

CiscoWorks Security Information Management Solution 3.1 is the Next Evolution in Securing Business Infrastructure

One of the greatest challenges in enterprise security is managing the flood of alerts generated by a growing number of multivendor security devices and systems. Automation is required to isolate and prioritize the few messages that indicate real security threats.

The key to more effective security automation lies in a software technology known as Security Information Management (SIM). CiscoWorks Security Information Management Solution (SIMS) 3.1 is based on technology from netForensics and incorporates powerful features for gathering and analyzing the overwhelming amount of security event data that companies are experiencing.

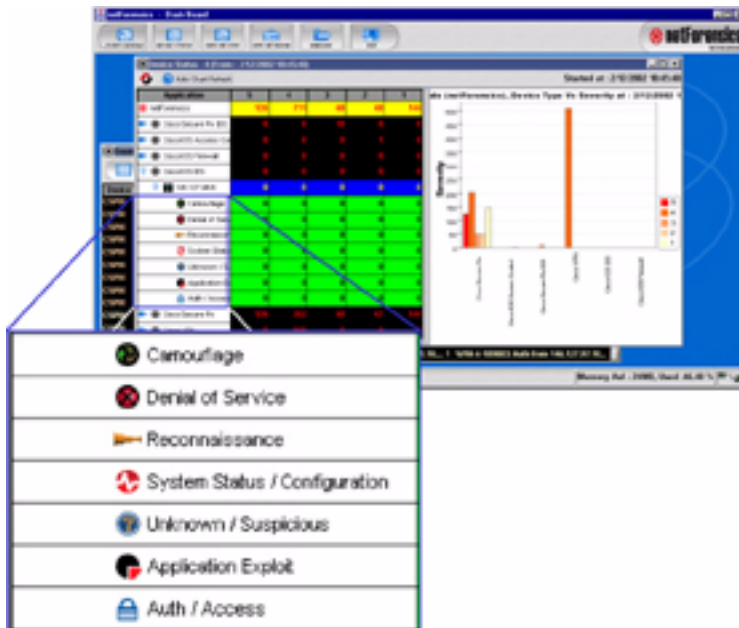
Companies can manage their growing security infrastructure and effectively monitor millions of event messages, without additional staff.

With CiscoWorks SIMS 3.1, the user has a solution that delivers:

- Complete event monitoring for SAFE and all multivendor security environments
- Advanced visualization for fast and intuitive security monitoring
- Integrated risk assessment to understand the overall vulnerability of any particular asset within the enterprise
- Comprehensive reporting and forensics for all levels of security operations
- Productivity gains and cost reduction

CiscoWorks SIMS 3.1 delivers these capabilities using the award-winning netForensics software, which is the central component of the solution.

CiscoWorks SIMS 3.1 collects, analyzes, and correlates security event information from across the enterprise in a series of four distinct phases: normalization, aggregation, correlation, and visualization.





Normalization and Aggregation

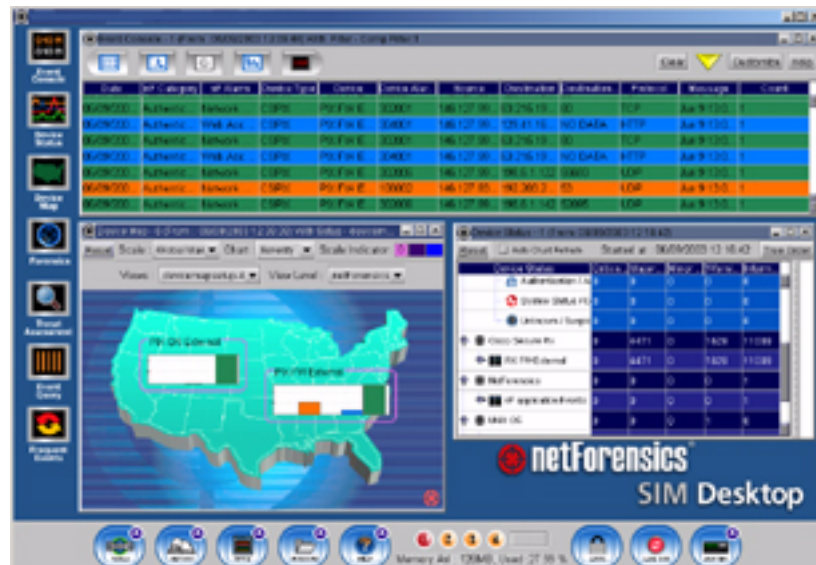
In the normalization and aggregation phases, security events are collected from virtually all intrusion detection systems, firewalls, operating systems, applications, and anti-virus systems and transformed into a common easy-to-understand XML format. Events are then aggregated to remove duplicate security event data – Security Operators see one message for a port scan against a PIX Firewall, not 6,000.

Correlation

Utilizing statistical correlation, normalized security events are categorized into security incident types by asset or asset group. Incident types can range from a reconnaissance attack, to a virus attack, to a denial of service attack, to name just a few. For each asset a threat score is continuously computed by combining event severity with asset value to determine an overall measurement of security incident potential. The key advantage is the ability to find those anomalies that may go undetected by a rules-based correlation implementation.

Visualization

CiscoWorks SIMS 3.1 displays correlated results on a centralized, real-time console with a graphical, Java-based interface that is powerful, intuitive, and user friendly.



The Executive Dashboard provides a real-time, enterprise-level view of security trends and the Real-Time Console facilitates fast isolation of security attacks using real-time correlation and analysis capabilities.



Risk Assessment

In security terms, risk assessment involves understanding the overall vulnerability of any particular asset within the enterprise. Risk is commonly defined as the combination of threat, vulnerability, and value, where:

- Threat is any abnormal traffic or activity directed against a system or asset. netForensics scores each threat type, whether it's a port scan or login failure. These scores are then considered in the overall risk calculation.
- Value is the level of importance (perhaps in dollars) of any particular system or asset. The value is a user-defined variable for each asset in the enterprise.
- Vulnerability is the likelihood that a threat will be successful against a system or asset.

The solution combines each of the above to formulate an overall risk score for each asset within the enterprise, with higher scores indicative of higher asset vulnerabilities. The solution produces a Risk Assessment Report that provides the necessary details behind each asset and its associated risk. By understanding the vulnerability of specific assets within an enterprise, companies can strengthen appropriate security policies.

Summary

As securing the enterprise IT infrastructure becomes more challenging, companies must rely on technology to help assimilate the amount of security event information that flows from an ever-increasing number of security devices and systems. In addition, technology must be used to not only aid organizations in reducing the risk of attacks, but also to help accelerate responses when attacks occur. CiscoWorks SIMS 3.1 increases the effectiveness of existing security teams and thereby helps achieve a real, measurable ROI.

Flexible Deployment Options

The CiscoWorks SIMS 3.1 is available for ordering as:

1. A software only option. This provides the flexibility to implement a multi-tier server architecture, This is suitable for larger deployments
2. An appliance option. Includes CiscoWorks SIMS 3.1 pre-installed on the Cisco 1160 hardware solution platform. This provides easier deployment for the customer.

The appliance option has the same functionality as the software only Starter Pack. The appliance includes a license for monitoring up to 30 devices. However if the overall event volume from the network is high, the appliance may support less than 30 devices.

If the event volume is low the user may purchase add-on licenses to monitor more than 30 devices. The actual number of devices that the appliance can support will vary depending on several variables, including the message rates, retention policy, and the device type. The appliance has several tools such as the System Health Monitor to measure the message rate and the performance of the software.

Software Only Option	Appliance Option
Distributed Architecture	Single Server
Global Scalability	Regional Scalability
1 to 4 Day Installation Service	Minimal Setup Time
Targeted for Medium to Large Sized Deployments	Targeted for Small to Medium Sized Deployments



Devices Supported for Monitoring.

Table 1 Event sources and versions supported

Application/Device	Version	nF Components
Arbor Peakflow DoS	2.1	Agent for Arbor Peakflow
Check Point FireWall-1	NG, 4.1	Agent for Check Point
Cisco IOS ACL, FW, IDS	12.2, 12.0	Syslog File Agent
Cisco Secure ACS	3.1,3.0	Agent for CSACS
Cisco Firewall Switch Module	1.1.2	Syslog File Agent
Cisco Secure IDS	4.1,4.0, 3.1, 2.5, 2.2	CSIDS Agent
Cisco Secure PIX	6.3, 6.2, 6.1, 6.0, 5.3, 5.2, 5.1, 5.0	Syslog File Agent
Cisco Secure PIX IDS	6.3, 6.2, 6.1, 6.0, 5.3, 5.2	Syslog File Agent
Cisco Security Agent	4.0	(requires Management Center for Cisco Security Agents to forward events)
Cisco VPN Concentrator	3.1, 2.5.2	Syslog File Agent
CyberGuard Firewall	5.1	Agent for CyberGuard
Dragon Sensor / Squire	6.1 / 1.3.1	Agent for Dragon
Entercept HIDS	4.0, 2.5, 2.0	Agent for Entercept
Intruvert	1.2	Agent for Intruvert
ISS RealSecure HIDS / NIDS	6.5, 6.0, 5.5 / 7.0, 6.5, 6.0	Agent for ISS RealSecure
ISS SiteProtector	2.0	Agent for ISS SiteProtector
NetScreen	4.0	Agent for NetScreen
Network Flight Recorder	3.0	Agent for NFR
Secure Computing Sidewinder	5.2	Agent for Sidewinder
Sourcefire	2.0	Agent for Sourcefire
Snort NIDS	1.8	Agent for Snort
Symantec Enterprise FW/VPN	7.0, 6.5	Agent for Symantec
Symantec ManHunt NIDS	2.2	Enterprise Firewall/VPN
Symantec ITA	3.6	Agent for Symantec
Tripwire NIDS	3.0	Agent for ManHunt
UNIX OS Events	Solaris 8/7/6, Linux 7.2/7.1	Agent for Tripwire
Web Servers	Apache, IIS, iPlanet	Agent for Web Servers
Windows Events	Win 2000 Server / Adv. Server	UNIX OS File Agent

The list of supported event sources and versions are frequently updated. This datasheet may not have the latest information.



System Requirements for Software Only Option

Supported Operating Systems

Table 2 lists the supported operating systems for different netForensics components.

Table 2 Quick Lookup for Supported Operating Systems

Component	Supported Operating System
nF Engine	Red Hat Linux, Solaris 8
nF Master	Red Hat Linux, Solaris 8
nF Provider/Oracle 9i Database	Red Hat Linux, Solaris 8
nF Web Server	Red Hat Linux, Solaris 8
nF Agent for Arbor Peakflow	Red Hat Linux, Solaris 8, Windows
nF Agent for Check Point	Red Hat Linux, Solaris 8, Windows
nF Agent for CSACS	Windows 2000
nF Agent for CSIDS	Red Hat Linux, Solaris 8
nF Agent for CSIDS 4.0	Red Hat Linux, Solaris 8, Windows
nF Agent for CyberGuard	Red Hat Linux, Solaris 8, Windows
nF Agent for Dragon	Red Hat Linux, Solaris 8
nF Agent for Entercpt	Windows 2000
nF Agent for ISS RealSecure	Windows 2000
nF Agent for ManHunt	Red Hat Linux, Solaris 8, Windows
nF Agent for Raptor	Solaris 8, Windows 2000
nF Agent for Sidewinder	Red Hat Linux, Solaris 8, Windows
nF Agent for Snort	Red Hat Linux, Solaris 8
nF Agent for Tripwire	Red Hat Linux, Solaris 8, Windows
nF Agent for Windows	Windows 2000
nF Batch Agent	Red Hat Linux, Solaris 8
nF Batch Agent for Check Point	Red Hat Linux, Solaris 8, Windows
nF Syslog File Agent	Red Hat Linux, Solaris 8, Windows
nF Universal Agents	Red Hat Linux, Solaris 8, Windows
nF UNIX File Agent	Red Hat Linux, Solaris 8

Note: Red Hat Linux 7.1 (Kernel 2.4.9) or Advanced Server only; Windows 2000 Server/Advanced Server (SP2) only; Solaris on SPARC only

Full Install

Table 3 Minimum System Requirements for Full Install of the Software Only Option

Component	Requirement
Operating System	See "Supported Operating Systems"
Processor	Linux: Dual Intel Pentium 4 1.5 GHz (server class) Solaris: Dual UltraSPARC-III 444 MHz (server class)
Memory	4 GB total system memory
Free disk space	18 GB (see "Disk Partitions" in the netForensics Quick Start Guide)
Storage Device	CD-ROM
Software packages	Linux: Anonymous FTP Server, development libraries, kernel development Solaris 8: See "Solaris Patches and Packages" in the netForensics Quick Start Guide)

Ordering Information

For Ordering Information, please refer to the product bulletin at <http://www.cisco.com/go/sims>.



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. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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) 203046/ETMG_06/03