cogent infotech

Case Study

Building an AI-Enabled Threat Detection & Incident Response

The Client

A large Omni channel retail enterprise operating hundreds of physical stores alongside e-commerce and digital platforms across North America. The organization manages a highly distributed technology environment spanning point-of-sale (POS) systems, cloud infrastructure, corporate networks, and customer-facing applications.

The Challenge

- High volume of security alerts generated by multiple security tools with limited prioritization and correlation
- Manual incident triage processes resulting in delayed investigation and response times
- Inconsistent threat visibility across stores, cloud environments, and corporate networks
- Limited ability to analyze historical data for recurring attack patterns and threat trends
- Growing exposure to ransomware, credential abuse, and lateral movement attacks
- Need for a centralized platform that integrates seamlessly with existing security investments

About Cogent Infotech

Founded in 2003, Cogent Infotech is a trusted, award-winning firm with **23+ years** of experience**, 150+** government contracts, **10,000+** projects, and a **96% employee retention rate**. Recognized as an SBA Small Business and MBE-certified, we deliver excellence through diverse talent, AI-driven recruitment, and cooperative contracts like **NASPO Value Point and TIPS-USA.**

Babu V.
Chief Revenue Officer | babu@cogentinfo.com | 972 – 439 - 0386

Solution and Process

- **Unified Security Event Console**
  Centralized ingestion and visualization of logs from endpoints, POS systems, cloud services, and network devices

- **AI-Assisted Threat Prioritization**
  Event correlation and risk scoring to identify high-impact incidents, attack chains, and anomalous behavior

- **Incident Response Workflow**
  Guided investigation steps, predefined response playbooks, and automated containment actions to reduce manual effort

- **Historical Threat Analytics**
  Trend analysis and pattern detection to identify repeat attacks, common vectors, and vulnerability exploitation

- **Executive Security Dashboard**
  Real-time metrics on threat volumes, response times, incident severity, and overall risk exposure

Outcome

- Achieved a **45% reduction in incident response time**

- Significantly reduced false-positive alerts, improving SOC analyst efficiency

- Improved threat visibility across both physical stores and digital retail platforms

- Strengthened defenses against ransomware and credential abuse attacks

- Delivered a **scalable security platform** ready to support new stores and digital channels

Risk Analysis

- Alert fatigue and missed high-risk incidents due to tool fragmentation

- Delayed containment risk from manual triage and investigation workflows

- Inconsistent security posture visibility across physical and digital environments

- Data integration risk when ingesting high-volume security telemetry

- Scalability risk as new stores, devices, and digital channels are added

Best Practices

✓ Centralized event ingestion and normalization across environments

✓ AI-assisted correlation to reduce false positives and alert noise

✓ Automated response playbooks to accelerate containment

✓ Unified visibility for SOC analysts and executive leadership

✓ API-first integration with existing security tool chains

TECHNOLOGIES

- **Azure Data Explorer**
- **Azure Machine Learning**
- **Azure Event Hub**
- **Azure Functions**
- **Java / Spring Boot**
- **Angular (secure, role-based UI)**
- **Azure Monitor & Microsoft Sentinel Integration**
- **Power BI**