[1]Mr. Rakesh Bhavsar
[2]Dr. Vishvjit Thakar

Cloud Incident Response: Enhancing Efficiency Through Redundancy

Journal of Electrical Systems

Abstract: - The focus of this study revolves around enhancing incident response within cloud environments. It begins by establishing a conventional incident response framework as a foundational structure for the cloud incident response model. A primary objective of this model is to reduce incident handling time significantly. This reduction is accomplished by adding a Security Domain devoted to threat analysis and cloud forensics, as well as by incorporating infrastructure redundancy into the cloud system through Network and Security Controllers.The paper delves into the architectural adjustments necessary for implementing these enhancements and applies them within the context of the cloud incident response model.

Keywords: Event Response, Monitoring, Minimize Handling Time ,Scanning of assets, security management

I. INTRODUCTION

As cloud technologies experience a surge in popularity, accompanied by heightened levels of virtualization, fresh challenges emerge in the realm of cyberattack investigation and timely incident response. The contemporary architecture of cloud systems necessitates forensic investigation and incident response models that are not only scalable and elastic but also seamlessly integrable with the data plane and easily manageable within the control plane. Given the inevitability of organizational compromise, it becomes imperative to develop an incident response model that meticulously considers the IT infrastructure of an organization during the initial design phase of cloud deployment. This paper introduce about how to identifying the overflow of event occur in the system ,where this event occur and how to solve this incident and minimize the time of that incident through response .

II. Navigating Challenges in Incident Response: Addressing Cloud Environment Dynamics

The Although they provide thorough guidance, the current incident response standards—NIST 800-61[1], ISO 27035[2], and SANS's Incident Handler's Handbook—are unable to adequately handle the complexities of cloud settings. To guarantee maximum efficacy, a strong incident response model designed for clouds needs to carefully take into account characteristics specific to cloud computing, such as distributed computing, high availability, and network function virtualization. Such a model's effectiveness is mostly determined by how responsive it is, especially when it comes to time efficiency.

In the context of security challenges[7] faced by organizations, early detection of threats and prompt incident response stand as paramount objectives. Consequently, the evaluation of model efficiency hinges on minimizing the duration between infection and threat discovery (TDs), as well as the time taken for incident handling (IHn) from threat discovery to remediation and prevention. In essence, the optimization function aims to minimize both TDs and IHn times, thereby enhancing the overall efficiency of the incident response process.

In mathematical terms, the objective function can be represented as follows:

$$W=\min[T(TDs)]+\min[T(IHn)]\ldots..(1)$$

This equation encapsulates the imperative to minimize both the time to detect threats and the subsequent time required for incident resolution and prevention, thereby optimizing the incident response framework for cloud environments.

[1] Ph.D. Research Scholar, Dept. of Computer Science Engineering School of Engineering, IndrashilUniversity,Mahesana,Gujarat, rakesh.bhavsar08@gmail.com

[2]Professor, Dept. of Computer Science Engineering School of Engineering, Indrashil University, Mahesana,Gujarat,vishvjit.thakar@indrashiluniversity.edu.in

III. Refined Incident Response Framework

Drawing from established standards models of Incident response refinement process model [6] undergoes a structured refinement process. Its key steps encompass:

1.Planning:

a. Prepare an Incident Response Team (IRT).

b. Formulation of a comprehensive algorithm ..

2.Detection:

Prompt identification initiated either by automated security scanners (e.g., IDS, firewalls, sandboxes) or through manual operator interventions, triggering security alerts.

3.Mitigation:

Implementation of containment measures aimed at curbing the extent of damage resulting from the incident.

4. Identification:

a. Comprehensive Information Gathering, including the duplication of forensic images.

b. Conducting threat analysis utilizing gathered data to compile a detailed report encompassing penetration details, payload analysis, and recommendations for remediation and prevention, with specific emphasis on identifying indicators-of-compromise (IoCs).

c. Identification and assessment of potential information losses, such as compromised passwords, keys, certificates, and other sensitive data.

5.Remediation:

a. Formulation of remediation recommendations by the Incident Response Team (IRT), including the removal of malicious code and associated artifacts from infected hosts, and the initiation of password, key, and certificate replacements.

b. Restoration of hosts and network devices from available backups.

c. Thorough scanning of recovered hosts and networks for residual threats.

d. Restoration of recovered hosts and networks to operational status.

6.Prevention:

a. Articulation of incident prevention measures by the IRT, including protocol revisions and the implementation of security updates to address identified vulnerabilities[7].

b. Regular updating of Intrusion Detection Systems (IDS), firewalls, and sandboxes with new rules derived from mined IoCs.

7.Lessons Learned:

Reflection and analysis phase aimed at extracting valuable insights from the incident response process, facilitating continuous improvement and refinement of incident response strategies and procedures.

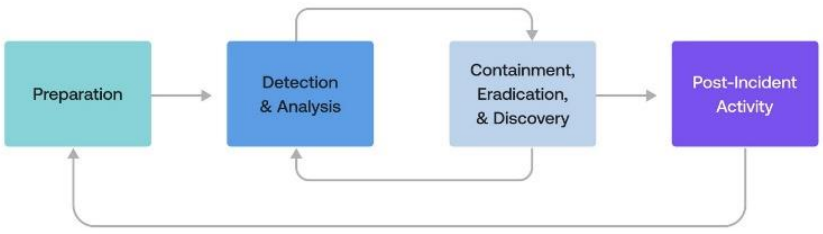

Figure 1 Incident Response Cycle[1].

This refined framework integrates best practices from various recognized incident response models, thereby enhancing readiness and efficacy in addressing security incidents within diverse operational environments[11].

Proposed Algorithm for Reducing Event Handling Time

Step1: Define Incident Severity Levels and Response Targets

a)Define severity levels (e.g., low, medium, high, critical) based on impact and urgency.

b)Assign corresponding response targets for each severity level (e.g., low: 4 hours, medium: 2 hours, high: 1 hour, critical: 30 minutes).

Step 2: Establish Incident Response Team

Assemble a dedicated incident response team with expertise in cloud architecture, security, networking, and application development.

Step 3: Implement Proactive Monitoring and calculate Mean Time to Detect (MTTD).

$$MTTD = \sum \frac{\text{Number of incidents detected}}{\text{Time taken to detect incidents}}$$

Step 4: Calculate False Positive Rate (FPR) .

$$FPR = \frac{\text{Total number of alerts}}{\text{Number of false positives}}$$

*It is also Consider as Mean Time Failure (MTBF).

Step 5: if event occur then Calculate Mean Time to Prioritize (MTTP) and consider this as Prioritize incident

$$MTTP = \frac{\text{Number of Incidents}}{\text{Time to prioritize incidents}}$$

Now Calculate

$$MTTC = \frac{\text{Number of incidents}}{\text{Time taken to contain incidents}}$$

Step 6: Analyze the collected the data based on event or Incident then calculate Mean Time to Investigate.

$$MTTI = \sum \frac{\text{Time taken to investigate incidents}}{\text{Number of incidents investigated}}$$

Step 7: Finalize the Response time using Step 5 & Step 6.

$$MTTR = MTTP + MTTC + MTTI$$

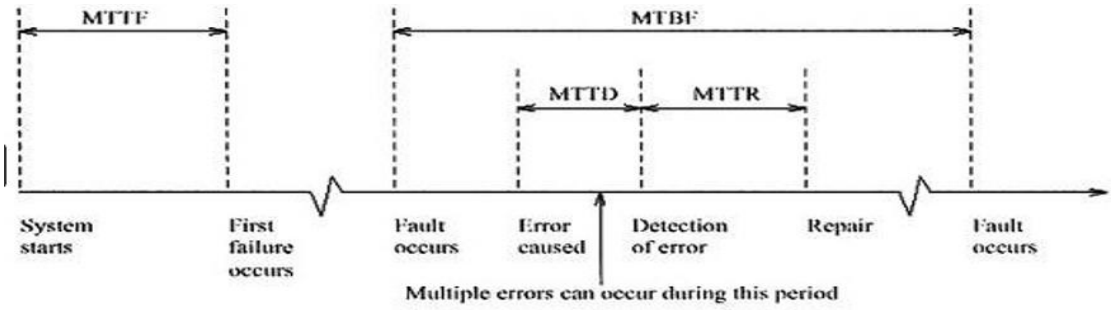

Figure 2 Relation Between MTTF & MTTR, MTTD[13]

IV. MINIMIZING INCIDENT HANDLING TIME

In the realm of incident response within cloud environments, the paramount objective is to minimize incident handling time[9], defined as the duration between the discovery (Ds) and response (Rs) of an attack. This optimization is expressed through the formula:

$$W=\text{Min}[T(IHn)]=\text{Min}[t(Rs)-t(Ds)]....(2)$$

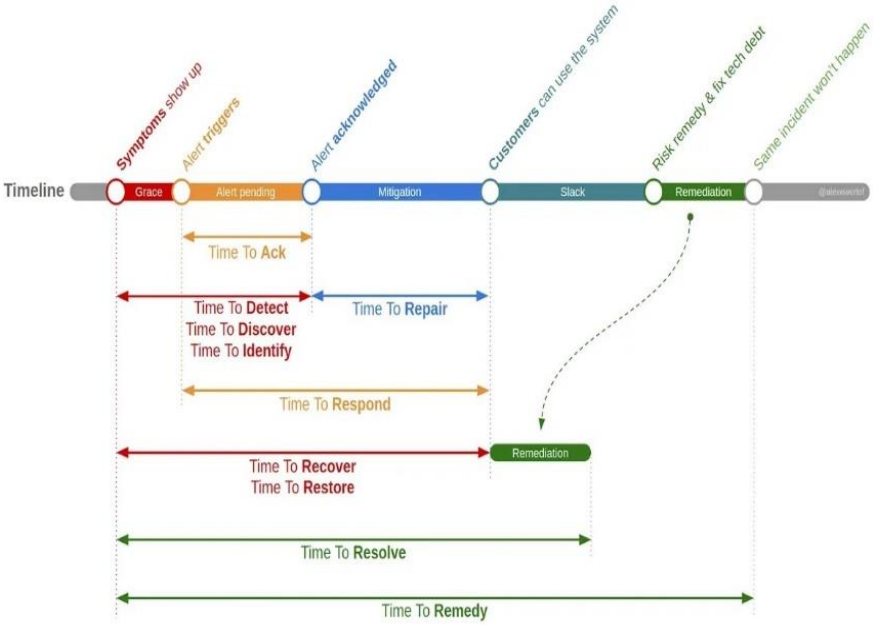

Figure 3 Metrics of Incident Response[3]

	Grace	Pending	Mitigation	Slack	Remediation
MTTAck	-	Yes	-	-	-
MTTDetect	Yes	Yes	-	-	-
MTTIdentify	Yes	Yes	-	-	-
MTTRepair	-	-	Yes	-	-
MTTRespond	-	Yes	Yes	-	-
MTTRecover	Yes	Yes	Yes	-	-
MTTRestore	Yes	Yes	Yes	-	-
MTTResolve	Yes	Yes	Yes	-	Yes
MTTRemedy	Yes	Yes	Yes	Yes	Yes

Table 1.Periods each MTT* metric measures

Efficient incident handling involves reducing time across every stage {Table 1}. of the response procedure post-discovery. Each stage is denoted as follows:

D: Detection

I: Identification

E: Escalation

R: Response

P: Incident retrospective

It's imperative to underscore that incident handling time excludes the time allocated for Preparation and Lessons Learned stages. Consequently, the formula (2) simplifies to:

$$W=\text{Min}[T(\text{IH}n)]=\text{Min}[T(\text{Detection})]+\text{Min}[T(\text{Identification})]+\text{Min}[T(\text{Escalation})]+\text{Min}[T(\text{Response})]+\text{Min}[T(\text{Incident retrospective})]\text{……..}(3)$$

This formula underscores the essence of time efficiency in cloud incident response models. Achieving time reduction entails the integration of new architectural elements, such as management and threat analysis infrastructure, seamlessly embedded within the cloud environment.

V. Cloud event Response Model

In the landscape of cloud environments, incident handling encounters several challenges, including:

- Aggregation and notification of security alerts (Detection)
- Management of security policies (Identification)
- Reconfiguration of networks (Identification)
- Collection of data.
- Scanning of Workstation (Detection)
- Execution of remediation and recovery scripts
- Modification of credential and certificates
- Application of security updates (Incident retrospective)

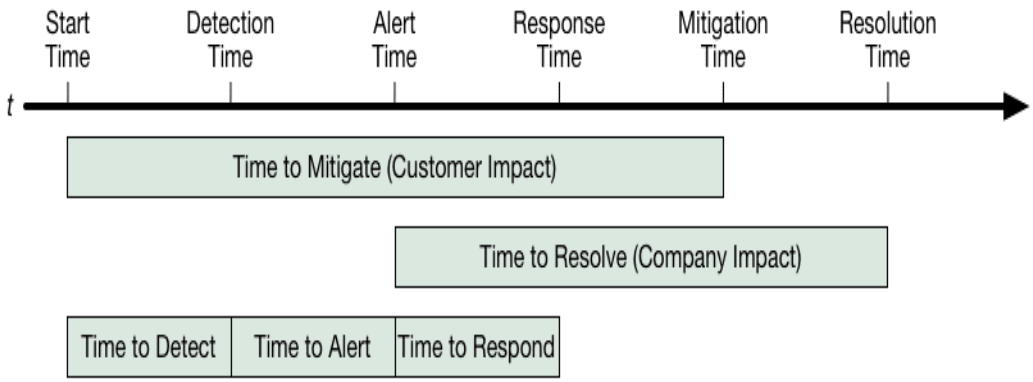

Figure 4 Enhance the responsiveness of incident handling [6].

To effectively address these issues, specific architectural elements are recommended for integration into the cloud environment, aiming to streamline incident handling and reduce incident response time[10]

• The Discovery module's Logging, Monitoring, and Alerts (LMA) module[12]
• Virtualization of Networking Services(VNS) for network scanning and security policy administration (Incident retrospective)
• The Security Domain, which includes threat analysis and forensic tools (Investigation)
•These components must be included in the architecture of a cloud environment in order to support seamless incident response operations, which will save the Incident Response Team (IRT) a great deal of time and effort.

The cloud incident response model can be delineated as follows:

1.Initiation:

Assembling an Incident Response Team (IRT) comprising individuals with diverse expertise.

Crafting a comprehensive incident response blueprint tailored to the cloud environment.

Enabling Software-Defined Networking (SDN) and Network Function Virtualization (NFV) capabilities to facilitate dynamic response.

Deploying a Security Controller to oversee and manage security measures across the cloud infrastructure.

Defining and structuring a Security Domain to delineate boundaries and responsibilities within the cloud environment.

2. Identification

Utilization of security scanners or operators triggering alerts via the LMA module.

3. Response:

Minimization of damage by transferring compromised assets to the Security Domain using the Security Controller.

4.Investigation:

a. Data collection, including forensic imaging, via the Security Domain.

b. Threat analysis within the Security Domain.

c. Assessment of information losses.

5.Remediation:

a. Implementation of remediation recommendations, including the removal of malicious code and altering compromised credentials, using Security Controller(SC).

b. Restoration of hosts and network devices from backups.

c. Scanning of recovered assets initiated by the Security Controller.

d. Restoration of assets to operational status.

6. Incident retrospective:

Description of event prevention measures, such as protocol revision and security updates, facilitated by the Security Controller.

7.Lessons Learned:

CONCLUSIONS

From the above article the challenge of cloud event response, various Cloud models. It stresses the importance of architectural redundancy to minimize incident or event response time. Key enhancements include Software Define Network with Network Function Virtualization, Expanding the cloud management infrastructure involves integrating a Security Controller (SC) to oversee security measures, while establishing a dedicated Security Domain for analyzing threats and conducting forensic investigations related to cloud events. the essence of the cloud alerting using response model centers on the integration of robust security controls and tools, fostering adaptability in network and security management.

ACKNOWLEDGMENT

The authors of this study self-funded and did not seek outside funding; they also revealed no relationships of concern.

REFERENCES

[1] Computer Security Incident Handling Guide, NIST 800 61, Sep 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.S P.800-61r2.pdf

[2] Information security incident management (ISO/IEC 27035-1:2016), Sep 2016 https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed 1:v1:en

[3] Incident Handler's Handbook, SANS Institute, Sep 2016, https://www.sans.org/reading room/whitepapers/incident/incident-handlers-handbook 33901

[4] Felix C. Freiling, Bastian Schwittay, A Common Process Model for Incident Response and Digital Forensics, IMF 2007, Stuttgart, September 2007, http://www.imf conference.org/imf 2007 /2%20Freiling%20common_model.pdf
[5] G. Grispos, W. B. Glisson, T. Storer, Rethinking Security Incident Response: The Integration of Agile Principles, Sep 2016, https://arxiv.org/ftp/arxiv/papers/1408/1408.2431.pdf
[6] Brent Chapman, www.greatcircle.com, Great Circle Associates, Inc, Apr 4, 2023
[7] Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643-652.
[8] Mitropoulos, S., Patsos, D., and Douligeris, C. 2006. "On Incident Handling and Response: A State of-the-Art Approach," Computers & Security (25:5), pp. 351-370.
[9] S Kai, T Shigemoto, T Kito, S Takemoto, T Kaji, ESEM '12: 2012 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement Lund Sweden 21 September 2012, https://doi.org/10.1145/2372225.2372232
[10] Gnatyuk, S., Berdibayev, R., Smirnova, T., Avkurova, Z., Iavich, M. (2021). Cloud-Based Cyber Incidents Response System and Software Tools. In: Lopata, A., Gudonienė, D., Butkienė, R. (eds) Information and Software Technologies. ICIST 2021. Communications in Computer and Information Science, vol 1486. Springer, Cham. https://doi.org/10.1007/978-3-030-88304-1_14
[11] Charles, E., Samuel, M., Roger, N., et al.: Pat. № US20020038430 A1. System and method of data collection, processing, analysis, and annotation for monitoring cyber-threats and the notification thereof to subscribers (2012)
[12] Adebola, Orogun. (2020). Reliability And Replication Techniques For Improved Fault Tolerance In Distributed Systems. 10.13140/Rg.2.2.10586.49607