DATENBLATT

WATCHGUARD SIEMFEEDER

Überwachung, Erkennung und Meldung von Sicherheitsereignissen im Netzwerk

Sicherheitsinformations- und Ereignismanagement: Überblick

System-Information-and-Event-Management(SIEM)-Lösungen sind mittlerweile unverzichtbar, um die Sicherheit der Mehrheit moderner Unternehmensinfrastrukturen zu gewährleisten. Dank Funktionen zum Erfassen und Korrelieren des Status von IT-Systemen können Unternehmen die zunehmende Menge von Ereignissen zu hilfreichen Informationen für die Entscheidungsfindung nutzen.

Die Integration einer neuen Quelle für wichtige Informationen in Ihren Sicherheitsinformationen kann bei der Bewältigung vieler Herausforderungen bei der Cybersicherheit hilfreich sein und Sicherheitsexperten mehr Zeit verschaffen, um moderne Cyberangriffe innerhalb umfangreicher protokollierter Ereignisse, komplexer Bedrohungen und komplexer Infrastrukturen zu erkennen und abzuwehren.

Umfassende Visualisierung von Sicherheitsereignissen in Ihrer SIEM-Konsole

Als Sicherheitsexperte benötigen Sie umfassende Einblicke in die Prozesse, die auf den Workstations und Servern ausgeführt werden. WatchGuard SIEMFeeder zentralisiert die Ereignisse, die Ihr SIEM-Tool von allen Endpoints empfängt, und hilft Ihnen so, Sicherheitsvorfälle zu überwachen und die Probleme vorherzusehen, die von hoch entwickelten Bedrohungen in Ihren Unternehmensnetzwerken verursacht werden.

Größte Herausforderungen von Sicherheitsadministratoren:

- Antizipation potenzieller Sicherheitsprobleme durch Ermittlung ausgeführter Programme, die noch nicht als Goodware oder Malware eingestuft wurden, und Feststellung, wie diese auf die Computer gelangt sind.
- Visualisierung von IOA (Indicators of Attack) und Erkennung von verdächtigen Aktivitäten, wie zum Beispiel Änderungen der Windows-Registrierung oder Treiberinstallationen.
- Monitoring der Ausführung rechtmäßiger Software, die sich Angreifer in Netzwerken oft unbemerkt zunutze machen, wie zum Beispiel Scripting- oder Fernzugriffs-Tools.
- Betriebliche Effizienz von IT-Infrastrukturen:
    1. **Monitoring der ein- und ausgehenden Kommunikation zur Vermeidung unerwünschter Verbindungen**
    2. **Verringerung des Bandbreitenverbrauchs**
    3. **Gestaltung von Richtlinien zur Vermeidung des Downloads großer Mengen an unproduktiven Inhalten**
- Erkennung von Daten-Exfiltrationsvorfällen, wobei ermittelt wird, welche Prozesse und Anwender auf Dateien mit sensiblen Daten zugreifen.

Vorteile:

- ✓ **Umfassende Visualisierung aller auf den Geräten ausgeführten Prozesse**

  Überwachung und Management der Sicherheit. Kontinuierliche Erkennung von Anomalien in der Ausführungsumgebung der einzelnen Kunden.

- ✓ **Zentrale Konfiguration**

  Gleichzeitige Konfiguration der Einstellungen von WatchGuard SIEMFeeder für alle Ihre Endpoints über die zentrale Management-Konsole (WatchGuard Cloud).

- ✓ **Leicht zu installieren, sicher und einfach skalierbar**

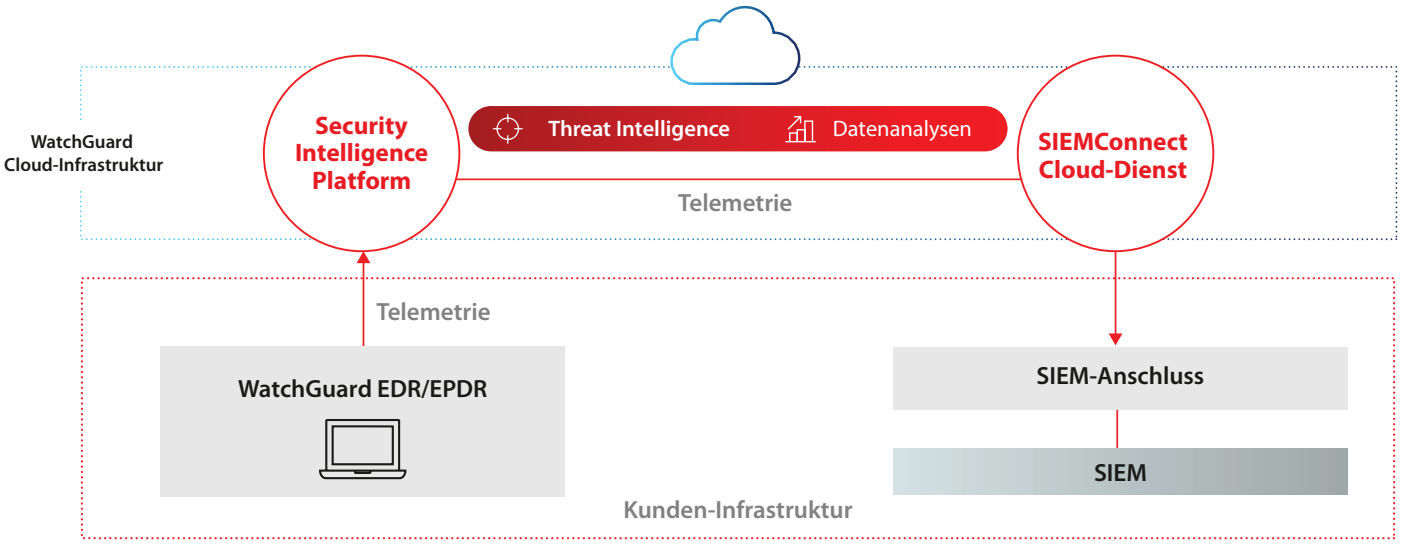
  Einmalige Konfiguration des Telemetrie-Downloaddienstes und Hinzufügen neuer Endpoints, ohne zusätzliche Komponenten bereitstellen oder installieren zu müssen. Sichere Downloads über sichere TLS-Verbindungen (Transport Layer Security) aus der WatchGuard Cloud.

- ✓ **Geringere SIEM-Speicherkosten**

  Filtern Sie erforderliche Ereignisse, bevor diese Ihre Infrastruktur erreichen, und minimieren Sie so die Speicherkosten.

- ✓ **Kompatibel mit den meisten SIEM-Lösungen auf dem Markt**

  Laden Sie Telemetrie im Common Event Format (CEF) oder Log Event Extended Format (LEEF) herunter. Diese nativen Formate von ArcSight sind mit den führenden SIEM-Lösungen auf dem Markt wie QRadar, AlienVault, Splunk, Devo usw. kompatibel.



Kompatibel mit:

ALIEN VAULT · ArcSight An HP Company · Radar · splunk> · elasticsearch · DEVO

Wichtige Funktionen:

- Zentrale Verwaltung von Endpoints über WatchGuard Cloud
- Einfach zu installieren und zu konfigurieren
- Ereignisfilterung vor der Integration in das SIEM-Tool
- Konfigurierbares Format: LEEF oder CEF
- Sicheres Herunterladen von Ereignissen über TLS-Verbindungen

Systemanforderungen und unterstützte Plattformen von WatchGuard SIEMFeeder

Siehe https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/installation/install-requirements.html

Dieses Modul ist erhältlich mit:
WatchGuard EPDR | WatchGuard EDR

DAS WATCHGUARD-PORTFOLIO

Network Security

Multifaktor-Authentifizierung

Sicheres, cloudverwaltetes WLAN

Endpoint-Sicherheit

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.