pallas
...SEDM

Security Event Detection Management

- Automatisch Anomalien erkennen
- Sicherheitsvorfälle detailliert analysieren
- Sicherheitsrelevante Korrelationen über lange Zeiträume herstellen und reporten
- Konfigurationsfehler in der Perimeter Sicherheit aufdecken

SEDM dient zur Analyse von Firewall-Logs sowie von NetFlow-Daten in denen automatisch Anomalien erkannt werden. Eine Anomalie ist eine Abweichung vom bisherigen Verhalten. Das bisherige Verhalten wird auf Basis von historischen Daten im Zeitrahmen von 15 bis 90 Tagen, je nach Erkennungsmodul, ermittelt.

Datenbasis für SEDM sind Firewall-Log-Daten die in einem ElasticSearch System gespeichert werden. Damit stehen diese Daten für SEDM zur Verfügung und – falls eine Anomalie entdeckt wird – ebenfalls für den Administrator zur dynamischen Auswertung mittels ELA (Enhanced Log Analysis).

SEDM liefert nicht die Ursache für die Anomalie, aber Anhaltspunkte. SEDM ist nicht invasiv, stört also den normalen Betrieb nicht, und hilft dennoch dem Administrator seltsames Verhalten zu erkennen und damit auch dieses seltsame Verhalten abzustellen.

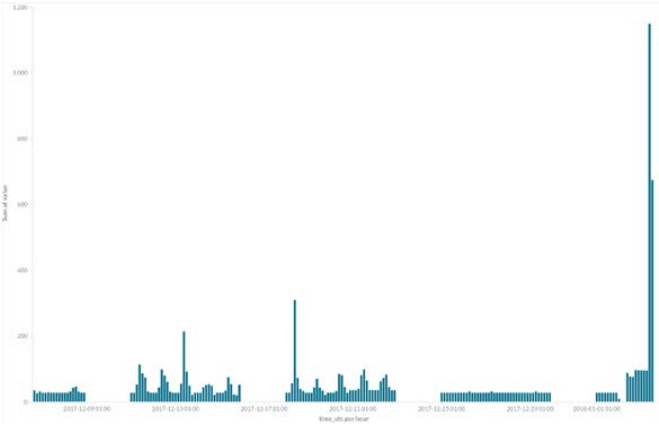
Auch wenn SEDM primär zur Erkennung von Angriffen, insbesondere durch Firewalls sonst schwer einzudämmenden APTs, entwickelt wurde, ist durch die Erkennung von Anomalien durch Konfigurationsfehler tatsächlich ein sehr schneller und wesentlicher Mehrwert auch ohne aktive Angriffe gegeben.

Gerade im Bereich Industrie 4.0, die durch gleichmäßigen, regelmäßigen und wenig sprunghaften Netzwerktraffic geprägt ist, ist SEDM ein hervorragendes Produkt um Befall der schlecht zu wartenden Industrieanlagen zu erkennen. Da SEDM allein auf Basis von Firewall-Logs arbeitet, kann der Einsatz von SEDM im laufenden Betrieb ohne Störung der Produktion erfolgen.

Ein Beispiel:

Information for high number of dropped connections

Eine nähere Analyse zeigte auf, dass bei dieser Anomalie die Firewall ein Software-Update verhindert hatte. Die Lösung war die benötigte Freischaltung auf der Firewall damit die gewollten Updates auch tatsächlich ausgeliefert werden konnten.



Pallas GmbH

Hermülheimer Str. 8a • 50321 Brühl

www.pallas.de • information@pallas.de

Tel: 02232-1896-0 • Fax: 02232-1896-29