



*20. Mai 2026*

**17. Bechtle**  
**IT-Forum**  
**Thüringen**  
Steigerwald Stadion Erfurt

**20**  
**26**

**Schwachstellen kennen  
reicht nicht –**

**entscheidend ist ihr  
Status.**

*Wie Enginsight aus Schwachstellen-Daten handlungsrelevante Security-Intelligenz macht.*

DAS PROBLEM

# Die unbequeme Wahrheit

~50.000

neue CVEs allein 2025

*Quelle: NIST NVD*

Das ist mehr als 130 neue Schwachstellen pro Tag. Kein Team der Welt kann alle patchen.



## Kein Kontext

Ein CVSS-Score allein sagt nichts darüber aus, ob das System exponiert oder bereits gepatcht ist.



## Falsche Prioritäten

Teams verlieren sich in Masse statt Klasse – kritische Lücken werden von unwichtigeren überlagert.



## Blindes Vertrauen

Schwachstellen-Scanner liefern Befunde. Wer kümmert sich um den Status danach?

# Status ist entscheidend – 4 Dimensionen



## Exponiert?

Ist das System öffentlich erreichbar?

*Bsp: Log4Shell auf internem Server – kein direktes Risiko.*

## Aktiv angreifbar?

Wird die Lücke aktiv in freier Wildbahn ausgenutzt?

*Bsp: CVSS 5.8 – aber aktiv durch Ransomware-Gruppen exploited.*

## Gepatcht?

Gibt es bereits einen Fix – und eingespielt?

*Bsp: Patch als 'erledigt' – aber nur 60 % der Hosts aktualisiert.*

## Zuständig?

Wer ist Owner – wann ist Deadline?

*Bsp: IT sagt 'Dev', Dev sagt 'Ops'. Offen seit 4 Monaten.*



# Der typische Alptraum

## 1 Scanner findet 4.200 Schwachstellen

CVSS  $\geq 7$  -> 820 als High markiert

## 3 2 Wochen Arbeit für... nichts Kritisches

Die wirklich gefährliche Lücke (CVSS 5.8, aktiv exploited) bleibt offen.

## 60 % aller Breaches 2024

hatten eine bekannte, ungepatchte Schwachstelle als Ursache – obwohl ein Fix verfügbar war.  
Quelle: Verizon DBIR 2024

## 2 Team priorisiert nach CVSS-Score

Ohne zu wissen: 600 davon sind bereits gepatcht oder nicht exponiert.

## 4 Incident

Genau diese Lücke wird ausgenutzt. Der Angreifer war schon 3 Wochen im Netz.

## Real: SharePoint ToolShell (2025)

Patch war verfügbar. Nicht ausgerollt. 396 Systeme kompromittiert, Angreifer 2+ Monate aktiv – Government & Healthcare.

**Ohne Status-Kontext wird Security zur Lotterie. Mehr Arbeit, mehr Risiko, weniger Schutz.**



# Der Enginsight Ansatz



## Hacktor

Automatisiertes  
Pentesting

Findet ausnutzbare Schwachstellen – nicht nur theoretische. Blackbox, Greybox, Lightgreybox.



## Pulsar Agent

CVE-Management  
& Host-Security

Inventarisiert Assets, mappt CVEs auf tatsächlich installierte Software, trackt Patch-Status.



## SIEM + SOAR

Korrelation  
& Automatisierung

Korreliert Schwachstellendaten mit Live-Events. Playbooks reagieren automatisch – priorisiert.






**Ergebnis: Jede Schwachstelle trägt ihren Status mit sich – exponiert, aktiv exploited, Owner, Deadline, gepatcht.**



J E T Z T L I V E

# Schwachstellen-Status in der Praxis sehen.

-  Hacktor findet ausnutzbare Schwachstellen – live
-  Agent zeigt CVE-Status je Asset in Echtzeit
-  SIEM korreliert & priorisiert automatisch



ENGINSIGHT

# LASSEN SIE UNS DIE WELT GEMEINSAM SICHERER MACHEN.

Demo →

Watchdog → Hacktor → Pulsar Agent → SIEM →  
Observer → SIEM

## IHR ANSPRECHPARTNER

Christoph Rütten

Account Manager ·

✉ [christoph.ruetten@enginsight.com](mailto:christoph.ruetten@enginsight.com)

☎ +49 151 237 44 657

📍 Enginsight GmbH · Leutragraben 1 · 07743 Jena