splunk>

CASE STUDY

MBDA Deutschland treibt Security Intelligence mit Splunk Enterprise Security voran

Kurzfassung

Die MBDA Deutschland ist das führende deutsche Systemhaus für Lenkflugkörper und Luftverteidigung. Als Teil des europäischen MBDA-Konzerns, einem Global Player auf dem Gebiet der Lenkflugkörpersysteme, konzentriert sich die MBDA Deutschland an den Standorten Schrobenhausen, Ulm und Aschau am Inn. MBDA Deutschland benötigte eine Lösung, mit der Hackerangriffe effektiver identifiziert und untersucht werden können. Seitdem das Unternehmen Splunk Enterprise und Splunk Enterprise Security (ES) einsetzt, profitiert MBDA Deutschland von folgenden Vorteilen:

- Weniger Zeit für die Untersuchung von Sicherheitsvorfällen notwendig
- Angriffe können besser identifiziert und klassifiziert werden
- Sicherheitslage hat sich insgesamt verbessert

Warum Splunk?

Das Unternehmen entwickelt, produziert und wartet Luftverteidigungs- und Lenkflugkörpersysteme für Luftwaffe, Heer und Marine. Als Hersteller von Lenkflugkörpern ist MBDA Deutschland oft Ziel von Advanced Threats. Das Unternehmen muss diese Angriffe identifizieren können, untersuchen woher sie kommen und entsprechend reagieren, um die Auswirkungen abzuschwächen. MBDA Deutschland benötigte Einblick in sicherheitsrelevante Daten im gesamten Unternehmen und wählte hierfür eine Lösung aus dem „Leader Quadrant“ im Gartner Magic Quadrant for Security Intelligence and Event Management (SIEM). Splunk Enterprise und Splunk ES hoben sich aufgrund folgender Faktoren von anderen Lösungen ab: nutzerfreundliche Oberfläche, Out-of-the-Box-Inhalte und schnell zu realisierender Mehrwert. Deshalb passte die Lösung vor allem für das kleine IT-Team bei MBDA Deutschland besonders gut, da das Security-Operations-Center (SOC) sehr effizient damit arbeiten kann.

Das übergeordnete Ziel bei der Nutzung von Splunk Enterprise und Splunk ES ist es, Sicherheitsbedrohungen und Angriffe schnell zu identifizieren und zu untersuchen. MBDA Deutschland analysiert Daten von über 20 Systemfamilien mit Splunk-Software. Darunter das gesamte Netzwerk mit etwa 2.500 Endpunkten, 350 Servern, Switches, Gateways, AAA-Servern und WAN-Verbindungen nach Frankreich, Italien und Großbritannien.

Branche

- Produktion

Splunk Use Cases

- Security

Herausforderungen

- Fehlender Überblick über die gesamte Infrastruktur
- Unentdeckte Sicherheitsbedrohungen im Netzwerk

Business Impact

- Zeitspanne für die Untersuchung von Sicherheitsvorfällen deutlich reduziert.
- Alerts identifizieren Angriffe in Echtzeit, die zuvor unentdeckt geblieben sind.
- Analysen historischer Daten fließen in künftige Sicherheitsmaßnahmen ein. Das Ergebnis: Sicherheitslage im Unternehmen ist insgesamt belastbarer.

Datenquellen

- Netzwerk-Logs
- Logs von Endpunkten
- Server-Logs
- Daten von Switches
- Daten von Gateways
- Authentifizierungs-Logs

Splunk Produkte

- Splunk Enterprise
- Splunk Enterprise Security (ES)

Zeitaufwand für die Untersuchung von Sicherheitsvorfällen auf ein Zwanzigstel reduziert

Der größte Durchbruch für MBDA Deutschland ist die Reduzierung der Zeitspanne, die das SOC-Team benötigt, um Indicators-of-Compromise-Hinweise verschiedener Computer Emergency Response Teams (CERT) auszuwerten. Seitdem das Unternehmen ES nutzt, wurde der durchschnittlich benötigte Zeitaufwand für die Analyse eines CERT-Hinweises von 372 Minuten auf 15 Minuten reduziert.

Echtzeit-Analysen ermöglichen Identifikation von zuvor unentdeckten Angriffen

Seitdem MBDA Deutschland die Splunk-Plattform als Security-Intelligence-Lösung einsetzt, konnte die Firma zudem eine größere Anzahl an Attacken aufdecken. Viele davon wären zuvor unbemerkt geblieben. Zu diesem Zweck hat das SOC-Team Alerts für eine Anzahl von kritischen Ereignissen festgelegt: Beispielsweise, wenn Maschinen mit Malware infiziert sind und nach außen kommunizieren oder falls böswillige Außenstehende über präparierte Webseiten versuchen, in das Netzwerk der MBDA Deutschland einzudringen. Als Ergebnis hat MBDA Deutschland potentiell schädliche Aktivitäten identifizieren können, bevor sie negative Auswirkungen hatten.

Analyse historischer Daten bietet Informationen für künftige Sicherheitsvorkehrungen

Es ist wichtig für MBDA Deutschland zu verstehen, woher eine Attacke kam, wie sie aussah und welche Auswirkungen sie hatte, um angemessen reagieren zu können. Splunk Enterprise und Splunk ES ermöglichen dem Unternehmen die einzelnen Stufen eines Angriffs im Detail nachzuvollziehen und vorhandene Lücken zu erkennen. Auf diese Weise kann die Firma den Vorfall schnell einschätzen, gegebenenfalls eskalieren, dokumentieren und kommunizieren.

"Splunk reduziert Sicherheitsrisiken bei MBDA Deutschland deutlich. Die Software hilft uns dabei, effektiver zu arbeiten, einen Überblick über unser gesamtes Netzwerk zu gewinnen und schneller auf Sicherheitsereignisse zu reagieren. Auch für unsere künftige Sicherheitsstrategie können wir die Erkenntnisse aus unseren Datenanalysen nutzen."

Patrick Schwarz
Head of IT und Project Manager
Information Technology
MBDA Deutschland

Zudem nutzt MBDA Deutschland die Einblicke aus vergangenen Vorfällen dazu, Maßnahmen gegen künftige Angriffe zu entwickeln. Das Ergebnis ist eine bessere Transparenz der Sicherheitslage, eine kürzere Reaktionszeit auf Vorfälle, eine verbesserte Nachweisbarkeit und demzufolge belastbare Aussagen zu Sicherheitsvorfällen.

splunk> SplunkCe@Splunk.com www.splunk.com

CS-Splunk-MBDA-A4-102