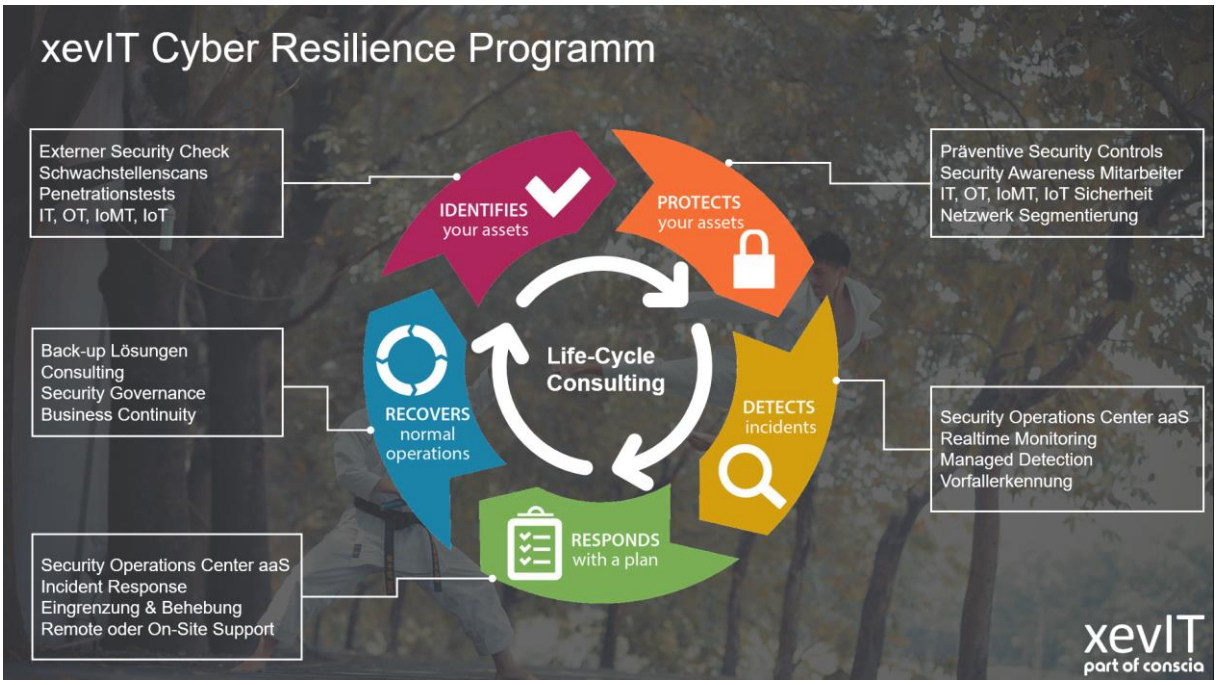
Cybersicherheit für Krankenhäuser

In Bezug auf Cybersicherheit sind die Angreifer immer im Vorteil: Es gibt immer mehr Angriffspunkte, als die Verteidiger schützen können und ein geschickter Hacker braucht nur einen!

Daher ist es äußerst wichtig, dass Sie Ihre Infrastruktur, Ihre Systeme und vor allem Ihre Schwachstellen gut kennen.
Die **Sicherheitsanalyse**, die wir im Rahmen unseres Cyber Resilience Programms durchführen, unterstützt Sie dabei und eignet sich als idealer Einstiegspunkt.
Dazu gehören:

- **Penetrationstests** der externen und internen Infrastruktur
- **Schwachstellenscans der IT-Systeme und vernetzten Medizingeräte,** sowie eine
- **Befragung zum Status** ihrer IT-Sicherheit.

Ideal ergänzt wird die Sicherheitsanalyse durch eine Bewertung Ihrer gesamten IT-Infrastruktur nach dem **HiMSS Analytics INFRAM** (Infrastructure Adoption Model) Reifegradmodell.
Ähnlich wie das HIMSS Analytics EMRAM (Electronic Medical Record Adoption Model) ist das INFRAM ein achtstufiges Modell (0 – 7), das IT-Führungskräften im Gesundheitswesen ermöglicht, die technologischen Infrastrukturfähigkeiten abzubilden, die erforderlich sind, um die klinischen und operativen Ziele Ihrer Einrichtung zu erreichen.



In den meisten Krankenhäusern nimmt die Zahl von **netzgebundenen Medizin- und IoT-Geräten** stark zu. Neben allen positiven Effekten, die die Vernetzung dieser Systeme bietet, stellt dies aber auch gleichzeitig eine massive **Erweiterung der digitalen Angriffsfläche** dar.
Zum Schutz dieser hochsensiblen Bereiche bieten wir spezielle Systeme und Verfahren an,

die die vernetzten Medizingeräte inkl. Schwachstellen und Kommunikationsbeziehungen **automatisiert** erkennen. Das schafft zum einen die dringend benötigte **Visibilität** über die vorhandenen Systeme und zum andern ermöglichen die gewonnenen Informationen eine effektive **Netzwerkzugangskontrolle** sowie die **Segmentierung** des Netzwerks, damit die vernetzte Medizintechnik wirkungsvoll geschützt werden kann.

Weitere Schwerpunkte des Cyber Resilience Programms liegen auf den Themen:

- **Erkennung und Reaktion** auf Bedrohungen und Angriffe.
- Security Information & Event Management (**SIEM**)
- Endpoint Detection & Response
- Cloud Security
- Identity & Access Management
- Network Security

Neben der Implementierung bieten wir auch den Betrieb dieser Systeme als **Managed Service** durch unser Security Operations Center (**SOC**) an. Selbstverständlich unterstützt Sie unser SOC auch bei der **Erkennung, Eindämmung und Beseitigung** von IT-Sicherheitsvorfällen.
Die Kombination aus **hochspezialisierten Security-Analysten**, modernen Software-Tools und mit den Kunden abgestimmte Prozesse, sog. **Incident Playbooks**, ermöglichen eine effektive Reaktion auf Sicherheitsvorfälle, damit im Ernstfall schnell die richtigen Entscheidungen gefällt werden können.

Lassen Sie sich in einem kostenfreien Webinar überzeugen.

Termine:
Bitte klicken Sie auf einen der Termine, um zur Registrierung zu gelangen.

Donnerstag 21.01.2021 – 11-12 Uhr	Donnerstag 28.01.2021 – 15-16 Uhr
Dienstag 02.02.2021 – 14-15 Uhr	Donnerstag 11.02.2021 – 11-12 Uhr
Dienstag 16.02.2021 –15-16 Uhr	Donnerstag 25.02.2021 –11-12 Uhr

Weitere Informationen finden Sie unter https://www.xevit.com/de/healthcare

Ihr Ansprechpartner für Fragen:
Frau Anja Fischer, Anja.Fischer@xevit.com