Domain 6 Security Monitoring

Introduction

Security monitoring in cloud environments requires addressing specific challenges, including:

- Unique telemetry sources, logs, and events.
- Multi-cloud and hybrid security complexities.
- AI's role in automating and improving security.

6.1 Cloud Monitoring

Cloud security monitoring is complicated by:

1. **Management Plane:** Controls administrative actions; requires strict monitoring.
2. **Velocity:** Cloud changes occur rapidly, demanding **automated security responses**.
3. **Distribution & Segregation:** Cloud environments are decentralized, so **centralized logging** is essential.
4. **Cloud Sprawl:** Multiple providers and workloads increase complexity.
5. **Shared Responsibility Model (SRM):** CSPs and CSCs share monitoring duties.

6.1.1 Logs & Events

Logs:

- Capture CRUD (Create, Read, Update, Delete) operations for forensic analysis.
- Used for compliance but may have **latency issues**.

Events:

- Immediate notifications for **Create, Update, Delete (C-UD)** operations.
- Essential for rapid threat detection.

6.2 Beyond Logs - Posture Management

Cloud security **goes beyond logs** by continuously assessing security configurations.

Security Posture Management Includes:

- **Misconfiguration detection**
- **Vulnerability assessment**
- **Automated remediation prioritization**

6.2.1 Management Plane Logs

- Record **administrative actions** via API, CLI, and console.
- Example: **AWS CloudTrail**, **Azure Audit Logs**.

6.2.2 Service & Application Logs

- Track **service-specific** actions (e.g., storage access, load balancing).

6.2.3 Resource Logs

- Logs for **VMs, databases, networking changes** (e.g., resource creation, data access).

6.2.4 Cloud Native Tools

Security tools categorized into different focus areas:

1. Cloud Security Posture Management (CSPM)

- Detects misconfigurations in **IaaS/PaaS** environments.
- Provides compliance reports and automated fixes.

2. Cloud Workload Protection Platform (CWPP)

- Secures cloud workloads (VMs, containers, Kubernetes, FaaS).
- Scans for vulnerabilities and hardening issues.

3. Data Security Posture Management (DSPM)

- Protects **sensitive data** with encryption, access control, and compliance checks.

4. Application Security Posture Management (ASPM)

- Ensures security in **development pipelines** (DevSecOps).
- Automates vulnerability detection.

5. Cloud Infrastructure Entitlement Management (CIEM)

- Manages cloud access permissions.
- Enforces **least privilege access**.

6. Cloud Detection & Response (CDR)

- Uses **AI/ML** for **threat detection and response**.

7. SaaS Security Posture Management (SSPM)

- Secures **SaaS applications** by enforcing proper configurations.

6.2.4.1 Key Security Events to Monitor

Based on **CIS AWS benchmarks**:
✓ **Access Management:** Unauthorized API calls, root account usage.
✓ **Resource Management:** Security group, ACL, and VPC changes.
✓ **Logging & Monitoring:** Authentication failures, logging service modifications.

6.3 Cloud Telemetry Sources

Telemetry provides **real-time visibility** into cloud environments.

- Tracks **management actions, service interactions, and system performance**.
- Essential for **threat detection and incident response**.

6.4 Collection Architectures

Different **log collection strategies** impact security monitoring effectiveness.

6.4.1 Log Storage & Retention

- Balancing **cost** vs. **data retention**.
- Compliance may **require long-term log storage**.
- Cloud **logs may not integrate easily** with on-prem SIEM.

6.4.2 Cascading Log Architecture

- Logs are collected from **Dev, Test, and Prod environments** into a central system.
- **Security-relevant logs** are forwarded to **SIEM** for detection & response.

6.5 AI for Security Monitoring

AI and **Machine Learning (ML)** improve cloud security by:

✓ **Anomaly Detection** – Identifies unusual user behavior and data traffic patterns.
✓ **Threat Intelligence** – Uses AI to detect emerging threats in real-time.
✓ **Automated Incident Response** – Reduces reaction time to security events.
✓ **Security Analyst Assistance** – Helps **simulate attacks, enrich logs, and patch vulnerabilities**.