Splunk Enterprise & Controlware CESAR App

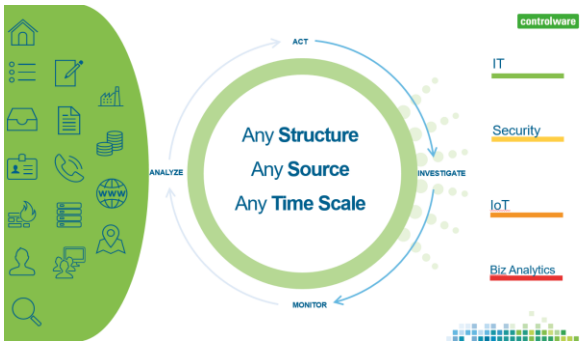
Effektives Monitoring Ihrer Firewall, AD, Proxy und Mail

Daten sind in der Regel in Unternehmen die Grundlage für businessrelevante Entscheidungen. Doch die größte Datensammlung nützt wenig, wenn die Parameter nicht in Relation gestellt und sinnvoll miteinander verknüpft werden. Was früher große Analysten-Teams leisteten, wird heute durch IT-Unterstützung effizienter und intelligenter gestaltet.

Controlware unterstützt Unternehmen seit 2014 mit Splunk Lösungen von der Beratung, Konzeption bis hin zur Realisierung. Unsere zertifizierten Experten erarbeiten gemeinsam mit Ihnen individuelle Konzepte, die eine optimale Nutzung Ihrer Daten ermöglichen und somit aktiv zum Geschäftserfolg beitragen.

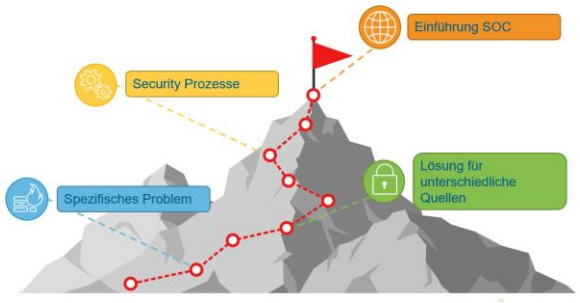
Was ist Splunk?

Die Operational Intelligence Plattform Splunk Enterprise ermöglicht Monitoring und Analyse von Maschinendaten und Kundentransaktionen bis hin zu Sicherheitsereignissen und Netzwerkaktivitäten. Durch die vollständige Palette an leistungsfähigen Suchen, Visualisierungen und vordefinierten Inhalten für Anwendungsfälle aus den Bereichen IT-Operations, IT-Security, IoT und Business Analytics können Sie schnell Erkenntnisse aus Ihren Daten gewinnen und diese nutzen – Unabhängig von Datenstruktur, Datenquellen und Zeitraum.



Übersicht Datenintegration vom Medium bis zum Use-Case

Der Weg zum erfolgreichen SOC ist steinig aber lohnenswert!



Der Weg zum funktionierenden Security Operations Center

Bis zur Einführung eines Security Operations Centers (SOC) müssen schrittweise! diverse Etappen abgeschlossen werden. Zu Beginn stehen securityspezifische Herausforderungen die es zu bewältigen gilt. Deshalb sollten anfänglich die Security-Problematiken identifiziert werden, um den tatsächlichen Sicherheitsbedarf zu ermitteln. Auf dem weiteren Weg zum Ziel ist es außerdem wichtig alle Quellen für die Datenerzeugung integrieren zu können. Nur durch den Einbezug aller Datenquellen wird es möglich Security Prozesse (u.a. Security Incident Handling) umfassend und effektiv aufzubauen und zu nutzen.

Controlware CESAR App

Die Controlware CESAR App ist eine IT-Security-Reporting-App und hilft Ihrem Personal in SOCs bei Ihrer täglichen Arbeit.

Das CESAR-Framework hat die Antworten auf die typischen Abfragen von SOCs. Dazu ist die App flexibel und nach Rücksprache mit unseren Analytics-Experten, speziell auf Ihre Bedürfnisse anpassbar (u.a. Rechte und Rollenkonzepte sowie Custom Use-Cases).

Übersicht des zentralen CESAR-Dashboards nach der Installation

CESAR Funktionen

Entscheidender Vorteil für den Einsatz der Controlware CESAR-App ist die Möglichkeit zeitnah, ohne den Einsatz wertvoller Personalressourcen, Erkenntnisse aus ihren vorliegenden Daten ziehen zu können.

Direkt nach der Installation sind folgende Funktionen standardmäßig verfügbar:

Welche Use-Cases sind standardmäßig enthalten?

Active Directory / Windows Server

- Fast Group Change
- Chained RDP Connection

Firewall

- IOC-Abgleich
- Success vs. Failed Connections

Proxy

- C2 Verbindungserkennung
- High Volume Uploads

Mail

- Datenabfluss Erkennung
- IOC Abgleich

Was kostet die Installation der CESAR-App?

Aktueller Aufwand für die Installation der CESAR App

5 Dienstleistungstage

Hinweise zur Controlware CESAR-App:

Die App wird kontinuierlich weiterentwickelt und nach Rücksprache mit unseren Experten bei Ihnen aktualisiert.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf: