TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

Kingshuk Chowdhury 194222 IVCM

CLOUD INCIDENT HANDLING: CHALLENGES AND BEST PRACTICES

Master's Thesis

Supervisor:
Lt Cdr Kieren Niĉolas Lovell RNorN RTD

Tallinn 2022

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kingshuk Chowdhury ....

(signature)

Date: January 03, 2022

Annotatsioon

Pilveandmetöötlus on Interneti põhine platvorm, mis pakub vastavalt nõudmistele ligipääsu salvestusruumile ning andemetetöötlusressurssidele. Pilveandmetöötlus platvormid on oma tulusate funktsioonide, kasutuslihtsuse, madalate kulude ning madala hooldusvajaduse tõttu saanud organisatsioonides populaarsemaks võrreldes kohalikele andmetöötlus ressursisdele. Organisatsioonid nihutavad oma resursse pilve selle funktsioonide tõttu ja selleks, et vältida kohalike andmekeskuste haldamise ja hooldamisega kaasnevat tüli. Kuid ressursside pilve nihutamisega muutus ka intsidentide käsitlemine keerukamaks. Intsidentide käsitlemine kohapealses keskkonnas on ressurssidele ligipääsu ja nähtavasue tõttu lihtsam, pilveandmetöötluse puhul on juurdepääs ja nähtavus pilvekasutajatele ebaselgem. Enamik turbe valdkonna organisatsioone ja eksperte tõid välja et intsidentide ja juhtumite käsitlemine on pilves on keerukam ning nad kahtlevad oma resursside turvalisuse üle pilves. Uuringu läbiviimist innustas leida ekspertide väljakutseid pilve platvormidel intsidentide käsitlemisel ning praeguse intsidentide käsitlemise raamistiku piisavus.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 53 leheküljel, 9 peatükki, 5 joonist, 20 tabelit.

Abstract

Cloud computing is an internet-based platform that delivers storage and access to computing resources on demand. Cloud computing has gained popularity over on-premise among organizations because of its lucrative features, ease-of-use, low cost, and low maintenance. Organizations are shifting their resources from on-premises to cloud computing due to its features and to avoid the inconveniences of maintaining data centers for on-premises resources. However, with the shifting of resources to the cloud, the complication of handling incidents also shifted to a different level. It is quite simple to handle incidents in the on-premises environment due to access and visibility to the resources, but in the case of cloud computing, access and visibility are unclear to the cloud users. Most of the organizations and experts in this field also expressed that it is complicated to handle incidents in the cloud and doubt the security of their resources in the cloud. Finding the challenges faced by experts and incident handlers in cloud incident handling, and the sufficiency of the present incident handling framework was an encouragement to conduct the research. There are several pieces of research on cloud computing regarding digital forensics investigations and a few regarding incident handling in the cloud. This research focuses on finding the best practices to handle incidents in the cloud and suggests an incident handling framework for SMEs that would provide guidelines for handling incidents in both cloud and on-premises environments. An online survey was performed to determine the experts' opinions regarding the difference between incident handling in the on-premises and cloud environments, the challenges they face in incident handling, and the sufficiency of the present incident handling framework available. Analysis of the survey results shows that most of the participating experts think cloud incident handling is different and more challenging than handling incidents in the on-premises environment. The respondents also believe that the present incident handling frameworks might not be suitable for handling cloud incidents. Based on the response, some best practices to handle cloud incidents and experts validated hybrid incident response framework was suggested that would provide the right direction to the SMEs to handle incidents in both cloud and on-premises environments.

The thesis is written in English and contains 53 pages of text, with 9 chapters, 5 figures, and 20 tables.

List of abbreviations and terms

AI	Artificial Intelligence
API	Application Programming Interface
AWS	Amazone Web Services
Amazon EC2	Amazon Elastic Compute Cloud
Amazon S3	Amazon Simple Storage Service
CLDAP	Connection-less Lightweight Directory Access Protocol
CSA	Cyber Security Alliance
CSP	Cloud Service Provider
CSU	Cloud Service User
DBSCAN	Density-based Spatial Clustering of Applications with Noise
DDoS	Distributed Denial-of-Service
GCE	Google Compute Engine
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SANS	SysAdmin, Audit, Network, and Security
SIEM	System Information and Event Management
SLA	Service-level Agreement
SME	Small and Medium Enterprises
SSO	Single Sign-On
SSRF	Server-Side Request Forgery
UDP	User Datagram Protocol
VPC	Virtual Private Cloud
WAF	Web Application Firewall

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Motivation

Cloud computing has gained prevalence over on-premises among organizations because of its advanced features like resource pooling, elasticity, on-demand self-service, and other vast ranges of options. Cloud features and resources are continuously increasing, so is the usage of the cloud. Organizations are moving their resources from on-premises infrastructure to the cloud. With the expansion of the usage of cloud resources, the complexity of handling incidents in the cloud is also rising. Incident handling in the on-premises infrastructure is a straightforward task, while handling cloud incidents requires different skills and approaches. In the cloud, data is spread over multiple cloud infrastructures [1], which makes incident handling trickier and complicated than on-premises incident handling. Due to less visibility, less accessibility to cloud resources and events [2], and lack of understanding of the cloud infrastructure and security responsibilities, organizations often face issues in handling incidents in the cloud computing environment. Several pieces of research show that cloud service users face issues either in cloud incident handling or in performing digital forensic investigations. Researches performed in the cloud computing field mostly focus on digital forensic investigations, and few focus on incident handling challenges faced by users in the cloud. As cloud computing is constantly evolving with services and resources, complexity is also continuously increasing. This research work was performed to identify the incident handling challenges CSU faces in the current cloud computing environment and suggest some best practices and a hybrid incident response framework to handle the incidents effectively.

1.2 Scope and Goal

The research aimed to identify the difference between handling incidents in the cloud and on-premises environments and the challenges cloud service users face in managing incidents. The study also focused on current incident handling frameworks and to what extent these frameworks are enough to provide guidelines to handle the incident in the cloud and on-premises. As the cloud comprises a vast range of facilities, identifying all kinds of challenges is not possible in such an amount of time. The research explored and suggested a hybrid incident response framework that can be a practical guideline for handling incidents in both on-premises and cloud environments and is beneficial for small and medium-sized enterprises (SMEs).

1.3 Research Method

The research work is done following the observational approach. A questionnaire was prepared using Google form for data collection and shared among incident response experts, security experts, DevOps/Cloud engineering professionals through social networking sites. Data is collected to determine the challenges they face while handling any incidents in the cloud environment. Are there any skillsets and approaches required for cloud incidents different from handling incidents in the on-premises environment? Finally, some recommended best practices will be presented to overcome the challenges with a suggested hybrid incident response framework that can be followed for handling incidents in both cloud and on-premises environments by SMEs. The proposed framework can be beneficial for SMEs running infrastructure in a hybrid environment to handle incidents.

The research was done by the following research questions:

Question 1: Is it different to handle incidents in the cloud than in the on-premises environment?

Question 2: What are the current challenges in terms of handling incidents in the cloud?

Question 3: Are the present incident handling frameworks useful enough to handle incidents in both cloud and on-premises environments?

Question 4: What do experts suggest regarding cloud incident handling?

Question 5: What practices should organizations follow to cloud incident handling challenges?

1.4 Novelty

Most of the studies are based on digital forensics investigation challenges in the cloud as a part of cloud incident handling. However, this study will focus and current incident handling challenges and suggest best practices to handle incidents in the cloud environment. Finally, a suggested hybrid incident response framework is proposed to provide guidelines to SMEs for handling incidents in both cloud and on-premises environments.

1.5 Validation

An online survey was performed to collect data regarding incident handling in the cloud and underlying challenges cloud users face. Based on the responses from the respondents, some best practices are suggested, and a hybrid incident response framework is created, which is validated by experts. These recommended best practices and the hybrid incident response framework would guide SMEs to handle incidents in infrastructure containing both cloud and on-premises resources.

1.6 Road Map

Chapter 2 includes the definition of cloud computing and the descriptions of characteristics and types of cloud computing models, and a discussion on security incidents and incident handling.

Chapter 3 discusses the difference between cloud and on-premises regarding incident handling, cloud shared responsibility model, cloud incident handling. There are also discussions on major cloud data breaches, some advanced incident handling tools and other related pieces of literature.

In chapter 4, the methodology and design of the research are present.

Chapter 5 includes the result from the analysis of the collected data through the research questionnaire

In chapter 6, the hybrid incident response framework created based on the responses from the participants is described in detail. This chapter also discusses the result of the analysis of collected data from the framework validation questionnaire.

In chapter 7, some best practices regarding cloud incident handling are suggested for organizations to handle incidents successfully.

Chapter 8 includes limitations of the thesis and possible future work.

Chapter 9 discuss the findings from the research and concludes the thesis.

2. Cloud Computing and Incident Handling

2.1 Cloud Computing

Cloud computing is an on-demand pay-as-you-go basis computing service with a vast range of options. NIST SP800-145 [3] provided a detailed description of cloud computing. According to NIST, SP800-145 [3], cloud computing is defined as “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [3]. According to NIST, a cloud model has five essential characteristics, three service models, and four deployment models [3].

Five essential characteristics are briefly described below:

On-demand self-service: Automatic provisioning of computing resources and capabilities as needed without human interaction with each cloud service provider.

Broad network access: Broad network access means the availability of resources and capabilities over a broad network through diverse platforms like mobile phones, tablets, desktops, and laptop computers.

Resource pooling: Location-independent multi-tenant model serves multiple cloud service users according to their demands on pooled computing resources like storage, memory, and processing capabilities. Resources and capabilities are dynamically distributed.

Rapid elasticity: Rapid and elastic provisioning of resources and capabilities according to cloud service users’ demand, sometimes automatic provisioning is also possible. Available resources and capabilities can be provisioned at any time to any amount according to users’ needs.

Measured service: Cloud systems can provide some level of monitoring and controlling facilities to both cloud service users and cloud service providers. Cloud systems can measure resource and service usage and perform automatic control and optimization in some cases.

Below given is the cloud reference architecture (Figure 1) [4].

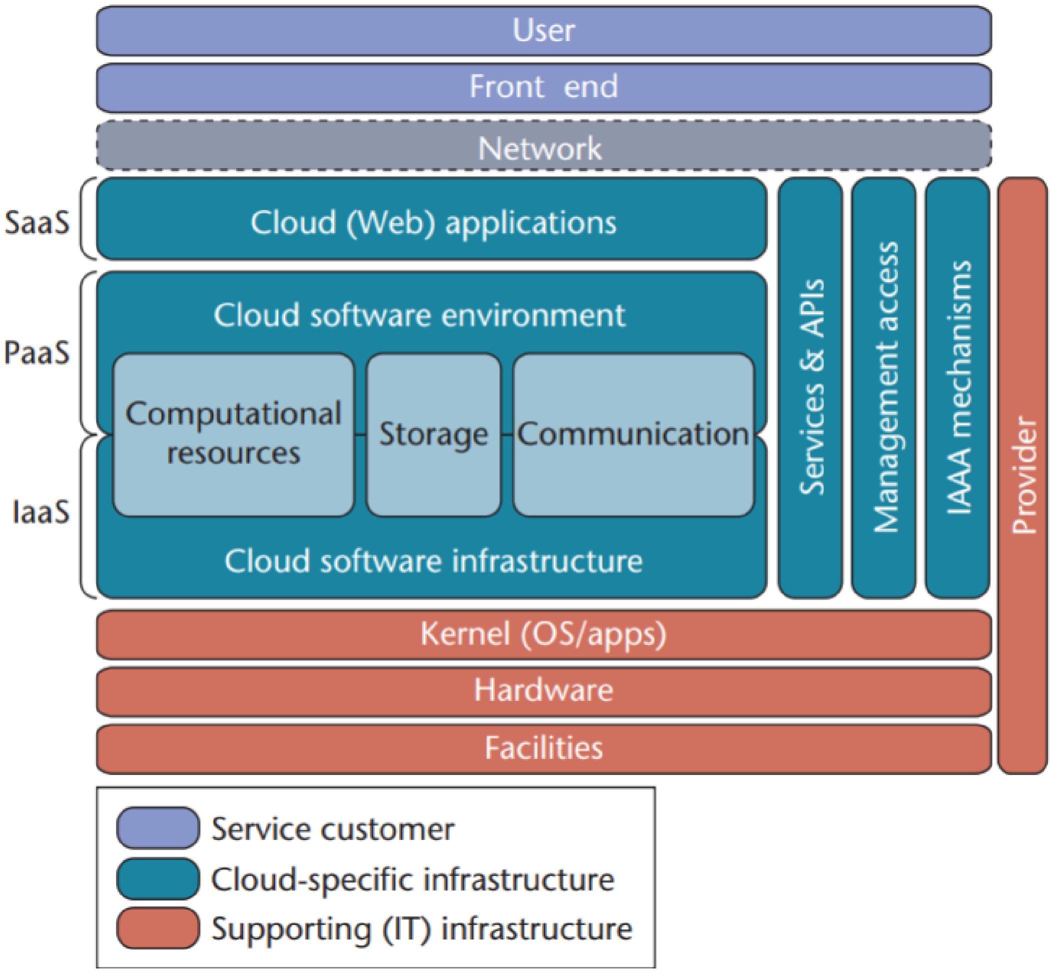


Figure 1. *Cloud Reference Architecture [4]*

Cloud computing consists of three main models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and brief descriptions of the three service models are given below [3].

Infrastructure as a Service (IaaS): IaaS consists of fundamental computing resources such as servers, networking capabilities, storage, and the like. Users have no right to modify or control the cloud infrastructure but have access to the operating system and software. Amazon Web Services (AWS) EC2, Google Compute Engine (GCE) are examples of IaaS.

Advantages of IaaS:

1. High flexibility and high scalability
2. On-demand

3. Low cost
4. No point of failure
5. Zero hardware investment

Platform as a Service (PaaS): PaaS provides facilities to users with deployment and control of software, or sometimes users have the facility to modify the environment's configuration. However, users have no right to modify or control the cloud infrastructure where their applications are running. Google App Engine, AWS Elastic Beanstalk are some known Pass.

Advantages of PaaS:

1. Flexibility and scalability
2. Load-balancing
3. Multi-tenancy
4. Easy development, testing, and deployment of applications
5. Zero infrastructure investment

Software as a service (SaaS): SaaS facilitates cloud service users' access to software and applications running on a cloud infrastructure. However, users have no right to modify or control the cloud infrastructure where their applications are running. Google Drive, Slack are some examples of SaaS.

Advantages of SaaS:

1. Multi-tenancy with customization
2. Scalability
3. Automatic updates
4. Ease of access
5. No installation and maintenance cost

The four deployment models are as follows [3]:

Private cloud: Usually, a single organization with multiple business units uses private cloud infrastructure. A private cloud is generally operated and owned by a single organization or a third party or sometimes combined. It can be configured on or off-premises.

Community cloud: Community cloud is used by multiple organizations that share computing resources and capabilities, for example, governmental bodies, educational institutions, and hospitals. Community cloud can be configured on-premises or off-premises and generally managed and owned by multiple organizations, third parties, or sometimes combined.

Public cloud: Public cloud infrastructure is generally operated and owned by an educational institution, business, or government department and is open for public use. It is located on the cloud service provider's on-premises.

Hybrid cloud: Hybrid cloud infrastructure consists of two or more unique cloud deployment models. These multiple cloud deployment models (private, community, or public cloud models) are tied together to provide software and data portability.

2.2 Security Incidents and Incident Handling

Any noticeable event that indicates evidence of network, system, data, compromise, or violation of system, data, or network protection measures can be considered a security incident. A security incident can be of any kind. An attacker launches Distributed Denial-of-Service (DDoS) attacks against vulnerable workstations to make the business network unusable and swamp the system. A worm infects thousands of computers in an organization, an attacker getting root-level access to the system and gaining access to sensitive data, an employee with bad intention disclosing a company's information. Such activities can be considered security incidents.

Incident handling is the set of processes to handle or manage an incident or a possible incident. Below given is the NIST Incident Handling Life Cycle (Figure 2).

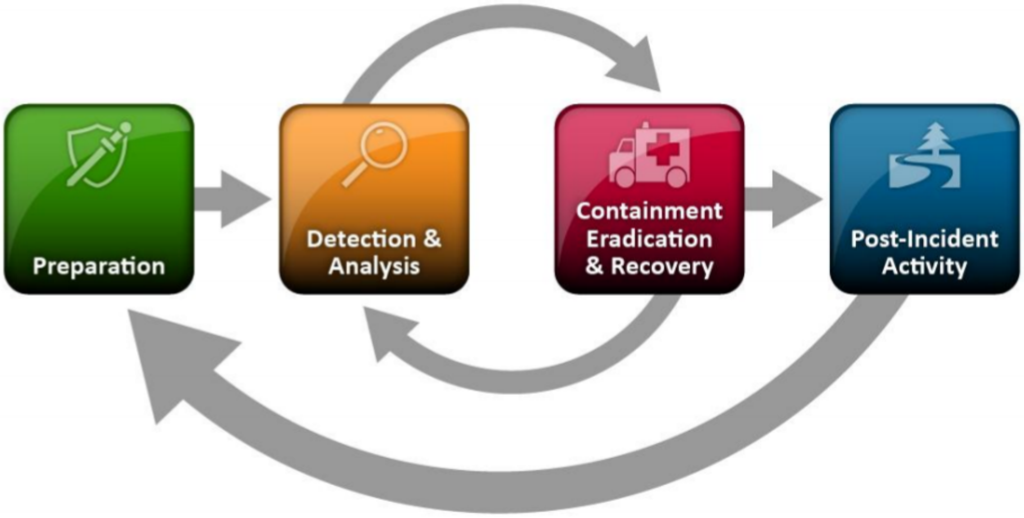


Figure 2. *Incident Handling Life Cycle [5]*

According to NIST's SP800-61 [5], the incident handling life cycle consists of 4 phases.

- *Preparation*: The preparation phase is the base of the incident handling procedure. It focuses on constructing incident response capabilities and ensuring the security of existing systems, networks, and applications to prevent incidents. It is essential for effective incident handling.

- *Detection and Analysis*: The incident or possibility of the incident is detected in this phase. Detection and analysis start when unusual behavior is marked as flagged when there are indications of an incident. The analysis is done to determine whether the flagged behavior is a threat. After analysis, the threat is prioritized in this phase as well.

- *Containment, Eradication, and Recovery*: Containment of the threat is ensured in this phase to prevent infection. After containment, the infected asset needs to be cleaned to eradicate the threat. Moreover, after eradication, the resource is recovered to operate normally.

- *Post-incident activity*: The incident handling procedure is evaluated by the incident response team in this phase to determine the exact occurrence, how they deal with the occurring incident and modify the incident management plan for preventing similar incidents in the future.

3. Reviewed Literature

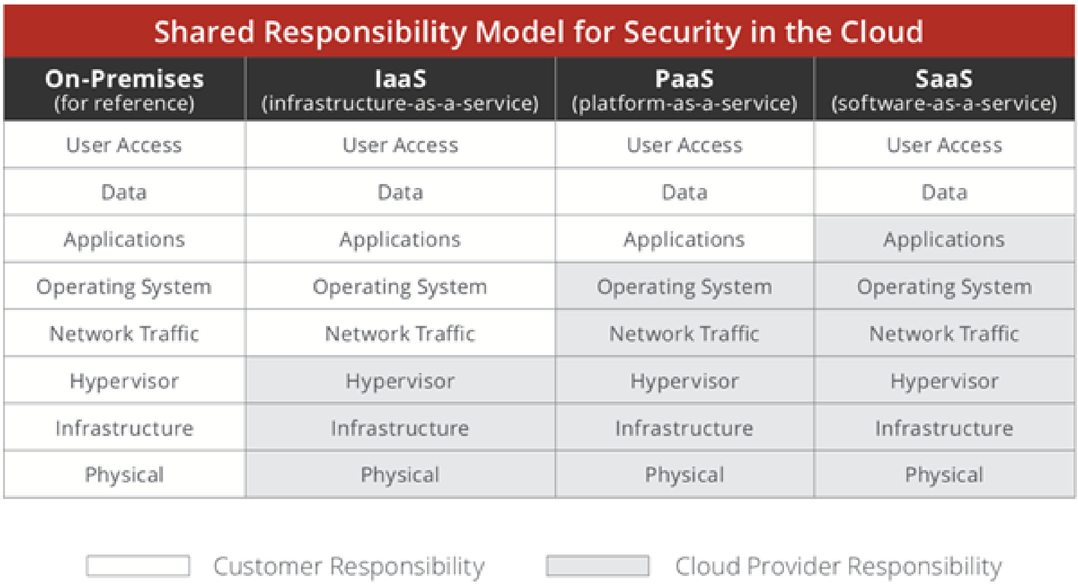
There are many research works performed in the field of cloud computing and incident handling. Most of the research focuses on cloud digital forensics investigation as a significant part of cloud incident handling in the cloud environment. There are also several pieces of research focusing on incident handling [5], cloud incident handling [6, 7, 8, 9, 10, 11, 12, 13], cloud forensics [14, 1, 15, 16, 17, 18, 19, 20, 21, 22, 23], cloud security [24, 25], threat [26, 27, 28], vulnerabilities [4, 29, 30], and data breaches. The Cloud Security Alliance have publications focusing extensively on challenges and best practices to handle the incident in the cloud [31]. There are studies from the past that focused on cloud incident handling. However, as the cloud computing environment is continuously evolving, there is less research on the sufficiency of existing incident handling procedures. There is no incident handling framework that organizations can follow in handling cloud and on-premises incidents. Findings from the reviewed literature regarding differences between cloud and on-premises incident handling, cloud shared responsibility model, cloud incident handling, cloud forensics, and known cloud data breaches, and some security tools are discussed below.

3.1 Cloud VS. On-Premises

In an on-premises computing environment, organizations have complete control, access, and visibility over the systems and installed software. However, regarding the cloud computing environments, there are shifts in access and control from the user to the provider [6], depending on the chosen cloud service provider and service models. AWS claims in their shared security model that they are responsible for protecting the infrastructure, in other words, software, hardware, and networking that run all AWS offering cloud services [32]. Microsoft Azure claims that they are responsible for the security of the physical hosts, networks, and data centers [33]. While CSPs' and CSUs' permission within a cloud environment depends on chosen service models, cloud infrastructure's location and control are described in cloud deployment models. In cloud environments, data are distributed across multiple systems or jurisdictions [1]. Multi-tenancy is another feature of cloud environments as well. Handling incidents in the cloud are different from handling incidents in an on-premises environment due to the characteristics mentioned above of the cloud.

3.2 Cloud Shared Responsibility Model

To establish incident response capability and ensure the security of cloud environments, cloud service users need to be aware of their and cloud service providers' security responsibilities. Below given is a shared responsibility model for security in the cloud (Figure 3) [34].



Shared Responsibility Model for Security in the Cloud

On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (platform-as-a-service)	SaaS (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

□ Customer Responsibility ▨ Cloud Provider Responsibility

Figure 3. *Cloud Shared Responsibility Model [34]*

From the model, it is visible that the cloud service provider is responsible for protecting the infrastructure that is composed of the hardware, software, networking, and facilities that run services in the cloud, and depending on the type of cloud services that customers are using, customer responsibilities can be determined [34]. For example, AWS EC2, AWS VPC, and AWS S3 have known Infrastructure as a Service (IaaS) from AWS, and, in such services, security controls responsibilities belong to customers [32]. Common security responsibilities of both CSPs and CSUs are pointed out below. CSPs' Common Security Responsibilities According to the shared responsibility model, specific items are the cloud service provider's responsibility. Which vary depending on the vendor, but the common items that the cloud service provider is responsible for include:

- *Hardware and Infrastructure*: Responsibility for control, maintenance, and security of the hardware and infrastructure always belongs to the CSP.

- *Physical Security*: Maintaining the security of the datacenters where instances/applications are hosted is always done by the CSP.

- *Network Connectivity*: CSPs always have to keep the network connectivity to the cloud up and running.

- *Availability*: CSPs are responsible for ensuring cloud computing capacity, storage, and database availability.

- *Disaster Recovery*: CSP is responsible for any disasters in the cloud environment and should have proper disaster recovery and service continuity assurance plans for infrastructure.

Think of these items as having the responsibility "of" the cloud, meaning that the service providers are responsible for the cloud's existence and uptime. In short, the virtualization layer, physical hosts, data center, and network controls are directly under CSP.

CSUs' Common Security Responsibilities [35]

- *Information and Data*: The users' responsibility is to manage how and when data is used by keeping control over information and data. The cloud computing environment is developed in such a way that restricts service providers from accessing user-controlled data.

- *Application and Code*: It is entirely the users' decision to spin up cloud assets. In any case, through the whole application lifecycle, users will ensure the control and security of their applications. This means users will be responsible for securing the code from malevolent abuse or interruption. From test to production, it is solely the users' responsibility to keep up the security of the associated frameworks during the development and integration of the application.

- *Identity and Access Management (IAM)*: Control of Identity and access management (IAM) is always CSUs' responsibility. CSU chose the methods of how the system will authenticate and authorize users. Selection of mechanisms like MFA, single sign-on (SSO), generation of certificates, access key, creation of users, and management of passwords are in CSUs' hands.

- *Platform and Resource Configuration*: Control of platform and resource configuration is based on the chosen instance types. Server-based instances are like physical servers in the cloud. In a server-based instance, users have more control over the security of the OS and application, the configuration of resources. In serverless instances, CSP provides users access to the configuration platform, but users need to have the knowledge of the configuration and security of the desired instance.

3.3 Cloud Incident Handling

Cloud Incident handling means handling incidents or possible incidents in the cloud. Cloud incident handling is a fundamental part of securely managing the cloud computing environment. There is some well-known incident handling guidelines. Incident handling is done by following these guidelines. However, in the case of handling incidents in the cloud, studies claim that these guidelines are insufficient. Researchers claim that the incident handling process is impacted by cloud computing, and it is challenging for users to handle security incidents in the cloud environment following the existing incident handling guideline as these guidelines are considered for the on-premises environment [6]. Researchers proposed a conceptual incident handling model for organizations that will support handling incidents, performing digital forensics investigations in the cloud environment, claiming that handling incidents in the cloud is a complicated task due to the distributed nature of the cloud. It is essential both for CSPs and CSUs to have a model beforehand for handling incidents in the cloud [7] effectively. Researchers propose an intruder detection framework for identifying intruders in the cloud computing environment and offer a procedure to handle cloud incidents in such a way that maintains a chain of custody and is acceptable in the court of law [14]. Researchers shared expert views on the importance of incident data sharing with the cloud service provider and suggested a tool to handle incidents by improving user-end incident data quality, improving CSPs' responsibility [8]. Researchers have developed an API and incident information sharing format to circulate incident information to CSP and make it uncomplicated and less time-consuming for CSIRT to respond to incidents [36]. With the expansion of cloud features, the incident handling procedures are getting complex. Researchers discussed the current issues and standards and introduced a cloud incident handling framework that fits the entire incident handling cycle [9]. Researchers used the results from comparing DBSCAN, K-means clustering, and Local Outlier Factor and Isolated Forest non-clustering based algorithms for incident handling to detect anomalies in the cloud cluster and figure out the results from clustering-based algorithms are more accurate in detecting anomalous clusters in the cloud [10]. Researchers interviewed organizational CSUs, and results were presented to find the strategy of acceptance of incident handling in the cloud [11]. Researchers suggest a cloud incident response model minimizes incident response time and that the model is based on existing well-known incident response frameworks [12]. Researchers focused on monitoring system integration and automating some essential parts of incident response, claiming that the complexity of the cloud computing environment makes it difficult to respond and diagnose incidents [13]. Researchers present a framework based on machine learning and event processing to detect anomalies in the cloud computing environment's network, service, and application layers [37].

3.4 Challenges in Cloud Incident Handling

As the cloud computing market is increasing, the security risk related to cloud services is also growing. Companies are concerned about the security of cloud services. CSU and CSP's level of control, visibility, and responsibility create a significant difference between on-premises computing and cloud computing. In an on-premises environment, dealing with a security incident is relatively straightforward. Performing forensic analysis by accessing logs, grabbing the server IP to detect the root cause of any security incident was not as complex as in a cloud environment. It is challenging to gather such information to perform any analysis in the cloud environment because CSUs do not know where to look for the logs, and IP addresses are spread globally. Lack of control, visibility, and insufficient information make it harder for users to detect an incident or a possible incident and handle those incidents accordingly. Brief descriptions of the challenges that arise with handling incidents in the cloud are provided below.

3.4.1 Data Collection

Data must be collected first when handling an incident, which is a major challenge in cloud environments. Sources of data need to be identified for data collection. New data sources introduced by cloud environments, such as cloud control planes, make it challenging for incident response teams to know the data sources [2]. Data collection is complicated when security teams do not have accurate information about the cloud architecture. Such situations may arise if the CSP-provided information is not complete or security teams have no idea of the current information about the cloud computing environment [2]. The unavailability of proper logs at each cloud [6] makes the data collection process challenging. Auto-scaling is a feature of the cloud computing environment. Auto-scaling improves the instance's fault tolerance by replacing an unhealthy instance with a healthy one according to defined conditions [38]. Sometimes important information gets lost due to the auto-scaling feature or sometimes by terminating instances [2]. The cloud's multi-tenancy features are another reason CSPs might not be willing to grant access to data because the desired data may include information about some other tenants. To maintain privacy, CSPs are not allowed to disclose data [6].

3.4.2 Data Analysis

Data analysis is another major challenge in cloud incident handling due to data distribution across multiple systems or jurisdictions [1]. The cloud computing environment consists of a large volume of data, which complicates the data analysis [2]. Due to the distributed nature and a large amount of data, collecting real-time and meaningful data for performing data analysis is also a challenge in the cloud. SANS found from a survey that CSUs face challenges in cloud incident handling due to improper skills, tools, and standards [15]. Additionally, logs are not universally available for analysis. In addition, data correlation is required for analysis and for that reason, organizations must use machine learning, and advanced systematic solutions [26]. Another reason is the lack of governance on the CSP-controlled resources, making it harder to analyze data in the cloud computing environment.

3.4.3 Understanding the Security Responsibilities

CSUs are not adequately aware of their security responsibilities in cloud environments, as the cloud environment control shifts from user to provider [6] depending on the type of cloud computing environments. CSUs must understand the cloud shared responsibility model to figure out the incident response responsibilities. The cloud shared responsibility model, and its concept may seem straightforward enough to be understandable by the CSUs. However, for multiple reasons, CSUs find it very confusing to understand the application of the cloud shared responsibility model. CSUs sometimes do not secure their assets in the cloud, assuming that their CSP is taking care of the security of the assets. At the same time, it is always the CSUs' responsibility to safeguard their assets from common attacks and implement proper security standards. Another reason CSUs face difficulties understanding their security responsibilities is the difference between shared responsibilities in the IaaS, PaaS, and SaaS environments because each service model has different shared responsibilities. An apparent incident management strategy is crucial, as there is a lack of chance to work with the CSP to handle cloud incidents [8].

3.4.4 Lack of Access and Visibility

Lack of visibility to the CSP-controlled event sources and cloud infrastructure is a significant cause of CSUs not knowing the incidents impacting the assets. In on-premises environments, users can enhance the security of their network, systems, and infrastructure. Users have control of their infrastructure and incident handling process, or it is possible to hire third-party service providers to handle incidents. Therefore, users do not have to face issues with access to information and visibility to incidents in the on-premises environment. Provisioning, de-provisioning, controlling, and maintaining the infrastructure in on-premises were straightforward, but responsibilities are shared between CSP and CSU in the cloud computing environment. Availability of full access to information and resources significantly impacts the incident handling process. Lack of access to the CSP-managed resources makes it harder to gather vulnerability information and other required information to handle incidents. No direct contact or limited contact with CSP can cause CSUs to have less access to information [2]. SANS surveyed about 500 IT professionals. Among them, 58% claimed that they have less visibility to CSP controlled resources and operations as the major problem with their CSP, 48% complained that they do not get enough incident management support. With a lack of visibility, 46% said they do not have enough visibility to the virtual machines and workloads, and 26% of the respondents complained that they faced data breaches in the cloud environment due to CSP-introduced vulnerabilities [24].

3.5 Cloud Digital Forensics

Cloud digital forensics refers to the application of digital forensics investigation in the cloud computing environment. According to NIST, cloud forensics refers to "the application of scientific principles, technological practices, and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence" [16]. Logs are a crucial part of digital forensics investigation as logs contains detailed information about users' action on the system or network. Logs are collected and analyzed to perform a digital forensics investigation. However, the collection of logs is a complicated job in the case of the cloud computing environment due to the multi-tenancy and volatility of the cloud, log diversity, other unavoidable challenges [17]. A logging framework was proposed by the researchers that will meet the need of forensics investigators from the business perspective [17]. Researchers proposed a conceptual framework for a digital forensics investigation, emphasizing the collection phase of a digital forensics investigation. It is difficult and time-consuming to gather data to analyze data in the cloud environment due to distributed data across multiple locations, and servers [1]. Researchers introduced coordinated cloud incident handling considering the SaaS, and organizations can use the forensic-by-design model during system or network designing [18]. This model can be helpful for organizations to fit the digital forensics investigations tasks to their existing plans for incident handling [18]. Researchers proposed a model that unifies digital forensics investigation with incident handling procedures focusing on increasing the efficiency of incident response from both CSU and CSP [25]. Researchers also introduced a secure cloud digital forensics investigation framework focusing on detailed user activity monitoring in the cloud, claiming that the framework can be effectively used with current and upcoming cloud architectures [19]. Researchers pointed out the challenges digital forensic investigators face while investigating cases in the cloud computing environment due to loss of authority and accountability. They suggested solutions to overcome such obstacles to perform a successful investigation [20]. Digital forensics investigators face many challenges in investigating the cloud computing environment. Researchers pointed out four significant challenges and suggested possible solutions and skills required to overcome those challenges [21]. Researchers explored the problems and challenges in cloud forensics investigation. They proposed a systematic approach to predict that this approach would minimize the cost of forensics investigations and help understand the forensics investigation's nature in cloud computing environments [22]. Researchers reviewed previous studies regarding cloud forensics challenges and existing cloud forensics investigation tools and strategies to compare and determine drawbacks and differences and provided guidance for researchers who are interested in developing cloud forensics services [23].

3.6 Cloud Vulnerabilities

Security incidents in the cloud often occur due to the presence of vulnerabilities. Studies have shown several vulnerabilities in the cloud computing environment. Among those, some of the significant vulnerabilities that cause and can cause security incidents are discussed below.

3.6.1 Poor Encryption

Encryption plays an essential role in the cloud computing environment. If the hybrid cloud architecture is considered, the risk of data theft is higher in the hybrid cloud environment as data is always in transit between one cloud computing environment to another through the interconnection between the cloud environments [39]. Due to this, poorly encrypted data are at risk of being stolen or altered.

3.6.2 Misconfigured Cloud Environment

Misconfigured cloud environment due to the lack of knowledge of the cloud computing environment is a major challenge. As organizations are shifting more workloads to the cloud, the cloud infrastructure is getting complex, causing complexity in handling incidents due to a lack of expertise. Misconfigured cloud environments are causing severe damage to the assets. The cloud computing environment is vulnerable to security incidents if there are unsecured data storage, users with unnecessary and excessive permissions, unchanged default configurations and credentials, weak or improper security controls, and standards [27].

3.6.3 Unauthorized Access

The cloud is an on-demand self-service computing environment. CSUs manage their cloud according to their needs through a web-based administrative interface. Someone can probably get unauthorized access to CSUs' administrative interface, leading to severe security incidents. Study shows that unauthorized access to the cloud is more probable than unauthorized access to the on-premises environment [4].

3.6.4 Insufficient Identity, Access and Credentials Management

Identity, access, and credentials management is crucial part of the cloud computing environment. Loss of IAM and credentials may result in loss of data and assets in the cloud. Insufficient and inappropriate identity, access, and credentials management may lead to major security incidents. Many organizations face severe data breaches due to insufficient identity, access, and credentials management in the cloud [28]. From a survey by CSA, it was found that 22% of the surveyed people faced data breaches due to compromised cloud credentials [40]. 65% of the respondents think that there is a possibility that their organization has chances of facing data breach in the future due to compromised cloud credentials [40].

3.6.5 Insecure APIs

Application Programming Interfaces (APIs) play an essential role in the cloud computing environment. Moving the assets to the cloud, organizations become more dependent on APIs. Cloud APIs are vulnerable because these APIs are accessible via the Internet. For that reason, an insecure API may open a field for attackers to exploit the cloud computing resources. APIs developed without proper authentication, authorization, and input validation control can be used by attackers to access the cloud data and resources [29]. If an attacker manages to exploit an insecure API vulnerability, it could cause harm to all of the resources running under the compromised account in the cloud computing environment.

3.6.6 Shared Tenancy Vulnerabilities

As the cloud computing environment is built based on multiple hardware and software that enable virtualization technology, an adversary with advanced knowledge of identifying running hardware or software in the cloud computing environment can escalate privileges [30]. Though exploiting shared tenancy vulnerabilities requires time, effort, and advanced skills, it can result in severe disaster as it affects the virtualization layer of the cloud computing environment.

3.6.7 Lack of Security Strategy and Architecture

The cloud computing environment with a lack of proper security strategies and architecture is highly vulnerable to security incidents. Cloud computing environments lack strict security strategies due to insufficiently experienced cloud professionals to understand the internal security architecture of the cloud or sometimes by human error, which results in major security incidents. Many data breaches occurred in the cloud computing environment due to insufficient security strategies and controls and a lack of proper security architecture to safeguard the cloud computing environment [28].

3.7 Cloud Data Breaches

Cloud data breaches occur when there is the presence of vulnerabilities in the cloud. Some of the vulnerabilities that result in data breaches are poor encryption, misconfigured cloud environment, unauthorized access, insufficient and inappropriate identity access and credentials management, insecure APIs, shared tenancy vulnerabilities, and lack of security strategy. Some of the data breaches that occurred due to the mentioned vulnerabilities are discussed below.

3.7.1 Experian

In 2017, an American credit bureau called Experian faced a major data breach which exposed the detailed personal information of 123 million households in America due to misconfigured AWS S3 cloud storage [27].

3.7.2 Exactis

In 2018, A marketing company in the United States named Exactis faced a data breach that resulted in the exposure of important personal information of 230 million Americans due to a publicly accessible database server with an unsecured AWS Elasticssearch database [27].

3.7.3 Capital One

In 2019, another major data breach was faced by a renowned financial corporation called Capital One due to a misconfigured Web Application Firewall (WAF) with overly permitted AWS EC2 and S3 roles [28]. That allowed Server-Side Request Forgery (SSRF), causing the exfiltration of sensitive personal data of 106M customers by accessing read-access enabled cloud folder [28].

3.7.4 Github

Github faced a massive Memcached DDoS amplification attack of 1.35Tbps network traffic in 2018, which resulted in denial of service due to a misconfigured cloud environment with an open UDP port and using outdated software [28]. That attack is considered the second-largest DDoS attack of 2018 after the 1.7Tbps confirmed by NETSCOUT [28].

3.7.5 Tesla

Tesla experienced AWS account credentials hijacking. The attacker got access to the data in the AWS S3 bucket and managed to install a cryptocurrency mining script in the Kubernetes instance. Moreover, this incident occurred due to insufficient identity, access, credentials management, lack of intrusion detection, monitoring, and the misconfigured administrative interface of Kubernetes [41].

3.7.6 Zoom

In 2020, due to the current Covid-19 pandemic, Zoom experienced a significant increase in users as organizations shifted their operations to remote mode. However, there was a misconfigured cloud computing environment, lack of proper security controls, lack of sufficient credentials and access controls, insecure APIs in use [28]. No reasonable procedures were present to check password reuse by users, which resulted in the credential stuffing attack, and 500 million user accounts were breached [28].

3.7.7 Amazon Web Services (AWS)

During the first quarter of 2020, AWS detected a 2.3Tbps CLDAP reflection DDoS attack, and AWS managed protection service AWS Shield claimed to have mitigated the DDoS attack [42]. AWS claims that this is the largest DDoS attack they have ever faced.

3.8 Security Tools

Security incidents are common in the digital era. Incidents like data theft, hacks, and breaches are occurring regularly and adversely impacting financial activities, and these are occurring due to a lack of proper security standards and solutions applied. To handle a security incident or to perform a digital forensics investigation, a security expert needs proper security tools besides skills. Many security tools are available to handle incidents, conduct digital forensics investigations, and detect and analyze. Security experts have the opportunity to choose tools according to their organization's security needs. Some of the tools and their functionalities are discussed below.

3.8.1 Splunk

Splunk is an advanced infrastructure monitoring and troubleshooting tool with an easy-to-use dashboard, customizable incident investigators, and other advanced features. It is suitable for cloud, and on-premises environments [43] and can be used by almost all types of organizations because of its high scalability. Splunk has an. Some of the critical features of Splunk are mentioned below [43].

- Advanced machine learning and AI technology for quick incident identification and classification
- Rapid and effective incident response
- Real-time and advanced troubleshooting
- Incident response automation
- Risk prioritization and scoring
- Fast threat detection and alerting

3.8.2 Dynatrace Infrastructure Monitoring

Dynatrace acquired SpectX is an advanced AI-powered infrastructure monitoring tool used to observe all types of infrastructure and automate incident handling response. It is capable of performing rapid analysis to detect suspicious activities and provide faster response [44]. Dynatrace can connect to any HTTP-enabled on-prem or cloud computing environment to analyze raw log files and present those raw data in a structured and easy-to-understand format. Some of the features of Dynatrace are discussed below [44].

- All-in-one intelligent platform monitoring
- AI-powered anomaly detection mechanisms
- Fullstack monitoring of application and microservices
- Automated incident response for faster resolution
- Runs on both on-premises and cloud environment
- Raw text-based log files to an advanced structured view

3.8.3 SolarWinds Orion

SolarWinds Orion is an advanced hybrid IT infrastructure monitoring platform that supports detailed monitoring of all applications, systems, and networks on-premises and cloud computing environments in a single dashboard [45]. SolarWinds Orion has six advanced tools in its platform, including Server and Application Monitor, Storage Resource Monitor, Virtualization Manager, Netflow Traffic Analyzer, Network Performance Manager, and Network Configuration Manager. Some key features of SolarWinds Orion are discussed below [45].

- Complete and Simplified IT stack administration in one place
- Infrastructure monitoring scalability
- Customizable dashboard with centralized settings and control
- Multiple tools integration in one dashboard

- Proper visibility to both cloud and on-premises

3.8.4 Wazuh

Wazuh is a free and open-source security tool. It is architected as a System Information and Event Management (SIEM) solution and Host-based Intrusion Detection System (HIDS). Wazuh agents are installed on multiple endpoint devices, and the Wazuh server monitors the endpoint devices. Some of the key features of Wazuh are discussed below [46].

- Available for both on-premises infrastructure and cloud platforms like AWS, Azure.
- Support integration with popular automation tools like Ansible, Chef, Puppet
- Wazuh is an advanced integrity monitoring, threat and vulnerability detection, incident response, and regulatory compliance solution.

3.8.5 ManageEngine EventLog Analyzer

ManageEngine EventLog Analyzer is an advanced SIEM tool for log management and analysis, auditing and keeping systems and services compliant with data protection rules and standards [47]. It comes with an advanced custom log parser to gather information from various logs from multiple resources and present them well-formatted. The key features of the ManageEngine EventLog Analyzer are provided below [47].

- Simple deployment and ease-of-use
- Real-time monitoring of systems and applications
- Threat intelligence and behavior tagging
- Advanced log management, analytics and reporting
- Network and application auditing
- Built-in incident response

4. Methodology

In this chapter a brief description of the design of the masters thesis is presented.

Data Collection: Data is collected through an online questionnaire to gather experts' opinions regarding incident handling in the cloud and on-premises.The online questionnaire was created to gather experts' opinions regarding the below topics.

- Types of infrastructures in their organization
- Opinion regarding the difference between incident handling in the cloud and on-premises
- Advantages and disadvantages of cloud in terms of incident handling
- How the experts rate their organizations considering the phases of incident handling
- If the experts follow any specific framework to handle cloud incidents
- If the experts find the currently available frameworks useful to handle cloud incidents and if not, do they wish to get a hybrid incident response framework
- Opinion regarding the cloud incident handling challenges that are mentioned in the literature
- If the exerts use any incident handling tool
- Experts' suggestion regarding incident handling

Data Processing: Frequency analysis is performed using a statistical analysis program called PSPP [48] on data that are collected through the questionnaire to get the responses from the participants. A hybrid incident response framework is created based on the responses.

Framework Creation: The hybrid incident response framework was created using an online tool [49]. Each phase of the hybrid incident framework described in details. The framework would guide regarding incident handling to organizations with cloud and on-premises infrastructure.

Framework Validation: For validating the hybrid incident response framework, another online questionnaire was created to collect experts' opinions regarding the usefulness of the framework. The questionnaire included a link to a website with each step of the hybrid incident framework described. The questionnaire was designed with the below topics.

- How the experts rate the hybrid incident response framework in terms of its usefulness.
- Experts suggestions regarding the improvement of the framework.

The thesis also includes some suggestions regarding best practices that would provide guideline to SMEs for effectively handling incidents in the cloud computing environment.

5. Result

A survey was conducted regarding cloud incident handling among experts from several types of organizations, including public, fintech, hosting providers, banks, and others around the world. The analyzed result from the survey is presented below.

- Experts from 6 Estonian, 13 global, and 1 Bangladeshi companies consisting of a different number of employees participated in the survey (Table 1).

Country of Operations				
	Frequency	Percent	Valid Percent	Cumulative Percent
Estonia	6	30.00%	30.00%	30.00%
Global (2 or more)	13	65.00%	65.00%	95.00%
Bangladesh	1	5.00%	5.00%	100.00%
Total	20	100%		

Table 1. Country of Operations

- 20% of the experts responded that their organizations use only cloud infrastructure, 55% of the organizations use hybrid infrastructure (combination of cloud and on-premises), 5% responded that their organization uses either cloud and on-premises separately or a combination of cloud, on-premises, and hybrid infrastructures (Table 2).

- 60% of the respondents responded that there are differences between handling incidents in the cloud and on-premises environment, 15% responded that there is no difference, and 25% responded that there might be differences between handling incidents on premises and handling incidents in the cloud (Table 3). Among the participants who responded that there are or might be differences, there are different opinions regarding handling incidents in the cloud and on-premises.

  Below are some expert-mentioned differences between handling incidents in

1. What type of infrastructure does your organization use?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Cloud	4	20.00%	20.00%	20.00%
Hybrid	11	55.00%	55.00%	75.00%
On-prem & cloud or all	5	25.00%	25.00%	100.00%
Total	20	100%		

Table 2. Types of Infrastructure in Use

2. Is there any difference between handling incidents on on-premises and handling incidents in the cloud?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	12	60.00%	60.00%	60.00%
No	3	15.00%	15.00%	75.00%
Maybe	5	25.00%	25.00%	100.00%
Total	20	100%		

Table 3. Difference Between Cloud and On-premises Incident Handling

the cloud and on-premises.

- *Skill requirement:* According to some of the participants, handling incidents in the cloud requires more skills than handling incidents in on-premises environments. As the cloud is a distributed system, it is obvious that there are some additional skills required to handle incidents in the cloud.

- *Less responsibility:* As the cloud is third-party provided, some participants said that experts have fewer security tasks and fewer things to handle. According to the cloud shared responsibility model, CSP's responsibility is to take care of incidents. However, organizations are responsible for the security of their resources in on-premises environments.

- *Less access and visibility:* Some also mentioned that there are fewer incident handling opportunities in cloud computing due to a lack of access and visibility to cloud resources and incident relevant logs. So there is a dependency on the

CSP. However, organizations have complete control over all resources and incident logs in on-premises environments.

– *On-premises risks*: In on-premises environments, there are risks of intruders getting physical access to on-premises resources if not secured properly. On-premises resources are exposed to other risks like electricity outage, flood or fire.

- 50% of the experts believe that there are advantages of using the cloud regarding incident handling, 10% responded that there are no advantages and 40% responded that there might be advantages of using the cloud (Table 4). Among the experts who answered that there are or might be advantages of using the cloud regarding incident handling, some said that as the cloud is outsourced, users do not need to worry about processing power, electricity, hardware issues, capacity, resources, and system failures. Some responded that data collection could be simpler in the cloud. Users only need to take care of the services they use. As CSPs have their incident handling professionals, users have fewer security tasks and responsibilities, fewer incidents to handle. Experts who believe that there are no advantages of using the cloud regarding incident handling say organizations need to hire cloud experts to handle incidents; also, there is a lack of access to cloud resources.

4. Regarding handling incidents, are there any advantages of using the cloud?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	10	50.00%	50.00%	50.00%
No	2	10.00%	10.00%	60.00%
Maybe	8	40.00%	40.00%	100.00%
Total	20	100%		

Table 4. Advantages of Cloud Regarding Incident Handling

- 45% of the participants responded that there are disadvantages of using the cloud regarding incident handling, and the other 55% responded that there might be disadvantages (Table 5). Most of the participants said that there is a lack of access and visibility to the cloud resources and cloud incidents. Some of the participants responded that there are not enough opportunities for experts to handle incidents in the cloud. Some said it is complicated to handle cloud incidents due to the distributed nature of data. Some experts said more dependency on CSP as users do not get to see the whole incident, or sometimes the involvement of third parties is required regarding incident management.

6. Regarding handling incidents, are there any disadvantages of using the cloud?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	9	45.00%	45.00%	45.00%
Maybe	11	55.00%	55.00%	100.00%
Total	20	100%		

Table 5. Disadvantages of Cloud Regarding Incident Handling

- 85% of the experts responded that their organizations handle cloud incidents with their in-house experts' support (Table 6). 10% responded that experts from outside their organizations handle cloud incidents in their organizations, and 5% said that depending on the type of incidents and its roots, the organization decides if in-house experts should do incident handling or outsourced (Table 6).

8. How does your organization handle cloud incidents?				
	Frequency	Percent	Valid Percent	Cumulative Percent
In-house	17	85.00%	85.00%	85.00%
Outsourced	2	10.00%	10.00%	95.00%
Others	1	5.00%	5.00%	100.00%
Total	20	100%		

Table 6. How Cloud Incidents Are Handled

- 65% of the experts responded that different skills are required to handle cloud incidents, 20% responded that there might be a requirement of different skills to handle cloud incidents. However, the other 15% said that cloud incident handling does not require different skills (Table 7).

9. Do you think handling incidents in the cloud requires different skillsets?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	13	65.00%	65.00%	65.00%
No	3	15.00%	15.00%	80.00%
Maybe	4	20.00%	20.00%	100.00%
Total	20	100%		

Table 7. Different Skillsets Requirements for Cloud Incident Handling

5.1 Incident Handling in the Cloud

- On a scale of 1 to 5, 5% of the respondents rated their organizations' incident response preparation phase 2, 35% rated 3, 50% of the respondent rated 4, and the other 10% rated 5 (Table 8).

10. On a scale of 1 to 5, How will you rate organization considering the preparation phase when it comes to incidents?				
Ratings	Frequency	Percent	Valid Percent	Cumulative Percent
2	1	5.00%	5.00%	5.00%
3	7	35.00%	35.00%	40.00%
4	10	50.00%	50.00%	90.00%
5	2	10.00%	10.00%	100.00%
Total	20	100%		

Table 8. Incident Response Preparation Phase Ratings

- On a scale of 1 to 5, 5% of the participants rated their organization incident response detection and analysis phase 2, 35% rated 3, 55% rated 4, and the other 5% rated 5 (Table 9).

- Regarding the incident response containment, eradication, and recovery phase, on a scale of 1 to 5, 10% of the respondents rated their organization 3, 75% rated 4, and the other 15% rated 5 (Table 10).

- Regarding the incident handling post-incident activity phase, On a scale of 1 to 5,

11. On a scale of 1 to 5, How will you rate organization considering the detection & analysis phase if the concerns incidents?

Ratings	Frequency	Percent	Valid Percent	Cumulative Percent
2	1	5.00%	5.00%	5.00%
3	7	35.00%	35.00%	40.00%
4	11	55.00%	55.00%	95.00%
5	1	5.00%	5.00%	100.00%
Total	20	100%		

Table 9. Incident Response Detection and Analysis Phase Ratings

12. On a scale of 1 to 5, How will you rate organization considering the containment, eradication and recovery phase when it comes to incidents?

Ratings	Frequency	Percent	Valid Percent	Cumulative Percent
3	2	10.00%	10.00%	10.00%
4	15	75.00%	75.00%	85.00%
5	3	15.00%	15.00%	100.00%
Total	20	100%		

Table 10. Incident Response Containment, Eradication and Recovery Phase Ratings

10% of the participants rated their organization 3, 40% rated their organization 4, and the other 50% rated their organization 5 (Table 11).

- 30% of the participants responded that their organizations use a specific framework for cloud incident handling, 50% said they do not use any particular framework or model. 20% responded that their organizations might use some framework or model to handle cloud incidents (Table 12).

- 25% of the participants believe that the currently used incident handling frameworks are efficient for handling cloud and on-premises incidents. 40% believe that the current frameworks are inefficient to handle both cloud and on-premises incidents. The other 35% of the respondents said the current framework might be efficient for both environments (Table 13).

13. On a scale of 1 to 5, How will you rate organization considering the post-incident activity phase if the concerns incidents?				
Ratings	Frequency	Percent	Valid Percent	Cumulative Percent
3	2	10.00%	10.00%	10.00%
4	8	40.00%	40.00%	50.00%
5	10	50.00%	50.00%	100.00%
Total	20	100%		

Table 11. Incident Response Post-incident Activity Phase Ratings

14. Does your organization use any specific framework or model to handle cloud incidents?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	6	30.00%	30.00%	30.00%
No	10	50.00%	50.00%	80.00%
Maybe	4	20.00%	20.00%	100.00%
Total	20	100%		

Table 12. Use of Specific Framework or Model for Cloud Incident Handling

- 55% of the participants wish to get a hybrid incident handling framework that will guide them to handle both cloud and on-premises incidents. 25% believe that the currently used frameworks are sufficient and do not wish to get any hybrid model, and the other 20% might want to get a hybrid framework (Table 14).

15. Do you think currently used incident handling frameworks are efficient for both cloud and on-premises environments?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	5	25.00%	25.00%	25.00%
No	8	40.00%	40.00%	65.00%
Maybe	7	35.00%	35.00%	100.00%
Total	20	100%		

Table 13. Efficiency of Current Incident Handling Frameworks

16. If no, do you wish to get a hybrid framework that will provide guidelines for handling incidents in the cloud and on-premises environment?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	11	55.00%	55.00%	55.00%
No	5	25.00%	25.00%	80.00%
Maybe	4	20.00%	20.00%	100.00%
Total	20	100%		

Table 14. Demand for Hybrid Incident Response Framework

5.2 Challenges in Cloud Incident Handling

- 60% of the respondents agreed with the statement that incident handling is trickier because it requires skillsets for identifying the data sources in the cloud. 10% did not agree with the statement, and the other 30% believe skillsets might be a requirement for handling incidents in the cloud (Table 15).

- 45% of the participants agreed that data analysis is challenging in the cloud due to distributed data across multiple systems or jurisdictions [1]. 10% of respondents denied the statement, and the other 45% said that distributed data might be a challenge for cloud data analysis (Table 16).

- 35% of the participated experts agreed that the shifting of security responsibilities between CSPs and CSUs based on the chosen cloud deployment model makes it harder for CSUs to understand their security responsibilities [6]. 25% of the experts

17. Study claims that handling incidents in the cloud is trickier because it requires skillsets to identify the data sources. Do you agree with the statement?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	12	60.00%	60.00%	60.00%
No	2	10.00%	10.00%	70.00%
Maybe	6	30.00%	30.00%	100.00%
Total	20	100%		

Table 15. Different Skillsets Requirement for Cloud Incident Handling

18. According to the study, due to the distributed nature of data across multiple systems or jurisdictions, data analysis is challenging in the cloud. Do you agree with the statement?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	9	45.00%	45.00%	45.00%
No	2	10.00%	10.00%	55.00%
Maybe	9	45.00%	45.00%	100.00%
Total	20	100%		

Table 16. Data Analysis is A Challenge in The Cloud

denied the statement, and 40% responded that security responsibility shifting might be an issue why CSUs lack of knowledge of and their security responsibilities (Table 17).

- 65% of the participated experts agreed with the statement that CSUs cannot handle cloud incidents properly due to lack of access and visibility to the CSP managed resources. 10% did not agree with the statement, and the other 15% believe that lack of access and visibility to CSPs resources might be an issue for CSUs inability to handle cloud incidents properly (Table 18).

19. Due to the shift in security responsibility between cloud service providers and cloud service users depending on chosen service models and providers, cloud service users have lack of understanding of security responsibilities. Do you agree with the statement				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	7	35.00%	35.00%	35.00%
No	5	25.00%	25.00%	60.00%
Maybe	8	40.00%	40.00%	100.00%
Total	20	100%		

Table 17. Lack of Understanding of Security Responsibilities

20. Lack of access and visibility to cloud service provider-managed resources make it harder for cloud service users to handle security incidents in the cloud. Do you agree with the statement?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	13	65.00%	65.00%	65.00%
No	2	10.00%	10.00%	75.00%
Maybe	5	25.00%	25.00%	100.00%
Total	20	100%		

Table 18. Lack of Access and Visibility Challenge in Cloud Incident Handling

5.3 Best Practices to Handle Cloud Incident

- 60% of the experts responded that their organizations use different cloud native logging and SIEM tools to handle cloud incidents, 25% said that their organizations do not use any tools, 15% responded that their organization might use some tools to handle cloud incidents (Table 19).

- Experts were asked for their suggestions regarding cloud incident handling. In response, experts suggested focusing on different important aspects of incident handling. Below given are some experts' suggestions.

  – Role defining and responsibility-sharing.

- Encourage the employees to gain skills in cloud environments and modern incident handling tools.
- Testing the deployments in the cloud before taking them to production.
- Employing skilled professionals to handle cloud incidents.

One of the experts believes that the cloud should not be treated differently from the on-premises environment.

21. Does your organization use any tool to handle cloud incidents?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	12	60.00%	60.00%	60.00%
No	5	25.00%	25.00%	85.00%
Maybe	3	15.00%	15.00%	100.00%
Total	20	100%		

Table 19. Tools Usage for Cloud Incident Handling

6. Hybrid Incident Response Framework

Based on the participated experts' responses, a suggested hybrid incident response framework is constructed. The suggested hybrid incident response framework would provide guidelines to handle incidents in the hybrid IT model. A hybrid IT model is a kind of IT technique in which an organization runs some of its services in an on-premises environment and some in the cloud environment [50]. Below given is the diagram of the hybrid incident response framework.

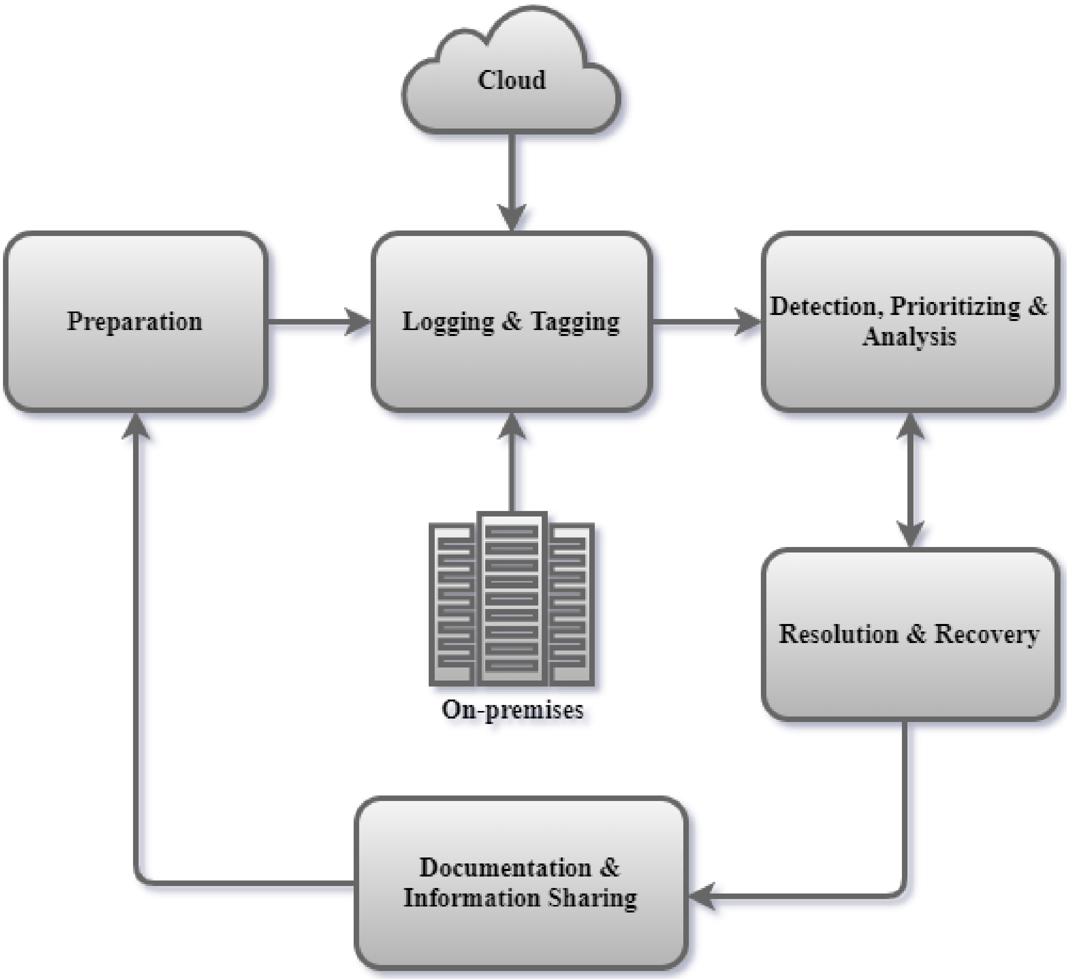

Cloud
Preparation
Logging & Tagging
Detection, Prioritizing & Analysis
On-premises
Resolution & Recovery
Documentation & Information Sharing

Figure 4. *Hybrid Incident Response Framework*

The hybrid incident response framework consists of five phases, and each phase is described below.

Preparation

The preparation phase is considered the most important phase of incident handling. A lack of proper preparation might result in failure to handle incidents. The preparation phase includes all tasks which are required to be completed before a possible incident. In a hybrid IT model, the preparation phase should include the following suggested steps to handle incidents properly:

- Ensure an updated incident handling plan always beforehand
- Ensure to have proper access to the required tools and resources, and follow the least privilege principle
- Maintain a collaboration tool for communication within the organization
- Maintain a 24x7 hierarchical communication within the organization
- Maintain a mailing list to keep the staff informed
- Maintain a list of allowed software and tools and an application form to apply for approval before installation of external applications
- Ensure the responsible parties have an understanding of the cloud SLA, response time and other support
- Train staff with realistic incident simulations and table-top exercises
- Perform simulations to test incident monitoring response tools

Logging & Tagging

Logging plays an important role in incident handling. Without efficient logging, it is impossible to troubleshoot system and application errors and respond to security incidents. In hybrid infrastructure, logging is not straightforward as logs are being collected from multiple resources. Incident responders need to identify the log sources. The logging and identifying the phase of incident handling should have the following suggested steps:

- Use advanced log collection and aggregation tools that support both cloud and on-premises

- Main a central dashboard to simplify the logging process as maintaining multiple dashboards can be challenging and time-consuming.

- Use log tagging to identify the log sources as there are multiple log sources both in the cloud and on-premises

- Use scalable centralized storage to store the logs, preferably in the cloud storage

- As systems and applications continuously generate logs and all logs are not useful, configure logging tools to collect useful logs only.

- Use an advanced logging tool with an automated log parser to make the collected logs organized

Detection, Prioritization & Analysis

In this phase of incident handling, the SIEM detects and analyzes events from the tagged logs to check for suspicious behavior and activities. The event source can be identified from the cloud or the on-premises infrastructure from the tagged logs. Organizations face issues in this part of incident handling due to the inability to prioritize when multiple events are detected from multiple sources. The detection, prioritization, and analysis phase of the incident handling should be focused on the suggested steps:

- Maintain an automated alerting system to inform staff within the organization during an incident or possible incident

- Ensure the entire cloud and on-premises resources are under monitoring

- Continuously monitor security tools to identify any abnormal behavior

- Maintain a dashboard for data visualization that helps to identify suspicious activities by matching with standard activity patterns

- In case of multiple incidents, prioritize risks based on impact and urgency

- Figure out the possible data loss

- Use advanced SIEM system for data correlation and analytics

- Review security alerts for accuracy and discard false-positive events to ignore overwork

- Maintain a collaboration platform specifically for the incident responders team to document each process to keep track of performed actions after any detected incident

- Use tools and APIs for automating processes

Resolution & Recovery

After detection and analysis, the next step is the resolution and recovery phase of the incident handling. In this phase, the incident responders apply fixes to solve the problems that triggered the incident. The resolution and recovery phase should have the following suggested steps:

- Identify and isolate the affected system from the environment

- Identify the attack behavior and attack source

- Establish contact with the CSP if their managed resources are under attack

- According to GDPR, inform the affected party within 72 hours if there is any personal data breach [51]

- Clean up the affected system and reinstall the operating system and restore data from trustworthy backups

- Cloud offers flexibility in terms of rebuilding systems so the affected cloud resources can be recreated instantly

- Infected virtual machines in the cloud might disclose management console access, so it is wise to change master credentials and other lower-level credentials to avoid large scale attacks

- Wait and verify that the systems are functional and issues are resolved

Documentation & Information Sharing

After each incident, the last phase of incident handling is documentation and information sharing. Gathered experience during resolving incidents is shared in this phase. Below suggested steps should be included in the documentation and information sharing phase of incident handling:

- Incident responders should draft their actions during each incident and document them in this phase for future reference.
- Incident responders should share their experience and how they handle the incident with other security experts within the organizations
- Apply security initiatives to defend against attacks in the future
- Fine-tune the procedures and strategies to handle future incidents more efficiently
- Review the handled incident and measure the efficiency of the tools used in the detection, analysis, resolution phase and update if required
- Review and update the incident response plan accordingly and ensure preparedness for any upcoming security incidents

6.1 Hybrid Incident Response Framework Validation

An online survey was performed to validate the hybrid incident response framework. Experts from multiple organizations participated in the survey. Regarding the usefulness of the hybrid incident response framework, experts rated the framework on a scale of 1 to 5. 14.3% of the experts rated the hybrid incident response framework as a 5, 64.3% rated it as a 4, 14.3% rated it as a 3 and other 7.1% rated it as a 2 (Table 20). Experts expressed different opinions in feedback regarding improving the hybrid incident response framework. Below given are the suggestions from experts.

- The framework could be more elaborate, and some incident-specific steps could be added.
- The framework should show the cloud log sources.
- The steps could be as short as possible because it is not possible to keep track of

each step by heart

- This could be a generalized framework as responses to incidents depends on incident type

- Some parts of the preparation phase of the hybrid incident response should be excluded as those are organization-specific and policy-based.

1. On a scale of 1 to 5, how would you rate the usefulness of the framework?				
Ratings	Frequency	Percent	Valid Percent	Cumulative Percent
2	1	7.1%	7.1%	7.1%
3	2	14.3%	14.3%	21.4%
4	9	64.3%	64.3%	85.7%
5	2	14.3%	14.3%	100.00%
Total	14	100%		

Table 20. Hybrid Incident Response Framework Validation

7. Cloud Incident Handling: Suggested Best Practices

Incident handling plays a crucial role in the development, better performance, and uninterrupted operations of any organization. With proper incident handling strategies, an organization can mitigate security risks that can hamper their business and handle incidents faster and effectively. As organizations are moving their assets to the cloud computing environment, the existing on-premises incident handling practices are becoming unsuitable in most cases because of the shift to cloud architecture. With the shift from on-premises to cloud computing, some security responsibilities also shift from cloud service users to providers. According to (ISC)2 2021 Cloud Security Report, 96% of the surveyed cybersecurity professionals said public cloud security is a matter of moderate concern [52]. 39% of organizations mentioned a lack of qualified professionals, 34% said data security, and 32% mentioned compliance with laws and regulations is the major cloud adoption barrier [52]. As the cloud computing environment is a complex combination of systems, applications, and networks, organizations should follow the best practices to handle security incidents in the cloud and mitigate security risks. Below given are some recommendations to handle incidents in the cloud computing environment.

7.1 Cloud-oriented Incident Response Plan

Cloud is an expanding platform with immense speed, and with such expansion of cloud, the number of security incidents is also increasing. Incident responders also need to prepare themselves for incidents as incidents sometimes occur in an unclear manner. Security experts cannot predict every kind of security incident that an organization is going to face. Therefore, it is better to have a proper cloud-oriented incident response plan beforehand. Each step of the response to handle a security incident is properly documented. Having an adequate incident response plan helps quickly respond and remediate an incident. It also helps to communicate internally and externally and eliminates miscommunication during a security incident. The cloud incident response plan should be continuously updated after each security incident for improvement and learning. Having a well-documented and updated cloud-oriented incident response plan can help continuously improve the cloud environment's security. It is even better to automate the incident response with quick action. Many tools are available to automate the incident response plan for quick and easier identification and mitigation of security incidents.

7.2 Security Questions and Compliance Requirements

In addition to understanding the SLA, before subscribing to any CSP, organizations should keep some important security questions beforehand to ask the CSP and let the CSP know about the compliance requirements. SLA might not include the information organizations need to know, or there might be some information need-to-know basis, so it is always a good idea to question the CSPs. There are multiple data compliance standards that organizations need to follow. An organization should let the CSP know if they need to follow any compliance standards and ask the CSP about the compliance standards that the CSP is following. Below are some suggested points about which organization should ask questions to the CSP before subscribing to their services.

- Level of technical support
- Supported compliance standards
- List of data compliant resources
- Supported authentication methods
- Actions against security incidents
- Disaster recovery plan

7.3 Training and Team Preparation

Successful handling of a security incident depends on proper teamwork. With sufficient training and team preparation, large-scale security incidents in the cloud computing environment can be remediated. Due to less visibility of resources, distributed nature of the data in the cloud, and inadequate training and knowledge about the cloud architecture and modern tools and techniques, it is not very easy to detect and handle security incidents in the cloud environment in some cases. An organization that is using the cloud environment should prepare a team with cloud incident response training. So that it can successfully detect incidents, identify the sources of incidents, perform analysis, gain knowledge and skills from incidents to develop and update the incident handling strategy to respond better in the future, and continuously develop and test the security of the cloud environment.

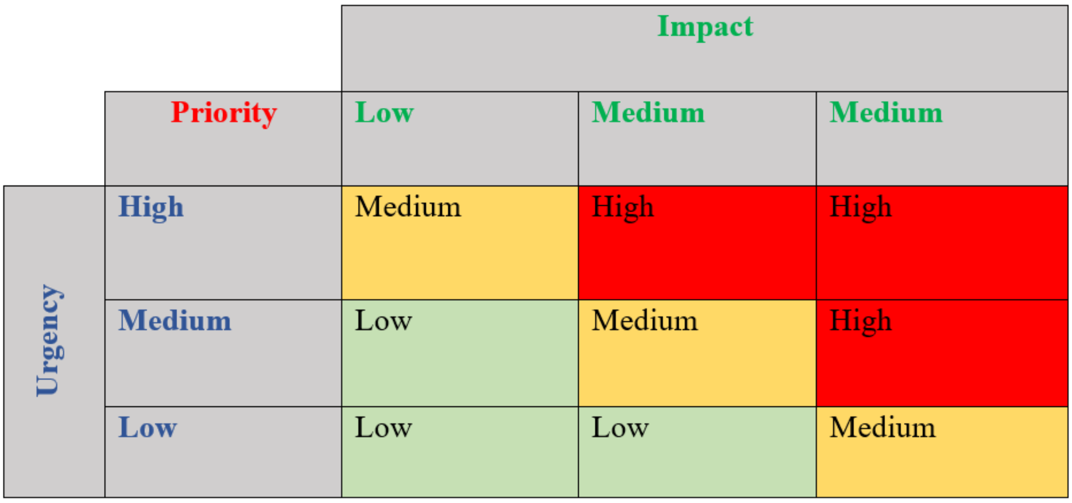
Organizations can offer cloud-oriented table-top exercises and realistic simulations of incidents to train their security experts.

7.4 Roles and Responsibility Assignment

According to Atlassian, their incident response strategy includes several roles, and each role has primary and secondary responsibilities [53]. Atlassian incident response team has an Incident Manager, a Tech lead, a Communication Manager, a Support Team Lead, a Subject Matter Expert, a Social Media Lead, Scribe and a Problem Manager. [53]. The incident Manager leads the incident response team, and the Tech Lead with advanced technical knowledge and acts as a primary incident responder [53]. The communication Manager maintains public communication during incidents, and the Support Team Lead handles customers complaint tickets and calls and responds to those promptly [53]. The Subject Matter Expert deals with the services or systems that are experiencing the incidents, and the Social Media Lead maintains communication through social media platforms during an incident [53]. The Scribe documents important information during an incident, and the Problem Manager performs incident root cause analysis [53]. Roles and responsibilities assignments play an important in handling large-scale incidents. Sometimes incidents occur in an unclear manner. In such cases, incident response team members should be responsible for responding across various stages of an incident. Cross-organizational communication between cloud service users and providers is essential during an incident, and information sharing also plays a significant role in cloud incident handling.

7.5 End-point Security

With the security of the cloud, securing endpoint devices play an important role in incident handling. Insecure endpoint devices may lead to major security incidents. Nowadays, IaC tools like Terraform and Ansible are used by organizations to create cloud resources and applications and scale them accordingly. IaC tools are used for recreation and provisioning of resources. IaC tools, scripts, and cloud credentials are generally saved in endpoint devices. Insecure endpoints may cause loss of access to cloud credentials, resources, and applications. It is essential to secure endpoint devices. There are several endpoint detection and response (EDR) tools available that can be used to secure endpoint devices from threats.



		Impact		
	Priority	Low	Medium	Medium
Urgency	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Figure 5. *Impact, Urgency and Priority Matrix [54]*

7.6 Risk Prioritization

Cloud consists of an enormous infrastructure of resources. Getting continuous and numerous alerts is common in large infrastructure. To respond appropriately to the alerts, the incident response team should prioritize the level of risk and assess the impact. Security risks are prioritized based on the urgency and impact of the risks. When multiple incidents occur, there is no time for evaluating and prioritizing a certain incident. It is important to know the priority of resources and the level of severity before an incident occurs so that security experts can take immediate action after an incident occurs. The measures should be based on the assessed impact risk priority when an incident occurs. Impact assessment and risk prioritization are done by continuously monitoring the system and based on risk mitigation time and process. Organizations can also prioritize risk using the impact, urgency, and priority matrix [54].

7.7 Access to Required Resources

Access management in the cloud computing environment is different from an on-premises environment. In an on-premises environment, an organization can access any resources in the infrastructure, but the organizations in the cloud environment can access only specific resources. Access to cloud environments and resources related to the incident is necessary to handle an incident. Incident response teams should have appropriate access to perform their task before an event occurs or during an event. Depending on the tasks the team members are performing, the level of access should be granted accordingly, and it should be provisioned in advance. Access to specialists should be limited to performing the required tasks only. Otherwise, misconfigured access might lead to security vulnerabilities.

Especially in the public cloud computing module, multiple tenants use the same resources. Improper security configurations and identity and access management can cause data breaches and data loss. Identity and access management should be strictly requirement-based.

7.8 Secure Application Programming Interface (API)

APIs connect the web application front-end with back-end features to deliver user requests to the web application and send web application responses back to the user. When a resource is created from a console or command-line interface in the cloud computing environment, APIs set up a communication channel between the front-end and back-end to provide the desired response to the end-user. However, insecure APIs can lead to vulnerable communication channels between the front-end and back-end, and attackers can gain access to the application back-end through insecure APIs [29]. APIs should be secure with proper authentication and authorization mechanisms before publishing. Penetration testing should be carried out to ensure that attacks cannot disrupt the API end-points functionalities [29].

7.9 Usage of Advanced Tools & Logging

Due to the large volume [2] and distributed nature [1] of data in the cloud, data collection and analysis are complex tasks. CSP provides a set of tools and APIs that help automate incident response processes. Using these APIs and tools, it is possible to automate data protection, network security, identity and access management, and monitoring facilities. CSPs offer tools that use statistical analysis and machine learning to analyze data. Many paid tools in the market can be used for data analysis. Logging also plays a vital role in incident handling. In the on-premises environment, logging is straightforward due to having access to all the resources, but it requires logging tools in the cloud. Depending on the price, CSPs offer various logging facilities, from basic logging to full detailed audit logging. There are also open-source and paid advanced log collection and aggregation tools available in the market that can be used for logging. These logs should be saved to alternative cloud storage or remote storage while keeping the integrity of the logs protected. There should be a shared platform for improved communication among teams during incidents as well.

8. Limitations & Future Work

8.1 Limitations

During the research, there were some limitations. Data collection through the online survey was time-consuming, and there were a limited number of respondents as people tend to avoid online surveys. For that reason, the result is generalized based on 20 respondents from different organizations worldwide. Data collection would be more fruitful if collected through a face-to-face interview. Due to the Covid-19 situation, data collection through a face-to-face interview was not possible. People tended to avoid meetings, and for that reason, data was collected through an online survey.

8.2 Future Work

Different ideas could be used to develop the research in the future. Future work regarding the research concerns the following:

- Data collection through interviews with a larger number of respondents
- A deeper analysis of currently used incident handling frameworks and their usefulness in cloud incident handling
- Determine more challenges in incident handling faced by experts
- Construction of a more detailed hybrid incident response framework
- Construction of a hybrid IT environment and to test the suggested incident response framework
- Identify and suggest some more best practices in incident handling that could be useful for organizations with hybrid IT infrastructure

9. Conclusion

With the emerging cloud computing market, organizations are switching from the on-premises environment to the cloud computing environment. Cloud computing offers advanced facilities like ease-of-use, low-cost, on-demand self-service, pay-per-use, multi-tenancy, location and device independence, web-based control and interfaces. Because of such facilities, organizations are shifting their on-premises resources to the cloud environment. However, still, there are some challenges many organizations face using the cloud environment compared to on-premises. There are several pieces of research on cloud computing challenges, cloud incident handling and digital forensic investigations. This research aimed to identify the difference between cloud and on-premises incident handling, the current challenges in handling incidents in the cloud environment, and if that can be handled with conventional incident handling plans and suggest the best practices to handle incidents in the cloud. The research focused on the importance of sharing security responsibilities between CSP and CSU and pointed out major cloud data breaches. Experts from various organizations worldwide were surveyed to find their opinion regarding incident handling in the cloud. From analyzing the survey data, it was found that experts from most organizations believe that handling incidents in the cloud environment are challenging. Handling incidents in the cloud requires different skillsets and knowledge of the cloud and modern incident handling tools. The survey also shows that most experts think that there are differences between cloud and on-premises incident handling. Most experts also believe that cloud incident handling is trickier due to less visibility and access to resources and events, lack of understanding of the cloud infrastructure, and shift of security responsibilities between CSPs and CSUs. Finally, some best practices and a hybrid incident response framework are suggested for organizations with resources on both cloud and on-premises. Experts in cloud computing validated the efficiency of the hybrid incident response framework and provided some suggestions regarding improving the framework. Handling incidents in the hybrid IT environment has different complexities. SMEs sometimes have limited capacity to run their services and resources in an on-premises environment as maintenance is costly, but security is a major concern. To minimize the cost of having an on-premises infrastructure SMEs run their services in a hybrid IT environment. Such organizations could have proper guidelines for handling security incidents in the hybrid IT environment following the suggested best practices and the hybrid incident response framework.

Bibliography

[1] Ben Martini and Kim-Kwang Raymond Choo. “An integrated conceptual digital forensic framework for cloud computing”. In: *Digital Investigation* 9.2 (2012), pp. 71–80. ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2012.07.001. URL: https://www.sciencedirect.com/science/article/pii/S174228761200059X.

[2] Rich Mogull et al. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Tech. rep. (Accessed on May 12, 2021). July 2017. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.

[3] Peter Mell and Timothy Grance. *The NIST Definition of Cloud Computing*. Tech. rep. U.S. Department of Commerce, Sept. 2011. DOI: 10.6028/nist.sp.800-145.

[4] Bernd Grobauer, Tobias Walloschek, and Elmar Stocker. “Understanding Cloud Computing Vulnerabilities”. In: *IEEE Security & Privacy* 9.2 (2011), pp. 50–57. DOI: 10.1109/MSP.2010.115.

[5] Paul Cichonski et al. *Computer Security Incident Handling Guide*. Tech. rep. U.S. Department of Commerce, Aug. 2012. DOI: 10.6028/nist.sp.800-61r2.

[6] Bernd Grobauer and Thomas Schreck. “Towards Incident Handling in the Cloud: Challenges and Approaches”. In: *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*. CCSW ’10. Chicago, Illinois, USA: Association for Computing Machinery, 2010, pp. 77–86. ISBN: 9781450300896. DOI: 10.1145/1866835.1866850. URL: https://doi.org/10.1145/1866835.1866850.

[7] Nurul Hidayah Ab Rahman and Kim-Kwang Raymond Choo. “A survey of information security incident handling in the cloud”. In: *Computers & Security* 49 (2015), pp. 45–69. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2014.11.006. URL: https://www.sciencedirect.com/science/article/pii/S0167404814001680.

[8] Martin Gilje Jaatun and Inger Anne Tøndel. “How Much Cloud Can You Handle?” In: *2015 10th International Conference on Availability, Reliability and Security*. 2015, pp. 467–473. DOI: 10.1109/ARES.2015.38.

[9] Victor Ion Munteanu et al. "Cloud Incident Management, Challenges, Research Directions, and Architectural Approach". In: *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*. 2014, pp. 786–791. DOI: 10.1109/UCC.2014.128.

[10] Chitranshu Raj, Lavanya Khular, and Gaurav Raj. "Clustering Based Incident Handling For Anomaly Detection in Cloud Infrastructures". In: *2020 10th International Conference on Cloud Computing, Data Science Engineering (Confluence)*. 2020, pp. 611–616. DOI: 10.1109/Confluence47617.2020.9058314.

[11] Nurul Hidayah Ab Rahman and Kim-Kwang Raymond Choo. *Factors Influencing the Adoption of Cloud Incident Handling Strategy: A Preliminary Study in Malaysia*. 2015. arXiv: 1505.02908 [cs.CY].

[12] Alexander Adamov and Anders Carlsson. "Cloud incident response model". In: *2016 IEEE East-West Design Test Symposium (EWDTS)*. 2016, pp. 1–3. DOI: 10.1109/EWDTS.2016.7807665.

[13] Rajeev Gupta et al. "Multi-dimensional Knowledge Integration for Efficient Incident Management in a Services Cloud". In: *2009 IEEE International Conference on Services Computing*. 2009, pp. 57–64. DOI: 10.1109/SCC.2009.48.

[14] Bksp Kumar Raju and G. Geethakumari. "A Novel Approach for Incident Response in Cloud Using Forensics". In: *Proceedings of the 7th ACM India Computing Conference*. COMPUTE '14. Nagpur, India: Association for Computing Machinery, 2014. ISBN: 9781605588148. DOI: 10.1145/2675744.2675766. URL: https://doi.org/10.1145/2675744.2675766.

[15] Paul Henry, Jacob Williams, and Benjamin Wright. *The SANS Survey of Digital Forensics and Incident Response*. Tech. rep. (Accessed on June 26, 2021). July 2013. URL: https://leonardarueyingho.com/wp-content/uploads/2019/10/Forensic-201.pdf.

[16] Peter Mell and Timothy Grance. *NIST Cloud Computing Forensic Science Challenges*. Tech. rep. (Accessed on June 29, 2021). U.S. Department of Commerce, June 2014. URL: https://csrc.nist.gov/CSRC/media/Publications/nistir/8006/draft/documents/draft_nistir_8006.pdf.

[17] Ameer Pichan, Mihai Lazarescu, and Sie Teng Soh. "Towards a practical cloud forensics logging framework". In: *Journal of Information Security and Applications* 42 (2018), pp. 18–28. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2018.07.008. URL: https://www.sciencedirect.com/science/article/pii/S2214212617305203.

[18] Nurul Hidayah Ab Rahman, Niken Dwi Wahyu Cahyani, and Kim-Kwang Raymond Choo. “Cloud incident handling and forensic-by-design: cloud storage as a case study”. In: *Concurrency and Computation: Practice and Experience* 29.14 (2017). e3868 CPE-16-0076.R1, e3868. DOI: https://doi.org/10.1002/cpe.3868. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.3868. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.3868.

[19] Alecsandru Pătraşcu and Victor-Valeriu Patriciu. “Beyond digital forensics. A cloud computing perspective over incident response and reporting”. In: *2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. 2013, pp. 455–460. DOI: 10.1109/SACI.2013.6609018.

[20] Dominik Birk and Christoph Wegener. “Technical Issues of Forensic Investigations in Cloud Computing Environments”. In: *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*. 2011, pp. 1–10. DOI: 10.1109/SADFE.2011.17.

[21] Guangxuan Chen et al. “Suggestions to digital forensics in Cloud computing ERA”. In: *2012 3rd IEEE International Conference on Network Infrastructure and Digital Content*. 2012, pp. 540–544. DOI: 10.1109/ICNIDC.2012.6418812.

[22] Shams Zawoad and Ragib Hasan. “Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems”. In: *CoRR* abs/1302.6312 (2013). arXiv: 1302.6312. URL: http://arxiv.org/abs/1302.6312.

[23] Stavros Simou et al. “A survey on cloud forensics challenges and solutions”. In: *Security and Communication Networks* 9.18 (2016), pp. 6285–6314. DOI: https://doi.org/10.1002/sec.1688. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.1688. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1688.

[24] Dave Shackleford. *Orchestrating Security in the Cloud*. Tech. rep. (Accessed on June 29, 2021). Sept. 2015. URL: https://pages.cloudpassage.com/rs/857-FXQ-213/images/sans-survey-orchestrating-security-in-the-cloud.pdf.

[25] Nurul Hidayah Ab Rahman and Kim-Kwang Raymond Choo. “Integrating digital forensic practices in cloud incident handling”. In: *The Cloud Security Ecosystem*. Elsevier Science, 2015. Chap. 17. ISBN: 978-0-12-801595-7.

[26] Oracle and KPMG. *Oracle and KPMG Cloud Threat Report*. Tech. rep. (Accessed on June 26, 2021). 2018. URL: https://www.oracle.com/us/dm/oraclekpmgcloudthreatreport2018-4437566.pdf.

[27] Jon-Michael C. Brook et al. *Top Threats to Cloud Computing: Egregious Eleven*. Tech. rep. (Accessed on July 2, 2021). Aug. 2019. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven.

[28] Suhas Bhat et al. *Top Threats to Cloud Computing: Egregious Eleven Deep Drive*. Tech. rep. (Accessed on July 2, 2021). Sept. 2020. URL: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/.

[29] Cypress Data Defense. *7 Cloud Computing Security Vulnerabilities and What to Do About Them*. (Accessed on July 3, 2021). July 2020. URL: https://towardsdatascience.com/7-cloud-computing-security-vulnerabilities-and-what-to-do-about-them-e061bbe0faee.

[30] National Security Agency. *Mitigating Cloud Vulnerabilities*. Tech. rep. (Accessed on July 8, 2021). Jan. 2020. URL: https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF.

[31] Alex Siow and Soon Tein Lim. *Cloud Incident Response Framework*. Tech. rep. (Accessed on July 3, 2021). Apr. 2021. URL: https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/.

[32] Amazon Web Services (AWS). *AWS Shared Responsibility Model*. (Accessed on September 21, 2021). URL: https://aws.amazon.com/compliance/shared-responsibility-model/.

[33] TerryLanfear. *Shared responsibility in the cloud*. (Accessed on September 21, 2021). URL: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.

[34] McAfee Cloud BU. *Are you Well-Architected?* (Accessed on September 21, 2021). URL: https://www.mcafee.com/blogs/enterprise/cloud-security/are-you-well-architected/.

[35] CloudPassage. *Shared Responsibility Model Explained*. (Accessed on September 21, 2021). URL: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/.

[36] Christian Frøystad, Inger Anne Tøndel, and Martin Gilje Jaatun. “Security Incident Information Exchange for Cloud Service Provisioning Chains”. In: *Cryptography* 2.4 (2018). ISSN: 2410-387X. URL: https://www.mdpi.com/2410-387X/2/4/41.

[37] Matthias Gander et al. "Anomaly Detection in the Cloud: Detecting Security Incidents via Machine Learning". In: *Trustworthy Eternal Systems via Evolving Software, Data and Knowledge*. Ed. by Alessandro Moschitti and Barbara Plank. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 103–116. ISBN: 978-3-642-45260-4.

[38] Amazon Web Services (AWS). *Amazon EC2 Auto Scaling*. (Accessed on June 24, 2021). URL: `https://aws.amazon.com/ec2/autoscaling/`.

[39] Hybrid Cloud Working Group. *Hybrid Clouds and Its Associated Risks*. Tech. rep. (Accessed on June 30, 2021). July 2020. URL: `https://cloudsecurityalliance.org/artifacts/hybrid-clouds-and-its-associated-risks/`.

[40] John Yeoh and Hillary Baron. *Identity Security*. Tech. rep. (Accessed on July 2, 2021). Apr. 2016. URL: `https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/`.

[41] Lily Hay Newman. *Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency*. (Accessed on July 14, 2021). Feb. 2018. URL: `https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/`.

[42] Casey Crane. *Re-Hash: The Largest DDoS Attacks in History*. (Accessed on August 19, 2021). June 2020. URL: `https://www.thesslstore.com/blog/largest-ddos-attack-in-history/`.

[43] *Splunk for Infrastructure Monitoring and Troubleshooting*. (Accessed on August 22, 2021). 2020. URL: `https://www.splunk.com/pdfs/solution-guides/splunk-for-infrastructure-monitoring-and-troubleshooting.pdf`.

[44] *Dynatrace Infrasturcture Monitoring*. (Accessed on September 15, 2021). URL: `https://www.dynatrace.com/platform/infrastructure-monitoring/`.

[45] *SolarWinds Orion Platform*. (Accessed on September 19, 2021). URL: `https://www.solarwinds.com/orion-platform`.

[46] *Wazuh*. (Accessed on September 19, 2021). URL: `https://wazuh.com/`.

[47] *ManageEngine EventLog Analyzer*. (Accessed on September 20, 2021). URL: `https://www.manageengine.com/products/eventlog/`.

[48] *GNU PSPP*. (Accessed on September 29, 2021). URL: `https://www.gnu.org/software/pspp/`.

[49] *Diagrams.net*. (Accessed on October 12, 2021). URL: `https://app.diagrams.net/`.

[50] Techopedia. *Hybrid IT*. (Accessed on September 22, 2021). URL: `https://www.techopedia.com/definition/26637/hybrid-it`.

[51] European Union (EU). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016*. (Accessed on September 26, 2021). 2016. URL: `https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng`.

[52] (ISC)2. *2021 Cloud Security Report*. Tech. rep. 2021. URL: `https://www.isc2.org/Landing/cloud-security-report#`.

[53] Atlassian. *Understanding the key incident response roles and responsibilities*. (Accessed on September 27, 2021). URL: `https://www.atlassian.com/incident-management/incident-response/roles-responsibilities`.

[54] Joseph Mathenge. *Impact, Urgency & Priority: Understanding the Matrix*. (Accessed on September 27, 2021). URL: `https://www.bmc.com/blogs/impact-urgency-priority/`.

Appendices

Appendix 1 - Online Survey Questionnaire 1

CLOUD INCIDENT HANDLING: CHALLENGES AND BEST PRACTICES

PROCESSING OF PERSONAL DATA

In accordance with Tallinn University of Technology Privacy Policy (https://taltech.ee/en/privacy-policy), any Personally-Identifiable Data (PID) collected during the survey is used to achieve the determined objective and collected data will not be saved or shared.

The purpose of the questionnaire is to collect data from Cloud Computing Professionals and Security Expert regarding incident handling in the cloud environment. Data is collected for my thesis work with the topic named "Cloud Incident Handling: Challenges and Best Practices".

Position:

Type of Organization:

Number of Employees:

Average Turnover:

Country of Operations:

1. What type of infrastructure do your organization use?

- On-premises
- Cloud
- Hybrid (Combination of Cloud and on-premises infrastructure)

2. Is there any difference between handling incidents on on-premises and handling incidents in the cloud?

- Yes
- No
- Maybe

3. If yes/maybe, what is the biggest difference between handling incidents in on-premises and handling incidents in the cloud?

4. Regarding handling incidents, are there any advantages of using cloud?

- Yes
- No
- Maybe

5. According to your selected answer from question no. 4, why do you think so?

6. Regarding handling incidents, are there any disadvantages of using cloud?

- Yes
- No
- Maybe

7. According to your selected answer from question no. 6, why do you think so?

8. How do your organization handle cloud incidents?

- In-house (Cloud Engineer/Security Experts)
- Outsourced
- Other

9. Do you think handling incidents in the cloud requires different skillsets?

- Yes
- No
- Maybe

Incident Handling in the Cloud

10. On a scale of 1 to 5, How will you rate organization considering the preparation phase when it comes to incidents?

- 1
- 2
- 3
- 4
- 5

11. On a scale of 1 to 5, How will you rate organization considering the detection & analysis phase if the concerns incidents? (1 = Dissatisfied, 5 = Satisfied)

- 1
- 2
- 3
- 4
- 5

12. On a scale of 1 to 5, How will you rate organization considering the containment, eradication & recovery phase when it comes to incidents? (1 = Dissatisfied, 5 = Satisfied)

- 1
- 2
- 3
- 4
- 5

13. On a scale of 1 to 5, How will you rate organization considering the post-incident activity phase if the concerns incidents? (1 = Dissatisfied, 5 = Satisfied)

- 1
- 2
- 3
- 4
- 5

14. Does your organization use any specific framework or model to handle cloud incidents?

- ■ Yes
- ■ No
- ■ Maybe

15. Do you think currently used incident handling framework are efficient for both cloud and on-premises environment?

- ■ Yes
- ■ No
- ■ Maybe

16. If no, do you wish to get a hybrid framework that will provide guideline for handling incident in the cloud and on-premises environment?

- ■ Yes
- ■ No
- ■ Maybe

Challenges in Cloud Incident Handling

17. Study claims that handling incidents in the cloud is trickier because it requires skillsets to identify the data sources. Do you agree with the statement?

- ■ Yes
- ■ No
- ■ Maybe

18. According to study, due to the distributed nature of data across multiple systems or jurisdictions data analysis is challenging in the cloud. Do you agree with the statement?

- ■ Yes
- ■ No
- ■ Maybe

19. Due to shift in security responsibility between cloud service provider and cloud service user depending on chosen service model and provider, cloud service users have lack of understanding of security responsibilities. Do you agree with the statement?

- ■ Yes
- ■ No
- ■ Maybe

20. Lack of access and visibility to cloud service provider managed resources make it harder for cloud service users to handle security incident in the cloud. Do you agree with the statement?

- ■ Yes
- ■ No
- ■ Maybe

Best Practices to Handle Cloud Incident

21. Does you organization use any tool to handle cloud incidents?

- ■ Yes
- ■ No
- ■ Maybe

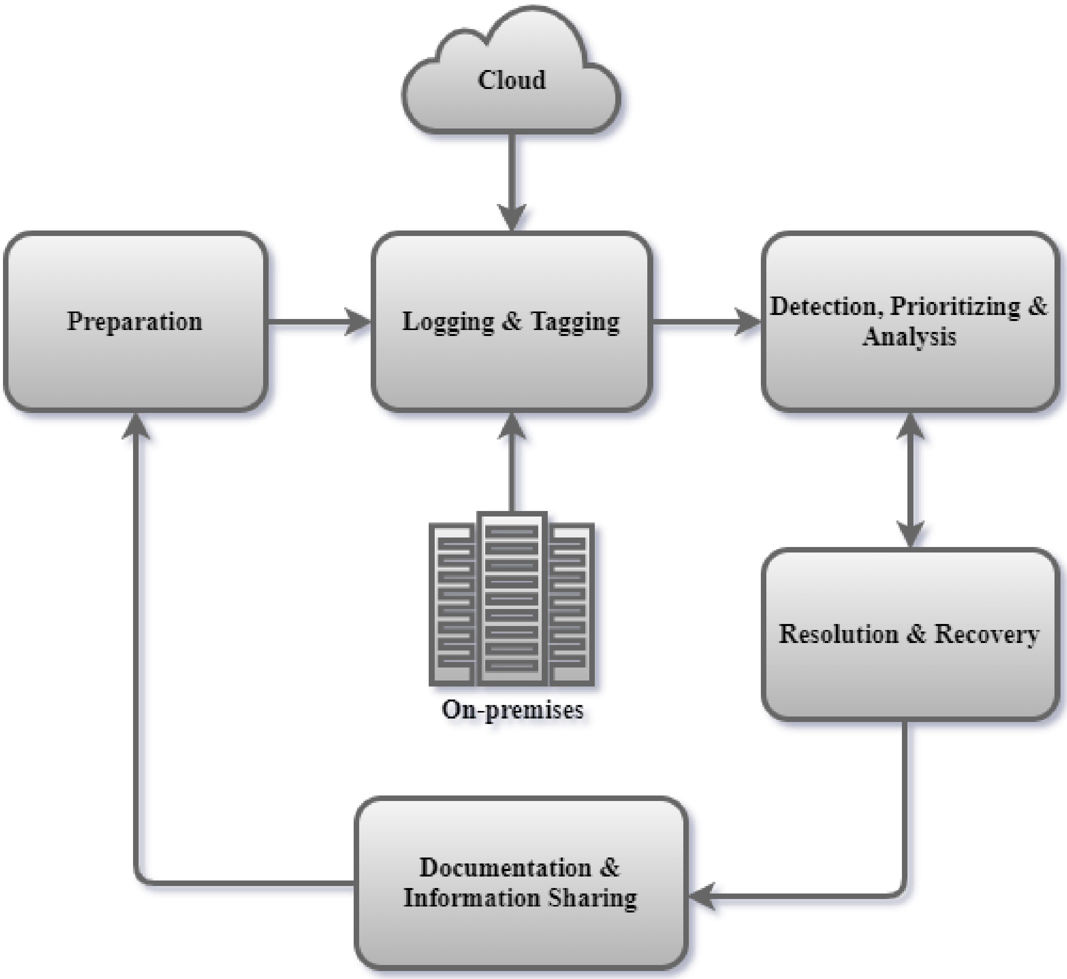
22. If yes, which tool does your organization use?

23. Do you have any suggestion regarding handling incidents in the cloud?

Appendix 2 - Online Survey Questionnaire 2

Hybrid Incident Response Framework Validation

The purpose of the questionnaire is to validate my research and the hybrid incident response framework. The hybrid incident response framework was constructed based on the responses from the experts who participated in my thesis survey (https://survey.system-ctl.net/).


Cloud
Preparation
Logging & Tagging
Detection, Prioritizing & Analysis
On-premises
Resolution & Recovery
Documentation & Information Sharing

The Hybrid IR framework consists of 5 phases of suggested incident response procedure for both cloud and on-premises environment. The phases included in the framework are Preparation, Logging & Tagging, Detection, Prioritizing & Analysis, Result & Recovery and finally Documentation & Information Sharing. For detailed description of each step, please visit: https://survey.system-ctl.net/hirf.html

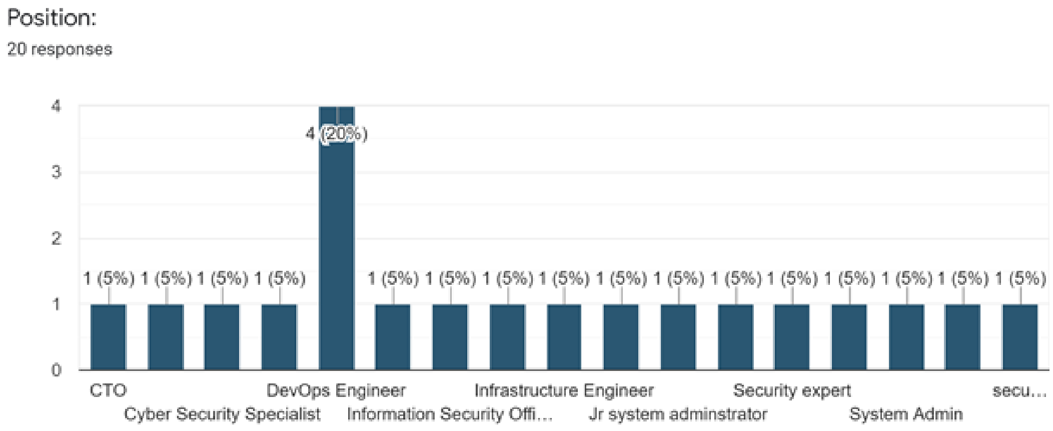
1. On a scale of 1 to 5, how would you rate the usefulness of the framework? (1 = Not useful, 5 = Very useful)

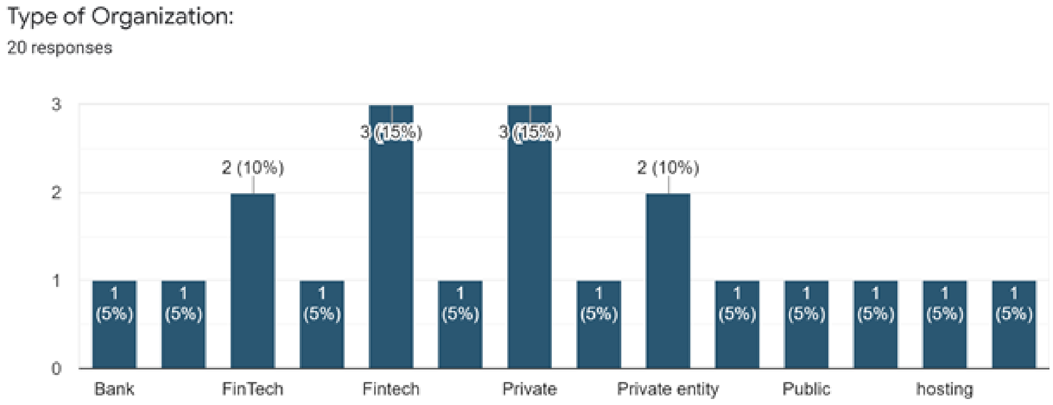
- 1
- 2
- 3
- 4
- 5

2. Do you have any suggestions regarding improvement of the framework?

Appendix 3 - Online Survey Questionnaire 1 Responses

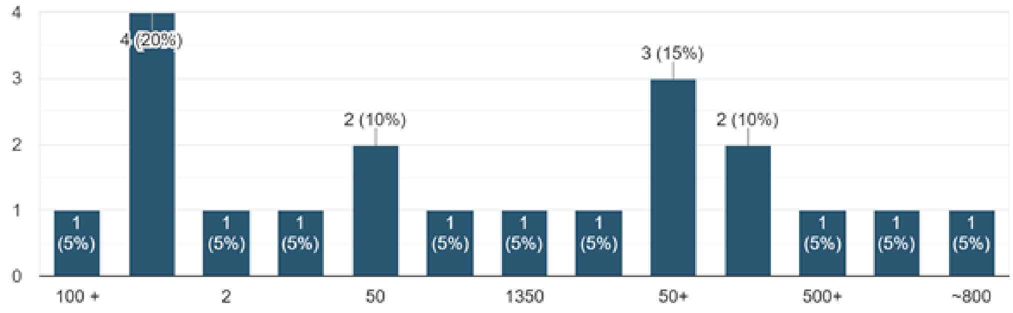
Cloud Incident Handling: Challenges and Best Practices Questionnaire Responses





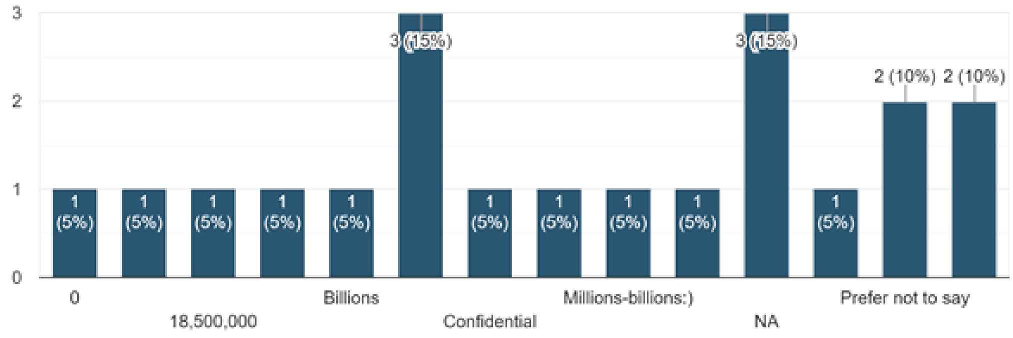
Number of Employees

20 responses



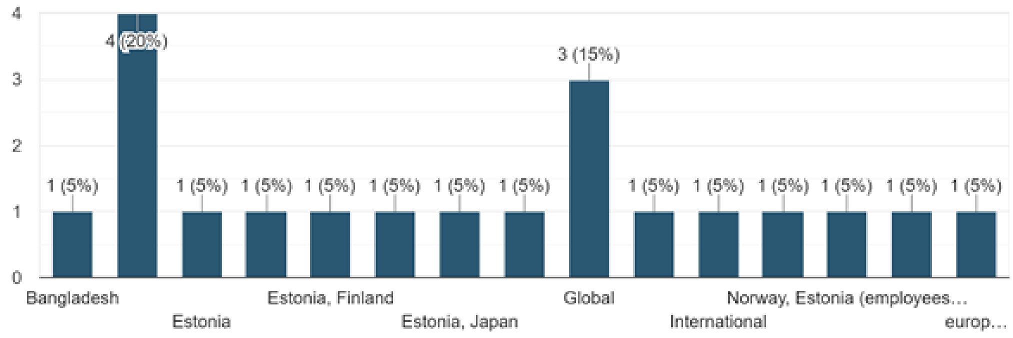
Average Turnover

20 responses



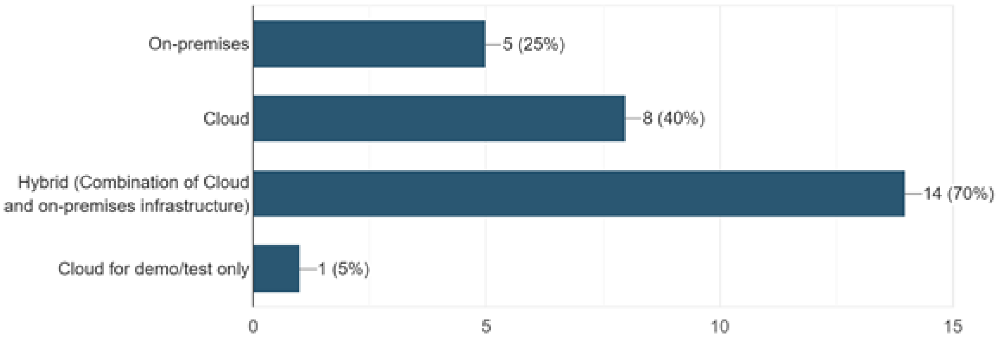
Country of Operations

20 responses



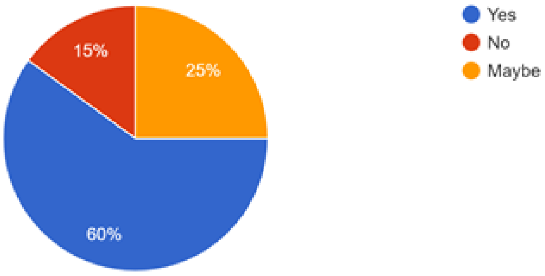
1. What type of infrastructure do your organization use?

20 responses



2. Is there any difference between handling incidents on on-premises and handling incidents in the cloud?

20 responses



3. If yes/maybe, what is the biggest difference between handling incidents in on-premises and handling incidents in the cloud?

1. Less things to take care of in the cloud

2. 1)The level of relevant details (logs). 2)cloud platforms are normally outsourced. So there is another organisation/component you need to secure. It comes down the outsourcing contracts and in practice you don’t control the vendor solutions. 3)you HOPE that the service provider informs you if shit hits the fan in the cloud and impacts your data/systems.

3. cloud - is third party provided thing

4. Requires more skills

5. Less tasks

6. In the cloud you are not responsible for lower layers.

7. No idea

8. No

9. On-premise activity has more risk categories (physical access, etc.)

10. Less security task for company’s security experts

11. Less responsibility

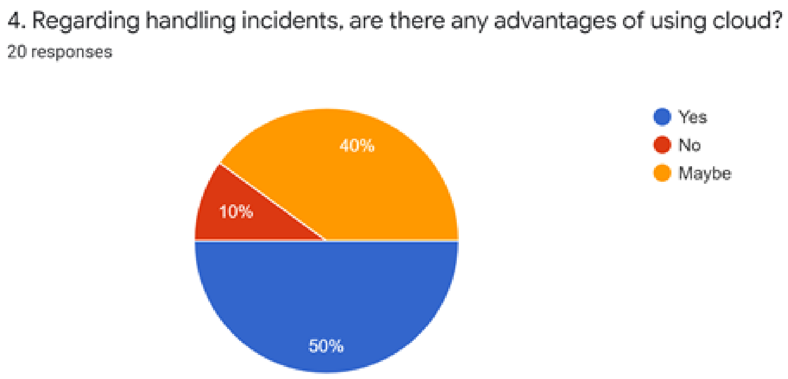
12. Incident responders

13. Less incident handling opportunity

14. Accessibility and visibility

15. Cloud requires more skills

16. As part of shared responsibility model, it might be responsibility of provider



4. Regarding handling incidents, are there any advantages of using cloud?

20 responses

5. According to your selected answer from question no. 4, why do you think so?

1. Less possibilities of system or system failures

2. using more processing power

3. shit happens, you can point the fingers to others and may not loose your job:)

4. no problems with hardware, outsourcing

5. Lack of level of access to resources

6. Cloud is the best since electricity

7. not very familair with incident handling in cloud, so can not say yes or not with certainty

8. Retrieving data or logs can be simpler.

9. Less task, less things to handle

10. You have to take care about only those services which you can manage. Cloud provider is also monitoring which is a good thing.

11. because some incidents can be outsourced to the cloud provider

12. Cloud requires hiring of smart hand

13. IFF cloud service is excluded from risk scope, then scope is smaller

14. Same as ans no. 3

15. Less tasks

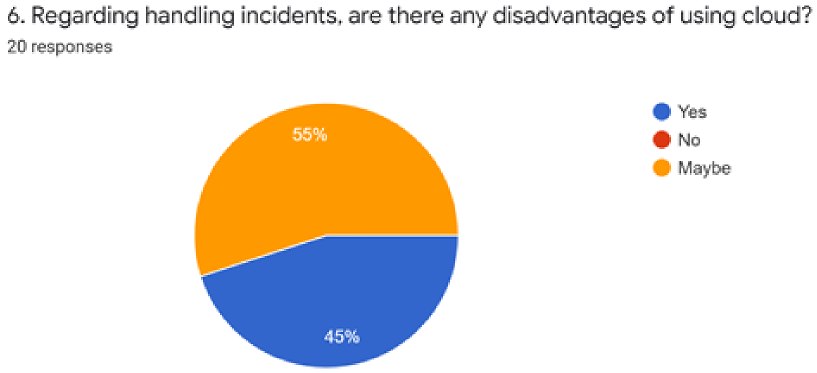
16. Cloud providers have more capabilities and resources to deal with the incident.

17. Less hassle

18. In some cases, incident handling is bit tougher in the cloud.

19. Less responsibilities

20. Providers have their own SOC teams, highly mature and professional



6. Regarding handling incidents, are there any disadvantages of using cloud?

20 responses

7. According to your selected answer from question no. 6, why do you think so?

1. Less clarity about incidents

2. might be security issue

3. Check answer no 3

4. lower possibilites, outsourcing

5. Less visibility to the incidents

6. Not sure

7. same as question 5. But I guess cloud may make it more complicated due their distributed nature

8. Depending on the contractual terms aside, I might need to involve additional parties in the incident management (cloud provider, expert, etc).

9. Lack of rights to get deep view of an incident

10. Again, you don't have access to all layers.

11. For some incidents you have to rely on the cloud provider

12. Cloud requires hiring of smart hand

13. More parties involved and less transparency

14. No detalied information about any incident

15. Less visibility to incidents

16. Depends who the cloud provider is. A 'small' provider might have a point of contact but not necessarily a quick response.

17. Limited incident handling opportunity for experts

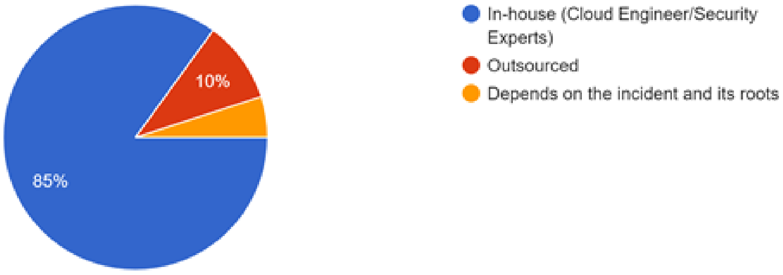
18. Lack of access and visibility

19. More dependency on service provider and may not have the proper view to an incident

20. Depending on communication and incident nature, it is unlikely you will get a priority in handling your case. Also, with shared model you don't see whole picture in real time

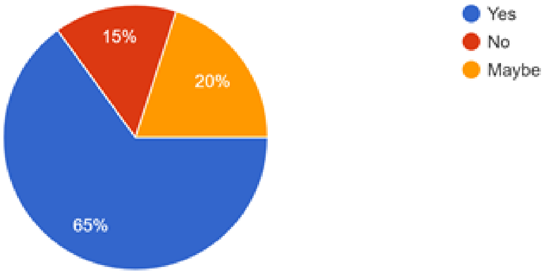
8. How do your organization handle cloud incidents?

20 responses



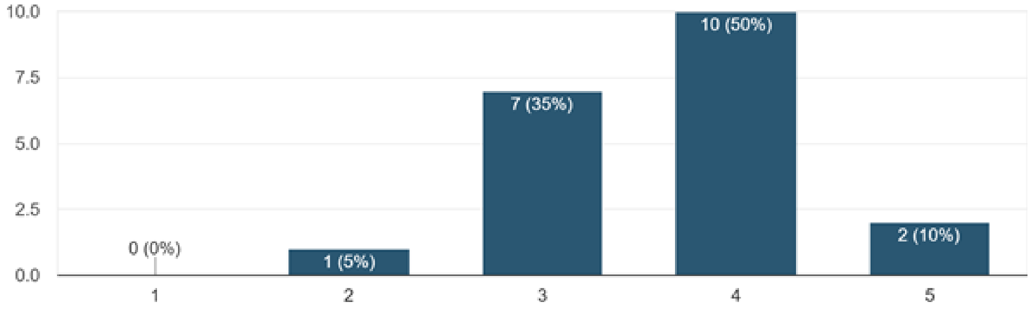
9. Do you think handling incidents in the cloud requires different skillsets?

20 responses



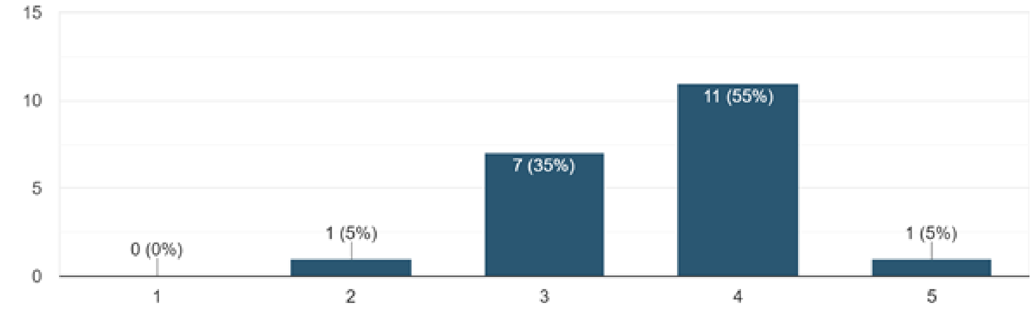
10. On a scale of 1 to 5, How will you rate organization considering the preparation phase when it comes to incidents?

20 responses



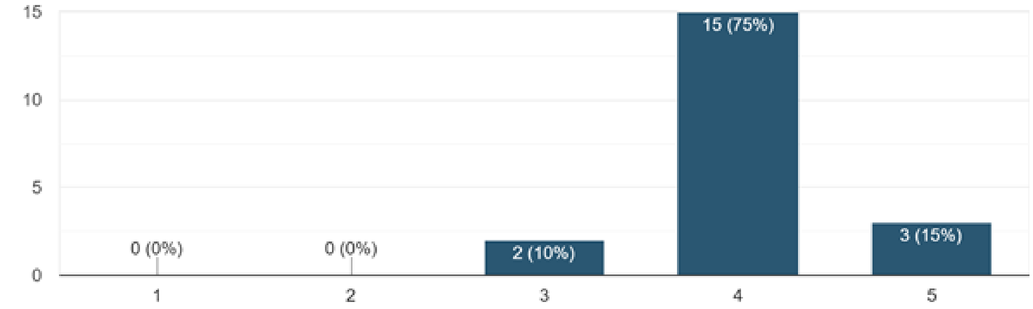
11. On a scale of 1 to 5, How will you rate organization considering the detection & analysis phase if the concerns incidents?

20 responses



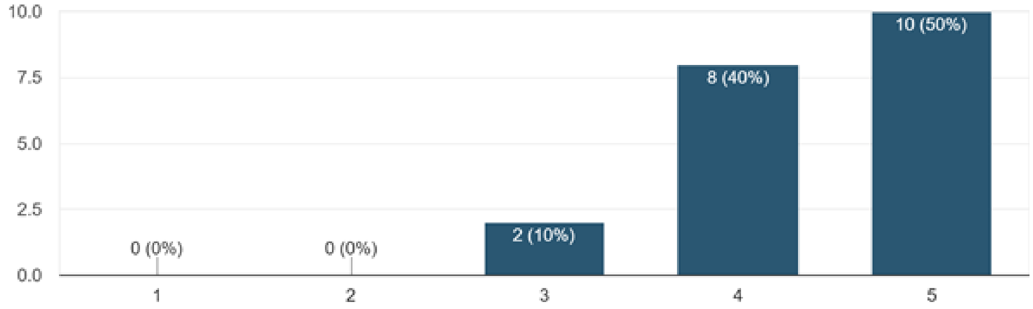
12. On a scale of 1 to 5, How will you rate organization considering the containment, eradication & recovery phase when it comes to incidents?

20 responses



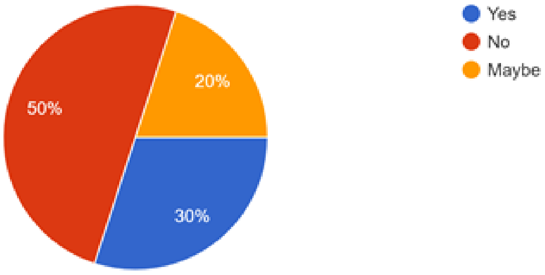
13. On a scale of 1 to 5, How will you rate organization considering the post-incident activity phase if the concerns incidents?

20 responses



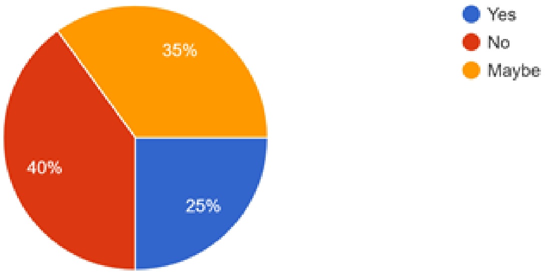
14. Does your organization use any specific framework or model to handle cloud incidents?

20 responses



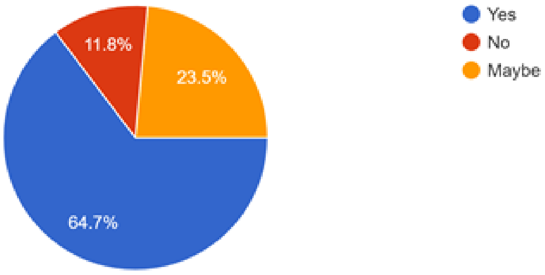
15. Do you think currently used incident handling framework are efficient for both cloud and on-premises environment?

20 responses



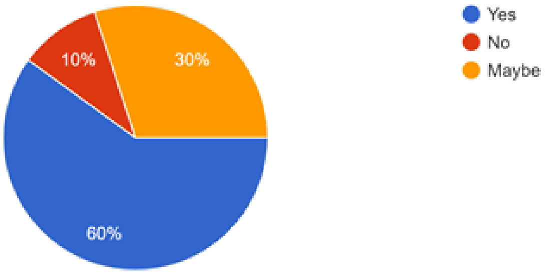
16. If no, do you wish to get a hybrid framework that will provide guideline for handling incident in the cloud and on-premises environment?

17 responses



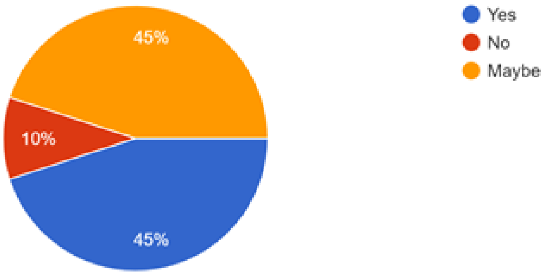
17. Study claims that handling incidents in the cloud is trickier because it requires skillsets to identify the data sources. Do you agree with the statement?

20 responses



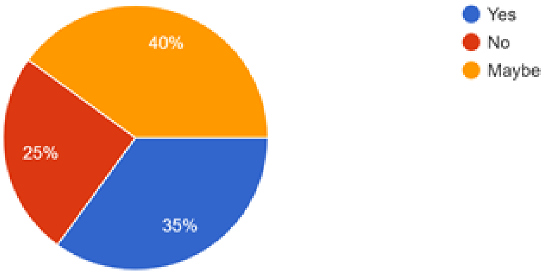
18. According to study, due to the distributed nature of data across multiple systems or jurisdictions data analysis is challenging in the cloud. Do you agree with the statement?

20 responses



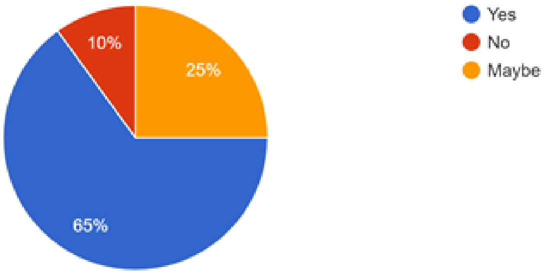
19. Due to shift in security responsibility between cloud service provider and cloud service user depending on chosen service model and provider, c...sponsibilities. Do you agree with the statement?

20 responses



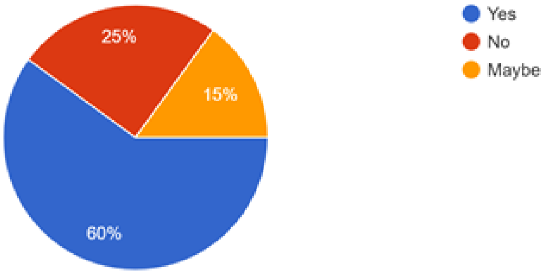
20. Lack of access and visibility to cloud service provider managed resources make it harder for cloud service users to handle security incident in the cloud. Do you agree with the statement?

20 responses



21. Does you organization use any tool to handle cloud incidents?

20 responses



22. If yes, which tool does your organization use?

1. Tools provided by cloud platform
2. N/A
3. Built-in logging, monitoring and alerting tools of the cloud
4. Idk
5. Multiple tools
6. Several
7. I don’t know all the tools we use since it is a shared responsibility between different teams, in my team we use different monitoring tools
8. No
9. NA
10. Different types of tools for different tasks
11. IPS, IDS, firewalls and others
12. Prefer not to say.
13. Different tools for different task but still dependent on service provider
14. Cloud native logging and SIEM

23. Do you have any suggestion regarding handling incidents in the cloud?

1. No
2. Gaining skills about recent and advanced security tools
3. Yes. Change the job and don’t be responsible for incident management, especially if

cloud is used

4. no

5. Not sure

6. clarify roles and responsibilities

7. It shouldn’t be treated any different then on-premises.

8. Hiring skilled professional to deal with cloud, sharing security responsibility and information

9. Testing is a must! Without it, any fancy paper written document would be useless.

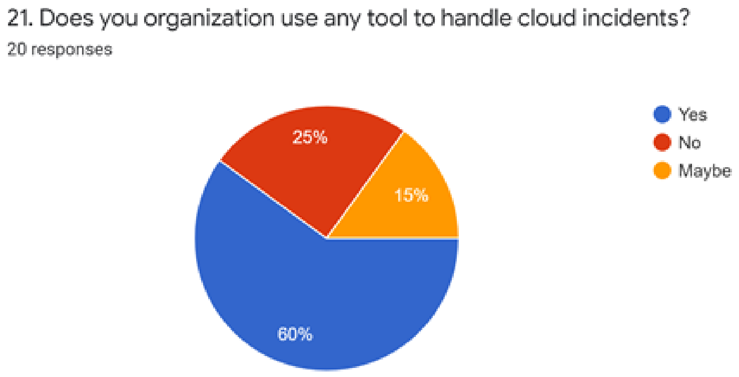
10. Information and responsibility sharing, using modern tools

11. Proper training to security experts on how to react to cloud Incident, responsibilities sharing and using advanced security tools.

12. Define and divide responsibilities between provider and local SOC/SIRT team. Regularly test it during DRT and similar red team exercises.

Appendix 4 - Online Survey Questionnaire 2 Responses

Hybrid Incident Response Framework Validation Questionnaire Responses



21. Does you organization use any tool to handle cloud incidents?

20 responses

2. Do you have any suggestions regarding improvement of the framework?

1. 1. The framework should clearly differentiate between certain main incident types: DoS, data breach, social and whether it's drive-by, targeted or apt. The first step (detect/prioritise) should then identify wich process to follow from that point on. A framework/process covering all of those cannot possibly be "learned by heart"; knowing that it's important that the necessary process documentation is as short and sweet as possible as soon as the incident has been classified. 2. Some of the items in the HIRF (preparation step) are depndent on policy. E.g. "list of allowed software" does not belong in the incident response framework; this is a policy decision that may or may not make sense for an organisation.

2. Incident response steps could be incident-specific, otherwise quite impressive.

3. Could be more elaborate

4. This is very advance technology already

5. The framework should show the sources from where the log data cloud is collected.

6. This can be considered as a generalized framework, but responses to incidents differ based on incident types.