x-tention Cybersecurity Services for Healthcare

Bestens abgesichert mit dem Security-Gesamtpaket zur Erkennung, Bewertung und Behandlung von möglichen Cyberangriffen

xtention
IT with care.

1 | Überblick

Cybervorfälle sind laut einer Umfrage[1] das wichtigste globale Geschäftsrisiko im Jahr 2023.

Laut einer Studie[2] dauerte es im Durchschnitt **207 Tage,** bis ein Cyberangriff in einem Unternehmen erkannt wird. Das ist wertvolle Zeit, die viele Unternehmen verstreichen lassen, in der bereits Gegenmaßnahmen eingeleitet und die weitere Ausweitung von Angriffen unterbrochen werden könnten. Somit ist es nicht verwunderlich, dass jährlich über **24 Milliarden Euro Schaden durch Ransomware** verursacht werden[3]. Ein Großteil dieser Ransomware-Angriffe hätte durch eine rechtzeitige Erkennung und gezielte Reaktion verhindert oder zumindest abgeschwächt werden können.

Für die möglichst frühzeitige Erkennung und Unterbindung von Cyberangriffen reichen herkömmliche Basis-Security-Produkte, wie beispielsweise NextGen Firewalls oder Antivirus nicht mehr aus, da sich Angreifer heute lange Zeit im internen Netz bewegen können, ohne einen Alarm auszulösen oder anderweitig Verdacht zu erregen.

Auch die Gesetzgeber haben dieses Problem erkannt und fordern mit diversen Regelungen und Gesetzen die Umsetzung von Maßnahmen im Bereich der **Angriffserkennung und -reaktion.** Beispielsweise sind Betreiber von kritischen Infrastrukturen in **Deutschland** ab 1. Mai 2023 verpflichtet, ein System zur Angriffserkennung einzusetzen. In **Österreich** sind vergleichbare Maßnahmen durch die Anforderungen aus dem Netz- und Informationssystemsicherheitsgesetz (NISG) und der NIS-Verordnung umzusetzen. In der **Schweiz** empfiehlt das NCSC den Einsatz eines Security Operations Center zur Identifikation und zum Einleiten entsprechender Gegenmaßnahmen im Ernstfall.

Diesen Vorgaben entsprechend haben wir die **x-tention Cybersecurity Services for Healthcare** entwickelt, welche durch die Kombination aus **intelligenter Software und durchdachten Serviceleistungen eine 360°-Full-Service-Abdeckung** ermöglichen. Damit wird es einerseits dem Angreifer erschwert in die Infrastruktur einzudringen und andererseits ermöglicht, Angriffe frühzeitig zu erkennen und zu mitigieren.

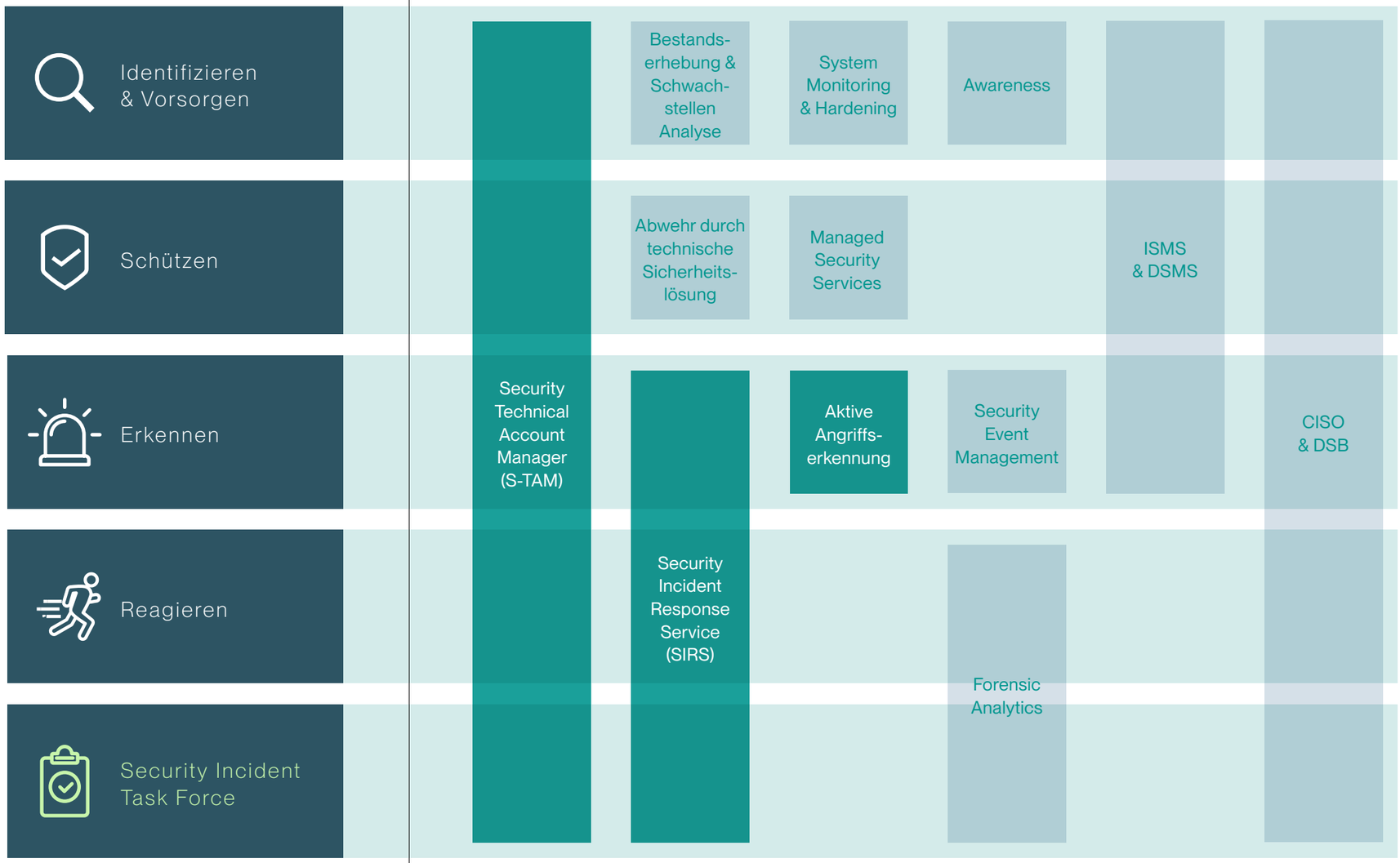

Abbildung 1: Das Cybersecurity Portfolio der x-tention Unternehmensgruppe
(Die Standard-Bestandteile der „Cybersecurity Services for Healthcare" sind türkis markiert)

1) Allianz Risk Barometer 2023: Cyber und Betriebsunterbrechung sind Top-Gefahren für Unternehmen, volkswirtschaftliche und Energierisiken die größten Aufsteiger
2) IBM Cost of a Data Breach Report 2022
3) Studie „Wirtschaftsschutz 2021", Bitkom e.V.

2 | Einsatz von künstlicher Intelligenz zur Erkennung von Angriffen

Als essentiellen Baustein zur Erhöhung der realen Sicherheit setzen wir modernste Technologien zur Erkennung von Cyberangriffen auf IT-Netzwerke und Systemlandschaften ein. Durch den Einsatz der ColdRead® Security Analytics Platform sind wir in der Lage, Angriffe mithilfe beeindruckender Algorithmen und künstlicher Intelligenz frühzeitig zu erkennen, zu analysieren und Maßnahmen zur Abwehr einzuleiten. Die Lösung kommt ohne Softwareinstallation am Endgerät aus und funktioniert auf Basis vorhandener Telemetriedaten. Somit ist die ColdRead® Security Analytics Platform für den Einsatz in sensiblen und stark regulierten Bereichen optimal geeignet und binnen weniger Stunden einsatzbereit.

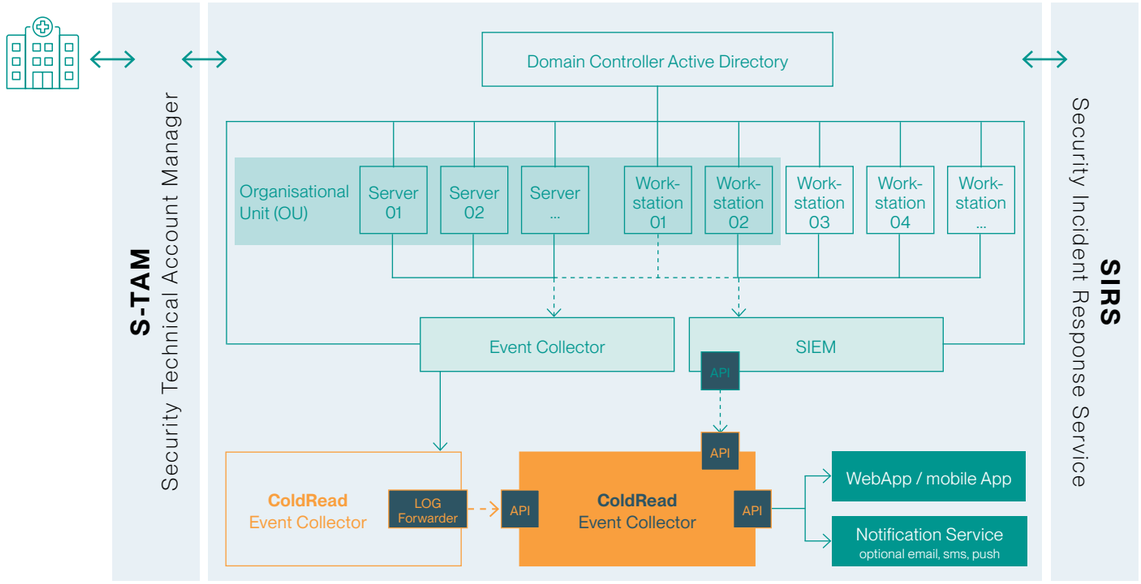

Abbildung 2: Schematische Darstellung des Systems zur aktiven Angriffserkennung. Die Lösung kann durch die Managed Cybersecurity Services S-TAM und SIRS ergänzt werden..

Beispiele für Angriffe, die durch die Software zur Angriffserkennung erkannt werden:

- In-Memory Angriffe
- Process Injection
- Lateral Movement
- Reconnaissance-Verhalten
- Brute Force Angriffe
- Fileless Malware
- RDP over SSH Tunneling
- Logon & Logoff Verhalten
- Active Directory Reconnaissance Verhalten (BloodHound / ShardHound)

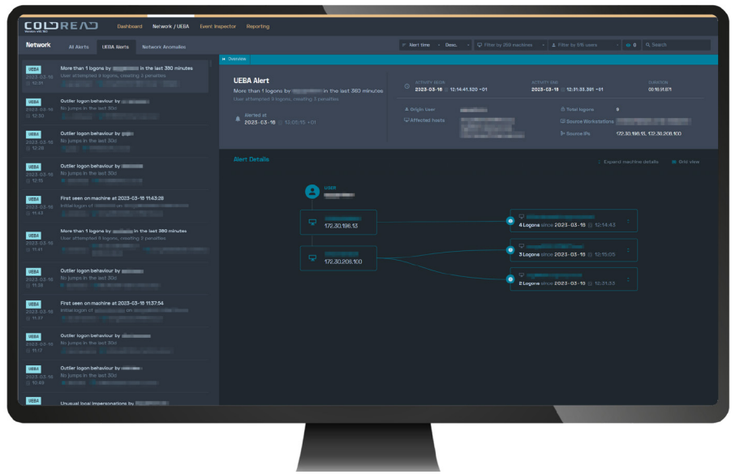

Abbildung 3: Screenshot des Threat Hunter-Dashboards

Die Vielzahl erkannter Angriffsvektoren steigert immens die Wahrscheinlichkeit einer äußerst frühzeitigen Erkennung und minimiert dadurch drastisch das Risiko eines erfolgreichen Angriffs und damit einhergehender Betriebsunterbrechungen.

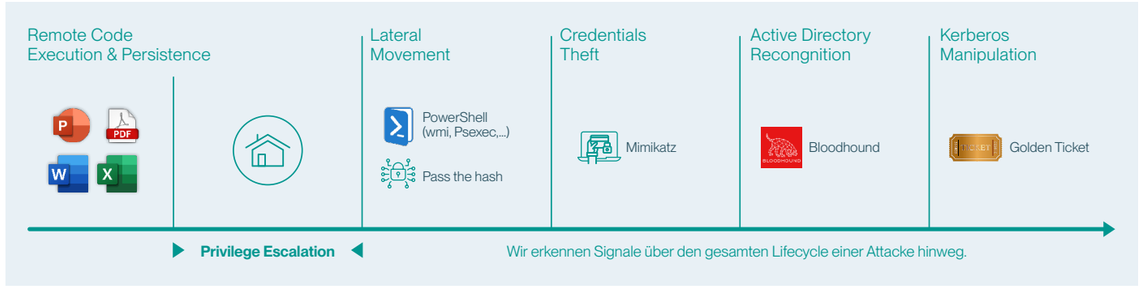

Abbildung 4: Beispiele für die Angriffe, die durch die Cybersecurity Services for Healthcare erkannt werden können

3 | Security Incident Response Service (SIRS)

Unser Security Incident Response Service Team beobachtet für Sie fortlaufend und pro-aktiv eingehende Hinweise, Detektionen, potentielle Bedrohungen und Security Events. **Alarmmeldungen aus unterschiedlichsten Quellen** (z. B. Threat Hunting, Monitoring, Angriffserkennung, Alarme von zentralen Sicherheitssystemen wie Firewalls oder Antivirus) werden bewertet, klassifiziert und dokumentiert. Zudem erstellen wir von jedem potentiellen Verdachtsfall eine Risikoeinschätzung und bewerten mögliche, schadhafte Auswirkungen.

Bei relevanten Bedrohungen kontaktieren wir Sie umgehend und liefern einen Action-Plan-Vorschlag zur Behandlung des Vorfalls, der dann unter Einbeziehung der verantwortlichen Stellen umgesetzt werden kann.

4 | Security Technical Account Manager (S-TAM)

Zur gesamtheitlichen Beratung bei allen Security-Themen steht Ihnen ein Security Technical Account Manager (S-TAM) stets zur Seite. Der S-TAM informiert Sie laufend über die aktuelle Bedrohungslage, die Ergebnisse der Angriffserkennung und den Status quo Ihrer Cybersecurity in Form eines monatlichen Cybersecurity Jour Fixe. Bei dem Auftreten von sicherheitsrelevanten Ereignissen erfolgt eine sofortige Kontaktaufnahme mit definierten Ansprechpartnern und die gezielte Weiterbehandlung der Vorfälle.

5 | Vorteile und Mehrwert

Schnellere Erkennung und sofortige Reaktion auf Angriffe

Durch die Kombination der Software zur Angriffserkennung in Verbindung mit unseren Serviceleistungen können Angriffe umgehend erkannt und gezielt behandelt werden.

Flächendeckender Einsatz der Angriffserkennung durch „Plug & Play“ Integration in Ihre bestehende IT-Infrastruktur:

Event Logs von Domain Controller, Server und Workstations werden an den von Ihnen zur Verfügung gestellten „Event Collector” weitergeleitet.

Unsere Systemtechniker richten einen Log Forwarder ein, der die Telemetriedaten sicher verschlüsselt in die ColdRead® Security Analytics Platform schickt. Hier werden die Daten von unserer Detection Engine verarbeitet und von unseren Security-Analysten überprüft.

Medizinische Systeme können so in die Gesamt-Cybersecurity-Strategie inkludiert werden.

Keine Installation am Endgerät erforderlich

Daher ist die Lösung auch in kritischen Netzbereichen flächendeckend einsetzbar.

Minimierung von False Positives

Durch den Einsatz von KI und die Vorabbetrachtung durch das SIRS werden ausschließlich relevante Informationen an Sie geliefert.

Wartungsfreier Betrieb

Unser „full-managed-service“ sorgt für stehts aktuelle Pattern und Engine Versionen, ohne jegliches Zutun ihrer IT.

Nicht invasive Lösung

Dank passiver Überwachung ist die Lösung für kritische Bereiche der Infrastruktur geeignet, wie zum Beispiel Medizintechnik oder Betriebstechnik.

Erfüllung gesetzlicher Anforderungen

Die Vorgaben zur Angriffserkennung können mit den x-tention Cybersecurity Services for Healthcare vollständig erfüllt werden.

Maßgeschneiderte Lösung für Ihre Organisation

Durch eine gesamtheitliche Betrachtung und regelmäßige Abstimmungen mit dem S-TAM ist es möglich, dass die Cybersecurity Services individuell an Ihre Bedürfnisse angepasst werden. Diese werden laufend verbessert und auf die aktuelle Bedrohungssituation abgestimmt.

Eigenes Team von IT-Sicherheits-, Informationssicherheits- und Datenschutzspezialisten

Alle x-tention Spezialisten sind zur Erfüllung des beschriebenen Leistungsumfangs bestens qualifiziert und beschäftigen sich täglich mit diesem Fachgebiet.

Durch laufende Fortbildungen und Zertifizierungen sowie durch den regelmäßigen Austausch mit anderen Experten im D-A-CH-Raum wird das fachliche Know-how und die Expertise unserer Spezialisten stets erweitert.

Wir lassen unsere Qualität und unser Sicherheits- und Datenschutzniveau regelmässig überprüfen

Der Rechenzentrumsbetrieb von x-tention ist seit Anfang 2011 durchgängig nach ISO/IEC 27001 zertifiziert und x-tention betreibt ein angemessenes und vom TÜV zertifiziertes Informationssicherheits-Managementsystem (ISMS) inkl. IT-Risikomanagement.

Im Dezember 2018 wurde x-tention als erstes Unternehmen mit dem TÜV-Austria-Zertifikat „Geprüftes Datenschutzmanagementsystem“ ausgezeichnet.

Seit 2019 ist das Qualitätsmanagementsystem von x-tention vom TÜV nach ISO 9001 zertifiziert.

Wir kennen die Branche und die täglichen Herausforderungen im Gesundheits- und Sozialwesen

x-tention ist IT-Betriebsführer mit eigenen zertifizierten Rechenzentren im Gesundheits- und Sozialwesen und bietet pragmatische und massgeschneiderte Informationssicherheits- und Datenschutzlösungen – optimiert für das Gesundheits- und Sozialwesen.

Aufgrund der Geschäftstätigkeit im D-A-CH-Raum verfügt x-tention über länderübergreifende Expertise und kann diese Erfahrung in die Projekte einbringen.

Wir wissen wie Cyberkriminelle in IT-Netzwerke eindringen

Jeder gezielte Cyberangriff folgt einem spezifischen Schema und wir haben die Lösung ausgewählt, die diese Schemata erkennt und so Cyberangriffe in IT-Netzwerken frühzeitig entdeckt.

SecAttack, der Hersteller von ColdRead®, baut auf langjährige Red Team Erfahrung und zahlreiche erfolgreich durchgeführte Cyberangriffe bei Top 30 DAX und ATX gelisteten Firmen.

Unterstützung im Anlassfall

In Cyber-Notfällen unterstützen Sie unsere Experten der Security Incident Task Force, um den Angriff so rasch wie möglich einzudämmen und einen sicheren Regelbetrieb wiederherstellen zu können.

Wir kümmern uns um Ihre Cybersecurity, damit Sie sich auf Ihre Kernkompetenz konzentrieren können.

Kontaktieren Sie mich gerne!

Peter Brillinger, MSc
Cybersecurity Competence Center
Infrastructure Enterprise Solutions

cybersecurity@x-tention.com
+43 7242 2155 6100