Cloud Incident Response - a Comprehensive Analysis

Livia Maria BRUMĂ
Economic Informatics Doctoral School
Bucharest University of Economic Studies, Romania
brumalivia@gmail.com, liviabruma@rocketmail.com

Data has become the most important asset for organizations because it directly influences development, performance and risk, helping to improve service, analyze customer satisfaction, maximize profit and operate effectively. In the current context of increasing cloud services utilizations and the rising number of cyber-attacks, incident response can be a significant challenge for organizations using the cloud, because the risk of being subjected to an attack is inevitable. This article provides an overview of the methods, tools, and processes that can be used to ensure effective cloud incident response. Furthermore, are presented the most specific cloud elements that introduce differences in the incident response process applied in on-premise technologies.

Keywords: *Incident response in the cloud, Cloud security, Cloud computing incident*
DOI: 10.24818/issn14531305/27.4.2023.03

1 Introduction

Data has become the most important asset for organizations because it directly influences development, performance and risk [3], helping to improve services, analyze customer satisfaction, maximize profit and operate effectively. Their importance underscores the need for data security to be one of the essential and necessary processes, regardless of whether cloud services or on-premise technologies are used. At the same time, cyber-attacks align with the implemented security mechanisms, being more and more sophisticated, harder to identify and counter, being able to cause significant damage to organizations, both financial, legal and image. According to [4], in 2021 the value of damage caused by cyber-attacks increased by 10% compared to the previous year, being the highest value recorded in recent years. This fact is due to the increasing number of attacks, with 54% of organizations being the target of cyber-attacks in the last 12 months [5], because the multiple types of attacks, such as ransomware, supply chain attack, phishing etc., can exploit vulnerabilities of a social, human and technical nature, managing to bypass or penetrate security mechanisms. Relatedly, incidents of an internal nature, such as improper handling of data, violation of work procedures, unauthorized access or sharing of access credentials, provide the opportunity to create new attack surfaces, which can later be exploited by attackers. The study [6] shows that 94% of businesses use at least one type of cloud service of which only 3% use exclusively private cloud implementations and 84% have also implemented a multi-cloud strategy. This huge percentage of companies using public cloud services contribute to forming an overall picture of the impact that cyber incidents can have - any internet connected device with exploitable vulnerabilities can become a gateway for attackers.

In 2021 the average time to identify an incident in mature cloud environments was 252 days and the financial damages caused by data breaches amounted to $12.96 million, increasing compared to the previous year.[4] Although the complexity of cyber-attacks has reached an extremely high level, it can be seen in figure 1 that over half of cloud security incidents are based on the simplest attack, phishing. This fact is caused by the lack of user security culture correlated with phishing emails created by attackers that are becoming increasingly difficult to identify. An increased level of security culture among users could contribute significantly to the decrease in the number of incidents but also to the reduction of the period of their identification, by the immediate reporting of abnormal events. Of all

the protection mechanisms that can be used (excluding of open-source solutions), investing in security training programs for users can have the highest return, in terms of cost, for reducing the number of security incidents.

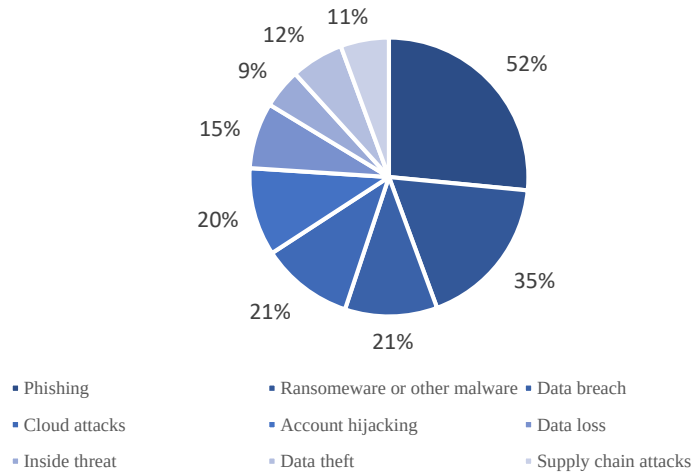

Fig. 1. Incident distribution for organizations with 1000+ employees [data from [5]]

Although security investments are increasing, they cannot completely prevent incidents from occurring. Thus, it becomes necessary to implement actions that can detect suspicious events in a shorter time, in order to identify incidents in the early phase and minimize the impact caused. To deal current threats from cyberspace, it is necessary that as the IR process matures in an organization, it should overcome the barrier of detection and response and help increase security resilience through proactive actions that can anticipate incidents and fix vulnerabilities before they are exploited. The previously presented aspects support the importance of the incident response process (Incident Response - IR) because the main purpose of this process is to reduce the impact of an incident on the organization assets, by previously establishing the measures and actions necessary to be carried out when an incident is detected. The first chapter of this article looks at the key challenges of cloud IR in terms of the methods, tools and processes that can be used to ensure effective incident response. At the same time, the specific cloud elements that introduce differences in the incident response process applied in on-premise technologies are presented. The second part of the article presents the incident response planning process with direct applicability to cloud environments.

2 Challenges of IR in the cloud

An incident response strategy can help organizations identify events and remediate security incidents as quickly as possible, helping to limit financial, legal and image damage and reduce the likelihood of spread to other assets. At the same time, to ensure compliance with certain standards, such as PCI DSS, HIPA etc., the IR plan is a mandatory criterion to be met. In order to manage security incidents in the cloud, it is necessary to perform the same activities as in on-premise environments, but using specific methods adapted for this environment. The operational advantages that have contributed to the adoption of cloud services raise the main challenges in conducting the IR process. Identifying and locating incidents is difficult due to the cloud distributed architecture, dynamics and control over the infrastructure, but also due to low visibility compared to on-premise infrastructures. The coordination of the incident response team is also poor because not enough training exercises are conducted for the team to know exactly the incident management procedures and to identify possible practical problems in the process [6]. At the same time, incident

response specialist must possess strong knowledge in the cyber security area and specific cloud solutions. The lack of specialized personnel affects companies regardless of their size, as human resources are still the basis of ensuring security. The report [7] states that only 26% of organizations using SaaS (Software as a Service) and 38% IaaS (Infrastructure as a Service) consider IR to be 'not at all difficult' and 15% of all respondents say it is 'very difficult' to respond in mixed IaaS/SaaS or hybrid environments. 74% of security professionals say their organizations need additional data and context to conduct forensic investigations in cloud environments, 64% that it takes too much time to collect and process data to conduct a timely investigation, and 35 % of cloud security alerts are not investigated [8].

Most of the time, incident detection is automated in SOC through modern correlation and behavior-based anomaly detection technologies, and preliminary analysis is done through sandboxes. However, human intervention is needed to analyze the real risk that an infected system can cause on the operational level, all in order to limit the impact on the organization assets. Another problem can arise when in order to fix and bring systems to operational state in the shortest time, best practice guidelines or work procedures are violated, creating vulnerabilities that can later be the cause of other incidents. Not infrequently, the violation of change management plans was the source of subsequent incidents that led to the unavailability of services, without the need for external attackers. In 2021, the company Meta through its three social media platforms Facebook, Instagram and WhatsApp, had a six-hour unavailability caused by network configuration errors, which produced a financial loss of $230 million and a 5% drop in stock price in the next 24 hours [9].

In order to meet all the security challenges mentioned before, incident response should be supplemented with activities such as:

- threat hunting - the active search for suspicious signs and behaviors that indicate a possible security threat;
- creating security patterns that identify abnormal behavior on the network;
- correlating events to identify TTP (Tactics, Techniques and Procedures) used by attackers;
- automating monitoring and alerting to quickly identify incidents and prevent the spread of the infection vector.

There are three elements specific to cloud environments that impact IR: cloud governance, visibility and shared responsibility [10]. Other distinct elements that contribute to cloud IR differences are in the area of automation, such as APIs for solution integration, continuous asset assessment, anomaly location, data acquisition for investigations, and automated incident remediation. Next, these three elements are analyzed as well as the proposal of adaptation methods according to the previously mentioned activities.

2.1 Cloud Governance

Cloud governance is a complex topic that can be discouraging, especially for small organizations when first adopting cloud services [11]. Although there is no standardized definition of cloud governance [12], this process can be summarized as a set of rules and policies to protect data, manage risk and enable the optimal functioning of cloud systems [13]. Cloud migration based on a governance model ensures an optimal transition, starting from the objectives of the organization, the choice of the right cloud provider and model, as well as the required applications, the associated costs and the advantages of this process. Security mechanisms derive from objectives, depending on the importance of assets and data, because is a necessary cost not an objective in itself. IR depends on the governance, risk and compliance model, which indicates how the technical and procedural tools and solutions in the cloud should be used to provide enhanced visibility and capabilities.

Definition of the concept of cloud governance from the most important cloud providers are presented in the table 1.

Table 1. Definition of the concept of Cloud Governance

IBM	AWS	GCP	Azure
Cloud governance is an agreed framework that consists of establishing, enforcing and overseeing the activities and guidelines that are required as part of the rules of conduct for cloud use. [14]	Cloud governance enables customers to define the security, cost and ongoing oversight requirements of their cloud journey and ensures that processes are consistently optimized and followed. [15]	Effective governance is essential to ensure the reliability, security and maintainability of assets. [16]	Governance provides mechanisms and processes to maintain control over applications and resources through strategic planning and prioritization. [17]

The definitions presented in Table 1 do not reflect the differences introduced by governance in the IR process of cloud versus on-premise technologies, but are rather an adaptation of the definition of IT governance: a process that ensures the effective use of IT resources to enable an organization to and achieve the goals [18]. The main problem with cloud governance is that while an organization can outsource responsibility for governance, a company can never outsource accountability (for actions or lack of actions), even when using external providers [19].

The governance model developed by an organization must address each component derived from migrating to the cloud to ensure a clear management strategy in order to maximize the benefits that the cloud can provide. The use of such a detailed and well-constructed model from the moment of cloud migration ensures cost optimization while maintaining a high level of performance, implicitly of an adequate level of data security. Figure 2 shows the six components of cloud governance

Fig. 2. The components of cloud governance [20]

The role of governance is also to ensure a uniform way of working, examined and properly managed by looking at both the macro and micro level of all elements in an organization, from assets to systems, processes, personnel and security. It is impossible to identify anomalous events that endanger assets without established what is normal and permissible. Some organizations do not allow users to log into social media platforms through work devices, while other organizations have no such restrictions, with governance setting

these policies based on the risk assumed. An effective governance strategy provides crucial benefits for the security of company data and assets. Beyond the classic, defensive objectives, such as gaining an overall view of data security level and the use of best practices in compliance management, the use of a responsive, scalable and adaptable data governance strategy generates value to the organization through the dynamic incorporation of data analysis. [21]. Among the specific cloud governance elements is the financial management of cloud service costs. While there are services, solutions and specialized teams that can provide security, the total costs of the logistics must be in line with the value of the business, and the use of the cloud must bring financial benefits and not excessive expenses for administration and security. Initially, at the onset of the cloud migration movement, financial costs formed the basis of pro-cloud arguments. However, over an extended period, the associated costs tend to become equivalent to on-premise solutions, with scalability remaining the primary advantage. Poor cloud governance can make incident response more difficult and ineffective, through a lack of transparency regarding resources and data stored in the cloud, inappropriate use of cloud services, and exposure to cloud specific vulnerabilities and threats. All these aspects have an impact on IR (Incident Response), with this stage involving the planning of either an efficient process or one prone to failure, which can lead to frustration among CSIRT (Computer Security Incident Response Team) members, financial losses, and may not contribute to the overall resilience of the organization.

2.2 Cloud Visibility

A high level of visibility provides the opportunity to have a detailed view of all cloud activities for the purpose of identifying security threats, assessing performance, cloud service costs, and efficiency, and applying remediation measures for real-time issues. Insufficient visibility can conceal blind spots, security threats, cause application or network performance issues, as well as delays in identifying events that could have been swiftly remediated without causing significant damage. In the study [22] is mentioned that lack of visibility into the cloud caused significant consequences, such as delays in resolving security alerts (26%), compliance issues (18%) and the inability to prevent security attacks (17%). This lack is mainly caused by the technological complexity of the cloud, but also by the fact that many organizations use cloud services from different providers, as well as a hybrid technology environment based on cloud elements with on-premise infrastructure. For example, for SaaS, proprietary devices are used to access the service, which can be compromised by attackers to exfiltrate data without explicitly accessing cloud data. While ensuring visibility for on-premise environments relies on monitoring events generated by systems (using tools like SIEM - Security Information and Event Management, SOAR - Security Orchestration, Automation, and Response, EDR - Endpoint Detection and Response, etc.), a different approach is needed for the cloud to create a comprehensive picture encompassing all specific elements – services, endpoint systems, compliance, applications, virtual machines, containers, etc. For cloud instances like PaaS (Platform as a Service), SaaS (Software as a Service), or FaaS (Function as a Service) such as AWS EKS, RDS, or Lambda, the cloud provider manages the underlying system, making it infeasible to install software on the equipment running the services, thus necessitating detection and response through alternative means. [23].

Adding redundancy to monitoring solutions can also reduce the likelihood of a total loss of visibility when various technical issues occur [24]. Figure 3 highlights the four questions and areas that can ensure we have a complete picture of cloud actions. In order to increase the level of visibility, it is necessary to identify the answer to the four questions: who, why, when and how for each detected incident. Correlating information obtained through enhanced visibility with elements of threat intelligence allows organizations to change behavior in the face of threats, from reactive to proactive (cyber threat intelligence is an area of cyber security that collects,

processes and analyzes data to understand the motives, targets and attack behaviors of a threat actor [25]).

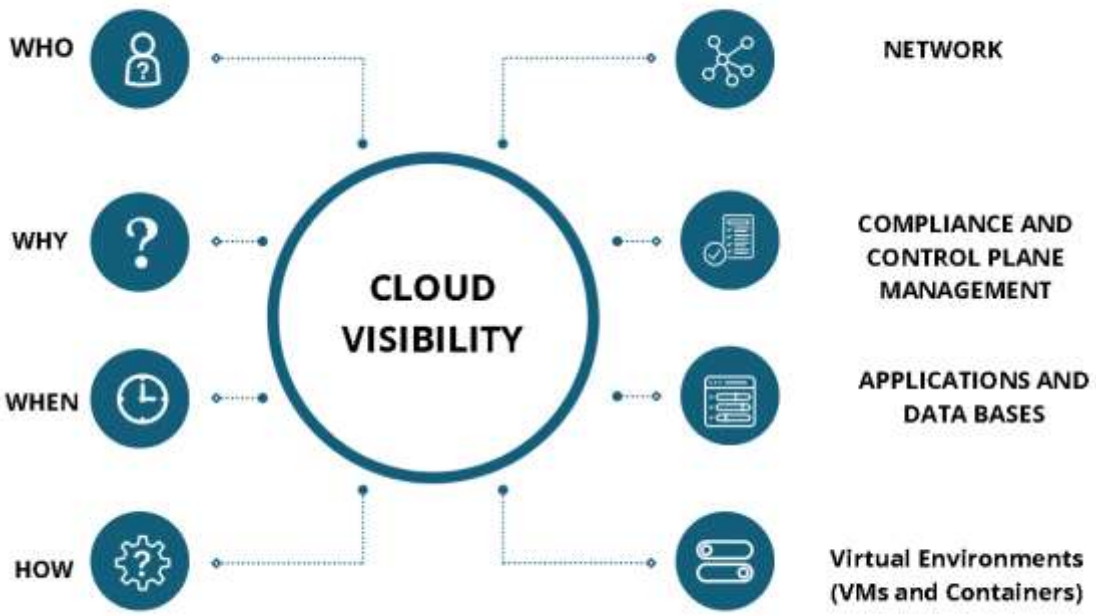

Fig. 3. Cloud Visibility Elements

2.3 Shared Responsibility for Cloud Security

The concept of shared responsibility in security involves sharing responsibility, and consequently, tasks among the parties involved in the delivery and use of cloud solutions. The most common models involve the management of cloud infrastructure operations and security by service providers, while data security is the responsibility of the contracting organizations. Responsibilities are delineated based on the chosen cloud service model, whether it is IaaS, PaaS, SaaS etc. Figure 4 illustrates the shared responsibility model, outlining the responsibilities of the CSP and the CSC.

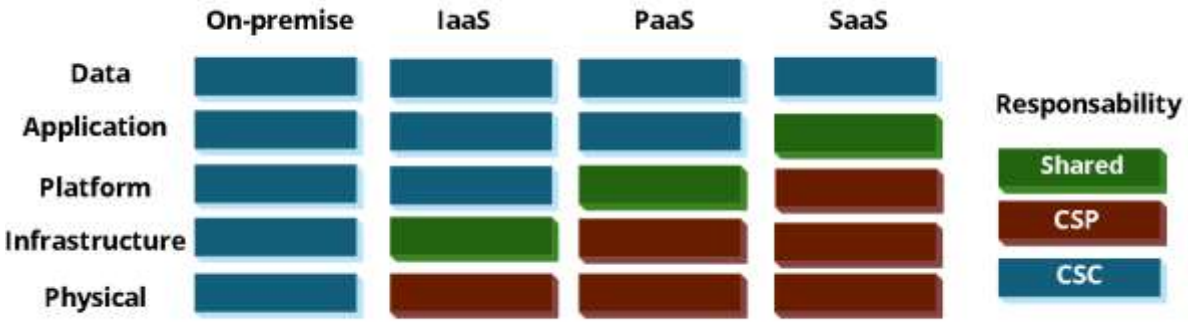

Fig. 4. Matrix of shared responsibilities for cloud asset (adapted from [26])

This model introduces challenges because the management entails responsibility for the good functioning of the services, especially from the perspective of legislative aspects that impose certain conditions depending on the type and location of data processing. As can be seen from Figure 4, in both on-premise and cloud models, the customer is responsible for ensuring that data is properly protected, labeled and classified to meet any compliance obligations [27]. The complexity and speed of change of the component technologies as well

as the security policies required to be applied lead to an ambiguity in assuming responsibility for an incident, in 99% of cases, the organization owning the data being responsible for the data breaches created [28].

Depending on the cloud deployment model used, the IR process must be adapted to respond to incidents within the organization area of responsibility and the shared area with the cloud provider. While it seems fairly clear how responsibility for security, implicitly the IR process, is shared between the two contracting entities, challenges arise from the differences in how each provider understands their part of responsibility [29].

The AWS model differentiates responsibility as 'security of' the cloud versus 'security in' the cloud, where the CSP is responsible for protecting the infrastructure supporting the provided services, and the responsibility of the CSC is determined by the services they use. For example, in IaaS, all security configuration and management tasks are within the responsibility of the CSC [30]. The responsibility matrix provided by Azure divides responsibilities according to service and resources, also for IaaS – network controls and host infrastructure can be the responsibility of both CSC and CSP [31]. Google Cloud mentions that for IaaS the hardware, storage and network are the responsibility of the CSP [32]. IBM Cloud, like Azure that provides cloud security for certain resources and domains by sharing responsibility: for example, for IaaS, physical servers are the responsibility of the CSP for Disaster recovery but for Security and Compliance they are shared with CSC [33]. For small, on-premises cloud providers, no research was identified regarding models used for security sharing, standards used, or compliance. The ambiguity and lack of standardization of how security is shared contributes significantly in a negative way to making it difficult to create an incident response model that can be applied regardless of the service provider, the service used, or the chosen implementation mode.

3. Cloud incident response planning

IR planning aims to prevent the exploitation of vulnerabilities or the occurrence of incidents and the IR process is triggered after an incident has been identified. Part of the activities that must be carried out prior to IR planning are audit processes, vulnerability analysis and penetration tests that include the technical, personnel and process components of the organization to provide information to management structures regarding the protection of confidentiality, integrity and systems availability. These allow an organization to validate its compliance with the standards it has set and measure the levels of risk it currently accepts [34]. A comprehensive analysis of the role and impact of auditing, vulnerability analysis and penetration testing for the cloud was published in [35]. For on-premise environments there are different incident response frameworks developed both by international organizations for standardization and by security companies that analyze the importance of each step necessary to create a plan that can be applied to all situations encountered. The development of IR plans based on these standards ensures that all the elementary steps for the identification and remediation of incidents are completed in order to ensure the lowest possible impact. Table 2 shows the component stages of the most well-known standards or framework processes.

Table 2. Incident response stages from different standards

Standard	NIST Special Publication 800-61	SANS Incident Handler's	ISO/IEC 27035-2:2016	CSA CIR Framework
Component stages	Preparation	Preparation	Planning and preparation	Preparation
	Detection and analysis	Identification	Identification, detection and report	Detection and analysis
	Containment, eradication and recovery	Containment	Assessment and decision	Containment, eradication and restoration
	Post-incident activities	Eradication	Response	Post-mortem
		Recovery	Lessons learned	
		Lessons learned		

The first three framework processes presented in the table are exclusively addressed to on-premise environments, while the last one is specific to the cloud. It can be seen that although the stages differ both in name and number, the actions carried out are identical, only assigned to a different step.

Each of the stages required to be completed in IR are composed of specific actions that can be carried out correctly and according to a plan only if the entire security structure of an organization is mature. Explicitly implemented security policies are needed, which make a clear differentiation between an event and an incident, change-management procedures that are respected regardless of the pressure to solve an operational situation, system backups for easy restoration to the initial form, both logical and physical access control, etc. Without the use and adherence to plans, incident response becomes a process of repairing damage without contributing to increasing the resilience of systems and preserving evidence for possible digital investigations becomes impossible.

The IR process is composed of all the activities that occur from the moment the incident is detected until it is resolved. The complexity of current technologies and the different objectives of organizations do not offer the possibility of defining incidents only based on the definition given by the standards. Thus, in the stage of developing the IR plan, the term organization-specific incident must be defined so that the CSIRT team can intervene and minimize its impact by following, as far as possible, the procedures in the IR plan.

4. Incident response process

The incident response process begins with the declaration of the incident, illustrated in Figure 5, at a time point T0. The four basic stages, preparation, detection and analysis, containment, eradication and restoration and post-mortem are made up of specific actions, as presented in Figure 5.

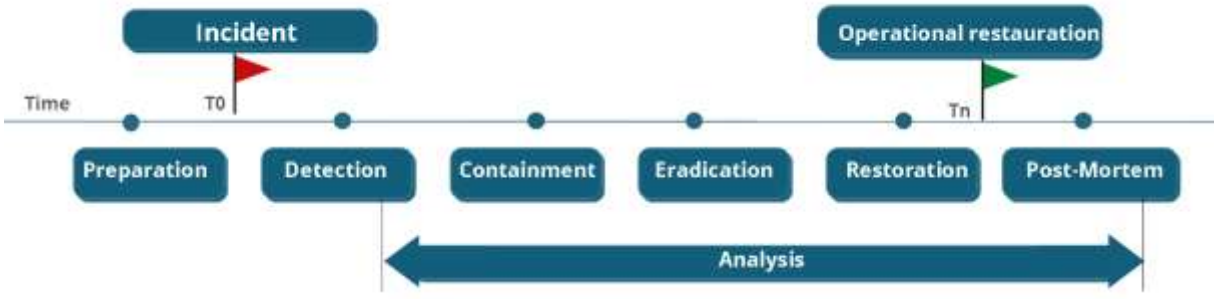

Fig. 5. Incident response timeline

4.1 Preparation

The initial phase in which preparatory measures take place (the development of processes, procedures, policies and communication protocols between institutions) in order to respond effectively to security incidents, is the most important stage because all future actions are based on the elements established in this phase. The ability to respond to incidents, implicitly the time to restore the systems to normal parameters, is based on good coordination of fundamental entities, trained people, functional processes, technology and integrated information [36]. Some attacks occurring in the cloud employ methods and techniques different from well-known attacks, representing a novelty. The emergence of technologies used in the cloud means that certain vectors and attack surfaces are used for new, complex attacks that are impossible to detect based on indicators alone, without using behavioral analysis. Table 3 shows the most common types of attacks on cloud environments:

Table 3. Cloud specific attacks

- Attacks on buckets	The attempt to gain unauthorized access to the data stored in an object storage bucket (Amazon S3, Google Cloud Storage or Microsoft Azure Blob Storage)
- Exploitation of OAuth tokens	The attempt to gain unauthorized access to resources protected by the OAuth (Open Authorization) system
- Abuse of resources	The unauthorized use of cloud services such as storage, data processing

The standard activities carried out by an incident response team from on-premise environments, detailed and analyzed in the standards in table 2, will not be mentioned because the article analyzes cloud specific IR, so the main activities in the preparation stage must include, at least, the following two activities:

1. A detailed understanding of the organization's purpose, objectives, and operational needs – the planning of incident response is initiated by the operational needs and critical missions of the organization. Depending on the type of cloud service used, based on the SLA (Service Level Agreement) in place and the concept of shared responsibility, the role and responsibilities of each party will be determined. Also, in this stage, it is advisable to analyze the results of risk analysis processes to identify critical assets and potential impacts.
2. Analyzing cloud architecture – when an incident occurs, emotional factors can negatively impact the understanding of certain technical configurations, making it imperative to have knowledge and understanding of the role that technical equipment plays in the architecture. The decentralization and scalability of the cloud can either make this task easy for the SOC (Security Operations Center) or extremely challenging, depending on the type of cloud used. Addition-ally, regardless of the type of cloud used, within organizations, there is a portion of hardware and software equipment that belongs entirely to the users, which must be analyzed in the con-text of cloud service utilization (laptops, memory sticks, storage units, network equipment etc.).

4.2 Detection and analysis

The average detection time for an incident is often quite lengthy, during which APT (Advanced Persistent Threat) attacks can exfiltrate massive amounts of data or successfully compromise an organization's entire infrastructure. Event detection relies on various security monitoring methods, both from on-premise Security Operation Centers (SOCs) utilizing solutions like IDS/IPS (Intrusion Detection/Prevention System) and SIEM, and specialized cloud security solutions such as DataDog, SumoLogic, Amazon CloudWatch, Azure Monitor, and others. In the case of SaaS, where CSC (Cloud Service Customer) is responsible only for data security, all other components are managed by the provider, and various logs, including those for applications,

access, errors, authentication, etc., can be employed. For IaaS, sources of evidence encompass system logs, hypervisor logs, raw virtual machine files, unencrypted RAM snapshots, firewalls, network traffic data, storage logs, backups, and more. PaaS relies on application specific logs, which can be accessed via APIs, to detect issues such as patches, operating system errors, malware alerts, and so forth. [37]
The effectiveness of incident detection is contingent on the visibility of events that can contribute to the early identification of suspicious activities, potentially even before security device alerts are triggered. As organizations migrate to the cloud, their overall infrastructure visibility diminishes, posing challenges to detection and, consequently, the entire incident response process. Ensuring the highest possible degree of cloud visibility is contingent on two key components: [38]

- visibility based on events - the main methods of collecting and analyzing events generated by operating systems, applications, network devices are the same as in on-premise SOCs, with the mention that a new category of events appears that needs to be monitored, generated by the CSP infrastructure, whose integration is sometimes achieved through the use of APIs;
- behavioral visibility – which can only be achieved by processing large amounts of data over a long period of time, which can provide critical information to identify insider abuse, account hijacking or illicit use of cloud resources.

4.3 Isolation, eradication and restoration

Third stage of IR consists of three major components: stopping the spread of the attack by isolating infected systems, eradicating the attack vector, and restoring systems. The effectiveness of this stage plays a significant role in mitigating the impact an incident can have by reducing the spread of the attack throughout the entire infrastructure and facilitating rapid restoration for business continuity. Depending on the type of cloud service used and the type of incident, the activities carried out in this stage can be diverse and complex. In [39] three scenarios are analyzed for IaaS, PaaS, and SaaS, highlighting the actions that CSP (Cloud Service Provider) can take in the incident response process: configuring the network, accessing virtual machine stop and snapshot functions, configuring granular functionality and access rights, as well as configuring the web application firewall.

4.4 Post-Mortem

The primary objectives of this stage are to assess the impact of the incident, prepare reports analyzing the incident, and identify methods to prevent recurrence [40] which are also used in the case of incidents in on-premise technologies. The main actions of IR, although it has a continuous preparation stage detailed in point 2, are triggered at the time of detection of an event with anomalies, at a time denoted as T0. As mentioned in the article's introduction, the average detection time for an attack is 252 days, which in the case of an APT (Advanced Persistent Threat) attack can pose a significant risk to the organization. Therefore, a visible attack causing noticeable user damage is preferred over one that establishes connections to C2 (command and control) servers and remains undetected for an extended period. From that moment, the primary method to minimize the impact of an incident is proper time management. After detection, the analysis phase can last until post-mortem activities, including isolation, eradication, and restoration, depending on the type of attack.
Therefore, from the previous analysis of IR process activities, it is evident that the main challenges arise from identifying all sources of relevant events and maintaining the chain of custody of data due to the decentralization of the architecture, limited visibility over the entire cloud system, the integration of on-premise services with off-premise ones, and the expertise of CSIRT personnel. An effective solution to these problems is process automation. Automating the collection of elements required for incident investigation contributes to improving the agility and efficiency of the IR process, ensuring that security events are properly analyzed before potentially escalating. The use of IR automation eliminates time-consuming repetitive steps and increases

the detection and remediation levels of incidents, regardless of their severity. Additionally, the risk of human errors is reduced, as automation is an efficient, scalable, and reliable process when implemented correctly. To enhance the overall security of the organization, it is necessary to implement a proactive threat detection plan alongside a reactive incident response activity.

5. Conclusions

The increasing number of cyberattacks and incidents involving cloud technologies emphasizes the importance of the incident response process to maintain the lowest possible impact on an organization's assets. The ability to maintain an efficient IR program for the cloud begins with identifying a comprehensive view of the entire cloud ecosystem, from governance, visibility, cloud tools available from the provider, and relies primarily on the successful integration of all security processes and mechanisms. As an organization's security level improves, the IR process matures, contributing to increased security resilience through proactive actions that can anticipate incidents and remediate vulnerabilities before they are exploited.

References

[1] Deloitte, "Understanding the value of your data assets Report," 2020.
[2] Ponemon Institute, IBM, “Cost of a Data Breach Report,” 2021.
[3] "15 Alarming Cyber Security Facts and Stats," 2020. [Interactive]. Available: https://www.cybintsolutions.com/cyber-security-facts-stats/.
[4] Flexera, “Annual State of the Cloud Report,” 2019.
[5] Netwrix, "Cloud data Security Report," 2021.
[6] [Interactive]. Available: https://cloudacademy.com/course/cloud-governance-risk-and-compliance/incident-management-1/.
[7] Palo Alto Networks, "The Critical Nature of Incident Readiness and Response in a Digitally Transformed World," 2021.
[8] 2021. [Interactive]. Available: https://www.helpnetsecurity.com/2021/11/18/investigations-cloud-environments/.
[9] "Facebook shutdown cost up to $230 million in 6 hours," 2021. [Interactive]. Available: https://www.masslive.com/news/2021/10/facebook-shutdown-cost-up-to-230-million-in-6-hours.html.
[10] Cloud Security Alliance, "Cloud Incident Response framework," 2021. [Interactive]. Available: https://cloudsecurityalliance.org/research/working-groups/cloud-incident-response/.
[11] [Interactive]. Available: https://www.zycomtec.com/five-disciplines-of-cloud-governance-to-consider-as-a-starting-business/.
[12] M. Al-Ruithe, E. Benkhelifa and K. Hameed, "A systematic literature review of data governance and cloud data governance," Personal and Ubiquitous Computing, 2019.
[13] "What is Cloud Governance?" [Interactive]. Available: https://www.imperva.com/learn/data-security/cloud-governance/.
[14] [Interactive]. Available: https://www.ibm.com/garage/method/practices/culture/key-attributes-cloud-governance/.
[15] [Interactive]. Available: https://pages.awscloud.com/GLOBAL-partner-OE-pmc_security-pas-2021-reg-event.html?trk=ep_card-reg.
[16] [Interactive]. Available: https://cloud.google.com/architecture/migration-to-google-cloud-building-your-foundation?hl=en.
[17] [Interactive]. Available: https://docs.microsoft.com/en-us/azure/governance/azure-management.
[18] [Interactive]. Available: https://www.gartner.com/en/information-technology/glossary/it-governance.
[19] G. Thompson, CCSK Certificate of Cloud Security Knowledge, McGraw Hill, 2020.
[20] [Interactive]. Available: https://www.cloudbolt.io/blog/cloud-

governance-the-key-to-better-cloud-management/.
[21] "How to master data governance and deliver value," [Interactive]. Available: https://www.collibra.com/us/en/resources/master-data-governance.
[22] Keysight, "The State of Cloud Monitoring," [Interactive]. Available: https://www.keysight.com/us/en/assets/3120-1271/reports/The-State-of-Cloud-Monitoring.pdf.
[23] [Interactive]. Available: https://www.mitiga.io/blog/7-best-practices-for-cloud-incident-response.
[24] C. Chio and D. Freeman, Machine Learning & Security, O'Reilly Media, 2018.
[25] [Interactive]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.
[26] [Interactive]. Available: http://blog.mesa.org/2018/06/manufacturing-in-cloud-part-xvii-cloud.html.
[27] [Interactive]. Available: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.
[28] L. Senko, "99% of cloud security failures will be the customer's fault," [Interactive]. Available: https://www.linkedin.com/pulse/99-cloud-security-failures-customers-fault-protect-user-lou-senko/.
[29] D. Shackleford, "A New Take on Cloud Shared Responsibility," [Interactive]. Available: https://www.sans.org/white-papers/40040/.
[30] [Interactive]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/.
[31] [Interactive]. Available: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.
[32] [Interactive]. Available: https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke.
[33] [Interactive]. Available: https://cloud.ibm.com/docs/overview?topic=overview-shared-responsibilities.
[34] [Interactive]. Available: https://www.auditscripts.com/ Auditing Incident Management.
[35] L. Bruma, "Cloud security audit – issues and challenges," in 16th International Conference on Computer Science & Education (ICCSE) , 2021.
[36] IBM, "Cost of a Data Breach Report," 2021.
[37] [Interactive]. Available: https://www.intechopen.com/chapters/64377.
[38] "Security Operations in the Cloud," [Interactive]. Available: https://pages.awscloud.com/AWSMP-H2-SEC-Splunk-Security-Visibility.html.
[39] B. Grobauer and T. Schreck, "Towards incident handling in the cloud," 2010.
[40] M. Ozer and S. Varlioglu, "Cloud Incident Response: Challenges and Opportunities," in International Conference on Computational Science and Computational Intelligence (CSCI), 2020.

Livia Maria BRUMĂ has graduated the Faculty of Military Electronic and Information Systems of the Military Technical Academy „Ferdinand I" from Bucharest in 2016. She holds a Master Degree in Electronics applied in robotics for security and defense. At present, she works in cyber security domain, as a Cyber Security Auditor and she is involved as a Ph.D. student in the Economic Informatics Doctoral School from the Bucharest University of Economic Studies.