Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

AWS Security Monitoring System with Datadog Integration

Puneeth M
B Tech in CSE
MS Ramaiah University of Applied Sciences

Gayathri V
B Tech in CSE
MS Ramaiah University of Applied Sciences

B Kavya
B Tech in CSE
MS Ramaiah University of Applied Sciences

Bhavana N
B Tech in CSE
MS Ramaiah University of Applied Sciences

Deepak Varadam
Assistant Professor, CSE
MS Ramaiah University of Applied Sciences

ABSTRACT **- This research paper provides Strong, real-time monitoring solutions are required for cloud systems since they pose special security issues. This paper presents a serverless cloud security monitoring solution that is connected with Datadog and created for Amazon Web Services (AWS). To give thorough insight into security issues, the solution makes use of AWS services including Lambda, S3, Guard Duty, Inspector, and WAF in addition to Datadog's visualization and alerting tools. The architecture ensures scalable and maintainable deployments by utilizing Terraform' s Infrastructure as Code (IaC). To find possible security events, statistical methodologies and anomaly detection techniques are used. The project's results show excellent integration, scalability, cost-effectiveness, and real-time monitoring, providing a workable answer for businesses looking to improve their cloud security posture.**

KEYWORDS**: Cloud Security, AWS, Datadog, Serverless, Infrastructure as Code, Security Monitoring, Anomaly Detection, Real-Time Alerting.**

1.INTRODUCTION

Due to the fact that cloud computing offers scalability, agility, and cost efficiency, its quick adoption has completely changed how businesses function. But there are also new security issues brought forth by this change. Because cloud-native settings are distributed and dynamic, traditional security models—which were created for on-premise infrastructure—frequently fail to meet these needs. Cloud infrastructure security necessitates proactive threat detection, ongoing monitoring, and an efficient incident response procedure.

1.1 The need for Cloud Security Monitoring

Many security risks, such as malware outbreaks, insider threats, data breaches, and misconfigurations, can affect cloud environments. Customers bear a large portion of the responsibility for protecting their data and apps on the cloud thanks to the shared responsibility model used by cloud providers. For these risks to be identified and promptly mitigated, minimizing possible damage and ensuring regulatory compliance, effective security monitoring is essential.

1.2 Challenges in Managing Security in Cloud-Native Environments

When it comes to handling security in cloud-native systems, organizations confront a number of challenges:

• Complexity: Because cloud environments are frequently dynamic and complicated, it can be challenging to have a thorough understanding of the security environment.
• insight: Threat identification and incident response may be hampered by a lack of insight into cloud resources and activities.
• Scalability: To adapt to the evolving requirements of cloud environments, security systems must be elastically scalable.
• Configuration Management: One of the biggest challenges is making sure that all cloud resources are configured securely and consistently.
• Skill Gap: An organization's capacity to efficiently manage security may be hampered by a lack of qualified

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

cloud security specialists.
• Integration: It can be difficult and time-consuming to integrate security products with current DevOps platforms and workflows.

1.3 Proposed solutions and its advantages

A serverless cloud security monitoring solution created to tackle those problems is presented in this study. The following fundamental ideas are utilized by the system:

• Serverless Architecture: By removing the need to manage underlying infrastructure, AWS Lambda and other serverless services improve scalability and lower operational overhead.
• Real-time Monitoring: Constant observation of AWS resources and services offers real-time insight into any security risks.
• Integration with Datadog: Security teams can swiftly detect and address security incidents thanks to Datadog's potent visualization and alerting features.

Terraform facilitates automated deployment and configuration management for Infrastructure as Code (IaC), guaranteeing scalability and consistency. Following are some of the advantages of the suggested solution:

• Increased Visibility: Better insight into AWS security activities and events.
• Quicker Threat Detection: Potential security problems can be identified more quickly thanks to real-time monitoring and anomaly detection.
• Lower Operational Overhead: Serverless architecture lowers operating expenses and streamlines management.
• Improved Scalability: To adapt to shifting demands, the system automatically scales.
• Enhanced Compliance: Organizations can better comply with regulations when they have thorough security monitoring.

2. LITERATURE REVIEW

Current cloud-based security monitoring systems frequently use cloud-native security technologies separately or rely on conventional security information and event management (SIEM) solutions. Cloud security monitoring features are available on a number of open-source and commercial platforms.

2.1 Overview of existing security monitoring

• Conventional SIEM systems: Security logs from cloud settings can be gathered and examined using conventional SIEM systems like Splunk and QRadar. These solutions might not be tailored for the dynamic nature of cloud systems, though, and they can be costly to implement and maintain.
• Cloud-Native Security Tools: AWS CloudTrail, AWS GuardDuty, and Azure Security Center are just a few of the security tools that cloud providers provide. Although these products offer insight into cloud security events, they might not be as integrated and correlated as more conventional SIEM solutions.
•Cloud Security Posture Management (CSPM) Solutions: These solutions concentrate on locating and fixing cloud environment configuration mistakes and compliance infractions. Usually, these solutions provide automated evaluations and suggestions for enhancing security posture.

• Security Orchestration, Automation, and Response (SOAR) Solutions: These solutions automate vulnerabilities, threat hunting, and incident response, among other security duties. Security teams can react to security incidents more rapidly and efficiently with the aid of these technologies.

2.2 Gaps addressed by proposed solution

A number of shortcomings in conventional security monitoring systems are addressed by the suggested remedy:
• Lack of Integration: Complex configuration and integration work are typically necessary for traditional SIEM solutions to seamlessly integrate with cloud-native applications. For improved visualization and alerting, our solution interacts with Datadog and makes use of native AWS capabilities.
• Scalability Problems: Because cloud settings are dynamic, traditional solutions could find it difficult to grow
• High-priced Deploying and maintaining traditional SIEM solutions can be costly. Our approach is more affordable because to AWS services' pay-as-you-go pricing structure and serverless design.
• Restricted Real-time Visibility: Timely threat identification and incident response are hampered by existing solutions' frequent lack of real-time visibility into security events. Our technology enables a quicker response to security problems by offering real-time alerting and continuous monitoring.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

3. SYSTEM ARCHITECTURE AND METHODOLOGY

Several AWS services are used in the serverless architecture of the AWS security monitoring system to gather, process, and analyze data. Datadog is incorporated for alerting and visualization. The system is made to be easily managed, scalable, and economical.

3.1 Serverless Architecture

Serverless technologies are used in the implementation of the system's essential components:

• AWS Lambda: Security events from different AWS services are gathered using Lambda functions, which then process and send the information to Datadog. A scalable and reasonably priced computing infrastructure for event-driven processing is offered by Lambda.

• Amazon S3: S3 is a central location to store data and security records. It is appropriate for long-term storage due to its affordability and scalability.

• Amazon EventBridge: This tool forwards security events for processing from AWS services (GuardDuty, Inspector, and WAF) to the relevant Lambda functions.

• IAM (Identity and Access Management): To provide AWS services with permissions and guarantee safe resource access, IAM roles and policies are utilized.

3.2 Data Collection from AWS Security Services

The following AWS security services provide data to the system:

• AWS GuardDuty: GuardDuty identifies illegal and harmful activity. GuardDuty results are gathered by the system and sent to Datadog for evaluation and notification.
• AWS Inspector: This tool evaluates the security flaws in container images and EC2 instances. The discoveries of vulnerabilities are gathered and sent to Datadog.
• AWS WAF (Web Application Firewall): WAF guards against frequent online threats. Potential attacks are identified by gathering and analyzing WAF records.

Real-time data collecting is made possible by lambda functions that are set up to run in response to events from these services.

3.3 Anomaly Detection Techniques

To find odd patterns of behavior that can point to a security risk, the system uses anomaly detection algorithms. Metrics like this are analyzed using statistical techniques:

• Network Traffic: keeping an eye on network flows to spot odd trends or traffic peaks.
• API Usage: Examining API requests for excessive or illegal use.
• User Activity: Monitoring user behavior to look for questionable activities, like accessing private information or trying to log in from odd places.

Lambda functions use anomaly detection tools, like time series forecasting and standard deviation analysis, find departures from typical behavior.

4. DATADOG INTEGRATION

The AWS security monitoring system is linked with Datadog to offer reporting, alerting, and visualization features.

4.1 Visualization and Alerting

• Custom Dashboards: To illustrate important security trends and metrics, Datadog dashboards are made. These dashboards offer a thorough summary of the AWS environment's security posture.
• API Integration: To programmatically send security data to Datadog and set up alerts, the system makes use of the Datadog API.
• Real-time Alerting: Datadog monitors are set up to sound an alarm in response to anomaly detection algorithms or predetermined criteria. Security teams receive alerts through Slack, email, and other lines of contact.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

4.2 Real-Time Alerting Capabilities

The alerting features of Datadog enable the creation of multiple alert types. When a measure above or falls below a predetermined threshold, a threshold alert is triggered.

• Anomaly Alerts: Set off when anomalous behavior is detected by Datadog's anomaly detection algorithms.
•Composite Alerts: Set off when several criteria are satisfied.
• Event-Based Alerts: Set off by particular occurrences, like WAF security incidents or GuardDuty discoveries

5. INFRASTRUCTURE AS A CODE WITH TERRAFORM

Terraform is used to manage the infrastructure for the AWS security monitoring system.

5.1 Benefits of using Terraform

• Automation: Terraform minimizes human error and effort by automating the deployment and configuration of AWS resources.
• Consistency: Terraform guarantees a repeatable and consistent deployment of the infrastructure.
• Version Control: Terraform configurations may be tracked and rolled back to earlier versions thanks to their storage in version control systems.
• Modularity: Terraform makes it easier to deploy and maintain complex infrastructure by enabling the development of reusable modules.
• Scalability: Terraform facilitates the infrastructure's easy scaling to meet fluctuating workloads.

5.2 Modularity, Version Control, and Scalability

By virtue of its modular architecture, the Terraform setup enables the reuse and customization of individual components. Changes are tracked using Git version control, which makes it easier to collaborate and rollback as needed. The IaC methodology guarantees that the system can be quickly and reliably scaled to meet expanding cloud environments and data volumes.

6. SECURITY AND COMPLIANCE MEASURES

Security is a paramount consideration in the design and implementation of the AWS Security monitoring systems.

6.1 IAM Policies and Encryption

• IAM Policies: These policies allow AWS resources to be accessed with the least amount of privilege. Only the permissions necessary to access the information and services needed for their particular jobs are given to lambda functions. In a similar manner, IAM policies limit access to S3 buckets.
• Encryption: Server-side encryption is used to protect data in S3 while it is at rest. TLS is used to encrypt data as it is moving between AWS services.

6.2 Log Management and Operational Security

• Log Management: To monitor API calls and other activity within the AWS account, CloudTrail logs are enabled. S3 is where these logs are kept for compliance and auditing purposes.
• Operational Security: Only authorized workers are able to access the Terraform infrastructure and the AWS account. Every AWS user has multi-factor authentication (MFA) enabled.

6.3 Adherence to Compliance Standards

The system is made to facilitate adherence to common security guidelines and standards, including:
• SOC 2: The system offers the logging and monitoring features required to meet SOC 2 specifications.
• HIPAA: For protected health information (PHI), the system facilitates the application of HIPAA security standards.
• PCI DSS: The solution assists businesses in adhering to the PCI DSS standard's security requirements for safeguarding cardholder data.

7. RESULTS AND ACHIEVEMENTS

The implementation of AWS Security Monitoring system has yielded several positive results:

7.1 Successful Integration and Real-time Monitoring Outcomes:

• Smooth Integration: Real-time data gathering and analysis are made possible by the successful integration of Datadog with AWS security services.
• Better Visibility: Better insight into AWS security incidents and activity throughout the whole cloud infrastructure.
• Quicker Threat Detection: Potential security threats can be identified more quickly thanks to real-time monitoring and anomaly detection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

7.2 Cost-Effectiveness and Scalability

• Cost reductions: When compared to conventional security monitoring solutions, AWS services' serverless architecture and pay-as-you-go pricing model yield notable cost reductions.
• Scalability: As the cloud environment expands, security monitoring keeps up with the system's automatic scaling to handle shifting workloads.

8. FUTURE ENHANCEMENTS

The following features can be added to the AWS security monitoring system to further improve it:
• CloudTrail Integration: For more extensive logging and auditing features, integrate with AWS CloudTrail.
• ML-based Threat Prediction: Using past data, apply machine learning algorithms to forecast upcoming security risks.
• Real-time Remediation: Automate security incident remediation in real time.
• SIEM Integration: For centralized security monitoring and analysis, integrate with current SIEM solutions.
• Automated Vulnerability Scanning: combining AWS Inspector with additional tools for vulnerability assessment to provide ongoing threat intelligence and scanning.
• Custom Rule Development: Developing adaptable regulations and guidelines in accordance with particular organizational or industry compliance needs.

9. CONCLUSION

This paper presented a serverless cloud security monitoring solution that was created for AWS and connected with Datadog. To give thorough insight into security issues, the solution makes use of AWS services including Lambda, S3, Guard Duty, Inspector, and WAF in addition to Datadog's visualization and alerting tools. The architecture ensures scalable and maintainable deployments by utilizing Terraform's Infrastructure as Code (IaC). The project's results show excellent integration, scalability, cost-effectiveness, and real-time monitoring, providing a workable solution for businesses looking to improve their cloud security posture. By offering a scalable, affordable, and real-time monitoring solution, the system successfully tackles the difficulties associated with contemporary cloud security. The system's threat detection and response capabilities will be further improved in future updates, allowing businesses to better defend their cloud environments against changing security threats.

10. REFERENCES

[1] M. Hillbert and P. Lopez, “The World’s Technological Capacity to Store, Communicate and Compute Information,” Compute Information Science, vol. III, pp. 62-65, 2011.

[2] Statista, “Statista,” 2020. [Online] Available: https://www.statista.com/statistics/871513/worldwide-data-created/

[3] Amazon Web Services, “AWS Security Overview.” 2023. Available: https://aws.amazon.com/security/

[4] Datadog, “Datadog Security Monitoring,” 2023. Available: https://www.datadoghq.com/product/cloud-siem/

[5] Terraform, “Infrastructure as Code,” 2023. Available: https://developer.hashicorp.com/terraform

[6] Krebs, B. “Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door.” Sourcebooks, Inc., 2014.

[7] Anderson, R. “Security Engineering.” John Wiley & Sons, 2020.

[8] Northcutt, S., & Novak, J. “Network Intrusion Detection: An Analyst’s Handbook.” New Riders, 2000.

[9] Vacca, J. R. “Cloud Security: Protecting the Enterprise.” Syngress, 2009.

[10] Subhashini, S., & Kavitha, V. “A survey on security issues in service delivery models of cloud computing.” Journal of Network and Computer Applications, 34(1), 1-11, 2011.

[11] Mell, P., & Grance, T. “The NIST Definition of Cloud Computing.” National Institute of Standards and Technology, 2011.

[12] Zissis, D., & Lekkas, D. “Addressing cloud computing security issues.” Future Generation Computer Systems, 28(3), 583-592, 2012.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

[13] Ryan, M. D. “Cloud computing security risks.” Wiley Interdisciplinary Reviews, 5(1), 51-59, 2013.

[14] M. Malathi, “Cloud Computing Concepts”, IEEE 2011.

[15] Dillon, T., Wu, C., & Chang, E. “Cloud computing: Issues and Challenges.” 24th IEEE International Conference on Advanced Information Networking and Applications.

[16] Takabi, H., Joshi, J.B.D., & Ahn, G. J. “Security and privacy challenges in cloud computing environments.” IEEE Security & Privacy, 8(6), 24-31, 2010.

[17] Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. “The rise of “big data” on cloud computing: Review and open research issues.” Information Systems, 47, 98-115, 2015.

[18] Al-Masri, E., & Tsai, W. T. “Context-aware security monitoring and management for cloud services.” Journal of Internet Services and Applications, 3(1), 1-16, 2012.

[19] Amazon GuardDuty Documentation, “AWS Threat Detection Service”, Available: https://docs.aws.amazon.com/guardduty/

[20] Amazon Inspector Documentation, “Automated Security Assessment Service”, Available: https://docs.aws.amazon.com/inspector/