



pallas
...ELA

Enhanced Log Analysis

- /// Unternehmenskritische Anomalien erkennen
- /// Schnell und zuverlässig auskunftsfähig zu Sicherheitsvorfällen
- /// Sicherheitsrelevante Korrelationen über lange Zeiträume herstellen und reporten
- /// Standortübergreifend Anomalien erkennen



ELA ist eine webbasierte, interaktive Plattform für den IT-Administrator, der detailliert seine Firewall-Logdaten analysieren möchte.

Zur Nutzung von ELA wird die Managed Firewall so konfiguriert, dass die Logdaten in Echtzeit in das ELA-System gesendet werden. Eingehende Logdaten werden indiziert, nach Kunden separiert gespeichert und für die Analyse bis max. 90 Tage im System vorgehalten.

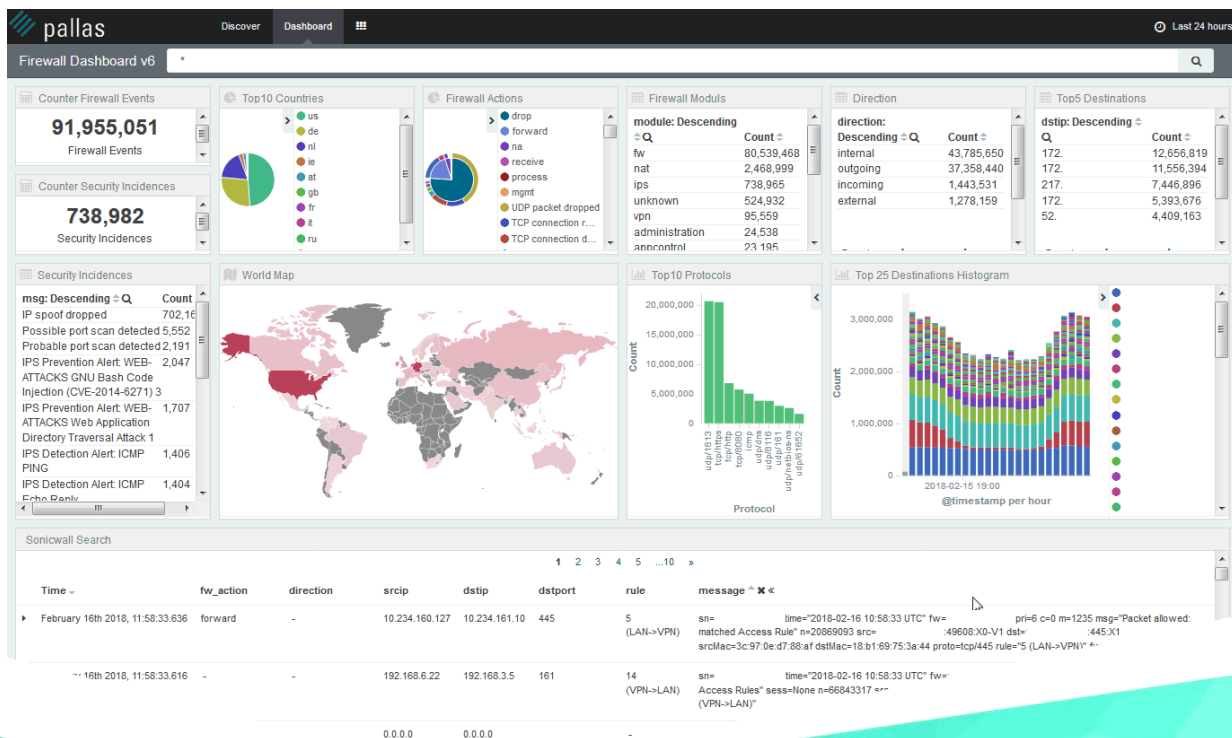
Durch das Zusammenführen von Logs mehrerer Firewalls in ein zentrales System sind Auffälligkeiten und Unterschiede mehrere Standorte einfach ermittelbar.

Muss ein Security Incident untersucht werden, so ist durch die flexible Auswertung der Logs eine schnelle Analyse möglich. Stößt der Kunden-Administrator bei der Auswertung an seine Grenzen, so können Security Spezialisten von Pallas aushelfen.

ELA basiert auf dem quelloffenen und leistungsfähigen Elasticsearch und Kibana, betrieben durch Pallas in Pallas Datacenter in Deutschland.

Jede Störung muss schnellstmöglich erkannt und behoben werden. Die in Firewall Systemen eingebauten Log-Auswertungen sind diesbzgl. häufig limitiert und unterstützen den Firewall Administrator nur unzureichend.

Pallas hat einen einfach zu bedienenden Managed Service entwickelt der das Sicherheitsniveau stark erhöht.



Pallas GmbH

Hermülheimer Str. 8a • 50321 Brühl

www.pallas.de • information@pallas.de

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