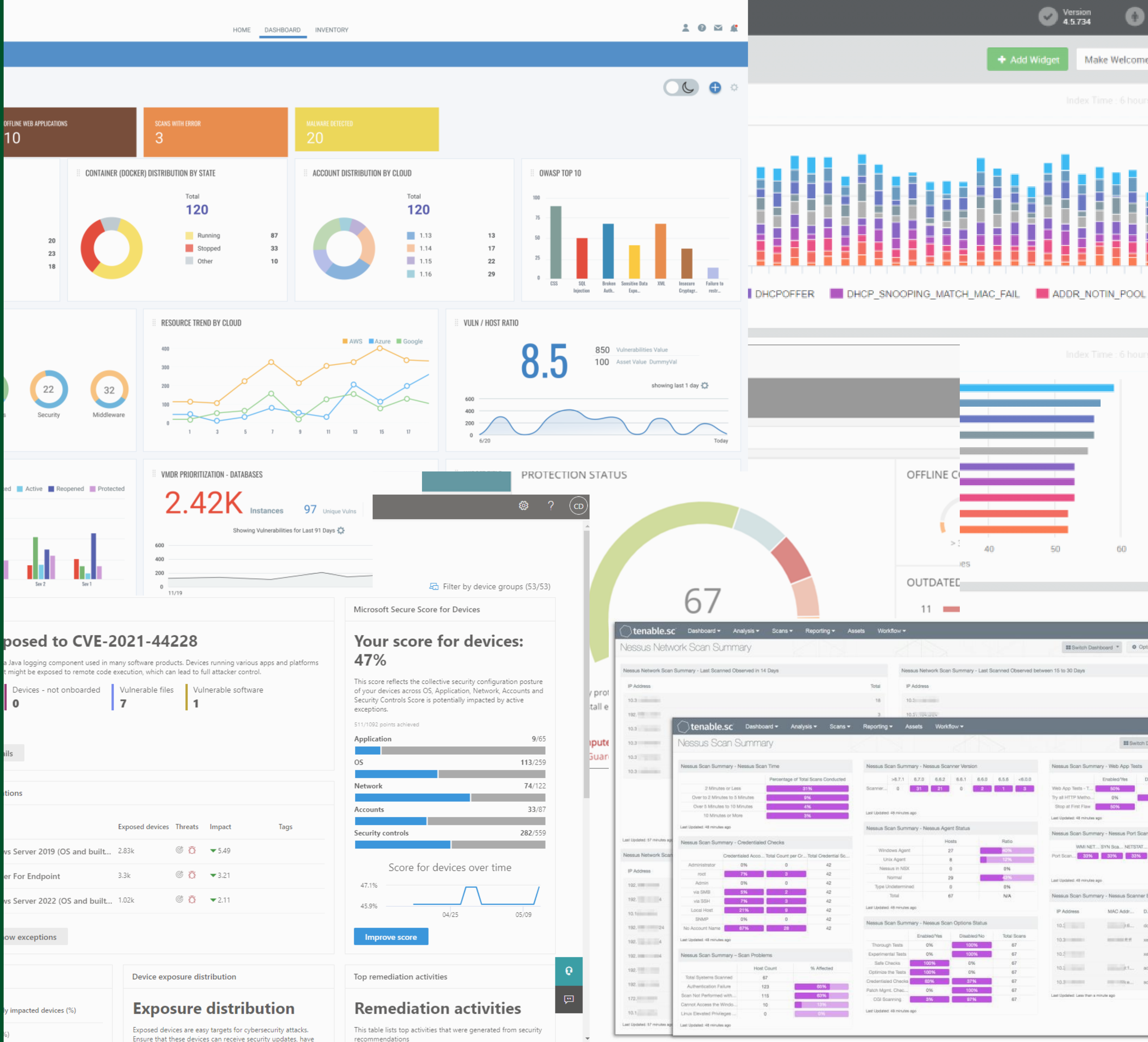
# Vulnerability management can suck (but does not have to)

Aleksander Groshev
CEO & Co-Founder

Autobahn security

# Our clients dealt with some serious pains…

- 🤯 **Fragmented tools**
- 🤯 **Vulnerability overload**
- 🤯 **Reporting hassle**



posed to CVE-2021-44228

a Java logging component used in many software products. Devices running various apps and platforms t might be exposed to remote code execution, which can lead to full attacker control.

| Devices - not onboarded | Vulnerable files | Vulnerable software |
|---|---|---|
| 0 | 7 | 1 |

| | Exposed devices | Threats | Impact | Tags |
|---|---|---|---|---|
| ws Server 2019 (OS and built… | 2.83k | | ▼5.49 | |
| er For Endpoint | 3.3k | | ▼3.21 | |
| ws Server 2022 (OS and built… | 1.02k | | ▼2.11 | |

Microsoft Secure Score for Devices

Your score for devices: 47%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

511/1092 points achieved

| | |
|---|---|
| Application | 9/65 |
| OS | 113/259 |
| Network | 74/122 |
| Accounts | 33/87 |
| Security controls | 282/559 |

Score for devices over time

Improve score

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have

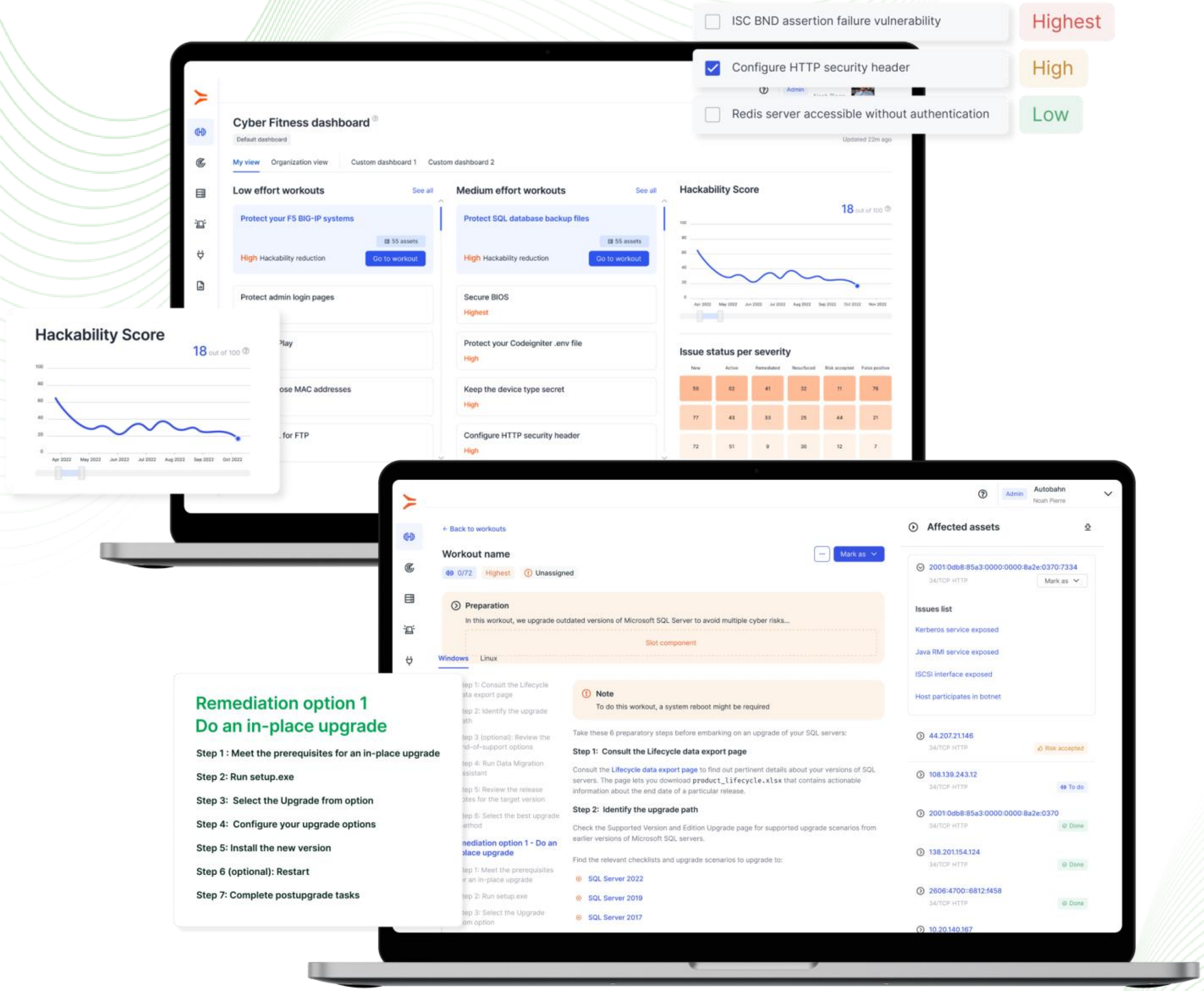
Top remediation activities

Remediation activities

This table lists top activities that were generated from security recommendations

tenable.sc
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Nessus Network Scan Summary
Nessus Network Scan Summary - Last Scanned Observed in 14 Days
Nessus Network Scan Summary - Last Scanned Observed between 15 to 30 Days
Nessus Scan Summary
Nessus Scan Summary - Nessus Scan Time
Nessus Scan Summary - Nessus Scanner Version
Nessus Scan Summary - Web App Tests
Nessus Scan Summary - Credentialed Checks
Nessus Scan Summary - Nessus Agent Status
Nessus Scan Summary - Nessus Port Scan
Nessus Scan Summary - Scan Problems
Nessus Scan Summary - Nessus Scan Options Status
Nessus Scan Summary - Nessus Scanner

# But then…



☐ ISC BND assertion failure vulnerability — Highest

☑ Configure HTTP security header — High

☐ Redis server accessible without authentication — Low

Cyber Fitness dashboard

Default dashboard

My view · Organization view · Custom dashboard 1 · Custom dashboard 2

Updated 22m ago

Low effort workouts — See all

- Protect your F5 BIG-IP systems — 55 assets — High Hackability reduction — Go to workout
- Protect admin login pages
- …Play
- …ose MAC addresses
- …for FTP

Medium effort workouts — See all

- Protect SQL database backup files — 55 assets — High Hackability reduction — Go to workout
- Secure BIOS — Highest
- Protect your Codeigniter .env file — High
- Keep the device type secret — High
- Configure HTTP security header — High

Hackability Score — 18 out of 100

Issue status per severity

| New | Active | Remediated | Resurfaced | Risk accepted | False positive |
|---|---|---|---|---|---|
| 56 | 62 | 41 | 32 | 11 | 76 |
| 77 | 43 | 33 | 25 | 44 | 21 |
| 72 | 51 | 9 | 30 | 12 | 7 |

← Back to workouts

Workout name

0/72 · Highest · Unassigned

Mark as

Preparation

In this workout, we upgrade outdated versions of Microsoft SQL Server to avoid multiple cyber risks...

Slot component

Windows · Linux

Note

To do this workout, a system reboot might be required

Take these 6 preparatory steps before embarking on an upgrade of your SQL servers:

**Step 1: Consult the Lifecycle data export page**

Consult the Lifecycle data export page to find out pertinent details about your versions of SQL servers. The page lets you download `product_lifecycle.xlsx` that contains actionable information about the end date of a particular release.

**Step 2: Identify the upgrade path**

Check the Supported Version and Edition Upgrade page for supported upgrade scenarios from earlier versions of Microsoft SQL servers.

Find the relevant checklists and upgrade scenarios to upgrade to:

- SQL Server 2022
- SQL Server 2019
- SQL Server 2017

Affected assets

- 2001:0db8:85a3:0000:0000:8a2e:0370:7334 — 34/TCP HTTP — Mark as
- Issues list: Kerberos service exposed; Java RMI service exposed; ISCSI interface exposed; Host participates in botnet
- 44.207.21.146 — 34/TCP HTTP — Risk accepted
- 108.139.243.12 — 34/TCP HTTP — To do
- 2001:0db8:85a3:0000:0000:8a2e:0370 — 34/TCP HTTP — Done
- 138.201.154.124 — 34/TCP HTTP — Done
- 2606:4700::6812:f458 — 34/TCP HTTP — Done
- 10.20.140.167

Remediation option 1
Do an in-place upgrade

Step 1 : Meet the prerequisites for an in-place upgrade

Step 2: Run setup.exe

Step 3: Select the Upgrade from option

Step 4: Configure your upgrade options

Step 5: Install the new version

Step 6 (optional): Restart

Step 7: Complete postupgrade tasks

## 🤩 Unified Platform

All your cyber sec tools aggregated in one view

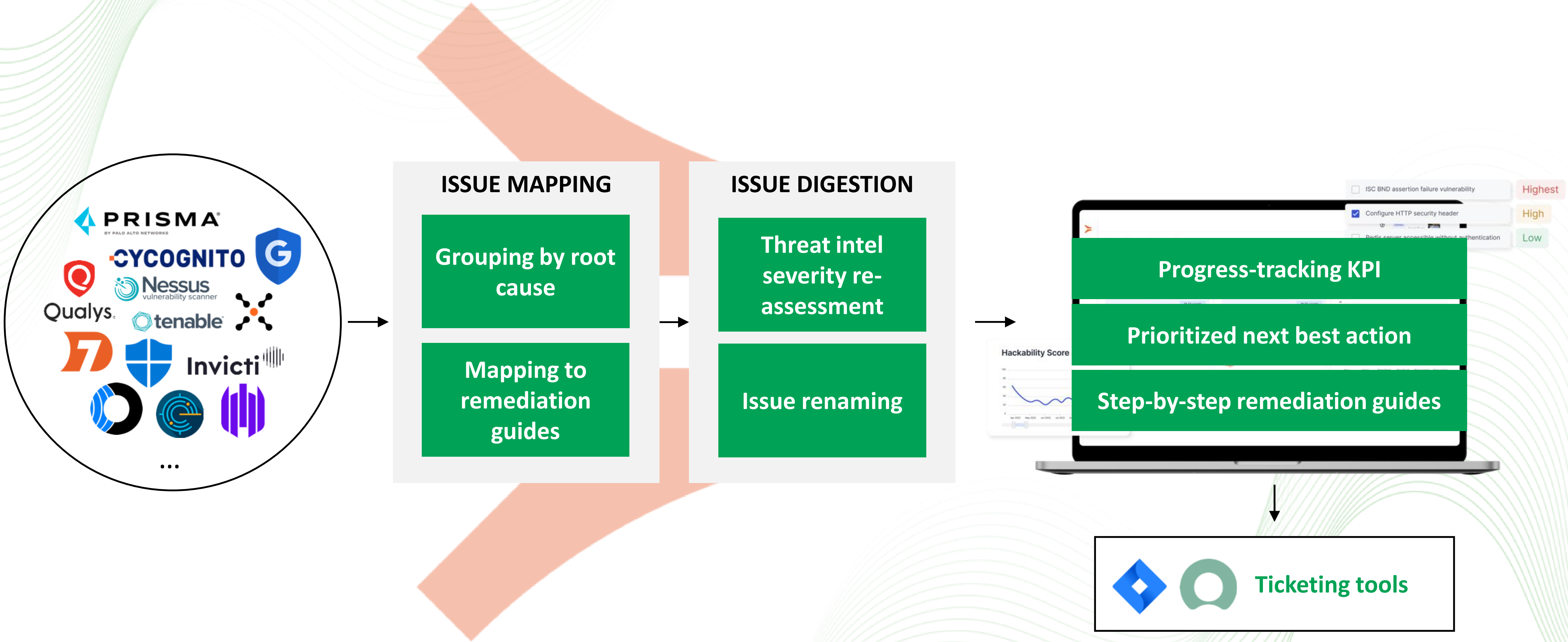
## 🤩 Automated Prioritization

Ethical hacker-view clustering and prioritization

## 🤩 Remediation Guides

Step-by-step instructions for efficient fixes

# How does that work?


PRISMA
BY PALO ALTO NETWORKS
CYCOGNITO
Nessus
vulnerability scanner
Qualys.
tenable
Invicti
...
ISSUE MAPPING
Grouping by root cause
Mapping to remediation guides
ISSUE DIGESTION
Threat intel severity re-assessment
Issue renaming
Hackability Score
☐ ISC BND assertion failure vulnerability
Highest
☑ Configure HTTP security header
High
☐ Redis server accessible without authentication
Low
Progress-tracking KPI
Prioritized next best action
Step-by-step remediation guides
Ticketing tools

# Who’s happy?

Security Analyst

SWISS POST

**Automate prioritization**

Delegating tedious and boring prioritization tasks

IT Admin

Taboola

**Effective remediation**

Less tickets, more time for strategic initiatives

CISO

Allianz

**Management clarity**

Single KPI & no extra personnel needed

# Let's make vulnerability remediation something to look forward to!

Visit **booth S03** to learn more :)

Autobahn security