Development of Incident Response Playbooks and Runbooks for Amazon Web Services Ransomware Scenarios

Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis
EIT Digital Master School
Cyber Security

Author:
Samuele Gandini

Supervisors:
Seppo Virtanen
Petri Sainio

University of Turku
September 2023

UNIVERSITY OF TURKU
Department of Computing, Faculty of Technology

Samuele Gandini: Development of Incident Response Playbooks and Runbooks for Amazon Web Services Ransomware Scenarios

Master of Science in Technology Thesis, 105 p.
September 2023

In today's digital landscape, enterprises encounter myriad cybersecurity challenges that jeopardize their critical digital assets.
Modern cyber threats have evolved drastically, adapting to the proliferation of cloud technologies that drive organizations towards platforms like AWS that offer convenience, cost-reduction, and reliability. However, this transition introduces new security risks because threat actors are motivated to craft and deploy advanced malware explicitly targeting the cloud.

Ransomware emerged as one of the most impactful and dangerous cyber threats, still in 2023, encrypting data and demanding payment (usually in untraceable tokens) for the decryption key. Confidentiality, integrity, and availability of cloud assets stand perpetually vulnerable, and sometimes, unprepared businesses suddenly hit by ransomware cannot find a way out. Besides financial loss and operation disruption, the breach of sensitive information compromises trust, leading to reputational damage that's hard to mend.

Corporations are urged to develop robust defensive strategies to identify, contain, and recover from ransomware and other cloud threat exploitation.
Traditional cybersecurity approaches must rapidly reshape to manage emerging menaces. Hence, they require new specialized and well-structured incident response plans to become the bedrock of the security tactics.

This thesis dives into the complexities of designing and implementing accurate incident response Playbooks and Runbooks, focusing on handling the common danger of ransomware, especially within Amazon Web Services (AWS).
This research journey is strictly connected to the real-world context, resulting from a six-month internship within *Bynder*, a digital asset management leader company. This experience culminated in conceptualizing the step-by-step procedures against ransomware incidents in cloud infrastructures, improving communication, and coordinating actions during high-pressure situations.

Keywords: Cybersecurity, Incident Response, Cloud Computing, Ransomware, Amazon Web Services (AWS), Cloud Security, Playbooks, Runbooks, proactive strategies

Contents

1 Introduction

The thesis focused on developing an effective incident response plan to safeguard the company's infrastructure against specific threats targeting cloud technologies. It results from a project realized during my information security internship at ***Bynder***, an IT SaaS company global leader in the Digital Asset Management field and based in the Netherlands. The introduction clarifies the background and motivation of the thesis, focusing on the initial problem statement and its importance. Additionally, I will talk about Bynder and the InfoSec team, providing general details about the organization's purpose and the security group's goals.

1.1 Background and Motivation

The evolving digital landscape sees organizations promoting innovative technologies that allow them to develop efficiency, scalability, reliability, and security. Innovation enables companies to streamline operations and adapt to market demands. However, as they embrace these new opportunities, they expose themselves to a wide range of cybersecurity threats that can have devastating consequences. Ransomware is among these threats, one of the most insidious and disruptive forms of attack. The background and motivation section starts by introducing the reasons for corporations to move towards cloud technologies, and after that, it analyzes cyber risks, narrowing down to ransomware attacks.

1.1.1 Into the Cloud Revolution: technological transformation in modern business

The launch of cloud technologies has revolutionized how businesses operate and deliver services. Cloud providers offer many solutions to empower their customers' features to scale rapidly, reduce expenses, and innovate rapidly. In 2023, 94% of companies worldwide adopted Cloud solutions to boost their services and productivity [1]. *Amazon Web Services*, *Microsoft Azure*, and *Google Cloud Platform* are the most diffused solutions to dominate the market. Implementing a cloud-based infrastructure can bring various benefits to the organization, as *OCloud Solutions* explains [2]:

1. *Convenience of use*: The cloud can store large datasets and provide an easy way to access them. Global presence, agility, and flexibility are the key features that motivate companies to move their environments toward the cloud.

2. *Cost reduction*: Need-basis services access is one of the main reasons for implementing cloud-based products. The business does not invest in on-premise solutions because it can exploit a subscription method that minimizes any other expense.

3. *Reliability*: products deployed over the Cloud can be accessed anywhere, and most providers can ensure 99.9% uptime. Unavailability of the services is usually caused by the company using the cloud's misconfigurations rather than the provider. Hence, as explained by the AWS Shared Responsibility Model, Amazon is in charge of the *Security of the Cloud*, and the customer deals with the *Security in the Cloud* [3].

4. *Security and Privacy*: Cloud systems enhance security and privacy thanks to their features, such as encryption, access control, authentication policies, and

DDoS protection. Moreover, they offer many tools to monitor the applications and Cloud-based assets, allowing data security and real-time threat detection.

5. *Collaboration*: The opportunity to upload resources in the Cloud allows users multiple accesses in real-time, making collaboration and organization on a higher level. People can modify the documents easily, keeping the changes under control thanks to versioning and assisting access to large files.

Nevertheless, with the growth of cloud infrastructures, a dynamic and complex threat landscape, where cyberattacks have increased in frequency and severity, targets modern businesses. Critical operations in interconnected systems have been digitalized and become fertile ground for threat actors to exploit vulnerabilities.

1.1.2 Navigating cloud risks: confronting modern security challenges

While the cloud brings several benefits, it is not risk-free. Cloud providers, such as Amazon Web Services, developed a shared responsibility model that, combined with a dynamic cloud environment that requires expertise for its setup, may lead to misconfiguration, vulnerabilities, and unauthorized access points.

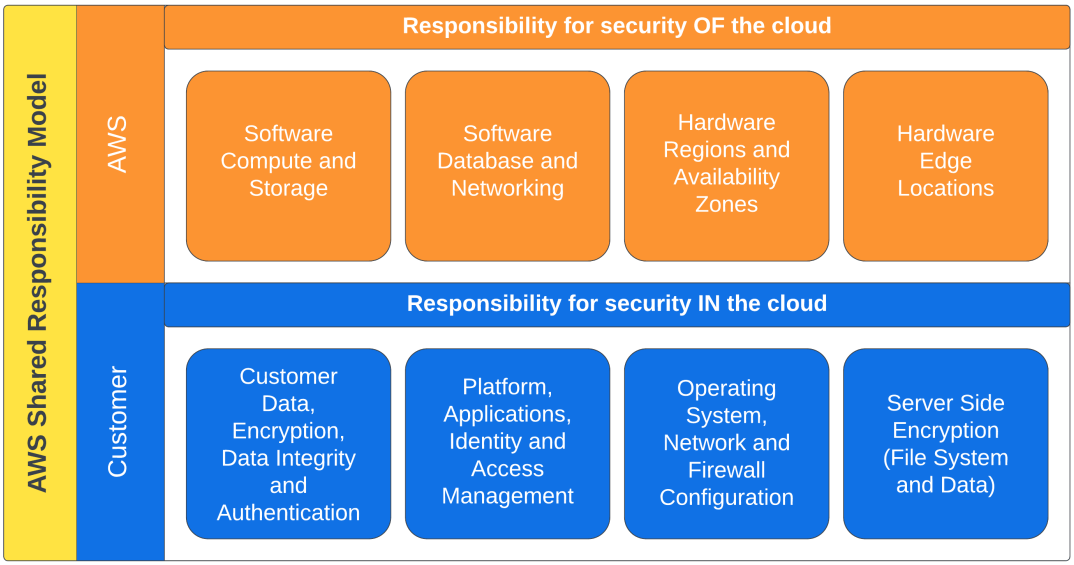

Figure 1.1: *AWS Shared Responsibility Model* pinpoints the customers' responsibility to protect their data, platforms, and applications when implementing the infrastructure. AWS is in charge of the *Security of the cloud*; clients address the *Security in the cloud* [3].

Cloud-based industries must be concerned about data breaches, loss of sensitive information, and potential disruption to business operations. Multi-cloud environments are becoming increasingly diffused, and their security is challenging and requires advanced skill sets and elaborated security tools. That's why cloud service providers are working hard to provide reliable native controls that their customers can purchase to reduce cyber risks. Cyber security threats targeting cloud technologies are evolving, as the *Checkpoint 2022 Cloud Security Report* confirms [4]. Among the top eight adversities for the cloud environment, we can find misconfiguration of the platforms, data exfiltration, insecure interfaces, unauthorized access, account hijacking, and, finally, **ransomware**. It represents a formidable adversary with a devastating impact.

1.1.3 Ransomware Menace in an Evolving Cloud Landscape

According to *Anthony Today*, all the big, medium, or small-size organizations are concerned with ransomware, which targets their operations, finances, and reputations [5]. Ransomware's first infection may come from multiple attack vectors, such as *phishing* communications, download of malicious programs, or even unauthorized access to the network. When the system is compromised, the malware can spread across the infrastructure and encrypt sensitive information. The data remains inaccessible for the business until a ransom is paid. Besides the catastrophic financial damage for the company, the brand is hit on its reputation, and customers may lose trust in it. Sometimes, a Ransomware attack may mean the end of the business because the provoked disruption is irreparable. These kinds of malware are classified into **Crypto-Ransomware**, which encrypts data using solid algorithms until the ransom is settled, and **Locker-Ransomware**, which locks the victims out of their devices by displaying a full-screen message that cannot be removed without paying the ransom.

Nivedita James explored the most destructive Ransomware attacks and researched the overall financial losses of the affected corporations [6]. *NotPetya* evolved from *Petya* Ransomware in 2017 and extorted around 10 billion dollars using the *EternalBlue* exploit. It was part of the *Sandworm* operation and is recorded as the most impactful malware in history. *WannaCry* is probably the most famous ransomware that exploited Microsoft Windows vulnerabilities across 150 countries. It was launched in 2017, and the loss is more than 4 billion dollars. *Sodinokibi* was released in 2019 by the *REvil* operation and oppressed transportation and financial sectors. The approximate losses for the affected industries are around 200 million dollars.

Ransomware attacks are still dangerous, and they have increased in the last year in line with *Zscaler 2023 Ransomware Report* [7], mainly in the form of *RaaS* (Ransomware as a Service): tools and information for conducting the attack are sold through the *Dark Web*, and affiliates can make profits by using the obtained instruments. Furthermore, new predictions for 2024 foresee the combination of Artificial Intelligence to build *AI-powered ransomware attacks*. Machine learning algorithms integrated into malware can make detection and prevention more sophisticated while allowing less expert threat actors to write malicious code.

Ransomware can, therefore, target cloud-deployed services, even with the security measures proposed to protect the infrastructure. All companies embracing the cloud evolution must assess the risks they may encounter and implement solutions to prevent but also identify and contain ransomware attacks. Here, it's clear the necessity of a well-structured and effective *incident response plan* to help organizations against ransomware that, although security measures are in place, can lead to catastrophic consequences.

1.2 Objectives and Limitations

A systematic incident response plan is a crucial component of the security posture of a cloud-based company. The publication "*Cloud incident handling and forensic-by-design*" affirms the necessity of incident handling strategies for the cloud, which is virtualized and geographically distributed. Existing models may not be adequate to limit the impact of cloud incidents, and every company must dedicate resources to planning [8].

1.2.1 Preparing for the Inevitable: The Necessity of Incident Response Planning

As reported by the **NIST** *"Computer Security Incident Handling Guide"* [9], IT programs require a computer security incident response program since cyber attacks have become more frequent and disruptive. Risk assessments and basic preventive measures are no longer enough to avoid an incident, and detection and response capabilities are thus necessary to minimize the damage, mitigate the weaknesses, and recover productivity, returning to business. With a well-defined plan, organizations may find it easier to manage an incident and lower the destruction, keeping an excellent firm reputation. The incident response needs continuous infrastructure monitoring, an effective technique to define whether the events are critical, and a methodology to establish efficient and quick communication among different departments. An innovative approach to address the development of an incident response process is by introducing scenario-based plans, which can be deployed considering three main stages:

1. Mapping out external and internal attack vectors to identify straightforward incident scenarios. In this stage, a risk assessment helps detect relevant threats targeting the main resources of the company.

2. Converting the created scenarios into Playbooks and Runbooks. As I will explain in Chapter 2, these step-by-step procedures are essential to making technical decisions on future actions.

3. Adding new controls and pre-written scripts that responders might use. Incident detection and response may be improved thanks to new security measures that can automate part of the process.

The implementation focused on deploying the playbooks and runbooks for Bynder's incident response plan, improving the ability to detect, analyze, contain, and re-

cover from ransomware targeting cloud services. As explained by Abi Tunggal, an UpGuard CyberSecurity expert [10], companies may not detect attacks or know how to recover from them without a formal incident response plan. Incident response planning based on **NIST Framework for Improving Critical Infrastructure Cybersecurity** industry standards [11] brings several benefits to the organization:

- **Improved Response and Recovery capabilities**: The **CSIRT** (*Cyber Security Incident Response Team*) boosts its capacity to handle incidents, and the response and recovery actions are quicker and more effective.

- **Minimized impact**: The risk of compromise, data breaches, system unavailability, and reputational damage is dramatically reduced with a plan in place. The CSIRT can follow exact guidelines depending on the scenario and prevent the incident from spreading.

- **Enhanced incident analysis and containment**: The incident response process also suggests new tools to help the team with the logs analysis and the impact containment. The effects of the events are mitigated more effectively, and all the steps are documented to enhance the CSIRT efficiency further.

- **Consistency**: All the incident response stakeholders follow the same plan. Consistency is critical to drive the response towards only one direction and lower the impact on business operations, ensuring business continuity and reducing financial losses.

- **Enhanced Communication**: The clear and structured process of the plan leads to reduced downtime due to the rapid communication between different teams. The communication strategies are defined for both internal and external stakeholders, and, in particular, the plan includes recommendations of potential tools that can be helpful, such as *Slack*, *Google Meet*, or *Microsoft*

Teams. Clear communication helps manage the situation transparently, maintaining trust among customers, partners, and employees.

- **Legal and security compliance**: Companies are subject to strict regulations regarding data breaches and incident reporting. After the incident happens, potential data loss must be communicated within a specific time frame according to the directives. Some security standards, such as *ISO27001* or *SOC2*, also expect an incident response plan.

- **Clear roles and responsibilities**: The CSIRT components must be defined before the incident happens. Depending on the scenario, individuals from different departments will be considered and follow the instructions of the IR manager.

- **Learning and Testing**: Once the incident has been resolved, the CSIRT must review all the IR stages to verify how the process can be improved. The debriefing procedure allows the organization to identify weaknesses and prevent similar events in the future. Furthermore, testing is fundamental before a potential incident, and the security Runbooks provide various ways to evaluate the plan's effectiveness.

- **Preparation for different scenarios**: An exhaustive Incident Response plan considers multiple use cases and attack vectors to cover myriad incidents. Depending on the business classification, some resources and assets must be prioritized.

- **Risk Management**: Businesses can better assess and manage the risk associated with different incidents with a well-structured plan. Therefore, this proactive approach may minimize the likelihood and impact of the attacks.

- **Protection of reputation**: The reputation is undoubtedly safeguarded by an incident response plan. The enterprise can demonstrate its commitment to Cybersecurity by quickly and responsively handling an incident.

Incident response planning is critical to creating a roadmap for the CSIRT to effectively navigate the challenging landscape of security incidents, maintaining business continuity, and protecting sensitive information.

1.2.2 Understanding the Constraints and Exclusions

Besides the several advantages already described, a few limitations are related to my project at Bynder. The complexity of cloud technologies, and in particular, Amazon Web Services, and the rapid evolution of cybersecurity threats posed certain constraints on the scope of this study. First, AWS is a multifaceted cloud platform that offers a vast selection of services and configurations. Hence, this thesis cannot encompass every Amazon resource, scenario, or potential threat. Instead, it focused on a subset of significant use cases to illustrate the principles of incident response. Furthermore, cyber threats continuously evolve, with new attack vectors, malware variants, and vulnerabilities emerging regularly. New ransomware may arise during the lifecycle of this thesis, and it might trick the exposed security solutions.

Finally, my limited period spent within Bynder posed relevant limitations to this project, starting from the methodology. An assessment is critical to evaluate the environmental risks and formulate security solutions. However, a complete evaluation was not part of the scope, and it focused on specific technologies. Another required phase of incident response is **testing**, which was part of the initiative. Unfortunately, simulations were too challenging due to the complex nature of the project and the effort needed to prepare the environment and mimic the attacks. Nevertheless, they were planned before I left the organization, and the incident response

scenarios will be tested, as clarified in Chapter 6. In conclusion, incident response planning is a never-ending process. Every time changes are applied to a specific product, new risks and threats may be considered, and new tools or different kinds of analysis may be integrated to improve security.

1.3 Bynder: Introduction to the Company

Even though it is not critical for understanding the thesis, I would like to introduce the company of my internship: *Bynder*. This section can help the comprehension of the background motivation and implementation choices.

Bynder is a leader in Digital Asset Management based in the Netherlands with a platform that provides the fastest features to manage creative files. It is a SaaS (*Software as a Service*) company that allows other business teams to collaborate with easy file sharing and storage and a central hub for all digital assets. Bynder's products use Cloud technologies, and, in particular, **Amazon Web Services** had a critical role in developing the business and speeding innovation. As explained by *AWS*, one of Bynder's top priorities was international expansion, which was made achievable through the utilization of *Amazon Simple Storage Service (S3)*, *Amazon Relational Database Service (RDS)*, or *Amazon Rekognition* [12]. *AWS* enabled Bynder to become one of the most competitive Digital Asset Management solutions on the market.

Hence, Bynder is an innovative company growing internationally and fast, and the presence and support of an **Information Security** team supervising security and compliance topics is essential. My internship of six months occurred within this critical unit to help deliver a secure and trustworthy Bynder brand by maintaining and further enhancing a resilient information security program. The ambition to

improve the incident response plan was born from a joint idea between the Information Security department and the *AWS Customer Support* team. Implementing new incident response plans is vital to further maturing Bynder's overall security posture, ensuring business continuity, and decreasing the impact of cyber threats.

1.4 Thesis Overview

The thesis is divided into eight chapters describing incident response *State of the Art* at first and then focusing on design and development. The final paragraphs explain the results of the plan and introduce future opportunities.
Apart from the introduction, there are the remaining sections:

2 **State of the Art**: This initial chapter will provide an overview of the incident response state-of-the-art, mainly concerning Amazon Web Services Cloud Computing since it is at the base of Bynder's products. I will analyze the Cyber Security Incident Response transition, starting from the **NIST** publication *800-61 Rev 2 (Computer Security Incident Handling Guide)*.

3 **Methodology**: This section will explore the arrangement of the project. It will outline its design, including charts and tables used to prepare the tasks and define the deadlines for each stage.

4 **Incident Response Development**: Incident response development includes the preliminary activities before implementing security Playbooks and Runbooks. I started with a risk assessment to identify the critical assets for Bynder and the most dangerous threats that may target a cloud-oriented enterprise. I also studied the available tools that may be used for incident response to understand the defensive capabilities of an organization to limit the impact in case of an incident.

5 **Incident Response Implementation**: Implementation is the core of this document since it contains the actual security Playbooks and Runbooks created during my internship. The procedures include *Preparation*, *Identification*, *Containment*, *Eradication*, *Recovery*, and *Lessons Learned*, even though each one has been reviewed to clear out the sensitive information of Bynder's final plan. These blow-by-blow documents resolve the problem by presenting how to face ransomware attacks.

6 **Incident Response Testing**: This chapter is dedicated to the simulations that may be carried out to improve the IR processes further. The attacks' replicas can be performed using multiple tools, such as AWS CloudSaga, and they can reproduce one or more analyzed scenarios. I will describe how to conduct infrastructure tests even if there was no time to conclude the testing during my last period at Bynder.

7 **Conclusion**: The conclusion includes evaluation and results, final remarks, and future trends for incident response. During the internship, I also created an IR template that can be revised for new scenarios to cover more use cases than the ones considered in this thesis. Considering the fast evolution of cybersecurity threats, the framework can be helpful for the organization.

2 State of the Art

State of the art refers to the highest level of advancement in a particular field, and this chapter analyses the current progress of the technologies surrounding the incident response area. According to the paper "*On Incident Handling and Response: a state-of-the-art approach*" by the researchers *Mitropoulos*, *Patsos*, and *Douligeris* [13], responding to an incident involves many management, legal, technical, and social aspects. I will compare the initial proposals elaborated by **NIST** (*National Institute of Standards and Technology*) with other solutions, and I will introduce playbooks and runbooks, talking about how they can be helpful during the remediation actions. Eventually, I will explain the best practices while developing an incident response plan, discussing how *AWS* suggestions may mitigate threats targeting cloud-driven companies.

2.1 Cyber Security Incident Response Frameworks

Incident Response has always been a hot topic in Information Security. All the devices are currently connected to the internet, from servers to personal laptops and IoT, and all organizations must now develop an effective incident response plan to avoid infrastructure compromise and ensure business continuity. In 2012, **NIST** published the first crucial paper dealing with Incident Response and providing insights and framework companies should follow to handle security incidents: *Computer Security Incident Handling Guide* (**NIST 800-61**). Even though the

publication is dated and was written when some technologies were mere imagination, it is still valid and used to mitigate the risks by implementing efficient response actions.

A **Computer Security Incident** is defined as a "*violation or an imminent threat violation of computer security policies, acceptable use policies, or standard security practices*" by Paul Cichonski (*NIST*) [9]. It involves different parties that interact with each other:

1. *An attacker*: the malicious party that tries to trick the user(s) or exploits the vulnerabilities of the infrastructure.
2. *The infrastructure*, which includes servers or other devices, is compromised by the attack.
3. *Optionally, one or more users* that the malicious entity may deceive.

When security breaches occur, the business must be ready to respond rapidly and competently. The company's approach should be well-defined and organized, and the incident response plan must be a roadmap on which the incident response capability is built. Therefore, the initial program designed by NIST included the goals of the procedure, the incident response strategy with internal and external communication approaches, some metrics to evaluate the current process that is in place, and guidelines for maturing the response capability. Incident response requires strategic planning that must be discussed among different departments because they may have an alternative perspective on the same argument. Furthermore, the tactics should be reviewed annually to protect the business against innovative threats and sustain its efficacy.

Incident response also needs several resources to implement security mechanisms and measures, which may increase the organization's expenses. As a result, the cor-

poration should evaluate which actions are essential for the operations and balance the costs and the integration of new defensive techniques. An excess of implemented technologies may result in huge prices, although the company is well-protected. Hence, it's imperative to design opportune procedures and protocols.

2.1.1 Sentinels of Security: Unveiling CSIRT Roles and Operational Tools

The plan's first step implies establishing a *Computer Security Incident Response Team*, or **CSIRT**. This group will be organized with a team manager overseeing the operations. This individual is vital to control the execution of the plan and ensure that the team has the required personnel and knowledge. On the other hand, the rest of the CSIRT must have the appropriate skills to manage the criticality of the incidents, such as system and network administration, investigation, malware analysis, and problem-solving. Moreover, the CSIRT should have the proper technology to detect, analyze, and mitigate the incident. As documented by the **NIST** publication **800-83**, "*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*" [14], several security tools can be used for vulnerability and threat mitigation:

- **EDR and XDR**: *Endpoint Detection and Response (EDR)* focused on monitoring and responding to security threats at the endpoint level, providing real-time visibility into endpoint activities, including processes, files, network connections, and user behavior. *Extended Detection and Response (XDR)* expands the scope beyond endpoints to cover various security layers throughout the infrastructure. XDR includes information from multiple sources, such as Cloud and application services, to recognize more complex or multi-stage attacks. Additionally, these technologies can directly act on the devices, such as network isolation or file deletion, helping the overall responding process.

- **IPS**: *Intrusion and Prevention Systems* can be categorized by *Host-based IPS* and *Network-based IPS*. The first product stops suspicious activities by monitoring a single host, while the second analyzes the organization's internal and external network traffic. Network-based IPS may detect many malicious events, and the administrator can customize its rules with new malware signatures.

- **Firewall**: This prevalent device filters the incoming and outgoing traffic of the organization. They provide numerous rules to be modified, and, as *NIST* recommends, firewalls must be configured with **deny-by-default** rulesets. **WAF** *(Web Application Firewall)* is now diffused across corporations and is designed to protect web applications from assorted online threats.

- **SIEM**: *Security Information and Event Management* It is a comprehensive solution that collects, correlates, and analyzes data from multiple security sources. Logs and event data are aggregated in real time to identify patterns and anomalies that can be correlated to potential security threats.

- **Defensive Architecture**: The infrastructure's architecture can dramatically reduce the impact of incidents. For instance, *Sandboxing* runs the applications within a controlled environment, and *Browser Separation* allows the users to access corporate applications using only a single brand of browser.

Although personnel and technologies are integral components of the response framework, NIST introduces another topic that should not be underestimated.

2.1.2 Information Sharing Obligations in Incident Response

Another sensitive matter the NIST **800-61** publication explores is information sharing with outside parties. As reported by the **General Data Protection Regulation art. 33**, the data controller must notify the supervisory authority within 72

hours in the case of a data breach [15]. The communication should include the data subjects and the number of records involved in the violation and describe the possible consequences of the loss. The CSIRT shall incorporate one or more individuals from the legal department to establish policies regarding information sharing. Once the team compositions and the tools are ready, the Incident Response plan can be prepared, starting from the NIST Framework.

2.1.3 Incident Handling

NIST's early *Computer Security Incident Handling Guide* has set the groundwork for all the current Incident Response plans. Four main phases were part of the initial structure.

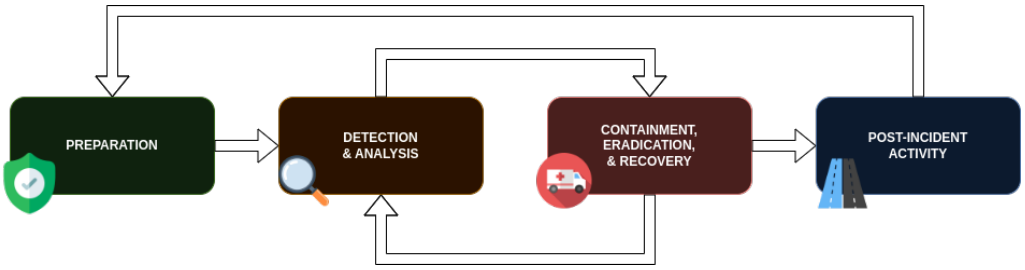

Figure 2.1: The NIST **Incident Response Life Cycle** is divided into four stages: *Preparation*, *Detection and Analysis*, *Containment, Eradication, Recovery*, and *Post-Incident Activity*.

The first important step is **Preparation**, which establishes and trains the team and sets up the required resources. Usually, the security department performs risk assessments to select the most critical assets and, lately, implements preventive controls to avoid incidents. Since the residual risk is inevitable, the **Detection and Analysis** will continuously seek threat traces, allowing for a prompt response. The security team receives alerts from the monitoring tools, and it can contain the impact of the incident.

Containment, Eradication, and Recovery limit the damage, remove the *Indicators of Compromise* (**IoCs**), and let the corporation return to business by restoring the unaffected version of the environment. The CSIRT should provide some directives to circumvent similar attacks in the future, and new controls should be added to the current infrastructure. The **Post-Incident Activity** is helpful to verify that all IoCs have correctly been removed and how future malicious events can be avoided. The CSIRT prepares a report that focuses on the causes of the violation and analyzes the team's behavior. However, although the *NIST* procedure is straightforward and apparently without gaps, it can be improved by expanding these four stages and offering more detailed instructions.

2.1.4 Elevating Incident Response: The Comprehensive Six-Phase SANS Framework

Expanding the NIST strategy leads to a second comprehensive incident response framework, commonly known as **SANS**. The *SANS Institute Incident Handler's Handbook* by *Patrick Kral* [16] is recalled by many cyber security experts. One of them is the *Incident Response leader* at **Cynet Security**, *Asaf Perlman* [17], who explains the SANS's six steps for a complete modern IR approach: *Preparation*, *Identification*, *Containment*, *Eradication*, *Recovery*, and *Lessons Learned*.
Incidents are a matter of when, not if, a violation will happen.

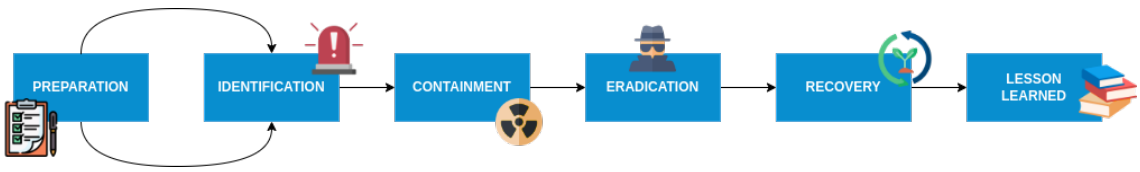

Figure 2.2: SANS **Incident Response** consists of more steps that CSIRTs should follow in sequence, as each is built on top of the other.

Preparation

Preparation and Identification are the steady phases since the organization is always preparing for a security incident. The team must be ready to handle an incident that can vary from anything, like a blackout, to something extreme, such as ransomware. *SANS Incident Handler's Handbook* lists some key elements that must be applied to the infrastructure to mitigate the risks:

1. A well-defined security policy is the business's primary goal because it comprises a set of rules and principles that define how to operate within the organization. Without a clear policy, employees are free to behave according to their inclinations, potentially making the company vulnerable to the outcomes of their conduct.

2. Access control systems should be in place to ensure the **Need-to-know security principle**. Microsoft expert Andreas Wolter mentions that users should access only the information they need for their job functions [18]. There are multiple ways to implement this rule, and the business must guarantee that the CSIRT has the proper permission to manage potential incidents.

3. Monitoring tools are critical resources that must be available for CSIRT. All the helpful technologies must be accessible before, during, and after the malicious event. They should be able to analyze the data sources because they are crucial for detection and investigation.

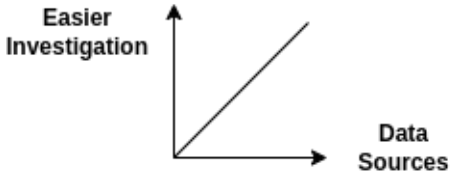

Figure 2.3: The ease of investigation is directly proportional to the number of sources at hand, and saving data from logging will add costs to the incident response process.

4. Since human error continues to be a contributing factor for security breaches and the average annual cost of incidents caused by human error is $3.36 million, as reported by the study of *Katherine Amoresano* and *Benjamin Yankson* [19], periodic **training** is fundamental to reducing the likelihood of an incident. Higher educational institutions must invest enough resources and time in educating their employees. The incident response team should be qualified to manage the alerts and potential infrastructure violations. At the same time, the rest of the organization must be informed of new security trends and attackers' techniques, such as *phishing*.

5. Escalation and the point of contact in other departments should be predefined. A clearly stated communication plan leads to a faster response, and the CSIRT is unlikely to contact the wrong people who may not know how to solve the issues.

6. Last but not least, all the systems must be backed up to facilitate restoring the production environment after an incident happens. The company risks a massive loss without a backup strategy since it should rebuild the infrastructure from scratch. Indeed, security incident response that is not supported by proper backups may imply the end of the business in the worst-case scenario.

This thesis explores AWS, which provides multiple tools that can help companies with the preparation phase.

Identification

In this stage, monitoring tools and the security team analyze unexpected and anomalous behavior to detect potential incidents within the infrastructure. Identification then depends on the services that should be protected and the available tools have been deployed during the preparation phase.

Logs are collected from multiple sources, such as IPS, firewalls, cloud technologies, and so on, to determine possible deviations from the expected operations of the users or the services. Monitoring tools must report events recognized as incidents as soon as possible using suitable notification systems, and the communications must include all the required information to make the investigation easier. The responding team should be able to reconstruct the malicious actions that have been performed considering the questions: *Who*, *What*, *When*, *Where*, *Why*, and *How*. Suitable identification mechanisms may detect internal and external irregular events by minimizing **alert fatigue**. Indeed, frequent alerts about threats can desensitize cybersecurity experts to accurate warnings, as written by *E. Segal* [20].

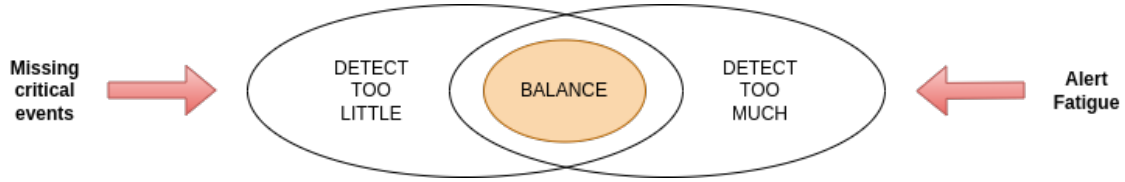

Figure 2.4: The organization should find the perfect balance between detecting too much or too little, considering all the significant events, and avoiding *alert fatigue*.

The Identification step can provide indispensable insights into the impacted resources and the bad actor's initial attack vector. Once the incident has been detected, the CSIRT must create an adequate communication channel and immediately proceed with the *Containment*. The team shouldn't focus on the investigation at this stage to avoid the spread of the incident that may affect other business assets.

Containment

The goal of the Containment is to minimize the damage of the incident. Different stakeholders can approach this step with conflicting ideas: for instance, the security perspective suggests isolating all the compromised machines immediately, while the business point of view prefers to keep the device reachable and running, some-

times without fixing the vulnerabilities because the services of the company cannot be paused or terminated. **All the infected devices must not be turned off** because they may contain vital information for the investigation and response activities. Furthermore, CSIRT must prioritize the critical assets, figuring out whether they have already been affected or are at risk.

The *SANS Incident Handlers Handbook* differentiates *Short-term Containment*, which is not a permanent solution to the problem but the first operation to limit it, and *Long-term Containment*, which allows fixing momentarily the system to be used in production. I didn't consider this separation while developing the plans since companies would need to uproot the problem as soon as possible because recent malware or infections can spread rapidly and without any control. Potential compromised accounts or backdoors should be removed instantly to block any further action of the attackers. Once the Containment is concluded, CSIRT should have restricted all bad actors' activities, and the business can move on with the *Eradication*.

Eradication

Eradication includes the investigation to understand deeply the incident and the removal of all the IoCs from the environment. Inspecting the events related to the bad actor's activities may determine the initial attack vector and any possible attempt the attacker made to maintain access to the infrastructure. During this process, CSIRT must ensure that all the proper actions were taken to delete all the malicious contents from the affected systems, and they have to figure out the overall impact on the business. Investigation can only start if the incident has been contained, and suitable tools for this step should be in place, such as agents on the endpoints that collect a lot of artifacts without the team needing forensic copies of the devices. Obviously, the logs and information examined may vary depending

on the compromised technologies. The digital forensic incident response makes the process faster because responders are not forced to go personally to the location of the incident.

The final result of Eradication's first part should be documented to catalog all the *Indicators of Compromise* and how it was possible to find them. CSIRT should restore any system that may contain malware, preventing reinfection. However, the team can't directly remove all data from the machines in light of a possible violation of the organization's policies. Incident documentation may help to fix any vulnerability by adding new security measures to improve the defenses, while network and appliance scans help to detect remaining anomalies. Before proceeding with the *Recovery*, it's essential to guarantee that the incident's root cause has been eradicated and no IoCs are still present within the infrastructure.

Recovery

The goal of Recovery is to return to business by bringing all the target apparatus back to the production environment. Nevertheless, all the stakeholders should pay attention because, without the required precautions, a too-early recovery may lead to another incident. The systems must be tested, monitored, and validated, and when possible, the affected software must be destroyed and substituted with a secure version from the backup. As mentioned in the *Preparation* section, backups must be performed before the incident happens because, without them, the worst-case scenario may lead to the end of the business. CSIRT should agree on the methods and the time to restore the operations and new monitoring tools that can detect unexpected behavior of the recovered appliances. The primary purpose is to avoid another security incident from happening due to the same or similar vulnerabilities.

Lessons Learned

The last incident response phase is Lessons Learned, a review of all the response procedures. CSIRT should have documented all the steps to provide a complete overview of the events and the activities and to answer the usual questions *Who*, *What*, *When*, *Where*, *Why*, and *How*. Each step of the responding process will be analyzed to determine the initial vulnerabilities that led to the incident and what can be improved to react faster and more effectively, reducing the overall damage. Lessons learned should focus on evaluating the team's performance and drafting clear documentation that will also be useful in the future as training material. The review is carried out within the team by organizing multiple *post-mortem* meetings that will finalize the response process. For example, CSIRT can examine some of the following questions:

1. "*How long was the incident detected after the initial compromise? Do we need better tools for Identification?*". The team will assess the monitoring and detection mechanisms to understand if and how they can be improved.

2. "*How long did Containment take and why?*" Containment is vital to minimize the loss of the business, and it should be as quick as possible.

3. "*After Eradication, did sign of malware or compromise still appear?*". CSIRT can study the effectiveness of the Investigation and IoCs removal and get the hang of new techniques to enhance the capabilities.

4. "*Were the affected resources correctly restored?*". The team will review the Recovery phase by considering better backup solutions if necessary.

Sharing ideas is highly beneficial for the security department and the whole company, and Lessons Learned can really help against future incidents.

In conclusion, incident response is a complex set of operations requiring management and as many data sources as possible to make the tasks and the investigation easier. Indeed, modern approaches expect the integration of *playbooks* and *runbooks*, which allow CSIRTs to follow specific guidelines depending on the scenarios and the role of the individuals dealing with the incidents.

2.1.5 Incident Response Playbooks and Runbooks

As reported by *S. Gatlan* [21], playbooks and runbooks can standardize the response process to lower the impact of an incident in both the private and public sectors. Security playbooks and runbooks are so important for the organizations that they were also included in *The White House Executive Order* to improve the US Cybersecurity (section 6) signed by President *Biden* [22]. They can guarantee a common understanding of security incidents and define the instructions to identify, remediate, and recover from threats and exploitations targeting the systems.

In general, playbooks and runbooks are comprehensive documents that outline procedures with the same goal of responding to cybersecurity incidents within an organization. They can be deployed facing multiple use cases impacting the business, making it easier to test out realistic attack simulations to verify whether the team's approach may work. The below sections explain their main differences, pointed out by the AWS senior security strategists *Nathan Case* and *Paul Hawkins* during the *2019 Amazon Web Services re:invent conference* [23].

Security Playbook

The *Incident Response Playbook* provides an overview of situational responses and planning for the future. They're critical for the business because Playbooks include non-technical people by reporting *C-level or UP-level information* and can be seen

as **RACI** (*Responsible, Accountable, Consulted, and Informed* to set the roles and responsibilities during the IR procedures. A Playbook can align all stakeholders on the same process, and they can generally understand how the IR team is treating the incident and which countermeasures it's been applying. *Avi Shaked*, *Yulia Cherdantseva*, *Pete Burnap*, and *Peter Maynard* point out the importance of cyber security playbooks because they can establish an effective response capability within the organization. They explain that the main issue of playbooks can be addressed as the lack of communication ability [24]. Hence, the implementation section also aims to cover all the problems highlighted by the journal.

Security Runbook

Similarly to playbook, *Incident Response Runbook* provides a tactical review of a situation but includes technical information to correct and investigate an incident. Runbooks contain strategic planning for the future, and they may be helpful for the individuals of the CSIRT: they follow specific steps for security scenarios to enact desired outcomes. Usually, Runbooks enclose a contact list for every situation and can also be part of testing when a new architecture is developed. For instance, every change to the infrastructure may lead to further vulnerabilities that should be examined while writing an incident response plan.

To summarize, new incident response designs are required to incorporate playbooks for the high-ranking executives of the organization and runbooks for the CSIRT that is in charge of managing the actual response activities. After introducing the standard incident response frameworks, I will focus on the cloud infrastructure, considering the AWS best practices that can be put in place to defend against the most severe threats.

2.2 AWS Incident Response: Best Practices

Deploying an operating and reliable cloud architecture to safeguard business data and appliances is crucial. AWS offers frameworks and services to improve the security posture and reduce the risks of customers' platforms. In particular, the **AWS Well-Architected Framework** helps organizations to create efficient and cost-effective multi-account environments that consider all the vulnerabilities exposed to cloud threats [25]. To be prepared against security events, the AWS framework security pillar suggests multiple architecture design principles while launching the cloud environment:

- *POLP*: The principle of *Least Privilege* restricts the interactions between users and resources according to their needs. Separation of duties allows to manage the authorizations to specific AWS assets.

- *Infrastructure Monitoring*: Controls and alerts qualify customers to trace real-time environmental changes.

- *All Layers Security*: Every AWS instance (Virtual Private Cloud, load balancers, network) is monitored without exception. AWS native tools provide 360 degrees of monitoring of the infrastructure.

- *Security Automation*: Security countermeasures automation is critical for scaling rapidly and cost-effectively. Customers with automated techniques in place can also respond quickly to security events that usually require a manual investigation.

- *Data Encryption*: Encryption in transit and at rest enables data protection for confidentiality and integrity.

- *Restricted Data Direct Access*: AWS tools enable reducing manual information access or processing, reducing the risk of human errors.

- *Incident Management*: Preparation for security incidents is one of the AWS best practices since it is strongly recommended to have incident management and investigation policies in place. Detection, analysis, and recovery procedures can improve by simulating security events and trying to stop the attacks.

Moreover, customers must get the full picture of the already mentioned *AWS Shared Responsibility Model*, which shows Amazon's limitation in protecting the infrastructure. Although users may assume that their services are 100% protected once they subscribe to the cloud, they must deploy some solutions to safeguard the information. AWS is only responsible for the infrastructure that permits services to run, while customers have to deal with the management and configurations of the instances and secure the platforms and applications. Understanding the design principles helps to identify the primary defensive objectives for customers deploying services in the cloud. Clients can prepare the infrastructure for any inconvenience only with a precise idea of these best practices.

2.2.1 AWS Incident Management

Amazon Web Services' best practices involve an incident response plan, even though the organization purchased all the most innovative and expensive preventive controls. AWS model promotes a few goals that the incident response plan should design. **Education** must be considered a priority. The CSIRT should be able to supervise a wide range of incident scenarios. They must have developed programming and investigation skills to lead the response process and recover from the compromise. Each specialist should have advanced craftworks in AWS cloud technologies and a complete knowledge of the services and applications running in the cloud. For instance, they may quickly identify the incident's root cause, whether they know which service released the logs, which is their meaning, and which is the traffic flow of the applications.

The team can acquire the required skills by running simulations of the incidents. *Simulate* is a critical part of the strategy since it spawns unexpected security events to test the preparation of the personnel. These practices may vary from *Blue Team* to *Red Team* exercises with a squad defending and the other attacking, and demand specific infrastructures to be deployed before the tests because the business can't risk compromising the production environment. Last but not least, one of the key AWS stages is *preparation*: CSIRT must have access to the appropriate tools to manage the incident and restore the previous unaltered versions of the systems. While preparing the architecture, the security department should assess the assets and identify the key personnel and resources that may be helpful during the response. Amazon Incident Response team suggests implementing playbooks and runbooks that bring several benefits by establishing transparent workflows to answer promptly.

The Playbook Framework underlined in the next section includes the guidelines for selecting the CSIRT individuals, roles, and responsibilities and explaining how to communicate during an incident without disclosing sensitive information. It taught the team how to classify the severity of incidents and how to prioritize the assets.

AWS Playbook Framework

Every customer utilizing AWS Cloud services can take advantage of the Playbook Development Guide that addresses multiple threat scenarios [26]. The framework is available in Github's repository, and security teams can create and integrate Playbooks for diverse attacks. Every playbook's title must encapsulate the scope of the document, emphasizing which use case it is covering and including an author and an approver assigned to the project. The playbook should be categorized with the date and the version number to monitor all the changes.

After an *Executive Summary* that summarizes its goals, AWS suggests building a clear-cut structure by analyzing the following points:

- *Threat and Response Steps*: The author should focus on the threat's description and the potential impact on the current infrastructure. Afterward, the writer can define step-by-step guidelines that will be used to respond chronologically to the security events.

- *Incident Classification and Tools*: Similar events will be classified with a criticality for the business depending on the compromised assets and the exposed sensitive information. Each playbook must list all the tools to detect, contain, investigate, and recover from the incident. AWS provides several native cloud technologies for this purpose.

- *Incident Handling*: This stage can drastically change depending on the analyzed threat and the selected framework. Incident handling starts from the *Preparation* and concludes with the *Lessons Learned* during the *post-mortem* activity. The structure of the playbook must facilitate CSIRT's arrangement and planning.

Security playbooks will be used only for general scenarios, enabling communication between C-level stakeholders of the organization. I redesigned the structure of the security Playbooks to create security runbooks to drive the technical responders against significant threats. Combining the information collected from the SANS and AWS frameworks, it is now possible to comprehend the successive chapters and the reasons for the implementation choices. Incident response is a broad field; every company must have plans to prepare and defend against future criticalities.

"If anything can go wrong, it will" (Murphy's Law, 1949).

3 Methodology

This chapter is dedicated to project design, focusing on the scope, milestones, and deadlines. It displays how to properly organize the tasks and the necessary stages to design an incident response strategy for specific scenarios. Bynder had already created an incident response plan based on the NIST publications before the beginning of my internship. On the other hand, playbooks and runbooks were necessary to cover all the critical scenarios of potential threats targeting the organization's cloud services.

3.1 Project Planning and Design

To reach the desired outcomes, I adhered to the established Information Security team's methodology, named **Agile**. This approach emphasizes flexibility and collaboration by breaking the project into smaller iterations called *sprints*, which usually last only two weeks. Agile was perfect for collecting feedback from the team and adjusting the plan accordingly. The described methodology allowed me to divide the project into several activities outlined by the *Milestones* of this section. The quantitative analysis of *Agile*, carried out by *Pedro Serrador* and *Jeffrey K. Pinto*, demonstrated that this methodology is one of the best because it usually brings success [27].

3.1.1 Scope

The project's scope has been discussed with the information security team before the plan of action.

Must Have	1) **Playbooks** provide a general overview of the incident response procedures and ensure all the stakeholders are aligned on the overall strategy. 2) **Runbooks** provide detailed guidelines to respond to specific incidents and ensure CSIRT preparation for threats.
Nice to Have	**Simulations** may identify potential issues with the IR procedures and help the CSIRT improve its incident-handling skills.
Not in Scope	1) A complete **Risk Assessment** wasn't required to identify the IR use cases. 2) **Monitoring** tools were already in place, and it wasn't necessary to analyze new technologies.

Table 3.1: The table highlights the "*must have*" that clearly describes the requirements, the "*nice to have*" that denotes functional tasks to improve the quality, and "*not in scope*", which includes the activities that are not needed to complete the program.

3.1.2 Project Planning

Project planning included the definition of some milestones that must have been fulfilled before the imposed deadlines. A project owner was responsible for supervising each phase, and the stakeholders must have been informed about the progress.

The milestones were matched with strict deadlines and a status that could be *Not Started*, *In Progress*, and *Done*. The plan should have been manually updated to report all the relevant exercises, and eventually, a *Gantt chart* assisted with the project planning and management, providing an overview and scheduling of all the tasks.

The initial project scheme was designed considering the *Problem Statement* and the SANS Incident Response framework composed of the six steps for a complete IR procedure. NIST recommends that information technology programs within organizations should be first generally prepared for any incident before moving on and reflecting on typical attack vectors. Since Bynder's general plan was already in place, I could focus directly on the use cases.

Milestone	**Owner**	**Deadline**	**Status**
IR Project Definition	@InfoSec	1 March 2023	Done
Risk Assessment	@Samuele Gandini	15 March 2023	Done
IR Scenarios Definition	@Samuele Gandini	1 April 2023	Done
Playbooks	@Samuele Gandini	1 June 2023	Done
Runbooks	@Samuele Gandini	15 June 2023	Done
IR Simulations	@Devops	1 July 2023	In progress
IR Finalization	@InfoSec	15 July 2023	Done
IR Review	@InfoSec	1 August 2023	In progress

Table 3.2: The table incorporates all the steps from the infrastructure analysis to the finalization of the project.

Each stage included multiple sub-tasks to satisfy the prerequisites of the Agile methodology. The assignments were expressed as follows:

1. **Incident Response Project Definition**

    - *Define the scope and the steps*: The first part of the project includes only the definition of its scope and steps to match the Agile methodology.The owner was the Information Security team because we scheduled multiple meetings to align on different topics.

2. **Risk Assessment**

    - *Identify the critical assets*: Risk assessments always start with the infrastructure analysis to determine which assets are more at risk. The evaluation focused on the cloud inventory and the likelihood of its violation. The result pointed out the most important systems for the business and enabled mapping out the attack vectors.
    - *Gathering information about the available tools for incident response*: While studying the company, I had to figure out the known mechanisms that may be useful to respond to any potential attacks. I collected information through Bynder's internal documentation and platforms, especially the AWS management console.

3. **Incident Response Scenario Definition**

    - *Identifying the principal threats*: Once the critical assets have been detected, I researched the main threats that may jeopardize cloud technologies.
    - *Mapping out the attack vectors*: This essential stage converted the multiple external and internal attack vectors into use case scenarios covered in the procedures.

4. **Playbooks**

   - *Creating Playbooks*: These procedures provide a general overview of the scenarios by selecting a category of attack vectors. Thanks to the Playbooks, all the stakeholders are aligned on the overall strategies.
   - *Writing Playbooks' steps*: Playbooks should be uploaded among the company's internal procedures, such as the internal wiki, and they are structured following the six stages of the SANS framework (Preparation, Identification, Containment, Eradication, Recovery, and Lesson Learned). Every playbook includes an Overview justifying why the threat class was chosen.

5. **Runbooks**

   - *Runbooks creation*: The use cases are converted into runbooks, the technical guidelines for the Computer Security Incident Response Team. Its members use their skills and the available tools to contain the events and restore the previous situation.
   - *Writing Runbooks' steps*: As for the Playbooks, Runbooks provide a whole procedure involving Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. The *post-mortem* activities are similar for most scenarios, although they were repeated in each runbook to build comprehensive directives for the team. The initial summary briefly clarifies the potential impacted resources and other information (insider threat, endpoint, credentials breach, malware, etc.).

6. **Incident Response Simulations**

   - *Researching for testing strategies and tools*: The security division must test the methods' effectiveness by running simulations. The assessment

strategy must not condition the production branch; it may consist of virtual environments, for example. Furthermore, they must look for simulation tools to speed up the process.

- *Run incident simulations*: The Information Security unit can launch specific simulations to analyze CSIRT behavior actively. Hence, InfoSec can collect data about their activities and the skills that may be valuable during an attack.
- *Evaluate and upgrade the runbooks*: Data collected from the previous step can be used to verify the processes' effectiveness and efficiency, and InfoSec can highlight any issue or gap to improve their quality.

7. **Incident Response Finalization**

   - *Assessing the outcomes*: The outcomes are shown during an incident response review meeting with Information Security and other individuals from IT, DevOps, Legal, and AWS Customer Support groups. The presentation includes final remarks and some opportunities for growth by promoting new detection mechanisms and simulation tools.

8. **Incident Response Review**

   - *Review the current scenario*: Information Security must periodically verify that the created scenarios are valid, considering the business infrastructure and potential new threats.
   - *Evaluate new playbooks and runbooks*: InfoSec should create new Incident Response use cases to cover as many security events as possible. Templates for playbooks and runbooks may be prepared for future purposes.

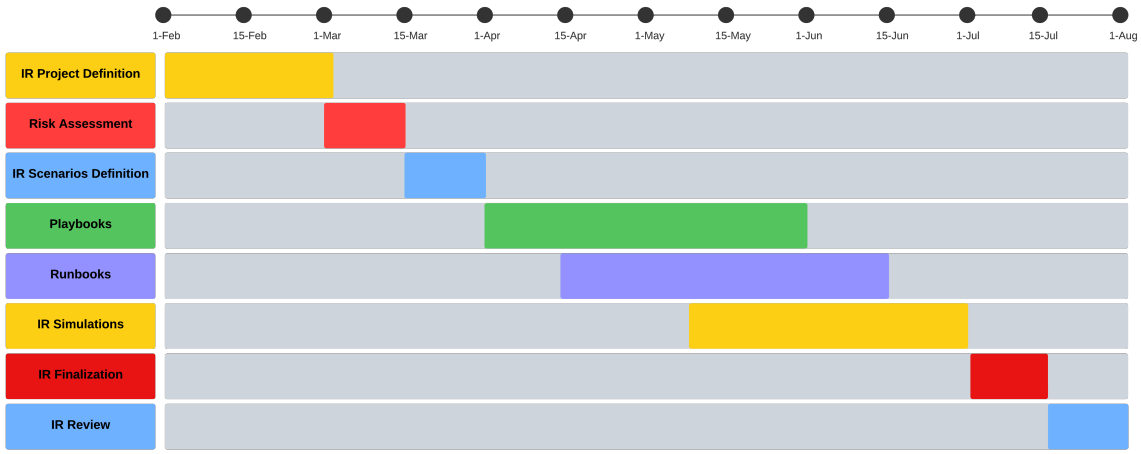

Figure 3.1: The Gantt chart helped visualize the project's various periods, starting from the beginning of February 2023 and ending six months later. *Playbooks*, *runbooks*, and *incident response simulations* had overlaps because the process was iterative, and one phase depended on the other.

Methodology gave input for the planning technique for defining incident response plan scenarios. The subsequent chapters focus on the incident scenario "*Ransomware in AWS*", showing how to conceive the stages from *risk assessment* to *incident response finalization*.

4 Incident Response Development

This chapter shows the preparatory steps required to write the playbooks and runbooks for the incident response plan. At the basis of the incident response strategy, we find the study of the current infrastructure, the risk assessment to recognize the critical assets and the most dangerous threats, and the selection of the tools to intercept and remediate incidents. This section describes the weaknesses of the target systems, leading to an evaluation that was required to craft the use case scenarios. Even though Bynder's cloud architecture was the target of this reflection, sensitive information will not be included, maintaining a general approach to incident response planning.

4.1 Studying the company's infrastructure

Exploring the architecture of a new company can be challenging. It would be best to familiarize yourself with the department, operations, and technologies before evaluating the vulnerabilities and threats for specific systems. Hence, risk assessment is a complex process that demands a comprehensive understanding of the business, research, and strategic arrangement.

4.1.1 Risk Assessment: An In-Depth Exploration of Stages and Prerequisites

According to the *NIST Guide for Conducting Risk Assessment (Publication 800-30)*, this methodology informs decision-makers about identified threats to the organization, internal and external vulnerabilities, the impact of threats exploiting the detected exposures, and the likelihood of the harm occurring [28]. Crossing these elements, we can obtain a crucial risk value (*impact X likelihood*) that helps determine which security measures we can apply to lower either or both the impact and the probability. The process is classified into three main steps that produce a final document containing the outcomes:

1. *Assessment Preparation*: The first stage focuses on identifying the scope of the assessment and choosing a proper risk model. Some related activities may be the definition of ways the risk can be accepted or rejected, how to enable information sharing, or highlighting any question relevant to the purpose of the evaluation. Before moving on, the security team must have declared assumptions and constraints for the assessment.

2. *Conducting the Assessment*: This phase assigns a risk level to the organization's assets. It starts by enumerating the company's critical assets of the selected landscape. Considering the scope of the incident response project, I prioritized the cloud services because they could lead to the most severe economic damage if violated.

   Once we get a complete inventory, it is possible to proceed as follows:

   - *Threat sources evaluation*: Each asset identified during the previous step may be targeted by many threats. The output of this stage includes a list of menaces that must be prioritized depending on their impact, intentions, and capabilities.

- *Vulnerabilities identification*: The vulnerability assessment allows the organization to understand whether there are weaknesses in the infrastructure that attackers can exploit. A single threat event can target multiple vulnerabilities, constantly increasing in growing corporations, such as Bynder, due to more extensive information systems and processes.
- *Determine Likelihood and Impact*: We can determine the likelihood and impact of an event from the threat attributes and the company conditions. The overall probability is calculated by combining the occurrence of the event and the possibility of adverse effects caused to the systems. An impact value should also be estimated by evaluating the potential harm to assets, operations, and individuals.
- *Risk value*: The last step resolves the risk to the organization by taking into account the impact and likelihood values. The risk may help identify which security measures can be applied to the prioritized assets to minimize either the impact or the likelihood of the malicious events.

Impact

Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Figure 4.1: The *risk matrix* visualizes the final value from likelihood and impact. The 5x5 matrix provides more insights into levels of severity by assuming a more granular approach [29].

3. *Sharing the results*: Last but not least, the security department must design a communication plan for concluding the risk assessment. The sharing method may vary depending on the designated stakeholders and the organizational policies.

The risk assessment NIST approach was applied to Bynder, as highlighted in the following subsections. They generally describe the main assets and threats for the cloud ecosystem, justifying the decision of the project's use cases.

4.1.2 Risk Assessment: Critical Assets

For a business-to-business corporation providing cloud-based services through AWS, the priority is for the cloud assets during an extensive environmental analysis. AWS offers plenty of services for its customers to develop new applications. Creating a web app is easy and fast, from making it reachable to the public to ensuring security and reliability. As reported by *Richter*, Amazon Web Services is maintaining the lead with 32% of the Cloud market [30] by providing a *pay-as-you-go* service that allows customers to be billed according to the resources they are utilizing and the duration they are using them.

Bynder relies on AWS and uses some of these services. Even though I cannot be too specific about their usage, I can list some of the most diffused Amazon resources. The assessment of Amazon Web Services technologies has been performed by following the approach of the paper "*Automated Security Assessments of Amazon Web Services Environments*", which suggests a complex solution to automate the discovery of security gaps. Although this thesis does not explore its method, the research mentions some of the most relevant Amazon solutions, giving insights for identifying assets and threats [31].

- **Amazon EC2**: Elastic Cloud Compute is one of the oldest tools that provides secure computing for applications. Customers can launch virtual computer instances and configure the operating system, CPU, memory, storage, and network.

- **Amazon ECS**: Elastic Container Service helps to build and manage apps with container orchestration rapidly. Once the Docker image is ready, customers can upload it to an ECS repository, setting the number of compute nodes.

- **Amazon S3**: Simple Storage Service can store content for the business, maintaining its availability and offering security and scalability. The objects are held into *S3 Buckets*, globally accessible and managed through **Amazon CloudFront**, a content delivery network that helps deliver static content at high transfer speed.

- **Amazon Route 53**: It serves as DNS, connecting the registered domain names with the servers' IP addresses. This service lets users request AWS resources, such as S3 Buckets content.

- **Amazon RDS**: Relational Database Service is an easy-to-use tool that enables setting up relational databases in the cloud. AWS provides all the administration support needed by databases, automating some tasks, such as patching and backup.

- **Amazon Lambda**: Serverless service that permits running code in the cloud without managing machines. Users can write and upload the code to a Lambda instance, creating a function.

- **Application Load Balancer**: AWS's crucial service that permits distributing the traffic across instances or containers. It can decide to add a machine

whether the traffic is overwhelming the resources, monitoring the availability of the applications.

- **Amazon VPC**: Virtual Private Cloud is one of the vital security services that contains the running AWS resources and controls how external applications access and retrieve information. VPC enables data protection with firewalls surrounding the infrastructure and maintaining the separation from other people's assets.

- **Amazon IAM**: Identity and Access Management helps to define roles and permissions, assigning them to AWS users and groups and monitoring access to AWS services. It is one of the central security tools since it manages *who can access what*.

- **Amazon CloudWatch**: One of the cores monitoring AWS services that control the status of the applications. ClowdWatch collects logs and data events and studies how resource utilization can be optimized, improving the performance of the services.

- **Amazon CloudTrail**: It allows monitoring users, roles, and AWS services actions to enable risk auditing, governance, and compliance. This tool can scan *who is doing what* on the applications.

Within the B2B cloud landscape, *S3* and *RDS* jointly compose the business's core infrastructure, offering scalable storage for data and digital assets and resilient databases vital for cloud-based applications. Other AWS tools may be relevant depending on the scope of the enterprise. Some will be introduced in the following sections, talking about incident response, while others will not be mentioned since they are not significant.

4.1.3 Risk Assessment: Threats Analysis

After identifying the main assets, I did some research to outline the main threats and the vulnerabilities within the cloud, exploited to compromise the confidentiality, integrity, or availability of services and data. *Serdal Kepil* proves that the main security issues of AWS technologies derive from a lack of configurations or credential theft and identifies multiple groups of dangers that should be evaluated while guarding the environment [32]:

- **S3 buckets misconfiguration**: S3 Buckets should be adequately configured when initiated in AWS. Attackers can exploit this vulnerability and compromise the content if unrestricted access is permitted to all users. The buckets can be targeted by **ransomware** when an attacker has read and write permissions; all the files can be encrypted, with a document left for extortion. S3 buckets may also cause severe data leaks because malicious actors might send undetected requests to access the objects within the storage service. If S3 access logs are not enabled, the attempts may remain hidden. *Chickowski* reports Amazon S3's worst breaches, showing that 7% of the servers are publicly accessible, while 35% result unencrypted [33]. It is relatively easy to access a public S3 Bucket (some websites allow researching for them, such as *Grayhat Warfare*), so it is essential to care about their configuration.

- **Malevolent AWS API request**: Malicious code can be injected into one of the numerous AWS APIs available, leading to Distributed Denial of Service or SQL injections. APIs must be supported with adequate encryption options and monitoring of Amazon CloudTrail, which can notify any unexpected API call.

- **Unfiltered traffic from untrusted sources**: Network protection is a critical component of the AWS infrastructure. If the deployed instances can be

accessed under any condition and there are no rules to deny traffic, DDoS and other attacks can be more easily performed against the AWS resources.

- **IAM improper permission and privileges**: Amazon IAM wrongly set up permissions may allow unauthorized users to access sensitive information. All users' privileges must be reviewed periodically to avoid any weaknesses in security and compliance.

- **Credential theft**: Several violations of cloud resources are possible thanks to credential theft attacks through *phishing* or other techniques. Some companies decide not to follow AWS best practices and do not enable multi-factor authentication or do not implement monitoring solutions, leaving the environment unprotected.

- **RDS misconfigurations**: Other critical resources that can be misconfigured and subject to attacks are *Amazon RDS*. Despite databases containing sensitive data, AWS is not responsible for securing the information, and there are multiple ways for attackers to exploit vulnerabilities in their settings. According to the Product Management at Eureka Security, exposed resources, weak encryption, and improper authentication may be fatal for the business, especially when combined with an inadequate retention period [34]. In the potential scenario of **ransomware** encrypting RDS, it becomes complicated to recover data without a proper backup policy.

In conclusion, considering these top menaces for AWS cloud resources, it is evident that many risks surround Amazon S3 and Amazon RDS, and they must be prioritized while designing the incident response strategy. Therefore, the first threat scenarios must be linked to these services, focusing on the most disruptive attack in circulation: **ransomware**.

4.2 Incident Response Scenario

Thanks to the risk evaluation, it was easy to prioritize some use cases rather than others. Referring to Bynder, the decision involved the entire Information Security branch, which received further recommendations from the Amazon Customer Support team. In the end, **Ransomware in AWS** was selected as the main scenario. The program converted the urgency of ransomware targeting Amazon Web Services resources into response actions. Consequently, it was possible to elaborate a playbook, including general information to explain how ransomware acts and how to deal with it, and runbooks, examining different incident response options depending on impacted technologies.

4.2.1 Designing a Ransomware Incident Response Plan

As we know from Chapter 1, ransomware **critically impacts business**. It may target AWS architectures, causing a disruptive effect on the operations and compromising sensitive information. Proper security tools and procedures should be ready for a strategic and adaptive response. Some AWS services can store data and assets, and *Crypto-Ransomware* may exploit weaknesses to act and block the systems. Each ransomware use case demands a nuanced response, and while the playbook provides the strategic framework, the runbooks translate these strategies into actionable tasks. I finally came up with one playbook and two diverse runbooks addressing the Amazon Web service use cases for *Amazon S3* and *RDS*, which store information and let the company run its cloud-based services:

- **Ransomware in AWS Security Playbook**: The playbook provides an overview of the Incident Response plan. All the stakeholders can understand what would happen in case of a ransomware attack compromise and which high-level process is carried out by the operatives.

- **Ransomware Response for AWS S3 (Simple Storage Service) Runbook**: S3 buckets are exposed to ransomware, especially when not correctly configured and monitored by Amazon native tools. In the third episode of *AWS The Safe Room* centered on incident response, the Amazon Web Services Security Consultant, *Jason Hurst*, presents how easy it is to delete all the data of an S3 bucket configured with improper permissions, leaving a simple text file containing a request for the payment [35]. This runbook is critical to limit the impact of an S3 bucket violation and includes the tech-level information to identify, contain, investigate, and recover malicious activities.

- **Ransomware Response for AWS RDS (Relational Database Service) Runbook**: As well as S3, RDS services can be vulnerable to ransomware. Database information can be encrypted or removed by potential attackers, and only a well-structured incident response plan can address the situation by solving the issue. The runbook contains the best practices for Amazon RDS to prevent Ransomware attacks and the technical guidelines for returning to business.

The described runbooks were preferred to the ransom response to *Amazon EC2*. Even though it is one of the primary services delivered by AWS, the overall risk remains with medium severity, leaving exclusive precedence for S3 and RDS. Accordingly, this thesis will not cover the EC2 strategy. The implementation of the step-by-step procedures will be discussed in Chapter 5, after a brief presentation of the tools that assist incident response.

4.3 Available Tools for Incident Response

A fundamental preliminary step of the project was to understand which tools were available. Each new technology can only be activated and configured with a proper evaluation of its capabilities, effectiveness, and a consideration of the expenses. This paragraph introduces vital solutions for ransomware opposition, illustrating what cannot be missing within the incident response arsenal of the organization.

Extended Detection and Response

XDR is already mentioned in Chapter 2 as an advanced version of EDR, and it can recognize malicious behaviors with the correlation of logs from different sources. The choice of using an XDR solution for an IT company is related to its capabilities of giving in-depth looks at the data in networks, endpoints, clouds, and applications, as reported by *Shaji George*, *A. S. Hovan George*, *T. Baskar*, and *Digvijay Pandey* [36]. Security agents are installed on the company's appliances, and XDR can monitor the activities, from the network communications to the event logs. For instance, every laptop employees use is furnished with an application that monitors the traffic and regularly scans for viruses. All the information the agents collect is agglomerated in a central platform accessible by the security team. The latter can respond to malicious events and take countermeasures directly on the devices by isolating them from the network or launching scripts. XDR is currently a must-have within an IT company because it is a practical solution to administer the security of the infrastructure.

Network-based Intrusion Detection System

NIDS is a powerful ally for incident detection. This technology analyzes internal and external network communications to identify any unexpected behavior, and, eventually, it may alert the security specialist whether any malicious attempt is discovered. The main issue for IDS was attributable to the false positive rate since

fake alerts were reported too often, overwhelming the security analysts with inaccurate notifications. Now, with new NIDS trends, Deep Learning integration can dramatically lower the false rate, allowing faster detection and clear correlation of the events. The article of *Zeeshan Ahmad* depicts how Deep Learning can be used for implementing more effective Intrusion and Detection Systems and how future efficient NIDS framework may also detect zero-day attacks [37].

4.3.1 AWS Incident Response Tools

Although XDR and NIDS are great solutions to safeguard the environment, I want to focus now on AWS native security tools that are more relevant considering the scenarios. The senior security consultant at Amazon, *Vesselin Tzvetkov*, wrote an AWS blog article underlining how to automate incident response in a cloud environment. He proposed architectures and tools that should be in place to avoid catastrophic consequences [38]. This section is dedicated to the native tools cited in the runbooks.

Amazon GuardDuty

As the principal AWS security tool for incident response, *GuardDuty* enables monitoring threats of instances, containers, users, databases, and storage. It offers a complete set of security functionalities and takes advantage of machine learning to create behavioral patterns of the environment to detect any anomaly. Thanks to GuardDuty, it is possible to automate the response by creating automatic activities triggered by specific actions. It can improve the visibility of the operations by showing unexpected data access and logins, analyzing files for malware, and identifying suspicious behavior in container workloads.

GuardDuty can be activated with multiple modules integrating with other AWS resources.

- **S3 Buckets**: CloudTrail S3 data events are continuously examined, monitoring accesses and activities of the S3 Buckets.
- **EKS Audit logs and runtime monitoring**: *Amazon EKS* (Elastic Kubernetes Service) is used to run *Kubernetes* in the AWS cloud. This feature allows a continuous security analysis of the audit logs and runtime monitoring of Amazon EKS instances, such as file access, network connections, and process execution.
- **Malware detection**: GuardDuty triggers an alert when an EBS volume is compromised by malware. *Amazon EBS* (Elastic Block Store) is a block storage service designed for EC2.
- **RDS**: GuardDuty looks for potential threats accessing RDS databases. It analyzes the logins and creates a standard behavior for the organization.
- **Lambda**: Lambda functions execution generates network activity logs constantly monitored for threat detection. GuardDuty may discover cryptocurrency mining or compromised functions communicating with known malicious IP addresses.

Security teams should evaluate the benefits of these features by considering the expenses for their activation. In a typical multi-account AWS architecture that separates the service account(s) from the security one, Amazon GuardDuty forwards its findings to CloudWatch, which sends the events to the central security infrastructure. Each event is mapped with a *Lambda Function* response action immediately initiated by calling the AWS System Manager. As a result, the automation is executed in the service account, and for example, a compromised EC2 instance can

be isolated when a certain event happens. It is crucial to test every operation in a non-production environment.

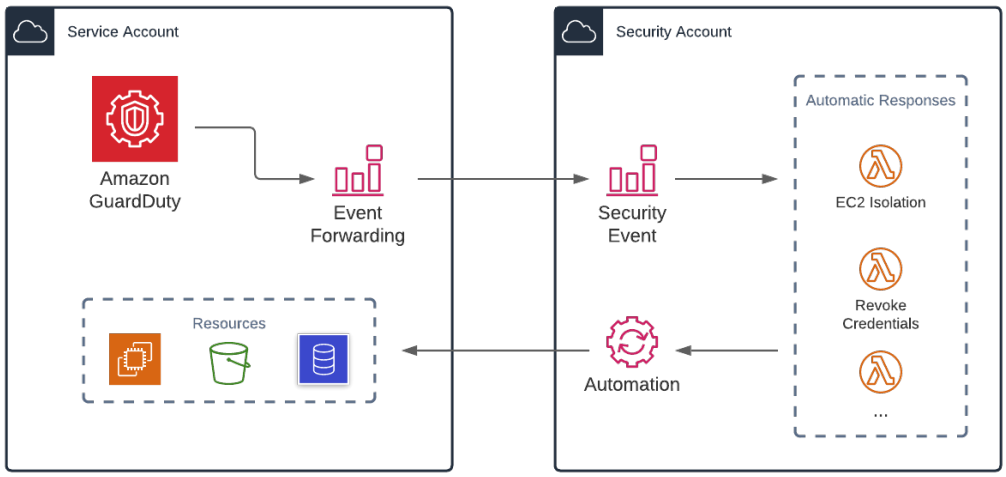

Figure 4.2: The AWS infrastructure can benefit by implementing this architecture with Amazon GuardDuty. Incident response automation may improve the whole process and instantly block several types of attacks.

Amazon Security Hub

Amazon Security Hub is a critical tool for security and compliance. It collects data from AWS accounts and active services to discover security issues [39]. Any deviation from the *AWS Foundational Security Best Practices*, which includes a list of controls, is reported in a central platform of the security account.

There are several advantages brought by Amazon Security Hub that also benefit the *preparation* phase of the incident response plan. First, with *findings prioritization*, each piece of information is collected from the accounts to a central place where the security team can analyze the issues. The alert is assigned to a criticality level (*high*, *medium*, *low*) that indicates which problem should be solved immediately to preserve the protection of the cloud. Security Hub continuously runs automatic

security checks based on AWS best practices, and it is possible to automate the updates and remediation of the findings by setting up custom actions on defined criteria. This is a crucial tool to monitor the status of the resources, and, for example, it controls if the encryption of RDS Databases is enabled or if any S3 bucket allows public access.

AWS Config Rules

Many controls are not applicable by using only Amazon Security Hub, and *AWS Config Rules* are the best solution to keep track of all the configuration changes. Indeed, AWS Config can monitor the active services' settings of the AWS account, and the rules permit the evaluation of the compliance information. For S3 Buckets, we can enable *s3-bucket-versioning-enabled* to check whether anyone turns off *S3 versioning* or *s3-bucket-public-read-prohibited* to verify if we are avoiding public read access. Moreover, AWS Config Rules for Amazon RDS, such as *rds-in-backup-plan* monitor if RDS Databases are included in the AWS Backup plan. AWS created a *complete list of the Config Rules* for its customers.

AWS IAM Access Analyzer

IAM Access Analyzer keeps track of resources and accounts shared with third parties. It can detect unauthorized access to AWS resources, giving relevant insights for identifying threat actors' activities. The product manager, *Mathangi Ramesh*, stated that the IAM Access Analyzer is also fundamental for generating fine-grained policies based on the access activities of users. Therefore, this powerful mechanism helps implement the **least privilege** principle, providing only the required workload permissions [40].

AWS Self-Service Security Assessment

This is an important service mainly for organizations new to AWS that have yet to implement other security measures. It is an easy-to-deploy, cheap solution for quick security assessments across the cloud infrastructure. This utility has been developed starting from *Prowler*, another popular open-source project that performs evaluations based on the best practices of AWS. It is relevant for incident response plans because, as stated by the *AWS Public Sector Blog Team*, it proposes a functionality to identify the missing controls to protect against Ransomware [41]. More than 256 checks are launched over the cloud instances, and a final report suggests which security measures should be added to the environment.

Amazon Athena Bootstrap

As *John Haggerty* and *Thomas Hughes-Roberts* noted, the complexity of incident-related logs may lead to temporal constraints due to the massive amount of information that can be recorded from operating systems and applications. The intricacy increases when cloud technologies are considered, and the two researchers advise being equipped with solutions that can rapidly classify and visualize the captured data [42].

Amazon Athena Bootstrap is the AWS critical service for log analysis during the *eradication*. It is a core serverless technology that allows inspecting several AWS data sources, such as information contained within S3, and using SQL or Python. The importance of Athena Bootstrap is clearly illustrated by the fifth episode of *AWS The Safe Room*, in which the Engineering Lead of the AWS Customer Incident Response team, *Ryan W Smith*, shows how to perform a log analysis [43]. In the presentation, Athena takes the logs from the S3 buckets of the log-archive account, which aggregates all the data received from all the organization's resources.

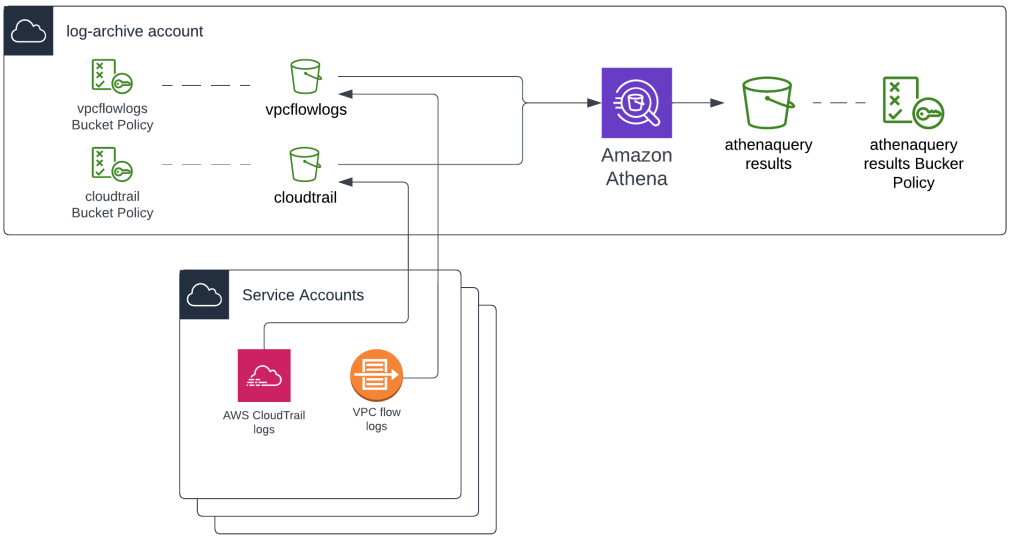

Figure 4.3: Athena uses a specific user's permissions (usually the analyst's) to conduct the operations; the query results are stored in a third S3 bucket of the same account, and the users examine it whenever needed.

The queries are submitted in the Athena editor, and we can simply use SQL to search all the data recursively from the S3 Buckets. This tool is beneficial during urgent investigations, such as the ones required in a security incident.

AWS Assisted Log Enabler

Another tool that can assist the *eradication* stage is Amazon Assisted Log Enabler, showcased by the AWS Security Consultant *Joshua McKiddy* [44]. Its features focus on turning on the logs, which are critical elements during an investigation. Assisted Log Enabler initially creates the buckets to store the information and then checks for all the running services within the cloud infrastructure: all the disabled logging is promptly turned on. Thus, customers can study future and possibly ongoing security incidents.

Amazon Detective

Detective is the Amazon Swiss Army knife for investigation. Even though many organizations prefer to rely just on *GuardDuty*, Detective provides visual representations of the security issues, boosting the analysis and the events' correlation. It shows the users' interactions with the resources and uses machine learning to produce activity diagrams.

Amazon S3 Versioning

Versioning is a remediation method that allows keeping multiple versions of the objects in S3 buckets. By enabling this technology, AWS customers can maintain the previous versions of the assets after they are modified. When an object is deleted, it is not removed permanently, but it is signed with a *delete marker* (only the bucket owner can permanently delete a version under certain circumstances, and MFA is required). *S3 Versioning* is a great functionality that can be used during the *Recovery* phase whenever a bucket is compromised.

Amazon Backup

AWS Backup is the leading service for the *Recovery* stage to restore all the impacted resources. Data protection can be centralized across the cloud, from creating a backup plan to setting the frequency and retention policy. These steps must be carried out during the first part of the incident response plan to be prepared in case of a potential violation.

Other AWS security tools might come in handy while responding to an incident. However, they might be too expensive for the enterprises that usually discard them from their security toolkit. Given that you have acquired background knowledge, I can finally present the developed playbook and runbooks.

5 Incident Response Implementation

Implementation is the heart of the thesis since it describes how playbooks and runbooks for the incident response plan were deployed. *Ransomware in AWS* proposes one playbook and two runbooks, describing the processes for the indispensable resources inside the AWS cloud infrastructure, *Amazon S3* and *Amazon RDS*. All the documents differ from the original ones currently part of Bynder's security posture because they cannot disclose private information about the business, such as internal technologies or financial choices. Overall, they generally reflect on a potential deployment for an incident response plan, also delivering helpful insights on specific architectures.

5.1 Ransomware in AWS Incident Response Plan

The scenario recalls the most dangerous threat in the cloud: ransomware. Ransomware is one of the biggest challenges for IT businesses since it can encrypt all data and significantly impact the services. As pointed out by the AWS report *"Securing your AWS Cloud environment from ransomware"*, these attacks are still effective because awareness among personnel is low and critical vulnerabilities are not patched within a restricted timeframe. Firms must define a consistent incident response plan because they cannot pay the ransom. Sending money to criminals would just raise their funds to carry out further attacks, and in addition, there is no guarantee that they will share the decryption key even after the payment [45].

The security playbook provides a general overview of the process, and it was created starting from the idea of the AWS security specialist solutions architect *Brad Dispensa*, with his Amazon blog's post *"Ransomware mitigation: Top 5 protections and recovery preparation actions"* [46]. Although he highlights some preparation steps for protecting against ransomware, there are no clues on the other incident response stages gained from research and environmental studies.

The first runbook extracts, instead, information from the relevant publication of *Megan O'Neil*, *Kyle Dickinson*, and *Karthik Ram*, underlining detection and response for the *Amazon S3* use case [47]. The collected insights were reprocessed to adapt the operations according to Bynder's cloud architecture. Two last useful articles for *Amazon RDS* were the following:

- The AWS solutions architects *Marshall Jones* and *Deric Martinez* released the one who detailed GuardDuty's role in RDS databases threat detection [48]. Even in this case, this writing is not enough to produce a complete incident response runbook, and it was just an input for *identification* and *eradication*.
- The blog post *"Investigate VPC flow with Amazon Detective"* by *Ross Warren* and *Jim Miller* illustrates how to determine the scope of security issues. *VPC Flow logs* collect data about IP traffic from and to a cloud private network and examine which addresses access RDS services [49].

Runbooks enclose flowcharts that characterize each step with basic instructions and queries to investigate the attacks. In conclusion, these reworked versions follow the *SANS* incident response framework. They present an overview of the use case and the six incident response phases, showing how to deal with security violations.

5.1.1 Ransomware in AWS - Security Playbook

Playbook Name	Ransomware Response in AWS
Playbook Description	Incident Response Plan for Ransomware attack scenarios targeting the AWS infrastructure
Playbook Manager	Information Security Senior Director
Informed	Executives, Information Security, IT, DevOps, Legal Department
Impacted Assets	AWS cloud services and resources
Version	1.0
Version Date	1 Apr 2023

Table 5.1: The table illustrates the general information about the playbook.

Overview

This **Playbook** informs the interested teams about the response procedure for ransomware attacks targeting AWS services. It ensures that all the stakeholders are aligned on the overall strategy for this scenario. Ransomware may cause the business billions of dollars of damage, interrupting operations. It tries to infect any accessible network and needs to gain access to an organization's infrastructure, encrypt files, and demand ransom to be successful. Ransom attacks are effective for multiple reasons:

- Low awareness among individuals;
- No backups available;
- Little effort and massive revenue for attackers;
- Slow vulnerability (CVE) patching;
- No planning strategy to address security issues;

- Multiple attack vectors;
- No customer reaction if the bad actors are exfiltrating data without encrypting or deleting information.

Affected organizations should not pay the ransom: there is no warranty that encrypted data and locked systems will be restored after the payment, which will only motivate malicious behaviors. Therefore, Ransomware is a severe threat, and responders must be adequately prepared to defend against it.

The following related **runbooks** include a step-by-step technical procedure for handling an incident aiming at specific AWS technologies:

1. **Ransom Response for AWS S3 (Simple Storage Service) - Runbook**
2. **Ransom Response for AWS RDS (Relational Database Service) - Runbook**

The incident response activities rely on security measures and AWS native services within the cloud infrastructure.

Preparation

The preparation steps must be completed before an incident.
Initially, the preparation phase involves establishing a communication plan and reviewing the current security controls and policies.

1. **Determine the CSIRT memebers**

    - CSIRT will be guided by an *incident response manager* responsible for designing roles and responsibilities for the other members.
    - CSIRT must include individuals from Information Security and DevOps managing the AWS environment.

- CSIRT must include one representative from the legal department to address any concerns related to sensitive information or third-party organizations.
- CSIRT's size must be limited to simplify communication and support efficiency and confidentiality.

2. **Establish a reliable communication channel**

   - Ensures Bynder's instant messaging program and video communication service are working correctly and are available during the incident response.
   - Create a dedicated channel with the messaging solution, adding all the CSIRT members.

3. **Conduct security awareness campaigns**

   - Security awareness campaigns increase employees' knowledge and attention to internal security, significantly reducing the likelihood of an incident.

4. **Review the current security measures and policies**

   - *Set up the ability to recover apps and data*: Bynder must ensure that it can recover its data, regardless of how the system was made inaccessible. *AWS Backup* can restore the data (simple snapshots of EC2 instances are insufficient) and supports the cross-account capability, placing the backups into separate and dedicated accounts. The likelihood that a threat actor may temper with the backup is reduced.
   - *Encrypt your data*: Encryption must have been enabled so that only authorized users and services can access the resources. Encryption prevents

double extortion schemes, in which threat actors exfiltrate data, encrypt it, and threaten its release.

- *Apply critical patches*: Misconfiguration and vulnerabilities make attackers' lives easier. Security-related patches with the slightest delay possible avoid bad actors exploiting existing CVEs. Monitoring applications must scan images and *Kubernetes* clusters.
- *Follow a security standard*: *AWS Security Hub* must be active to automate controls across AWS services and third-party tools, identifying gaps in security according to *AWS Foundational Security Best Practices*.
  Furthermore, the *least privilege principle* must enforce policies to limit actors' capabilities. *AWS IAM Access Analyzer* facilitates the generation of permissions; short-lived *IAM Access Keys* must be applied to restrict access duration to compromised resources.
- *Strong Authentication*: AWS suggests applying strong authentication policies, combining *Single Sign-On* with *Multi-Factor Authentication*.
- *Make sure to monitor and automate responses*: Intense infrastructure monitoring can help protect against Ransomware. Integrating AWS native and third-party tools with an AWS multi-account architecture leads to an advanced cloud environment where the business can count on automation and prompt response.

Identification

The identification phase depends on the services that need protection and the tools available for detection. Ransomware detection may occur in many different ways, and the CSIRT must review one of the linked security runbooks for more specific use cases.

Overall, as mentioned by AWS, the attack can be notified in many different forms, depending on the architecture configuration:

- An alert is generated on *Amazon GuardDuty*, *AWS Security Hub*, or alternative monitoring systems;
- An EC2 instance cannot be accessed anymore, although it appears appropriately configured and running;
- *Amazon CloudWatch* reports alarms about network reachability issues;
- The bad actor demands ransom via email or alternative communication channels.

Identification furnishes the first insights about the impacted AWS resources (S3, RDS, etc.) and the initial attack vector the threat actor utilizes. Once the ransomware has been detected, CSIRT must create a dedicated communication channel and a ticket that documents the response progress before proceeding with the containment.

Containment

Containment tries to mitigate the incident by limiting the damage to the business. It might vary depending on the compromised AWS resource, and stakeholders may have dissimilar opinions on containment (some would focus on returning to business rather than fixing the vulnerabilities). However, early detection is essential to reduce the impact of the incident. CSIRT must always prioritize critical information, and they must follow the below steps, depending on the affected asset(s) (refer to the incident response runbooks for more specific use cases):

1. **Do not pay the ransom**: The payment does not guarantee that the attacker(s) will restore your data. If data is encrypted and no backups are available, a representative from the financial team should help the CSIRT by

performing a cost-benefit analysis to weigh the value of the data/reputational compromise against the payment to the attacker.

2. **Determine the type of ransomware *(if possible)***: ransomware can encrypt objects or files (Crypto-Ransomware), lock out access to the AWS infrastructure or resources (Locker-Ransomware), or others.

3. **Limit access to network and/or resources**: Modify the Security Groups to isolate the network and limit access. Change S3 Bucket(s) policies and delete IAM users, policies, and roles to minimize the opportunity for the attacker(s) to spread the infection.

4. **Check AWS tools logs**: AWS logs (CloudTrail, S3 logs, etc.) may provide insights about unauthorized activity, such as creating IAM users, policies, roles, or temporary security credentials and deleting/revoking them.

5. **Check for unpatched software**: If the attacker(s) exploited unpatched software, out-of-date OSs, or AV tools to spread the malware into the infrastructure, EC2 instances must be updated with all software packages, virus signatures, and definition files. This may prevent the bad actor(s) from exploiting the same vulnerabilities (if the vulnerabilities cannot be fixed, CSIRT must ensure that the security measures are blocking similar attacks).

6. **Check for resources at risk**: Remove any resources targeted by the same attack vector, depending on the previous steps' considerations.

Once the Containment stage is complete, CSIRT should have restricted all bad actors' activities, and the environment should be safe.

Eradication

The eradication phase helps determine the attack vector and investigate any possible attempt the attacker(s) made to maintain access to the resources. During the investigation, the CSIRT should look for every vulnerability in the AWS environment and add security measures to avoid any possible future damage. CSIRT has to understand if the impact from the incident has been correctly contained and if there is any ability to restore the ransomed data from backups/snapshots.

The investigation determines the impact and the amount of resources affected, with the criticality of the disclosed data. CSIRT can assess the attack vector and retrace the bad actors' activities with the following steps:

1. **Enable tools for logs analysis**: AWS native services may help CSIRT examine the logs. Depending on the affected application(s), different tools can be activated and used (supposing that *Amazon GuardDuty* and *Security Hub* are already working).

    - *Amazon Athena* uses SQL to query the records;
    - *AWS Assisted Log Enabler* activates critical logs to identify the bad actor's persistence;
    - *AWS Config Rules* may detect any change in the infrastructure's configuration;
    - *Amazon CloudWatch* provides information on abnormal data transfer spikes;
    - *AWS Detective* helps visualize the correlations of the threat actor's activities;
    - *Amazon CloudTrail* can detect unexpected user activity and API usage.

2. **Analyzing the logs and retracing the bad actor's activity**

   - CSIRT must determine when the infection occurred and how through logs analysis (CloudWatch can help you review logs such as application logs, operating system logs, database logs, etc.)
   - Reviewing the findings from GuardDuty and Security Hub may help reduce the additional effort required to search application-level logs.
   - CSIRT must identify all the IoCs (Indicators of Compromise). Any malware identified during the analysis must be removed.
   - Determine if any third-party decryption software is available when the ransomware has been identified (*No More Ransom Project* may provide a decryptor for the data).
   - *(Optional)* If any unexpected activities or unauthorized IAM users, roles, or policies are detected, the CSIRT should return to containment to isolate the environment and limit the threat actor's capabilities.

3. **Review the Security Controls**

   - CSIRT should assess the current security measures and evaluate whether they are enough to perform quick and effective incident response actions.
   - New Amazon GuardDuty features or AWS Config Rules may be introduced, and they must ensure all the logs are available (AWS Assisted Log Enabler may help with this task).
   - *AWS Self-Service Security Assessment* may provide critical insights, identifying security measures that could improve the protection against ransomware.

4. **Determine the business impact**

   - *This step can be carried out ONLY after the incident has been contained and the impact has been limited.*

- CSIRT must prove all applications impacted during the incident and any data the attacker may have disclosed.

  The bad actor may have compromised Confidentiality, Integrity, and Availability, and the team must determine the incident's overall impact (low, medium, high, or critical).
- Any impact/experience of the issue must have been documented in the incident ticket. This process will be helpful during the Lessons Learned stage.

The end of the eradication guarantees the cloud operations security, and the firm can now recover from the incident and return to business.

Recovery

Recovery is the incident response last phase, and CSIRT must be sure that all the IoCs have been removed from Bynder's infrastructure. This stage of the process may vary depending on the impacted AWS services. Overall, CSIRT should go over the below steps to complete the procedure:

1. **Identify the restore point for any restore operation**: Diverse Amazon resources have diverse restore points (for instance, S3 buckets can be recovered using S3 Versioning or AWS Backup).

2. **Restore the data from the backup**: Use the selected application (S3 Versioning, AWS Backup, etc.) to recover your data. Before restoring it, CSIRT must confirm that it is clean (there is no guarantee that every detected IoC has been removed from the AWS infrastructure).

3. **Review the backup strategy**: CSIRT must check if all the compromised data can be recovered (this step will depend on the backup policies of the AWS resources).

4. ***(Alternative)*** **Decrypt your data**: If any backup is available, use an open-source decryptor to decrypt the data and, before restoring it, perform any required analysis to ensure that it is clean. CSIRT can recharge the resources by creating new instances and moving the decrypted data into them.

5. ***(Alternative)*** **New environment**: If neither backups nor decryptors are valid, consider starting a new AWS environment.

The business would have enough resources to restore data from its backups if it followed the preparation process. The team can now proceed with the Lessons Learned.

Lessons Learned

Lessons learned are critical for the organization since they can provide essential insights into the Incident Response procedure and how the incident affected the services. CSIRT documented all the actions performed to contain the impact and recover the data, reporting any information in the ticket. Lessons Learned focus on improving incident response, starting from detecting the attack. All the stakeholders should participate in the *post-mortem* activities to provide their perspectives on managing the incident.

Reviewing Questions	**IR Phases**	**Hints**
Was the IR team properly organized?	*Preparation*	Review the team formation and prepare each member for possible future incidents.
Were the employees properly trained?	*Preparation*	Create a new awareness campaign to fix the gaps.

How long after the initial compromise was the incident discovered?	*Identification*	Review Bynder's detection solutions (Amazon GuardDuty features, AWS logs, AWS Config Rules, etc.) and set up more assertive notifications.
How long did the containment take? Was it effective?	*Containment*	Review the containment and consider automation solutions.
How can you mitigate the risk of re-occurrence of the incident?	*Containment*	Review the mitigation and define how it can be improved, making the procedure faster, consistent, and reliable.
After eradication, did signs of the compromise still show up?	*Eradication*	Review the eradication and think about potential improvements (Amazon Detective, Amazon Athena, etc.).
Were the impacted AWS resources correctly restored?	*Recovery*	Review the recovery and evaluate new solutions to accelerate it (AWS Backup, etc.).
Can any step of the IR process be automated?	*All*	Review each incident response step, determining whether actions may be automated.

Table 5.2: This is an opportunity to strengthen the overall security posture, and it may consider the questions in the table.

A final technical report that would be helpful in case of future incidents and the playbook's workflow must be updated considering the outcomes of *Lessons Learned*.

5.1.2 Ransom Response for AWS S3 - Security Runbook

Runbook Name	Ransomware Response for AWS S3 (Simple Storage Service)
Runbook Description	Incident Response Runbook for Ransom attacks targeting Amazon S3 Buckets
Runbook Manager	Information Security Senior Director
Informed	Information Security, IT, DevOps, Legal Department
Impacted Assets	Amazon S3 buckets and objects
Version	1.0
Version Date	1 May 2023

Table 5.3: The table illustrates the general information about the runbook.

Overview

This Runbook is a step-by-step procedure to respond to a ransom attack involving Amazon S3 buckets. *Amazon S3* is a storage service offering security and data availability. Organizations store their contents in S3 buckets that must be protected from unauthorized access.

Ransomware can target Amazon S3 buckets' data, stealing and possibly modifying/deleting it. Threat actors may exploit a wide range of vulnerabilities to gain unauthorized access to the target's system, taking advantage of unpatched software flaws, weak credential misuse, or social engineering. This record delivers the essential guidelines for responding to a ransomware event in Amazon S3.

Preparation

The preparation steps must be completed before an incident.

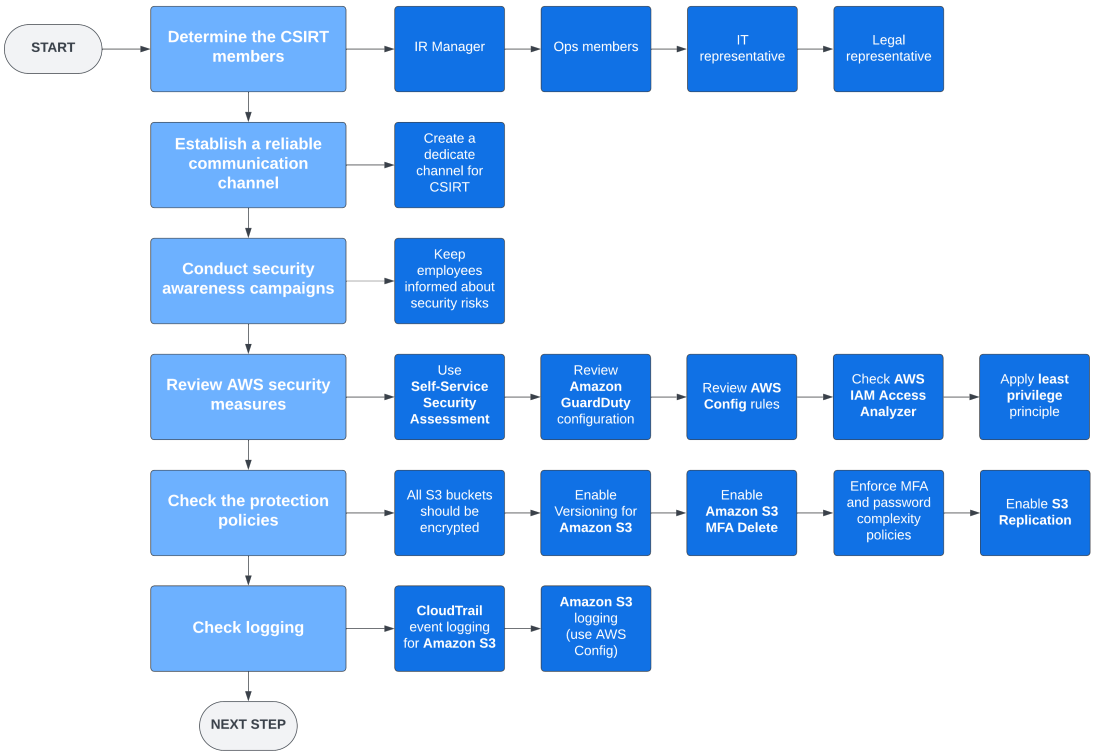

Figure 5.1: The flowchart illustrates how to approach the preparation for ransom attacks involving Amazon S3 buckets.

1. **Determine the CSIRT members**

   - The incident response manager will monitor the whole process, supervising the team and assigning tasks to each member.
   - The operative members will receive indications from the manager to contain, investigate, and recover the incident. They will examine the potential attack vectors and look for IoCs.
   - The IT representative will be central in dealing with internal user requests when needed. The participation of IT keeps their department informed about the progress.

- The legal representative will address any concerns related to sensitive data or external organizations.

2. **Establish a reliable communication channel**

   - A dedicated communication channel for CSIRT must be used for sharing progress, reporting encountered issues or planning meetings. It must be immediately created.

3. **Conduct security awareness campaigns**

   - Bynder must periodically inform employees about authentication policies (password complexity, MFA, etc.) and security best practices. Presenting phishing attempts and the best ways to protect the account reduces the likelihood of incidents.

     Developers must be trained with crafted campaigns on Amazon S3 security.

4. **Review AWS security measures**

   - Evaluate using *AWS Self-Service Security Assessment*'s Ransomware module that generates security assessment reports indicating the susceptibility to ransomware damage.
   - Control if *Amazon GuardDuty* is properly running: the S3 features must be activated to protect data stored in S3 buckets.
   - Apply these *AWS Config rules* to monitor the configuration changes affecting Amazon S3 services.
   - *AWS IAM Access Analyzer* must monitor access to Bynder's resources and data. Ensure unintended read or write actions are notified and permissions are correctly applied (**s3:*** is not permitted).

5. **Check the protection policies**

   - All S3 objects must have been encrypted using *AWS KMS* (Key Management Service) for generating encryption keys (*s3-default-encryption-kms* Config rule checks if S3 Buckets are correctly encrypted).
   - *S3 Versioning* must be enabled to restore modified or deleted objects (*s3-bucket-versioning-enabled* Config rule checks if S3 Versioning is correctly enabled).
   - *Amazon S3 MFA Delete* must be enabled to double-check the activity before deleting any S3 object.
   - Passwords must follow the complexity policies, and MFA must be enforced to access AWS.
   - *Amazon S3 Buckets Replication* must be activated to maintain object copies under different ownership and store them over multiple AWS regions.

6. **Check logging**

   - *AWS CloudTrail event logging for S3 buckets and objects* informs about Amazon S3 activities. *CloudTrail Server Level Logging for S3 Buckets* also records the requests made to a bucket (by default, Amazon S3 does not collect server access logs).
   - Control if Amazon S3 logging works (use the AWS Config rule *s3-bucket-logging-enabled*).

Identification

A ransomware attack targeting AWS S3 Buckets can be performed in many different ways, and in this regard, organizations require multiple controls, such as *Amazon GuardDuty*.

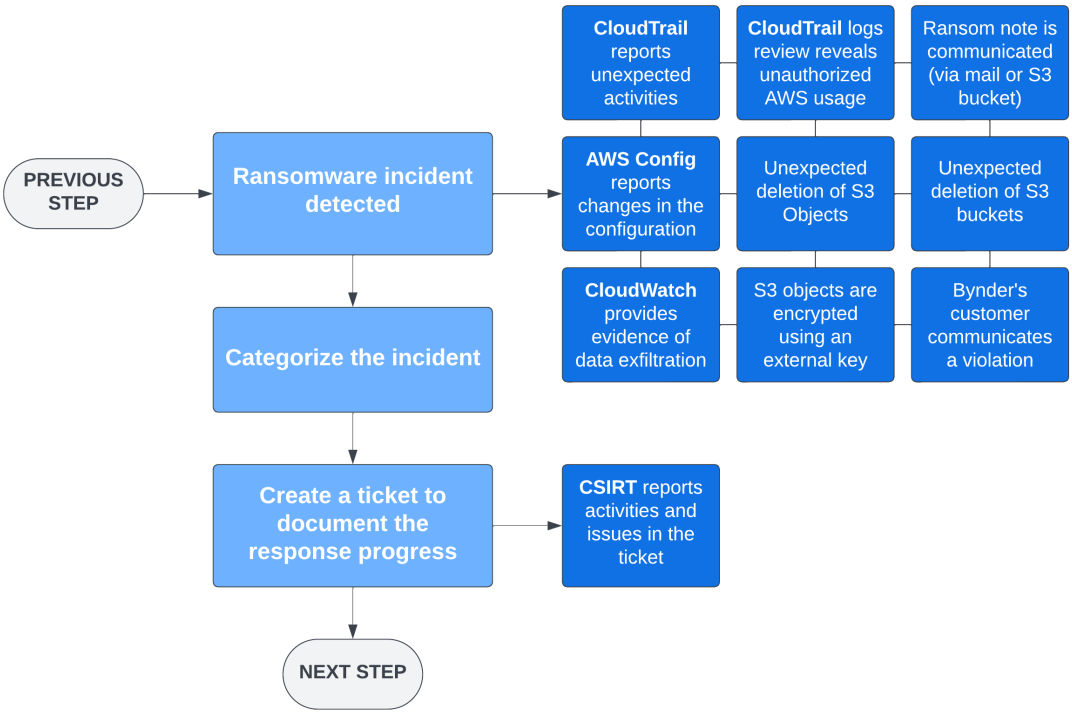

Figure 5.2: The flowchart incorporates as many valuable detection scenarios as possible. *The effectiveness of the identification phase depends on the security controls in place.*

1. **Ransomware incident detected**

   - AWS native security services (GuardDuty, CloudTrail, AWS Config, etc.) may report unauthorized activities performed within the environment.

- Compromised S3 buckets can be generally identified by one of the following:
  - ☐ Unauthorized IAM user creation;
  - ☐ Unauthorized IAM policies creation;
  - ☐ Unauthorized IAM roles creation;
  - ☐ Unauthorized IAM temporary security credentials creation;
  - ☐ Unauthorized AWS usage (EC2 instances, Lambda functions, etc.);
  - ☐ Unexpected bills from the *Billing* console;
  - ☐ Ransom note provided within the S3 bucket or via email;
  - ☐ S3 objects are deleted unexpectedly;
  - ☐ Entire S3 buckets are deleted unexpectedly;
  - ☐ Data exfiltration evidence;
  - ☐ S3 Objects are inaccessible because they are encrypted with an external key.
- Other unexpected activities can turn out to be ransom attacks and must not be underestimated.

2. **Categorize the incident**
   - The incident severity can vary depending on the assets that are impacted. Usually, ransom attacks targeting Amazon S3 buckets are classified as **Critical**.
   - Depending on the specific S3 bucket, the severity can change.
3. **Create a ticket to document the response progress**
   - CSIRT will update the ticket by documenting the response actions and the constraints that have been found. The ticket must include:
     - ☐ Incident description;

- ☐ Date and time of the identification;
- ☐ Impacted instance(s) description;
- ☐ Type of affected data (e.g., personal data);
- ☐ Root cause analysis (RCA);
- ☐ Containment and eradication summary;
- ☐ Motivation of CSIRT's activities;
- ☐ Other relevant evidence/information.

When an incident is discovered, CSIRT must start the *containment* immediately to limit the attack's impact (no investigation must be carried out for now).

Containment

Containment is a critical step to minimize the incident's impact, blocking the attackers' actions and the financial damage to the organization.

1. **Do not pay the ransom**

   - AWS recommends not paying the ransom regardless of the type of ransomware (Crypto-Ransomware, Locker-Ransomware, or others) since the business cannot know whether the criminal will honor the transaction after receiving the payment.
   - If data is encrypted and no backups are available, a representative from the financial team should help the CSIRT by performing a cost-benefit analysis to weigh the value of the data/reputational compromise against the payment to the attacker.
   - *No More Ransom Project* helps find an available decryptor for the ransomware that encrypts your data.

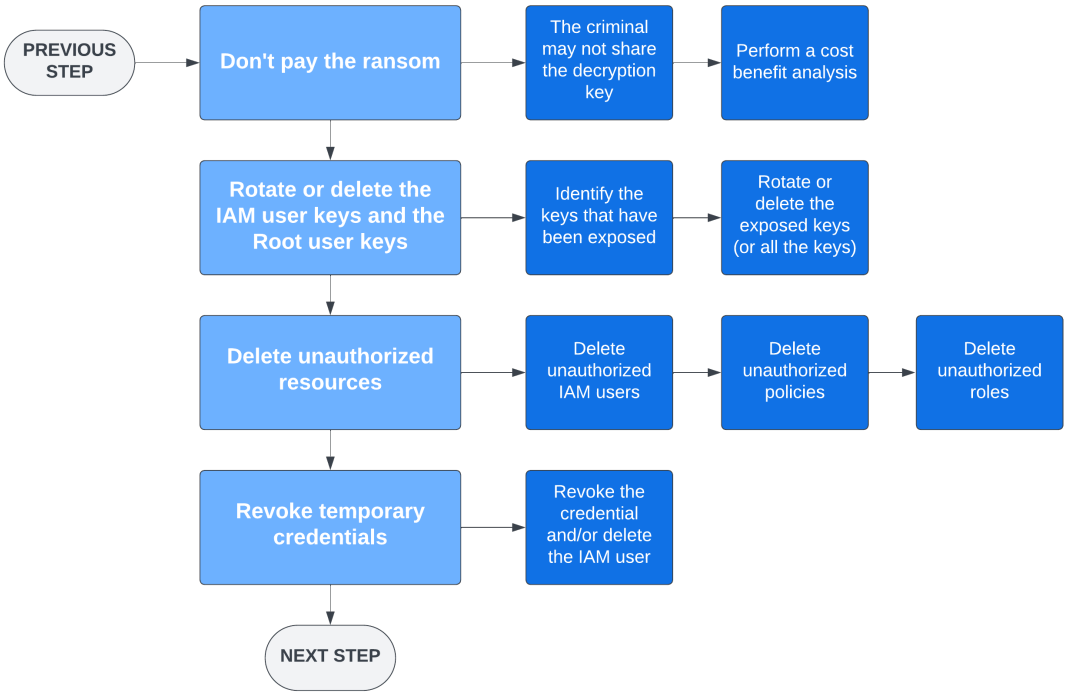

Figure 5.3: This flowchart provides multiple steps CSIRT must follow to address the incident.

2. **Rotate or delete the IAM user keys and the Root user keys**

   - The first step to contain the attack is to deal with the IAM User Keys and the Root User Keys: the CSIRT must identify which Keys have been exposed to proceed with their rotation or deletion.
   - The team can then go on with the rotation or the deletion of the IAM User Keys and the Root User Keys that have been exposed. All the Keys must be rotated or deleted whether the specific key(s) cannot be identified.

3. **Delete unauthorized resources**

   - The attacker(s) may create unauthorized resources inside the infrastructure during its period of action. The CSIRT must ensure that all these

unexpected users, policies, or roles are deleted during the containment.

- The CSIRT will continue monitoring for every unexpected change.

4. **Revoke temporary credentials**

   - Temporary security credentials cannot be revoked and remain valid until expiration. CSIRT can remove all permissions from the temporary credentials denying access to them.

     There are specific use cases that may be taken into account [50]:

     - ☐ *Denying access to the creator of the temporary security credentials*;
     - ☐ *Denying access to temporary security credentials by name*;
     - ☐ *Denying access to temporary security credentials issued before a specific time*.

   - Alternatively, the team may delete the IAM User to revoke the credentials, although doing so may impact production workloads.

Containment is a critical phase and must be conducted carefully. Once the ransom attack targeting Amazon S3 has been contained, CSIRT can proceed with eradication and recovery.

Eradication

Eradication helps determine the attack vector and investigate any possible attempt the attacker(s) made to maintain access to the resources. The investigation is the first stage of eradication, and CSIRT has to look at and mitigate every vulnerability in the AWS environment, avoiding any possible future damage. The CSIRT evaluates how the attacker(s) gained access to the infrastructure, whether they created any further unauthorized resources, and whether any other services or third-party companies were engaged in the violation.

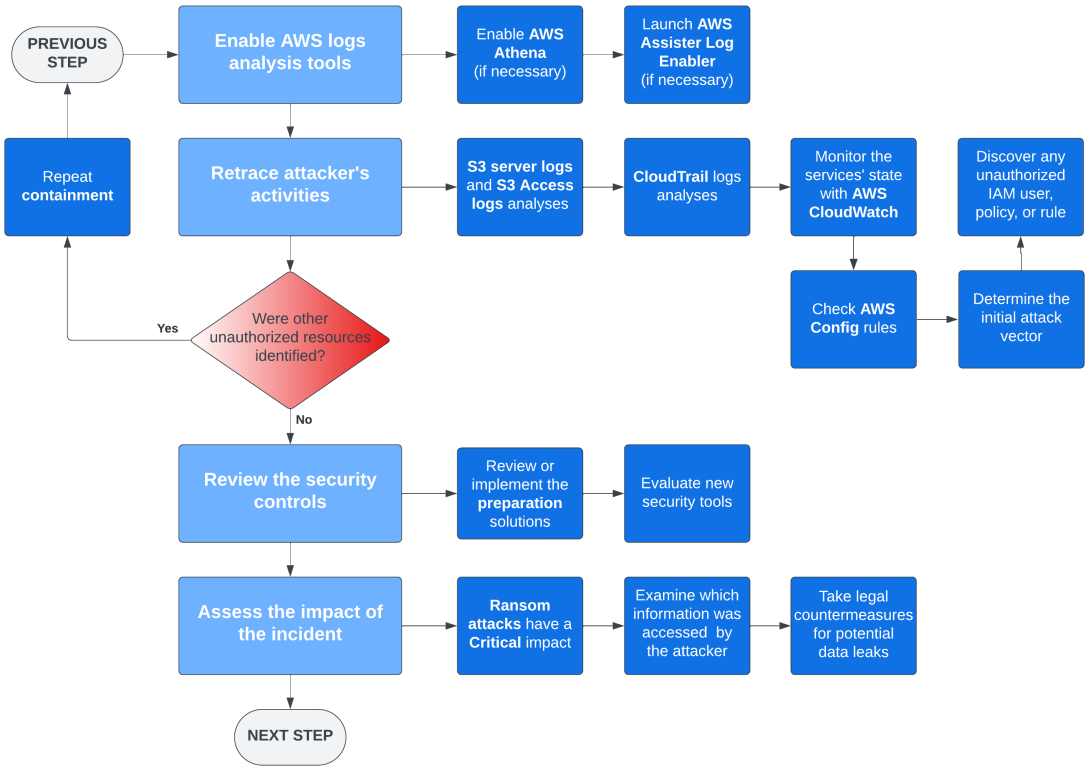

Figure 5.4: This eradication flowchart illustrates how CSIRT must conduct the investigation.

1. **Enable AWS logs analysis tools**

   - The first step of the investigation involves the logs analysis; in this regard, many AWS tools may be helpful for the CSIRT.
   - *AWS Athena* makes it easy to query the logs already stored in Amazon S3 using the IAM permissions of the analyst. It can be activated directly during the eradication (or before when necessary).
   - *AWS Assisted Log Enabler* checks whether the business is missing any logs. It facilitates the investigation of the ongoing security incident.

2. **Retrace the attacker's activities**

   - The team has to track all the attacker's activity from the initial compromise.
   - *Amazon S3 Server Logs* capture detailed information about the operations performed on the S3 buckets at the server level. Logs may provide clues such as the time of the requests, IP addresses, request types, and more.
   - *Amazon S3 Access Logs* provide information about the requests made to objects within the S3 bucket. They include the time of the requests, IP addresses, requested object's key, and more.
   - *AWS CloudTrail* dashboard and event history can provide CSIRT with IAM-related activities, and the team must search for logs from compromised IAM users or roles. CloudTrail Event Logs detect potential persistent access that a malicious actor may have created.
   - CSIRT may query CloudTrail logs (using Amazon Athena) to identify the last-used access key, user creation time, and last-used passwords. Otherwise, the team may consult the IAM Credential Report from the IAM console (updated every 4 hours).

```
1 SELECT eventtime, eventname, awsregion, sourceipaddress, useragent
2 FROM cloudtrail
3 WHERE useridentity.arn = 'arn:aws:iam::1234567890:user/Name' AND
4 (event_date >= '2023/05/27' AND event_date <= '2023/06/27')
5 ORDER BY eventtime ASC
```

Figure 5.5: The code snippet queries CloudTrail event logs, selecting an IAM user's ARN to show its activities in a specific time frame (with source IP and user agent).

- *Amazon CloudWatch* gives information on abnormal transfer spikes. CSIRT can track the activities until the initial attack vector. Alternatively, the *region-DataTransfer-Out-Bytes* metric (enabled by default) shows the amount of data transferred from S3 to the internet.
- Configuration changes trigger *AWS Config rules* and can be related to the attacker's activity.
- Once the analysis is complete, CSIRT must have discovered the attack vector, all the impacted AWS resources, and any unauthorized IAM users, policies, or roles.

3. **Repeat Containment (when necessary)**

   - *(optional)* If CSIRT discovers the attacker's persistent access through any further unauthorized IAM user, policy, or role, it must revisit containment to limit the impact on the business.

4. **Review the security controls**

   - CSIRT revisits the controls of the preparation phase (sections 4, 5, and 6). In particular, *Amazon GuardDuty*'s features and *AWS Config* rules must be enabled, and all the logs must be available (refer to *AWS Assisted Log Enabler*).
   - CSIRT may introduce new AWS native security tools or features.

5. **Assess the impact of the incident**

   - *This step can be carried out ONLY after the incident has been contained and the impact has been limited.*

     Not only confidentiality but integrity and availability may have been affected: probably, the incident may have a **critical** impact. CSIRT must

have identified all the AWS S3 that have been impacted, and it is responsible for determining whether Bynder or customers' information has been leaked.

- If either customers' information or personal data are involved in the incident, the legal representative of the CSIRT is in charge of analyzing the impact, evaluating the investigation outcomes, and eventually informing the interested corporations. The assessment should be documented by reporting the following:
  - ☐ Which measures against unauthorized processing of personal data were in place, and how these protections were likely compromised;
  - ☐ Potential consequences for data subjects;
  - ☐ Regulatory and contractual obligations regarding notifying authorities, data subjects, and other third parties;
  - ☐ Other applicable regulatory and contractual obligations.

Once eradication is concluded, the attack vector and all the impacted resources should have been detected, and the CSIRT can move on to the Recovery phase.

Recovery

Recovery is the last incident response step, and CSIRT must be sure that all the IoCs have been removed from Bynder's infrastructure.

1. **Address any weaknesses found during the investigation**

   - CSIRT should be able to address any weakness of the cloud environment.
   - CSIRT can propose additional measures for protection, such as *S3 Buckets Replication*, *AWS Detective*, or external solutions (e.g., *SIEM*).

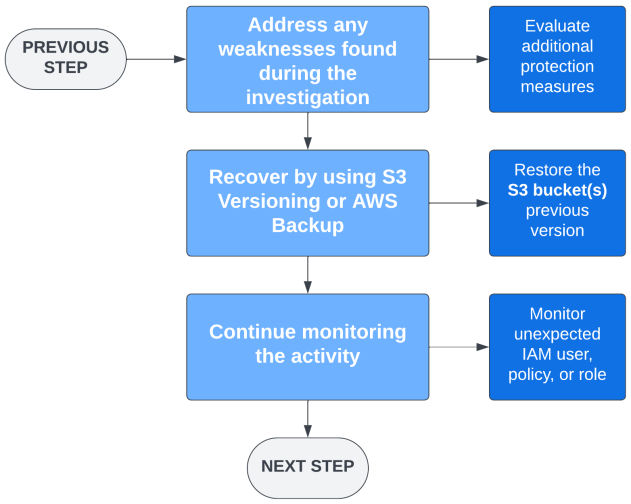

Figure 5.6: CSIRT relies on the recovery flowchart to restore the affected Amazon S3 bucket(s).

2. **Recover by using S3 Versioning or AWS Backup**

   - Use *S3 Versioning* to restore the previous version of the objects that have been compromised during the attack. Versioning is keeping multiple versions of an object in the same bucket and gives the ability to restore a particular version during the recovery. The team should select the previous version of the affected bucket(s) and return to business.
   - If S3 Versioning cannot be used, rely on *AWS Backup* and recover the modified/deleted data from the AWS backup account (the architecture is divided into service(s) account(s) and backup account).

3. **Continue monitoring the activity**

   - Once the recovery is complete, CSIRT must continue monitoring the situation by checking for alerts from AWS security tools. Discovering unexpected IAM users, policies, or roles is still possible, and the team should be ready to respond promptly.

The incident response process is ended, and CSIRT can start the *post-mortem*, wrapping up outcomes and constraints.

Lessons Learned

Lessons Learned go over the entire incident response process again, documenting the main constraints and what can be improved. This stage can provide concrete insights to understand better how the architecture was breached and where the business was vulnerable. Lessons Learned may focus on where visibility was lacking and how automation can improve the response procedure. This is an opportunity to strengthen the security posture, addressing S3 and the AWS infrastructure. The technical incident response members must plan a meeting with all the stakeholders and reply to the questions in the playbook's *Lessons Learned* section.

5.1.3 Ransom Response for AWS RDS - Security Runbook

Runbook Name	Ransomware Response for AWS RDS (Relational Database Service)
Runbook Description	Incident Response Runbook for Ransom attacks targeting Amazon RDS
Runbook Manager	Information Security Senior Director
Informed	Information Security, IT, DevOps, Legal Department
Impacted Assets	Amazon RDS databases
Version	1.0
Version Date	20 May 2023

Table 5.4: The table illustrates the general information about the runbook.

Overview

This Runbook is a step-by-step procedure to respond to a ransom attack targeting Amazon RDS services. *Amazon RDS* (Relational Database Service) is a collection of services to set up, operate, and scale databases in the cloud. It has several properties to guarantee data security, such as at-rest and in-transit encryption, access control, network isolation, firewall, and others.

However, ransomware can target cloud databases by gaining access to systems, encrypting data, and denying legitimate users' requests. RDS is required to be protected from stealing and deletion. Threat actors can exploit a wide range of tactics to gain unauthorized access to the target's system: taking advantage of unpatched software flaws, weak credential misuse, or social engineering.

This document provides essential steps for responding to a ransomware attack in Amazon RDS. Some stages of this runbook are similar to the ones of ransom attacks targeting Amazon S3 instructions. Therefore, those will not be covered again. Nevertheless, the actual procedure is completed with all descriptions to avoid misunderstanding between team members.

Preparation

The preparation steps must be completed before an incident.

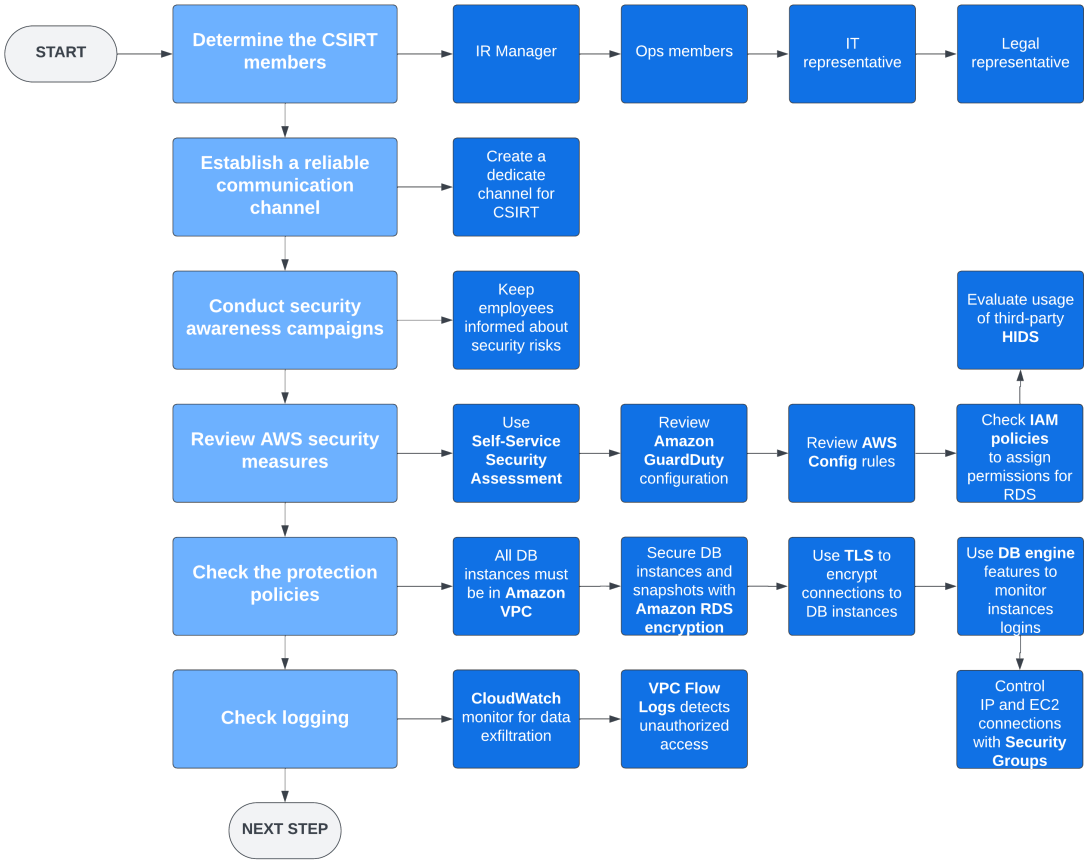

Figure 5.7: The flowchart illustrates how to approach the preparation for ransom attacks involving Amazon RDS.

1. **Determine the CSIRT members**

2. **Establish a reliable communication channel**

3. **Conduct security awareness campaigns**

4. **Review AWS security measures**

   - The *AWS Self-Service Security Assessment*'s Ransomware module focuses on weaknesses that can lead to this violation, while the *Amazon GuardDuty* RDS feature analyzes database access.
   - Apply *AWS Config rules for RDS* that assess the configuration of Relational Database Services.
   - Review *AWS IAM* policies to determine who can read, modify, and delete database instances.
   - Evaluate deploying a third-party host-based intrusion detection system (**HIDS**) for database violation detection.

5. **Check the protection policies**

   - The database instances must run in an *AWS Virtual Private Cloud*, enabling control over the virtual networking environment. VPC restricts IP address range, creates subnets, and configures routing and ACLs.
   - Control *Amazon RDS encryption* that secures data at rest, including backups, replicas, and snapshots. Industry-standard AES-256 algorithm encrypts data of the DB instances stored on the servers.
   - *TLS* (Transport Layer Security) must encrypt the databases (MySQL and PostgreSQL) communications.
   - Use database security features to prevent unauthorized access to the DB instances. Control and Monitor who can log in to the databases.

- Use and periodically review *Security Groups* to control the IP addresses and EC2 instances that can connect to the databases on a DB instance.
- Check that *AWS Backup* technology is appropriately configured to include all the RDS instances.

6. **Check logging**

   - Verify *AWS CloudWatch* logs collection. Its metrics monitor threat actor(s) activity, discovering data exfiltration.
   - *VPC Flow Logs* must be activated to identify unauthorized access to DB instances from external IP addresses.
   - Verify *Amazon RDS* logging (turn on the AWS Config rule *rds-logging-enabled*).

Identification

Bad actors may violate Amazon RDS in multiple ways, and identification technologies must be deployed. *The effectiveness of the identification phase depends on the security controls in place (their operation must be reviewed occasionally).*

1. **Ransomware incident detected**

   - The following anomalies may generally identify AWS RDS ransom attacks:
     - ☐ Suspicious behavior reported by *AWS GuardDuty*, such as data exfiltration attempts;
     - ☐ EC2 instances reveal unexpected logins, installation of unknown software, or the presence of unrecognized files;
     - ☐ *AWS Config* rules report suspicious changes to the configuration of the resources;

- ☐ Use *AWS CloudWatch* metrics to search for exfiltration spikes (open the AWS console >select *"All Metrics"* >click on *"NetworkPacketsOut"*);
- ☐ *VPCFlowLogs* may notify unknown external IP addresses accessing databases;
- ☐ A bad actor destroys data and leaves a ransom note;
- ☐ A Bynder's customer communicates evidence of a violation.

- Other unexpected activities can turn out to be Ransom attacks and must not be underestimated.

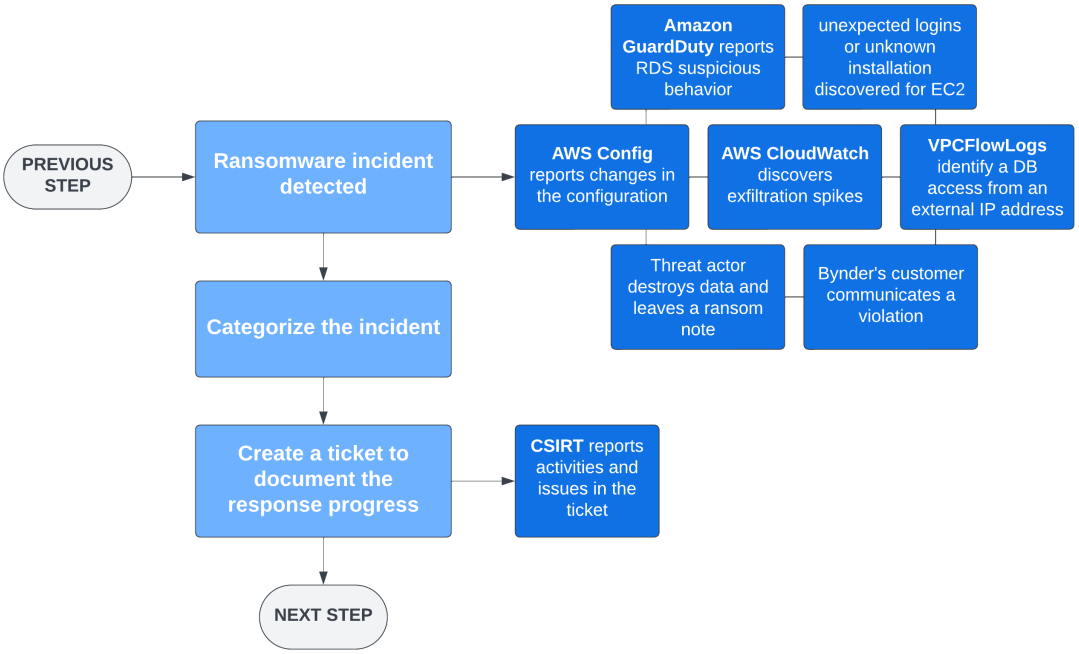

Figure 5.8: The flowchart tries to include as many different detection scenarios as possible for Amazon RDS.

2. **Categorize the incident**

3. **Create a ticket to document the response progress**

Containment

Containment is a critical step to minimize the incident's impact, blocking the attackers' actions and the financial damage to the organization.

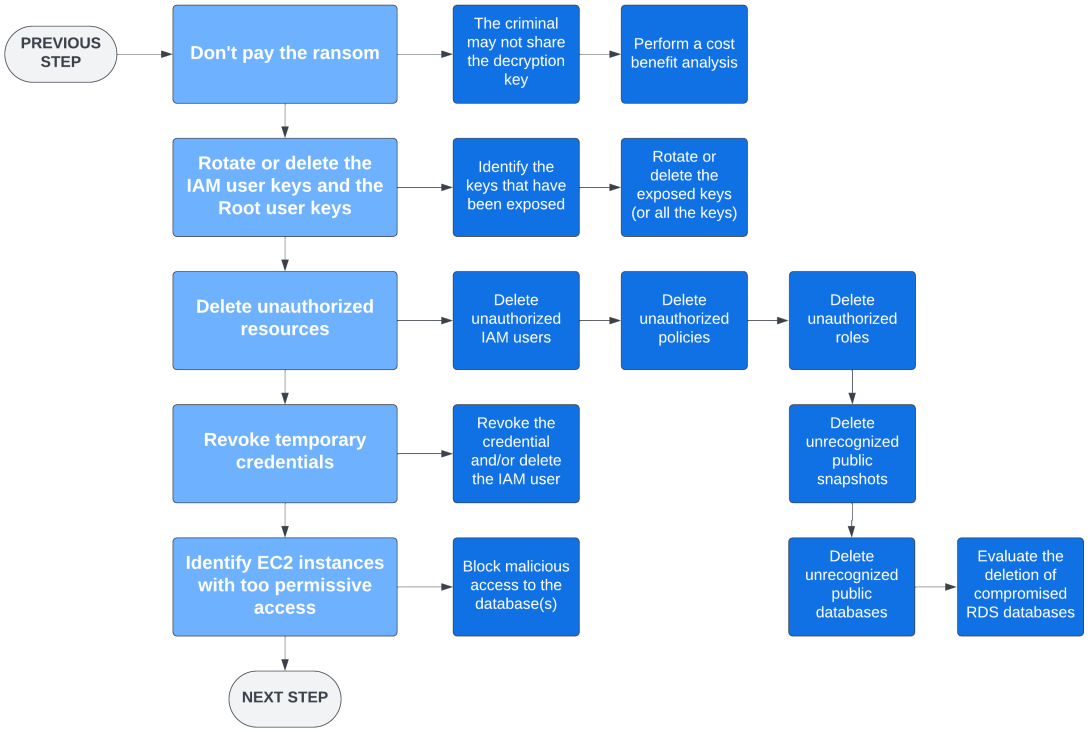

Figure 5.9: CSIRT must follow this chart to limit the incident's damage.

1. **Do not pay the ransom**
2. **Rotate or delete the IAM User Keys and the Root User keys**
3. **Delete unauthorized resources**
    - The CSIRT must ensure that all the unexpected resources created by the attacker(s) are deleted. Besides unauthorized users, policies, and roles, the team must search for any public snapshot or database.
    - Compromised RDS databases must be deleted to limit attacker(s) capability. Be sure that the backup solutions are correctly working before removing the data.

4. **Revoke temporary credentials**

5. **Identify EC2 instances with too permissive access**

    - Bad actor(s) may exploit EC2 permissive access to the database(s) to exfiltrate information. CSIRT must identify any EC2 instances that had permissive access and block them, limiting any further malicious activity.

Once the RDS service has been isolated, CSIRT can proceed with eradication and recovery.

Eradication

Eradication helps discover all the IoCs that allow the attacker(s) to maintain access to the RDS services. CSIRT must investigate how the threat actor(s) obtained permissions to read, modify, or delete RDS databases. Every additional unauthorized resource or service must be removed, and the legal department must inform every external organization involved in the security breach.

1. **Enable AWS logs analysis tools**

    - CSIRT improves investigation abilities by activating *AWS Detective*. Since most of the actions related to RDS services are visible through *Amazon VPCFlowLogs*, Detective can show visual summaries about the network flows without impacting the existing flow log collection. This technology is critical to trace the root cause instantly.
    - *AWS Assisted Log Enabler* enables all the missing logs. CSIRT needs as much information as possible about the ongoing security incident.

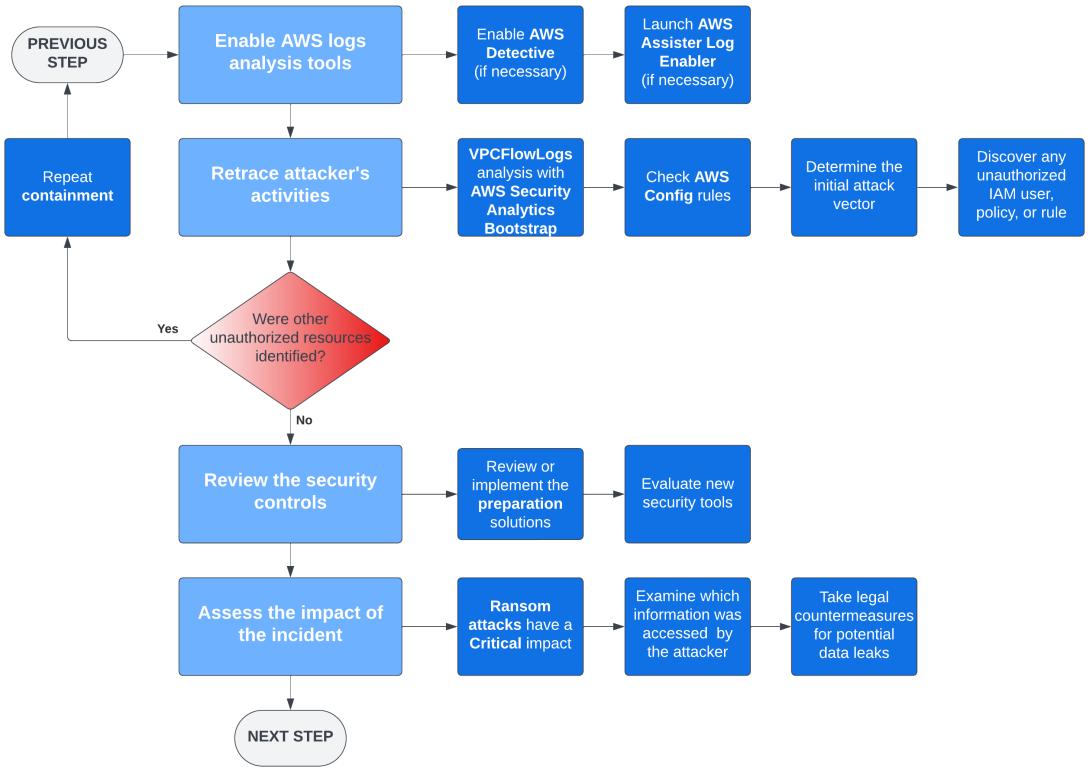

Figure 5.10: Eradication is more complicated than the previous stages, and the incident response manager must assign tasks to make it faster and more effective.

2. **Retrace the attacker's activities**

   - With new tools available for the investigation, CSIRT must start studying threat actor(s) behavior and how RDS databases were infected. *Amazon Detective* elaborates data to present observed behaviors and guidance for interpretation. The **overall VPC flow volume** panel illustrates inbound or outbound traffic spikes that may be revealed as malicious communications.

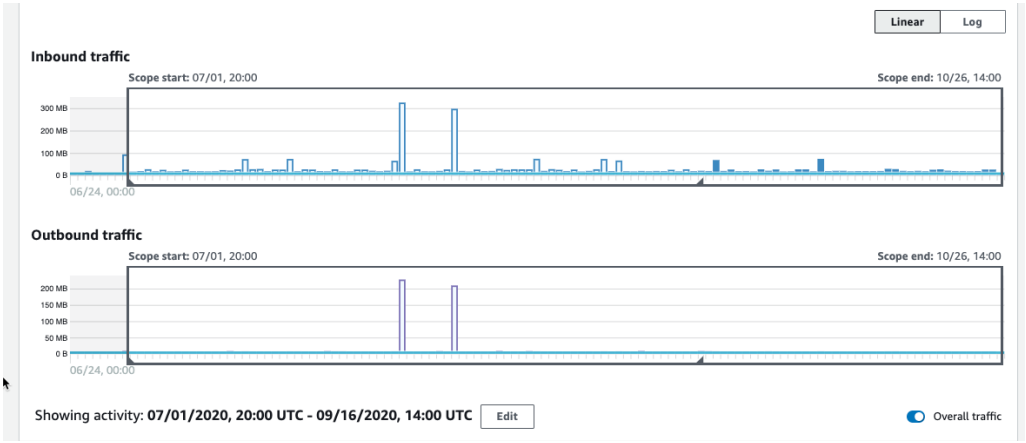

Figure 5.11: Selecting specific ranges, CSIRT can figure out which IP addresses exchange information, the data transmission ports were used, and which communications were granted or rejected [49].

- *Amazon Athena* can ease the investigation of CSIRT through the environment set up by *AWS Amazon Analytics Bootstrap*, which aggregates the service logs of AWS CloudTrail, Amazon VPC FlowLogs, and Amazon Route 53 DNS resolver query logs. *AWS CloudTrail* assesses persistent access thanks to the records of IAM users or roles. Even with *Amazon Athena*, CSIRT can get a summary of the number of bytes sent or received by an IP address.

```
SELECT sourceaddress, destinationaddress, sourceport, destinationport, sum(numbytes) as byte_count FROM vpcflow
WHERE (sourceaddress = '192.0.2.1' OR destinationaddress = '192.0.2.1')
AND destinationport = 443
AND date_partition >= '2023/08/20'
AND date_partition <= '2020/08/28'
AND account_partition = '111122223333'
AND region_partition in ('us-east-1','us-east-2','us-west-2', 'us-west-2')
GROUP BY sourceaddress, destinationaddress, sourceport, destinationport
ORDER BY byte_count DESC
```

Figure 5.12: The query returns the bytes exchanged by the IP *192.0.2.1* between the 20th and the 28th of August via port **443**. Other interesting queries can be found on the *GitHub page of Amazon Security Analytics Bootstrap*.

- *AWS Config* must work non-stop to observe configuration changes across RDS resources.
- This step ends when the incident response team realizes the initial attack vector and pinpoints all the affected resources.

3. **Repeat Containment (when necessary)**

   - *(optional)* If the infrastructure turns out to be still affected by the ransomware, CSIRT must replicate the containment phase, limiting further damage.

4. **Review the security controls**

   - CSIRT reviews and evaluates using new native features for detection, containment, and investigation (Amazon GuardDuty RDS features, AWS Config rules, etc.) or third-party solutions.

5. **Assess the impact of the incident**

   - *This step can be carried out ONLY after the incident has been contained and the impact is limited.* The overall severity is **critical**, considering that *Amazon RDS* is a vital service for the business.
   - If either Bynder or customers' information has been leaked, the legal member of the team is responsible for contacting the interested entities. The assessment should report:
     - ☐ Which measures against unauthorized processing of personal data were in place, and how these protections were likely compromised;
     - ☐ Potential consequences for data subjects;
     - ☐ Regulatory and contractual obligations regarding notifying authorities, data subjects, and other third parties;
     - ☐ Other applicable regulatory and contractual obligations.

Eradication must have isolated the RDS instances, snapshots, and backups from any risks, and CSIRT can start restoring the data.

Recovery

The last phase of the procedure aims to reinstate data into RDS databases, qualifying the return to business.

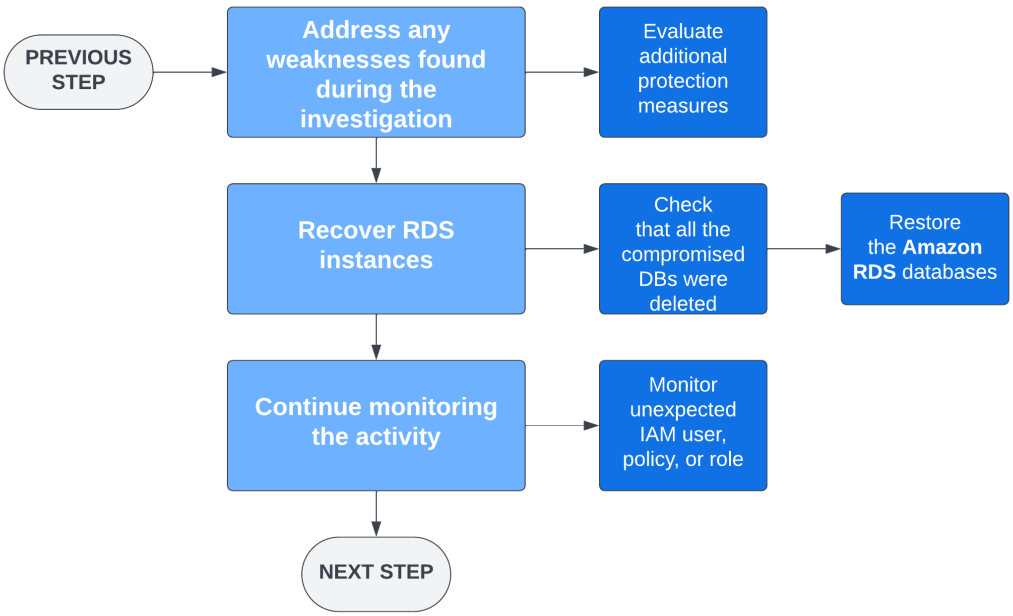

Figure 5.13: Besides addressing the cloud weaknesses, CSIRT must recover the RDS instances following the flowchart.

1. **Address any weaknesses found during the investigation**

   - CSIRT must fix the vulnerabilities of the preparation, identification, and containment before restoring the information. The attacker(s) may infect the system again. The technical members can activate new AWS native security tools or rely on third-party applications or devices.

2. **Recover RDS instances**

   - If *AWS Backup* or the custom backup solution includes all the breached instances, the CSIRT can remove all the compromised or unauthorized databases or snapshots. This step ensures that the attacker(s) will not have access to the system in the future.
   - The DevOps team members can create new Amazon RDS instances and transfer all the data using the chosen backup technology.

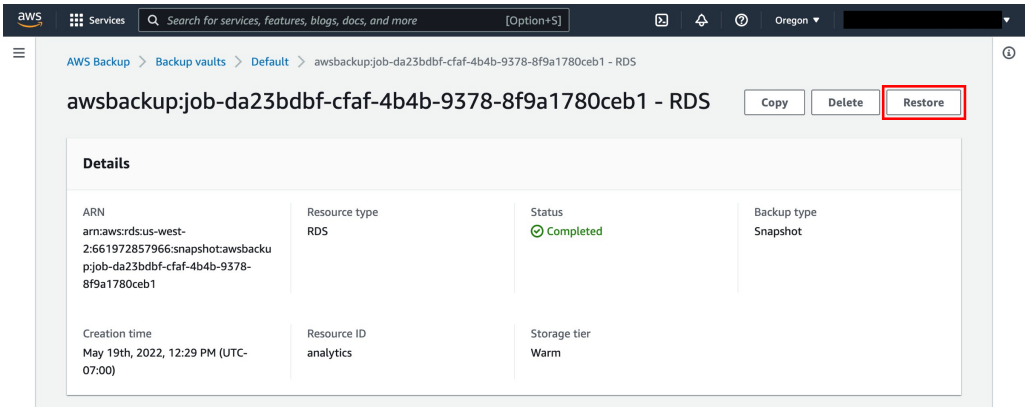

Figure 5.14: Navigating to the backup section of Amazon RDS on the AWS management console, CSIRT can select *Restore*, initiating the recovery of the instances [51].

3. **Continue monitoring the activity**

   - Restoring the Amazon RDS instances does not mean the risk of new attacks is mitigated. CSIRT must continue monitoring the situation through *GuardDury* and other security tools. The team must always be ready for a rapid response.

After restoring the production environment, CSIRT can advance to the *post-mortem* activities, focusing on final reporting and discussion with executives.

Lessons Learned

The incident response *post-mortem* tasks for ransom attacks targeting Amazon RDS are parallel to the ones of Amazon S3. CSIRT must have recorded all the activities in a ticket or a document that must be shared with Bynder's top-level executives. Together with them, the incident response manager and some operative members must exchange opinions about how they dealt with the incident, referring to the review questions of the *"Ransomware in AWS"* playbook. This opportunity can improve the procedure's effectiveness and strengthen the overall security posture.

After implementing the Ransomware in AWS security runbooks, testing their application is imperative. AWS offers an excellent simulation solution: *AWS Cloud-Saga*. Testing concludes the incident response plan for a complete action.

6 Incident Response Testing

The ability to effectively respond to incidents is essential to minimize the damages. However, organizations can deploy thousands of playbooks and runbooks with detailed instructions for the technical incident response team, but they would only know if they are adequately working once the business is attacked by ransomware or similar malware. At that moment, the company would discover whether the incident response manager can adeptly guide the department through the various stages of the procedures. This approach is hazardous and not adequate for the security standards that have been examined in this thesis.

For this reason, the business needs a pivotal practice for preparing to navigate multiple cyber threats before the breach happens: *incident response testing*. This chapter explores the importance of incident response simulations, particularly within AWS, which proposes a service designed to test CSIRT preparation.

6.1 The Role of Simulation in Incident Response

Incident response is an intricate practice that combines human expertise, security tools, and rapid decision-making. *Giddeon N. Angafor*, *Iryna Yevseyeva*, and *Ying He*'s study confirmed that tabletop exercises can be crucial in CSIR training because they encourage collaboration and communication, which are essential within such a team. Cyber incident simulations are usually made up of executives and interactive

exercises to test staff with diverse backgrounds and skills to collaborate and share information [52]. Therefore, simulating data breaches, network compromise, and other attacks is necessary to anticipate the unpredictable. Responders can train to deal with real-world scenarios, familiarizing themselves with the process and understanding the significance of the communication. Moreover, since the team works in a high-pressure situation, each individual can learn how to manage the stress while remaining focused on the tasks. Last but not least, the incident response plan may appear complete and functional, but on the other hand, testing helps identify weaknesses and gaps in the procedure.

Defining a simulation plan and practicing under controlled conditions is imperative for learning how to work together effectively and ensuring a unified response in a crisis. Amazon recognized that testing is as necessary as the other incident response steps and created **AWS CloudSaga**, a tool for simulating attack use cases in safe cloud environments [53].

6.2 Incident Response Simulation with AWS CloudSaga

AWS CloudSaga is a powerful technology that allows orchestrating and executing incident response simulations within the AWS domain. The first rule for testing is to avoid the production environment since we may provoke delays or malfunctions to the company's services or, in the most unfortunate cases, compromise the availability of the resources. Indeed, AWS sets up a protected environment for CloudSaga, permitting it to work freely and without worries about production. Amazon CloudSaga can validate the response strategies, determine areas of refinement, and reinforce playbooks and runbooks.

Users may explore its main features after entering a straightforward command to install it on the AWS management console.

Figure 6.1: AWS CloudSaga includes several use case scenarios, such as *Bitcoin mining*, *compromised IAM credentials*, and *exposed resources*. They can be customized to meet specific AWS configurations and architectures.

AWS CloudSaga use cases simulate prominent attack vectors that can lead to a ransomware violation. For instance, *"network changes"* create a customized AWS VPC and modify the *Security Groups*. Thus, this exposure may be exploited by a potential attacker, infecting the system with ransomware (Security Groups' misconfiguration accepts connections from known malicious IP addresses). However, the most valuable scenario considering the runbooks deployed in this thesis is, without any doubt, *"public resources"*. CloudSaga creates public S3 buckets and RDS databases within the AWS account, and their data may be modified or deleted before leaving a ransom note.

The security team must monitor AWS security tools to spot the simulated issues and kick off the incident response protocol. CSIRT can now follow the runbooks, developing the team coordination and modeling the joint decision-making actions. At the end of the simulation, Amazon CloudSaga deletes all the unexpected resources and generates detailed reports to highlight strengths, weaknesses, and areas of improvement, depending on how the group reacted.

In conclusion, the significance of incident response simulations in AWS becomes clear. By proactively preparing for the worst, organizations can achieve the best outcomes, continuously adapting to a dynamic cloud ecosystem. Regrettably, as previously mentioned, I did not have time to try out AWS CloudSaga within Bynder, even though it would have been a perfect occasion to point out the strengths and flaws of the incident response plans. Nonetheless, every now and then, InfoSec and DevOps departments schedule meetings to test the performance of the manuals, and they will use this powerful resource.

7 Conclusion

7.1 Evaluation and Results

The journey undertaken in this thesis culminated in creating accurate incident response playbooks and runbooks for Amazon Web Services ransomware scenarios, focusing on *Amazon S3* and *Amazon RDS*. These blow-by-blow guides offer a roadmap that not only Bynder but other organizations can follow when facing the challenge of a ransomware incident. They may readjust these complex playbooks and runbooks, considering their cloud architecture.

An AWS Customer Support Specialist was involved in the process, providing valuable insights and validating the efficacy of the developed playbooks and runbooks. He suggested maintaining documentation to register each step during the preparation phase, guaranteeing a more robust and transparent incident response process. Additionally, the AWS support team must be involved in the strategy since their *Technical Account Manager* (TAM) has more experience dealing with cloud threats and can help the incident response manager administrate the activities. TAM's contact must be included in the runbooks to communicate the violation immediately.

In conclusion, the objective was to bolster the security posture of Bynder with this comprehensive solution covering preparation, detection, containment, eradication,

recovery, and lessons learned, ensuring a holistic approach to incident response. The result was accomplished because this study provided tailored incident response documentation to enhance the security landscape of the AWS domain. *Amazon S3* and *RDS* are critical services for all the companies based on AWS as a cloud provider. Completing playbooks and runbooks for the ransomware use case equips them with a structured approach to counteract threats effectively and with faster decision-making.

7.2 Final Remarks

As we conclude, it is essential to recognize the impact of this thesis on the companies relying on AWS cloud infrastructure. Businesses with a general document describing their incident response approach without practical advice on carrying out the procedure would be in trouble while facing ransomware targeting the AWS resources. Lack of communication, poor automation, and no decision-making experience during high-pressure situations would have a critical impact on the business. The initial problem of ransomware targeting AWS cloud services has been met with a resolute response, a suite of procedures guided by Amazon Web Services, NIST, and SANS best practices. Overall, the infrastructure vulnerable to many evolving cloud threats has been transformed into a fortress with a step-by-step, well-structured incident response plan.

7.3 Future Trends

The cloud and cyber threat landscape is constantly changing. This study will not always be able to face new threat actors targeting Amazon Web Service resources. Hence, the *future trends* section suggests how evolving menaces may be handled, protecting confidentiality, integrity, and availability stored in the cloud.

Extending Playbooks and Runbooks

During the project, I developed a blueprint that can be used for both ransomware scenarios targeting other AWS resources or even other threats that can impact virtual or tangible assets. The template includes all the incident response stages with a brief description highlighting its requirements. It can be seen as a framework for evaluating and creating incident response plans for various security breaches, strengthening the business across multiple fronts.

Integrating into Threat Modeling

As suggested by *AWS Playbook Framework*, the evolution of the incident response need not conclude with creating playbooks and runbooks [54]. Integrating these resources into the *threat modeling* process may offer a proactive approach. Threat modeling identifies and assesses potential security risks in systems, applications, and operations. Integrating it with security playbooks and runbooks means not only detecting weaknesses but also planning how to respond to potential incidents that could arise due to those vulnerabilities. This approach ensures an efficient incident response since playbooks and runbooks are directly aligned with the specific threats explored. Furthermore, teams are more coordinated and trained to understand the situation and act quickly to solve the issue. The integration benefits the minimized impact because security events can be immediately discovered and mitigated, reducing downtime, data loss, and reputational damage.

Combining Cyber Threat Intelligence and Incident Response

As presented by the research article "*Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure*", Cyber Threat Intelligence (CTI) collects information about threat actors, such as attack vectors, victims, and courses of action, and can dramatically upgrade the incident response procedure [55]. Indeed, CTI can receive real-time information about menaces and directly trigger the incident response tools, which can detect anomalies promptly and execute automated actions when necessary. The authors focused on healthcare organizations but also punctuated the possibility of integrating their *CTI-IR* process with other security products or operations, such as SIEM, SOAR, or SOC. Once the strategy has been established and the team is well-equipped to handle emergencies, enterprises can update their playbooks and runbooks to include CTI technologies.

In closing, this thesis illustrated the collaborative efforts required to safeguard digital assets in an evolving environment targeted by more and more cyber threats. By innovating the incident response protocols, adapting them to the dynamic cloud environment, and providing the business with strengthened resources, we are contributing to a more secure digital future.

References

[1] V. Sumina, *26 Cloud Computing Statistics, Facts & Trends for 2023*, en, Jul. 2021. [Online]. Available: https://www.cloudwards.net/cloud-computing-statistics/.

[2] OCloud Solutions, *Impacts of Cloud Computing on Businesses | LinkedIn*, May 2022. [Online]. Available: https://www.linkedin.com/pulse/impacts-cloud-computing-businesses-ocloud-solutions/.

[3] Amazon Web Services, *Shared Responsibility Model - Amazon Web Services (AWS)*, en-US, 2023.

[4] "2023 Cloud Security Report", en, Checkpoint, Tech. Rep., Feb. 2023.

[5] A. Today, *Impact of Ransomware Attacks on Businesses and Individuals*, en, Feb. 2023. [Online]. Available: https://infosecwriteups.com/impact-of-ransomware-attacks-on-businesses-and-individuals-cc6b35620887.

[6] N. James, *10 of the Biggest Ransomware Attacks in History*, en-US, Section: Security Audit, Feb. 2023. [Online]. Available: https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/.

[7] "Zscaler ThreatLabz 2023 Ransomware Report", en, ThreatLabz Zscaler, Tech. Rep., 2023.

[8] N. H. Ab Rahman, N. D. W. Cahyani, and K.-K. R. Choo, "Cloud incident handling and forensic-by-design: Cloud storage as a case study", eng, *Concur-*

rency and computation, vol. 29, no. 14, 2017, Place: Hoboken Publisher: Wiley Subscription Services, Inc, ISSN: 1532-0626.

[9] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology", en, National Institute of Standards and Technology, Tech. Rep. NIST SP 800-61r2, Aug. 2012, NIST SP 800–61r2. DOI: 10.6028/NIST.SP.800-61r2. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[10] A. T. Tunggal, *What is an Incident Response Plan?*, en, Apr. 2023. [Online]. Available: https://www.upguard.com/blog/incident-response-plan.

[11] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1", en, National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST CSWP 041620 18, Apr. 2018. DOI: 10.6028/NIST.CSWP.04162018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[12] Amazon Web Services, *Bynder Case Study*, en-US, 2023. [Online]. Available: https://aws.amazon.com/solutions/case-studies/bynder/.

[13] S. Mitropoulos, D. Patsos, and C. Douligeris, "On Incident Handling and Response: A state-of-the-art approach", en, *Computers & Security*, vol. 25, no. 5, pp. 351–370, Jul. 2006, ISSN: 01674048. DOI: 10.1016/j.cose.2005.09.006. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404805001574.

[14] M. Souppaya and K. Scarfone, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops", en, National Institute of Standards and Technology, Tech. Rep. NIST SP 800-83r1, Jul. 2013, NIST SP 800–83r1. DOI:

10.6028/NIST.SP.800-83r1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[15] *Art. 33 GDPR – Notification of a personal data breach to the supervisory authority*, en-US, Apr. 2016. [Online]. Available: https://gdpr-info.eu/art-33-gdpr/.

[16] P. Kral, *Incident Handler's Handbook*, en, Dec. 2011.

[17] J. Azar, *Master the Six Phases of Incident Response*, en, Webinar, Online, Mar. 2023. [Online]. Available: https://thehacker.news/incident-response-phases?source=upcoming.

[18] A. Wolter, *The Need-to-know principle*, en, Feb. 2021. [Online]. Available: https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393.

[19] K. Amoresano and B. Yankson, "Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education", *Holistica – Journal of Business and Public Administration*, vol. 14, no. 1, pp. 110–132, 2023. DOI: doi:10.2478/hjbpa-2023-0007. [Online]. Available: https://doi.org/10.2478/hjbpa-2023-0007.

[20] E. Segal, *'alert fatigue' can lead to missed cyber threats and staff retention/recruitment issues: Study*, en, Forbes, Nov. 2021.

[21] S. Gatlan, *CISA releases cybersecurity response plans for federal agencies*, en-us, Nov. 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/cisa-releases-cybersecurity-response-plans-for-federal-agencies/.

[22] J. R. Biden Jr., *Executive Order on Improving the Nation's Cybersecurity*, en-US, May 2021. [Online]. Available: https://www.whitehouse.gov/

briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[23] N. Case and P. Hawkins, *AWS re:Invent 2019: Prepare for & respond to security incidents in your AWS environment (SEC356)*, en, Dec. 2019. [Online]. Available: https://youtu.be/8uiQ0Z5meCs?t=2097&si=6tu6DC9dKsvdW69B.

[24] A. Shaked, Y. Cherdantseva, P. Burnap, and P. Maynard, "Operations-informed Incident Response Playbooks", *Computers & Security*, p. 103 454, Aug. 2023, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103454. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823003644.

[25] Amazon Web Services, *AWS Well-Architected Framework*, en, 2023. [Online]. Available: https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html.

[26] Amazon Web Services, *AWS Customer Playbook Framework*, Sep. 2023. [Online]. Available: https://github.com/aws-samples/aws-customer-playbook-framework.

[27] P. Serrador and J. K. Pinto, "Does Agile work? — A quantitative analysis of agile project success", en, *International Journal of Project Management*, vol. 33, no. 5, pp. 1040–1051, Jul. 2015, ISSN: 02637863. DOI: 10.1016/j.ijproman.2015.01.006. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0263786315000071.

[28] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments", en, National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-30r1, Sep. 2012, Edition: 0, NIST SP 800–30r1. DOI: 10.6028/NIST.SP.800-30r1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[29] V. Vicente, *The Risk Assessment Matrix: What Is It and Why Is It Important?*, en-US, May 2023. [Online]. Available: https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/.

[30] F. Richter, *Amazon Maintains Lead in the Cloud Market*, en, Aug. 2023. [Online]. Available: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers.

[31] V. Engström, P. Johnson, R. Lagerström, E. Ringdahl, and M. Wällstedt, "Automated Security Assessments of Amazon Web Services Environments", *ACM Trans. Priv. Secur.*, vol. 26, no. 2, Mar. 2023, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 2471-2566. DOI: 10.1145/3570903. [Online]. Available: https://doi.org/10.1145/3570903.

[32] S. Kepil, *The Top 8 AWS Security Risks: What You Need to Know*, en, Oct. 2022. [Online]. Available: https://medium.com/@serdalkepil/the-top-8-aws-cloud-security-risks-what-you-need-to-know-786b3144fee8.

[33] E. Chickowski, *Leaky Buckets: 10 Worst Amazon S3 Breaches*, en, Bitdefender Blog, Jan. 2018.

[34] G. Rosenthal, *Common RDS Misconfigurations That Can Damage Your Cloud Data Security Posture*, en, 2023. [Online]. Available: https://www.eureka.security/post/common-rds-misconfigurations-that-can-damage-your-cloud-data-security-posture.

[35] A. Meridian, *Incident response planning*, en-US, Dec. 2021. [Online]. Available: https://www.twitch.tv/videos/1235087932.

[36] A. S. George, A. S. H. George, T. Baskar, and D. Pandey, "XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future", en, *International Journal of*

Advanced Research in Science, Communication and Technology, pp. 493–501, Aug. 2021, ISSN: 2581-9429. DOI: 10.48175/IJARSCT-1888.

[37] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", en, *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, e4150, Sep. 2020, ISSN: 2161-3915. DOI: 10.1002/ett.4150.

[38] V. Tzvetkov, *How to perform automated incident response in a multi-account environment*, en-US, Section: Advanced (300), Jun. 2020. [Online]. Available: https://aws.amazon.com/blogs/security/how-to-perform-automated-incident-response-multi-account-environment/.

[39] Amazon Web Services, *What is AWS Security Hub?*, en, 2023. [Online]. Available: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html.

[40] M. Ramesh, *Use IAM Access Analyzer to generate IAM policies based on access activity found in your organization trail | AWS Security Blog*, en-US, Section: Amazon Simple Storage Service (S3), Aug. 2021. [Online]. Available: https://aws.amazon.com/blogs/security/use-iam-access-analyzer-to-generate-iam-policies-based-on-access-activity-found-in-your-organization-trail/.

[41] AWS Public Sector Blog Team, *Assess your security posture to identify and remediate security gaps susceptible to ransomware*, en-US, Section: Announcements, Aug. 2020. [Online]. Available: https://aws.amazon.com/blogs/publicsector/assess-your-security-posture-identify-remediate-security-gaps-ransomware/.

[42] J. Haggerty and T. Hughes-Roberts, "Visualization of System Log Files for Post-incident Analysis and Response", in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas and I. Askoxylakis, Eds., Cham: Springer International Publishing, 2014, pp. 23–32, ISBN: 978-3-319-07620-1.

[43] A. Meridian, *Log analysis with Athena Bootstrap*, en-US, Dec. 2021. [Online]. Available: https://www.twitch.tv/videos/1235087932.

[44] J. McKiddy, *Introducing Assisted Log Enabler for AWS*, en-US, Section: Amazon Simple Storage Service (S3), May 2021. [Online]. Available: https://aws.amazon.com/blogs/opensource/introducing-assisted-log-enabler-for-aws/.

[45] Amazon Web Services, "Securing your AWS Cloud environment from ransomware", en-US, Amazon Web Services, Tech. Rep., Apr. 2020. [Online]. Available: https://d1.awsstatic.com/WWPS/pdf/AWSPS_ransomware_ebook_Apr-2020.pdf.

[46] B. Dispensa, *Ransomware mitigation: Top 5 protections and recovery preparation actions*, en-US, Section: Intermediate (200), Sep. 2021. [Online]. Available: https://aws.amazon.com/blogs/security/ransomware-mitigation-top-5-protections-and-recovery-preparation-actions/.

[47] M. O'Neil, K. Dickinson, and K. Ram, *The anatomy of ransomware event targeting data residing in Amazon S3*, en-US, Section: Intermediate (200), Feb. 2023. [Online]. Available: https://aws.amazon.com/blogs/security/anatomy-of-a-ransomware-event-targeting-data-in-amazon-s3/.

[48] M. Jones and D. Martinez, *Detect threats to your data stored in RDS databases by using GuardDuty*, en-US, Section: Advanced (300), May 2023. [Online]. Available: https://aws.amazon.com/blogs/security/detect-threats-to-your-data-stored-in-rds-databases-by-using-guardduty/.

[49] R. Warren and J. Miller, *Investigate VPC flow with Amazon Detective*, en-US, Section: Advanced (300), Nov. 2020. [Online]. Available: https://aws.amazon.com/blogs/security/investigate-vpc-flow-with-amazon-detective/.

[50] Amazon Web Services, *Controlling permissions for temporary security credentials - AWS Identity and Access Management*, 2023. [Online]. Available: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access.html.

[51] Amazon Web Services, *Amazon RDS Backup & Restore using AWS Backup*, en-US, 2023. [Online]. Available: https://aws.amazon.com/getting-started/hands-on/amazon-rds-backup-restore-using-aws-backup/.

[52] G. N. Angafor, I. Yevseyeva, and Y. He, "Game-based learning: A review of tabletop exercises for cybersecurity incident response training", en, *SECURITY AND PRIVACY*, vol. 3, no. 6, e126, Jul. 2020, ISSN: 2475-6725, 2475-6725. DOI: 10.1002/spy2.126.

[53] Amazon Web Services, *AWS CloudSaga - Simulate security events in AWS*, Jul. 2022. [Online]. Available: https://github.com/awslabs/aws-cloudsaga.

[54] Amazon Web Services, *Responding to Ransom Attacks within AWS*, en, Feb. 2022. [Online]. Available: https://github.com/aws-samples/aws-customer-playbook-framework/blob/main/docs/Responding_to_Ransom_in_AWS.md.

[55] Y. He, L. Maglaras, A. Aliyu, and C. Luo, "Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure", English, *Security and Communication Networks*, vol. 2022, Feb. 2022, Place: London, United Kingdom Publisher: Hindawi Limited, ISSN: 19390114. DOI: 10.1155/2022/2775249.