Case Study - Intelligent Response in a Multicloud Environment with AI

Context:

In 2024, a multinational financial company faced an expanding attack surface due to rapid migration to multicloud infrastructures (AWS, Azure, GCP). The volume of data exchanged via APIs and distributed systems had grown exponentially. The security team was overwhelmed and struggled to respond to incidents quickly, letting advanced threats slip through.

Challenge:

A highly sophisticated attack campaign was underway, leveraging living-off-the-land (LotL) techniques, credential exposure, and automated lateral movement across hybrid, multigeographic environments. Real-time detection and response were vital to ensure business continuity and protect global reputation.

Solution:

1. AI-Powered Security Architecture

Luan Felipe led the design of a modular security architecture built on three pillars:

- Unified Observability: centralizing logs, events, and traffic with Splunk, Chronicle Security, and OpenTelemetry.
- Adaptive AI: custom detection models developed in Python using scikit-learn and deployed in real-time with TensorFlow Lite at the edge.
- Smart SOAR: automated playbooks via Cortex XSOAR integrated with CrowdStrike Falcon for rapid containment.

2. Real-Time Behavioral Correlation

Behavioral models identified baseline deviations in privileged IAM accounts, flagging unauthorized lateral movements in Azure. AI correlated these anomalies with exfiltration attempts in GCP,

enabling early threat detection before attack consolidation.

3. Intelligent Isolation and Dynamic Reconfiguration

Vulnerable apps were automatically isolated using container segmentation, Kubernetes Network Policies, and Ansible scripts for auto-remediation. Visibility was preserved with autonomous telemetry agents.

Impact:

- 87% reduction in Mean Time to Respond (MTTR) for critical incidents
- Zero downtime for core applications during containment
- Estimated $4.8M in avoided losses (post-incident analysis)
- AI model reused and retrained for global incident correlation and prevention

Tools Used:

- Cloud: AWS, Azure, GCP
- SIEM & SOAR: Splunk, Chronicle, Cortex XSOAR
- AI & Scripting: Python, TensorFlow, scikit-learn, Bash
- Endpoint & Identity: CrowdStrike, Okta, Azure AD
- Automation & Infra: Kubernetes, Terraform, Ansible

Lessons Learned:

- AI doesn't replace human intuition-it enhances it.
- Unified visibility is critical in multicloud environments.
- Clear communication with global stakeholders is just as important as automation.
- Luan's multilingual communication was key in coordinating efforts across time zones, languages, and regulatory frameworks.