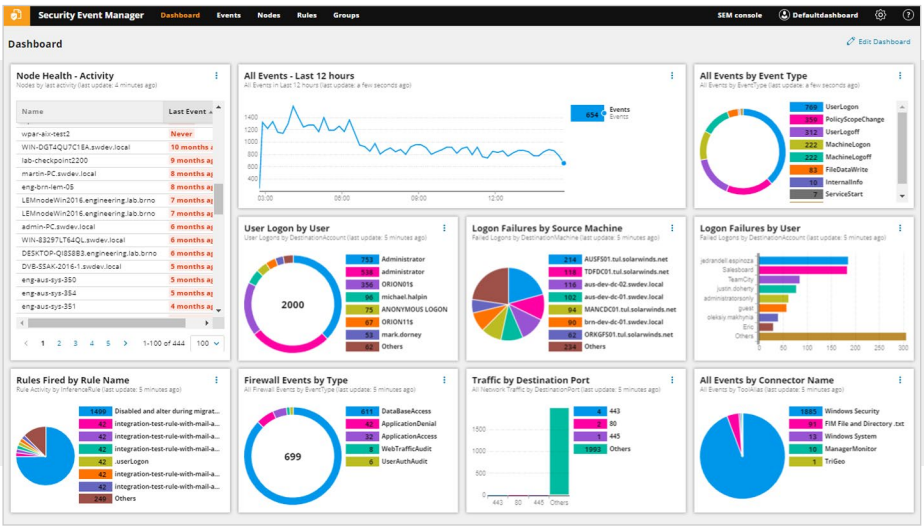
solarwinds

Security Event Manager

(ehemals Log & Event Manager)



Eine All-in-One-SIEM-Lösung für Protokollerfassung, Speicherung, Analyse und Berichterstellung, die darauf ausgelegt ist, IT-Experten bei der Identifizierung und Reaktion auf Cyberangriffe sowie beim Nachweis der Compliance zu unterstützen.

Tausende von IT- und Sicherheitsexperten mit eingeschränkten Ressourcen verwenden SolarWinds® Security Event Manager für die kostengünstige und effiziente Bedrohungserkennung, automatische Vorfallanalyse und -reaktion sowie Compliance-Berichte für die IT-Infrastruktur. Unsere All-In-One-SIEM-Lösung kombiniert Protokollverwaltung, Bedrohungserkennung, Normalisierung und Korrelation, Weiterleitung, Berichterstellung, Überwachung der Dateiintegrität und Benutzeraktivität, USB-Erkennung und -Gefahrenabwehr, Bedrohungsanalysen und Active-Response-Technologie in einer virtuellen Appliance, die einfach zu implementieren, zu verwalten und zu benutzen ist. Wir haben unsere SIEM-Lösungen so konzipiert, dass Sie alle Funktionen erhalten, die Sie benötigen – ohne die Komplexität und Kosten anderer SIEM-Unternehmenslösungen.

TESTVERSION DOWNLOADEN

30 Tage volle Funktionalität

SECURITY EVENT MANAGER IM ÜBERBLICK

- Erfasst, konsolidiert, normalisiert und visualisiert Protokolle und Ereignisse von Firewalls, IDS/IPS-Geräten und -Anwendungen, Switches, Routern, Servern, Betriebssystemen und anderen Anwendungen
- Korreliert Rechnerdaten in Echtzeit, um Bedrohungen und Angriffsmuster zu identifizieren
- Reagiert automatisch mit Active-Response-Aktionen auf verdächtige Aktivitäten, u. a. Blockieren von USB-Geräten, Beenden bösartiger Prozesse, Abmelden von Benutzern usw.
- Erleichtert Compliance-Berichte und -Prüfungen mit vorkonfigurierten Berichten und Filtern für HIPAA, PCI DSS, SOX, ISO, DISA STIGs, FISMA, FERPA, NERC CIP, GLBA usw.
- Eine intuitive Oberfläche und eine breite Auswahl vorgefertigter Inhalte sorgen dafür, dass Sie kein Sicherheits- oder Compliance-Experte sein müssen, um den vollen Nutzen aus unserer SIEM-Lösung zu ziehen
- Kostengünstige, skalierbare Lizenzierung auf Basis von protokollausgebenden Quellen, nicht Protokollvolumen

Einfache Erfassung und Normalisierung von Netzwerkgeräte- und Rechnerprotokollen

Security Event Manager bietet Hunderte vorgefertigter Konnektoren, um den Prozess der Erfassung, Standardisierung und Katalogisierung von Protokoll- und Ereignisdaten zu vereinfachen, die im gesamten Netzwerk generiert werden. Unsere branchenführende Protokollkompressionsrate ermöglicht es, mehr Daten mit weniger Ressourcen zu speichern.

TESTVERSION DOWNLOADEN

30 Tage volle Funktionalität

Anpassbare Visualisierungen und Dashboard

Mit einer Vielzahl von anpassbaren Visualisierungen und einem flexiblen Dashboard lassen sich wichtige oder verdächtige Muster in Maschinendaten schnell identifizieren. Mit nur einem Klick können Sie interessante Muster näher analysieren und eine umfassende Liste zugehöriger Protokolle und entsprechende Details anzeigen.

Leistungsfähige und einfache Suche für forensische Analyse und Fehlerbehebung

Security Event Manager ist so konzipiert, dass Benutzer wichtige Protokolldaten mithilfe einer einfachen Stichwortsuche sowohl in Echtzeit-Ereignisdaten als auch in historischen Daten zu vordefinierten oder benutzerdefinierten Zeiträumen schnell finden können. Vorgefertigte und benutzerdefinierte Filter ermöglichen außerdem eine schnelle Datenaufbereitung.

In-Memory-Korrelation von Ereignissen in Echtzeit

Dadurch, dass Protokolldaten verarbeitet und normalisiert werden, bevor sie in die Datenbank geschrieben werden, kann Security Event Manager eine Protokoll- und Ereigniskorrelation in Echtzeit bieten. Vordefinierte und benutzerdefinierte Korrelationsregeln erlauben Security Event Manager, bei möglichen Sicherheitsverstößen und anderen kritischen Problemen automatisch Warnungen zu senden.

Vorkonfigurierte Vorlagen für Sicherheits- und Compliance-Berichte

Mit über 300 Berichtsvorlagen und einer Konsole, mit der Sie anpassbare Berichte entsprechend den spezifischen Anforderungen Ihrer Organisation erstellen können, vereinfacht und beschleunigt Security Event Manager die Generierung und Planung von Compliance-Berichten.

Bedrohungsdaten-Feed und Gruppen

Die Korrelationsregeln werden durch einen vollständig integrierten, regelmäßig aktualisierten Bedrohungsdaten-Feed ergänzt, der böswillige Aktivitäten von bekannten gefährlichen IPs automatisch identifiziert und kennzeichnet. Erstellen Sie mühelos Gruppen mit Werten, die für Ihre Umgebung relevant sind, wie Benutzer- und Computernamen, sensible Dateispeicherorte und zugelassene USB-Geräte. Diese Gruppen können über Korrelationsregeln automatisch ausgefüllt werden und vereinfachen die Suche und die Berichterstellung.

Integrierte Active Response

Security Event Manager kann viel mehr als E-Mail-Warnungen auslösen. SEM ist darauf ausgelegt, sofort auf sicherheits-, betriebs- und richtlinienbezogene Ereignisse zu reagieren. Dabei kommen vordefinierte Reaktionen zum Einsatz, etwa infizierte Maschinen unter Quarantäne stellen, IP-Adressen sperren, Prozesse beenden und die Einstellungen von Active Directory® anpassen.

Erweiterte integrierte Echtzeit-Überwachung der Dateiintegrität

Die integrierte Dateiintegritätsüberwachung (FIM) soll eine breitere Compliance-Unterstützung und umfangreichere Sicherheitsinformationen über Insider-Bedrohungen, Zero-Day-Malware und andere erweiterte Angriffe bieten. Nutzen Sie verbesserte Filterfunktionen zur feineren Abstimmung und reduzieren Sie das Hintergrundrauschen an unwichtigen Informationen, das durch Änderungen an Dateien mit niedriger Priorität entsteht, um ein Vielfaches – so steigern Sie die Effizienz und Produktivität.

USB-Erkennung und -Gefahrenabwehr

Security Event Manager kann dazu beitragen, den Verlust von Endpunktdaten zu verhindern und vertrauliche Daten durch Echtzeitbenachrichtigungen bei Verbindungen zwischen USB-Geräten zu schützen. Dieses Tool kann diese Geräte automatisch sperren und integrierte Berichte zur Überprüfung der USB-Nutzung erstellen.

Protokollweiterleitung und -export

Security Event Manager leitet Rohprotokolldaten mit Syslog-Protokollen (RFC 3164 und RFC 5244) zur weiteren Verwendung an andere Anwendungen weiter. Darüber hinaus können Benutzer Protokolle in eine CSV-Datei exportieren, sodass die Daten mit anderen Teams und externen Anbietern ausgetauscht, in andere Tools hochgeladen oder an Helpdesk-Tickets angehängt werden können.

TESTVERSION DOWNLOADEN

30 Tage volle Funktionalität

VM-ANFORDERUNGEN VON SECURITY EVENT MANAGER

Alle Systemanforderungen und Informationen zur Bestimmung der Bereitstellungsgröße finden Sie in den SEM-Systemanforderungen im SEM Install or Upgrade Guide.

HARDWARE	KLEINES UNTERNEHMEN	MITTELSTÄNDISCHES UNTERNEHMEN	GROSSES UNTERNEHMEN
CPU	Prozessoren mit 2-4 Kernen bei 2,0 GHz	Prozessoren mit 2-4 Kernen bei 2,0 GHz	Prozessoren mit 2-4 Kernen bei 2,0 GHz
Arbeits-speicher	8 GB	16-48 GB RAM	48-256 GB RAM
Festplatte	250 GB, 15.000 U/Min (RAID 1/gespiegelte Einstellungen)	500 GB, 15.000 U/Min (RAID 1/gespiegelte Einstellungen)	1 TB, 15.000 U/Min (RAID 1/gespiegelte Einstellungen)
Ein- und Ausgabe-vorgänge pro Sekunde (IOPS)	40-200 IOPS	200-400 IOPS	400 oder mehr IOPS
NIC	NIC mit 1 GbE	NIC mit 1 GbE	NIC mit 1 GbE

SOFTWARE	MINDESTANFORDERUNGEN
BS/virtuell	VMware® vSphere ESX 5.5 oder ESXi 5.5 und höher Public Cloud-Option verfügbar für Amazon Web Services und Microsoft Azure
Umgebungen	Microsoft Hyper-V® Server 2016, 2012 R2 oder 2012
Datenbank	In die virtuelle Appliance integriert
Datenbank	In die virtuelle Appliance integriert

SIE KÖNNEN DAS PROGRAMM VOR DEM KAUF AUSPROBIEREN UND EINE KOSTENLOSE TESTVERSION DOWNLOADEN.

Überzeugen Sie sich selbst. Bei SolarWinds sind wir davon überzeugt, dass Sie unsere Software vor dem Kauf ausprobieren sollten. Daher bieten wir kostenlose Testversionen mit vollem Funktionsumfang an. Sie brauchen Security Event Manager nur herunterzuladen, und in weniger als einer Stunde ist alles für die Analyse Ihrer Protokolldateien bereit. Es ist wirklich so einfach! Laden Sie Ihre kostenlose Testversion mit vollem Funktionsumfang noch heute herunter!

TESTVERSION DOWNLOADEN

30 Tage volle Funktionalität

ÜBER SOLARWINDS

SolarWinds (NYSE:SWI) ist ein führender Hersteller leistungsstarker und erschwinglicher IT-Infrastrukturmanagement-Software. Unsere Produkte bieten Unternehmen jeder Art und Größe weltweit leistungsstarke Tools zum Überwachen und Verwalten der Leistung ihrer IT-Umgebungen, egal wie komplex ihre IT-Infrastruktur ist – ob lokal, in der Cloud oder in hybriden Modellen. Wir sind im ständigen Austausch mit Technikexperten aus den unterschiedlichsten Bereichen – Experten für IT-Betrieb, DevOps und Managed Service Provider (MSPs) – um herauszufinden, welchen Herausforderungen sie bei der Verwaltung leistungsfähiger, hochverfügbarer IT-Infrastrukturen gegenüberstehen. Mithilfe der Erkenntnisse aus diesem Austausch, beispielsweise in unserer Online-Community THWACK®, können wir Produkte für bekannte Herausforderungen im IT-Management entwickeln und die von Technikexperten gewünschten Lösungen bereitstellen. Dieser Schwerpunkt auf den Benutzer und unser Engagement für Spitzenleistungen in der End-to-End-Leistungsverwaltung in der hybriden IT haben SolarWinds zu einem weltweit führenden Anbieter von Netzwerkverwaltungssoftware und MSP-Lösungen gemacht. Weitere Informationen finden Sie unter www.solarwinds.com/de.

WEITERE INFORMATIONEN

NORD- UND SÜDAMERIKA
Telefon: +1 866 530 8100
Fax: +1 512 682 9301
E-Mail: sales@solarwinds.com

ASIEN:
Telefon: +65 6422 4123
Fax: +65 6593 7601
E-Mail:apacsales@solarwinds.com

EMEA
Telefon: +353 21 5002900
Fax: +353 212 380 232
E-Mail: emeasales@solarwinds.com

PAZIFIKRAUM
Telefon: +61 2 8412 4910
E-Mail: apacsales@solarwinds.com

Produktinformationen zu SolarWinds-Produkten finden Sie auf solarwinds.com oder per Telefon oder E-Mail.
7171 Southwest Parkway | Building 400 | Austin, Texas 78735, USA

Für weitere Informationen wenden Sie sich bitte an SolarWinds: Tel. +1 866.530.8100, E-Mail sales@solarwinds.com. Besuchen Sie http://www.solarwinds.com/partners/reseller_locator.aspx, um Händler in Ihrer Nähe zu finden.

© 2019 SolarWinds Worldwide, LLC. Alle Rechte vorbehalten.

Die Marken SolarWinds, SolarWinds & Design, Orion und THWACK stehen im alleinigen Eigentum der SolarWinds Worldwide, LLC oder ihrer verbundenen Unternehmen, sind im U.S. Patent and Trademark Office eingetragen und können in anderen Ländern eingetragen oder angemeldet sein. Alle sonstigen Marken, Dienstleistungsmarken und Logos von SolarWinds können Marken nach nicht kodifiziertem Recht, eingetragen oder angemeldet sein. Alle sonstigen hier erwähnten Marken dienen lediglich zu Identifikationszwecken und sind Marken oder eingetragene Marken der jeweiligen Unternehmen.

Dieses Dokument darf nicht ohne schriftliche Zustimmung von SolarWinds in irgendwelcher Weise reproduziert oder (weder ganz noch teilweise) modifiziert, dekompiliert, disassembliert, veröffentlicht oder verteilt oder anderweitig auf einen elektronischen Datenträger übertragen werden. Alle Rechte und Ansprüche hinsichtlich der Software, Dienste und Dokumentation sind und bleiben das alleinige Eigentum von SolarWinds, seinen verbundenen Unternehmen und/oder dessen Lizenzgebern.

SOLARWINDS LEHNT ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, VORBEHALTE BZW. SONSTIGEN BEDINGUNGEN, VERTRAGLICH GEREGELTE ODER GESETZLICH VORGESCHRIEBENE, HINSICHTLICH DER DOKUMENTATION AB, EINSCHLIESSLICH AUSSCHLUSS DER RECHTSVERLETZUNG, KORREKTHEIT, VOLLSTÄNDIGKEIT ODER NÜTZLICHKEIT DER HIERIN ENTHALTENEN INFORMATIONEN. IN KEINEM FALL SIND SOLARWINDS ODER LIEFERANTEN ODER LIZENZGEBER VON SOLARWINDS FÜR SCHÄDEN HAFTBAR, DIE UNRECHTMÄSSIG, VERTRAGSMÄSSIG ODER AUS EINER ANDEREN RECHTSTHEORIE HERVORGEHEN, SELBST WENN SOLARWINDS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.