Case Study

Schutz bei IT-Sicherheitsvorfällen

Mit Managed SOC Services für mehr Sicherheit.

Über Hochland SE

Die Hochland SE ist ein führendes europäisches Unternehmen in der Milchverarbeitungsbranche. Gegründet im Jahr 1927 in Deutschland, hat sich Hochland zu einem international agierenden Unternehmen entwickelt, das eine breite Palette von Käseprodukten herstellt und vertreibt. Das Unternehmen ist bekannt für seine hochwertigen Käsesorten, darunter Frischkäse, Schnittkäse, Hartkäse und Schmelzkäse.

Hochland hat seinen Sitz in Heimenkirch, Deutschland, und betreibt Produktionsstätten und Vertriebszentren in verschiedenen Ländern weltweit. Das Unternehmen legt großen Wert auf Qualität, Innovation und Nachhaltigkeit in allen Aspekten seiner Geschäftstätigkeit, angefangen von der Beschaffung hochwertiger Milch von lokalen Bauern bis hin zur Entwicklung neuer Käseprodukte, die den sich ständig ändernden Verbraucherbedürfnissen gerecht werden.

Durch kontinuierliche Investitionen in Forschung und Entwicklung sowie durch Partnerschaften mit Einzelhändlern und Gastronomiebetrieben ist Hochland in der Lage, seine Präsenz auf dem globalen Markt zu stärken und gleichzeitig die Bedürfnisse seiner Kunden zu erfüllen. Mit einem starken Fokus auf Kundenzufriedenheit, Qualität und soziale Verantwortung ist Hochland bestrebt, ein vertrauenswürdiger Partner für Käseliebhaber auf der ganzen Welt zu sein.

Zielsetzung

- Unterstützung der Kommunikation und Dokumentation des Datenverkehrs durch ein SIEM
- Automatisiertes Reporting
- Compliance, operatives Geschäft und IT-Sicherheit gewährleisten

Facts

- Molkereiprodukte
- > 6.000 Assets
- > 6.000 Mitarbeitende

Herausforderung: Security und Event Monitoring

Durch die wachsenden Compliance-Anforderungen und die immer weiter steigende Anzahl an Cyberangriffen hatte der CISO der Hochland SE erkannt, dass ein externes Security Monitoring plus Incident Response eine passende Lösung sei.

Daraus ergab sich die Aufgabenstellung, die Kommunikation und Dokumentation des Datenverkehrs durch ein „Security Information and Event Management System" (SIEM) zu unterstützen. Dieses sollte systembezogenen Berichte (Logs) automatisch qualifizieren, korrelieren und melden können. Eine Meldung kann eine Aufnahme oder Alarmierung als Sicherheitsvorfall bedeuten sowie in regelmäßigen Abständen als Report abgerufen oder versendet werden. Das SIEM unterstützt damit den Betrieb aus drei Perspektiven: Compliance, operatives Geschäft und IT-Sicherheit.

Unsere Lösung

In der vorbereitenden Onboarding-Phase begann die Abstimmung und Planung der Kommunikationswege und Installation der **Managed SOC-Lösung**. Im Anschluss erfolgte die Durchführung und Anbindung der Log-Quellen und im weiteren Verlauf wurden die Serviceelemente optimiert. In der letzten Phase wurde der Service weiter ausgebaut und spezifische Use-Cases entwickelt.

Der Managed SOC-Service analysiert und korreliert die Logdateien der Hochland SE und reichert Incidents mit externen Sicherheitsinformationen, wie Indicators of Compromise (IOCs), an und alarmiert die SOC-Analysten im Service Operations Center bei Anomalien und potenziellen Bedrohungen. Die SOC-Expert:innen der Axians können somit jeden Alarm weiterführend qualifizieren und entsprechende Handlungsempfehlungen einleiten.

Kernkomponente des Services ist die Überwachung des Kundennetzwerkes auf potentielle IT Sicherheitsvorfälle. Bei einem sicherheitsrelevanten Ereignis erfolgt eine Alarmierung und Unterstützung des Kunden-Teams, indem konkrete Handlungsempfehlungen zum Vorfall durch SOC-Analysten der Axians gegeben werden.

Hochland SE nutzt folgende Leistungsbestandteile:

01 Incident Response

02 Incident Monitoring

03 KPI Reporting

04 Threat Intelligence

05 Threat Modeling & Use Case

Eingesetzte Lösungen

- **Managed SOC**
- **Security Information and Event Management System (SIEM)**
- **Incident Response Retainer**

Innerhalb dieser Services sind folgende Aktivitäten vorgesehen:

- Analyse von Eventdaten zur Identifizierung von maliziösen Aktivitäten, die nicht automatisch von den vorhandenen Sicherheitssystemen erkannt und mitigiert werden
- Bewertung, Priorisierung und Event-Triage
- Handlungsempfehlung auf Basis gewonnener Erkenntnisse
- Fall- und kritikalitätsbezogene Kommunikation mit den festgelegten Ansprechpartnern des Kunden

Die allgemeinen Erkennungslogiken werden durch Axians ständig weiterentwickelt und konnten in gewissem Umfang mit dem Kunden parametrisiert werden. Die Entwicklung von Custom Use Cases nach Kundenspezifikation ist hierbei möglich, wenn diese einen Cyber Security Bezug haben. Die 24/7-Überwachung beinhaltet Alarmierungen der Priorität 1 (kritisch). Diese werden durch das ständig besetzte Servicecenter der Axians alarmiert und wenn notwendig durch einen Incident Handler aus der Rufbereitschaft unterstützt. Die Auswahl der Alarmierungen obliegt der Axians.

In einem dreimonatigen Service Review Meeting werden auf Basis der monatlichen Service Reports die allgemeine Service-Qualität anhand von zurückliegenden Service-Vorgängen und Service-Tickets, vertragsrelevante Aktualisierungen und zu erwartende Änderungen des kommenden Quartals besprochen. Zusätzlich werden Service Reportings nach vordefinierten KPI und anerkannten Standards wie MITRE ATT&CK geliefert.

„Dank des Managed SOC werden unsere Logdateien analysiert und mit externen Sicherheitsinformationen angereichert. Bei Anomalien und potenziellen Bedrohungen erhalten wir rechtzeitig Alarme, die von den Analysten im SOC weiterqualifiziert werden. Auf diese Weise können wir schnell und gezielt angemessene Maßnahmen ergreifen."
Chief Information Security Officer, Hochland SE

Axians magellan GmbH · Albin-Köbis-Str. 5 · 51147 Köln
cad-aml@axians.de · www.axians.de/magellan