

Cisco Info Center for Security Management

Q. What is the Cisco® Info Center for Security Management?

A. Cisco Info Center for Security Management is a policy-based network security information management solution that can assess, track, network events, and visually display their service and business Impact.

Q. Is Cisco Info Center required to install Cisco Info Center for Security Management?

A.

- Yes it is. In particular, Info Server Module must be installed in the environment.
- For Cisco Info Center product information visit:
<http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/index.html>

Q. What features does Cisco Info Center for Security Management offer?

A.

- End-to-end visibility of security across the complete enterprise (core data network, voice over IP [VoIP], storage)
- Software-based resilience for 24-hour performance
- Visibility of the effect of security threats on business operations
- Powerful user interface, with different real-time views of the security infrastructure and services (Custom Security Overview (CSO) view,

security-operations-center (SOC) manager view, SOC operator view, and customer or user view)

- Proven, tested, and documented scalability; more than 1500 of the world's largest service providers and enterprises are using this technology

The product is already integrated into all Cisco security devices, and it supports integration with Solsoft NP.

Q. Explain deduplication, cross correlation, and filters in Cisco Info Center for Security Management?

A. *Filtering and deduplication* are key challenges with a subscriber identity module, based on the huge volumes of information that need to be analyzed by the operator to identify threats. This analysis must be accomplished in real time in order to deal with the threat before it incurs costly business Impact.

Deduplication, correlation, and filtering are used to condense the core information that the operator has to deal with, removing background noise to focus the operator on the potential threats.

Deduplication

The Cisco Info Center Info Mediator (probes) collects information from the security, network, and infrastructure devices and systems.



Mediators provide deduplication to reduce much of the superfluous information generated by the security appliances before passing the information to the event database (Cisco Info Center Info Server) and the correlation engine Impact Security Policy Manager. The deduplication condenses many instances of the same alert into a single alert with information on how many times the alert occurred and over what time interval.

The Cisco Info Center Info Mediator can collect information from a wide range of devices—both security and standard infrastructure components; more than 400 Cisco Info Center mediators are available for connecting to different types of systems, including but not limited to:

- Cisco security devices—All the Cisco network intrusion devices, Cisco Host Intrusion Detection System (IDS) Sensor, Cisco Network IDS (NIDS), Cisco PIX[®] Firewall, and Cisco IOS[®] Firewall
- Third-party security—ISS Real Secure Firewall1, Nixsun Netdetector, Johnson Control's Metasys, Netscreen, UNIX AAA, Windows NT AAA, and virus checking
- Network infrastructure components (Cisco switches, routers)
- Servers and applications
- Third-party devices; for example, environmental security systems
- Other management systems

Correlation

Cisco Info Center for Security Management Impact Security Policy Manager identifies and prioritizes threats. For each threat, it identifies in real time the Impacted devices and the associated services provisioned.

The strength of this solution is that it can take information from security devices as well as network and infrastructure nodes for cross-domain correlation and assessment. IMPACT includes a security correlation policy pack that has the following:

“Threat Score” Policy

This policy definition assigns scores to categories of security attacks and creates a new synthetic threat based on activity from each unique source or destination in the Cisco Info Center Info Server. Each threat is assigned a priority.

- The policy tracks individual attackers and attack targets as single entities.
- The score is computed by severity and number of correlated events.
- The threat score is related to the possible severity of the security event as provided via the best practices of the industry.
- The threat event is escalated if the threat score is greater than the threshold.

Of the synthetic “threat events” created, there are two classes, common source address and common destination (target) address. These are referred to respectively as *probe threats* and *attack threats*. Probe threats indicate a single source triggering alerts in numerous security devices. An attack threat indicates a single device generating numerous alerts.

The threat score policy is used as a way to determine the priority of the threats that are affecting the most systems at any one time.



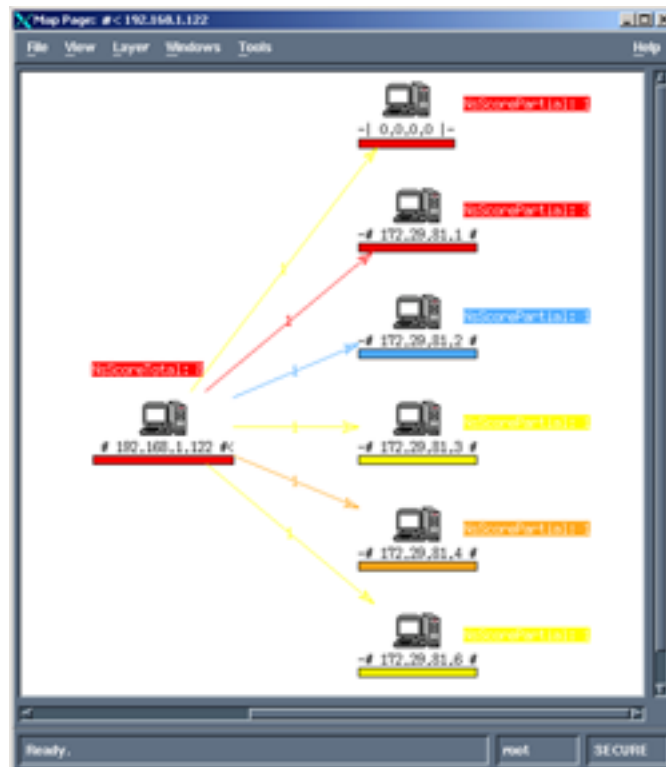
For example, the service provider or enterprise may be subject to a sophisticated hacker targeting numerous resources in different parts of the network, looking for weaknesses. Each possible attack will trigger an alarm. However, these alerts will come from different devices (Cisco PIX firewalls, host-based intrusion detection systems [HIDSs], NIDSs, Cisco IOS Software, switches, servers, and so on). And at any one time, there are many thousands of other alarms and background event noise.

In this case, the threat score policy automatically indicates that each of these alarms is related to the same hacker and correlates them into a single prioritized “probe” threat in real time.

Another example may be that many individuals are attempting to “hack” a known target—for example, a well-known corporate server, perhaps in a denial-of-service (DoS) attack. In this case, the threat score policy automatically identifies in real time the system that is under attack and the systems that are responsible for the attack, correlating to a single attack threat and thereby enabling prevention in real time before the DoS attempt can have any business impact.

The threat score policy enables visualization of the threat via the threat fingerprint tool (shown in Figure 1).

Figure 1
Visual Result of Threat Score Analysis



Filtering

The user interface enables users to set up filters related to a particular area, thereby reducing much of the background noise. Filters may be based on many combinations of variables and logic, including device type, alert type, time, and address range. Filters can be created using drag and drop with an intuitive interface.



The user interface displays the filtered events in real time.

Q. Can you describe scalability, performance, and resilience in Cisco Info Center for Security Management?

A. The Cisco Info Center for Security Management solution can be run completely from a single server or it can be distributed, depending on customer requirements.

The benefits of a distributed system include:

- *More efficient communications to remote Cisco PIX firewalls*—By placing the Cisco Info Center Info Mediator close to the Cisco PIX Firewall at a remote customer site, much of the superfluous management information can be reduced before it is transmitted back to the central SOC.
- *More secure communications to remote Cisco PIX firewalls*—Management information can be transmitted by authenticated TCP (with encryption if required) using Cisco Info Center Info Mediator rather than basic User Datagram Protocol (UDP) and syslog.
- The solution has been thoroughly tested and benchmarked for scalability. The scalability feature and tools include:
 - *Event reduction, correlation, and filtering*—Event reduction by deduplication dramatically reduces the number of events the system needs to deal with, thereby improving scalability. These key scalability features enable operators to quickly cut through the background noise in real time.
 - *Real-time memory*—All alerts are stored in memory in a database, enabling correlation and event management in real time with high performance; there is no need for disk input/output (I/O).
 - *Read-only servers*—Support for both read-only and read/write servers enable the system to scale to a very large number of users.
 - *Trouble ticketing*—This feature includes basic trouble ticketing and “journaling” features. It enables multiple operators to work effectively as a team in real time.
 - *Resilience*—Software-based resilience with synchronized databases across multiple hardware platforms enables automatic, hot standby.

Q. Can you explain Cisco Info Center for Security Management integration with other third-party products and SIM technologies?

A. The product is integrated with a wide range of third-party applications and includes support for a wide range of multivendor devices through a library of more than 400 Cisco Info Center mediators that cover many protocol interfaces across a variety of security as well as other infrastructure nodes.

The product can be integrated with other third-party information management tools such as NetForensics, Solsoft, and OpenSystems for an Integrated SIM operational environment.

Cisco Info Center for Security Management is Integrated with Cisco IP Solution Center
The product can be integrated with Cramer, Metasolv, and Granite systems for asset management. This enables assessment of any business impact from a threat.

Cisco Info Center for Security Management can initiate contact with case management, trouble ticketing, and customer relationship management (CRM) systems such as Remedy, Clarify, Siebel, and PeopleSoft. This integration enables automatic generation of trouble tickets if a security breach occurs.



Cisco Info Center for Security Management packages are integrated and interoperable with all Cisco element management systems, including CiscoWorks, Cisco WAN Manager, Cisco Transport Manager, and the Cisco Element Management System (EMS).

Q. Explain the correlation engine in Cisco Info Center for Security Management.

A. The correlation technology used in Cisco Info Center for Security Management is based on the original equipment manufacturer (OEM) technology from Micromuse called IMPACT. Cisco Info Center for Security Management provides customized Cisco based security monitoring policies for VPN. The pre-customization includes escalation and notification policies that enable the operator to perform automated standard practices and procedures as well as additional customization to automate many of the tasks associated with SIM. The user can also create customized security correlation policies via a graphical user interface (GUI).

Q. Can you recommend a deployment strategy for Cisco Info Center for Security Management and other event management applications?

A. Cisco Info Center for Security Management is targeted for deployments at any medium to large enterprise, data center, MSSP, or service provider. Cisco Info Center for Security Management components may be run from a single server or can be distributed as required.

In the cases where other event management applications such as NetForensics or OpenView are installed, the Cisco Info Center for Security Management solution provides the following added value:

- Comprehensive device support, including security, network infrastructure, and data center; consolidation and processing of events from all other applications in one console
- End-to-end security correlation between the different management domains for multiservice impact analysis
- Resilience
- Scalability in terms of devices, events, and users
- Business-level visibility and impact assessment of security threats
- Intuitive GUIs that can support all levels of user interaction, including CSO, SOC, network operations center (NOC), and customer network management (CNM)
- Integration with other management applications to provide multilayered security support

Q. Can you explain the systems requirement for Cisco Info Center for Security Management?

A.

- Recommended entry-level environment: Sun Microsystems Sunfire 280R, two CPUs (900 MHz), 2-GB RAM, 72-GB disk (approximately US\$14,000 per system)
- Recommended data-center solution (approximately 100 Windows servers, 2 Cisco PIX firewalls, 2 IDSs, 2 routers or more): Sunfire 880, 4 CPUs (900 MHz), 4-GB RAM, 72-GB disk (approximately US\$60,000 per system)

Memory is the most important resource for this application.

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R) VT/LW4441 0503