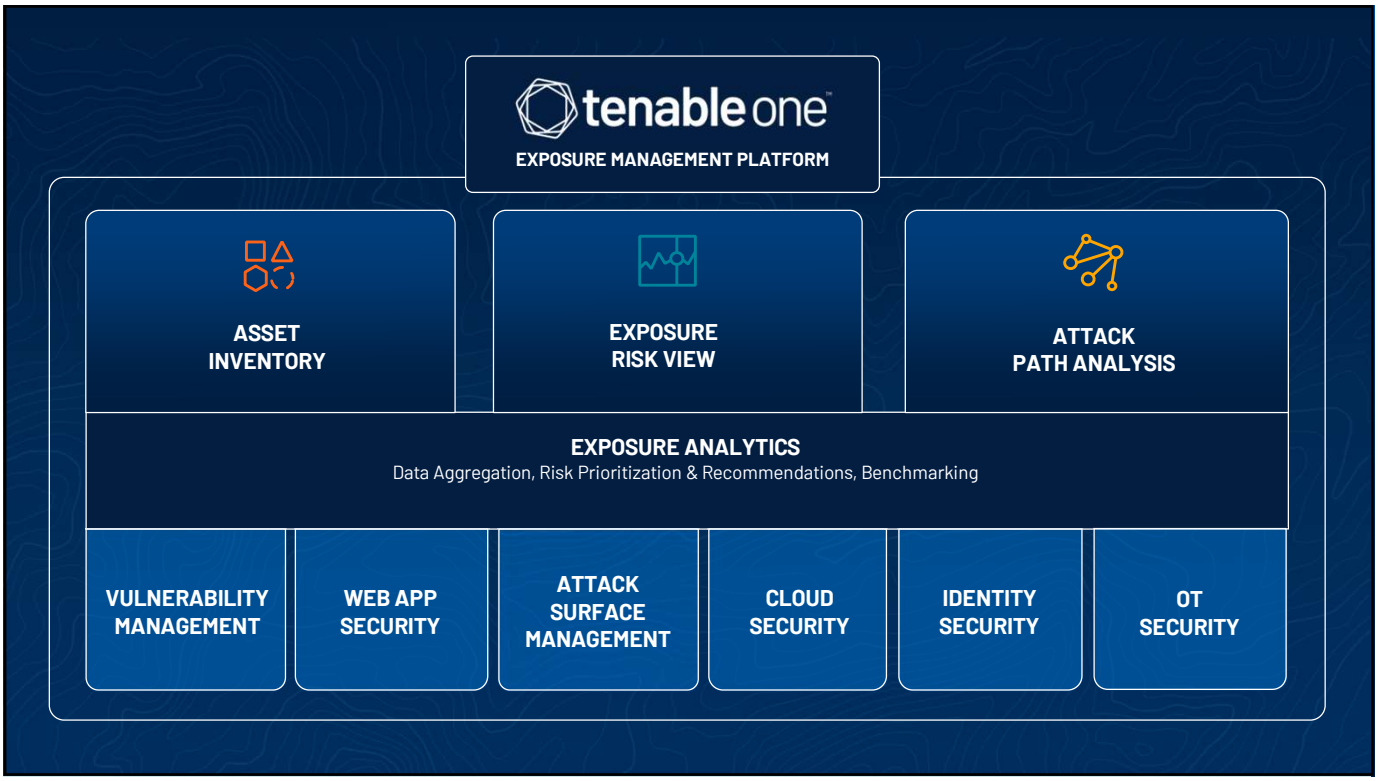
Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025

AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025



AVANTEC
Competence. Security. Trust.

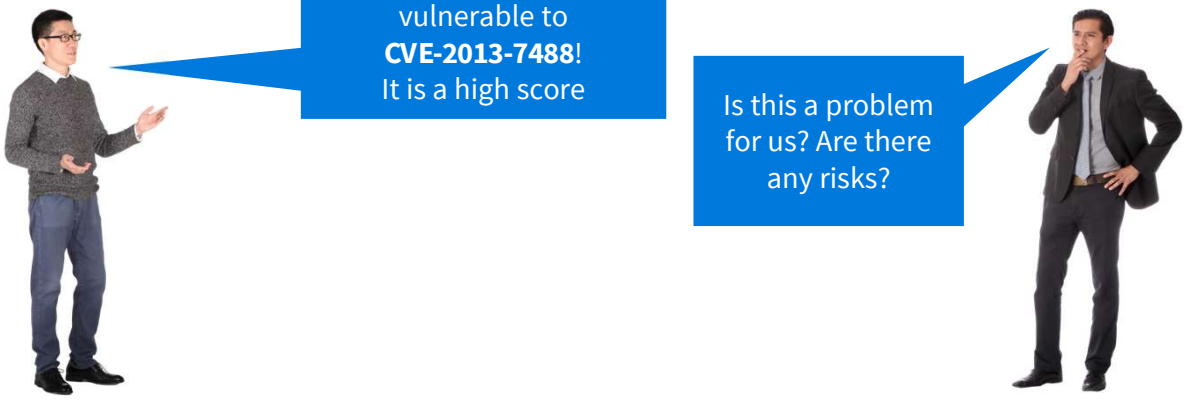
Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025

Agenda

1. **Initial Situation**
2. **Vulnerability Scanning**
3. **Vulnerability Assessment**
4. **Main Challenge**
5. **Further Challenges**
6. **Get it Done!**
7. **AVANTEC Approaches – Your Support**
8. **Outlook Implementation AVANTEC VM Service**

tenable

Initial Situation

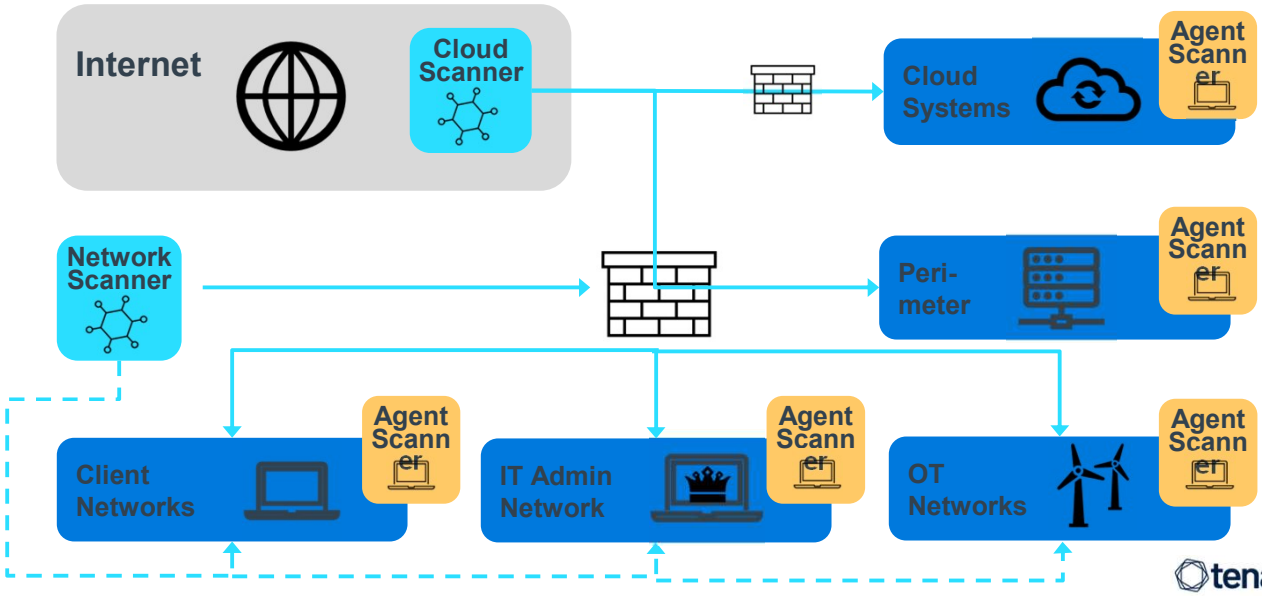


tenable

AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025

Vulnerability Scanning – Big Picture



Vulnerability Scanning - Techniques

Network Scanner

- All TCP/UDP ports are scanned
- Identify open ports and services running on scanned systems
- Identify vulnerabilities according enumerated services
- Launch proof of concept exploits
- Advanced: Provide Credentials for authenticated scans

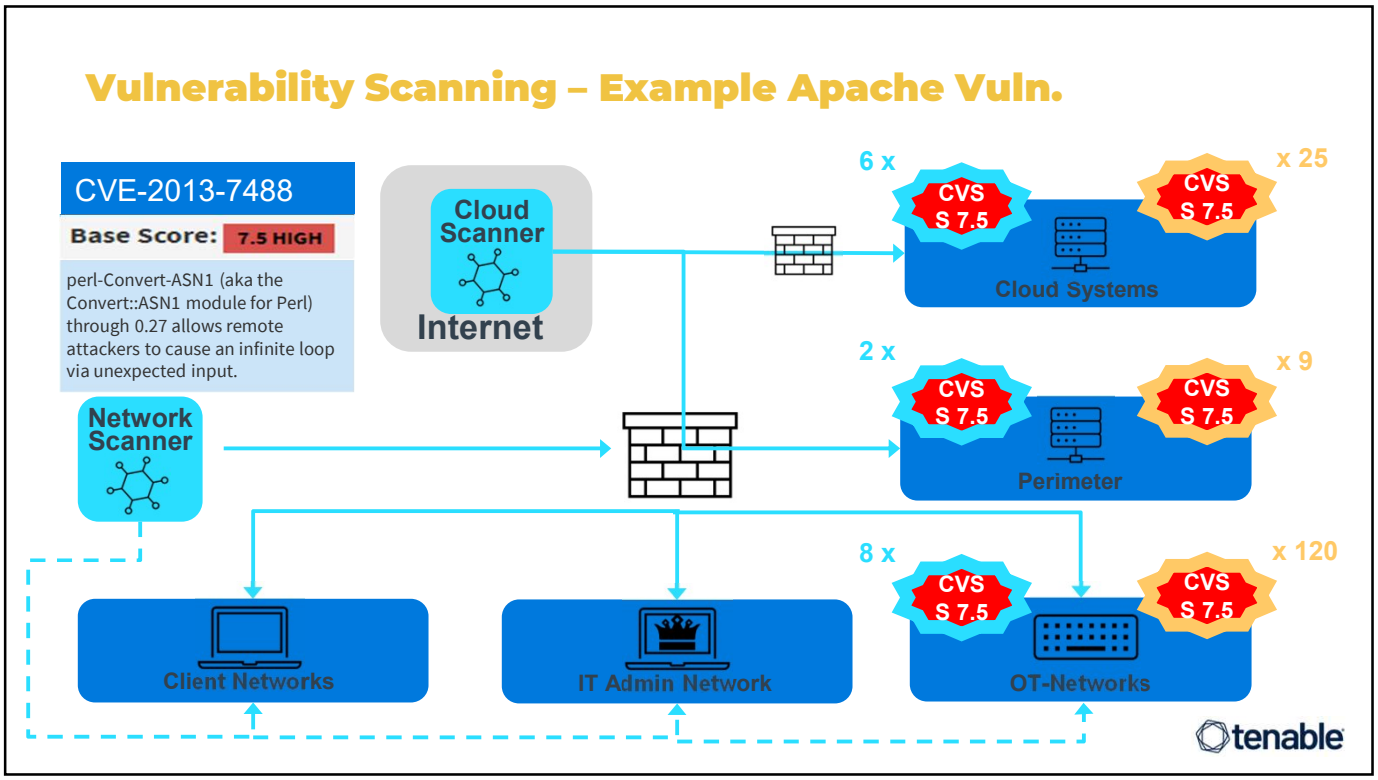
Agent Scanner

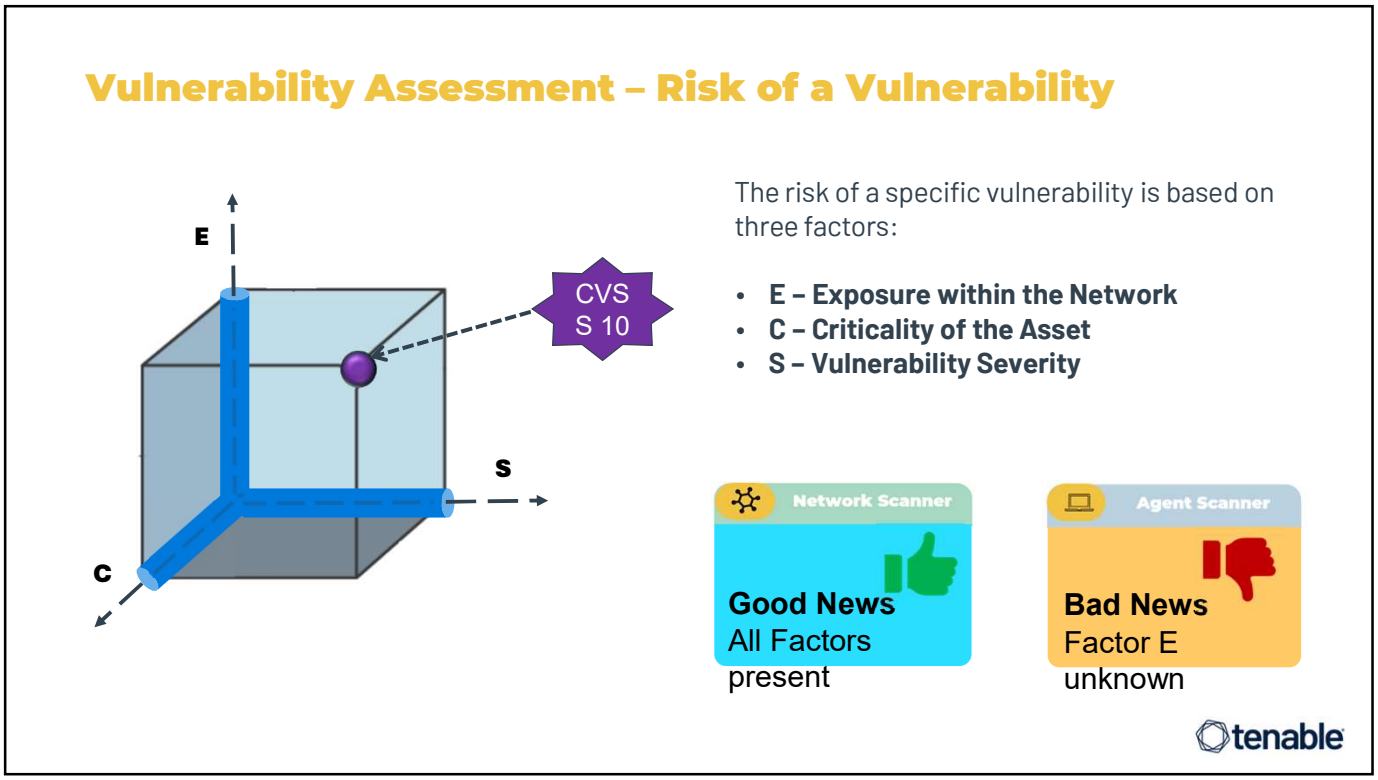
- Install agent on host
- Agent scans executable files
- Identify vulnerabilities according identified files
- No information about affected tcp/udp ports
- Configuration aspects are often not included

tenable

AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025





AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025

Vulnerability Assessment

Network Scanner

Simple and fast: Vulnerable or not vulnerable

- Sometimes:
  "Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number"

Agent Scanner

Often very difficult do decide if vulnerable or not

- Example: CVE-2013-7488: Can the Perl vulnerability be exploited?
- Additional metrics can help
- At least 10 minutes for every vulnerability

tenable

Main Challenge – Facts and Figures

~ 15 **Perimeter Systems**

~ 65 **Workstations**

~ 70 **Servers**

		Perimeter	Clients	Client Services	Client Servers	All Hosts
Active Scanning	Critical	1	0	Not impl.	0	Not impl.
	High	4	0	Not impl.	21	Not impl.
	Medium	2	0	Not impl.	85	Not impl.
	Low	3	130	Not impl.	5	Not impl.
Agent-based	Critical	205	419	N/A*	1'027	1'651
	High	4'212	7'571	N/A	19'877	31'596
	Medium	8'966	3'272	N/A	34'998	47'235
	Low	132	226	N/A	541	899

* N/A = not available resp. not possible to implement

tenable

AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025

Main Challenge - Conclusion

Number of Vulnerabilities

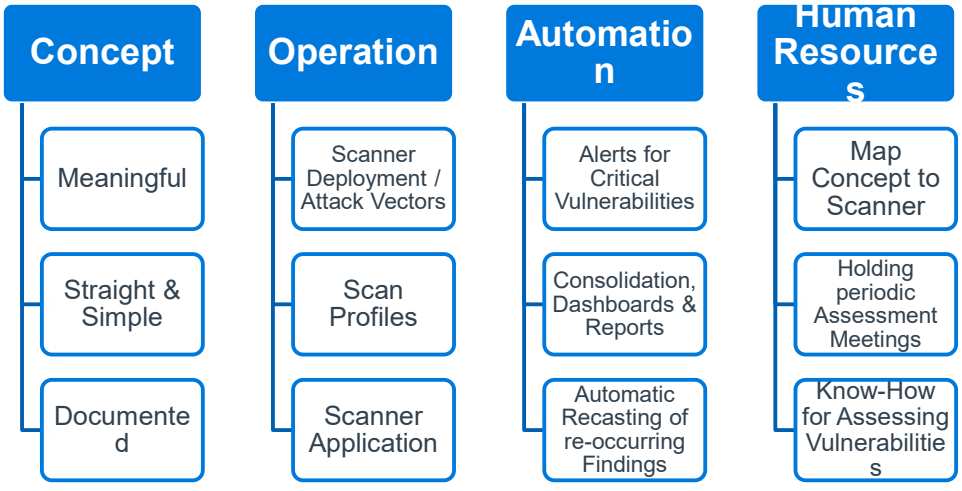
- There are **"few" vulnerabilities** using the **network scanner**
- There are **tons of vulnerabilities** using the **agent scanner**
- There are **tons of "false positives"** for "our" environment using **agent scanner**

Vulnerability Assessment

- Vulnerability assessment for **network scanner** findings is **easy**
- Vulnerability assessment for **agent scanners** findings is **time-consuming**

tenable

Further Challenges Vulnerability Management



tenable

AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025

Get It Done!

Self-Made

Implement a vulnerability management process yourself incl. creation of concept, operation of platform, and execution of vulnerability assessments.

AVANTEC Vulnerability Scanning Service

- Best of Breed Technology
- Define fixed Set of Scans
- Apply Annual Adjustments

AVANTEC Vulnerability Management Service

- Best of Breed Technology
- Define Scans Step-By-Step
- Documented KISS Concept
- Automation & Alerting
- AVANTEDC Support (Incidents / Assessm.)

tenable

AVANTEC VM Service – Details Key Points

AVANTEC VM Service

Usage of Best of Breed Technology

- Ability using Active (Network) Scanning
- Ability Agent-based Vulnerability Identification
- Ability to assess exposure of the environment

Risk-Based VM Concept

- Concept following KISS (Keep it straight and simple)
- Concept based on Best of Breed Technologies
- Documented VM Policy & Concept

Step-By-Step

- Same effort every week/month
- Knowhow shifts over months from AVANTEC
- Master Scan Level by Scan Level
- Rule of thumb: 10 Vulns/Week

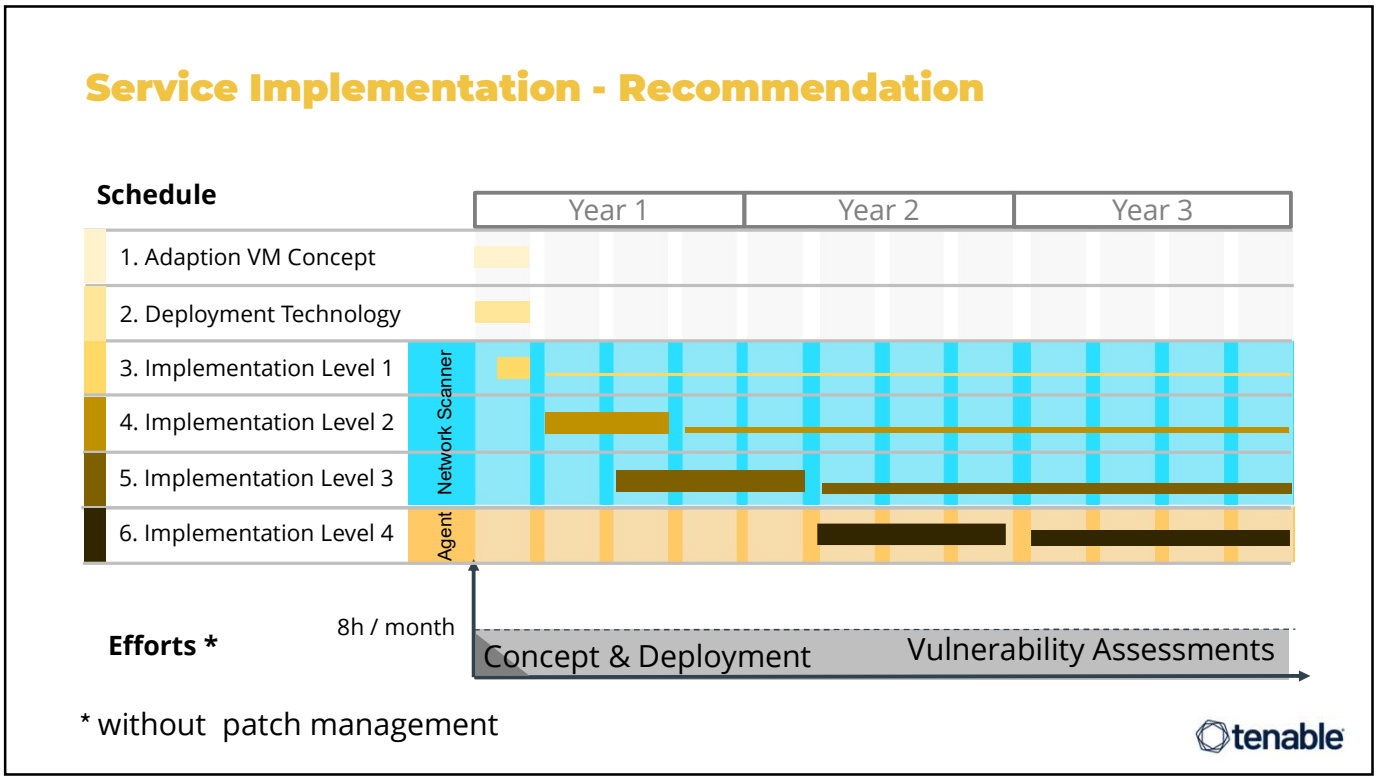
Automation & Alerting

- Trigger alerts for high and critical vulnerabilities
- Manual Triage by AVANTEC CDC
- Auto-Generation of recasting rules
- Consolidate all scans in one report

tenable

AVANTEC
Competence. Security. Trust.

Webinar: Effektives Vulnerability Management mit Tenable.one
21. / 30. Januar 2025



AVANTEC
Competence. Security. Trust.