SIEM Feeder

Integration in Unternehmens-SIEM-Systeme, um Zugang zu Details und Kontext von allen Programmen zu erhalten, die in Ihrem IT-Netzwerk ausgeführt werden

panda
a WatchGuard brand

EINE NEUE INFORMATIONSQUELLE: ANWENDERPROGRAMME

SIEM-Lösungen (System Information and Event Management) sind notwendig geworden, um die Sicherheit sowohl großer als auch mittlerer IT-Infrastrukturen zu verwalten. Die Funktion zur Erfassung und Korrelation des Status von IT-Systemen ermöglicht es Organisationen, aus großen Datenmengen nützliche Informationen für Entscheidungen für Entscheidungen für Entscheidungen zu ziehen.

Integrieren Sie eine neue, wichtige Datenquelle in die Sicherheitsinformationen, die vom SIEM erfasst und korreliert werden: Alle Prozesse und Programme werden auf Ihren Geräten ausgeführt und durchgehend von Panda Adaptive Defense überwacht.

EIN NEUER SICHERHEITSSTATUS

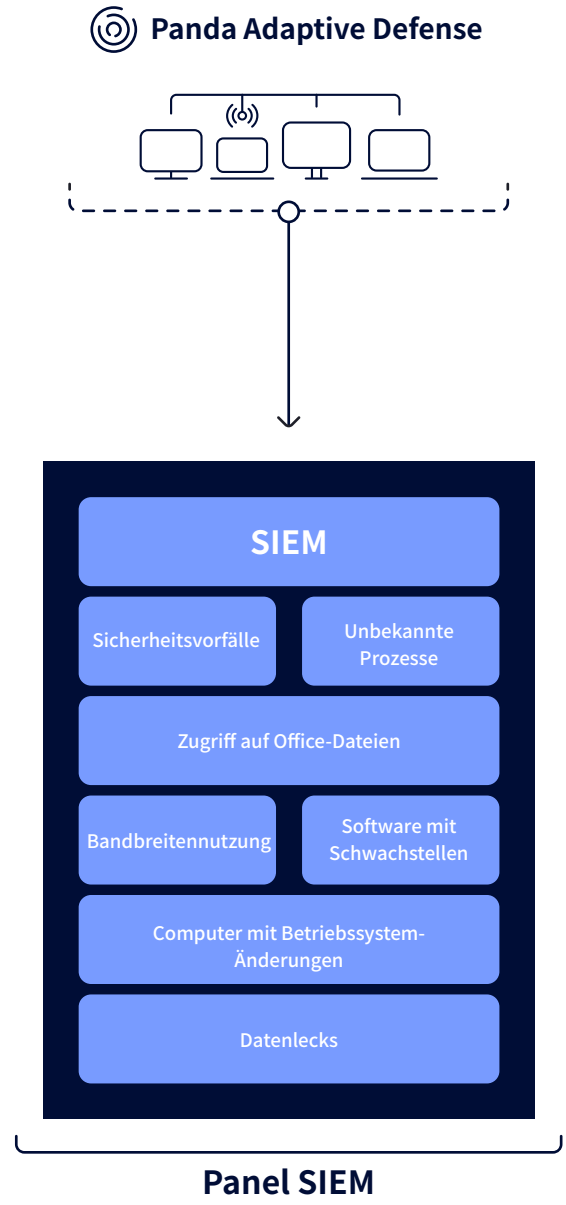
IT-Abteilungen benötigen ein hohes Maß an Transparenz und Steuerbarkeit, um die Sicherheitsprobleme, die Malware der nächsten Generation verursacht, rechtzeitig erkennen zu können.

Panda Adaptive Defense unterstützt Administratoren dabei, die großen Datenvolumen zu filtern, die SIEM-Systeme verarbeiten und sich auf das Wesentliche zu konzentrieren:

- Welche neuen Programme werden ausgeführt und wurden noch nicht als Goodware oder Malware eingestuft?
- Wie sind diese Programme in das Netzwerk gekommen?
- Welche verdächtigen Aktivitäten führen sie auf Anwendergeräten durch (Registry-Bearbeitung, Hooks, Treiberinstallation usw.)?
- Welche legitime Software mit bekannten und ausnutzbaren Schwachstellen wird verwendet?
- Welche Prozesse greifen auf Anwenderdokumente zu und senden Informationen?
- Wie ist die Netzwerkauslastung jedes Prozesses, der im IT-Netzwerk läuft?

NAHTLOSE INTEGRATION UND BETRIEB

Panda Adaptive Defense lässt sich nahtlos in bestehende Unternehmens-SIEM-Lösungen integrieren, ohne dass zusätzliche Bereitstellungen auf den Geräten der Benutzer erforderlich sind. Überwachte Ereignisse werden sicher, entweder direkt oder indirekt über Plug-Ins, über das LEEF/CEF-Format gesendet, das mit den meisten SIEM-Systemen auf dem Markt kompatibel ist. SIEM Feeder ermöglicht native Integration der Telemetrie in eine DEVO-Plattforminstanz in kürzester Zeit, ohne eigenes Integrationsprojekt (SIEM Feeder to Devo).



Unterstützte Plattformen und Systemanforderungen von SIEM Feeder

http://go.pandasecurity.com/siem-feeder/requirements

Dieses Modul ist verfügbar als Teil von:

Panda Adaptive Defense **Panda Adaptive Defense 360**

Kompatibel mit:

ALIEN VAULT · ArcSight An HP Company · Radar · bracora · lookwise · Kompatibel mit LEEF- und CEF-Format

WatchGuard

VERTRIEB DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.com | pandasecurity.com