X-SPIErience Day 2020

SOUVERAINETÉ NUMÉRIQUE

SPIE

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
SOUVERAINETÉ NUMÉRIQUE

SPIE

Gestion efficace des vulnérabilités grâce à une infrastructure d'IA suisse

NICOLAS GOBET

Consultant Microsoft
SPIE ICS

CISCO Partner

L'IA : une menace... mais aussi un levier majeur pour les SecOps

Cyberattaques 2.0

- Industrialisation des attaques
- Frameworks publics pour automatiser des tests d’intrusion
- Deepfake, voice cloning… (confiance fragilisée)
- Efficacité des attaques

Le défi opérationnel

- **Explosion du volume de vulnérabilités**
- Surcharge d'alertes
- Outils cloisonnés et manque de visibilité
- Pénurie de personnels qualifiés
- Automatisation complexe
- Réponses rapides aux incidents

La cybersécurité augmentée par l'IA repose sur une architecture souveraine.

Maîtrise des données & des modèles

Gouvernance, sécurité et opérationnel

- Qui décide, qui contrôle les flux et accès, qui fixe les règles
- Protéger les informations, éviter leur fuite
- Garder la maitrise, comprendre et expliquer les actions de l'IA

Edge & proximité

Rapprocher l'IA des données grâce à l'Edge

- Réduire l'exposition, la latence et la dépendance aux plateformes centrales.

Cisco UCS Edge

Architectures hybrides

Aller au-delà du cloud standard

- Tous les cas d'usage IA critiques ne peuvent pas reposer sur le cloud public.

Gouvernance durable

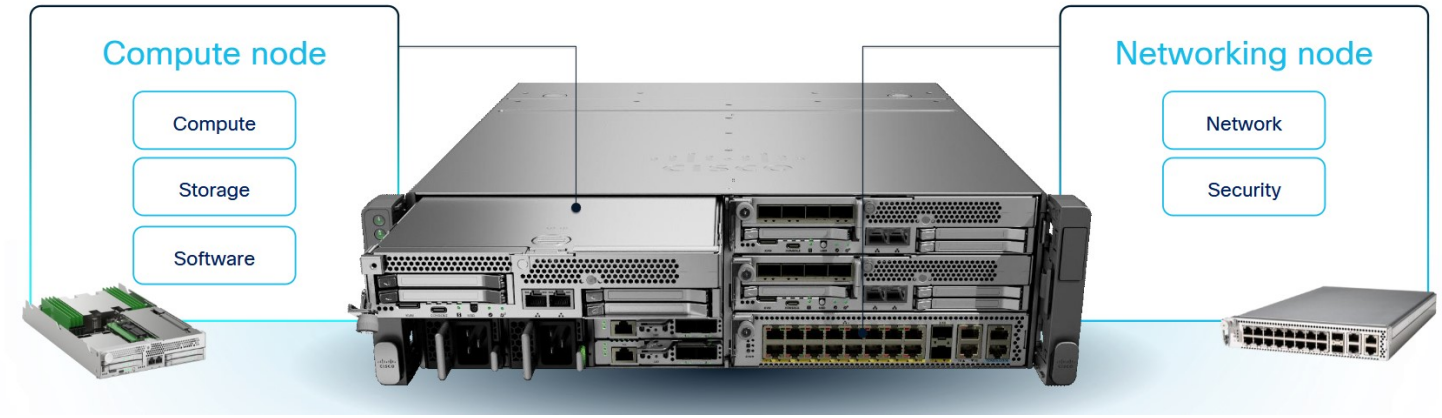
Assurer gouvernance IA, sécurité et exploitation dans la durée

- Une IA qui avance au rythme des équipes sécurité
- **SPIE ICS** maîtrise toute la chaîne de valeur de l'IA souveraine : stratégie, technologie et l'opérationnel.

Comment Cisco nous accompagne?

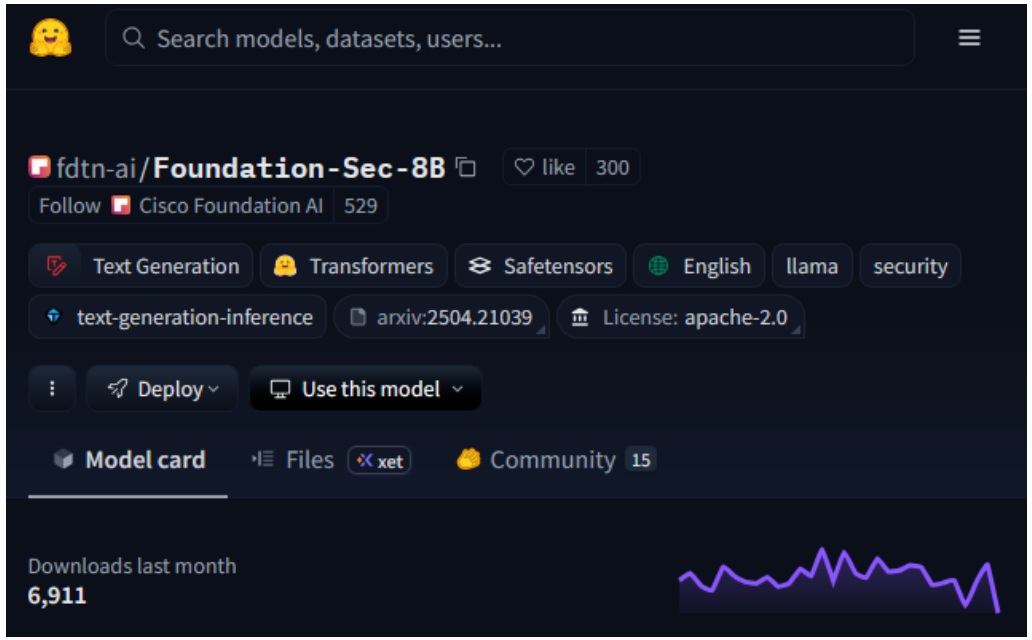
Hardware - Cisco Unified Edge

- Réseau, sécurité et puissance **GPU** intégrés dans une seule plateforme
- Orchestration centralisée
- Calcul au plus près des données (Edge)



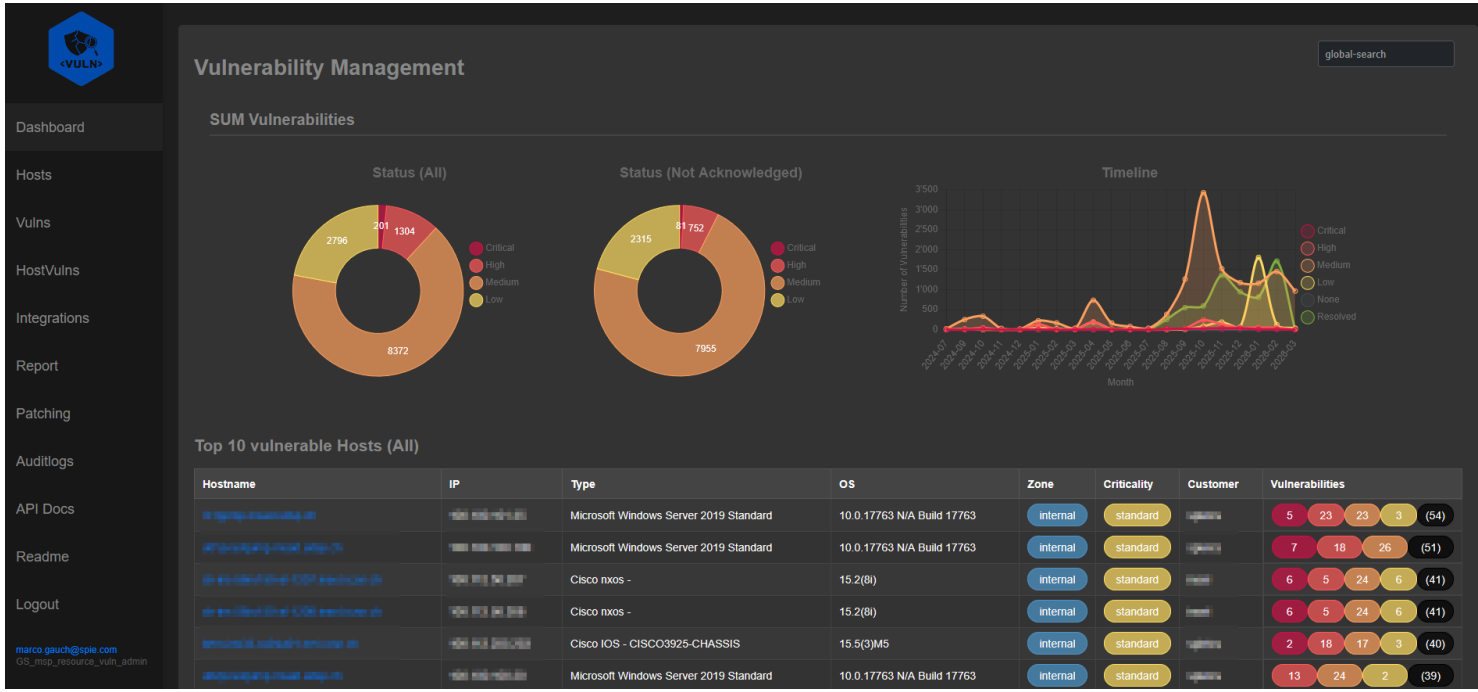
LLM Cisco

Foundation-Sec-8B – LLM de cybersécurité déployable localement, conçu pour aider les organisations à identifier, prioriser et analyser systématiquement les vulnérabilités, tout en préservant la souveraineté des données et la conformité réglementaire.



Détection et priorisation automatisée des vulnérabilités

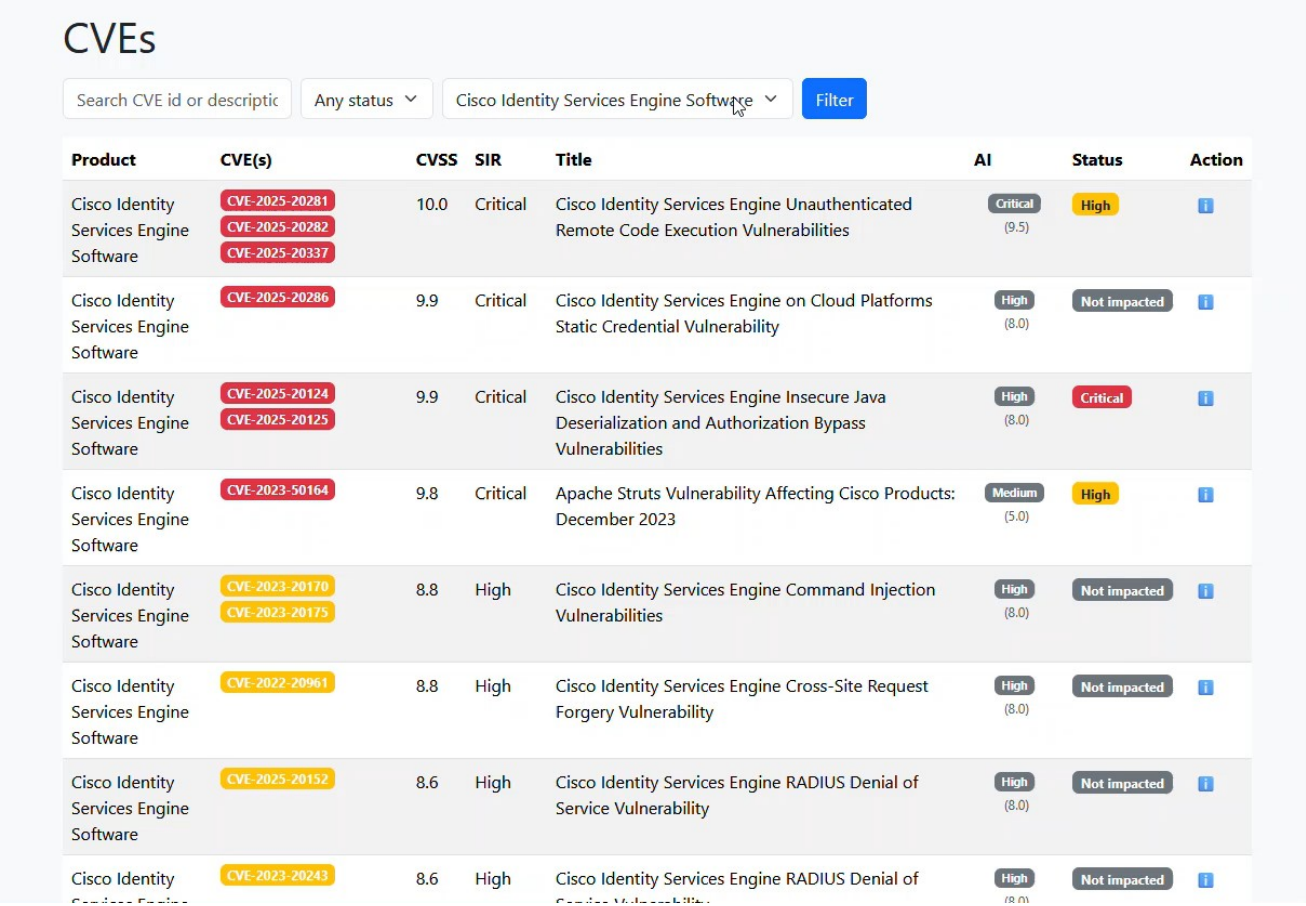
- Identification continue des vulnérabilités.
- Consolidation de différentes sources API Cisco openVuln NIST
- Analyses Nessus



Service de gestion des vulnérabilités

SPIE’s AI-Vulnerability-Agent in Action!

- LLM Foundation-Sec-8B exécuté localement
- Détection et priorisation continue des vulnérabilités
- L'IA **contextualise** la CVE dans l’infrastructure cible afin de **recalculer** sa criticité, **expliquer** l’impact réel de la vulnérabilité et **proposer** un plan de remédiation priorisé.
- Accélération des actions de remédiation



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	

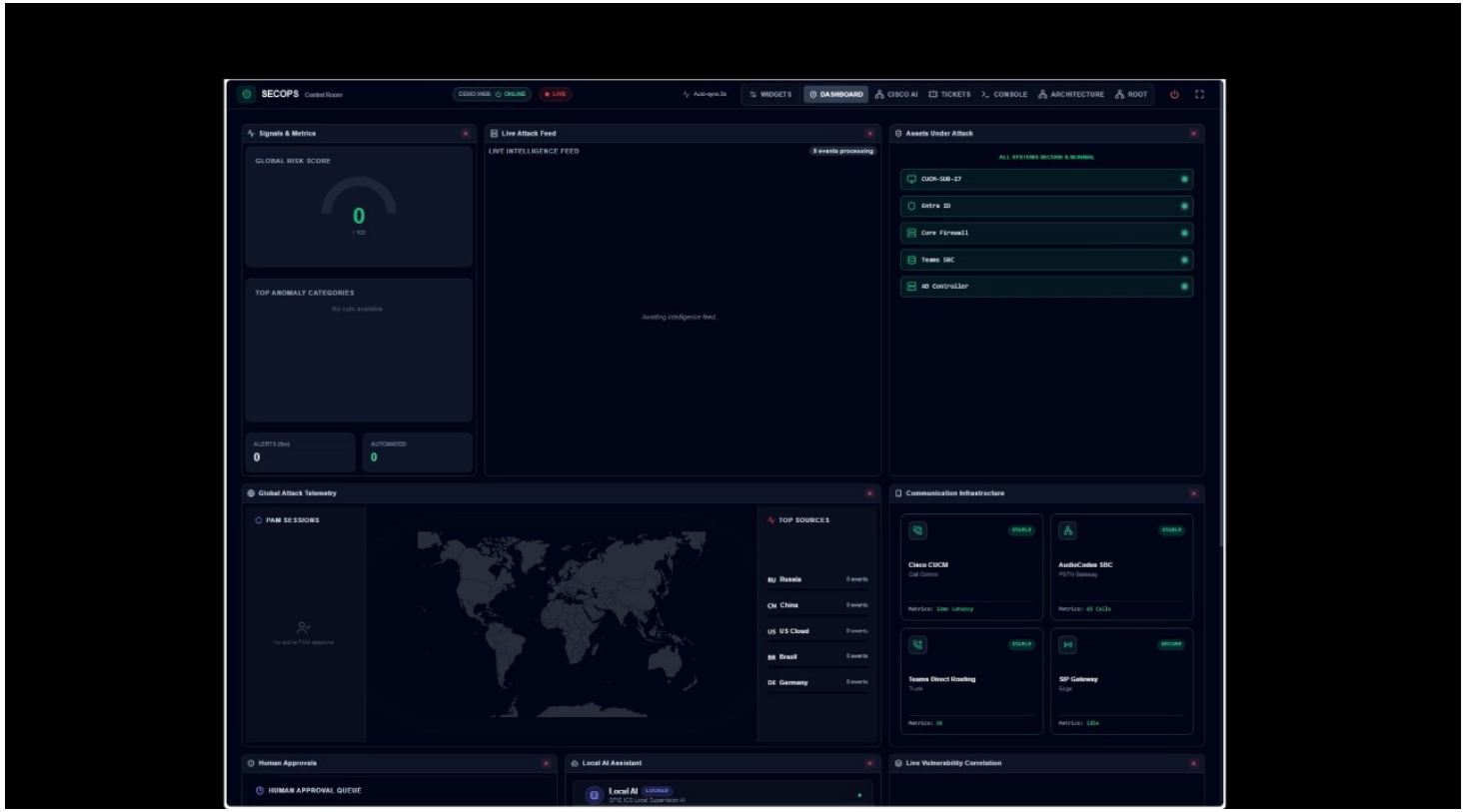
IA au service des opérations de sécurité

Cas d’usage 2

- Chatbots interactifs pour l’investigation et l’assistance SecOps
- IA de maintenance pour garder les modèles performants
- Réduction du bruit, amélioration du MTTR et de la visibilité

Plan d’adoption :

- ➢ Pilotes Edge
- ➢ Déploiement AI Pod
- ➢ Industrialisation sécurisée et souveraine



En route vers une IA souveraine et opérationnelle

La souveraineté de l'IA est un enjeu stratégique pour protéger nos données et maîtriser nos usages

Les risques liés à l'IA exigent gouvernance, transparence et infrastructures contrôlées

Des solutions concrètes existent : Edge, AI Pods, automatisation, SecOps augmentées

SPIE ICS accompagne la mise en œuvre, du pilote à l'industrialisation

Prochaine étape : identifier ensemble vos premiers cas d'usage souverains

Votre interlocuteur chez SPIE ICS

« La souveraineté numérique n'est pas un concept : c'est un avantage opérationnel. »

spie.ch/ia

Nicolas Gobet

Lead Data IA Practice

Tél. +41 58 301 10 62

Mail nicolas.gobet@spie.com