PKA®
Secure Networking Company

SIAM – Theltos Server für effektiven Angriffsschutz

Seit über 30 Jahren entwickeln, beraten, lehren und forschen im Bereich Netzwerk und IT Sicherheit. Unsere Service ist das einsammeln und auswerten von Log-Dateien. Hieraus leiten wir mögliche Angriffs-Szenarien ab, erkennen potentielle Angriffsversuche, verhindern diese und verbessern gleichzeitig Schutz-Maßnahmen für zukünftige Attacken.

SIAM: Theltos Server

Theltos gehört zur neuesten SIEM Generation, dem **SIAM: Security Information Automatic (Analyse) Management.**
Während bestehende SIEM Lösung manuell bedient werden müssen, arbeitet SIAM - Theltos vollautomatisiert. Theltos Log-Server liefert zuverlässig 24x7 Daten, welche mittels unseres patentierten „pre-crime" Verfahrens automatisiert analysiert werden und nachhaltig Angriffe verhindern.

Log Analysen:
Theltos sammelt alle Log-Files aus Ihrem Netzwerk, unabhängig davon, ob es sich um Client´s, Server, IOT oder Netzwerkgeräte handelt.

Diese Logs werden in einer Datenbank auf einem hierfür vorgesehenen Rechner in Ihrem RZ gespeichert. Die Erstinstallation wird seitens PKA vorgenommen. Die Verarbeitung und Löschung dieser Logs erfolgt zertifiziert nach den DSVGO Regeln. Theltos Architektur unterstützt eine oder mehrere Server in einer hierarchischen Struktur.

Delta Analysen:
Kern der Analyse ist die einfache automatisierte Analyse, die abnormales Verhalten für Sie bewertet, weiter verfeinert und mit Ihren historischen Daten bearbeitet. So erhalten Sie nur *„Informationen"* über auffälliges Verhalten in Ihrem Netzwerk, *„Warnungen"* über außer gewöhnliches Verhalten oder *„Emergency"* bei definierten Einbrüchen.

- ⇨ Eine sofortige Reaktion hierauf ist ebenfalls individuell automatisiert

Beispiel: Wenn Sie sich immer von zu Hause oder Ihrem Arbeitsplatz aus zwischen 08:00 und 10:00 Uhr anmelden ist das in der Datenbank als „normales" Verhalten gespeichert. Sollten Sie sich nun zu einer ganz anderen Zeit von einem ganz anderen Ort aus anmelden, können wir das erkennen und handeln. Dazu messen wir die durchschnittliche Anzahl der Fehlversuche und bewerten diese im Zusammenhang.

- ⇨ Möglichkeit z.B. Prozess starten und Account deaktivieren

Mustererkennung / Vorhersage:
Ein Muster sind mehrere Fehlversuche und / oder Ausnahmen aus der *Delta Analyse* die korreliert werden und kundenspezifisch bewertet werden. Vordefinierte Muster sind als Vorlage der PKA Datenbank zu entnehmen und zu individualisieren.

Beispiel: Fünf fehlerhafte Login-Versuche pro Minute auf dem DSL Port seit Messbeginn. Das ist zunächst keine Ausnahme, sondern wird zu Anfang als normales Verhalten bewertet.
Sobald die Login-Versuche aufhören, kann daraus ein abnormales Verhalten erkannt werden. Hinzu kommt beispielsweise zeitversetzt mehrere protokollierte Fehlversuche beim Dateizugriff und ebenfalls zeitversetzt eine größere Datenmenge als übliche, welche per DSL Post versendet

werden. Die Korrelation der drei Ereignisse entspricht dem Muster der Einbruchserkennung. In diesem Beispiel liegt somit ein erfolgreicher, juristisch nachweisbarer Einbruch vor.

Theltos ermöglicht diese Ereignisse als Muster zu hinterlegen und versetzt Unternehmen in die Lage, Vorhersagen zu erkennen und ähnliche Musterangriffe abzuwehren.

⇨ Dank Theltos können Sie zukünftig frühzeitig Angriffsversuche wie z.B. Ransomsoftware erkennen und vorzeitig handeln.

Der Theltos-Server:
Vorhersagen – Erkennen – Angriffsabwehr durch automatisierte Prozesse

- Einsammeln aller Log-Files
- Bearbeitung nach der DSVGO
- Delta Analysen zum Auffinden von „Abnormalitäten"
- Mustererkennung – Vorhersage bei Einbruchsversuchen
- Aggregation und Korrelationen innerhalb der Analysen
- Datenvisualisierung
- Statistiken
- Übersichtliche Aufbereitungen aller Ergebnisse
- Zentrales Fehlermanagement
- Individuelle, automatisierte, fehlerfreie Einbruchsanalyse
- Intuitive Bedienbarkeit

PKA bietet:

- Erstinstallation inkl. Konfiguration zum Festpreis
- Einweisung und Schulung
- Messwerterfassung über einen Zeitraum von circa 6 Monate
- keine Nachbereitung nötig
- Notfallschutzkonzepte und Unterstützung bei Erpressungsversuchen
- Angriffs-Nachbehandlung
- Unterstützung von *„multi Theltos-Server*" in verteilten Umgebungen
- Support, Beratung, Eskalationsmanagement, Blog und Schulungen
- Nutzen Sie unsere jährliche *„Security information Conference*" SiC (Termine auf www.pka.de)

Die SIAM Theltos Lösung ist bereits ab € 600,- pro Monat erhältlich.

Sie können den Theltos-Server gerne testen, bei Interesse sprechen Sie und gerne an.

Kontaktdaten:
PKA Peter Kämper
Gedererstraße 12, 83233 Bernau a. Chiemsee
Telefon +49-8051-6404888
Mobil +49-173-5372217
per Mail: info@pka.de