sure[secure]
your security operations center

secure mag

Managed SOC auch für deine OT-Umgebung.

Wir öffnen den Maschinenraum und zeigen, wie es geht.

Intro

Cybersecurity ist im Grunde das Verschieben von Wahrscheinlichkeiten. Je stärker meine Cyber-Resilienz ist, desto geringer ist die Wahrscheinlichkeit, einen Cyberangriff mit schweren Auswirkungen zu erfahren. Um die Wahrscheinlichkeit so gering wie möglich zu halten, ist es wichtig, einige grundlegende Dinge zu beachten. Dazu gehören Dinge wie Awareness-Schulungen für Mitarbeitende, Patch-Management, Multi-Faktor-Authentifizierung oder durchdachte Backup-Strategien sowie Frühwarnsysteme. Allerdings beziehen sich diese Maßnahmen in der Regel nur auf die IT-Infrastruktur der Unternehmen.

Doch nicht wenige Unternehmen verfügen auch über eine OT-Infrastruktur. Die produzierende Industrie in Deutschland umfasst rund 9.000 Unternehmen. Stillstände oder Ausfälle in diesen Bereichen hätten maximale Auswirkungen auf diese Unternehmen, da mit der Produktion weitere sensible Prozesse wie z.B. die Logistik verbunden sind. Aber warum gibt es gerade in diesem sensiblen Bereich so wenige Basics im Bezug auf Security? Häufig wird Sicherheit hier untergeordnet behandelt, und das ist durchaus nachvollziehbar: Solange die Maschine läuft, fühlt sich eben alles in Ordnung an. Deshalb bleibt die OT meist isoliert, mit möglichst wenigen Schnittstellen zur IT-Umgebung.

Die Wahrscheinlichkeit eines Cyberangriffs soll so reduziert werden, aber das Problem ist: im Falle eines Angriffs kann ich diesen gar nicht sehen. Visibilität und Monitoring der OT-Infrastruktur gelingt auch mit minimaler Einflussnahme auf die bestehenden Systeme. Wir haben einen Weg erarbeitet, wie wir auch OT-Daten in unserem Managed SOC zielführend verarbeiten und aufbereiten können.

Nun, die Produktionsumgebungen haben diverse Herausforderungen.

- Unterschiedliche Technologien und Protokolle (wie z. B. SCADA)
- Update- & Patch-Strategie gestaltet sich schwierig, da es in der Regel keine Wartungsfenster gibt
- Legacy Systeme im Einsatz, die „security-by-design“ nicht kennen, weil diese vor Jahrzehnten gebaut wurden
- Incident Response muss anders gedacht werden, da Maschinen in der OT nicht einfach isoliert werden können o. Ä.
- Fehlende Visibilität und unzureichendes Monitoring machen die OT-Infrastruktur oftmals zu einer Blackbox
- Asset-Management: Welche Assets habe ich eigentlich alle in meiner Produktionsumgebung?

Die Security ist der Verfügbarkeit der Systeme untergeordnet und das ist auch verständlich. Denn solange die Maschine läuft, ist gefühlt alles in Ordnung. So bleibt die OT isoliert mit möglichst wenigen Schnittstellen in die IT-Umgebung.

Mit Verfügbarkeit zur Transparenz

Die Verfügbarkeit muss nicht unter der Implementierung von Sensoren leiden. Denn die internationalen Hersteller haben den Schmerz der Entscheider mittlerweile verstanden. Ganz ohne eine Art der Sensorik funktioniert es aber natürlich auch nicht. Im Rahmen eines Implementierungsprojektes werden diese Sensoren installiert und es wird sofort eine automatische Abfrage der Assets gestartet. Die gefundenen Assets werden dann in einem Asset-Inventar gesammelt, definiert und letztlich in einen digitalen Zwilling gewandelt.

Das ist enorm wichtig, da die gesamte weitere Verarbeitung der Daten somit keinen Einfluss auf die Produktionsumgebung nehmen kann. Der digitale Zwilling wird dann kontinuierlich erneuert, um Veränderungen auch mitzubekommen. Nach Einbau der Sensorik gibt es also:

- Für das Schwachstellenmanagement ein Asset-Inventar
- Priorisierung der Schwachstellen nach Kritikalität
- Visibilität und Monitoring im Managed SOC

Aber wie funktioniert das genau?

Wir packen es an: Managed SOC für die OT

Mit einem Managed SOC inklusive der OT-Log-Dateien werden die Wahrscheinlichkeiten für einen folgenschweren Cyberangriff weiter verschoben. Blind-Spots verschwinden und es entsteht ein vollständigeres Monitoring sowie Transparenz für die gesamte Infrastruktur des Unternehmens.

Der Aufbau und die Bestandteile sind fast identisch. Das Managed SOC for OT benötigt ebenfalls die richtige Auswahl an People, Processes und Products wie ein SOC für die IT. Der perfekte Mix ist entscheidend für den richtigen Output und die Wirtschaftlichkeit eines Security Operations Centers. Dann habe ich ein interdisziplinäres Team, welches 24x7 mit klaren Prozessen und Eskalationsstufen sowie einem hohen Automatisierungsgrad dafür sorgt, dass die skalierbare Architektur mit SIEM und SOAR die IT-Infrastruktur optimal schützt.


PODCAST
CYBER SECURITY
Basement
In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.
Jetzt reinhören
Spotify
Apple Podcast
YouTube Music
amazon music
und noch mehr...

Das Team an der Schaltzentrale

Interdisziplinär bedeutet, dass alle notwendigen Kompetenzen mindestens doppelt besetzt sind. Dazu zählen auch Fachkräfte mit dediziertem OT-Security Know-How. Unser SOC-Team besteht aus:

- **Platform Engineers:** Unabhängig von der Plattform sind Wartung, Entwicklung und Automatisierung elementare Bestandteile, um kontinuierlich an der Effizienz zu arbeiten.
- **Incident Analysts:** Wenn das SOC anschlägt, muss sichergestellt sein, dass der Vorfall auch fachlich korrekt und gründlich aufgearbeitet wird. Nachlässigkeiten können schnell auch Fahrlässigkeit bedeuten. Incident Analysten verfügen über Wissen von APT-Angriffen, Spionage und weiteren komplexen Angriffsmustern.
- **SOC-Analysts:** Alles, was die Technologie nicht automatisch klären kann, wird manuell untersucht. Das ist wichtig, denn nicht alles lässt sich durch Automatisierung lösen. Sie ist zwar leistungsstark und deckt den Großteil ab, doch es gibt immer wieder Anomalien, die einer intensiven Prüfung bedürfen.
- **Detection Engineers:** Exzellente Detection Engineers sind notwendig, wenn ein SOC effizient arbeiten soll. Es wird an der Automatisierung gearbeitet, Playbooks und Detection Rules programmiert und ausgerollt, um die individuellen Anforderungen der Infrastrukturen zu berücksichtigen. So sind die Detection Rules immer auf dem neuesten Stand und das Unternehmen dadurch noch besser geschützt.
- **Incident Manager:** Der Incident Manager übernimmt die Leitung bei einem Sicherheitsvorfall. Er koordiniert den gesamten Einsatz und ist für die schnellstmögliche Wiederherstellung der Betriebsfähigkeit verantwortlich. Die ersten Stunden nach der Identifizierung eines Vorfalls sind besonders entscheidend. In dieser Phase müssen die richtigen Entscheidungen schnell und konsequent getroffen werden, um Folgeschäden zu verhindern.
- **Consultants:** Da unser SOC die IT- und OT-Infrastruktur überwacht, ist es unerlässlich, dass Security Consultants regelmäßig nach Optimierungspotenzialen schauen. Sind irgendwelche Blind-Spots vorhanden, die angebunden werden sollten? Durch die Dynamik der Infrastruktur muss auch die Security Infrastruktur mitwachsen.
- **Customer Success Manager:** Was ist ein Service wert, der sich nicht gut anfühlt? Wir haben ein Team von Customer Success Managern, die im ständigen Austausch dafür sorgen, dass alles so läuft, wie es soll. Die Ergebnisse des SOC werden verständlich aufbereitet und in regelmäßigen Review-Meetings erläutert. Gleichzeitig gibt es die Gelegenheit für konsequente Feedbackschleifen.

Ein Blick in den Maschinenraum

Unser SOC hat einen hohen Reifegrad erreicht und setzt auf eine Cloud-native Lösung von Google. Wenn Google etwas beherrscht, dann ist es die Suche und Korrelation von Daten. Zudem ist Google als Hyperscaler der ideale Partner für sämtliche Skalierungsmöglichkeiten. Genutzt werden das Security Event and Information Management System (SIEM), das Security Orchestration, Automation and Response (SOAR) Tool sowie Google Threat Intelligence (GTI). Schauen wir uns die Begriffe kurz an.

- **SIEM:** Sammelt die Logs der relevanten und angebundenen Log-Quellen ein und korreliert diese, sodass die Daten nutzbar werden. Auf dieser Basis können dann Analysen durchgeführt werden. Anbinden lassen sich nahezu alle Log-Quellen. Per Standard können mehr als 300 Cloud-Log-Quellen und über 2.000 On-Prem Quellen via Parser schnell und effizient angebunden werden.
- **SOAR:** Führt automatisierte Reaktionen auf bestimmte Detections aus, wodurch Sicherheitsvorfälle schneller bearbeitet und manuelle Eingriffe reduziert werden. Dadurch gewinnt das SOC erheblich an Effizienz und kann Bedrohungen schneller eindämmen.

Zusätzlich verfügt unser SOC-Service über einen integrierten Schwachstellen-Scanner, der kontinuierlich kritische Schwachstellen automatisch erkennt und diese wichtigen Erkenntnisse an das SOC-Team übermittelt. Dort landen die Events, die nicht automatisiert gelöst werden können. Sollte sich darunter ein kritisches oder auffälliges Event befinden, wird es per Eskalation an das Incident Response Team weitergeleitet, und gegebenenfalls wird der Incident Management Prozess eingeleitet. Über diesen Prozess wird der Partner umgehend informiert und ist sofort auf dem neuesten Stand.

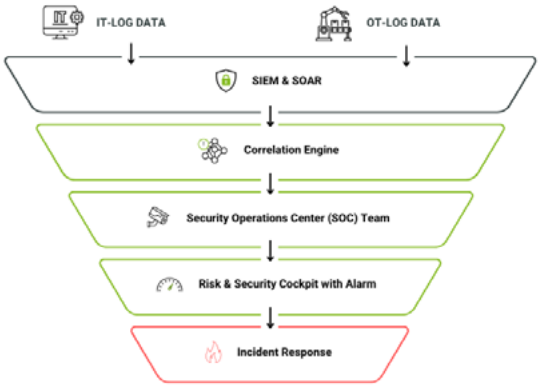
Diese Prozesse sind ein wichtiger Faktor für den Mehrwert eines SOCs. Prozesse sorgen für die nötige Effizienz und Qualität. In diesem sensiblen Bereich gibt es nichts Wichtigeres, als der übertragenen Verantwortung auch gerecht zu werden. Dazu gehört nicht nur die Definition klarer Eskalationsstufen, sondern auch ein hoher Grad an Automatisierung durch Detection Rules und Playbooks. Gerade mit Blick auf die OT können oftmals keine Standard-Regelwerke angewendet werden. Hier braucht es Custom Detection Engineering.

Ein solches Konstrukt aufzubauen, erfordert vor allem Erfahrung. Sobald ein Cyberangriff identifiziert wurde, wird das integrierte Incident Response Management aktiviert. Dieser Part geht bei uns weit über die Forensik hinaus.

Incident Response inklusive

Bei der Bewältigung eines Sicherheitsvorfalles geht es um weit mehr als nur darum, technische Maßnahmen zu ergreifen. Neben tiefgehender technischer Expertise müssen auch Aspekte wie rechtliche Vorgaben und Kommunikation berücksichtigt werden, da hier gravierende Fehler gemacht werden können. Es gibt Meldepflichten mit strengen Fristen, Informationspflichten gegenüber Betroffenen und einen vorgeschriebenen Umgang während der forensischen Analyse. Darüber hinaus müssen andere Parteien, wie z. B. Cyberversicherungen, unverzüglich informiert werden. All diese Faktoren erfordern eine koordinierte und gut strukturierte Reaktion, um den Vorfall effektiv zu bewältigen.

In einer Notsituation ist es schwierig, alle Aspekte im Blick zu behalten. Deshalb bieten wir unseren Incident Retainer mit einem Service-Level-Agreement, das eine 2-stündige Reaktionszeit und den Anspruch auf Vollständigkeit garantiert. Wir steuern nicht nur den Krisenstab, sondern stellen auch Expertisen für die Krisenkommunikation zur Verfügung. Darüber hinaus wissen wir genau, welche Behörden wir wann und auf welche Weise kontaktieren müssen, um eine schnelle und effiziente Reaktion zu gewährleisten.



Noch während wir die Erstinformation für die Mitarbeitenden abstimmen, beginnt in einem anderen Workstream bereits die Planung zur Wiederherstellung der Infrastruktur. Viele verschiedene Workstreams werden vom Incident Manager täglich koordiniert und dokumentiert. Das ist unser Verständnis einer ganzheitlichen Betreuung in einem Sicherheitsvorfall – und genau das bietet unser SOC-Service.

Mit diesem Setup werden Cyberangriffe nicht nur frühzeitig identifiziert, sondern wirklich auch effizient abgewehrt.

Onboarding

Wir akzeptieren es nicht, dass Onboardings lange dauern. Daher investieren wir erheblich in die Optimierung der Abläufe. Vom ersten Tag an, an dem sich ein Partner für uns entscheidet, stellen wir einen Transition Manager bereit, der sicherstellt, dass das Onboarding reibungslos verläuft. Unser Ziel ist es, eine langfristige Partnerschaft aufzubauen. Service Provider im Security-Sektor und Unternehmen benötigen eine vertrauensvolle Basis, und diese entsteht nur durch Transparenz und Expertise.

Nach der Beauftragung beginnen wir sofort, alle relevanten Informationen für das Onboarding bereitzustellen. Dabei benötigen wir auch erste Informationen vom Partner. Bereits nach etwa einer Woche findet das Kick-Off statt, in dem wir uns über die gegenseitigen Erwartungen austauschen. Denn zur Wahrheit gehört, dass wir während des Onboardings auf die Zusammenarbeit und Zuarbeit des Partners angewiesen sind.

Wir benötigen unter anderem:

- Einen dedizierten Ansprechpartner für das Projekt
- Ressourcen in Form von Zeit für die technische Umsetzung
- Systembezogene Zugänge und Passwörter
- Enge, projektbegleitende Abstimmung

Wenn das alles gegeben ist und keine Komplikationen auftreten, geht unser Service bereits nach vier Wochen live. Im Anschluss werden noch letzte Aufgabenpakete abgeschlossen und die vollständige Überwachung durch unser SOC ist nach spätestens sechs Wochen in place.

Foto: Annabelle Gunzelmann

Unser Managed SOC - ohne Kompromisse:

- Automated Response (SOAR)
- Standard Sources
- Cyberaudit
- Incident Response
- suresecure Detection Rules
- Incident Drill
- Customer Success Manager
- Attack Surface Monitoring
- SIEM
- Vulnerability Management
- Security Advisory

Google Security Operations

Google Threat Intelligence

txOne networks

OTORIO

Schlusswort:

Wer Cyberbedrohungen nachhaltig entgegenwirken möchte, sollte sich Gedanken über ein Frühwarnsystem machen. Ein SOC, wie hier beschrieben, stellt derzeit die effektivste Verteidigung dar. Zwar garantiert auch ein SOC keine 100%ige Sicherheit, aber früh erkannte Angriffe führen in der Regel nur zu minimalen Folgeschäden. Sicherheit ist tief in unserer Kultur verankert, und wir setzen alles daran, eure digitale Souveränität zu gewährleisten. Wir freuen uns auf ein Kennenlernen.

Weitere Informationen zum Thema:

Podcast-Folge:

Los SOCos: Security Operation Center - Make or Buy?

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de