Domain 6: Security Monitoring

Introduction

This domain presents security monitoring challenges and solutions for cloud environments. It emphasizes the distinct aspects of cloud telemetry, management plane logs, service and resource logs, and the integration of advanced monitoring tools. It explores the complexities of hybrid and multi-cloud setups, including interoperability and security considerations. Further highlighted is the critical role of logs, events, and configuration detection in comprehensive security monitoring. Lastly follows the introduction of Artificial Intelligence (AI) as an innovative tool for enhancing cloud security and providing a multi-faceted approach to protecting cloud infrastructures.

Learning Objectives

In this domain, you will learn to:

- Identify unique security monitoring challenges in cloud environments.
- Describe the importance of cloud telemetry sources in monitoring cloud environments.
- Analyze collection architectures for security telemetry in cloud environments.
- Recognize monitoring and alerting as foundational components of cloud security.
- Implement detection paths for comprehensive security monitoring.

6.1 Cloud Monitoring

Here are factors that drive complexity in security monitoring:

1. **Management plane:** The management plane controls all administrative actions, like a captain navigating a ship. The cloud console must be monitored closely because it makes the most critical decisions and grants access to everything in the cloud.

2. **Velocity:** Changes occur in the cloud at a high speed. This rapid pace means security processes must be agile, and automated responses are necessary to keep up with potential threats.

3. **Distribution and segregation:** Cloud resources are spread out and isolated, like compartmentalized sections of a large warehouse. As a result, to perform effective monitoring - a degree of centralization of the logs and configuration is also required.

4. **Cloud sprawl:** This refers to the widespread proliferation of diverse workload types and the adoption of multiple CSPs within a CSC environment. It is the phenomenon of dispersed cloud assets across various platforms and services that complicates security monitoring and management.
5. **Allocation of Responsibility:** the shared security responsibility model (SSRM) indicates that the CSC will be responsible for some aspects of monitoring, while the CSP will handle others. This will vary by service.

6.1.1 Logs & Events

Logs and events are foundational in security monitoring, compliance, accountability, and the broader context of cloud security and risk management practices. They provide crucial insights into the activities and behaviors occurring within cloud applications. They provide anomaly detection, but also forensics data and operational insights. They are different for each CSP.

Logs provide detailed records of all system activities, including Create, Read, Update, and Delete (CRUD) operations, and are usually stored for long-term analysis. Log delivery can sometimes be delayed, and quality may vary.

In contrast, *events* focus on key system changes, such as Create, Update, and Delete (C-UD) actions, triggered by specific security alerts. They are temporary and lack the detailed context of logs but are valuable for their immediacy, often available seconds after the activity occurs, enabling rapid response.

6.2 Beyond Logs - Posture Management

In security, posture refers to an organization's overall defensive readiness against potential threats. Logs are essential for security monitoring, but the cloud offers new monitoring capabilities. Cloud service configurations are often easy to review with a simple query, which provides opportunities for monitoring based on analyzing the organization's posture management.

Security posture management involves continuously monitoring the organization's cloud configurations. It includes analyzing the current state for security misconfigurations, comparing the current configuration to various best practices and standards, alerting on potential vulnerabilities and attack vectors, and prioritizing the remediation process.

6.3 Cloud Telemetry Sources

Cloud telemetry sources offer visibility into the organization’s cloud environments, tracking everything from management actions to individual service interactions and resource performance. They provide the ability to 'see' and 'hear' what is happening in the cloud environment by continuously collecting and sharing detailed information. This information is then processed by security tools, administrators, or automated processes to analyze and understand the health, performance, and security of the CSC’s cloud environment. Please reference the figure below for an overview of the cloud telemetry sources, which will be elaborated on in the following sections.

Management Plane Logs	Service Logs	Resource Logs	Cloud Tools
• Critical source given the importance of protecting the management plane.	• API Gateway: Access logs • Storage: Access logs • Network: VPC Flow logs • Function/Serverless: Activity logs • Cloud load balancer: Activity logs • Cloud DNS: Query logs • Cloud WAF/Firewall: Activity logs	• Workload: Instance, VM logs • Configuration change logs • Cloud function invocation logs • Database transaction logs • Object storage file access logs • Snapshot and image logs (block storage)	• CSPM (Cloud Security Posture Management - SPM) • CASB (Cloud Access Security Broker) • CNAPP (Cloud Native Application Protection Platform) • SSPM (SaaS SPM) • DSPM (Data SPM) • IAM analytics • Cloud detection and response

Figure 15: Cloud Telemetry Sources

6.2.1 Management Plane Logs

Management plane logs contain all the information on the activities that take place in the cloud management plane, either by console/GUI, API, or command-line interface (CLI) access. Resource creation, alteration, and deletions are reported there. Examples are Amazon Web Services (AWS) Cloudtrail or Microsoft Azure audit logs.

6.2.2 Service & Application Logs

Service and application logs record interactions with specific services inside the cloud. These logs capture a wide range of activities in service-specific events. Examples can be Load Balancer logs or storage access logs.

6.2.3 Resource Logs

Resource logs are specialized logs for resources like virtual machines (VMs), databases, and software-defined networks that record every operation and change. These include events such as resource provisioning, configuration changes, data access and transfers, and system-level activities.

6.2.4 Cloud Native Tools

At the scale of cloud, more comprehensive tooling is required. Cloud security posture management tools offer functionalities such as configuration management, compliance monitoring, misconfiguration detection, and automated remediation. Organizations can effectively monitor, analyze, and respond to security events across their cloud environments by integrating cloud tools into their security operations.

Multiple tools fall under posture management tools. Most of them have been grouped under the new title: Cloud Native Application Protection Platform (CNAPP).

- **Cloud Security Posture Management (CSPM)** are tools and practices that help organizations continuously monitor, assess, and improve the security status of their IaaS/PaaS cloud infrastructure. They help identify misconfigurations, compliance violations, and security risks across cloud services and resources. Capabilities offered by CSPM tools include continuous monitoring, automated remediation, and compliance reporting.

- **Cloud Workload Platform Protection (CWPP)** offers a suite of tools designed to enhance the security of workloads running in the cloud. These tools are capable of scanning workloads for vulnerabilities, misconfigurations, and hardening challenges. A key differentiator of CWPP is its ability to perform these scans on modern workload types such as containers, Kubernetes, and Functions as a Service (FaaS).

- **Data Security Posture Management (DSPM)** are tools that help protect sensitive data and ensure compliance with data protection regulations within cloud environments. They offer capabilities such as data discovery, classification, encryption policy enforcement, and ensuring proper access controls to safeguard data against unauthorized access, data breaches, and insider threats. DSPM can be implemented on IaaS/PaaS and also SaaS services.

- **Application Security Posture Management (ASPM)** are tools that manage the application security process and tools. ASPM provides a platform for collaborating between security, operations, and developers and detecting, prioritizing, and remediating vulnerabilities while implementing security policies in the application development and deployment phases

- **Cloud Infrastructure Entitlement Management (CIEM)** are tools designed to manage and govern access to cloud resources by providing detailed visibility and control over cloud infrastructure identities. They help organizations enforce the principle of least privilege by ensuring that users, applications, and services have only the necessary access to perform their functions.

- **Cloud Detection and Response (CDR)** are tools designed to detect and respond to security threats and incidents within cloud environments. They leverage advanced analytics, threat intelligence, and possibly machine learning algorithms to identify suspicious activities, anomalous behavior, and indicators of compromise. CDR tools facilitate rapid incident detection, investigation, and response, helping to mitigate the impact of security breaches and unauthorized access attempts in the cloud.

- **SaaS Security Posture Management (SSPM)** are tools that enable organizations to manage and monitor SaaS applications, ensuring proper configuration and entitlements. These tools offer centralized visibility into security controls, configurations, and compliance status across multiple SaaS applications. SSPM tools help assess the effectiveness of SaaS security, enforce security policies, and ensure alignment with contractual obligations and regulatory requirements.

6.2.4.1 Examples of Events to Monitor

The following non-exhaustive list is based on the Center for Internet Security (CIS) AWS benchmarks, which are highly recommended in cloud monitoring:

Access Management:

- Unauthorized API calls
- Management console login without MFA
- Disabling or scheduling the deletion of a customer-managed key
- Any IAM policy change
- Any use of the root account

Resource Management:

- S3 bucket policy changes
- Configuration monitoring changes
- Security group changes
- Network Access Control List (ACL) changes
- Network gateway changes
- Virtual private cloud (VPC) changes (e.g., subnets, routing tables, service endpoints)

Logging & Monitoring:

- Logging service configuration changes
- Management console authentication failures

Similar benchmarks exist for many other cloud providers and cloud services.

6.4 Collection Architectures

There is no single correct collection architecture since every provider and technology stack will be different. The core principles in this section highlight the different collection options and major architectural approaches.

6.4.1 Log Storage & Retention

Log storage and retention are affected by the following considerations:

- Storage costs for storing the data in the cloud vs. external storage
- Cost of moving and exporting the logs from the cloud to external storage
- Requirements to integrate cloud logs with logs of other sources (i.e, on-premises SIEM solution)
- Log retention limitation at the cloud provider vs what is required by compliance and best practices

One option is to leave the logs in the CSP's storage service, but this could create problems with detection, analysis, and other activities. An organization may then be limited to only using the CSP's analysis tools, which are not compatible with other security monitoring efforts or do not meet performance requirements. Moving logs back on-premises could result in even larger costs in terms of data transfer and physical storage requirements.

6.4.2 Cascading Log Architecture

Cascading log architecture is a hierarchical approach to log management. With it, logs are collected, filtered, aggregated, and analyzed in a cascading fashion, flowing from one layer to another to facilitate centralized monitoring and analysis. The following figure presents a sensible architecture for security purposes when managing logs in a cloud environment. Development (Dev), Testing (Test), and Production (Prod) environments each generate their own logs that are sent to a centralized log management system for multiple accounts associated with a specific project.[30]

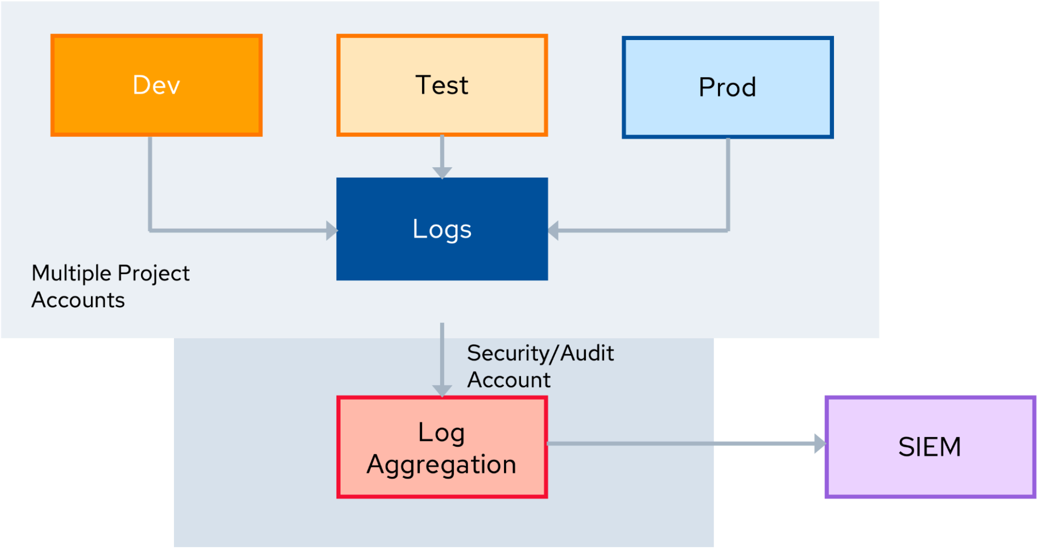

Figure 16: Cascading Log Architecture

[30] The CSC's account hierarchy must be considered when designing the cascading log architecture.

Each environment (Dev, Test, Prod) can be configured to forward logs to a central repository. The central log system aggregates these logs and sends the security-relevant ones into a single security/audit environment.

Finally, the aggregated logs can be fed into a SIEM application. The Security Information and Event Management (SIEM) system analyzes these logs to identify potential security incidents. This architecture provides a view of security-related events across all cloud environments, facilitating timely detection and response to threats.

6.5 AI for Security Monitoring

The greatest challenge of security monitoring is the ability to process huge amounts of data, correlate them with business indicators, and perform automatic remediation. Machine Learning (ML) and AI can assist in most of the mentioned tasks by enhancing:

- **Anomaly Detection:** Using machine learning to identify unusual patterns in data traffic and user behavior, flagging potential security threats faster and more accurately than traditional methods.
- **Threat Intelligence and Threat Hunting:** Integrating AI to analyze vast amounts of data from various sources to identify emerging threats and provide real-time alerts.
- **Automated Responses**: Implementing AI-driven automation to respond to security incidents quickly, reducing the time between threat detection and mitigation.
- **Assisting Analysts:** Enriching logs, simulating attacks, patching vulnerabilities, and reducing the overall burden on security teams.