DefendByVirtual Information Security Management Systems (ISMS) Plan

Cyber Security Management TTC6020-3003

Toni Peltola

Michael Herman

Project report

Instructor: Jarmo Nevala

05.03.2023

TIC2021SS

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Contents

Figures

Tables

1 Introduction

This Information Security Management System (ISMS) proposal has been commissioned by DefendByVirtual. The company requires an analysis of its current network and cyber security systems. The system is outdated and vulnerable to threats. The purpose of this report is to provide recommendations for bringing the network up to standard. The report focuses on providing concrete steps based on the most recent ISO asset management, vulnerability and risk assessment standards. It outlines steps to be taken to educate employees and ensure they are informed about the tools they use and the security environment. However, the primary focus is on the concrete steps required for system hardening. ISO standards were selected as the basis for this report due to their widespread use in the industry, although other frameworks such as NIST are also available.

It provides an overview of the current state of DefendByVirtual's network and cyber security systems. This includes vulnerability and risk identification. It provides a detailed analysis of the steps required to bring the system up to ISO standards. The report also provides a roadmap for implementation. This includes timelines and resource requirements. The report aims to provide DefendByVirtual with a clear understanding of the concrete steps required to secure its network and cyber security systems in accordance with ISO standards. Implementing these recommendations will improve considerably the security of company systems and increase protection against potential threats.

2 Project description

An ISMS (information security management system) provides a systematic approach for managing information security. An ISMS framework is centrally managed. It enables the management, monitoring, review and improvement of information security practices in one place. It contains policies, procedures and controls designed to meet the three objectives of information security: confidentiality, integrity and availability. Confidentiality ensures data can only be accessed by authorized personnel. Integrity ensures data accurate and complete. Availability ensures data can be accessed when it is required (Irwin, 2021).

DefendByVirtual required an assessment and update of their security posture in accordance with the technical vulnerability management standards of ISO/IEC 270001:2022 (hereinafter ISO 27001) and ISO/IEC 27002:2022 (hereinafter ISO 27002). Assessment was undertaken on both qualitative and quantitative bases. Qualitative assessment involved an examination of the existing vulnerability management policy framework. The purpose was to identify areas of their technical vulnerability management systems which should be reoriented to reflect international benchmarks and best practice. Quantitative assessment involved a detailed vulnerability testing of the organization’s IT infrastructure and systems.

2.1 Organization description

DefendByVirtual has a past developing defense mechanisms and educational services for companies on a B2B basis. In the future the focus of the company will be on cyber security consulting and information security training.

2.1.1 Business focus

The company offers security specialists to work on consulting projects within the field of cyber security. The main focus is security control evaluation, planning and building. On the training side DefendByVirtual focuses on information security management systems within the boundaries of the ISO standards.

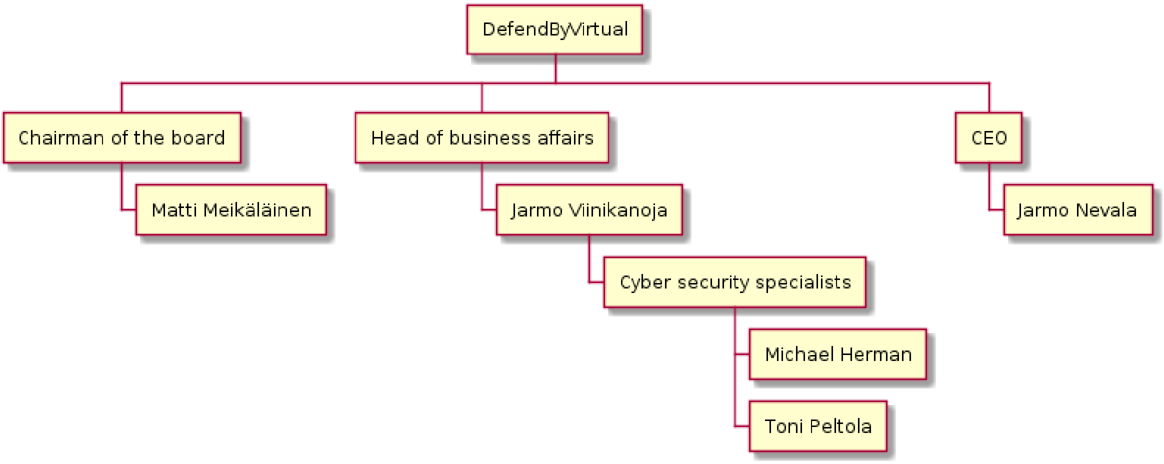
2.1.2 Services

The training focuses for companies that are aiming to receive their ISO certificates. The client's system environments are used as examples.

2.1.3 Organizational structure

DefendByVirtual employs four people in addition to Matti Meikäläinen, who is the company's chairman of the board. The CEO is Jarmo Nevala. The head of business affairs is Jarmo Viinikanoja. Toni Peltola and Michael Herman work as security specialists.

Figure 1: Organizational structure



3 Cyber strategy

The company's cyber strategy is based on ISO 27001:2022 and 27002:2022. These standards deal with a wide range of issues related to the management of IT systems. The foundation of the cyber strategy is the ISMS (Information Security Management System). ISO 27001 outlines general guidelines and ISO 27002 provides concrete steps to be taken to secure organizational assets. It is these steps which are referred to in this report. The purpose of the cyber strategy is to ensure clients and partners are reliably informed about the company's security posture.

3.1 Operating environment SWOT analysis

3.1.1 Strengths

The systems within the environment are in an exposed and abandoned state but the system and assets it contains are solid. Once everything is up and running, the best available resources are available to work on the company's goals. DefendByVirtual has valid SOAR and SIEMS systems, Kali Linux tools for penetration testing, Security Onion and so forth. A great deal can be achieved with the tools available.

3.1.2 Weaknesses

The company is taking its first steps, so it is tied to using open-source software. With better funding, systems like Cortex XDR could be implemented. There seems to be a lack of institutional knowledge as to how these systems should be maintained. This is in and of itself poses a critical threat to security. It is imperative that DefendByVirtual has on hand employees capable of understanding and maintaining these complex systems.

3.1.3 Opportunities

There are clear opportunities for growth. Once a decent customer base is established, the environment can be updated. For now, company assets can be secured using open-source tools. In the future the company should consider upgrading to more advanced tools which provide greater security. Palo Alto Cortex XDR is an advanced security system which the company should consider investing in once basic security systems are in place.

3.1.4 Threats

The system is vulnerable to a wide range of malicious threats. These range from cyber-attacks to data breaches, to security breaches and environmental disasters. A lot of work needs to be done to secure the physical environment. This document has been compiled to meet this objective.

DefendByVirtual's systems and assets are at risk from a range of cyber-attacks. These include malware infections, phishing scams, and denial-of-service (DoS) attacks. Implementing additional security measures, such as better firewalls, intrusion detection systems, and employee training programs can minimize these risks.

The company's systems are at risk of data breaches. This could result in the loss or theft of sensitive company and client information. Appropriate data encryption, access controls, and data backup procedures should be in place in order to protect against this threat. The company's operations may also be vulnerable to natural disasters. These can disrupt business operations and damage assets. Contingency plans should be in place to minimize the impact of such events. This could include backup power generators, disaster recovery plans, and insurance coverage. Threat management is discussed in greater detail in section 6.2.

3.2 Public security policy

There are two aspects of the security framework: private and public. Maintaining a publicly accessible security framework has a range of advantages. First, it promotes transparency. This is of critical importance from a business standpoint; clients and partners should be made aware our security policies. This adds predictability and a layer of professionalism to business activities. It also compels the company to adhere to well defined principles and clearly delineates responses to potential threats. The involvement of the company in the promotion of ISO standards necessitates a strict adherence to its principles.

3.3 Implemented Enterprise Security

DefendByVirtual does not currently have a meaningful security framework in place. Quantitative assessment practices and the qualitative policy framework underpinning them require urgent revision. Almost all systems are exposed. The company is highly vulnerable in its current state. The report provides details on the specific nature of these vulnerabilities. It identifies key problem areas and proposes a structured framework with which to address them. The scope of the report is limited to asset management and vulnerability assessment. A mitigation strategy is expected to follow at a later date.

4 ISO Standards

ISO 27001 and 27002 provide guidelines for managing IT systems. Section 5 of both documents specifically address asset management standards. ISO 27002 provides concrete steps for securing organizational assets. This includes maintaining an inventory of assets, establishing rules for acceptable use, setting standards for asset return, classifying information based on importance, labeling information, and securing information during transfer. Adherence to these principles can help protect sensitive information.

4.1 ISO 27001

ISO 27001 is an international management-related standard. It is used to evaluate and address the various risks related to an organization's daily functions. This is specified in the Information Security Management System (ISMS). The ISMS covers the informational security environment in which companies operate and future security needs. ISO 27001 does not specifically delineate how risk should be managed. It instead establishes general principles which organizations should consider when developing and implementing cybersecurity frameworks.

4.2 ISO 27002

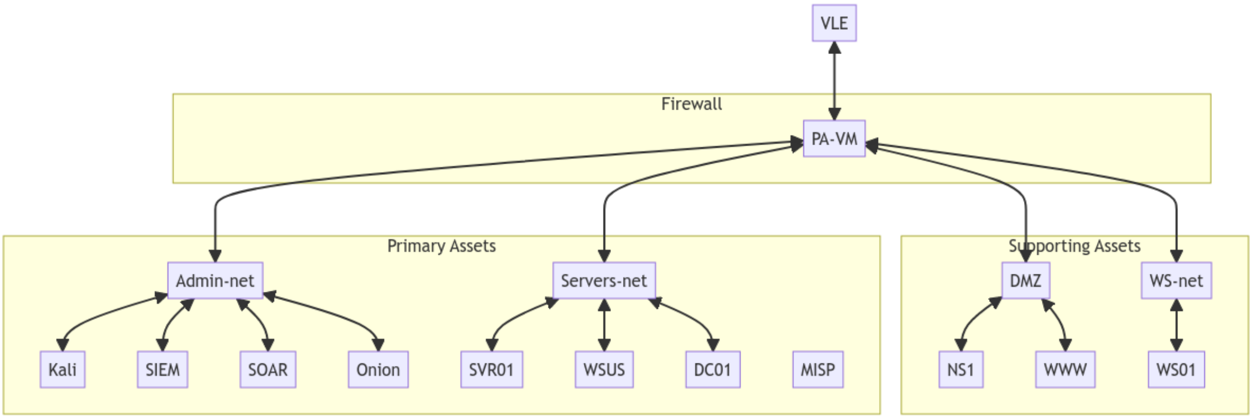
ISO 27002 expands on the principles outlined in ISO 27002. It provides best practices for information security management and covers a range of information security subjects. These include risk management, security policy, physical and environmental security, access control, and incident management. The standard provides a comprehensive framework for organizations to protect information assets and ensure their confidentiality, integrity, and availability. The key difference from ISO 27001 is that it provides concrete steps designed to help organizations implement and maintain an effective information security management system.

5 Asset Management

5.1 Asset classification

Assessing assets in an IT ecosystem involves identifying and evaluating resources most essential to the functioning and success of the system. This includes hardware software, data, networks, people and processes. Primary assets are identified on the basis of impact. A failure of any one of these components would impose significant costs on the business. It is of critical importance to assess the current state of these assets with a view towards improving their overall resilience and reliability. Risk profiles for each element of the system is outline the likelihood and impact of various risks. This helps prioritize areas for improvement and future investment. The report proposes a framework to address these issues.

Figure 2: Asset classification



5.1.1 Primary assets

On Admin-net, Onion, SIEM, SOAR, Kali, Rocky-WS, MISP are good examples of primary assets according to the above criteria. The firewall, PA-VM, which is the first line of defence against attackers also falls into this category. The same can be said of the DC01, WSUS, SRV01 on the server side. These machines form the backbone of DefendByVirtual's IT infrastructure. A loss of such machines would incur significant replacement costs. The financial and business implications of a failure of any one of these machines is considerable. Both the physical machines and the data they contain are both of vital importance to business operations. It is of critical importance the vulnerabilities identified in these machines be remedied at the earliest possible date.

5.1.2 Secondary assets

The assets in the DMZ and WS-net are considered secondary assets. These include WSO1, WWW and NS1. Losses of or damage to these assets in this class only impose short-term financial costs. Such costs are manageable from a business standpoint. Individual workstations can be replaced with little fanfare because such assets do not have a direct impact on business operations. Their role is instead to facilitate the work of others. They do not contain sensitive data. Losing machines in this asset class would not pose a severe threat to the company.

5.1.3 People and processes

IT systems are ultimately maintained by people. People and processes play a crucial role in the proper functioning and success of any IT system. End-users interact with technology, data, and all other components of the system. Their actions and decisions can impact system performance and security. Having skilled and knowledgeable staff who can effectively operate and maintain the system is essential to ensure its optimal performance. It is of critical importance that DefendByVirtual have appropriately skilled staff on hand to manage the security of its IT infrastructure.

Processes refer to the set of activities and procedures in place designed to ensure the efficient and effective functioning of the IT ecosystem. Well-designed and documented processes help ensure tasks are performed consistently, accurately, and in compliance with regulations and policies. This ensure updates and modifications to the system are properly tested and implemented, minimizing the risk of downtime or other issues. Adherence to international standards is one way of ensuring the processes associated with maintaining the company's security posture are systematic and sufficiently wide in scope.

5.2 Key assets

Key assets are identified on the basis of their significance to the continued functioning of the business. Primary assets are not necessarily considered key assets. The role of the primary assets located in Admin-net is to administer business operations. The role of Servers-net is to store company data. The company's business model assumes a steady flow of client and business data into its servers. The role of primary assets is to store and protect company data. Company data is considered a key asset. The loss of this data would be catastrophic.

Data is thought of as a key asset from a security perspective because it is often the primary target of cyber attacks. Attackers seek to gain unauthorized access to sensitive information which can be used for a range of malicious purposes. This can include personal information, financial information, or intellectual property. Data is essential for business operations and decision-making. Loss of access to or control of critical data could lead to significant financial and reputational damage. As DefendByVirtual matures the value of its data will increase. This data will inform strategic decisions and drive innovation. Data protection must therefore be the core of the security posture. Encryption, firewalls, intrusion detection systems and other security measures are implemented in primary assets with the express purpose of safeguarding these assets.

5.2.1 Asset valuation

The selected assets are assessed on a scale of 1 to 5, with 5 being the most valuable and 1 the least valuable.

Table 1: Asset scale valuation

Asset	IP	Scale values	Network	Valuation basis
Kali-WS	10.2.0.13	5	Admin-net	Managerial system within the company's security environment
SIEM	10.2.0.11	5	Admin-net	Automated alert collection and notification system
SOAR	10.2.0.12	5	Admin-net	Incident analysis and triage
Onion	10.2.0.10	5	Admin-net	Intrusion detection (IDS), network security monitoring (NSM), and packet capture (PCAP) analysis
SRVR01	10.3.0.12	5	Servers-net	Houses business critical data
WWW	10.4.0.11	2	DMZ	Internet-facing; does not have local access to sensitive data
WS01	10.1.0.10	3	WS-net	Location within the secured network from which basic administrative functions are performed

5.2.2 Qualitative and quantitative assessment

Qualitative and quantitative assessments are critical to ensuring IT infrastructure is well-managed, optimized, and aligned with organizational objectives. Qualitative assessment of IT infrastructure policy focuses on the policies, procedures, and practices governing the use and management of IT infrastructure. Quantitative assessments of physical IT infrastructure focus on the physical components of the IT infrastructure. These include servers, networks, and storage devices.

Quantitative assessment of DefendByVirtual security framework involves analyzing its security policies and procedures. The strengths, weaknesses, opportunities and threats identified are the basis for the recommendations proposed in this report. The purpose of these recommendations is to improve the policies and procedures associated with the company’s IT governance. Quantitative assessment of physical IT infrastructure involves analyzing data on the physical components of the infrastructure. The purpose is to identify measurable areas for improvement and optimization. Implementing the recommended changes to the physical environment would improve the performance, capacity and scalability of the IT system.

6 Threat management

6.1 Introduction

Threat management identifies, assesses and prioritizes vulnerabilities within asset environments. It then takes steps towards eliminating and mitigating them. The aim is to protect assets from security breaches, unauthorized access, sensitive information-loss and exploitation. This is achieved through regular scans, software updates and patch management. Regular monitoring of network activity and implementation of security controls is also necessary.

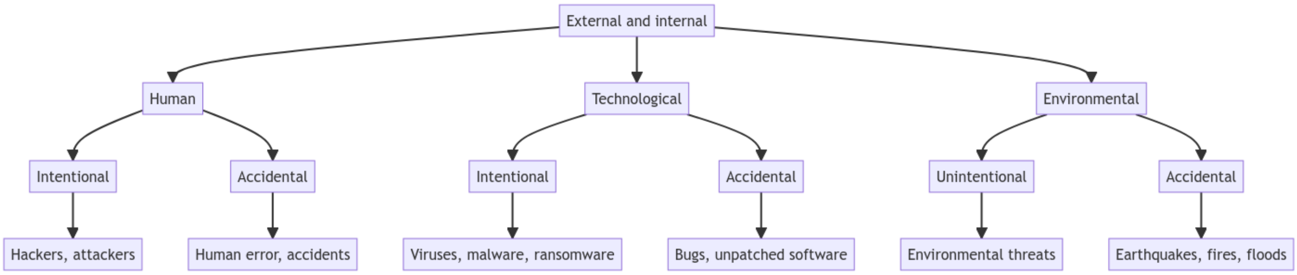
The report proposes a security framework based on structured policy-level governance of physical infrastructure. Policy in this case refers to management frameworks. IT infrastructure refers to physical assets. A cohesive security framework should entail meaningful and effective management of physical infrastructure. It is not enough to simply assess the state the company's assets. A systematic, actionable framework for sustainable and secure asset management is a critical component of the security posture.

ISO 27001 and ISO 27002 have specific standards relating to threat management. These form the basis of the proposals presented in this report. The most relevant sections are section 8.8 and 8.19. Section 8.8 concerns the prevention and management of technical vulnerabilities. Section 8.19 concerns the secure management of software installation and the prevention of possible security breaches.

6.2 Threat classification

Base-level threat classifications can be divided into two sections: external and internal. Threats are further divided into human, technological and environmental threats. Within these there are both malicious and non-malicious actions. These can be further described as either accidental or intentional.

Figure 3: Threat typology (adapted from Jouini et al, 2014)



Any one of the listed threats can lead to multiple different types of security breaches. This can then lead to loss or destruction of information or assets, monetary loss or reputational damage.

6.3 Company asset threat management

Some assets within the DefendByVirtual environment are more exposed to internal threats. Some are exposed to external threats. Internal and external threats are understood in terms of human, technological and environmental factors and are broken down below.

6.3.1 Human threats

Kali, SIEM, SOAR, SVR01, WWW, WS01 and Onion are mostly in danger from human-related threats, both accidental and intentional. These systems are used by humans and are vulnerable to errors and accidents. This also makes them attractive to malicious attackers. DefendByVirtual's involvement in the cyber-security industry could easily generate interest among bad actors in the company's systems and data. System and client information are all stored in company assets within company assets. The protection of physical assets and confidential client information are central to the company's operations.

6.3.2 Technological threats

As the assets stand today, they are extremely vulnerable to technological threats. The environment has been abandoned and is out of date. Bugs, unpatched software and poor passwords are rampant in all of the chosen assets. Immediate action towards fixing these problems should be taken. Vulnerabilities are in most cases accidental and related to previous workers leaving the company. No intentional technological threats have been documented.

6.3.3 Environmental threats

Great care should be taken to prevent potential environmental threats, such as fires, electrical malfunctions and 'acts of god'. None of the assets are safe from this type of environmental threat. The greatest care should therefore be paid towards server room allocations. Following carefully all relevant governmental safety regulations is one way to mitigate environmental threats.

6.3.4 Vulnerabilities within the environment

Assets in the environment were scanned using the Greenbone Security Assistant. Multiple vulnerabilities were found. Results over 6.0 were considered the most threatening. The most vulnerable machines are the ones described in this report. Four assets belong to the Admin-net environment. Admin-net constitutes the core of DefendByVirtual's security systems. Admin-net assets pose the most significant security risk.

Admin-net computers are critical for day-to-day operations. The loss of such assets to any kind of attack would be a serious blow to company credibility. DefendByVirtual cannot claim to be a leader in the field of cyber-security while running outdated security software in their core administrative environment. Fixing these vulnerabilities is of vital importance. The WWW environment, while not business-critical, was also found to be at risk. A comprehensive assessment of these vulnerabilities is presented below.

7 Security environment

7.1 Threat management

DefendByVirtual's IT network is divided into four segments connected via a Palo Alto firewall. WS-net contains a single workstation used by the company. Admin-net contains security related instances which include SIEM and SOAR systems, the Security Onion, Kali Linux, Rocky-WS and MISP. Server systems are maintained on the Servers-net machine. The DMZ (demilitarized zone) contains Internet-facing websites.

7.2 Threat assessment

Figure 4: Overall vulnerability

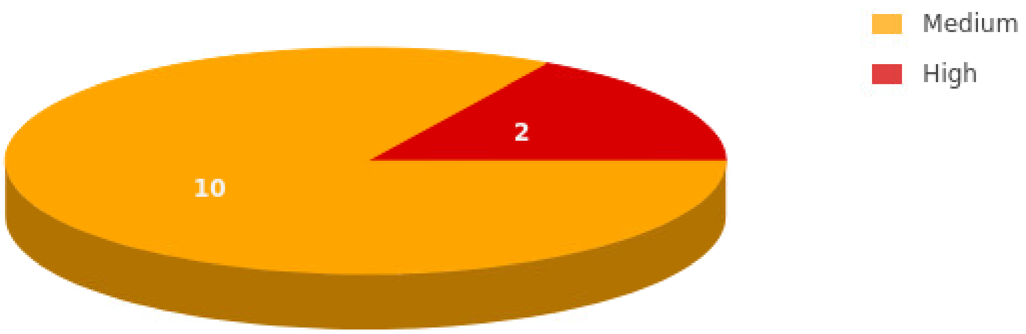
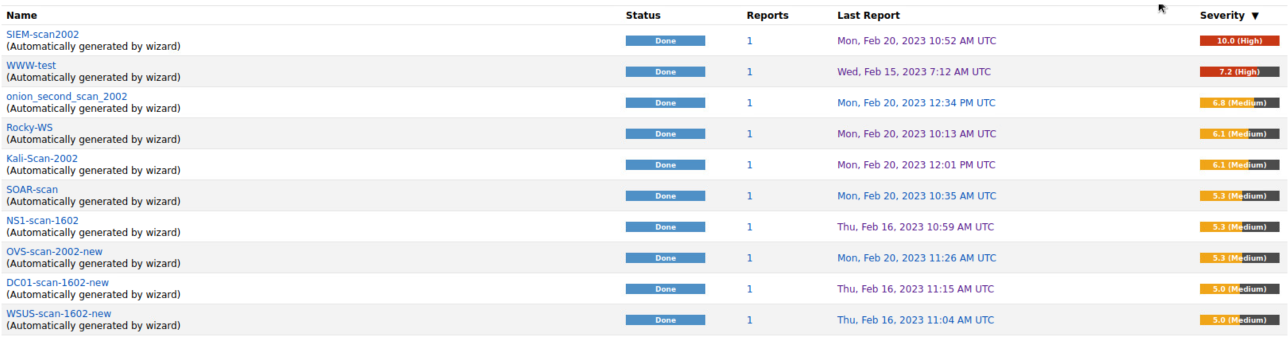


Figure 5: Overall vulnerability breakdown



Name	Status	Reports	Last Report	Severity ▼
SIEM-scan2002 (Automatically generated by wizard)	Done	1	Mon, Feb 20, 2023 10:52 AM UTC	10.0 (High)
WWW-test (Automatically generated by wizard)	Done	1	Wed, Feb 15, 2023 7:12 AM UTC	7.2 (High)
onion_second_scan_2002 (Automatically generated by wizard)	Done	1	Mon, Feb 20, 2023 12:34 PM UTC	6.8 (Medium)
Rocky-WS (Automatically generated by wizard)	Done	1	Mon, Feb 20, 2023 10:13 AM UTC	6.1 (Medium)
Kali-Scan-2002 (Automatically generated by wizard)	Done	1	Mon, Feb 20, 2023 12:01 PM UTC	6.1 (Medium)
SOAR-scan (Automatically generated by wizard)	Done	1	Mon, Feb 20, 2023 10:35 AM UTC	5.3 (Medium)
NS1-scan-1602 (Automatically generated by wizard)	Done	1	Thu, Feb 16, 2023 10:59 AM UTC	5.3 (Medium)
OVS-scan-2002-new (Automatically generated by wizard)	Done	1	Mon, Feb 20, 2023 11:26 AM UTC	5.3 (Medium)
DC01-scan-1602-new (Automatically generated by wizard)	Done	1	Thu, Feb 16, 2023 11:15 AM UTC	5.0 (Medium)
WSUS-scan-1602-new (Automatically generated by wizard)	Done	1	Thu, Feb 16, 2023 11:04 AM UTC	5.0 (Medium)

Vulnerabilities associated with individual machines are discussed below. Admin-net vulnerabilities and their impacts are discussed fist. This is followed by a discussion of vulnerabilities in Servers-net, WS-net and the DMZ.

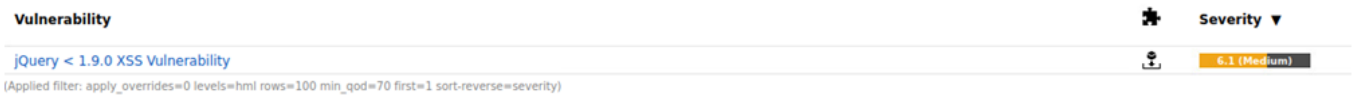
7.2.1 Admin-net

7.2.1.1 Kali vulnerabilities and impacts

The Greenbone scan indicates version 1.9.0 of the jQuery JavaScript library is out of date. This makes the Kali environment susceptible to cross-site scripting (XSS) attacks. Through this exploit malicious code injected into a website could be executed by Kali's browser. This puts sensitive information located on the Kali machine at risk.

Kali is one of the most important systems within the company's environment. The impact of an attack on this machine would be catastrophic and would severely affect the capacity of DefendByVirtual to continue its operations. This vulnerability should be addressed with the highest priority.

Figure 6: Kali scan result



Vulnerability		Severity ▼
jQuery < 1.9.0 XSS Vulnerability		6.1 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

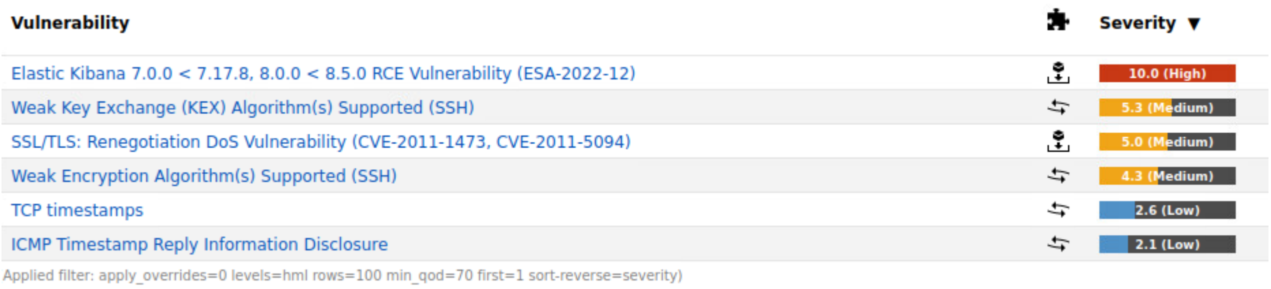
7.2.1.2 SIEM vulnerabilities and impacts

Greenbone indicates Elastic Kibana is out of date. Versions 7.0.0-7.17.8 and 8.0.0-8.5.0 are vulnerable to XSS attacks. ESA-2022-12 suggests the vulnerability could potentially lead to a remote code execution (RCE). This would allow attackers to excecute commands with Kibana permissions.

The risks associated with this vulnerabiilty are considerable. Greenbone assigns it a CVSS score of 10.0. This is the highest severity rating possible. There is a high risk of exploitation.

SIEM vulnerabilities have a high impact value. An RCE could potentially hand control of company assets to malicious actors. It would cripple day-to-day operations and inflict serious reputational damage. It poses an existential threat to the company. This vulnerability should be addressed without delay.

Figure 7: SIEM scan result



Vulnerability	🧩	Severity ▼
Elastic Kibana 7.0.0 < 7.17.8, 8.0.0 < 8.5.0 RCE Vulnerability (ESA-2022-12)	⤓	10.0 (High)
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	⇆	5.3 (Medium)
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	⤓	5.0 (Medium)
Weak Encryption Algorithm(s) Supported (SSH)	⇆	4.3 (Medium)
TCP timestamps	⇆	2.6 (Low)
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)

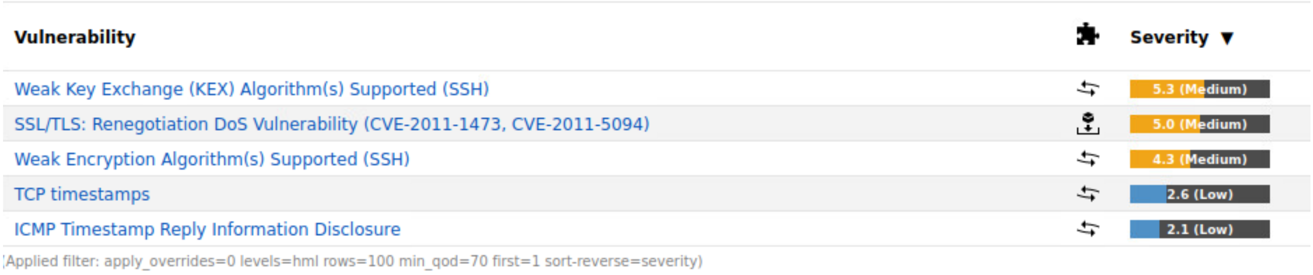
Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

7.2.1.3 SOAR vulnerabilities and impacts

The SOAR environment contains a range of vulnerabilities. But these vulnerabilities represent only medium level threats. While they do not exceed the 6.0 threshold they should nevertheless be fixed. The most significant threat within the environment is a 5.3 medium vulnerability known as Weak Key Exchange (KEX). This means the remote SSH server is configured to allow and support KEX algorithms.

SOAR is a primary asset within DefendByVirtual's environment. Its role is to protect key assets. It should be fully operational and secure at all times. Automated responses to threats detected within the SIEM and MISP environments are run through the SOAR ma chine. Automated threat detection is the first line of defense. A failure of this system could have a potentially high impact.

Figure 8: SOAR scan result



Vulnerability	🧩	Severity ▼
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	⇆	5.3 (Medium)
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	⤓	5.0 (Medium)
Weak Encryption Algorithm(s) Supported (SSH)	⇆	4.3 (Medium)
TCP timestamps	⇆	2.6 (Low)
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)

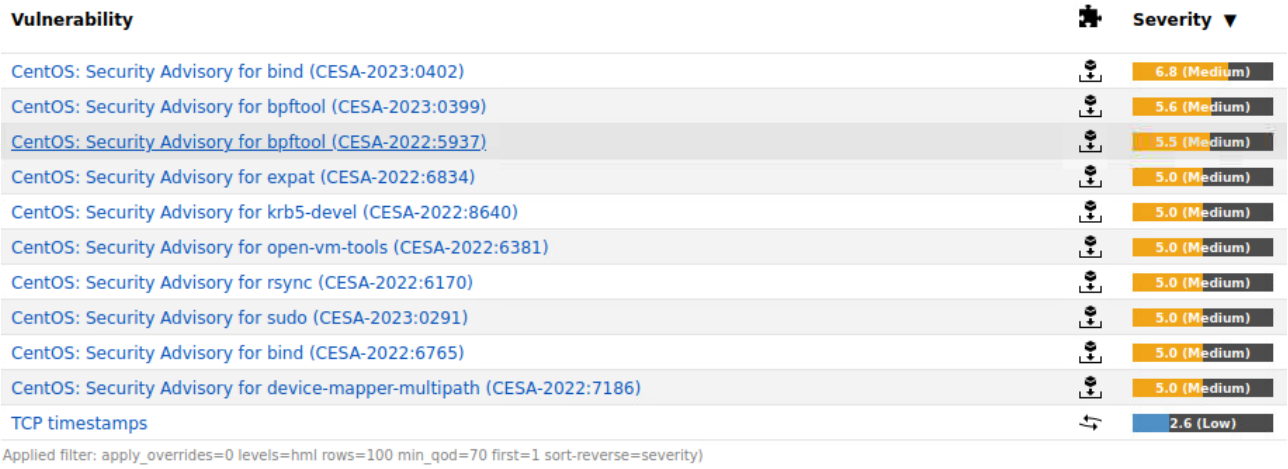
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

7.2.1.3 Onion vulnerabilities and impacts

The Onion system contains multiple medium level vulnerabilities. Most of these are not the most pressing concerns. They are nevertheless on the higher side of the spectrum. These include multiple threats concerning CentOS security advisor. CentOS: Security Advisory for bind (CESA-2023:0402) is the top-rated vulnerability with a CVSS score of 6.8. This makes the environment vulnerable to possible cache poisoning.

Onion is one of the most important systems within the DefendByVirtual environment. Even low and medium level vulnerabilities should be addressed as soon as possible. The onion system is one of the company’s primary assets. Any compromise of the Onion system would have a high financial and reputational impact. The company’s activities in cyber-security development and training demand all assets and environments be up-to-date and hardened to the maximum.

Figure 9: Onion scan result



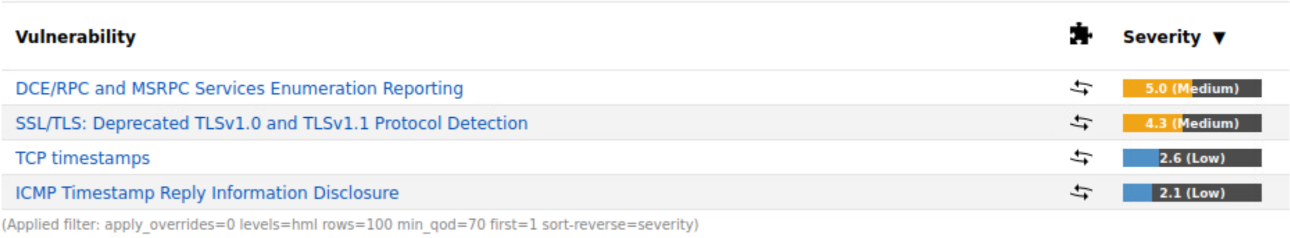
Vulnerability	Severity ▼
CentOS: Security Advisory for bind (CESA-2023:0402)	6.8 (Medium)
CentOS: Security Advisory for bpftool (CESA-2023:0399)	5.6 (Medium)
CentOS: Security Advisory for bpftool (CESA-2022:5937)	5.5 (Medium)
CentOS: Security Advisory for expat (CESA-2022:6834)	5.0 (Medium)
CentOS: Security Advisory for krb5-devel (CESA-2022:8640)	5.0 (Medium)
CentOS: Security Advisory for open-vm-tools (CESA-2022:6381)	5.0 (Medium)
CentOS: Security Advisory for rsync (CESA-2022:6170)	5.0 (Medium)
CentOS: Security Advisory for sudo (CESA-2023:0291)	5.0 (Medium)
CentOS: Security Advisory for bind (CESA-2022:6765)	5.0 (Medium)
CentOS: Security Advisory for device-mapper-multipath (CESA-2022:7186)	5.0 (Medium)
TCP timestamps	2.6 (Low)

Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

7.2.1.4 WS01 vulnerabilities and impacts

There are no major vulnerabilities found from WS01 but they are noted nonetheless. None of the threats rise above the 6.0 threshold. The top vulnerability is the 5.0 medium threat known as the DCE/RPC and MSRPC Services Enumeration Reporting issue.

Vulnerabilities on WS01 are medium level in nature. The workstation machine falls under the human error threat classification factor. Workstations should be closely monitored. They are extremely vulnerable to phishing attempts and other threats caused by unpredictable end-user behavior. The workstation should be tightly controlled and all vulnerabilities should be fixed. The impact of the abovementioned vulnerabilities is not large but they can potentially cascade into larger problems.



Vulnerability		Severity ▼
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)
TCP timestamps	⇆	2.6 (Low)
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

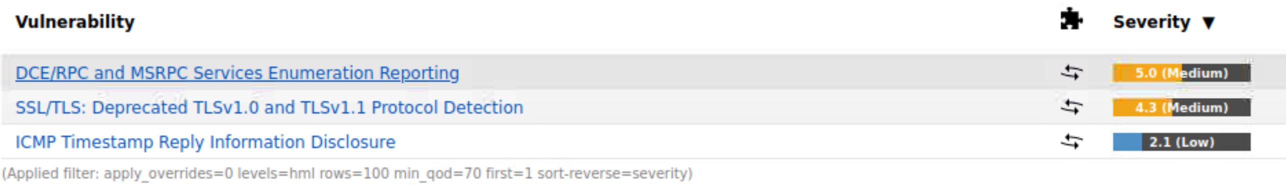
7.2.2 Servers-net

7.2.2.1 SVR01 vulnerabilities and impacts

SVR01 does not contain any significant vulnerabilities. They should nevertheless be treated the same as high-level vulnerabilities given the importance of the server environment. The highest-level vulnerability is 5.0. This relates to the Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) and Microsoft Remote Procedure Call (MSRPC) Services Enumeration Reporting. The issue indicates services running on the remote host can potentially be enumerated by connecting to port 135 and making the appropriate queries.

The integrity of the server environment is of critical importance. Even minor vulnerabilities should be addressed. A server loss or outage could have a potentially serious impact on daily operations. Data on company servers should be backed up and secured at all costs.

Figure 10: SRVR02 scan result



Vulnerability		Severity ▼
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

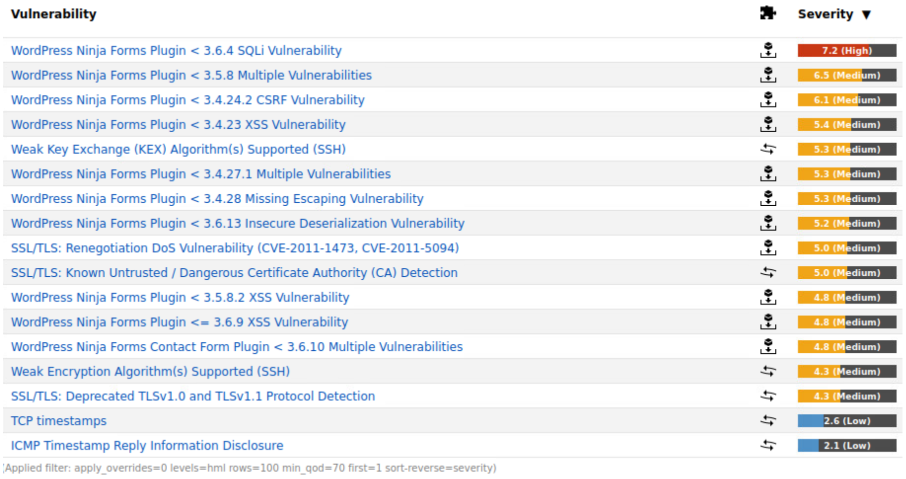
7.2.3 DMZ

7.2.3.1 WWW vulnerabilities and impacts

The WWW environment has a number of vulnerabilities with a CSVV value of over 6.0. Many of these are associated with the WordPress content management system. These primarily affect the Ninja Forms Plugin. Vulnerabilities occur over a wide range of versions and affect multiple WordPress features. These include an SQLi vulnerability affecting version 3.4.24.2 and a CSRF vulnerability affecting version 3.5.8. Of greatest concern is the SQLi vulnerability. The vulnerability has a CSVV value of 7.2. These problems can be resolved through software updates. In its current state the system is vulnerable to SQL injections, email injections through an unprotected REST-API and cross-site request forgery.

There are considerable problems within the WWW environment but they are fixable. The WWW machine is located in the DMZ and is isolated from the rest of the network. Even though the machine is vulnerable it is easily contained. Breaches are logged in the Admin-net, SIEM and SOAR systems. A malicious event would not have a meaningful impact on the daily activities at DefendByVirtual. This does not mean these vulnerabilities should be ignored. All potential backdoors in the system should be shut. Any access point can allow attackers access to sensitive internal data.

Figure 11: WWW scan result



Vulnerability	Severity ▼
WordPress Ninja Forms Plugin < 3.6.4 SQLi Vulnerability	7.2 (High)
WordPress Ninja Forms Plugin < 3.5.8 Multiple Vulnerabilities	6.5 (Medium)
WordPress Ninja Forms Plugin < 3.4.24.2 CSRF Vulnerability	6.1 (Medium)
WordPress Ninja Forms Plugin < 3.4.23 XSS Vulnerability	5.4 (Medium)
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)
WordPress Ninja Forms Plugin < 3.4.27.1 Multiple Vulnerabilities	5.3 (Medium)
WordPress Ninja Forms Plugin < 3.4.28 Missing Escaping Vulnerability	5.3 (Medium)
WordPress Ninja Forms Plugin < 3.6.13 Insecure Deserialization Vulnerability	5.2 (Medium)
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)
SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection	5.0 (Medium)
WordPress Ninja Forms Plugin < 3.5.8.2 XSS Vulnerability	4.8 (Medium)
WordPress Ninja Forms Plugin <= 3.6.9 XSS Vulnerability	4.8 (Medium)
WordPress Ninja Forms Contact Form Plugin < 3.6.10 Multiple Vulnerabilities	4.8 (Medium)
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)
TCP timestamps	2.6 (Low)
ICMP Timestamp Reply Information Disclosure	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

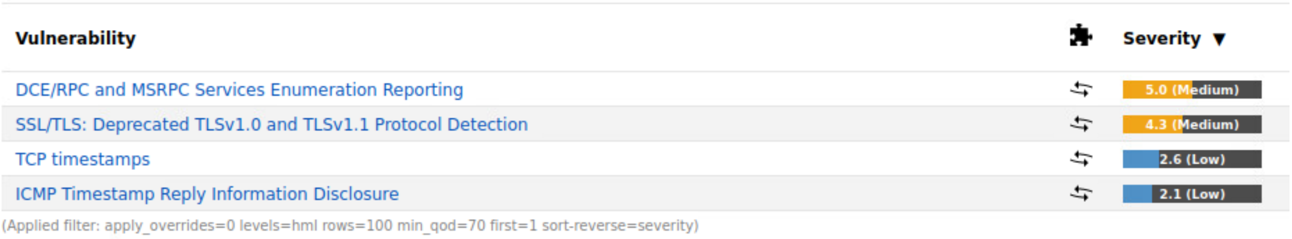
7.2.4 WS-net

7.2.4.1 WS01 vulnerabilities and impacts

There are no major vulnerabilities found from WS01 but they are noted nonetheless. None of the threats rise above the 6.0 threshold. The top vulnerability is the 5.0 medium threat known as the DCE/RPC and MSRPC Services Enumeration Reporting issue.

Vulnerabilities on WS01 are medium level in nature. The workstation machine falls under the human error threat classification factor. Workstations should be closely monitored. They are extremely vulnerable to phishing attempts and other threats caused by unpredictable end-user behavior. The workstation should be tightly controlled and all vulnerabilities should be fixed because minor vulnerabilities can potentially still have a larger impact down the line.

Figure 12: WS-01 scan result



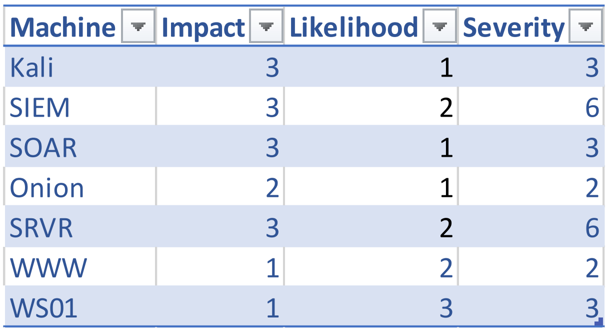
Vulnerability		Severity ▼
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)
TCP timestamps	⇆	2.6 (Low)
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

7.2.5 Threat levels

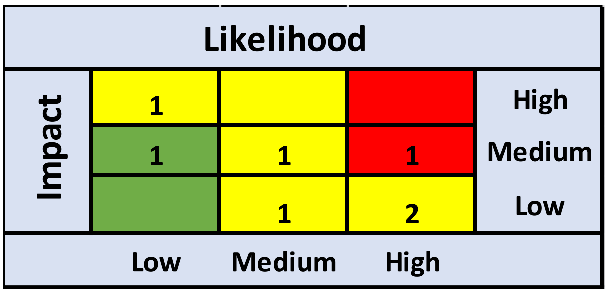
The table below contextualizes the analysis in section 7.2 into a semi-quantitative risk analysis matrix. The matrix has predefined values based on possibility and severity. Values are on a scale of 1-3. Severity values are multiplied by likelihood values. Green values are associated with low-possibility, low severity risks. Yellow values are associated with moderate risk or severity. High risk values are associated with the color red. The highest instance of risk occurs in the topmost, rightmost quadrant. This means an attack is both highly likely and highly impactful. From a triage standpoint these are the risks which should be dealt with first as a matter of course.

Table 2: Threat level distribution



Machine	Impact	Likelihood	Severity
Kali	3	1	3
SIEM	3	2	6
SOAR	3	1	3
Onion	2	1	2
SRVR	3	2	6
WWW	1	2	2
WS01	1	3	3

Table 3: Threat level matrix (adapted from lecture material)



	Likelihood			
Impact	🟨 1	🟨	🟥	High
	🟩 1	🟨 1	🟥 1	Medium
	🟩	🟨 1	🟨 2	Low
	Low	Medium	High	

Tables 2 and 3 provide a graphic illustration of the state of company IT infrastructure. Each machine is assessed by the impact or likelihood of an attack. The purpose of the matrix is to provide security personnel with a greater understanding of the relationship between likelihood and impact. This provides valuable information in terms of resource allocation. It is immediately apparent attacks with the highest likelihood of occurrence are also the least impactful.

WSO1, the machine represented by the leftmost and topmost 1, is the most vulnerable. But an attack on this machine would have a negligible impact on the network as a whole. No machine falls into the high impact, high likelihood category. The SIEM machine is the most at risk in terms of impact and likelihood. But even this is not a doomsday scenario. Most machines are somewhere in the middle. Risk to the Kali and SOAR machines is high impact but low likelihood. The matrix indicates the network is in better shape than the raw scans suggest.

8 Risk management

The best way to manage cyber security risks is to prevent them from occurring. This can be achieved through various measures. These include implementing strong passwords and access controls, regularly updating software and systems, and conducting regular security audits. Preventative measures should be accompanied by strong detection mechanisms. Such mechanisms should be able to identify potential threats. Intrusion detection and prevention systems, firewalls, and SIEM systems should be at the core of DefendByVirtual's security posture.

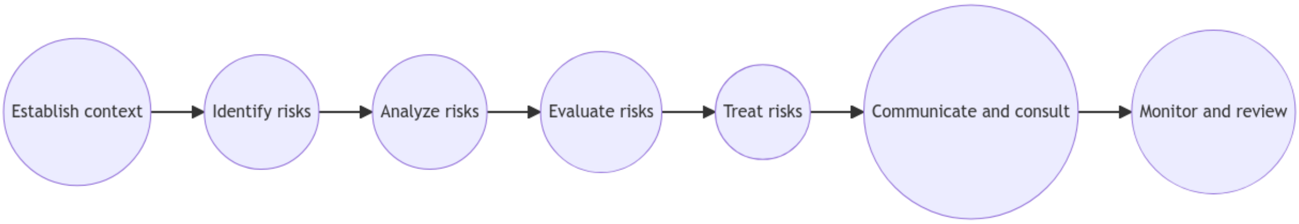
It is also necessary to have a well-defined incident response plan in event of a cyber-attack or data breach. A team should be in place at all times to respond to incidents, isolate affected systems, and take steps to minimize any attack impacts. Data should be quickly and easily recoverable. Systems and data should be restorable. Incident analysis procedures should be in place so attack causes can be identified. The purpose of incident analysis should be to understand and address whatever vulnerabilities allowed the attack to happen. Active measures should be taken to prevent similar incidents from occurring in the future.

Cyber security risks are constantly evolving. It is important to continuously monitor and improve the risk management strategy over time. Policies and procedures should be reviewed on a regular basis. It is important to stay up to date with the latest cyber security threats and trends. Training should be provided to staff to ensure they are aware of security issues and best practice.

8.1 Threat management framework

An effective security regime should include a policy framework based on appropriate guidelines for measuring and addressing risk. It should also cover practical aspects of operational security. The framework should provide systematic steps for managing risk. The proposed framework is based on sections 8.8 and 8.19 of ISOs 27001 and 27002 (2022) and provides reasonable means by which to achieve this. Key themes include confidentiality, integrity and availability of information assets. It also proposes specific processes to identify, assess and manage security risks.

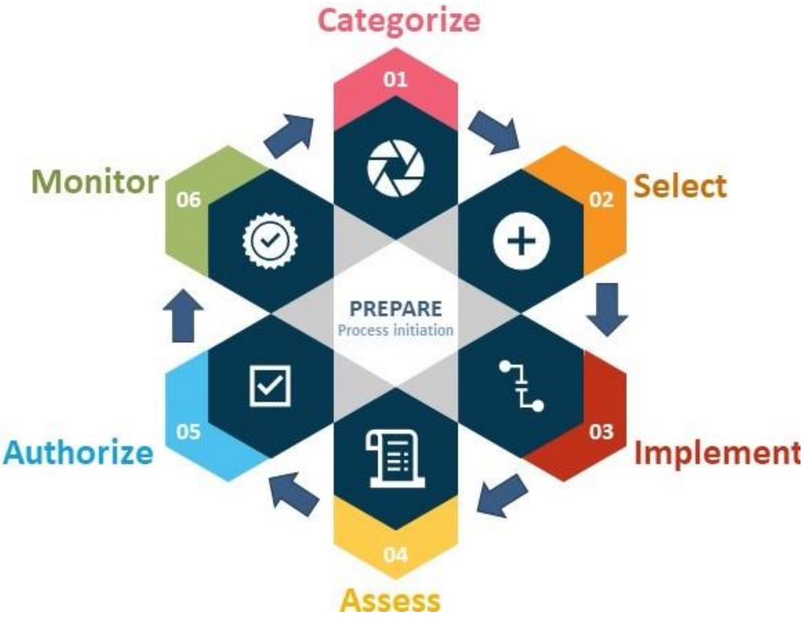
Figure 13: Threat management taxonomy (adapted from ISO 27001, 2022)



The diagram above illustrates the different categories of the ISO threat management framework. A more detailed breakdown follows.

1. *Establish context*. Identify the scope of the threat management process and internal and external factors affecting it.
2. *Identify risks*. Identify potential threats and vulnerabilities which could impact organizational assets. This includes information, systems, and processes.
3. *Analyze risks*. Assess the likelihood and impact of each identified risk and prioritize based on potential impact.
4. Evaluate risks. Evaluate the effectiveness of existing controls in place to manage the identified risks.
5. *Treat risks*. This stage involves implementing appropriate risk treatment measures to mitigate the identified risks.
6. *Communicate and consult.* Communicating the results of the risk assessment to relevant stakeholders and seeking input and feedback to improve the risk management process.
7. *Monitor and review*. Monitoring and reviewing the effectiveness of the risk management process and making necessary adjustments to ensure it remains effective over time.

Figure 14: Risk management framework (adapted from lecture material)



The diagram above depicts a continuous cycle of ISO-based risk management. The keyword *Prepare* at the center. The other keywords, namely *Categorize*, *Select*, *Implement*, *Assess*, *Authorize*, and *Monitor* interact with the Prepare keyword on a circular basis. The cycle initiates with preparation. The cycle is not static and stages are cycled through continuously. This ensures risks are managed over time.

The first stage, Categorize, involves categorizing risks based on factors such as likelihood and potential impact. The next stage, Select, involves selecting appropriate risk management strategies to mitigate the identified risks. The Implement stage involves implementing the selected risk management strategies.

The Assess stage involves assessing the effectiveness of the implemented risk management strategies. In the Authorize stage authorization is obtained from relevant stakeholders to continue the risk management process. The final stage, Monitor, involves monitoring the effectiveness of the implemented risk management strategies and making necessary adjustments to ensure the risks are effectively managed. The circular pattern emphasizes the cyclical nature of risk management.

8.2 Risk management implementation

Risk management is the process of identifying, assessing, and prioritizing potential risks in order to develop strategies to mitigate or avoid them. The implementation of risk management involves integrating risk management practices and procedures into operations and processes. This prevents security incidents and minimizes their impact.

One key aspect of risk management is the use of vulnerability scans to identify potential weaknesses in an organization's security posture. This involves using automated tools to identify potential vulnerabilities in software, hardware, or network infrastructure. Such scans are essential for identifying potential security risks which may not be immediately apparent.

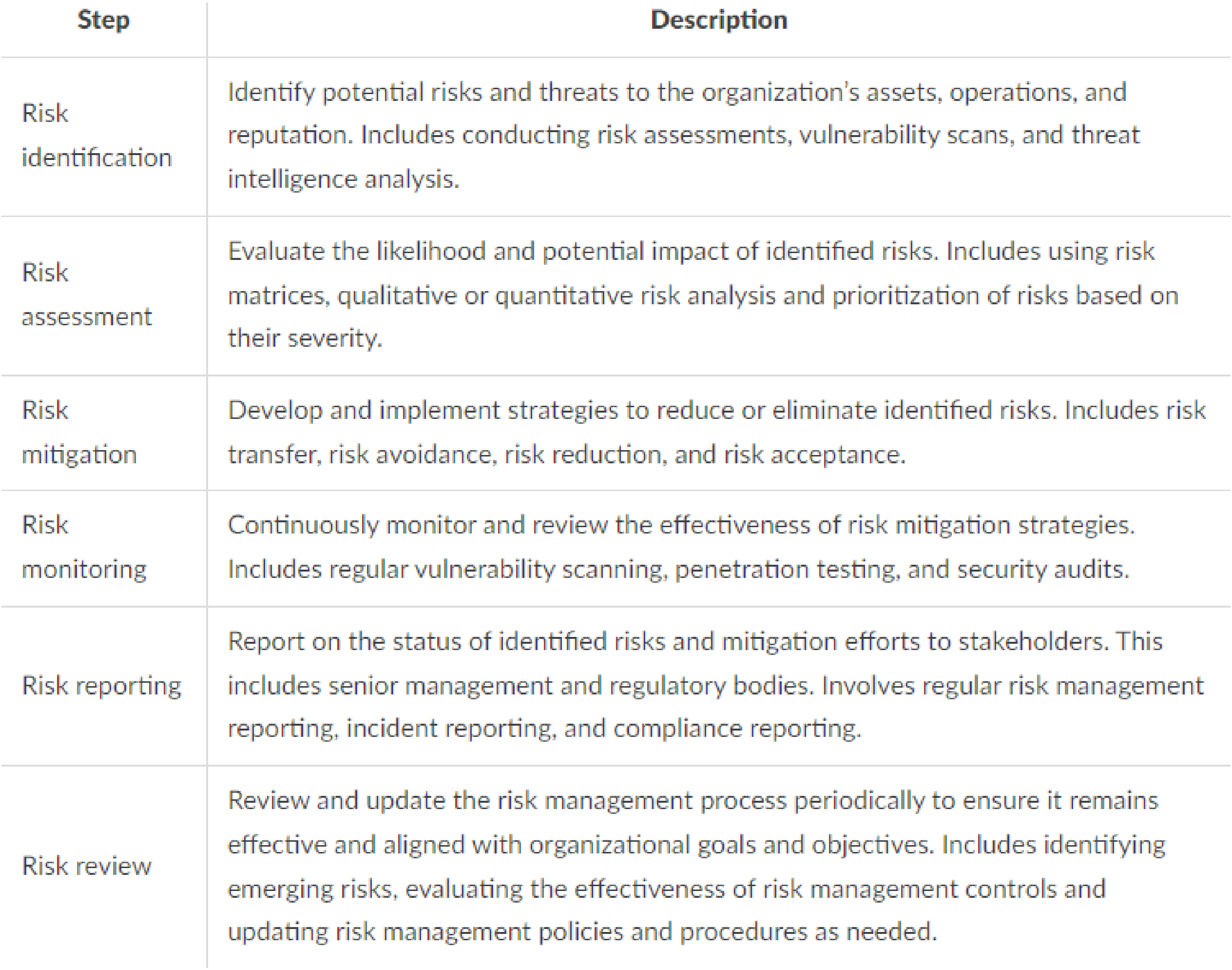
It is necessary to perform regular vulnerability scans on all critical systems and applications. Scan results should be reviewed by security personnel to identify potential vulnerabilities. Remediation should be prioritized based on the level of risk posed to the organization. The use of Security Information and Event Management (SIEM) tools to monitor network activity for signs of potential security incidents is another important tool. SIEM systems collect and analyze log data from network devices, applications. Systems and use this information to identify potential threats in real-time.

The first step in effective SIEM-based security management is to identify which systems and applications need to be monitored and what events or activities should trigger an alert. Once these parameters have been established SIEM tools can be configured to collect and analyze log data from these sources. Alerts will then be triggered when potential security incidents are detected.

Security Orchestration, Automation, and Response (SOAR) tools can automate incident response processes and improve overall security posture. SOAR tools use automation and machine learning to quickly identify and respond to potential security incidents. This allows the security team to focus on more complex tasks. Incident response processes can be automated through the SOAR system. It is the responsibility of the security team to decide what triggers should be used to initiate automated responses. For example, SOAR tools can be configured to automatically block suspicious IP addresses, quarantine infected systems, or alert security teams when specific events occur.

The steps of the risk management process are broken down below.

Figure 15: Risk management table (ISO 27001, 2022)



Step	Description
Risk identification	Identify potential risks and threats to the organization's assets, operations, and reputation. Includes conducting risk assessments, vulnerability scans, and threat intelligence analysis.
Risk assessment	Evaluate the likelihood and potential impact of identified risks. Includes using risk matrices, qualitative or quantitative risk analysis and prioritization of risks based on their severity.
Risk mitigation	Develop and implement strategies to reduce or eliminate identified risks. Includes risk transfer, risk avoidance, risk reduction, and risk acceptance.
Risk monitoring	Continuously monitor and review the effectiveness of risk mitigation strategies. Includes regular vulnerability scanning, penetration testing, and security audits.
Risk reporting	Report on the status of identified risks and mitigation efforts to stakeholders. This includes senior management and regulatory bodies. Involves regular risk management reporting, incident reporting, and compliance reporting.
Risk review	Review and update the risk management process periodically to ensure it remains effective and aligned with organizational goals and objectives. Includes identifying emerging risks, evaluating the effectiveness of risk management controls and updating risk management policies and procedures as needed.

8.2.1 Risk values taxonomy

The above can also be conceived as a traffic-light system. Security is conceptualized as a series of functions with an associated safety value in this case.

Table 4: Risk values traffic light system (NIST, 2018)

Function	Category
Identify	Asset management
	Business governance
	Governance
	Risk assessment
	Risk management strategy
	Supply chain risk management
Protect	Identity management and access control
	Awareness and training
	Data security
	Information protection processes and procedures
	Maintenance
	Protective technology
Detect	Anomalies and events
	Security continuous monitoring
	Detection processes
Respond	Response planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery planning
	Improvements
	Communications

8.3 Security controls

Concrete steps can be taken to achieve operational security. It is important to note these measures only concern physical infrastructure. Explicitly non-technical measures such as training programs, access control and so on will be presented elsewhere.

In terms of technical controls, this discussion concerns the digital protection of physical infrastructure. This includes the use of Firewalls, antivirus software, encryption and intrusion detection and prevention systems. Device management, software updates and automation also need to be incorporated into digital security control systems. Device management systems should be in place to manage configuration, security and monitoring of all company devices. This can include inventory management, remote wipe capabilities and compliance checks.

It is essential for all security software is up to date. Automatic software updates can be enabled to ensure patches and bug fixes are applied on an automated basis. Automation is a useful tool to streamline security processes and should be implemented wherever possible. This reduces the risk of human error and ensures that updates occur according to a set schedule. Automation can also ensure vulnerabilities and suspicious activity are checked on a consistent basis.

8.4 Methods

ISO/IEC 31010:2022 provides a range of risk assessment techniques to identify, analyze, and evaluate risks. These include brainstorming, checklists, expert judgment, fault tree analysis, event tree analysis, and modeling to predict the probability of a variety of outcomes when the potential for random variables is present (also known as Monte Carlo Simulation). The choice of method depends on the purpose of the organization and the resources available. The complexity and novelty of the situation also determines method choice.

An organization with no prior experience in assessing risks may choose a simpler method such as brainstorming. A more mature organization may opt for a more thorough technique like Monte Carlo simulation. It is also important to consider factors. These include the resources available, the scope and type of risks, and communication between internal and external parties. DefendByVirtual faces a wide array of risks. In many cases these can be sophisticated attacks. It is essential that the company meets these risks head-on and devotes sufficient resources to their prevention.

9 Continuity management

It is critical that DefendByVirtual has a solid and structured plan on how to recover from potential security breaches. This is non-negotiable for a company working within the cyber security field. It directly correlates to their professional status as a trustworthy and effective company relative to their peers. DefendByVirtual is not only responsible for their own cyber security. They are also responsible for creating it for others.

The report up to now has discussed the steps involved in established effective preventative measures against attacks. It is also necessary to have a clear understanding of what to do in case these systems fail. Cyber security systems can only protect against known attacks. This means the company should have procedures in place and deployable resources available in the event of a zero-day attack or system failure. Such responsibilities are typically assigned to a recovery team. Their main priority should be investigating possible breaches and recovering / restoring compromised data.

9.1 Infection recovery plan

It is not enough to have an attack prevention plan in place. Clear procedures need to be established in the event of an attack. Responsibilities should be well understood by all relevant parties.

DefendByVirtual can mitigate damage and reduce threats by keeping software updated and the systems hardened. Such strategies reduce the likelihood of an attack. But they do not reduce the likelihood of an attack to zero. Cyber security company are considered attractive targets by malicious actors. The SIEM, SOAR and Security Onion will greatly improve the security posture once the proposed plan is implemented. When these systems are up to date potential security breaches will not only be easier to identify; they will also be less likely to occur.

9.2 In case of infection

In the case of an infection the first thing to do is to contain the threat. If the SIEM system is infected, it should be disconnected from the rest of the network. This removes the possibility of the attacker gaining access to information on other computers in the network. Once the attacker is contained and the network disconnected an investigate as to where the attacker gained access and what damages were caused can be launched. The extent of information loss or compromise can be determined. The scope of the infection and nature and origin of the attack can be established.

Systems should be restored as quickly as possible. This ensures normal operations can resume with minimal interruption. It is of equal importance this is done with all necessary security precautions in mind. The infected system should remain isolated until vulnerabilities are definitively removed. Full vulnerability scans on the infected asset should be performed to determine the root cause of the breach. Unpatchable software should be removed from the system until a fix has been provided by the product owner. If a fix is not possible the infected systems should be replaced. Replacements should meet all appropriate security standards.

9.3 Triage strategies

It should be a matter of priority to determined what, if any, information was lost and who is affected. The affected parties, be they clients or the company itself, should be informed at the earliest possible juncture. Isolated backups should be on hand so lost information can be retrieved. Once all assets are secured the company can return to its day-to-day operations. All passwords should be changed and login regulations tightened. Effective communication and collaboration with affected parties can greatly reduce negative spillover effects of an attack.

9.4 Business impact analysis (BIA)

The likelihood of a total failure of Admin-net machines are unlikely. The impact of such a failure would nevertheless be severe should it occur. These machines lie at the heart of the company’s operations. They are critical to its success. The loss of Admin-net would by all measures be catastrophic. The SIEM and WWW machines also pose substantial risks in their current state. Clients would almost certainly think twice about doing business with the company were they made aware of the state of its systems. The business is built on securing client systems. DefendByVirtual must be secure if it is to credibly provide this service.

Ready.gov proposes a range of methods to ensure employees have the necessary skills. All employees in the company should be made aware of the steps proposed in this report. Roles and procedures in the event of an attack should be well understood. This can be achieved via workshops, questionnaires or a range of other methods. Interviews with the staff can validate information and identify gaps in knowledge and procedure.

9.5 Education and training

A high level of industry awareness must be maintained if the security posture is to be strengthened. The field of cyber security changes constantly and new threats emerge in short intervals. Education should be available to fill possible knowledge gaps. Employees should be encouraged to work towards new personal certifications and attend cyber security-related events. General security training should be arranged on a continuous basis.

9.6 Continuous management

Software and skills should be upgraded on a continuous basis. Staff should have a basic understanding of how the software they use works. Both digital and physical assets should be updated according to a set schedule. Scheduling should be automated wherever possible. DefendByVirtual must as a company follow new developments in the field of cyber security. The software approach should be agnostic. If better tools become available they should be implemented into the system. Staff should be trained to use new software and tested for knowledge. DefendByVirtual needs to be ready for anything.

9.7 Timetable

It its current state the environment is highly fragile. DefendByVirtual should have the environment in a working state in the first quarter of the fiscal year. While the systems are being updated a training program should be implemented. It is of critical importance that staff are aware of nature of and limitations to the software they are working with. Work should be assessed within two week-long sprints. Employees should be tested for their knowledge. Physical assets should be resilience-tested to ensure they are battle-ready. Work with customers should begin only after all systems are operational, updated and online. Employee education and training during this period should be on a continuous basis.

10 Conclusion

The path to recovery is long and difficult. Physical assets are usable but the digital environment is out of date. The system overall requires a great deal of attention. This mostly concerns software updates and management. The system should be objectively assessed and unnecessary software should be removed. All software should have a clearly defined role within the system.

The scope of the company's future is clear and the steps required to return to operational viability are feasible. DefendByVirtual should by now be aware of the risks and threats to its business. But the news is not all bad. The cyber security industry is growing rapidly. The SWOT analysis indicates there are clear opportunities midst the chaos.

Careful alignment to internationally accepted standards in a centrally managed ISMS framework is a necessary step to reestablishing credibility and securing revenue streams. The report proposes concrete steps by which to achieve this. By implementing the changes proposed the company will be well-placed to take advantage of increased demand for cyber-security services in an industry where growth is assured for many years to come.

Works Cited

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022:fi*. In Suomen Standardisoimisliitto SFS. ISO/IEC.

International Organization for Standardization (ISO). (2022). *ISO/IEC 270021:2022:fi*. In Suomen Standardisoimisliitto SFS. ISO/IEC.

International Organization for Standardization (ISO). (2022). ISO/IEC *31010:2019, Risk Management-Risk Assessment Techniques*; ISO/IEC: Geneva, Switzerland.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.

Irwin, L. (2021, June 15). *What an ISMS is and 5 reasons your organisation should implement one*. IT Governance Blog En. Retrieved March 5, 2023, from https://www.itgovernance.eu/blog/en/what-is-an-isms-and-why-does-your-organisation-need-one

Works Consulted

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1.* National Institute of Standards and Technology. Retrieved March 2, 2023, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nevala, J. (2023). *TTC6020 – Kyberturvallisuuden hallinta 04A-Risk Management* [Slide show]. JAMK. https://moodle.jamk.fi/pluginfile.php/948000/mod_resource/content/0/04-2023K-Risk_management.pdf

Business Continuity Plan | Ready.gov. (n.d.). Ready.gov. Retrieved March 3, 2023, from https://www.ready.gov/business-continuity-plan