TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Holger Rünkaru 179929IVSB

ENDPOINT DETECTION AND RESPONSE SOLUTION AS A SECURITY AS A SERVICE PLATFORM BY THE EXAMPLE OF FIREEYE HX

Bachelor's thesis

Supervisor: Pavel Laptev
Bachelor's Degree

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Holger Rünkaru 179929IVSB

LÕPPSEADMETE TUVASTUSE- JA REAGEERIMISLAHENDUS KUI TURBETEENUSE PLATVORM FIREEYE HX NÄITEL

Bakalaureusetöö

Juhendaja: Pavel Laptev
Bakalaureusekraad

Tallinn 2020

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: Holger Rünkaru

30.04.2020

Abstract

The cyber-criminals are more financially motivated than ever, and there are no signs of this situation changing. Threat actors are choosing targets able to pay a ransom, have valuable data, or otherwise be useful for cybercriminals while being easy to breach. Small and medium-sized businesses are often the target - while having enough resources to be valuable targets, the cybersecurity maturity level is often low due to the complexity and cost of cybersecurity.

The thesis focuses on finding a cost-efficient approach to provide security as a service to small and medium-sized businesses while not sacrificing on threat detection rate and analysis capability. Modern Endpoint Detection and Response solution is tested from alerting, incident investigation, and threat hunting capabilities point of view to analyse the potential to be the platform for security as a service with low start-up cost and implementation complexity.

This thesis is written in English and is 36 pages long, including 6 chapters, 15 figures and 1 table.

Annotatsioon

Kaasaegne lõppseadmete tuvastuse- ja reageerimislahendus kui turbekeskuse-teenuse platvorm väikestele klientidele FireEye HX näitel

Küberründeid teostatakse üha enam finantseesmärkidel ning ei ole näha märke, et olukord muutuks. Küberkriminaalid valivad sihtmärkideks neid, kes on võimelised maksma lunaraha, omavad väärtuslike andmeid või on muul moel ründajatele ahvatlevad ning on samal ajal kerge saak. Sageli on sihtmärkideks väike- ja keskmised ettevõtted, kellel on piisavalt ressursse, et olla ahvatlevaks sihtmärgiks, kuid kelle küberkaitse võimekus on madal tulenevalt küberturbe kallidusest ning keerukusest.

Antud bakalaurusetöö keskendub kuluefektiivse lahenduse leidmisele küberkaitse-teenuse pakkumiseks väikestele ja keskmistele ettevõtetele, ilma tuvastuse- ja analüüsivõimekuse ohverdamiseta. Töös testitakse kaasaegset lõppseadmete tuvastuse- ja reageerimislahendust teavituste, intsidendi analüüsi ning ohujahtimise võimekuste osas, et analüüsida lahenduse sobivust olla teenuse pakkumise platvormiks madala sisenemiskulu ja juurutamiskeerukusega.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 36 leheküljel, 6 peatükki, 15 joonist, 1 tabelit.

List of abbreviations and terms

EDR	Endpoint Detection and Response
EPP	Endpoint Protection Platform
MSSP	Managed Security Service Provider
SME	Small and Medium-sized Enterprise
SIEM	Security Information and Event Management
APT	Advanced Persistent Threat
API	Application Programming Interface

Table of contents

List of figures

List of tables

1 Introduction

In the current day and age, cybersecurity should be a part of the business for every company. A single cybersecurity breach could potentially have a severe impact on smaller businesses – be that the lost trust of the customers or significant fines for European General Data Protection Regulation violation in case customers data has been lost.

Alternatively, it could be just the fact that the necessary data to continue companies' everyday business is either encrypted or destroyed, and all activities are brought to a halt.

In order to stay in business, companies should consider investing in cybersecurity.

In 2019, a Data Breach Investigation report showed that 43% of breaches involved small businesses, and 71% of breaches were financially motivated [1]. The two pieces of information could be interpreted as small and medium businesses are easier targets, and attackers are picking the low hanging fruit, not targeting specific companies.

1.1 Problem statement

The difficulty for small and medium businesses comes primarily from the complexity and cost of cybersecurity. Even if the management would like to invest in cybersecurity, they often lack the competence and resources and would require additional dedicated staff for cybersecurity. In the current market state, it is both difficult and expensive to find skilled cybersecurity staff, which is making the security as a service market a more appealing and reasonable approach for small and medium businesses.

A large part of expenses still consists of the license fees of cybersecurity tools and products – depending on the model of security service provided the costs can also vary tenfold or more. The small and medium businesses need a way to improve their security posture to detect and respond to opportunistic attacks while keeping the initial investment low, complexity of added cybersecurity capability manageable and recurring costs small.

1.2 Thesis objective

The objective of this thesis is to find a more cost-efficient approach to provide security as a service to small and medium businesses. Traditionally, separate central management platforms have been used to aggregate and correlate data from endpoints, but modern endpoint protection solutions have significantly improved.

The goal of the thesis is to analyse the potential of a modern Endpoint Detection and Response solution in the service provider approach to be the platform for security as a service while keeping the implementation complexity and cost of entry down. Enabling the small and medium-sized businesses with restrictive cybersecurity budget and no in-depth cybersecurity knowledge to improve their security posture by using the service.

The aim is to analyse the potential of using a modern Endpoint Detection and Response solution with remote management as a platform for security as a service without additional tools. Including the means to detect, analyse, respond to and hunt for threats with high confidence, ease of use and providing enough detail for the security operations to rely on the endpoint solution.

1.3 The scope of the thesis

The analysis and testing are based on operating system level attacks and techniques – attacks to specific applications are not included in the scope.

The thesis focuses on up-to-date Windows 10 operating system. Other operating systems could be covered in the future as most modern protection software vendors are working towards adding similar features to macOS and Linux operating systems.

1.4 Methodology

In the theoretical part of the thesis, different security as a service models and commonly used security tools are analysed to form the capability requirements for the platform. To compose a list of test-cases MITRE ATT&CK framework is used, and threat intelligence reports data is aggregated to find the most popular attack techniques of recent years for analysis.

An empirical approach is used to get data for analysis. For validation, several automation options are analysed to select the most aligned approach for thesis goal.

Tests are performed in an isolated testing environment and based on defined test-cases in the earlier research. Conclusions are composed based on the requirements defined in the earlier stage.

2 Background information

Attackers today are driven by something more tangible than celebrity status. They are motivated by financial gain. The longer attackers can remain undetected on the network, the longer they can exfiltrate valuable corporate assets, whether they are sensitive customer data, intellectual property, or everyday operational files. The bottom line is that these assets have financial value. Attackers can sell intellectual property on the dark web or use sensitive customer data to commit financial fraud. Even operational files have value [2].

Attackers can cash in big by invading large enterprises, but they do not have to. SMEs also have valuable data and are often easier pickings. Because they have a weaker security posture, once, inside the network, attackers can stay hidden longer [2].

The No. 1 challenge small and medium enterprises face when it comes to shoring up their defences is a limited IT budget. They simply lack the financial resources needed to properly operate their network, let alone hunt down security threats in their environment [2].

In the following sections, different self-managed and outsourced approaches to cybersecurity are explained.

2.1 Security Operations Centre

Security Operations Centre (hereafter: SOC) can be both internal or outsourced and is also the most complicated and expensive approach to security. As the field of cybersecurity likes using acronyms, there are many naming conventions for functionally very similar teams:

- Computer Security Incident Response Team (CSIRT)
- Computer Incident Response Team (CIRT)
- Computer Incident Response Centre (or Capability) (CIRC)
- Computer Security Incident Response Centre (or Capability) (CSIRC)

- Security Operations Centre (SOC)
- Cybersecurity Operations Centre (CSOC)

A SOC is defined primarily by what it does— computer network defence. Which can be characterised as [3]:

The practice of defence against unauthorised activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

SOCs can range from small, five-person operations to large, national coordination centres. A typical midsize SOC's mission statement typically includes the following elements [3]:

1. Prevention of cybersecurity incidents through proactive:

    1) Continuous threat analysis
    2) Network and host scanning for vulnerabilities
    3) Countermeasure deployment coordination
    4) Security policy and architecture consulting.

2. Monitoring, detection, and analysis of potential intrusions in real-time and through historical trending on security-relevant data sources
3. Response to confirmed incidents, by coordinating resources and directing the use of timely and appropriate countermeasures
4. Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behaviour to appropriate organisations
5. Engineering and operating defence technologies such as Intrusion Detection Systems and data collection/ analysis systems.

2.1.1 Common tools of SOC

An enterprise-wide data collection, aggregation, detection, analytic and management solution is the core technology of a successful SOC. An effective security monitoring system incorporates data gathered from the continuous monitoring of endpoints (PCs, laptops, mobile devices and servers) as well as networks and log and event sources. With the benefit of the network, log and endpoint data gathered before and during the incident, SOC analysts can immediately pivot from using the security monitoring system as a detective tool to using it as an investigative tool. For reviewing suspicious activities that make up the given incident, and even as a tool to manage the response to an incident or breach. Often, an alert is associated with a network or host-based activity and, initially, may contain only the suspicious endpoint's IP address. In order for the SOC analyst to investigate the system in question, the analyst generally needs other information, such as the owner and hostname of the machine or DHCP-sourced records for mapping IP and host information at the time of the alert [4].

For the described use-case of log aggregation and correlation security information and event management (hereafter: SIEM) solution has been a commonly used approach.

In case Endpoint Detection and Response (hereafter: EDR) is included in the security stack, it generally is either a separate tool or one of the data sources feeding to the SIEM platform.

2.1.2 Modern endpoint security solutions

The endpoint security solutions have generally been divided into two categories - Endpoint Protection Platforms (hereafter: EPP) and Endpoint Detection and Response solutions.

An EPP is an integrated security solution designed to detect and block threats at the device level. Typically, this includes antivirus, anti-malware, data encryption, personal firewalls, intrusion prevention and data loss prevention [5].

EDR solutions are focussed on real-time anomaly detection, alerting, forensic analysis and endpoint remediation capabilities. By recording every file execution and modification, registry change, network connection and binary execution across an organisation's endpoints, EDR enhances threat visibility beyond the scope of EPPs [5].

Nowadays, both EPP and EDR can be considered as a single solution.

According to Gartner in "Magic Quadrant for Endpoint Protection Platforms" from 2019 August we are in a transformative period for the EPP market, and as the market has changed, so has the analysis profile used for this research. In the 2019 Magic Quadrant for Endpoint Protection Platforms, capabilities traditionally found in the endpoint detection and response (EDR) market are now considered core components of an EPP that can address and respond to modern threats [6].

When marking the generally included features of Modern EDR with a solid line and with a dashed line, the features for which the inclusion depends on the software provider (Figure 1. Modern EDR solution capabilities) it becomes quite visible that modern EDR solutions can cover most of the features smaller companies might need to significantly improve their security posture [6] [7].

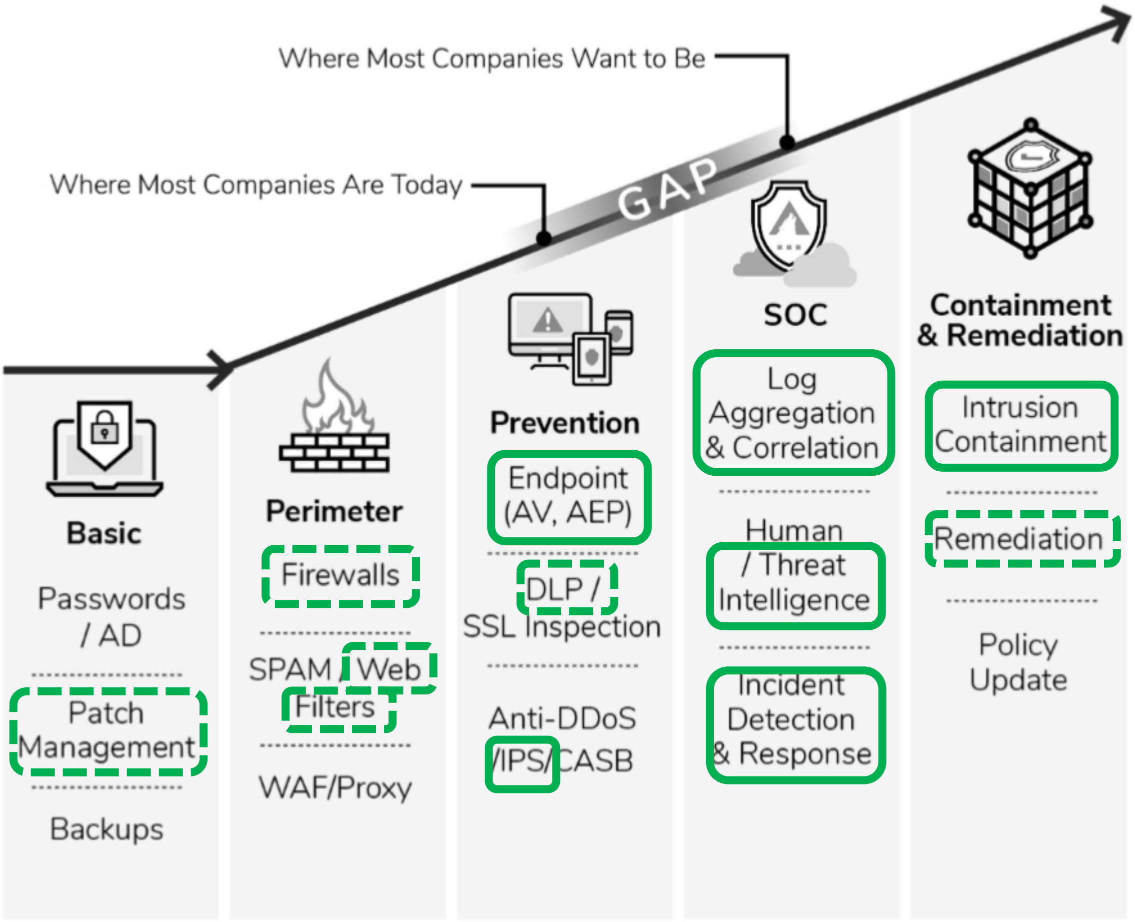


Figure 1. Modern EDR solution capabilities

2.1.3 FireEye HX overview

The following research is based on FireEye HX. FireEye is a platform vendor providing endpoint, email, web, network and cloud security solutions and threat intelligence. Mandiant, the service arm of FireEye, provides a full range of security services [6].

FireEye HX is the endpoint protection solution. Consisting of the signature-based detection engine, machine learning engine called MalwareGuard, real-time IOC engine using the latest threat intelligence and EDR capabilities with behaviour-based analytics engine called ExploitGuard. Additionally, remote data and memory acquisition capabilities are included.

2.1.4 Implementation complexity comparison of EDR and SIEM

SIEM solutions are very flexible – this could be considered SIEM's most significant advantage, but it can also be the biggest disadvantage if fewer resources are available for cybersecurity.

SIEM deployments could be divided into three broad steps – planning, implementation, usage and fine-tuning.

1. Planning – as SIEM solutions generally are very customisable and can be used for compliance reports among other use-cases. The specific use-cases must be defined before-hand to importing data-sources and creating rules.

   Errors in the planning stage could mean that the final solution is under par and does not give the analysts enough data, is not covering critical systems or is lacking the Threat Intelligence to create alerts.

   On the other hand, it is similarly possible to over-plan the solution – collecting and processing too much information, requiring a massive amount of hardware and creating higher licensing expenses, which are often based on Events-per-second. Alternatively, having the SIEM tuned to be too sensitive, burying the analysts with false-positives and making it difficult to filter out the events needing actual and immediate attention.

2. Implementation – depending on specific use cases, the implementation complexity can vary. From the endpoint protection point of view, data from workstations and laptops must be collected.

   Collecting could be done via Windows Event Forwarding, requiring additional Windows Server resource. Alternatively, by installing agents on the endpoints to forward logs, which might require additional licenses and configuration to select what information to collect and forward.

Collected logs might only include the IP address of log source and to make the logs useful for analysts' data from DHCP and DNS servers is required to enrich the logs.

Depending on the SIEM provider, Threat Intelligence might be licensed separately to generate alerts. Similarly, the rulesets by a vendor can include necessary rules to alert on suspicious endpoint activities. However, as the SIEM is not focussed on the endpoint logs only, the alerting capability might need creation or improvement by analysts.

3. Usage and fine-tuning – some SIEM providers could include pre-made alerts and dashboards, but often the alerts and dashboards must be configured by analysts. The world of cybersecurity is in rapid change and so should be the detection and monitoring solutions. As new vulnerabilities and techniques are adopted by attackers, the SIEM rules should be improved to keep up.

Of course, many of the steps could be fully or partially outsourced to service providers. However, there are steps which are highly customer-specific, like the setup of log forwarders, forwarding DNS and DHCP logs, determining use-cases and configuring the environment.

Comparing with EDR solutions, which mostly only require agent installation on the endpoints, deployment of the management console and creating default policy, which due to the solutions strict focus on endpoints, is easier to set up by someone outside the organisation.

As modern EDR solutions also include preventive capabilities, which from Operating System point of view are more intrusive. A staged deployment of preventive capabilities is suggested to avoid a wider negative impact, in case some business applications require custom exclusions.

EDR solutions are kept up-to-date by the vendor to detect latest malicious or suspicious activities and include dashboards. In the case of on-premise installations, occasional system updates are required for the management console, but otherwise, little maintenance is needed. Endpoint agent updates can be done with the management solution used for initial deployment, or via the central management console of EDR, which usually has the means to update endpoint agents automatically.

2.1.5 Functional comparison of EDR and SIEM based setups

Both EDR and SIEM solutions can technically be hosted in cloud service providers environments. However, as most of the analysis by SIEM solutions are done centrally in the SIEM platform the resources needed are significantly higher compared to the EDR central management platforms where most of the data correlation and alert generation is performed on the endpoints.

Due to these architectural differences, the SIEM solutions are often unable to provide preventive actions on the endpoints to limit or stop the malicious actions, and separate protection layer is necessary at the endpoints.

EDR solutions are less affected by the perimeter of organisation networks, which for the SIEM solutions might require additional attention. Most log forwarding protocols are not encrypted, and enabling real-time log forwarding might need additional encapsulation and more bandwidth compared to EDR solutions.

From the flexibility point of view, SIEM solutions have many advantages – the SIEM platform can often incorporate several segregated data stores to provide strict role-based access control and enable organisations to leverage tiered data storage options. Such flexibility could be useful to use less expensive and slower storage for data archives needed by compliance requirements and faster storage for security operations.

EDR solutions generally are much more limited in the data storage configuration capabilities. They often are not usable for storing compliance, troubleshooting and other operational logs, which allow SIEM solutions to be more widely leveraged by the organisations.

2.2 Security as a Service

Security as a Service could be full SOC outsourced, as described earlier, although most common approaches to Security as a Service will only include part of traditional SOC capabilities.

As the objective of the thesis is to focus on SMEs with limited resources the use of Security as a Service with limited features is reasonable and building their own SOC is generally not suggested for SMEs [2].

2.2.1 Managed Security Services Provider

Managed Security Services Provider (hereafter: MSSP) is the predecessor to Managed Detection and Response. Managed security service providers (MSSPs) monitor network security events and send alerts when anomalies are identified. MSSPs do not investigate the anomalies to eliminate false positives, nor do they actively respond to security threats. Some MSSPs also provide a variety of other network services such as virus protection and firewall management. MSSPs can help focus investigation efforts, but leave it up to end customer to perform the actual investigations, eliminate false positives, and prepare incident responses [8].

2.2.2 Managed Detection and Response

The goal of Managed Detection and Response (hereafter: MDR) services is to rapidly identify and limit the impact of security incidents to customers. These services are focused on remote 24/7 threat monitoring, detection and targeted response activities. MDR providers may use a combination of host and network-layer technologies, as well as advanced analytics, threat intelligence, forensic data, and human expertise for investigation, threat hunting and response to detected threats. For example, the MDR providers might be looking for specific tactics, techniques and procedures that indicate a threat is active in a customer’s environment. All of which can be expensive, difficult to obtain and hard to sustain for many midsize enterprises, as well as larger enterprises [9].

2.2.3 Managed Endpoint Detection and Response

Managed Endpoint Detection and Response (hereafter: managed EDR) could be considered a light version of MDR. The managed EDR services utilise a software agent installed on endpoints that send information to a centralised database for analysis. The endpoint solutions used to be limited to signature-based detections, but modern endpoint protection solutions have significantly evolved.

Modern EDR solutions are further explained in chapter Modern endpoint security solutions.

3 Defining detection use-cases for thesis scope

One of most common models used for cyber-attacks next to MITRE ATT&CK is Cyber Kill Chain by Lockheed Martin, now having many modifications. The original Cyber Kill Chain breaks cyber-attack down into seven distinct steps in the order of occurrence – Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control, Actions on Objective [10].

As the Cyber Kill Chain model is high level and lacks descriptions of specific techniques, the MITRE ATT&CK is a better fit for the thesis in general. Although understanding the Cyber Kill Chain remains a good value for modelling incident response plans to cover all steps in the investigation and preparation.

3.1 MITRE ATT&CK framework

The MITRE ATT&CK framework was started in 2013, and the first release of the framework, which stands for Adversarial Tactics, Techniques and Common Knowledge was released in 2015 [11]. MITRE ATT&CK is a curated knowledge base and model for cyber adversary behaviour, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. ATT&CK focuses on how external adversaries compromise and operate within computer information networks [12].

Among other use-cases documented by MITRE, the use-cases of ATT&CK framework includes "Defensive Gap Assessment" with the following explanation- a defensive gap assessment allows an organisation to determine what parts of its enterprise lack defences and/or visibility. These gaps represent blind spots for potential vectors that allow an adversary to gain access to its networks undetected or unmitigated [12].

As the objective of the thesis is to evaluate modern EDR solutions, such a framework would seem an excellent way to analyse the alerting and investigative capabilities of the platform in a structured approach.

The MITRE ATT&CK framework uses Tactics, Techniques and Sub-Techniques to break down the attacks [12] [13].

- Tactics represent the "why" of a technique or sub-technique – the reason adversary is performing an action. For example, to access credentials, achieve persistence, move laterally or to discover information.
- Techniques represent "how" an adversary achieves a tactical objective by performing an action. For example, dumping credentials or creating a new service.
- Sub-techniques further break down behaviours described by techniques into more specific descriptions. For example, credential dumping could be done by accessing LSASS Memory or exporting Windows registry hives.

3.2 MITRE ATT&CK Evaluations for APT tactics

MITRE has many projects like ATT&CK, one of which is ATT&CK Evaluations – the purpose of the project is to evaluate security products and vendors capabilities. At the time of writing the thesis, three evaluation rounds have been announced. Rounds are focussing on APT3, APT29 and Carbanak+FIN7 adversaries [14].

As the naming of rounds suggests, the focus is on evaluating security products against APT, an Advanced Persistent Threat [15], tactics and techniques which are not necessarily matching with the most prevalent tactics and techniques selected for the thesis.

The testing of MITRE ATT&CK Evaluations also includes Managed Detection and Response services like FireEye Managed Defense [16] and CrowdStrike Falcon Overwatch [17] to be part of the alerting capability, which is making the use of the assessment results challenging to analyse the products themselves.

In the MITRE ATT&CK Evaluations, the scoring of a technique is generally based only on one sub-technique. While it is giving some overview of the technique detection, there are often up to 10 and more sub-techniques per MITRE ATT&CK technique. Therefore full testing will be done even when the same technique is covered in the APT evaluation.

In April 2020, the results of APT3 and APT27 evaluation rounds results have been published.

4 Testing goal

An EDR solution must meet the following criteria to be a viable platform:

- Alerting - provide alerts with high confidence rates based on popular MITRE ATT&CK techniques
- Investigation - support analysts with enough detail to remotely investigate alerts
- Threat hunting - enable analysts to hunt for threats remotely over multiple tenants simultaneously
- Response - Include response capabilities to contain threats rapidly

The requirements are explained in more detail in the chapter Requirements for EDR platform.

Additionally, the platform should be able to support the management of multi-tenant environment from a single pane of glass view.

4.1 Requirements for EDR platform

4.1.1 Alerting

On first glance, it might appear like a good idea to strive for 100% coverage of the MITRE ATT&CK framework. The full coverage is both unrealistic and unreasonable. Many of the tactics like T1195 Supply Chain Compromise are hard to identify and often would require scarce resources more useful elsewhere [18].

While it would be convenient for the security analysts to receive alerts for all malicious techniques used in the networks, the adversaries are working hard to stay undetected and receiving alerts for all malicious activities will never happen. The goal might be to get at least one alert from the attackers’ activities and the earlier the detection is in the cyber kill chain, the better for the defenders.

The focus of the thesis is SMEs with restrictive security budget. Therefore the techniques in the scope are the most common ones to achieve coverage for most common attacks with limited resources.

4.1.2 Investigation

The capability to investigate past malicious activities, system changes and the initial infection vector after the alert has been received is at least as important as alerting. The investigation might be done by analysing constant data stream saved to a central management solution, triage packages created and forwarded in case alerts are triggered or via receiving forensic acquisitions from the endpoints remotely. A modern EDR solution should be able to provide the data with details needed for incident response.

4.1.3 Threat hunting

In case the attacker manages to bypass all detection rules for creating the alerts, the security operations must rely on threat hunting. Creating automatic recurring searches or custom alerts for possible indicators of compromise or suspicious activities to cover many managed environments at once is a feature of great value. By using such features, a service provider can leverage the threat intelligence of current active threats to verify if there are sightings of similar malicious activities on any of the service users' networks and if possible, give proactive mitigation recommendations.

4.1.4 Response

Upon detecting an active threat in high-value target, an EDR solution should provide incident responders with the capability to respond to the threat. The containment could be a more general approach like blocking all network connections, except management and investigation tools. Alternatively, the approach can be more targeted – for example, remotely killing specific processes, blocking specific network connections or providing incident responders with a remote shell to respond to threats manually.

4.2 Selection of MITRE ATT&CK techniques for analysis

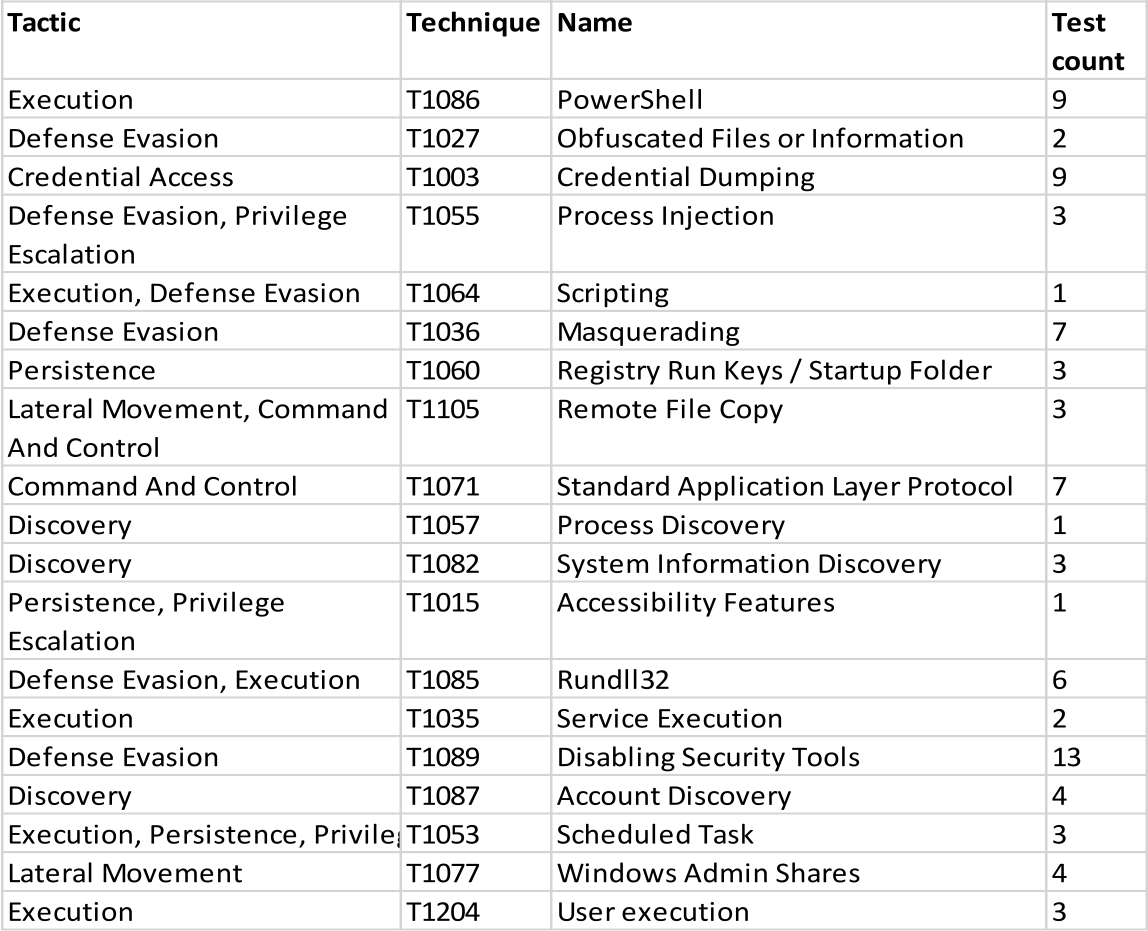
Six threat intelligence reports were analysed, and the data regarding most prevalent MITRE ATT&CK techniques used in the wild was aggregated. The reports cover period from years 2018 to 2020 [19] [20] [21] [22] [23] [24].

The reports included 61 different techniques in total. Twelve techniques were excluded due to being not applicable for Windows operating system or missing tests for the techniques in Atomic Red Team project.

As the reports included a varying amount of techniques the top 10 techniques received a higher score and were marked as “primary”, other techniques were marked as “secondary”. Techniques prevalence score was calculated by giving 1 point for each ‘primary’ mark and 0,5 points for each ‘secondary’ mark to each technique in each of the reports.

For evaluation of the FireEye HX, all techniques with prevalence score of at least 1,5 points were selected. In total it included 20 MITRE ATT&CK techniques and 100 possible Atomic Red Team tests for sub-techniques. Final test results included 19 techniques and 84 sub-technique tests (Table 1. Prevalent MITRE ATT&CK techniques for evaluation). Some tests were excluded due to the testing environment limitations, and a few tests were not working as intended. Fixing existing tests and developing new ones for new attack sub-techniques looks like an exciting project to tackle for people wanting to learn about endpoint protection. The full table of techniques can be found in Appendix 2 – Technique mapping.

Table 1. Prevalent MITRE ATT&CK techniques for evaluation



Tactic	Technique	Name	Test count
Execution	T1086	PowerShell	9
Defense Evasion	T1027	Obfuscated Files or Information	2
Credential Access	T1003	Credential Dumping	9
Defense Evasion, Privilege Escalation	T1055	Process Injection	3
Execution, Defense Evasion	T1064	Scripting	1
Defense Evasion	T1036	Masquerading	7
Persistence	T1060	Registry Run Keys / Startup Folder	3
Lateral Movement, Command And Control	T1105	Remote File Copy	3
Command And Control	T1071	Standard Application Layer Protocol	7
Discovery	T1057	Process Discovery	1
Discovery	T1082	System Information Discovery	3
Persistence, Privilege Escalation	T1015	Accessibility Features	1
Defense Evasion, Execution	T1085	Rundll32	6
Execution	T1035	Service Execution	2
Defense Evasion	T1089	Disabling Security Tools	13
Discovery	T1087	Account Discovery	4
Execution, Persistence, Privile	T1053	Scheduled Task	3
Lateral Movement	T1077	Windows Admin Shares	4
Execution	T1204	User execution	3

After collecting the prevalent techniques, the mapping to MITRE ATT&CK Evaluations APT3 and APT27 rounds was done to see how different the most prevalent techniques are from the techniques used by APT's – the similarity is surprising. Fourteen APT techniques of selected twenty are used by both APT3 and APT27 evaluations, and only two techniques out of the twenty most common techniques were not used in the APT evaluations. Although there were thirty-six additional techniques used in the APT evaluations but had no records in any of the threat intelligence reports the prevalent techniques table is based on.

More details on MITRE ATT&CK evaluations are described in chapter MITRE ATT&CK Evaluations for APT tactics.

The full list of mentioned MITRE ATT&CK techniques, prevalence scores, and APT evaluation mapping is in Appendix 2 – Technique mapping.

4.3 Automated testing of MITRE ATT&CK techniques

MITRE ATT&CK framework describes how adversaries might use the techniques, describes what could be monitored for detection and what defences could be bypassed. However, there are no tests described in MITRE ATT&CK, and it is not documented as being part of the framework.

Other sources for tests mapped to the MITRE ATT&CK exist and, therefore, can easily be included in the use of the framework. For the thesis, only open-source testing tools are considered.

According to authors own research and several articles on the Internet there seem to be four popular options for open-source testing tools – Red Canary Atomic Red Team, MITRE CALDERA, Endgame Red Team Automation and Uber Metta. [25] [26] [27]

The Atomic Red Team and Invoke-AtomicRedTeam projects are used in the thesis.

4.3.1 Atomic Red Team and Invoke-AtomicRedTeam

Atomic Red Team is developed by Red Canary. As the name suggests, the focus is on test security controls by executing simple "atomic tests" that exercise the techniques in MITRE ATT&CK framework. The tests have few dependencies, and installation is not required. The project is actively maintained and has an active community for support. [28]

For automation, a PowerShell module called Invoke-AtomicRedTeam is developed. Invoke-AtomicRedTeam allows checking and gathering dependencies for tests, provides details of tests, includes clean-up methods and enables users to run tests from PowerShell. Windows, macOS and Linux are supported. [29]

The isolated test-cases and the ability to execute single tests without significant setup process makes the projects suitable for the thesis approach.

The documentation for the projects is up-to-date, specifications and details are available for each test, and support channels for the projects are active. During the testing, the thesis author noticed some bugs in a few of the tests, and by addressing them in the project communication channel, the project was updated within 24 hours with fixes.

4.3.2 Alternative solutions

Endgame Red Team Automation – developed for testing detection capabilities. The approach is based on Python, comprised of scripts and compiled binary files. The project seems to be abandoned. [30]

Uber's Metta – developed for testing security solutions by running adversarial simulations. More focussed on running scenarios rather than single tests. The project seems to be abandoned. [31]

CALDERA – automated red team system by MITRE. Created to test detections and attacks by running multi-staged activities to simulate big attack scenarios. Used for MITRE APT Evaluations [32].

4.4 Testing environment and configuration

The testing is done in the authors' virtualisation environment based on Proxmox cluster [33]. For FireEye testing, virtual machines were used which on next reboot would configure themselves as new clients to FireEye management console. Such setup allowed to isolate testing data per technique tested and allow for more straightforward evaluation of detection capabilities.

Testing virtual machine configuration:

- Hardware
  - RAM: 4GB
  - Disk: 32GB
  - CPU: 4 cores
- Software
  - Windows 10 Professional N, 64bit
    - Build 138362.720, latest updates installed
  - FireEye HX Agent 31.28.8
  - Sysmon [34] with configuration by SwiftOnSecurity [35]
- Configuration changes
  - Windows Defender disabled
  - FireEye HX monitoring only

  - PowerShell ScriptBlock logging enabled

For testing purposes, all preventive actions by FireEye HX were disabled and where possible, configured to only monitor and generate alerts. Such configuration is done to avoid blocking the first stages of attack techniques and possibly missing the opportunity to analyse gathered data and alerting on later stages.

Sysmon was installed to be able to verify if tests were executing correctly quickly.

The virtualisation environments resources allowed the author to use six testing virtual machines simultaneously and snapshots were used to stop and run different instances of virtual machines when needed, depending on the number of tests per technique. From FireEye management console's point of view, twelve hosts were used.

4.4.1 Testing procedure

The testing of techniques is separated into different virtual machines. Generally, one virtual machine was used for all sub-techniques for one MITRE ATT&CK technique to keep the environment clean and identical for all tests.

Each test result of sub-technique was verified using EDR alerts and collected data, if available. When unable to verify the results with the EDR, the installed Sysmon and Windows event logs were used to verify if a test was running correctly.

In case a test did not execute according to documentation, results were not included in the overall results of testing.

If alerts were triggered, but not by the exact technique in focus, zero scores were assigned.

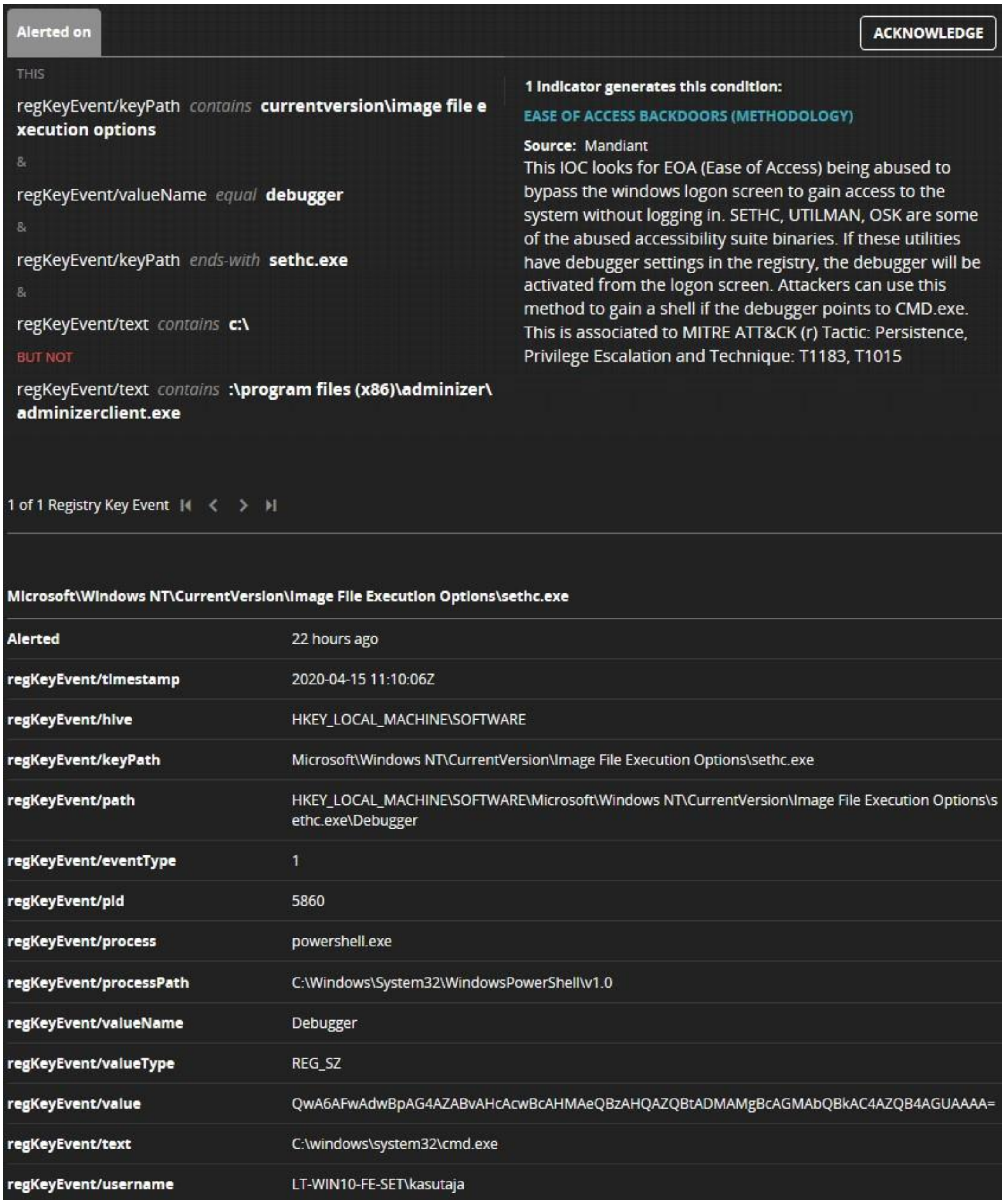
5 FireEye HX effectiveness as a platform

5.1 Alerting on common MITRE ATT&CK techniques

It must be kept in mind that detecting techniques based on documented tests might give better results than real-life situations facing attackers. However, many alerting methods are general enough to be challenging to avoid and yet using keywords which are specific to malicious activities. Similarly, to other cybersecurity areas, the alerting in EDR products is a never-ending cat-and-mouse game with the attackers.

Testing included some techniques not triggering any alerts. Some examples are techniques T1082 System Information Discovery and T1057 Process Discovery, T1064 Scripting, T1071 Standard Application Layer Protocols and T1027 Obfuscated Files or Information and T1060 Registry Run Keys / Startup Folder. Each of these techniques is also commonly used by regular users and applications, making it difficult to alert without false positives, which is also why the techniques end up in the list of popular approaches by attackers.

FireEye HX alerts give the incident responders detailed information on what exactly triggered the alert together with a description of suspected malicious activity (Figure 2. FireEye Alert).



THIS

regKeyEvent/keyPath *contains* **currentversion\image file execution options**

&

regKeyEvent/valueName *equal* **debugger**

&

regKeyEvent/keyPath *ends-with* **sethc.exe**

&

regKeyEvent/text *contains* **c:\**

BUT NOT

regKeyEvent/text *contains* **:\program files (x86)\adminizer\adminizerclient.exe**

1 Indicator generates this condition:

EASE OF ACCESS BACKDOORS (METHODOLOGY)

Source: Mandiant

This IOC looks for EOA (Ease of Access) being abused to bypass the windows logon screen to gain access to the system without logging in. SETHC, UTILMAN, OSK are some of the abused accessibility suite binaries. If these utilities have debugger settings in the registry, the debugger will be activated from the logon screen. Attackers can use this method to gain a shell if the debugger points to CMD.exe. This is associated to MITRE ATT&CK (r) Tactic: Persistence, Privilege Escalation and Technique: T1183, T1015

1 of 1 Registry Key Event

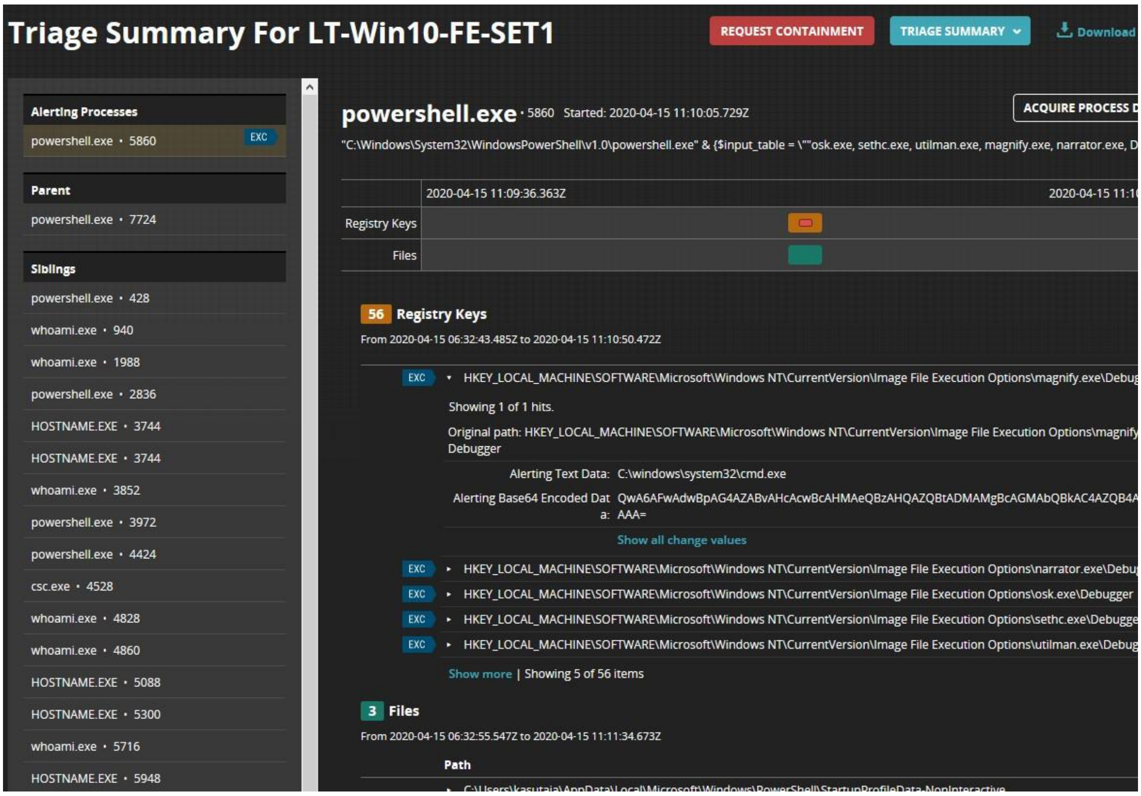
Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe

Alerted	22 hours ago
regKeyEvent/timestamp	2020-04-15 11:10:06Z
regKeyEvent/hive	HKEY_LOCAL_MACHINE\SOFTWARE
regKeyEvent/keyPath	Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe
regKeyEvent/path	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe\Debugger
regKeyEvent/eventType	1
regKeyEvent/pid	5860
regKeyEvent/process	powershell.exe
regKeyEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0
regKeyEvent/valueName	Debugger
regKeyEvent/valueType	REG_SZ
regKeyEvent/value	QwA6AFwAdwBpAG4AZABvAHcAcwBcAHMAeQBzAHQAZQBtADMAMgBcAGMAbQBkAC4AZQB4AGUAAAA=
regKeyEvent/text	C:\windows\system32\cmd.exe
regKeyEvent/username	LT-WIN10-FE-SET\kasutaja

Figure 2. FireEye Alert

5.2 Incident investigations and collected data

In case a FireEye HX alert is triggered the management console also triggers an automated collection of a triage package for more detailed information to enable responders to verify if the alert is true-positive and start the investigation immediately if needed (Figure 3. Triage Summary).



Triage Summary For LT-Win10-FE-SET1

Alerting Processes

powershell.exe • 5860

Parent

powershell.exe • 7724

Siblings

powershell.exe • 428
whoami.exe • 940
whoami.exe • 1988
powershell.exe • 2836
HOSTNAME.EXE • 3744
HOSTNAME.EXE • 3744
whoami.exe • 3852
powershell.exe • 3972
powershell.exe • 4424
csc.exe • 4528
whoami.exe • 4828
whoami.exe • 4860
HOSTNAME.EXE • 5088
HOSTNAME.EXE • 5300
whoami.exe • 5716
HOSTNAME.EXE • 5948

powershell.exe • 5860 Started: 2020-04-15 11:10:05.729Z

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & {$input_table = \""osk.exe, sethc.exe, utilman.exe, magnify.exe, narrator.exe, D

	2020-04-15 11:09:36.363Z	2020-04-15 11:1
Registry Keys	🟧	
Files	🟩	

56 Registry Keys

From 2020-04-15 06:32:43.485Z to 2020-04-15 11:10:50.472Z

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe\Debug
Showing 1 of 1 hits.
Original path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify
Debugger
        Alerting Text Data:  C:\windows\system32\cmd.exe
  Alerting Base64 Encoded Dat  QwA6AFwAdwBpAG4AZABvAHcAcwBcAHMAeQBzAHQAZQBtADMAMgBcAGMAbQBkAC4AZQB4A
                           a:  AAA=
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\narrator.exe\Debu
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\osk.exe\Debugger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe\Debugge
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe\Debug
```

| Showing 5 of 56 items

3 Files

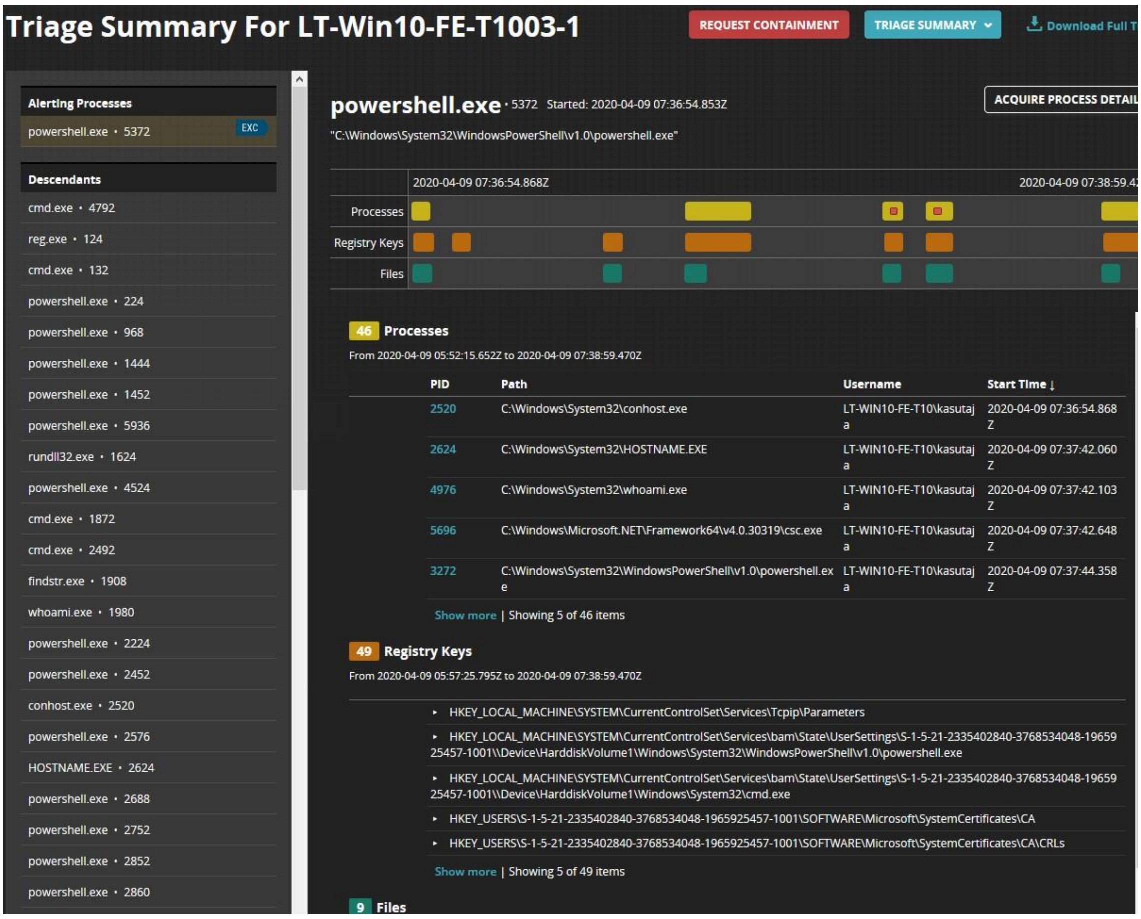
From 2020-04-15 06:32:55.547Z to 2020-04-15 11:11:34.673Z

Path

C:\Users\kasutaja\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Figure 3. Triage Summary

The triage package displays in a concise view of the related activities on the endpoint. For example, suspicious PowerShell usage (Figure 4. Triage Summary, suspicious PowerShell usage). Processes, registry key changes and file changes are shown on a timeline, with red marks on the alerting items. A table with some details of each category is shown for an overview.



Triage Summary For LT-Win10-FE-T1003-1

Alerting Processes

powershell.exe • 5372

Descendants

cmd.exe • 4792
reg.exe • 124
cmd.exe • 132
powershell.exe • 224
powershell.exe • 968
powershell.exe • 1444
powershell.exe • 1452
powershell.exe • 5936
rundll32.exe • 1624
powershell.exe • 4524
cmd.exe • 1872
cmd.exe • 2492
findstr.exe • 1908
whoami.exe • 1980
powershell.exe • 2224
powershell.exe • 2452
conhost.exe • 2520
powershell.exe • 2576
HOSTNAME.EXE • 2624
powershell.exe • 2688
powershell.exe • 2752
powershell.exe • 2852
powershell.exe • 2860

powershell.exe • 5372 Started: 2020-04-09 07:36:54.853Z

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

2020-04-09 07:36:54.868Z 2020-04-09 07:38:59.4

46 **Processes**

From 2020-04-09 05:52:15.652Z to 2020-04-09 07:38:59.470Z

PID	Path	Username	Start Time ↓
2520	C:\Windows\System32\conhost.exe	LT-WIN10-FE-T10\kasutaja	2020-04-09 07:36:54.868Z
2624	C:\Windows\System32\HOSTNAME.EXE	LT-WIN10-FE-T10\kasutaja	2020-04-09 07:37:42.060Z
4976	C:\Windows\System32\whoami.exe	LT-WIN10-FE-T10\kasutaja	2020-04-09 07:37:42.103Z
5696	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	LT-WIN10-FE-T10\kasutaja	2020-04-09 07:37:42.648Z
3272	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	LT-WIN10-FE-T10\kasutaja	2020-04-09 07:37:44.358Z

Show more | Showing 5 of 46 items

49 **Registry Keys**

From 2020-04-09 05:57:25.795Z to 2020-04-09 07:38:59.470Z

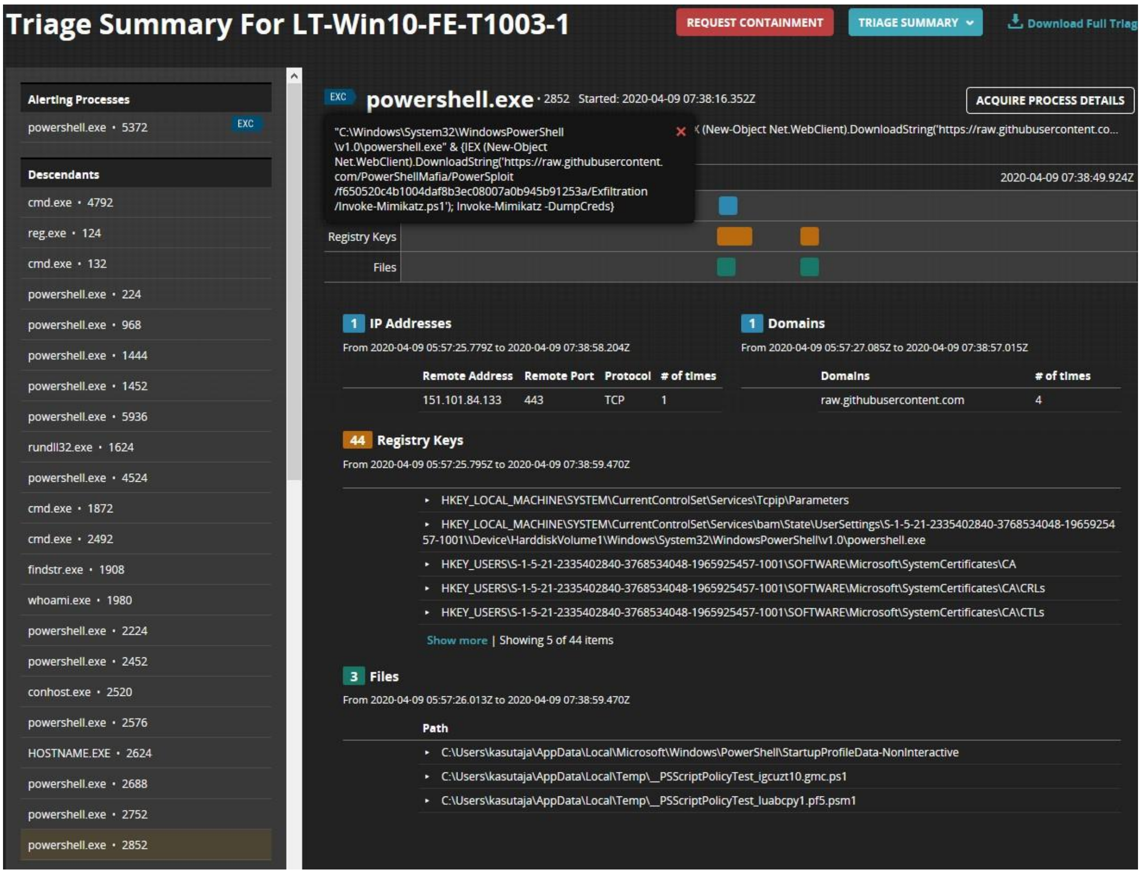
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2335402840-3768534048-1965925457-1001\\Device\HarddiskVolume1\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2335402840-3768534048-1965925457-1001\\Device\HarddiskVolume1\Windows\System32\cmd.exe
- HKEY_USERS\S-1-5-21-2335402840-3768534048-1965925457-1001\SOFTWARE\Microsoft\SystemCertificates\CA
- HKEY_USERS\S-1-5-21-2335402840-3768534048-1965925457-1001\SOFTWARE\Microsoft\SystemCertificates\CA\CRLs

Show more | Showing 5 of 49 items

9 **Files**

Figure 4. Triage Summary, suspicious PowerShell usage

To further focus on a specific process or modification of the system, the incident responder can open a detailed view of a specific process (Figure 5. Triage Summary, process details) which includes the full command-line used to execute the process, file and registry changes, network connections initiated, and domain names involved.



Triage Summary For LT-Win10-FE-T1003-1

Alerting Processes

powershell.exe • 5372 EXC

Descendants

cmd.exe • 4792
reg.exe • 124
cmd.exe • 132
powershell.exe • 224
powershell.exe • 968
powershell.exe • 1444
powershell.exe • 1452
powershell.exe • 5936
rundll32.exe • 1624
powershell.exe • 4524
cmd.exe • 1872
cmd.exe • 2492
findstr.exe • 1908
whoami.exe • 1980
powershell.exe • 2224
powershell.exe • 2452
conhost.exe • 2520
powershell.exe • 2576
HOSTNAME.EXE • 2624
powershell.exe • 2688
powershell.exe • 2752
powershell.exe • 2852

EXC **powershell.exe** • 2852 Started: 2020-04-09 07:38:16.352Z

```
"C:\Windows\System32\WindowsPowerShell
\v1.0\powershell.exe" & {IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.
com/PowerShellMafia/PowerSploit
/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration
/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds}
```

X (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.co...

2020-04-09 07:38:49.924Z

Registry Keys

Files

1 IP Addresses

From 2020-04-09 05:57:25.779Z to 2020-04-09 07:38:58.204Z

Remote Address	Remote Port	Protocol	# of times
151.101.84.133	443	TCP	1

1 Domains

From 2020-04-09 05:57:27.085Z to 2020-04-09 07:38:57.015Z

Domains	# of times
raw.githubusercontent.com	4

44 Registry Keys

From 2020-04-09 05:57:25.795Z to 2020-04-09 07:38:59.470Z

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2335402840-3768534048-1965925457-1001\\Device\HarddiskVolume1\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- HKEY_USERS\S-1-5-21-2335402840-3768534048-1965925457-1001\SOFTWARE\Microsoft\SystemCertificates\CA
- HKEY_USERS\S-1-5-21-2335402840-3768534048-1965925457-1001\SOFTWARE\Microsoft\SystemCertificates\CA\CRLs
- HKEY_USERS\S-1-5-21-2335402840-3768534048-1965925457-1001\SOFTWARE\Microsoft\SystemCertificates\CA\CTLs

Show more | Showing 5 of 44 items

3 Files

From 2020-04-09 05:57:26.013Z to 2020-04-09 07:38:59.470Z

Path

- C:\Users\kasutaja\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
- C:\Users\kasutaja\AppData\Local\Temp\__PSScriptPolicyTest_igcuzt10.gmc.ps1
- C:\Users\kasutaja\AppData\Local\Temp\__PSScriptPolicyTest_luabcpy1.pf5.psm1

Figure 5. Triage Summary, process details

Depending on the incident responders’ decisions or Standard Operating Procedures, the endpoint could be contained, meaning all network connections would be blocked except specific exclusions needed for endpoint management and data acquisitions.

In case in-depth investigation is needed, the following data acquisition options are available from FireEye HX platform:

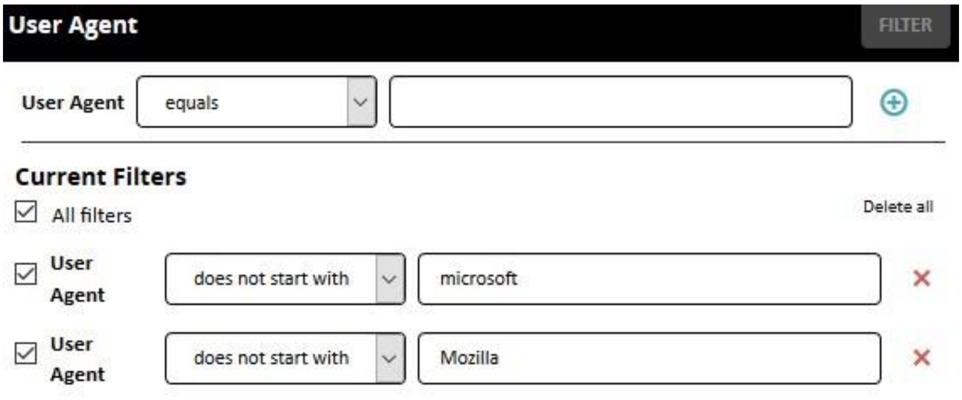
- File
- Triage
- Standard Investigative Details
- Comprehensive Investigative Details
- Quick File Listing
- Command Shell History (XP/2000/2003)
- Process Memory
- Driver Memory
- Full Memory
- Raw Disk

- PowerShell History (From Event Logs)
- Agent Diagnostics

While some of the data acquisitions can be analysed with the FireEye HX console, memory dumps and larger acquisitions require extra tools. FireEye provides a free tool called Redline to analyse memory and disk acquisitions, in addition to FireEye HX triage collections [36].

For the acquisition’s analysis within the console when Triage Summary is not providing enough detail, the Audit Viewer can be used to search and filter all the data in Triage packages or other smaller acquisitions.

For example, the Url Monitor Events category could be used and when filtering out a few common User Agents (Figure 6. Audit Viewer, User Agent filter) the outliers can be spotted with associated domain names, IP addresses and processes (Figure 7. Audit Viewer, Url Monitor Events).



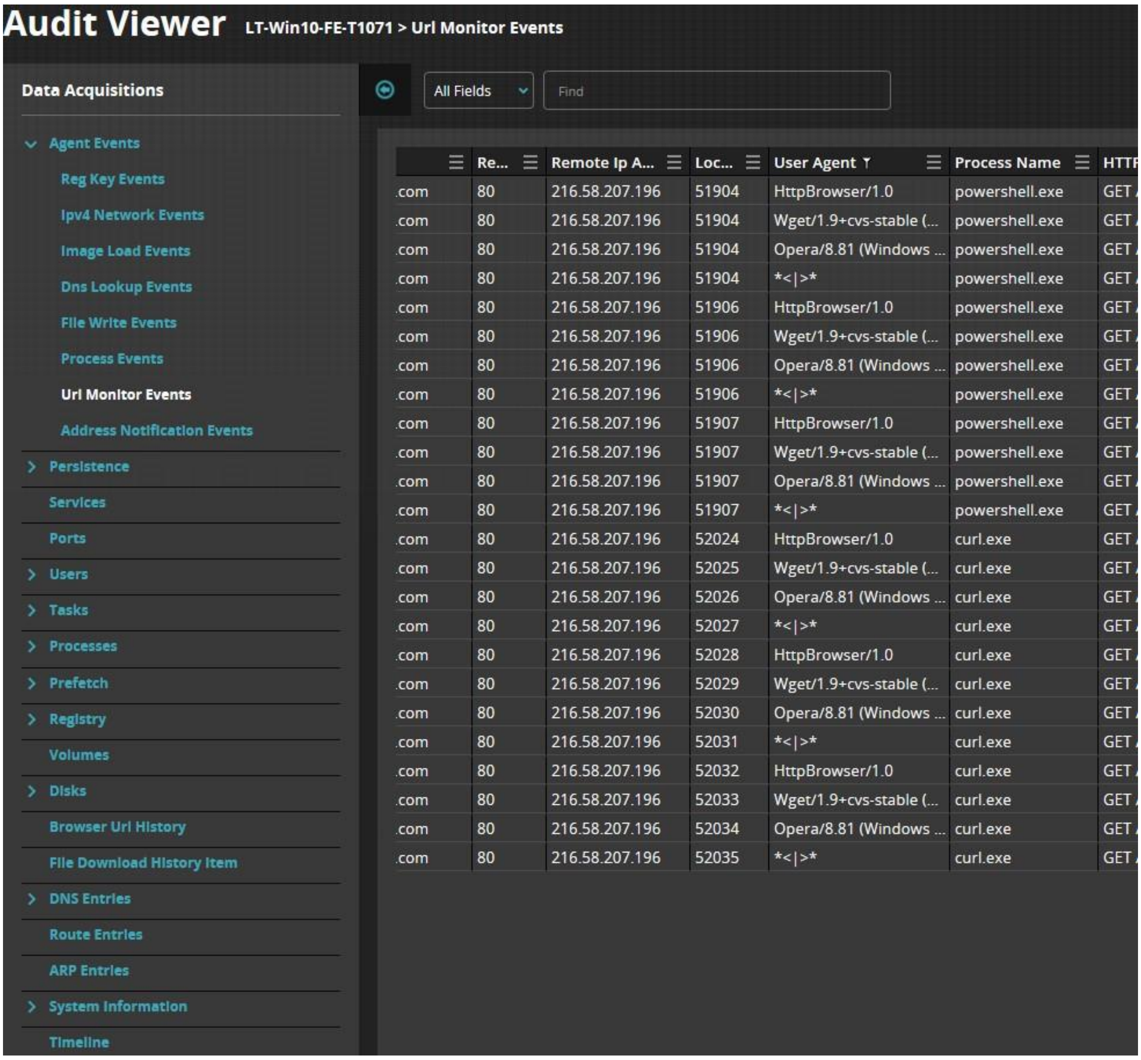
User Agent equals

☑ All filters

☑ User Agent does not start with microsoft

☑ User Agent does not start with Mozilla

Figure 6. Audit Viewer, User Agent filter



	Re...	Remote Ip A...	Loc...	User Agent	Process Name	HTT
.com	80	216.58.207.196	51904	HttpBrowser/1.0	powershell.exe	GET
.com	80	216.58.207.196	51904	Wget/1.9+cvs-stable (...	powershell.exe	GET
.com	80	216.58.207.196	51904	Opera/8.81 (Windows ...	powershell.exe	GET
.com	80	216.58.207.196	51904	*<|>*	powershell.exe	GET
.com	80	216.58.207.196	51906	HttpBrowser/1.0	powershell.exe	GET
.com	80	216.58.207.196	51906	Wget/1.9+cvs-stable (...	powershell.exe	GET
.com	80	216.58.207.196	51906	Opera/8.81 (Windows ...	powershell.exe	GET
.com	80	216.58.207.196	51906	*<|>*	powershell.exe	GET
.com	80	216.58.207.196	51907	HttpBrowser/1.0	powershell.exe	GET
.com	80	216.58.207.196	51907	Wget/1.9+cvs-stable (...	powershell.exe	GET
.com	80	216.58.207.196	51907	Opera/8.81 (Windows ...	powershell.exe	GET
.com	80	216.58.207.196	51907	*<|>*	powershell.exe	GET
.com	80	216.58.207.196	52024	HttpBrowser/1.0	curl.exe	GET
.com	80	216.58.207.196	52025	Wget/1.9+cvs-stable (...	curl.exe	GET
.com	80	216.58.207.196	52026	Opera/8.81 (Windows ...	curl.exe	GET
.com	80	216.58.207.196	52027	*<|>*	curl.exe	GET
.com	80	216.58.207.196	52028	HttpBrowser/1.0	curl.exe	GET
.com	80	216.58.207.196	52029	Wget/1.9+cvs-stable (...	curl.exe	GET
.com	80	216.58.207.196	52030	Opera/8.81 (Windows ...	curl.exe	GET
.com	80	216.58.207.196	52031	*<|>*	curl.exe	GET
.com	80	216.58.207.196	52032	HttpBrowser/1.0	curl.exe	GET
.com	80	216.58.207.196	52033	Wget/1.9+cvs-stable (...	curl.exe	GET
.com	80	216.58.207.196	52034	Opera/8.81 (Windows ...	curl.exe	GET
.com	80	216.58.207.196	52035	*<|>*	curl.exe	GET

Figure 7. Audit Viewer, Url Monitor Events

5.3 Enterprise Search

FireEye HX incorporates a feature called Enterprise Search, allowing analysts to search the endpoints for suspicious activities, which might have bypassed detection and prevention mechanisms. The quicker, default search, uses the ring-buffer on the endpoints. The ring-buffer stores a configured amount of recent data rotationally regarding the recent process and network activities and system changes for analysis. The more thorough and therefore slower option is the exhaustive search, which goes through required registry hives or disk locations to look for matches to the search criteria.

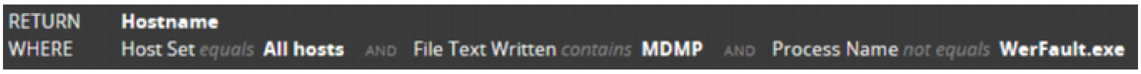
Enterprise Search includes criteria to search for:

- web browser name and version

- cookie names flags and values
- DNS hostnames
- driver device names and module names
- indications of process injections
- executable PE types
- file attributes
- certificate issuer name and subject
- file download referrer and download type
- file full paths and hashes
- filename
- if a file is signed and if the signature is verified
- first bytes of written files
- HTTP headers
- IP addresses
- process names
- parent processes
- process arguments
- registry paths and values

This list is not complete. The search criteria can be combined and used to create logical expressions.

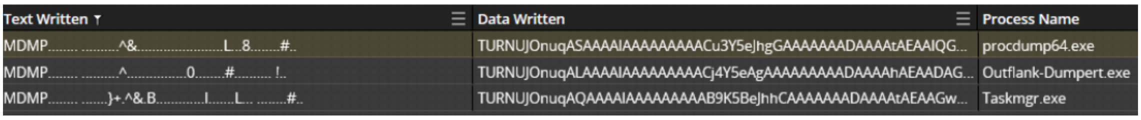
For example, to look for process memory dumps, which often are in the file format where the headers first bytes are “MDMP”, not created by the WerFault.exe process – the Windows process part of Error Reporting tool (Figure 8. Enterprise Search - Process memory dump).



RETURN Hostname
WHERE Host Set *equals* **All hosts** AND File Text Written *contains* **MDMP** AND Process Name *not equals* **WerFault.exe**

Figure 8. Enterprise Search - Process memory dump

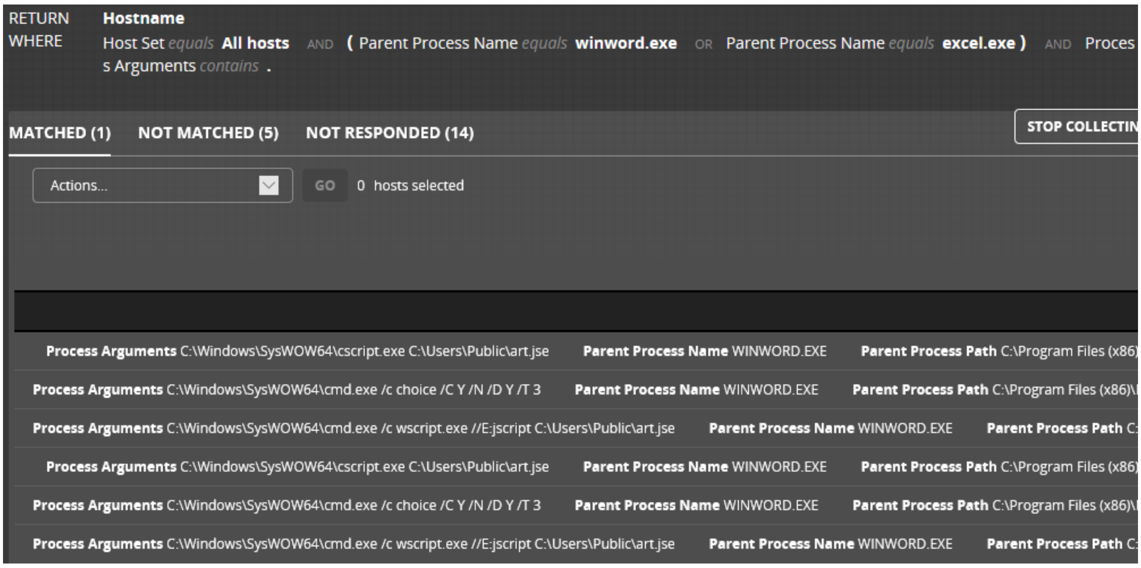
In this example, three suspicious processes creating process memory dumps are detected and could be the starting points of investigations (Figure 9. Enterprise Search - Process memory dump results). Memory dump of lsass.exe process could be exfiltrated, with the purpose to use Mimikatz [37] or other similar tools to extract passwords from the dump while never copying the tools themselves to the compromised endpoint to avoid detection.



Text Written	Data Written	Process Name
MDMP........ ....^&......................L..8........#..	TURNUJOnuqASAAAAIAAAAAAAAACu3Y5eJhgGAAAAAAADAAAAtAEAAIQG...	procdump64.exe
MDMP........ ....^................0........#.......... !..	TURNUJOnuqALAAAAIAAAAAAAAACj4Y5eAgAAAAAAAAADAAAAhAEAADAG...	Outflank-Dumpert.exe
MDMP........ ....}+.^&.B............I.......L... ....#..	TURNUJOnuqAQAAAAIAAAAAAAAAB9K5BeJhhCAAAAAAADAAAAtAEAAGw...	Taskmgr.exe

Figure 9. Enterprise Search - Process memory dump results

The second example could be the search for Microsoft Office applications spawning new processes and to get the arguments used to execute the processes – it is not common for Office applications to start new processes (Figure 10. Enterprise Search - Microsoft Office as a parent process). Most likely a user has opened a document with malicious use of macros, Dynamic Data Exchange, embedded objects retrieving malicious HTA files or by some other means executing arbitrary code.



RETURN Hostname
WHERE Host Set *equals* **All hosts** AND (Parent Process Name *equals* **winword.exe** OR Parent Process Name *equals* **excel.exe**) AND Process Arguments *contains* .

Process Arguments C:\Windows\SysWOW64\cscript.exe C:\Users\Public\art.jse **Parent Process Name** WINWORD.EXE **Parent Process Path** C:\Program Files (x86)

Process Arguments C:\Windows\SysWOW64\cmd.exe /c choice /C Y /N /D Y /T 3 **Parent Process Name** WINWORD.EXE **Parent Process Path** C:\Program Files (x86)\

Process Arguments C:\Windows\SysWOW64\cmd.exe /c wscript.exe //E:jscript C:\Users\Public\art.jse **Parent Process Name** WINWORD.EXE **Parent Process Path** C:

Process Arguments C:\Windows\SysWOW64\cscript.exe C:\Users\Public\art.jse **Parent Process Name** WINWORD.EXE **Parent Process Path** C:\Program Files (x86)

Process Arguments C:\Windows\SysWOW64\cmd.exe /c choice /C Y /N /D Y /T 3 **Parent Process Name** WINWORD.EXE **Parent Process Path** C:\Program Files (x86)\

Process Arguments C:\Windows\SysWOW64\cmd.exe /c wscript.exe //E:jscript C:\Users\Public\art.jse **Parent Process Name** WINWORD.EXE **Parent Process Path** C:

Figure 10. Enterprise Search - Microsoft Office as a parent process

From the testing results, most of the used techniques would have been discoverable via Enterprise Search, in case the suspicious activity would not have triggered the alert, as it happened for some tests.

Overall the Enterprise Search capability was able to cover 95% (weighted average) of the test case scenarios. Depending on the search types performed there are limits on the number of responses gathered from the endpoints, forcing the analysts to create more specific queries compared to other tools like SIEM.

5.4 Containment

FireEye HX includes a Containment feature to enable incident responders to isolate hosts from the network, with the isolation the attackers would be suspended from their access to the host and give responders more time to mitigate. While the containment can be useful, it can also be a signal to the attacker that the security team has noticed them and motivate them to change the tactics and techniques. In some cases, the containment can cause interruptions in mission-critical work – to avoid such situation some hosts can be excluded from the containable hosts.

The containment configuration includes the possibility to do whitelisting by IP addresses or DNS names. Useful to ensure that the contained hosts are still able to communicate with the FireEye management server, VPN gateway if necessary, or with additional incident response team tools to analyse and respond to detected threats.

5.5 Testing results

The overall testing results show that FireEye HX is capable of providing enough details in the automatically collected triage packages or manually triggered triage collections to successfully detect MITRE ATT&CK techniques in nearly all the tests performed on the prevalent techniques.

Similarly, excellent results were shown with the Enterprise Search capability for threat hunting to discover suspicious activities without any alerting. Currently, the FireEye HX is not providing means to apply the same search to several tenants of a service provider from a single interface making the threat hunting more time-consuming. API could be used to automate the process – documentation with sample code is available from FireEye.

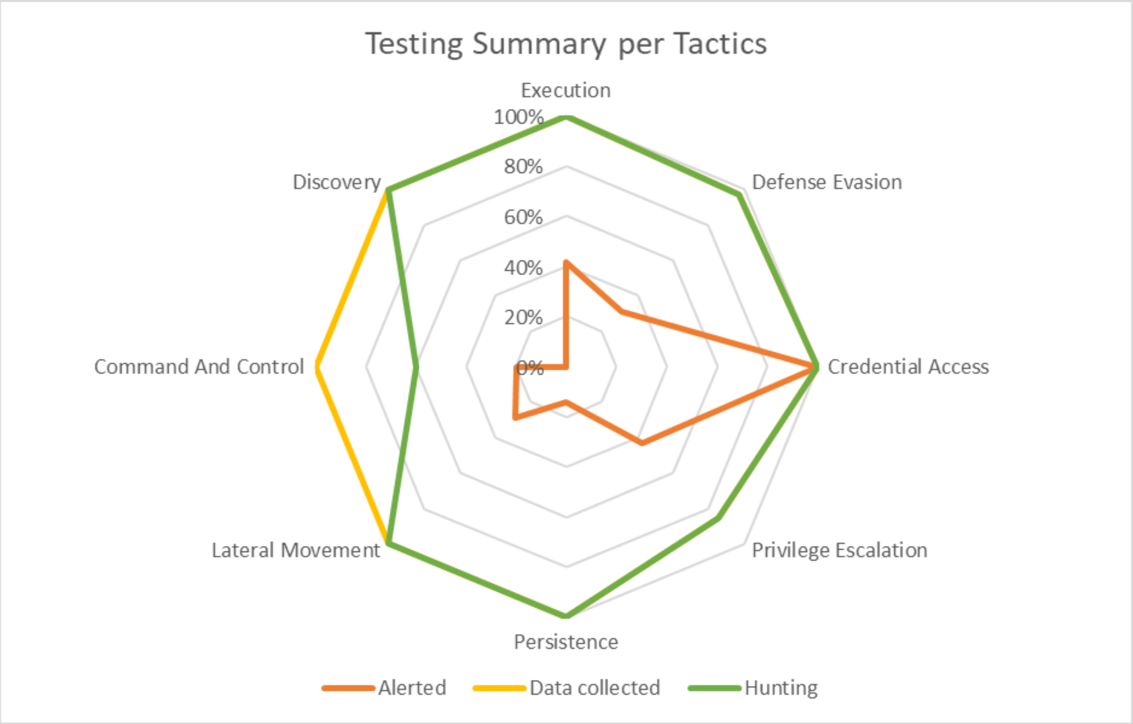


Figure 11. Testing summary per Tactics

The alerting results are probably the reason why the selected prevalent techniques are the most used in the wild – one of the goals of attackers is to stay undetected. From 19 tested techniques, 27% generated an alert in general. Out of 84 performed tests overall, 30 sub-techniques generated an alert, giving a weighted average of 36% for alerting. Although the result of alerting is significantly lower than alerting on each test, it was expected – many of the techniques are performed by users and system administrators while doing daily activities. For example, using scheduled tasks, commands for acquiring details about the system and accounts on the system, scripting and registry run keys among others can create loads of false positives if alerting is set up too generally.

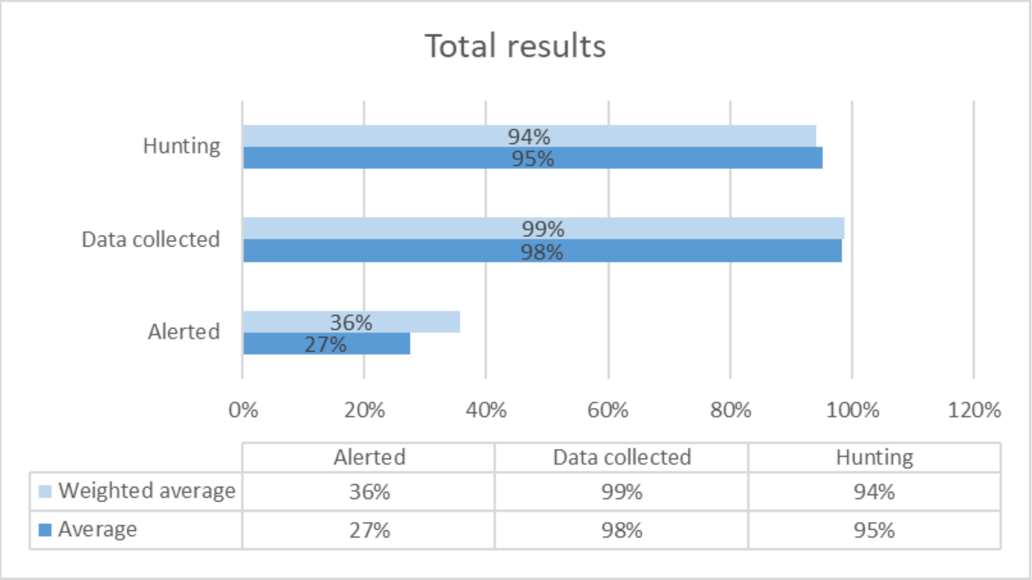


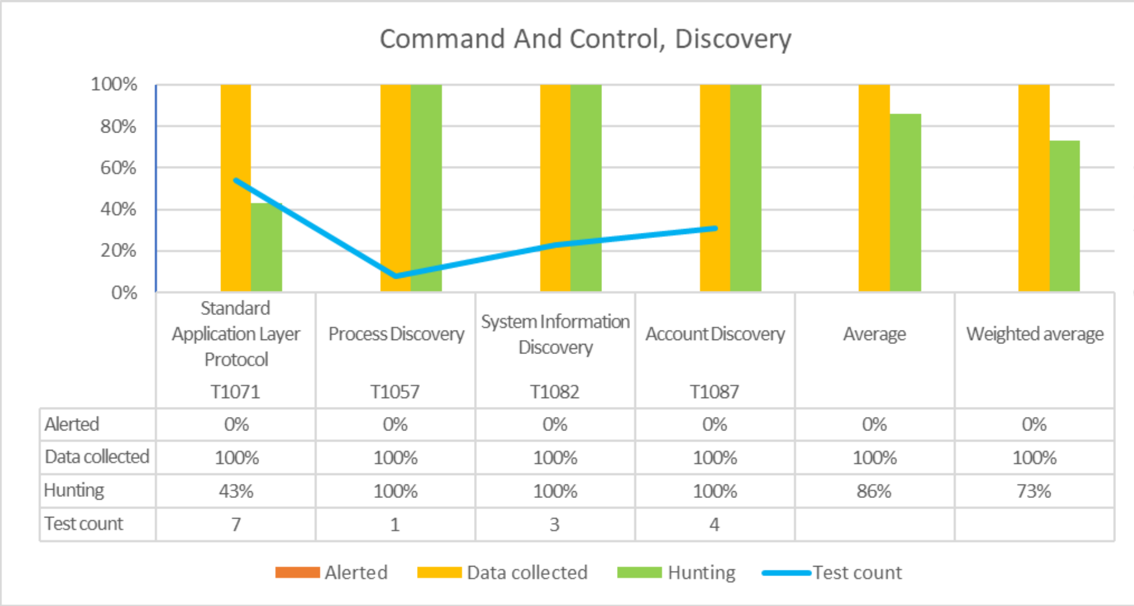
Figure 12. Total results per capability

5.5.1 Results per tactic

The tested tactics are divided into groups by thesis author to analyse the results in more detail. Groups are based on the potential of causing harm to the victim. Groups are listed from least harmful to most.

- Command And Control, Discovery - vital for the attacker for planning further attack stages and maintaining control, not causing any significant harm to the victim.
- Execution, Defense Evasion – necessary for achieving the final goals of the attacker while staying undetected, will directly lead to the last group of tactics.
- Credential Access, Privilege Escalation, Persistence, Lateral Movement – activities are potentially harming and are a direct threat to the victim. Activities can lead to loss of credentials and persistent access to the victim, while possibly increasing the access for the attacker on a single host and spreading in the network.

It is visible that the least harmful tactics are also least likely to generate alert for the defenders (Figure 13. Results per tactics – Command And Control, Discovery). In the testing out of the total 15 sub-techniques tested no alerts were generated, giving an average of 0% for alerting. The activities performed by the tests were commonly used commands and protocols where malicious intent is difficult to distinguish – it is noteworthy for Data collected and Hunting results as well. The data is visible, but interpreting the data can be misleading without further investigation.

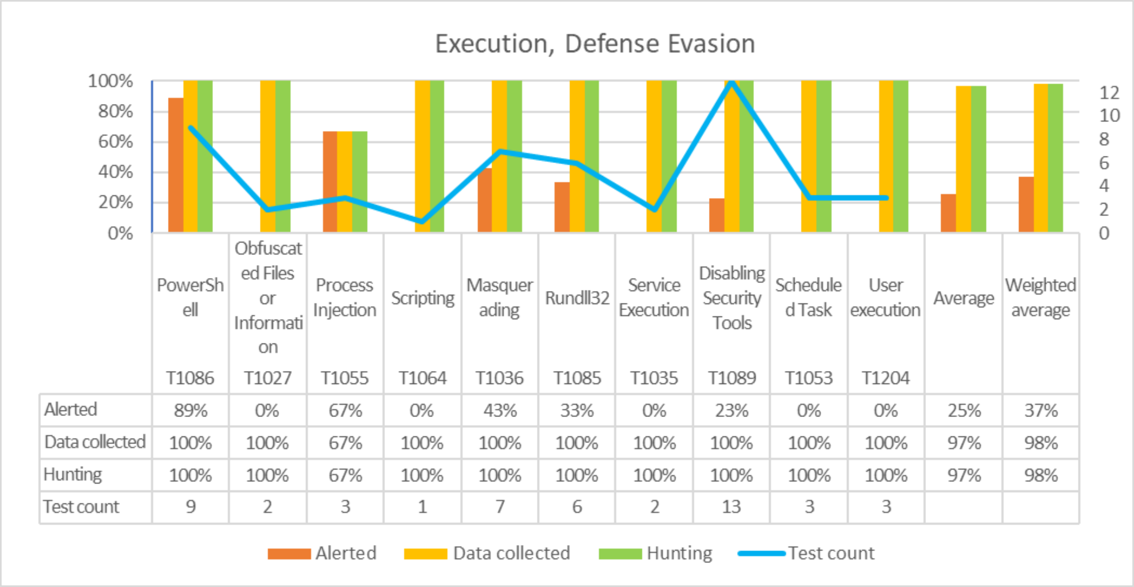


	Standard Application Layer Protocol T1071	Process Discovery T1057	System Information Discovery T1082	Account Discovery T1087	Average	Weighted average
Alerted	0%	0%	0%	0%	0%	0%
Data collected	100%	100%	100%	100%	100%	100%
Hunting	43%	100%	100%	100%	86%	73%
Test count	7	1	3	4		

Figure 13. Results per tactics – Command And Control, Discovery

The middle group, including tactics from Execution and Defense Evasion, involves activities more useful for attackers and more interesting for the defenders (Figure 14. Results per tactics - Execution, Defense Evasion). The techniques in this group are less cumbersome to detect as suspicious and weighted average of alerts per sub-techniques tested is 37%. Some techniques are classified as part of multiple tactics as they can serve multiple purposes.

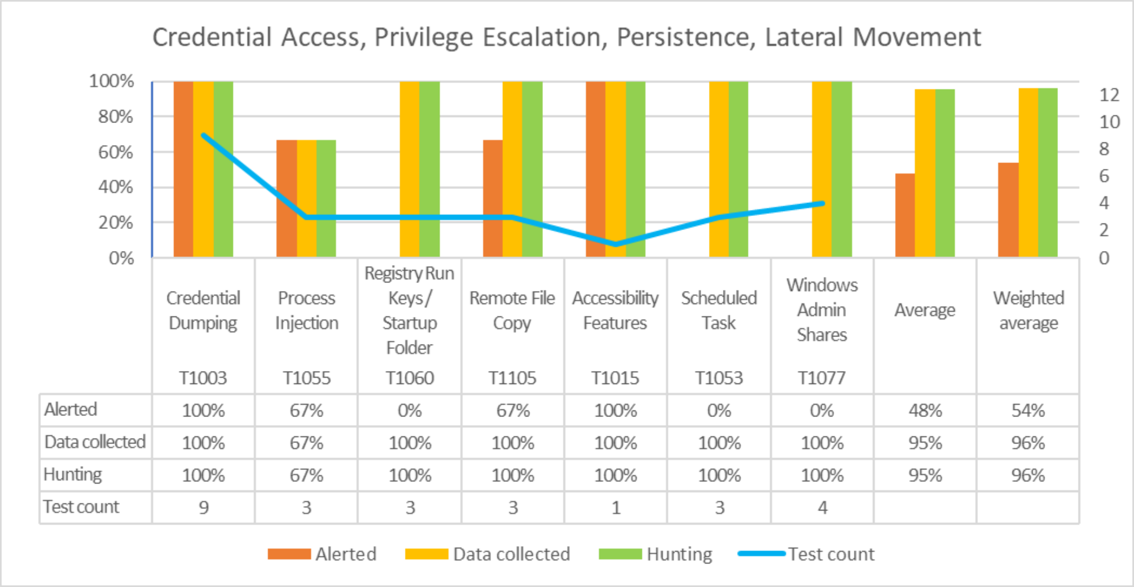
One such technique is T1055 Process Injection, which can be used for Defense Evasion – executing arbitrary code in the address space of a separate live process, which can also lead to Privilege Escalation, depending on the process injected into [38]. The T1055 Process Injection technique is also significant in the thesis context because the Atomic Red Team sub-technique of using C# for process injection bypassed Alerting, Data collection and Hunting capabilities in the testing scope of FireEye HX as only technique.



	PowerShell T1086	Obfuscated Files or Information T1027	Process Injection T1055	Scripting T1064	Masquerading T1036	Rundll32 T1085	Service Execution T1035	Disabling Security Tools T1089	Scheduled Task T1053	User execution T1204	Average	Weighted average
Alerted	89%	0%	67%	0%	43%	33%	0%	23%	0%	0%	25%	37%
Data collected	100%	100%	67%	100%	100%	100%	100%	100%	100%	100%	97%	98%
Hunting	100%	100%	67%	100%	100%	100%	100%	100%	100%	100%	97%	98%
Test count	9	2	3	1	7	6	2	13	3	3		

Figure 14. Results per tactics - Execution, Defense Evasion

The group of Credential Access, Privilege Escalation, Persistence and Lateral Movement tactics is the group with the most potential of causing harm to victims and their computer systems – this group also has the highest alerting score (Figure 15. Results per tactics - Credential Access, Privilege Escalation, Persistence, Lateral Movement).



	Credential Dumping T1003	Process Injection T1055	Registry Run Keys / Startup Folder T1060	Remote File Copy T1105	Accessibility Features T1015	Scheduled Task T1053	Windows Admin Shares T1077	Average	Weighted average
Alerted	100%	67%	0%	67%	100%	0%	0%	48%	54%
Data collected	100%	67%	100%	100%	100%	100%	100%	95%	96%
Hunting	100%	67%	100%	100%	100%	100%	100%	95%	96%
Test count	9	3	3	3	1	3	4		

Figure 15. Results per tactics - Credential Access, Privilege Escalation, Persistence, Lateral Movement

Out of 26 performed sub-technique tests, the average of 54% generated an alarm for the specific techniques. Results are not including the related alerts which might be generated by invoking the malicious activity on the system. The preventive capabilities were not in the testing scope in the thesis, and the capabilities of prevention are unclear. However, the good alerting results in this group show that the FireEye HX has the potential to alert the incident responders in a timely fashion. Enabling quick response and providing an excellent position to stop the attackers from using the acquired information and access in victims network to move towards the goal of the attack campaign.

5.5.2 Summary of FireEye HX testing results

Overall the results of FireEye HX testing were impressive, especially in terms of providing access to detailed data for incident investigation and proactive threat hunting capabilities. Regarding alerting, there were many techniques which did not trigger alerts, although this was to be expected as the techniques tested included standard tools used by regular users and administrators.

Commonly attackers would use many techniques during the single campaign, and on a single host, the chance of triggering at least one alarm is considerably higher than shown testing result averages of alerting. The data collection and hunting abilities are then ready to assist responders in analysing the incident and searching the network for other affected hosts.

On the positive side, no alerts stood out as being prone to generate false positives.

Only single tested sub-technique out of 84 was completely hidden from the author in all aspects. Nearly all techniques were visible on the Triage data collections and searchable with the Enterprise Search feature.

Collection of Triage packages and data acquisitions, in general, feel slower and seem to use endpoint resources more heavily than expected but provide necessary details for incident analysis without needing additional access to systems investigated. However, the data collected for the analysis and threat hunting capabilities is a strong starting point for incident response.

From service providing aspect, FireEye HX is not entirely service provider ready out of the box – FireEye Helix platform can consolidate all alerts and provide incident management capability in a multi-tenant environment. However, the solution does not support using Enterprise Search over multiple FireEye HX instances with a single query. Enterprise Search for multiple instances is automatable with API but requires extra work to build.

6 Summary

In terms of previously set expectations and testing results for alerting, investigation, threat hunting, and response capabilities, FireEye HX achieved outstanding results. Alerting capability showed a good balance of providing actionable alerts and generating no alerts prone to be false positive. The collected data provides a strong foundation for incident response, and Enterprise Search is a capable tool to surface malicious activities by threat hunting. Response capability could be more flexible and targeted, but containment function can be used to stop advancements of the attacker when necessary.

Overall FireEye HX is a capable product and demonstrates that EDR solutions are capable of meeting set requirements for being used as a security as a service providing platform for small and medium-sized businesses to improve the security posture significantly.

Following possibilities for future research were recognised:

- A broader comparison of EDR solutions for service providers
  Few strong contenders are CrowdStrike Falcon, Elastic EDR (former Endgame) and Fortinet FortiEDR who have multi-tenant architecture and could potentially be strong competitors for FireEye HX.

- Improvements for Atomic Red Team project
  Improvement in documentation and reliability of the existing tests would be useful. Additional tests could be added to improve the testing and measurable comparison capability for security solutions further.

- Comparison of EDR preventive capabilities
  Comparison and analysis of preventive capabilities of EDR products mapped to MITRE ATT&CK framework.

References

[1] Verizon, “2019 Data Breach Investigations Report,” 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Accessed 23 04 2020].

[2] C. Bedell and M. Bouchard,, in *Definitive Guide to SOC-as-a-Service*, CyberEdge Group, LLC, 2018, pp. 2-3, 6, 23, 31.

[3] C. Zimmerman, in *Ten Strategies of a World-Class Cybersecurity Operations Center*, MITRE Corporation, 2014, pp. 8-10.

[4] A. Torres, “SANS Institute - Building a World-Class Security Operations Center: A Roadmap,” 15 04 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/membership/35907. [Accessed 12 04 2020].

[5] Redscan, “EPP vs EDR - what's the difference?,” Redscan, 25 03 2020. [Online]. Available: https://www.redscan.com/news/epp-vs-edr-whats-the-difference/. [Accessed 12 04 2020].

[6] P. Firstbrook, D. Zumerle, P. Bhajanka, L. Pingree and P. Webber, “Gartner - Magic Quadrant for Endpoint Protection Platforms,” 20 08 2019. [Online]. Available: https://www.crowdstrike.com/resources/reports/gartner-magic-quadrant-endpoint-protection-platforms-2019/. [Accessed 12 04 2020].

[7] CrowdStrike, “Falcon Firewall Management,” CrowdStrike, [Online]. Available: https://www.crowdstrike.com/endpoint-security-products/falcon-firewall-management/. [Accessed 13 04 2020].

[8] M. K. Hamilton, “MDR vs. MSSP vs. SIEM – InfoSec Acronyms Explained | CI Security,” [Online]. Available: https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained. [Accessed 12 04 2020].

[9] T. Bussa, K. Kavanagh, S. Deshpande, C. Lawson and P. Shoard, “Gartner - Market Guide for Managed Detection and Response Services,” 15 07 2019. [Online]. Available: https://secure2.sophos.com/en-us/security-news-trends/reports/gartner/market-guide-for-mdr-services.aspx. [Accessed 12 04 2020].

[10] “Applying Cyber Kill Chain® Methodology to Network Defense,” Lockheed Martin Corporation, 2015. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. [Accessed 12 04 2020].

[11] C. Brook, “What is the MITRE ATT&CK Framework?,” Digital Guardian, 24 11 2019. [Online]. Available: https://digitalguardian.com/blog/what-mitre-attck-framework. [Accessed 11 04 2020].

[12] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, “MITRE ATT&CK: Design and Philosophy,” 03 2020. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-19-01075-28-mitre-attack-design-and-philosophy.pdf. [Accessed 11 04 2020].

[13] Vincent Le Toux; Ed Williams, Trustwave, SpiderLabs, “Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®,” MITRE, 11 10 2019. [Online]. Available: https://attack.mitre.org/techniques/T1003/. [Accessed 11 04 2020].

[14] “MITRE ATT&CK® EVALUATIONS,” MITRE, [Online]. Available: https://attackevals.mitre.org/. [Accessed 11 04 2020].

[15] “APT - Glossary | Computer Security Resource Center,” [Online]. Available: https://csrc.nist.gov/glossary/term/APT. [Accessed 11 04 2020].

[16] “Managed Detection and Response (MDR) | FireEye,” FireEye, [Online]. Available: https://www.fireeye.com/solutions/managed-defense.html. [Accessed 11 04 2020].

[17] “Managed & Proactive Threat Hunting - Falcon OverWatch | CrowdStrike,” [Online]. Available: https://www.crowdstrike.com/endpoint-security-products/falcon-overwatch-threat-hunting/. [Accessed 11 04 2020].

[18] K. Nickels, “How to Be a Savvy ATT&CK Consumer,” The MITRE Corporation, 13 12 2019. [Online]. Available: https://medium.com/mitre-attack/how-to-be-a-savvy-attack-consumer-63e45b8e94c9. [Accessed 13 04 2020].

[19] “Top 10 MITRE ATT&CK™ Techniques,” [Online]. Available: https://www.trustedsec.com/blog/top-10-mitre-attck-techniques/. [Accessed 11 4 2020].

[20] “Global Threat Report 2019,” 2019. [Online]. Available: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf. [Accessed 11 04 2020].

[21] “McAfee Labs Threats Report August 2019,” 08 2019. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf. [Accessed 11 04 2020].

[22] “2019 Threat Detection Report,” 2019. [Online]. Available: https://resources.redcanary.com/hubfs/ThreatDetectionReport-2019.pdf. [Accessed 08 04 2020].

[23] Red Canary, “2020 Threat Detection Report,” 2020. [Online]. Available: https://redcanary.com/threat-detection-report/introduction/. [Accessed 11 04 2020].

[24] “Defense Evasion Dominant in Top MITRE ATT&CK Tactics of 2019,” Recorded Future, 31 03 2020. [Online]. Available: https://www.recordedfuture.com/mitre-attack-tactics/. [Accessed 11 04 2020].

[25] D. Strom, “4 open-source Mitre ATT&CK test tools compared,” CSO, 12 04 2018. [Online]. Available: https://www.csoonline.com/article/3268545/4-open-source-mitre-attandck-test-tools-compared.html. [Accessed 11 04 2020].

[26] D. Kerr, “Introducing Endgame Red Team Automation | Elastic Blog,” Elastic, 19 03 2018. [Online]. Available: https://www.elastic.co/blog/introducing-endgame-red-team-automation. [Accessed 11 04 2020].

[27] C. Thompson, “Penetration Testing Versus Red Teaming: Clearing the Confusion,” Security Intelligence, 01 05 2019. [Online]. Available: https://securityintelligence.com/posts/penetration-testing-versus-red-teaming-clearing-the-confusion/. [Accessed 11 04 2020].

[28] "GitHub - redcanaryco/atomic-red-team: Small and highly portable detection tests based on MITRE's ATT&CK.," Red Canary, [Online]. Available: https://github.com/redcanaryco/atomic-red-team. [Accessed 11 04 2020].

[29] "GitHub - redcanaryco/invoke-atomicredteam," [Online]. Available: https://github.com/redcanaryco/invoke-atomicredteam. [Accessed 11 04 2020].

[30] "GitHub - endgameinc/RTA," [Online]. Available: https://github.com/endgameinc/RTA. [Accessed 11 04 2020].

[31] "GitHub - uber-common/metta: An information security preparedness tool to do adversarial simulation.," [Online]. Available: https://github.com/uber-common/metta. [Accessed 11 04 2020].

[32] "CALDERA | The MITRE Corporation," [Online]. Available: https://www.mitre.org/research/technology-transfer/open-source-software/caldera. [Accessed 19 04 2020].

[33] "Proxmox - powerful open-source server solutions," [Online]. Available: https://www.proxmox.com/en/. [Accessed 15 04 2020].

[34] "Sysmon - Windows Sysinternals | Microsoft Docs," [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon. [Accessed 15 04 2020].

[35] "GitHub - SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing," [Online]. Available: https://github.com/SwiftOnSecurity/sysmon-config. [Accessed 15 04 2020].

[36] "Redline | Free Security Software | FireEye," [Online]. Available: https://www.fireeye.com/services/freeware/redline.html. [Accessed 16 04 2020].

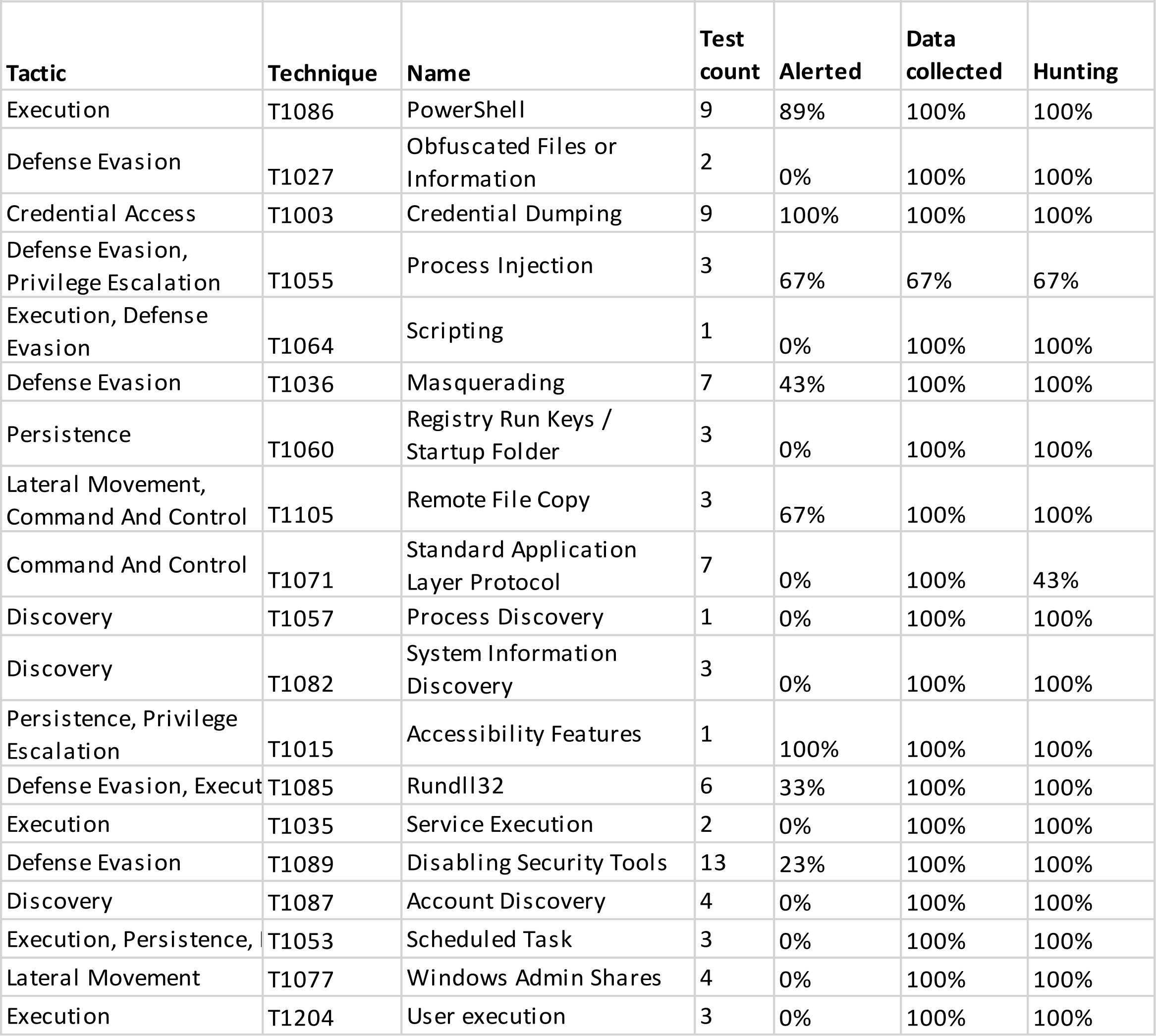
[37] "Mimikatz – Active Directory Security," [Online]. Available: https://adsecurity.org/?page_id=1821. [Accessed 16 04 2020].

[38] A. Pingios, C. Beek and R. Becwar, "Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®," 18 07 2019. [Online]. Available: https://attack.mitre.org/techniques/T1055/. [Accessed 29 04 2020].

[39] "Continuous validation of your security control.," [Online]. Available: https://attackiq.com/. [Accessed 11 04 2020].

[40] "Accessibility Features, Technique T1015 - Enterprise | MITRE ATT&CK®," [Online]. Available: https://attack.mitre.org/techniques/T1015/. [Accessed 16 04 2020].

Appendix 1 – Test results per technique



Tactic	Technique	Name	Test count	Alerted	Data collected	Hunting
Execution	T1086	PowerShell	9	89%	100%	100%
Defense Evasion	T1027	Obfuscated Files or Information	2	0%	100%	100%
Credential Access	T1003	Credential Dumping	9	100%	100%	100%
Defense Evasion, Privilege Escalation	T1055	Process Injection	3	67%	67%	67%
Execution, Defense Evasion	T1064	Scripting	1	0%	100%	100%
Defense Evasion	T1036	Masquerading	7	43%	100%	100%
Persistence	T1060	Registry Run Keys / Startup Folder	3	0%	100%	100%
Lateral Movement, Command And Control	T1105	Remote File Copy	3	67%	100%	100%
Command And Control	T1071	Standard Application Layer Protocol	7	0%	100%	43%
Discovery	T1057	Process Discovery	1	0%	100%	100%
Discovery	T1082	System Information Discovery	3	0%	100%	100%
Persistence, Privilege Escalation	T1015	Accessibility Features	1	100%	100%	100%
Defense Evasion, Execut	T1085	Rundll32	6	33%	100%	100%
Execution	T1035	Service Execution	2	0%	100%	100%
Defense Evasion	T1089	Disabling Security Tools	13	23%	100%	100%
Discovery	T1087	Account Discovery	4	0%	100%	100%
Execution, Persistence,	T1053	Scheduled Task	3	0%	100%	100%
Lateral Movement	T1077	Windows Admin Shares	4	0%	100%	100%
Execution	T1204	User execution	3	0%	100%	100%

Appendix 2 – Technique mapping

					https://www.trustedsec.com/blog/top-10-mitre-attck-techniques/	https://resources.redcanary.com/hubfs/ThreatDetectionReport-2019.pdf	https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf	https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf	https://redcanary.com/threat-detection-report/techniques/	https://www.recordedfuture.com/mitre-attack-tactics/			
Tactic	Technique	Name	Count of Atomic tests for Windows	Prevalence	Techniques in the report: 10	Techniques in the report: 40	Techniques in the report: 13	Techniques in the report: 8	Techniques in the report: 20	Techniques in the report: 10	Tested with FireEye	AttackEval APT3	AttackEval APT29
Execution	T1086	PowerShell	13	4		primary	primary	primary	primary		yes	yes	yes
Defense Evasion	T1027	Obfuscated Files or Information	2	3.5	primary	secondary		primary		primary	yes	yes	yes
Credential Access	T1003	Credential Dumping	16	3.5	primary	primary	primary		secondary		yes	yes	yes

Defense Evasion, Privilege Escalation	T1055	Process Injection	3	3.5		secondary	primary		primary	primary	yes	yes	yes
Execution, Defense Evasion	T1064	Scripting	1	3		primary	primary		primary		yes	yes	
Defense Evasion	T1036	Masquerading	8	3		primary	primary		primary		yes	yes	yes
Execution	T1059	Command-Line Interface		2.5	primary	secondary	primary					yes	yes
Persistence	T1060	Registry Run Keys / Startup Folder	3	2.5	primary	primary	secondary				yes	yes	yes
Lateral Movement, Command And Control	T1105	Remote File Copy	5	2.5	primary	secondary			primary		yes	yes	yes
Initial Access	T1193	Spearphishing Attachment	1	2.5		primary		primary	secondary		yes		
Command And Control	T1071	Standard Application Layer Protocol	7	2	primary			primary			yes	yes	yes
Discovery	T1057	Process Discovery	1	2	primary					primary	yes	yes	yes
Discovery	T1082	System Information Discovery	3	2	primary					primary	yes	yes	yes

Persistence, Privilege Escalation	T1015	Accessibility Features	1	2		secondary	primary		secondary		yes	yes	
Defense Evasion, Execution	T1085	Rundll32	6	1.5		primary			secondary		yes	yes	yes
Execution	T1035	Service Execution	2	1.5		primary			secondary		yes	yes	yes
Defense Evasion	T1089	Disabling Security Tools	13	1.5		secondary			primary		yes		
Discovery	T1087	Account Discovery	4	1.5		secondary	primary				yes	yes	
Execution, Persistence, Privilege Escalation	T1053	Scheduled Task	4	1.5		secondary			primary		yes	yes	
Lateral Movement	T1077	Windows Admin Shares	4	1.5		secondary			primary		yes	yes	yes
Execution	T1204	User execution	3	1.5		secondary		primary			yes	yes	yes
Discovery	T1083	File and Directory Discovery	2	1	primary							yes	yes
Credential Access, Collection	T1056	Input Capture	1	1	primary							yes	yes
Defense Evasion, Execution	T1117	Regsvr32	3	1		primary						yes	

Defense Evasion, Command And Control	T1090	Connection Proxy	1	1		primary							
Execution	T1047	Windows Management Instrumentation	6	1		secondary			secondary				yes
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	2	1		secondary			secondary				yes
Defense Evasion	T1070	Indicator Removal on Host	4	1		secondary	secondary						
Defense Evasion, Execution	T1170	Mshta	4	1		secondary			secondary				
Defense Evasion, Persistence	T1158	Hidden Files and Directories	4	1			primary						
Collection	T1005	Data from Local System		1			primary						yes
Exfiltration	T1020	Automated Exfiltration		1				primary					
Exfiltration	T1041	Exfiltration on C2 channels		1				primary				yes	yes
Command And Control	T1043	Commonly used ports		1				primary				yes	yes
Persistence, Privilege Escalation,	T1038	DLL Search Order Hijacking	1	1					primary				yes

Defense Evasion													
Discovery	T1482	Domain Trust Discovery	3	1					primary				
Discovery	T1063	Security Software Discovery	4	1						primary		yes	yes
Defense Evasion	T1045	Software packing		1						primary			yes
Defense Evasion	T1073	DLL Side-Loading	1	1						primary			
Exfiltration	T1022	Data Encrypted	3	1						primary		yes	yes
Execution	T1106	Execution through API		1						primary		yes	yes
Command And Control	T1032	Standard Cryptographic Protocol	1	1						primary		yes	yes
Lateral Movement	T1097	Pass The Ticket	1	0.5		secondary							yes
Defense Evasion, Persistence	T1197	BITS Jobs	3	0.5		secondary							
Defense Evasion, Privilege Escalation	T1088	Bypass User Account Control	6	0.5		secondary						yes	yes

Collection	T1074	Data Staged	2	0.5		secondary						yes	yes
Persistence, Privilege Escalation	T1100	Web Shell	1	0.5		secondary							
Defense Evasion, Execution	T1127	Trusted Developer Utilities	1	0.5		secondary							
Discovery	T1069	Permission Groups Discovery	3	0.5		secondary						yes	yes
Defense Evasion	T1146	Clear Command History		0.5		secondary							
Execution, Lateral Movement	T1028	Windows Remote Management	5	0.5		secondary							yes
Exfiltration	T1002	Data Compressed	2	0.5		secondary						yes	yes
Defense Evasion, Execution	T1218	Signed Binary Proxy Execution	8	0.5		secondary							
Exfiltration	T1048	Exfiltration Over Alternative Protocol	1	0.5		secondary						yes	yes
Defense Evasion, Execution	T1118	InstallUtil	8	0.5		secondary							
Privilege Escalation	T1068	Exploitation for Privilege Escalation		0.5		secondary							

Defense Evasion, Execution	T1121	Regsvc/Regasm	2	0.5		secondary							
Execution	T1203	Exploitation for Client Execution		0.5			secondary						
Defense Evasion	T1093	Process Hollowing	1	0.5					secondary				
Persistence, Execution	T1168	Local Job Scheduling		0.5					secondary				
Discovery	T1420	File and Directory Discovery		0.5		secondary							
Persistence, Defense Evasion	T1122	Component Object Model Hijacking											yes
Persistence	T1136	Create Account										yes	yes
Persistence, Privilege Escalation	T1050	New Service										yes	yes
Initial Access, Persistence, Privilege Escalation, Defense Evasion	T1078	Valid Accounts											yes
Persistence	T1084	Windows Management Instrumentation event Subscription											yes

Privilege Escalation, Defense Evasion	T1134	Access Token Manipulation										yes	yes
Defense Evasion	T1107	File Deletion										yes	yes
Defense Evasion	T1112	Modify Registry											yes
Defense Evasion	T1096	NTFS File Attributes											yes
Defense Evasion	T1099	Timestomp											yes
Defense Evasion, Discovery	T1497	Virtualization/Sandbox Evasion											yes
Defense Evasion, Command And Control	T1102	Web Service											yes
Credential Access	T1081	Credentials in Files										yes	yes
Credential Access	T1145	Private Keys											yes
Discovery	T1120	Peripheral Device Discovery											yes

Discovery	T1012	Query Registry										yes	yes
Discovery	T1018	Remote System Discovery										yes	yes
Discovery	T1016	System Network Configuration Discovery										yes	yes
Discovery	T1033	System Owner/User Discovery										yes	yes
Collection	T1119	Automated Collection											yes
Collection	T1115	Clipboard Data										yes	yes
Collection	T1114	Email Collection											yes
Collection	T1113	Screen Capture										yes	yes
Command And Control	T1065	Uncommonly Used Port											yes
Execution	T1061	Graphical User Interface										yes	
Defense Evasion	T1126	Network Share Connection Removal										yes	

Credential access	T1110	Brute Force										yes	
Discovery	T1010	Application Window Discovery										yes	
Discovery	T1135	Network Share Discovery										yes	
Discovery	T1201	Password Policy Discovery										yes	
Discovery	T1049	System Network Connections Discovery										yes	
Discovery	T1007	System Service Discovery										yes	
Lateral Movement	T1076	Remote Desktop Protocol										yes	
Collection	T1039	Data from Network Shared Drive										yes	
Command And Control	T1132	Data Encoding										yes	
Command And Control	T1026	Multiband Communication										yes	