Cyber Exposure im OT-Umfeld

Wie Tenable verwundbare Systeme und ausnutzbare Schwachstellen identifiziert

Max Rahner, Tenable
Senior Manager Business Development

17.09.2025, Congress Park Hanau

U ÀŸš ¥ÈÐm¡ ŸĆ¥¡ ŸÐÀÈÀÔ╙4¯Ł^ Ð šÀ

4¯Ł^ Ð šÀ Ð ÀÔ ş ÀšÓ À∆¿¥šÀÐ+ · ¿ Àš* À šÀ¿ Ðš Á^ ╠¥ÐÓ €
ÀÔÀš Ÿ^ ŸÀÔÇ ¥ŸšÐ ŸÀÔÈ ŸÁÀ ş^ Ô╔Ô' šÀ ÀšÔ¥² Ð ÀÔ² Ď Ć€šΔ
v V0 Δ¥Ð ^ ÀÔ ¥ÈŸ¥ ╠€ ÀÐÀÔ È ŸÀÔ4 Ô↑² ÐÐ¥² ' ÀÔ╔
* À šÀ¿ ÐÀš'^ È Ď ÔÀŸÓ ÀÔ

ÅÀšÓ À∆¿¥š

Å^ š'πÈÀšÀÐ ÈÀšÀÔÐ À Ð¥² Ð
=ÀŸÈÁ^ Ô ' ² š¥ € ÔÀÔ╠
¾¿ Àš¿ ^ šΔÀÔΔÀÔ i À¡ Ÿ ÀÔ² ÔΔ╔
m¡ ŸĆ¥¡ ŸÐ ÀÈÀÔ╥

² ÐÔ² Ď¿ ¥š

i ÐÁÀÔ╠ÀÀÔ'¥¡ Ÿ Ď ÀšÁÀÔÔÀÔ
² ÔΔ¥² ÐĎ Ô² ĎÀÔÐÔΔ ╠^ š¥ÈÀÓ
¥¿ Àš ▪Ô╔ŸÀ€ Δ▫ ¥² Ð ÀÔ² Ď
ĆÀšΔÀÔ╥

ÐÓ Ł¥¡ –'² È

i ÐÁÀÔ'¾š À╔À šÀ¿ Ð▪
Ð¥¿ €π ╠ Ó Ð Ď ÀÔÀš€š² Ô' ╠
0 ¥ ÀÔÐ ŸÀšŸÀ€² ÔΔ▪Ô À' š€π

tenable

Predictive Maintenance: Cloud

f š^ ¿ÈÄÓ 1: Was ist überhaupt OT?

Abhängigkeiten zu anderen Prozessen, z.B. ERP

OT ist keine Asset-Klasse oder Gerätetyp.

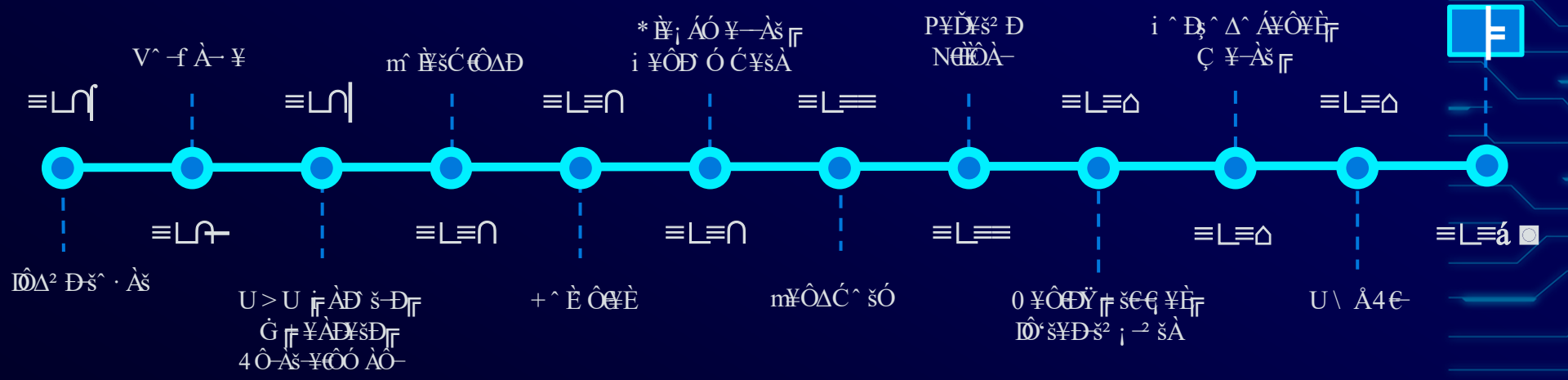
OT ist die Antwort auf die Frage, wofür ein Asset genutzt wird.

tenable

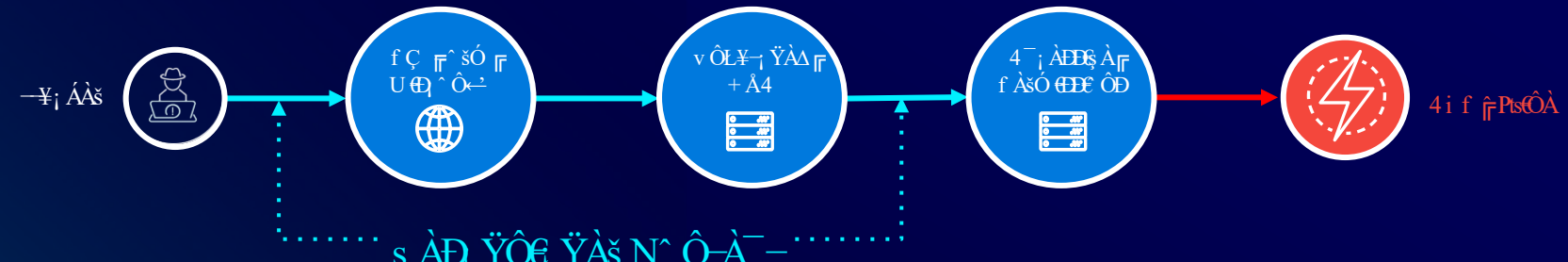
>šˆþÀ Ô’š€‘ÐĆÀÈÈÀÔ€ÔĻÀÔĻÀš’¥Ô’ÀÔÀÔM¥ŸšÀÔ

Ç ˆ ĻÈÀ’ ÀÔΔ€ÀĻ ÀÓ À€ÔÐ¥Ó ÁÀ€–ÀÔ├

Verknüpfung mehrerer Technologien



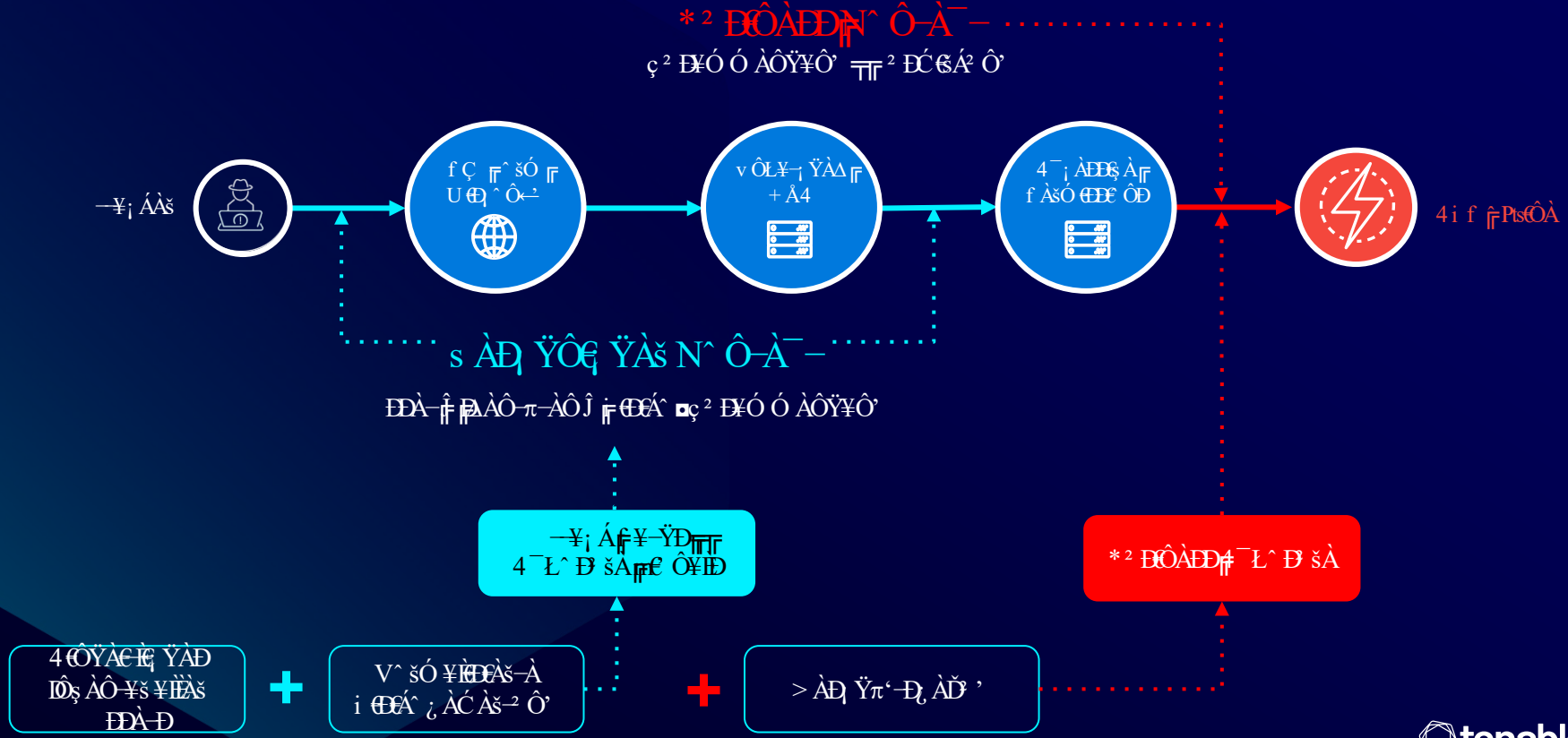
f š^ ¿ ÈÀÓ ╒╚NÀ¢Ô¥² ÐšÀ¢ ŸÀÔΔÀš –À¡ ŸÔ¢ ŸÀš N^ Ô–À¯–╘Ó ╒¯Ł^ Ð³ šÀ╒³ şÀšÐ–ÀŸÀÔ



tenable


LSASS Memory
Exploitation for Privilege Escalation
Exploitation of Remote Services
Program Download
(2) Path Interception by PATH Environment Variable
APAWS
10.100.112.152
Logged in
Administrator
APADOMAIN\administrator
Member of
Administrators
APADOMAIN\administrators
Admin on
APADC
10.100.112.151
Exploit
CVE-2017-0144
Affects
apaeng
10.100.112.20
44818
I16er_apa

tenable


*² ÐŒÔÀÐÐ╣Nˆ Ô–À¯–
ç² Ð¥Ó Ó ÀÔŸ¥Ô’ ╤╤² ÐĆ€šÁ² Ô’
f Ç ╔ˆ šÓ ╔
U Œ¦ˆ Ô‹’
v ÔŁ¥¬¡ ŸÀΔ╔
+ Å4
4¯¡ ÀÐĐş À╔
f ÀšÓ ŒÐ€ ÔÐ
¬¥¡ ÁÀš
4 i f ╔PtsŒÔÀ
s ÀÐ¦ ŸÔ€¦ ŸÀš Nˆ Ô–À¯–
ÐÐÀ¬Ê╔ÐÀÔ π¬ÀÔĴ ¡ŒÐÁˆ ◘ç² Ð¥Ó Ó ÀÔŸ¥Ô’
¬¥¡ Á╔¥¬ŸÐ╤╤
4¯Łˆ Ð³ šA╔€ Ô¥ÐÐ
*² ÐŒÔÀÐÐ╣¯Łˆ Ð³ šÀ
4 ŒÔŸÀ€Ê¦ ŸÀÐ
ÐÔş ÀÔ¬¥š ¥ÐÐÀš
ÐÐÀ¬Ð
+
Vˆ šÓ ¥ÐÐŒÀš–À
¡ ŒÐÁˆ ¿ ÀĆ Àš–² Ô’
+
> ÀÐ¦ Ÿπ‘¬Ð¿ ÀÐ³ ’

tenable

z ¿ ÀšĆ¥¡ Ÿ² Ô’ ĐÁ¥Ó Às¥Đ

Å² ÌÔÀš¥¿ ŒĆÀĐ

- ➔ —šĆĢ¥È
- ➔ ⌠é ÀΔĆ Ó
- ➔ ⎓Ÿ€ Ÿ

0 Às ÑˆÔ–À¯–

4 Vs m+ B4 I0 4 s

Å² ÌÔÀš¥¿ ŒĆÀĐ

- ➔ —šĆĢ¥È
- ➔ ⌠é ÀΔĆ Ó
- ➔ ⎓Ÿ€ Ÿ

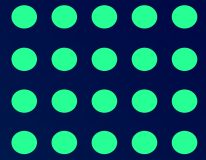
tenable

s À¡ ŸÔŒÐ¡ ŸÀÔ€ÔÐ╒À–š€À¿ Ì€¡ ŸÀÔç² Ð¥Ó Ó ÀÔŸ¥Ô’ ¾¿ ÀšÐÀ–ĎÀÔ

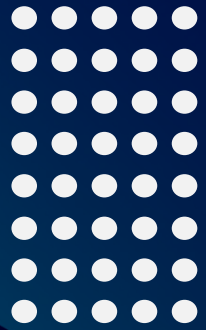
² ‘ΔÀ¡ ÁÀÔΔÀš╒
Ô’ š€‘Ð┴π¡ ŸÀ

∩

DΔÀÔ€Ð€ÀÐ



ÐÐÀ–Ð

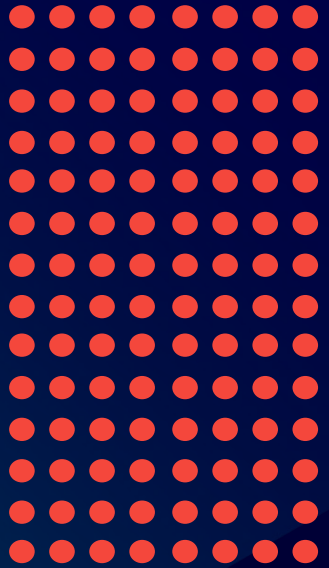


4šÁÀÔÔÀÔşˆÔ

şÀšÓ À€¿¥šÀi €Ð€ÁÀÔ

≡

Å² ÌÔ┌┌┌┌Ð¡ˆÔ←┌┌┌┌¯¡ ÀÐÐ╣ÀšÓ €ÐÐ€ ÔÐ

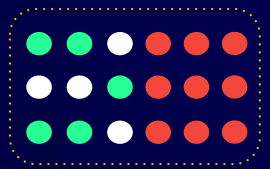


0 ¥šÐ–ÀÌË Ô’ ΔÀÐ

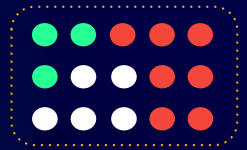
*² ÐŒÔÀÐÐ╒Nˆ Ô–À¯–

⌂

*² ÐŒÔÀÐÐ╒mÀšş€¡ À╒



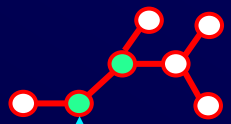
*² ÐŒÔÀÐÐ╒šˆ¡ ÀÐÐ╒



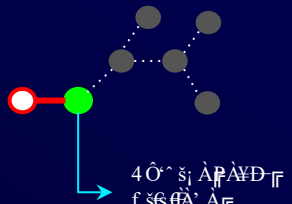
* ÀŸÀ¿ ÀÔΔÀš

4¯Ł^Ð² šÀ

4



4¯¡ ÀÐÐş À╒
U¥¡ ŸŒÔÀ╒
f ÀšÓ €ÐÐ€ ÔÐ

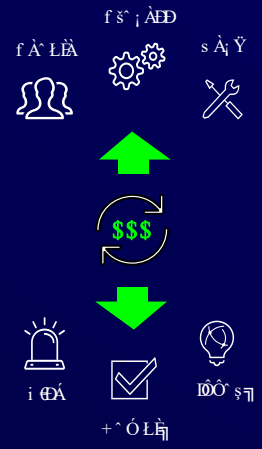


4Ô’ˆš¡ À╒À¥Ð–╒
f šş€ÐÀ’ À╒

Nˆ Ô–Œ²€ÀšÌ€¡ ŸÀ

f š^ ĎÀÐÐ’Ł–ÓŒÀš² Ô’

5



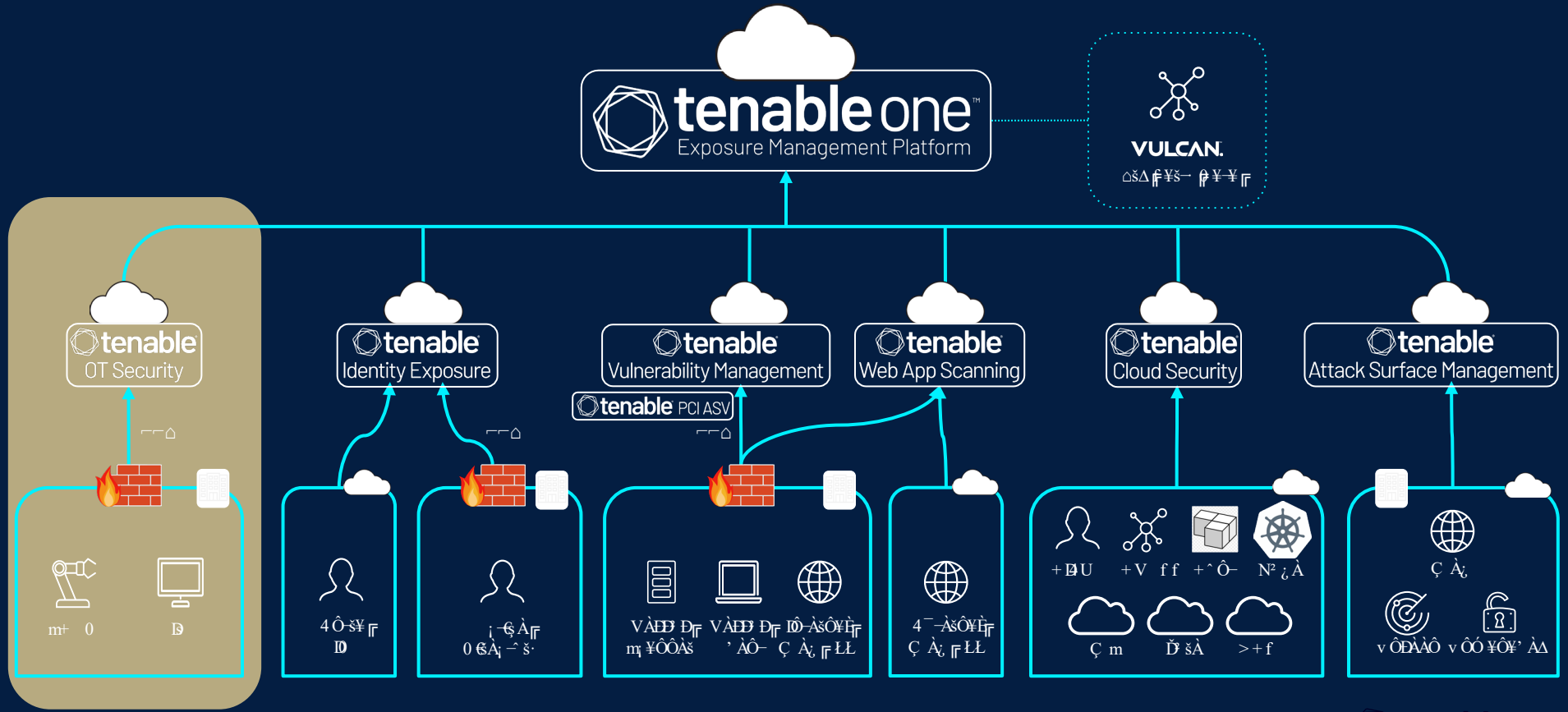
DΔÀÔ€6–Á¥–€ Ô¥ÌÈÀš ÐÐÀ–Ð╠╒
€Ô–ÀšÔ╠╒¯–ÀšÔ╒Ð’ Ć€À
DΔÀÔ€π–ÀÔ

s À¡ ŸÔŒÐ¡ ŸÀ4šŸÀ¿² Ô’ ╠╒ΔˆŸ
² ÔŁš€ šŒÐÈÀš–

Å ÀšÁÔ³Ł‘ÀÔşˆÔ╒ÐÐÀ–Ð╠╒
DΔÀÔ–€π–ÀÔ╠╒À¡ ŸÔŒÐ¡ ŸÀÔi €ÐÁÀÔ
² ÔΔ╒É˜’ Ì€¡ ŸÀš ² ÐĆ€Á² Ô’ ÀÔ¥² ‘╒
ΔÀÔ╒À–š€¿

Ô’ š€‘Ð‘¥ΔÀ² Ô–ÀšÐ’¡ ŸÀÔ
² ÔΔ╒Ì€Ð¡ ŸÀÔŸ¥ÌÐ×–ÔΔÀÔ

tenable


tenable one
Exposure Management Platform
VULCAN.
tenable OT Security
tenable Identity Exposure
tenable Vulnerability Management
tenable PCI ASV
tenable Web App Scanning
tenable Cloud Security
tenable Attack Surface Management

V¢ Ÿ–Ê² š ╔À¡ ² š€ ╠Ê ÔΔÀšÔ¥² ¡ Ÿ ╔¥‘À–

s ÀÔ¥¿ ÈÀ╠ s ╔À¡ ² š€–

Umfassendes, automatisiertes Asset-Inventar

Risikobasiertes Schwachstellen-management

Angriffs- und Anomalie-Erkennung

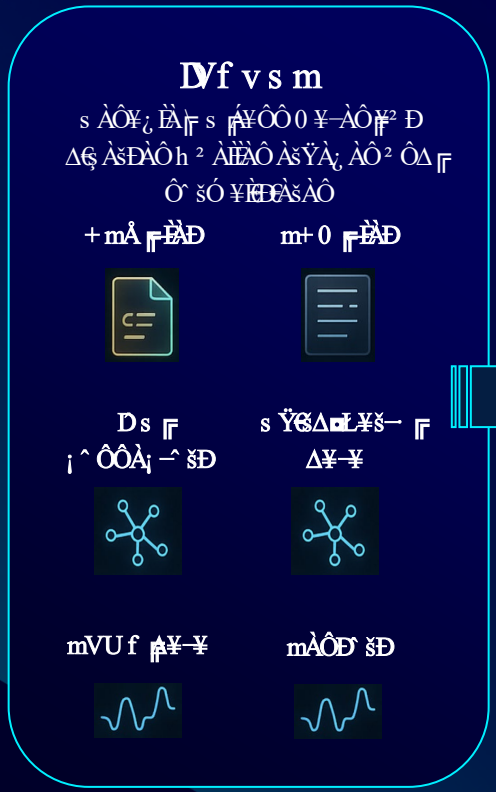
Erkennen und Verfolgen von Konfigurations-änderungen

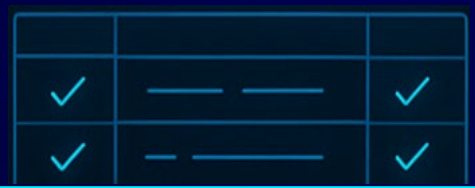
B à * i D0 ╔ Dn+ \ Å4 i à

m4+ v i Ds à ╠U \ VDs \ i DV>

tenable

> š² ÔΔÈ¥’ ÀÔÐ¦ Ÿ¥‘‘ÀÔ╚Ę ¥Ð╔¥Ô╔ę¦ Ÿ–ÁÀÔÔ–╘á¥ÔÔÓ ¥Ô╔ę¦ Ÿ–Ð¦ Ÿ¾ĎÀÔ



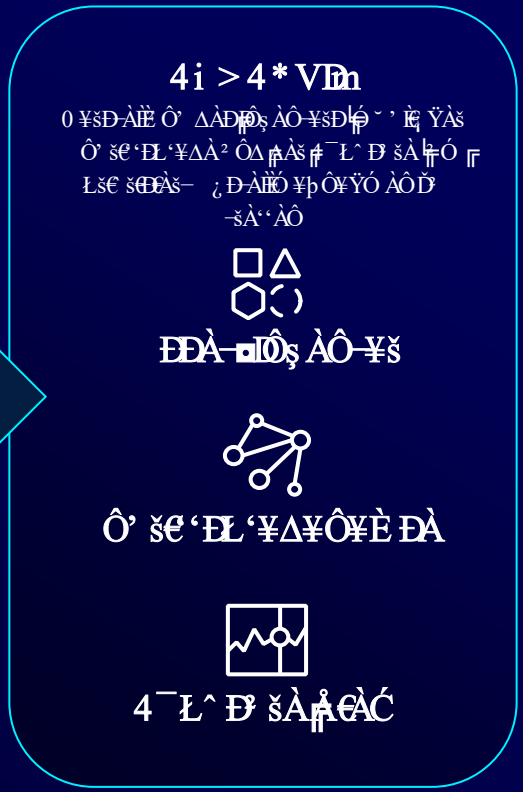


tenable OT Security

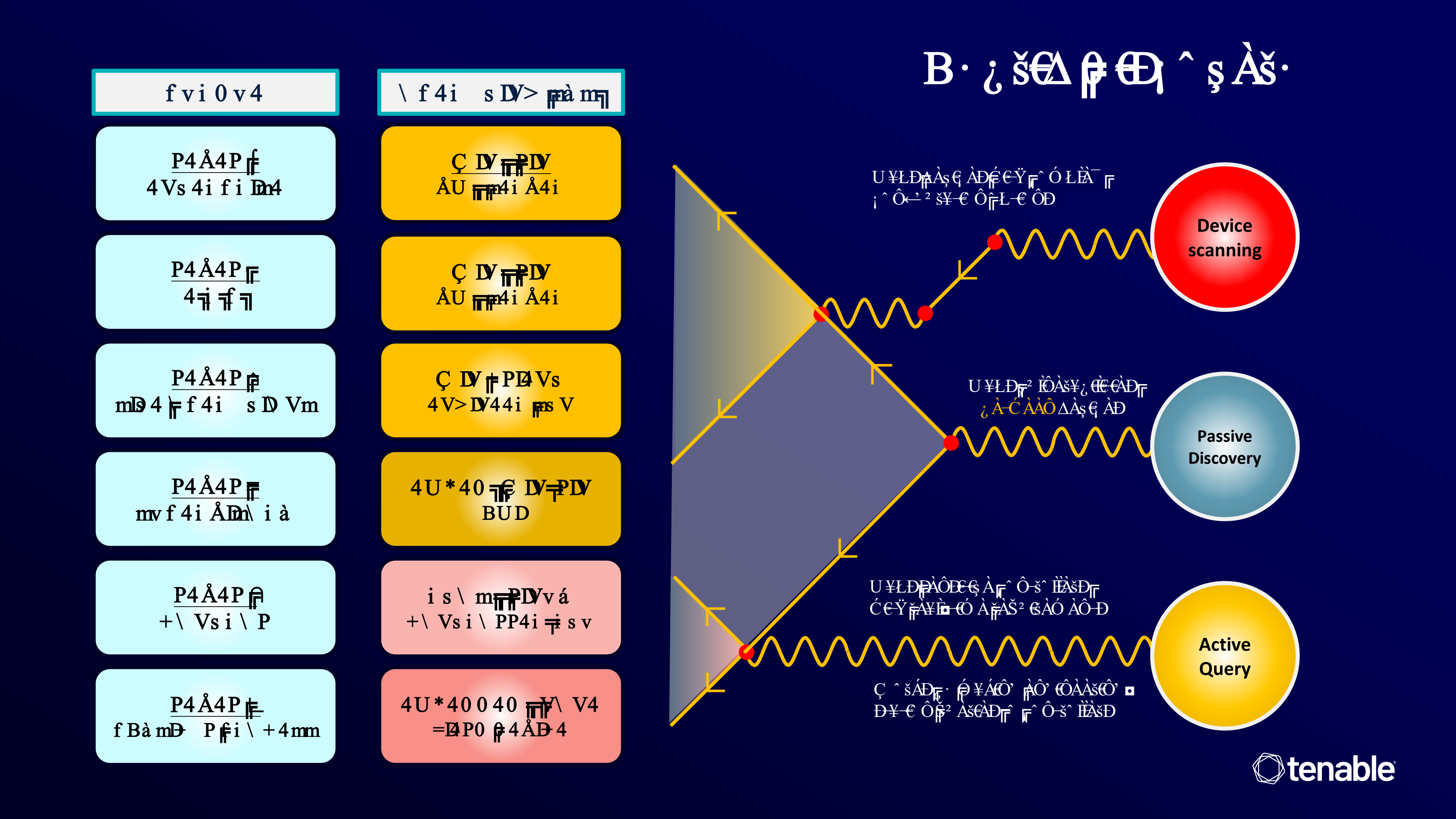
B· ¿ š€Δ╔ę¦ ˆ ş Àš· ╔Ô’ €ÔÀ

Á–€ş À ¿ ‘š¥’ ÀÔ
B ÀšÐ–ÀÈÈÀšÐŁ ÀĎ€–Ð¦ Ÿ

f ¥ÐÐ€ş ÀÐ╔ U ˆ Ô€–˜ š€Ô’

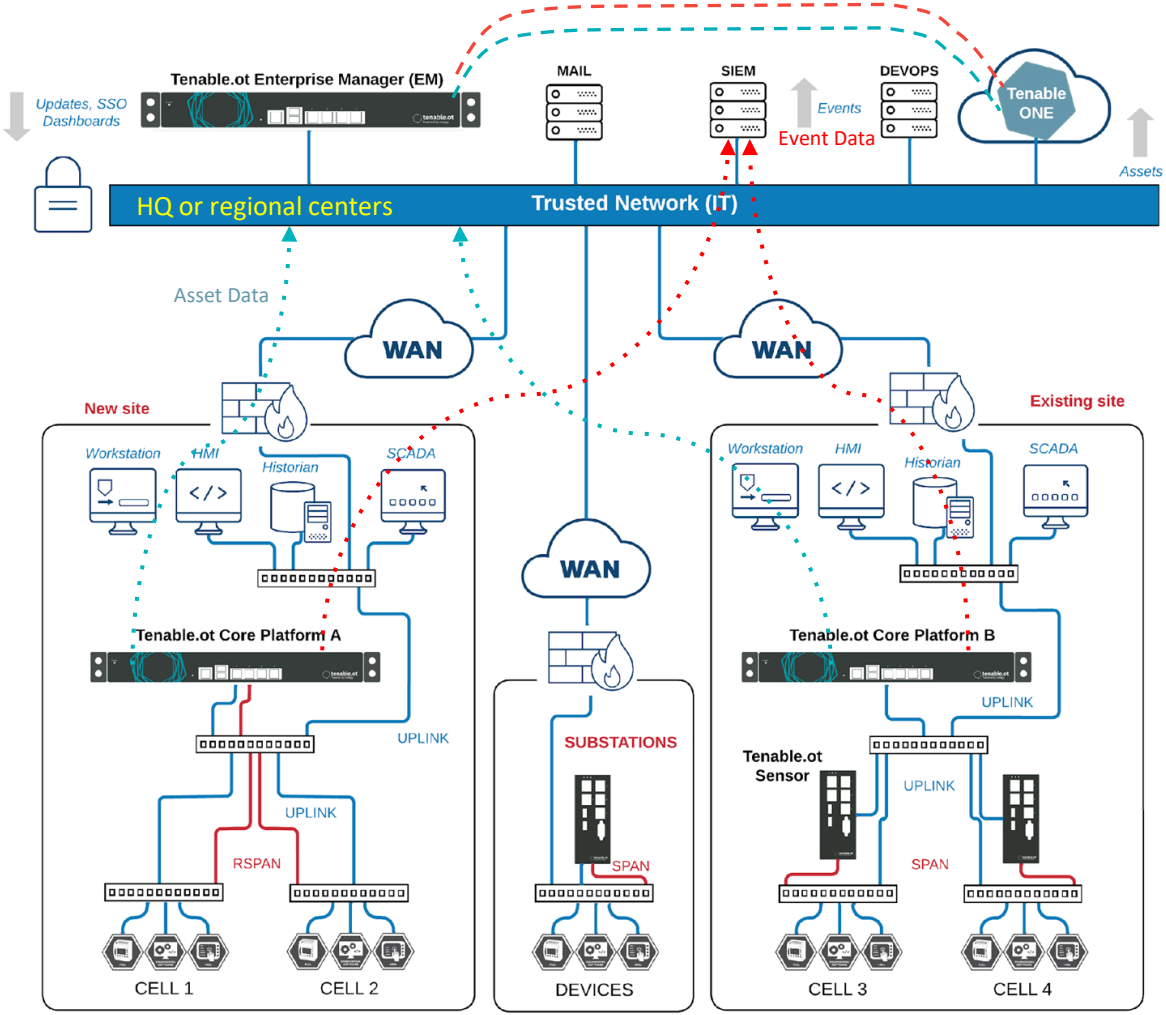


tenable


Device scanning
Passive Discovery
Active Query

s ÀÔ¥¿ ÈÀ╒s ╙

- \ s ╒Ñ^ Ó Ł^ ÔÀÔ–ÀÔ ş^ ÈÐ¬ÔΔ€ ^ Ô¤ŁšÀÓ
- 4 ¯Ł^ Ð šÀ╒ U ¥Ô¥’ ÀÓ ÀÔ–₣Ô╒ÀšÍ + È ² Δ♠s ÀÔ¥¿ ÈÀ╒ ÔÀ♣╒ ş Àš¿ ² ÔΔÀÔ¾¿ Àš Ð ╒ Δ^ Ó ¥€Ô
- \ s ╒Ð ^ ş Àš· ╘ÅU ²╒ÔΔ╒ mÀ¡ ² š€ ÐÞ^ Ô€^ š€Ô’ ╒ ¿ ÈÀ€¿ ÀÔ ş^ ÈÈ ‘² ÔÁ–€ ÔÐ¬ŸÝ€ ^ ŸÔÀ + È ² Δ¤ Ô¿ €ÔΔ² Ô’



Eine bessere Strategie ist gefragt

GEWÜNSCHTE ERGEBNISSE

Unterstützung des Business

Risikominderung

Optimierung von Kosten und Effizienz

Kommunikation und Automatisierung

Prioritäten | Workflow

Anreicherung durch Kontext

Technik | Business

Aggregation und Normalisierung

Assets | Risiken

- Fehlkonfigurationen
- Schwachstellen
- Übermäßige Berechtigungen

WACHSENDE ANGRIFFS-OBERFLÄCHE

AWS | Azure | GCP | Identitäten | Hybride Apps | OT/IoT | Private Cloud/IT

> ÀÆŁšπ¡ ŸÀÓ €–U¥Ô¥’ ÀšÔ¦

tenable

> ÀÆŁšπ¡ ŸÀÓ €–U¥Ô¥’ ÀšÔ¦

tenable

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.

tenable