Cisco Security Intelligence Operations

Executive Summary

Today's organizations require security solutions that accurately detect threats, provide holistic protection, and continually adapt to a rapidly evolving, constantly changing threatscape. The Cisco SecureX™ Architecture, supported by Cisco Security Intelligence Operations (SIO), helps organizations achieve these goals. Cisco SIO is composed of three pillars: **Cisco SensorBase™**, a comprehensive threat database; **Threat Operations Center** with 500 security analysts and constant **dynamic updates** fed to Cisco security devices. Together, these pillars allow SIO to better enable accurate, efficient, and up-to-date coverage, including protection from advanced and zero-day threats, in Cisco® security products.

The Challenge

Organizations are facing more security challenges than ever. In the past, it was adequate to focus on content, ports and IP addresses, but the threatscape has shifted and evolved. Fast-flux botnets constantly shift domains and addresses, while spam and malware are now well obfuscated and in many cases unique. Employees demand access to social media sites, yet these very sites are being used for social engineering and malware delivery.

In the past, IT was also in a better position to dictate standards and had control over the endpoint. Now, with employees bringing their own devices to the workplace, the user expects to be able to use any device, anywhere to gain seamless, secure access to corporate resources. This has created challenges for IT, as the attack surface has grown, increasing opportunities for the "bad guys" and increasing challenges for the "good guys."

Attacks are taking different forms. Threats propagate over multiple vectors, including social networks, email, and web. Multiple scan engines from multiple vendors can improve catch rates, but due to the inherent limitations of signature-based scanning, this approach can only take you so far, regardless of how deep you look into the packet. Then there is the problem of zero-day threats–threats for which no signatures exist yet.

False positives and negatives are another challenge. Security should not prevent communication, which could happen should intrusion prevention systems (IPSs) or firewalls generate a large number of false positives. In the past, whitelists were common workarounds, but this approach presents its own challenges. For example, what happens when a whitelisted domain is hit with a virus that spreads by email? Far better to have consistently accurate security, with low false negatives and low false positives.

Cisco Security Intelligence Operations Overview

Cisco SIO enables:

- Accurate detection of malware
- Holistic protection from business disruption and data loss
- Continual adaptation to stay ahead of the latest threats

Cisco SIO provides comprehensive threat intelligence that allows the organization's security team and network infrastructure to accurately detect malware and other threats. Analysis of content alone is no longer enough. With SIO, Cisco security products are able to make security policy enforcement decisions augmented by context, an enhancement enables more accurate and timely security protection.

The three pillars of Cisco Security Intelligence Operations:

- Cisco SensorBase
- Threat Operations Center
- Dynamic updates

Cisco SensorBase

- 1 TB of data per day
- More than 700,000 network devices
- 40,000 vulnerabilities
- 20 billion HTTP requests per day
- 100 million email messages per day
- 35% of all email traffic
- More than 150 million endpoints

Executive Summary
The Challenge
Cisco Security Intelligence Operations Overview
Dynamic Updates
Distributed Threat Intelligence
Global Correlation Mode
What are the benefits of Cisco Security Intelligence Operations?
Why Cisco?

A key part of any security plan is understanding the threats one faces. Cisco SensorBase is the largest, most comprehensive threat database in the world with telemetry from over 700,000 Cisco deployments worldwide, including web security, email security, IPSs, firewalls, and endpoint systems. SIO processes 20 billion http requests and 35% of the world's email traffic, resulting in more than 1 TB of data per day. This threat intelligence is augmented by third-party news and data feeds and a global network of spam traps–all monitored around the clock.

This data provides context to make security policy enforcement decisions. We look not only at the content itself, but also consider the who, what, where, when, and how of the transaction, which is important because experienced spammers and malware authors have developed considerable expertise in obfuscating code and making messages appear unique.

If we look at what we know about the source or the sender, we can make better security decisions. Is the domain known good, known bad, or somewhere in between? How long has it been registered? Is the address static or dynamic? What is the physical location? Is it an employee? Are they inside or outside the firewall? These and many other factors are taken into consideration when making security enforcement decisions, allowing more accurate, more precise decisions to be made.

Threat Operations Center

- Global, distributed, virtual team
- 24x7x365 operations
- 500 engineers, researchers, and technicians
- 111 PhDs, advanced degrees, and industry certifications
- Nine patents, plus another four pending
- More than 40 languages
- 200 parameters tracked
- 8 million rules pushed our per day

While algorithms, rules, and heuristics facilitate fast, accurate security, as threats evolve it is useful to hand-tune and optimize the system. Thus, the heart of Cisco SIO is the Threat Operations Center, a virtual team of more than 500 engineers, technicians, and researchers holding 111+ PhDs and industry certifications, collectively speaking over 40 languages.

Cisco's powerful, automated algorithms process SensorBase data in real time. These tools generate about 95 percent of the rule updates used in Cisco devices. The remaining rules are defined and hand-tuned for optimal performance by analysts in the Threat Operations Center.

One team reverse engineers malware and spam. Another takes that information and uses it to create update packages.

Together they allow Cisco to deliver better protection.

Reputation Filtering

Cisco security deployments use reputation information about the sender in order to provide better, more accurate security. We define reputation in terms of a score, a value that can range from −10.0 for the worst to +10.0 for the best. The reputation score is based on more than 200 aggregated and weighted parameters.

Cisco security deployments can be configured to reject data from senders with low scores (below −3.0.) and rate-limit senders that have medium to low reputation scores. This first line of defense improves the efficiency and overall block rate of the overall security system.

Cisco Security Intelligence Operations

In addition to conducting research, threat operations teams also collaborate across Cisco and with Cisco customers to gather feedback and build secure products.

The Threat Operations Center also provides the data that is used for outreach to the security community and as the backbone for the Cisco IntelliShield Alert Manager Service.

Dynamic Updates

Cisco SIO delivers a constant stream of information and updates to Cisco customers and devices. Threat mitigation data is provided through:

- Automatic rule and filter updates
- IntelliShield vulnerability aggregation and alert services
- Security best practice recommendations and community outreach services

Some security updates are available in real time, such as the reputation data used by Cisco security devices to block traffic from known malicious senders. Other systems, such as Cisco IPS with Global Correlation, check for new rules roughly every three to five minutes.

Raw data is stored in Cisco SensorBase, where it is analyzed by both automated systems and human threat analysts. Reputation scores are adjusted based on observed behavior while threat technicians ensure hand-tuned filters and algorithms provide the best possible protection. Reputation updates are immediate, while filters and other updates are updated every few minutes. This interaction between devices and Cisco SIO enables advanced protection and enforcement, including protection against zero-day threats.

Threat Operations

Current TOC presence in the following regions:

- California
- Texas
- Ohio
- Idaho
- China
- Ukraine
- UK
- Israel
- Canada
- India
- Australia

Global Correlation

Cisco SIO uses sophisticated algorithms to turn SensorBase data into actionable intelligence that is used by the Global Correlation engine.

Supervised Learning

Real-time Anomaly Detection

Reputation Scoring

Distributed Threat Intelligence

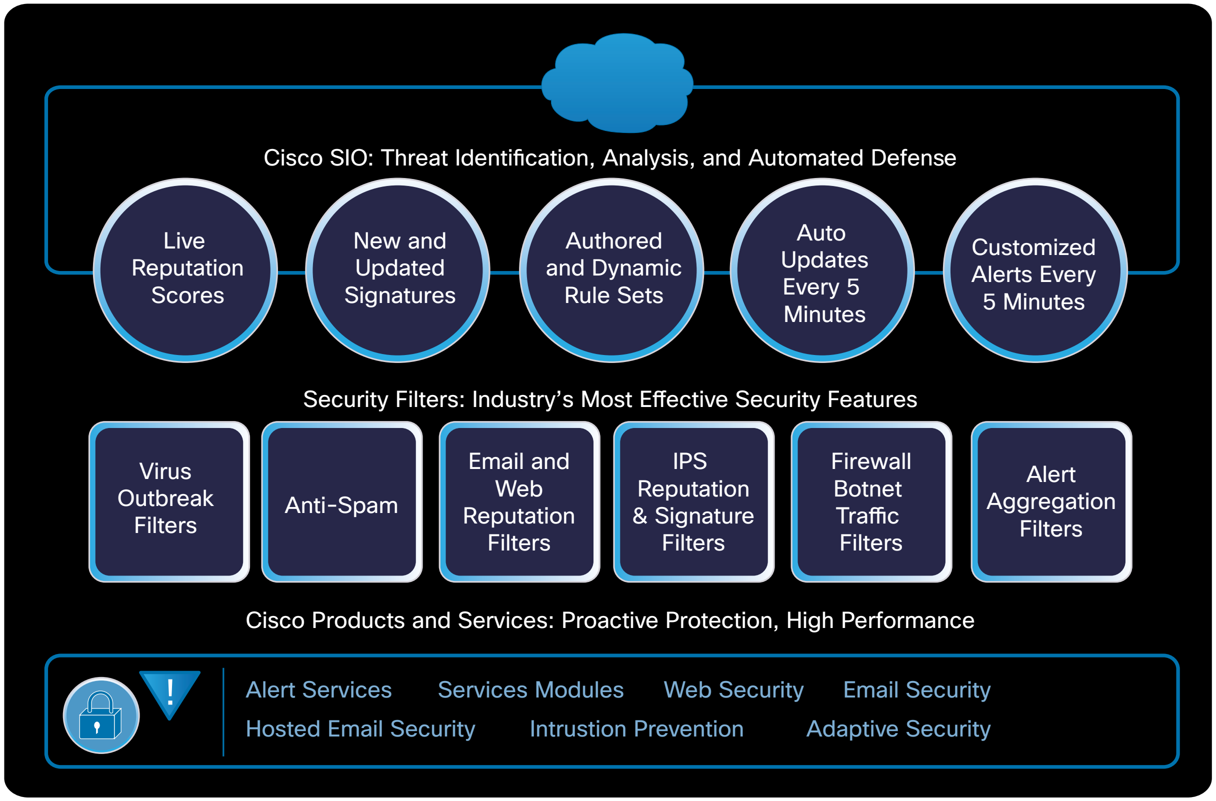
Cisco SIO is the command and control center for Cisco security services and appliances around the world. However, the intelligence is distributed, with devices in the field playing an important role. Cisco SIO operates in three ways:

Device-to-Cisco SIO and Cisco SIO-to-Device

First, Cisco devices, whether on-premise or cloud-based, act as the enforcement points in this ecosystem—they use the Cisco SIO filters and reputation data to block (or allow) traffic. They also contribute threat intelligence and data back into Cisco SIO. Just by making reputation queries, customers are contributing to the Cisco SensorBase data set.

Device-to-Device

A second way that Cisco SIO works is within a corporate network. When one device in the network detects an event or a rule fires, that device informs other Cisco security deployments in that network. An IPS sending an access control list (ACL) to a firewall is an example of this. Not all customers implement this level of Cisco SIO integration, but it does enable faster responses to new threats.



Cisco SIO: Threat Identification, Analysis, and Automated Defense

Live Reputation Scores
New and Updated Signatures
Authored and Dynamic Rule Sets
Auto Updates Every 5 Minutes
Customized Alerts Every 5 Minutes

Security Filters: Industry's Most Effective Security Features

Virus Outbreak Filters
Anti-Spam
Email and Web Reputation Filters
IPS Reputation & Signature Filters
Firewall Botnet Traffic Filters
Alert Aggregation Filters

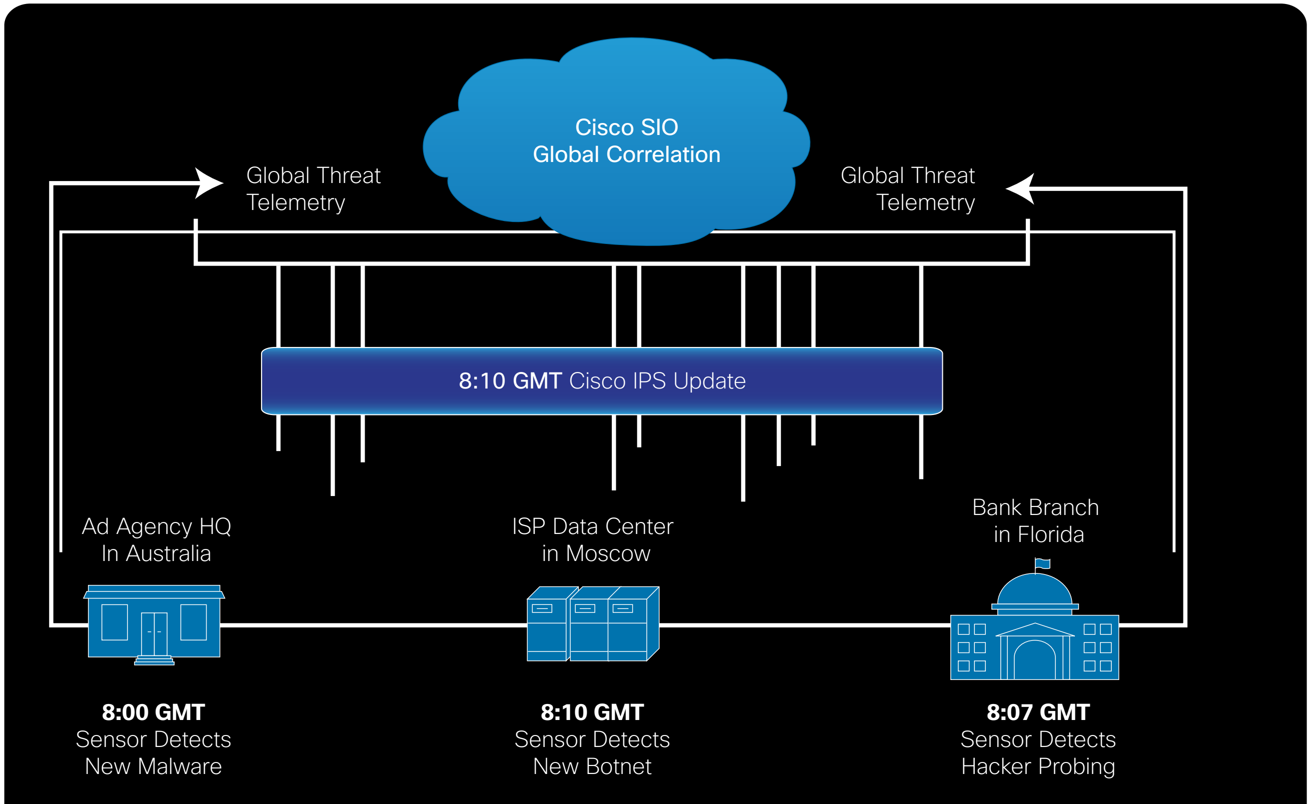
Cisco Products and Services: Proactive Protection, High Performance

Alert Services
Services Modules
Web Security
Email Security
Hosted Email Security
Intrusion Prevention
Adaptive Security

Global Correlation Mode

Cisco SIO works in a third, more global way. When new threats are detected, that data is shared with Cisco SIO and then with other Cisco customers around the globe. Cisco SIO is already the world's largest global security ecosystem. The distributed nature of the SIO threat intelligence network ensures that, with each additional appliance, module, or cloud-based service coming online, our visibility into global threats and the effectiveness and accuracy of the security we deliver cooperation increases.

> "Ten years of compelling data clearly indicates the virus problem shows no sign of abating. Real progress will be made when companies rely less on defensive technologies and more on proactive security policies and practices."
>
> – LARRY BRIDWELL
> Content Security Programs Manager, ICSA Labs


Cisco SIO
Global Correlation
Global Threat Telemetry
Global Threat Telemetry
8:10 GMT Cisco IPS Update
Ad Agency HQ In Australia
ISP Data Center in Moscow
Bank Branch in Florida
8:00 GMT Sensor Detects New Malware
8:10 GMT Sensor Detects New Botnet
8:07 GMT Sensor Detects Hacker Probing

In this example, Cisco IPS with Global Correlation detects threats propagating in various countries and creates a new ruleset within 5 minutes to protect against the emerging threat.

What are the benefits of Cisco Security Intelligence Operations?

Cisco SIO helps organizations:

- Block more spam/malware
- Prevent false positives
- Protect valuable corporate intellectual property and financial records
- Maintain regulatory compliance (PCI, HIPAA, etc.)
- Protect brand/reputation
- Avoid unnecessary cleanup costs
- Increase system uptime/availability
- Speed growth by embracing new technologies
- Optimize operational efficiency
- Gain visibility into the latest threatscape
- Improve protection against zero-day, advanced, and emerging threats
- Increase spam and threat prevention through higher detection accuracy

> "Email Outbreak Filters are a big winner for us. We know that our network is protected, even as we wait for antivirus signature updates."
>
> – MARK DIAL
> E-Messaging Team Manager,
> Tellabs, Inc.

Email

Highest Accuracy

- Visibility into 30% of GLOBAL email traffic
- Spam capture rate: 99% + lowest false positive rate
- Our edge on the competition = 35 hours

Why Cisco?

With the increase in blended, cross-protocol, and cross-vendor vulnerability threats, the security industry has come to recognize that point defenses, which provide protection from individual threats or for individual products, are no longer enough. Integrated security management, real-time reputation assessment, and a layered, multipoint approach are needed.

A more distributed infrastructure greatly increases the opportunities for attack–and the attack surface itself. With the rise of consumerization and BYOD (Bring Your Own Device), greater mobility, increased adoption of cloud services, and wider acceptance of social media, increased risk is inevitable. Cisco SIO enhances organizations' ability to understand, identify, and mitigate today's threats. Cisco is committed to providing complete, integrated, effective security solutions–enabling pervasive security for organizations worldwide.

Learn more about Cisco security:

- Cisco Security Intelligence Operations (SIO): www.cisco.com/go/sio
- Cisco Security Solutions: www.cisco.com/go/security