FORTIT
SECURE DIGITAL BUSINESS

SOC: Angriffe effektiv abwehren

Sie können jederzeit von einem Cyberangriff betroffen sein. Bereiten Sie Ihr Unternehmen vor, **Angriffe** frühzeitig **zu erkennen** sowie gezielt darauf zu **reagieren**, um Ausfälle der Geschäftstätigkeit oder grössere **Schäden zu verhindern.**

FortIT unterstützt Sie zielgerichtet, um Ihre **Fähigkeiten** in den Bereichen **Detection und Response aufzubauen**, zu verbessern und bei der Beschaffung zu unterstützen.

Herausforderungen und Treiber:

- Fehlendes Wissen im Aufbau von Detection und Response Fähigkeiten
- Komplexe Abhängigkeiten zu anderen Systemen (OT, Cloud, etc.)
- Aufwändige Evaluation von Technologien und Anbieter

Ihr Mehrwert durch effektive Detection und Response Fähigkeiten:

- Schnelle Angriffserkennung zur Minimierung potenzieller Schäden
- Effektive Prozesse und automatisierte Reaktionspläne zur Abwehr von Angriffen
- Erhöhte Cyber-Resilienz und Einhaltung gesetzlicher Vorschriften

FortIT hilft Ihnen mit:

- ✓ Analyse der bestehenden und aufzubauenden Fähigkeiten FortIT SOC Framework
- ✓ Unabhängige Empfehlungen und Insights zu Marktteilnehmer und deren Fähigkeiten
- ✓ Erfahrung über alle Phasen hinweg von der Planung bis hin zur Implementierung

Ihre Reise zu einem erfolgreichen SOC

Initialisieren SOC-Programm — 1

Identifizieren von Risiken — 2

Anforderungen & Lösungsdesign — 3

Strategie und Roadmap

Ausgangslage:
- Initiative Detection und Response Fähigkeiten auf- oder auszubauen
- Fehlende Sicht der aktuellen Maturität und der Anforderungen
- Unzureichende Einbindung des Top-Level Managements und der Stakeholder

FortIT Dienstleistungen
- Projekt Initialisierung
  - Projekt-Kickoff vorbereiten und durchführen
  - Projekt-Governance aufsetzen, Vision und Ziele definieren
  - Stakeholder-Map entwickeln
  - Initiale High-Level Anforderungen erheben
- Risikobewertung und Bedrohungsszenarien sammeln und dokumentieren
- Definition des (Projekt-)Umfangs
- Ist-Analyse der vorhandenen Fähigkeiten (Sicherheits-Architektur)
- Definition der spezifischen Anforderungen

Resultate
- Dokumentierter Ist-Stand
- Projektcharta
- Detection und Response Strategie
- High-Level Roadmap

Mehrwerte

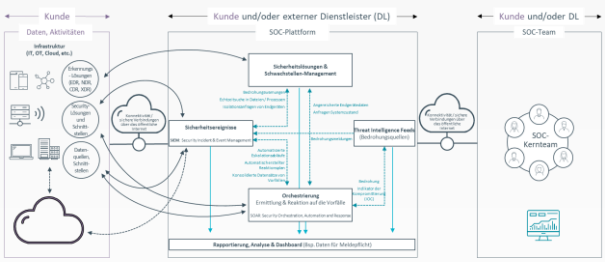
- ✓ Gemeinsames Verständnis für das Vorgehen
- ✓ Kosteneffizienz und Priorisierung dank Risiko-basiertem Ansatz
- ✓ Klare Übersicht der Anforderungen und fehlender Fähigkeiten

Design

Ausgangslage
- Projektumfang ist definiert, Stakeholder sind bekannt
- Unklares oder fehlendes Betriebsmodell
- Detailanforderungen und Use Cases nicht vorhanden

FortIT Dienstleistungen
- Anwendungsfälle
- Entwurf des Target Operating Modell
- Definition der Rollen und Schnittstellen
- Definition der Prozesse und Verantwortlichkeiten
- «Make» vs. «Buy» Empfehlung auf Basis der Strategie, Anforderungen, vorhandenen Fähigkeiten sowie Ressourcen und Anbieterlandschaft
- Entwurf detailliertes Lösungsdesign mit Technologieempfehlung
- Entwicklung des konkreten Umsetzungsplans (Roadmap)

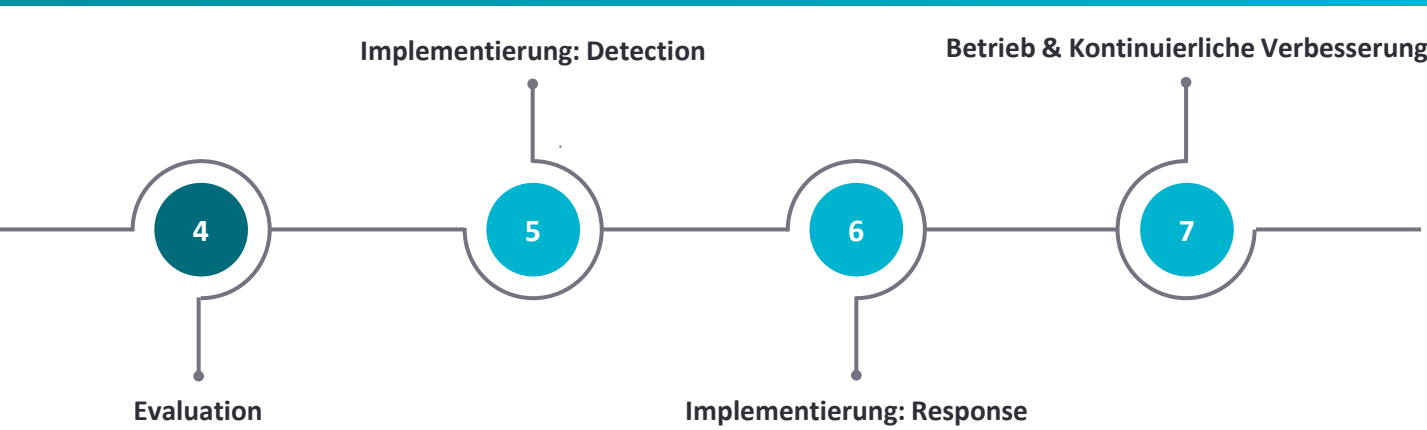
Resultate
- Betriebsmodell
- Definition der aufzubauenden / zu beschaffenden Fähigkeiten
- Detaillierte Roadmap zur Implementierung



Mehrwerte

- ✓ Klare Ziel-Architektur und Prozesse
- ✓ Anwendungsfälle sind dokumentiert
- ✓ Fundierte «Make» vs. «Buy» Entscheidungsgrundlage

mit unserem strukturierten Ansatz



Evaluation

Ausgangslage

- Definiertes Betriebsmodell und konkrete Anforderungen
- Unklarheit über die konkreten Angebote im Markt
- Fehlender Kriterienkatalog für das gewünschte Lieferobjekt

FortIT Dienstleistungen

- Durchführen Marktanalyse
- Ende zu Ende Begleitung einer Ausschreibung
  - Entwicklung Anforderungskatalog, Bewertungskriterien und Ausschreibungsunterlagen
  - Auswertung der eingegangenen Offerten
  - Vorbereiten und begleiten von Anbieterpräsentationen
  - Vergleich und Empfehlung
- Durchführen von Proof of Concept / Proof of Value

Resultate

- Messbarer Anforderungskatalog und Ausschreibungsunterlagen
- Anbieter Shortlist
- Entscheidungsgrundlage für einen Anbieter
- Dokumentierter POV/POC

Mehrwerte

- ✓ Erfahrungsbasierte und marktfähige Anforderungen
- ✓ Reduktion der internen Aufwände
- ✓ Unabhängige Bewertung

Implementierung und Betrieb

Ausgangslage

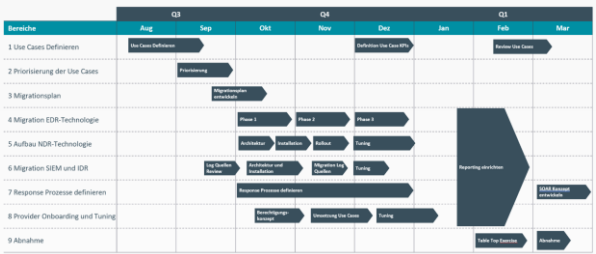
- Ausgewählte Technologien und/oder Dienstleister
- Fehlendes Wissen zu neuen Dienstleistungen, Technologien und Prozessen
- Schwierige Prüfung der Effektivität der implementierten Lösung gegenüber Anforderungen

FortIT Dienstleistungen

- Definition der Prozesse innerhalb der Organisation
- Konzeption und Einführung von Incident Response Playbooks
- Unterstützung in der Implementierung neuer Technologien (EDR-, XDR-, SIEM-, SOAR-Lösungen, etc.)
- Implementierung der kundenspezifischen Use Cases
- Konzeption und Implementation von Automatisierungslösungen zur schnellen Reaktion auf Vorfälle
- Abnahme der implementierten Lösungen
- Effektivitätsprüfung der Massnahmen (Konfigurations-, Systemreview, Red Teaming, Purple Teaming)
- Ableiten zukünftiger Massnahmen und weiterer Handlungsfelder

Resultate

- Transitionsplan
- Incident Response Pläne
- Implementierte Use Cases
- Abschlusspräsentation und Dokumentation
- Planung weiterer Massnahmen für die Optimierung



Mehrwerte

- ✓ Definiertes Vorgehen in Krisensituationen
- ✓ Resultate sind messbar und beschrieben
- ✓ Unabhängige Prüfung des neuen Ist-Standes

Referenzen

Referenzprojekt 1
SOC-Architektur und Evaluation

Ausgangslage: Ein grosses Energie- und Infrastrukturunternehmen wollte die SOC-Fähigkeiten in einem hybriden SOC-Betriebsmodell neu definieren und eine Ausschreibung für die Services lancieren. Um die Ausschreibung zielgerichtet zu formulieren, wurde die FortIT hinzugezogen, um die Ausschreibungsunterlagen fachlich zu prüfen.

Rolle der FortIT: Analyse des angedachten Betriebsmodells hinsichtlich der technischen und organisatorischen Anforderungen. Die Analyse zeigt Optimierungsmöglichkeiten beim Betriebsmodell auf und beschreibt diese marktgerecht. Im nächsten Schritt wurden der Anforderungskatalog und das Pflichtenheft auf Konsistenz fachlich überprüft und Änderungsvorschläge unterbreitet. Abschliessend wurde das Preisblatt auf Vollständigkeit überprüft. Des Weiteren wurde eine Marktanalyse durchgeführt und anzufragende Anbieter identifiziert.

Generierter Mehrwert: Das Betriebsmodell ist auf den Kunden abgestimmt. Der Kunde lanciert eine Ausschreibung, die marktkonform ist und somit Aufwände während der Evaluation reduziert und vergleichbare Offerten ermöglicht.

Referenzprojekt 2
SOC-Architektur und Ausschreibung

Ausgangslage: Medizinische Einrichtungen werden vermehrt Ziel von Angriffen. Ein Schweizer Kantonsspital möchte sich daher besser auf die auf Cyber-Angriffe vorbereiten und ihre Resilienz mit einem SOC ausbauen. Insbesondere der Schutz der Medizinaltechnik sowie der Prozesse im Gesundheitswesen stehen im Fokus.

Rolle der FortIT: Erhebung und Definition der organisatorischen und technischen Anforderungen an das SOC. Konzeption der geforderten SOC-Fähigkeiten. Ausarbeiten der Empfehlung für ein Betriebsmodell. Erstellung aller notwendigen Ausschreibungsunterlagen für eine gesetzeskonforme Beschaffung inclusive Ausarbeitung der Anforderungen und Kriterien. Bewertung der Angebote sowie Evaluation der Anbieter. Übergabe an die interne Projektleitung für die Realisierung mit dem evaluierten MSSP.

Generierter Mehrwert: Gesamtheitliche interne Sicht auf den Leistungsumfang und den Mehrwert des SOC. Transparente Kosten-Nutzen Betrachtung für die Kreditfreigabe. Klar strukturierte Anforderungen für die Evaluation.

Referenzprojekt 3
SOC-Strategie

Ausgangslage: Der Verband möchte eine Strategie aufzeigen, wie die Verbandsmitglieder die Anforderungen aus dem Datenschutzgesetz und der Meldepflicht für Cyberangriffe sicherstellen kann und zeitgleich das Risiko durch Angriffe reduziert werden kann. Die Strategie muss dabei OT-spezifische Aspekte berücksichtigen

Rolle der FortIT: Darlegung der Relevanz eines SOC als kompensierende Massnahme, wenn präventive Massnahmen Angriffe nicht verhindern können. Ausarbeitung eines Strategiepapiers für die Einführung eines SOC, der notwendigen Fähigkeiten und Empfehlung eines Betriebsmodells. Vergleich der unterschiedlichen Ausbaustufen und technologischen Bestandteile mit besonderem Fokus auf die OT-spezifischen Anforderungen. Präsentation der Ergebnisse mit konkreten Handlungsmassnahmen für die Verbandsmitglieder.

Generierter Mehrwert: Klarheit über die Mehrwerte eines SOCs und wie diese Cyberangriffen entgegenwirken können. Pragmatischer und praktikabler Umsetzungsplan, in welchem Synergiepotentiale maximal ausgeschöpft werden können.

Key take aways

Warum ein SOC?

- ✓ Visibilität: Erkennen Sie Angriffe schnell und reduzieren so die Auswirkungen.
- ✓ Kompensation von Schwächen oder Lücken Ihrer Schutzmassnahmen mittels einem SOC.
- ✓ Effektive Reaktion auf Cyber-Ereignisse dank gezielten Technologien und Prozessen.

Erhöhen Sie Ihre Fähigkeiten in den Bereichen Detection und Response.

Warum FortIT?

Unsere Expertise hilft Ihnen Angriffe zu erkennen und abzuwehren.

- Fundiertes Wissen in den Bereichen Monitoring, Detection und Response.
- Reger Austausch mit unterschiedlichen MSSPs und Kenntnis aktueller Produkte.
- Ganzheitliches, erprobtes SOC-Framework über People, Process und Technology.

Kontaktieren Sie uns heute!

FortIT AG
Badenerstrasse 281
8003 Zürich
fort-it.ch

Saner Çelebi
Head Consulting Services
saner.celebi@fort-it.ch

Michael Neesen
Security & Technology Expert
michael.neesen@fort-it.ch