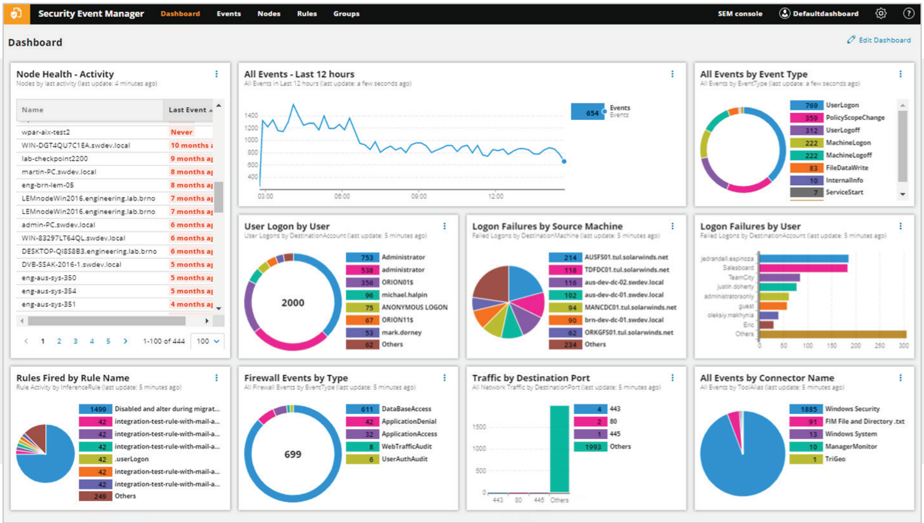
Security Event Manager


Security Event Manager
Dashboard
Events
Nodes
Rules
Groups
SEM console
Defaultdashboard
Dashboard
Edit Dashboard
All Events - Last 12 hours
All Events in Last 12 hours (last update: a few seconds ago)
1400
1200
1000
800
600
400
03:00
06:00
09:00
12:00
654 Events
All Events by Event Type
All Events by EventType (last update: a few seconds ago)
769 UserLogon
359 PolicyScopeChange
312 UserLogoff
222 MachineLogon
222 MachineLogoff
83 FileDataWrite
10 InternalInfo
7 ServiceStart
User Logon by User
User Logons by DestinationAccount (last update: 5 minutes ago)
2000
753 Administrator
538 administrator
356 ORION01$
96 michael.halpin
75 ANONYMOUS LOGON
67 ORION11$
53 mark.dorney
62 Others
Logon Failures by Source Machine
Failed Logons by DestinationMachine (last update: 5 minutes ago)
214 AUSFS01.tul.solarwinds.net
118 TDFDC01.tul.solarwinds.net
116 aus-dev-dc-02.swdev.local
102 aus-dev-dc-01.swdev.local
94 MANCDC01.tul.solarwinds.net
90 brn-dev-dc-01.swdev.local
62 ORKGFS01.tul.solarwinds.net
234 Others
Logon Failures by User
Failed Logons by DestinationAccount (last update: 5 minutes ago)
jedrandell.espinoza
Salesboard
TeamCity
justin.doherty
administratorsonly
guest
oleksiy.makhynia
Eric
Others
0
50
100
150
200
250
300
Rules Fired by Rule Name
Rule Activity by InferenceRule (last update: 5 minutes ago)
1499 Disabled and alter during migrat...
42 integration-test-rule-with-mail-a...
42 integration-test-rule-with-mail-a...
42 integration-test-rule-with-mail-a...
42 .userLogon
42 integration-test-rule-with-mail-a...
42 integration-test-rule-with-mail-a...
249 Others
Firewall Events by Type
All Firewall Events by EventType (last update: 5 minutes ago)
699
611 DataBaseAccess
42 ApplicationDenial
32 ApplicationAccess
8 WebTrafficAudit
6 UserAuthAudit
Traffic by Destination Port
All Network Traffic by DestinationPort (last update: 5 minutes ago)
1500
1000
500
0
443
80
445
Others
4 443
2 80
1 445
1993 Others
All Events by Connector Name
All Events by ToolAlias (last update: 5 minutes ago)
1885 Windows Security
91 FIM File and Directory .txt
13 Windows System
10 ManagerMonitor
1 TriGeo

Node Health - Activity

Nodes by last activity (last update: 4 minutes ago)

Name	Last Event
wpar-aix-test2	Never
WIN-DGT4QU7C1EA.swdev.local	10 months a
lab-checkpoint2200	9 months ag
martin-PC.swdev.local	8 months ag
eng-brn-lem-05	8 months ag
LEMnodeWin2016.engineering.lab.brno	7 months ag
LEMnodeWin2016.engineering.lab.brno	7 months ag
admin-PC.swdev.local	6 months ag
WIN-83297LT64QL.swdev.local	6 months ag
DESKTOP-QI8S8B3.engineering.lab.brno	6 months ag
DVB-SSAK-2016-1.swdev.local	5 months ag
eng-aus-sys-350	5 months ag
eng-aus-sys-354	5 months ag
eng-aus-sys-351	4 months ag

‹ 1 2 3 4 5 › 1-100 of 444 100

An all-in-one SIEM solution for log collection, storage, analysis, and reporting designed to help IT pros identify and respond to cyberthreats and demonstrate compliance.

Thousands of resource-constrained IT and security pros rely on SolarWinds® Security Event Manager (SEM) for affordable and efficient threat detection, automated incident analysis and response, and compliance reporting for their IT infrastructure. Our all-in-one SIEM combines log management, threat detection, normalization and correlation, forwarding, reporting, file integrity monitoring, user activity monitoring, USB detection and prevention, threat intelligence, and active response in a virtual appliance that's easy to deploy, manage, and use. We've designed our SIEM to provide the functionality you need without the complexity and cost of most other enterprise SIEM solutions.

SECURITY EVENT MANAGER AT A GLANCE

- Collects, consolidates, normalizes, and visualizes logs and events from firewalls, IDS/IPS devices and applications, switches, routers, servers, OS, and other applications
- Performs real-time correlation of machine data to identify threats and attack patterns
- Responds to suspicious activity automatically with Active Response, including blocking USB devices, killing malicious processes, logging off users, and more
- Eases compliance reporting and audits with out-of-the-box reports and filters for HIPAA, PCI DSS, SOX, ISO, DISA STIGs, FISMA, FERPA, NERC CIP, GLBA, and more
- Intuitive interface and ample selection of out-of-the-box content means you don't need to be a security or compliance expert to get value from our SIEM solution
- Affordable, scalable licensing based on log-emitting sources, not log volume

Easy Collection and Normalization of Network Device and Machine Logs

Security Event Manager comes with hundreds of out-of-the-box connectors to simplify the process of collecting, standardizing, and cataloging log and event data generated across your network. Our industry leading log compression rate allows more data to be stored with fewer resources required.

Customizable Visualizations and Dashboard

Quickly identify important or suspicious patterns in machine data with a wide variety of customizable visualizations and a flexible dashboard. Drill into interesting patterns with a click of a button and see the full list of related logs and their details.

Powerful and Simple Searching for Forensic Analysis and Troubleshooting

Security Event Manager is designed to allow users to quickly find important log data using simple keyword searches in both real-time event data as well as historical data at predefined or custom time periods. Out-of-the-box and user-defined filters also provide fast data refinement.

Real-Time, In-Memory Event Correlation

By processing and normalizing log data before it's written to the database, Security Event Manager can deliver true real-time log and event correlation. Predefined and custom correlation rules allow Security Event Manager to automatically alert on possible security breaches and other critical issues.

Out-of-the-Box Security and Compliance Reporting Templates

Security Event Manager makes it easy to generate and schedule compliance reports quickly using over 300 report templates and a console allowing for customizable reports to meet your organization's specific needs.

Threat Intelligence Feed and Groups

Correlation rules are enhanced with a fully-integrated, regularly updating threat intelligence feed that automatically identifies and tags malicious activity from known bad IPs. Easily build groups containing values relevant to your environment, such as user and computer names, sensitive file locations, and approved USB devices. These groups can be auto-populated via correlation rules and can help simplify searching and reporting.

Built-in Active Response

Security Event Manager can do much more than trigger email alerts. SEM is designed to immediately respond to security, operational, and policy-driven events using predefined responses, such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings.

Enhanced, Real-Time File Integrity Monitoring

Embedded File Integrity Monitoring (FIM) is designed to deliver broader compliance support and deeper security intelligence for insider threats, zero-day malware, and other advanced attacks. Leverage enhanced filter capabilities for finer tuning and significantly reduce the noise associated with lower priority file changes, increasing productivity and efficiency.

USB Detection and Prevention

Security Event Manager can help prevent endpoint data loss and protect sensitive data with real-time notifications when USB devices connect, the ability to automatically block their usage, and built-in reporting to audit USB usage.

Log Forwarding and Exporting

Security Event Manager forwards raw log data with syslog protocols (RFC3164 and RFC 5244) to other applications for further use. Additionally, users can export logs to a CSV file so the data can be shared with other teams and external vendors, uploaded to other tools, or attached to helpdesk tickets.

Analyze Historical Data

Pick up key trends by analyzing historical data via simplified network event searches. The intuitive query builder presents tips and suggestions as you enter query parameters, and then the event histogram and custom time picker allow you to zero in on specific results in a designated time span.

SECURITY EVENT MANAGER SYSTEMS REQUIREMENTS

To see all systems requirements and to determine deployment size, see SEM system requirements in the SEM Install or Upgrade Guide.

SECURITY EVENT MANAGER SYSTEMS REQUIREMENTS

Don’t just take our word for it. At SolarWinds, we believe you should try our software before you buy. That’s why we offer free trials that deliver full product functionality. Simply download Security Event Manager, and you can be up and analyzing your log files in less than an hour. It’s just that simple! Download your free, fully-functional trial today!

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of simple, powerful, and secure IT management software. Our solutions give organizations worldwide—regardless of type, size, or complexity—the power to accelerate business transformation in today's hybrid IT environments. We continuously engage with technology professionals— IT service and operations professionals, DevOps and SecOps professionals, and Database Administrators (DBAs) – to understand the challenges they face in maintaining high-performing and highly available IT infrastructures, applications, and environments. The insights we gain from them, in places like our THWACK community, allow us to address customers' needs now, and in the future. Our focus on the user and commitment to excellence in end-to-end hybrid IT management has established SolarWinds as a worldwide leader in solutions for observability, IT service management, application performance, and database management. Learn more today at www.solarwinds.com.

TRY IT FREE

30 days, full version

ABOUT LOOP1

Loop1 is a leading global IT Operations Management (ITOM) company specializing in the SolarWinds ITOM product offerings—we offer the most comprehensive training and professional services for SolarWinds clients across the globe. Headquartered in Austin, TX, United States, with offices in the United Kingdom, Ireland, Germany, Sri Lanka, and Singapore, the group has more than 100 employees across four continents, clients in more than 60 countries, and 25+ SolarWinds Certified Professional (SCP) engineers, holding 130+ individual certifications.

www.loop1.com | **info@loop1.com**

LOOP1 SOLARWINDS Elite Partner

A SOLARWINDS ELITE PARTNER

CONTACT US
US +1 (877) 591-1110
UK +44 (0)1285 647900
IRE +353 (0)21 601 7548

solarwinds

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.