International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

IMPROVING THE SECURITY INCIDENT RESPONSE PROCESS IN CLOUD INFRASTRUCTURE ENVIRONMENTS

Karthik Chandrashekar
Staff Software Engineer
Intuit Inc
ckinnovative@gmail.com

Vinay Dutt Jangampet
Staff Software Engineer
Intuit Inc
yanivdutt@gmail.com

Abstract

Cloud computing has dramatically reshaped how organizations provision, deploy, and manage business-critical applications. Offering unmatched scalability, flexibility, and cost-efficiency, the cloud environment also introduces unique security challenges that can outpace traditional incident response (IR) strategies. Conventional IR frameworks—encompassing Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-Incident Activity, and Testing—were originally designed for more static, on-premises infrastructures and can prove insufficient when defending against large-scale, rapidly evolving threats in complex cloud ecosystems.

This paper presents an enhanced incident response model tailored to the dynamic characteristics of cloud computing. At its core, our approach emphasizes high-fidelity threat detection, automated containment tools, and continuous posture management to address recurring vulnerabilities. First, we propose an iterative methodology for refining detection rules, employing multiple stages—Draft, Monitoring, and Real-Time Execution—to progressively improve alert precision while minimizing false positives. By the time a rule reaches real-time mode, it is expected to exhibit near 100% accuracy, thus dramatically reducing alert fatigue and false alarms.

We then detail an automated containment mechanism that leverages snapshots and granular resource lockdown. Upon recognizing a verified threat, the system captures the state of the affected instances for forensic analysis before quarantining them from the broader environment. This immediate isolation helps halt potential data exfiltration, lateral movement, and service disruption. Concurrently, cloud-specific security controls—such as security group rules, access policies, and credential rotation—ensure comprehensive lockdown of the compromised resource.

Next, our model focuses on eradication through continuous posture management (CSPM). Rather than merely removing compromised virtual machines or containers, we advocate a holistic remediation strategy that identifies and fixes the underlying misconfigurations or software flaws. Automated vulnerability scans paired with baseline posture assessments enable a swift discovery of root causes, closing gaps that attackers could exploit again. This culminates in a structured recovery phase, where validated updates and patches are deployed, and resources are carefully

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

reintroduced into production, ensuring minimal downtime and reducing the risk of re-infection.

Finally, we integrate post-incident activities—including thorough forensic review, compliance reporting, and lessons-learned sessions—to drive continuous improvement. Testing remains a pivotal element, supported by routine drills, red-team exercises, and feedback loops that further refine detection, containment, and remediation procedures. Collectively, these enhancements result in a resilient, scalable incident response architecture optimized for cloud-specific challenges.

In closing, our proposed enhancements—spanning the entire IR lifecycle—empower security teams to respond to incidents faster, more accurately, and with greater clarity regarding underlying causes. By mitigating alert fatigue, speeding containment, and fostering root-cause eradication, this framework equips organizations with the agility and depth of insight needed to thrive in a continuously evolving threat landscape. Our findings underscore the critical role of high-fidelity detection, automated resource lockdown, and robust posture management in modern cloud security. We conclude by outlining practical steps for adoption and highlighting areas for future work, including the broader integration of machine learning analytics, cross-cloud orchestration, and advanced forensic capabilities.

I. INTRODUCTION

The widespread adoption of cloud computing has significantly reshaped the information technology (IT) landscape, introducing a myriad of opportunities alongside equally intricate challenges in managing and securing IT assets. The inherent advantages of cloud platforms, such as on-demand scalability, resource pooling, and broad network access, offer organizations unprecedented agility and cost-efficiency. These features enable businesses to scale their operations dynamically, optimize resource utilization, and focus on innovation rather than infrastructure management. However, the same qualities that make the cloud attractive also introduce complexities and expand the attack surface, creating unique security challenges for organizations.

In traditional on-premises IT environments, security incident response (IR) is guided by a well-established framework comprising six primary phases: (1) Preparation, (2) Detection and Analysis, (3) Containment, (4) Eradication, (5) Recovery, and (6) Post-Incident Activity. This framework has proven effective in addressing security threats within controlled, static environments. However, the shift to cloud platforms disrupts these traditional approaches. Unlike static on-premises infrastructures, cloud environments are characterized by multi-tenancy, ephemeral workloads, geographically distributed resources, and complex service-level agreements (SLAs). These distinct features demand a revaluation and enhancement of existing IR practices to effectively address cloud-specific security threats.

Cloud-specific challenges are numerous and multifaceted. Multi-tenancy, a core feature of cloud platforms, involves multiple organizations sharing the same physical hardware, creating potential security vulnerabilities. Ephemeral workloads, such as server less functions or containerized applications, further complicate detection and response as these workloads can be instantiated or terminated within seconds. Moreover, the dynamic nature of cloud resource allocation makes tracking and logging activities more difficult, increasing the likelihood of delayed detection and

mitigation of security incidents. Distributed resources across multiple data centers and regions also add a layer of complexity to incident response coordination, as organizations must navigate varying regulatory and compliance requirements.

Another critical challenge in cloud environments is the lack of integrated and effective tools for detecting, containing, and remediating complex attacks. Traditional IR tools often struggle to provide high-fidelity alerts in dynamic, fast-paced cloud settings. The prevalence of false-positive alerts exacerbates this issue, leading to "alert fatigue"—a phenomenon where security analysts become desensitized to alerts due to their high volume and low relevance. This fatigue increases the risk of genuine threats being overlooked, resulting in potential data breaches or service disruptions.

Containment operations in the cloud present additional hurdles. While isolating or terminating compromised resources is a standard approach, the automation required to perform these actions at scale introduces technical and operational challenges. Snapshots, isolation, or deletion of resources must be executed swiftly to prevent lateral movement of threats while minimizing downtime and preserving business continuity. These operations must also comply with organizational policies and regulatory standards, adding another layer of complexity.

To address these challenges, this paper proposes an enhanced cloud security incident response model. Building upon the traditional six-phase IR cycle, our model introduces refinements specifically tailored for cloud environments. Key enhancements include a focus on high-fidelity detection mechanisms, automated containment strategies, and robust posture management practices to streamline eradication and recovery efforts. By leveraging automation, advanced analytics, and proactive posture management, this model aims to empower organizations to respond effectively to cloud-specific security threats while maintaining operational resilience.

The remainder of this paper is structured as follows: Section II provides a review of related work on cloud security incidents and existing frameworks, highlighting gaps in traditional approaches. Section III introduces the proposed enhancements to the IR model, detailing their design and implementation. Section IV discusses operationalization strategies, emphasizing practical steps for integrating the enhanced model into existing cloud environments. Section V explores the benefits and limitations of the proposed approach, offering insights into its potential impact on organizational security. Finally, Section VI concludes the paper with recommendations for future research and practical directions for improving cloud incident response.

II. BACKGROUND AND RELATED WORK

2.1 Traditional Incident Response in Cloud

Incident response (IR) in cloud computing environments retains the core phases—Preparation, Detection, Containment, Eradication, Recovery, Post-Incident Analysis, and Testing—but requires an agile and dynamic adaptation to meet the unique demands of cloud ecosystems. Researchers have highlighted the challenges of maintaining consistent visibility across diverse cloud components, including virtual machines (VMs), containers, and virtual networks. In the shared responsibility model prevalent in cloud computing, customers are tasked with securing their applications and data within defined boundaries, while cloud service providers (CSPs) manage the

underlying infrastructure. This arrangement necessitates close collaboration between customers, CSPs, and third-party security vendors to ensure comprehensive protection.

One significant challenge in cloud environments is ensuring adequate forensic capabilities. Martini and Choo (444) noted that the ephemeral nature of cloud storage and dynamic resource provisioning can hinder effective evidence preservation and digital forensics. When incidents occur, critical data or logs may be lost if not captured promptly, complicating investigations. To address these issues, cloud security posture management (CSPM) solutions have emerged as essential tools. These solutions automatically scan cloud environments for known vulnerabilities and misconfigurations, enhancing visibility and reducing the attack surface.

By integrating these tools into the incident response process, organizations can proactively identify potential risks, streamline detection efforts, and improve their ability to respond effectively to cloud-specific threats. Such advancements underscore the need for an evolved incident response framework tailored to the complexities of cloud ecosystems.

2.2 Tools and Automation

Automated detection and response mechanisms are critical in modern cloud security practices. Several researchers, including Modi et al., have emphasized the need for automation in intrusion detection systems (IDS) to address the challenges posed by high alert volumes and frequent false positives. High alert volumes can overwhelm human analysts, reducing their ability to focus on genuine threats. Reducing false positives in IDS is, therefore, a priority, as it ensures that analysts can efficiently allocate their efforts to addressing confirmed security incidents. Effective automation refines detection capabilities, providing maximum fidelity and contextual accuracy before initiating containment measures. This capability not only reduces manual intervention but also minimizes the time to respond to potential threats, improving overall security posture.

Containment strategies in cloud environments typically involve actions such as snapshotting compromised instances, revoking compromised credentials, and isolating networks or subnets. These approaches serve to limit the lateral movement of attackers and mitigate potential damages. However, despite their widespread adoption, many existing solutions lack the ability to provide real-time response features. This gap creates opportunities for malicious actors to exploit short windows of opportunity to execute their attacks, such as data exfiltration or launching further compromises.

The automation of containment mechanisms is vital to address this challenge. By incorporating real-time monitoring and response capabilities, cloud security systems can detect anomalous activities and trigger containment protocols instantly. For instance, the automation of snapshotting ensures that forensic data is preserved while isolating the compromised resource from the operational environment. Similarly, automated credential revocation prevents further misuse of compromised accounts, and network isolation halts the spread of malicious traffic within the cloud infrastructure. These measures, when integrated into a seamless and automated workflow, significantly reduce the attacker's window of opportunity.

Moreover, the use of machine learning (ML) and artificial intelligence (AI) in tools and automation has proven to enhance the efficacy of intrusion detection and containment processes. ML models

can analyze vast amounts of data to identify patterns indicative of threats, while AI-driven decision-making systems can recommend or execute containment actions based on predefined criteria. These technologies enable a proactive security posture, where potential threats are identified and neutralized before they escalate into full-scale incidents.

Despite these advancements, challenges remain in achieving fully automated containment. Factors such as the accuracy of threat detection, integration complexities, and the potential for unintended disruptions must be carefully managed. For example, overly aggressive automated responses could lead to the unnecessary shutdown of critical services, impacting business operations. Balancing automation with controlled human oversight is, therefore, essential to maintain the integrity and availability of cloud resources while ensuring robust security.

To address these challenges, many organizations are adopting hybrid approaches that combine automated tools with human-in-the-loop systems. This strategy leverages the strengths of both automation and human expertise, ensuring a rapid yet reliable response to threats. Additionally, organizations are increasingly investing in advanced automation frameworks that incorporate threat intelligence feeds, behaviour-based anomaly detection, and real-time incident response capabilities. These frameworks provide a comprehensive solution for detecting, analyzing, and containing security threats in cloud environments.

In conclusion, the integration of tools and automation in cloud security is pivotal to overcoming the limitations of traditional approaches. By focusing on reducing false positives, enabling real-time containment, and leveraging advanced technologies such as AI and ML, organizations can significantly enhance their ability to detect and respond to threats. The continued evolution of automated security solutions will play a crucial role in safeguarding cloud infrastructure against the ever-growing landscape of cyber threats.

2.3 Gaps in Existing Practices

Despite progress in tools for monitoring, logging, and governance, many organizations still rely on manual processes or semi-automated workflows that are not scalable 888. Moreover, most incident response guidelines focus on detection and analysis but provide less emphasis on how to achieve near 100% fidelity in alerting, how to automate containment effectively, or how to carry out comprehensive eradication with minimal downtime.

The literature highlights the importance of continuous vulnerability management. Traditional vulnerability scanning schedules may fail to detect newly introduced misconfigurations in highly dynamic cloud settings 999. This gap can lead to repeated incidents exploiting the same vulnerabilities. Therefore, a renewed focus on posture management throughout the entire incident response lifecycle is required.

III. PROPOSED APPROACH

To address the gaps in traditional Incident Response (IR) processes, we propose an enhanced methodology that augments the standard phases with additional controls and automation specific to cloud infrastructure. Our framework aligns with the NIST guidelines and best practices outlined

in prior research but incorporates the following focal points to address the unique challenges of cloud environments:

High-Fidelity Detection Rules

One of the primary enhancements is the introduction of a structured, iterative process to refine detection rules. Detection rules often require continuous tuning to minimize false positives and maximize their effectiveness. In our proposed approach, new rules follow a three-stage lifecycle:

1. **Draft Mode:** New detection rules are created and evaluated in a controlled test environment. During this phase, the rules are adjusted to eliminate false positives and improve accuracy.
2. **Monitoring Mode:** Rules are deployed to monitor real-world environments. Alerts generated during this stage are reviewed manually to ensure the rules are functioning as intended without disrupting operations.
3. **Real-Time Execution Mode:** Once detection rules consistently demonstrate near 100% true positives, they graduate to active use in real-time environments, enabling automated responses to identified threats.

This structured process ensures that detection rules are both robust and reliable before they are relied upon for automated incident response actions.

Automated Containment Tools

Containment is a critical step in the IR process, and automation is essential to achieving rapid and effective containment. Our proposed framework includes an integrated set of APIs and scripts designed to perform the following actions:

- **Snapshotting Impacted Resources:** Automate the creation of snapshots for compromised instances to preserve forensic evidence while minimizing data loss.
- **Locking Down Network Activity:** Immediately isolate affected instances by applying restrictive network security policies to prevent lateral movement and data exfiltration.

These tools are designed to operate in real-time, reducing the attacker's window of opportunity and ensuring that containment is both swift and effective.

Comprehensive Eradication via CSPM

Post-containment, our approach leverages Cloud Security Posture Management (CSPM) systems to ensure comprehensive eradication of threats. CSPM systems perform the following functions:

- **Vulnerability Scanning:** Identify misconfigurations, open vulnerabilities, and compliance issues across cloud resources.
- **Automated Fixes:** Apply patches or configuration changes to eliminate identified vulnerabilities.
- **Verification:** Perform re-scanning to confirm that all issues have been resolved and the environment is secure.

This step ensures that the root cause of the incident is fully addressed, reducing the risk of recurrence.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

Structured Recovery Process

Recovery involves restoring affected services while ensuring that the vulnerabilities that led to the incident have been resolved. Our structured recovery process includes the following steps:

1. **Automated Validation Checks:** Use automated tools to confirm that all vulnerabilities have been remediated before reintroducing recovered resources.
2. **Gradual Reintroduction**: Restore services systematically, starting with low-priority resources and progressing to critical systems, to minimize potential disruptions.
3. **User Verification**: Validate with end-users and stakeholders that services are functioning as expected post-recovery.

This process ensures that recovery is thorough and minimizes the risk of reintroducing vulnerabilities into the production environment.

Continuous Posture Management and Testing

Security is an ongoing process, and continuous posture management plays a critical role in maintaining resilience. Our approach emphasizes the following:

- **Continuous Scanning and Assessment:** Conduct regular vulnerability scans and compliance checks as part of routine operations, not just in response to incidents.
- **Table top Exercises**: Simulate incident scenarios through table top exercises to test the readiness of the IR process.
- **Red-Team Drills:** Conduct red-team drills to identify gaps in detection, response, and containment capabilities, and use the findings to improve the IR process.

By integrating these activities into daily operations, organizations can proactively identify and address vulnerabilities, ensuring a state of continuous improvement.

Figure 1

Figure 1 outlines the proposed enhancements integrated into the traditional IR cycle, showcasing the additional layers of automation, structured processes, and continuous improvement measures.

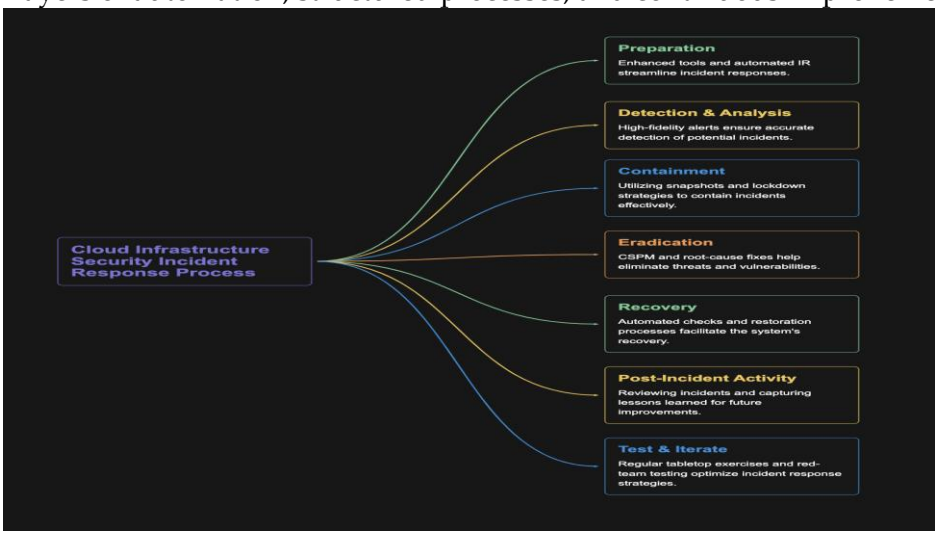

Figure 1. Enhanced Incident Response Life Cycle with Cloud-Focused Improvements

IV. IMPLEMENTATION AND DISCUSSION

4.1 High-Fidelity Detection Rules

One of the primary issues in cloud environments is the volume of alerts that security analysts must evaluate. High false-positive rates cause alert fatigue, leading analysts to overlook genuine threats. To address this, we propose a phased approach to detection rules:

- **Draft Mode:** New or updated detection rules are first deployed in a passive or "draft" environment, collecting statistics on how often they trigger and how relevant the alerts are.
- **Monitoring Mode:** After initial tuning, move the rules to a "monitoring" environment where they generate alerts but do not trigger automated containment. The rules continue to be refined based on real-world data.
- **Real-Time Execution Mode**: Once a rule consistently demonstrates near 100% precision, it can be upgraded to active mode, where it triggers real-time automated containment.

This workflow ensures that only the most accurate alerts can initiate high-impact actions, minimizing disruptive false positives 777. The iterative feedback loop from analysts is crucial, as it provides the contextual intelligence needed to refine rule logic continuously.

4.2 Automated Containment Tools

In cloud environments, manual containment procedures are often impractical, given the rapid elasticity of services. We propose integrating containment workflows with Infrastructure-as-Code (IaC) scripts and CSP APIs:

1. **Snapshot Creation:** Immediately upon detecting a potential compromise, the system triggers the creation of snapshots for affected VMs or containers. This snapshot serves as a forensic baseline for subsequent investigation and evidence collection 444.
2. **Resource Lockdown**: The compromised instance is automatically quarantined from the network by applying updated firewall rules or security group policies. This prevents further data exfiltration and lateral movement within the cloud environment.
3. **Credential Rotation**: If any access credentials (e.g., API keys, tokens) are suspected of compromise, the automation rotates or revokes them.

These steps can be orchestrated via server less functions or CI/CD pipelines that interface with the CSP's APIs, enabling near real-time response.

4.3 Comprehensive Eradication via CSPM

Eradication in the cloud context extends beyond deleting a resource or restoring a snapshot; it involves identifying and remediating the root cause. A single misconfiguration in security groups or an unpatched vulnerability could lead to repeated breaches 555. Cloud Security Posture Management (CSPM) tools play an integral role in scanning the environment for misconfigurations.

- **Vulnerability Identification:** CSPM solutions automatically identify known Common Vulnerabilities and Exposures (CVE) in the OS, middleware, and application layers of the affected resources.
- **Baseline Deviation Detection:** Many CSPM tools track a baseline posture and can detect significant deviations. If the attacker exploited a newly introduced misconfiguration, the

solution flags it for remediation.

- **Remediation Verification:** After applying patches or reverting configurations, a subsequent scan verifies that the root cause is indeed addressed.

4.4 Structured Recovery

Once the root cause has been eradicated, the organization must carefully reintegrate affected systems into production. Our framework prescribes:

1. **Validation Testing:** Automated scripts verify the integrity of the recovered system, ensuring no residual malware or vulnerabilities.
2. **Performance/Load Testing**: If the incident impacted a business-critical service, performance and load tests confirm that the system meets pre-incident benchmarks.
3. **Gradual Reintroduction**: Instead of instantly returning the recovered resources to full production load, a gradual approach allows monitoring for any anomalous behavior.

This systematic recovery reduces the risk of reintroducing compromised components or triggers.

4.5 Continuous Posture Management and Testing

A key failing in many organizations is the lack of continuous validation. Post-incident activities often focus on root-cause analysis and documentation but rarely maintain the necessary vigilance to prevent repeat incidents. We integrate:

- **Ongoing Vulnerability Scanning:** CSPM and other security scanners run on a regular schedule (daily or weekly) to catch configuration drift.
- **Regular IR Drills:** Tabletop exercises and red-team engagements test the incident response workflows, ensuring the new tools and processes function under realistic pressure.
- **Metrics & Reporting:** Key performance indicators (KPIs) such as "Time to Detect" (TTD), "Time to Contain" (TTC), and "Time to Restore" (TTR) are tracked to identify trends and drive improvements.

V. BENEFITS AND LIMITATIONS

5.1 Benefits

1. **Reduced Alert Fatigue:** By moving detection rules through draft, monitoring, and real-time execution modes, security teams face fewer false positives.
2. **Rapid Containment**: Automated snapshotting and quarantine reduce the window for data exfiltration and lateral attacks.
3. **Thorough Eradication**: Leveraging CSPM tools ensures that vulnerabilities and misconfigurations leading to the breach are fully addressed, preventing recurrence.
4. **Structured Recovery**: Automated checks allow safe reintroduction of resources to production, minimizing the risk of residual compromise.
5. **Continuous Improvement**: Built-in testing cycles drive iterative improvements to both detection logic and posture management.

5.2 Limitations

1. **Tooling Dependencies**: The proposed model relies heavily on CSP APIs, CSPM tools, and automation scripts. Organizations with limited DevSecOps maturity may face steep adoption

curves.

2. **Potential Overhead:** Iterative rule refinement requires initial manual effort from analysts, especially during the "Draft" and "Monitoring" phases.
3. **Cost Considerations**: Cloud snapshots, additional scanning tools, and quarantined instances can incur additional cloud service charges, which may be prohibitive for smaller entities.

VI. CONCLUSION

The advent of cloud computing has necessitated a fundamental revaluation and enhancement of traditional incident response (IR) processes. Unlike on-premises environments, cloud ecosystems introduce complexities such as multi-tenancy, ephemeral workloads, and distributed resources. These challenges require a proactive and adaptive approach to ensure security and resilience. This paper introduces a comprehensive framework designed to address these challenges, focusing on high-fidelity alerting, automated containment, posture management-driven eradication, and rigorous recovery steps.

Our proposed framework emphasizes the importance of high-fidelity detection to minimize false positives. By refining detection rules through a structured lifecycle—from draft to monitoring to real-time execution—organizations can achieve a higher degree of confidence in their alerts. This reduces the noise that often overwhelms human analysts and allows them to focus on genuine threats. Automated containment further enhances the speed and efficacy of incident response by isolating compromised instances, snapshotting affected resources, and locking down network activity. These actions limit attackers' ability to move laterally or exfiltrate data, significantly reducing the impact of security incidents.

Posture management-driven eradication ensures that incidents are not merely contained but thoroughly addressed at their root cause. Leveraging Cloud Security Posture Management (CSPM) tools, organizations can identify vulnerabilities, apply automated fixes, and verify remediation. This comprehensive approach minimizes the risk of recurrence and ensures that environments remain secure. Recovery processes are equally critical, and our framework advocates for structured recovery steps that validate the remediation of vulnerabilities before reintroducing resources to production. This methodical approach reduces the likelihood of reintroducing weaknesses into the operational environment.

Continuous posture management and regular testing further strengthen organizational resilience. By integrating vulnerability assessments, tabletop exercises, and red-team drills into routine operations, organizations can identify and address gaps in their incident response processes. These proactive measures ensure readiness for emerging threats and foster a culture of continuous improvement.

Looking ahead, future work in this domain should prioritize the integration of advanced machine learning (ML) techniques to further enhance detection capabilities and reduce false positives. ML models have the potential to analyze large datasets, identify patterns indicative of threats, and recommend or execute containment actions with minimal human intervention. Additionally, the development of cross-cloud orchestration tools that offer vendor-neutral automated responses could bridge the gap between heterogeneous cloud environments, enabling seamless incident

response across platforms such as AWS, Azure, and Google Cloud.

Another critical area for exploration is the impact of data privacy regulations on incident response measures. As regulatory requirements evolve across regions, organizations must balance the need for rapid containment and eradication with compliance obligations. For instance, data localization requirements or restrictions on transferring data across borders may influence how containment and recovery processes are executed. Studies could provide valuable insights into best practices for navigating these complexities without compromising security.

By adopting the proposed enhancements and aligning them with evolving best practices, organizations can bolster their cloud security posture and mitigate incidents effectively at scale. The framework outlined in this paper serves as a blueprint for addressing the unique challenges of cloud environments while fostering a proactive, adaptive, and resilient approach to incident response. As threats continue to evolve, it is imperative that organizations embrace innovation and collaboration to stay ahead of adversaries and protect their critical assets.

REFERENCES

1. S. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A Survey of Intrusion Detection Systems in Cloud Computing," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42-57, Jan. 2013.
2. S. Subashini and V. Kavitha, "Cloud Security Issues and Challenges: A Survey," International Journal of Computer Applications, vol. 47, no. 2, pp. 19-23, Feb. 2011.
3. M. Almorsy, J. Grundy, and A. S. Ibrahim, "Toward Achieving Automated Incident Response in Cloud Environments," in Proc. IEEE 5th Int. Conf. Cloud Comput., Honolulu, HI, USA, 2012, pp. 484-491.
4. S. Pearson and A. Benameur, "Security and Privacy Challenges in Cloud Computing Environments," in Proc. IEEE 3rd Int. Conf. Cloud Comput., Miami, FL, USA, 2010, pp. 93-100.
5. B. Grobauer, T. Walloschek, and E. Stocker, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," IEEE Commun. Surveys Tuts., vol. 13, no. 3, pp. 50-57, 2011.
6. K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "Cloud Computing Security Issues and Challenges: A Survey," Int. J. Inf. Manage., vol. 33, no. 5, pp. 494-501, Oct. 2013.
7. M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "An Analysis of Security Challenges in Cloud Computing," in Proc. Int. Conf. Adv. Comput. Sci. Appl. Technol., Kuala Lumpur, Malaysia, 2012, pp. 190-195.
8. P. M. Mell, K. Scarfone, and S. Romanosky, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Cloud Comput., Washington, DC, USA, 2013, pp. 217-224.
9. Z. Xiao and Y. Xiao, "Security Issues and Solutions in Cloud Computing: A Survey," IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 853-858, 2013.
10. M. R. Asghar, G. Russello, and B. Crispo, "A Survey of Security Concerns in Cloud Computing: Solutions and Challenges," ACM Comput. Surveys, vol. 44, no. 1, pp. 1-31, Jan. 2012.
11. T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Perth, WA, Australia, 2010, pp. 27-33.
12. J. Heiser and M. Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner, June 2008. [Online]. Available: https://www.gartner.com
13. W. Rittinghouse and J. Ransome, Cloud Computing: Implementation, Management, and

Security. Boca Raton, FL, USA: CRC Press, 2010.
14. E. Grosse and M. Upadhyay, "Authentication at Scale," IEEE Secur. Privacy, vol. 11, no. 1, pp. 15-22, Jan. 2013.
15. D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583-592, Mar. 2012.
16. H. Takabi, J. B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Secur. Privacy, vol. 8, no. 6, pp. 24-31, Nov. 2010.
17. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," J. Supercomput., vol. 63, no. 2, pp. 561-592, Feb. 2013.
18. S. Bouchenak, "Automated Management of Multi-Tier Internet Applications in the Cloud," IEEE Trans. Cloud Comput., vol. 2, no. 2, pp. 171-183, Apr. 2014.
19. P. Samarati and S. De Capitani di Vimercati, "Access Control: Policies, Models, and Mechanisms," in Foundations of Security Analysis and Design. Berlin, Germany: Springer, 2001, pp. 137-196.
20. K. Hwang, D. Li, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," in Proc. IEEE Int. Conf. Dependable, Auton. Secur. Comput., Chengdu, China, 2011, pp. 717-722.