Bachelor's Thesis

Information and Communications Technology

2024

Vertti Rantalaiho

Technical Implementation and Operational Enhancements of a Vulnerability Management Tool in an Organization

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2024 | 87 sivua

Vertti Rantalaiho

Haavoittuvuudenhallintajärjestelmien tekninen implementointi ja operatiiviset kehitykset organisaatiossa

Opinnäytetyössä tutkittiin haavoittuvuudenhallintajärjestelmien käyttöönottoa ja kehittämistä organisaatioissa, jossa erityisesti keskityttiin tehokkuuteen kasvavien kyberturvallisuusuhkien luomien paineiden keskellä. Työn tavoitteena oli tunnistaa parhaat käytännöt, jotka tukevat näiden järjestelmien käyttöönottoa ja varmistavat niiden mukautuvuuden sekä tehokkuuden pitkällä aikavälillä, kiinnittäen erityishuomiota kunkin organisaation ympäristön ainutlaatuisiin vaatimuksiin.

Tutkimuksessa käytettiin kvalitatiivisia menetelmiä, analysoiden tapaustutkimuksia, dokumentaatiota sekä kirjallisuutta kyberturvallisuuden ja haavoittuvuudenhallinnan alueelta. Tämän lähestymistavan avulla pystyttiin tutkimaan teoreettisia perusteita sekä niiden käytännön soveltuvuutta, pyrkien kaventamaan teorian ja käytännön välistä kuilua. Havaintojen perusteella voidaan sanoa, että on tarpeellista löytää tasapaino perustason operatiivisten vaatimusten ja edistyneiden ratkaisujen välille. Lisäksi kirjallisuudessa korostettiin strategisen, joustavan lähestymistavan merkitystä haavoittuvuudenhallinnassa. Tämä sisältää jatkuvan teknisen kehityksen ja aktiivisen sidosryhmien osallistumisen, jotka ovat välttämättömiä muuttuvassa kyberturvallisuuden uhkaympäristössä.

Avainsanat:

Kyberturvallisuus, tietoturva, haavoittuvuus, haavoittuvuudenhallinta

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2024 | 87 pages

Vertti Rantalaiho

Technical Implementation and Operational Enhancements of a Vulnerability Management Tool in an Organization

This thesis explored the implementation and enhancement of IT vulnerability management systems within organizations, where the focus was especially on developing both effective and tailored to specific organizational needs in increasing cybersecurity threats. The objective was to identify best practices for deploying these systems and ensuring their adaptability and effectiveness over time, with a particular emphasis on customization for diverse organizational environments.

Employing a qualitative approach, the study combined case study analyses with a review of current literature and documentation on cybersecurity and vulnerability management practices. This allowed for an in-depth examination of both theoretical principles and their practical application, aiming to bridge the gap between concept and execution. Key findings highlighted the importance of balancing fundamental operational requirements with advanced solutions and underscored the need for a strategic, adaptable approach to vulnerability management. This involves continuous technical improvement and active stakeholder engagement to navigate the evolving landscape of cyber threats effectively.

Keywords:

Cybersecurity, data security, vulnerability, vulnerability management

Content

Figures

Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
CIA	Confidentiality, Integrity and Availability
CISA	Cybersecurity and Infrastructure Security Agency
CRR	Cyber Resilience Review
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized Zone
GPO	Group Policy Object
GUI	Graphical User Interface
IT	Information Technology
ICS	Industrial Control Systems
ITSM	Information Technology Service Management
KPI	Key Performance Indicator
ML	Machine Learning
NSG	Network Security Group
OT	Operational Technology
PoC	Proof of Concept
PII	Personally Identifiable Information
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement

SIEM	Security Information and Event Management
TCP	Transmission Control Protocol
UEBA	User and Entity Behavior Analytics
UDP	User Datagram Protocol
UX	User Experience
VM	Vulnerability Management
Q&A	Question and Answer

1 Introduction

In the evolving landscape of cybersecurity, the escalating frequency and composure of cyber threats pose a real challenge to organizations seeking to secure their digital assets. Vulnerability management (VM) emerges as a critical component in the arsenal against these threats, demanding attention, and effective implementation.

This thesis is conducted as Fortum Oyj as its commissioner, a leading organization in the energy sector across the Nordics and Europe. This topic was chosen due to the increasing frequency and severity of cyber-attacks, highlighting the need for comprehensive vulnerability management, but also from personal engagement in the cybersecurity landscape at Fortum.

Through direct involvement in the deployment of a vulnerability management system from the ground up within Fortum, hurdles of technical and organizational challenges have been encountered and navigated. These experiences have afforded a unique perspective on the subject, blending professional responsibilities with a personal journey in cybersecurity. The content and direction of the thesis are deeply intertwined with work at Fortum, detailing the initial steps required for the tool's effective implementation, subsequent operational enhancements to refine its utilization, and the development of a future continuous improvement plan for the service. This approach ensures that the thesis does not only address the theoretical aspects of vulnerability management but also reflects practical insights and strategies derived from real-world implementation within a leading entity in the energy industry. Furthermore, this thesis is committed to maintaining a technical focus, in alignment with Fortum’s broader strategy on vulnerability management.

The motivation behind this research is two-fold: to contribute to the broader understanding of how organizations can navigate the difficulty of vulnerability management, from initial implementation to sustained operational effectiveness, and to share the practical lessons and insights gained from direct experience in the field. This study aims to bridge the gap between theoretical frameworks and

real-world application, highlighting the importance of a technical approach and continuous improvement in vulnerability management.

1.1 Research Questions

The research questions are as followed:

1. How can organizations implement a vulnerability management system, considering both basic requirements and best practice solutions, and what are the critical factors influencing successful integration into existing infrastructures?
2. What measures and attributes are essential for ensuring the sustained operational effectiveness of a vulnerability management system, addressing potential changes and future developments in the organizational landscape following the initial implementation?
3. How can organizations adopt technical continuous improvement in vulnerability management, incorporating feedback mechanisms and continuous development based on the organization's needs and user feedback?

1.2 Justification, Relevance, and Overview of Source Material

The choice of vulnerability management as a focal point is justified by the nature of protecting organizations against cyber threats. A critical analysis of existing literature reveals a gap in understanding the comprehensive implementation and ongoing effectiveness of vulnerability management systems within organizational contexts. By critically examining key source materials, it is aimed to identify and clarify these gaps, raise thoughts, and connect the work to previous knowledge and publications on the subject.

1.3 Objectives, Content Areas, and Hypotheses

This thesis's main objective is to provide practical implementation and enhancement recommendations for organizations to improve their vulnerability management capabilities. It is aimed to achieve this by:

- Investigating different stage technical implementation methods, considering both basic and best practices.
- Suggesting ways for operational enhancements, addressing integration surfaces, and adapting to organizational changes.
- Suggesting a method to continuously improve technology to foster a culture of ongoing enhancement in managing vulnerabilities.

The content areas will encompass the technical implementation strategies, operational enhancements, and continuous technical improvement practices within vulnerability management. The hypotheses are grounded in the belief that a well-structured and adaptable vulnerability management system, aligned with organizational goals and infrastructure, can significantly enhance an organization's cybersecurity resilience.

1.4 Structure of the Thesis

The subsequent chapters will delve into each aspect outlined in the research questions. Chapter 2 will establish the foundational understanding of vulnerability management, its principles, and its importance in cybersecurity. Chapter 3 will adopt a tool-agnostic approach, examining core tool capabilities and organizational considerations. Chapters 4 and 5 will focus on the organizational assessment, planning, and various implementation methods. The subsequent chapters will explore operational enhancements, continuous technical improvement strategies, and conclude with a conclusion with answers to the research questions and what to expect from the future. Chapters 5 and 6 are also established in a way that they are separately readable if the reader is only interested in technical implementation or operational enhancements.

By incorporating this structured review, source criticism is applied, and significant other research and documentation that have influenced the direction and content of this work are referenced. For example, Tom Palmaers' study for the SANS Institute in 2013, "Implementing a Vulnerability Management Process," focuses on designing and implementing a vulnerability management process within an organization. Palmaers' work emphasizes not just the technological aspects but the importance of a foundational vulnerability management process that can be easily adapted and implemented in any part of the organization. (Palmaers, 2013) The Cyber Resilience Review (CRR) Supplemental Resource Guides published by Carnegie Mellon University in 2016, developed in collaboration with the Department of Homeland Security (DHS), provide comprehensive insights into various cybersecurity areas, such as vulnerability management (Carnegie Mellon University, 2016d), risk management (Carnegie Mellon University, 2016b), and training and awareness (Carnegie Mellon University, 2016c). These guides discuss the development and enhancement of operational resilience capabilities for critical IT services, which are in this case applicable to vulnerability management. Additionally, to this, a lot of different service providers’ technical documentation has been used to construct the information of this thesis.

2 Fundamentals of Vulnerability Management

This segment serves as a bridge, transitioning from the broader context established in the introductory chapter to a brief examination of vulnerability management's conceptual framework, operational principles, and its important role in protecting an organization's cyber ecosystem. It aims to provide a thorough understanding of vulnerability management, essential for navigating the complex landscape of cybersecurity threats.

2.1 Definition and Principles

In the world of cybersecurity, vulnerability management is a crucial strategic process that entails identifying, evaluating, remediating, and monitoring security vulnerabilities within an organization's systems and software. This proactive approach is essential for safeguarding digital assets against potential exploits and cyber-attacks, highlighting the importance of a comprehensive vulnerability management strategy in maintaining the integrity, confidentiality, and availability of data and systems.

2.1.1 Vulnerability Management Defined

Vulnerability management is the systematic process aimed at controlling vulnerabilities in organizational technologies and information systems. It plays a critical role in preventing unauthorized access and potential data breaches by identifying weaknesses that could be exploited by cyber threats. Failure to implement effective vulnerability management can lead to significant security incidents, financial losses, and damage to an organization's reputation. In an IT environment and broader organizational context, effective vulnerability management ensures the resilience and continuity of operations against a backdrop of evolving cyber threats. (Microsoft, 2023d)

2.1.2 Core Principles

Tackling the terrain of vulnerability management requires adherence to a set of core principles. These principles encompass:

1. Proactive Identification: Vulnerability management demands an approach to scanning that extends beyond surface-level assessments. It involves advanced scanning techniques capable of finding latent vulnerabilities that might otherwise go unnoticed. This principle also emphasizes predictive analysis to anticipate and address emerging threats, underscoring the importance of staying ahead of potential adversaries. (Desai, 2023)
2. Vulnerability and Risk Assessment: Vulnerabilities exist within a contextual framework. To effectively manage them, organizations must conduct nuanced vulnerability and risk assessments, since assessing vulnerabilities in their context helps understand their potential exploitability and the risks they pose. Such as assessments ensure resources are prioritized and directed towards vulnerabilities that pose the greatest threat. A balanced evaluation of a vulnerability's characteristics, combined with its potential impact within the specific organizational context, is paramount. (Mathenge, 2020)
3. Prioritization of Risks: Resource allocation within vulnerability management should be a strategic and analytical process. This principle entails developing a hierarchical model for prioritizing threats, aligning with the organization's risk appetite, and considering operational realities. By categorizing vulnerabilities based on their potential impact, organizations can allocate resources effectively to address the most critical risks (Paskoski, 2022b).
4. Remediation and Mitigation: Remediation and mitigation strategies extend beyond simple fixes. Effective vulnerability management requires intelligent solutions that optimize resource allocation and effectiveness. It involves a blend of technical interventions, adjustments to organizational policies, and sometimes, creative problem-solving to address

vulnerabilities in the most efficient and effective manner. (Sitcawich, 2020)

5. Continuous Monitoring: In an evolving threat landscape, continuous monitoring is the key to adaptability and resilience. It represents a systematic approach to keep the vulnerability management process coordinated with new developments in both the threat environment and technological advancements. Embracing continuous monitoring ensures that organizations can promptly identify and respond to emerging threats. (Ideboen, 2021)

Figure 1 below visualizes the vulnerability management lifecycle, closely mirroring the core principles detailed above. It starts with 'Discover', reflecting 'Proactive Identification' through advanced scanning. 'Assess' and 'Prioritize' depict the assessment and ranking process of vulnerabilities. 'Report' ensures findings are effectively communicated, while 'Remediate' aligns with the strategies of addressing identified issues. 'Verify' encapsulates 'Continuous Monitoring', crucial for validating remediation and beginning the VM lifecycle from the beginning again.

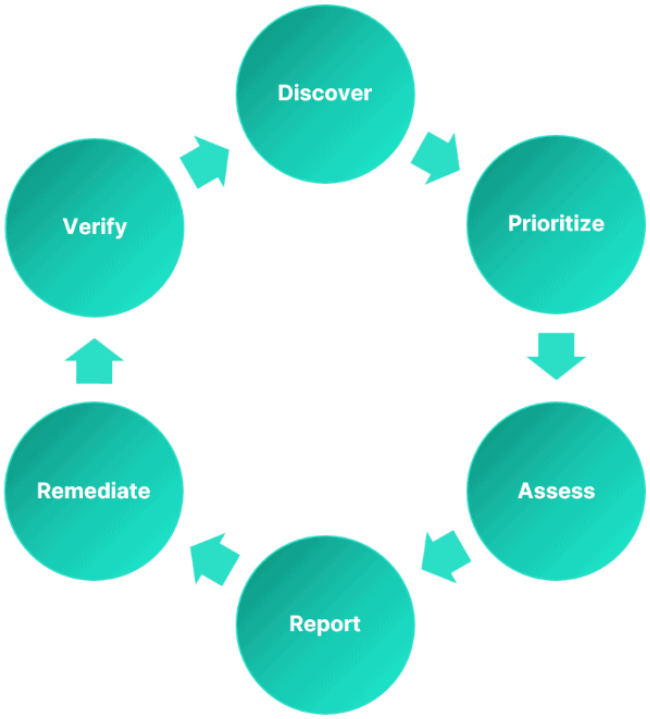

Figure 1. Vulnerability Management Lifecycle. (Digby, 2024)

2.2 Importance in Cybersecurity

Effectively managing vulnerabilities is similar to putting up a strategic shield that protects organizations from a large number of cyber threats. It goes beyond defending against attacks; it is about creating a resilient and responsive infrastructure that not only repels intruders but also reduces the probability and potential impact of security incidents. In an era marked by cyber threats, vulnerability management emerges as an essential side of a proactive cybersecurity posture. (SecurityScorecard, 2024)

In a landscape characterized by strict regulatory requirements and international standards such as NIST, ISO 27001, and SOC2 (Vulnera, 2023), vulnerability management is not only recommended but often required to ensure an organization's compliance with legal and industry-specific mandates. This adherence to regulatory frameworks is essential in establishing a secure and responsible data environment, enabling organizations to mitigate risks effectively. By implementing vulnerability management practices as stipulated by these standards, organizations can demonstrate their commitment to data security and, as a result, gain a competitive advantage in their respective fields. (Faistauer, 2021)

Building and maintaining trust with stakeholders, including customers, partners, and regulatory bodies, depends on a proactive and transparent vulnerability management strategy. Such a strategy signifies a commitment to protecting not only an organization's assets but also the data and privacy of its stakeholders. By highlighting dedication to security and privacy, organizations can instill confidence, solidify relationships, and strengthen their reputation. (Rohrs and Wolf, 2022)

3 Tool Agnostic Approach

When trying to accomplish effective vulnerability management, a tool agnostic approach is often advocated to accommodate the diverse requirements and challenges faced by organizations. This chapter introduces common core capabilities of vulnerability management tools and touches on where the future of the tools is heading and what features different size organizations must emphasize when deciding on the tool to use.

3.1 Introduction to Tool Capabilities

In addressing the complexity of vulnerability management, adopting a tool agnostic approach is pivotal. This perspective not only accommodates diverse organizational requirements but also underscores the importance of selecting a tool based on its merits and alignment with specific needs. (OWASP, 2020) This section elucidates the core capabilities of vulnerability management tools like Rapid7's InsightVM, Tenable Vulnerability Management, and others, chosen specifically to gain a thorough understanding of the core capabilities available in the market.

3.1.1 Core Capabilities of Vulnerability Management Tools

Comprehensive Vulnerability Management

The market offers tools from specialized vulnerability scanners to comprehensive integrated management platforms, each embedded with features that cater to diverse operational and cybersecurity maturity levels. The scanning accuracy and coverage of vulnerability management tools are very important in assessing their effectiveness and quite similar in all tools due to their importance. Advanced scanning capabilities, powered by sophisticated algorithms, enable these tools to detect vulnerabilities across a variety of systems and applications, illustrating the breadth and depth of vulnerability

identification and assessment essential for robust cybersecurity management (Rapid7, 2023a).

Integration with IT and Security Processes

The integration of vulnerability management tools with existing IT and security infrastructures is a critical factor for enhancing operational efficiency and establishing a cohesive cybersecurity infrastructure. Such integration capabilities are pivotal for enabling effective threat response mechanisms and reducing the manual administrative burden, thereby enhancing an organization's agility and responsiveness to emerging threats. (Chopskie, 2023) For instance, InsightVM's compatibility with over 40 technologies illustrates the importance of flexible integration capabilities. (Rapid7, 2024g)

Customization and Scalability

As organizations evolve, so do their security needs. Tools that offer extensive customization and scalability ensure they can adapt over time. The ability to tailor tools through APIs and other mechanisms such as internal automation through workflows (Rapid7, 2024p.), supports this adaptability, ensuring tools remain effective against the backdrop of a changing cybersecurity landscape. (Miehe, 2023)

User Experience (UX)

The design and functionality of user interfaces are important for maximizing the efficiency and effectiveness of vulnerability management tools. A focus on usability is great for ensuring that these tools deliver maximum value, facilitating user engagement and operational efficiency. (Signiant, 2024)

Advanced Reporting and Analytics

Advanced reporting and analytics capabilities are essential in vulnerability management, transforming raw data into actionable insights. Such functionality is integral to organizations as it provides clarity on the cybersecurity landscape, facilitating informed decision-making. With modern tools, organizations benefit

from detailed analyses that drive strategic planning, helping prioritize remediation efforts effectively. This does not only conclude with decision-making but also extends to guiding and triggering appropriate actions, ensuring that resources are allocated efficiently, and security measures are enacted precisely where needed most. (NCSC, 2020)

3.1.2 Importance of Key Features and Future of VM Tools

The significance of these features lies in their collective contribution to a robust and proactive vulnerability management strategy. Comprehensive vulnerability management ensures thorough risk identification, while integration capabilities facilitate a cohesive security posture. Customization and scalability allow the tool to evolve within the organization, ensuring long-term viability. An intuitive UX ensures widespread adoption and maximizes the utility of the tool, and advanced reporting and analytics drive informed decision-making and strategic prioritization of security efforts.

The future direction of vulnerability management tools is characterized by significant innovations, including the integration of artificial intelligence (AI), machine learning (ML), and predictive analytics. These advancements signify a shift towards more automated, intelligent vulnerability management strategies that not only react to identified threats but also anticipate potential vulnerabilities. This proactive approach is very important for offering advanced protection and resilience in an increasingly complex and dynamic cybersecurity landscape (Bowen, Frank, and Golden, 2021).

3.2 Organizational Suitability

In evaluating the suitability of vulnerability management tools for different organizational types, it's essential to consider the specific context of each organization, including size, industry, technological infrastructure, and regulatory requirements. The choice of a vulnerability management tool should

not be based solely on organizational size but also on the unique challenges and requirements each entity faces.

For SMEs, while simplicity, ease of use, and cost-effectiveness are important considerations, it's also crucial to recognize that some small organizations may face stringent regulatory and compliance requirements. Therefore, tools that offer straightforward integration capabilities, scalability to accommodate growth, and features that support compliance are necessary. Scalability and cost-effectiveness remain critical considerations, but without compromising the tool's ability to meet regulatory demands. (Vishwakarma, 2023)

Large organizations, with their complex and distributed IT environments, require tools that provide extensive integration options and advanced reporting and analytics to navigate regulatory landscapes effectively. Such entities benefit from customization capabilities, allowing them to tailor tools to their specific operational and regulatory needs, ensuring compliance and security across a larger scale. (Dildy, 2017)

Startups and cloud-first companies, despite their agility and dynamic development practices, must also consider regulatory compliance and data protection as crucial factors in their tool selection process (Arora, 2023). Prioritizing tools with strong cloud integration capabilities and flexibility to adapt to rapid deployment cycles is essential. These tools should support modern infrastructure demands, including containerized environments and IoT devices, while ensuring compliance and data security. (Paskoski, 2022a)

By taking into account the organization's size, regulatory requirements, and specific cybersecurity challenges, entities can select vulnerability management tools that best fit their needs, ensuring effective protection and compliance across different organizational landscapes.

4 Organizational Assessment and Planning

This chapter focuses on the critical importance of organizational assessment and planning in the context of vulnerability management. Highlighting the steps necessary for conducting comprehensive risk assessments, this section guides readers through methodologies to identify key steps in risk assessment. Additionally, the chapter touches on tailoring a vulnerability management plan for the organization’s needs, considering key components, consideration and continuous review and adaptation.

4.1 Conducting Risk Assessment and Understanding Its Impact

Risk assessment is a cornerstone of effective vulnerability management, providing a structured approach to identify and address cybersecurity risks within an organization. It's a systematic process that involves identifying the vulnerabilities within IT assets, evaluating the potential risks associated with these vulnerabilities, and then prioritizing them based on their potential impact on the organization. This process aids in the strategic allocation of resources to safeguard critical assets and supports informed decision-making. (Evrin, 2021)

Risk assessment is about comprehending the potential negative outcomes and the opportunities that various risks present to IT assets. It's a proactive strategy designed to enable organizations to foresee and address threats before they evolve into significant security incidents. This involves more than just an assessment of the technological aspects; it also requires an understanding of the broader business context in which these IT asset's function. By doing so, organizations can assess the true impact of potential vulnerabilities on their operations and objectives, guiding effective mitigation strategies. (Schmittling and Munns, 2010)

Moreover, risk assessment recognizes that not all vulnerabilities will or can be mitigated fully. In some cases, security incidents are allowed to occur because the assessed impact is deemed minimal or non-existent. This decision-making process is informed by the risk assessment, which not only identifies potential

threats but also evaluates the effectiveness of existing controls and the need for new controls. It's a nuanced process that balances the cost and feasibility of mitigation efforts against the potential impact of threats, allowing organizations to focus on the most critical vulnerabilities that could impact their core operations and assets. This strategic approach ensures that vulnerability management efforts are both efficient and aligned with the organization's risk tolerance and business goals. (Evrin, 2021)

4.1.1 Key Steps in Risk Assessment

Risk assessment is an integral component of vulnerability management, addressing risks specifically arising from vulnerabilities within an organization's IT infrastructure. It is a continuous and cyclic process that ensures vulnerabilities are effectively managed and mitigated. The following are the fundamental steps in the risk assessment process, as represented in the accompanying figure:

1. Asset Identification: This foundational step involves cataloging all IT assets within the organization, which includes not only hardware and software but also data repositories and any other digital resources that could be affected by vulnerabilities. (RiskOptics, 2023)
2. Vulnerability Identification: While scanning tools like Rapid7, Tenable, and Qualys are common methods for identifying vulnerabilities, organizations also leverage other sources like CERT-FI advisories (Traficom, 2024), CISA alerts (CISA, 2024), vendor announcements, and industry-specific vulnerability databases. (NIST, 2019)
3. Impact Analysis: Once vulnerabilities are identified, the next step is to assess their potential impact on business operations. This involves understanding how the exploitation of a vulnerability could affect confidentiality, integrity, and availability of IT assets and the resulting impact on business processes. (Evrin, 2021)
4. Likelihood Determination: This involves estimating the probability of each identified vulnerability being exploited by threat actors. Factors such as

the complexity of exploitation, availability of exploit tools, and presence of mitigating controls can influence this likelihood. (Evrin, 2021)

5. Prioritization: The final step is to rank vulnerabilities based on their potential impact and the likelihood of exploitation. This prioritization helps in allocating resources more effectively, focusing on remediating vulnerabilities that pose the greatest risk to the organization. (Chatterton, 2023)

Figure 2 below illustrates these key steps in a cyclical pattern, emphasizing the repetitive nature of the risk assessment process. This continuous loop reflects the ongoing nature of vulnerability and risk management, where after the implementation of remediation actions, monitoring continues, feeding back into the identification stage to begin the cycle anew. This visual representation clarifies how each stage flows into the next, creating a systematic approach to managing the risks associated with IT vulnerabilities.

Figure 2. The Operational Risk Management Life Cycle. (Boddam-Whetham, 2023)

4.1.2 Risk Assessment Tools and Techniques

To support the risk assessment process, organizations can employ a range of tools and techniques that prioritize vulnerabilities effectively, recognizing that it is impractical to perform in-depth risk assessments for every vulnerability identified by scanning tools:

- Automated Tools: These tools are instrumental in categorizing and suggesting the prioritization of vulnerabilities, allowing organizations to adopt a more operationally efficient approach to risk assessment. By following the recommendations provided by these tools, combined with business impact, organizations can concentrate on remediating vulnerabilities that have a higher likelihood of being exploited and may cause more significant impact, based on objective criteria such as CVSS scores and the tool's internal algorithms. (Ballejos, 2024)
- Risk Assessment Methods: Both qualitative and quantitative risk assessment methods are utilized to gain a nuanced understanding of risks. Qualitative methods involve scenario-based analysis using simple scales to evaluate risks based on perception or judgment. Quantitative methods, on the other hand, rely on mathematical and statistical models to provide objective numerical values, offering a data-driven approach to risk evaluation. (Evrin, 2021)

By integrating these tools and methods, organizations ensure that risk assessments are conducted efficiently and effectively, focusing on the most critical vulnerabilities while also considering the operational realities and constraints. (Ballejos, 2024)

4.2 Tailoring a Vulnerability Management Strategy

The development and refinement of a vulnerability management strategy is critical for establishing a robust and resilient cybersecurity posture for an organization. This strategy must be tailored to the organization's specific needs, considering factors such as operational context, size, industry, and risk profile.

A well-designed strategy serves as a strategic guide through various stages: from discovery and assessment to remediation and continuous monitoring of vulnerabilities. (Dudley, 2021)

A customized vulnerability management strategy addresses the distinct challenges and requirements of an organization, encapsulating an approach that aligns with the organization's unique operational nuances and risk appetite. This ensures the strategy is not only effective in mitigating risks but also efficient in the use of resources. Such a strategy lays the foundation for effective vulnerability management, guiding the organization through the complexities of cybersecurity and ensuring ongoing protection against emerging threats. (Dudley, 2021)

4.2.1 Key Components of a Vulnerability Management Strategy

The vulnerability management strategy consists of several key components that collectively ensure a comprehensive approach to managing cybersecurity risks:

- Scope and Objectives: This defines the boundaries and primary goals of the vulnerability management program, ensuring all stakeholders understand what the program aims to achieve. (Clearfin, 2021)
- Roles and Responsibilities: Clear definitions of responsibilities across the organization are crucial for the effective execution of the vulnerability management strategy. This ensures accountability and efficient management of vulnerability-related tasks. (TraceSecurity, 2018)
- Resource Allocation: Determining the necessary tools, personnel, and budget is essential for the strategy's successful implementation. This includes selecting appropriate vulnerability management tools and allocating skilled personnel to manage and execute the strategy. (GanttPRO, 2021)
- Implementation Timeline: Establishing a realistic timeline for the deployment of the vulnerability management strategy is critical. This

timeline should consider the complexity of implementation and the organization's capacity for change. (Fitzgerald and Rubbinaccio, 2023)

- Policies and Procedures: Developing comprehensive guidelines and procedures for regular vulnerability scanning, risk assessment, and remediation activities ensures consistency and effectiveness in managing vulnerabilities. (OWASP, 2020)
- Incident Response Plan Integration: Integrating the vulnerability management strategy with the organization’s broader incident response plan ensures a coordinated and rapid response to security incidents that arise from vulnerabilities, safeguarding continuity and reducing the impact of such events. Additionally, this integration allows for lessons learned to be fed back into the vulnerability management process, improving its effectiveness and responsiveness. (Gorecki, 2020)

The successful implementation of a vulnerability management strategy relies on the seamless interplay of these components. It is a holistic process that not only establishes a defensive posture against current threats but also evolves to address future challenges. By considering these elements, organizations can build a dynamic and responsive framework.

4.2.2 Considerations for Strategy Development

When developing a vulnerability management strategy, several considerations should be considered to ensure its effectiveness:

- Organizational Size and Complexity: The strategy should be tailored to the size and complexity of the organization, with more streamlined processes for smaller organizations and more detailed plans for larger ones. (Carnegie Mellon University, 2016c)
- Regulatory Compliance: The strategy must align with industry-specific regulatory requirements, ensuring the organization remains compliant with relevant laws and standards. (Carnegie Mellon University, 2016c)

- Cultural Fit: The strategy should be adapted to fit the organization's culture and operational style, ensuring it is embraced by all stakeholders and effectively integrated into daily operations. (Carnegie Mellon University, 2016c)
- Vendor Remediation Obligations: Acknowledging the role of external vendors in the vulnerability management ecosystem is critical. Contracts should specifically demand that vendors tasked with providing vulnerability remediation services commit to timely and effective resolution of identified vulnerabilities. (Carnegie Mellon University, 2016c)

Incorporating these considerations into the development of a vulnerability management strategy ensures a robust, compliant, and culturally aligned approach.

4.2.3 Continuous Review and Adaptation

The cybersecurity landscape is constantly evolving, making regular reviews and updates necessary to the vulnerability management plan. This continuous review process ensures the plan remains relevant and effective in addressing new threats and adapting to organizational changes. Emphasizing continuous vulnerability management, the plan should enable the organization to swiftly acquire, assess, and act on new information, minimizing the window of opportunity for attackers and ensuring ongoing protection against emerging threats. (Ideboen, 2021)

5 Technical Implementation of Vulnerability Management Tools

This chapter delves into the nuanced decisions and steps involved in effectively deploying these tools, from selecting the appropriate technology to configuring it to fit an organization's infrastructure and requirements. The chapter outlines two implementation methods, from basic configurations to best practice approaches, and discusses the implications of each for organizational security. By providing a comprehensive overview of how to practically apply the strategies and principles previously touches on, this chapter aims to equip organizations with the knowledge needed to enhance their cybersecurity posture through the implementation of vulnerability management tools.

5.1 Basic Implementation Method

The Basic Implementation Method offers a streamlined approach for organizations with limited resources to implement a vulnerability management tool effectively. This method prioritizes essential cybersecurity measures while balancing resource constraints.

5.1.1 Understanding the Infrastructure

The foundation of implementing a vulnerability management tool into your organization lies in understanding the standard requirements and architecture of your organization’s infrastructure. Before making any mandatory changes for the maximum benefit of the tool, there must be a proper understanding of the organization's digital structure and of what is wanted to be achieved. (Palmaers, 2013)

When thinking of what is needed in an implementation scenario, understanding the minimal yet sufficient hardware specification required to support the chosen vulnerability management tool is needed. These specifications include server

capabilities, which should align with the tool's processing and data storage demands. The server must have adequate processing power to handle the computational load and sufficient storage capacity for data retention and logs. The need for these features increases linearly with the organization's size of technical infrastructure. (ManageEngine, 2024b)

A large part of different tools on the market are hosted on the vendor's cloud, but some essential features like scan engines—dedicated software components designed to perform security scans within networks to detect vulnerabilities—databases and security consoles are still recommended to be hosted in your own environment to streamline the effectiveness and use of the service. Organization policies and standards may limit what can be done through the public internet. Vulnerability scanning is also recommended to be done internally in an organization on assets to find the internal threats available, and externally with externally provided scan engines on internet-facing assets. (PWC, 2022)

When acquiring a tool, compatibility and seamless operation between other software and the tools software must be carefully reviewed. Certain software like antivirus programs should be carefully examined when implementing a vulnerability management tool. Tools like these are often already compatible with antivirus software or they can be separately allowlisted. Obsolete software interfering with the tool should be removed or updated. (Rapid7, 2024h)

Special attention is given to the cost-effectiveness of these selections. For organizations with limited budgets, cheaper open-source options with less customization like integration capabilities, might provide viable alternatives without compromising essential functionalities. The goal is to create a strong yet economical infrastructure that supports the effective implementation of the vulnerability management tool. (Cole, 2022)

5.1.2 Configuring the Network for Vulnerability Management

A secure and well-configured network is fundamental to the successful implementation of a vulnerability management tool. The technical setup of the network should include establishing adequate firewalls that can manage incoming and outgoing traffic. The configuration of these firewalls is mandatory for the needed functions of the vulnerability management tool to work properly.

The essential network openings needed for proper vulnerability scanning will be discussed below. If the VM platform is hosted entirely in the cloud by the service provider, then none of the following openings are needed. Due to organizations typically having different policies and directives in use, the subsequent instructions are provided for scenarios where the vulnerability management tool or console is hosted internally. Although all the next steps would not apply if the console were hosted externally, they could still be followed to inform about VM tool implementation. The architecture figure 3 provided below can be followed for a visual representation of the required network openings and configurations necessary for an internally hosted vulnerability management setup.

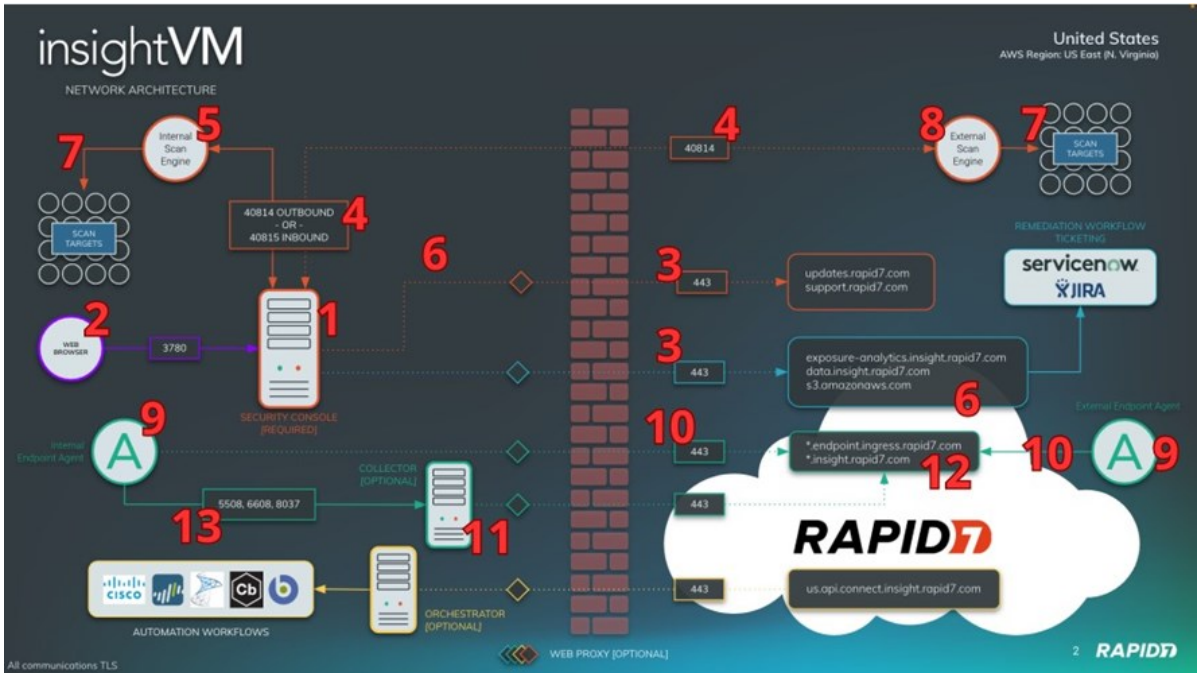

Figure 3. Reference Architecture Example of VM Tool's Port and Firewall Openings with numbers. (Rapid7, 2023b)

The vulnerability management tool's main feature from where all the actions are run from, is called (1) the console. The console's network openings are crucial to be on point since the console requires different connections to work properly. The console's (2) web graphical user interface (GUI) is developed by the service provider and usually requires access to the internet to install properly. These consoles and their connections are usually managed by (3) outbound connections, where the console often uses APIs through port 443 to fetch update information and a (4) designated port internally to communicate with (5) internal scan engines. Also, if the console is hosted internally, but part of the service is hosted in the (6) service provider's cloud, an outbound connection must be configured for proper communication. Outbound connections from the console to the service provider's cloud are also needed to collect vulnerability data of assets that have an agent installed in them. (Tenable, 2024c)

The scan engines of the vulnerability management tool require connectivity between the console and the engine to work properly. This is usually done by either opening an engine to console connection where the scan engine will actively inform the console that it is available for communication or a console to engine connection where the scan engine listens for communication from the console to start the scanning. The first option is usually recommended, because of its capabilities of sending its live status to a tracking tool to check the scan engine's status. (Rapid7, 2024e)

To achieve a scan that gathers any vulnerability data, (7) connections between the scan engine and the assets need to be established. If these are not established, only open public ports can be scanned, which limits the depth of vulnerability detection to what is externally visible, potentially missing internal vulnerabilities that could be exploited once an attacker gains access. When allowlisting any/any connections for the scan engine's IP, the scan engine can confidently scan any TCP/UDP ports on the asset and gather vulnerability data. Assets owned by the organization but hosted outside the organization network e.g., assets hosted by a vendor, in best practice, should be scanned with an (8) external scan engine (either hosted by the service provider or internally) that

can scan public internet facing IP addresses. This approach highlights the importance of fortifying the outer layer of the organizational "onion," ensuring enhanced protection where it is most visible and potentially vulnerable to attackers. The scan engine can in this scenario also be allowlisted to not be blocked by set firewalls, but if this is not done, the scan engine replicates how an attacker would scan the target. If the organization wants vulnerability data from inside the externally hosted network, hosting a scan engine on that network is mandatory. (Rapid7, 2024l)

Almost every vulnerability management tool tries to utilize software components known as (9) “agents” to achieve more accurate vulnerability data from an organization’s environment. For these agents to work, they need their communication to be allowed inside the network through various endpoints. Due to the agents working like software components that monitor and report on the security posture of their host systems, (10) usually through port 443, they need to have connection to the cloud either directly or by (11) a proxy, which acts as an intermediary for data transmission, enhancing security and control. The endpoints usually consist of provided (12) DNS’s or static IP addresses that can be allowlisted for the needed connections. These connections are mandatory for the agent to be able to send data out to the cloud and vulnerability management platform, get software updates and upload needed data and logs. (Tenable, 2024b)

If a package for (11) the proxy is available, it is provided by the service provider. This is a way for (10) the agent to connect to the cloud to send vulnerability data of the asset and for the agent to retrieve updates. The proxy needs a (13) connection to be opened between the agent and the proxy and the same ports and endpoints need to be allowlisted than in the agent scenario mentioned above. (Tenable, 2024d) This is usually configured and taken into use if the asset is prohibited to access the internet or the cloud directly e.g., due to the location of the asset being in contact with e.g., industrial control systems (ICS) in a demilitarized (DMZ) zone. (Rapid7, 2024l)

5.1.3 Basic Vulnerability Scan Configurations and Reporting

A way to scan the organization's assets is an essential requirement. There are multiple ways of scanning an asset, and the most common ways are agent-based, credential-based and network-based scanning. (Fortra, 2023) Two out of three of these scanning methods include utilizing the scan engine for acquiring the scan results and one lightweight software, working as a beacon to send data of the system to the vulnerability management platform. Usually these agents acquire 80-90% of the vulnerabilities on an asset, when credential-based scanning, utilizing a scan engine, only finds vulnerabilities that the credentials have access to, and less efficiently. Network-based scanning covers the outer surface of the asset, scanning its ports and vulnerable software from the outside, usually offering the rest of the vulnerability data, that the agents cannot see. (Wallis, 2022) Usually when using credential-based scanning on an asset, an outer and inner scan is configured in the same scan configuration, when on an agent-based scan method, an outer scan must be configured separately. (GeeksforGeeks, 2022)

The deployment strategy of agents, integral to the server maintenance processes, varies based on the organization's size, structure, and the extent of outsourced services. In smaller organizations, agents can be manually installed or deployed through basic script-based methods, such as PowerShell scripts. For larger organizations, agent deployments may require coordination with internal IT maintenance schedules or external vendor support to ensure seamless integration and minimal disruption to ongoing operations. This approach aligns the deployment of vulnerability management tools with the organization's broader server maintenance and IT management strategies, ensuring consistency and efficiency across IT practices. (Rapid7, 2024j)

In credential-based scanning application or asset owners need to make credentials to the asset for the scan engine to get access for vulnerability scanning. This can either be done with a centralized solution, as in a local admin account that can access many assets owned by the same asset owner.

(GeeksforGeeks, 2022) To have this and network-based scanning working properly, an organization needs to apply network ruling correctly between the scan engines and assets to achieve connectivity. Network configurations need to be configured in such a way that the IP address of the scan engine is allowlisted on each asset needed to be scanned. (Rapid7, 2024l) If an asset being scanned is hosted in the cloud, network security groups (NSGs) may also need configuration changes. (Microsoft, 2023a)

When initially tackling the scan configurations, there are usually ready-made scan template configurations that can be used for initial scans of the environment. Often so-called Audit-scans are used for scanning an asset for vulnerabilities and Discovery-scans are used for initially finding assets in your network and populating these into your platform. This is also a great way to know your situation about available assets on the network, without agents installed or scans configured. (Tenable, 2024e)

Basic reporting mechanisms should be enabled and linked to certain scan results, providing important vulnerability data to an asset owner. The vulnerability reports can be e.g., automatically sent to an asset owners' email or the service can be customized into a self-managed service, where asset owners are able to access the vulnerability management tool and check the vulnerability information for themselves, or even create their own customized reports. (Rapid7, 2024f)

5.2 Best Practice Implementation Method

The more optimal way of implementing a vulnerability management tool in this thesis, will be named "Best Practice Implementation Method", to represent a more extensive approach to implementing a vulnerability management tool, suitable for organizations with greater resources aiming for a robust cybersecurity posture. This method aims to integrate advanced technologies and involve a broader scope of organizational involvement. (Firch, 2023)

5.2.1 Advanced Infrastructure and Integration

Conducting a detailed analysis of the organizational infrastructure is crucial when implementing a vulnerability management tool. This involves not only extensive understanding of an organization's current digital and network architecture but also the capability in identifying potential growth areas, integration points, and future scalability.

In contrary to the earlier basic implementation method, in best practice you should be selecting high-performance hardware and software capable of handling extensive data processing, without thinking of resource constraints. The server running the vulnerability management tool should be able to run the service without buffering or stagnant processes. (ManageEngine, 2024b) The chosen tool solutions must support advanced features like continuous monitoring (Microsoft, 2023b), semi-automated or automated patch management and extensive workflow and integration capabilities internally in the tool and with other IT and security tools (Neagu, 2021).

A focus should be on automation capabilities to streamline vulnerability management processes and administration of the platform. Integrating the vulnerability management platform with tools like existing IT management systems, such as Information Technology Service Management (ITSM) and Configuration Management Database (CMDB), can produce more efficient vulnerability reporting and asset data correlation in the vulnerability management platform. (Balbix, 2022)

Figure 4 below serves as an illustrative example of how different components, including scan data, asset information, and threat intelligence, can be aggregated through an automated and integrated vulnerability management system. It also includes the critical role of API integrations, which facilitate seamless data exchange and support the automation of ITSM and CMDB systems. (Allen, 2022)

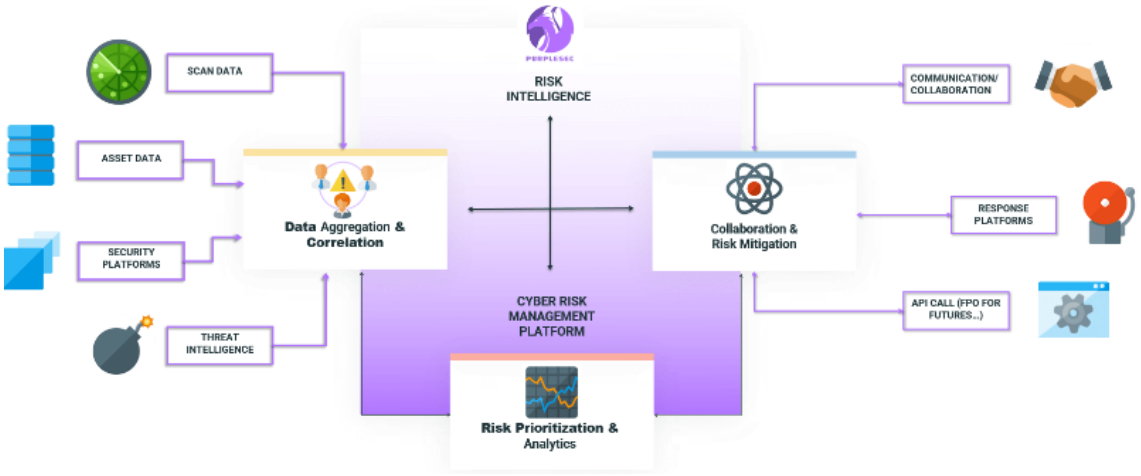

Figure 4. Possible VM Integration/Automation Layers. (Allen, 2022)

5.2.2 Comprehensive Network Configuration and Asset Management

A best practice implementation method of a vulnerability management tool requires a detailed approach to network and asset management, ensuring comprehensive coverage of all wanted organizational assets across physical, virtual, cloud and mobile environments. (Balbix, 2022) When implementing this an organization must map out all its assets and decide on which assets the organization wants to have in its vulnerability management scope. (Palmaers, 2013) For example, many companies leave out their OT (Operational Technology) environment out of scope, since these assets might be frail to new software and extra traffic from different scanning methods designed for scanning complex IT and cloud infrastructure (Claroty, 2024).

The network openings included in the implementation method mentioned earlier would be necessary in best practice, as being minimum requirements. When implementing a vulnerability management tool, concluding a comprehensive plan about all needed network openings would be optimal. Before implementing the tool, as mentioned above, the person or team responsible for the implementation, should map out all the assets and the openings needed between those assets, scan engines and other needed systems. This should be done by consulting e.g., the organizations network technician to get a more

comprehensive view of the scenario. A well-planned plan and mapped out view of the network and organizations asset infrastructure forms a sturdy base for the implementation phase. (Palmaers, 2013) In a best-case scenario, all organization assets that are in the implementation scope, would be mapped out beforehand and network openings would be waiting for the tool implementation to be concluded.

If an organization follows best practice in other areas than just vulnerability management, they usually have their network and assets segmented in an advanced way of working. This means that they follow certain guidelines relying on network frameworks like ISA/IEC 62443 (ISA, 2024) or, as illustrated in the figure 5 below, the Purdue Model to map out their assets into different layers or levels, depending on their tasks or location in the organization and network. The visualized Purdue Model effectively demonstrates this layering concept, providing a clear structure for asset categorization from enterprise zones down to field-level devices, which is central to effective vulnerability management. Assets closer to the ICS-zones usually are mapped to be of higher importance in contrast to the IT level assets. (Claroty, 2023)

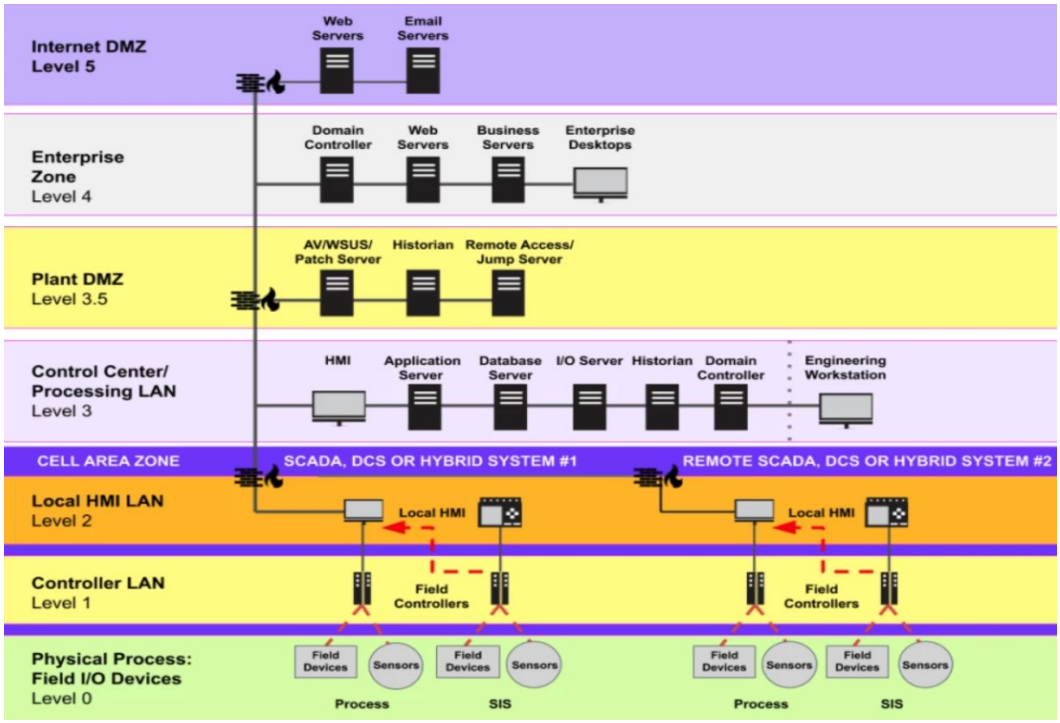

Figure 5. Architecture Example of The Purdue Model. (Claroty, 2023)

In vulnerability management, the "layering" method considers network segmentation, such as dividing assets into areas for security management. For instance, if an asset resides within the IT Zone—a network segment typically containing corporate IT resources—the scan engine responsible for vulnerability assessments should also operate within this zone to ensure targeted scanning. This principle applies equally to the DMZ and other network layers defined by the organization's architecture. Deploying scan engines in this zone-focused manner ensures that each area's specific security protocols are respected, and only necessary network openings are established to facilitate comprehensive scanning while maintaining security controls. (Rapid7, 2024l)

In the context of the vulnerability management tool, essential network configurations include establishing connectivity from assets to scan engines, scan engines to the vulnerability management tool, and, when utilized, from the proxy to the cloud. As a scan engine must be deployed on each layer of the framework, a proxy for the installed agents should also be available in each zone. For example, an asset in an ICS (industrial control system) DMZ should not have permission for direct access to external resources, to relay data to the service provider's cloud. By enabling the agent to communicate on the same layer as the asset, an opening can be done, and the proxy can relay the data forward to the cloud. (Rapid7, 2024l)

Most of the organizations have already moved everything that is not considered OT/ICS, DMZ, or legacy assets into the cloud. Integrating a vulnerability management tool into the cloud opposes new challenges with the needed communication between the VM platform and the assets. The cloud differs from the on-premises environment so that more openings must be considered. (Wagenseil, 2022) On top of normal firewall openings, there are cloud network security groups, that also manage and control the traffic of the cloud asset. When scanning a cloud asset and not getting connectivity to the asset after making a regular firewall rule, the issue usually lies in the assets network security group denying the traffic. (Microsoft, 2023a)

Figure 6 below offers a modern visualization of a Hybrid IT, OT and Cloud environment, illustrating the connections between various network segments and security layers. It contextualizes the chapter's discussion above on network segmentation and asset categorization, showing how different zones from cloud to production floor integrate and communicate within an organization's network. (Microsoft, 2023c) This serves as a contemporary contrast to the traditional Purdue model, highlighting the evolution of network structures in line with advanced vulnerability management practices.

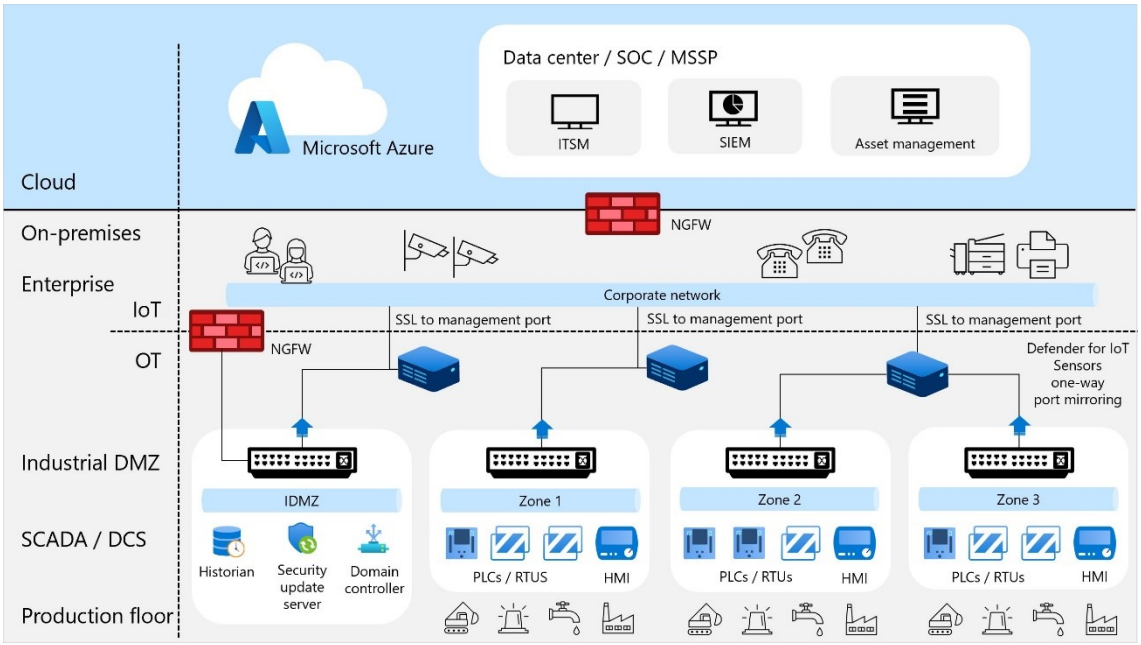

Figure 6. A Hybrid IT/OT Environment. (Microsoft, 2023c)

5.2.3 Advanced Scanning

Leveraging different vulnerability scanning technologies and methodologies is essential for effectively identifying and prioritizing vulnerabilities. Dynamic scans, as opposed to standard, static scans, are designed to adapt to network changes and continuously update scanning parameters in real-time. This adaptability ensures that the scanning process reflects the current state of the network, offering timely and accurate detection of vulnerabilities. Customized scans are also integral, tailored to specific asset types or environments for

targeted assessment. (Fortra, 2023) Vulnerability prioritization is based on asset criticality, vulnerability severity, and exploitability, focusing efforts on mitigating the highest risks first. (Chatterton, 2023)

A best practice implementation method usually involves taking advantage of multiple scan configurations for different purposes. (Rapid7, 2024n) Different ready-made templates like the earlier mentioned discovery and full audit can be utilized, but other templates should be taken advantage of as well. performing a SCADA (Supervisory Control and Data Acquisition) audit requires a specialized approach. SCADA systems, which monitor and control industrial, infrastructure, or facility-based processes, are critical to operational continuity and often sensitive to high network traffic. Therefore, "polite" or less aggressive scanning is used to minimize the risk of disrupting these control systems. (Rapid7, 2024m) On top of this, scan configurations should vary, whether the scan is internal or external. In this case, the tool’s operator needs to carefully examine and set up the right configurations. Additionally, the ready-made templates and their configurations should also be examined and be configured to the organization's best needs. (Rapid7, 2024n)

Assets get terminated and created faster than ever due to the cloud migration happening worldwide in organizations. For this, dynamic scans should be configured, so the VM tool’s data is up to date. These dynamic scans for the network can be quite easily added into the vulnerability management tool. In the case of internal resources, organizations tend to use certain subnet scopes, where their assets are located, and because of this the dynamic scans can be set to scan the whole subnet. (Rapid7, 2024b) Due to this configuration, the scan engine finds all the internal assets on the network, if the network openings mentioned earlier are done correctly. Another way to keep all assets up to date is to leverage API and the information from the organizations CMDB. This method is dependent on the accuracy of the organization’s CMDB and the technical competence of the people working on the integration. (Balbix, 2022)

The scan scopes should be configured in a way that they are layer-based, meaning that if a company follows a certain framework or connectivity structure,

the scan scopes should follow that as well. By using this method and following the earlier mentioned best practice of network communication of the scan engine, we can map out e.g., cloud, on-premises, and industrial DMZ into different scan configurations scopes, and thus keep those layers as secure as needed, when doing vulnerability scanning. (Rapid7, 2024l) Discovery scans, which are for identifying all active devices and services within the network for further vulnerability assessment, are typically divided into external and internal scopes. Furthermore, each external resource scanned and hosted by e.g., an external vendor, should be separated into different scan scopes to streamline the management of the VM tool. (Crockett, 2022)

Figure 7 below visually represents the infrastructure for conducting internal and external vulnerability scans within an organization. It illustrates a network architecture that segregates assets into different zones, such as the internal network and a screened subnet known as the Demilitarized Zone (DMZ). In this setup, scan engines are assessing the security posture from both an external perspective (facing the internet) and an internal perspective (facing the internal network). (Rapid7, 2024l)

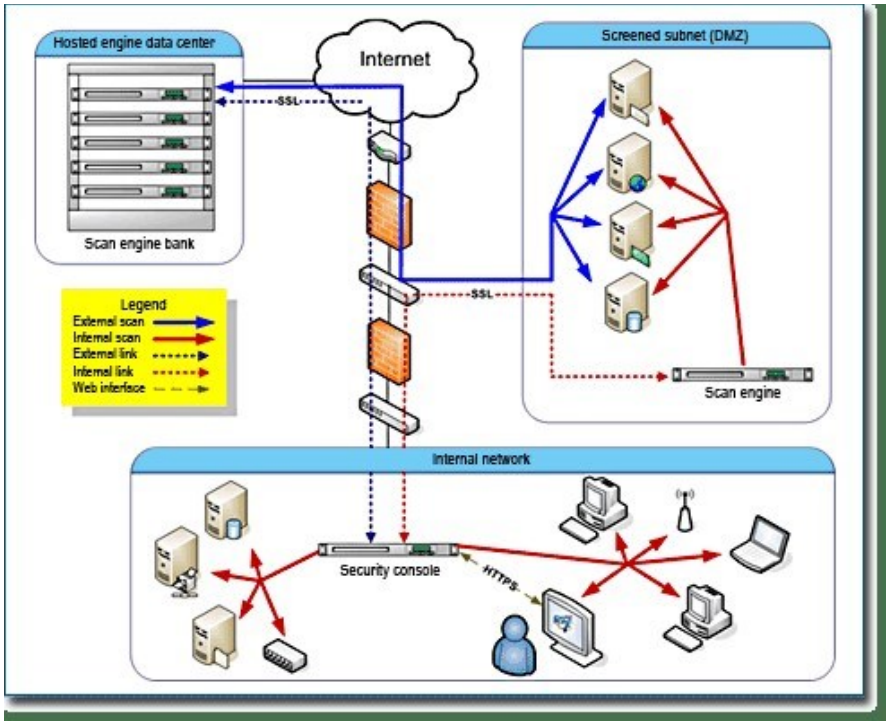

Figure 7. Internal/External Scans and Zones. (Rapid7, 2024l)

When implementing agents to assets in best practice, the delivery of the agents should be thought upon. A few sustainable solutions for the Windows and cloud assets would be to use Microsoft GPO (Group Policy Object) to remotely install the agent software or to include the agent software into a ready-made image. Deploying the agent through GPO would involve creating a script or a batch file to install the agent and then using the GPO in Windows to distribute and execute the wanted script across your desired assets within an Active Directory environment. (Microsoft, 2018) Similar agent delivery for Unix/Linux systems can be managed through equivalent methods such as automated shell scripts or configuration management platforms like Ansible, which can streamline the installation process across diverse operating systems. (BasuMallick, 2022)

An even more sustainable way to deliver the agents in the cloud more efficiently would be to include the agent software into a ready-made virtual machine image. The same principle is followed in different cloud solution platforms like Azure (Microsoft, 2023b) and AWS (Amazon, 2024), and the service of including different software into these images is usually offered by different service providers. This includes creating a virtual machine, which has the agent installed, generalizing the machine to be used as an image, by removing system-specific data like computer names and security identifiers, capturing the image and lastly offer the ready-made virtual machine image for use. (Microsoft, 2023b)

If an organization has “legacy servers” in use, delivery of assets needs to be reconsidered. The installation methods in this case could be e.g., manual installation, scripted installation via local network or the delivery of the software via third-part management tools, if in use. (Barney, 2022)

5.2.4 Advanced Reporting

The reporting structure and configurations of vulnerabilities can be done in many ways. As mentioned earlier, reporting can be done e.g., scan-specific, or even in some cases self-managed. It is an internal discussion that must be held

in an organization, consulting application or asset owners and executives, to clarify the best solution for reporting. (Carnegie Mellon University, 2016)

Vulnerability management tools have ready-made reports that can be used for different styles of reporting. For example, there are audit reports, baseline comparison reports, executive overviews, policy compliance reports and remediation plans. There are also reports that list your assets including the most critical vulnerabilities to the least critical ones. These tools also offer the solution to export files like XML (Rapid7, 2024c) and make reports using SQL queries (Rapid7, 2024d). The reporting capabilities are extensive and there are many ways to use this to an organization's advantage.

In managing vulnerability assessments, it is critical to communicate findings effectively across all organizational levels. Monthly or weekly vulnerability status reports are typically designed for operational staff and middle management, who require detailed insights into the remediation process, trends in risk levels, and areas of critical vulnerability. These reports should be concise yet comprehensive, providing at-a-glance information on risk trends, severity of vulnerabilities, and progress against Service Level Agreements (SLAs) without overwhelming recipients with excessive detail. (Juett, 2022)

For senior executives, the focus of reporting shifts toward strategic overviews rather than granular technical data. Reports aimed at this level should summarize key performance indicators (KPIs) and highlight critical insights from threat intelligence that may influence business decisions or risk posture. While detailed vulnerability data is essential for operational management, executive summaries should distill this into strategic insights that align with the organization's broader business objectives and SLAs defined by management. (Juett, 2022)

Integrating the use of dashboard tools provided by vulnerability management platforms can greatly assist in creating these differentiated reports. With these tools, organizations can generate tailored reports that meet the specific informational needs of both the operational teams and executive leadership,

ensuring that each group receives the most relevant and actionable data to inform their respective responsibilities and decision-making processes. Below in figure 8, is an example of what an executive SLA report could look like. (Juett, 2022)

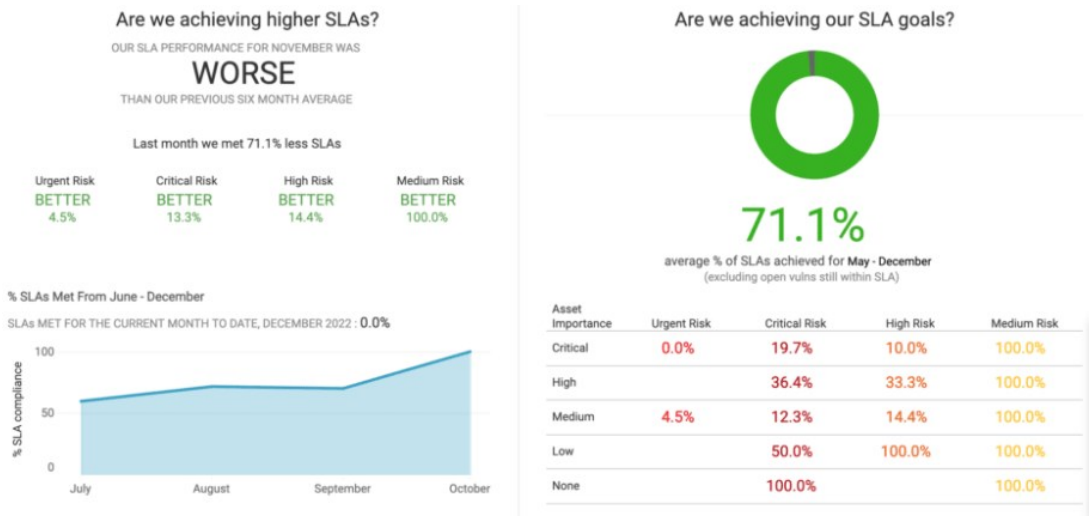

Figure 8. Executive Overview of SLA report. (Juett, 2022)

Most of the vulnerability management tools have a feature, that you can make an account for an application owner with view capabilities of their own assets. This ensures that the application owner cannot make any scan configuration changes but can view vulnerabilities and do their own reports using the ready-made templates, if needed. (Rapid7, 2024i) This might be useful, since often in organizations, the application owner is responsible for the security of their application and is thus responsible for their applications vulnerabilities (Raza, 2021). If a self-managed reporting service is not an option for an organization, can reports also be configured to be scan-linked, where e.g., a remediation report for an application is sent out to the application owner through email on a set period. If an organization has external application owners, and these would not be allowed to login into the tool, could this reporting method be utilized in that scenario. (Rapid7, 2024f)

Often large organizations tend to use third party suppliers of a VM reporting service, where the vendor is responsible of creating tickets of relevant

vulnerabilities affecting the systems. This service might be also just used in some applications or assets in the organization, since some organizations have guidelines that an asset having critical information or functions, cannot be managed or viewed by anyone else than themselves and/or internal employees. These services also tend to cost by a per application or asset basis, so the more an organization utilizes this service, the more it costs. (McCloskey, 2019)

Most of the vulnerability management tools also offer automated and semiautomated ticketing functionalities. Depending on the organization's size and number of vulnerabilities, automated ticketing should be considered upon. (Resolver, 2019) Tools, like earlier mentioned in chapter three, usually support ticketing integrations with commonly used IT solutions like Jira and ServiceNow. Configuring automated ticketing would mean that your VM tool automatically reports vulnerabilities on applications or assets. This can be configured in diverse ways e.g., that it only reports vulnerabilities over a certain risk or CVSS (Common Vulnerability Scoring System) threshold. Semiautomatic ticketing would mean that the ticketing would need a manual approval from a technician before sending it to the IT solution, where the tickets are managed. (Rapid7, 2024o) These are functions that need to undergo a PoC (Proof of Concept) carefully, since they can easily overwhelm the ticketing solution used, as well as application owners, if wrongly configured.

Some modern vulnerability management tools have established the use of AI for fixing vulnerabilities and removing the need for reporting. These tools can automatically do needed software or operating system patching, by analyzing the vulnerability present, locating the vulnerable component, and automatically providing patches to that component. They also provide an opportunity to manually approve the patching decision before it is done. (Kaminski, 2021) More of the use and future of AI in vulnerability management, will be tackled in chapter 6.8.

5.2.5 Prioritization

Asset and application prioritization are an important part of an organization's vulnerability management process. Determining assets on e.g., their impact and availability on the organization in various ways, can determine the most critical applications that need remediation of vulnerabilities the fastest. (Palmaers, 2013)

Often it is thought that the CIA (Confidentiality, Integrity, and Availability) Triad (figure 9 below) is a good enough security model to follow to determine prioritization. It provides a simple and comprehensive checklist for evaluating security procedures, tools, and systems. It is a security model that includes three components: the information being safe from accidental or intentional disclosure, modification or alteration, as well as being available to authorized users when needed. While the principles of the CIA Triad are relevant and important, they might not be sufficient on their own for determining prioritization. (Fortinet, 2024)

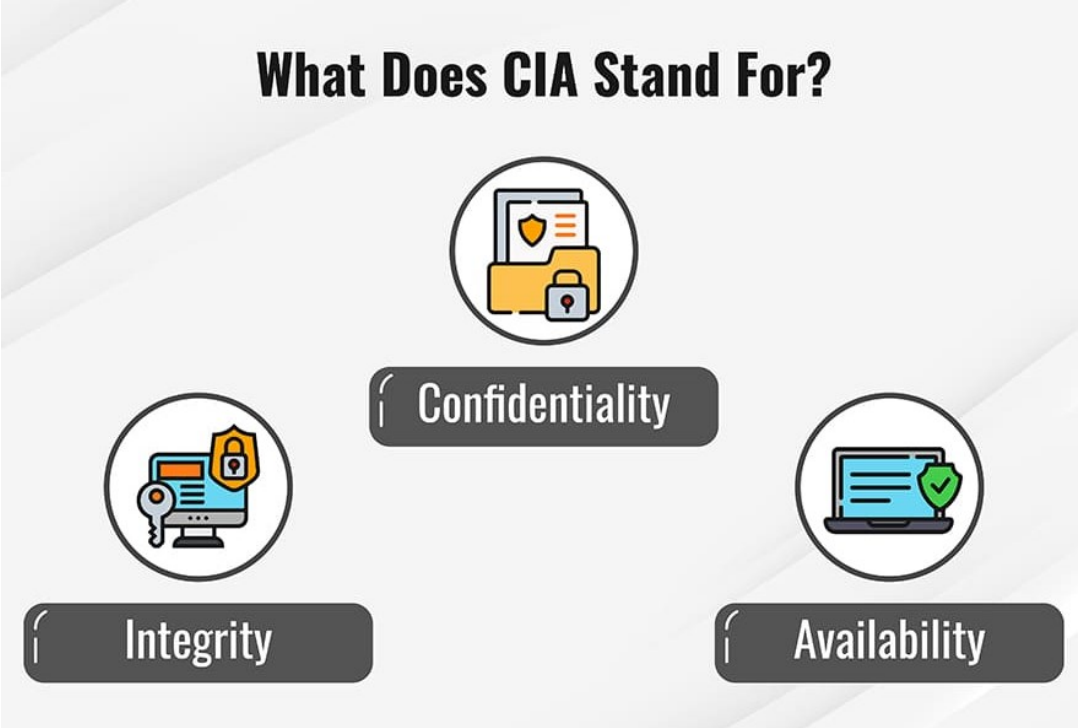

Figure 9. CIA Triad. (Fortinet, 2024)

Assets and applications should be prioritized by their type, purpose, and sensitivity. (Chatterton, 2023) This involves grouping assets in an organizations CMDB or relevant platform with data, such as public-facing or internal, regulated, or non-regulated data, and critical or non-critical systems. The criticality of each asset to business operations should be considered. This would include factors such as the asset's role in business impact, revenue generation and importance to the organization's mission. A similar impact analysis to that used in risk assessments should be conducted on each asset to determine its criticality. This analysis considers the potential consequences of a security breach, including monetary losses, operational disruptions, and indirect impacts such as reputational damage or regulatory penalties. Also, the environment type should be considered, such as is the asset a test, development, or production environment. (Schmittling and Munns, 2010)

From a technical point of view, this would be done by utilizing an integration between the CMDB and the vulnerability management tool (ServiceNow, 2024), and/or making use of the tagging (Tenable, 2024a) and grouping methods available (ManageEngine, 2024a). If a "criticality" level is not determined in the CMDB, it can be created through using the data brought from the integration, by using the tags to form different criticality groups (ServiceNow, 2024). These groups could contain variables like; internal and external, business impact level and data classification level (Schmittling and Munns, 2010). These variables could be used to form a group that gives a certain criticality level e.g., very high or low, to an asset, which could correlate to the vulnerability score, or impact level provided by the vulnerability management tool by default. Very high assets would provide a higher score of risk by multiplying it with a specified number and low assets would have their score of risk decreased. (Rapid7, 2024a)

Enabling a tagging system mentioned, including criticality and business impact, would highly improve the manageability of application and assets, depending also on the reporting method used. A tagging system would extensively benefit 3rd party services for remediating and prioritizing important assets and applications first. There is also a benefit for application owners to see which

assets they should prioritize, considering that an application owner managing tens of applications or assets would perhaps not be able to remember each one's criticality.

6 Operational Enhancements

Chapter 6 shifts the focus more towards the operational enhancements that can progress the effectiveness of vulnerability management tools within organizations. This section examines the integration of vulnerability management tools with existing IT infrastructure, the role of automation in streamlining vulnerability response processes, and the importance of API integrations in enhancing tool functionality. By examining how these operational improvements can be implemented, the chapter aims to provide actionable insights for organizations looking to optimize their vulnerability management practices.

6.1 Integration with Existing Infrastructure

Integrating vulnerability management tools within an organization's IT infrastructure is critical for enhancing security measures and operational efficiency. This integration, orchestrated by a designated individual responsible for the oversight of the implementation process, involves careful planning and execution. The goal is to ensure that the tool complements and extends the capabilities of existing systems, processes, and policies, creating a unified security framework that maximizes the potential of vulnerability management solutions without disrupting current operations. (Balbix, 2022)

6.1.1 Implementation Strategies

The integration process starts with a comprehensive review of the organization’s IT infrastructure. This detailed process covers hardware specifications, software applications, network layouts, and current security frameworks to pinpoint where and how the vulnerability management tool can be integrated effectively. It is crucial to understand the specifics of the organization's technological environment to identify suitable integration points and to ensure compatibility. This assessment is needed for recognizing

necessary modifications, allowing the new tool to enhance the existing setup without causing disruptions. (Carnegie Mellon University, 2016d)

Effective integration needs collaboration between the organization, the vulnerability management tool providers, and internal IT departments. Engaging with the tool vendors is important for understanding the full capabilities of the product and for gaining insights into best practices for its integration. Meanwhile, the internal IT team's deep knowledge of the organization's existing digital infrastructure is invaluable for customizing the tool to meet specific organizational needs and ensuring it operates correctly with current systems. (Carnegie Mellon University, 2016a)

Configuring the vulnerability management tool to align with the organization's unique requirements is a critical phase. (Carnegie Mellon University, 2016d) This involves configuring the tool's settings, such as customizing scan schedules and setting appropriate alert thresholds. It also requires integrating the tool with existing security systems, including SIEM (Security Information and Event Management), firewalls, and incident response mechanisms. Proper configuration is key to enabling the tool to monitor the organization's network effectively and to interact seamlessly with other security measures. (Balbix, 2022)

Prior to full deployment, rigorous testing of the tool within the existing infrastructure is imperative to verify its functionality and to ensure it meets all security and operational benchmarks. This testing phase is essential for identifying and rectifying any issues, confirming that the tool delivers the expected security enhancements without introducing any issues. Successful validation against security and operational standards signifies that the integration process has been completed effectively and that the tool is ready for operational use. (Carnegie Mellon University, 2016d)

6.1.2 Addressing Compatibility Challenges

Integrating modern vulnerability management tools into an environment with legacy systems presents a notable challenge due to potential compatibility issues. Early identification of these challenges is critical. Strategies to mitigate these issues may involve utilizing middleware to facilitate communication, upgrading outdated systems, or employing specialized adapters to achieve connectivity. Overcoming these obstacles is essential for the seamless operation of the vulnerability management tool across the organization's entire IT landscape. (Filkins, 2019)

Achieving integration across diverse platforms and environments demands a strategic approach. Leveraging APIs and custom scripting enables effective communication among disparate systems, ensuring the vulnerability management tool operates efficiently across the organizational technology ecosystem. This level of integration is crucial for establishing a unified security framework capable of addressing threats from multiple vectors. (Filkins, 2019)

Moreover, the integration strategy must be designed with scalability in mind to accommodate future growth and technological advancements within the organization. Regular reviews and updates to the integration framework are necessary to preserve its relevance and effectiveness. A scalable and adaptable integration approach ensures that the organization can respond to evolving security landscapes without the need for complete system overhauls. (McAbee and O'Neil, 2023)

6.2 Automation and Workflow Integration

The role of automation in cybersecurity, especially in vulnerability management, is transformative. It enhances efficiency, reduces the risk of human error, and ensures timely responses to vulnerabilities. By integrating automated processes into vulnerability management workflows, organizations can streamline their security operations, from detection through to remediation.

Integrating vulnerability management with patch management systems through automation streamlines the remediation process. This setup allows for the prioritization of patching activities based on the severity of vulnerabilities and the criticality of affected systems, ensuring mitigation of significant risks. By defining criteria for when patches should be applied automatically versus when manual review is necessary, organizations can blend the efficiency of automation with the perspective of human oversight. (Balbix, 2022)

The implementation of automated notifications for critical vulnerabilities is essential for ensuring that security teams are immediately aware of potential threats. These alerts, customizable based on factors like vulnerability severity or system criticality, facilitate prompt attention to urgent security issues. Tailoring these notification methods and formats to fit organizational response protocols enhances the efficacy of the communication process, enabling quicker action. (Rapid7, 2024k)

Extending automation to report generation and documentation provides stakeholders with consistent updates on the vulnerability management program's status. Customizable reports cater to various informational needs, from technical analyses for IT personnel to executive summaries that outline key metrics and progress in remediation efforts. This automated documentation is important for supporting compliance and managing the vulnerability management program effectively. (Resolver, 2019)

Incorporating automated feedback mechanisms allows for the continuous refinement of vulnerability management processes. By evaluating the outcomes of automated scans, patch applications, and response strategies, security teams can pinpoint areas for improvement and adjust their approaches accordingly. This cycle of assessment and adjustment ensures that the vulnerability management strategy remains dynamic, adapting to new threats and evolving organizational requirements. (Scarfone, 2023)

6.2.1 Integration with IT Processes

Effective vulnerability management necessitates its integration with broader IT processes, enhancing the organization's capacity for comprehensive vulnerability management and aligning security measures with overall IT operations. This integration promotes a unified approach to security management, leveraging existing IT workflows to optimize the response to and remediation of vulnerabilities.

Integration with IT Service Management (ITSM) platforms, such as ServiceNow or Jira, is critical. It automates the creation of tickets or tasks upon detecting vulnerabilities, facilitating their assignment to appropriate teams for remediation. This ensures that vulnerability management is seamlessly woven into regular IT operations, aiding in the prioritization and systematic tracking of remediation activities. (Rapid7, 2024o)

Coordination with change management processes is needed to ensure that remediation-related changes are implemented effectively without introducing new risks. Integrating vulnerability management activities with change management workflows guarantees that all changes undergo thorough review and approval, maintaining system stability and security throughout the remediation process. (Carnegie Mellon University, 2016d)

Aligning vulnerability management efforts with the organization's risk management framework ensures prioritization of remediation efforts based on their potential impact on the organization's risk profile. Evaluating vulnerabilities against the organization's risk tolerance and business objectives allows security teams to concentrate their efforts on the most critical vulnerabilities, facilitating informed decision-making and efficient resource allocation. (Tenable, 2020)

While automation accelerates vulnerability management processes, the value of human oversight remains undeniable. Establishing a balance between automated actions and human judgment is essential, particularly for complex decisions requiring nuanced understanding. Security teams must define

boundaries for automated operations, with protocols for escalating issues that necessitate human analysis. (Kumar et al., 2023)

As organizations grow and their networks evolve, the scalability and adaptability of automated systems become critical for sustaining an effective vulnerability management process. Automated systems must be capable of managing increased data and scan volumes and adaptable to new technologies and changing threat landscapes. Regular updates to automation protocols ensure the system's ongoing relevance and effectiveness. (Balbix, 2022)

Commitment to continuous process improvement is crucial for maintaining operational efficacy in vulnerability management. Regular evaluations of automation impact, integration with IT workflows, and the overall effectiveness of the vulnerability management program inform continual refinements, driving improvements and ensuring the organization's resilience against new and emerging threats. (Carnegie Mellon University, 2016d)

6.3 API Integrations and Tool Fine-Tuning

The integration of Application Programming Interfaces (APIs) into vulnerability management tools markedly enhances their functionality, facilitating direct and seamless communication with a wide scope of systems that constitute an organization's cybersecurity infrastructure. This capability is for crafting a cohesive security strategy that effectively leverages the interconnectivity of modern IT environments, enabling more efficient and effective management of vulnerabilities through automation and improved integration with existing tools and systems.

APIs are instrumental in enabling vulnerability management tools to establish connections with essential security systems, SIEM systems, firewalls, and intrusion detection systems. This level of integration is critical for unifying the cybersecurity framework across different platforms, allowing for a synchronized flow of data and insights that strengthen threat detection and speed up response mechanisms. Moreover, the integration through APIs extends to IT

management systems, enhancing asset management and visibility throughout the network. (Tenable, 2024f) This aspect is crucial for executing comprehensive vulnerability assessments and planning targeted remediation strategies, underlining the emphasis on accurate and up-to-date asset information detailed in Chapter 5.

Beyond facilitating integrations, APIs are pivotal in automating key vulnerability management workflows, significantly enhancing the efficiency of the process. Automation via APIs can include the generation of tickets within ITSM platforms upon the detection of vulnerabilities, thereby streamlining the initiation of the remediation process. (Tenable, 2024f).

Additionally, APIs can enable real-time data exchange and analytical processing, augmenting the adaptability and responsiveness of the vulnerability management system. This ensures that security operations can rapidly adjust based on the most current data, maintaining an optimal defense posture. (PubNub, 2024)

The adaptability afforded by APIs also allows for the development of custom integration solutions tailored to the unique needs and challenges faced by an organization. Such customization ensures that vulnerability management tools are aligned with specific security requirements and operational workflows, enhancing the overall effectiveness and integration within the organizational context. (Thomsen, 2023)

6.3.1 Advanced Integrations and Fine-Tuning

Customizing vulnerability management tools to align with an organization's unique security policies, risk tolerance, and operational procedures is essential for their optimal functionality. This entails adjusting settings such as scan frequencies, alert thresholds, and reporting formats to fit the specific needs of the organization. Such customization ensures that the tools are not merely operational but fully integrated into the security strategy, delivering actionable

insights tailored to the organization's requirements (Carnegie Mellon University, 2016d).

Fine-tuning tools for advanced integrations can lead to more effective resource utilization, a reduction in false positives, and an increase in the accuracy of vulnerability detection and prioritization (Balbix, 2022). Finding a balance between vulnerability detection and maintaining operational efficiency is essential to ensure that security teams are not overwhelmed with false alarms and that critical vulnerabilities are promptly and accurately identified and addressed. (Vijayan, 2021)

Given the dynamic nature of cybersecurity threats and the continual evolution of organizational IT infrastructures, it is imperative to regularly evaluate and adjust the configurations of vulnerability management tools. Establishing a feedback loop that incorporates insights from user experiences and incident analysis is crucial for the iterative refinement of tools and strategies. This process of continuous improvement, underscored in Chapter 5 and later in Chapter 7, ensures that vulnerability management tools remain effective against emerging threats and are flexible enough to adapt to organizational changes, thereby sustaining a resilient and proactive security posture. (Carnegie Mellon University, 2016c)

6.4 Data Classification and Prioritization

An effective vulnerability management strategy is rooted in the systematic organization of data according to its sensitivity and criticality to the business. (Palmaers, 2013) This chapter explains the imperative process of data classification and the subsequent prioritization of vulnerabilities that could potentially jeopardize the integrity of the organization's most valuable data assets.

6.4.1 Establishing a Data Classification Framework

Data classification is a structured approach to sorting organizational data into defined categories that reflect the confidentiality, regulatory mandates, and business importance of each data type. This framework is crucial for guiding the prioritization of vulnerability management, ensuring a focused approach towards safeguarding critical data. (De Groot, 2023)

A comprehensive data classification framework commences with the delineation of data categories such as public, internal, confidential, and restricted. These categories are crafted to mirror the data's significance, the ramifications of its unauthorized disclosure, and the legal compliance obligations it may include. (Spirion, 2024)

Following the categorization, the organization must articulate precise criteria for classification. This involves specifying the nature of information each category encompasses, ranging from personally identifiable information (PII) and financial records to intellectual property and operational data. (Spirion, 2024)

The implementation phase is crucial, requiring the classification framework to be applied consistently across the organization. This often requires cross-departmental collaboration to ensure all data assets are accurately categorized. (Spirion, 2024)

Given the nature of data and business priorities, the data classification scheme requires periodic reviews and revisions. This ensures the framework remains aligned with evolving business models, regulatory landscapes, and emerging threats. (Carnegie Mellon University, 2016c)

6.4.2 Prioritization of Vulnerabilities Based on Data Classification

With a robust data classification framework in place, the organization can now strategically prioritize vulnerabilities based on the criticality of the impacted data assets. This aligns with the prioritization methodologies discussed at the

conclusion of Chapter 5, optimizing resource allocation towards mitigating risks against the most sensitive and valuable data.

Integrating the data classification schema into vulnerability management tools is a strategic move. This allows for the correlation between vulnerability assessments and data criticality, enabling a prioritized approach to vulnerability management, informed by the affected data's sensitivity. (Palmaers, 2013) Figure 10 below compliments the needed features for prioritization that have been discussed earlier in this chapter.

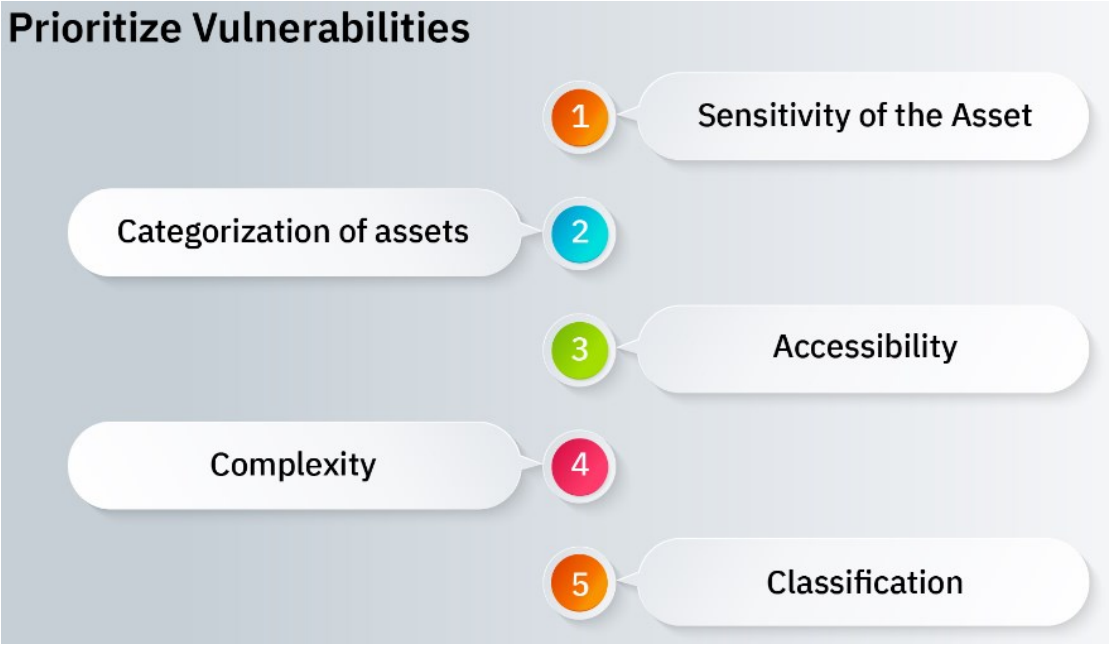

Figure 10. Approach to Prioritizing Vulnerabilities. (Strobes Security, 2023)

Risk assessments of identified vulnerabilities take on a new dimension with data classification. Assessing the risk involves considering the data's sensitivity, the potential impact of a breach, and the vulnerability's severity and exploitability. This culminates in a prioritized list of vulnerabilities for remediation, focusing on those threatening the most critical data. (Spirion, 2024)

Remediation strategies should be then crafted, tailored to the urgency of the vulnerability and the sensitivity of the compromised data. Regular updates to

stakeholders about the prioritization strategy's effectiveness and the overall security posture are essential. (Spirion, 2024)

Lastly, the prioritization strategy must be mindful of compliance and regulatory obligations related to data protection. This is vital for sensitive data governed by strict regulations, where non-compliance can result in significant legal and financial consequences. (Spirion, 2024)

6.4.3 Integration Techniques for Enhanced Data Management

The strategic use of tagging within vulnerability management tools (Tenable, 2024a) stands out as a powerful mechanism for aligning the vulnerability management process with the organization's data classification schema. By assigning tags to data assets based on their classification (e.g., confidential, internal, public) (Schmittling and Munns, 2010), organizations can instantly identify the sensitivity of the data affected by a vulnerability. This tagging system not only simplifies the process of prioritizing vulnerabilities but also enables customized reporting and alerts based on the criticality of the affected data, ensuring that high-priority issues are escalated appropriately. (Qualys, 2023)

API integrations with CMDBs present another important path for enhancing data management within the vulnerability management framework. CMDBs, which house detailed information about an organization's IT assets and their configurations, can be leveraged to automate the process of data classification and vulnerability prioritization. Through API integrations, vulnerability management tools can dynamically retrieve and update information from the CMDB, ensuring that the vulnerability assessment tool and prioritization processes are informed by the most current data asset information. (Tenable, 2024f) This real-time synchronization facilitates a more agile and accurate response to emerging threats, particularly those targeting critical data assets. (The White House, 2023)

Collaboration platforms and workflow management tools also play a crucial role in integrating data classification and vulnerability management processes. By embedding data classification insights into collaborative platforms, organizations can facilitate important communication and coordination in addressing vulnerabilities. This ensures that all stakeholders, from IT security teams to data owners, are aligned in their efforts to protect sensitive data, fostering a cohesive and unified approach to cybersecurity. (The White House, 2023)

6.5 Enhancing Incident and Vulnerability Response with Vulnerability Management Tools

Integrating vulnerability management tools into incident and vulnerability response plans offers organizations a significant advantage in addressing and mitigating security incidents quickly and effectively. (CISA, 2021) This chapter discusses the technical strategies for seamlessly incorporating vulnerability management tools into incident response frameworks, aiming to enhance organizational readiness and response to cybersecurity threats.

A key strategy in modern cybersecurity is the technical integration of vulnerability management tools with incident and vulnerability response processes (figure 11 below). This integration is essential for ensuring swift and informed actions against emerging threats. Automated alerting systems within vulnerability management tools are configured to generate instant alerts when critical vulnerabilities are detected. These alerts contain detailed information about the vulnerability's severity, location, and the potential impact of its exploitation, which are directly sent to the incident response platform. (CISA, 2021)

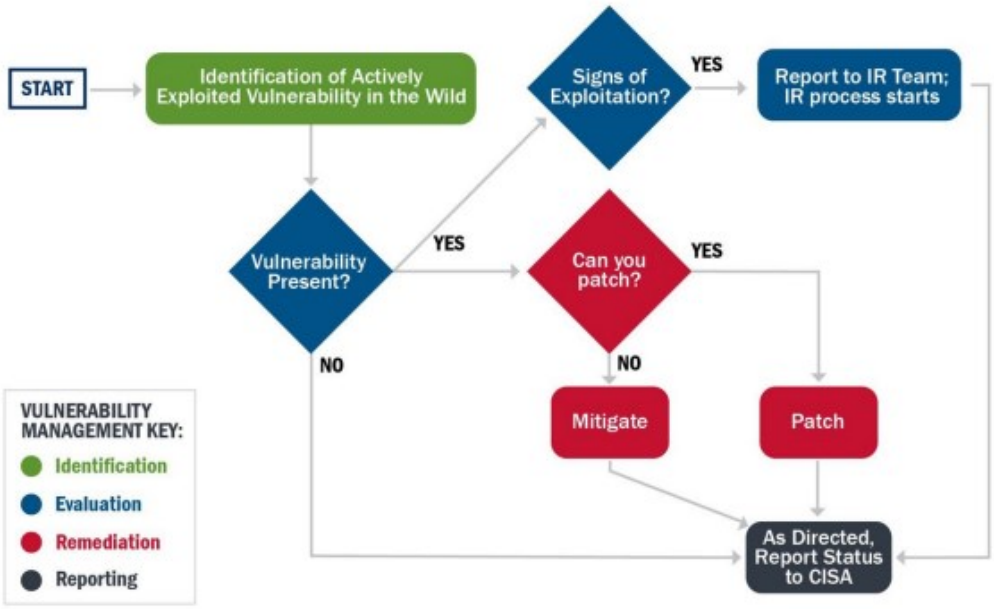

Figure 11. Vulnerability Response Process. (CISA, 2021)

API integration plays a crucial role in this process, establishing a direct line of communication for transferring critical vulnerability information between management tools and incident response platforms. This enables the automatic creation of incident tickets based on vulnerability alerts, facilitating a structured and efficient response. (CISA, 2021) Furthermore, the use of advanced dashboard and reporting features in vulnerability management tools gives response teams a comprehensive view of the organization's security posture.

Automated response playbooks activated by specific vulnerability detections streamline the incident response process. These playbooks detail the steps for assessment, containment, and remediation based on the characteristics of the detected threat, enabling a rapid and effective response. (CISA, 2021)

Beyond technical integration, the strategic use of vulnerability management tools significantly improves the incident and vulnerability response process. These tools enable incident response teams to prioritize and triage threats effectively, focusing on the most significant vulnerabilities first based on their potential impact on critical systems and data. (CISA, 2021)

Continuous improvement is a fundamental aspect of using vulnerability management tools in incident response. Analyzing the effectiveness of the response post-incident helps identify weaknesses in the organization's defenses and refine the incident response plan to better address future threats.

6.6 Training Programs and User Awareness

The success of vulnerability management within an organization crucially depends on the proficiency and awareness of its users. Effective utilization of vulnerability management tools is significantly enhanced through dedicated training programs and initiatives aimed at raising user awareness. This chapter focuses on the key role that structured training and sustained awareness play in optimizing the functionality and impact of these tools across the organization. (Carnegie Mellon University, 2016d)

6.6.1 Designing Basic Training Modules

Developing comprehensive training modules is important for enabling users to effectively utilize vulnerability management tools. These modules should be accurately designed to cater to the diverse roles within the organization, ranging from IT personnel and security teams to application and asset owners. The goal is to ensure all users possess a fundamental understanding of how to navigate and utilize these tools for maximum benefit. (Carnegie Mellon University, 2016c)

The initial step involves creating training content that outlines the basic functionalities and features of the vulnerability management tools. This includes guidance on how scans work, interpreting results, and executing follow-up actions. Tailoring this content to suit different user groups within the organization ensures a wide-reaching and impactful learning experience. (Carnegie Mellon University, 2016c)

Beyond basic tool usage, it is essential to educate users on the best practices in vulnerability management. This encompasses regular software updates,

effective patch management, and comprehensive risk assessment procedures. Highlighting the significance of adhering to organizational policies and the critical role these practices play in securing the organization's digital environment is fundamental. (Carnegie Mellon University, 2016c)

To accommodate various learning preferences, training personnel should embrace a variety of formats. This could include workshops, e-learning modules, hands-on sessions, and live demonstrations. Incorporating engaging elements such as scenario-based learning exercises could significantly increase user engagement and facilitate the practical application of the tools. (Carnegie Mellon University, 2016c)

6.6.2 Advanced Training for Ongoing Awareness

With a foundation of basic training established, it is crucial to offer advanced sessions for users who require a deeper understanding of the tools' capabilities. Security analysts, IT administrators, and other specialized roles benefit from in-depth lessons of advanced features such as custom reporting, detailed analytics, and integration options. (Carnegie Mellon University, 2016c)

The dynamic nature of cybersecurity demands a commitment to continuous education. Establishing a program that regularly updates users on the latest in vulnerability management technologies and threat landscapes is essential. Encouraging engagement with external educational opportunities, such as industry seminars, webinars, and conferences, further enriches the learning environment. (Carnegie Mellon University, 2016c)

To effectively disseminate knowledge and foster a culture of security awareness, organizations should consider implementing a range of training initiatives. Publishing tutorials on the organization's intranet, conducting live demo sessions, and offering Q&A forums where users can seek advice and share experiences are practical approaches. Additionally, creating a repository of training materials and resources accessible to all needed employees

encourages ongoing education and support. (Carnegie Mellon University, 2016c)

The aim of training programs and user awareness initiatives is to cultivate an organizational culture that prioritizes cybersecurity. Regular communications emphasizing the importance of vulnerability management and the collective responsibility of all employees in maintaining security are key to achieving this goal. Organizational campaigns that celebrate best practices and highlight the role of each individual in protecting against vulnerabilities can further reinforce a security-conscious mindset. (Carnegie Mellon University, 2016c)

6.7 Key Performance Indicators (KPIs) and Metrics

Key Performance Indicators (KPIs) and metrics are essential for assessing the effectiveness and efficiency of vulnerability management processes. They provide critical data that helps organizations measure performance, identify areas needing improvement, and justify cybersecurity investments.

6.7.1 Defining Essential KPIs and Metrics for Effectiveness

Setting KPIs for vulnerability management involves tracking a wide range of activities from detecting vulnerabilities to their resolution. An important measure is the number of vulnerabilities found over certain periods, with these findings broken down by severity to give a clear view of the risk landscape. The speed at which vulnerabilities are classified and prioritized after discovery is also a key indicator of the responsiveness of the vulnerability management process. (Swanagan, 2023)

Tracking the remediation process is crucial. This includes how long it takes to fix critical vulnerabilities, indicating the speed and efficiency of the response. Additionally, the percentage of vulnerabilities fixed within set timeframes provides insight into how well the process adheres to and achieves its goals. (Swanagan, 2023)

Coverage and compliance metrics are also vital. The extent to which vulnerability scans cover organizational assets can highlight gaps in the management strategy, ensuring nothing is missed. Measuring adherence to internal policies and external regulations ensures the organization upholds its security commitments and legal obligations. (Risto, 2021)

Beyond initial KPIs, continuously monitoring additional metrics can drive the improvement of vulnerability management programs. This includes assessing patch management success, the frequency and severity of incidents from known vulnerabilities, and user engagement and awareness levels. These metrics offer a comprehensive view of the process's strengths and areas for improvement, promoting a culture of ongoing enhancement. (Risto, 2021)

6.7.2 Implementing Technical Aspects of KPIs and Metrics

Implementing KPIs and Metrics technically within vulnerability management tools or by retrieving data to another platform is crucial. Using dashboard features in these tools allows for real-time tracking of KPIs, offering an immediate overview of the cybersecurity posture. Customizing dashboards to show metrics like the number of vulnerabilities, their severities, and remediation statuses helps quickly inform decisions and actions. Usually, vulnerability management tools also offer loading customized queries to the dashboard features to filter needed data to the KPIs. (Risto, 2021)

Integrating vulnerability management tools with data analysis platforms like PowerBI enables deeper data analysis. Exporting data to these platforms allows advanced analytics to identify trends and patterns, aiding in strategic decision-making. This process facilitates the generation of detailed reports and visualizations, providing valuable insights for improving vulnerability management processes. (Risto, 2021)

6.8 Artificial Intelligence in Vulnerability Management

The integration of Artificial Intelligence (AI) in vulnerability management represents a shift towards more efficient, accurate, and dynamic cybersecurity defenses. This section delves into the operational enhancements AI brings to vulnerability management within organizations, underscoring its important role in addressing contemporary cybersecurity challenges.

6.8.1 Leveraging AI for Enhanced Vulnerability Detection and Prioritization

AI and machine learning algorithms significantly better vulnerability management by refining the processes of data classification and vulnerability prioritization. Through the analysis of data sensitivity patterns and vulnerability impacts over time, AI technologies can potentially forecast potential risks and suggest prioritization strategies. This proactive stance enables organizations to preemptively tackle vulnerabilities, enhancing their security posture. (Kaminski, 2021)

AI-driven insights also play a crucial role in identifying data classification inconsistencies or previously overlooked vulnerabilities. By automating the threat detection and analysis process, AI technologies such as user and entity behavior analytics (UEBA) enhance the detection capabilities of security teams. These tools analyze user behavior to identify anomalies that may indicate a compromise, thereby offering a more nuanced understanding of which assets are critical and warrant enhanced protection. (Kaminski, 2021)

Furthermore, AI aids in reducing false positives in vulnerability detection, a common issue with legacy vulnerability management tools. By evaluating the legitimacy of identified vulnerabilities based on the detection mechanism and other factors, AI technology streamlines the vulnerability management process, enabling security teams to focus on genuine threats. (Kaminski, 2021)

6.8.2 AI-Driven Remediation and Strategic Vulnerability Management

The advent of AI in vulnerability management tools has revolutionized the approach to fixing vulnerabilities. Some modern tools, particularly those not leading the market, have begun to automate the patching of software or operating systems. By analyzing the vulnerability, identifying the vulnerable component, and automatically applying patches, these tools significantly reduce the manual labor involved in vulnerability management. Additionally, they often include features allowing manual approval of patching decisions, offering a balance between automation and control. (Kaminski, 2021)

The challenge for organizations now lies in leveraging AI to derive actionable intelligence from data, aiming for a unified information source that facilitates automated orchestration and informed decision-making. This is particularly crucial in an environment marked by fragmented data and numerous threats, where the ability to act on accurate and comprehensive intelligence is key. (Kaminski, 2021)

7 Continuous Technical Improvement Strategies

The need for an adaptable and proactive approach to vulnerability management is important for organizations. This chapter delves into the importance of continuous technical improvement strategies, focusing on creating a comprehensive continuous improvement plan for technical enhancements, integrating a feedback loop for ongoing improvement, and maintaining documentation on planned changes. These strategies ensure that vulnerability management systems not only respond to current threats but are also aimed to evolve with future cybersecurity challenges.

Acknowledging this, it becomes clear that vulnerability management naturally aligns with the lifecycle and patch management routines inherent to the development, deployment, and maintenance of systems. This inherent integration highlights that vulnerability management should be perceived as a fundamental, continuous activity that automatically accompanies the system development lifecycle and update processes. By embedding vulnerability management as a core aspect of these processes, organizations ensure that it becomes a seamless, indispensable part of their operational rhythm, enhancing cybersecurity measures efficiently alongside the evolution of technology and organizational needs. (Palmaers, 2013)

Building upon this understanding, the chapter further explores how organizations can implement continuous improvement strategies to not only address current security challenges but also proactively prepare for future threats. By embedding vulnerability management deeply within the lifecycle and patch management processes, organizations can create a solid foundation for these continuous improvement efforts, ensuring that their vulnerability management practices are both robust and resilient.

7.1 Establishing a Continuous Improvement Plan for Technical Improvements

A continuous plan for technical improvements in vulnerability management contains a structured approach to documenting, scheduling, and implementing system enhancements. This plan serves as a roadmap for the systematic upgrade of tools, processes, and capabilities within the vulnerability management framework. (SolveXia, 2023)

Key Components of the Continuous Improvement Plan:

- Documentation of Planned Changes: Detailed records of upcoming updates, enhancements, and the integration of new technologies. This documentation should outline the objectives, expected outcomes, implementation timelines, and responsible parties for each planned change. (WIZ, 2023)
- Strategic Improvement Plans: Identifying areas that need enhancement and making plans for enhancing system capabilities (WIZ, 2023) e.g., including the adoption new technologies like AI and machine learning mentioned in chapter 6.8.
- Risk Management: An analysis of potential risks associated with planned changes and strategies for mitigating these risks to maintain system integrity during transitions. (Carnegie Mellon University, 2016b)
- Resource Allocation: Identification and allocation of necessary resources, including budget, personnel, and technology, to support the planned improvements. (WIZ, 2023)

This continuous improvement plan should be maintained in a centralized, accessible team workspace platform, ensuring that all stakeholders have visibility into the roadmap for technical improvements and the status of ongoing projects.

7.2 Integrating a Feedback Loop for Continuous Improvement

Incorporating a feedback loop into the vulnerability management process is crucial for capturing insights from e.g., users, KPI's and vulnerability data, identifying areas for enhancement, and fostering a culture of continuous improvement. This loop facilitates the collection of feedback from different sources like system performance, user experiences, and the effectiveness of recent enhancements. (Carnegie Mellon University, 2016c)

Mechanisms for Feedback Collection:

- User Surveys and Feedback Forms: Tools for gathering direct input from users regarding their experiences with the vulnerability management system and suggestions for improvement. (Carnegie Mellon University, 2016c)
- System Analytics: Analysis of system performance and vulnerability data to identify trends, anomalies, and areas where enhancements could increase efficiency or effectiveness. (WIZ, 2023)
- Incident Reports: Reviews of incident response activities to extract lessons learned and opportunities for system or process enhancements. (Carnegie Mellon University, 2016c)

Integrating this feedback loop into a workspace like earlier mentioned allows for the transparent documentation and sharing of improvement ideas, feedback on current processes, role-specific enhancement suggestions, and requests for additional training sessions. This visibility encourages collaboration and engagement among all stakeholders in the vulnerability management process, ensuring that continuous improvement is a shared objective. (Carnegie Mellon University, 2016c)

7.3 Fostering a Proactive Culture for Technical Advancements

The transition from a reactive to a proactive stance in vulnerability management emphasizes the need for a forward-thinking organizational culture. This culture

supports the anticipation of future cybersecurity challenges and the early adoption of innovative technologies and methodologies to address these challenges. (Carnegie Mellon University, 2016c)

Cultivating this Culture Involves:

- Leadership Commitment: Leaders play a crucial role in fostering a culture of proactive improvement by prioritizing cybersecurity initiatives, allocating resources efficiently, and championing the adoption of innovative technologies and methodologies. Their involvement ensures alignment with organizational goals and amplifies the effectiveness of technical advancements in e.g., vulnerability management. (ENISA, 2021)
- Regular Training and Education: Ensuring that all members of the organization are informed about the latest cybersecurity threats, best practices, and technological advancements. (Carnegie Mellon University, 2016c)
- Open Communication: Encouraging open dialogue about potential improvements, emerging threats, and innovative solutions within and across teams. (Ryan, 2023)
- Stakeholder Engagement: Involving stakeholders in the planning and implementation of technical improvements to ensure alignment with organizational goals and user needs. (Carnegie Mellon University, 2016c)

By committing to leadership involvement, continuous education, open communication, and stakeholder engagement, organizations can cultivate an environment that not only anticipates future threats but also embraces innovation and collaboration.

8 Conclusion

This thesis investigates vulnerability management systems within organizational contexts. Focused on identifying effective strategies for the implementation and perpetual refinement of these systems, this thesis emphasizes the necessity of developing solutions that are specifically tailored to meet the distinct needs and challenges faced by various organizational environments.

The thesis started with a thorough investigation into how organizations can effectively implement a vulnerability management system either by implementing basic requirements or best practice solutions. It demonstrated that effective vulnerability management is not uniform but rather nuanced and tailored to the specific needs and infrastructure of each organization. From small to medium enterprises to large corporations, deploying vulnerability management tools necessitates a customized approach. This customization is crucial for addressing unique challenges and maximizing specific organizational strengths. Critical factors identified for successful integration include compatibility with current systems, scalability, and flexibility to adapt to evolving cybersecurity landscapes, ensuring security and operational efficiency.

Addressing the essential measures and attributes for maintaining the operational effectiveness of a vulnerability management system, this thesis illuminated the importance of seamless integration with existing infrastructure, automation of routine security tasks, and refinement of incident response mechanisms and training programs. Such operational enhancements strengthen an organization's cybersecurity posture, enabling agile and precise responses to vulnerabilities. Moreover, continuous evaluation and adoption of emerging technologies like artificial intelligence contribute to the adaptability and effectiveness of vulnerability management systems against new threats.

Technical continuous improvement in vulnerability management was tackled by establishing a guide for a robust feedback loop. Actively soliciting and incorporating feedback from users, analyzing system performance data, and learning from incident responses allow organizations to identify product and

process enhancement areas and iteratively refine their vulnerability management practices. This culture of continuous improvement, underscored by proactive stakeholder engagement and strategic technology use, equips organizations to adapt their vulnerability management strategies dynamically. Ensuring these practices remain effective, resilient, and aligned with both current needs and future expectations require a strategic upper-level framework for vulnerability management, tied directly to leadership incentives to foster progression.

In conclusion, this thesis has not only provided a comprehensive overview of the technical and operational aspects of implementing vulnerability management tools but also highlighted the dynamic nature of cybersecurity. It underscores the need for ongoing adaptation and improvement in vulnerability management practices to address the ever-changing landscape of cyber threats. As we look to the future, the proactive and innovative use of technology, coupled with a deep understanding of organizational needs, will be key to advancing the field of vulnerability management.

The insights and frameworks developed in this thesis pave the way for further research, particularly in the areas of AI integration and the impact of emerging technologies on vulnerability management strategies. It is hoped that this work will serve as a foundation for future endeavors aimed at enhancing the security and resilience of our digital world.

Sources

Allen, J. (2022). How To Automate Vulnerability Management In 2023. [online] PurpleSec. Available at: https://purplesec.us/learn/vulnerability-management-automation/ [Accessed 12 Mar. 2024].

Amazon (2024). *Importing a VM as an image using VM Import/Export*. [online] docs.aws.amazon.com. Available at: https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html. [Accessed 19 Feb. 2024]

Arora, A. (2023). Cloud Vulnerability Management Best Practices For 2024. [online] CloudDefense.AI. Available at: https://www.clouddefense.ai/guide-to-cloud-vulnerability-management/ [Accessed 8 Mar. 2024].

Balbix (2022). *Automating Vulnerability Management*. [online] Balbix. Available at: https://www.balbix.com/insights/automating-vulnerability-management/. [Accessed 12 Feb. 2024]

Ballejos, L. (2024). Vulnerability Prioritization: How to Prioritize Patches | NinjaOne. [online] www.ninjaone.com. Available at: https://www.ninjaone.com/blog/vulnerability-prioritization/ [Accessed 18 Mar. 2024].

Barney, N. (2022). *What is legacy application?* [online] SearchITOperations. Available at: https://www.techtarget.com/searchitoperations/definition/legacy-application. [Accessed 23 Feb. 2024]

BasuMallick, C. (2022). What Is Ansible? Uses, Working, Architecture, Features. [online] Spiceworks. Available at: https://www.spiceworks.com/tech/devops/articles/what-is-ansible/ [Accessed 20 Mar. 2024].

Boddam-Whetham, J. (2023). What is Operational Risk Management and why is it crucial for businesses? [online] www.noggin.io. Available at: https://www.noggin.io/blog/what-is-operational-risk-management-and-why-is-it-crucial-for-businesses [Accessed 12 Mar. 2024].

Bowen, E., Frank, W. and Golden, D. (2021). *Cyber AI: Real defense*. [online] Deloitte Insights. Available at:

https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html. [Accessed 9 Feb. 2024]

Carnegie Mellon University (2016a). *CRR Supplemental Resource Guide Asset Management*. [online] Available at: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-AM.pdf [Accessed 21 Feb. 2024].

Carnegie Mellon University (2016b). CRR Supplemental Resource Guide Risk Management. [online] Available at: https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-RM.pdf [Accessed 8 Mar. 2024].

Carnegie Mellon University (2016c). CRR Supplemental Resource Guide Training and Awareness. [online] Available at: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-TA_0.pdf. [Accessed 26 Feb. 2024]

Carnegie Mellon University (2016d). *CRR Supplemental Resource Guide Vulnerability Management*. [online] Available at: https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf [Accessed 24 Jan. 2024].

Chatterton, C. (2023). *The Ultimate Guide to Risk Prioritization*. [online] Hyperproof. Available at: https://hyperproof.io/resource/the-ultimate-guide-to-risk-prioritization/. [Accessed 24 Jan. 2024]

Chopskie, E. (2023). *Vulnerability Assessment Tools: Key Features and 5 Tools You Should Know*. [online] Bright Security. Available at: https://brightsec.com/blog/vulnerability-assessment-tools-key-features-and-5-tools-you-should-know/. [Accessed 5 Feb. 2024]

CISA (2021). Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. [online] Available at: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf. [Accessed 25 Feb. 2024]

CISA (2024). Cybersecurity Alerts & Advisories | CISA. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories [Accessed 18 Mar. 2024].

Claroty (2023). *ICS Security: The Purdue Model*. [online] Claroty. Available at: https://claroty.com/blog/ics-security-the-purdue-model. [Accessed 19 Feb. 2024]

Claroty (2024). *The Ultimate Guide to OT Vulnerability Management*. [online] Claroty. Available at: https://claroty.com/blog/the-ultimate-guide-to-ot-vulnerability-management [Accessed 19 Feb. 2024].

Clearfin (2021). *Vulnerability Management Made Simple*. [online] Clearfin Security. Available at: https://clearfinsecurity.com/blog/vulnerability-management-made-simple-your-scoping-guide [Accessed 24 Jan. 2024].

Cole, N. (2022). *How Much Should a Vulnerability Assessment Cost in 2023?* [online] networkassured.com. Available at: https://networkassured.com/security/vulnerability-assessment-cost/. [Accessed 16 Feb. 2024]

Crockett, E. (2022). *External vs. Internal Vulnerability Scans: What's the Difference?* [online] Datamation. Available at: https://www.datamation.com/security/external-vs-internal-vulnerability-scans-whats-the-difference/. [Accessed 16 Feb. 2024]

De Groot, J. (2023). What is Data Classification? A Data Classification Definition. [online] Digital Guardian. Available at: https://www.digitalguardian.com/blog/what-data-classification-data-classification-definition [Accessed 12 Mar. 2024].

Desai, T. (2023). *AI-Driven Solutions for Proactive Vulnerability Management*. [online] ITSecurityWire. Available at: https://itsecuritywire.com/featured/ai-driven-solutions-for-proactive-vulnerability-management/. [Accessed 24 Jan. 2024]

Digby, A. (2022). Vulnerability Management Lifecycle: A Guide For 2023 — Informer. [online] informer.io. Available at: https://informer.io/resources/vulnerability-management-lifecycle [Accessed 12 Mar. 2024].

Dildy, T.J. (2017). Enterprise Vulnerability Management. [online] ISACA. Available at: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/enterprise-vulnerability-management [Accessed 8 Mar. 2024].

Dudley, A. (2021). *Developing a Vulnerability Management Plan*. [online] Nucleus Security. Available at: https://nucleussec.com/blog/part-2-developing-a-vulnerability-management-plan/ [Accessed 24 Jan. 2024].

ENISA (2021). Management Commitment. [online] ENISA. Available at: https://www.enisa.europa.eu/securesme/cyber-tips/protect-employees/management-commitment [Accessed 10 Apr. 2024].

Evrin, V. (2021). *Risk Assessment and Analysis Methods: Qualitative and Quantitative*. [online] ISACA. Available at: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods. [Accessed 24 Jan. 2024]

Faistauer, F. (2021). *Why should you care about vulnerability management?* [online] PwC. Available at: https://www.pwc.ch/en/insights/cybersecurity/why-should-you-care-about-vulnerability-management.html. [Accessed 18 Jan. 2024]

Filkins, B. (2019). *A SANS Survey*. [online] Available at: https://threatconnect.com/wp-content/uploads/Survey_Automation-2019_ThreatConnect.pdf [Accessed 23 Feb. 2024].

Firch, J. (2023). Vulnerability Management Best Practices. [online] PurpleSec. Available at: https://purplesec.us/learn/vulnerability-management/ [Accessed 15 Feb. 2024].

Fitzgerald, A. and Rubbinaccio, M. (2023). *A Step-by-Step Guide to the Vulnerability Management Process*. [online] Secureframe. Available at: https://secureframe.com/blog/vulnerability-management. [Accessed 5 Feb. 2024]

Fortinet (2024). *What is the CIA Triad and Why is it important?* [online] Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad.

Fortra (2023). *What is the difference between agent-based scanning, and authenticated and unauthenticated scanning?* [online] Fortra | AlertLogic. Available at: https://support.alertlogic.com/hc/en-us/articles/4410491393435-

What-is-the-difference-between-agent-based-scanning-and-authenticated-and-unauthenticated-scanning [Accessed 13 Feb. 2024].

GanttPRO (2021). *Resource Allocation in Project Management: An Ultimate Guide*. [online] Gantt Chart GanttPRO Blog. Available at: https://blog.ganttpro.com/en/resource-allocation-project-management/. [Accessed 12 Feb. 2024]

GeeksforGeeks (2022). *What is Credentialed Vulnerability Scan?* [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/what-is-credentialed-vulnerability-scan/. [Accessed 12 Feb. 2024]

Gorecki, A. (2020). Crafting an Incident Response Plan. In: *Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk*. Wiley Data and Cybersecurity. [Accessed 23 Jan. 2024]

Ideboen, A. (2021). *Why Continuous Vulnerability Management Is Essential*. [online] CrowdStrike. Available at: https://www.crowdstrike.com/blog/why-continuous-vulnerability-management-is-essential/. [Accessed 16 Feb. 2024]

ISA (2024). *ISA/IEC 62443 Series of Standards - ISA*. [online] isa.org. Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 16 Feb. 2024]

Juett, A. (2022). *How to Create Vulnerability Management Reports for Executives*. [online] NopSec. Available at: https://www.nopsec.com/blog/how-to-create-vulnerability-management-reports-for-executives/ [Accessed 20 Feb. 2024].

Kaminski, E. (2021). *Is AI-Based Vulnerability Management Really that Efficient?* [online] AiThority. Available at: https://aithority.com/machine-learning/is-ai-based-vulnerability-management-really-that-efficient/. [Accessed 24 Jan. 2024]

Kumar, S., Gupta, U., Singh, A. and Singh, A.K. (2023). Artificial Intelligence. Journal of Computers Mechanical and Management. doi:https://doi.org/10.57159/gadl.jcmm.2.3.23064. [Accessed 12 Mar. 2024].

Lee, D. (2023). *The Future Roadmap to Vulnerability Management Intelligence*. [online] Armis. Available at: https://www.armis.com/blog/the-future-roadmap-to-vulnerability-management-intelligence/ [Accessed 19 Jan. 2024].

ManageEngine (2024a). *Creating custom groups| Vulnerability Manager Plus*. [online] www.manageengine.com. Available at: https://www.manageengine.com/vulnerability-management/help/creating-custom-groups.html [Accessed 20 Feb. 2024].

ManageEngine (2024b). *Vulnerability Manager Plus system requirements | ManageEngine Vulnerability Manager Plus*. [online] www.manageengine.com. Available at: https://www.manageengine.com/vulnerability-management/system-requirements.html [Accessed 9 Feb. 2024].

Mathenge, J. (2020). *Risk Assessment vs Vulnerability Assessment: How To Use Both*. [online] BMC Blogs. Available at: https://www.bmc.com/blogs/risk-assessment-vs-vulnerability-assessment/. [Accessed 29 Jan. 2024]

McAbee, A. and O'Neil, M. (2023). *Building a scalable vulnerability management program on AWS AWS Prescriptive Guidance*. [online] Available at: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/vulnerability-management/vulnerability-management.pdf#introduction [Accessed 23 Feb. 2024].

McCloskey, K.F. (2019). *Current trends in outsourcing and addressing third party risk Outsourcing -A growing trend*. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Current%20trends%20in%20outsourcing%20and%20addressing%20third%20party%20risk.pdf. [Accessed 24 Jan. 2024]

Microsoft (2018). *Group Policy API*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-start-page [Accessed 20 Feb. 2024].

Microsoft (2023a). *Azure network security groups overview*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview. [Accessed 20 Feb. 2024]

Microsoft (2023b). *Azure VM Image Builder overview - Azure Virtual Machines*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/virtual-machines/image-builder-overview?tabs=azure-powershell. [Accessed 20 Feb. 2024]

Microsoft (2023c). Sample OT network connectivity models - Microsoft Defender for IoT. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/best-practices/sample-connectivity-models [Accessed 12 Mar. 2024].

Microsoft (2023d). *What is Vulnerability Management? | Microsoft Security*. [online] www.microsoft.com. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management. [Accessed 16 Jan. 2024]

Miehe, S. (2023). *Scaling vulnerability management across thousands of services and more than 150 million findings*. [online] The GitHub Blog. Available at: https://github.blog/2023-12-14-scaling-vulnerability-management-across-thousands-of-services-and-more-than-150-million-findings/. [Accessed 22 Jan. 2024]

Naveen, B. (2020). *InsightVM's Custom Policy Builder: Assessment & Compliance | Rapid7 Blog*. [online] Rapid7. Available at: https://www.rapid7.com/blog/post/2020/06/03/custom-policy-builder-is-now-in-open-preview-in-insightvm/ [Accessed 22 Jan. 2024].

NCSC (2020). *Vulnerability Disclosure Toolkit*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit. [Accessed 29 Jan. 2024]

Neagu, C. (2021). *Introduction to Automated Patch Management*. [online] Heimdal Security Blog. Available at: https://heimdalsecurity.com/blog/automated-patch-management-process/. [Accessed 16 Feb. 2024]

NIST (2019). NVD - Home. [online] Nist.gov. Available at: https://nvd.nist.gov/ [Accessed 18 Mar. 2024].

OWASP (2020). *OWASP Vulnerability Management Guide (OVMG)*. [online] Available at: https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf. [Accessed 31 Jan. 2024]

Palmaers, T. (2013). *Implementing a Vulnerability Management Process | SANS Institute*. [online] www.sans.org. Available at: https://www.sans.org/white-papers/34180/. [Accessed 31 Jan. 2024]

Paskoski, N. (2022a). Best Practices for Cloud Vulnerability Management. [online] RH-ISAC. Available at: https://rhisac.org/cloud-security/best-practices-cloud-vulnerability-management/ [Accessed 8 Mar. 2024].

Paskoski, N. (2022b). *Prioritize Remediation with Risk-Based Vulnerability Management*. [online] RH-ISAC. Available at: https://rhisac.org/vulnerability-management/prioritize-remediation-risk-based-approach/. [Accessed 24 Jan. 2024]

Principled Technologies (2019). *Comparing vulnerability and security configuration assessment coverage of leading VM vendors*. [online] Available at: https://www.principledtechnologies.com/Tenable/Tenable-io-CVE-comparison-1019.pdf [Accessed 22 Jan. 2024].

PubNub (2024). What are Realtime APIs? [online] PubNub. Available at: https://www.pubnub.com/guides/realtime-api/ [Accessed 26 Feb. 2024].

PWC (2022). Vulnerability management. [online] Available at: https://www.pwc.ch/en/publications/2022/ch-vulnerability-management-EN.pdf [Accessed 12 Mar. 2024].

Qualys (2023). *VMDR® with Qualys TruRisk*. [online] Available at: https://www.qualys.com/docs/vmdr-datasheet.pd [Accessed 26 Mar. 2024]

Rapid7 (2021). Integrating Rapid7 Products Into the DevSecOps Cycle | Rapid7 Blog. [online] Rapid7. Available at: https://www.rapid7.com/blog/post/2021/08/02/3-steps-to-integrate-rapid7-products-into-the-devsecops-cycle/ [Accessed 8 Mar. 2024].

Rapid7 (2023a). *What is Vulnerability Management and Vulnerability Scanning*. [online] Rapid7. Available at: https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/. [Accessed 22 Jan. 2024]

Rapid7 (2023b). insightVM Deployment Handbook. [online] Available at: https://www.rapid7.com/globalassets/_pdfs/product_consulting/InsightVM-Nexpose_Pre-Deployment_Guide.pdf/ [Accessed 12 Mar. 2024].

Rapid7 (2024a). *Adjusting risk with criticality | Nexpose Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/nexpose/adjusting-risk-with-criticality/ [Accessed 20 Feb. 2024].

Rapid7 (2024b). Configuring asset discovery | InsightVM Documentation. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/configuring-asset-discovery/. [Accessed 19 Feb. 2024]

Rapid7 (2024c). *Creating a basic report | Nexpose Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/nexpose/creating-a-basic-report/ [Accessed 13 Feb. 2024].

Rapid7 (2024d). Creating reports based on SQL queries | Nexpose Documentation. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/nexpose/creating-reports-based-on-sql-queries [Accessed 6 Mar. 2024].

Rapid7 (2024e). Distributed Scan Engines | InsightVM Documentation. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/configuring-distributed-scan-engines [Accessed 6 Mar. 2024].

Rapid7 (2024f). *Distributing, sharing, and exporting reports | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/distributing-sharing-and-exporting-reports#using-the-web-based-interface-to-configure-report-sharing-settings [Accessed 20 Feb. 2024].

Rapid7 (2024g). *InsightVM Product Integrations*. [online] Rapid7. Available at: https://www.rapid7.com/products/insightvm/integrations/. [Accessed 16 Feb. 2024]

Rapid7 (2024h). *InsightVM Quick Start Guide | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/insightvm-quick-start-guide#programs-and-services [Accessed 20 Feb. 2024].

Rapid7 (2024i). *Managing users and authentication | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/managing-users-and-authentication#configuring-roles-and-permissions [Accessed 20 Feb. 2024].

Rapid7 (2024j). *Mass Deploy | Insight Agent Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insight-agent/mass-deployments [Accessed 13 Feb. 2024].

Rapid7 (2024k). *Notifications | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/notifications/#notification-details [Accessed 23 Feb. 2024].

Rapid7 (2024l). *Planning your Scan Engine Deployment | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/planning-your-scan-engine-deployment/. [Accessed 20 Feb. 2024]

Rapid7 (2024m). Scan templates appendix | InsightVM Documentation. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/scan-templates [Accessed 6 Mar. 2024].

Rapid7 (2024n). Scanning with multiple templates | InsightVM Documentation. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/scanning-with-multiple-templates [Accessed 6 Mar. 2024].

Rapid7 (2024o). Ticketing Integration for Remediation Projects | InsightVM Documentation. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/ticketing-integration-for-remediation-workflow-projects/ [Accessed 6 Mar. 2024].

Rapid7 (2024p). *Vulnerability Management Tool, Top Rated Scanner: InsightVM*. [online] Rapid7. Available at: https://www.rapid7.com/products/insightvm/. [Accessed 22 Jan. 2024]

Raza, M. (2021). What's An App Owner? Application Owner Roles & Responsibilities. [online] BMC Blogs. Available at: https://www.bmc.com/blogs/application-owner/. [Accessed 26 Feb. 2024]

Resolver (2019). *5 Best Practices To Automate Your Vulnerability Management Process*. [online] Resolver. Available at: https://www.resolver.com/blog/vulnerability-management-automation-best-practices/. [Accessed 31 Jan. 2024]

RiskOptics (2023). *Identifying Assets for IT Risk Analysis*. [online] RiskOptics. Available at: https://reciprocity.com/blog/identifying-assets-for-it-risk-analysis/ [Accessed 24 Jan. 2024].

Risto, J. (2021). Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Vulnerability Management Program | Part 1 of 2 | SANS Institute | Jonathan Risto. [online] www.sans.org. Available at: https://www.sans.org/blog/5-metrics-start-measuring-vulnerability-management-program/. [Accessed 31 Jan. 2024]

Rohrs, M. and Wolf, A. (2022). *Cyber trust issues: How vulnerability creates cyber resilience*. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2022/07/cyber-trust-issues-how-openness-creates-cyber-resilience/. [Accessed 18 Jan. 2024]

Rootshell Security. (2023). *Vulnerability Management Trends 2024*. [online] Available at: https://www.rootshellsecurity.net/vulnerability-management-trends/ [Accessed 19 Jan. 2024].

Ryan, E. (2023). The Four Stages of Psychological Safety. [online] Mentorloop Mentoring Software. Available at: https://mentorloop.com/blog/the-four-stages-of-psychological-safety/ [Accessed 8 Mar. 2024].

Scarfone, K. (2023). *How to build a better vulnerability management program | TechTarget*. [online] Security. Available at: https://www.techtarget.com/searchsecurity/tip/How-to-build-a-better-vulnerability-management-program [Accessed 23 Feb. 2024].

Schmittling, R. and Munns, A. (2010). *Performing a Security Risk Assessment*. [online] www.isaca.org. Available at: https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment. [Accessed 20 Feb. 2024]

SecurityScorecard (2024). *8 Top Strategies for Cybersecurity Risk Mitigation in 2024*. [online] SecurityScorecard. Available at: https://securityscorecard.com/blog/8-top-strategies-for-cybersecurity-risk-mitigation/. [Accessed 18 Jan. 2024]

ServiceNow (2024). *Product Documentation | ServiceNow*. [online] docs.servicenow.com. Available at: https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/vulnerability-response/concept/vuln_integrations.html [Accessed 20 Feb. 2024].

Signiant (2024). *Security Concepts: The Importance of Usability | Signiant*. [online] www.signiant.com. Available at: https://www.signiant.com/resources/tech-articles/security-concepts-the-importance-of-usability/. [Accessed 29 Jan. 2024]

Sitcawich, T. (2020). *Vulnerability Remediation vs. Mitigation: What's the Difference? | Rapid7 Blog*. [online] Rapid7. Available at: https://www.rapid7.com/blog/post/2020/09/14/vulnerability-remediation-vs-mitigation-whats-the-difference/. [Accessed 18 Jan. 2024]

SolveXia (2023). 5 Continuous Improvement Examples You Need to Know. [online] www.solvexia.com. Available at: https://www.solvexia.com/blog/5-continuous-improvement-examples-you-need-to-know [Accessed 8 Mar. 2024].

Spirion (2024). Data Classification (Data Management): A Complete Overview. [online] Spirion. Available at: https://www.spirion.com/data-classification/. [Accessed 20 Feb. 2024].

Strobes Security (2023). Vulnerability Prioritization: An Effective Security Approach. [online] Strobes Security. Available at: https://strobes.co/blog/vulnerability-prioritization-an-effective-security-approach/ [Accessed 13 Mar. 2024].

Swanagan, M. (2023). Top 10 Vulnerability Management Metrics & KPIs To Measure Success. [online] PurpleSec. Available at: https://purplesec.us/learn/vulnerability-management-metrics/. [Accessed 20 Feb. 2024]

Tenable (2024a). *Examples: Asset Tagging*. [online] docs.tenable.com. Available at: https://docs.tenable.com/vulnerability-management/Content/Settings/Tagging/ExampleTagging.htm [Accessed 20 Feb. 2024].

Tenable (2024b). *Port Requirements (Tenable Nessus Agent 10.5)*. [online] docs.tenable.com. Available at: https://docs.tenable.com/nessus-agent/10_5/Content/RequirementsDataflow.htm [Accessed 9 Feb. 2024].

Tenable (2024c). Port Requirements (Tenable Security Center 6.3.x). [online] docs.tenable.com. Available at: https://docs.tenable.com/security-center/Content/PortRequirements.htm [Accessed 20 Feb. 2024].

Tenable (2024d). *Proxy Settings (Tenable Nessus Agent 10.5)*. [online] Tenable.com. Available at: https://docs.tenable.com/nessus-agent/Content/ProxySettings.htm [Accessed 9 Feb. 2024].

Tenable (2024e). *Scan Templates*. [online] docs.tenable.com. Available at: https://docs.tenable.com/vulnerability-management/Content/Scans/Templates.htm [Accessed 13 Feb. 2024].

Tenable (2024f). Welcome. [online] Tenable Developer Portal. Available at: https://developer.tenable.com/docs/welcome [Accessed 26 Feb. 2024].

The White House (2023). NATIONAL CYBERSECURITY STRATEGY. [online] The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. [Accessed 21 Feb. 2024].

Thomsen, B. (2023). DATA INTEGRATION PLATFORM VS CUSTOM API INTEGRATION. [online] www.rapidionline.com. Available at: https://www.rapidionline.com/blog/data-integration-platform [Accessed 26 Feb. 2024].

TraceSecurity (2018). *Vulnerability Management Roles and Responsibilities*. [online] TraceSecurity. Available at: https://www.tracesecurity.com/blog/articles/vulnerability-management-roles-and-responsibilities. [Accessed 5 Feb. 2024]

Traficom (2024). CERT. [online] NCSC-FI. Available at: https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert [Accessed 18 Mar. 2024].

Vijayan, J. (2021). 5 tips for reducing false positive security alerts. [online] CSO Online. Available at: https://www.csoonline.com/article/571649/5-tips-for-reducing-false-positive-security-alerts.html. [Accessed 26 Feb. 2024]

Vishwakarma, P. (2023). Vulnerability management for small business | SecOps® Solution. [online] www.secopsolution.com. Available at: https://www.secopsolution.com/blog/vulnerability-management-for-small-business [Accessed 8 Mar. 2024].

Vulnera (2023). Where Vulnerability Management and Compliance Intersect - VULNERA. [online] Vulnera. Available at:

https://vulnera.com/2023/01/25/where-vulnerability-management-and-compliance-intersect/ [Accessed 18 Mar. 2024].

Wagenseil, P. (2022). *Scanning assets in the cloud: Challenges and improvements to make*. [online] SC Media. Available at: https://www.scmagazine.com/resource/scanning-assets-in-the-cloud-challenges-and-improvements-to-make [Accessed 19 Feb. 2024].

Wallis, C. (2022). *Agent-Based vs Network-Based Internal Vulnerability Scanning | Intruder*. [online] www.intruder.io. Available at: https://www.intruder.io/blog/agent-based-vs-network-based-internal-vulnerability-scanning. [Accessed 23 Feb. 2024]

WIZ (2023). 11 Vulnerability Management Best Practices | Wiz. [online] wiz.io. Available at: https://www.wiz.io/academy/vulnerability-management-best-practices [Accessed 8 Mar. 2024