Unified SOC as a Service

Accelerated Threat Response Powered by Cisco XDR and Splunk

In an era of escalating cyber threats and data complexity, traditional security operations struggle with high costs and fragmented visibility. Our SOC-as-a-Service bridges this gap by unifying Cisco XDR and Splunk Enterprise Security into a single, AI-driven defense engine.

We deliver high-fidelity detections and automated response actions, allowing your team to focus on strategic risk rather than manual triage.

The Challenge: The Cost of Complexity

Modern enterprises face three critical security hurdles:

1. **Exploding Data Costs:** Sending raw telemetry from every endpoint and network device to a SIEM is often prohibitively expensive.
2. **Alert Fatigue:** Security teams are overwhelmed by thousands of disconnected alerts, leading to missed critical threats.
3. **Slow Response (MTTR):** Manually correlating data across siloed tools takes hours — time that attackers use to move laterally.

Our Approach: A Smarter Security Stack

Our architecture optimizes your security investment by layering telemetry-centric detection with data-centric governance, and augmenting analysis with AI.

1. **Rapid Triage with Cisco XDR**

   Cisco XDR acts as the high-speed engine, natively correlating telemetry from the six most critical sources: endpoint, network, firewall, email, identity, and DNS.

   Outcome – It produces high-fidelity "incident bundles" at machine speed, drastically reducing the volume of data that needs to be stored in your SIEM.

2. **Advanced Analytics & Governance with Splunk Enterprise Security**

   Splunk serves as the central intelligence platform, providing long-term retention, forensic investigation, and compliance reporting.

   Outcome – High-priority incidents are automatically escalated from XDR to Splunk Enterprise Security, where they are enriched with broader business context and mapped to the MITRE ATT&CK framework.

3. **AI-Native Security Operations with Cisco and Splunk**

   We leverage the latest AI innovations to augment human analysts. The Cisco AI Assistant explains malicious scripts and suggests guided remediation steps. While the Splunk AI Assistant enables analysts to perform complex forensic queries using natural language.

   Outcome – Analysts resolve incidents faster with greater confidence, improving the effectiveness of security operations.

Key Features & Benefits

Feature	Customer Benefit
Integrated Telemetry	Gain unified visibility across on-prem, cloud, and hybrid environments without the "SIEM tax".
Automated Response	Isolate infected hosts or block malicious identities instantly via Splunk SOAR and Cisco XDR.
Talos Intelligence	Every detection is backed by Cisco Talos, one of the world's largest private threat intelligence teams.
Cost Efficiency	Reduce log ingestion costs by triaging high-volume data in the XDR layer before it hits Splunk.
Federated Search	Analyze data where it lives — search Cisco's security data lake directly from your Splunk console.

Service Outcomes

- **Faster Detection:** Identify complex attacks up to 64% faster than traditional SIEM-only models.
- **Reduced Noise:** A 90% reduction in false positives through automated incident correlation.
- **Immediate ROI:** Maximize SIEM investments while adding modern XDR capabilities.

64% *faster*

90% *reduction*
in false positives

Ready to modernize your defense?
Contact us for a tailored service analysis or a live demonstration of our integrated Cisco & Splunk dashboard.

compucom
Technology Driven.
People Powered.

cisco
Partner

Learn more at compucom.com/cisco