Orange
Cyberdefense

Kundenreferenz

Automatisiertes Logmanagement für Compliance und Security, Datalake, SIEM, Analytics

Auf einen Blick

Kunde:
Josef Witt GmbH

Branche:
Handel

Firmensitz:
Weiden i.d.OPf, Deutschland

Leistungen:
SIEM (Exabeam)

Witt-Gruppe
Member of the otto group

Das Unternehmen

Für die beste Zeit des Lebens – seit 1907

Die Witt-Gruppe ist einer der führenden europäischen Mode-Versandhändler auf dem wachsenden Zukunftsmarkt “50 plus”. Mit mehr als 110 Jahren Erfahrung kennt das Unternehmen seine Zielgruppe wie kaum ein anderer. Rund 3.700 Mitarbeitende bringen ihr Know-how ein, um mehr als 21,6 Millionen Kund*innen die beste Zeit ihres Lebens zu ermöglichen. Die Witt-Gruppe ist mit elf Marken in zehn Ländern sowie mit 23 Online-Shops aktiv. Seit 1987 ist der Omnichannel-Einzelhändler aus Weiden in der Oberpfalz ein Teil der Otto Group.

Ausgangssituation

Basierend auf einer Vorgabe der Otto Group müssen alle Unternehmen Zugriffe auf personenbezogene Daten monitoren und auditieren. Missbrauch und Verstöße müssen alarmiert werden.

Die Lösung sollte möglichst viel Automatisierungspotenzial mitbringen und „ease of use“ sollte im Vordergrund stehen. Idealerweise sollte maschinelles Lernen einen hohen Grad des Konfigurationsaufwandes abnehmen. Die Witt-Gruppe hatte kein zentrales Logmanagement und es war sehr schwer nachzuvollziehen wer wann auf personenbezogene Daten zugegriffen hat. Partielle Speicherung von Loginformationen machte es unmöglich Investigationen eines Gesamtbildes durchzuführen. Der manuelle Aufwand war enorm und lückenhaft.

Das sagt der Kunde:

» Mit Exabeam haben wir alle unsere Systeme security-seitig im zentralen Überblick. Ein selbst-lernendes System, welches im SOC essenziell ist. «

Daniel Beaudet // Head of IT Network and Security // Witt-Gruppe

Eingesetzte Hardware

- Exabeam Datalake Appliances EX3000 im Cluster Verbund
- Exabeam Advanced Analytics Appliance EX4000

Eingesetzte Software

- Exabeam Datalake + Advanced Analytics Lizenzen

Lösung

Mit Exabeam SIEM + Advanced Analytics konnten folgende Anforderungen erfüllt werden:

Zentrales Log Management
Alle Loginformationen werden nun zentral in einem Data Lake gespeichert und können für Reporting, Auditierung und Forensik genutzt werden.

Advanced Analytics
Mittels maschinellem Lernen kann sich die Lösung automatisch auf das Netzwerkgeschehen der Witt-Gruppe einstellen. Sie erkennt nach einer Lernphase Abweichungen in der Kommunikation der Endgeräte, Server, etc., oder auch in ungewöhnlichem Verhalten von Nutzern z.B. beim Zugriff auf personenbezogen Daten.

Detektion & Alarmierung
Das System bietet Detektion & Alarmierung von modellbasierten Anomalien beim Überschreiten eines Risiko-Scores und hilft den SOC-Mitarbeitenden sich auf das Wesentliche zu fokussieren. Diese Technologie ermöglicht das Aufdecken von „unknown unknowns“ – also unbekannte Bedrohungen z.B. durch maliziöse Insider oder kompromittierte Insider.
Das System bietet Alarmierung von faktbasierten Verstößen, sogenannte „ known unknowns“. Hierfür wird ein statisches Regelwerk hinterlegt, um eine Alarmierung für einen bekannten Bedrohungsfall zu einem unbekannten Zeitpunkt zu ermöglichen.

Reporting, Compliance, Auditierung
Die Lösung bietet die Möglichkeit vorgefertigte Compliance Reports oder auch kundespezifische Reports zu erstellen und zu exportieren.
Die Logs werden entsprechend der internen Policy für einen bestimmten Zeitpunkt gespeichert und stehen für Investigationen und Audits mehrere Monate zur Verfügung.

Vorteile

Die Vorgabe des Mutterkonzerns (Otto Group) wurde mit der eingesetzten Lösung erfüllt. Außerdem werden alle Logs und Security Alerts zentral gespeichert. Somit müssen die Securitymitarbeiter nicht versuchen die Puzzleteile mit manuellen, aufwendigen Prozessen zusammenzuführen, sondern bekommen ein Gesamtbild in der Plattform präsentiert.
Der hohe Grad an Automatismus ermöglicht deutlich bessere Visibilität, höhere Detektion und viel weniger manuellen Aufwand bei Investigationen.
Eine Effizienzsteigerung der Arbeit im Security Team ist die Folge und eine erhöhte Security Maturität im Unternehmen.

Über Orange Cyberdefense

Orange Cyberdefense ist eine Geschäftseinheit der Orange Group, welche sich der Cybersecurity widmet. Als führender Anbieter für Cybersecurity ist unser Bestreben eine sichere digitale Gesellschaft aufzubauen. Wir bieten unseren Kunden Consulting, Solutions und Managed Security Services. Speziell mit unseren Managed Detection & Response und Threat Intelligence Services helfen wir unseren Kunden Bedrohungen zu erkennen, Risiken zu identifizieren und auf Vorfälle angemessen zu reagieren. Mit über 2.100 Mitarbeitern in weltweit 19 Ländern sind wir stets dort, wo unsere Kunden uns brauchen. Erfahren Sie mehr auf unserer Website.

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00