splunk> a CISCO company

CASE STUDY

Johnson Matthey bekämpft mit Splunk Phishing-Attacken und führt Untersuchungen 83 % schneller durch

Zentrale Herausforderungen

Vor der Implementierung von Splunk wurde das Security-Team von Johnson Matthey von der Vielzahl an Warnmeldungen geradezu überrollt – ohne jedwede Möglichkeit, die kritischsten Meldungen effektiv zu filtern und zu priorisieren.

Wichtige Ergebnisse

Dank Splunk Enterprise Security, Splunk SOAR und Splunk Attack Analyzer erhält Johnson Matthey heute verlässlichere Warnmeldungen, agiert bei der Phishing-Erkennung präziser und konnte so sein allgemeines Sicherheitsniveau deutlich steigern.

Johnson Matthey
Inspiring science, enhancing life

Branche: Industrie und Fertigung

Lösungen: Security

Produkt: Splunk Enterprise Security, Splunk SOAR, Splunk Attack Analyzer

Nachhaltigkeit geht uns alle an

Johnson Matthey mit Sitz in London ist ein weltweit führender Anbieter nachhaltiger Technologien, dessen Geschichte bis ins frühe 19. Jahrhundert zurückreicht. Zahlreiche führende Akteure aus der Energie- und Chemieindustrie sowie der Automobilbranche setzen auf die Technologie und das Know-how des Unternehmens, um treibhausgasarme Prozesse umzusetzen, ihren Schadstoffausstoß zu reduzieren und nachhaltiger zu werden.

Aufgrund seiner starken Ausrichtung auf Forschung und Innovation in diversen Sektoren unterhält Johnson Matthey neben IT-Funktionsbereichen auch OT-Strukturen für seine Betriebstechnik. Umso wichtiger ist daher das Thema Cybersicherheit – denn Datenpannen könnten nicht nur den Betrieb lahmlegen, sondern auch die Sicherheit der Mitarbeitenden gefährden.

Ergebnisse

- 30 % höhere Genauigkeit der Warnmeldungen
- 83 % weniger Zeitaufwand für das Ticket-Management
- automatisierte Bearbeitung von 61 % aller Phishing-Fälle mit SOAR

Das Security Operations Center (SOC) des Unternehmens sah sich mit einer enormen Zahl an Warnmeldungen konfrontiert – ohne dabei Zugriff auf den Kontext oder die Technologie zu haben, die Aufschluss darüber geben würden, welche Meldungen legitim und besonders kritisch sind. Was Johnson Matthey brauchte, war eine Lösung, die den nötigen Kontext lieferte, um Warnmeldungen effektiver auf den Grund zu gehen und das Unternehmen und damit auch sein wichtigstes Ziel abzusichern: den Kampf gegen den Klimawandel.

Klarer Fokus ohne störendes Rauschen

Vor dem Einsatz von Splunk stellte die überwältigende Menge an Sicherheitswarnungen zunehmend eine Herausforderung für das Security-Team von Johnson Matthey dar. Mangels Kontext ließen sich die Meldungen nicht effektiv priorisieren. Daraus die 15–20 % auszumachen, die sofortiger Aufmerksamkeit bedurften, war so nur schwer möglich. Vielmehr glich die Erkennung der tatsächlichen Bedrohungen der sprichwörtlichen Suche nach der Nadel im Heuhaufen.

Entlastung brachte schließlich Splunk Enterprise Security, in dessen Rahmen das Team Risk-Based Alerting (RBA) implementierte. Aus mehreren Warnmeldungen werden damit solche mit mehr Aussagekraft zusammengefasst, die das Team dann gezielt angehen kann. Hierzu erfasst RBA eine Vielzahl separater Security-Warnungen und ordnet die Informationen einer einzelnen Meldung zu einem Asset oder einer Identität zu, die sofortiger Aufmerksamkeit bedarf. So werden sämtliche eingehenden Daten analysiert und für das Threat Hunting nutzbar, jedoch wird das SOC-Team nicht von Tausenden irrelevanten Warnungen überrollt – ein Ansatz, der nicht nur die betriebliche Effizienz, sondern auch das Sicherheitsniveau insgesamt verbessert. Dank dieser mit Daten angereicherten Warnmeldungen konnte Johnson Matthey 40–50 % mehr Use Cases umsetzen und zugleich die Zahl der Meldungen wie auch die Falsch-Positiv-Rate reduzieren.

„Mit Risk-Based Alerting ermöglicht es uns Splunk Enterprise Security, präzise zu justieren, was das System ausgeben soll. Sämtliche Daten werden dabei auch weiterhin zur Analyse erfasst, allerdings ohne dass unser SOC-Team mit irrelevanten Warnungen bombardiert wird“, kommentiert Nathan Lowey, Cybersecurity Engineer bei Johnson Matthey.

„Teamwork makes the dream work“

Infolge von Datensilos und uneinheitlichen Reporting-Prozessen kam es in der Vergangenheit mitunter vor, dass mehrere Analysten dieselbe Warnmeldung unabhängig voneinander bearbeiteten und dabei nicht im Austausch miteinander standen. Entsprechend unterschiedlich waren die Herangehensweisen der einzelnen Analysten, da es an einem gemeinsamen Standard fehlte. Und obendrein gingen 90 % der Warnmeldungen auf nur 20 % der fallspezifischen Use Cases zurück. Effizienter und standardisiert ließ sich der Prozess durch Splunk SOAR gestalten, mit dessen Hilfe Johnson Matthey Playbooks einsetzte, nach deren Vorgabe die Arbeit der Analysten besser organisiert und einheitlicheres Reporting gewährleistet werden konnte. Neben der Etablierung einheitlicher Prozesse trug dies auch zu mehr Datengenauigkeit für eine proaktive Optimierung bei.

In der Vergangenheit galt es für Analysten, zur Erfassung einer Bedrohungen manuell ein Ticket zu erstellen und auch relevante Details von Hand einzugeben. Mit Splunk SOAR können sie repetitive Aufgaben wie diese nun automatisieren und erhalten dabei zusätzliche Kontextdetails für Warnmeldungen. Dadurch sparen sie bei der Untersuchung der zugehörigen Tickets enorm viel Zeit ein: Wo es früher noch 30 Minuten waren, sind es heute im Schnitt gerade einmal fünf. „Splunk SOAR vereinfacht die Kommunikation erheblich“, so Lowey. „Wenn einer unserer Analysten ein Ticket an das OT-Team weiterleiten muss, extrahiert er die nötigen Details einfach per Mausklick und weist es ihm im IT-Service-Management zu. Alles bleibt in einem System und ist somit optimal geschützt.“

> Mit der Hilfe von Splunk SOAR und Splunk Attack Analyzer konnten wir Teile unseres Phishing-Prozesses automatisieren. Dadurch müssen unsere Analysten weniger Tickets bearbeiten, da automatisch die Tickets geschlossen werden, die keine echte Bedrohung darstellen. Anhand weiterer Verbesserungen stellen wir dabei sicher, dass das, worauf sie ihren Blick richten, so funktioniert wie vorgesehen. Ohne dass wir eingreifen müssen, werden so aktuell 61 % der Phishing-Bedrohungen analysiert und bearbeitet.”
>
> **Nathan Lowey,** Cybersecurity Engineer, Johnson Matthey

Absicherung gegen alte und neue Risiken gleichermaßen

Angreifer führen immer neue und raffiniertere Cyberbedrohungen ins Feld. Daher gilt es, ihnen einen Schritt voraus zu sein. So auch, als die Teams von Johnson Matthey mit einer neuen Form von Phishing-Angriffen namens „Quishing“ konfrontiert waren. Zum Einsatz kommen dabei QR-Codes, die Standardsysteme zur Bedrohungserkennung nicht von regulären Bildern unterscheiden können. So entschied man sich, Splunk Attack Analyzer zu implementieren.

Mit beachtlichen Ergebnissen: Das gesamte System zur Phishing-Erkennung operiert nun erheblich präziser und produziert deutlich weniger Fehlalarme. Denn in der Vergangenheit hatte es beispielsweise jede E-Mail, deren Betreff die Wörter „dringend“, „Zahlung“ oder „Ankündigung für Bericht“ enthielt, als verdächtig gekennzeichnet. Durch den Einsatz von Splunk Attack Analyzer ließ sich die Genauigkeit der Phishing-Erkennung von 50 % auf 80 % erhöhen. So werden dank der Lösung 61 % der Phishing-Versuche automatisch als Fehlalarm identifiziert und das zugehörige Ticket wird geschlossen, ohne dass ein Analyst eingreifen muss. Wird dagegen eine schädliche URL erkannt, fügt die Lösung sie automatisch dem Cloud-Proxy hinzu.

Dank Splunk Enterprise Security, Splunk SOAR und Splunk Attack Analyzer konnte Johnson Matthey seine Datensicherheitsstrategie einfacher und zielführender gestalten, seine Prozesse optimieren und die Entscheidungsfindung verbessern. So kommunizieren die vormals in Silos isolierten Cybersecurity-Teams nun nahtlos miteinander und arbeiten koordiniert zusammen, um die Sicherheit des Unternehmens zu gewährleisten..

24_CMP_cust_Johnson-Matthey-626458_de-DE