



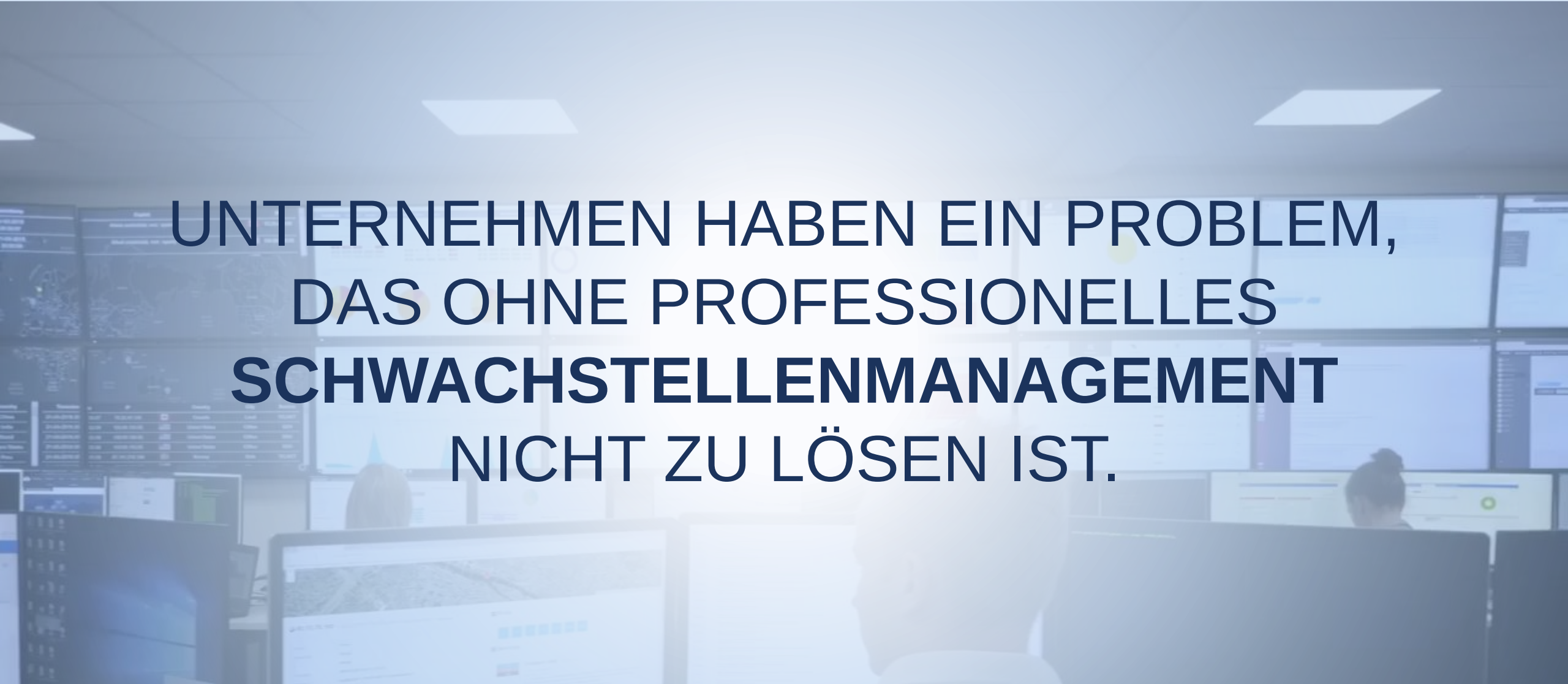
ERIK ZIMMERMANN
Vulnerability Management Specialist

PATCH ME IF YOU CAN:

**WARUM SCHWACHSTELLENMANAGEMENT EIN
MUST-HAVE IST**

7A-406





UNTERNEHMEN HABEN EIN PROBLEM,
DAS OHNE PROFESSIONELLES
SCHWACHSTELLENMANAGEMENT
NICHT ZU LÖSEN IST.

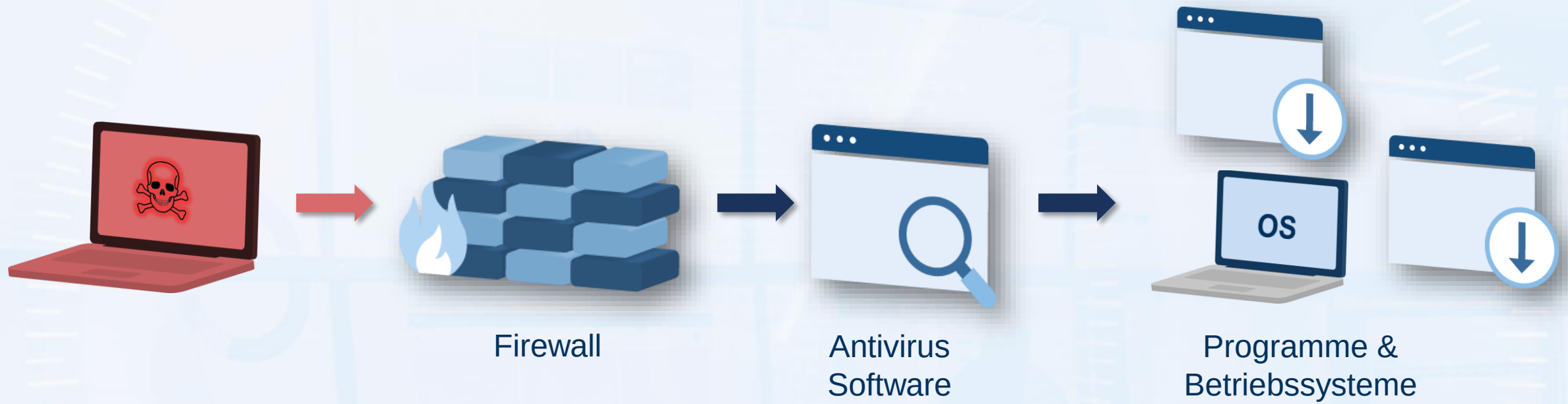
PATCH ME IF YOU CAN

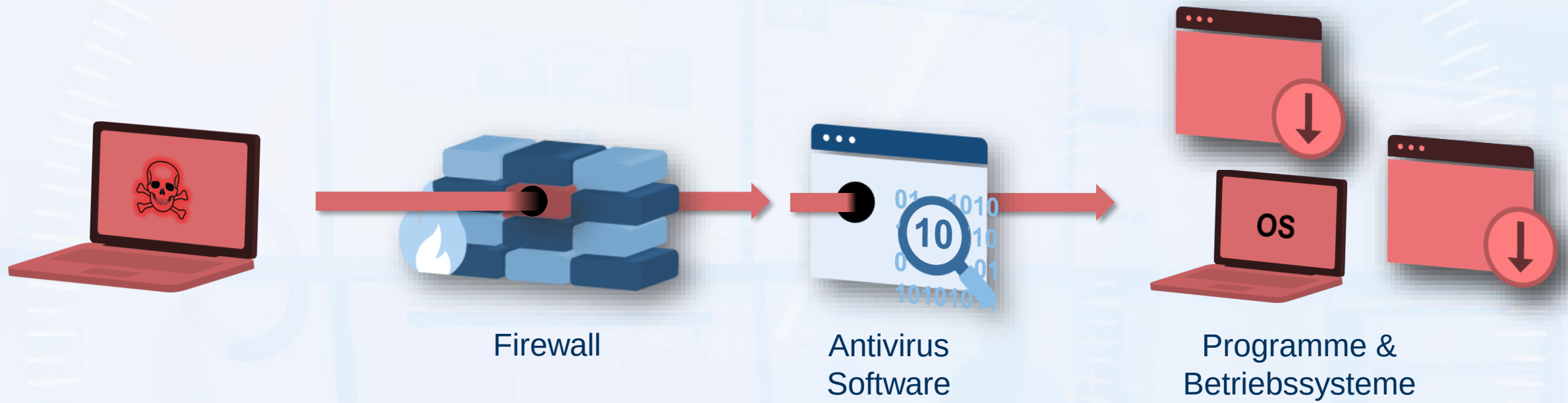
7A-406



Warum ist die Bedrohungslage so ernst?







Navy CIS: L.A. S06E19

DAS PROBLEM

7A-406

8COM
CYBER SECURITY



PATCHEN

<https://www.youtube.com/watch?v=msX4oAXpvUE>
„NCIS hacking“

DIE LÖSUNG?

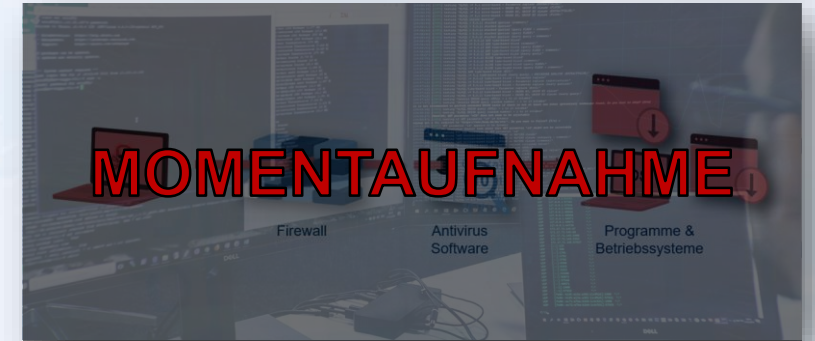
7A-406

 **8COM**
CYBER SECURITY

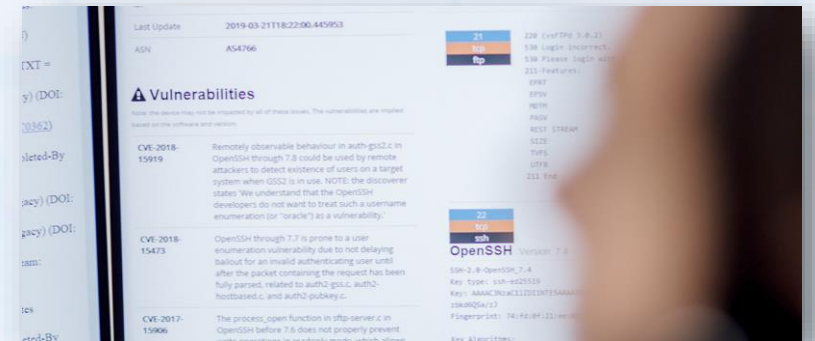


Sichtbarkeit | Kontinuität

~~Penetrationstests~~



Schwachstellenmanagement



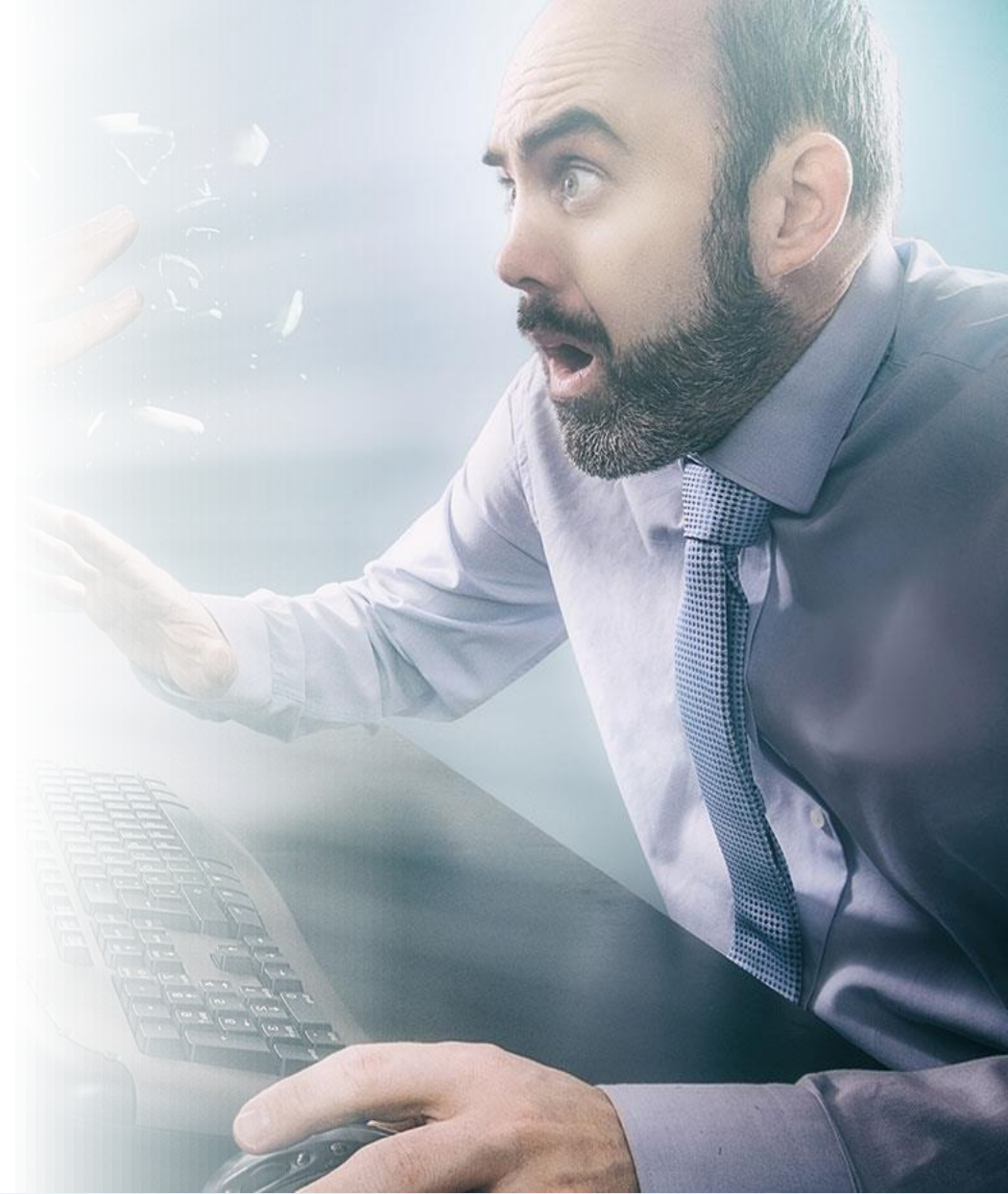
PATCHEN, ABER WAS?

7A-406



SICHTBAR

- ⚡ Sicherheitslücken
 - ⚡ Fehlende Updates
 - ⚡ Fehlende oder falsche Konfigurationen
- ⚡ Erfolgskontrolle



KONTINUIERLICH SICHTBAR

7A-406



KONTINUIERLICH

↳ Datensammlung Software Agent

- ↳ Alle 4 Stunden aktuelle Daten
- ↳ Extrem gute Datenqualität
- ↳ Updatet sich selbst

↳ Scanner

- ↳ Virtual Scanner Appliance
- ↳ Perimeter Scans

Vulnerabilities

Note: the device may not be impacted by based on the software and version.

CVE-2018-15919

Remotely ob
OpenSSH th
attackers to
system when
states "We u
developers c
enumeration

CVE-2018-15473

OpenSSH th
enumeration
bailout for a
after the pa
fully parsed

Wir müssen sie alle erwischen!

- ⚡ Wir müssen alles patchen – der Angreifer benötigt nur 1 Lücke
- ⚡ Was ist mit dem alten PC im Lager?
- ⚡ Aber wir müssen priorisieren:
Alle Daten, aber gezieltes Patchen





**Wir schützen unsere
Kunden vor fortschrittlichen und
professionellen Cyber-Angriffen!**

⚡ Schneller und einfacher Start

- ⚡ Sie profitieren von unserem Know-How und unseren Kapazitäten
- ⚡ Vorbereitung der Best Practice Vorlagen (Dashboards, Reports, Option Profiles, Scans, etc.)
- ⚡ Hilfestellung bei der Anpassung vorhandener oder neuer Vorlagen nach Kundenwünschen
- ⚡ Benutzerverwaltung

⚡ Segregation of Duties

- ⚡ Trennung zwischen Audit und Operations



Das ist einfach, das geht ganz schnell!



8com GmbH & Co. KG

Europastraße 32
67433 Neustadt/ Weinstraße
Deutschland

info@8com.de | www.8com.de

Kurzanleitung | Qualys Cloud Agent (Win)

Der Agent muss
<https://qagpublic.qg2.apps.qualys.eu>
erreichen können.

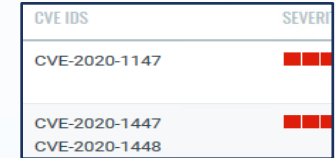
Die Installation muss mit
administrativen Rechten durchgeführt
werden!

Vulnerability Management

Standardmodule VMDR

Vulnerability Management

Schwachstellen auf den Assets detektieren, bewerten und Lösungswege aufzeigen



CVE IDS	SEVERITY
CVE-2020-1147	■■■■
CVE-2020-1447	■■■■
CVE-2020-1448	■■■■

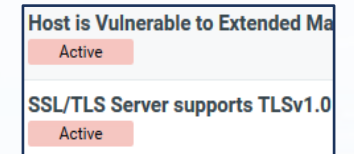
Agent & Virtuelle Scanner Appliance

Sensorik: Scannen im Netzwerk und auf Systemebene



Perimeter Scans & Continuous Monitoring

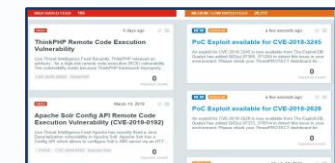
Angreifer-Sicht auf die Perimeter-Systeme erhalten und direkte Alarmierung über priorisierte Schwachstellen mit deren Detektion generieren



Host is Vulnerable to Extended Ma
Active
SSL/TLS Server supports TLSv1.0
Active

Threat Protection

Anreicherung der Schwachstellen-Informationen mit Threat Intelligence Daten (z.B. Public Exploit)



Qualys Gateway Service

Zentraler Zugangspunkt für Agents in Richtung Qualys Portal mit Cache-Funktion



ANZAHL SERVER INTERN/AGENT

102

showing last 90 days ⚙️



ANZAHL CLIENTS

97

showing last 90 days ⚙️



OTHER INTERN/AGENT

23

showing last 90 days ⚙️



SERVER - EXPLOIT - CRITICAL

0

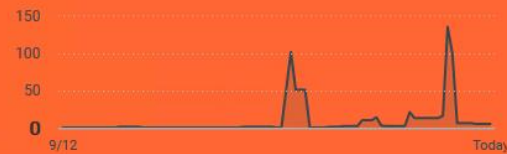
showing last 90 days ⚙️



SERVER - EXPLOIT - HIGH

5

showing last 90 days ⚙️



SERVER - NONEXPLOIT - CRITICAL

4

showing last 90 days ⚙️



SERVER - NONEXPLOIT - HIGH

59

showing last 90 days ⚙️



Vulnerabilities

54.5K

Total Detections

SEVERITY

4	40.2K
3	8.47K
5	5.59K
2	234

CATEGORY

Local	45.7K
Windows	6.3K
Office Application	2.18K
Security Policy	262
Internet Explorer	72

6 more

OPERATING SYSTEM

Microsoft Windo...	12.1K
Microsoft Windo...	4.74K

Vulnerability ▼ vulnerabilities.vulnerability.threatIntel.publicExploit:true× + ? ≡ Qualys Insights consolidates data to get an enhanced view of the security posture.[View Qualys Insights](#) ×

Asset

Vulnerability

Group by:

Vulnerability × ▼ 4 Filters ▼1 - 50 of 784 ◀ ▶ ⬇ ↺ 📊 ⚙

QID	TITLE	CVE IDS	SEVERITY	QDS ⓘ	VULNERABILITY COUNT
90044	Allowed Null Session	CVE-2002-1117 CVE-2000-1200		36 ... 79	993
376546	Oracle Java Standard Edition (SE) Critical Patch Update - April 2022 (CPUAPR2022)	CVE-2022-21426 CVE-2022-21476 4 more		41 ... 83	869
376733	Oracle Java Standard Edition (SE) Critical Patch Update - July 2022 (CPUJUL2022)	CVE-2022-21549 CVE-2022-34169 2 more		33 ... 83	778
378425	Oracle Java Standard Edition (SE) Critical Patch Update - April 2023 (CPUAPR2023)	CVE-2023-21938 CVE-2023-21939 5 more		35 ... 37	747
378332	Microsoft WinVerifyTrust Signature Validation Vulnerability	CVE-2013-3900		95	730
379151	Microsoft Edge Based on Chromium Prior to 120.0.2210.77 Multiple Vulnerabilities	CVE-2023-6705 CVE-2023-6704 5 more		35 ... 42	536
379174	Microsoft Edge Based on Chromium Prior to 120.0.2210.91 Multiple Vulnerabilities	CVE-2023-7024		95	535



VULNERABILITIES ÜBERSICHT

7A-406



Qualys - Beispielansichten



Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012)
(Spectre/Meltdown Variant 4)

QID: 91462 Active

Last Found on 5 hours ago

Vulnerability Result

HKLM\System\CurrentControlSet\Control\Session Manager\Environment PROCESSOR_IDENTIFIER = Intel64 Family 6 Model 94 Stepping 3, GenuineIntel

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management FeatureSettingsOverride is missing.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management FeatureSettingsOverrideMask is missing.

Identification		CVSS Summary	
QID:	91462	CVSSv2 Base:	4.9
Category:	Windows	CVSSv2 Temporal:	3.8
Modified Date:	Dec 11, 2020 05:06 a m	CVSSv3 Base:	5.5
		CVSSv3 Temporal:	5

Exploitability

This section lists known exploits for this vulnerability available from third-party vendors and/or publicly available sources

1 - 1 of 1

SOURCE	REFERENCE	DESCRIPTION
The Exploit-DB	CVE-2018-3639	AMD / ARM / Intel - Speculative Execut http://www.exploit-db.com/exploits/44

REFERENCE	TYPE
ADV180012	-
ADV180012	-
ADV180012	-

WIE SIEHT SO EIN FINDING AUS?

7A-406

Technische Reports

Detailed Results

5	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2020-55) (10)
5	Microsoft Windows Security Update for January 2021 (16)
5	ECOL/Oletole Software: Adobe Flash Player Detected (13)
5	ECOL/Oletole Software: SAP GUI 7.30 to 7.40 Detected (11)
5	ECOL/Oletole Software: Microsoft XML Parser and Microsoft XML Core Services (MSXML) 4.0 Detected (4)
5	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2020-48) (1)
5	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2020-38) (1)
5	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2020-49) (1)
5	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-30) (1)
5	Microsoft Windows TCP/IP Remote Code Execution Vulnerability (1)
4	Wireshark Multiple Vulnerabilities (wnpa-sec-2018-51 to wnpa-sec-2018-56) (2)
4	Microsoft Edge Based On Chromium Prior to 87.0.664.57 Multiple Vulnerabilities (ADV200002) (12)
4	Microsoft Edge Based On Chromium Prior to 87.0.664.57 Multiple Vulnerabilities (ADV200002) (13)
4	Microsoft Edge Security Update for December 2020 (9)
4	Microsoft Office and Microsoft Office Services and Web Apps Security Update January 2021 (13)
4	Microsoft Edge Based On Chromium Prior to 87.0.664.75 Multiple Vulnerabilities (ADV200002) (12)
4	Adobe Security Update for Adobe Acrobat and Reader (APSB20-07) (14)
4	Wireshark Gryphon (Descriptor infinite loop Vulnerability)wnpa-sec-2018-21) (2)
4	Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability(cisco-sa-anyconnect-dll-F26WwJW) (15)
4	Cisco AnyConnect Secure Mobility Client Arbitrary Code Execution Vulnerability(cisco-sa-anyconnect-gp-KID090K) (14)
4	Adobe Security Update for Adobe Acrobat and Reader (APSB20-48) (15)
4	Microsoft Windows Security Feature Bypass in GRUB (ADV200011) (BootHole) (15)
4	Detected LanManNTLMv1 Authentication method (16)
4	Oracle Java SE Critical Patch Update - April 2020 (16)
4	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2021-01) (8)
4	Adobe Security Update for Flash Player (APSB20-59) (8)
4	Adobe Flash Player Arbitrary Code Execution Vulnerability (APSB20-30) (5)
4	Microsoft Outlook Information Disclosure Vulnerability Security Update December 2020 (3)
4	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2020-51) (1)
4	Mozilla Firefox ESR Multiple Vulnerabilities (MFS2020-37) (1)
4	Symantec Endpoint Protection (SEP) Multiple Vulnerabilities (SYM201762) (2)
4	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4) (3)
4	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-41) (1)
4	Microsoft Internet Explorer Security Update for September 2017 (3)
4	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) (3)
4	Adobe Reader and Acrobat Information Disclosure Vulnerability (APSB19-40) (1)
4	Adobe Reader and Acrobat Information Disclosure Vulnerability (APSB19-13) (1)
4	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-02) (1)
4	Adobe Security Update for Adobe Acrobat and Reader (APSB19-41) (1)
4	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-07) (1)
4	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-29) (1)
4	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-21) (1)
4	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) (3)
4	Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021 (1)
4	Microsoft Edge Based On Chromium Prior to 85.0.564.41 Multiple Vulnerabilities (ADV200002) (1)
4	Microsoft .NET Framework Security Updates for October 2020 (1)
4	Microsoft Edge Based On Chromium Prior to 84.0.522.63 Multiple Vulnerabilities (ADV200002) (1)
4	Microsoft Edge Based On Chromium Prior to 86.0.622.51 Multiple Vulnerabilities (ADV200002) (1)
4	Microsoft Windows Security Update for October 2020 (1)
4	Microsoft Edge Based On Chromium Prior to 86.0.622.38 Multiple Vulnerabilities (ADV200002) (1)
4	Microsoft Windows Adobe Flash Player Security Update for October 2020 (ADV200012) (1)
4	Microsoft Internet Explorer Security Update for September 2020 (1)
4	Red Hat Update for kernel (RHSA-2020-1524) (1)
4	Red Hat Update for kernel (RHSA-2019-3878) (1)
4	Red Hat Update for kernel (RHSA-2019-3878) (1)
4	Red Hat Update for kernel (RHSA-2019-3878) (1)
2	Allowed Null Session (18)
2	Citrix Workspace Privilege Escalation Vulnerability (CTX27662) (2)
2	Microsoft Windows Servicing Stack Security Update September 2020 (1)
2	Microsoft Windows Servicing Stack Security Update October 2020 (1)
2	Microsoft Windows Servicing Stack Security Update November 2020 (1)

➤ **Priorisierung nach Kritikalität und Ausnutzbarkeit**

➤ **Klare Vorgehensweise für die Admins**

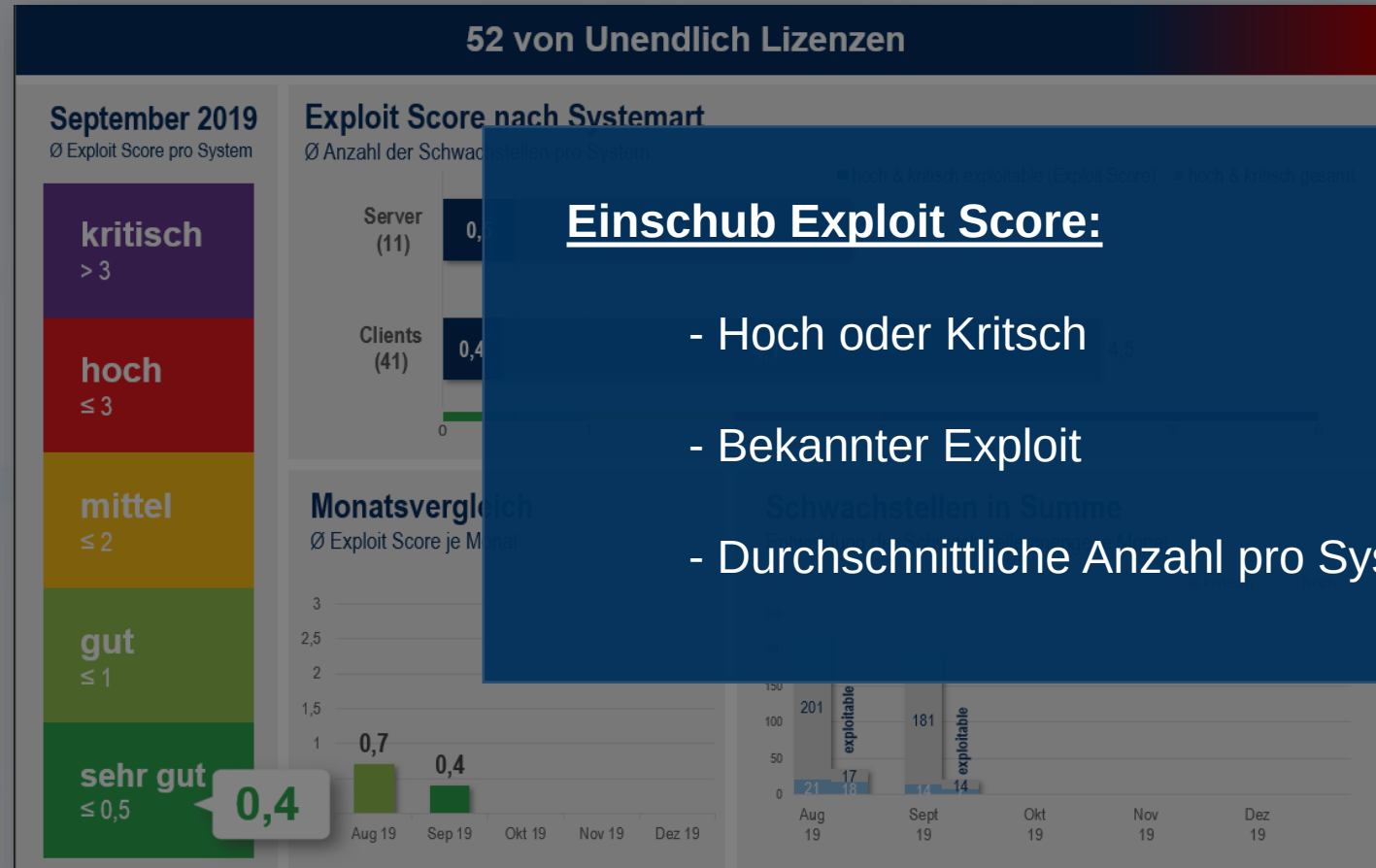
➤ **Nachhaltiges Steigern des Sicherheitsniveaus**

Detailed Results

Vulnerabilities

4	Wireshark Multiple Vulnerabilities (wnpa-sec-2018-51 to wnpa-sec-2018-56) (2)
4	Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability(cisco-sa-anyconnect-dll-F26WwJW) (15)
4	Oracle Java SE Critical Patch Update - April 2019 (16)
4	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4) (3)
4	Adobe Security Update for Adobe Acrobat and Reader (APSB19-41) (1)
4	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) (3)
4	Red Hat Update for kernel (RHSA-2020:1524) (1)
4	Red Hat Update for kernel (RHSA-2019:2473) (1)
3	Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability(cisco-sa-ac-win-path-traverse-qO4HWBsj) (15)
3	FortiOS and FortiClient Man-In-The-Middle Attack Vulnerability (FG-IR-18-100) (15)

Management Report



Einschub Exploit Score:

- Hoch oder Kritisch
- Bekannter Exploit
- Durchschnittliche Anzahl pro System

8com – Mitigation Advisory

Spectre Meltdown Mitigation Windows

Die Schwachstellengruppe Spectre-Meltdown hat ihren Ursprung in diversen Prozessoren und deren Implementierung. Für Windows Systeme bietet Microsoft Maßnahmen zur Abschwächung der Schwachstelle auf Betriebssystemebene an.

Der Artikel aus der MS Knowledge Base (<https://support.microsoft.com/de-de/help/4072698/>) ist mit der Zeit gewachsen und nennt daher fortschreitende Werte für die Mitigation.

Die folgenden Commands erzeugen die notwendigen Registry-Einträge und ordnen diesen den Wert zur maximal möglichen Abschwächung zu:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session  
Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 72  
/f
```

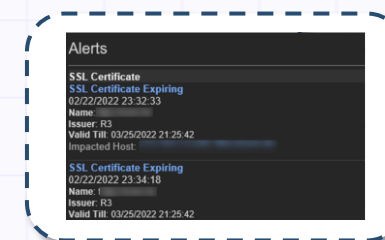
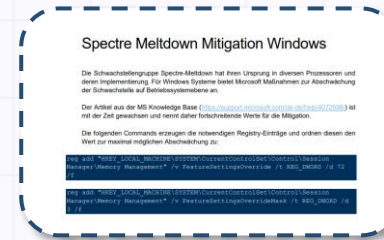
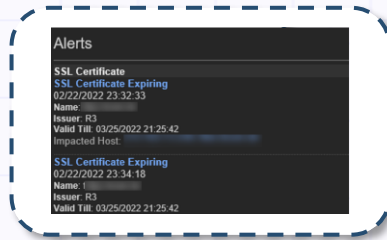
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session  
Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d  
3 /f
```

Hierbei wird das Hyperthreading nicht deaktiviert und es sollten keine merklichen Performance-Verluste feststellbar sein.

Sollte das Hyper-V-Feature auf den betroffenen Systemen installiert sein, ist der folgende Schritt ebenfalls notwendig:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization"  
/v MinVmVersionForCpuBasedMitigations /t REG_SZ /d "1.0" /f
```

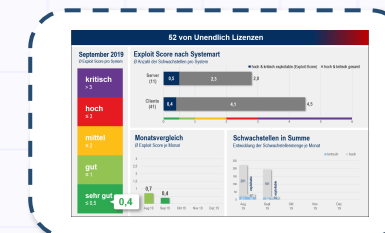
Nach erfolgter Konfiguration ist ein Neustart der betroffenen Systeme Notwendig.



anlassbezogen



zwei-wöchentlich



monatlich



Konfiguration
Bewertung
& Auswertung



▲ Agent-Daten
einchecken



Agents
(Clients und Server)

▲ Scan-Daten
übermitteln

Ext. Scanner



Perimeter

▲ Scan-Daten
übermitteln

VSA



Netzwerktechnik
Appliances
Drucker

▼ Aufbereiten
& mitteilen



CM Alarme
VM Berichte
Perimeter Berichte
EDR Alarme
PC Berichte

GEHT DA NOCH MEHR?



**ZUSATZMODULE UND SERVICE LEVEL
AGREEMENT**

7A-406

8COM
CYBER SECURITY

Zusatzfunktionen und Module

Portalzugang

Der Portalzugriff bietet mehr Komfort und hoch aktuelle Daten



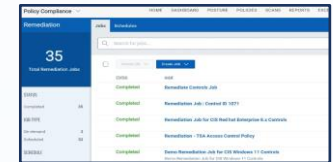
Regelmäßige Meetings

Lassen Sie uns sprechen: z.B. im Quartal, alle zwei Monate, jeden Monat oder in Ihrem gewünschten Rhythmus



Policy Compliance

Definieren und Überwachen von Konfigurationsstandards, z.B. nach CIS Controls



Patch Management

Patches gezielt auswählen und auslösen, oder Automatisieren von regelmäßigen Jobs



Total Cloud

Cloud Ressourcen anbinden und Konfigurationen sowie Berechtigungen überwachen.



Easy like
that:

1.

Installation der Agents

2.

Einrichten der Perimeter Scans

3.

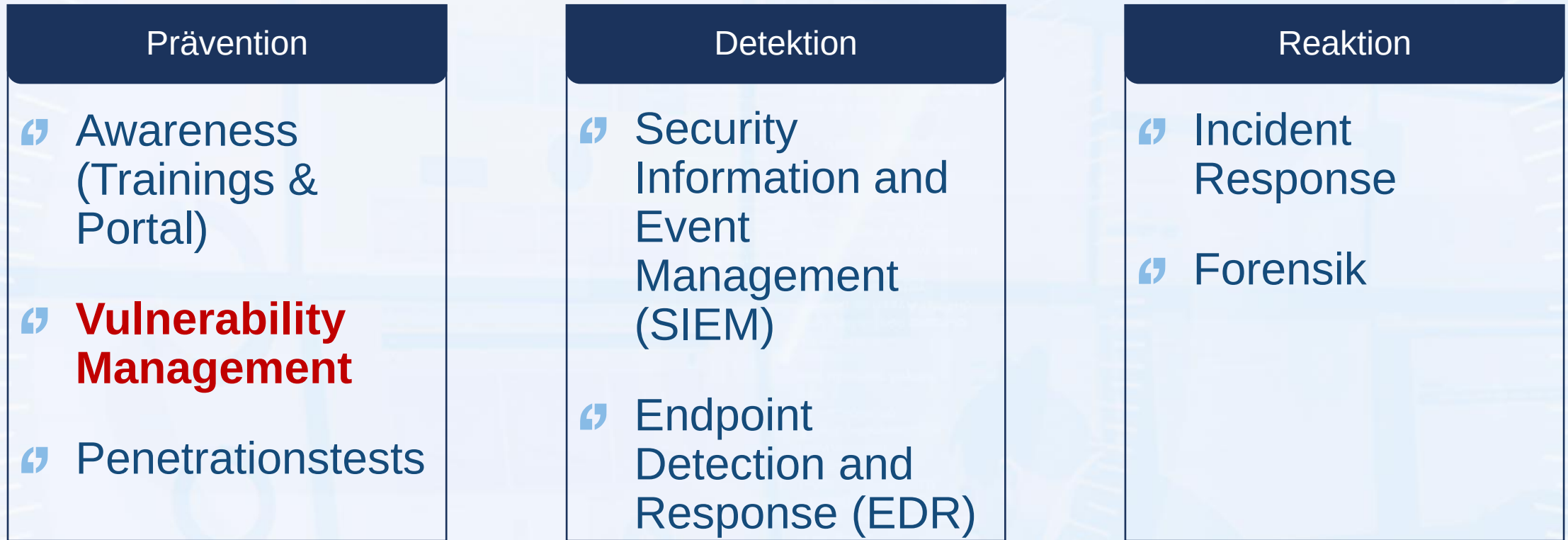
Einrichten des Reportings

1.

(4.)

Einweisung in das Qualys Portal + Anlegen der User

- 
- ⚡ **SICHTBARKEIT!**
 - ⚡ **Kontinuierliche Prüfung**
 - ⚡ **Nachhaltige Steigerung des Sicherheitsniveaus**
 - ⚡ **Klare Lösungsstrategie für Admins**
 - ⚡ **Nachweis über geleistete Arbeit und ToDOs**
 - ⚡ **Schneller und günstiger Einstieg**





KEEP ON PATCHING!
DENN PATCHEN HÖRT NIEMALS AUF.

SEIT 2004

7A-406

