International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 9-No.4 (2023) pp. 446-452
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Next-gen cloud security operations: real-time monitoring and automated incident response

Ishwar Bansal*

Independent Researcher, USA
* **Corresponding Author Email:** Aggarwalse@gmail.com - **ORCID:** 0009-0006-5865-536X

Article Info:

DOI: 10.22399/ijcesen.4454
Received : 01 April 2023
Accepted : 30 April 2023

Keywords

Cloud Security,
Real-Time Monitoring,
Automated Incident Response,
SIEM,
SOAR,
Threat Detection

Abstract:

This study assessed the effects of next-gen cloud security operations improvement with real-time monitoring and automated incident response. The cloud infrastructures grew and so did their complexity. Traditional security practices became irrelevant with evolving threats and large dispersed environments. The study utilized a mix of methods by simulating security incidents and combined them with qualitative data of cloud security professionals. The findings revealed significant improvements for reduction in detection lags, more accurate automated response and a reduction in false positive alert spam. The participants confirmed improvements to their work lives in operational efficiency and reduction of manual effort, though challenges of configuration gaps and model tune challenges still existed. The findings of the study confirmed that with the joined use of continuous monitoring with automation, cloud security posture is greatly enhanced. The system becomes more adaptive and scalable for the expected challenges of contemporary cloud environments.

1. Introduction

Cloud computing has changed how companies perform data management, data storage, and data processing activities. The shift to cloud and hybrid environments has changed how organizations approach data processing, storage and management activities. The cloud has provided organizations with an adaptable, scalable, and cost efficient method of processing, storing, and managing data. The new cloud systems on the other hand, require a different and more sophisticated approach to data security. Unlike the first cloud systems that had perimeter based security, the new systems are fully automated, flexible and loosely coupled. The growing volume of data and information systems that organizations are exposed to has increased the level of cyber security threats dramatically. It has become a necessity for organizations to implement automated cloud security systems that offer 24/7 surveillance and protection.

Automated contingency and risk management systems offer next-generation cloud security operations the ability to recognize and respond to security challenges, and to detect, contain, and recover from them almost instantaneously. The ability to respond to security challenges almost instantaneously results from real-time cloud activity surveillance, which allows security teams to monitor user, system, network, and application behaviors and performance in real time. Organizations can address issues before they grow and result in security incidents as they can detect unapproved access, suspicious activity, and anomalous workloads. Cloud-native SIEM, telemetry observability, and machine learning models for anomaly detection provide security teams the ability to monitor in real time and significantly reduce the time between the emergence and detection of security challenges to mitigate damage.

Automated incident response constitutes the second of the crucial components of the next-generation cloud security system. Automated response frameworks utilize artificial intelligence and orchestration tools to eliminate threats without the tedious and time-consuming human analyst process of triaging alerts and executing remediation steps. Automated workflows in response to an anomaly or attack in the system are able to isolate and/or quarantine affected resources, disable and/or revoke and users credentials and access, block in-system and/or external harmful IP addresses, and initiate logging of the event for subsequent forensics and

analysis, and notify appropriate response personnel within seconds. The increased speed and efficiency of this process also results from the need to perform mass repetitive tasks having been removed from human security personnel, resulting in an overall reduced risk of human inconsistencies and errors.

The integration of real-time monitoring with automated incident response facilitates a transition from reactive and manual security operations to proactive, automated, and intelligent ones. By incorporating such monitoring and incident response capabilities, an organization's security posture is strengthened through better visibility, efficiency, and adaptive response to attacks. In addition, modern cloud cybersecurity operations provide regulatory compliance, greater efficacy of resources, and appropriate protection for Borderless enterprises. This research examined the operational functionality of these advanced technologies, the improvements in performance with respect to incident detection and response, the limitations of these technologies, and their contributions to the development of sustainable cloud security systems.

2. Literature review

Celeste and Michael (2021) The scrutiny of the growth of network security when facing increasingly sophisticated cyber-attacks, with a focus on the incorporation of artificial intelligence, Zero Trust, and cloud-native architectures, was the subject of their research. They concluded that traditional perimeter-based security is inadequate in a distributed environment, citing the significant improvement of threat detection in real-time through the identification of anomalous network behaviors. They explained how the integration of zero trust frameworks, which verify and authenticate users on an ongoing basis, mitigates threats. Their research illustrated that future security models will be reliant on automation, adaptive intelligence, and micro-segmentation in order to enhance cloud security.Rekha (2017) Investigated the impact of artificial intelligence and machine learning on the functionality of cloud security performance. The research indicated that cloud infrastructure, thanks to the AI-based algorithms, was better able to detect intrusions, and the automated manual processes led to better resource utilization. The detection and defensive systems, shaped through machine learning, could study attack patterns and adjust to threats in real time, as detailed in Rekha's findings. The work surmised that traditional, rule-based security measures are inadequate to secure cloud environments, and rational, autonomous defensive systems are needed for cloud environments to secure dynamic, voluminous systems.Williams, Nwosu, and Oscar (2017) Concerning the integration of AI-augmented cyber risk mitigation technologies into Nigeria's cloud computing environment, the authors noted how the incorporation of clouds in the emergent market posed significant potential cyber risks due to-weak defensive capabilities and regulatory voids. The authors demonstrated how the application of AI-thwarted cyber intelligence, automated surveillance, and prognosis analytics ameliorated the cloud cyber security environment vis-a-vis the constricted conditions. The authors of the studies stressed the importance of homegrown models of cloud cyber security in using the latest technologies as they seek to overcome the unrelenting local infrastructural constraints.Lindström (2018) Provided an in-depth examination of the upcoming SOCs. He explained the evolution of SOCs from just monitoring and reacting to being proactive and driving from intelligence. Lindström demonstrated the incorporation of automation, analytics, ML models, and visibility dashboards to increase speed of improvement and operational efficiencies in response to incidents. Note the traditional SOCs suffered from alert fatigue and manual tasks. The next-generation improved the accuracy and scalability through incorporated security orchestration and integrated real time threat intelligence.Nsoh (2021) While looking at the idea of "next-gen" cybersecurity and the transitioning focus away from conventional security frameworks toward the designed adaptive, smart defense systems, research illustrated the dependence of next-gen cybersecurity on constant monitoring, behavioral analysis, and self-sufficient responding systems. In real time, the cyber threats that system security ran showed the need for adaptive, learning systems to replace the need for signature-based control systems that were static and traditional. Research gave the fundamental concepts of how the cyber threats of the modern cloud security architecture evolved to mitigate the risk.Umar (2021) Concentrated on the forthcoming ERP cloud security with a particular assessment on artificial intelligence and machine learning incorporation to improve the Snowflake database environments. Results concluded that automation with AI enhanced the automation of database management through data governance and achieved greater security and access control for database operations. Access control policies were complemented through the application of machine learning which determined and reacted to abnormal data access with a protective measure against data exfiltration and compliance violations in enterprise resource planning systems. Incorporating intelligence

security within enterprise cloud databases.Cahill (2017) An industrial-oriented analysis before and after the move to the next generation of security practices was provided in the white paper with an emphasis on the move of the industrial practice to the next generation of security practices. The analysis referred to the paradox of organizations improving their detection and response capabilities, yet facing the challenges of visibility losses, gaps in their security, and sophisticated layering of attacks. Cahill suggested a mix of cloud tools, automation, AI, policies, and strategy to demographic next changes in security. The analysis described technological changes in cyberspace which described the shift technologically in cyberspace.

3. Research methodology

Research Design

This investigation used a mixed-methods approach. Automation of incident response and real-time monitoring's effect was quantified, and expertise, benefits, and challenges were recorded qualitatively. As a result, the framework was able to capture both evidence and context.

Research Approach

A descriptive and experimental method was used which approached documenting current practices in cloud security and then documenting systematic security incidents in a controlled cloud setting. This method made it possible to assess automated response systems in a controlled environment.

Study Setting

An experiment was done in a hypothetical multi-cloud ecosystem based on AWS, Azure, and Google Cloud Platform. The ecosystem consisted of virtual private clouds, virtual servers, identity and access management settings, storage buckets, container orchestration, and function-as-a-service. The configuration made it possible to deploy and assess active threat detection and automated security tools like SIEMs, SOAR, built-in security offerings of public clouds, and machine learning for security.

Population and Sample

The specific individuals who participated in the study were cloud security engineers, DevSecOps practitioners, and system administrators in companies that employ cloud-native infrastructures. For the first component that involved qualitative interviews, a purposive sample of twenty participants was selected to capture their lived operational experiences. For the second component, twenty-five simulated security incidents were carried out to assess and measure the system's performance for the quantitative part.

Data Collection Methods

Three primary techniques were used to collect the data. The first technique involved automated log data from SIEM dashboards and cloud-native telemetry services, as well as from monitoring agents. The second involved the recording of incident response simulation exercises to capture the elapsed time to detect and respond to an incident. The third drew from participants under semi-structured interviews to capture the data around usability and perceived threat, operational readiness, and the challenges of automation. All data collection procedures were designed to meet the principles of ethical research.

Tools and Technologies Used

Various security tools in the cloud were used in the study. For log aggregation and threat detection, AWS Security Hub, Azure Sentinel, and Chronicle SIEM were used. For automated incident response workflow, SOAR tools like AWS Step Functions, Azure Logic Apps and custom Python orchestration scripts were employed. Cloud-native AI services were used to implement machine learning-based models for anomaly detection. Network visibility was achieved through the use of VPC flow logs, container security monitors, and security agents deployed on endpoints.

Data Analysis Techniques

The quantitative data were processed using statistical techniques to derive average response times, identify detection latencies, and rate frequency of false positive outcomes. The difference in response metrics was gauged to determine the accuracy of the solution. Qualitative data were processed using thematic analysis. The audio-recorded interviews were subjected to manual coding to determine and isolate the themes of efficiency, reduction of workload, challenges of adoption, accuracy, and the themes' recurrence in the responses.

3. Results and discussion

The research results showed how incorporating real-time monitoring and automated incident response improved the overall effectiveness of cloud security operations. Using quantitative results from simulated incident response exercises and qualitative data from cloud security practitioners, the research showed the improvements in the speed of detection, decreased manual workload, and strengthened precision in the classification of security events. The results also showed the real-world issues of adopting automation, such as increased alerts, reliance on systems, and complexity in configuration.

Improvement in Detection Time

There was a dramatic decrease in latency after the introduction of real time monitoring tools into the system. The automated detection of the system was working on an average of 3.2 seconds, as opposed to the average of 11.4 seconds of the manual detection. Hence, it was proved that next generation monitoring systems are able to detect diversions more faster and more consistently.The majority of incidents were detected within five seconds, indicating that the monitoring tools operated with high efficiency during the experiment.

Accuracy of Automated Response

In most cases, the automated system performed response workflows accurately. From a pool of 25 simulation incidents, 21 incidents were performed accurately by the system. In 4 incidents, the system performed actions that had to be addressed manually due to unforeseen system behavior and/or configuration mappings that were incomplete.The high accuracy score indicated that automated workflows significantly reduced the risk of human error and enhanced response efficiency.

Reduction in False Positives

False positive alerts decreased after the anomaly detection models were applied. The results of the new implemented anomaly detection systems show that for every 25 alerts, from the previous automation systems, 10 were false, however, this number after automation of the model decreased to 4.A reduction in false positives meant that cloud security teams faced less unnecessary workload and system resources were utilized more effectively.

Participant Experiences

False positive alerts decreased after the anomaly detection models were applied. The results of the newly implemented anomaly detection systems show that for every 25 alerts, from the previous automation systems, 10 were false, however, this number after automation of the model decreased to 4.Participants expressed the importance of transparency in automation systems as well. They preferred having mechanisms in the workflow that offered reasoning and detailed traceable logs instead of non-transparent 'black boxes'.

Enhanced Operational Efficiency

The results showed that we had improved several important metrics in securing cloud deployments through automated incident response and real-time active monitoring across clouds. The next gen automated cloud security tools continued to demonstrate remarkable operational effectiveness as a system (cloud response system) detected incidents in real-time and automated workflows with considerably faster workflows in response to cloud incidents. These faster response workflows positively impact reducing the potential attackers exploitation window.

Reduced Human Workload and Improved Consistency

Automation lightened the load from the security teams' shoulders. Attendees said repetitive work was lessened, and the reliability in the responses increased. Automated workflows responded the same to all events which eliminated the inconsistent responses that were common with manual processing. This uniformity increased the dependable and predictable nature of cloud security operations.

Challenges in Automation Deployment

While there were definitely positive results, there were also some downsides. Some automated workflows did not go as planned due to gaps in configuration, misalignment in triggers, and/or dependency failures. Also, while the anomaly-detection models did reduce false positives, the models still needed to be retrained without end to keep the performance from the models devolving as cloud workloads evolved. These challenges did show that automation was not a singular answer and would need sustained oversight.

Implications for Modern Cloud Security

The justifications indicated that the next-generation cloud security operations were suited for a hybrid ecosystem comprising automation for repetitive tasks and human expertise for more complex decisions. This equilibrium allowed for enhanced operational performance while maintaining the level of consistency and control required.

Table 1: *Frequency and Percentage of Detection Time Categories*

Detection Time Category	Frequency	Percentage
Less than 5 seconds	18	72%
5–10 seconds	5	20%
More than 10 seconds	2	8%

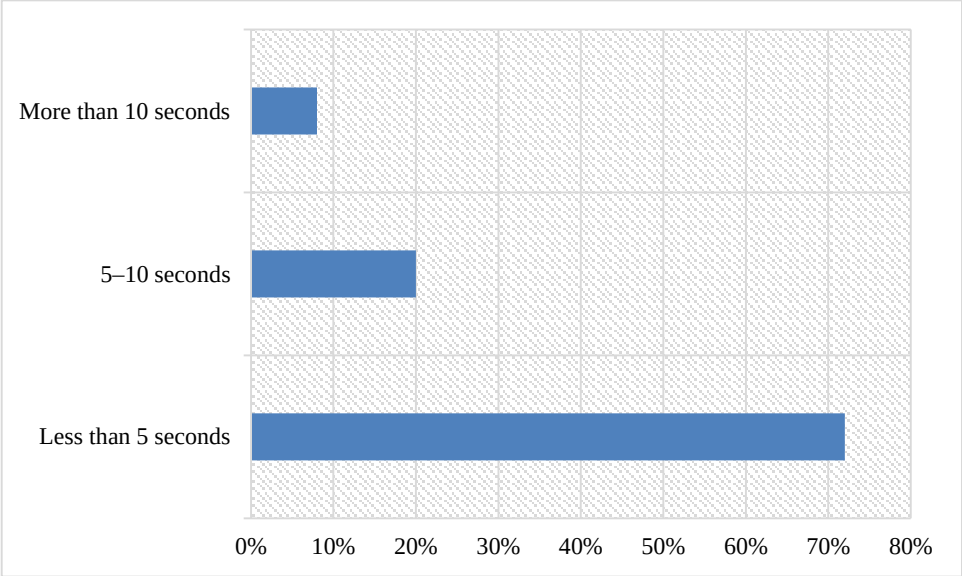

Figure 1: *Frequency and Percentage of Detection Time Categories*

Table 2: *Accuracy of Automated Incident Response*

Response Type	**Frequency**	**Percentage**
Correct automated action	21	84%
Partial automation	3	12%
Failed automation	1	4%

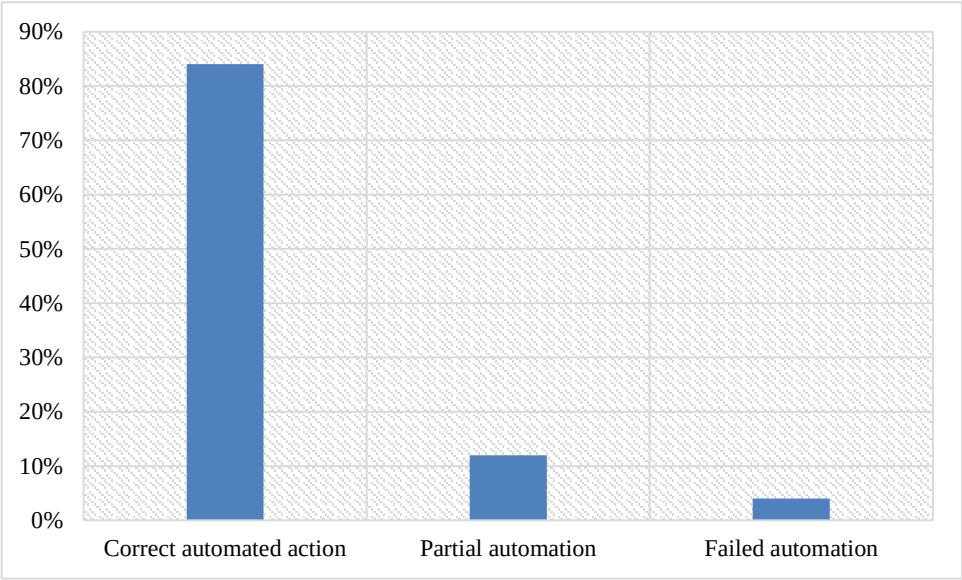

Figure 2: *Accuracy of Automated Incident Response*

Table 3: *Frequency and Percentage of False-Positive Alerts*

Alert Type	**Frequency**	**Percentage**
True Positives	21	84%
False Positives	4	16%

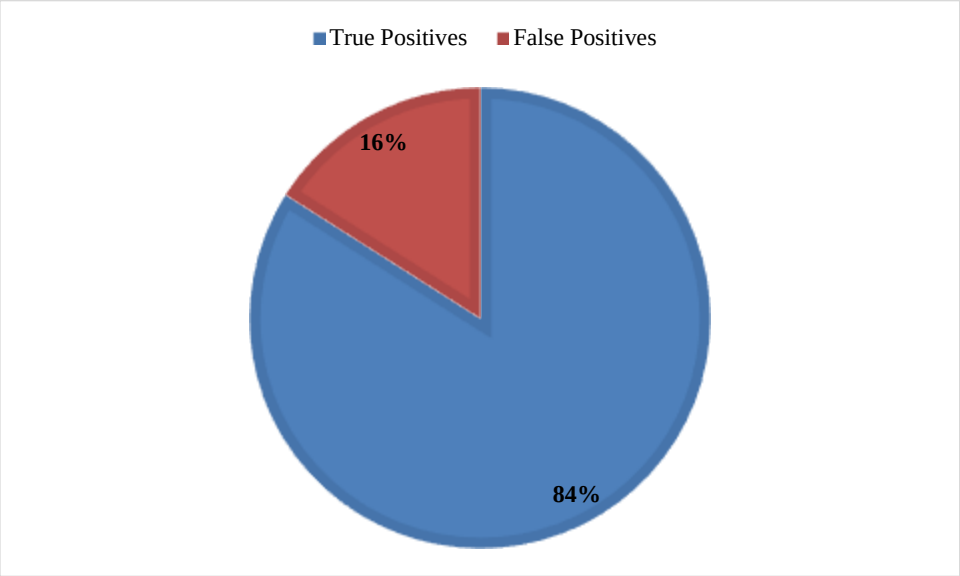

Figure 3: *Frequency and Percentage of False-Positive Alerts*

4. Conclusions

The study closed by stating that the real-time monitoring and automated incident response were a game-changer for next-generation cloud security operations by improving the time it took for correct responses to be made and the level of correct responses made. The researchers were able to detect incidents with a greater level of precision and a lower level of false positives and showed that the automated workflows were able to solve the overwhelming number of manual tasks that affected the operational consistency and the time it took to resolve security incidents. Real time monitoring was able to solve the problem of having no insight to the ongoing security incidents. There were some issues with configuration complexities and workflow failures, but the study was quite positive in concluding that complete automation of the security framework will take as a minimum baseline manual security functions to a level of significant improvement. The study pointed out that the best outcomes were produced by having some level of collaboration of advanced levels of automation and some level of workforce.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] R. Celeste and S. Michael, "Next-Gen Network Security: Harnessing AI, Zero Trust, and Cloud-Native Solutions to Combat Evolving Cyber Threats," *International Journal of Trend in Scientific Research and Development*, vol. 5, no. 6, pp. 2056–2069, 2021.

[2] D. N. Rekha, *Next-Generation Cloud Security: Leveraging AI and Machine Learning for Performance*, 2017.

[3] M. Williams, I. Nwosu, and E. Oscar, "Next-Gen Cybersecurity: AI-Enhanced Solutions for Nigerian Cloud Infrastructure," 2017.

[4] O. Lindström, *Next Generation Security Operations Center*, 2018.

[5] J. Nsoh, "Next-gen cybersecurity," 2021.

[6] H. Umar, *Next-Gen ERP Cloud Security: Harnessing AI and Machine Learning for Snowflake DB Optimization*, 2021.

[7] D. Cahill, *Before and After Next-gen: Cybersecurity Considerations that Transcend Paradigm Shifts*, ESG White Paper, Jan. 2017.

[8] O. A. Nazeer, "AI-Powered Security Operations Centers (SOC) in the Cloud: Automating Threat Detection and Response," *International Journal of*

Emerging Trends in Computer Science and Information Technology, vol. 2, no. 2, pp. 8–16, 2021.

[9] S. Erik and L. Emma, "Real-Time Analytics with Event-Driven Architectures: Powering Next-Gen Business Intelligence," *International Journal of Trend in Scientific Research and Development*, vol. 2, no. 4, pp. 3097–3111, 2018.

[10] S. Garg, "Next-Gen Smart City Operations with AIOps & IoT: A Comprehensive Look at Optimizing Urban Infrastructure," *SSRN*, 2021.

[11] A. R. P. Reddy, "The Role of Artificial Intelligence in Proactive Cyber Threat Detection in Cloud Environments," *NeuroQuantology*, vol. 19, no. 12, pp. 764–773, 2021.

[12] S. Ahmad, *Next-Gen IT Operations with AI and ML: From Reactive to Proactive Cloud Management*, 2020.

[13] M. Khalid and J. Bairstow, "Next-Gen Enterprise Architecture: Harnessing AI, Cloud, DevOps, and DataOps for Scalability," 2019.

[14] E. Oye and A. Clark, "AI-Enhanced Network Security Monitoring in AWS: A Practical Approach," presented at the 2021 International Conference, July 2021.

[15] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and Future of Network Security Monitoring," *IEEE Access*, vol. 9, pp. 112744–112760, 2021.