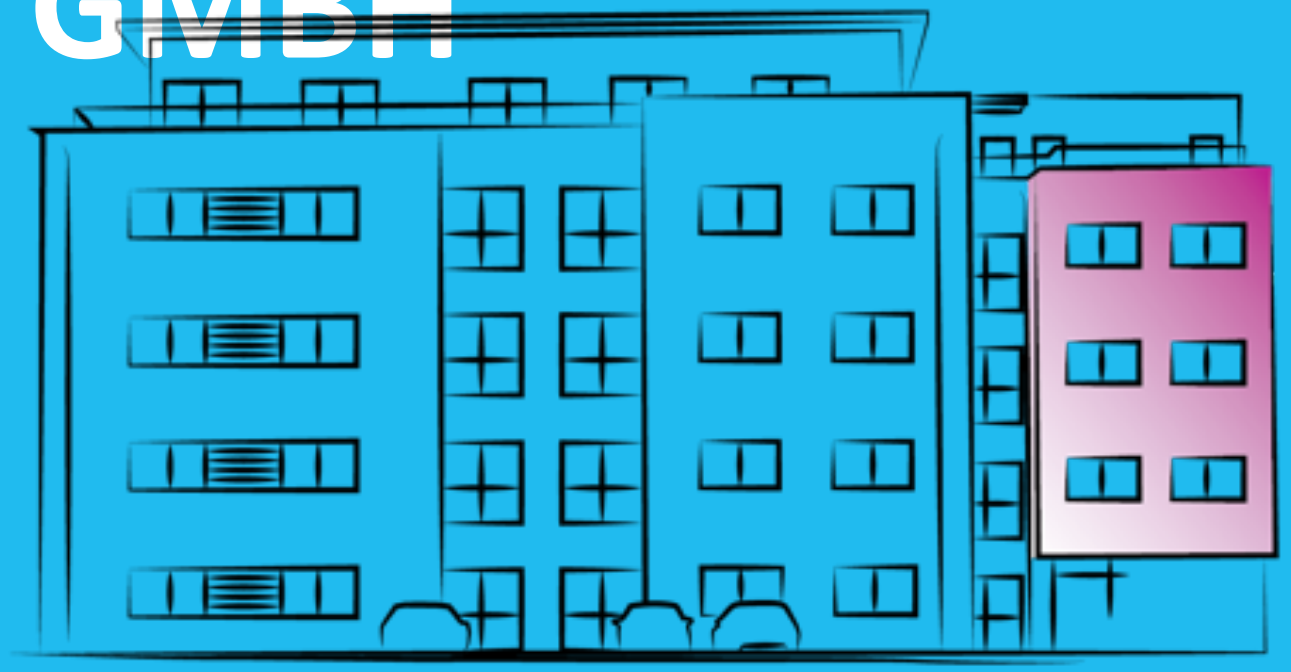
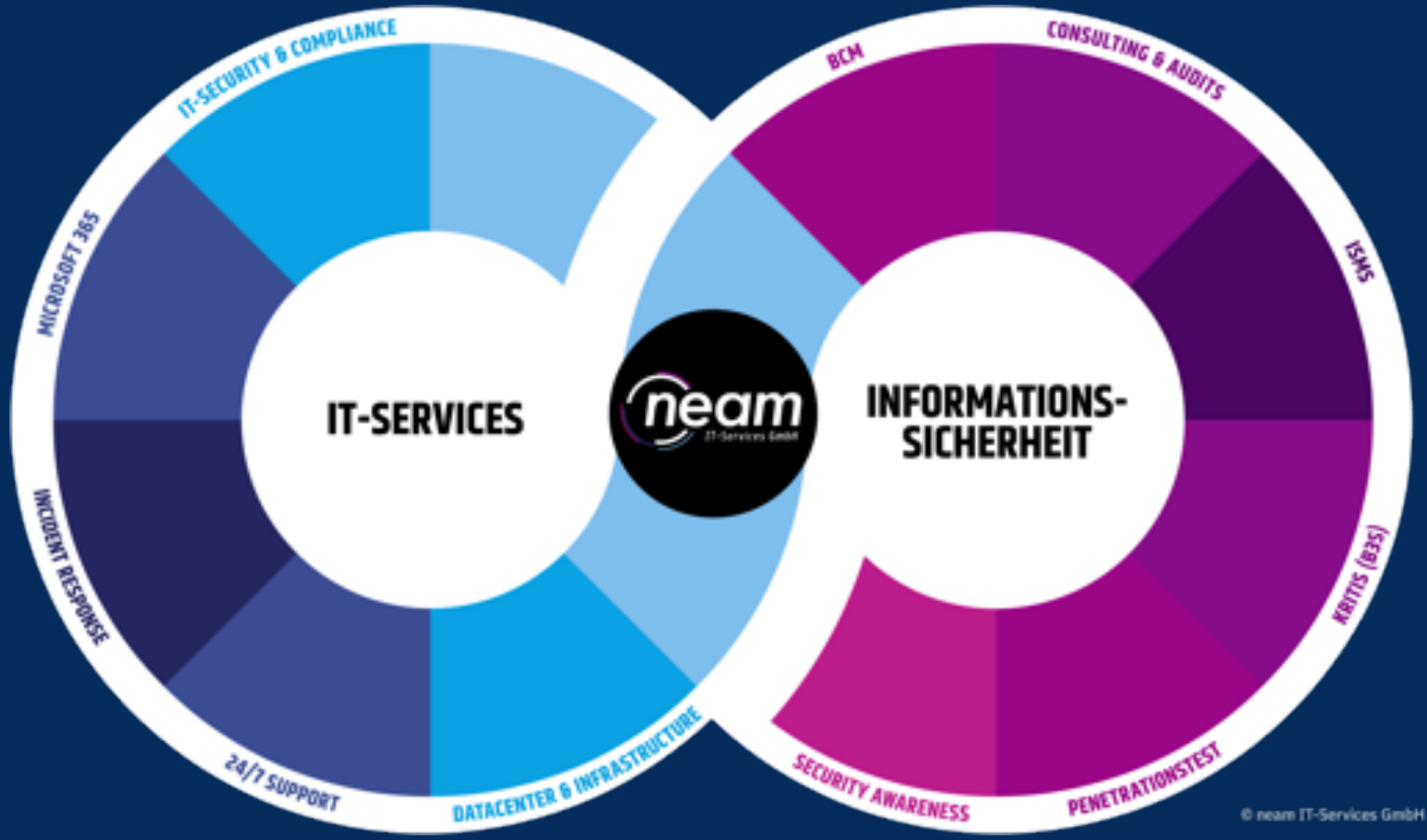

BEING
HUMAN
AND MAKING IT
BETTER

NEAM IT-SERVICES GMBH



- 1996 gegründet
- mehr als 90 Mitarbeiter
- Paderborn & Wiesbaden
- ISO 9001 QM
- ISO 27001 ISMS
- 1. Systemhaus in Deutschland mit IT-GS-Zertifikat in 2005


IT-SECURITY & COMPLIANCE
MICROSOFT 365
INCIDENT RESPONSE
24/7 SUPPORT
DATACENTER & INFRASTRUCTURE
IT-SERVICES
neam
IT-Services GmbH
BCM
CONSULTING & AUDITS
ISMS
KRITIS (B3S)
PENETRATIONSTEST
SECURITY AWARENESS
INFORMATIONS-
SICHERHEIT
© neam IT-Services GmbH

Kurzvorstellung: Vorfall Experte BSI

Kursziele

1. Rahmenbedingungen für den Vorfall-Experten (inkl. Zf. VP)
2. Ablauf des Standardvorgehens
3. Angriffsszenarien und Sofort- bzw. Gegenmaßnahmen
4. Vorfallbearbeitung bei OT & Threat Hunting E-Mail-Header
5. Vor-Ort-Unterstützung: Überblick verschaffen
6. Vor-Ort-Unterstützung: Analyse
7. „Nach einem Vorfall ist vor einem Vorfall"

Themenverteilung und zeitliche Planung

Tag 1

- 1. Rahmenbedingungen für den Vorfall-Experten
- 2. Ablauf des Standardvorgehens

Tag 2

- 3. Angriffsszenarien und Sofort- bzw. Gegenmaßnahmen

Tag 3

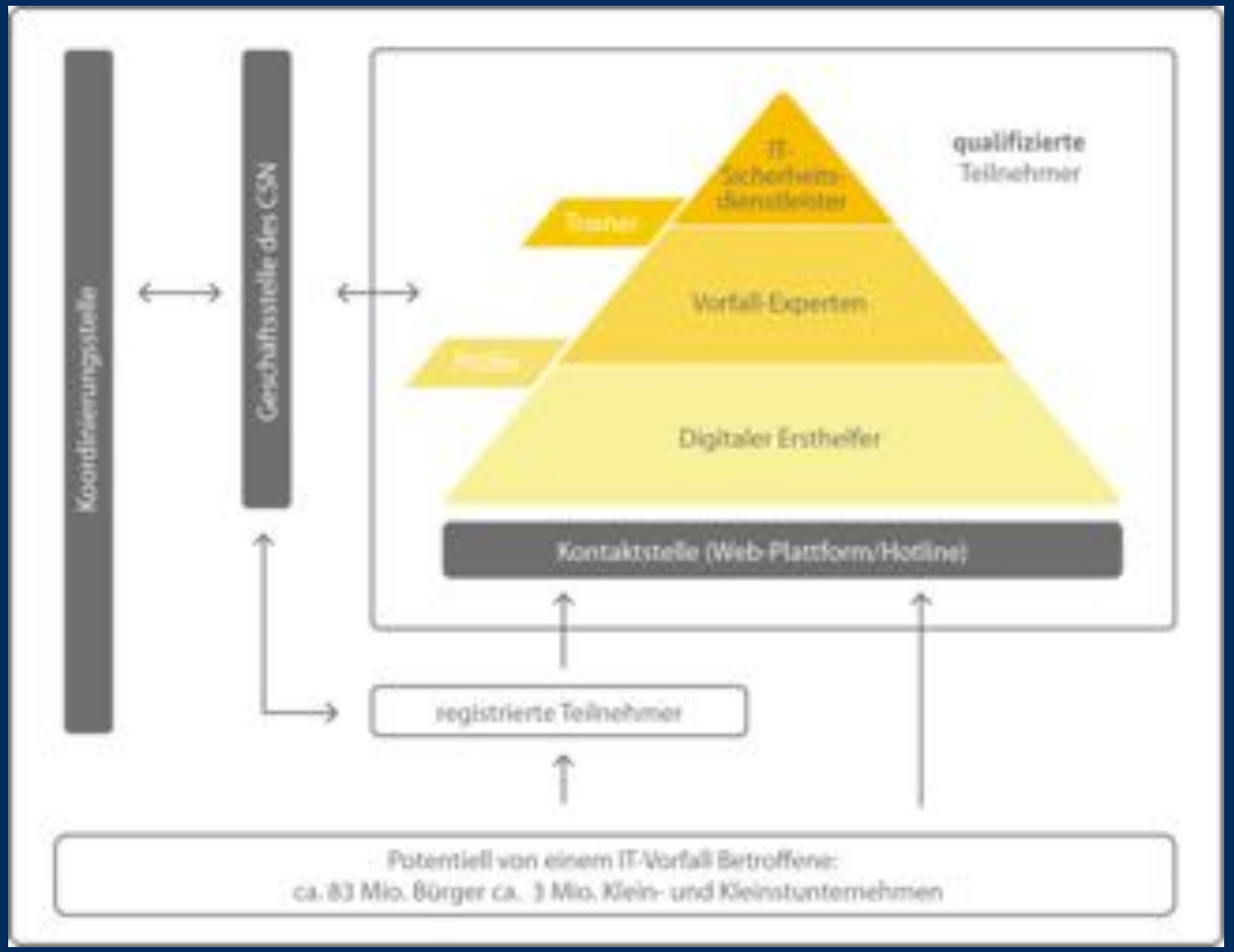
- 4. Vorfallbearb. bei OT 5. Vor-Ort-Unterstützung: Überblick verschaffen
- 6. Vor-Ort-Unterstützung: Analyse
- 7. „Nach einem Vorfall ist vor einem Vorfall"

CSN

- Freiwilliger Zusammenschluss von Experten zur Vorfallbearbeitung
- Reaktive Tätigkeiten mit Erkennung und Analyse von Vorfällen zur Begrenzung von Schäden

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210927_Digitale_Rettungskette.pdf

CSN



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Aufbau/Aufbau_node.html

Digitaler Ersthelfer

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs.html

In 4 Schritten zum Digitalen Ersthelfer

1

Schritt 1

Modul 1.1: Das Cyber-Sicherheitsnetzwerk und die Rolle des Digitalen Ersthelfers (Dauer ca. 20 Minuten)

Als Einstieg in diesen Basiskurs beginnen Sie mit den Grundlagen und der Arbeitsweise des Cyber-Sicherheitsnetzwerks sowie der Tätigkeit des Digitalen Ersthelfers. Sie lernen die Digitale Rettungskette mit ihren einzelnen Gliedern kennen und betrachten die Rollen und Aufgaben der Digitalen Ersthelfer im Cyber-Sicherheitsnetzwerk. Das entsprechende Video auf der rechten Seite, hilft Ihnen somit, einen ersten Einblick zu bekommen, sowie sich ein Verständnis für die Notwendigkeit, die Vorgehensweise und das Tätigkeitsfeld des Cyber-Sicherheitsnetzwerks zu verschaffen.

Modul 1.2: Definitionen und Hilfe bei IT-Störungen (Dauer ca. 15 Minuten)

Nachdem Sie die Grundlagen des Cyber-Sicherheitsnetzwerkes kennengelernt haben, beginnt der eigentliche Inhalt des Basiskurses. Im dazugehörigen Video lernen Sie typische IT-Störungen kennen, wie Sie diese identifizieren und welche Handlungsempfehlungen ausgesprochen werden können.

Eine Übersicht typischer IT-Störungen gibt vorab folgende Grafik:

Ihr neu erlerntes Wissen in Bezug auf IT-Störungen können Sie im folgenden Selbsttest erproben:

HIER GEHT ES ZUM QUIZ:

Hilfsmittel:

1. Online-Kurs für Ersthelfer zur Behandlung von IT-Vorfällen Modul 1.1
1. Online-Kurs für Ersthelfer zur Behandlung von IT-Vorfällen Modul 1.2

Digitaler Ersthelfer

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210712_Leitfaden_Digitaler_Ersthelfer.pdf?__blob=publicationFile&v=8

Verhalten bei Kontaktaufnahme

Grundsätzlicher Ablauf

1. Erfassen

2. Analysieren

3. Bewerten

Digitaler Ersthelfer

Wer ruft an? In welchem Umfeld wird sich bewegt? (KMU oder privat)

Was ist geschehen? Welche Auswirkungen sind spürbar?

Welche IT-Systeme bzw. welche Prozesse sind betroffen?

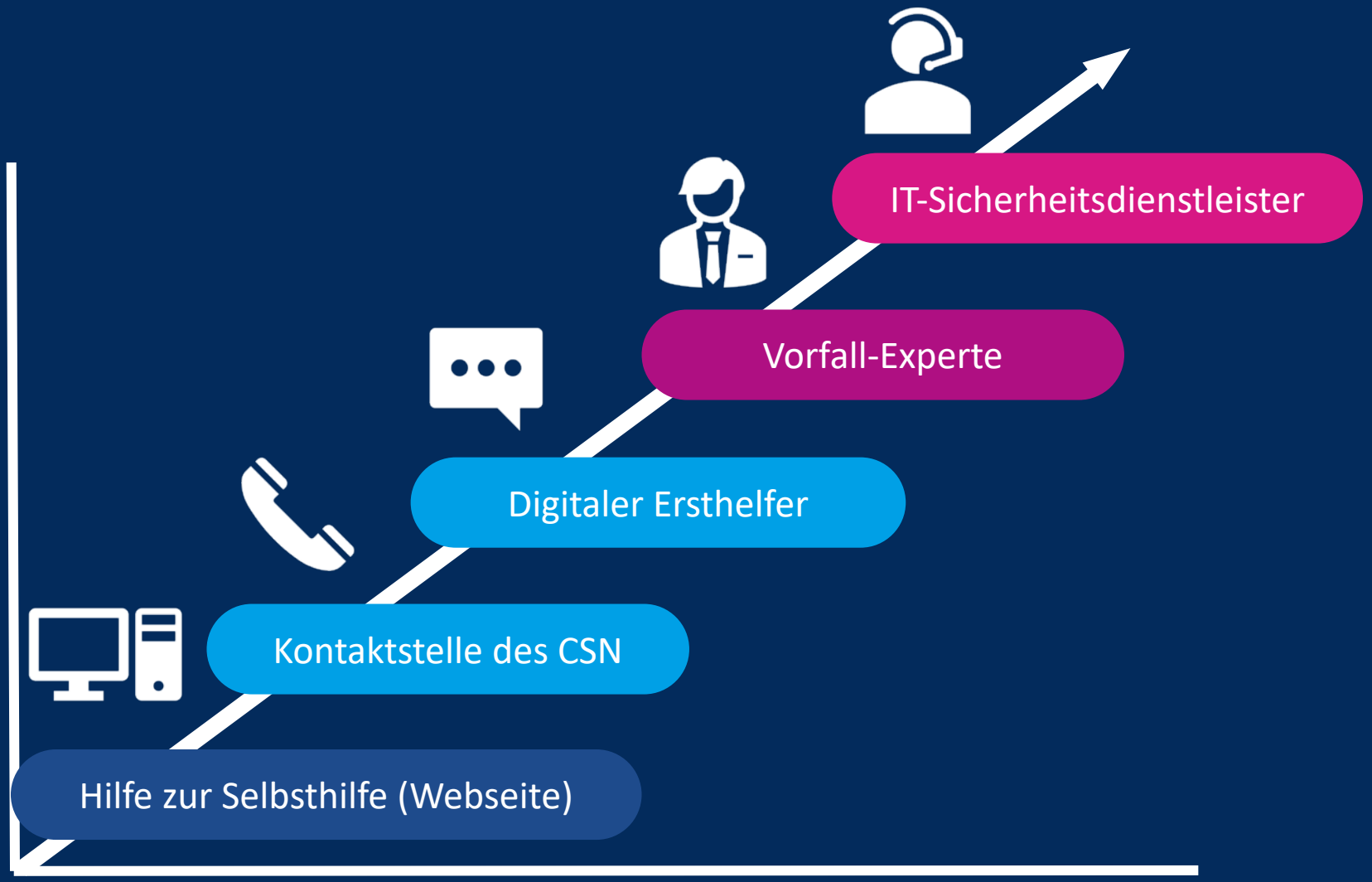
Sind Externe bzw. Dritte von dem IT-Sicherheitsvorfall betroffen? (z. B. Partner oder Kunden)

1. Differenzierung

IT-Störung

IT-Sicherheits-vorfall

Überblick über die digitale Rettungskette



Lust auf einen abenteuerlichen Vorfall?

Besser nicht, daher:

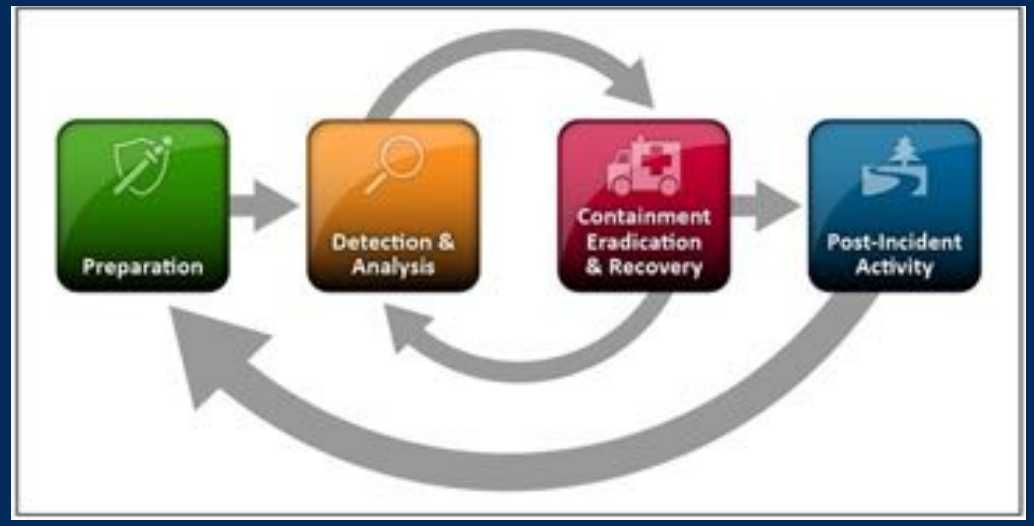
> Abenteuer sind nur schlechte Planung.
>
> ~ Roald Amundsen

Welcher Incident-Response Life Cycle passt zu uns?

-IR Life Cycle -

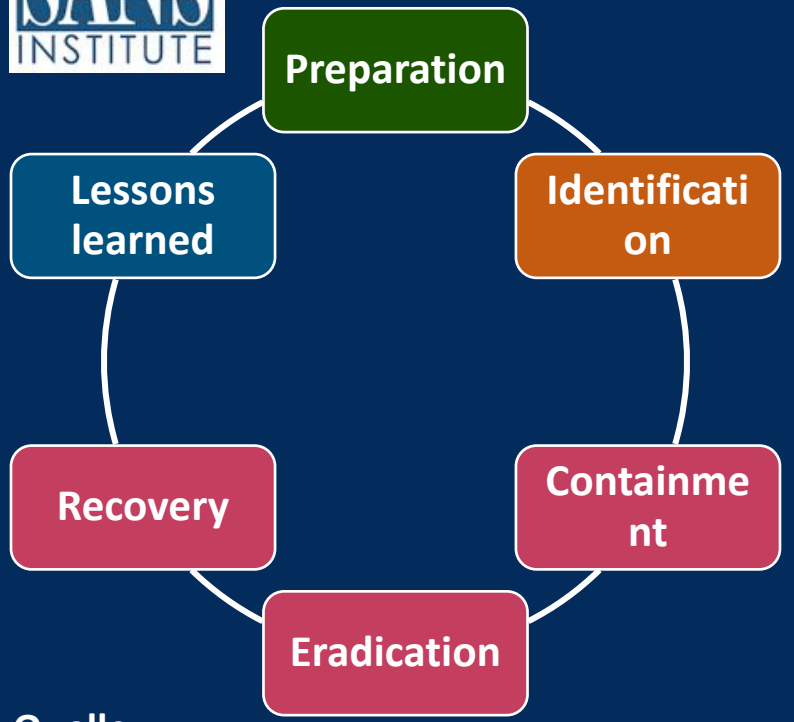
IR Life Cycle

NIST
National Institute of Standards and Technology



Quelle:
NIST - Computer Security Incident Handling Guide (NIST.SP.800-61r2)

SANS INSTITUTE



Quelle:
SANS Institute - Incident Handler's Handbook

IR Life Cycle

BSI Vorfall Experte Kap.2:

Vorbereitung auf potenzielle Vorfälle	↔	Preparation
Identifikation des IT-Sicherheitsvorfalls	↔	Identification
Eindämmung des Schadensausmaßes	↔	Containment
Ermitteln der Ursachen bzw. Auslöser des IT-Sicherheitsvorfalls	↔	Eradication
Wiederherstellung der Systeme	↔	Recovery
Dokumentation des IT-Sicherheitsvorfalls	↔	Lessons learned

Bundesamt für Sicherheit in der Informationstechnik

SANS INSTITUTE

Preparation <>

Vorbereitung auf potenzielle Vorfälle

„Pläne sind nichts,
Planung ist alles.“

neam IT-Services GmbH

Preparation <>

Vorbereitung auf potenzielle Vorfälle

IRP - Verhalten

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte.html

IRP - Dokumentatio des Vorfalls

Meldung IT-Vorfall

Betroffene Firma/Behörde:	
Meldende Person:	
Erreichbarkeit:	
Rückfragen:	
Datum:	
Uhrzeit:	
Vorläufige Klassifizierung durch den Meldenden:	☐ - Missbräuchliche Inhalte *(Spam, Belästigung, Gewalt...)* ☐ - Schadcode *(Ransomware, Virus, Trojan, Spyware)* ☐ - Informationsbeschaffung *(Scanning, Sniffing, Social engineering)* ☐ - Einbruchsversuche *(Exploiting, Login attempts, New attack signat.)* ☐ - Intrusion *(Privileged acc. comp., unprivileged acc. comp., ...)* ☐ - Verfügbarkeit *(DoS, DDoS, Sabotage)* ☐ - Informationssicherheit *(Unauthorized access, Unauthor. modification)* ☐ - Betrug *(Unauthorized use of resources, Copyright, Masquerade)* ☐ - Sonstige *(Alle Vorfälle, die nicht in eine der Kategorien passen)*
Sachverhalt & Leitfragen	☐ - Screenshots vorhanden?
1. **Was** ist geschehen?	
2. **Wo** ist es passiert?	
3. **Welche** Systeme/Netze sind betroffen?	
4. **Wann** ist es passiert?	
5. **Wie** ist es passiert?	

Zu melden an:
BSI IT-Lage- und Analysezentrum
[illegible]@bsi.bund.de
022899 9582 -5110 oder -5499

Preparation <>
Vorbereitung auf potenzielle Vorfälle

https://www.it-planungsrat.de/fileadmin/beschluesse/2017/Beschluss2017-04_Leitlinie-Cybersicherheit-Anlage-1.pdf

IRP – Reaktion ?

Vorfall Klasse
Missbräuchliche Inhalte
Schadcode
Informationsbeschaffung
Intrusion Attempts
Intrusion
Verfügbarkeit
Informationssicherheit
Betrug
Sonstige

Preparation <>

Vorbereitung auf potenzielle Vorfälle

https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

Sind Sie bereit für den ersten IT-Sicherheitsvorfall?

Ohne angemessene Vorbereitungen und einem überprüften Reifegrad zur Vorfallbewältigung (Incident Readiness) wird es dem Angreifer leicht fallen eine Umgebung zu infiltrieren, sich lateral in ihr zu bewegen und eine dauerhafte Persistenz aufzubauen.

Preparation

Vorbereitung auf potenzielle Vorfälle

Identification <>

Identifikation des IT-Sicherheitsvorfalls

Finding Evil

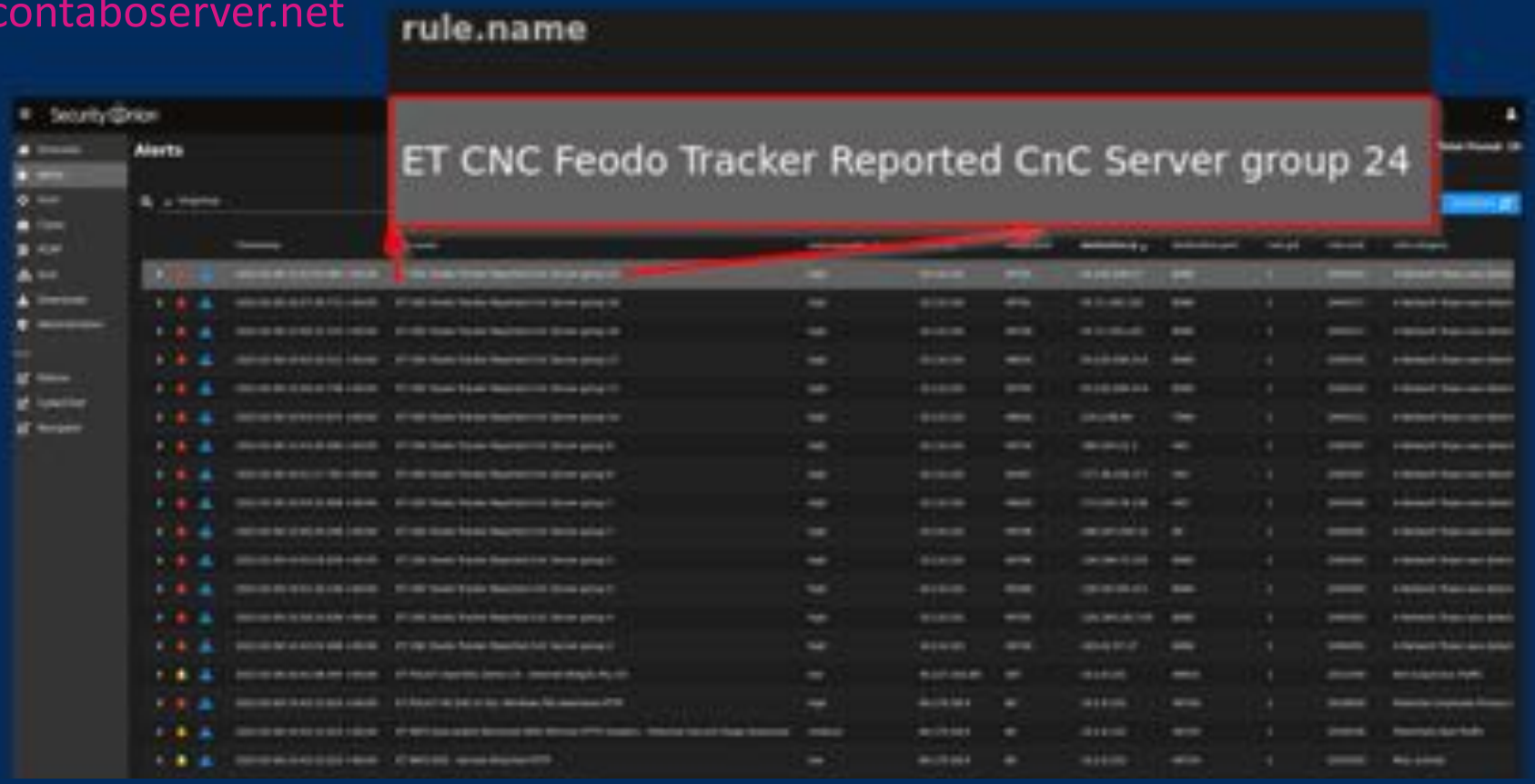
Ungewöhnliche Ports:

Malware kommuniziert häufig mit einem Tor-Server über das Tornetzwerk, der auf dem lokalen Host über den TCP-Port 9050 lauscht.

Ungewöhnliche Verbindungen:

Emotet Epoche 5 mit SecurityOnion – connecting to:

vmi464590.contaboserver.net



https://blog.securityonion.net/2022/02/quick-malware-analysis-emotet-epoch-5.html

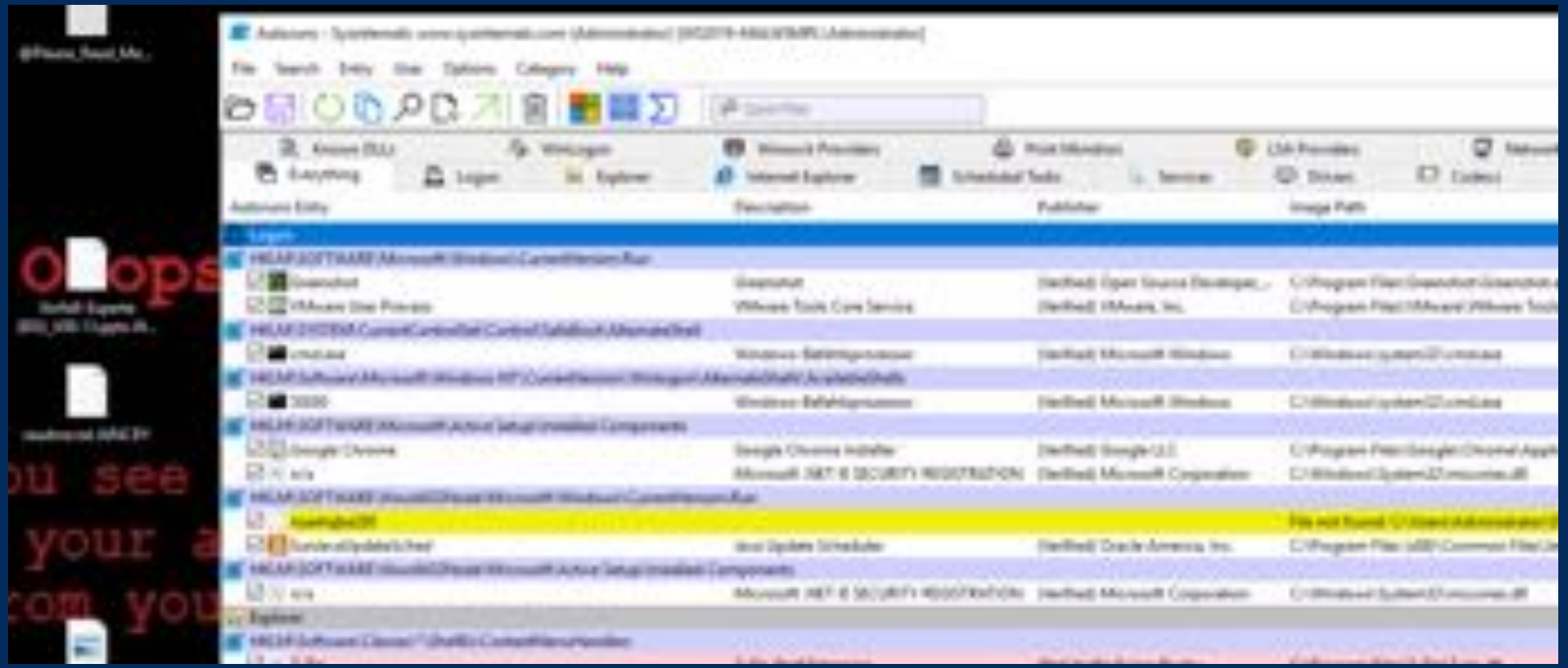
Ungewöhnliche Prozesse:

Ungewöhnliche Prozesse welche sich als svchost.exe tarnen können bspw. mit einer wmic Abfrage erkannt werden. Dazu vergleicht man die PID mit der PPID.

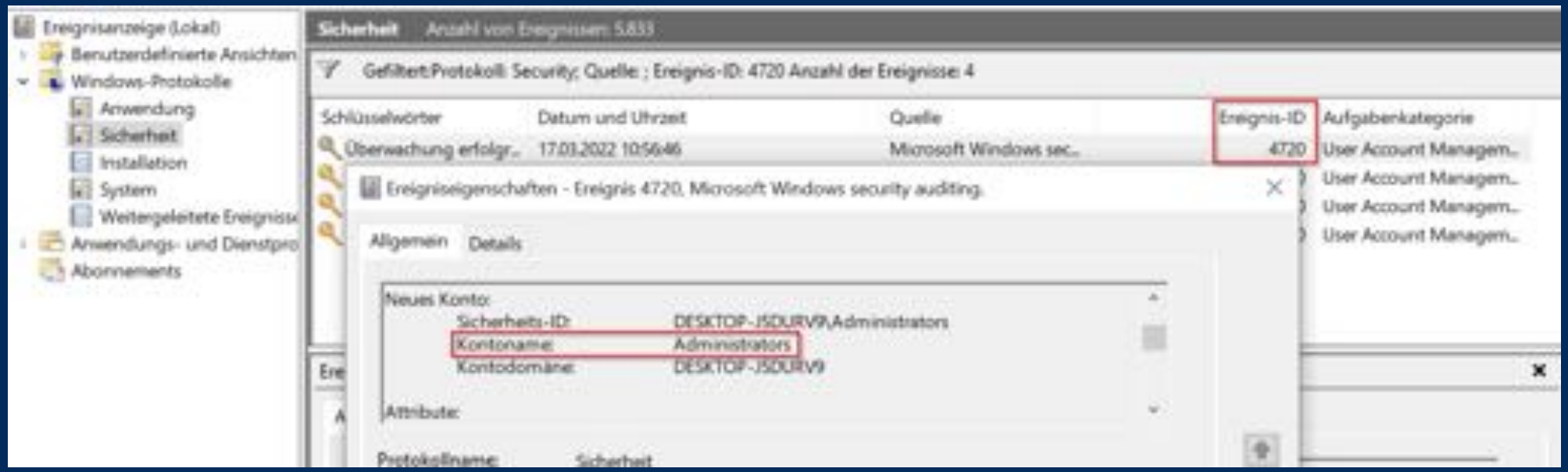
```
wmic process where name="svchost.exe" get name, processid, parentprocessid, commandline
```

```
C:\Users\Administrator>wmic process where name="svchost.exe" get name, processid, parentprocessid, commandline
CommandLine                                                                    Name         ParentProcessId  Proces
C:\Windows\system32\svchost.exe -k DcomLaunch -p -s PlugPlay                   svchost.exe  680              828
C:\Windows\system32\svchost.exe -k DcomLaunch -p                               svchost.exe  680              852
C:\Windows\system32\svchost.exe -k RPCSS -p                                    svchost.exe  680              968
C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM                        svchost.exe  680              1016
C:\Windows\System32\svchost.exe -k termsvcs -s TermService                     svchost.exe  680              724
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService  svchost.exe  680          1040
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc  svchost.exe  680       1104
C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p                    svchost.exe  680              1208
C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog  svchost.exe  680           1248
```

Ungewöhnlicher Autostart:



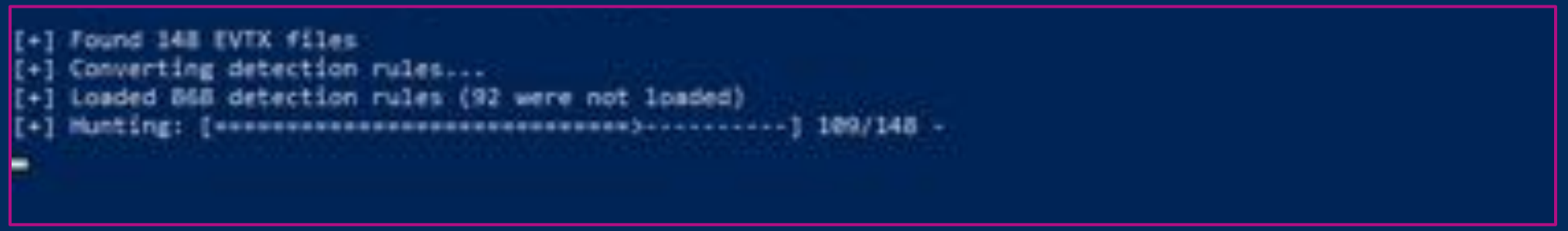
Ungewöhnliche Accounts:



Datenanalyse <>

Ungewöhnliche Windows Event IDs

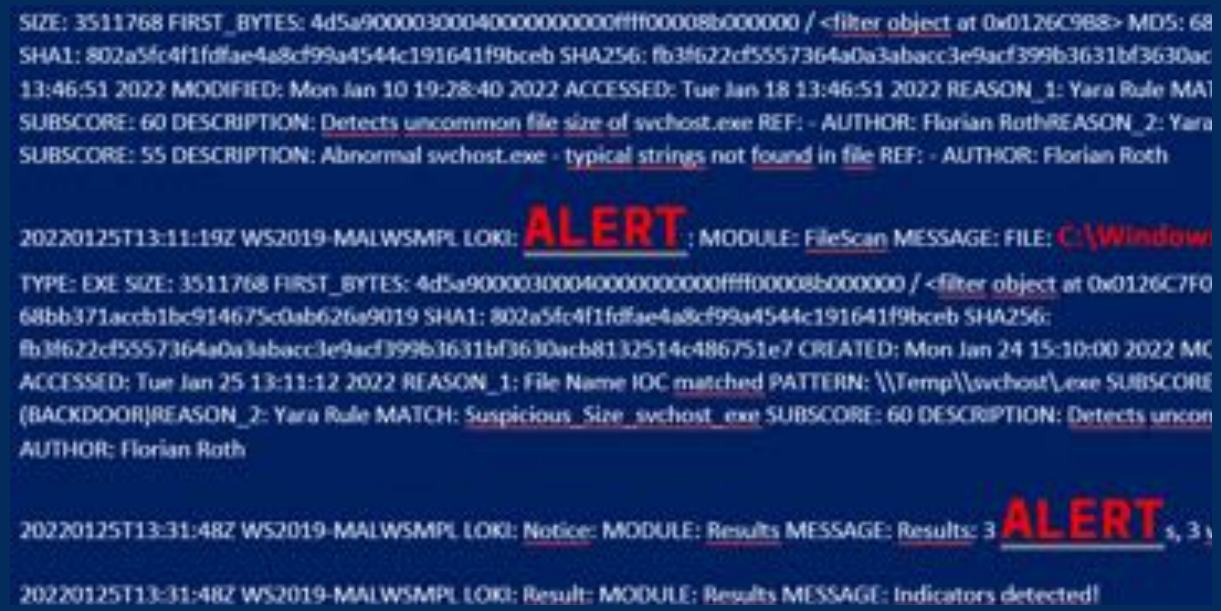
148 Event Logs in wenigen Minuten auswerten



Ungewöhnliche Dateien:

IOC Scanner

Loki:



https://www.nextron-systems.com/loki/

https://www.fireeye.de/current-threats/freeware/ioc-finder.html

Lesetipp:

Ziel der…

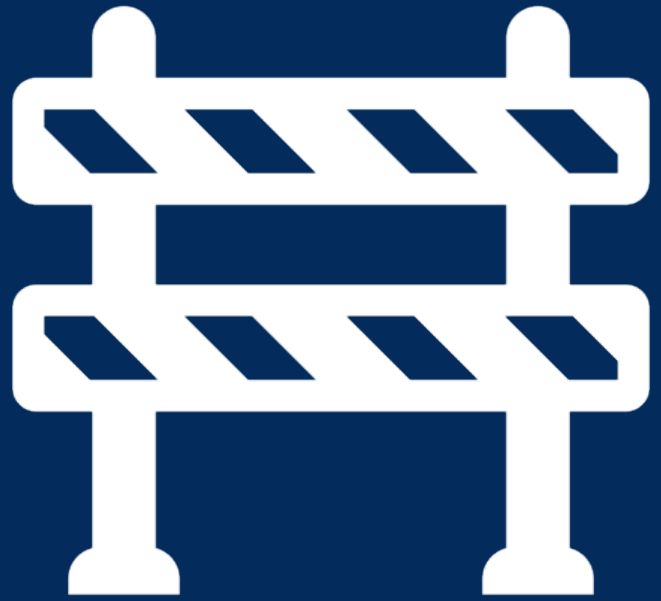
…Ursachenermittlung ist die Beantwortung folgender **5** Fragen:

- **Was** ist geschehen?
- **Wo** ist es passiert?
- **Welche** Systeme/Netze sind betroffen?
- **Wann** ist es passiert?
- **Wie** ist es passiert?

Containment <>

Eindämmung des Schadensausmaßes

Stop the Att4ck



First, Do No Harm!

Ein wichtiger Grundsatz der Medizin gilt auch für die Reaktion auf IT-Sicherheitsvorfälle:
Keinen Schaden verursachen.

https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf

Vorkehrungen Containment

Es sollte klar sein, dass jede interaktive Anmeldung (bspw. RDP) am infizierten Host, dass Potenzial hat, die zugehörigen Anmeldeinformationen offenzulegen weil der Angreifer bereits „mithört“ (mimikatz). Daher sollte zuvor auf Windows Systemen für RDP „Restricted Admin“ eingeschaltet sein!

https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard

Eradication <>

Ermitteln der Ursachen bzw. Auslöser des IT-Sicherheitsvorfalls

Recovery <>

Wiederherstellung der Systeme

Lessons learned <>

Dokumentation des IT-Sicherheitsvorfalls

Detektieren wird essentiell

Die Tendenz moderner Angreifer, vorhandene Werkzeuge und Netzwerkprotokolle zu nutzen, um in Netzwerken von Betroffenen zu persistieren und ihre Rechte weiter zu eskalieren macht die Erkennung von Lateralbewegungen zu einer entscheidenden Fähigkeit für jeden Vorfall-Experten.

Detektieren wird essentiell

Daher verpflichtet u.a. das IT-SiG 2.0 KRITIS-Betreiber – in §8a, Absatz 1a – dazu, Systeme zur Angriffserkennung zu implementieren und zeitnah Maßnahmen zu ergreifen, um diese Angriffe einzudämmen.

https://www.gesetze-im-internet.de/bsig_2009/__8a.html

OT am Beispiel

.stub

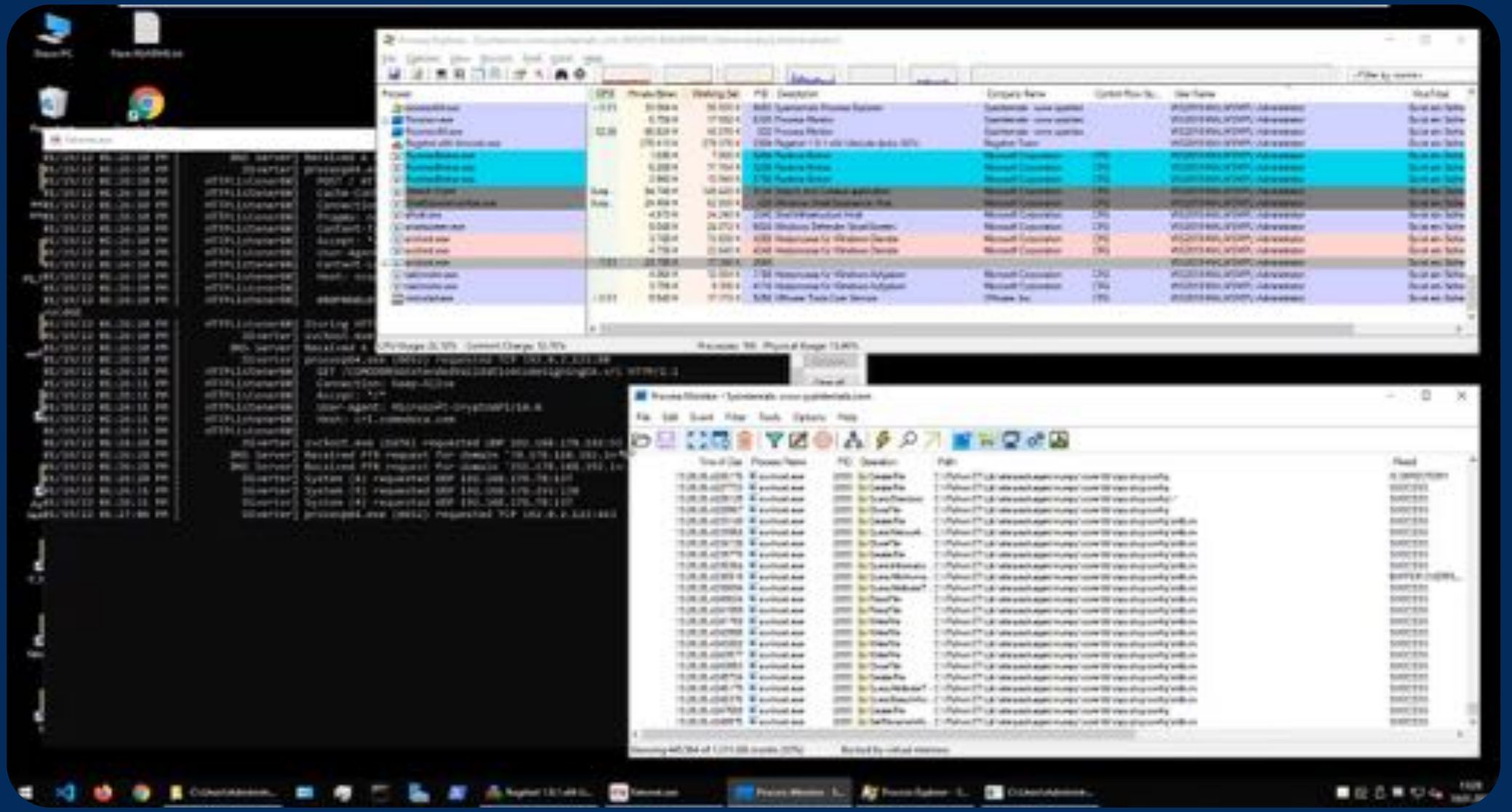
MrxNet.sys

Erster Eindruck – Sie sind also kompetent?

vs.

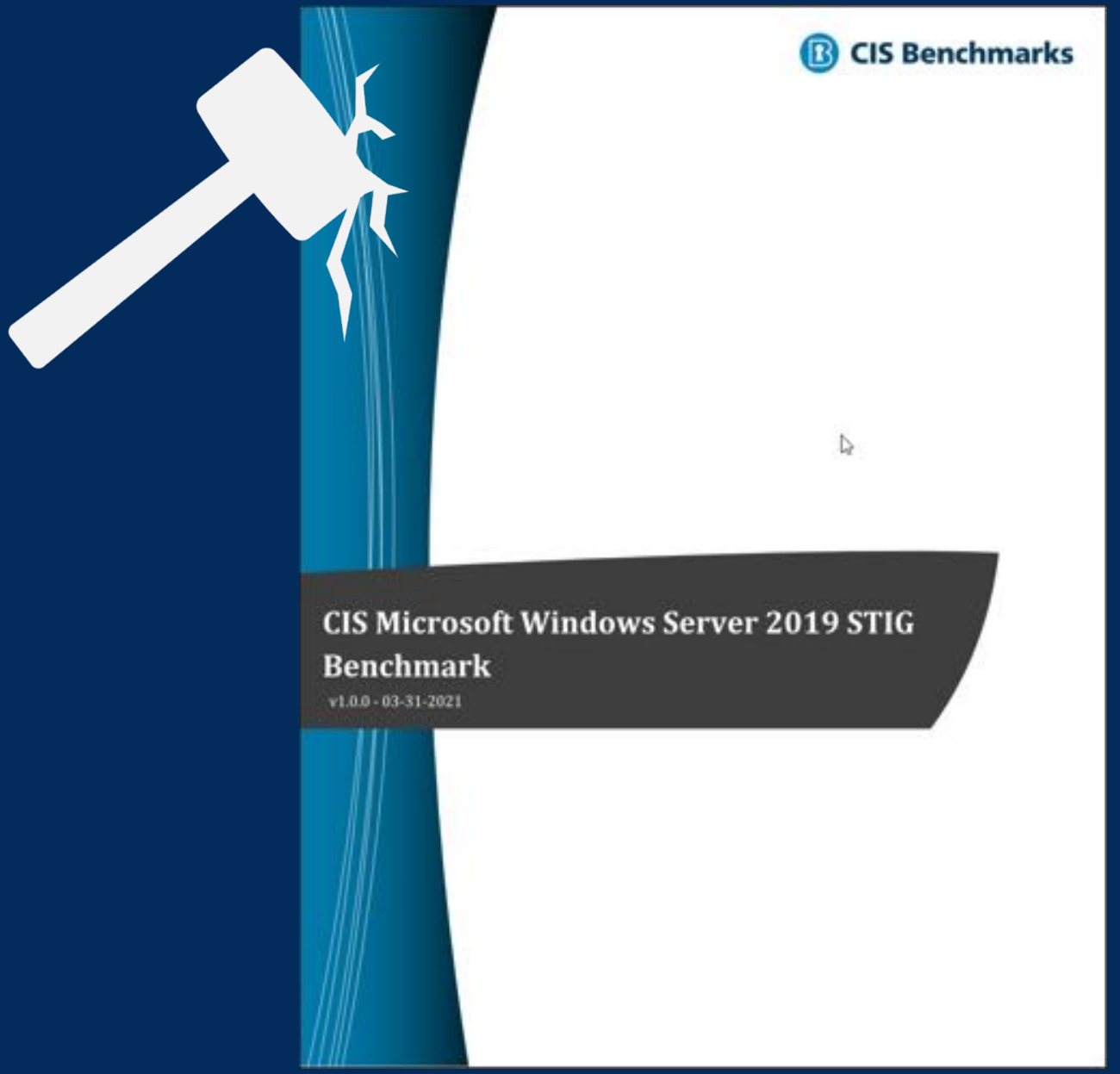
Krisenmanager etablieren

Live Infektion



Hardening

Grundsätzlich sollten die betroffenen Systeme anschließend gehärtet werden.

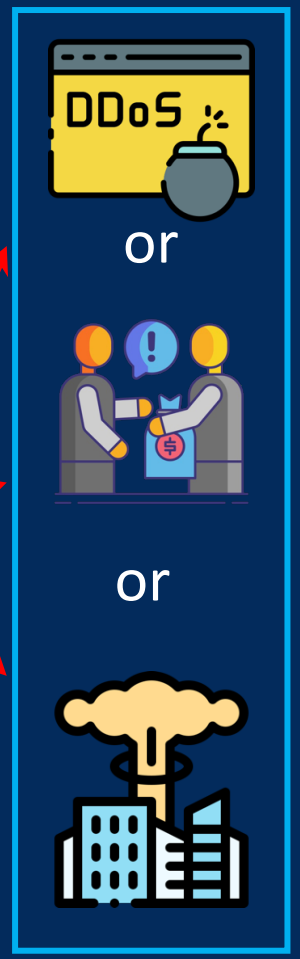


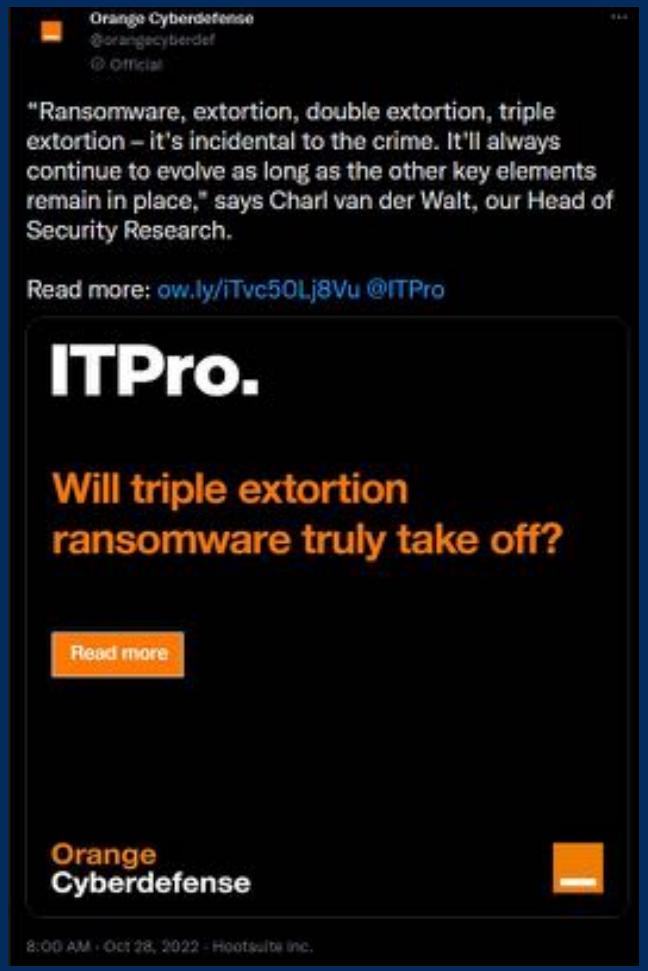
https://www.cisecurity.org/benchmark/microsoft_windows_server/

Prävention Monitoring (am Beispiel PRTG)

aller guten Dinge sind drei

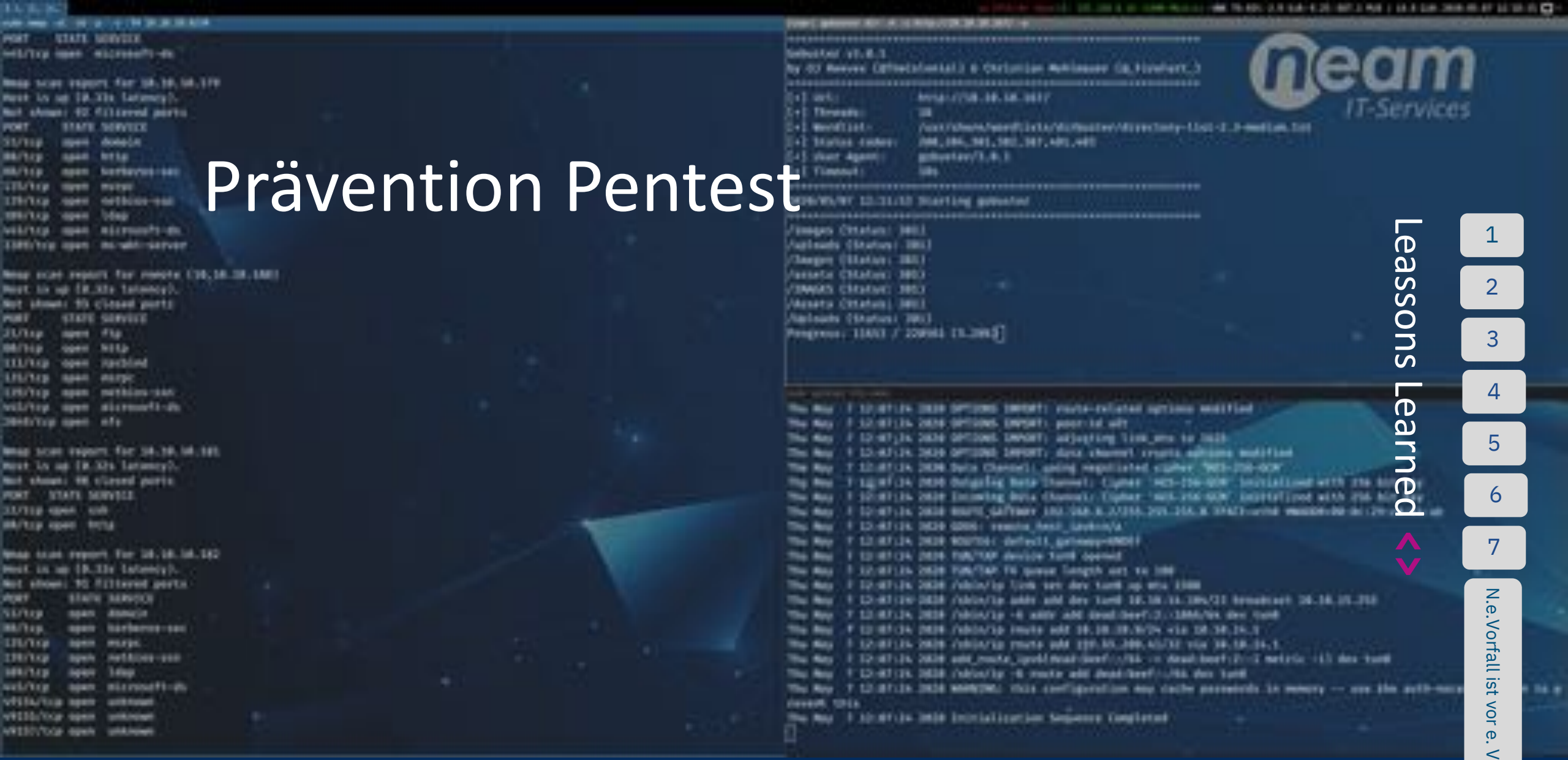
Single
Double
Triple extortion





Leassons Learned

Prävention Pentest



neam IT-Services

Leassons Learned

1
2
3
4
5
6
7

N.e.Vorfall ist vor e. V.

https://www.neam.de/informationssicherheit/penetrationstest/

Präv. Sicherheitskonzept nach BSI 200-2

ISO 27001 zertifiziert
ISO 9001 zertifiziert

SICHERHEITSKONZEPT NACH BSI 200-2

FÜR DIE DIENSTSTELLE XYZ

Dateiname:	
Dokumentenebene:	
Erstellt von:	David Oster | neam.de
Version:	00.00
Status:	

Happy Hunting 4 the evil bit ☺

Vielen Dank für Ihre Aufmerksamkeit