Cisco Security Intelligence Operations At-A-Glance

What Is the Value of Cisco Security Intelligence Operations?

Cisco Security Intelligence Operations (SIO) is an advanced security infrastructure that provides threat identification, analysis, and mitigation to continuously provide the highest level of security for Cisco customers. Using a combination of threat telemetry, a team of global research engineers, and sophisticated security modeling, Cisco SIO enables fast and accurate protection, allowing customers to securely collaborate and embrace new technologies.

What Problems Does It Help Solve?

Today's collaborative infrastructure and evolving security landscape bring an abundance of risk. Newly adopted tools and services, often untried and vulnerable, can be sabotaged by cybercriminals or exploited for financial gain. The newest wave of threats often target personal data and are blended in nature, propagating by way of multiple vehicles such as web, email, and USB keys in order to bypass legacy security tools. Even strong security technologies are often unable to keep up with today's attacks: They are too nimble, specialized, and targeted. The consequences from security breaches include company image damage, personally identifiable information (PII) theft, service downtime, cleanup and remediation costs, compliance penalties, and corporate liability. The following threat statistics highlight the level of risk:

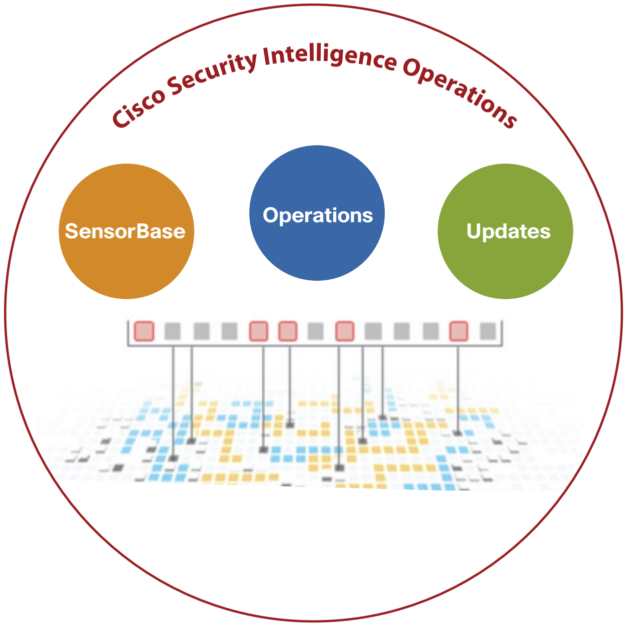
- Spam accounts for more than 100 billion messages each day, which is approximately 85 percent of the email sent worldwide. Eighty percent of spam is from infected clients.
- The number of disclosed vulnerabilities grew by 6.77 percent from 2007 to 2008.
- Vulnerabilities in virtualization products tripled to 103 in 2008 from 35 in 2007.
- Approximately 50 percent of attacks are by serial offenders. Approximately 70 percent of botnets use dynamic IP addresses to evade blacklists.
- Over the course of 2008, there was a 90 percent growth rate in threats originating from legitimate domains; nearly twice the amount of 2007.[1]
- Organizations that experienced a data breach in 2008 paid an average of $6.6 million last year to rebuild their brand image and retain customers.[2]

With limited resources to deploy and maintain more technology and clean-up after system compromises, organizations need a solution that can provide protection against evolving threats while reducing overhead costs. The following sections describe the Cisco SIO infrastructure, and explain how it can help organizations overcome today's security challenges.

Cisco Security Intelligence Operations Overview

Cisco Security Intelligence Operations is a sophisticated security ecosystem consisting of three components:

1. Cisco SensorBase: The world's largest threat monitoring network that captures global threat telemetry data from an exhaustive footprint of Cisco devices and services
2. Cisco Threat Operations Center: A global team of security analysts and automated systems that extract actionable intelligence
3. Dynamic updates: Real-time updates automatically delivered to security devices, along with best practice recommendations and other content dedicated to helping customers track threats, analyze intelligence, and ultimately improve their organization's overall security posture



Comprehensive Threat Intelligence

The intelligence arm of Cisco SIO includes the world's largest real-time threat monitoring network: Cisco SensorBase. SensorBase sources include:

- More than 700,000 (and growing) globally deployed Cisco security devices collecting threat information
- Cisco IntelliShield, a historical threat database of 40,000 vulnerabilities and 3300 IPS signatures
- More than 600 third-party threat intelligence sources, which track over 500 third-party data feeds and 100 security news feeds around the clock

More than 1000 threat collection servers process 500 GB of data a day. The Cisco Threat Operations Center processes this global real-time threat intelligence and incorporates it into the security services available on Cisco security devices, for unrivaled protection.

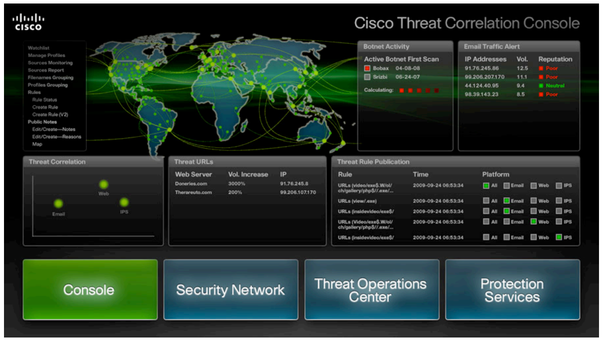
[1] Cisco 2008 Annual Security Report: https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=4026&keyCode=171020_1

[2] Poneman Institute Study 2008: http://www.washingtonpost.com/wp-dyn/content/article/2009/02/02/AR2009020203064.html?hpid=sec-tech

Threat Operations Center

The operations arm of Cisco SIO is a combination of people and automated algorithms that:

- Process Cisco SensorBase data in real time
- Create machine-generated and manually generated rules
- Provide actionable intelligence for protection against new and dynamic threats



Botnet Activity

Active Botnet First Scan	
🟥 Bobax	04-08-08
□ Srizbi	06-24-07
Calculating:	🟥 🟥 🟥 🟥 🟥

Email Traffic Alert

IP Addresses	Vol.	Reputation
91.76.245.86	12.5	🟥 Poor
99.206.207.170	11.1	🟥 Poor
44.124.40.95	9.4	🟩 Neutral
98.39.143.23	8.5	🟥 Poor

Threat URLs

Web Server	Vol. Increase	IP
Doneries.com	3000%	91.76.245.8
Therareuto.com	200%	99.206.107.170

Threat Rule Publication

Rule	Time	Platform
URLs (video/exe$.W/ol/ch/gallery/php$//.exe/...	2009-09-24 06:53:34	🟩 All □ Email □ Web □ IPS
URLs (view/.exe)	2009-09-24 06:53:34	□ All 🟩 Email □ Web □ IPS
URLs (insidevideo/exe$/	2009-09-24 06:53:34	□ All 🟩 Email □ Web □ IPS
URLs (Video/exe$.W/ol/ch/gallery/php$//.exe/...	2009-09-24 06:53:34	□ All □ Email 🟩 Web □ IPS
URLs (insidevideo/exe$/	2009-09-24 06:53:34	□ All □ Email □ Web 🟩 IPS

The Threat Operation Center teams consist of more than 500 people dedicated to 24x7x365 threat research, analysis, and quality assurance spanning five global locations. The threat operations teams not only research Internet threats, but also collaborate across Cisco to build and maintain capabilities for engineering security products and provide outreach to help combat cyber-crime. These teams include:

- Cisco IronPort Email and Web Threat Research Teams: Provide the latest protection for SMTP and Web-based attacks.
- Cisco Malware Research Lab: A centralized malware lab focused on researching the latest malicious activity.
- Intrusion Protection Signature Team: Researches and develops vulnerability and exploit-specific signatures that are used by IPS product lines.
- Cisco Product Security Incident Response Team (PSIRT): Evaluates and works across Cisco to mitigate vulnerabilities reported in Cisco products.
- Strategic Assessment Technology Team (STAT): Advanced, area-specific security research and product vulnerability testing.
- Infrastructure Security Research & Development (ISRD): A research-oriented, business enablement function that maintains strong expertise in the area of security and creates security solutions for customers engaged in emerging industries and infrastructures.
- Remote Management Services (RMS): Provides 24x7x365 remote monitoring and management of Cisco security devices that are deployed on your network.
- IntelliShield Security Analysts: Collect, research, and provide information about security events that have the potential for widespread impact on customer networks, applications, and devices.
- Applied Intelligence: Researches, documents, and tests potential mitigations for Cisco Security Advisories and Responses, Microsoft Security bulletins, and other vendor security advisories to help Cisco customers improve network security, protect infrastructure investments, and ensure business continuity.

Global Correlation

Cisco Global Correlation is a sophisticated, automated security capability that gives IPS devices unprecedented threat management efficacy. Global Correlation automatically correlates SensorBase threat information, including reputation, known exploits, anomalous behaviors, and vulnerability information, to detect blended, widespread, and targeted attacks.

Global Correlation is powered by the complete visibility across all threat vectors gathered from SensorBase.

Whereas traditional network IPSs examine only the packet contents, Global Correlation performs a full-context analysis to better understand if the traffic contains suspicious activity—not just what the contents are, but who sent it, what it contains, where it came from, and how it has evolved. The following parameters are considered in the Global Correlation engine:

- Who: The reputation of counterparty. The Reputation Filter blocks the worst offenders, stopping 10 to 15 percent of attacks, and assigns an appropriate reputation to suspected attacks.
- What: The packet contents that match an exploit or vulnerability signature. Cisco has more than 3300 signatures and continues to dedicate resources towards this endeavor.
- Where: Geographic and vertical trends of the packets.
- How: The propagation and mutation methods. The IPS performs global inspection to correlate reputation scores, using the risk rating assigned through signature analysis and anomaly detection.

Global Correlation uses these parameters to continuously builds, tests, and publishes new rules to deliver a more effective, accurate, and timely halting of attacks through Cisco IPS sensors. Results include:

- Twice the effectiveness of signature-only IPSs
- More accurate detection of attacks and fewer false positives, due to reputation analysis
- Updates that are 100 times faster than traditional signature-only methods

Cisco Security Intelligence Operations At-A-Glance

Dynamic Updates

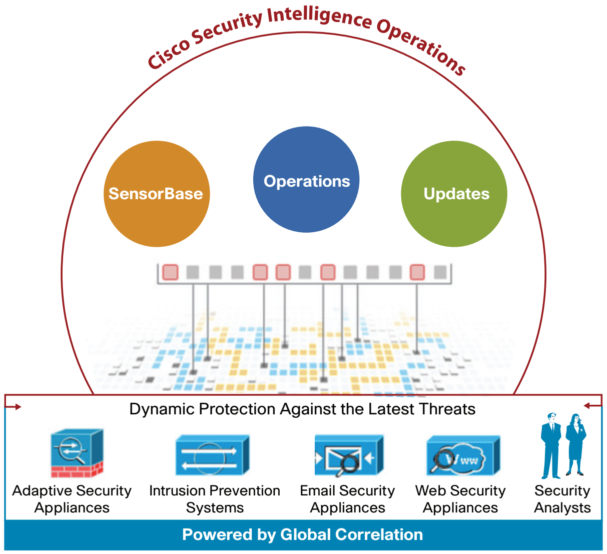
Cisco SIO's dynamic updates deliver current and complete security information to Cisco customers and devices. Threat mitigation data is provided through:

- Automatic rule updates for Cisco products, such as firewall, web, IPS, or email devices
- IntelliShield vulnerability aggregation and alert services
- Security best practice recommendations and community outreach services

Some security updates are available in real-time, for example reputation data that is used by Cisco security devices to block traffic from known malicious senders. Other systems, such as Cisco IPS with Global Correlation, query for new rules every 5 minutes.

In addition to dynamic updates, Cisco's security intelligence is represented in many forms for the benefit for the general public, end customers, enterprises, and even governments. Examples of the other forms of Cisco security intelligence include:

- Cisco IntelliShield Alerts, including Malicious Code Alerts, Security Activity Bulletins, Security Issue Alerts, Threat Outbreak Alerts, and Geopolitical Security Reports
- Cisco Annual Security Reports
- Cisco PSIRT Security Advisories and Security Responses
- Applied Mitigation Bulletins
- Cyber Risk Reports
- Security Intelligence Best Practices
- Service Provider Security Best Practices
- Cisco IPS Active Update Bulletins
- IntelliShield Event Responses
- Annual Security Report
- Cisco IronPort Virus Outbreak Reports


Cisco Security Intelligence Operations
SensorBase
Operations
Updates
Dynamic Protection Against the Latest Threats
Adaptive Security Appliances
Intrusion Prevention Systems
Email Security Appliances
Web Security Appliances
Security Analysts
Powered by Global Correlation

Through this full security lifecycle approach to understanding and combating threats, you gain the knowledge required to make educated decisions to increase your security posture while helping to ensure that your network is automatically protected from the latest attacks.

What Are the Benefits of Cisco Security Intelligence Operations?

The business benefits of Cisco SIO are as follows:

- Avoid unnecessary cleanup costs
- Protect brand reputation
- Increase uptime
- Speed growth by embracing new technologies
- Optimize operational efficiency
- Increase compliance posture
- Gain visibility into the latest threat landscape
- Improve protection against new and emerging threats with increased effectiveness of security devices, including Cisco IronPort Email and Web Security, Cisco IPSs, and Cisco Adaptive Security Appliances
- Increase spam and threat prevention through higher detection accuracy

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 protect from individual threats or protect individual products, are no longer enough. Integrated security management, real-time reputation assessment, and a layered, multi-point approach are needed.

As infrastructures become more collaborative, increased risk is inevitable. Cisco Security Intelligence Operations enhances the ability to identify, analyze, and mitigate today's threats. Cisco is committed to providing complete security solutions that are integrated, timely, and effective—enabling pervasive security for organizations worldwide to collaborate with confidence.