques that use various entry vectors to gain an initial foothold within a network. In this case, the webshell serves as a means to initially access and potentially control the target machine, fitting the description of TA0001.	The attacker's use of a reverse callback from the target machine to connect back to their own machine in SINET suggests communication over application layer protocols, such as HTTP or HTTPS, to blend in with existing traffic and avoid detection, which aligns with technique T1437.001, "Application Window Discovery: Application Layer Protocol".
AD-ACCESS-RDP_SESSION	Remote Desktop Protocol session was established to the target machine.	TA0008	T1437.001	The event describes a Remote Desktop Protocol session being established to the target machine, which indicates an adversary is attempting to access and control a remote system on a network, aligning with the Lateral Movement tactic.	The attacker's use of a reverse callback from the target machine to connect back to their own machine in SINET suggests communication over application layer protocols, such as HTTP or HTTPS, to blend in with existing traffic and avoid detection, which aligns with technique T1437.001, "Application Window Discovery: Application Layer Protocol".
AD-ACCESS-SSH_SESSION	SSH session was established to the target machine.	TA0008	T1437.001	The event describes an SSH session being established, which implies that the adversary is attempting to access and control a remote system on	The attacker's use of a reverse SOCKS proxy to connect to the target network matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid

				the network, aligning with the definition of Lateral Movement.	detection/network filtering, which is described in T1437.001. This technique involves blending in with existing traffic to evade detection, and the use of a reverse SOCKS proxy is a common method for achieving this goal.
AD-ACCESS-REMOTE_INVOCATION	Remote command invocation was accomplished to the target machine eg via WinRM, WMI, SSH, RPC, etc.	TA0008	T1437.001	The event describes remote command invocation to a target machine using various protocols such as WinRM, WMI, SSH, RPC, etc., which aligns with the definition of Lateral Movement (TA0008), as it involves entering and controlling remote systems on a network.	The attacker's use of a reverse SOCKS proxy to connect to the target network matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001. This technique involves blending in with existing traffic to evade detection, and the use of a reverse SOCKS proxy is a common method for achieving this goal.
AD-ACCESS-KNOWN_MALWARE	Known malware was used to establish access to the target machine.	TA0001	T1437.001	The event describes the use of known malware to establish access to the target machine, which aligns with the Initial Access tactic, representing techniques that use various entry vectors to gain an initial foothold within a network.	The attacker's use of a reverse port forward to connect to the target machine suggests that they are attempting to blend in with existing traffic, potentially using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is consistent with the technique ID T1437.001, "Application Window Discovery: Web Service". However, given the context of the reverse port forward and connection establishment, a more suitable match would be a technique related to command and control or communication. Since none of the provided IDs directly mention reverse port forwarding, but T1437.001 involves using existing protocols for communication, it's a reasonable match based on the information given, although ideally, a technique directly related to "Command and Control" or "Reverse Port Forwarding" would be more appropriate if available in the options.
AD-ACCESS-CUSTOM_MALWARE	Custom malware was used to establish access to the target machine.	TA0001	T1437.001	The event describes the use of custom malware to establish access to the target machine, which aligns with the Initial Access tactic. This tactic represents the vectors adversaries use to gain an initial foothold onto a system or network.	The attacker's use of a reverse port forward to connect to the target machine suggests that they are attempting to blend in with existing traffic, potentially using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is consistent with the technique ID T1437.001, "Application Window Discovery: Web Service". However, given the context of the reverse port forward and connection establishment, a more suitable match would be a technique related to command and control or communication. Since none of the provided IDs directly mention reverse port forwarding, but T1437.001 involves using existing protocols for communication, it's a reasonable match based on the information given, although ideally, a technique directly related to "Command and Control" or "Reverse Port Forwarding" would be more appropriate if available in the options.
AD-ACCESS-OPERATIONS_MALWARE	One of the main RT malware was used to establish access to the target machine. Such as Cobalt Strike or Havoc.	TA0001	T1437.001	The event describes the use of malware, such as Cobalt Strike or Havoc, to establish access to a target machine, which aligns with the Initial Access tactic, represented by the ID TA0001. This tactic involves techniques used to gain an initial foothold within a network, which matches the scenario described in the event.	The attacker's use of a reverse port forward to connect to the target machine suggests that they are attempting to blend in with existing traffic, potentially using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is consistent with the technique ID T1437.001, "Application Window Discovery: Web Service". However, given the context of the reverse port forward and connection establishment, a more suitable match would be a technique related to command and control or communication. Since none of the provided IDs directly mention reverse port forwarding, but T1437.001 involves using existing protocols for communication, it's a reasonable match based on the information given, although ideally, a technique directly related to "Command and Control" or "Reverse Port Forwarding" would be more appropriate if available in the options.
AD-ACCESS-OPEN_PORT	A port was open on the target machine that allowed RT access.	TA0008	T1437.001	The event describes a situation where an open port allowed for potential access to the target machine, which aligns with Lateral Movement tactics as it could enable an adversary to move through the network and access remote systems.	The attacker's use of a reverse callback from a previously compromised machine to connect to the target and pivoting through it matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001. This technique involves using existing protocols to blend in with expected traffic, making it difficult to detect the malicious activity.
AD-ACCESS-MALWARE__TROJAN	Malware or a Trojan was used to access the target.	TA0043	T1437.001	The event describes the use of malware or a Trojan to access the target, which aligns with the Reconnaissance tactic as it involves gathering information about the target system, but since there is no specific mention of reconnaissance, the closest match would be the Resource Development tactic (TA0042) or Initial Access tactic. However, considering the context provided and focusing on the action described (accessing the target through malware), the most fitting initial phase for such an action would be gaining access to a system, which best matches with TA0001 - Initial Access, as it directly involves using various entry vectors like malware to gain initial foothold within a network. But since TA0043 also represents an action that precedes actual targeting and could involve gathering resources or initial steps towards accessing	The attacker's use of a reverse callback from a previously compromised machine to connect to the target and pivoting through it matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001. This technique involves using existing protocols to blend in with expected traffic, making it difficult to detect the malicious activity.

				a target, the closest given the direct action (use of malware) would be more aligned with gaining initial access. Therefore, aligning closely with tactics involving initial compromise, TA0001 seems the most appropriate answer based on provided IDs and descriptions.	
AD-ACCESS-REMOTE_INVOCATION	Red team had remote invocation access	TA0010	T1437.001	The event mentions "remote invocation access", which implies that the red team has the ability to execute code or commands remotely, aligning with the Execution tactic. However, since TA0010 (Exfiltration) is not directly applicable, we look for a closer match and find that "remote invocation access" could enable the adversary to achieve their goals through executing malicious code or commands on the system, which matches more closely with the idea of running code to gain access to resources as described in Execution.	This technique ID is chosen because it involves communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which could be related to other network attack vectors.
AD-ACCESS-TRAFFIC_INJECTION	Red team had traffic injection access	TA0010	T1625.001	The event mentions "traffic injection access", which implies the ability to insert or manipulate data in a network, aligning with Exfiltration tactics where an adversary might use such access to steal data by manipulating network traffic. However, given the context of "traffic injection" more broadly, it could also relate to Command and Control (TA0037) for establishing communication channels. But since "injection" can imply altering or inserting data into existing communications or streams, which is a method that could be used to exfiltrate information by modifying traffic to carry additional data out of the network, TA0010 (Exfiltration) seems like the closest match among the provided options for describing an action related to manipulating or utilizing network traffic for data extraction purposes.	The use of a webshell to establish access to the target machine matches with the technique of hijacking the way an operating system runs applications, which can be achieved by overwriting standard OS API library with a malicious alternative to hook into core functions and achieve persistence.
AD-ACCESS-OTHER	Other access vectors	TA0042	T1437.001	The event "Other access vectors" can be matched to the Resource Development tactic, which involves creating, purchasing, or compromising/stealing resources that can be used to support targeting, including infrastructure and accounts that could serve as alternative access vectors.	The technique ID T1437.001 is a match for this event because it involves communicating using application layer protocols, and Remote Desktop Protocol (RDP) is an application layer protocol that can be used to establish a remote session with a target machine, potentially allowing adversaries to blend in with existing traffic and avoid detection.
AD-NETWORK-IPV4_DIRECT	Direct IPv4 access to the target was possible from the attacker's machine located in SINET	TA0001	T1437.001	The event describes a scenario where direct IPv4 access to the target was possible from the attacker's machine, indicating an initial entry point into the network, which aligns with the "Initial Access" tactic.	The technique ID T1437.001 is a match for this event because it involves communicating using application layer protocols, and Remote Desktop Protocol (RDP) is an application layer protocol that can be used to establish a remote session with a target machine, potentially allowing adversaries to blend in with existing traffic and avoid detection.
AD-NETWORK-IPV6_DIRECT	Direct IPv6 access to the target was possible from the attacker's machine located in SINET	TA0001	T1437.001	The event mentions "Direct IPv6 access to the target was possible from the attacker's machine", which indicates that the attacker has gained initial access to the target network, making TA0001 (Initial Access) the most suitable tactic ID for this event.	The establishment of an SSH session to the target machine suggests that the adversary is using application layer protocols associated with web protocols traffic to communicate with the compromised system, which matches the description of technique T1437.001, "Application Window Discovery: Web Service". However, a more suitable match would be a technique related to remote access or command and control. Since none were directly provided, the closest match from the given list is T1437.001 as it involves communication over a network protocol, but ideally, a technique like "T1078: Valid Accounts" or "T1563: Remote Service Session Hijacking" would be more accurate if they were in the provided list.
AD-NETWORK-REVERSE_CALLBACK	The attacker's machine located in SINET was able to connect to the target using a reverse callback from the target machine.	TA0037	T1437.001	The attacker's use of a reverse callback from the target machine to connect to their own machine is an example of establishing command and control, which is represented by the Tactic ID TA0037.	The establishment of an SSH session to the target machine suggests that the adversary is using application layer protocols associated with web protocols traffic to communicate with the compromised system, which matches the description of technique T1437.001, "Application Window Discovery: Web Service". However, a more suitable match would be a technique related to remote access or command and control. Since none were directly provided, the closest match from the given list is T1437.001 as it involves communication over a network protocol, but ideally, a technique like "T1078: Valid Accounts" or "T1563: Remote Service Session Hijacking" would be more accurate if they were in the provided list.
AD-NETWORK-SOCKS_PROXY	The attacker's machine located in SINET was able to connect to the target using a reverse SOCKS proxy located within target network.	TA0008	T1437.001	The attacker's use of a reverse SOCKS proxy to connect to the target from their machine in SINET indicates an attempt to move through the environment, which aligns with the Lateral Movement tactic.	The establishment of an SSH session to the target machine suggests that the adversary is using application layer protocols associated with web protocols traffic to communicate with the compromised system, which matches the description of technique T1437.001, "Application Window Discovery: Web Service". However, a more suitable match would be a technique related to remote access or command and control. Since none were directly provided, the closest match from the given list is T1437.001 as it involves communication over a network protocol, but ideally, a technique like "T1078: Valid Accounts" or "T1563: Remote Service Session Hijacking" would be more accurate if they were in the provided list.
AD-NETWORK-FIREWALL_PORT_FORWARD	The attacker's machine located in SINET was able to connect to the target using a reverse	TA0011	T1437.001	(no, just kidding, that was not in the options) TA0008 The attacker's machine connecting to the target using a reverse port forward indicates lateral	The establishment of an SSH session to the target machine suggests that the adversary is using application layer protocols associated with web protocols traffic to

	port forward from the target machine.			movement within the network, allowing them to access and control remote systems. This matches with the Lateral Movement tactic.	communicate with the compromised system, which matches the description of technique T1437.001, "Application Window Discovery: Web Service". However, a more suitable match would be a technique related to remote access or command and control. Since none were directly provided, the closest match from the given list is T1437.001 as it involves communication over a network protocol, but ideally, a technique like "T1078: Valid Accounts" or "T1563: Remote Service Session Hijacking" would be more accurate if they were in the provided list.
AD-NETWORK-PIVOT_THROUGH_EXISTING_ACCESS	The attacker's machine located in SINET was able to connect to the target using a reverse callback from previously compromised machine and pivoting through it.	TA0008	T1437.001	The attacker is moving through the environment by connecting to a previously compromised machine and pivoting through it, which matches the description of Lateral Movement.	The establishment of an SSH session to the target machine suggests that the adversary is using application layer protocols associated with web protocols traffic to communicate with the compromised system, which matches the description of technique T1437.001, "Application Window Discovery: Web Service". However, a more suitable match would be a technique related to remote access or command and control. Since none were directly provided, the closest match from the given list is T1437.001 as it involves communication over a network protocol, but ideally, a technique like "T1078: Valid Accounts" or "T1563: Remote Service Session Hijacking" would be more accurate if they were in the provided list.
AD-NETWORK-OTHER	Other network attack vectors	TA0008	T1625.001	This event is related to "other network attack vectors", which aligns with the description of Lateral Movement (TA0008) as it involves techniques that enable an adversary to access and control remote systems on a network.	The event describes remote command invocation to the target machine, which matches with the technique of hijacking execution flow to execute malicious payloads, in this case, via various remote management protocols such as WinRM, WMI, SSH, RPC, etc.
AD-ACCESS-WEBSHELL	Webshell was used to establish access to the target machine.	TA0001	T1437.001	The use of a webshell to establish access to the target machine aligns with the Initial Access tactic, which involves techniques that use various entry vectors to gain an initial foothold within a network. In this case, the webshell serves as a means to initially access and potentially control the target machine, fitting the description of Initial Access.	The technique ID T1437.001 is matched with this event because it involves communication using application layer protocols, which could include the use of known malware to establish access to a target machine, blending in with existing traffic to avoid detection.
AD-ACCESS-RDP_SESSION	Remote Desktop Protocol session was established to the target machine.	TA0008	T1437.001	The event describes a Remote Desktop Protocol session being established, which indicates an adversary is attempting to access and control a remote system, aligning with the Lateral Movement tactic.	The technique ID T1437.001 is matched with this event because it involves communication using application layer protocols, which could include the use of known malware to establish access to a target machine, blending in with existing traffic to avoid detection.
AD-ACCESS-SSH_SESSION	SSH session was established to the target machine.	TA0008	T1625.001	The establishment of an SSH session to the target machine indicates that the adversary is attempting to enter and control a remote system on a network, which aligns with the Lateral Movement tactic.	The technique ID T1625.001 is matched with this event because it describes "Hijacking execution flow" which could be related to custom malware being used to establish access, implying the malware may have hijacked normal system processes to execute its payload and gain access to the target machine.
AD-ACCESS-OPEN_PORT	A port was open on the target machine that allowed RT access.	TA0008	T1625.001	The event describes a situation where an open port on the target machine allows for potential remote access, which aligns with Lateral Movement tactics as it could enable an adversary to enter and control remote systems on a network.	The technique ID T1625.001 is matched with this event because it describes "Hijacking execution flow" which could be related to custom malware being used to establish access, implying the malware may have hijacked normal system processes to execute its payload and gain access to the target machine.
AD-ACCESS-MALWARE__TROJAN	Malware or a Trojan was used to access the target.	TA0043	T1625.001	The event describes the use of malware or a Trojan to access the target, which aligns with the Reconnaissance tactic as it involves gathering information or access to support future operations, but since there's no direct mention of reconnaissance activities like scouting or information gathering about the target, and focusing strictly on the provided options, a more fitting match from the given choices would be the Execution tactic (TA0035 or TA0041), however, considering the context that malware was used "to access" which could imply gaining initial access to a system, it closely aligns with Initial Access tactics. Given these considerations and the limitations of the provided IDs, Initial Access seems more directly related as it specifically involves techniques for gaining an initial foothold. Among the options provided, TA0001 (Initial Access) is a direct match for such an event involving malware or a Trojan for accessing a target system initially.	The event mentions the use of Remote Access Tool (RT) malware, such as Cobalt Strike or Havoc, to establish access to the target machine. This matches with the technique ID T1625.001, which involves hijacking the way an operating system runs applications, allowing for persistence and potentially leading to further malicious activities.
AD-ACCESS-REMOTE_INVOCATION	Red team had remote invocation access	TA0010	T1625.001	The event mentions "remote invocation access", which implies that the red team has the ability to execute code or commands remotely, aligning with the Execution tactic. However, since TA0010 (Exfiltration) is not directly applicable, we should consider other tactics. In this case, the closest match from the provided STIX data is actually TA0037 (Command and Control), but a more suitable option would be to choose an ID that represents the ability to execute code or commands, which in this context would be related to Execution (TA0010 does not fit perfectly). Given the options and focusing on "remote invocation access", a better match from the provided IDs is actually TA0037 is closer, but based on the details given TA0010 was initially considered. Upon reevaluation considering "remote invocation" as a form of command execution: The best choice should reflect the idea of running code or commands. Considering all, a more fitting ID is	The event mentions the use of Remote Access Tool (RT) malware, such as Cobalt Strike or Havoc, to establish access to the target machine. This matches with the technique ID T1625.001, which involves hijacking the way an operating system runs applications, allowing for persistence and potentially leading to further malicious activities.

				actually related to Execution which aligns with running commands/code, thus it seems there was an oversight in the initial selection process given the context provided. Given this correction and focusing strictly on the "remote invocation access" as a means to execute commands, the actual tactic that should be chosen reflects this capability directly, hence: TA0037 is more aligned with command and control which can involve remote invocation for execution purposes. Therefore, considering all provided options again and focusing on the context of "remote invocation access", it seems there was an initial misalignment in the selection process based on the strict definitions provided for each tactic ID. Reassessing strictly based on "remote invocation access" implying the ability to execute commands/code remotely, a more accurate alignment with the tactics provided should reflect this capability. Thus, focusing on execution and command/control aspects as they relate to remote invocation: The actual best match considering all nuances should indeed be TA0037 given its closer association with command and control which encompasses remote invocation for code/command execution purposes. Thus, correcting my approach to strictly adhere to the format requested while ensuring alignment with the context of "remote invocation access" for executing commands/code: TA0037 The correct reasoning is that "remote invocation access" implies the ability to execute commands or code remotely, aligning closely with command and control capabilities which are essential for remote execution and management of compromised systems/devices. This capability is a key aspect of TA0037 (Command and Control), making it the most suitable choice given the context provided in the event description.	
AD-ACCESS-TRAFFIC_INJECTION	Red team had traffic injection access	TA0043	T1641.001	The best match for "Red team had traffic injection access" is Reconnaissance (TA0043), as it involves gathering information and potentially manipulating network traffic to support targeting, which aligns with the concept of having traffic injection access.	The event mentions a port being open for remote access, which could allow an adversary to manipulate transmitted data by intercepting and altering information sent through that port, matching the description of Transmitted Data Manipulation in T1641.001.
AD-ACCESS-OTHER	Other access vectors	TA0042	T1641.001	This event "Other access vectors" can be matched with the MITRE ATT&CK Tactic ID TA0042, which represents "Resource Development" and involves creating, purchasing, or compromising/stealing resources that can be used to support targeting, including infrastructure, accounts, or capabilities that could serve as alternative access vectors.	The event mentions a port being open for remote access, which could allow an adversary to manipulate transmitted data by intercepting and altering information sent through that port, matching the description of Transmitted Data Manipulation in T1641.001.
AD-VULNERABILITIES-ADVANTAGE_ADDED_IN_EARLIER_PHASE	The attacker was able to use a vulnerability that was added in an earlier phase.	TA0040	T1512	The event mentions that the attacker used a vulnerability that was added in an earlier phase, which suggests that the attacker is attempting to manipulate or interrupt the system, aligning with the Impact tactic.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points

					more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-EXPLOIT_RCE	Remote code execution was used against the target machine.	TA0029	T1512	The event describes remote code execution, which aligns with the tactic of gaining higher-level permissions or executing malicious code, but given the options, it most closely matches Privilege Escalation as it involves exploiting a weakness to potentially gain elevated access or execute code remotely. However, considering the exact phrasing and available tactics, Execution (TA0041 or TA0003) would be more directly related to running malicious code. Since TA0029 is not the best fit upon reevaluation, the most suitable choice under the provided rules and context should actually focus on executing code. Given this correction, the correct answer should align with execution tactics. Therefore, a better match considering standard interpretations would indeed be TA0003 or its equivalent in terms of executing malicious code. Given the direct relation to executing code: TA0003 is the most fitting choice for remote code execution as it directly involves running adversary-controlled code on a system, which is what remote code execution achieves. My initial reasoning was misguided due to an overemphasis on privilege escalation without considering the broader context of code execution tactics provided in the STIX data.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-MISCONFIGURATION	A misconfiguration was used against the target machine.	TA0004	T1512	The misconfiguration was likely exploited to gain higher-level permissions on the system, which aligns with the Privilege Escalation tactic.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly

					related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-UNCHANGED_CREDS	Unchanged default credentials were used to establish access to the target machine.	TA0001	T1512	The event describes using unchanged default credentials to gain access, which aligns with the Initial Access tactic, specifically exploiting weak passwords or default credentials on a public-facing system or service to gain a foothold.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g.,

					through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-STOLEN_CREDS	Previously stolen credentials were used to establish access to the target machine.	TA0008	T1512	The event describes using previously stolen credentials to gain access to a target machine, which aligns with Lateral Movement tactics where an adversary uses legitimate credentials to move through a network. However, since the primary action here is gaining initial access rather than moving laterally within the network after access has been established, it more accurately fits into the Initial Access category, but given the specifics of using "previously stolen credentials," this scenario seems to blend elements of both. Yet, considering the closest match from the provided options and focusing strictly on the action described (using credentials for access), TA0008 (Lateral Movement) seems most appropriate as it directly involves utilizing credentials to gain or maintain access within a network environment. Nonetheless, acknowledging the nuance, in broader MITRE ATT&CK context, this might align more closely with Initial Access if considering the establishment of access as the primary goal rather than movement post-access. Given the constraints and focusing on credential usage for network access, TA0008 is selected as the best match from provided options, understanding that typical initial access tactics involve gaining the first foothold, which may not perfectly align with lateral movements' definition emphasizing intra-network traversal.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-NONE	No vulnerabilities were used to establish access to the target machine.	TA0001	T1512	The event states that no vulnerabilities were used to establish access, which suggests that the initial access was gained through other means, such as valid credentials or social engineering, aligning with the Initial Access tactic.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying

					method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-OTHER	Other vulnerabilities were used to establish access to the target machine.	TA0001	T1512	The event mentions that other vulnerabilities were used to establish access to the target machine, which aligns with the Initial Access tactic. This tactic involves using various entry vectors to gain an initial foothold within a network, including exploiting weaknesses on public-facing systems or targeted spearphishing. In this case, the use of other vulnerabilities to establish access suggests an initial access attempt, making TA0001 the most suitable match.	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-EXPLOIT_RCE	Remote code execution was used against the target machine.	TA0029	T1512	The event mentions "remote code execution", which implies that an attacker is trying to execute malicious code on a remote system, but in this context it also implies privilege escalation as the attacker needs to gain higher level permissions to execute the code. However, given the information provided and focusing on the exact phrase "remote code execution", it more closely aligns with gaining higher-level permissions or executing code, which	The given event mentions that malware or a Trojan was used to access the target, but it does not specifically mention the use of cameras. However, among the provided options, T1512 (which involves leveraging a device's cameras) is the closest match as it implies an exploitation of device features for malicious purposes, similar to how malware or a Trojan would be used to access a target. Nonetheless, given the exact details in the question and available techniques, T1625.001 could

				could be seen under Privilege Escalation (TA0004) in a broader sense but since we are strictly matching against provided IDs and descriptions, TA0029 (Privilege Escalation) seems like the closest match because it directly involves an action that can lead to or is a form of privilege escalation through code execution. Nonetheless, considering standard MITRE ATT&CK classifications, Execution (TA0041 or TA0003 in different contexts) would typically be a more direct match for remote code execution events as it directly involves executing adversary-controlled code. Given the strict rules and the provided context, TA0029 is chosen based on the closest alignment with potential outcomes of remote code execution in terms of privilege escalation, but ideally, Execution tactics should be considered for such events.	also seem relevant due to its mention of overwriting OS API libraries for persistence, which aligns more closely with the concept of malware accessing a target. Yet, based on direct implications of "accessing" through malicious means without explicit camera usage mentioned, one might lean towards techniques directly related to execution and persistence like T1625.001, but since that's about hijacking execution flow for persistence rather than initial access, it leaves us with limited perfect matches. The most fitting given the context provided seems to actually relate more broadly to techniques involving malicious applications or code execution which isn't perfectly captured by any single ID here without more specific details on how "access" was achieved (e.g., via camera as in T1512 or other means). However, given the need for a single best choice and based on typical understandings of such events involving Trojans for device access, a closer alignment might actually be with techniques like T1625.001 when considering code execution aspects but since it directly mentions "access" without specifying method (like camera use), we face a challenge in precise matching without assuming specifics not provided in the question prompt. Thus, an initial instinct towards T1512 may mislead due to its specific context of camera usage which isn't explicitly mentioned in the event description. Reevaluating with this understanding points more towards code execution and access methods not strictly tied to cameras or specific persistence mechanisms initially described, hence suggesting a reconsideration is necessary for accurate alignment with provided techniques, especially those directly implying malicious code execution or access facilitation on the device without over-specifying the method of such access beyond "malware or Trojan" usage. Given these considerations and aiming for the best fit from provided IDs while acknowledging potential gaps in perfect matching based on event details given, T1625.001 emerges as a contender due to its relation with code execution aspects which could encompass initial access methods via malware but isn't a precise match without further context specifying how access was gained (e.g., through camera exploitation or other means). Thus, aligning closely with the provided scenario of using malware for target access without over-assuming specifics not detailed in the event description leads us to prioritize execution-related techniques when choosing among available options.
AD-VULNERABILITIES-DEFAULT_CREDS	Unchanged default credentials were used to establish access to the target machine.	TA0001	T1437.001	The event describes using unchanged default credentials to establish access, which aligns with gaining an initial foothold into a network through exploiting weaknesses such as easily guessable or default passwords, fitting the description of Initial Access.	The event mentions "remote invocation access", which suggests that the red team has the ability to execute commands or payloads remotely, likely using application layer protocols associated with web protocols traffic to avoid detection/network filtering, as described in T1437.001.
AD-VULNERABILITIES-STOLEN_CREDS	Previously stolen credentials were used to establish access to the target machine.	TA0008	T1437.001	The event describes using previously stolen credentials to establish access, which aligns with lateral movement tactics where adversaries use legitimate credentials to move through a network and gain access to remote systems.	The event mentions "remote invocation access", which suggests that the red team has the ability to execute commands or payloads remotely, likely using application layer protocols associated with web protocols traffic to avoid detection/network filtering, as described in T1437.001.
AD-VULNERABILITIES-ACCESS_FROM_PREVIOUS_PHASE	Access from previous phase that is still not discovered	TA0003	T1641.001	The event describes access from a previous phase that is still not discovered, which aligns with the definition of Persistence (TA0003), as it involves maintaining access to systems across interruptions, allowing the adversary to remain undetected.	The Red team having traffic injection access indicates the ability to manipulate transmitted data, which aligns with the description of T1641.001, Transmitted Data Manipulation, specifically modifying the contents of data in transit.
AD-VULNERABILITIES-NONE	No vulnerabilities were used to establish access to the target machine.	TA0001	T1641.001	The event states that no vulnerabilities were used to establish access to the target machine, which aligns with the Initial Access tactic. This tactic represents the vectors adversaries use to gain an initial foothold onto a system or network, and it includes methods such as targeted spearphishing, exploiting weaknesses on public-facing web servers, and using valid accounts or external remote services.	The Red team having traffic injection access indicates the ability to manipulate transmitted data, which aligns with the description of T1641.001, Transmitted Data Manipulation, specifically modifying the contents of data in transit.
AD-VULNERABILITIES-OTHER	Other vulnerabilities were used to establish access to the target machine.	TA0001	T1437.001	The event mentions that other vulnerabilities were used to establish access to the target machine, which aligns with the Initial Access tactic. This tactic represents the vectors adversaries use to gain an initial foothold onto a system or network.	The event "Other access vectors" can be related to the use of application layer protocols associated with web protocols traffic, which is described in T1437.001, to avoid detection and blend in with existing traffic, potentially using other access vectors.
AD-ESCALATION-UNCHANGED_DEFAULT_CREDENTIALS	Unchanged default credentials were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes a situation where unchanged default credentials were used to escalate privileges, which aligns with the Privilege Escalation tactic. This tactic involves techniques that allow an adversary to gain higher-level permissions on a system or network, and using default credentials is a common approach to achieve this goal.	The event "Other access vectors" can be related to the use of application layer protocols associated with web protocols traffic, which is described in T1437.001, to avoid detection and blend in with existing traffic, potentially using other access vectors.
AD-ESCALATION-STOLEN_ADMIN_CREDENTIALS	Previously stolen credentials were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes the use of previously stolen credentials to escalate privileges, which aligns with the Privilege Escalation tactic. This tactic involves techniques used by an adversary to gain higher-level permissions on a system or network, often leveraging existing weaknesses or misconfigurations. In this case, the stolen credentials	The event describes direct IPv4 access to the target, which suggests that the attacker is communicating with the target using standard web protocols, likely blending in with existing traffic to avoid detection. This matches with technique T1437.001, which involves communicating using application layer protocols associated with web protocol traffic to evade detection.

				serve as a means to achieve elevated access, fitting the description of Privilege Escalation.	
AD-ESCALATION-BACKDOOR_ESCALATION_MECHANISM_SERVICE	A backdoor was used to escalate privileges on the target machine. Backdoor type is 'service'.	TA0004	T1437.001	The event describes a backdoor being used to escalate privileges on the target machine, which aligns with the definition of Privilege Escalation, allowing an adversary to gain higher-level permissions on a system or network.	The event describes direct IPv4 access to the target, which suggests that the attacker is communicating with the target using standard web protocols, likely blending in with existing traffic to avoid detection. This matches with technique T1437.001, which involves communicating using application layer protocols associated with web protocol traffic to evade detection.
AD-ESCALATION-BACKDOOR_ESCALATION_MECHANISM_WMI	A backdoor was used to escalate privileges on the target machine. Backdoor type is 'WMI'.	TA0004	T1437.001	The event describes a backdoor being used to escalate privileges on the target machine, which aligns with the definition of Privilege Escalation, allowing an adversary to gain higher-level permissions on a system or network.	The event describes direct IPv6 access to the target, which suggests that the attacker is using application layer protocols associated with web protocols traffic to avoid detection/network filtering, blending in with existing traffic, as described in technique T1437.001.
AD-ESCALATION-EXCESSIVE_ACCOUNT_PRIVILEGES	Excessive account privileges were used to escalate privileges on the target machine.	TA0004	T1437.v	The event describes a situation where excessive account privileges were used to escalate privileges on the target machine, which matches the description of Privilege Escalation in the MITRE ATT&CK framework.	The event describes direct IPv6 access to the target, which suggests that the attacker is using application layer protocols associated with web protocols traffic to avoid detection/network filtering, blending in with existing traffic, as described in technique T1437.001.
AD-ESCALATION-WEAK_SERVICE_PERMISSIONS	Weak service permissions were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes a scenario where weak service permissions were used to escalate privileges, which aligns with the definition of Privilege Escalation, allowing an adversary to gain higher-level permissions on a system or network.	The attacker's use of a reverse callback from the target machine to connect back to their own machine in SINET suggests communication via application layer protocols associated with web protocols traffic, which is consistent with T1437.001, "Application Window Discovery: Web Service". This technique involves using existing web protocols to blend in with expected traffic and avoid detection.
AD-ESCALATION-WEAK_AUTO_ELEVATION_SETTINGS	Weak auto elevation settings were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes a scenario where an attacker takes advantage of weak auto elevation settings to escalate privileges on the target machine, which aligns with the Privilege Escalation tactic. This tactic involves techniques used by an adversary to gain higher-level permissions on a system or network, and exploiting weaknesses in auto elevation settings is a common approach to achieve this goal.	The attacker's use of a reverse callback from the target machine to connect back to their own machine in SINET suggests communication via application layer protocols associated with web protocols traffic, which is consistent with T1437.001, "Application Window Discovery: Web Service". This technique involves using existing web protocols to blend in with expected traffic and avoid detection.
AD-ESCALATION-EXCESSIVE_DOMAIN_PERMISSIONS	Excessive domain permissions were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes escalating privileges on a target machine using excessive domain permissions, which aligns with the definition of Privilege Escalation, allowing an adversary to gain higher-level permissions on a system or network.	The attacker's use of a reverse SOCKS proxy to connect to the target network matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001. This technique involves blending in with existing traffic to evade detection, and the use of a reverse SOCKS proxy is a common method for achieving this goal.
AD-ESCALATION-ACCESS_FROM_PREVIOUS_PHASE	Access from previous phase that is still not discovered	TA0003	T1437.001	The event describes access from a previous phase that is still not discovered, which aligns with the Persistence tactic. This tactic involves techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access, allowing them to maintain a foothold on the system without being detected.	The attacker's use of a reverse SOCKS proxy to connect to the target network matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001. This technique involves blending in with existing traffic to evade detection, and the use of a reverse SOCKS proxy is a common method for achieving this goal.
AD-ESCALATION-OTHER	Other escalation vectors	TA0004	T1437.001	The event "Other escalation vectors" is most closely related to the tactic of Privilege Escalation, which involves techniques used by an adversary to gain higher-level permissions on a system or network. This aligns with the concept of escalating privileges through various vectors.	The attacker's use of a reverse port forward to connect to the target machine suggests that they are attempting to blend in with existing traffic, potentially using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is consistent with the technique ID T1437.001, "Application Window Discovery: Web Service". However, considering the context of the event more closely, it seems more aligned with evading network filtering by using a reverse port forward, but since there isn't a direct match for this behavior in the provided IDs and T1437.001 involves communication using web protocols which could be leveraged to avoid detection, it becomes a plausible choice given the options available.
AD-ESCALATION-DEFAULT_CREDENTIALS	Default credentials were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes using default credentials to escalate privileges, which aligns with the Privilege Escalation tactic. This tactic involves techniques that allow an adversary to gain higher-level permissions on a system or network, and using default credentials is a common approach to achieve this.	The attacker's use of a reverse port forward to connect to the target machine suggests that they are attempting to blend in with existing traffic, potentially using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is consistent with the technique ID T1437.001, "Application Window Discovery: Web Service". However, considering the context of the event more closely, it seems more aligned with evading network filtering by using a reverse port forward, but since there isn't a direct match for this behavior in the provided IDs and T1437.001 involves communication using web protocols which could be leveraged to avoid detection, it becomes a plausible choice given the options available.
AD-ESCALATION-LEAKED_CREDENTIALS	Leaked credentials were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes a situation where leaked credentials were used to escalate privileges, which aligns with the Privilege Escalation tactic. This tactic involves techniques that allow an adversary to gain higher-level permissions on a system or network, and using leaked credentials is a common approach to achieve this goal.	The attacker's use of a reverse port forward to connect to the target machine suggests that they are attempting to blend in with existing traffic, potentially using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is consistent with the technique ID T1437.001, "Application Window Discovery: Web Service".

					However, considering the context of the event more closely, it seems more aligned with evading network filtering by using a reverse port forward, but since there isn't a direct match for this behavior in the provided IDs and T1437.001 involves communication using web protocols which could be leveraged to avoid detection, it becomes a plausible choice given the options available.
AD-ESCALATION-INJECTED_BACKDOOR	An attacker injected backdoor was used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes an attacker using a backdoor to escalate privileges, which aligns with the Privilege Escalation tactic, as it involves gaining higher-level permissions on a system.	The attacker's use of a reverse callback from a previously compromised machine to connect to the target and pivoting through it matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001.
AD-ESCALATION-EXCESSIVE_HOST_USER_PRIVILEGES	Excessive host user privileges were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes a situation where excessive host user privileges were used to escalate privileges on the target machine, which aligns with the Privilege Escalation tactic. This tactic involves techniques that allow an adversary to gain higher-level permissions on a system or network, and the use of existing privileges to escalate further matches this description.	The attacker's use of a reverse callback from a previously compromised machine to connect to the target and pivoting through it matches with the technique of communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering, which is described in T1437.001.
AD-ESCALATION-MISCONFIGURATION	Misconfiguration in application or any of the services running on the host were used to escalate privileges on the target machine.	TA0004	T1437.001	The event describes a situation where misconfiguration is used to escalate privileges, which aligns with the Privilege Escalation tactic. This tactic involves techniques that allow an adversary to gain higher-level permissions on a system or network, and exploiting misconfigurations is a common approach to achieve this goal.	This technique ID is the best match because it involves communicating using application layer protocols associated with web protocols traffic, which could include other network attack vectors that blend in with existing traffic to avoid detection.
AD-ESCALATION-OTHER	Other escalation vectors	TA0004	T1625.001	This event is related to "Other escalation vectors", which implies that the adversary is trying to gain higher-level permissions or access, aligning with the Privilege Escalation tactic.	The use of a webshell to establish access to the target machine matches with the "Hijack Execution Flow" technique, where an adversary may execute their own malicious payloads by hijacking the way an operating system runs applications, which can include using webshells to maintain access and execute commands on the compromised system.
AD-METHOD-DEFACE_VIA_DATABASE	The target was defaced via database modification.	TA0040	T1437.001	The event describes the target being defaced via database modification, which indicates that the adversary has manipulated or interrupted the target's systems and data, aligning with the "Impact" tactic.	The establishment of a Remote Desktop Protocol (RDP) session can be associated with communicating using application layer protocols to avoid detection or blend in with existing traffic, which aligns with the description of technique T1437.001, specifically leveraging web protocols or other common network traffic for command and control (C2) communications.
AD-METHOD-DEFACE_VIA_CODE_MODIFICATION	The target was defaced via application code modification.	TA0040	T1437.001	The event describes the target being defaced via application code modification, which aligns with the tactic of Impact (TA0040), as it involves manipulating or interrupting the system, in this case, by modifying application code to deface the target.	The establishment of a Remote Desktop Protocol (RDP) session can be associated with communicating using application layer protocols to avoid detection or blend in with existing traffic, which aligns with the description of technique T1437.001, specifically leveraging web protocols or other common network traffic for command and control (C2) communications.
AD-METHOD-DEFACE_VIA_FILESYSTEM_MODIFICATION	The target was defaced via changing file on disk.	TA0040	T1623.001	The event describes the target being defaced via changing a file on disk, which aligns with the tactic of Impact, as it involves manipulating or interrupting the target's devices and data to achieve a specific goal, in this case, defacement.	The establishment of an SSH session to the target machine suggests that the adversary is using Unix shell commands and scripts for execution, which aligns with the technique ID T1623.001, "Abuse Elevation Control Mechanisms: Unix Shell". This technique involves abusing Unix shell commands and scripts to execute various commands or payloads, including interactive shells accessed through command and control channels or during lateral movement such as with SSH.
AD-METHOD-DEFACE_VIA_SERVER_SIDE_APPLICATION_CACHE	The target was defaced via Server Side Application Cache modification.	TA0040	T1623.001	The event describes a scenario where the target was defaced, which implies manipulation or interruption of the system, aligning with the "Impact" tactic that involves disrupting availability or compromising integrity by manipulating business and operational processes. Defacing via Server Side Application Cache modification fits within the scope of techniques used for impact, such as destroying or tampering with data, to achieve the adversary's goals.	The establishment of an SSH session to the target machine suggests that the adversary is using Unix shell commands and scripts for execution, which aligns with the technique ID T1623.001, "Abuse Elevation Control Mechanisms: Unix Shell". This technique involves abusing Unix shell commands and scripts to execute various commands or payloads, including interactive shells accessed through command and control channels or during lateral movement such as with SSH.
AD-METHOD-DEFACE_VIA_EXTERNAL_DEPENDENCY	The target was defaced via external dependency modification.	TA0040	T1437.001	The event describes the target being defaced, which implies a disruption or manipulation of the target's environment, aligning with the "Impact" tactic that involves techniques to disrupt availability or compromise integrity by manipulating business and operational processes.	The event mentions a port being open, which could be related to web protocols traffic, and T1437.001 is about communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic, but more generally it can be related to open ports for remote access.
AD-METHOD-DEFACE_VIA_BROWSER_CACHE	The target was defaced via Browser Cache modification.	TA0040	T1437.001	The event describes a situation where the target was defaced, which implies manipulation or interruption of the system's normal state, aligning with the Impact tactic that involves disrupting availability or compromising integrity by manipulating business and operational processes. In this case, modifying the Browser Cache to deface the target affects how the website is displayed, fitting into the Impact category as it alters the intended presentation or functionality.	The event mentions a port being open, which could be related to web protocols traffic, and T1437.001 is about communicating using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic, but more generally it can be related to open ports for remote access.
AD-METHOD-BT_MIGHT_HAVE_BROKEN_IT	The target was likely destroyed by the BT	TA0040	T1512	The event describes the target being "likely destroyed", which aligns with the Impact tactic, specifically TA0040, as it involves techniques that result in the disruption or destruction of systems and data.	The event describes malware or a Trojan being used to access the target, but since there's no specific mention of camera interaction in the given event details, we should consider more general techniques related to malicious access. However, T1512 is related to using

					device cameras, which doesn't directly apply here based on the information provided. Given the context and the rules, a better match isn't clearly defined from the options provided, suggesting a misunderstanding or misapplication of the given STIX data in relation to the event described. Nonetheless, following the instruction for format but acknowledging the mismatch: A more appropriate technique considering common MITRE ATT&CK tactics for malware access might not be directly listed in the provided STIX data based on typical usage. Techniques like T1204 (User Execution) or others related to execution and persistence might be more applicable in a real-world scenario, but adhering strictly to the format and options given isn't feasible without further context or clarification of the event's specifics in relation to the provided technique IDs.
AD-METHOD-DELETED_FILES	The target was destroyed by deleting important files	TA0040	T1512	The event describes the destruction of a target by deleting important files, which aligns with the tactic of Impact, where techniques are used to disrupt availability or compromise integrity by manipulating business and operational processes, such as destroying or tampering with data.	The event describes malware or a Trojan being used to access the target, but since there's no specific mention of camera interaction in the given event details, we should consider more general techniques related to malicious access. However, T1512 is related to using device cameras, which doesn't directly apply here based on the information provided. Given the context and the rules, a better match isn't clearly defined from the options provided, suggesting a misunderstanding or misapplication of the given STIX data in relation to the event described. Nonetheless, following the instruction for format but acknowledging the mismatch: A more appropriate technique considering common MITRE ATT&CK tactics for malware access might not be directly listed in the provided STIX data based on typical usage. Techniques like T1204 (User Execution) or others related to execution and persistence might be more applicable in a real-world scenario, but adhering strictly to the format and options given isn't feasible without further context or clarification of the event's specifics in relation to the provided technique IDs.
AD-METHOD-FILLED_UP_DISK_SPACE	The target was destroyed by filling up disk space	TA0040	T1512	The event describes the target being destroyed by filling up disk space, which aligns with the "Impact" tactic that involves disrupting availability or compromising integrity, such as destroying or tampering with data. This matches the description of TA0040, which includes techniques used to disrupt availability or compromise integrity.	The event describes malware or a Trojan being used to access the target, but since there's no specific mention of camera interaction in the given event details, we should consider more general techniques related to malicious access. However, T1512 is related to using device cameras, which doesn't directly apply here based on the information provided. Given the context and the rules, a better match isn't clearly defined from the options provided, suggesting a misunderstanding or misapplication of the given STIX data in relation to the event described. Nonetheless, following the instruction for format but acknowledging the mismatch: A more appropriate technique considering common MITRE ATT&CK tactics for malware access might not be directly listed in the provided STIX data based on typical usage. Techniques like T1204 (User Execution) or others related to execution and persistence might be more applicable in a real-world scenario, but adhering strictly to the format and options given isn't feasible without further context or clarification of the event's specifics in relation to the provided technique IDs.
AD-METHOD-RECONFIGURED_APP_BADLY	The target was destroyed by maliciously reconfiguring the application	TA0040	T1437.001	The event describes the destruction of a target through malicious reconfiguration, which aligns with the "Impact" tactic that involves disrupting availability or compromising integrity by manipulating business and operational processes.	The technique ID T1437.001 is the best match for this event because it involves communicating using application layer protocols, which could include remote invocation access, to avoid detection and blend in with existing traffic. This technique is relevant to the event as it implies a level of remote access and control, which aligns with the concept of remote invocation.
AD-METHOD-STOPPED_OR_DISABLED_CRITICAL_SERVICES	The target was destroyed by stopping or disabling critical services	TA0040	T1437. 001	The event describes the destruction of a target by stopping or disabling critical services, which aligns with the "Impact" tactic that involves disrupting availability or compromising integrity by manipulating business and operational processes. This is consistent with the description of TA0040 in the provided STIX data.	The technique ID T1437.001 is the best match for this event because it involves communicating using application layer protocols, which could include remote invocation access, to avoid detection and blend in with existing traffic. This technique is relevant to the event as it implies a level of remote access and control, which aligns with the concept of remote invocation.
AD-METHOD-SHUT_DOWN_VM	The target was destroyed by shutting down the VM	TA0040	T1641	The event describes the destruction of a target, which aligns with the Impact tactic (TA0040), as it involves manipulating or interrupting systems and data, in this case, shutting down a VM to destroy the target.	The technique ID T1641, which represents "Transmitted Data Manipulation", is the best match for this event because having traffic injection access implies the ability to modify or manipulate data being transmitted over a network, which aligns with the description of T1641.
AD-METHOD-FIREWALL_RECONFIGURATION_LOCAL	The target was destroyed by misconfiguring the local firewall	TA0040	T1641	The event describes the target being destroyed by misconfiguring the local firewall, which aligns with the "Impact" tactic that involves manipulating, interrupting, or destroying systems and data, and can include techniques such as tampering with security mechanisms like firewalls.	The technique ID T1641, which represents "Transmitted Data Manipulation", is the best match for this event because having traffic injection access implies the ability to modify or manipulate data being transmitted over a network, which aligns with the description of T1641.
AD-METHOD-OTHER	Other methods of destruction	TA0040	T1641	The event "Other methods of destruction" aligns with the MITRE ATT&CK Tactic ID TA0040, which is described as techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes, including destroying or tampering with data. This	The technique ID T1641, which represents "Transmitted Data Manipulation", is the best match for this event because having traffic injection access implies the ability to modify or manipulate data being transmitted over a network, which aligns with the description of T1641.

				description matches the concept of "destruction" mentioned in the event.	
AD-ACCESS_LEVEL-HOST__LOW	The attacker had a unelevated host level access on the target.	TA0001	T1481	The attacker having an unelevated host level access on the target suggests that they have gained initial access to the system, but do not yet have elevated privileges, which aligns with the Initial Access tactic.	This technique ID is the best match because "Other access vectors" could imply using existing, legitimate external services as a means for relaying data to/from a compromised system, which aligns with the description of T1481, "Web Service". This technique involves using popular websites and social media as a mechanism for command and control (C2), providing cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise.
AD-ACCESS_LEVEL-HOST__ELEVATED	The attacker had a elevated host level access on the target.	TA0004	T1481	The attacker having elevated host level access on the target matches with the Privilege Escalation tactic, which involves techniques used by an adversary to gain higher-level permissions on a system or network.	This technique ID is the best match because "Other access vectors" could imply using existing, legitimate external services as a means for relaying data to/from a compromised system, which aligns with the description of T1481, "Web Service". This technique involves using popular websites and social media as a mechanism for command and control (C2), providing cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise.
AD-ACCESS_LEVEL-CONTAINER__LOW	The attacker had a unelevated container level access on the target.	TA0008	T1481	The attacker having an unelevated container level access implies they are in the process of moving through the environment, which aligns with Lateral Movement.	The attacker using a vulnerability that was added in an earlier phase matches with the concept of utilizing an existing, legitimate external service as a means for relaying data to/from a compromised system, which is described in technique ID T1481, although it's more closely related to the idea of reusing existing vulnerabilities or backdoors, however since there isn't a direct match from the provided IDs, T1481 can be considered due to its relation with using pre-existing infrastructure for malicious purposes.
AD-ACCESS_LEVEL-CONTAINER__ELEVATED	The attacker had a elevated container level access on the target.	TA0004	T1481	The attacker having elevated container level access on the target indicates they have gained higher-level permissions, which aligns with the Privilege Escalation tactic.	The attacker using a vulnerability that was added in an earlier phase matches with the concept of utilizing an existing, legitimate external service as a means for relaying data to/from a compromised system, which is described in technique ID T1481, although it's more closely related to the idea of reusing existing vulnerabilities or backdoors, however since there isn't a direct match from the provided IDs, T1481 can be considered due to its relation with using pre-existing infrastructure for malicious purposes.
AD-ACCESS_LEVEL-NONE	The attacker had no access to the target.	TA0001	T1481	The attacker had no access to the target, which means they need to gain initial access, making TA0001 (Initial Access) the most suitable tactic for this event.	The attacker using a vulnerability that was added in an earlier phase matches with the concept of utilizing an existing, legitimate external service as a means for relaying data to/from a compromised system, which is described in technique ID T1481, although it's more closely related to the idea of reusing existing vulnerabilities or backdoors, however since there isn't a direct match from the provided IDs, T1481 can be considered due to its relation with using pre-existing infrastructure for malicious purposes.
AD-ACCESS_LEVEL-OTHER	Other access levels	TA0004	T1625.001	This event is related to "Other access levels", which implies that an adversary is trying to gain higher-level permissions or access, aligning with the Privilege Escalation tactic.	The event mentions remote code execution, which aligns with hijacking the way an operating system runs applications to execute malicious payloads, as described in T1625.001.

Graphical material