SecGenieAI

Security Automation Use Cases

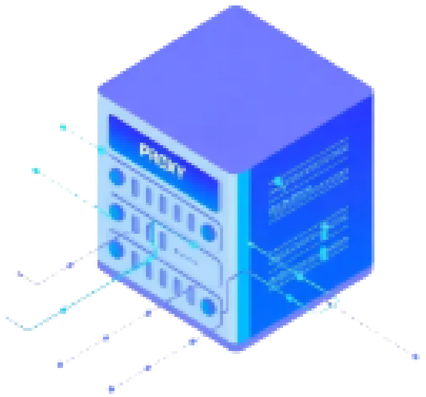
An overview of automated threat detection, analysis, and response workflows for modern security operations.

Advanced security automation workflows to strengthen its Security Operations Center (SOC). The framework reduces false positives, enriches alerts with contextual data, and streamlines incident response. Key integrations include SIEM (Arcsight), Symantec DLP/EDR, threat intelligence feeds, and ServiceNow.

Key Use Cases & Integration

Arcsight – Proxy Use Case

- False positive/Duplicate check
- Malicious IOC indicators (Intsights threat feed integration)
- Contextual asset details - Integration with local MDM - Assigned to analyst queue

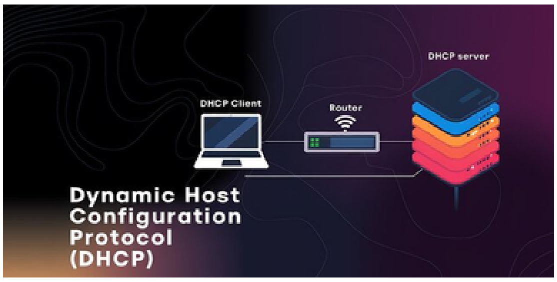


Arcsight - Palo Alto Use Case

- False positive/Duplicate check
- Malicious IOC indicators (Intsights threat feed integration)
- Contextual asset details - Integration with local MDM
- Assigned to analyst queue

DHCP Logs – Asset Synchronization

- Synchronizes endpoints with dynamic IPs into SocView asset repository
- Ensures accurate asset-to-alert mapping
- Reduces manual reconciliation and improves visibility

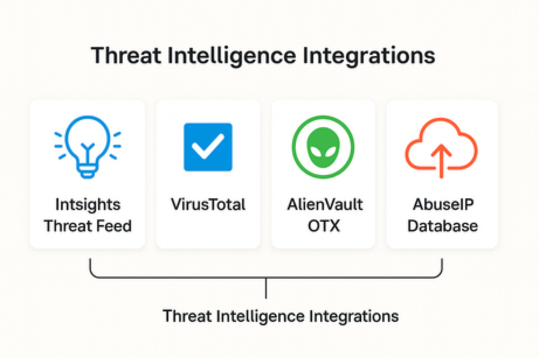


Symantec Use Case Details

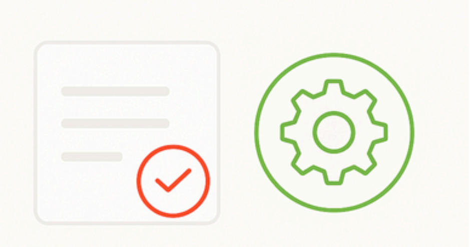
Platform	Key Features
Symantec DLP	• False positive/Duplicate check • Email trigger to employee’s manager on file transfer • Based on response: reject alert or escalate for investigation
Symantec EDR	• False positive/Duplicate check • Enriched contextual information • Auto-populates alert and host-based events for 30 days • Saves analyst time and accelerates triage

Threat Intelligence Integrations

- Intsights Threat Feed
- VirusTotal
- AlienVault OTX
- AbuseIP Database


Threat Intelligence Integrations
Intsights Threat Feed
VirusTotal
AlienVault OTX
AbuseIP Database
Threat Intelligence Integrations

ServiceNow Integration

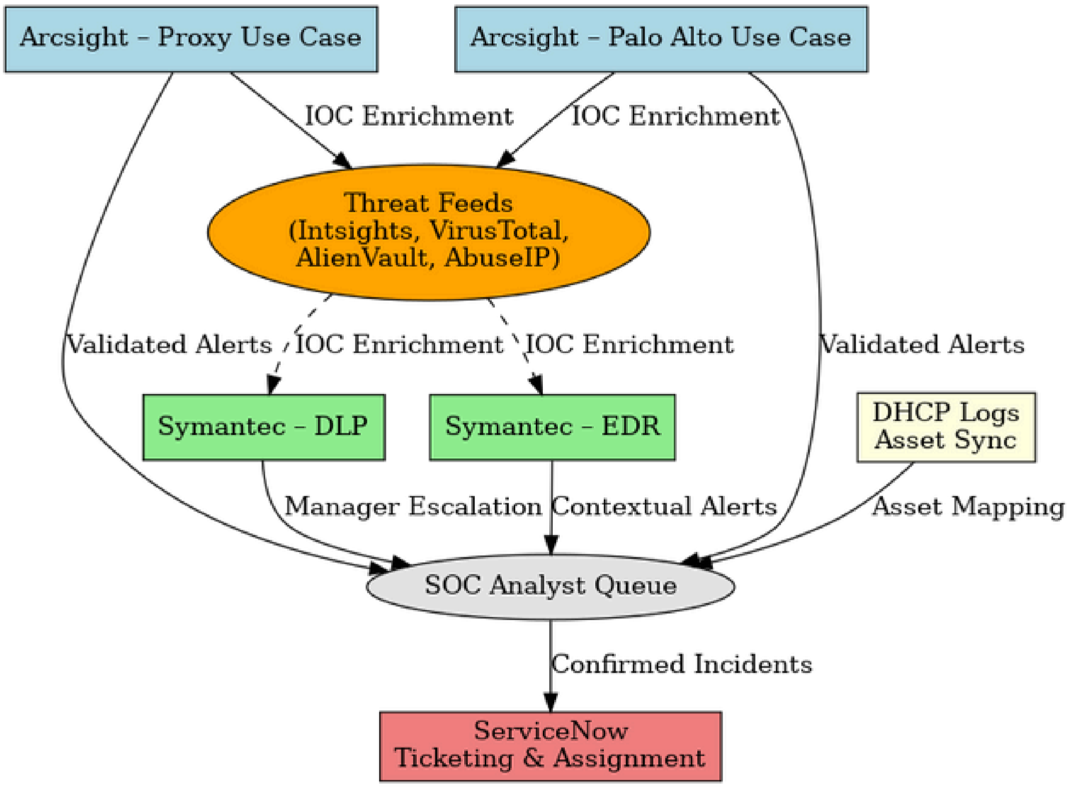


- Automatic ticket creation for confirmed incidents
- Tickets enriched with contextual details
- Assigned to relevant response teams
- Ensures faster resolution and seamless workflows

Key Benefits

- Reduced false positives and duplicate alerts
- Accelerated triage with contextual enrichment
- Improved detection accuracy via IOC feeds
- Streamlined response through ServiceNow integration
- Increased SOC efficiency and reduced analyst workload

Visual Workflow Diagram



Conclusion: The implementation of an automated SOC framework leveraging Arcsight, Symantec DLP/EDR, threat intelligence feeds, and ServiceNow has significantly enhanced the organization’s security posture. By improving the speed, accuracy, and consistency of threat detection and incident response, the framework has streamlined SOC operations and enabled a more proactive, efficient, and resilient security environment.