SPIE

X-SPIErience Day 2020

DIGITALE SOUVERÄNITÄT

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
DIGITALE SOUVERÄNITÄT

SPIE

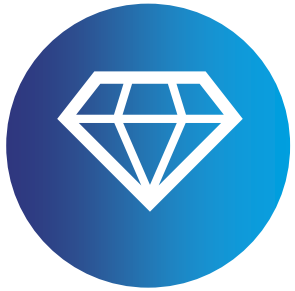
Effizientes Schwachstellenmanagement mit KI-Infrastruktur aus der Schweiz

MARCO GAUCH

Network Consultant
SPIE ICS

Digitale Souveränität – Der Schlüssel im Zeitalter von KI

Daten als strategischen Vermögenswert
Schwachstellendaten sind hochsensibel und geschäftskritisch.



Souveränität bedeutet Kontrolle
Souveränität gewährleistet eine bessere Kontrolle über diese Daten, deren Zugriffe und über regulatorische Vorschriften.

Die Herausforderung
Souveräne KI im Schwachstellenmanagement ohne Kompromisse bei:
Wirtschaftlichkeit, Geschwindigkeit und Flexiblität

Neue Risiken für die digitale Souveränität durch KI

Vertraulichkeit

Unbeabsichtigte Offenlegung sensibler Schwachstellen

Sicherheit

Einsatz von LLMs und Tools zur Analyse und Priorisierung von Schwachstellen.

Verfügbarkeit

Abhängigkeit von externen KI-Services und Cloud-Infrastruktur.

Governance und Auditierbarkeit

KI beeinflusst Priorisierung und Behandlung von Schwachstellen.

Infrastrukturkontrolle

Verarbeitung sensibler Schwachstellendaten erfordert kontrollierte Umgebung.

Aufbau souveräner KI

Daten- und Modellmanagement

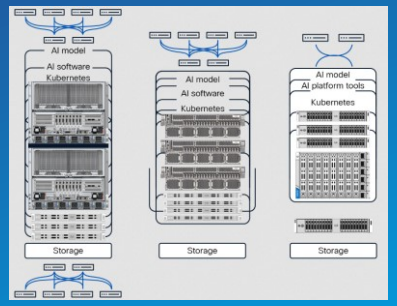
Verständnis, wo die Schwachstellendaten und Modelle liegen

Edge und Datennähe

KI näher zur Infrastruktur bringen mit dem Cisco Edge

Einsatz souveräner KI-Infrastrutkuren

Verlassen Sie sich auf die modularen AI-PODs von Cisco



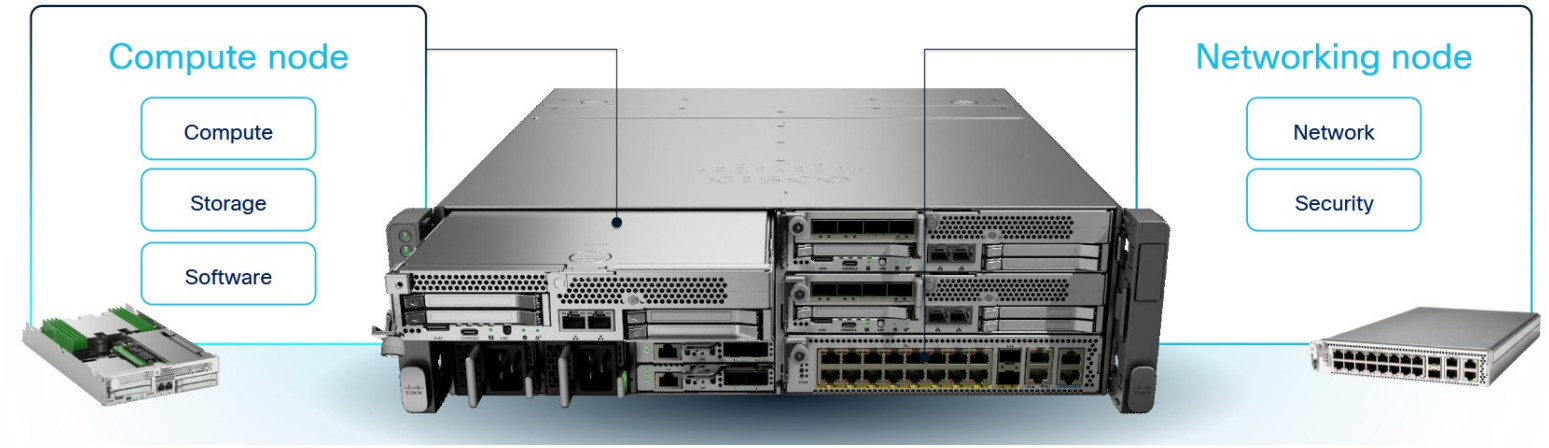
Governance & nachhaltiger Betrieb

Beratung, Integration, Betrieb und Governance durch SPIE ICS

Wie kann uns Cisco unterstützen?

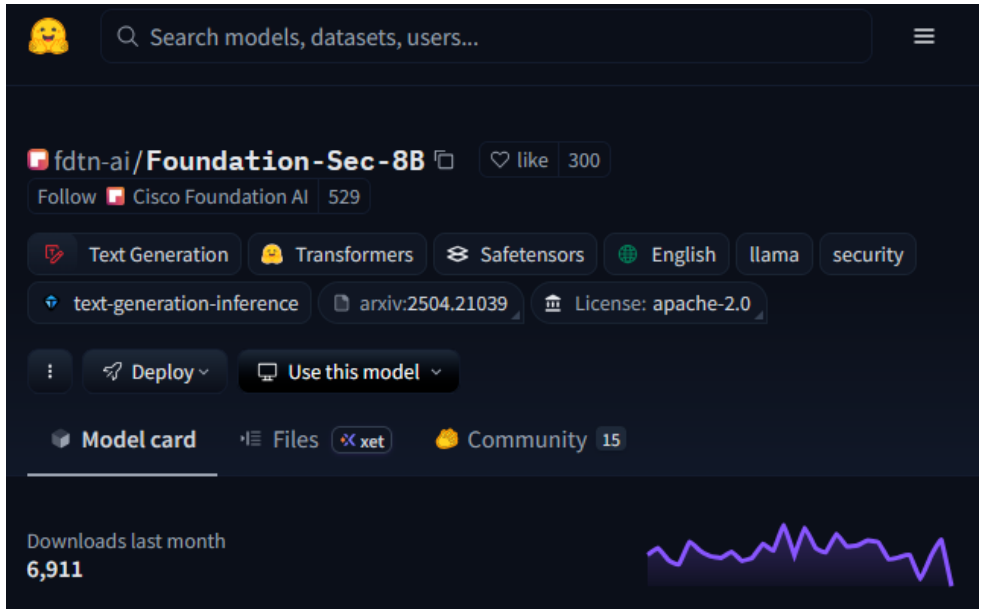
Hardware - Cisco Unified Edge

- Netzwerk, Security, Compute in einer Plattform
- Compute am Edge
- Zentrale Orchestrierung



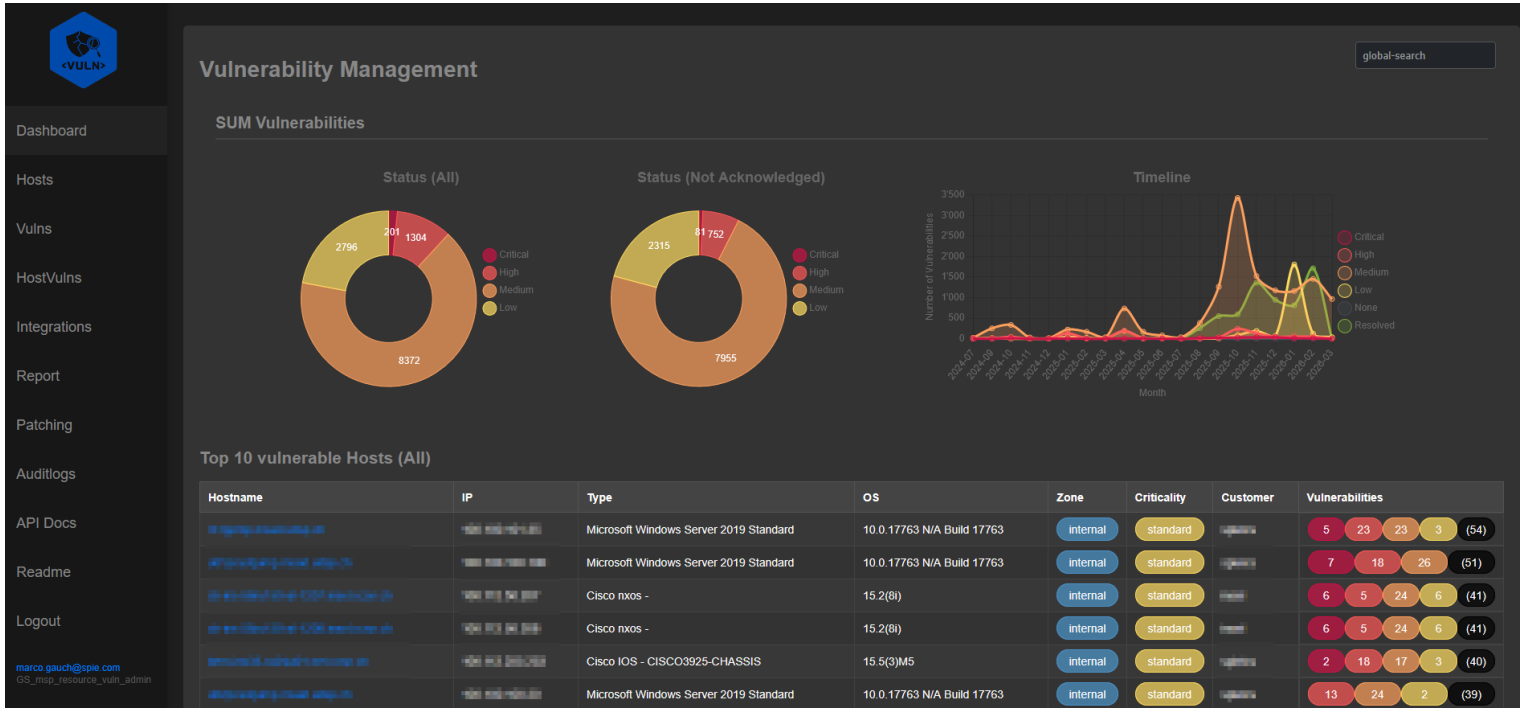
Wie kann uns Cisco unterstützen?

Foundation-Sec-8B – lokal einsetzbarer, cybersecurity-fokussierter **LLM**, der Organisationen hilft, Schwachstellen systematisch zu identifizieren, zu priorisieren und Sicherheitsanalysen zu automatisieren, während Datenhoheit und regulatorische Compliance gewahrt bleiben.



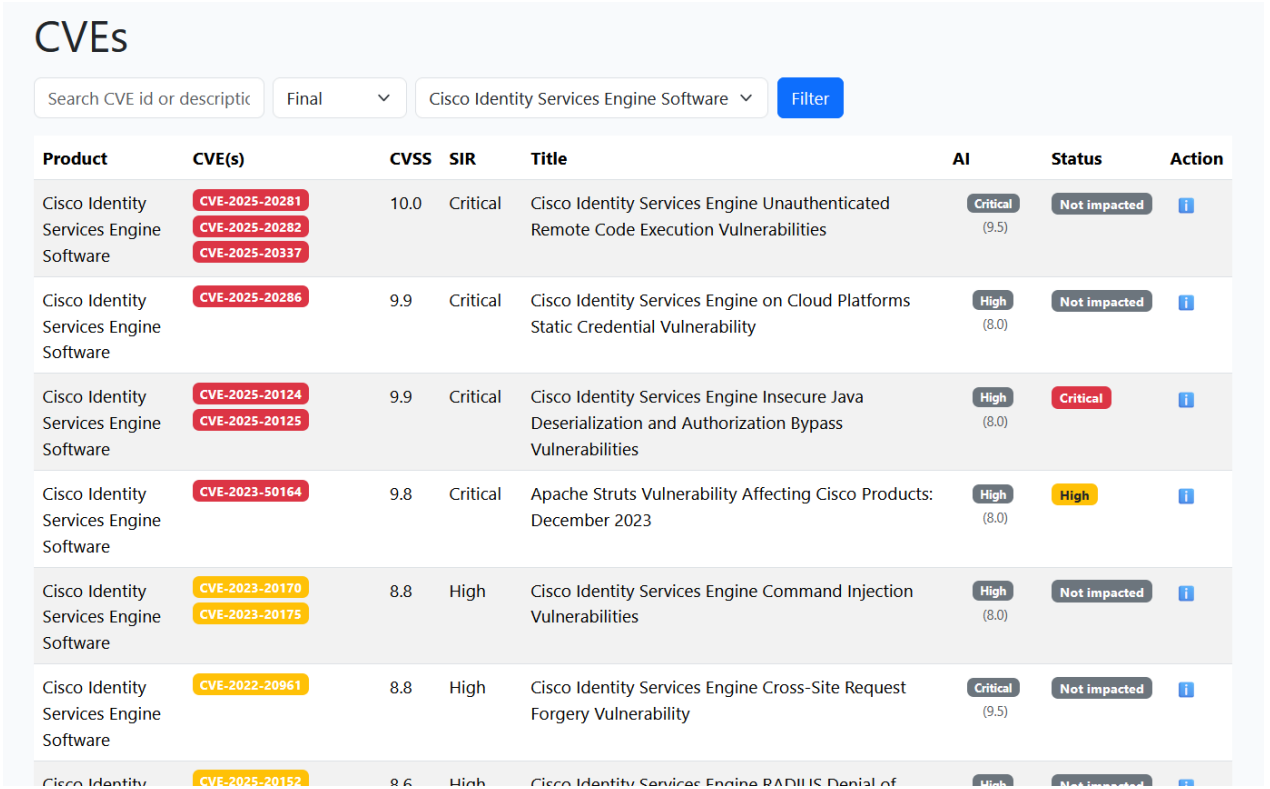
SPIE’s etablierten Vulnerability-MGMT as a Service

- Kontinuierliche **Identifikation** von **Schwachstellen**.
- Konsolidierung **unterschiedlicher Quellen**
  - Cisco openVuln API
  - Fortinet PSIRT
  - CVE Mitre
  - Nessus Scans

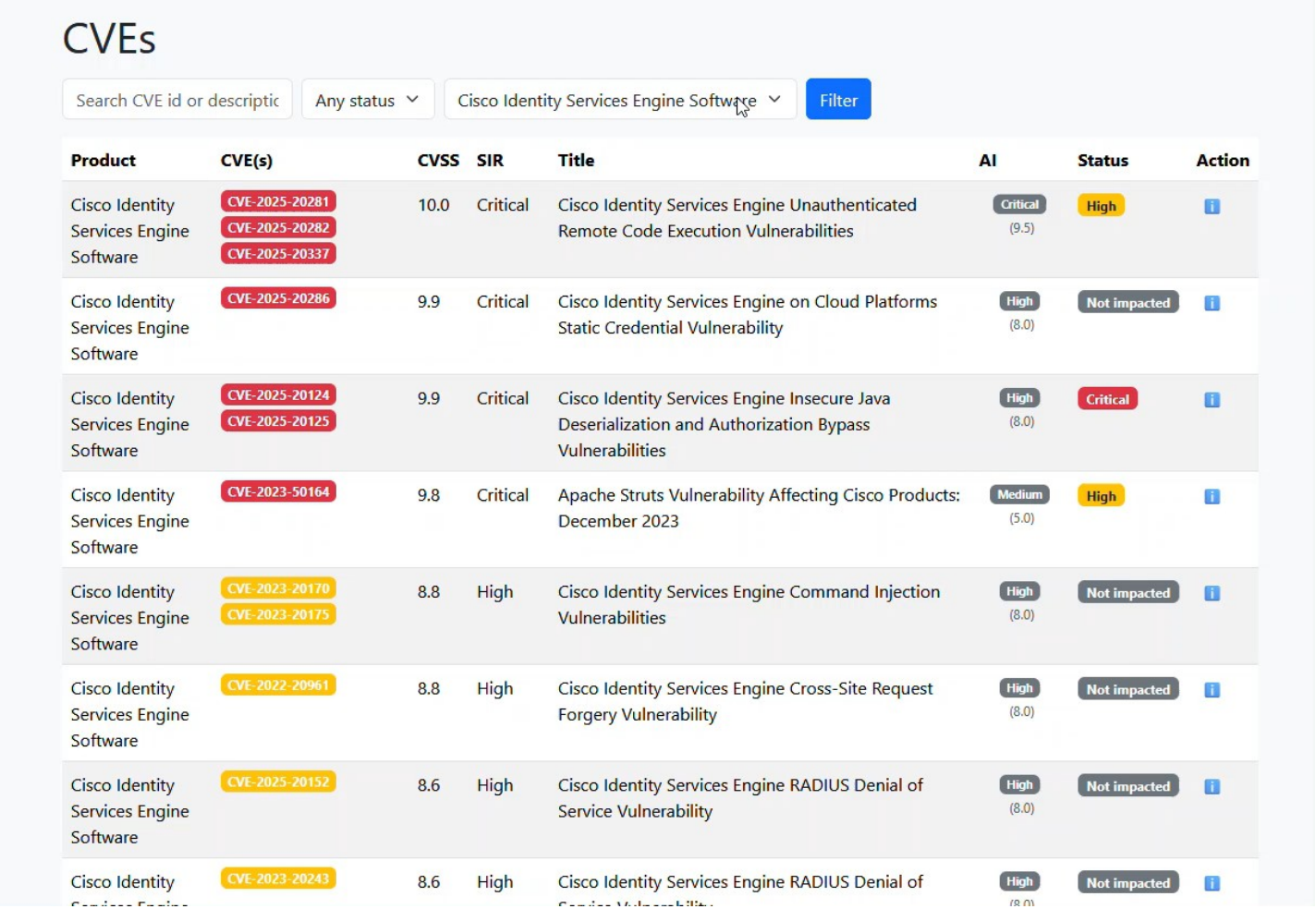


SPIE’s AI-Vulnerability-Agent

- Verwendung von **lokal** eingesetztem **Foundation-Sec-8B** LLM
- Kontinuierliche **Identifikation** von Schwachstellen
- **Agent priorisiert** anhand Inventar, Zugriffsmöglichkeiten, exponierten Services/Produkte die **Schwachstellen** neu und reduziert/erhöht allenfalls den CVSS Score
- **Schnellere** Massnahmen



SPIE’s AI-Vulnerability-Agent in Action!



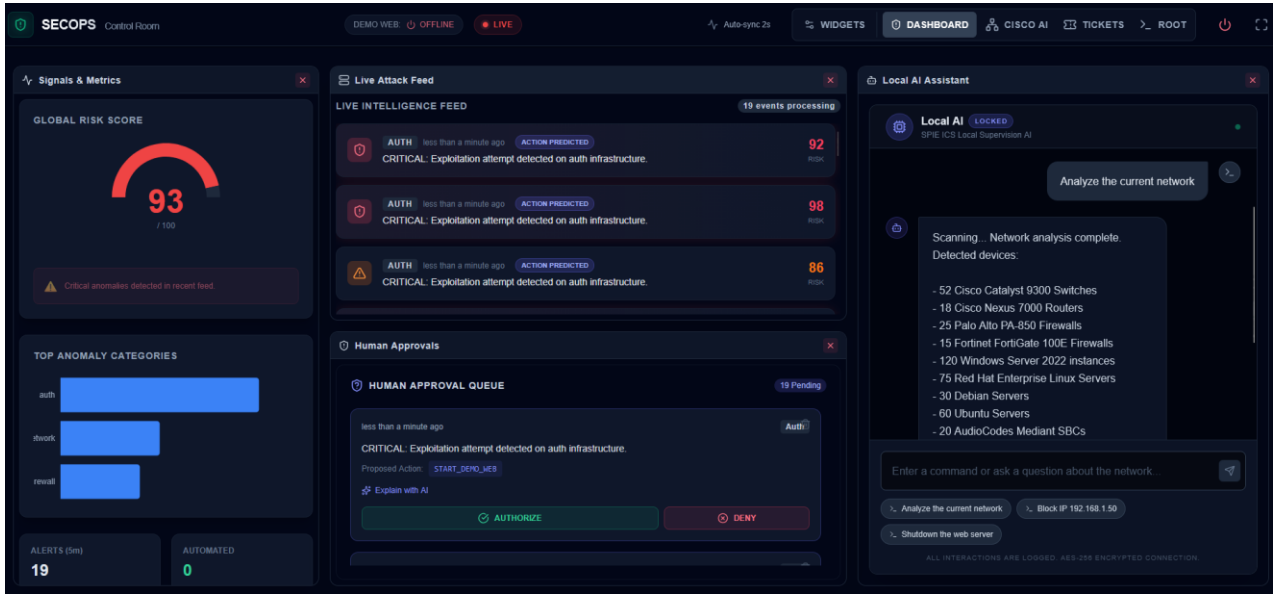
CVEs

Search CVE id or descriptic | Any status | Cisco Identity Services Engine Software | Filter

Product	CVE(s)	CVSS	SIR	Title	AI	Status	Action
Cisco Identity Services Engine Software	CVE-2025-20281 CVE-2025-20282 CVE-2025-20337	10.0	Critical	Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerabilities	Critical (9.5)	High	
Cisco Identity Services Engine Software	CVE-2025-20286	9.9	Critical	Cisco Identity Services Engine on Cloud Platforms Static Credential Vulnerability	High (8.0)	Not impacted	
Cisco Identity Services Engine Software	CVE-2025-20124 CVE-2025-20125	9.9	Critical	Cisco Identity Services Engine Insecure Java Deserialization and Authorization Bypass Vulnerabilities	High (8.0)	Critical	
Cisco Identity Services Engine Software	CVE-2023-50164	9.8	Critical	Apache Struts Vulnerability Affecting Cisco Products: December 2023	Medium (5.0)	High	
Cisco Identity Services Engine Software	CVE-2023-20170 CVE-2023-20175	8.8	High	Cisco Identity Services Engine Command Injection Vulnerabilities	High (8.0)	Not impacted	
Cisco Identity Services Engine Software	CVE-2022-20961	8.8	High	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability	High (8.0)	Not impacted	
Cisco Identity Services Engine Software	CVE-2025-20152	8.6	High	Cisco Identity Services Engine RADIUS Denial of Service Vulnerability	High (8.0)	Not impacted	
Cisco Identity	CVE-2023-20243	8.6	High	Cisco Identity Services Engine RADIUS Denial of	High	Not impacted	

SPIE’s AI-Enhanced-SecOps

- **Interaktive Chatbots** für **SecOps**-Tätigkeiten und Unterstützung
  - Analyse der Incidents
  - Analyse vom Netzwerk
  - Vorschläge zur Behebung durch KI
  - Visibilität
- Chat mit dem lokalen Security LLM
- Schnellstmögliche Behebung der Schwachstellen



SPIE’s AI-Enhanced-SecOps in Action!

Auf dem Weg zu souveräner und operativer KI

Die Souveränität von KI ist ein strategisches Thema, um unsere Daten zu schützen und unsere Nutzung zu kontrollieren

KI-Risiken erfordern Governance, Transparenz und kontrollierte Infrastruktur

Konkrete Lösungen existieren: Edge, AI-Pods, Automatisierung, erweiterte SecOps

SPIE ICS unterstützt die Umsetzung vom Pilotprojekt, über die Einführung und den Betrieb

Nächster Schritt: Gemeinsam die ersten souveränen Anwendungsfälle identifizieren

Ihr Ansprechpartner bei SPIE ICS

Lasst uns gemeinsam die ersten Anwendungsfälle identifizieren!

spie.ch/ai

Marco Gauch

Network Consultant

Tel. +41 58 301 18 34

Mail marco.gauch@spie.com