Hacknowledge

Einfache Sicherheitsüberwachung – Dedizierte Detektionsszenarien für den Gesundheitssektor anhand von konkreten Praxisbeispielen

Information Security in Healthcare Conference

14.06.2023 - Cham

Agenda

1) Vorstellung
2) Hacknowledge
3) Besonderheiten im Gesundheitssektor - unsere Erfahrungen
    a. Herausforderungen im Gesundheitssektor
    b. Dedizierte Detektionsszenarien
4) Konklusion und Empfehlungen
5) Fragen & Antworten

Hacknowledge

01

Vorstellung

SPRECHER

Sarah MERZ

Schweizerische Post
Key Account Manager

Mathieu DELAVY

Hacknowledge
Chief Commercial Officer

ÜBER UNS

Purer Cybersecurity Player

Wir bieten einfache, effiziente und pragmatische Dienstleistungen, um die Cybersicherheit unserer Kunden zu verbessern.

Schweiz: Hauptsitz und zentrale Drehscheibe für den Betrieb, einschließlich Rechenzentren

Luxemburg: Handelsvertretung für BENELUX-Kunden, Drehscheibe für Offensive Sicherheit

52 Mitarbeitende – inkl. 47 Sicherheitsingenieure

ISO 27001 Zertifizierung (kein Ausschluss)

SWISS POST Mehrheitsaktionärin seit 2022

Hacknowledge

02

Hacknowledge

Vorstellung

Hacknowledge

UNSERE WERTE

Unabhängig

Hacknowledge ist ein unabhängiger Anbieter von Sicherheitsüberwachungs-lösungen für Unternehmen.

Wir verkaufen keine Produkte oder Dienstleistungen weiter.

Fair

Wir sind davon überzeugt, dass Sicherheitsüberwachung einfach und kostengünstig sein kann.

Wir nutzen Ihre vorhandenen Sicherheitslösungen und -geräte.

Effektiv

Wir helfen Ihrem Unternehmen, IT-Sicherheitsbedrohungen zu erkennen und die Zeit zwischen Sicherheitsverletzung und Entdeckung zu verkürzen.

Agil

Hacknowledge entwickelt, betreibt und verwaltet seine eigene Software- und Hardwarelösung.

UNSERE SERVICES

Cyber Überwachung

- Security Operation Center (SOC)

Offensive Sicherheit

- Penetration Testing
- Red/Purple Team
- Phishing
- Cyber Incident Simulation
- Adversary Simulation

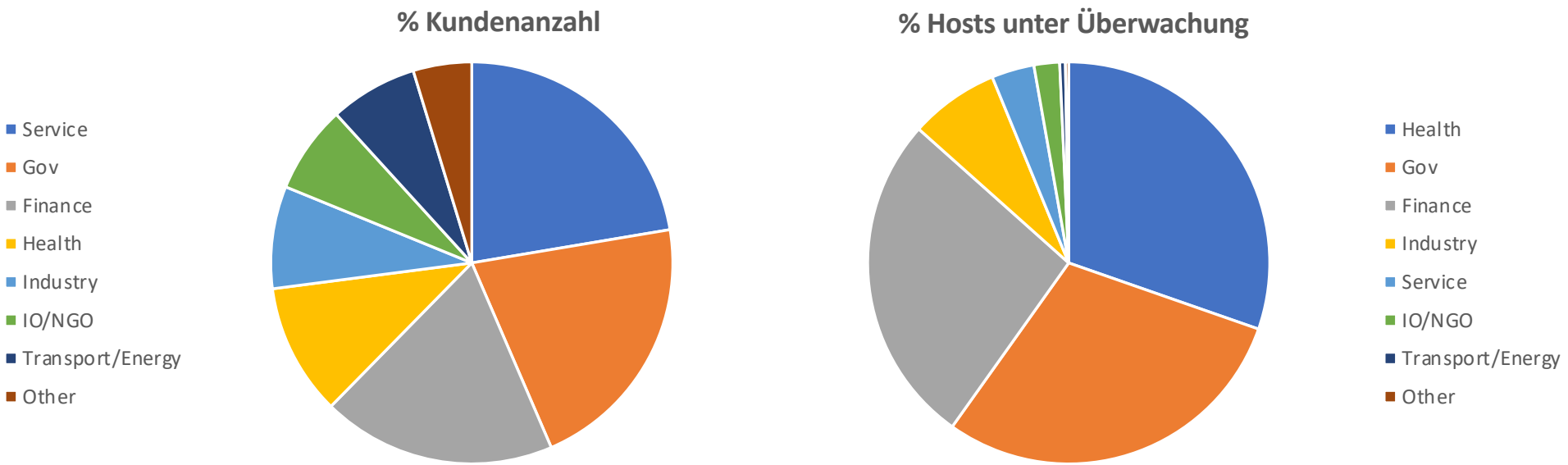
Digitale Forensik

- Incident Preparation
- Threat Hunting
- Incident Response
- Digitale Forensik

Security Akademie

- Mitarbeiter Awareness
- Security Certification Trainings
- Massgeschneiderte Trainings

KUNDENPORTFOLIO



Hacknowledge

03

Besonderheiten im Gesundheitssektor – unsere Erfahrungen

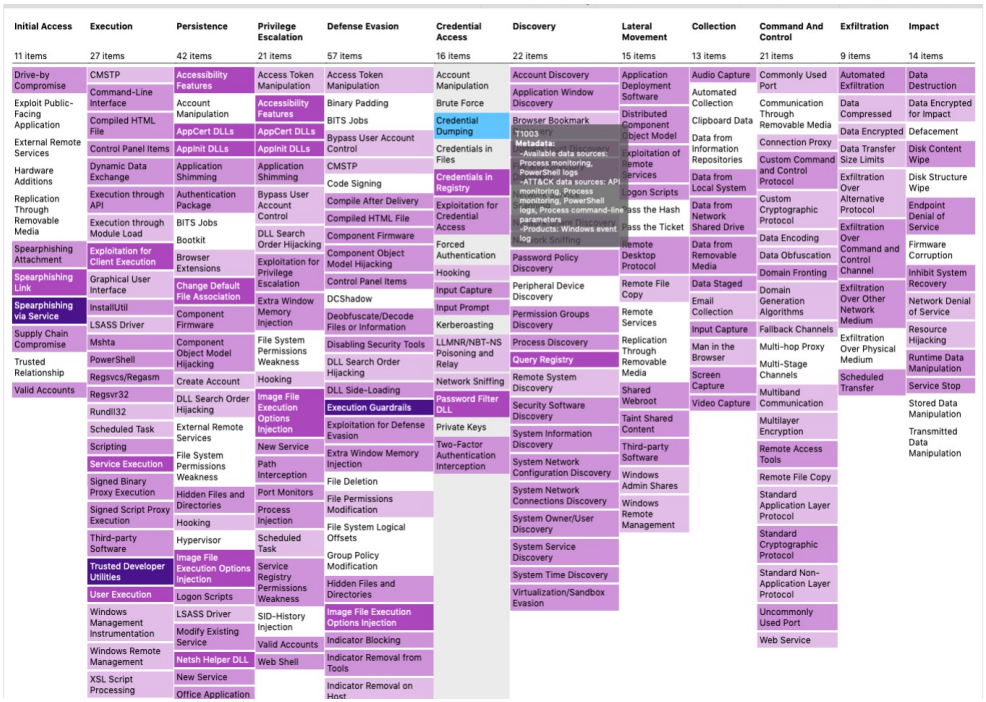
A – Herausforderungen im Gesundheitssektor

B – Dedizierte Detektionsszenarien

A – Herausforderungen im Gesundheitssektor

MITRE FRAMEWORK

Wir benützen das MITRE als Framework für unsere Use Cases



- Die meisten Kunden sind ähnlich (vergleichbare use cases sind implementiert)
- Inkl. Gesundheitssektor

N.B: fake coverage, Hacknowledge coverage is confidential

Hacknowledge

Komplexe Faktoren im Gesundheitssektor

Viel Legacy

System manchmal unmöglich zu patchen

Offene Umgebung

Universitätspitäler, BYOD, …

Viele proprietäre Geräte

Scanners, …

Viele Standorte

Datencenter, Gebäude, …

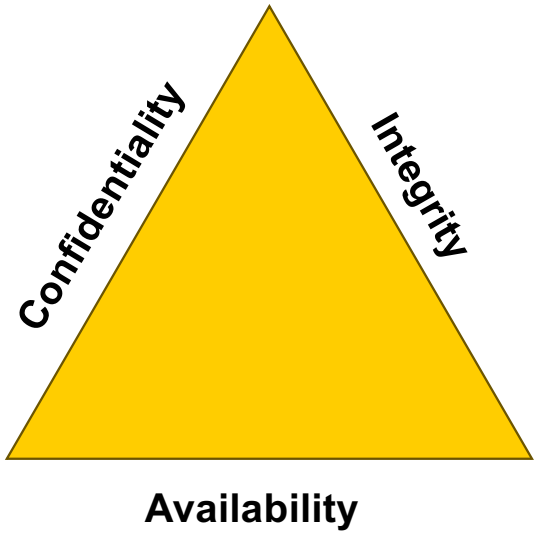
Grosses Datenvolumen

Forschung, …

Gleichgewicht zwichen der Vertraulichkeit und Verfügbarkeit schwer zu finden

z.B.: Computer mit Patientendaten im Operationssaal

CIA Triad



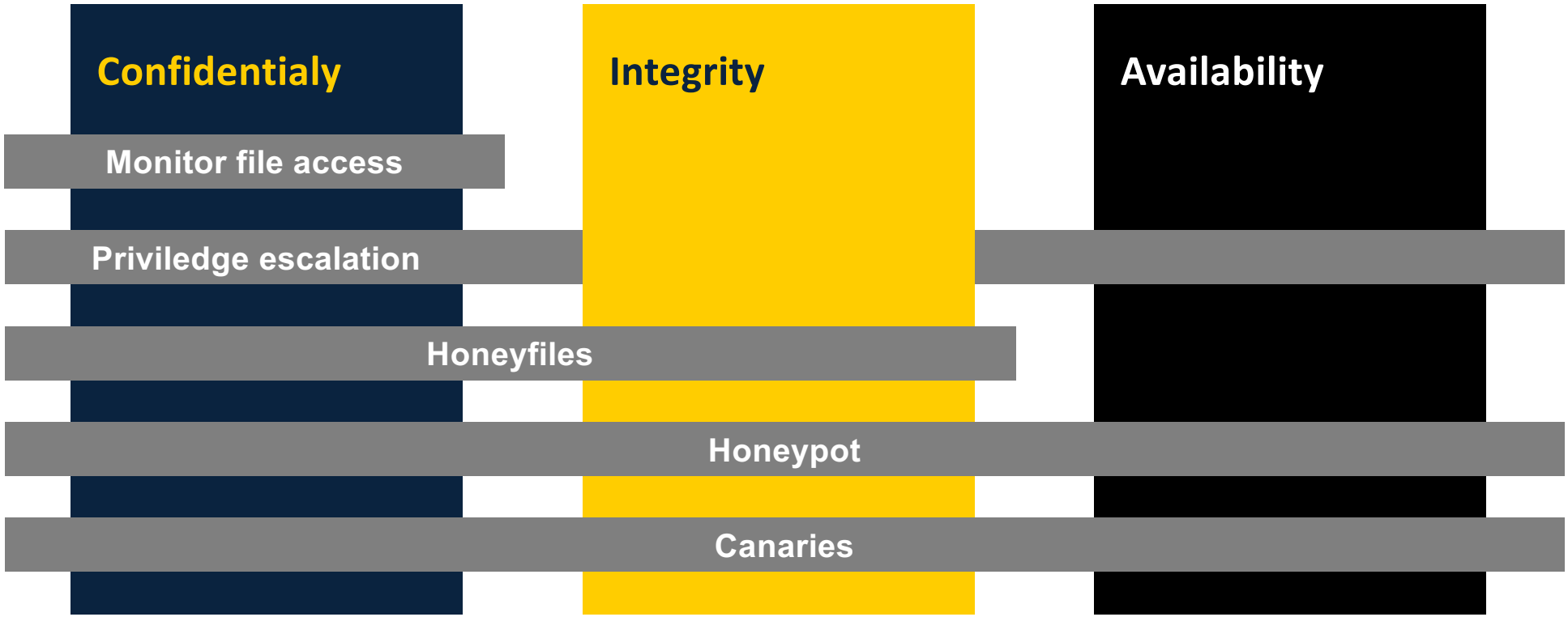
Sektor	Priorität	Kommentar
Finanzen	C > A > I	Kundendaten als Hauptfokus
Industrie	A > C > I	Produzierende Maschinen
Behörden	I > C > A	Mitbewohnerndaten
Gesundheit	C = A = I	C: Vertraulichkeit der Patientendaten A: Verfügbarkeit der Medizinalgeräte I: Datenintegrität der Analysen

B – Dedizierte Detektionsszenarien

Cyberrisiken im Gesundheitssektor aus unserer Erfahrung

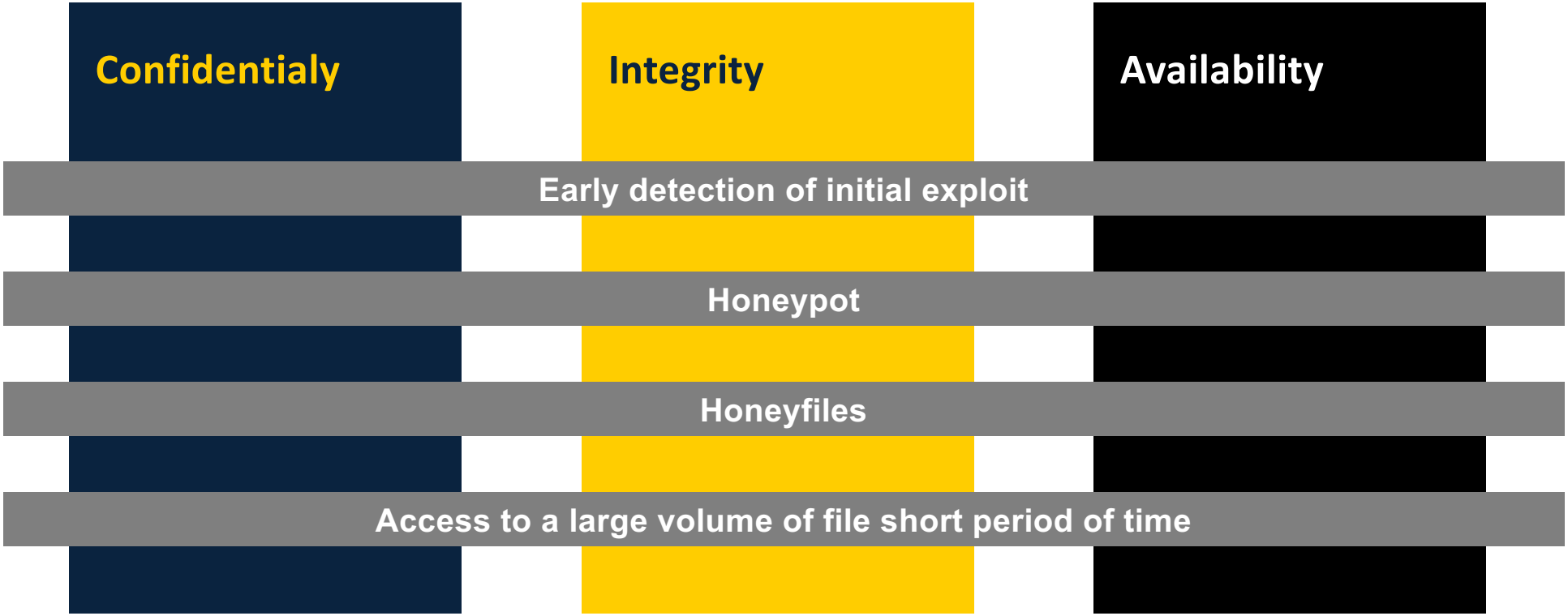
Insider threats	Computer ohen Zugriffskontrolle z.B.: Notfall / Intensivstation, …
Ransomware	Sehr geöffnete Infra / Netzwerk z.B.: Forschung in Universitätsspitäler, BYOD,…
Medical devices - OT	Grosse Scanner gemanaged beim Hesteller. Verbindung mit dem IT Netzwerk (nicht wie beispielsweise im Energie Sektor)
Legacy Software	Gesundheitssektor inverstiert mehr in die “Pflege” als in die IT

Risk 1 – Insider threats



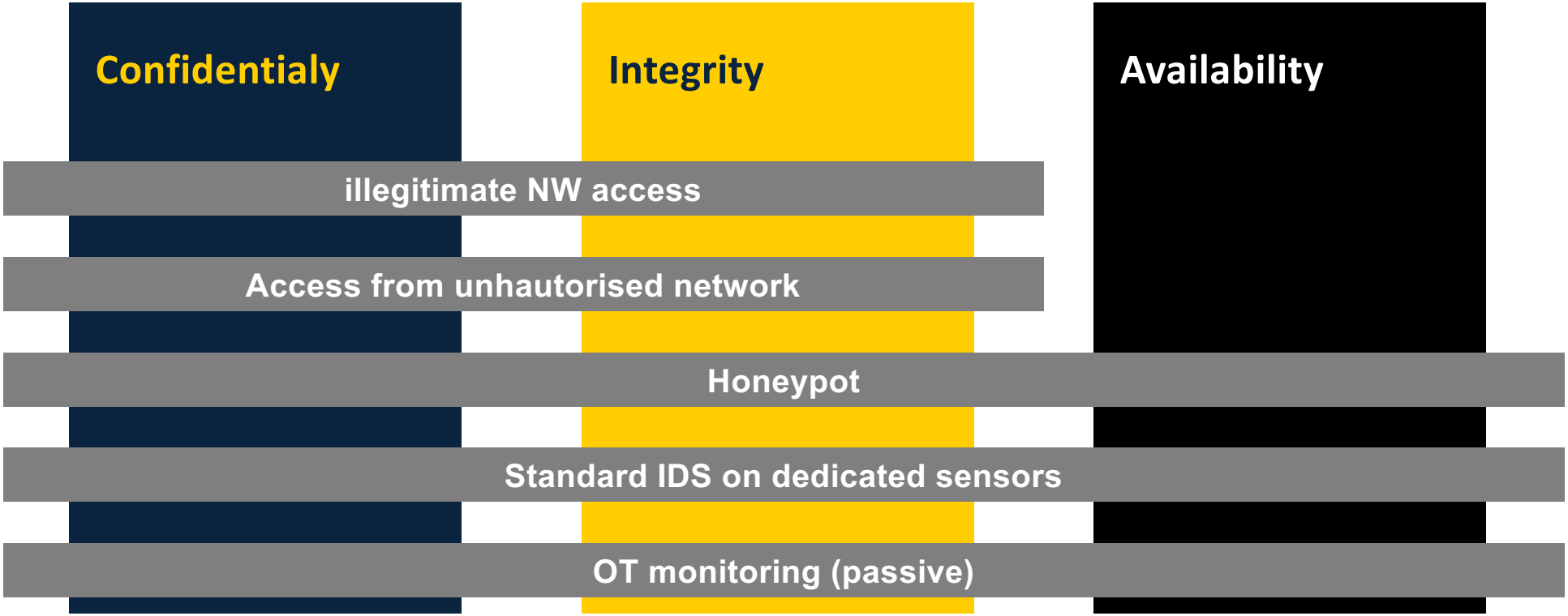
Hacknowledge

Risk 2 – Ransomware



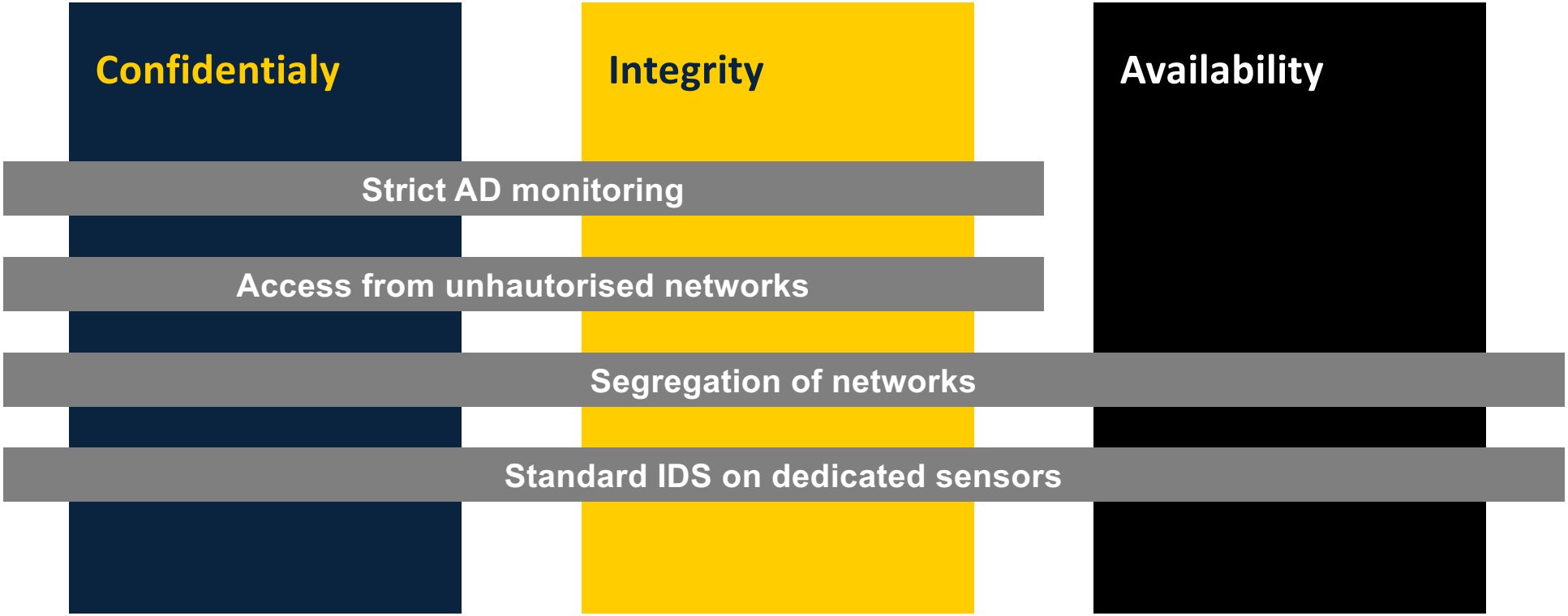
Hacknowledge

Risk 3 – Medical devices / OT equipement



Hacknowledge

Risk 4 – Software legacy



Hacknowledge

KONKLUSION

- Grosse Netzwerke
- Viele Gebäude/Standorte
- Viele verschiedene Geräte
- Grosses nicht-standardisiertes Volumen
- Tiefe Maturität X Grosse Risiken
- Schwierigkeiten beim Scannen (Auswirkung auf die Leistung) und um ein Inventar zu haben

EMPFEHLUNGEN

- Durchsetzung von passiver Überwachung und perimetrischer Analyse
- Use Case basierend auf der Log Collection
- Vermeiden von Verfügbarkeitsrisiken der Umgebung

Hacknowledge

Hacknowledge

Hacknowledge SA
Rue de Lausanne 35A
1110 Morges
Switzerland
+41 21 519 05 01

Hacknowledge Lux SA
9 Rue du Laboratoire
1911 Luxembourg
Luxembourg
+352 20 30 15 86

hacknowledge.com