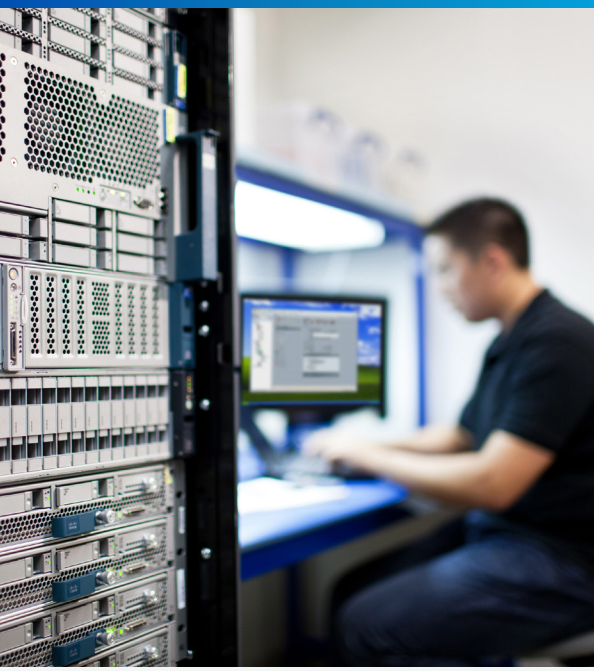
Threat Management



Benefits

- Protect your data, resources, and reputation against advanced, sophisticated threats
- Identify compromised endpoints and malicious actors operating inside your enterprise, where they can do the most damage
- Improve your overall security with ongoing analysis and mitigation guidance that's customized for your business, based on your historical traffic patterns and the specific threats you face

Cisco Security Advisory Services:
Custom Threat Intelligence

Networks are coming under attack everywhere. Hackers, thieves, and spies are hammering away at defenses in the largest corporations and individual PCs. Cisco created the Cisco® Custom Threat Intelligence (CTI) Service to help our customers understand what's really happening in their networks. That includes analyzing inbound traffic as well as outbound traffic coming from inside the enterprise.

Your Network Is Threatened as Never Before

Major network attacks are now conducted by sophisticated, well-funded teams that can evade corporate security measures and steal millions of records from companies like yours. Traditional security measures are very good at identifying risky traffic that is inbound to your company. But they're not very good at identifying the risky outbound traffic initiated from within your enterprise. And it's that outbound traffic—containing your trade secrets, customer data, or worse—that adversaries want to exploit.

In 2013, Cisco identified multiple indicators of compromise on nearly 100 percent of the enterprise networks we analyzed. Many enterprises don't keep network traffic log data, and very few keep more than 90 days of traffic logs to analyze for anomalous behavior—even though it takes 243 days on average to discover an advanced threat. These undetected threats place you at significant risk for compromised intellectual property, loss of sensitive customer and financial data, and high costs from disrupted operations and remediation efforts.

The Intelligence You Need

The Cisco CTI Service collects and analyzes multiprotocol traffic and metadata across your network to uncover threats, malicious behavior, and indicators of compromise (IOCs).

Using extensive sources of threat intelligence along with contemporary and historical knowledge of your network telemetry, the service provides periodic reports that identify suspicious and anomalous network traffic. It reveals possible attacks, breaches, and data exfiltration. Cisco security experts analyze this information based on block lists, observed trends in cyber compromises, unique vulnerabilities facing your industry, and geopolitical factors that might affect actors and targeted information. Then they provide detailed advice to mitigate and remediate threats.

Combining Cisco's unparalleled understanding of network traffic flows with continually expanding global threat intelligence, the Cisco CTI Service gives you the visibility and guidance you need to understand ongoing security incidents and safeguard your business.

Cisco Security Advisory Services: Custom Threat Intelligence

Safeguard Your Business

The Cisco CTI Service exploits the unique position and power of the network to identify malicious behavior inside your network. With these capabilities, you can:

- **Monitor and analyze outgoing traffic** and track every communication event in your network to detect malicious devices and actors inside your enterprise
- **Identify compromised endpoints** that are communicating with competitors, rogue sites, and other known bad actors, or generating unusual traffic patterns and admin connections
- **Gain actionable intelligence to mitigate threats** with expert guidance from Cisco cyber security analysts to plan and prioritize your remediation strategies
- **Measure and continually improve your overall security** by combining ongoing traffic flow monitoring with repeated custom analysis of your specific business and industry threats to track the efficacy of your threat monitoring approach

Why Cisco?

Cisco's unique approach for threat intelligence is a completely customized capability (including customized consulting support to interpret analyses and advise on remediation) to analyze communication events using a minimally intrusive approach.

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.

Case Study

Case Study: Cisco Helps Global Automaker Uncover Corporate Spy

By monitoring outbound network traffic, Cisco spotted anomalous activity in a major automaker's network that normally would have gone undetected but disguised a serious breach. Analysts alerted the company to an otherwise unremarkable desktop computer that suddenly started transmitting large amounts of data and then stopped.

An investigation revealed that the PC belonged to the head of procurement. He was responsible or sensitive negotiations with suppliers. And he had just quit the company to take a job with a competitor. The executive was pilfering confidential data to use against his former employer. With the Cisco CTI Service, the automaker was able to detect this corporate espionage and pinpoint the source. Ultimately, the company received a judgment against the executive's new employer worth more than $1 billion.

DEC14CS4667 07/15