TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
ITC70LT

Jürgen Erm 204787IVCM

HYBRID ANALYSIS OF VULNERABILITY MANAGEMENT PRACTICES IN ORGANIZATIONS TO OUTLINE SUCCESS FACTORS

Master's Thesis

Supervisor
Hayretdin Bahşi
PhD

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
ITC70LT

Jürgen Erm 204787IVCM

HÜBRIIDANALÜÜS UURIMAKS TURVANÕRKUSTE HALDUST ORGANISATSIOONIDES LEIDMAKS EDU FAKTOREID

magistritöö

Juhendaja
Hayretdin Bahşi
Ph.D

Tallinn 2022

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: Jürgen Erm .....
(signature)

Date: Month Day, Year

Annotatsioon

Tehnilised turvanõrkused infosüsteemides mõjutavad organisatsioone negatiivselt. Selleks, et pidevalt kasvava nõrkuste hulgaga toime tulla kasutavad organisatsioonid turvakontrollina paiga ja turvanõrkuste haldust. Töö eesmörk on tuvastada kui edukad on organisatsioonid oma turvanõrkuste halduse kontekstis ning mis on peamised edu ja probleeme põhjustavad faktorid. Meie kontektstis on turvanõrkuste haldus defineeritud kui protsess, mis tuvastab ja kõrvaldab tarkvara vigu mida vastasel juhul saaks organisatsioonide vastu ära kasutada.

Mõistmaks kuidas turvanõrkuste haldus on erinevates organisatsioonides korraldatud kasutasime hübriidanalüüsi, mis koosnes kvantitatiivsetest ja kvalitatiivsetest meetoditest. Analüüsisime turvanõrkuste skaneeringu andmeid mõistmaks trende ja nõrkuste kõrvaldamise efektiivsust ning pool struktureeritud interviud vastutavate isikutega loomaks arusaama nende kogemusest protsessis.

Tulemused näitavad, et viies läbi regulaarset turvanõrkuste haldust organisatsioonid suutsid märkimisväärselt vähendada turvanõrkuste hulka. On oluline märkida, et keskendusime organisatsioonidele, kes on juba mõnda aega turanõrkuste halduse protsessi praktiseerinud. Tuleviku tööna oleks huvitav kõrvutada andmeid organisatsioonidega, kellel on väga kõrged turvanõuded. Töö tulemusena võime märkida, et regulaarne turvanõrkuste haldus on organisatsioonidele kasulik eemaldamaks süsteemidest kriitilisi nõrkusi ja antud informatsiooni saab edukalt ära kasutada parendamaks oma ettevõte turvapaiga protsessi.

Võtmesõnad: turvanõrkuste haldus, turvanõrkuste skaneerimine, küberturvalisus

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 59 leheküljel, 7 peatükki, 21 joonist, 5 tabelit.

Abstract

Organizations are impacted by technical vulnerabilities found in their information systems. To handle the ever increasing amount of weaknesses organizations are using patch and vulnerability management as a security measure. This research aims to determine how successful organizations are in in their vulnerability management efforts and what are the enablers and obstacles they are facing. In this context vulnerability management is defined as a process of detecting and remediating software errors that can be used against the subjects.

To understand how vulnerability management is handled in different organizations we used hybrid analysis approach consisting of quantitative and qualitative methods. Vulnerability scan data was analysed to understand the trends and effectiveness of the remediation of weaknesses and semi-structured interviews were held with people responsible for the process to get information about their experiences.

The results showed that conducting vulnerability management process activities on a regular basis helps organizations significantly reduce security vulnerabilities. It is important to note that this research focused on organizations who had been conduction vulnerability management for some period and it would be interesting to compare vulnerability data with organizations who have strict security requirements. The results suggest that it is beneficial for organizations to conduct regular vulnerability management to reduce their critical weaknesses and the information derived also enables to improve patch management processes.

The thesis is in English and contains 59 pages of text, 7 chapters, 21 figures, 5 tables.

Keywords: vulnerability management, vulnerability scanning, patch management, cybersecurity

List of abbreviations and terms

CCTV	Closed-circuit television
CSV	comma-separated values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
EoL	End of Life systems, meaning the official support from vendor has ended
FTE	Full Time Employee
ISCM	Information Security Continuous Monitoring
KPI	Key Performance Indicator
MSSP	Managed Security Service Provider
NDA	Non Disclosure Agreement
RACI model	Responsible Accountable Consulted Informed model for sharing tasks
SMB	Small and Mid-Size Business
VM	Vulnerability Management
VPR	Vulnerability Priority Rating

Table of Contents

List of Figures

List of Tables

1. Introduction

Digitization has increased the technology adoption across all fields of life and different types of organizations enabling businesses to be more effective in serving their clients. No technological system can ever be perfect from security perspective and safe from technical vulnerabilities.

Security vulnerabilities pose a risk to organisations and give malicious attackers the possibility to gain unauthorised access, steal information or disrupt operations. To avoid negative consequences a procedure needs to be in place on how to find and close the gaps in the information systems developed to serve businesses. The European Parliament and the Council of of the European Union *Directive 2016/1148* state that "Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market [1]."

Different types of vulnerabilities wreak havoc globally and cause chaos and financial losses. Estonian Cyber Security Branch of the Information System Authority (RIA) in their 2022 yearbook [2] noted that the year 2021 will go down in history as the year of security vulnerabilities. As an example RIA brings out an example: "In March last year, when Microsoft disclosed its Exchange server vulnerability and provided information on how to patch it, we notified our partners and other authorities. However, a week later our monitoring revealed that two-thirds of those informed had not yet taken the necessary action [2]."

By NIST definition vulnerability management is ISCM capability that identifies vulnerabilities (CVEs) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network [3]." This definition matches our research definition of VM.

Concern, recommendations and warnings about vulnerabilities can be found throughout different advocates, institutions and non-profit organizations materials. ENISA - European Union Agency for Cybersecurity in their minimum security measures for operators of essential services bring out technical vulnerability management as one component [4]. The

same organisation educates SME-s in their 12-step guide to protect devices by keeping software up to date [5].

Estonian information security standard (E-ITS) [6] outlines an operational security measures such as patch and change management to present measures for applying, managing, and optimising the patch and change management of an organisation, regular updates of IT systems and monitoring information on security vulnerabilities and security updates [7].

The Center for Internet Security, Inc. (CIS®) a community-driven nonprofit, responsible for the CIS Critical Security Controls lists Continuous Vulnerability Management as a critical security control number 7 in the whole set of 18 critical controls [8].

The Open Web Application Security Project (OWASP®) an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted [9] lists using vulnerable and outdated components as a number 6 in their latest top 10 security risks to application security.

Major security incidents like WannaCry [10] and NotPetya [11] ransomware cases are prime examples of global incidents that were enabled by a vulnerability that could be exploited. Some of the most famous include *Log4J* [12], *The Heartbleed Bug* [13], *Apache Struts* [14], *EternalBlue* [15], *Spectre and Meltdown* [16], *DROWN* and the list goes on. New vulnerabilities are discovered daily and then vendors of vulnerable software race with time to create fixes. Patches, bug- and hot-fixes are shared with clients, but the underlying responsibility to be aware of your vulnerabilities and remediating them relies on the capability and willingness of the organizations and is considered a fundamental practice to protect against different type of threats.

1.1 Background

Vulnerability management is one security service offering of a MSSP CYBERS - leading Nordic cybersecurity company, providing end-to-end security solutions to both private and public sector customers [17]. Patching activities and the mitigation portion of the process for organizations in our research is either in-house and handled with respective administrators, or in some cases this service has been outsourced to a IT service provider.

The study aims to analyze vulnerability management processes of 9 organizations to understand success factors that enable successful remediation of vulnerabilities and common obstacles that hinder this process. Our thesis is based on hybrid research combining both qualitative an quantitative data about the subject. Research is conducted on 9 unrelated

organizations who have a vulnerability management process in place and have been conducting the activity for an extended period of time. We have the possibility to view the same process from different perspectives such as the scope of the assets, size of the IT teams, patching tooling used and management perceived support. The organizations are representing distinct industries like healthcare, manufacturing, retail, finance and consultation services and have approached their patch management activities with available resources. By analysing VM scan data which were represented in detail on monthly vulnerability CSV reports and interviews to gauge opinions and experience related questions directly from the people involved in the process will enable us to have a more complete picture and derive interesting material.

1.2 Problem Statement

The continued increase in the vulnerabilities discovered and quick weaponizing of these vulnerabilities by threat actors require organizations to be capable of withstanding this challenge. However news about cyber incidents keep on coming and frequently the incident started because a vulnerability that was not fixed in time.

Vulnerability management requires process, resources and continued effort from numerous stakeholders in the organization, all of which have a role to fill. Unfortunately not all organizations are following this practice on a regular basis and might need guidance on how to start or what to improve in the process.

1.3 Objectives of the Research

Vulnerability management is a process that can help a business to stay secure and reduce the probability of falling victim to a cyber attack. Yet still some organisations still struggle with this cyber security capability. Our research objective is to use hybrid analysis to give us complete information and analyze organizations who have this capability today, what are the success factors that make this process effective. Also what are the obstacles organizations face that hinder progress.

Key objectives of the research:

- How successful are the organizations in their vulnerability management programs?
- Is patch management an enabler for effective vulnerability management for these organizations?
- What are the key learning points that can be used to help organizations that are still

in the process of implementing vulnerability management?

The research would be valuable to organizations who are still for some reasons not performing vulnerability management or are seeking information from others to learn from their experience. Information presented here would be useful to IT service managers, administrators and information security teams to begin or improve their internal practices.

1.4 Novelty

Literature research did not yield results on studies where quantifiable data has been combined with qualitative information on the topic of VM. We saw this as an unique opportunity to observe numerous organizations who were conducting vulnerability management. Measuring their progress with concrete vulnerability data and enrich the context of this data with responsible people's experience, opinions and expertise. The coverage of different industries adds additional dimensions for the research and makes it more valuable to a wider audience. The research could be extended in the future to investigate the detailed vulnerabilities organizations are having difficulties.

1.5 Structure

Introduction outlines the importance of vulnerability management and gives background information what it is and forms our problem statement on research objectives. In literature review we research different materials to create understanding on patch management and vulnerability management by checking different frameworks and best practice guidance's. Methodology part outlines our hybrid analysis and describes the participating organizations, qualitative and quantitative data gathering methods and following analysis. In the results section we give detailed information of our research results. Discussion and conclusion highlight the most important findings and describe our findings for the general audience.

2. Literature Review

Cyber attacks are increasing and the time what organizations have for reaction is decreasing [18]. To combat this threat organizations are implementing vulnerability management to reduce their risks [19]. NIST defines vulnerability management as ISCM capability that identifies vulnerabilities (CVEs) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network [3]."

Vulnerability management is relatively old information security practice. To understand the different aspects of this topic a literature review was conducted. Patch and asset management were also areas of interest due to their connection to the success of effective VM. The following information were searched for literature review: VM best practices, guidance on how VM is conducted in and enterprise environment, studies that have analyzed VM in organizations or in specific context, security frameworks that mandate how VM should be conducted and Estonian government produced materials. Information for the literature review was gathered using different approaches. Literature review structure is presented in a thematic approach, this gives the opportunity to understand the aspects of VM in the best manner.

2.1 Vulnerability Management Related Literature

VM process is conducted and interacted by humans and also the organizational factors play a role [20]. Since our research is looking into the human side as well we find this source to be useful. The study found evidence of these factors playing a significant role for vulnerabilities. One of the interesting findings was the causal connection of latent decisions made by management - for example not submitting funding for a security tooling and this can result in errors at the workplace for example higher workload and time-pressures. Lack of patch application that over time can lead to breach. Study is from 2009, but human behaviour is something that takes time to change so the findings could be relevant today.

Estonian Hospital Cyber Threat Vulnerability: Evaluation of Cyber Security Standards Deployed at Hospitals to Deter Cyber Threats by Michael Anywar [21] thesis objective was to identify and explore cyber security flaws in the security measures and standards already

implemented at Estonian Hospitals. Qualitative study in the form of semi-structured interviews was used as data collection method. The major flaw what was identified was the lack of standards used, limited human resources regarding cyber security skill set. The author highlights that the foreign language used in the interviews could have had a limiting effect on the outcomes and possibility that the answers would have been more accurate when the researcher would have been using local language. These findings are of interest to our research due to the fact of health care sector organizations are in the scope of our work. The language barrier was taken into consideration when we prepared our semi-structured questionnaire and conducted our interviews. Organizations could benefit improving their IT system risk assessments with vulnerability information and apply this to their IT systems [22].

Prioritizing vulnerabilities is one important part of VM. Different approaches and metrics are being used to make the prioritization process more effective. Improving CVSS-based Vulnerability Prioritization and Response With Context Information [23] argues that CVSS scores alone are of limited use for vulnerability prioritization in practice. They investigated what would be the changes in prioritization if context information is also used in CVSS scoring besides relying only on the base metric. By adding the additional information there is a reduction of most critical vulnerabilities and this translates to resource savings in the remediation efforts. However the cost factor in this research was estimated and this is viewed as a limitation on this study. Rieke in Modelling and Analysing Network Security Policies in a Given Vulnerability Setting [24] also recommends to use caution for prioritization solely on CVSS due to their approximate nature of values. Remediation should be based on a combination of underlying asset value and severity of the vulnerability [25]. VULCON uses 2 components for better VM strategy: time-to-vulnerability remediation and total vulnerability exposure [26]. Another possibility is to set priorities is detect functional dependencies between vulnerable assets, other assets, and business processes [27].

Enterprise Vulnerability Management and Its Role in Information Security Management [28] outlines the central role of VM in ensuring enterprise security. *PDCA - Plan Do Check Act* model is proposed for successful management of vulnerabilities. Vulnerability management is a process and, in the ideal case, a culture that continuously identifies vulnerabilities and takes corrective measures to address risks to assets requiring protection. Military organizations have listed five requirements for the efficient vulnerability management procedure: quickness, continuousness, clearness, interdependence, and completeness [29]. The Practical Vulnerability Management a Strategic Approach to Managing Cyber Risk [30] outlines also a basic process for vulnerability management. VM life cycle on a high level can be divided into 4 activities: collect data, analyze data, make recommendations

and implement recommendations. For our research the cycles of vulnerability management are interesting because we could check what are the steps that our subject process follows and in the qualitative part of research observe if some cultural changes have taken place.

Vulnerability scanners play a vital role in the VM process by being the software tools that enable teams to detect vulnerabilities in their systems. SANS institute have outlined the following vendors who offer these solutions [31]. These vendors are: McAfee[1], Qualys, Rapid 7, Tenable Network Security as well as a few open source projects. Note, all the scanning solutions need to be properly configured and tuned to limit the false positives in the scanning results.

2.2 Patch Management Related Literature

The need for an organizational patching policy is well known, as is the fact that the task of patching is rather challenging to most organizations [32]. What kind of policy approach would be appropriate to organisations and what aspects should the IT manager take into consideration were the topic of Optimal Policies for Security Patch Management [33]. The authors first conclude that it would be better to have this policy in written, that states when and how often patches must be applied. For the distribution of updates automated patching where possible is preferred. Since the patch management is a part of successful vulnerability management we are exploring the situation in our work and study how respective organizations handle patch management themselves.

Effective patch management is a systematic and repeatable patch distribution process for closing IT system vulnerabilities in an enterprise [34]. The journal article brings out the necessary components for patch management. Patching is a necessity for security, but can be difficult to manage systematically. To be able to control patch management a system for timely and practical alerts is needed to detect vulnerabilities when they are discovered. Assessment of vulnerabilities is required to evaluate risk of disruption to business to enable the prioritization of remediation. To avoid negative effects of applying patches testing is required. For distributing updates automated tools are an important part of the update cycle that comes with its own benefits and drawbacks. The components outlined here are valuable input to our work and we can investigate how this research subjects handle their own processes. "The patching process can be fully automated, semi-automated or manual, but the degree of automation will depend primarily on the target environment. Automated and semi-automated tools are sometimes free or vendor-specific. For standard Windows desktop operating systems, for instance, Microsoft's free Windows Server Update Services

[1]McAfee has been re branded to Trellix `https://www.trellix.com/en-us/index.html`

tool can manage and automate the patching process. Vendor-specific tools can manage and automate third-party software patches [34]."

2.3 Frameworks and Guidance

ENISA[2] has deceloped Minimum Security Measures for Operators of Essentials Services [4] where Technical Vulnerability Management has been highlighted as a necessary part of security measures. ENISA also has a guidance for SMEs where keeping software patched and up to date is one of the 12 most important steps for protecting a business [5].

Estonian Information Security Standard [7] lists the following key measures relevant for security and our research topic. A Procedure for patch and change management must be established with responsibilities assigned. Automatic updates must be securely configured. IT systems must be regularly updated and IT administrators need to regularly monitor information about known vulnerabilities and when they are know they need to be fixed at the earliest opportunity.

NIST Special Publication NIST SP 800-40r4 Guide to Enterprise Patch Management Planning [35] outlines the recommendations for patch and vulnerability management. One interesting thought from this literature is about perception that needs to change that an operational disruption caused by patching is harm that the organization is doing to itself, while an operational disruption caused by a cyber security incident is harm caused by a third party. While those may be true statements in isolation, they are misleading and incomplete as part of an organization's risk responses. Disruptions from patching are largely controllable, while disruptions from incidents are largely uncontrollable. Disruptions from patching are also a necessary part of maintaining nearly all types of technology in order to avoid larger disruptions from incidents.

CIS Center for Internet Security community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data recommended 18 CIS Critical Security Controls [36] outline continuous vulnerability management as a critical control number 7. Organisations are instructed to develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information [37].

[2]European Union Agency for Cybersecurity `https://www.enisa.europa.eu/`

2.4 Literature Review Conclusion

The material and work researched in this chapter will help us to understand the different aspects of vulnerability management process, obstacles and gaps. The prioritization of vulnerabilities and effectively remediating them is area of interest and we can compare the existing research to our results from the vulnerability data analysis. In addition understanding of patch management process enables us to ask more relevant questions from our research subjects. Our work could be considered in some sense as extension of the Hospital research [21], but with a more wider scope and as empirical research.

The current literature is lacking a practical overview of the vulnerability management programs experience in different organizations and an internal overview of how well are organizations managing this security control. Knowing the common issues and obstacles would help others in better planning and improve their own processes.

3. Methodology

Vulnerability management involves different activities and stakeholders, each having a role to fulfill. To create comprehensive understanding how successful organizations have been in their vulnerability management programs an hybrid research method was selected. There were two main parts for the research. First, quantitative research focused on gathering and analyzing historical vulnerability scan results data (scan data is output of the vulnerability detection software). Second qualitative part focused on analysing each organization experience from the process via semi-structured interviews. The methods complement and reinforce each other. Results of the first data analysis gives more effectiveness for the interviews.

3.1 Participating Organizations

To compose a selection of organizations we reached out to a number of participants who have been running a vulnerability management program. For all the vulnerability management program was created by MSSP. We reached out to 9 different organisations with the a proposal to participate in our study and got acceptance for each one of them. Representation of organizations cover different industries ranging from SMB-s to Enterprises, have varying availability of resources, manage their infrastructure in individual ways and have varying amount of assets to protect, details are brought out in Table 2. In our work we have given each organization a unique identifier which consist of letter *"C"* and a number. We assess that this amount of organizations considering their different nature is sufficient for our research.

3.2 Data Analysis

Vulnerability scan data for each organization was collected. Results from monthly scan results were gathered in the form of CSV-s. Giving us an overview of all vulnerabilities the underlying assets faced from the start of respective programs that are outlined in the Table 2 until April 2022. Scan data is gathered with Tenable Nessus Professional software [38]. As information about new vulnerabilities is discovered and released into the general public domain, Tenable Research designs programs to detect them. These programs are named plugins. The plugins contain vulnerability information, a simplified set of remediation

actions and the algorithm to test for the presence of the security issue [39]. Each plugin, a vulnerability check provides additional information some of the most interesting ones for our research are listed in Table 1 with explanations.

Capability	Explanation
plugin id	Unique identifier for the vulnerability detection program
plugin name	Name of the vulnerability that is being checked
risk	Severity Rating based on CVSSv3 score
ip address	IP Address of the affected host
port	Port on which the vulnerability is detected
fqdn	Fully Qualified Domain Name
os	Operation System
plugin text	Description of the vulnerability discovered
synopsis	Brief summary about the vulnerability
description	Longer description about the vulnerability
solution	Information of action needed for remediation
see also	Additional information sources
cve	Identifier in the Common Vulnerabilities and Exposures Catalogue
patch publication date	Date when a patch for this vulnerability was released
vuln publication date	Date when vulnerability was made public
in the news?	Has the vulnerability been discussed in the news
exploit availability and framework	Information about publicly know exploits
exploit ease	Rating of the complexity of the exploitation
exploited by malware?	Is the vulnerability being used by malware
cvss scoring info	Covering CVSSv2 and v3
plugin publication and modification date	When a program was developed and modified
scan start and end times	When a scan was run
VPR	Vulnerability Priority Rating combines Severity and Threat Intelligence to improve prioritization

Table 1. Tenable Nessus Professional Scan Data Components.

3.3 Interviews

Semi-structured interviews were conducted using Microsoft Teams platform for an online meeting. Questions were divided into 4 domains: operational, patch management, vulnerability management and open discussion. This approach helps us to see the enablers and obstacles of the whole process from the organization involved personnel experience. The quantitative scan data analysis was also shown to the participants to validate our findings. Details of the questions asked are show in Appendix 2. Participants were se-

lected based on their involvement in the vulnerability management and patch management activities, details about the interviewed persons is listed in Table 5. The main goal was to interview both roles, the administrative position and possibly managerial position. In some organisations both roles are represented in one person. All other cases we managed to invite all the respective positions to the meeting. We also opted for not sending the questionnaire up front to gather the most authentic answers of the current situation and since for some organizations there where multiple participants in the same interview it would be interesting to see what are their immediate answers. During the interview the screen to questionnaire was shared and notes were taken about participants answers that were visible for parties during the course of the meeting.

3.4 Ethics

Vulnerability data about an organization is sensitive information that in the wrong hands can cause damage. Also MSSP-s have written NDA-s not to disclose organization information without prior agreement. Consent for the organisations to participate in this study was asked. To further protect the participants following precautions where implemented. The data is anonymous, participating organization names are not made public. The same principles apply for the interviews, participants are described only by the positions they hold in the organization and the interviews are not recorded. After the completion of the research all notes, vulnerability scan data and respective analysis will be securely deleted.

4. Results

To understand fully how an organization is handling its vulnerability management practices we need an empirical approach due to the fact that VM is a process which success depends on tooling and co-operation of many stakeholders. Quantitative data in Section 4.4 enables us to measure how well have the vulnerabilities been remediated. This information is necessary to spot trends and tendencies in the remediation. To learn how organizations have approached vulnerability management and understand what are the human aspects of this process we use qualitative data in Section 4.5 that gives us insight of the interactions between stakeholders. We have gathered information via semi-structured interviews. Quantitative data gives us information how well has an organization been able to remediate their known vulnerabilities and qualitative data helps us to understand the reasons behind the results.

4.1 Overview of the Vulnerability Management Process

The vulnerability management process is similar for all the participant organizations since process is built by the same MSSP. Necessary characteristics are brought out in Section 4.3 Differences are the following:

- Stakeholders - if the patching responsibility relies on another provider the process is signed between all stakeholders: organization, IT Service provider, VM Service provider
- KPI's - organizations have set themselves different goals (e.g remediation of Critical severity vulnerabilities in 7 calendar days.)
- Scheduled scanning and patching times

The VM process created by the MSSP that the organizations follow has three major phases that can be seen in Figure 4.1. The first phase lays out the base for process, second is focused on the detection of vulnerabilities and the last is about prioritization, remediation and mitigation efforts.

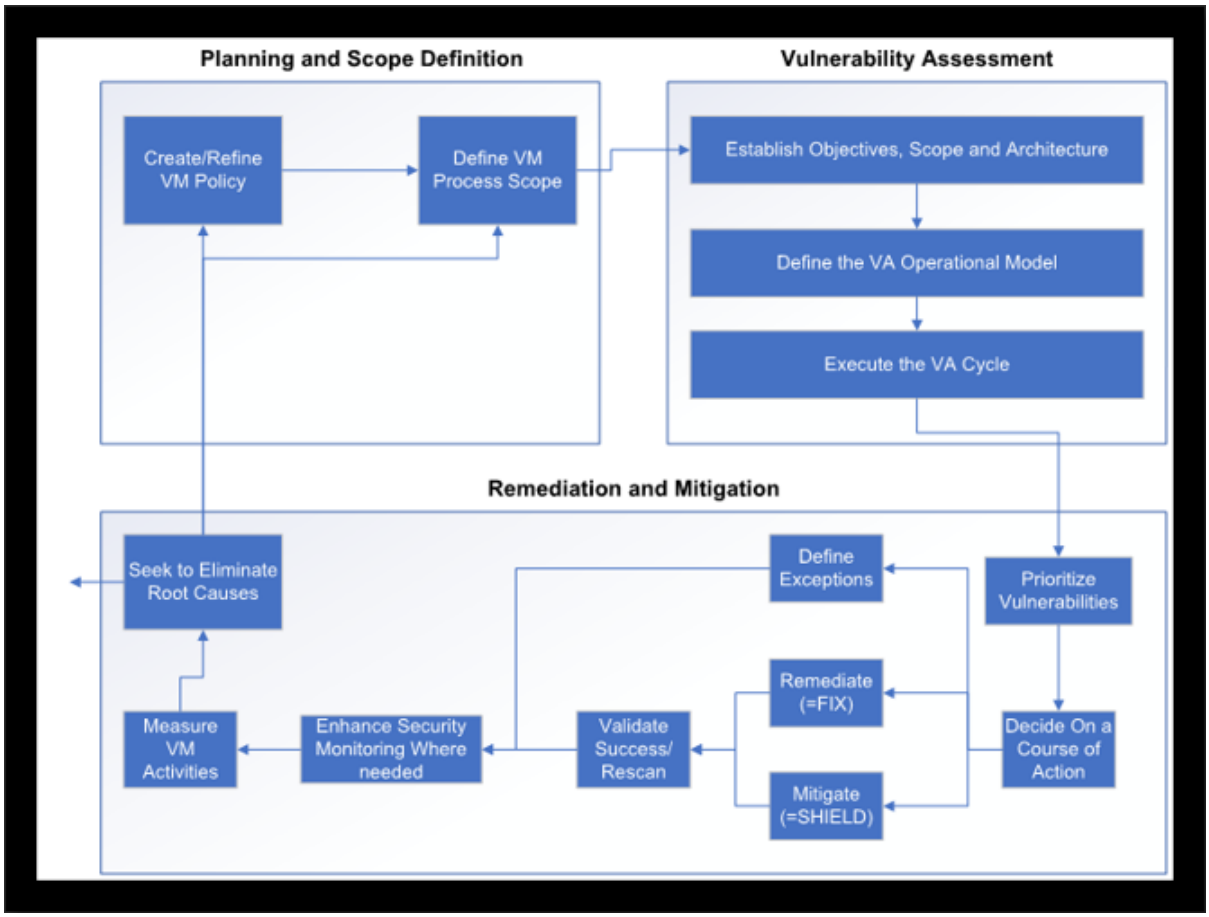

Figure 1. VM Process for Participant Organizations

We can see that the process have three distinct phases:

- Planning and Scope Definition
- Vulnerability Assessment, also known as Vulnerability Scan
- Remediation and Mitigation

Phase - Planning and Scope Definition

This phase is responsible of outlining the policy of the whole process. Points like scope, KPI-s, regularity, scan approach and how special cases for example discovery of EoL (End of Life) systems are treated outside of VM and in the scope of organization risk management.

Phase - Vulnerability Assessment

This phase is about the activity of scanning. The individual month scan target lists are updated, some assets might have been decommissioned and new might have been added. Scanner node requirements are also defined here, outlining what technical resources are

necessary such as scanner node virtual server, license, firewall accesses and scanning credentials. The operational model is defined via RACI model (acronym RACI stands for responsible, accountable, consulted, and informed) outlining individuals responsible for updating information and vulnerability plugins [39], schedule the scan to be run, verification if the scan was successful, creation of report and prioritize findings. Execution of the scan is agreed and defined and shared with participants.

Phase - Remediation and Mitigation

Most important phase in the process is remediation and mitigation. Assessment responsible person will be prioritizing the vulnerabilities taking into account severity ratings, their expertise and current situation demands. Customer in this case can highlight business needs and requirements and IT service provider will be responsible responding and fixing the findings. Not all vulnerabilities found can be or should be fixed immediately. But the ones what are deemed necessary will have to. If remediation is not possible, then the second choice is mitigation (shielding an asset).

Validation of remediation will be done by the next month scan in our participant organizations. In a situation where fix or shield are impossible an exception is made. This means business risk acceptance by the organization. Improving security monitoring can be an additional control. For situations where some vulnerability re-appears a root cause analysis needs to be performed.

4.2 Scanning Software

For vulnerability assessment (scanning) activity a tool is used. In our study the selected scanning software was Tenable Nessus Professional [38].

Tenable severity ratings [40] are used to communicate the seriousness of the finding and it is tied directly to CVSS - "The Common Vulnerability Scoring System is an open framework for communicating the characteristics and severity of software vulnerabilities [41]."

VPR - Vulnerability Priority Rating is a dynamic score to reflect the current threat landscape. [40] This gives additional context for the vulnerabilities and helps better to prioritize the vulnerabilities. In addition to CVSSv3 score exploit code maturity, product coverage, threat sources, intensity and recency is taken into account.

The most common security problem in an organization is that security patches are not

applied in a timely manner. A Nessus credentialed scan can quickly determine which systems are out of date on patch installation [42]. This is why credentialed scan also sometimes referred as authenticated scan is used. The opposite unauthenticated scan can also determine vulnerabilities, but relies on finding them on external network services and is not capable checking system services and configuration settings.

4.3 Characterization of the Participants

Participated organizations are characterized in the below Table 2. First column is the unique identifier. The industry where these organizations operate, average number of assets in the vulnerability management scope. The patching responsibility, is it in house or delegated to third party, and the asset categorization in the scope of VM. Also when was the start of their VM process. For clarification the VM process sign off date might not match with scan data start dates due to initial testing being conducted, that can be limited in the results. None of the participants had a documented vulnerability management in place or it was performed ad-hoc.

Identifier	Industry	No. of assets (Avg)	Patching	Scope of VM	VM start
C1	Manufacturing	180	third party	servers	2020 05
C2	Retail	170	in-house	servers	2020 10
C3	Healthcare	30	in-house	servers	2020 10
C4.1	Healthcare	136	in-house	servers	2020 10
C4.2	Healthcare	31	in-house	servers	2020 11
C5	Retail	61	in-house	servers	2020 12
C6	Manufacturing	44	in-house	servers	2021 10
C7	Healthcare	441	third-party	servers+workstations	2022 01
C8	Financial	350	in-house	servers	2022 02
C9	Consultation	22	in-house	servers	2021 07

Table 2. Overview of Participated Organizations.

The organizations in the scope operate in different industries with varying degree of assets to manage. Patching responsibility is primarily managed in house with few exceptions who are buying this service from third party. The scope of the VM is dominated on the servers, with an exception of C7 that has taken all workstations also into scope. 5 out of 9 organizations have been conducting the activities of VM more than 12 months from which longest has been 23 months and 4 out of 9 organizations less that 12 months from which the shortest has been 3 months.

To measure the vulnerability management process success organizations have established internal KPI-s to achieve. Table 3 outlines the ones used by our participants. For the sake

of anonymity we are not going to tie these directly to any of them.

Number	KPI
1	CVSS >= 9.0 + public exploit available remediate in 7 calendar days
2	Critical, High + public exploit remediate in 30 calendar days
3	CVSS >= 9.0 + public exploit remediate in 10 calendar days
4	VPR >= 7.0 remediate in no longer than 30 calendar days.
5	VPR >= 9.0 remediate in no longer than 7 calendar days.

Table 3. Overview of KPI-s Used by Organizations.

Patch management is connected to vulnerability management via the remediation phase. Organizations have different approaches working with that process. In the Table 4 we see details about each organization practices.

Identifier	Patching approach	Patching Employees	Tech used	Operating system
C1	automated	1	Datto RMM	Windows Server
C2	semi-automated	2	WSUS	Windows Server
C3	semi-automated	2	WSUS; Ansible;	Windows Server; Linux
C4.1	semi-automated	5	N/A	Windows Servers
C4.2	semi-automated	5	N/A	Windows Servers
C5	semi-automated	1	SCCM	Windows Server
C6	semi-automated	1.5	SCCM	Windows Server
C7	semi-automated	N/A	Datto RMM	Windows; Windows Server
C8	automated	1	Katello	Linux
C9	manual	3	SSH	Windows Server; Linux

Table 4. Overview of Patch Management Approach.

4.4 Observed Trends in Vulnerability Scan Data

We have detailed vulnerability scan data from each organization. Below is the most notable findings from analysis worth mentioning.

To put the scales into perspective Figure 2 gives an overview of how many assets each organization has had on average in their VM scope.

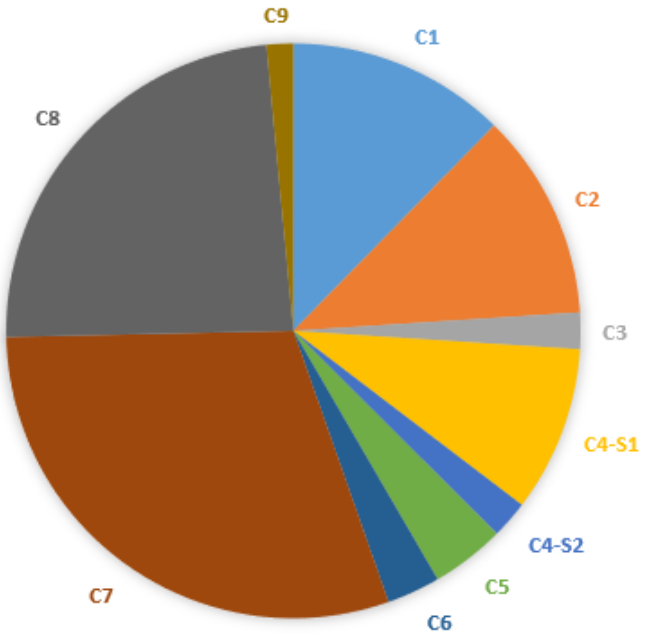

Figure 2. Scan Scope by Asset Count for Organizations

In the following sections we will be demonstrating different graphs of vulnerability findings for each individual organization. Important to note here if we are counting unique vulnerabilities found for the whole of one organization, the Y-axis is demonstrating the count of these vulnerabilities. For example if the count is 50 then this means this organization has 50 different unique vulnerabilities.

When we are exploring how many servers are affected by vulnerabilities we are summarizing the discovered unique vulnerabilities on each server together. Meaning for example if the organization had 50 servers and each one of those were effected by 10 vulnerabilities we get the affected host number of 500. Intuitively it is confusing how can this be since the organization only had 50 servers, but we would want to see trends of reduction for the assets affected and this enables us to do this.

Scope is used in the graphs to show the change over time in the number of assets being scanned. This can be thought of as target list that are in the scope of vulnerability scanning. If the scope shows number 50 this means 50 servers were scanned. We sometimes refer to average scope, this is calculated by taking each month server count and divided by the number of month's the scans have been conducted.

4.4.1 C1 Progress

Figure 3 shows the trends of vulnerabilities detected with following severity indicators: high, critical, CVSS score >=9.0 that have a publicly known exploit available and also vulnerabilities that have a VPR score assigned, meaning they have been seen being exploited in the wild by threat intelligence. In blue we also bring out the new vulnerabilities found for the scope of these assets. The high peak in September 2020 is caused probably by the fact that previous month 125 assets were scanned versus 155 in the peak month. Overall trend shows us that C1 has been capable of reducing vulnerabilities steadily, in April 2021 we can see that the the mitigation trends synchronize with new known vulnerabilities being discovered in the world.

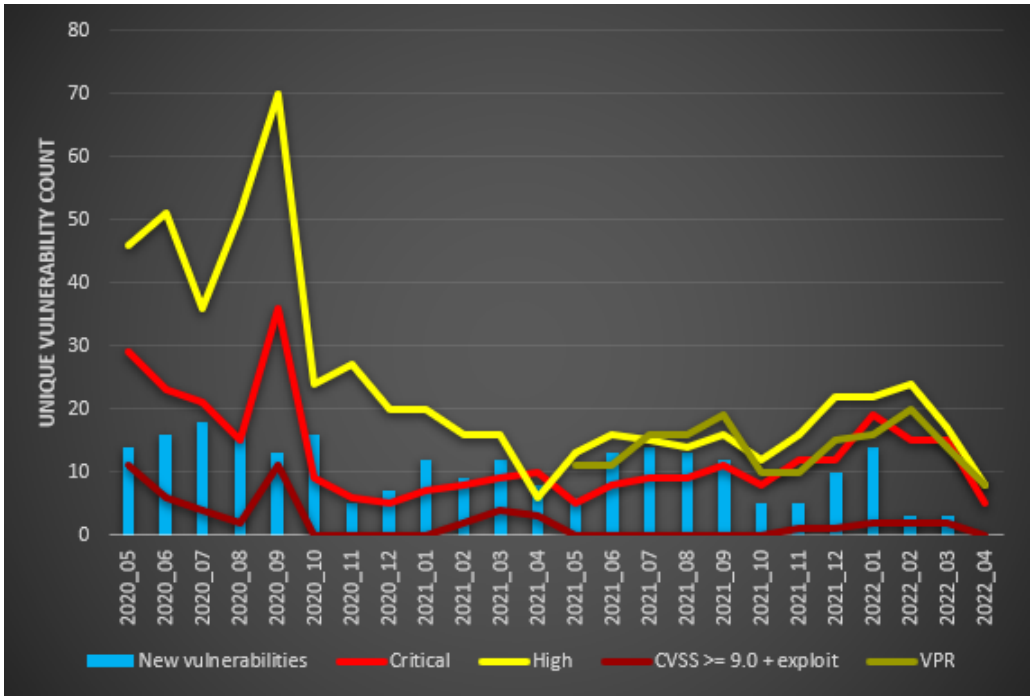

Figure 3. Unique Vulnerabilities Discovered for C1 Over Time

During the interview C1 patching team representative told that they have also focused on fixing high and medium severity vulnerabilities. Figure 4 shows that progress. At the beginning of the process the servers held 90 unique vulnerabilities and the combined sum of affected servers was 2609 in May 2020, meaning that on average during that time each server had approximately 15 different medium severity vulnerabilities. When we compare this to the April 2022 scan results we see that the unique vulnerabilities number has decreased to 31 and total sum of affected servers is 303. This is 65.6% decrease on unique vulnerabilities count and 88.4% decrease in the affected servers.

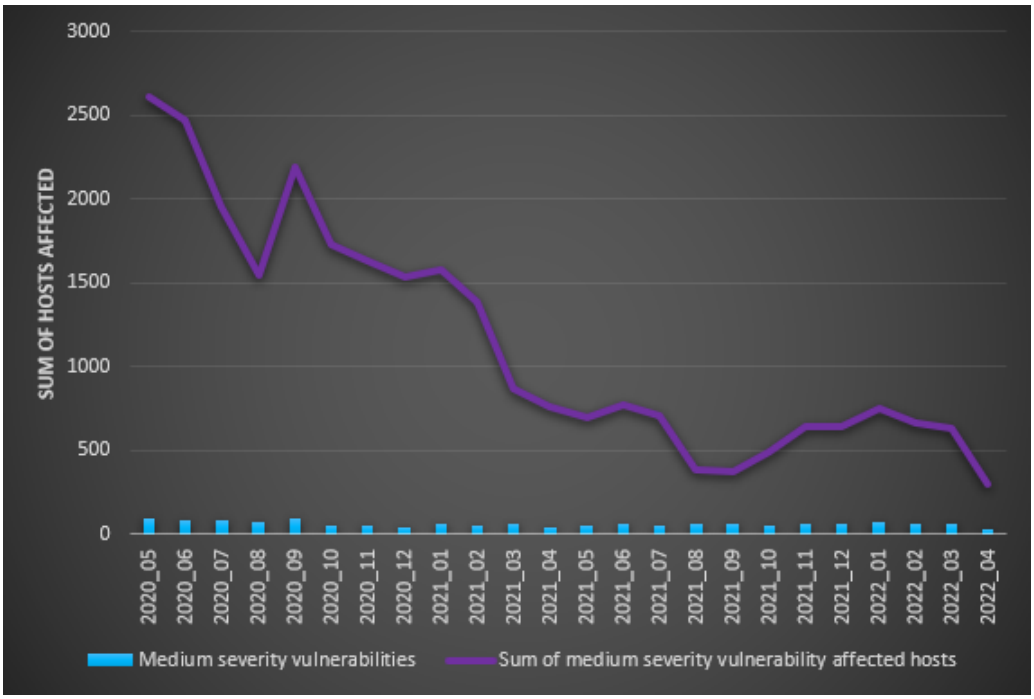

Figure 4. C1 Medium Severity Vulnerability Mitigation Trend

To highlight the overall patching effectiveness we can review data about affected servers in Figure 5. We see a high spike in January 2022, this was caused by Apache Log4J vulnerability. The September 2020 spike was caused by an issue with patch deployment. January 2021 saw an increase in the scope by adding additional 10 servers to the scope of scans which also caused a spike since they were older servers.

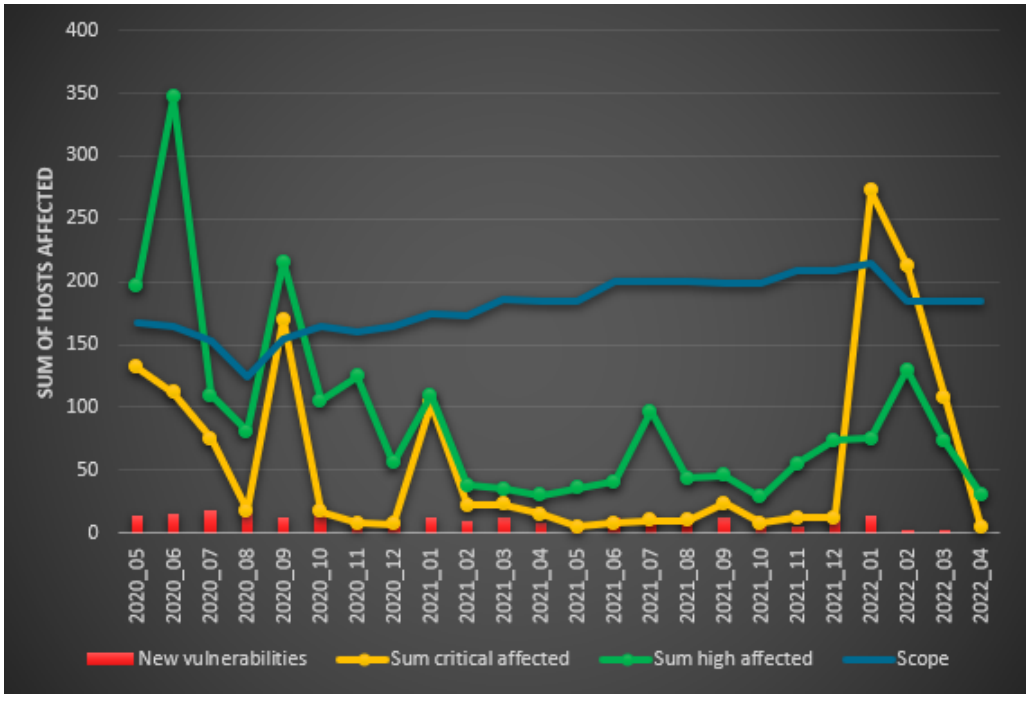

Figure 5. C1 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.2 C2 Progress

C2 has had success on their remediation efforts which can be seen on Figure 6. Most significant is that after 4 months of starting the process the organization was able to reduce amount of unique critical vulnerabilities to 1 and high's to 3. However after this we see that vulnerabilities have been increasing. Reasons for this primarily is the patching responsible people availability and additional servers being deployed. If we look at the fixing of CVSS score 9.0 which also have publicly know exploit available it was achieved during 8 out of 19 months. The months that this indicator was not met there was minimum 1 unique vulnerability to maximum of 4.

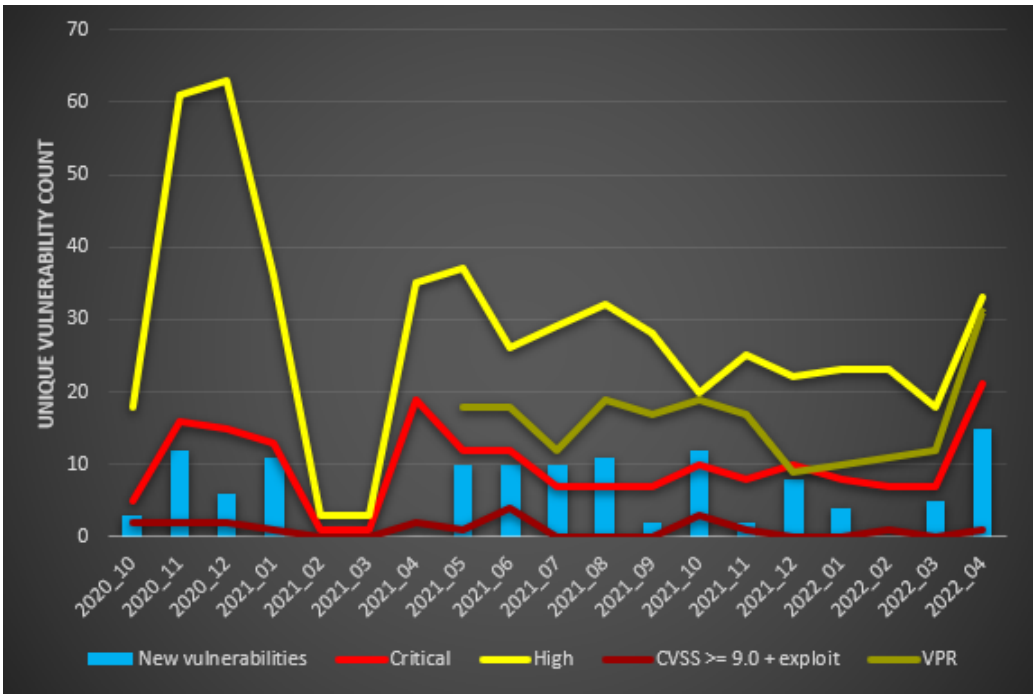

Figure 6. Unique Vulnerabilities Discovered for C2 Over Time

C1 and C2 have similar amount of servers with the same operating systems as described in Table 4. While C1 is using automated tooling and C2 describes their approach as semi-automated and also noted issues with chasing stakeholders to mitigate vulnerabilities. Figure 5 and Figure 7 show that for C2 the sum of affected servers is close or over the scope line that shows how many servers were scanned, while C1 critical and high affected servers is steadily well below the scope line. This means C2 has more vulnerabilities per server as their similar counterpart. Possibly indication that C1 patching approach is better compared to C2's practices. Also the amount of people doing the patching is lower for C1 showing higher effectiveness per employee.

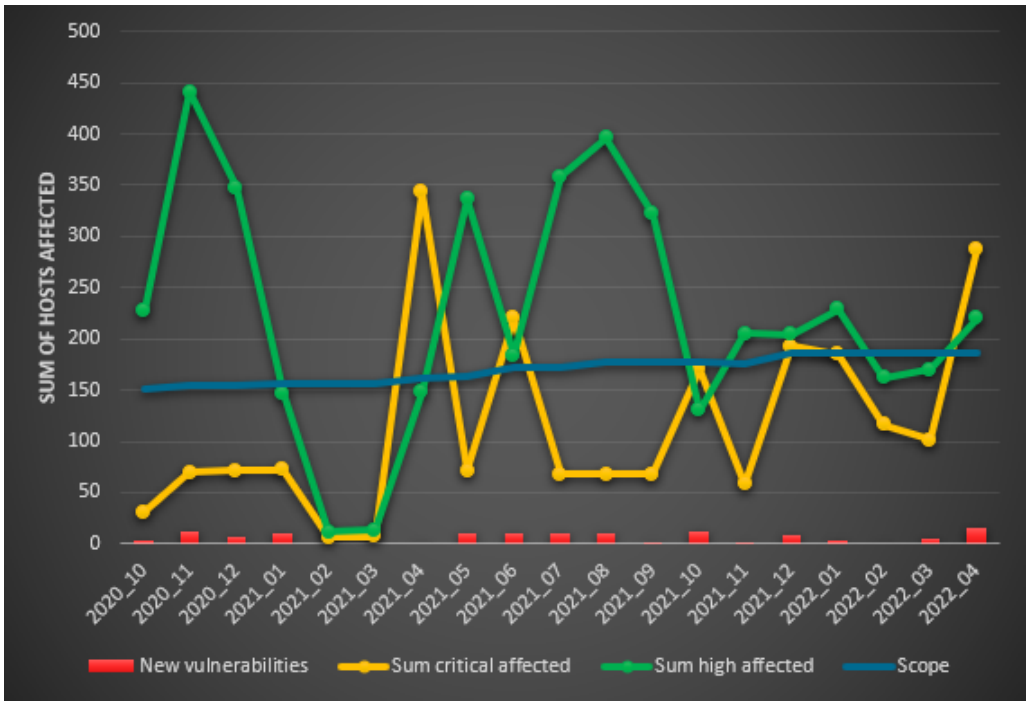

Figure 7. C2 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.3 C3 Progress

Figure 8 shows C3's most important vulnerabilities mitigation trend over time. We can see a steady decline on the mitigation side. For the peaking of vulnerabilities in the beginning of the process detected correlates to the solving of issues of scan failures (represented by the purple line) on some servers adding the previously not visible vulnerabilities with a spike in high severity vulnerabilities in February 2021.

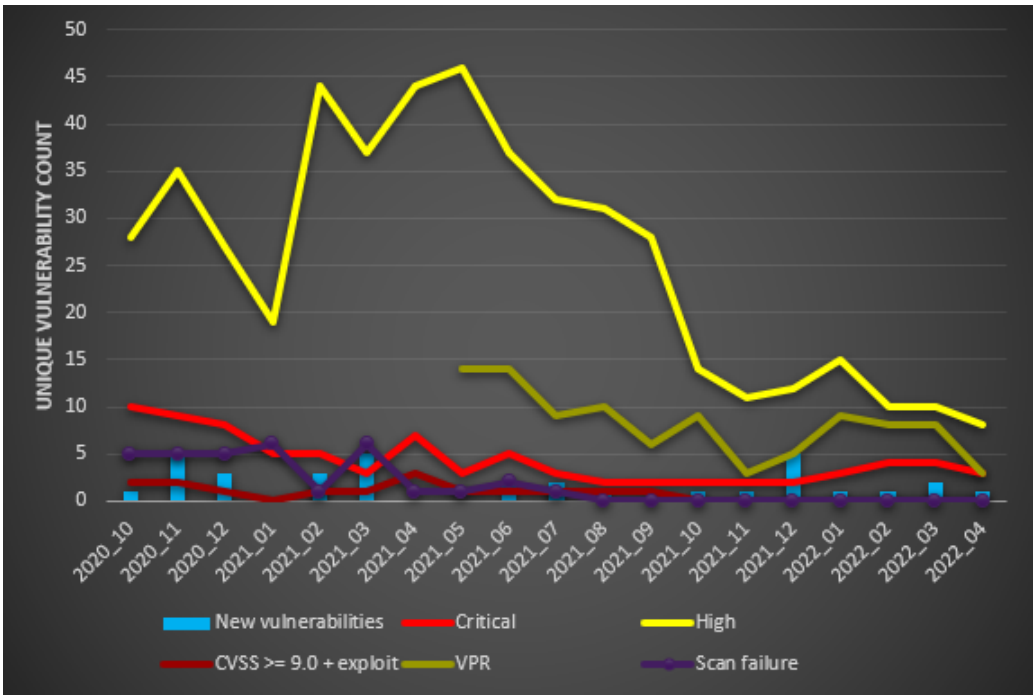

Figure 8. Unique Vulnerabilities Discovered with Scan Failures for C3 Over Time

Comparing Figure 5 to Figure 7 and Figure 9 we note that C3 has been capable of keeping the affected hosts by critical vulnerabilities well below the scope line and over time brought the high severity's findings close to the level of servers in the scope of scans. Meaning that there is 1 high severity vulnerability per server on average. Peak in the hosts affected by critical severity is due to Log4J vulnerability. However the amount of servers C3 needs to maintain is 5.7 times lower comparing to C2. The semi-automated approach that the organization follows indicated in Table 4 can be an option if the amount of assets needed to be maintained by one person is low.

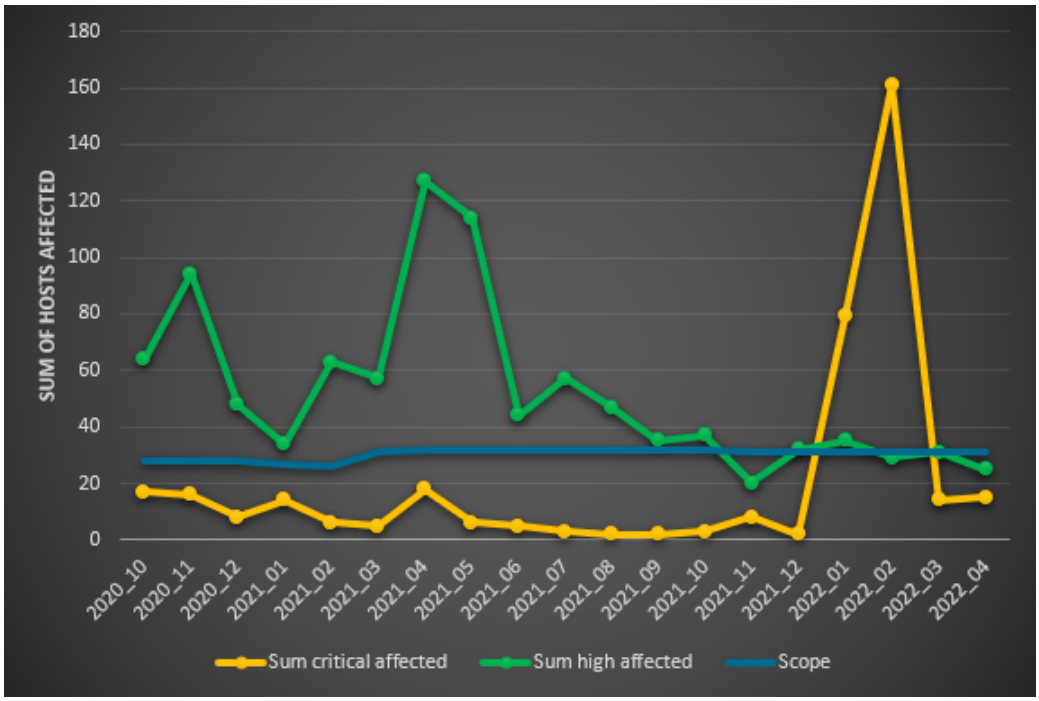

Figure 9. C3 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.4 C4 Progress

In organization C4 there are two departments responsible for their own servers noted in our figures as S1 and S2. We can observer two spikes in the new vulnerabilities discovered (February 2021, March 2022), both of the times the majority of the new vulnerabilities was monthly Windows Server Security updates and since the vulnerability scan was close to Microsoft Patch Tuesday the patches have not been applied yet. Patching procedure for S2 is every two months and sometimes the updates are not possible to do due to the nature of devices. While S1 has seen a steady decline of all severity categories of vulnerabilities show in Figure 10 we see that S2's progress in Figure 11 has stalled and even sees an increase in the vulnerabilities. The amount of servers these departments are responsible for on average for S1 is 137 and S2 is 31. This means that patching every two months even with 4.4 times less servers and skipping patching times makes the remediation progress worse.

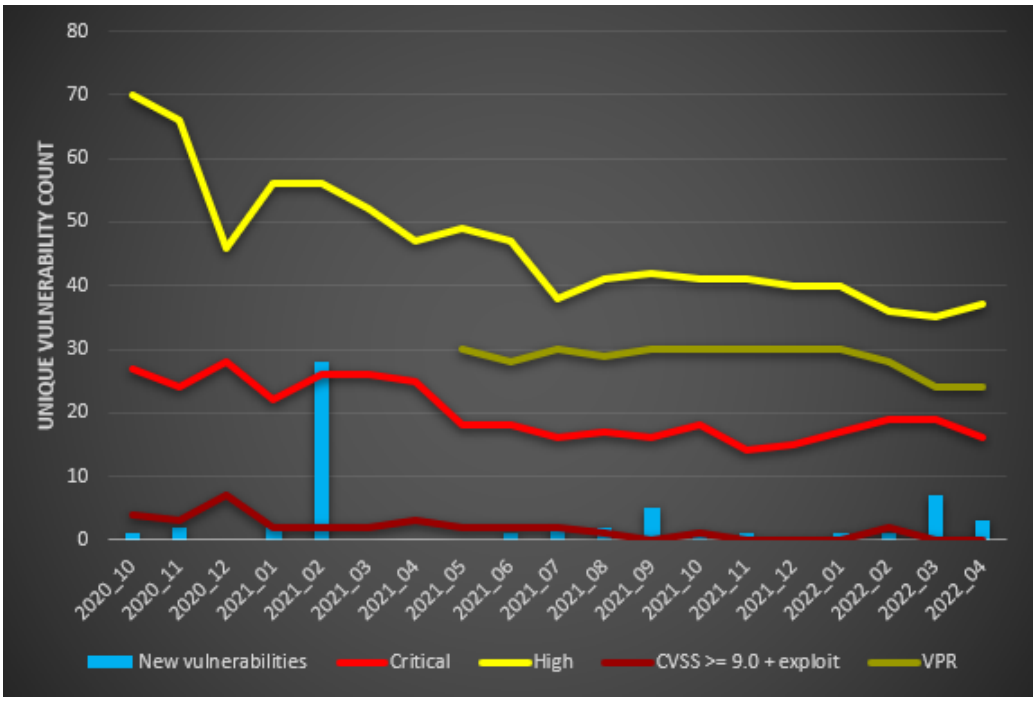

Figure 10. Unique Vulnerabilities Discovered for C4-S1 Over Time

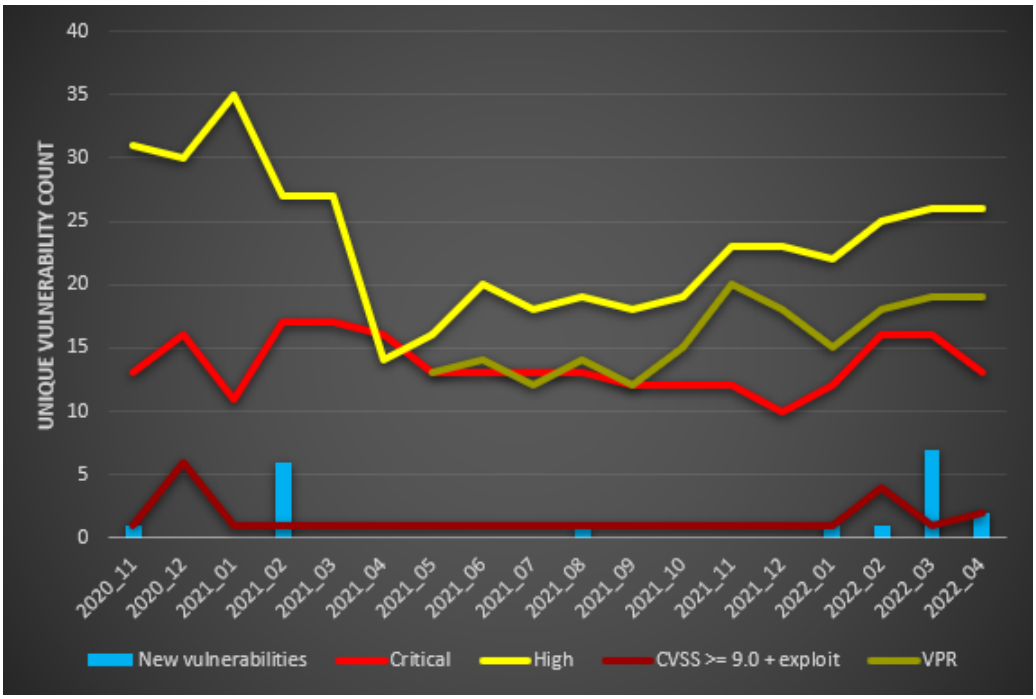

Figure 11. Unique Vulnerabilities Discovered for C4-S2 Over Time

4.4.5 C5 Progress

C5 has no written vulnerability management process in place and the organization has not chosen KPI-s to commit to in this process. However responsible parties for patch and

vulnerability management meet regularly to check the scan results. In Figure 12 we can see that the trend of vulnerabilities has been moving sideways with a slight increase at the latest months.

Figure 13 shows servers that are affected by vulnerabilities to be below the 1/3 mark of the overall scope of assets being scanned each month. Possibly meaning that the centrally managed tool has made improvements to the patching process and helps to keep vulnerabilities in control.

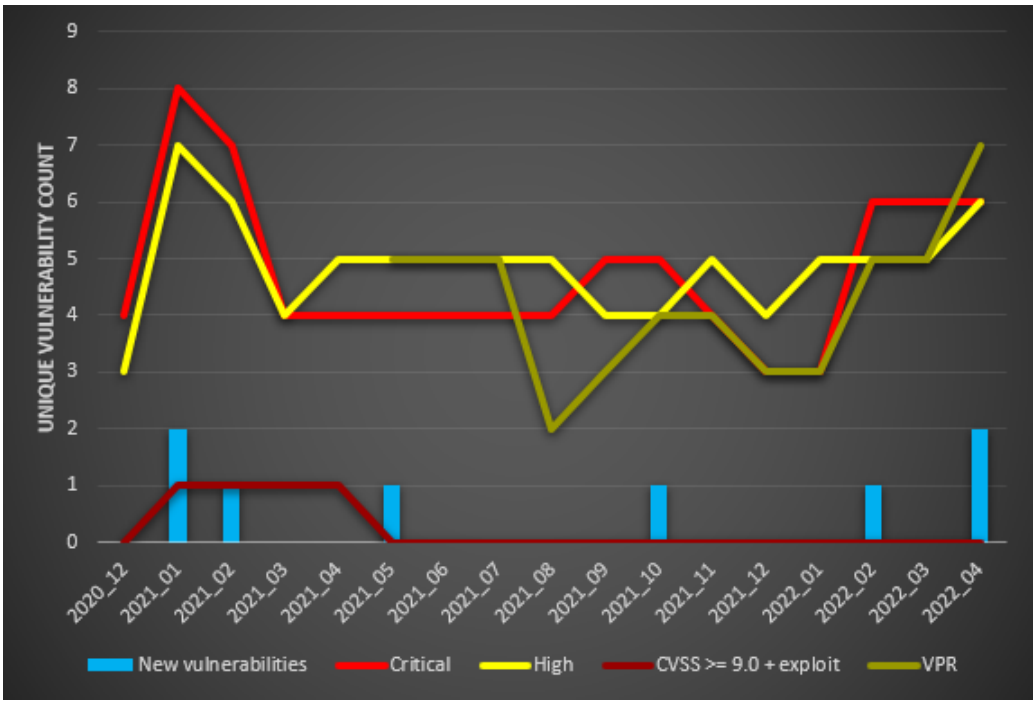

Figure 12. Unique Vulnerabilities Discovered for C5 Over Time

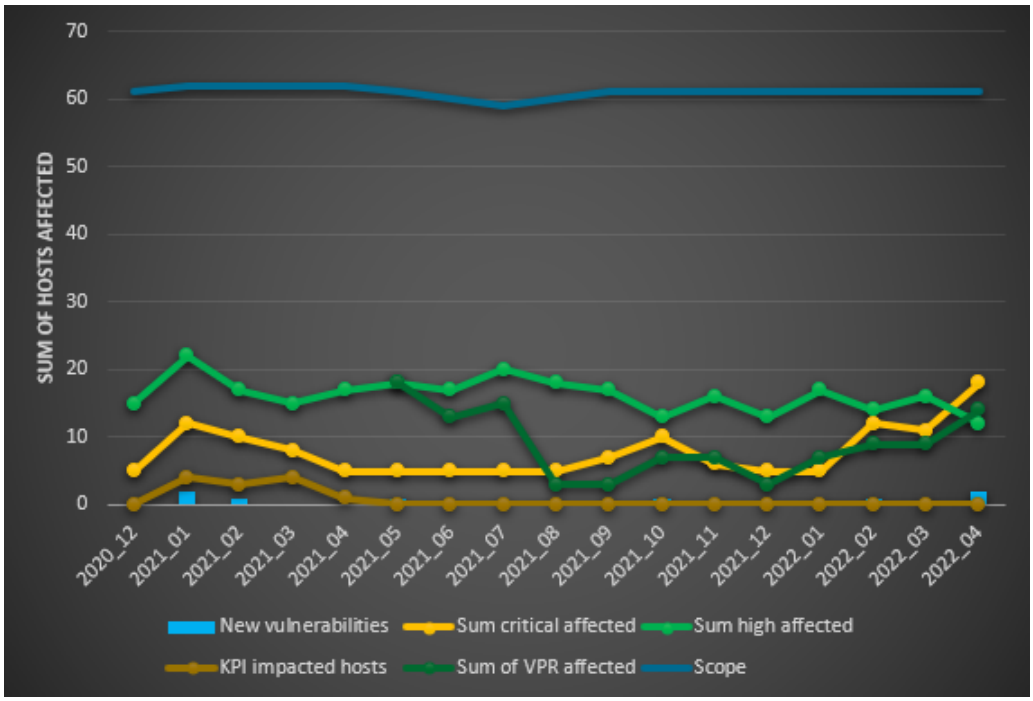

Figure 13. C5 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.6 C6 Progress

Figure 14 C6 has been conducting vulnerability management process for 6 months at the time of the research. We can see a progress of remediating vulnerabilities despite the addition of new ones each month.

When we take into observation vulnerabilities with a VPR rating for this organization we see in Figure 15 that the sum of servers that have a vulnerability with a VPR rating has been reduced 4.5 times when comparing October 2021 to March 2022. Since the organization also has experienced a security incident in the beginning of Q3 that could be a contributing factor to the remediation efforts.

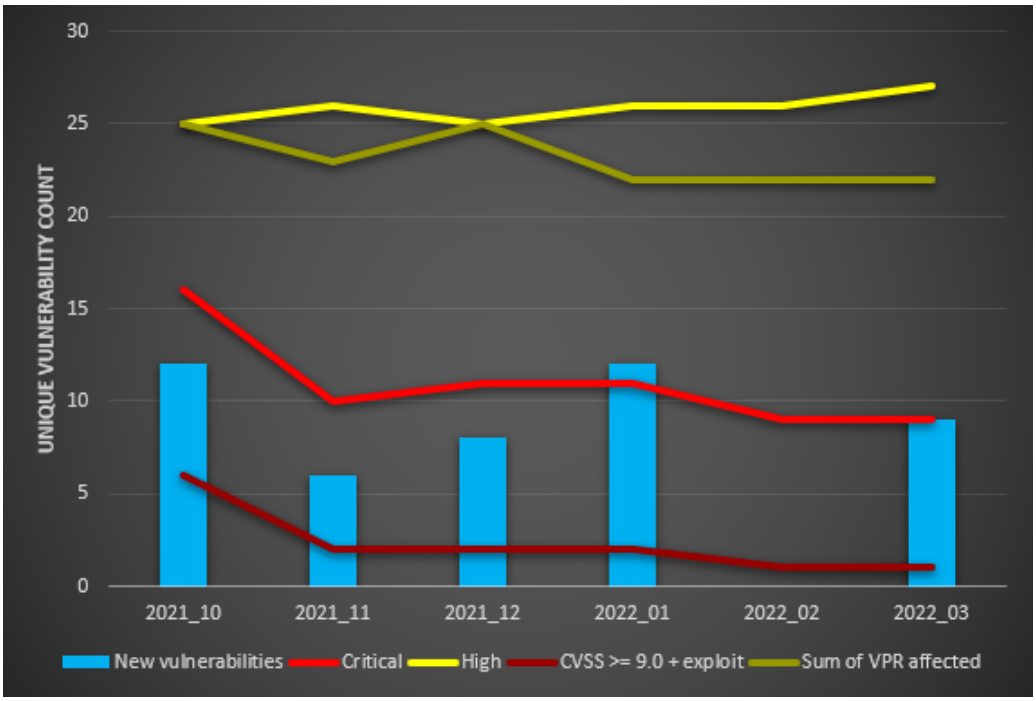

Figure 14. Unique Vulnerabilities Discovered for C6 Over Time

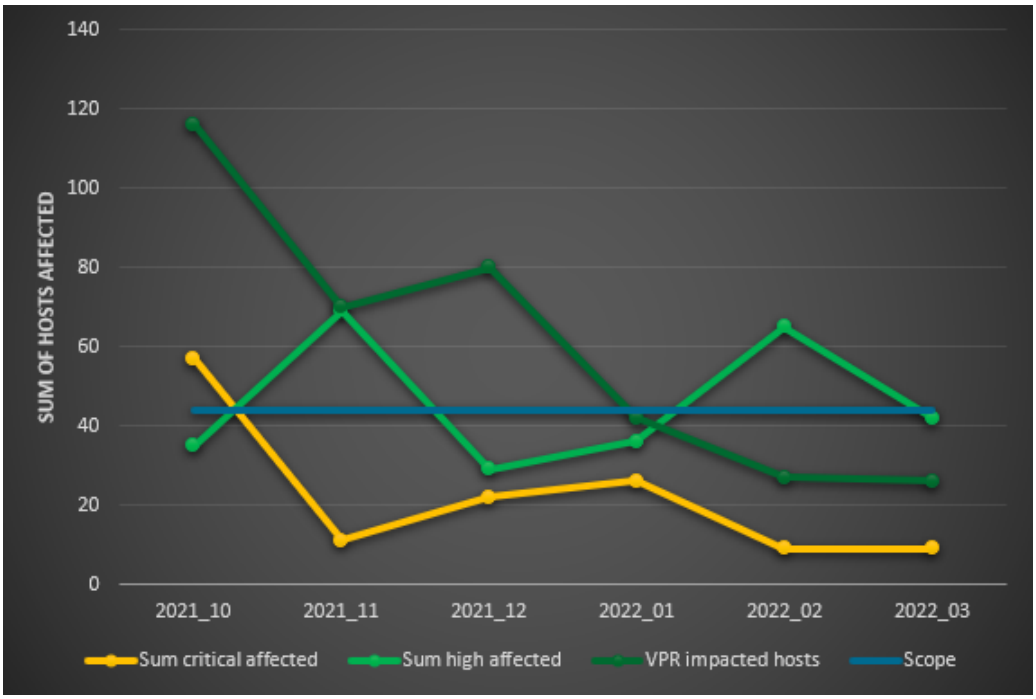

Figure 15. C6 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.7 C7 Progress

C7 is an interesting participant since the scanning scope is the highest of the participants with an average of 441 assets (Figure 2). Please note the VM process has only been running

from January 2021. In addition to servers all workstations are being scanned as-well. In Figure 16 we see that in April 2022 many vulnerabilities were detected. This is due to the fact that three previous months were scanned using the unauthenticated scan method, which was changed to authenticated method. We consider this as significant proof to the need of authenticated scans for Windows based environments.

Based on current data it is difficult to draw conclusions on vulnerability management effectiveness, however in Figure 17 we can see that compared to the overall scope of assets the sum of vulnerable assets for all severity categories (Critical, High, VPR) is under 15%. The patching responsibility for this organization had been fully outsourced.

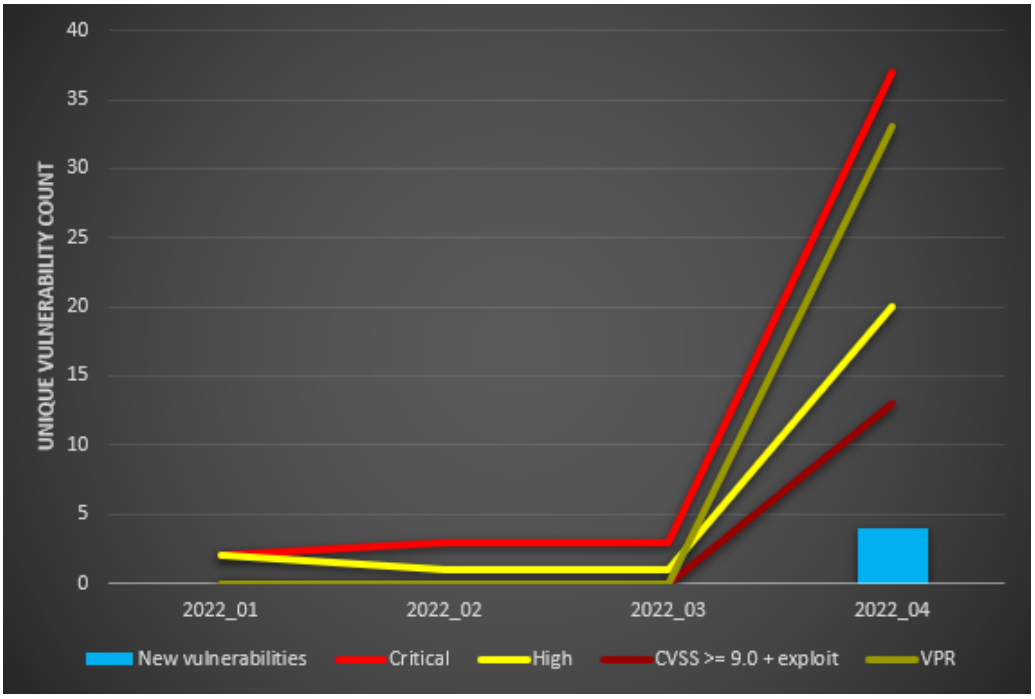

Figure 16. Unique Vulnerabilities Discovered for C7 Over Time

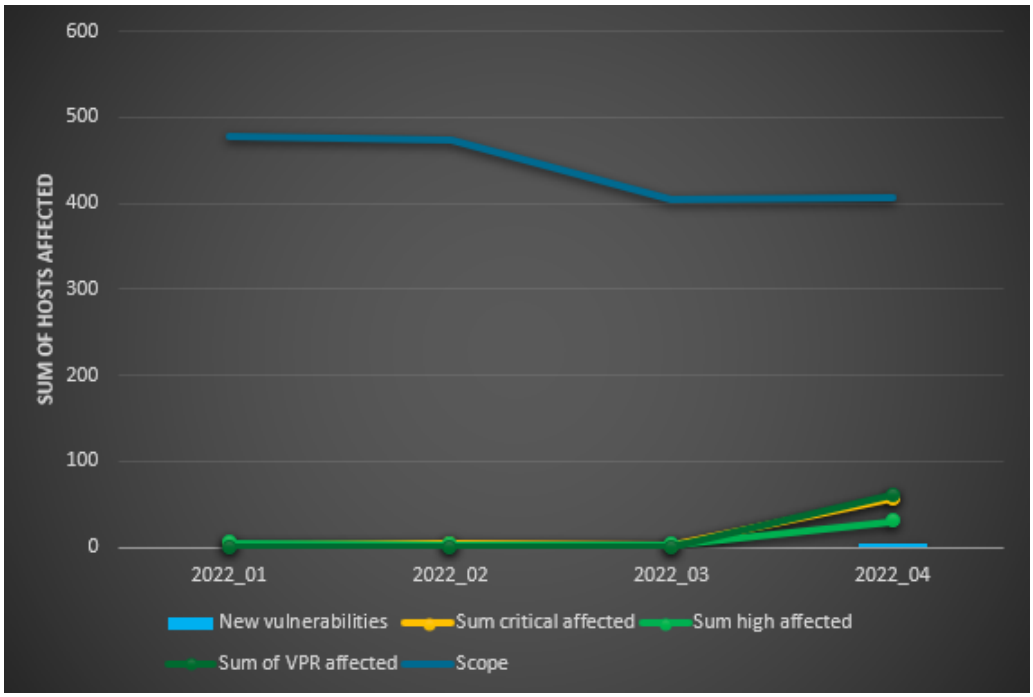

Figure 17. C7 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.8 C8 Progress

C8 has the second largest asset scope (Table 2), considering unique vulnerabilities discovered in Figure 18 is very low it could mean two things. Either C8 patch management is highly effective, this can be a result of the automation. Or the unauthenticated scans are not detecting all the vulnerabilities similar to C7. In the interview 4.5.1 the C8 representative told that the scans have not been producing false positives and the high amount of medium vulnerabilities in Figure 19 are cipher suite related. Unfortunately we do not have data of authenticated scans in the time of writing to answer conclusively what the situation is.

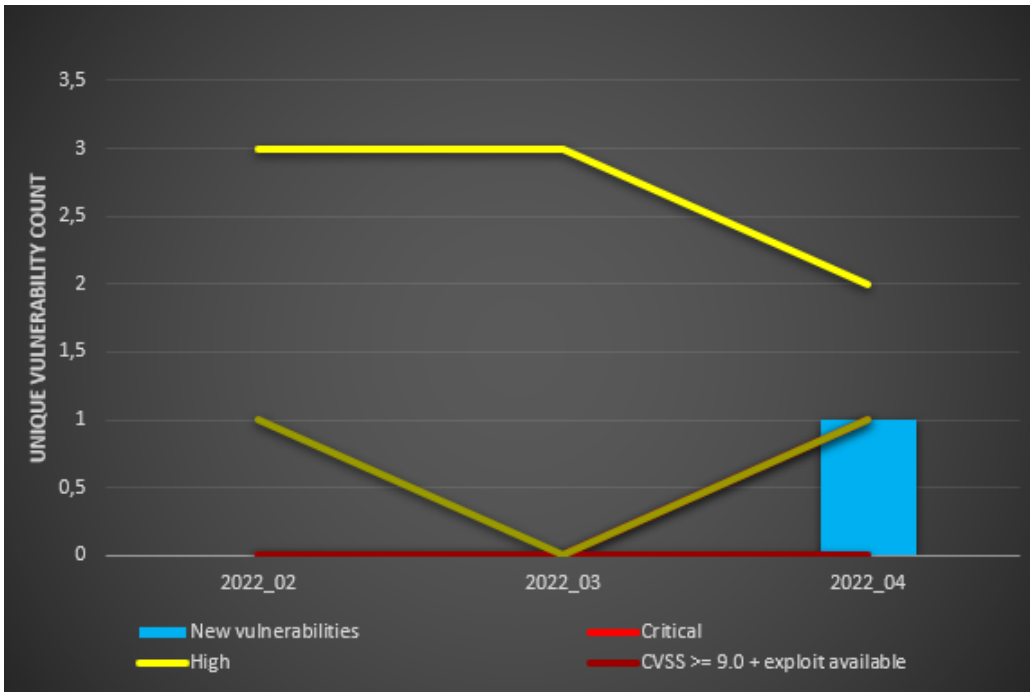

Figure 18. Unique Vulnerabilities Discovered for C8 Over Time

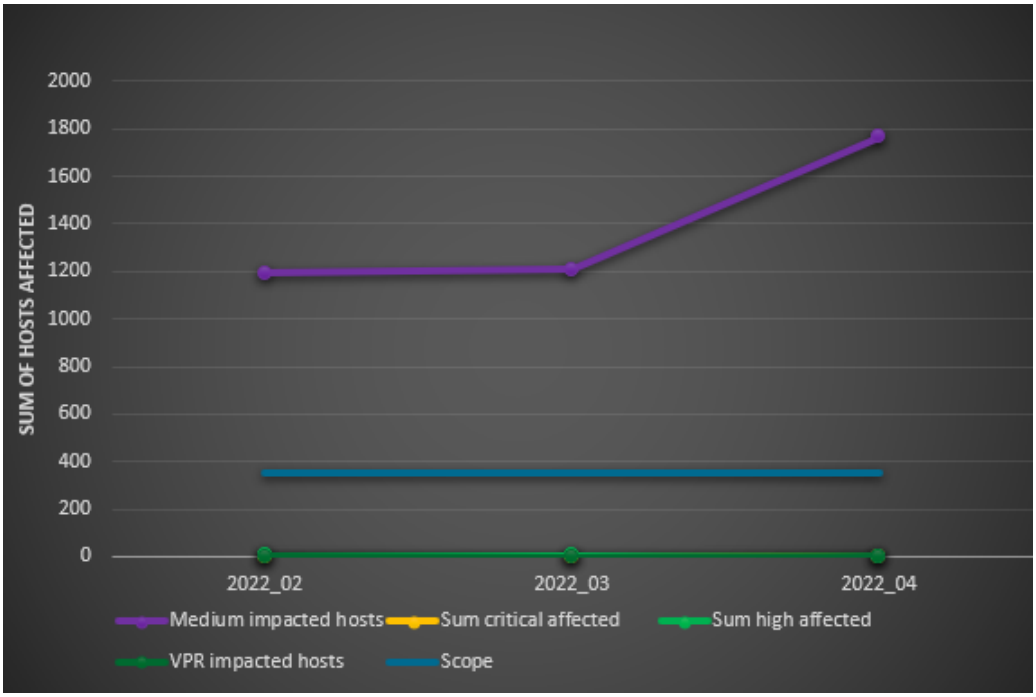

Figure 19. C8 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.4.9 C9 Progress

C9 has been able to control the critical severity vulnerabilities well, For VPR and high severity findings there has been an increase as we can see in Figure 20. The average

scope of assets being scanned has been 22 servers and for each server the amount of vulnerabilities detected is in line with new vulnerabilities discovered for this month. This means that the patching effort could be at their limit and needs additional resources. This could be supported by evidence from the increase of the sum of medium severity findings per server in Figure 21 and in the interview with C9 in Section 4.5.1 where the one responsible person said that some server owners have left and the remaining administrators have distributed the ownership among remaining employees while having additional time constraints to perform this activity..

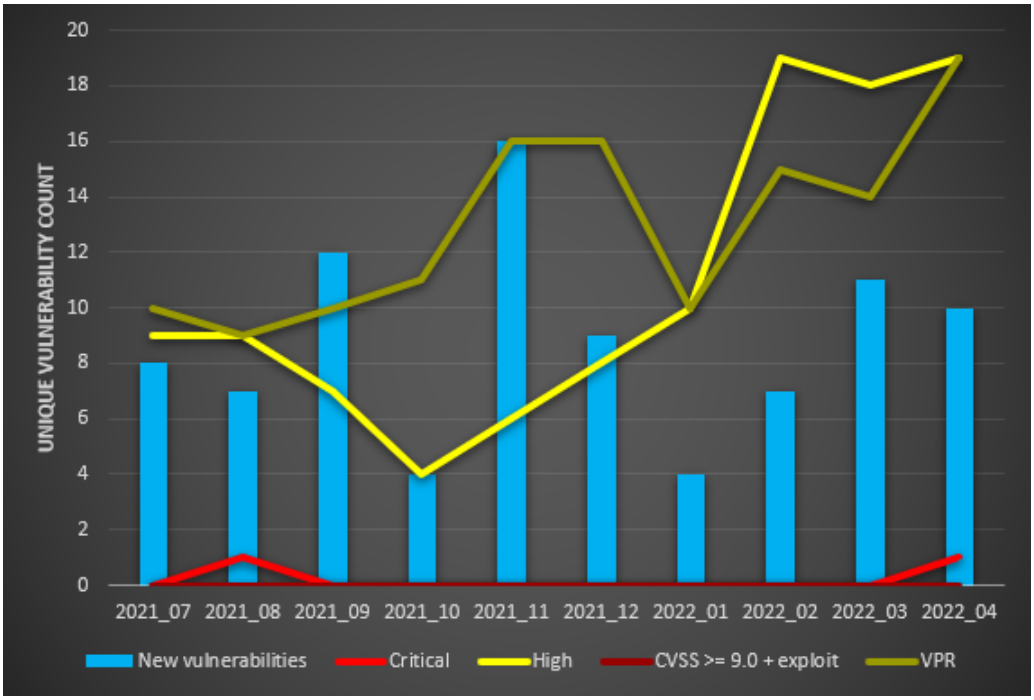

Figure 20. Unique Vulnerabilities Discovered for C9 Over Time

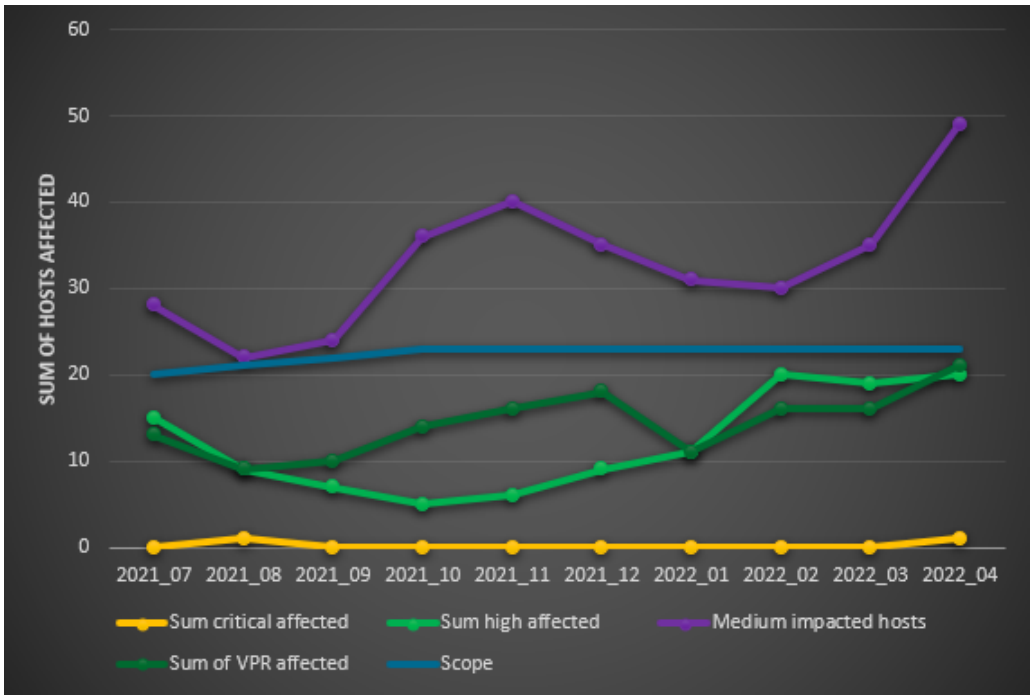

Figure 21. C9 Critical and High Vulnerability Affected Hosts with Scan Target Scope

4.5 Qualitative Data Analysis

4.5.1 Interviews

To ask questions and understand how organizations conduct their vulnerability and patch management activities interviews were held with each participant. Questionnaire is brought out in Appendix 2. To improve the overall understanding of the processes in scope interviews were conducted with personnel involved, Table 5 outlines the roles of the interviewees in the respective organisation.

Identifier	Position	Responsibility
C1	CISO	Org information security
	CEO IT Service Provider	Owner of patching service
C2	CISO	Org information security
	IT Operations Manager	Oversees IT operations
	IT Administrator	Conducts patching activities
C3	IT Administrator	Conducts patching activities
C4	System administrator	Conducts patching activities
C5	IT Manager	Responsible of IT
C1	IT Director	IT operations
	IT Specialist	Conducts patching activities
C7	IT Director	Responsible for IT service
C8	System administrator	Conducts patching activities
C9	IT Administration Team Lead	IT operations

Table 5. Interviewees and their Roles.

Operations

Table 4 outlines information regarding patch management approaches. C4 is brought out in two different entities due to the divided responsibility of patching servers. When discussing IT operations related to patch management and applying fixes for vulnerabilities the prevailing operational mode was thought to be semi-automated by most of the participants. C1 and C8 stated that their approach is automated, and C7 leaned more on the automated side, but since they have assets that are fully manual settled for semi-automated. C9 was the only participant who stated their approach to be manual and the patching responsibility is divided by ownership. Patch management in our research involves OS and application level of patching, also scanning is able to detect vulnerabilities in custom business applications, though fixing those findings may require involvement of developers from the organization side.

The patching approaches and their meaning was outlined in Section 2.2 for us automated patching means that a native or a third-party tool is used to deliver patches and updates. Semi-automated means that some automation tool is used, but significant amount of assets rely on manual approach. Manual patching in our research context means that administrator logs into server and applies updates on each server separately.

The organizations who were using automated patching approach used a third party software, for example C1, and C7 used Datto RMM, and Foreman Katello was used by C8. C1 IT Service provider stated that the tool enables to reduce the load of employee needing only to configure it once. Application and operating system updates arrive via this tool. Firmware

and driver updates are done manually, but due to their nature less frequently and done with larger number of employees. C7 stated that their IT Service provider uses the same tool, but since the representative from them was not present in the interview we cannot elaborate. C8 server environment is purely Linux based and Katello automated tool checks on the background if some packets are vulnerable and adds the new updates. Organizations using the semi-automated approach use the following tools WSUS (C2), SCCM (C5, C6) - C6 says that it covers 99 percent of the business needs, but has also tested Microsoft InTune to cover security aspects, Ansible (C9) but more to discover missing patches or do a deployment in case of emergency. The semi-automated approach organisation state that some servers are configured to receive updates automatically and C4 is planning to implement tools, WSUS has been tested.

When it comes to manpower who conduct patching we get different results, overview of the counts can be found in Table 4 For example in organisations C1, C8 there is only one person responsible for updating systems. C1 one has highlighted that this is possible due to automation, but note this person is on the side of IT service provider meaning it is responsible for conducting patching for other organisations as well. C8 says that to this day there has been one person, but there are plans to add additional 1 employee to distribute workload. C5 is too using 1 person and says the workload is manageable. C6 says that most of the patching activities relies on one person, but historically there are systems that are partially updated by other person, hence the 1.5. C7 service provider uses the same tool as C1, but unfortunately we can not say for certain how many people are responsible for updating this organization systems. C2 and C3 have both 2 employees. C4 and C9 have more than 2 people, C4 conducts patching with 3 administrators and 2 service-desk employees also help. C9 has divided the patching responsibility among 3 server owners respectively.

To elaborate on the operational responsibility we investigated on what departments or teams are responsible for the patching activities. For C1 it was third party IT infrastructure team, C2 IT Management department, C3 it is IT teams work, C4 mentioned that the responsibility is divided between system administrators, development teams, operational teams and medical team who have their own servers. C5 and C8 do not have a team and it is one person who does all of this. C6 highlighted that an IT team is the owner and inside there are responsibilities shared between infrastructure and business software maintainers. C7 stated that the provider has a dedicated server management team. C9 has given this task to individual server owners.

Patch Management

Patching processes are conducted, but interesting finding is that only C1 and C4 have specific written patching processes in place. C5 and C7 highlight that the responsibility of applying patches and keeping systems up to date is written is in the contract with the provider. C8 and C9 reference to general documents and guidance in the organization where the topic of patching is described. We discussed the steps of the processes of patch management. Patching times are set for C1 for every third week in a month, physical servers are patched separately on the fourth week. They also always restart the server before applying patches and once more if the installation is complete. C4 highlights that some servers in their scope are updated only every two months. C3 brings out that only if an update is required a patching window is searched and not being relied upon dedicated windows. C5 describes how patching process is influenced by monitoring information channels and input from the vulnerability management. The patching activities are not heavily regulated for this organisation and rely on communication with respective stakeholders. C6 patching process is built heavily around Microsoft patch Tuesdays. Packet of updates is prepared from the new releases and applied to a small patch of servers for testing. If no issues occur a wider deployment is done. C7 mentions that a staging is done by service provider before mass deployment of new updates. C8 describes that Linux server are updated automatically and where not possible then *yum dnf* to update manually. For critical vulnerability fixes manual approach is taken. C2 describes their patching maturity as primarily still too reactive.

When it comes to metrics to measure patching activities no organization said that this is described in the process. However there are different approaches how these organizations measure their effectiveness. For example C1 and C8 uses the same patch management tool dashboard to see what is the status. C4 monitors the Jira tickets created for people responsible for patching and their closure rate. C6 have an internal deadline to apply all this months patches latest by 28.th of the month. C2's KPI input for patch management is considered the results from vulnerability management.

To prioritize patches organizations have different approaches. C1 keeps firmware and driver updates separately and no other prioritization, approach is that updates are for applying. Patching is put on hold if there are emerging issues. The gaps will be revealed by VM. C2 and C9 focus solely on results from the VM taking into account criticality and exploit ease. C3 gets considers Azure notification based on alert criticality. C4 does not have specific rules, closer attention is given if there is a security update available and not going to wait for the window if necessary. Similarly C5 applies security updates immediately, other updates are prioritised by responsible person keeping Windows versions 2-3 months

behind. C6 does not use any direct prioritization approach, Microsoft releases are routine activity, as for the same reasons like C5 they do not chase all the latest patches, since it might cause issues or potentially service downtime. Business software downtime needs to be avoided at all costs. C7 priorities are set by the service provider and organization as the service customer has the opportunity to make suggestions. C8 focuses on the criticality and what the bug fix improves.

Information feeds play a role distributing information regarding patching. C1 sometimes works on the Microsoft Patch Tuesday's emails, and Reddit subsections have been proved useful. C2 focuses the feed monitoring efforts more on vulnerability side, because vulnerability is always before a patch. CERT-EE and CERT-US provide also valuable information. C3 is too keeping eye out on CERT-EE alerts. C6 focuses on user populated sources, similar approach as C1. C4, C5, C7, C8, C9 do not really monitor any patch related feeds.

Asset management is part of patch management and asset inventory is a critical part of it. The organizations in scope do not have any separate asset management inventory in place. C1, C8 rely on patch management software to show the accurate asset list where C8 is planning to expand to Ansible inventory. C2, C3, C6 asset inventory is on hypervisor. C5 do not have any other systems and keeps information by heart. All new server orders go through the responsible person. C7 has delegated this responsibility to service provider. C9 has Confluence documentation of all servers and their respective owners. C4 has built their inventory based on Jira and Insight plugin is used to gather data.

Legacy systems can be difficult to manage, frequently they have vulnerabilities that can not be fixed. C1 has taken approach that these systems are not patched, but are being decommissioned when possible. Isolation is a practice if the system needs to be up and running for some time. C2 has the same approach, unfortunately many legacy systems are still present. Isolation is the first risk mitigating action and decommissioning as soon as possible. C3 also has these kind of systems left primarily for specific business need due to the fact that these are maintained by third party there is nothing much to do besides isolation. C4 have plenty of EoL systems since some legacy applications need older servers to run. C5 when it comes to legacy software they have extended licenses, but other then that no major problems. C6 also has minimal amount of legacy systems remaining and the focus is on getting rid of them instead of fixing. C7, C8, C9 report that they do not have any legacy systems to operate.

Third party applications or systems can stall effective patch and vulnerability management. C2 brings this out as the most critical problem, but the situation is caused by their operation logic. Even fourth parties can be involved. IT is considered a hosting provider where

internal customer can come for resources and contract other parties to install some required software. If contracts change it is hard to see who is the responsible person and can fix the vulnerabilities found. C1 brings out one specific third party who is taking too much time to fix their systems. C8 has similar experience where one specific third party is causing problems. C3 and C4 also have third party systems primarily related to their business. C7 has outsourced only to one third party that is the same service provider responsible for servers. C5 and C9 have outsourced their web-servers.C6 is content with their third parties and says communication is effective, patching date is set and communicated to stakeholders and if required this can be moved in a three day frame, but once in a month is fixed.

Testing is important part of patch management to avoid impact. We investigated how organisations approach this step. C1 brings out that full non-production environment where all systems would be duplicated is too expensive. Test environment is maintained only for business critical systems. Same can be said for others organizations too with the exception of C7 who do not have their own test servers, but the service provider has.

New server installation approaches vary, C1 have a golden image for every customer and this is standard operating procedure. Golden image approach is also followed by C9. C2 has this for some servers, but not for all since internal customers usually order a clean server and apply additional software by themselves. C3 also have a template for servers, but it is not kept so up to date compared with workstation installation templates. C5 tells that their template is usually renewed after every six months. C8 updates the templates after every three months. C4 and C6 do not use templates to install new servers. The latest installation is used for this.

Incidents or downtime from patching of servers is not recalled by C2, C3, C4, C7, C9. Some minor issues were indicated by C5 which was caused by a faulty Windows update, but the impact was only limited to a couple of servers. C1 recalls issues with domain controllers, but the contributing factor was their age. C6 has also had negative experience with both on servers and workstations explaining their standpoint on not applying the latest and greatest. C8 has had problems with specific software and systems that were not connected to central management. Also some issues with patching has been caused by human error.

Vulnerability Management

We investigated if the current VM process helps to prioritize patching activities. C1 tells that it does not do this directly. It brings out vulnerabilities that have been missed by

the automating tool and is in a sense a extra control. The experience has been that every time there are 1-2 servers that are reported fixed in the tool, but VM results still detect the vulnerability, cause of this situation has been an additional missing registry key change that needs to be performed manually. C2, C6, C7, C9 confirm that it helps prioritizing and C3 adds that the VPR score is useful. C4 elaborates that critical vulnerabilities are visible, but the mitigation progress is being hindered by their underlying infrastructure and man power. C5 confirms that it helps to prioritize and since he cannot manage everything by him self it reduces his workload. C8 tells that it definitely helps and results can be used as leverage to push third party to fix their software.

VM scope for all organizations in the scope of this research are primarily servers, with exception of C7 who has workstations also in the scope. C8 has fully Linux based server park and is the only one who is using unauthenticated described in Section 4.2 scan approach. Others have primarily Windows server parks or mixed with Linux.

Upper management interest and support is crucial for the vulnerability management process. We investigated what has been the perceived experience of our subjects on this matter. We measured this on a subjective scale from 1-5, 1 being the lowest and 5 highest. C6 indicated a score 7.5 marking very high management interest, due to a recent security incident. C7, C8. C9 marked also high interest with a score of 4 and saying vulnerability related issues get a green light to fix. C1 marked the interest as 3 saying that vulnerability KPI-s are reviewed and presented on group level 2 times a year. C5 mentions similar group level interest, but since it is high level it is more risk based, however reports are sometimes asked and then it is good to show. C2 mentions that management interest is primarily that everything is secure and if there is a capability that enables us to do it it gets resources and advises that when it comes to vulnerabilities it is better to communicate the risk. C3 have not seen direct interest, approach is that it is assumed that everything is well. C2 indicates the interest with score of 2, does not feel concrete interest, but management gets the reports.

When it comes to sharing the vulnerability reports C1 mentions a benefit that it has been used to communicate the danger and risk on legacy systems. C4 indicates that it has enabled them to bring management attention to resource constraints. C2 has not shown these reports and C3 believes that his manager is talking about it, but we could not confirm this during the interview. C5 has show only specific vulnerabilities and overall outcome of the results.C6 and C7 tell that the scan reports purely are too technical and need translation about the risks and threats coming from these. C8 has used them to register bugs in their own developed software. C9 management have been directly asked about data for critical weaknesses.

To get a better understanding how vulnerability management remediation and mitigation phase works we asked the mitigating teams how do they work with data in the reports. For all of the recipients some form of internal distribution takes place after initial review, there is indication that this can require effort (C2). Some (C5) treat it as a communication tool to communicate vulnerability information to server owners or responsible people. Severity scoring is paid attention by all participants and some make decision on what to patch first based on the results (C8, C9).Interesting comments observed that there would be less findings if we would have automated patching (C4). Vulnerability management have made C7 to pay more attention on the patch management activities. C1 has also focused on fixing some high spread lower severity findings to improve the overall picture, plus new personnel joining soon could help even more and C6 adds that 20% of effort sometimes gives 80% of results. Some older systems tend to repeat from scan to scan, but plan is do get rid of those.

Clear roles help do facilitate co-operation, we investigated how the lines of responsibilities are felt from the organizations side. All organizations confirmed that roles are clearly defined. C1 added that they are making sure this stays that way. C4 noted that the problem is more on the physical human capability side of managing all of this. C7 says that it can be improved, but the current state is sufficient.

From time to time you find vulnerabilities that you cannot fix, organizations have similar approaches to handle these situations. C1 primary goal is decommission and separation with concrete risk registration process. C2 network level is already on a good level, but if there are systems that are vulnerable additional isolation controls will be added. They also noted why this kind of vulnerabilities develop in their organization and this is due to the fact that building new systems get more priority than the clean up of the older ones. C3 mentions that these situations have happened when they have to wait behind developers, also applying a patch sometimes need a configuration settings changes, this is done by modifying group policy. C4 puts vulnerable systems on a separate network segment. C5 inspects the systems individually to understand their function and making sure they are not domain joined. Limitations from network side are set. Replacing those kind of systems is difficult since they are connected to some older hardware that is very expensive to replace, for example CCTV. C6 follows similar approach as C5 and when it comes to problematic systems they investigate and monitor for a while how many users this actually have to learn what would be to business impact if applied patch breaks the application. C7 has never experience this kind of issues, their approach is that old systems are decommissioned regularly, C7 similarly only notes that there has been experience with one third party application vulnerability. C9 has network level segmentation as a security control.

Communication is important part of the whole process. Besides sharing report all the organizations have meetings. We investigated how they see that part. All organizations rated communication as good, some added polite indicating satisfaction. When focusing on what could be improved C1 added that it would help if the mitigating team sends a commented report back before the meeting. C2 added that sometimes more back and forth communication has been used for example when handling a difficult vulnerability to fix. C3 and C5 uses the vulnerability meetings between teams to discuss and set plans. C4 suggested that if the vulnerability service provider gets more knowledge about their infrastructure would be a helping factor and if they have more workforce to handle the load. C6 brings out that the meetings is a place where we communicate in the *human language* to discuss issues, make conclusions, and the list of resolutions is helpful to understand what needs to be done also in the course of the meetings both teams get to know each other. C8 values that during the meetings we discuss things in the local language. C7 suggested improvements from the remediation aspect, the process especially verification and feedback has a long feedback loop, if something was fixed during we get this confirmation during the next scan, at the moment we have plenty of work to do, but it could be a future topic.

Vulnerabilities can be exploited by bad actors and we were curios to ask if there has been security incidents among our participants. 4 out of 9 have not had or do not recall any. Remaining 5 have had experience. There has been issues with Log4J vulnerability being exploited, some have had experience with ransomware, sometimes vulnerabilities exploitation was enabled by an accompanied configuration error made by a human.

To tie our hybrid research together we went through the vulnerability statistics for each organization separately to get their opinion on the matter. C1, C3 noted the results as expected. C2 notes that the amount of vulnerabilities should be lower, and the graphs confirm that their process today is reactive, also a question rose about the scanning date having effect since it is relatively close to Microsoft Patch Tuesday. WSUS could patch majority of those, but cannot make the full coverage by the scan time. Agreeing maintenance windows is a major contributing factor since these are hard to get and systems need to be up 24/7. C4 rates the results as logical and points out that the C4.2 section in their organization have a patching cycle once every two months. For C5 results make sense and it is useful to routinely check the status this way. C6 see from the graphs a positive trend, which varies in strength in different categories, but overall situation is improving. This is enabled by partners, proper tools and the support on the highest level of management and motivating fear from past incidents. Rating the management support as the most critical factor, otherwise it would be difficult to talk about these topics. C7 explains that the spike in the results was the turn on of authenticated scans. The unauthenticated scans found vulnerabilities, but the authenticated found more. C8 the high count of medium severity

vulnerabilities are caused due to a certification error. C9 brings out the restricted time of the responsible people has been a contributing factor.

Open Dialogue

To grasp what have been positive about the vulnerability management process for organisations we found the following. C1, C4 are pleased with the process. C2 pointed out that they do not need to perform the scanning and reporting by themselves and external party gives evaluation without bias. Also being aware of our problems. C3 mentioned the monthly routine is a good and helps to keep things in order. C5 tells that information moves quickly and appreciates the notifications if there are vulnerabilities that require immediate action. Since their business wants to focus on their main activities outsourcing the vulnerability management service have proved to be the best option. C6 says emphasises routine in the process is a must and that the approach from the vulnerability detection team is personal and is not just sending over an report, but there exists a dialogue between stakeholders. C7 values regularity of the VM and with out it you would just assume that all is well. Knowing about the vulnerabilities are where they are in the organization and being able to show it rated high by C8. C9 says the scanning works and the detection levels are good.

There is also room for improvements, we investigated what could be these points and what are the obstacles the organizations see themselves. C1 says that the risk management part should be always followed when there exists vulnerabilities that cannot be remediated. The difficulty there is that vulnerabilities are very technical and hard to put into the risk management context. Resource on the remediation side is needed, because the positive impact in vulnerability management comes from closing the gaps. Also estimating what could be the configuration change effect company wide requires too much time. To improve the monthly meeting C1 IT service provider considered an internal meeting, before the vulnerability meeting to agree on their internal plans. This will be taken into action once more resources are available. Legacy systems will be considered as a primary obstacle in the near future as well. C2 mentions lack of resources and focus on automation with notification to stakeholders, unclear responsibilities between third parties accompanied by communication issues, lack of system standardization and rules on how new services are established in the policy, difference in operating systems, database engines and software as obstacles to improving the overall process. C3 says that there are no obstacles, the workload is bearable. C4 finds that the communication with stakeholders is too much for one person, some missing licensing for tooling, issues in administration practices and gaps in configuration management and inventory should be resolved. C5 considers lack of personnel as an issue, a dedicated FTE is required. C6 emphasises that they are not a modern IT company, time factor can be an obstacle, but not a major one. Some

legacy systems that have remained are difficult to patch because the decisions to replace them were not made when the time was right. Also the nature of their suppliers and vendors focus on security can sometimes be less than desired. C7 wishes for a high level management overview that could improve their management interest and the issue of fixing the authenticated scans took time. C8 does not see much obstacles, saying if they can fix the main culprit for medium severity vulnerabilities they can get the picture very clean and adding one more responsible person can improve their speed. C9 brings out that some people have left and their previous responsibilities have been divided among the team causing delays.

5. Discussion

Our research objectives in Section 1.3 set out to see how successful are the organizations in their vulnerability management programs. Is patch management an enabler for effective vulnerability management for these organizations and what are the key learning points that can be used to help organizations that are still in the process of implementing vulnerability management. By performing hybrid analysis using quantitative and qualitative methods has given us insight on the topic. Vulnerability management is an important security control for any business who wants to protect themselves from the destructive consequences for cyber incidents.

Asset management inventory management could be an overlooked issue. Some of the organizations rely on hypervisor virtual server list or the same tools that are used to conduct patching activities for populating asset information as we found during the interviews in Section 4.5.1. This could be sufficient, but this approach also lacks information regarding the business criticality of the assets in one concise place and is usually accessible to personnel in the IT team.

Our research shows VM positive effects to the overall reduction of vulnerabilities in an enterprise environment for majority of the participated organizations with different levels of reduction.

Upper management support is crucial for any process to be successful including VM. Majority of organizations outlined good levels of management support and interest in the results of VM, indicating higher interest on organizations that have experienced security incidents. One organization have made the results to be KPI on business group level. For organizations where the interest was not that high the expectation was still that systems need to be secure.

We observed in our research that organizations who are employing automated tools for their patch management efforts have better results from the vulnerability management perspective. This was evident when we compared two organizations C1 and C2 of similar size. We can also see that with these tools one person can maintain a wider scope of assets meaning that this could be a solution for the human resources challenge. Based on our

findings in the example of C1 who has outsourced the IT systems management has good results on patches being applied timely and vulnerabilities fixed.

It is important to have the resources available who conduct patch and vulnerability management. In some cases we saw degraded results on remediation performance such as slower pace of remediating vulnerabilities and scope creep of old vulnerabilities remaining. Additional workload for already constrained employees was highlighted during the interviews as a negative experience. Sensing the need of extra personnel was commented during the interviews by several organizations (C1, C4, C5, C8, C9).

All participants found value in the vulnerability management process and are content with the results in open dialogue in Section 4.5.1. C2 outlined an interesting point during the interviews that if scanning and reporting is done by another party the bias is removed and honest evaluation of the security situation is given. C2, C7, C8 and C5 brought out the creation of awareness about the problems shown in the reports and enables keeping systems in order. Outsourcing the vulnerability management has proven for them to be the best option. It is valued that vulnerability management in this case was not just a report sent over, but more of a dialogue between different stakeholders as C6 put it.

New vulnerabilities are found daily and system vendors release fixes constantly. Indicating that vulnerability management to detect weaknesses in your environment is supposed to be a regular activity. During the interviews in Section 4.5.1 all participants found that when it comes to vulnerability management routine is an important factor. VM regular meetings between all stakeholders as mentioned by C6 facilitate co-operation and forces to take action and if required review processes.

If the enterprise environment has a large amount of assets to maintain and if the ownership and responsibility of keeping system up to date is distributed, stakeholder management can quickly become a complicated task. Chasing responsible individuals is unnecessary burden on the vulnerability remediating teams in some of our observed cases it was suggested that a separate project manager working full time would be appropriate for this task by C4 and C2 also needs to chase correct owners.

Credentialed patching gives more detailed information about possible local vulnerabilities that a system might have. We saw that un-authenticated scans do find issues, but it probably is not the complete picture, since for C7 the amount of detected vulnerabilities rose significantly when authenticated scans were turned on.

It can be that for patching some business systems the patches are delayed in the fear of

causing a undesired disruption. We were curious to see if that has been the case. Majority of the participants did not recall any notable issues such as loss of stability of servers when applying new patches. Indicating that the quality of the vendor patches has improved over time and possibly for Windows environments relying on automatic updates could be set. This enables a faster deployment of patches without the additional activities of the administrative personnel. Automatic updates potentially could reduce administration team workload and help in the remediation of vulnerabilities faster.

Decommissioning legacy systems can be difficult thing to do, but is the preferred approach for majority of the organizations. If remediation of vulnerabilities on those systems is not possible the organizations have opted for mitigation activities such as shielding and limiting access on network level. It is important to communicate the risk to business and get their acceptance C1. Vulnerability management results could be used to convey the message why these kind of systems are problematic and also bring up conversations on executive level when new systems implementation is being delayed, C1 has used vulnerability data to communicate this message.

Third party (in our research meaning a service provider who manages their provided systems or applications) management is important especially if vulnerabilities are detected on the systems and applications they provide. For example C1 and C6 outlined that systems that are maintained by third parties it is difficult to find correct people to contact and this delays the remediation of weaknesses. Vulnerability management results can be used to demonstrate issues and problems to third parties. One possible solution to prevent these situation is to outline responsibilities and commitments promised when it comes to the maintenance of these systems when signing agreements and contracts.

Testing new releases and patches is important part of the patch management cycle. All organizations in the interviews told to have test servers for a least some business critical applications to make sure new updates do not interfere with the functionality of the important programs. A subset of servers could be considered as a test group to which the latest patches are applied and after a period of wait time if there are no issues these updates can be rolled out to the whole scope.

If you have templates for installing. it is better to check templates regularly if you install from scratch that could be a better alternative from security perspective. C8 an organization who has full Linux environment for example re-creates all the templates after every three months.

On discussion how to improve vulnerability management the participants outlined the

following. C1 highlighted that risk management should be integrated into the VM, but their tries doing this have not been successful since vulnerability data is technical and detailed in nature and communicating this is not straightforward, but ideally it should be followed each time there is a situation when a vulnerability cannot be fixed.

Keeping systems updated and free from weaknesses is utmost priority for any business or organization. The importance of vulnerability management is stressed at the highest level of our governing institutions. Our research demonstrates that having a vulnerability management process in place helps to detect vulnerabilities and creates the necessary visibility to enable organizations to take action.

Some key learning's could be applied to any of the organizations who today are not managing this process in an effective way. With regular and routine scanning even once a month enables the organizations to react and mitigate the most severe vulnerabilities threatening their security. Also it gives valuable input and forces to evaluate patch management practices to be able to stay current with the application of the latest patches, that for example Windows systems are released usually once a month.

We researched different types of organizations from various industries with each their own practices and approaches. Meaning that it is possible for any organization to start their vulnerability management program and improve it over time. The added visibility will enable to take action and see where are the vulnerable systems to avoid negative consequences later. The results of our organizations confirm in general have made progress on remediation vulnerabilities and their example could be guidance for others as well.

It is important to note that we have been directly involved of setting up the vulnerability management process in the respective organizations and have participated in the monthly meetings when results and plans are discussed. We see this as a contributing factor since this gives additional understanding of the practices and first hand encounters of problems that are more *day to day* in nature. To eliminate possible bias we chose the hybrid research approach so we can combine quantitative and qualitative data to provide concrete evidence.

Our research used for quantitative data primarily from internal vulnerability scan results. Assets focused on in most of the cases were servers, in some organizations servers and workstations if they were in the scope. This means that the view is endpoint (servers and workstations) based and would not reflect the whole scope of every possible enterprise asset such as networking equipment, IoT devices, containers, etc.

The vulnerability management is one of many security controls that an organization can

apply for protecting themselves from cyber threats. Indication how well an organization is handling its vulnerability management cannot be translated to direct probability of a security incident to occur. However broadly speaking the less vulnerabilities there is in the IT systems the possibility of the incident should decrease.

Although we covered different organizations form different industries with similar infrastructure the generalizations on the topic here could not be suitable for every type of organizations due to a fact that some may have stricter security requirements or more complex IT systems.

As for future research this could be repeated with the same organizations after some years to see how the vulnerability management process has matured and how the increasing scope has been dealt with. This would give valuable data about the complexities of managing weaknesses in different type of assets and what technological solutions are optimal to be used.

To further develop this research another perspective would be to combine vulnerability threat intelligence and the measurement of remediation time in detail for the most critical weaknesses and to compare which organizations are more capable of rapid response. This would give us more insight on how to improve timelines and KPI-s for this type of fixing.

Vulnerability management research in more dynamic environments would be interesting research topic. For example container platforms, broadly defined, are software solutions that allow you to manage containerized applications. They provide capabilities like automation, orchestration, governance, security, customization, and enterprise support for container architectures [43]. The nature of these environments is more dynamic and requires security and administration teams to adapt different approaches.

The research did not go into details of specific vulnerabilities that the organizations have and did not bring them out in the thesis due to the sensitivity of this information. This could have been done if we would not have added the qualitative methods where we bring out some details about the participated organizations.

Organizations who today are not performing vulnerability management or are approaching this on an *ad-hoc* level could read this paper and study the experience of organizations who today are already following this process. It could serve as a guidance to answer some of the questions one would have in the beginning of this journey.

6. Conclusion

Threat actors are weaponizing vulnerabilities and if organizations do not want to deal with the consequences they need to be proactive and conduct vulnerability management. Unfortunately new vulnerabilities are discovered daily and this has put business into a race of remediating weaknesses before they can be used against them.

Vulnerability management is a security control that can help organizations to stay secure and lower the possibility of a cyber attack against them. Our research objective was to find information on how successful organizations are in this process, what are the enablers of successful VM program and what could be the obstacles hindering this process.

To get complete picture we used hybrid analysis for our research method. Detailed quantitative vulnerability scan data was analysed and used to create different graphs that could outline trends in the remediation efforts. Semi-structured interviews were conducted with each organization employees closest to the process to give us qualitative information of their experience.

Our results outlined that from vulnerability remediation perspective all organizations have benefited from the process and reduction of most critical vulnerabilities have declined. The good experience with outsourcing the VM service has given organisations routine and visibility into their weaknesses without biased results. Interestingly majority of the organizations could not recall issues with the application of patches, possibly indicating the vendor side quality improvement for patches. Also management support for most the organizations was on an adequate level.

Remediation progress has been made difficult primarily with lack of human resources, complex ownership of systems and third party applications and their maintenance responsibilities. Legacy systems were outlined as an issue stopping remediation on some cases.

Some topics that were interesting to see was the possibility of improvement for asset management that currently for majority of organizations is handled with tools that do not have business criticality information. The un-credentialed scanning is able to detect more

vulnerabilities and is recommended to be used. Some organizations see the benefits of integrating risk management into vulnerability management.

7. Summary

Most devastating cyber incident in the world have been enabled by security vulnerabilities. New bugs and issues are discovered daily and businesses and organizations need to react to them with speed to avoid negative consequences to their systems and work. Vulnerability management is a practice to detect vulnerabilities and fix them in a timely manner. Making organizations safer and more resilient to cyber threats. In our research we investigated the experience of different organizations who already conduct their VM practices to see what have been the results and are there any learning points about the process to others as well.

We used a hybrid analysis approach to conduct our research. Quantitative data was collected from each organization in the form of vulnerability scan results that were analyzed to discover trends and measure performance. Qualitative data was composed of answers from semi-structured interviews with responsible people .

Most contributing success factor to VM is routine that enables constantly discover new vulnerabilities. Followed by prioritization and management support and good communication. Obstacles that hinder VM progress are primarily lack of personnel resources, communication issues during stakeholder management, patching management approach and tools available.

Bibliography

[1] *EUR-Lex - 32016L1148 - EN - EUR-Lex*. Doc ID: 32016L1148 Doc Sector: 3 Doc Title: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union Doc Type: L Usr_lan: en. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (visited on 03/12/2022).

[2] *The new yearbook of the Information System Authority (RIA) on cyber security summarises the most influential incidents in cyber space | Estonian Information System Authority*. URL: https://www.ria.ee/en/news/new-yearbook-information-system-authority-ria-cyber-security-summarises-most-influential.html (visited on 05/11/2022).

[3] CSRC Content Editor. *Vulnerability Management - Glossary | CSRC*. URL: https://csrc.nist.gov/glossary/term/vulnerability_management (visited on 04/10/2022).

[4] *Minimum Security Measures for Operators of Essentials Services*. ENISA. URL: https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services (visited on 04/24/2022).

[5] *Cybersecurity guide for SMEs - 12 steps to securing your business*. ENISA. URL: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes (visited on 05/01/2022).

[6] *Estonian information security standard | Estonian Information System Authority*. URL: https://www.ria.ee/en/cyber-security/estonian-information-security-standard.html (visited on 05/11/2022).

[7] *E-ITS*. URL: https://eits.ria.ee/et/avalehe-menueue/security-measures-v2021/ops/#1description113 (visited on 05/01/2022).

[8] *The 18 CIS Controls*. CIS. URL: https://www.cisecurity.org/controls/cis-controls-list/ (visited on 05/03/2022).

[9] *About OWASP - OWASP Top 10:2021*. URL: https://owasp.org/Top10/A00-about-owasp/ (visited on 05/11/2022).

[10] "Cyber-attack: US and UK blame North Korea for WannaCry". In: *BBC News* (Dec. 19, 2017). URL: https://www.bbc.com/news/world-us-canada-42407488 (visited on 04/04/2022).

[11] *The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED*. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (visited on 04/08/2022).

[12] *Log4j – Apache Log4j Security Vulnerabilities*. URL: https://logging.apache.org/log4j/2.x/security.html (visited on 04/15/2022).

[13] *Heartbleed Bug*. URL: https://heartbleed.com/ (visited on 04/15/2022).

[14] *Apache Struts : List of security vulnerabilities*. URL: https://www.cvedetails.com/vulnerability-list.php?vendor_id=45&product_id=6117&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&cweid=0&order=1&trc=70&sha=5369e34293062ebe460c99e6878e0792ac23944c (visited on 04/09/2022).

[15] *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? URL: https://www.avast.com/c-eternalblue (visited on 04/15/2022).

[16] *Meltdown and Spectre*. URL: https://spectreattack.com/ (visited on 04/11/2022).

[17] *About*. CYBERS. URL: https://cybers.eu/en/about (visited on 05/11/2022).

[18] Julian Jang-Jaccard and Surya Nepal. "A survey of emerging threats in cybersecurity". In: *Journal of Computer and System Sciences* 80.5 (Aug. 2014), pp. 973–993. ISSN: 00220000. DOI: 10.1016/j.jcss.2014.02.005. URL: https://linkinghub.elsevier.com/retrieve/pii/S0022000014000178 (visited on 04/14/2022).

[19] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. "Information security management needs more holistic approach: A literature review". In: *International Journal of Information Management* 36.2 (Apr. 2016), pp. 215–225. ISSN: 02684012. DOI: 10.1016/j.ijinfomgt.2015.11.009. URL: https://linkinghub.elsevier.com/retrieve/pii/S0268401215001103 (visited on 04/22/2022).

[20] Sara Kraemer, Pascale Carayon, and John Clem. “Human and organizational factors in computer and information security: Pathways to vulnerabilities”. In: *Computers & Security* 28.7 (Oct. 1, 2009), pp. 509–520. ISSN: 0167-4048. DOI: 10.1016/j.cose.2009.04.006. URL: https://www.sciencedirect.com/science/article/pii/S0167404809000467 (visited on 04/30/2022).

[21] Michael Anywar, Liisa Parv, and John Walker. “Eesti haiglate küberohu võimalikkus: Haiglates kasutusel olevate küberjulgeoleku standardite hindamine, tõkestamaks küberohte”. In: (May 31, 2018). URL: https://digikogu.taltech.ee/en/Item/4abba52d-0ee5-4f4a-914a-fefb43c52c06 (visited on 05/01/2022).

[22] M. Ugur Aksu et al. “A quantitative CVSS-based cyber security risk assessment methodology for IT systems”. In: *2017 International Carnahan Conference on Security Technology (ICCST)*. 2017 International Carnahan Conference on Security Technology (ICCST). Madrid: IEEE, Oct. 2017, pp. 1–8. ISBN: 978-1-5386-1585-0. DOI: 10.1109/CCST.2017.8167819. URL: http://ieeexplore.ieee.org/document/8167819/ (visited on 04/18/2022).

[23] Christian Fruhwirth and Tomi Mannisto. “Improving CVSS-based vulnerability prioritization and response with context information”. In: *2009 3rd International Symposium on Empirical Software Engineering and Measurement*. 2009 3rd International Symposium on Empirical Software Engineering and Measurement. ISSN: 1949-3789. Oct. 2009, pp. 535–544. DOI: 10.1109/ESEM.2009.5314230.

[24] Roland Rieke. “Modelling and Analysing Network Security Policies in a Given Vulnerability Setting”. In: *Critical Information Infrastructures Security*. Ed. by Javier Lopez. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2006, pp. 67–78. ISBN: 978-3-540-69084-9. DOI: 10.1007/11962977_6.

[25] Gerhard Eschelbeck. “The Laws of Vulnerabilities: Which security vulnerabilities really matter?” In: *Information Security Technical Report* 10.4 (Jan. 1, 2005), pp. 213–219. ISSN: 1363-4127. DOI: 10.1016/j.istr.2005.09.005. URL: https://www.sciencedirect.com/science/article/pii/S1363412705000646 (visited on 04/25/2022).

[26] Katheryn A. Farris et al. “VULCON: A System for Vulnerability Prioritization, Mitigation, and Management”. In: *ACM Transactions on Privacy and Security* 21.4 (Oct. 13, 2018), pp. 1–28. ISSN: 2471-2566, 2471-2574. DOI: 10.1145/3196884. URL: https://dl.acm.org/doi/10.1145/3196884 (visited on 04/27/2022).

[27] Omer Keskin et al. “Scoring Cyber Vulnerabilities based on Their Impact on Organizational Goals”. In: *2021 Systems and Information Engineering Design Symposium (SIEDS)*. 2021 Systems and Information Engineering Design Symposium (SIEDS). Charlottesville, VA, USA: IEEE, Apr. 30, 2021, pp. 1–6. ISBN: 978-1-66541-250-6. DOI: 10.1109/SIEDS52267.2021.9483741. URL: https://ieeexplore.ieee.org/document/9483741/ (visited on 04/17/2022).

[28] Matunda Nyanchama. “Enterprise Vulnerability Management and Its Role in Information Security Management”. In: *Information Systems Security* 14.3 (July 2005), pp. 29–56. ISSN: 1065-898X, 1934-869X. DOI: 10.1201/1086.1065898X/45390.14.3.20050701/89149.6. URL: http://www.tandfonline.com/doi/abs/10.1201/1086.1065898X/45390.14.3.20050701/89149.6 (visited on 04/27/2022).

[29] Seungjin Baek and Young-Gab Kim. “Efficient Vulnerability Management Process in the Military”. In: *2019 International Conference on Platform Technology and Service (PlatCon)*. 2019 International Conference on Platform Technology and Service (PlatCon). Jeju, Korea (South): IEEE, Jan. 2019, pp. 1–5. ISBN: 978-1-72811-288-6. DOI: 10.1109/PlatCon.2019.8669420. URL: https://ieeexplore.ieee.org/document/8669420/ (visited on 04/15/2022).

[30] Andrew Magnusson. *Practical vulnerability management: a strategic approach to managing cyber risk*. San Francisco, CA: No Starch Press, Inc, 2020. 1 p. ISBN: 978-1-59327-989-9.

[31] Tom Palmaers. “Implementing a Vulnerability Management Process”. In: (Mar. 23, 2013), p. 23. URL: https://sansorg.egnyte.com/dl/2IL7fioFhM.

[32] Murugiah Souppaya and Karen Scarfone. *NIST Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies*. July 1, 2013. DOI: 10.6028/NIST.SP.800-40r3.

[33] Debabrata Dey, Atanu Lahiri, and Guoying Zhang. “Optimal Policies for Security Patch Management”. In: *INFORMS Journal on Computing* 27.3 (Aug. 2015), pp. 462–477. ISSN: 1091-9856, 1526-5528. DOI: 10.1287/ijoc.2014.0638. URL: http://pubsonline.informs.org/doi/10.1287/ijoc.2014.0638 (visited on 04/14/2022).

[34] Simon Liu, Rick Kuhn, and Hart Rossman. “Surviving Insecure IT: Effective Patch Management”. In: *IT Professional* 11.2 (Mar. 2009). Conference Name: IT Professional, pp. 49–51. ISSN: 1941-045X. DOI: 10.1109/MITP.2009.38.

[35] Murugiah Souppaya. *Guide to Enterprise Patch Management Planning:: Preventive Maintenance for Technology*. NIST SP 800-40r4. Gaithersburg, MD: National Institute of Standards and Technology, 2022, NIST SP 800–40r4. DOI: 10.6028/NIST.SP.800-40r4. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf (visited on 05/01/2022).

[36] *The 18 CIS Controls*. CIS. URL: https://www.cisecurity.org/controls/cis-controls-list/ (visited on 04/27/2022).

[37] *CIS Control 7: Continuous Vulnerability Management*. CIS. URL: https://www.cisecurity.org/controls/continuous-vulnerability-management/ (visited on 05/01/2022).

[38] *#1 Vulnerability Assessment Solution | Nessus Professional™*. Tenable®. URL: https://www.tenable.com/products/nessus/nessus-professional?gclid=CjwKCAjwve2TBhByEiwAaktM1Fr-DiNVGodWRnNO49I6-dzWiCQS2ROFDbfDBwE&utm_campaign=gs-%7B11596512479%7D-%7B110256808702%7D-%7B537515898680%7D_00023779_fy22&utm_geo=apac&utm_medium=cpc&utm_promoter=tenable-hv-brand-00023779&utm_source=google&utm_term=nessus%20pro (visited on 05/12/2022).

[39] *Plugins*. URL: https://www.tenable.com/plugins (visited on 05/12/2022).

[40] *CVSS vs. VPR (Tenable.sc)*. URL: https://docs.tenable.com/tenablesc/Content/RiskMetrics.htm (visited on 05/12/2022).

[41] *NVD - Vulnerability Metrics*. URL: https://nvd.nist.gov/vuln-metrics/cvss (visited on 05/12/2022).

[42] *Nessus Credentialed Checks (Nessus)*. URL: https://docs.tenable.com/nessus/Content/NessusCredentialedChecks.htm (visited on 05/12/2022).

[43] *Container Platforms: 6 Best Practices and 15 Top Solutions*. Aqua. URL: https://www.aquasec.com/cloud-native-academy/container-platforms/container-platforms-6-best-practices-and-15-top-solutions/ (visited on 05/12/2022).

Appendices

Appendix 1 - Non-exclusive licence

I Jürgen Erm

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Hybrid Analysis of Vulnerability Management Practices In Organizations To Outline Success Factors" , supervised by Hayretdin Bahşi
   (a) to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   (b) to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

Appendix 2 - Questionnaire

Operational

1. *What tools do you use to conduct patching?*
2. *What is the patching approach? (Automated, Semi-Automated, Manual)*
3. *How many people work on patching the servers?*
4. *Which team in your organisation has the responsibility to keep systems up to date?*

Process - Patch Management

1. *Do you have a patch management process in place? Is it in written?*
2. *Please describe shortly your PM process.*
3. *Do you have any internal metrics to measure the patch management process?*
4. *How are patches being prioritized?*
5. *What feeds to you monitor when it comes to new patches?*
6. *How is your asset management inventory maintained. How do you know if new servers are added?*
7. *Do you have legacy systems and how do you treat patching those?*
8. *Do you have assets which patching relies on third parties?*
9. *Do you have a non-prod environment to test out the patches? What is the experience? Is responsibilities in the contract?*
10. *How do you approach new server installations. Is there a "golden" image that is being regularly updated?*
11. *Have you had any IT incidents related to deploying a new patch?*

Process - Vulnerability Management

1. *Does the current process help in prioritize patching activities?*
2. *What is in the scope of vulnerability scans, what assets namely?*
3. *How would you rate your management interest in the Vulnerability Management results from 1-5. 1 being the least and 5 the most?*
4. *Do you share vulnerability reports with upper management? What has been the feedback?*
5. *How do you use the data provided in the scanning results?*
6. *Are the roles defined clearly and responsibilities understood?*

7. *What actions have you taken if patching is not possible?*
8. *How you would rate the communication between vulnerability reporting teams and patching teams?*
9. *Have you had any security incidents related to a vulnerability?*
10. *Let's look at the graphs. What is your opinion and what you would like to improve?*

Open dialogue

1. *In your view the things in the whole process that is well?*
2. *What are the three main obstacles that hinder your progress the most?*