

# Cybersecurity im Gesundheitswesen: Angriffserkennung, nicht nur für KRITIS-Häuser

---

**Name**

Christoph Isele



## Christoph Isele



Lead Regulatory Affairs Strategist

Oracle Cerner

[Christoph.isele@cerner.com](mailto:Christoph.isele@cerner.com)

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Warum IT Sicherheit auf einer Datenschutztagung?

- Verfügbarkeit, Integrität, Vertraulichkeit  
gemeinsame Ziele von Datenschutz und IT Sicherheit
- DSGVO Art 32: Sicherheit der Verarbeitung
- Vertrauen der Bürger / Patienten in die Verarbeitung von Gesundheitsdaten

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Aktuelle Herausforderung

## ✓ Viren, Würmer

- Virens scanner, Anti Malware

## !! Ransomware

- Schaden
- Wissen
- Geld

## Kommerzialisierung

## Malware as a Service

## Ethische Bedenken ??

## Angriffsfläche

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

ur documents, photos, databases and other important files have been e  
t  
n  
e p  
s  
can  
struc  
re

aa 76

**All your important files are encrypted!**

Your personal files (including those on the network disks, USB, etc) have been encrypted: photos, videos, documents, etc. Click "Show files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was made using a unique strongest RSA-2048 public key generated for this computer. To decrypt files you need to acquire the private key. The only copy of the private key, which will allow you to decrypt your files, is located on a secret TOR server in the Internet; the server will eliminate the key after a time period specified in this window. Once this has been done, nobody will ever be able to restore files...

In order to decrypt files press button to open your personal page and follow the instruction.


**File decryption button**

in case of "File decryption button" malfunction use one of public gates:  
<http://iq3ahijcfeont3xx.p0oekds4we39.com> or  
<https://iq3ahijcfeont3xx.tor2web.blutmagie.de>

Use your Bitcoin address to enter the site: **1K23HDxnozzdfnzgmLeGGUkwyqpPmucnQS**

**Click to copy Bitcoin address to clipboard**

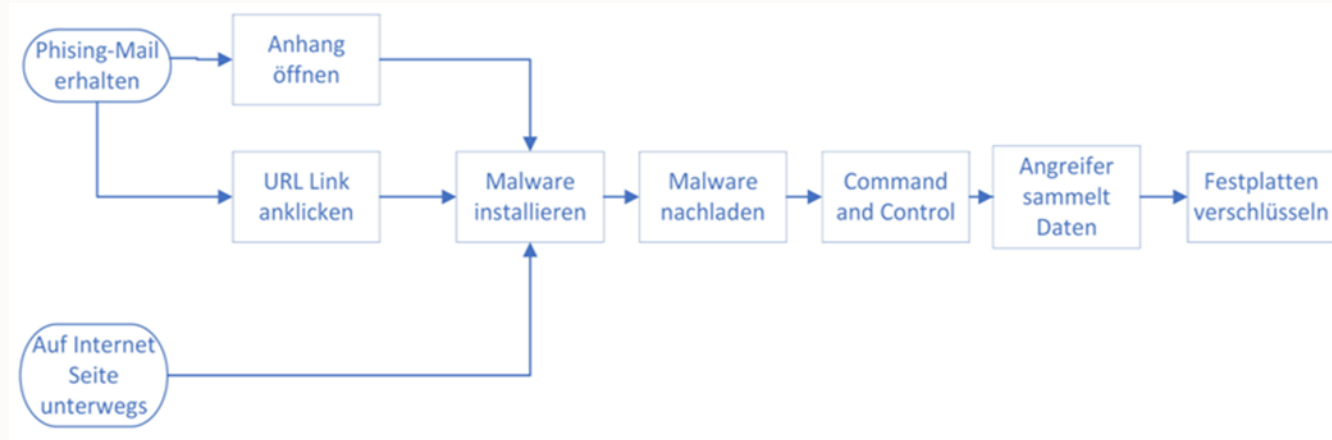
if both button and reserve gates not opening, please follow these steps:  
You must install TOR browser [www.torproject.org/projects/torbrowser.html.en](http://www.torproject.org/projects/torbrowser.html.en)  
After installation, run the browser and enter address [iq3ahijcfeont3xx.onion](http://iq3ahijcfeont3xx.onion)  
Follow the instructions on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

 **There is no other way to restore your files except of making the payment. Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.**

**Show files** **Time left: 95:57:28** **Enter Decrypt Key**

At the moment, the cost of private key for decrypting your files is 0.6 BTC ~=  
Your Bitcoin address for payment: 1K23HDxnozzdfnzgmLeGGUkwyqpPm

# Aktuelle Herausforderung: Mehrstufiger Angriff



## Erster Zugang

- Social Engineering
- Phishing

## Seitliche Bewegung (Lateral Movement)

Rechteauserweiterung,  
„Command and Control“

Persistenz  
(Aufrechterhalten des Zugriffs)

## Kopieren von Daten (Exfiltration)

Verschlüsseln von  
Dateien

## Lösegeldforderung Schädigung des Opfers

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Backup and Disaster Recovery



Hilfreich, wenn eine **nicht kompromittierte Kopie** vorhanden ist und **die Inhalte wiederhergestellt** werden können

Hilft nicht nur bei **Ransomware-Angriffen!**

Hilft nicht bei **Datendiebstahl!**

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Envia which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Envia entities have been made where an integration has not already occurred.



# Angriffserkennung - gesetzliche „Motivation“



## **Für Betreiber einer kritischen Infrastruktur (BSIG):**

- Die Verpflichtung ... angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung.
- Orientierungshilfe des BSI
- Der Nachweis erfolgt indirekt über die routinemäßigen Auditberichte.

## **Andere Krankenhäuser (vgl SGB V §75c):**

- Krankenhäuser sind verpflichtet nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu treffen

# Hilfsmittel

---

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.





# B3S „Medizinische Versorgung“

- Enthält die Konkretisierung für die Medizinische Versorgung
- Version 1.2 verfügbar
- Zur Feststellung der Eignung gemäß § 8a Abs. 2 BSI-Gesetz eingereicht



Branchenspezifischer Sicherheitsstandard  
„Medizinische Versorgung“

Gesamtdokument

28.06.2022

TLP-Klassifikation: WHITE

Kategorie: öffentlich

Status: zur Feststellung der Eignung gemäß § 8a Abs. 2 BSI-Gesetz eingereicht

Version: 1.2



## 6.13.5 Intrusion Detection / Prevention (ab 1.05.23)

- ANF-0113: Es MUSS ein Erkennungsverfahren zur **Vorbeugung** und Erkennung von nicht autorisierten Aktivitäten und gefährlicher Software im Krankenhausnetzwerk implementiert werden. Hierbei sind insbesondere die KRITIS-Schutzziele BEHANDLUNGSEFFEKTIVITÄT und PATIENTENSICHERHEIT in der Implementierung zu berücksichtigen, um negative Auswirkungen auf die kDL zu vermeiden.
- ANF-0114: An den Perimeter-Schnittstellen SOLLEN Systeme zur Angriffserkennung (wie z.B. IDS/IPS) eingesetzt werden, welche aktiv Bedrohungen von außerhalb des eigenen Netzwerkes blockieren.
- ANF-0115: Diese Systeme SOLLEN unter Beachtung der kritischen Prozesse und der wirtschaftlichen und organisatorischen Aspekten ebenfalls bei internen Übergängen aktiv eingesetzt werden.
- ANF-0116: Es MÜSSEN regelmäßige Überprüfungen auf Schwachstellen des eigenen Netzes erfolgen, um sowohl externe Angriffsmöglichkeiten zu identifizieren, als auch interne Schwachstellen zu erkennen, die aufgrund eines Firewallschutzes (derzeit) nicht zu einer direkten Gefährdung führen.

# Informationssicherheitsmanagementsystem (ISMS)



Managen der Informationssicherheit mittlerweile erwarteter „Standard“

Inventur

- Was habe ich?
- Was möchte ich schützen?

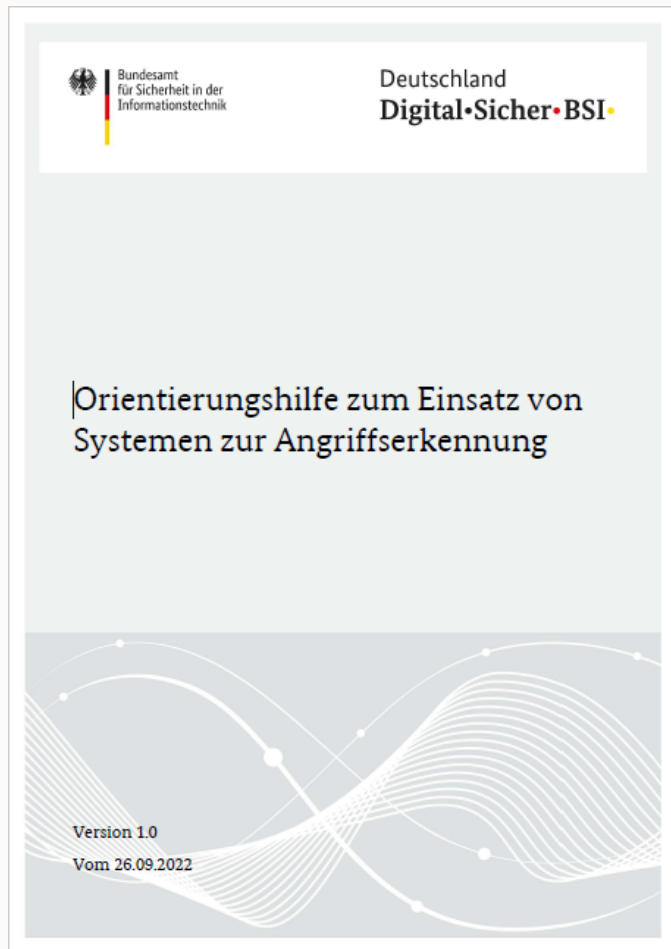
Priorisierung, Clusterung,  
Trennung in „teil autonome“ Bereiche

Automatisierung:

- rechnergestützte Inventarisierung und Übersichten
- Sensoren - was, wo?

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (SzA)



## Orientierungshilfe des BSI

- Unterstützt bei der richtigen Aufstellung, enthält eher organisatorische oder Prozessanforderungen als konkrete Tipps und Ziele
- Version 1.0 veröffentlicht Ende September 2022

In den folgenden Folien sind die wichtigsten Inhalte zusammengefasst.

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Systeme zur Angriffserkennung (SzA)

## Inhalt

1	Überblick .....	4
	Zielsetzung und Adressatenkreis der Orientierungshilfe .....	4
	Aufbau der Orientierungshilfe.....	5
	Weiterführende Informationen .....	5
2	Grundlagen.....	6
	Gesetzlicher Hintergrund.....	6
	Systeme zur Angriffserkennung und ihr branchenspezifischer Einsatz .....	6
3	Anforderungen .....	8
	Protokollierung .....	9
	Planung der Protokollierung .....	9
	Umsetzung der Protokollierung.....	9
	Detektion.....	11
	Planung der Detektion.....	11
	Umsetzung der Detektion .....	11
	Reaktion.....	14
4	Nachweis von Systemen zur Angriffserkennung.....	15
	Das Umsetzungsgradmodell .....	15
	Nachweiserbringung .....	16
5	Glossar .....	17

## Ziele der SzA:

- (frühzeitiges)Erkennen von Cyberangriffen
- Schadensreduktion und -vermeidung

## Ziele der Orientierungshilfe:

- Anhaltspunkt zur Einschätzung der individuellen Umsetzung
- Einheitliche Nachweiserbringung
- Unterstützung bei der Entwicklung der B3S



# Aufgaben: Protokollierung, Detektion und Reaktion

Für die Systeme zur Angriffserkennung ergeben im Hinblick auf deren Funktionalität drei wesentlichen Aufgabenbereiche:



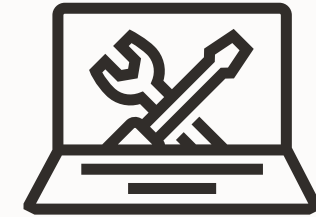
## Protokollierung

Die Systeme müssen fortlaufend Ereignisse protokollieren und diese an zentraler Stelle sammeln



## Detektion

Die gesammelten, (sicherheitsrelevanten) Ereignisse werden analysiert. Dies kann beispielsweise durch Missbrauchserkennung oder Anomalieerkennung erfolgen.



## Reaktion

Idealerweise sollten Systeme zur Angriffserkennung auch Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren. Dies kann sowohl durch technische als auch durch organisatorische Maßnahmen umgesetzt werden.

# Protokollierung (SzA)

Datum/Uhrzeit/User	Anzahl	Externe Identifikation	Objekttext	Unterojekttext	Transaktionsc...	Programm	Modus	Protokollnummer
> 03.01.2023 03:35:18 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050960
> 03.01.2023 03:35:18 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050961
> 03.01.2023 03:35:20 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050962
> 03.01.2023 03:35:20 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050963
> 03.01.2023 03:35:26 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050964
> 03.01.2023 03:35:26 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050965
> 03.01.2023 03:35:40 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050966
> 03.01.2023 03:35:40 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050967
> 03.01.2023 03:35:47 C5004356	3	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050968
> 03.01.2023 03:35:47 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050969
> 03.01.2023 03:35:49 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050970
> 03.01.2023 03:35:49 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050971
> 03.01.2023 03:35:50 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050972
> 03.01.2023 03:35:50 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050973
> 03.01.2023 03:36:00 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050974
> 03.01.2023 03:36:00 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050975
> 03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050977
> 03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050978
> 03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050979
> 03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050976
> 03.01.2023 03:36:12 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050980
> 03.01.2023 03:38:59 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050989
> 03.01.2023 03:38:59 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	000000000000050990
> 03.01.2023 03:44:53 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	0000000000000501019
> 03.01.2023 03:44:53 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	0000000000000501020
> 03.01.2023 03:44:55 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051021
> 03.01.2023 03:44:55 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051022
> 03.01.2023 03:45:01 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051023
> 03.01.2023 03:45:01 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051024
> 03.01.2023 03:45:14 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051025
> 03.01.2023 03:45:14 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051026
> 03.01.2023 03:45:22 C5004356	3	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051027
> 03.01.2023 03:45:22 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051028
> 03.01.2023 03:45:23 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051029
> 03.01.2023 03:45:23 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051030
> 03.01.2023 03:45:24 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051031
> 03.01.2023 03:45:24 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051032
> 03.01.2023 03:45:33 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051033
> 03.01.2023 03:45:33 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051034
> 03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051036
> 03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051037
> 03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051038
> 03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051035
> 03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051039
> 03.01.2023 03:48:30 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gateway Runtime Prozesse			SAPMHTTP	Dialog-Betrieb	00000000000005051047

- In der **Planungsphase SOLLTE**, basierend auf den Ergebnissen der Risikoanalyse und in Anbetracht der kritischen Prozesse des Betreibers, eine schrittweise Vorgehensweise für die Umsetzung der Protokollierung geplant werden. Die Schritte **MÜSSEN** dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Umsetzungsphase Protokollierung (SzA)

**Als Mindestanforderung für die Umsetzung der Protokollierung MÜSSEN alle Basisanforderungen von OPS.1.1.5 Protokollierung ...**

- A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung
- A3 Konfiguration der Protokollierung auf System- und Netzebene
- A4 Zeitsynchronisation der IT-Systeme
- A5 Einhaltung rechtlicher Rahmenbedingungen (z.B. DSGVO)

**... und die folgenden Anforderungen erfüllt werden:**

- Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.
- Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.





# Gliederung der Protokolle

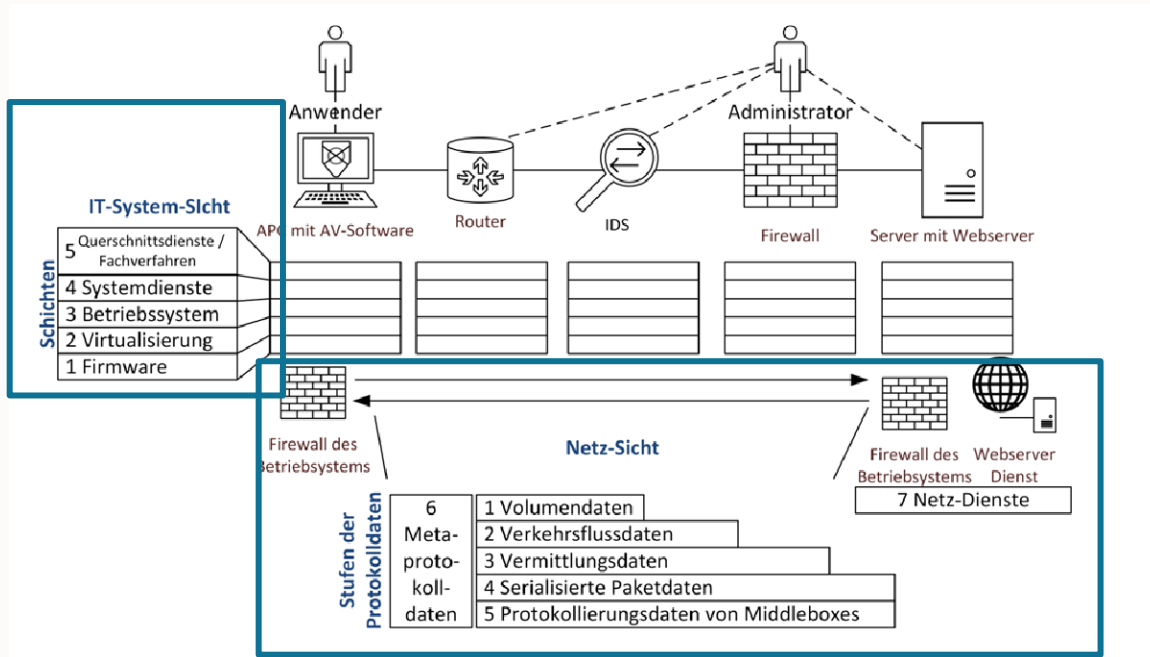


Abbildung 1: Detaillierte Darstellung der Sichten auf Protokollierungsdaten

In der Protokollierungsrichtlinie für die Bundesbehörden nutzt das BSI eine Systematisierung der Protokolle:

- Protokolle in der Netzsicht können Applikationsübergreifend geführt werden und greifen nicht in die Performance ein.
- Abgelehnte Loginversuche, Gewährung kritischer Rechte, sind Beispiele für wichtige sicherheitsrelevante Ereignisse (SRE) auf der Anwendungsebene (im Behörden Deutsch Fachverfahren).

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard\\_BSI\\_Protokollierung\\_und\\_Detektion\\_Version\\_1\\_0a.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf)

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Datenschutz beachten

## Protokollierung und Protokollierungskonzept – Eine Einführung in die Thematik

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.  
Arbeitsgruppe „Datenschutz & IT-Sicherheit“



Deutsche Gesellschaft für Medizinische Informatik, Biometrie und  
Epidemiologie e. V.  
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“



IHE Deutschland e.V.



### Autoren

Ammon, Danny	Universitätsklinikum Jena
Backer-Heuveldop, Andrea	ds² Unternehmensberatung GmbH & Co. KG
Isele, Christoph	Cerner Deutschland GmbH
Kadi, Hasan	VISUS Health IT GmbH
Letter, Michael	5medical management GmbH
Rüdlin, Mark	Rechtsanwalt + Datenschutzbeauftragter
Schlütter, Johannes	net.ter GmbH
Schütze, Bernd	Deutsche Telekom Healthcare and Security GmbH
Wichterich, Eric	ZTG Zentrum für Telematik und Telemedizin GmbH

## Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen

<https://www.gesundheitsdatenschutz.org/html/protokollierungskonzept.php>

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Detektion (SzA)



## Planung der Detektion

- Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden.

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Umsetzung der Detektion (SzA)

**Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 Detektion von sicherheitsrelevanten Ereignissen (SRE) ...**

- A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von SRE
- A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten
- A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse
- A4 Sensibilisierung der Mitarbeiter
- A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion

**... und die folgenden Anforderungen erfüllt werden:**

- Kontinuierliche Überwachung und Auswertung
- Einsatz zusätzlicher Detektionssysteme (netzbasierte Intrusion Detection Systeme)
- Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse
- Auswertung von Informationen aus externen Quellen
- Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal
- Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Umsetzungsempfehlung: MITRE ATT&CK Framework

MITRE   ATT&CK®											
Matrices   Tactics   Techniques   Data Sources   Mitigations   Groups   Software   Campaigns   Resources											
MATRICES	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
	10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques
Enterprise	Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)
PRE	Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Windows	Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	BITS Jobs	Build Image on Host	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
macOS	Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Linux	Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking
Cloud	Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Input Capture (4)	Clipboard Data
Network	Search Closed Sources (2)	Obtain Capabilities (6)	Native API	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage
Containers	Search Open Sources (5)	Stage Capabilities (6)	Serverless Execution	Shared Modules	Create or Modify System Process (4)	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (8)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (2)
Mobile	Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship	Software Deployment Tools	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Process (8)	Debugger Evasion	Device Driver Discovery	Data from Information Repositories (3)
ICS	Search Victim-Owned Websites		Serverless Execution	System Services (2)	Event Triggered Execution (16)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery	Taint Shared Content	Data from Local System
			Trusted Relationship	User Execution (3)	External Remote Services	Hide Artifacts (10)	Hijack Execution Flow (12)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive
			Valid Accounts (4)	Windows Management Instrumentation	Hijack Execution Flow (12)	Impair Defenses (10)	Process Injection (12)	Network Sniffing	File and Directory Discovery	Group Policy Discovery	Data from Removable Media
				Modify Authentication Process (8)	Implant Internal Image	Indicator Removal (9)	Scheduled Task/Job (5)	OS Credential Dumping (8)	Group Policy Discovery	Network Service Discovery	Data from Removable Media
				Office Application Startup (6)	Modify Authentication Process (8)	Indirect Command Execution	Valid Accounts (4)	Steal Application Access Token	Network Share Discovery	Network Service Discovery	Data Staged (2)
				Pre-OS Boot (5)	Office Application Startup (6)	Masquerading (8)	Masquerading (8)	Steal Application Access Token	Network Sniffing	Network Service Discovery	Email Collection (3)
				Scheduled Task/Job (5)	Pre-OS Boot (5)	Modify Authentication Process (8)	Modify Authentication Process (8)	Steal or Forge Authentication Certificates	Password Policy Discovery	Network Service Discovery	Input Capture (4)
				Server Software Component (5)	Scheduled Task/Job (5)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Steal or Forge Kerberos Tickets (4)	Peripheral Device Discovery	Permission Groups Discovery (3)	Screen Capture
				Traffic Signaling (2)	Server Software Component (5)	Modify Registry	Modify Registry	Steal Web Session Cookie	Process Discovery	Process Discovery	Video Capture
				Valid Accounts (4)	Traffic Signaling (2)	Modify System Image (2)	Modify System Image (2)	Unsecured Credentials (8)	Query Registry	Remote System Discovery	
					Valid Accounts (4)	Network Boundary Bridging (1)	Network Boundary Bridging (1)	System Information Discovery	Software Discovery (1)		
						Obfuscated Files or Information (11)	Obfuscated Files or Information (11)				

<https://attack.mitre.org/matrices/enterprise/>

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Envida which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Envida entities have been made where an integration has not already occurred.



# Umsetzungsempfehlung: MITRE ATT&CK Framework

The screenshot shows the MITRE ATT&CK Framework website. The main navigation bar includes: MITRE | ATT&CK, Matrices, Tactics, Techniques, Data Sources, Mitigations, Groups, Software, Campaigns, Resources. A secondary navigation bar includes: MITRE | ATT&CK, Matrices, Tactics, Techniques, Data Sources, Mitigations, Groups, Software, Campaigns, Resources, Blog, Contribute. A banner at the top right states: ATT&CK v13 has been released! Check out the blog post or release notes for more information.

The left sidebar shows the MATRICES menu with categories: Enterprise, PRE, Windows, macOS, Linux, Cloud, Network, Containers, Mobile, ICS. The 'Reconnaissance' matrix is expanded, showing 10 techniques, with 'Phishing for Information' (3) highlighted in a blue box.

The main content area shows the 'TECHNIQUES' section for 'Phishing for Information'. The breadcrumb trail is: Home > Techniques > Enterprise > Phishing for Information. The title is 'Phishing for Information'. Below the title is a dropdown for 'Sub-techniques (3)'. The description states: Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from Phishing in that the objective is gathering data from the victim rather than executing malicious code. It further explains that all forms of phishing are electronically delivered social engineering, and that adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means. It notes that phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: Establish Accounts or Compromise Accounts) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing the identity of the sender which can be used to fool both the human recipient as well as automated security tools. It also mentions that phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., Email Hiding Rules).

On the right side, there is a metadata box for T1598: ID: T1598, Sub-techniques: T1598.001, T1598.002, T1598.003, Tactic: Reconnaissance, Platforms: PRE, Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad\_mz; Philip Winther, Robert Simmons, @MalwareUtkonos; Scott Cook, Capital One; Sebastian Salla, McAfee, Version: 1.2, Created: 02 October 2020, Last Modified: 14 April 2023, and a Version Permalink.

Below the description is the 'Procedure Examples' section, which includes a table:

ID	Name	Description
G0007	APT28	APT28 has used spearphishing to compromise credentials. <sup>[1][12]</sup>
G0128	ZIRCONIUM	ZIRCONIUM targeted presidential campaign staffers with credential phishing e-mails. <sup>[13]</sup>

<https://attack.mitre.org/matrices/enterprise/>

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Reaktion (SzA)



Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 Behandlung von Sicherheitsvorfällen erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Umsetzung der Reaktion (SzA)

Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 Behandlung von Sicherheitsvorfällen erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.

- A1 Definition eines Sicherheitsvorfalls
- A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
- A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
- A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
- A5 Behebung von Sicherheitsvorfällen
- A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen





# Vorsicht bei der Intervention bei Systemen in der Klinik



- Wünschenswert: automatische Reaktion bei „erfolgreicher“ Detektion
- Einige Reaktionen sind für Einrichtungen im Gesundheitswesen kritisch
  - Überführung von Medizinprodukten in einen sicheren Zustand
  - Operative Notwendigkeit des Weiterbetriebs trotz IT technisch schwieriger Situation

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

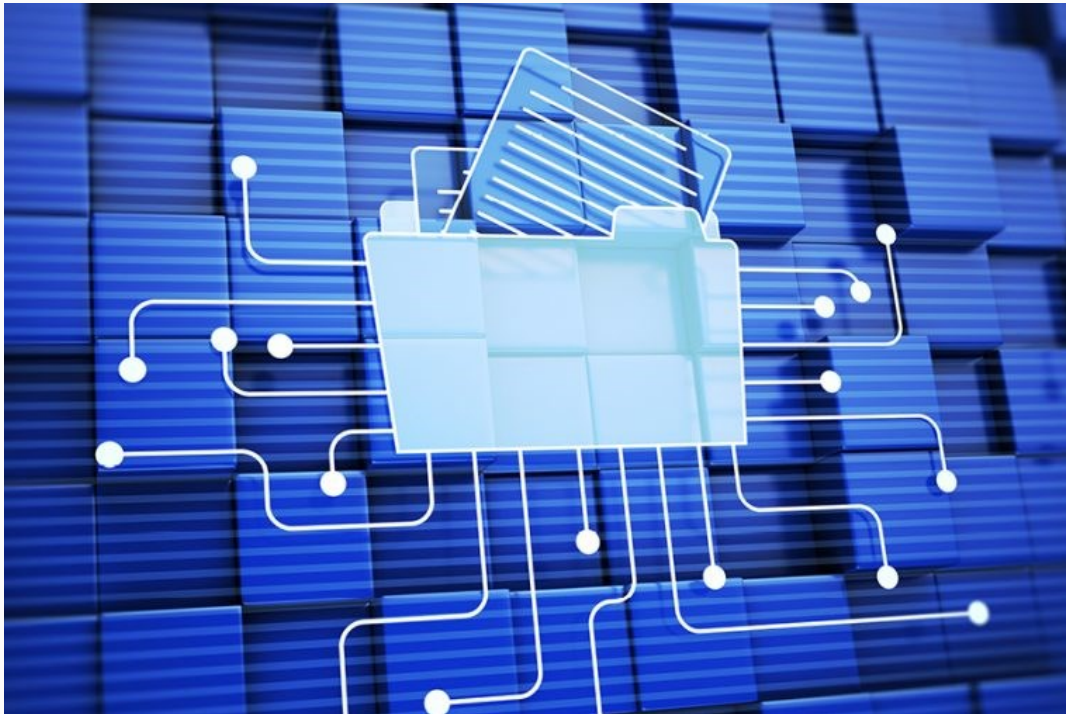
# Werkzeuge und Dienstleistungen

---

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



# Security Information and Event Management (SIEM)

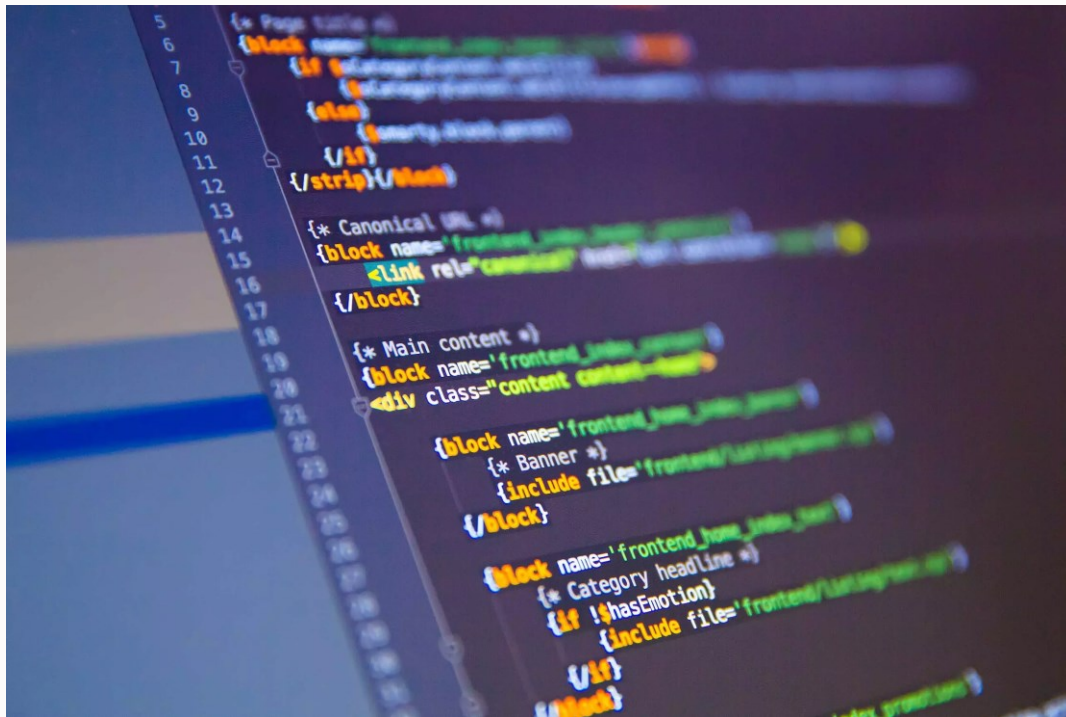


Folgt dem Schema:

- **Sammeln** von Informationen, Events, ...
  - ... sammelt „unternehmensweit“,
  - ... standardisiert die Protokolleinträge
- **Analyse:** z.B.
  - Ereigniskorrelation
  - Mustererkennung
  - Gewichtung der Schwachstellen
  - (Externes Wissen abrufen, einbinden)
- **Reaktion:** z.B.
  - Warnmeldung
  - Gegenreaktionen
  - Automatisierung

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# User and entity behavior analytics (UEBA)



UEBA besteht in der Regel aus drei Schritten:

1. **Analytics** sammelt Daten zu dem, wie ein normales Verhalten von Nutzern aussieht. Anschließend werden statistische Modelle formuliert und angewendet, um ungewöhnliches Verhalten zu erkennen. (Machine Learning).
2. **Integration** mit anderen Sicherheitsprodukten und -systemen, die bereits vorhanden sind, z.B. SIEM für das Einsammeln der Datenpunkte.
3. **Präsentation** der Ergebnisse und der Ausarbeitung einer angemessenen Reaktion.  
Z.B. sofortige Maßnahmen ergreifen, wie automatisch die Netzwerkverbindung für den betreffenden Mitarbeiter bei einem vermuteten Cyberangriffs unterbrechen.

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# Security Operations Center (SOC)



Organisationseinheit, die IT sicherheitsrelevante Leistungen bündelt

- Überwachung „rund um die Uhr“
- Beratung / Management von IT Sicherheitswerkzeugen
- Analysen der Bedrohungen und Bericht zu Vorfällen
- Weitere Leistungen wie:
  - Vordefinierte Meldewege, abgestimmte Reaktionen, Vernetzung mit Dritten (KRITIS)
  - Unterstützung bei Backup / Disaster Recovery
  - Betrieb von Virenscannern etc.

Bedarf und Strategie klären (siehe ISMS)

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.

# „Take home“

- Durch die „Industrialisierung“ auf der Seite der Angreifer steigt das Risiko auch als „einfache“ Einrichtung gehackt zu werden
- Managen Sie ihre Sicherheit: Analyse der eigenen Situation und Feedback zu getroffenen Maßnahmen
- Setzen Sie automatisierte Verfahren zur „Verteidigung“ ein:
  - Auswahl der richtigen Messpunkte/Sensoren: angemessen für die Gefährdungen, interpretierbar
  - Auswahl einiger zu überwachenden Muster: je nach Daten und Verfahren, statistische Ansätze, „baseline“
  - Klärung der Meldekette: Automatische Benachrichtigung, wer welche Maßnahmen in welcher Situation
- Tauschen Sie sich mit vergleichbaren Einrichtungen über Erfahrungen und über die aktuelle Situation aus
- ... und lassen Sie sich keine Angst machen!



# Vielen Dank für Ihre Aufmerksamkeit

---

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.



**ORACLE**  
**Cerner**



# Berücksichtigte Quellen

- [Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung](#)
- [Branchenspezifischer Sicherheitsstandard \(B3S\) für Krankenhäuser - Version 1.2 \(Entwurf zur Eignungsfeststellung eingereicht\)](#)
- [BSI Grundschatz: OPS.1.1.5 Protokollierung](#)
- [BSI Grundschatz: DER.1 Detektion von sicherheitsrelevanten Ereignissen](#)
- [Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen](#)
  - Enthält auch Protokollierungsrichtlinie Bund (PR-B)
  - Rahmendatenschutzkonzept Protokollierung und Detektion

MITRE <https://attack.mitre.org/matrices/enterprise/>

<https://www.gesundheitsdatenschutz.org/html/protokollierungskonzept.php>