



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

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)



Mehrheitsaktionärin seit 2022



02

Hacknowledge

Vorstellung

UNSERE WERTE

Unabhängig



Hacknowledge ist ein unabhängiger Anbieter von Sicherheitsüberwachungslösungen 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

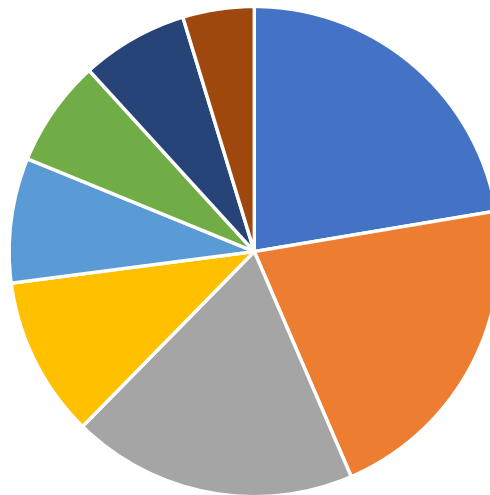


- Mitarbeiter Awareness
- Security Certification Trainings
- Massgeschneiderte Trainings

KUNDENPORTFOLIO

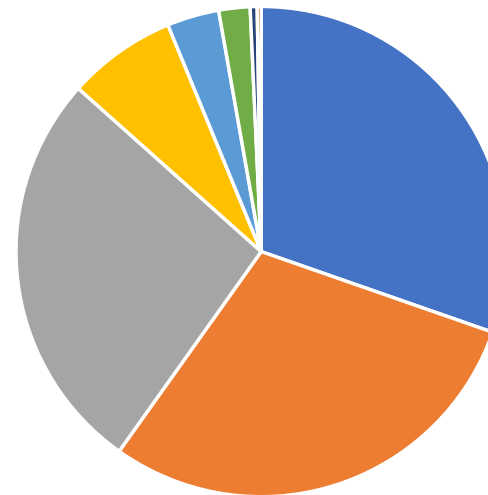
% Kundenanzahl

- Service
- Gov
- Finance
- Health
- Industry
- IO/NGO
- Transport/Energy
- Other



% Hosts unter Überwachung

- Health
- Gov
- Finance
- Industry
- Service
- IO/NGO
- Transport/Energy
- Other



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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Automated Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark	Distributed Component Object Model	Clipboard Data	Removable Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	Appint DLLs	Appint DLLs	Bypass User Account Control	Credentials in Files	File Metadata	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Code Signing	Available data sources: Process monitoring, Powershell logs	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Compile After Delivery	Compiled HTML File	Available data sources: API monitoring, Process monitoring, Powershell logs, Windows event log	Logon Scripts	Custom Network Shared Drive	Data Obfuscation	Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	Bootkit	Component Firmware	Component Firmware	Forced Authentication	Hashes the Ticket	Data from Removable Media	Data Encoding	Over	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Browser Extensions	Exploitation for Privilege Escalation	Control Panel Items	Control Panel Items	Hooking	Input Capture	Desktop Protocol	Domain Fronting	Exfiltration Over Other Network	Network Denial of Service
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Extra Window	DCShadow	DCShadow	Input Prompt	Peripheral Device Discovery	Data Staged	Email Collection	Domain Generation Algorithms	Network Denial of Service
Trusted Relationship	Install/Uninstall	Component Firmware	Memory Injection	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Kerberoasting	Permission Groups Discovery	Remote Services	Input Capture	Fallback Channels	Resource Hijacking
Valid Accounts	LSASS Driver	Mshta	File System Permissions Weakness	Disabling Security Tools	DLL Search Order Hijacking	LLMNR/NBNS Poisoning and Relay	Process Discovery	Query Registry	Man in the Browser	Multi-hop Proxy	Exfiltration Over Physical Medium
	PowerShell	Component Object Model Hijacking	File System Permissions Weakness	DLL Search Order Hijacking	Hooking	Network Shifting	Remote System Discovery	Shared Webroot	Screen Capture	Multi-band Communication	Scheduled Transfer
	Regsvcs/Regasm	Create Account	Image File Execution Options Injection	DLL Side-Loading	Execution Guardrails	Private Keys	Security Software Discovery	Tampered Content	Third-party Software	Remote Access Tools	Service Stop
	Regsvr32	DLL Search Order Hijacking	Path Interception	Extra Window Memory Injection	File Deletion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Admin Shares	System Network Connections Discovery	Windows Remote Management	Stored Data Manipulation
	Rundll32	Image File Execution Options Injection	File Permissions Modification	File Permissions Modification	File Permissions Modification	System Information Discovery	System Owner/User Discovery	System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Transmitted Data Manipulation
	Scheduled Task	External Remote Services	File System Logical Offsets	Group Policy Modification	Hidden Files and Directories	System Information Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service	
	Scripting	File System Permissions Weakness	Port Monitors	File Permissions Modification	File System Logical Offsets	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Service Execution	File System Permissions Weakness	Path Interception	File Permissions Modification	File System Logical Offsets	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Signed Binary Proxy Execution	Hidden Files and Directories	Process Injection	File System Logical Offsets	Group Policy Modification	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Signed Script Proxy Execution	Hooking	Scheduled Task	Group Policy Modification	Hidden Files and Directories	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Third-party Software	Hypervisor	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Trusted Developer Utilities	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories	Hidden Files and Directories	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	User Execution	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Windows Management Instrumentation	LSASS Driver	LSASS Driver	SID-History Injection	Image File Execution Options Injection	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Windows Remote Management	Modify Existing Service	Modify Existing Service	Valid Accounts	Indicator Blocking	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	XSL Script Processing	Netsh Helper DLL	Web Shell	Web Shell	Indicator Removal from Tools	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
		New Service	Indicator Removal on Host	Indicator Removal on Host	Indicator Removal on Host	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	
		Office Application	Indicator Removal on Host	Indicator Removal on Host	Indicator Removal on Host	System Network Connections Discovery	System Owner/User Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	

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

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

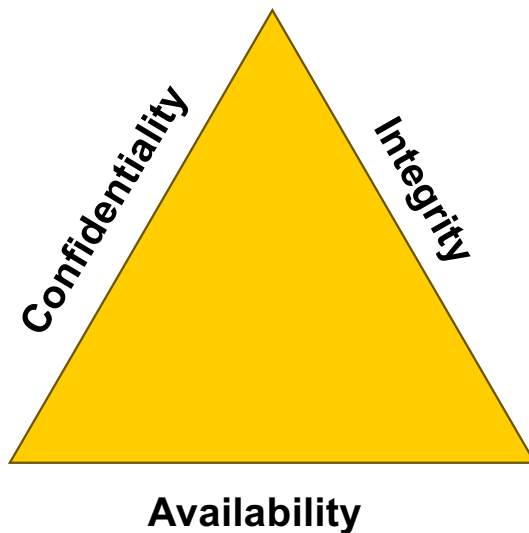
Forschung, ...



Gleichgewicht zwischen der Vertraulichkeit und Verfügbarkeit schwer zu finden

z.B.: Computer mit Patientendaten im Operationsaal

CIA Triad



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

B – Dedizierte Detektionsszenarien

Cyber Risiken im Gesundheitssektor aus unserer Erfahrung

Insider threats

Computer ohne Zugriffskontrolle
z.B.: Notfall / Intensivstation, ...

Ransomware

Sehr geöffnete Infra / Netzwerk
z.B.: Forschung in Universitätskliniken, BYOD, ...

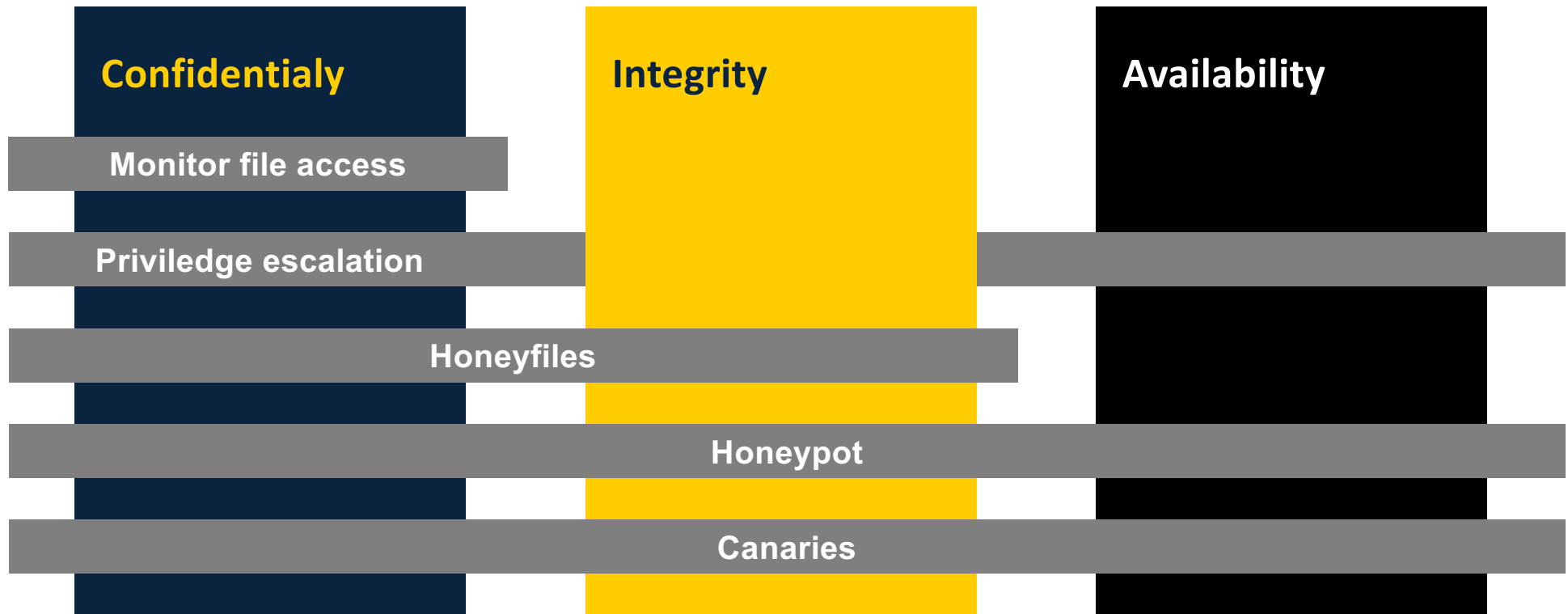
Medical devices - OT

Große Scanner gemanagt beim Hersteller. Verbindung mit dem IT Netzwerk (nicht wie beispielsweise im Energie Sektor)

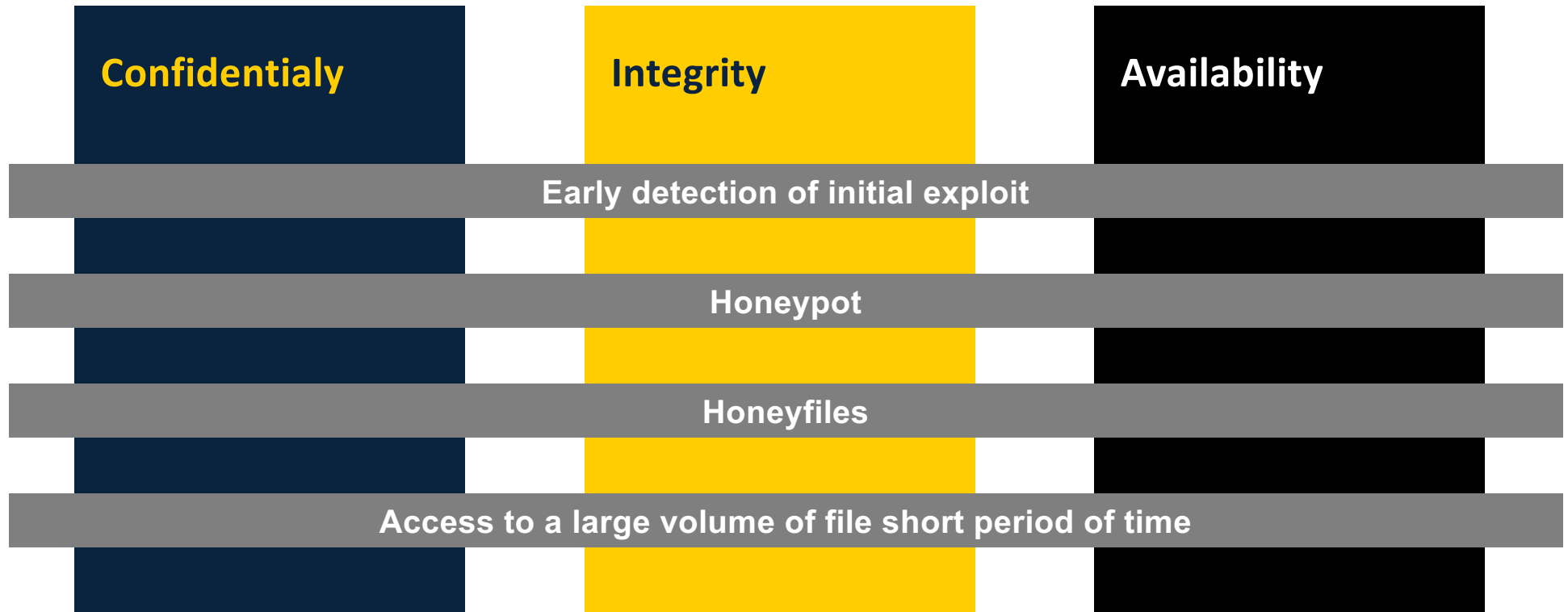
Legacy Software

Gesundheitssektor investiert mehr in die "Pflege" als in die IT

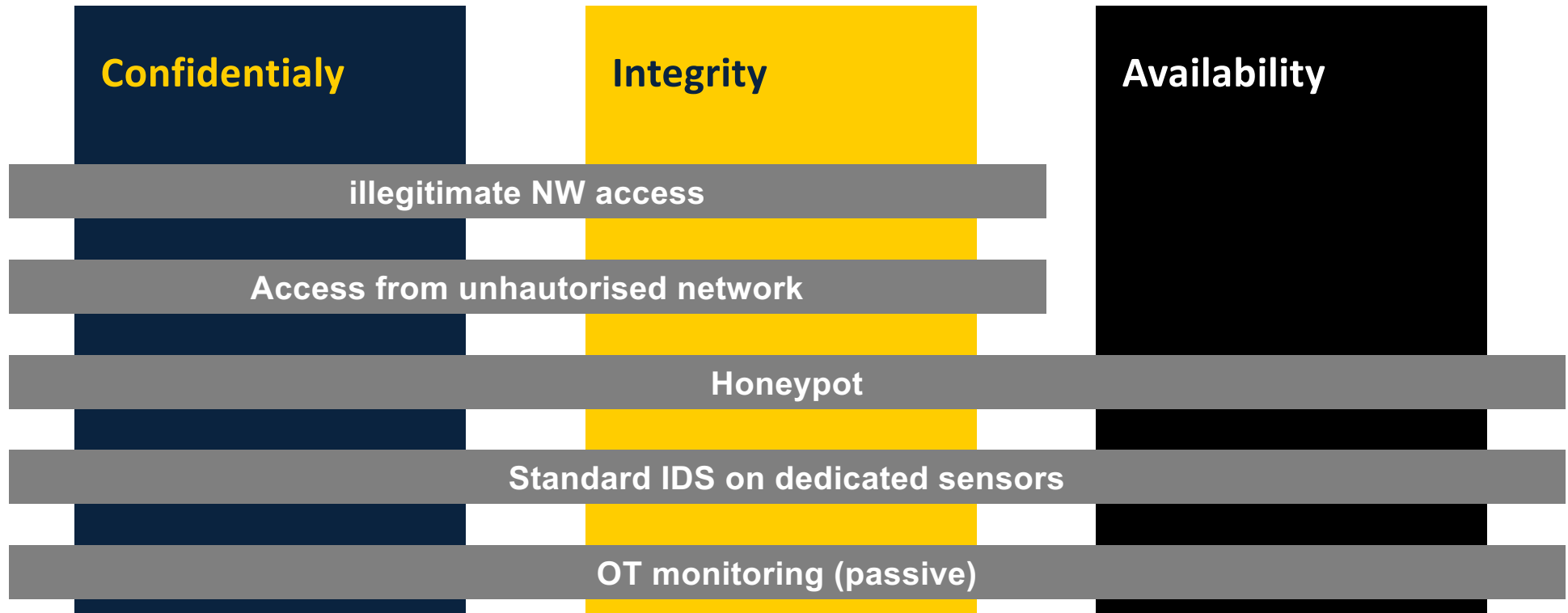
Risk 1 – Insider threats



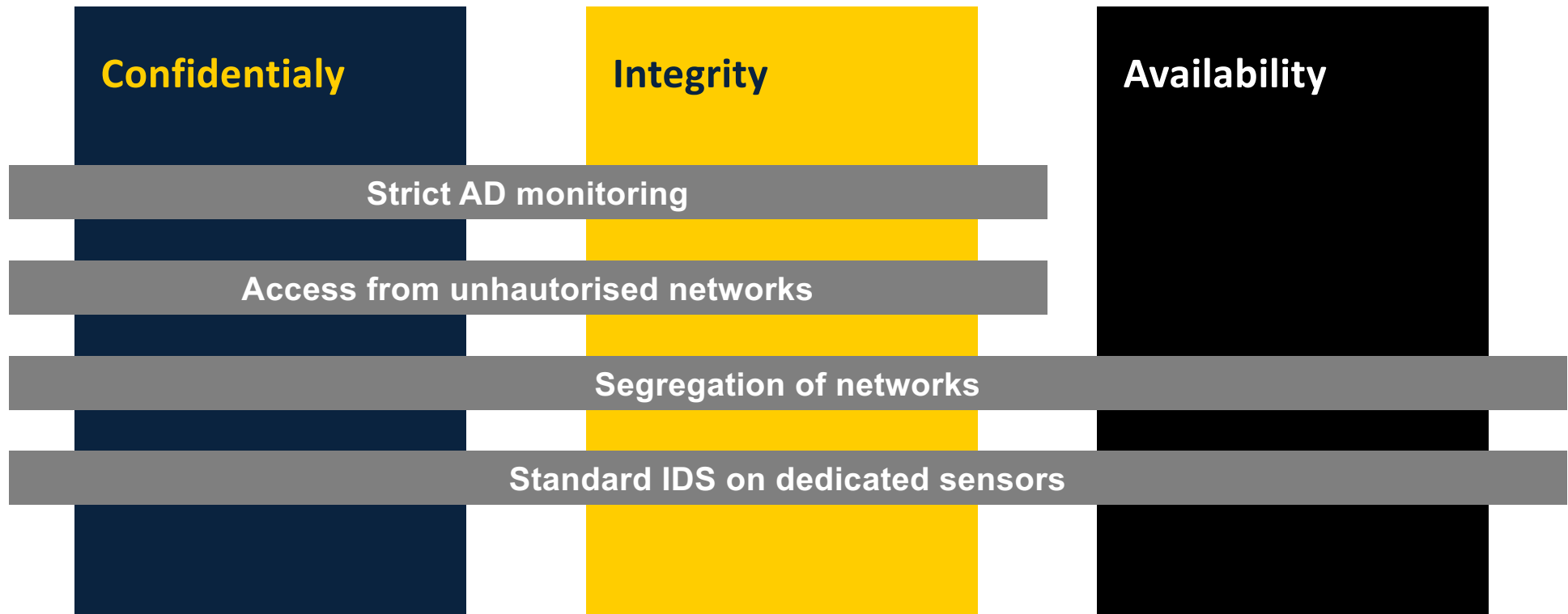
Risk 2 – Ransomware



Risk 3 – Medical devices / OT equipment



Risk 4 – Software legacy



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



**Thank you!
Questions?**



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