LOGICALIS
Architects of Change

CISCO
PARTNER

Solution Brief

From Alert Fatigue to Action

Operationalizing Cisco Managed XDR for Real-Time Threat Response

The Problem Every SecOps Teams Recognizes

Today's threat actors multiple tactics and techniques that can come from anywhere, at any time, through any number of vectors, including network, cloud, endpoint, email, identity, and application systems. The result is that most security operations (SecOps) teams and Security Operations Centers (SOCs) are buried in alerts.

Dozens of tools spread out across the expanding threat surface all focus on a different layer of the security stack, leaving teams spread thin, siloed, and overwhelmed. Burnout is rampant and turnover continues to hamper the operational capabilities of SecOps teams.

Organizations need an approach that unifies and simplifies operations, so teams can separate the signal from the noise, act decisively, and focus on activities that matter.

Simplify SecOps with

Cisco Managed XDR, Delivered by Logicalis

Cisco XDR integrates and correlates data from multiple security products across an organization's networks, cloud, endpoints, email, and applications. Logicalis, one the first global Cisco partners to launch Cisco XDR as a fully managed service, combines Cisco's modern SecOps solution with Logicalis' deep expertise, global network of SOCs, and 24/7 support to deliver unified protection at scale.

With Logicalis Managed Cisco XDR, SecOps teams can:

Detect complex threats sooner

Gain a comprehensive view of attacks with deep network insights and visibility via integrations across the Cisco security portfolio and several third-party tools. Expose gaps in threat detection using actionable insights from network-powered defense, Cisco Talos and third-party threat intelligence, and MITRE ATT&CK coverage maps.

Act on what matters most, faster

Reduce mean time to respond (MTTR) with AI-driven guidance for identification, containment, eradication, and recovery for consistent and effective decision-making. Simplify investigations with unified context, prioritized alerts, and progressive disclosure to avoid information overload.

Simplify network and security operations

Unify visibility and context with enriched network telemetry from Meraki MX devices, including traffic patterns, device behavior, and system changes. Reduce the risk of successful attacks while identifying potential threats earlier by combining network logs from Meraki MX devices with security telemetry within Cisco XDR.

Accelerate response times

Quickly remediate threats using customizable orchestration playbooks and deep integrations across various security tools. Get the right threat context and practical advice to guide next best actions via Cisco AI Assistant in XDR.

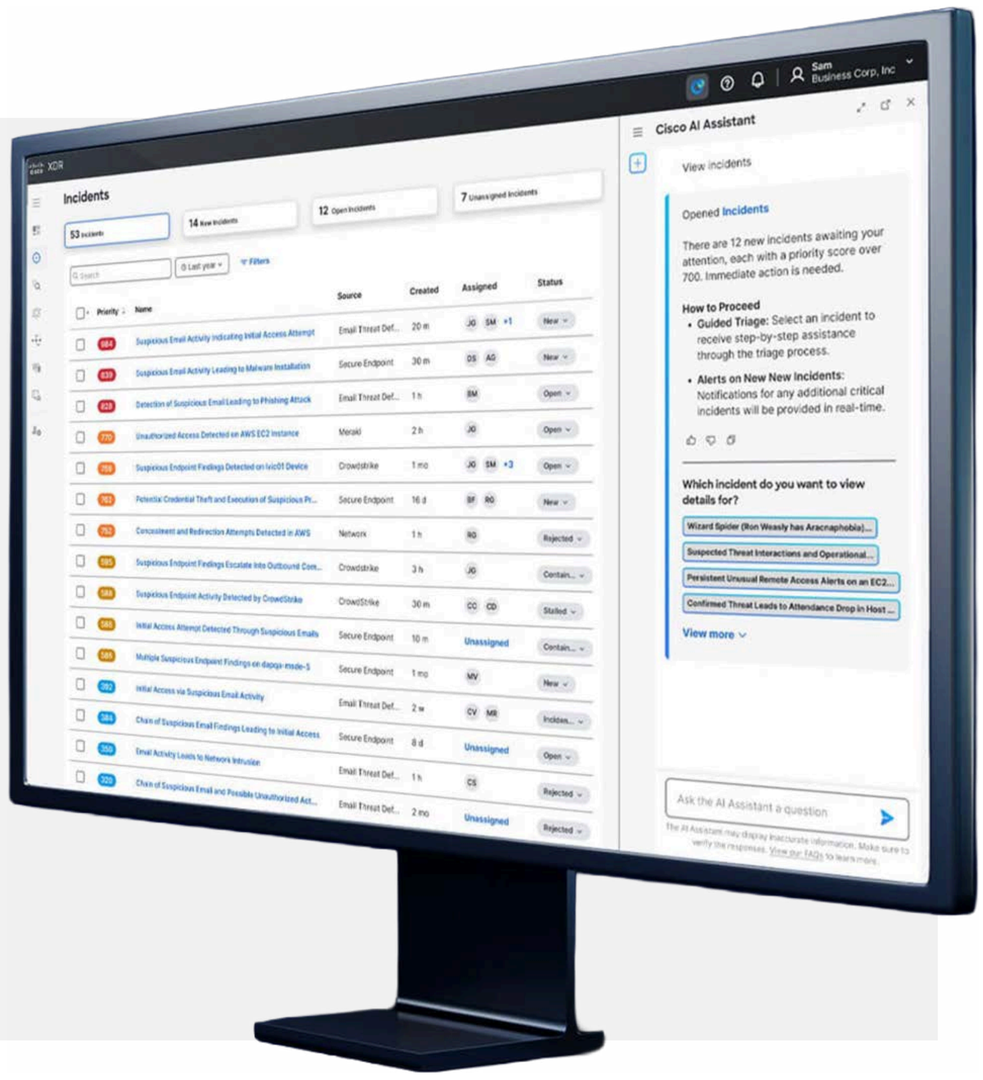
Stop ransomware in its tracks

Prevent data loss by triggering your backup and recovery solution to create a snapshot of high-value assets at the first signs of a ransomware attack. Restore your last known good configuration, getting your organization up and running with as little downtime and data loss as possible.

With Logicalis Managed Cisco XDR, analysts can focus on verified threats, cut response time, and reduce fatigue by automating repetitive tasks. A single managed service, with one unified platform, offers organizations the proactive defense posture that reactive, tool-heavy environments cannot deliver.

Key Capabilities of Cisco XDR

- **Security Analytics and Correlation**
  Cisco XDR's built-in analytics and correlation engine can ingest a vast variety of events and telemetry, including EDR security events, public cloud and private network flow logs, and more.
- **Network Telemetry Ingestion**
  SecOps teams can remove “blind spots” by ingesting public cloud logs (AWS, Google Cloud Platform, and Microsoft Azure) using an agentless monitoring of workloads and API integrations.



- **Asset Context**
  The Cisco XDR Asset Insights feature collects data from security products and traditional device managers, resulting in a unified asset inventory that can support investigations and reports.

- **Custom Automation Workflows**
  No-to-low-code automated workflows can interact with various types of resources and systems, whether from Cisco or third-party vendor.

- **Automation Workflow Exchange**
  The Cisco XDR Automation Exchange allows team members to quickly find and install new automation workflows, and operationalize the workflows within a few clicks.

- **Threat Intelligence**
  In addition to the built-in threat intelligence from Cisco Talos, teams can combine other sources of threat intelligence to gain crucial context during incident enrichment, investigation, validation, and hunting.

- **Incident Prioritization**
  New incidents are assigned a priority score and are automatically enriched. New detections that are discovered in the enrichment process that are relevant to an incident are added to that incident.

- **Incident Response**
  The built-in Response Playbook allows security analysts and incident responders to quickly respond to incidents with step-by-step, guided responses for incidents follow the SANS “PICERL” incident response model.

- **Threat Hunting and Threat Investigation**
  Cisco XDR Investigate offers advanced threat hunting capabilities, retrieving both local and global threat intelligence as well as any reported sightings of the investigated items in your environment.

- **Digital Forensics and Incident Response**
  Cisco XDR Advantage and Premier offers the XDR Forensics capability, which triggers digital forensics to collect over 350 artifacts on endpoints, including compromised or partially encrypted ones.

- **Third-Party Telemetry**
  Cisco XDR Advantage customers benefit from commercially supported and curated integrations with select third-party tools across a range of vectors, EDR, ETD, NGFW, NDR, and SIEM.

Go from Alert Fatigue to Action

with Logicalis Managed Cisco XDR

Logicalis Managed Cisco XDR services put our global team of security experts at your disposal. Our SecOps teams function as a virtual extension of your own team, taking on operational and analytical work that many in-house security teams lack the capacity to handle:

- Global SOCs operate 24/7 with Level 1-3 analysts, SOC managers, incident responders, threat hunters, and compliance auditors
- Plan and deploy the Cisco XDR environment and configure integrations across your existing tools and infrastructure
- Build custom automation playbooks, monitor for threats continuously, investigate and triage incidents, and execute containment and remediation

With over 15 years of managed security expertise and a global network of SOCs, we enable your organization to leverage an enterprise-grade SOC without needing to deploy and manage it yourself.

If your team is ready to simplify security operations and move from alert fatigue to action, reach out to Logicalis today to book a complimentary security briefing.

Schedule free consultation

- One of the first global Cisco partner to launch Cisco XDR as a managed service
- Over 15 years of managed security expertise across enterprise, government, and regulated industries
- Cisco XDR Certified Partner Specialization status for managed service delivery
- 24/7 global SOC coverage
- AI-driven threat correlation, automated response playbooks, and digital forensics built into a single managed offering

LOGICALIS
Architects of Change

CISCO PARTNER
Cisco Preferred Cloud and AI Infrastructure Partner
Cisco Preferred Security Partner
Cisco Preferred Collaboration Partner
Cisco Preferred Services Partner
Cisco Preferred Networking Partner
Splunk Partner