DATA SHEET

Security Information & Event Manager (SIEM)

Compliance through Security Information and Event Management, Log Management, and Network Behavioral Analysis

Benefits

- Enables NOC and SOC staff to focus on actionable information rather than struggle to interpret millions of daily events generated by network security appliances, switches, routers, servers, and applications
- Uses advanced surveillance and forensics analysis to deliver situational awareness of both external and internal threats including inappropriate content, IM, file transfers, traffic from undesirable geographies, data theft, and malicious worm infections
- Leverages existing investments in network and security infrastructure while accelerating time to value through out-of-box functionality, rapid deployment, and staff efficiency gains
- Integrates with Extreme Networks Intrusion Prevention System (IPS), Network Access Control (NAC), and NMS Automated Security Manager solutions to provide a unified, real-time view of the threat landscape and effectively detect, isolate, and automatically remediate threats
- Integrates with a broad array of third party security and network products, including firewalls and routers, for the highest level of visibility and protection
- Virtual Flow Collector allows the analysis of network behavior and enables Layer 7 visibility within virtual infrastructures
- Meets the deployment requirements of the largest enterprises with modular component options and easily deployed high availability functionality

Delivers fast, accurate data about security threats:

- Severity of an attack
- Importance of the affected asset
- Identity of the attacker
- Credibility of data sources
- Identification of abnormal behavior

Product Overview

The Extreme Networks Security Information and Event Manager (SIEM) product combines best-in-class detection methodologies with behavioral analysis and information from third party vulnerability assessment tools to provide the industry's most intelligent security management solution. Extreme Networks SIEM delivers actionable information to effectively manage the security posture for organizations of all sizes.

The challenge created by most threat detection systems is the volume of information they generate — making it difficult to determine which vulnerabilities require an immediate, high priority response. The Extreme Networks SIEM solution addresses this challenge and provides powerful tools that enable the security operations team to proactively manage complex IT security infrastructures.

Extreme Networks Security Information and Event Manager:

- Goes beyond traditional security information and event managers and network behavioral analysis products to deliver threat management, log management, compliance reporting, and increased operational efficiency
- Collects and combines network activity data, security events, logs, vulnerability data, and external threat data into a powerful management dashboard that intelligently correlates, normalizes, and prioritizes — greatly improving remediation and response times, and greatly enhancing the effectiveness of IT staff
- Baselines normal network behavior by collecting, analyzing, and aggregating network flows from a broad range of networking and security appliances including JFlow, NetFlow, and SFlow records. It then discerns network traffic patterns that deviate from this norm, flagging potential attacks or vulnerabilities — anomalous behavior is captured and reported for correlation and remediation

- Tracks extensive logging and trend information, and generates a broad range of reports for network security, network optimization, and regulatory compliance purposes; report templates are provided for COBIT, GLB, HIPAA, PCI, and Sarbanes Oxley

All SIEM appliances offer High Availability (HA) functionality that ensures availability of SIEM data in the event of a hardware or network failure. HA provides automatic failover and full disk replication between a primary and secondary host. The secondary host maintains the same data as the primary host by either replicating the data on the primary host or accessing a shared external storage. At regular intervals the secondary host sends a heartbeat ping to the primary host to detect hardware or network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host. The Extreme Networks SIEM HA functionality is easily and cost-effectively deployed through appliances and wizards without requiring additional fault management solutions and storage options.

The Extreme Networks SIEM solution portfolio features appliances for quick and easy setup. The Extreme Networks SIEM solution complements its appliances with the Virtual Flow (VFlow) Collector. This virtual flow collector appliance enables application layer traffic monitoring and security intelligence in a virtual infrastructure. Available Extreme Networks SIEM solution components include:

- SIEM Base Appliance
- Flow Anomaly Processor
- Event Processor
- Network Behavioral Flow Sensors
- Virtual Flow Collector
- SIEM Console Manager
- High Availability options

Features

SIEM ALL-IN-ONE AND ENTERPRISE BASE APPLIANCES

Extreme Networks SIEM All-In-One and Base Appliances deliver actionable security intelligence in a rack-mount, network-ready platform. With flexible deployment options, they provide on-board event collection and correlation, Layer 7 traffic analysis, aggregation of flow data from multiple network connected devices, and a feature-rich management interface. Pre-installed software and web-based setup simplifies deployment and configuration for unified security management.

Extreme Networks' SIEM All-In-One appliances provide easy deployment and cost efficient network monitoring for small offices or enterprise branches. The SIEM Small Office Appliance (model DSIMBA7-GB) suits a small office need to monitor minimal rates of network events and flows where no expansion will be required. A small central site or enterprise department may have higher event and flow collection rate requirements. The SIEM Appliance for Small Enterprises (model DSIMBA7-SE) provides an ideal all-in-one option for these environments.

The SIEM Enterprise Base Appliance models (DSIMBA7-LX and DSIMBA7-LU) provide a range of options for large and geographically dispersed organizations. They are ideal for users that demand a scalable, enterprise-class solution that can be easily upgraded to support additional flow and event monitoring capacity as required.

All SIEM platforms capture event and flow data from a broad range of networked devices including application servers, web servers, workstations, routers, switches, firewalls, VPN tunnel servers, and IDS/IPS appliances. For a listing of supported devices please refer to the SIEM product information at http://www.extremenetworks.com/product/extreme-security-information-event-management/

SIEM FLOW ANOMALY PROCESSOR

The SIEM Flow Anomaly Processor (model DSIMBA7-FAP) is an expansion unit for Extreme Networks SIEM. It offloads and enhances the processing of flow data from the Base Appliances and interfaces with Behavioral Flow Sensors to collect IP traffic flow information from a broad range of devices. Each SIEM Flow Anomaly Processor can process up to 1,200,000 flows per minute (unidirectional).

SIEM EVENT PROCESSOR

The SIEM Event Processor (model DSIMBA7-EVP) is an expansion unit for Extreme Networks SIEM. It offloads and enhances processing of event data from the Base Appliances. Status events are collected from a broad array of network and security devices — including router syslogs, SNMP events, and firewall events. Each SIEM Event Processor can process up to 10,000 events per second and, for added flexibility, multiple Event Processors may be connected to a single Base Appliance.

SIEM COMBINED EVENT/FLOW ANOMALY PROCESSOR

The SIEM Combined Event/Flow Anomaly Processor (model DSIMBA7-EVP-FAP) is an expansion unit for Extreme Networks SIEM. It processes both flow data and event data. The Combined Processor supports 1,000 EPS and up to 50,000 FPM when fully licensed. Deployment of the Combined Event/Flow Anomaly Processor enables a highly distributed enterprise to provide cost effective local event and flow collection. It is well suited as an introductory event and network activity processor for remote or branch offices.

SIEM NETWORK BEHAVIORAL FLOW SENSORS

A network traffic flow is a sequence of packets that share common characteristics — such as source/destination IP address,

source/destination TCP port, and IP protocol used. SIEM Network Behavioral Flow Sensors are deployed at strategic points in the network to collect IP traffic flow information from a broad range of networked devices — including switches, routers, security appliances, servers, and applications. SIEM Network Behavioral Flow Sensors go beyond traditional flow-based data sources to enable application-layer (L1-L7) flow analysis and anomaly detection. Deep packet and content inspection capabilities identify threats tunneled over standard protocols and ports. Network Behavioral Flow Sensors interface with the Extreme Networks SIEM Base Appliances or the SIEM Flow Anomaly Processor.

SIEM VIRTUAL FLOW COLLECTORS

Gain the same visibility and functionality that SIEM Network Behaviorial Flow Sensors provide for the physical environment for the virtual network infrastructure. A SIEM Virtual Flow Collector is a virtual appliance that enables the analysis of network behavior and Layer 7 visibility within the enterprise's virtual infrastructure. SIEM Virtual Flow Collectors support up to 10,000 flows per minute and monitoring of three virtual interfaces with one additional switch designated as the management interface.

SIEM CONSOLE MANAGER

For large deployments, the SIEM Console Manager distributes the collection and processing of flows and logs while maintaining a global view of the entire network. Console Manager requires a minimum of one Processor Appliance (Event Processor, Flow Processor and/or Combined Event/Flow Processor). NBAD sensors are required for Layer 7 monitoring.

Specifications*

Technical Specifications for all SIEM appliances are shown in the tables below. All appliances support RAID 10 for high availability and redundancy of OS and storage. Extreme Networks SIEM appliances support external storage options including iSCSI SAN and NAS.

SIEM BASE ALL-IN-ONE VIRTUAL & HARDWARE APPLIANCES

MODEL	DVSIEM	DSIMBA7-SE DSIMBA7-SE-HA	DSIMBA7-LX DSIMBA7-LX-HA	DSIMBA7-LU DSIMBA7-LU-HA
Description	All-in-One security information and event management virtual appliance	All-in-One Security Information and Event Management for minimal event and flow rates	All-in-One High performance scalable security information & event management	All-in-One High performance scalable security information & event management for Large Enterprises
Upgrade Options*	Software License Upgrades Additional Flow processing: DVSIEM-25KF-UP, DVSIEM-50KF-UP Additional Event processing: DVSIEM-200E-UP, DVSIEM-500E-UP, DVSIEM-1KE-UP	Software License Upgrade Additional Flow processing: DSSES7-UP	Software License Upgrades Additional Flow processing: DLX25-50KF-UP, DKX25-100KF-UP, DLX25-200KF-UP, DLX50-100KF-UP, DLX50-200KF-UP, DLX100-200KF-UP Additional Event processing: DLX1-2.5KE-UP, DLX1-5KE-UP, DLX2.5-5KE-UP	Software License Upgrades Additional Flow & Event processing: DSLUS7-UP
Behavioral Flow Sensor	Uses Virtual Flow (VFLOW) Collector	Integrated Flow sensor	Uses External Flow sensor	Uses External Flow sensor
Flow per minute (FPM)	Base: 15,000 Flows (Bidirectional) 30,000 Flows (Unidirectional) Maximum: 50,000 Flows (Bidirectional) 100,000 Flows (Unidirectional)	Base: 25,000 Flows (Bidirectional) 50,000 Flows (Unidirectional) Maximum: 50,000 Flows (Bidirectional) 100,000 Flows (Unidirectional)	Base: 25,000 Flows (Bidirectional) 50,000 Flows (Unidirectional) Maximum: 200,000 Flows (Bidirectional) 400,000 Flows (Unidirectional)	Base: 100,000 Flows (Bidirectional) 200,000 Flows (Unidirectional) Maximum: 200,000 Flows (Bidirectional) 400,000 Flows (Unidirectional)
Events per second (EPS) Base & Maximum	Base: 100 EPS Maximum: 1000 EPS	Base: 1000 EPS Maximum: 1000 EPS	Base: 1000 EPS Maximum: 5000 EPS	Base: 2500 EPS Maximum: 5000 EPS
Appliance Form Factor	-	1 RU	2 RU	2 RU
Processor	-	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB
Memory	-	24 GB	48 GB	48 GB

MODEL	DVSIEM	DSIMBA7-SE DSIMBA7-SE-HA	DSIMBA7-LX DSIMBA7-LX-HA	DSIMBA7-LU DSIMBA7-LU-HA
Hard Disk	-	6 x 500GB 7200 RPM SATA 2.5"	9 x 1TB 7200 SATA 3.5"	10 x 1TB 7200 SATA 3.5"
Network Interfaces	-	4x10/100/1000 Base-T (on-board)	4x10/100/1000 Base-T (on-board)	4x10/100/1000 Base-T (on-board)
Power Supply	-	675W Redundant	675W Redundant	675W Redundant

* Note: Higher Scalability beyond the upgrade options can be achieved using External Flow Anomaly Processors & Event Processors

SIEM CONSOLE MANAGER

MODEL	DVSIEM-CON	"DSIMBA7-CON
Description	SIEM Virtual Console Manager	SIEM Console Manager Appliance
Flow per minute (FPM)	N/A (External Virtual Flow Anamoly Processor Required)	N/A (External Flow Anamoly Processor Appliance Required)
Events per second (EPS)	N/A (External Virtual Event Processor Required)	N/A (External Event Processor Applaince Required)
Appliance Form Factor	-	2 RU
Processor	-	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB
Memory	-	48 GB
Hard Disk	-	9 x 1TB 7200 SATA 3.5"
Network Interfaces	-	4x10/100/1000 Base-T (on-board)
Power Supply	-	675W Redundant

SIEM COMBINED EVENT AND FLOW ANAMOLY PROCESSOR

MODEL	DSIMBA7-EVP-FAP
Description	SIEM EVENT/FLOW Processor Appliance
Flow per minute (FPM)	Base: 25,000 Flows (Bidirectional) Maximum: 50,000 Flows (Bidirectional)
Events per second (EPS)	1000 EPS
Upgrade Options	Software License Upgrade
Upgrade Options	Software License Upgrade Additional Flow processing: DSEVPFAPS-UP
Appliance Form Factor	2 RU
Processor	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB
Memory	48 GB
Hard Disk	9 x 1TB 7200 SATA 3.5"
Network Interfaces	4x10/100/1000 Base-T (on-board)
Power Supply	675W Redundant

SIEM EVENT PROCESSOR

MODEL	DVSIEM-EVP	DSIM-EVP2500 DSIM-EVP2500-HA
Description	SIEM Virtual Event Processor	SIEM Event Processor Appliance
Events per second (EPS)	Base: 100 EPS	Base: 2500 EPS
Upgrade Options	Maximum: 1000 EPS	Maximum: 10,000 EPS
Appliance Form Factor	Software License Upgrades Additional Event processing: DVEVP-200E-UP, DVEVP-500E-UP, DVEVP-1KE-UP	Software License Upgrades Additional Event processing: DSEVPS7-UP
Processor	-	2 RU
Memory	-	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB
Hard Disk	-	48 GB
Network Interfaces	-	9 x 1TB 7200 SATA 3.5"
Power Supply	-	4x10/100/1000 Base-T (on-board)

** The maximum event processing may require an optional license upgrade.

SIEM FLOW PROCESSOR

MODEL	DVSIEM-FAP	DSIM-FAP100K DSIM-FAP100K-HA
Description	SIEM Virtual Flow Processor	SIEM Flow Processor Appliance
Flow per minute (FPM)	Base: 15,000 Flows Maximum: 50,000 Flows	Base: 100,000 Flows Maximum: 600,000 Flows
Upgrade Options	Software License Upgrades Additional Event processing: DVFAP-25KF-UP, DVFAP-50KF-UP	Software License Upgrades Additional Event processing: DSFAP-100K-UP
Appliance Form Factor	-	2 RU
Processor	-	2 x Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz; L3 Cache: 12 MB
Memory	-	48 GB
Hard Disk	-	9 x 1TB 7200 SATA 3.5"
Network Interfaces	-	4x10/100/1000 Base-T (on-board)
Power Supply	-	675W Redundant

** The maximum event processing may require an optional license upgrade.

SIEM NETWORK BEHAVIORAL FLOW SENSOR APPLIANCES

MODEL	DSNBA7-50-TX** / DSNBA7-50-TX-HA**
Rated Throughput	1 Gbps
Processor	Quad-Core Intel Xeon Processor; Frequency: 2.4 GHz
Memory	6 GB
Hard Disk Drive	160 GB SATA (x2)
Network Interfaces	"4x10/100/1000 Base-T (on-board) 4X1000 Base-SX"
Power Supply	90-264 VAC, Autoranging, 47-63 Hz, 502 W
Form Factor	1 RU

** Revision 5x appliances

ENVIRONMENTAL SPECIFICATIONS

- Operating Temperature: 10º C to 35º C (50º F to 95º F)
- Storage Temperature: -40º C to 65º C (-40º F to 149º F)
- Operating Relative Humidity: 20% to 80% non-condensing
- Storage Relative Humidity: 5% to 95% non-condensing
- Maximum Humidity Gradient: 10% per hour, operational and non-operational
- Operating Altitude: -16 m to 3,048 m (-50 ft to 10,000 ft)
- Storage Altitude: -16 m to 10,600 m (-50 ft to 35,000 ft)

SIEM VIRTUAL FLOW COLLECTOR SYSTEM REQUIREMENTS

(VFlow Collector 7.6.3.1)

- VMware ESXi 4.0
- VMware Infrastructure Client installed on the desktop system (VMware server applications are bundled with client software)
- VMware host requires 512 MB of free memory
- VMware host requires 36 GB of free disk space
- Extreme Networks SIEM Console version 7.6.3.1

AGENCY AND REGULATORY STANDARD SPECIFICATIONS

Safety

- UL 60950-1
- FDA 21 CFR 1040.10 and 1040.11
- CAN/CSA-C22.2 No. 60950-1
- EN 60950-1
- EN 60825-1
- EN 60825-2
- IEC 60950-1
- 2006/95/EC (Low Voltage Directive)

Electromagnetic Compatibility (EMC)

- FCC 47 CFR Part 15 (Class A)
- ICES-003 (Class A)
- EN 55022 (Class A)
- EN 55024
- EN 61000-3-2
- EN 61000-3-3
- AS/NZS CISPR-22 (Class A)
- VCCI V-3
- CNS 13438 (BSMI)
- 2004/108/EC (EMC Directive)

Environmental

- 2002/95/EC (RoHS Directive)
- 2002/96/EC (WEEE Directive)
- Ministry of Information Order #39 (China RoHS)

Ordering Information

ORDERING INFORMATION FOR SIEM APPLIANCES

CATEGORY	PART NUMBER	DESCRIPTION
SIEM BASE ALL-IN-ONE	DSIMBA7-SE DSIMBA7-SE-HA	All-in-One Security Information and Event Management for minimal event and flow rates
	DSSES7-UP	Adds additional 25K flow processing for DSIMBA7-SE (25K to 50K Flows)
	DSIMBA7-LX DSIMBA7-LX-HA	All-in-One High performance scalable security information & event management
	DLX25-50KF-UP	Adds additional 25K flow processing for DSIMBA7-LX (25K to 50K Flows)
	DKX25-100KF-UP	Adds additional 75K flow processing for DSIMBA7-LX (25K to 100K Flows)
	DLX25-200KF-UP	Adds additional 175K flow processing for DSIMBA7-LX (25K to 200K Flows)
	DLX50-100KF-UP	Adds additional 50K flow processing for DSIMBA7-LX + DLX25-50KF-UP (25K to 50K Flows)
	DLX50-200KF-UP	Adds additional 150K flow processing for DSIMBA7-LX + DLX25-50KF-UP (25K to 50K Flows)
	DLX100-200KF-UP	Adds additional 100K flow processing for DSIMBA7-LX + DLX50-100KF-UP (25K to 50K Flows)
	DLX1-2.5KE-UP	Adds additional 1500 EPS event processing for DSIMBA7-LX (1000 to 2500 EPS)
	DLX1-5KE-UP	Adds additional 4000 EPS event processing for DSIMBA7-LX (1000 to 5000 EPS)
	DLX2.5-5KE-UP	Adds additional 2500 EPS event processing for DSIMBA7-LX + DLX1-2.5KE-UP (2500 to 5000 EPS)
	DSIMBA7-LU DSIMBA7-LU-HA	All-in-One High performance scalable security information & event management for Large Enterprises
	DSLUS7-UP	Adds additional 100K flow & 2500 EPS processing for DSIMBA7-LU (100K to 200K Flows & 2500 to 5000 EPS)
	DVSIEM	All-in-One security information and event management virtual appliance
	DVSIEM-25KF-UP	Adds additional 10K flow processing for DVSIEM (15K to 25K Flows)
	DVSIEM-50KF-UP	Adds additional 25K flow processing for DVSIEM + DVSIEM-25KF-UP (25K to 50K Flows)
	DVSIEM-200E-UP	Adds additional 100 EPS event processing for DVSIEM (100 to 200 EPS)
	DVSIEM-500E-UP	Adds additional 300 EPS event processing for DVSIEM + DVSIEM-200E-UP (200 to 500 EPS)
	DVSIEM-1KE-UP	Adds additional 500 EPS event processing for DVSIEM + DVSIEM-500E-UP (500 to 1000 EPS)
SIEM CONSOLE MANAGER	DSIMBA7-CON DSIMBA7-CON-HA	SIEM Console Manager Appliance
	DVSIEM-CON	SIEM Virtual Console Manager

Ordering Information Continued

ORDERING INFORMATION FOR SIEM APPLIANCES

EXTERNAL FLOW AND EVENT PROCESSOR	DSIMBA7-EVP-FAP	SIEM Combined Event/Flow Processor Appliance
	DSEVPFAPS-UP	Adds additional 25K flow processing for DSIMBA7-EVP-FAP (25K to 50K Flows)
	DSIM-EVP2500 DSIM-EVP2500-HA	SIEM Event Processor Appliance
	DSEVPS7-UP	Adds additional 2500 EPS event processing for DSIM-EVP2500
	DVSIEM-EVP	SIEM Virtual Event Processor
	DVEVP-200E-UP	Adds additional 100 EPS event processing for DVSIEM-EVP (100 to 200 EPS)
	DVEVP-500E-UP	Adds additional 300 EPS event processing for DVSIEM-EVP + DVEVP-200E-UP (200 to 500 EPS)
	DVEVP-1KE-UP	Adds additional 500 EPS event processing for DVSIEM-EVP + DVEVP-500E-UP (500 to 1000 EPS)
	DSIM-FAP100K DSIM-FAP100K-HA	SIEM Flow Processor Appliance
	DSFAP-100K-UP	Adds additional 100K flow processing for DSIM-FAP100K
	DVSIEM-FAP	SIEM Virtual Flow Processor
	DVFAP-25KF-UP	Adds additional 10K flow processing for DVSIEM-FAP (15K to 25K Flows)
	DVFAP-50KF-UP	Adds additional 25K flow processing for DVSIEM-FAP + DVFAP-25KF-UP (25K to 50K Flows)
SIEM ADD LOG SOURCES	DSIMBA7-DEV	SIEM Additional 1 Log source
	DSIMBA7-DEV-50	SIEM Additional 50 Log sources
	DSIMBA7-DEV-500	SIEM Additional 500 Log sources
	DSIMBA7-DEV-1K	SIEM Additional 1,000 Log sources
	DSIMBA7-DEV-5K	SIEM Additional 5,000 Log sources
	DSIMBA7-DEV-10K	SIEM Additional 10,000 Log sources
FLOW SENSORS & COLLECTORS	DSIMBS7-VFLOW	SIEM VFLOW Collector for VMWARE ESX-ESXI
	DSNBA7-1G-SX DSNBA7-1G-SX-HA	Behavioral Flow Sensor with 1 Gbps rated throughput (fiber interfaces)

POWER CORDS
In support of its expanding Green initiatives as of July 1st 2014, Extreme Networks will no longer ship power cords with products. Power cords can be ordered separately but need to be specified at the time order. Please refer to www.extremenetworks.com/product/powercords/ for details on power cord availability for this product.

Warranty

As a customer-centric company, Extreme Networks is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Extreme Networks SIEM comes with a one-year warranty against manufacturing defects. For full warranty terms and conditions please go to: www.ExtremeNetworks.com/support/warranty.aspx.

Service & Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Extreme Networks account executive for more information about Extreme Networks Service and Support.

Extreme networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800