



the Lippis Report

Lippis Report 125: Cisco Launches Cloud-Based Global Correlation Threat Defense

During this downturn Cisco has taken the opportunity to launch initiatives that rivals simply do not have the scale and wherewithal to deliver. Cisco is delivering well thought out solutions to big problems with its smart grid initiative, EnergyWise energy management, Unified Computing System (UCS), collaboration, and now IT security. At RSA Cisco launched its Cisco Security Intelligence Operations (SIO) that leverages its presence in service provider and enterprise networks to deliver a global correlation of threats and in the process offers the deepest and widest range of IT security defenses available in the industry. SIO is in essence a “security cloud” service capable of identifying



Sneak Peak at the May 7th IT Innovation Forum and Cisco’s Spring Innovations Launch

[Listen to the Podcast](#)

threats propagating throughout the internet and intranets before corporate networks are infected by transmitting mitigating code to enterprise security devices such as IPS, firewall, Web and email systems.

IT security has been delivered piece meal and aligned with an IT supplier’s core competency. For example, Microsoft delivers security patches and fixes to Windows often, Anti-X firms such as McAfee, Trend Micro, IBM, Symantec, etc., focus on desktop malware, application firms such as Oracle, et al., deliver security solutions to protect their applications, Juniper, Check Point, and others offer firewalls and IPS, etc. All of these security solutions are useful and needed, but they are not systemic. They cannot correlate and interact with other security software to bolster defenses and provide SECOPS with contextual information that reduces false alarms and focuses defenses to mitigate an attack. This is where networking acting as a threat mitigation system offers unique value and where Cisco SIO delivers.



Cisco Security Intelligence Operations Delivers Global Correlation for Threat Defense via a Security Cloud

[Listen to the Podcast](#)

First let’s frame the problem most, if not all, SECOPS and business leaders are confronted with on a daily basis. Over the past business cycle enterprises have significantly increased their use of collaborative and social networking



applications which deliver productivity value but also an abundance of risk. Cybercriminals are front and center to either sabotage or gain financially through these new applications. The newest wave of threats often target personal data and are blended in nature, propagating via multiple vehicles such as web, email, and USB keys to bypass legacy or siloed security tools. The all-too familiar consequences from security breaches include company image damage, personally-identifiable information (PII) theft, service downtime, cleanup and remediation costs, compliance penalties, and corporate liability. Consider the level of risk:

- Spam accounts for over 100 billion messages each day, which is approximately 85% of email sent worldwide. Eighty percent of spam is from infected clients
- The number of disclosed vulnerabilities grew by 6.77% between 2007 to 2008
- Vulnerabilities in virtualization products tripled, from 35 in 2007 to 103 in 2008
- Fifty percent of attacks are by serial offenders, and 70% of botnets use dynamic IP addresses to evade blacklists
- Over the course of 2008, there was a 90% growth rate in threats originating from legitimate domains, nearly 2 times the amount of 2007
- 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

WAN Advantage: New Thinking in Branch Office and WAN Edge Design plus Services

[Get the White Paper](#)

The goal of Cisco's SIO and global correlation is to both close the above vulnerabilities and give employees the freedom to use collaborative, social, mobile and other IT assets with significantly reduced risk. SIO is built upon Cisco's security products including Cisco IPS and Cisco ASA and leverages IronPort and IntelliShield to deliver security intelligence. But SIO is an architecture or framework made up of three components: SensorBase, Threat Operations Center and Dynamic Updates. It's these three components working in unison that deliver global correlation to threat mitigation and in the process also delivers a security infrastructure that dynamically protects a corporation against the latest threats. Let's look more closely at them:

Cisco SAFE: A Security Reference Architecture: The Changing Network and Security Landscape

[Get the White Paper](#)

SensorBase: The first SIO component is Cisco SensorBase, which identifies threats by collecting information from over 700,000 plus and growing globally deployed sensors such as IPS devices, firewalls, web security and e-mail security devices and 600 third-party feeds. The number of sensors and partner feeds continues to grow as Cisco customers can choose to opt in to SensorBase and send traffic samples to it on the order of 500GB/day allowing SIO to detect malicious activity in their traffic. As a point of scale SensorBase is able to examine over 30 percent of the world's e-mail thanks to strategically located honey-pot accounts equipped with e-mail addresses that have been publicized on lists that spammers might use to send spam, thanks to relationships with 8 of the top 10 global ISPs. SensorBase has enhanced the ability to sniff out and identify the latest threats.

Cisco Security Intelligence Operations At-A-Glance

[Get the White Paper](#)

With so many of today's threats being blended, meaning that an exploit might enter a corporation through e-mail, then pass through the web which ends up having botnet traffic that eventually infects a client and phones home to the botnet server. An exploit could traverse or use three or four different vehicles before it launches a full-scale attack. Therefore, the more that security defenses can view the better the defense. To address blended threats, SensorBase is collecting information from four initial sensors and correlating this information with approximately 3,300 IPS signatures. The combination of IPS signatures with massive sensor feeds allows SensorBase to expand beyond exploit-specific to vulnerability-specific threats allowing IPS signatures to cover a wider range of exploits. For example, there may be 100 exploits intending to affect a vulnerability but by SensorBase addressing vulnerability

specific threats, one IPS signature can mitigate 100 exploits, making SensorBase IPS signatures much more potent than traditional IPS device signatures.

In addition to the sensors and IPS signatures, SensorBase also has integrated Cisco's IntelliShield, which contains the largest vulnerability database on the planet with 40,000 different vulnerabilities that are continually tracked. In addition to sensors, IPS signatures, and IntelliShield, SensorBase also collects information from 600 third-party feeds as well. The benefit of SensorBase is being able to collect real time network traffic threats from so many devices into a live information feed, where security threat information is always being collected and used to correlate and extrapolate more sophisticated intelligence to warn customers and mitigate threats.

Threat Operations Center: The second SIO component is Cisco's Threat Operations Center (TOC) that consists of five global teams of researchers and analysts. The most important attribute of TOC is that it develops automated techniques that extract SensorBase threat information and deliver actionable tasks to close vulnerabilities. These automated techniques build upon SensorBase live information feeds, a reputation database to deliver globally-correlated identified threats, and develop automated mitigation strategies quickly which are then transmitted to email, web, IPS and firewall devices hopefully before an enterprise is infected.

Dynamic Updates: The third SIO component is Cisco's dynamic updates and actionable intelligence distributed in real time to customer security devices around the globe. Reputation is at the heart of global correlation as TOC is able to score threats from 1 to 10, 10 being threats with the worse reputations. Reputation-scored threats contain such parameters as the originator, its source destination, IPS signature, etc., across multiple types of threats. Reputation data is generated in real time as threats are emerging, so that TOC may send dynamic updates of threat mitigation information to IPS devices around the world. In short, TOC analyzes the SensorBase live information feed for threats, calculates reputation scores and automatically sends out security updates and alerts to e-mail, web, firewall and IPS devices via dynamic updates.

Dynamic updates, in the case of reputation-identified threats scoring between 8 and 10 are distributed in real time. These high reputation-scoring threats afford high priority and speed of mitigation as SECOPS can automatically block the threat, because their threat reputation indicates that they've sent large percentages of malicious traffic to the point that it's not worth inspecting. Dynamic updates are sent, on average, every three to five minutes for low scoring reputation-based threats.

The scale of SIO is cloud spec. SensorBase is based upon 1000 plus servers processing 500GB of data/day streaming in from 700,000 sensors and 600+ partner feeds. To use SIO, Cisco customers only need to upgrade their IPS to software version 7.0 and ASA 5500 Series software version 8.2. IPS version 7.0 provides IPS reputation filtering with global correlation, which doubles the attack coverage and significantly reduces false positives. ASA version 8.2 is equipped with Botnet traffic filter, which detects infected clients as they attempt to phone home at a rate of blocking 100,000s of malware connections per week. Cisco IronPort was the pioneer of automatically gathering threat intelligence and global correlation, and Cisco Web and Email customers only need to maintain their subscriptions to continue benefiting from SIO.

Full Context Threat Analysis

With IPS and ASA supported by SIO Cisco is offering a fuller context to threat analysis and mitigation. For example, traditionally IPSs analyzed content, meaning that they analyzed packets; but now with SIO threats are identified by source reputation and location plus propagation and mutation methods. This is key to correlation in that in addition to sending out updates every five minutes from SensorBase to IPS, email, web, firewalls and other appliances, they have the option to send their information to SensorBase too; i.e., the data flow is bi-directional increasing the number of sensors over time. In addition to receiving this security data, it's gathered over multiple technologies, increasing the context of the threat. What is key about this bi-directional information feed is that it draws from multiple types of technologies, i.e., email, web, firewall, IPS, etc., enabling SIO to defend against blended attacks or offer different mitigation tactics over time as the attack mutates, as has been observed with Conficker, McColo, Srizbi, etc., botnets and other types of threats.

Recommendations and Guidance:

For Cisco customers upgrading to IPS v7.0 and ASA v8.2 software versions will offer a large functionality upgrade and access to SIO. Botnet threat mitigation and global correlation through reputation scoring are powerful defenses to add to IT security operations. For those Cisco customers with Cisco IronPort Web and Email Security Appliances, they will continue to enjoy the full power and defense against blended attacks with global correlation.

I recommend that a pilot first be deployed so that SECOPS gain an understanding of the SIO “system” meaning its alarms, feeds, threat mitigation results, false alarm rate and overall effectiveness. Once SECOPS and NETOPS are comfortable and skilled then a more phased deployment can commence.

SIO is clearly targeted to the Cisco installed base; however for those who are investing in IT security and have yet to purchase IPS and ASA (vertically integrated security appliance offering VPN, firewall, IPS, etc., security services), SIO should be considered, as it’s currently unmatched in the industry. SIO and in particular SensorBase, reputation scoring and global correlation offer a unique approach to defending against today’s complex and increasing volume of threats.