redIT

REDIT SECURITY OPERATIONS CENTER

LEISTUNGSBESCHREIBUNG / NUTZUNGSBEDINGUNG

Inhaltsverzeichnis

1 SERVICE LEVELS

- 7 X 24h automatische Ticketerstellung bei Vorfällen
- Maximal 2h Reaktionszeit während Betriebszeit
- Betriebszeit ist abhängig von der Produktwahl
    - Geschäftszeiten (5x10) Mo - Fr von 07.00 - 17.00
    - Erweiterte Geschäftszeiten (5x15) Mo – Fr von 07.00 – 22.00
    - Erweiterte Geschäftszeiten und Samstag (6x15) Mo – Sa von 07.00 - 22.00
    - Rund um die Uhr (7x24) Mo – So 00.00 - 24.00

2 EINLEITUNG

Ein Security Operation Center ist eine zentrale Stelle, welche die Fähigkeit eines Unternehmens verbessert, Bedrohungen zu erkennen, auf diese zu reagieren und präventive Massnahmen zu ergreifen.
redIT SOC überwacht und schützt Ihre IT-Infrastruktur gegen Cyberbedrohungen. Dies geschieht durch Datenkonnektoren, welche Logs aus verschiedenen Datenquellen aggregieren und auf Unregelmässigkeiten überwachen. Im Ereignisfall werden Alarme ausgelöst, wobei durch implementierte Automatisierungsregeln entsprechende Gegenmassnahmen eingeleitet werden. Zudem werden Alarme durch die redIT bewertet und gegebenenfalls weitere Massnahmen initiiert.

redIT SOC eignet sich für alle Unternehmen, egal ob klein oder gross, die einen hohen Anspruch an ihre IT-Sicherheit haben.

3 PRODUKTSPEZIFIKATIONEN

Bestandteil vom redIT SOC sind folgende Komponenten enthalten:

- Betrieb redIT SOC
    - Implementation Datenkonnektoren
        - Azure Activity
        - Microsoft Defender for Endpoint
        - Microsoft Defender for Office
        - Microsoft Defender XDR
        - Microsoft Entra ID
        - Microsoft Entra ID Protection
    - Implementierung Analyseregeln
        - Erstellung/Ausführung von verdächtigen Prozessen
        - Detektion von spezieller Malware
        - Detektion von Malware im Papierkorb
        - Veränderungen im Security Log
        - Verdächtige Kommandozeileneingaben
        - Ausführung verdächtiger Binaries
        - Veränderungen an Security Policies
        - Registry Veränderungen
        - Mehrmalige fehlgeschlagene Login Versuche
        - Zuweisung von privilegierten Rollen an neue User
    - Implementierung Automationen
        - Automatic Notification
        - Automatic response to Ransomware (Isolation)
        - Automation Antivirus Scan
- Update Analyseregeln, Automationen, Datenkonnektoren

- Benachrichtigung redIT Helpdesk/Ansprechpartner Kunde nach redIT best practice
- Bewertung der Alarmmeldungen
    - Aufgrund der Bewertung werden Massnahmen initiiert

3.1 OPTIONEN

- Weitere Datenkonnektoren
- Weitere Automationen
- Weitere Analyseregeln
- Onboarding Geräte in Intune
- Onboarding Geräte im Defender for Endpoint
- Kundenspezifische Anforderungen

4 VORAUSSETZUNGEN

Für den Einsatz des redIT SOC gelten folgende Voraussetzungen

- Globale Administratoren Berechtigung für redIT Services AG
- Azure Subscription (Wird benötigt für Logspeicher, Cloud Consumption aufgrund Analyseregeln, Automationen)
- Geräte sind Intune/Microsoft Defender for Endpoint verwaltet
- Alle Benutzer/Geräte verfügen über eine der folgenden Lizenzen:
    - Microsoft Business Premium
    - Microsoft Defender for Business
    - Microsoft Defender for Endpoint Plan 2
    - M365 E5
    - Microsoft Defender for Business Server
    - Microsoft Defender for Servers-Plan 1
- Die Endpunkte verfügen über Internetkonnektivität

5 NICHT ENTHALTENE LEISTUNGEN

- Azure Subscription für Cloud Consumption
- Benötigte Lizenzen

6 ALLGEMEINE BESTIMMUNGEN

- Die Kündigungsfrist beträgt 20 Tage
- Die Implementierungszeit beträgt 2-4 Wochen, die Kosten für Cloud Consumption, fallen bereits in der Implementierungszeit an
- Downgrades oder Deaktivierung des Services wird nach effektivem Aufwand verrechnet
- Kundenseitige Mengenanpassungen müssen redIT Services AG innerhalb von 30 Tagen gemeldet werden
- Produktanpassungen innerhalb der Vertragslaufzeit sind vorbehalten
- redIT Services AG behält sich vor, Aufträge abzulehnen
- Es gelten unsere Allgemeinen Geschäftsbestimmungen