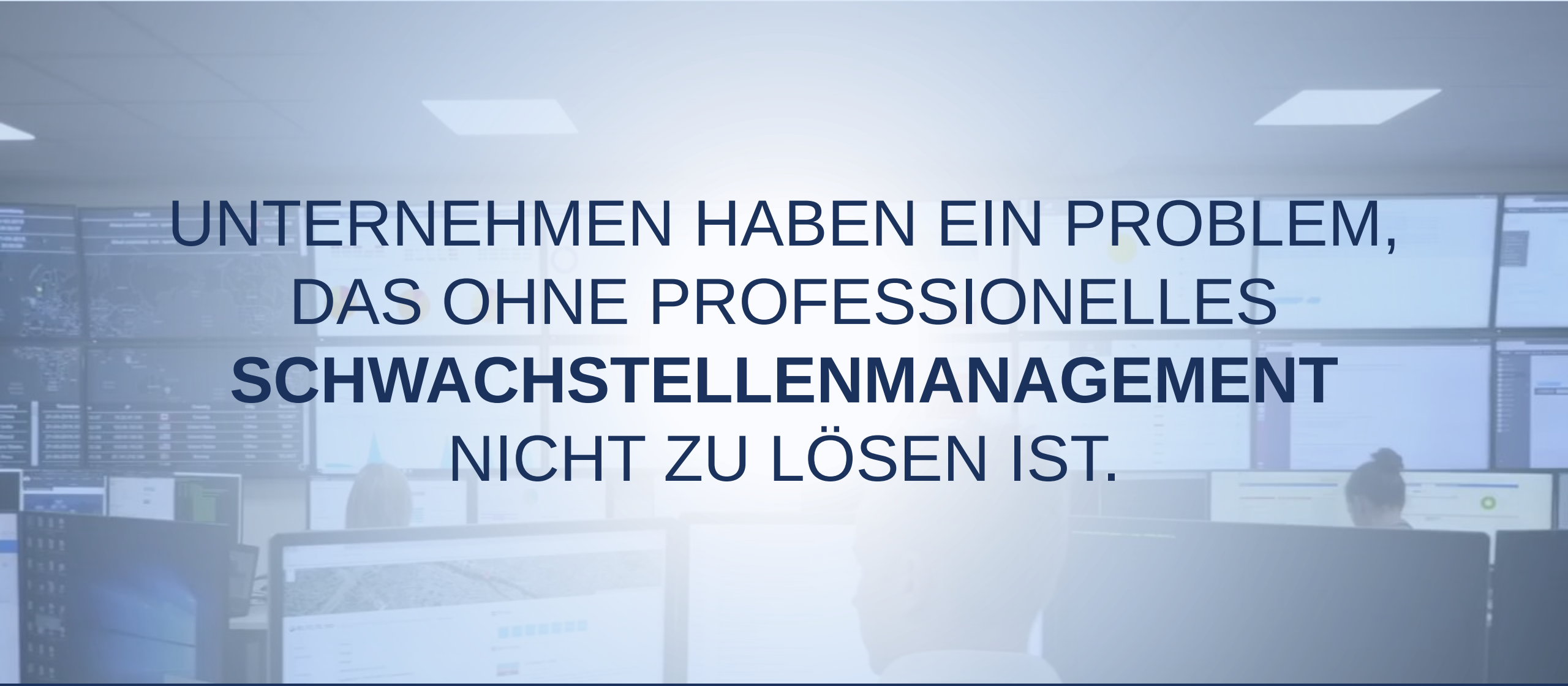
ERIK ZIMMERMANN
Vulnerability Management Specialist

PATCH ME IF YOU CAN:

WARUM SCHWACHSTELLENMANAGEMENT EIN MUST-HAVE IST

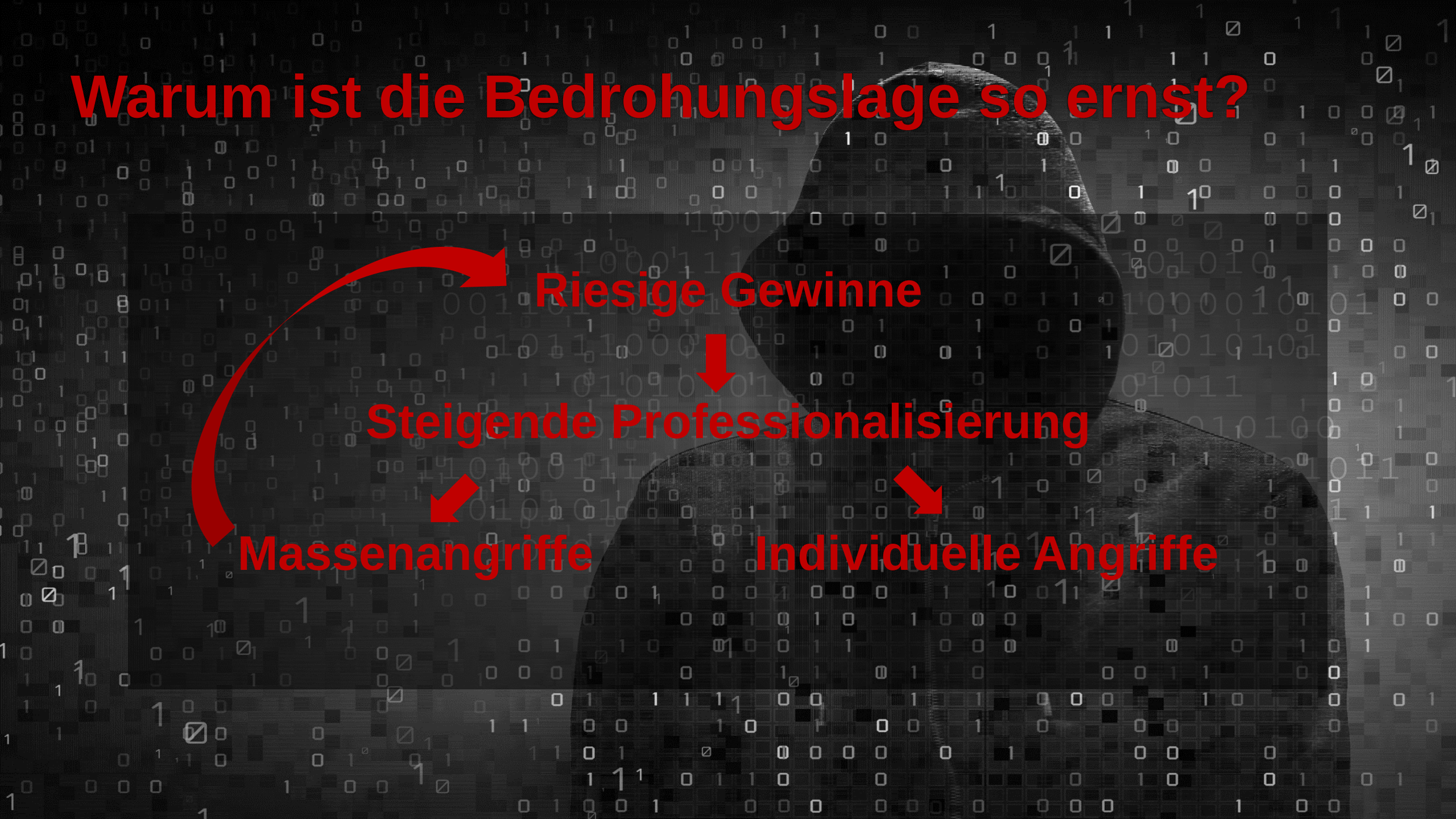
7A-406

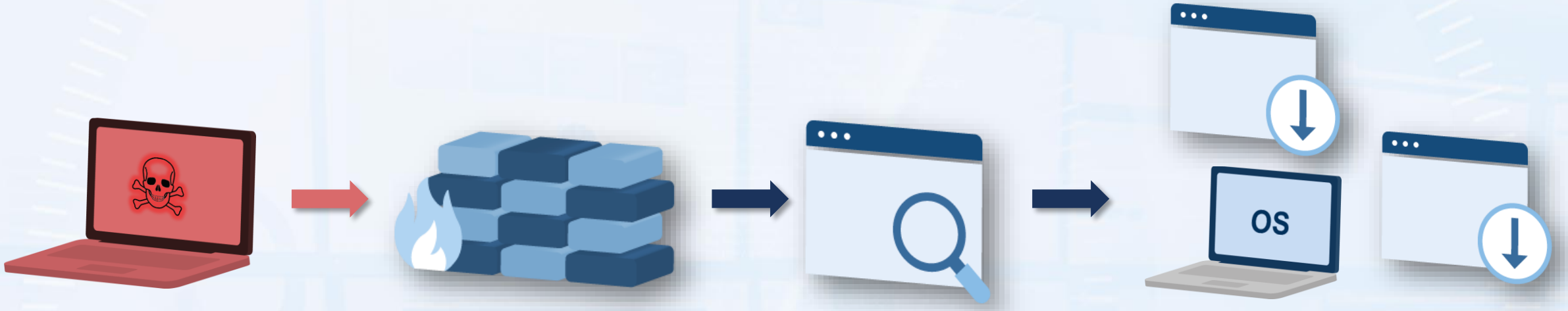
8COM CYBER SECURITY



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

Warum ist die Bedrohungslage so ernst?





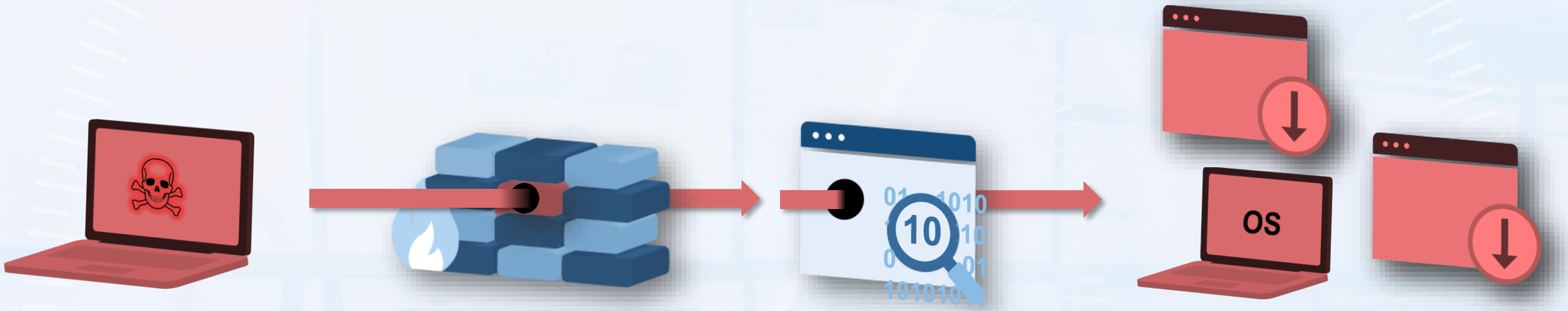
Firewall

Antivirus Software

Programme & Betriebssysteme

DAS PROBLEM

8COM CYBER SECURITY



Firewall

Antivirus Software

Programme & Betriebssysteme

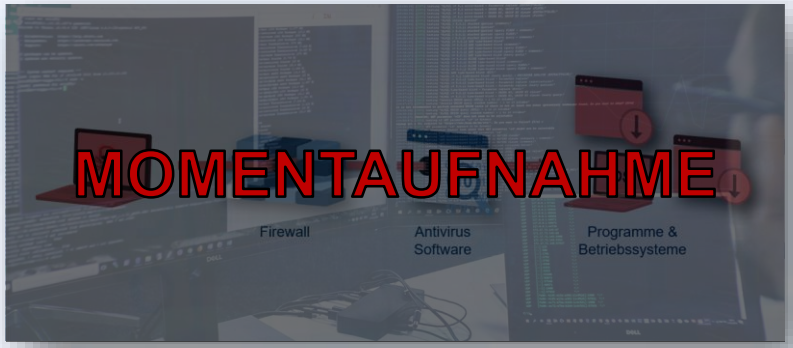
Navy CIS: L.A. S06E19

PATCHEN

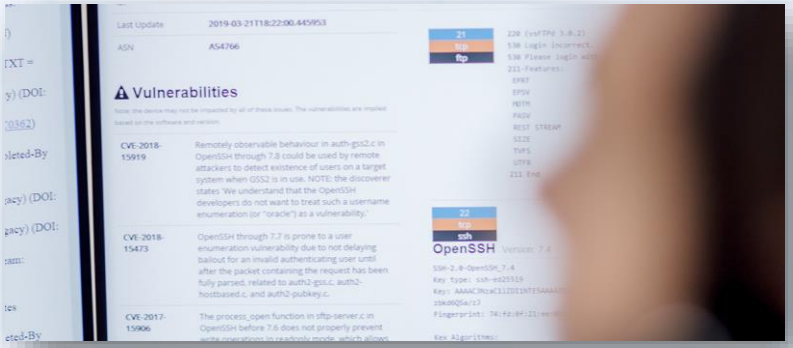
https://www.youtube.com/watch?v=msX4oAXpvUE
„**NCIS hacking**“

Sichtbarkeit | Kontinuität

~~Penetrationstests~~

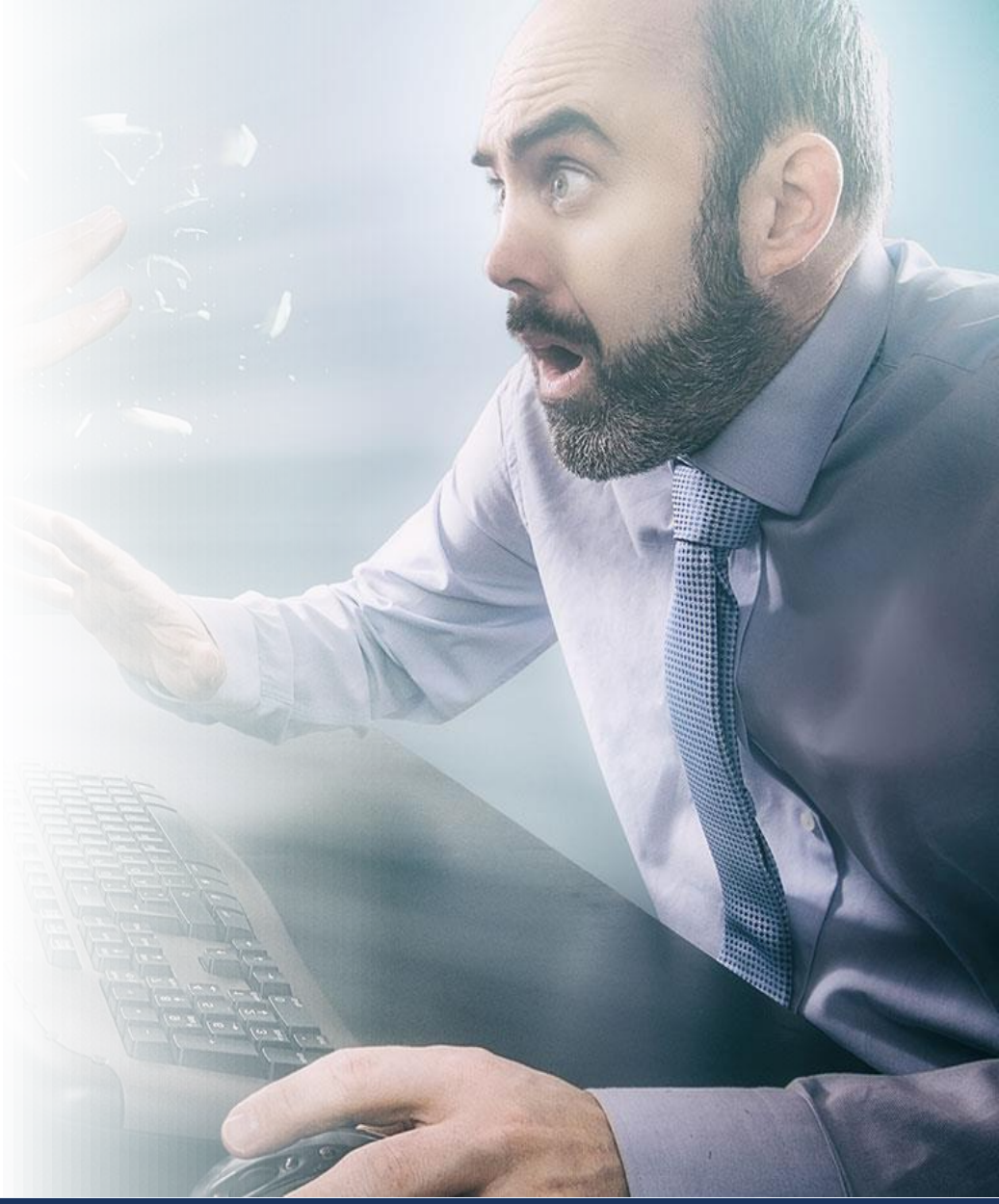


Schwachstellenmanagement



SICHTBAR

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



KONTINUIERLICH

- Datensammlung Software Agent
  - Alle 4 Stunden aktuelle Daten
  - Extrem gute Datenqualität
  - Updatet sich selbst
- Scanner
  - Virtual Scanner Appliance
  - Perimeter Scans

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

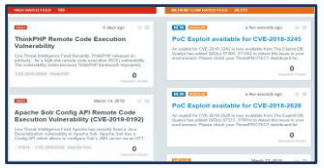
- Segregation of Duties
  - Trennung zwischen Audit und Operations

Das ist einfach, das geht ganz schnell!

Vulnerability Management

Standardmodule VMDR

Vulnerability Management	Schwachstellen auf den Assets detektieren, bewerten und Lösungswege aufzeigen
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
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



Qualys.

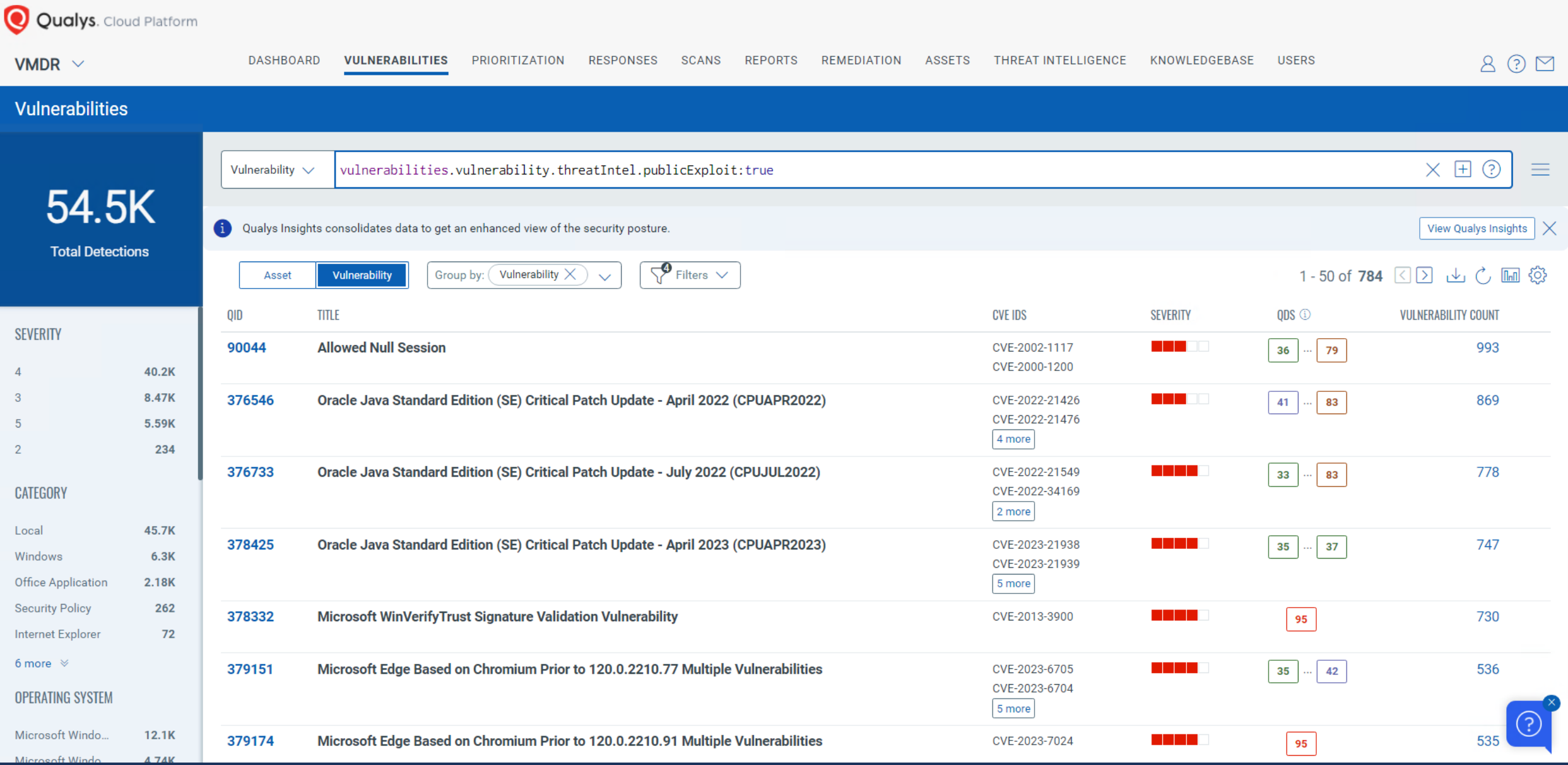
7A-406

8COM CYBER SECURITY

DASHBOARDS

7A-406

8COM CYBER SECURITY

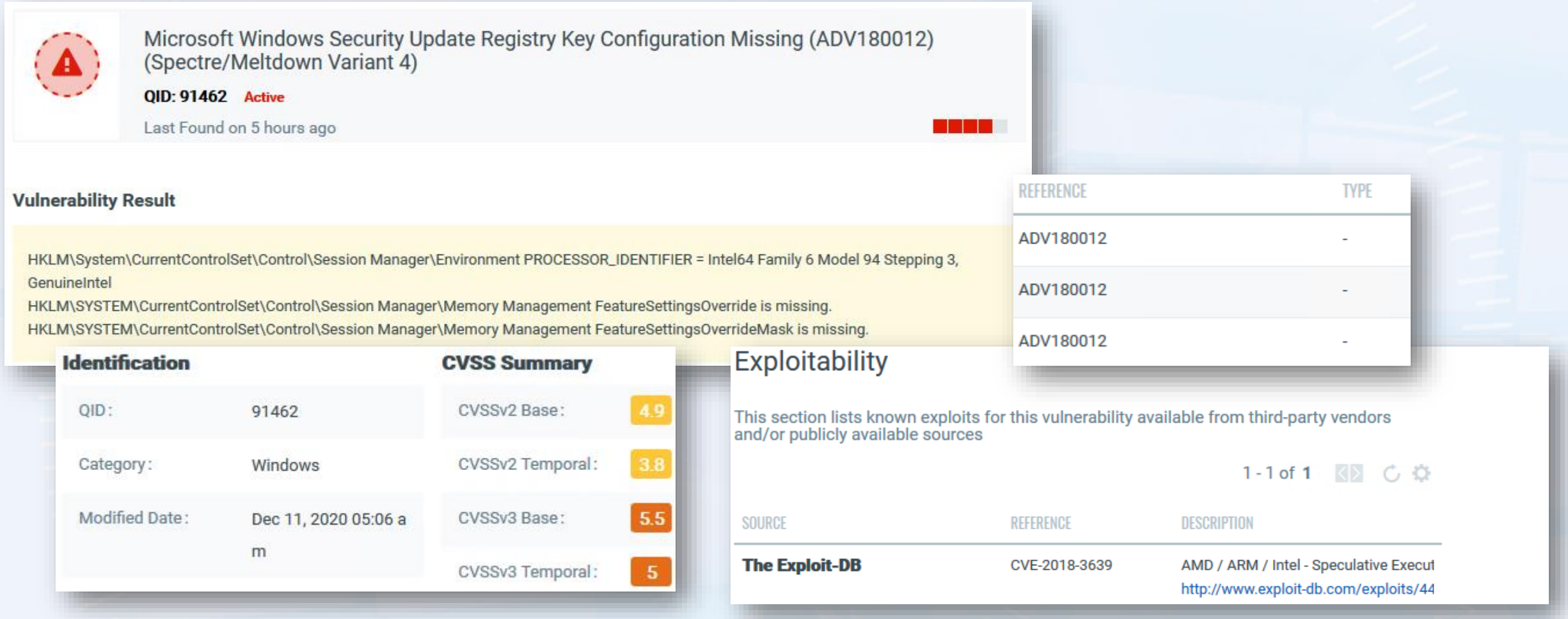


VULNERABILITIES ÜBERSICHT

7A-406

8COM CYBER SECURITY

Qualys - Beispielansichten

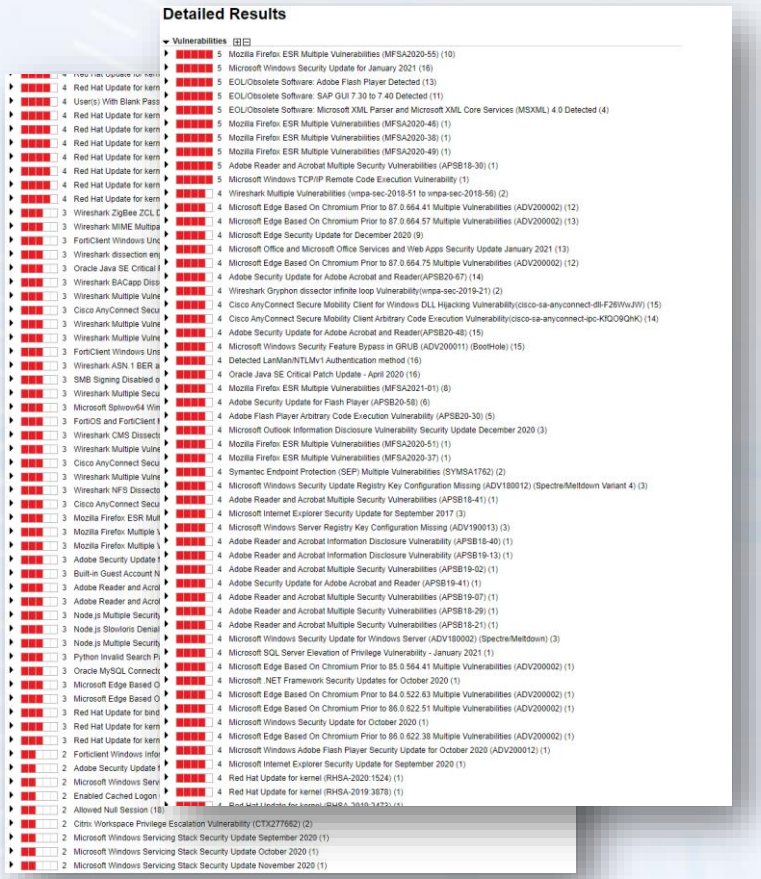


WIE SIEHT SO EIN FINDING AUS?

7A-406

8COM CYBER SECURITY

Technische Reports



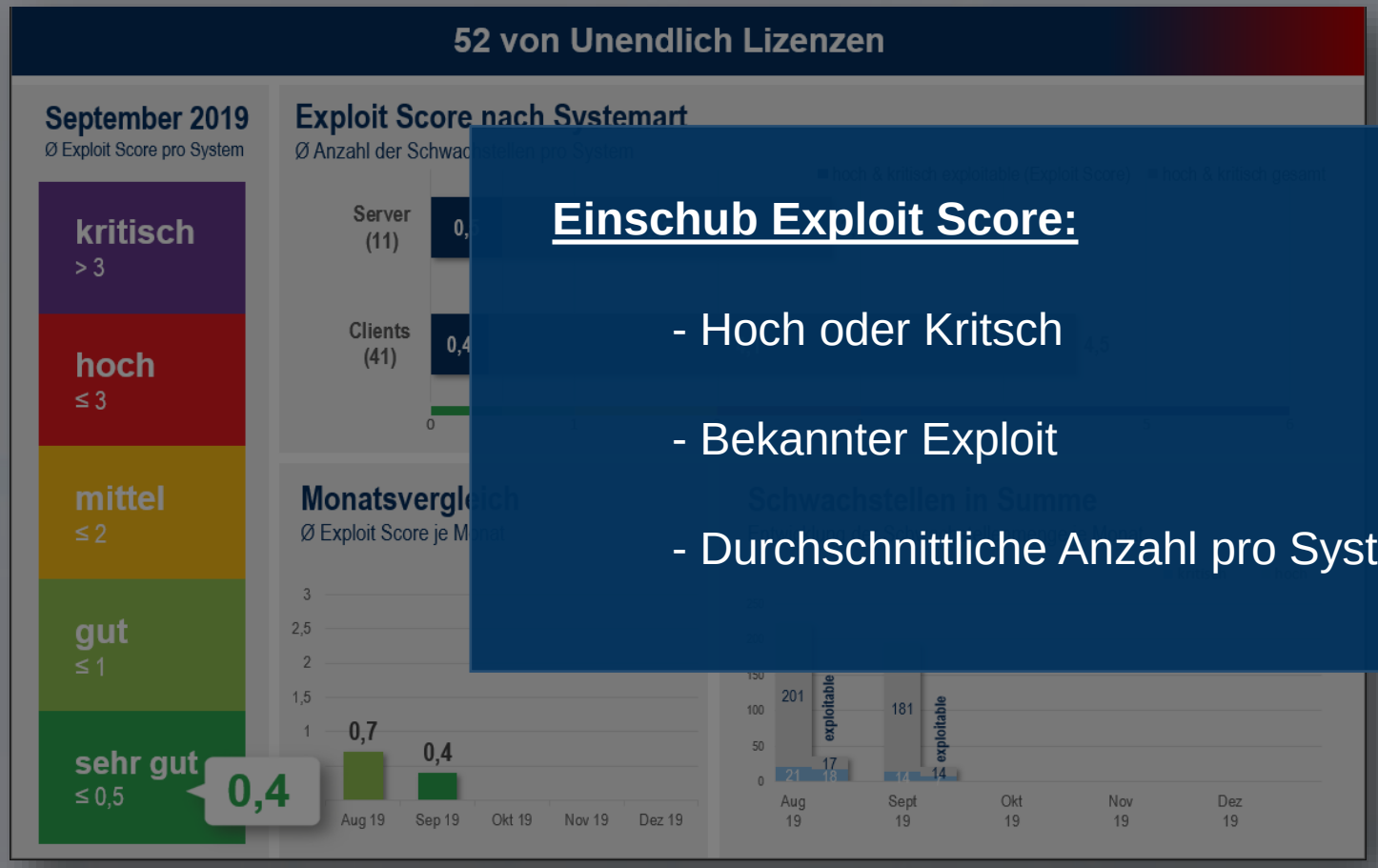
- **Priorisierung nach Kritikalität und Ausnutzbarkeit**
- Klare Vorgehensweise für die Admins
- Nachhaltiges Steigern des Sicherheitsniveaus

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 Kritsch
- 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
```

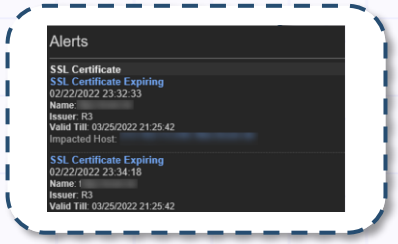
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d
3 /f
```

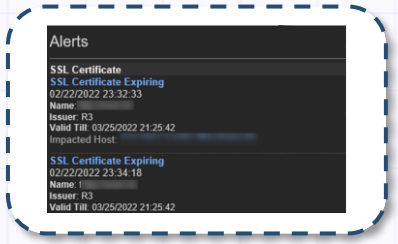
Hierbei wird das Hyperthreading nicht deaktiviert und es sollten keine merklichen Performance-Verluste feststellbar sein.

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
```

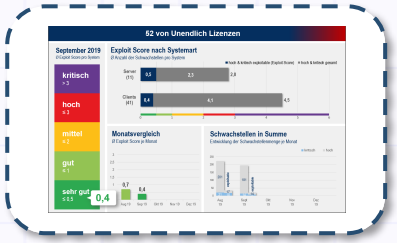
Nach erfolgter Konfiguration ist ein Neustart der betroffenen Systeme Notwendig.





anlassbezogen

zwei-wöchentlich



monatlich

Qualys Portal

Qualys.

Konfiguration
Bewertung
& Auswertung

8COM CYBER SECURITY

Agent-Daten einchecken

Scan-Daten übermitteln

Scan-Daten übermitteln

Aufbereiten & mitteilen

Agents
(Clients und Server)

Ext. Scanner

Perimeter

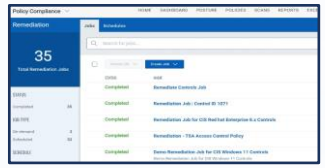
VSA

Netztwerktechnik
Appliances
Drucker

CM Alarme
VM Berichte
Perimeter Berichte
EDR Alarme
PC Berichte

GEHT DA NOCH MEHR?

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.	

Qualys.

7A-406

8COM CYBER SECURITY

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**

Prävention

- Awareness (Trainings & Portal)
- **Vulnerability Management**
- Penetrationstests

Detektion

- Security Information and Event Management (SIEM)
- Endpoint Detection and Response (EDR)

Reaktion

- Incident Response
- Forensik

KEEP ON PATCHING!

DENN PATCHEN HÖRT NIEMALS AUF.

SEIT 2004

7A-406

8COM CYBER SECURITY