Certificate of Cloud Security Knowledge (CCSK)

Notes by Al Nafi

Domain 6

Security Monitoring

Author:

Suaira Tariq Mahmood

Beyond Logs - Posture Management

Cloud security extends beyond traditional logging and event monitoring by incorporating Cloud Security Posture Management (CSPM), which focuses on maintaining security configurations, identifying risks, and ensuring compliance across cloud environments. While logs provide a detailed record of system activities, posture management takes a proactive approach by continuously evaluating the security state of cloud infrastructure, applications, and resources. Organizations must enforce best practices, detect misconfigurations, and remediate security risks before they lead to incidents.

Posture management involves analyzing the management plane, application and service logs, and individual resource configurations to gain a holistic view of cloud security. Cloud-native tools enable security teams to assess vulnerabilities, detect anomalous behavior, and automate remediation workflows. This section builds upon log-based monitoring concepts from Section 6.1 and introduces posture management techniques to enhance cloud security.

6.2.1 Management Plane Logs

The management plane in cloud environments governs how cloud resources are created, modified, and accessed. Unlike the data plane, which deals with actual data processing, the management plane controls administrative configurations, access permissions, and cloud service interactions. Monitoring management plane logs is essential for detecting unauthorized access, identifying policy violations, and preventing privilege escalations.

Cloud providers generate detailed logs of API calls, user activities, and configuration changes that affect the management plane. These logs provide insight into how cloud services are governed and help organizations enforce security policies. Unauthorized API requests, sudden privilege escalations, or unexpected configuration changes indicate potential security threats that require immediate attention.

Organizations rely on management plane logs to track IAM modifications, resource provisioning, and policy enforcement across multiple accounts and cloud environments. Logging solutions provided by AWS CloudTrail, Azure Activity Logs, and Google Cloud

Audit Logs allow security teams to detect misconfigurations and security violations, ensuring that governance policies are consistently applied.

6.2.2 Service & Application Logs

Monitoring service and application logs is crucial for maintaining visibility into how cloud-based applications operate. These logs capture detailed information about runtime events, API requests, and user interactions, allowing organizations to detect security anomalies, performance issues, and potential cyber threats.

Service logs provide visibility into cloud-native services such as serverless computing, managed databases, and containerized workloads. Cloud providers generate logs for these services to track execution metrics, performance bottlenecks, and security vulnerabilities. In contrast, application logs capture information related to business logic, authentication failures, and API integrations, helping organizations troubleshoot application-level issues.

Security teams analyze service and application logs to detect unauthorized API requests, failed authentication attempts, and suspicious activity patterns. By integrating logging solutions such as AWS Lambda Execution Logs, Azure Application Insights, and Google Cloud Operations Suite, organizations can monitor the behavior of applications in real time, detect breaches, and enforce compliance policies.

6.2.3 Resource Logs

Resource logs provide detailed records of how cloud resources—such as virtual machines, storage buckets, databases, and network configurations—are accessed and modified. These logs help organizations detect unauthorized changes, misconfigured security settings, and suspicious activities that could lead to data breaches.

Compute logs capture information about virtual machine activity, instance reboots, and software updates. Monitoring compute logs helps organizations track unauthorized access to cloud instances and detect potential malware infections. Storage logs record file access attempts, modifications, and deletion events, allowing organizations to identify data exfiltration risks or misconfigured permissions.

Database logs provide insight into SQL query executions, failed login attempts, and privilege changes. These logs are essential for detecting suspicious database queries, unauthorized schema modifications, and potential SQL injection attacks. Network logs capture information about traffic patterns, firewall rule enforcement, and connectivity issues, helping security teams identify denial-of-service (DoS) attacks, lateral movement attempts, and insecure network configurations.

Organizations use AWS VPC Flow Logs, Azure NSG Flow Logs, and Google VPC Flow Logs to monitor network interactions and enforce segmentation policies. By continuously analyzing resource logs, security teams can detect vulnerabilities and implement real-time security controls.

6.2.4 Cloud Native Tools

Cloud-native security tools provide automated posture management capabilities, allowing organizations to assess risks, detect misconfigurations, and enforce best practices. These tools integrate with logging, monitoring, and compliance frameworks to provide real-time security assessments and remediation workflows.

Cloud security posture management solutions such as AWS Security Hub, Azure Security Center, and Google Security Command Center provide centralized visibility into security vulnerabilities across cloud environments. These tools automatically scan cloud configurations, detect security gaps, and recommend remediation steps based on industry best practices.

Organizations leverage security automation frameworks to detect and remediate security risks in real time. Cloud-native tools enable security teams to apply predefined security baselines, monitor access control policies, and enforce encryption standards. By integrating cloud-native security solutions with SIEM platforms, organizations can streamline compliance enforcement and incident response.

6.2.4.1 Examples of Events to Monitor

Organizations must monitor key security events that indicate potential threats, misconfigurations, or policy violations. Continuous monitoring of critical events helps prevent data breaches, unauthorized access, and security incidents.

IAM and access management events must be tracked to detect privilege escalations, unauthorized API calls, and suspicious login attempts. Unauthorized modifications to IAM policies or excessive permission grants pose security risks that require immediate remediation. Organizations monitor AWS CloudTrail, Azure Active Directory Logs, and Google Cloud IAM Logs to track access control modifications.

Network security events such as firewall rule changes, anomalous outbound traffic, and failed VPN authentication attempts indicate potential cyber threats. By analyzing network flow logs, security teams can detect denial-of-service (DDoS) attacks, malicious IP connections, and unauthorized data transfers.

Storage and data access events provide visibility into file modifications, mass data downloads, and attempts to access restricted storage locations. Organizations monitor cloud storage logs to detect ransomware activity, data exfiltration attempts, and insider threats.

Compute and infrastructure changes must be tracked to detect unexpected instance terminations, unauthorized container deployments, and high CPU utilization spikes. Organizations monitor logs for unusual activity that could indicate cryptojacking, unauthorized software installations, or resource hijacking.

Compliance and policy violations must be continuously monitored to enforce regulatory standards such as GDPR, HIPAA, and ISO 27001. Non-compliant configurations, unencrypted data storage, and insecure IAM roles increase security risks. Cloud-native security posture management tools provide automated compliance monitoring and remediation workflows.

Case Study: Strengthening Cloud Security Posture with Automated Monitoring

Background

A multinational technology firm operating across AWS, Azure, and Google Cloud required real-time visibility into cloud security risks, automated compliance enforcement, and proactive posture management. The organization faced challenges in detecting misconfigurations, enforcing IAM policies, and securing cloud workloads.

Solution

The firm deployed AWS Security Hub and Azure Security Center to assess security vulnerabilities and detect non-compliant configurations. Management plane logs were integrated with a SIEM solution, enabling real-time detection of IAM policy changes and API misconfigurations. Automated remediation workflows were implemented to enforce encryption standards, prevent unauthorized storage access, and block excessive privilege grants.

Outcome

By implementing cloud-native security posture management, the organization reduced the risk of cloud misconfigurations, ensured compliance with regulatory frameworks, and improved threat detection capabilities. Automated posture assessment and event monitoring allowed security teams to respond to security incidents in real time, minimizing the impact of potential attacks.

For additional insights into cloud security posture management, refer to:

- **AWS Security Hub Documentation**
- **Azure Security Center Overview**
- **Google Security Command Center**

Conclusion

Cloud security posture management extends beyond traditional logs and events by automating risk detection, enforcing security policies, and preventing security incidents. Organizations must integrate management plane monitoring, resource security assessments, and cloud-native tools to maintain continuous security and compliance in cloud environments. The next section will explore incident response strategies, including automated remediation, threat intelligence, and forensic analysis for cloud security events.