Date: April 2025
Reported by: Cloud SIEM Detection Engine (Microsoft Sentinel)
Escalation Path: Security Ops → DevSecOps Lead → ML Engineering Lead → CISO

🚨 Incident Summary

A targeted attack was attempted against the AI orchestration layer of our cloud-native ML infrastructure. The adversary used compromised credentials and attempted to access model weights and metadata through a misconfigured container environment.

Deception technology (cloud honeypot) successfully triggered a high-severity alert. The intrusion was sandboxed, analyzed, and contained. A zero-day serialization flaw was discovered in the ML pipeline.

📊 Timeline of Events

- **00:00**: Unusual API activity from IAM service account
- **00:03**: Suspicious Lambda function execution outside standard hours
- **00:06**: Access attempt to honeypot storage labeled "model_weights_v3.conf"
- **00:08**: Outbound traffic flagged to suspicious domain via DNS firewall
- **00:12**: Container sandboxed; exploit confirmed as zero-day
- **00:16**: DevSecOps rotates IAM keys, blocks IP, restores container from image

🪧 Technical Indicators

Attack Vector: Privilege escalation via cloud container access
Techniques: API misuse, credential abuse, Lambda injection
Targeted Assets: AI model storage, training pipelines

MITRE TTPs:

- T1203: Exploitation for Client Execution
- T1078: Valid Accounts
- T1529: Service Manipulation (Reboot)
- T1606: Data Poisoning (AI Threats)

🌐 Risk & Impact Assessment

Data Exfiltrated: None
Business Impact: Medium risk; early detection avoided breach
Customer Impact: None reported; vendor advisory prepared

🔒 Remediation Actions

- Compromised container rebuilt from golden image
- IAM credentials rotated with forced MFA
- Alert rules adjusted for cloud function anomaly detection
- Vulnerability disclosed to ML orchestration vendor
- Staff retrained on AI security risks and misconfig detection

📝 NIST 800-53 Mapping

- **SI-4**: Monitoring and Detection
- **RA-5**: Vulnerability Scanning (custom codebases)
- **AC-6(9)**: Least Privilege for Service Accounts
- **PL-8**: Secure Planning for Emerging Tech (AI/ML)

🔍 Lessons Learned

- Cloud-native environments require AI-specific deception and alerting
- Model assets must be monitored like PII
- Threat actors are evolving toward ML poisoning and data skew attacks