iT-CUBE SYSTEMS

Referenz: Splunk für MBDA Deutschland

MBDA Deutschland – auch in der Cyberabwehr optimal ausgerüstet

MBDA Deutschland ist führend im Bereich der Entwicklung und Produktion von Luftverteidigungs- und Lenkflugkörpern für Luftwaffe, Heer und Marine. Das Unternehmen ist Teil der europäischen MBDA Gruppe, ein weltweit führender Konzern im Bereich von Lenkflugkörpersystemen. Das Unternehmen hat seine Standorte in Schrobenhausen, Aschau am Inn und Ulm. Der Wunsch von MBDA Deutschland war eine IT-Sicherheitslösung, welche eine umfassende Transparenz des Unternehmensnetzwerkes gewährleistet und so das Identifizieren und Analysieren von IT-Sicherheitsbedrohungen effektiver macht.

Ausgangssituation

Als wehrtechnisches Unternehmen ist MBDA Deutschland oft komplexen Cyberattacken ausgesetzt. Deswegen war es umso wichtiger, dass die gewünschte Sicherheitslösung das Identifizieren, Nachverfolgen und Auswerten solcher Attacken ermöglicht. Um dies zu gewährleisten, benötigte MBDA Deutschland Transparenz aller sicherheitsrelevanten Daten im Unternehmen und eine optimale Lösung im Bereich Security Information & Event Management (SIEM).

Die Herausforderung an die Sicherheitslösung bestand darin, die fehlende Sichtbarkeit im Unternehmensnetzwerk zu beseitigen und bisher unbemerkte Sicherheitsrisiken zu erkennen. Die Zeit, die zur Erkennung und Analyse der Security Incidents benötigt wurde, sollte drastisch reduziert werden. Darüber hinaus war die Verbesserung von Identifizierung und Klassifizierung der Cyberattacken notwendig. Die allgemeine Lage der IT-Sicherheit sollte durch diese Maßnahmen enorm gestärkt werden.

Key Facts !

Branche:
Rüstungsindustrie

MBDA MISSILE SYSTEMS

Leistung:
Durchführung eines Konzeptworkshops und Implementierung von Splunk Enterprise und der Splunk ES App.

» Die iT-CUBE hat mit ihrer Expertise und Erfahrung maßgeblich zum Projekterfolg beigetragen, unsere zukünftige Sicherheitsstrategie auszubauen. Die Zusammenarbeit war außerordentlich gut.«

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

Lösung

Um diese Ziele zu erreichen, wurde eine Sicherheitslösung aus dem „Leader"-Bereich des Gartner Magic Quadrant for Security Information and Event Management gewählt. Splunk Enterprise und Splunk Enterprise Security (ES) konnten sich bei dieser Entscheidung gegen die Konkurrenz durchsetzen. Die Sicherheitslösungen von Splunk überzeugten unter anderem durch eine benutzerfreundliche Oberfläche, out-of-the-box-Inhalten und einem schnellen Mehrwert bereits nach kurzer Zeit. Nach der Evaluierung verschiedener Anbieter zur Implementierung der Sicherheitslösung fiel die Wahl auf iT-CUBE SYSTEMS. Unsere Experten waren bereits bei der Planung und Konzeption der Implementierung von Splunk Enterprise und Splunk ES mit eingespannt. In einem Konzeptworkshop wurden unter anderem verschiedene Use Cases entwickelt und das Sizing der Splunk-Lösung festgelegt. Im Anschluss übernahmen unsere Consultants die Implementierung der beiden Security-Intelligence-Lösungen und setzten die geplanten Use Cases um.

Warum iT-CUBE?

Dank der langjährigen Erfahrung in bereits mehr als 60 SIEM-Projekten war auch diese Anbindung von Splunk in die Unternehmensinfrastruktur kein Problem für die Experten der iT-CUBE. Durch dieses Know-How und den Überblick über verschiedenste SIEM-Lösungen konnten unsere Consultants fundierte Vorschläge einbringen und von sich überzeugen. Die Entscheider bei MBDA Deutschland fühlten sich sofort in ihrer Problemstellung verstanden und setzen seit Beginn großes Vertrauen in unsere Experten. Auch unsere bisherige Zusammenarbeit mit anderen Unternehmen des Konzerns konnte die Entscheider bei MBDA Deutschland überzeugen.

Das Ziel der Implementierung von Splunk war, Sicherheitsrisiken und -attacken schnell erkennen und identifizieren zu können. MBDA Deutschland kann nun Daten aus dem gesamten Netzwerk, inklusive den ca. 2.500 zugehörigen Endpoints, 350 Servern, Switches, Gateways, AAA Servern und WAN-Verbindungen nach Frankreich, Italien und Großbritannien analysieren. Den größten Durchbruch schaffte MBDA Deutschland bei der Minimierung der Zeit, die das SOC (Security Operations Center)-Team benötigte, um IOCs (Indicators of Compromise) von verschiedenen CERTs (Computer Emergency Response Teams) zu verfolgen. Durch Splunk ES konnte die Zeit, die benötigt wurde, eine CERT-Nachricht zu analysieren von 372 Minuten auf 15 Minuten reduziert werden. Mit der Security-Intelligence-Lösung kann MBDA Deutschland nun kritische Events wie das Infizieren einer Maschine oder die Kommunikation von Malware nach außen schnell erkennen und Sicherheitsvorfälle abwenden, bevor sie Schaden anrichten können. Für den Kunden ist es wichtig zu erkennen, woher der Angriff kam und welche Auswirkungen er hatte, um effektiv darauf reagieren zu können. Splunk Enterprise und Splunk ES erlauben es, die einzelnen Schritte des Angriffs detailliert nachzuvollziehen und Schwachstellen zu erkennen. MBDA Deutschland kann nun die Daten aus vergangenen Attacken nutzen, um sich zukünftig vor ähnlichen Attacken zu schützen.

Unsere Partner !

splunk>

iT-CUBE SYSTEMS AG

Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de

Unsere Experten sind für Sie da, wir helfen Ihnen gern weiter. Kontaktieren Sie uns jederzeit, unverbindlich!