

# Security Information & Event Manager (SIEM)

## Supported Devices/Event Sources

Enterasys SIEM (also known as DSCC) collects security events from a heterogeneous set of sources that includes network infrastructure, security devices, servers, and applications. It normalizes all events to enable automatic out-of-the-box correlation with other events and network flows. In addition, Enterasys SIEM surveys the entire network, using native flow sources in a customer's routing/switching infrastructure or data from distributed collectors to gather a detailed history of all network flow activity. Enterasys SIEM supports the following industry-flow formats:

### **NetFlow, J-Flow, SFlow, cFlowd, Packeteer Flow Data Records**

New devices and event sources are continually being added. Contact Enterasys for the latest information.

### **Antivirus**

- McAfee AV/e-Policy Orchestrator
- Sophos Enterprise Console
- Symantec System Center and Antivirus Client
- Trend Micro Antivirus
- Trend Micro Control Manager

### **Authentication and DHCP**

- Bridgewater Systems, Service Controller
- Cisco ACS (Authentication Control Server)
- Cisco NAC Appliance
- Cyber Ark PIM Suite
- ForeScout CounterACT
- FreeRadius RADIUS Server
- Generic Authentication Server
- ICS BIND
- Juniper Steel Belted Radius
- Lieberman Software
- Linux Red Hat DHCP logs
- MetalInfo MetalIP DHCP Server
- Microsoft DNS
- Microsoft IAS
- Microsoft DHCP Server
- RSA Authentication Manager
- Sun Solaris DHCP Server
- Symark Power Broker

### **Databases**

- IBM DB2
- IBM Informix
- IBM IMS
- Microsoft SQL Server
- Oracle (v9i, v10G)
- Oracle Audit Vault
- Oracle Database Listener
- Sybase ASE Database
- Imperva SecureSphere

### **Storage Management**

- NetApp Data ONTAP

### **Firewalls/VPN**

- Cisco ACE Firewall
- Check Point, FireWall-1 & OPSEC (NG, FP1, FP2, FP3, AI R54, NGX R60)
- CheckPoint Endpoint Security
- Cisco FWSM
- Cisco IOS Firewall
- Cisco PIX Firewall
- Enterasys NAC
- Fortinet
- Generic Firewall Device Support
- Juniper NetScreen Firewall
- Juniper Secure Access SA

- Linux Iptables
- Nokia Firewall
- Nokia IP Series
- Nortel Switched Firewall
- PaloAlto Networks PA Series
- Secure Computing Cyberguard
- Symantec SGS Appliance

### **Generic/Custom**

- Any custom device that emits Syslog, SNMP, or SDEE.
- File-based logs can be sent via syslog, FTP, SFTP and SCP
- Events retrieved via JDBC
- Log Event Enhanced Format(LEEF)
- Asset Exchange Information Source(AXIS)

### **Host Logs**

- Apple OSX
- CA ACF2
- CA Top Secret
- Cisco, Security Agent (CSA)
- EMC VMWare ESX vSphere
- IBM, AIX
- IBM RACF
- Microsoft Windows
- IBM AS/400 iSeries (OS 400)

- Open source Linux
- Open BSD Linux
- Redhat Linux
- Sun Solaris
- HP Tandem
- HP/UX

## Intrusion Detection

- Cisco CSA
- Cisco IDS
- Enterasys IDS (also known as Dragon)
- Fortinet Fortigate FortiGuard
- Juniper ISG
- Network Associates McAfee Enterscept
- Nixsun NetVCR
- SNORT
- SourceFire Intrusion Sensor
- Trust Wave IPAngel

## Intrusion Prevention

- Bit9 Parity
- Cisco, IPS
- FireEye
- ForeScout CounterACT
- IBM Site Protector & Proventia
- Juniper NetScreen IDP
- McAfee Intrushield
- Nortel Threat Protection System
- Sourcefire Defense Center (syslog and eStreamer)
- Radware Defense Pro
- Symantec Endpoint Protection
- Tipping Point X Series
- Top Layer IPS 5500
- Trust Wave IPAngel

## Management Platforms

- Enterasys EMS (also known as Dragon)
- Enterasys NMS Automated Security Manager (ASM)
- Fair Warning
- IBM Domino (Notes)
- IBM Websphere
- ISS Site Protector
- Juniper Infranet Controller
- Juniper Netscreen Security Manager
- McAfee e-Policy Orchestrator
- McAfee Change Control (Solidcore)
- Microsoft MOM 2005
- Microsoft SCOM 2007
- Oracle BEA WebLogic
- SAP ERP
- Starent Networks Home Agent
- Tripwire Enterprise/Manager

## Routers/Switches

- 3Com, 8800 Series Switch
- Cisco CatOS
- Cisco Catalyst Switches
- Cisco NSEL
- Cisco Routers
- Enterasys Matrix Router
- Extreme Extremeware
- F5 ASM
- F5 BIG IP
- HP Procurve
- Juniper Router
- Nortel BayRS NAS, Secure Router

## Point of Sale/Measurement

- ITron OpenWay
- Radiant PSeries

## Security Appliance & UTM

- Astaro Security Gateway
- Fortinet
- Juniper AUM
- Juniper DPI
- Juniper MX
- Juniper DX Platform
- Juniper Integrated Security Gateway
- Juniper Secure Services Gateway
- Juniper SRC
- Juniper SRX Gateway
- Secure Computing SideWinder G2
- SonicWall UTM
- Sophos PureMessage
- Tipping Point X Series and SMS
- Vericept Content 360
- Websense Security

## VPN

- Array Networks, ArraySP SSL VPN
- Check Point VPN-1
- Cisco ASA
- Cisco VPN 3000 Series Concentrator
- Cisco VPN 3000 Concentrator
- Juniper RA/SA Series SSL VPN
- Juniper RA/SA SSL VPN
- Nokia IP Series
- Nortel VPN Gateway VPN Router
- Secure Computing Cyberguard

## Wireless Management

- Motorola Symbol Access Point
- Aruba Wireless Management Controller
- Cisco Aironet
- Enterasys Wireless

## Web Server, Proxies, Mail, Other

- Apache, HTTP Server
- BlueCoat SG
- Cisco Ironport
- CryptoCard CryptoShield
- F5 Load Balancer
- Microsoft DHCP
- Microsoft Exchange
- Microsoft IIS
- Microsoft ISA
- ProFTP FTP
- Squid Web Cache
- Starent Networks Home Agent
- Sun Sendmail

## Vulnerability Scanners

- eEye REM
- McAfee Foundstone Foundscan
- Juniper NSM Profiler
- nCircle IP360
- Nessus
- NMap
- Patchlink (Lumension/Harris) Scan
- Qualys
- Rapid7 NeXpose
- Saint
- SecureScout

## Network and Application Flow Data

- Q1 Labs, QFlow w/Layer 7 application identification
- Cisco NetFlow NDE versions 1, 2, 5, 7 and 9
- Cisco NSEL Netflow v9
- Foundry S-Flow
- Juniper J-Flow
- Packeteer FDR - Flow Data Records

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

