



Autonomous Security Operations Center (SOC) Services Powered by Splunk Cisco

Security teams must investigate alerts quickly and accurately while minimizing false positives. NTT DATA's Autonomous SOC Services powered by Splunk Cisco uses agentic AI to combine real-time detection, autonomous investigation and controlled response. AI agents reconstruct attack paths and recommend or execute remediation in seconds, while human analysts remain in control.

This delivers high-quality investigations with up to **95% accuracy, 70% faster investigations, 60% faster response and scalable operations** that meet your enterprise governance requirements.

Security teams are under growing pressure

In many organizations, the security operations center (SOC) operates under constant strain. Analysts move across disconnected systems to validate alerts, collect evidence and repeat manual investigation steps.

Experienced analysts spend time on triage and evidence collection instead of advanced threat analysis. Compliance teams require structured case documentation for major events, adding reporting overhead.

The challenge is not detection but the time, complexity and inconsistency of investigation and response.

As environments expand across cloud, software as a service (SaaS), hybrid infrastructure and distributed identities, investigations demand greater cross-system correlation, all of which become more important as attackers use automation and AI to scale.

Security operations must improve speed and precision without expanding overhead.



NTT DATA's Autonomous SOC operating model

Our Autonomous SOC Services powered by Splunk Cisco applies autonomous investigation to high-risk alerts within a governed operating model.

This model brings together:

- Splunk Cisco for detection, correlation and risk-based analytics
- Agentic AI for autonomous investigation and response orchestration
- NTT DATA for governed deployment and operational delivery

It goes beyond alert automation to deliver structured, autonomous investigation with human oversight.

Our solution keeps humans in the loop

When Splunk Cisco detects a high-risk alert, agentic AI initiates a structured investigation.

Structured investigation, executing several tasks in parallel:

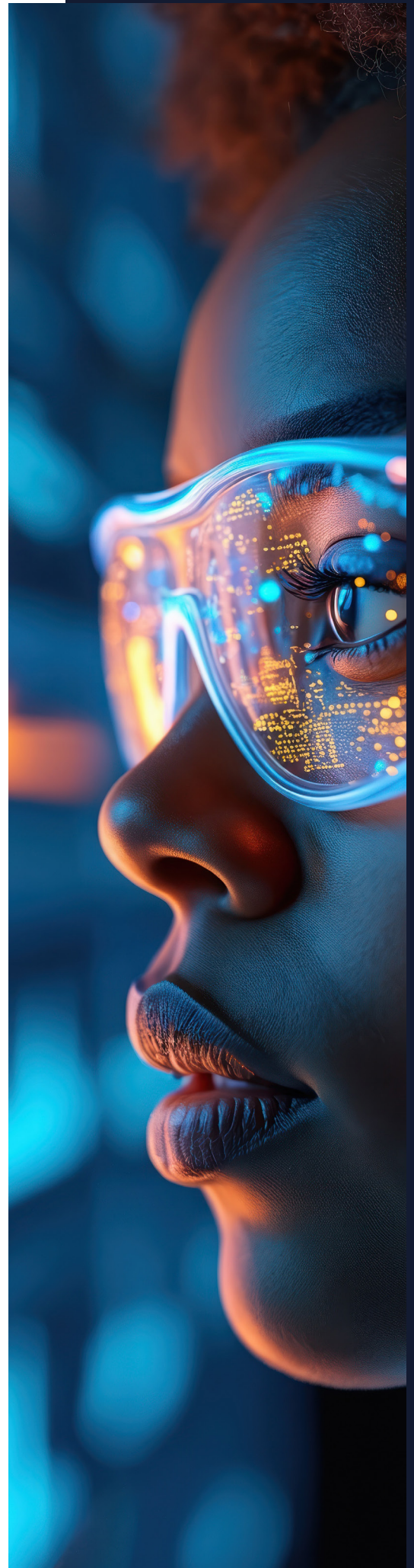
- Correlates related user and system behaviors
- Evaluates multiple attack paths simultaneously
- Reconstructs the full attack progression
- Distinguishes legitimate activity from compromise
- Produces a confidence-based verdict

Each case automatically generates:

- Documented evidence
- Clear reasoning and traceability
- Severity and impact assessment
- Recommended remediation steps

Instead of a manual investigation across disconnected workflows that takes hours of analysts' time, investigations are reduced to seconds.

The result is a consistent, repeatable and audit-ready process with human oversight.



Operational results at scale

Benefits for security teams

Reduced analyst fatigue

Tier 1 investigations are handled autonomously, allowing analysts to focus on higher-value threat analysis.

Consistent decision-making

Structured logic reduces dependency on individual expertise.

Accelerated mean time to detect (MTTD) and mean time to respond (MTTR)

Parallel autonomous analysis reduces exposure windows.

Scalable security operations

Handle growing alert volumes and infrastructure complexity without increasing analyst headcount.

Stronger compliance alignment

Structured, traceable documentation supports frameworks such as the:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO/IEC 27001
- Network and Information Security Directive 2 (NIS2)
- Digital Operational Resilience Act (DORA)

Embedding agentic AI into SOC workflows delivers measurable improvements in performance:

- More than 80% of investigations are handled autonomously
- False-positive handling time is reduced by approximately 95%
- Responses are up to 40% faster

Our solution enables autonomous response with defined controls

NTT DATA and Splunk Cisco enable an autonomous SOC model where response actions operate within a clear governance framework. You establish your approval thresholds, escalation paths and risk tolerance up-front, ensuring that autonomous actions execute only within the boundaries you have defined.

Following the investigation, agentic AI can recommend or execute remediation actions such as:

- Blocking malicious IP addresses
- Disabling compromised accounts
- Quarantining endpoints
- Reversing unauthorized changes

Responses may be fully automated, approval-based or selectively applied, based on risk posture and regulatory requirements.

Automation increases speed while governance preserves control and human analysts retain oversight.

Our AI-powered cybersecurity services

Advisory services

Our assessment, guidance and strategy development services allow you to continuously evaluate and improve security strategies, linking the value of investments to tangible results.

Strategic Sourcing

Optimize costs, reduce risk and accelerate access to cutting-edge, multivendor technology through our global supply chain services and strategic partnerships.

Professional Services

Design, implement and integrate multivendor technology solutions with speed and precision to reduce risk, accelerate cybersecurity transformation and maximize ROI.

Software-defined Infrastructure Services

Boost efficiency, utilization and business outcomes with our reimagined agentic services and client experience platform.

Global Field Services

Our global onsite expertise for the installation, maintenance and support of multivendor infrastructure helps you ensure operational continuity and resolve issues rapidly.

Adoption Services

Maximize ROI and accelerate business outcomes with our training, onboarding and change management solutions for user enablement and the consumption of cybersecurity solutions.

Managed Services

Our managed cybersecurity services, supports your business outcomes.

Why NTT DATA

NTT DATA delivers AI-powered security operations that are practical, governed, and built to work within your existing environment.

- 30+ years of managed security experience with global SOC coverage and local expertise
- Proven impact with 50% fewer false positives and 40% faster response times
- Certified Splunk Cisco and cybersecurity specialists with established SOC practices
- Unmatched threat intelligence powered by the world's 4th largest IP backbone, providing early threat visibility and actionable alerts
- Global Analyst Workbench enables automated triage and context-aware incident response at machine speed
- Awarded Cisco Global Sustainability Partner of the Year 2025, reflecting leadership in infrastructure, AI, and security services
- Agentic AI built into operations to automate investigation, support faster decisions and maintain full governance

The result is resilient security operations with clear oversight, strong discipline and enterprise control.

Visit nttdata.com to learn more.

NTT DATA is a \$30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.



