# SOC and Infrastructure Automation Case Study

Building a unified SOC and infrastructure automation framework

## Overview

From June to July 2019, the client embarked on a strategic initiative to enhance its Security Operations Centre (SOC) and strengthen its infrastructure monitoring and automation capabilities.

The objective was to streamline security workflows, reduce manual dependencies, and achieve centralized visibility across malware detection, vulnerability management, firewall alerts, and infrastructure performance.

This project established a cohesive and resilient SOC automation framework—enabling faster incident response, reduced false positives, and a unified platform for real-time monitoring and alert management.


## Project Focus Area

- SOC Automation
- Infrastructure Monitoring
- Vulnerability Management
- Workflow Optimization
- Security Tool Integration

# Challenges

## Fragmented Security Ecosystem

Multiple security tools such as McAfee, Nessus, Sophos, and Nagios were operating in silos, resulting in disconnected data flows and limited operational visibility.

## Manual Alert and Report Processing

The SOC team was manually processing malware, vulnerability, and firewall alerts—leading to slower response times and repetitive workloads.

## High False Positives & Duplicates

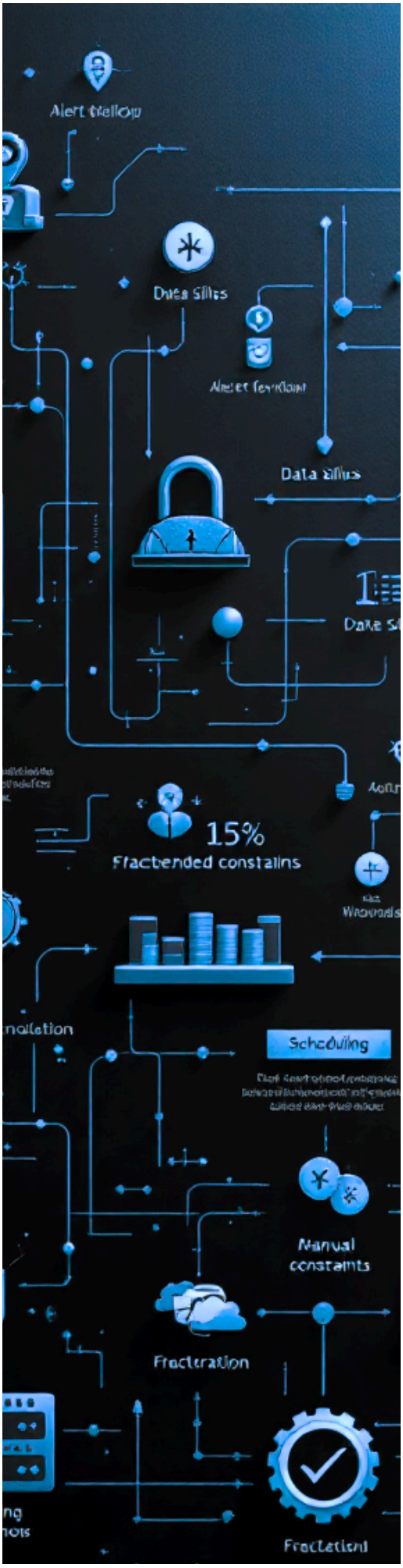
Redundant or invalid alerts from vulnerability scans overwhelmed analysts, reducing focus on high-priority threats.

## Limited Automation & Scalability

Alert assignments, user onboarding, and approval workflows required manual steps, limiting scalability as the organization grew.

## Visibility Gaps

Critical events from infrastructure monitoring tools were not centrally correlated, delaying the identification of potential issues.



# Solution Implementation

A comprehensive tool integration strategy was implemented to address the identified challenges and create a unified security operations framework.

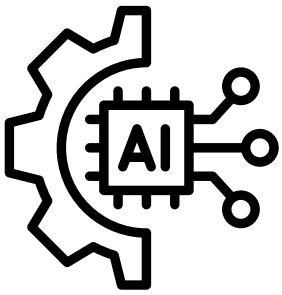
## Tool Integration Summary

| Platform | Primary Function | Key Activities / Notes |
|---|---|---|
| **Arcsight** | SOC Event Management | Monitored invalid logins, applied false positive checks, malicious IP validation, and custom dashboards for high-count alerts. |
| **InsightIDR** | Identity Detection & Response | API integration for basic data sharing; detailed integrations planned for later phases. |
| **InsightVM** | Vulnerability Management | Automated scanning, report pulling, event creation, integrated with Ansible for remediation workflows. |
| **Insight AppSec** | Application Security | Automated vulnerability scans and comprehensive reporting capabilities. |
| **Ansible** | IT Automation & Remediation | Integrated with InsightVM to automate vulnerability remediation processes. |
| **Contrast Security** | App Vulnerability Scanning | APIs explored for potential integration; full implementation not pursued. |
| **SonarQube** | Static Code Analysis | Integrated to automatically pull static analysis reports for code quality assessment. |
| **Nessus** | Vulnerability Scanning | Report integration achieved; scheduling not possible without Nessus Manager. |

# Key Implementations

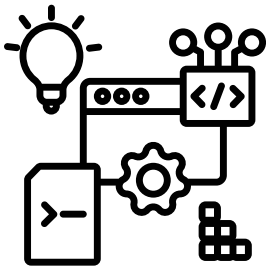
### Arcsight Dashboard Configuration

Configured sophisticated dashboards to flag invalid login attempts exceeding 15 occurrences, significantly improving threat visibility and enabling faster response to potential security incidents.



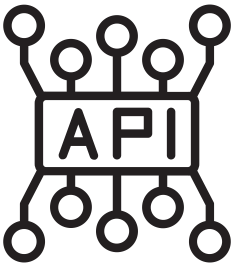

### InsightVM Automation

Enabled scheduled vulnerability scans, automated reporting mechanisms, and event creation workflows; seamlessly integrated with Ansible for streamlined remediation processes.



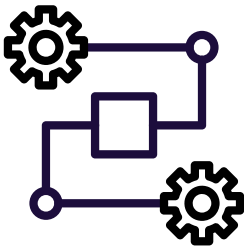
### SonarQube Integration

Implemented automated report pulling for static code analysis, enabling continuous monitoring of code quality and security vulnerabilities in the development pipeline.




### Contrast Security API Exploration

Thoroughly explored Contrast Security APIs to understand
integration capabilities; full implementation deferred based on prioritisation and resource allocation decisions.



### InsightVM Automation

Successfully integrated reporting capabilities whilst identifying scheduling limitations that would require Nessus Manager for full automation potential.

# Results & Impact

## 75%

**False Positive Reduction**

Significant decrease in false positives and alert noise in SOC operations

## 60%

**Time Savings**

Reduced manual workload through automated scanning and remediation

## 40%

**Faster Response**

Improved incident detection and response times with automated workflows

### Enhanced Incident Visibility

Improved incident visibility through automated dashboards providing real-time insights into security events, enabling proactive threat hunting and faster decision-making across the SOC team.

### Streamlined Vulnerability Management

Streamlined vulnerability scanning and remediation processes, dramatically reducing manual workload and accelerating time-to-remediation for critical vulnerabilities across the infrastructure.

### Strengthened Security Posture

Strengthened application security posture with automated testing and code analysis integrations, ensuring vulnerabilities are identified and addressed earlier in the development lifecycle.

**Future Roadmap:** IIdentified clear next steps for deeper integrations and tool upgrades, including Nessus scheduling enhancements and InsightIDR data expansion initiatives to further strengthen the automation framework.

## Conclusion

This project successfully established a structured and scalable security automation framework that transformed the client's security operations capabilities. By integrating SIEM, IDR. vulnerability management, and application security tools with automated workflows, the SOC achieved remarkable improvements in detection accuracy, accelerated remediation timelines, and enhanced overall operational efficiency.

The implementation demonstrated that strategic tool integration and workflow orchestration can significantly reduce manual effort whilst improving security outcomes. The foundation laid during this three-month engagement positions the organisation for continued security maturity and operational excellence.

## Key Achievements

- Unified security operations platform
- Automated vulnerability lifecycle
- Reduced false positive rates
- Enhanced threat visibility
- Improved team efficiency
- Scalable automation framework

A well-integrated security operations framework doesn't just respond to threats-it anticipates them, automates responses, and empowers security teams to focus on strategic initiatives rather than repetitive tasks.