AYI NEDJIMI Consultants

Splunk : Plateforme SIEM Observability (Cisco)

10 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3621 mots •

Splunk est la plateforme commerciale de reference pour la collecte et l'ana
donnees machine, leader Gartner SIEM depuis 2013 et rachete par Cisco e
2024 pour 28 Md$. Tour d'horizon de l'architecture (Indexers, Search Hea
Forwarders), du langage SPL, des modules Enterprise Security, SOAR, Mis
Control, Observability Cloud et MLTK, du pricing workload et du comparati
Sentinel, Wazuh, Elastic et QRadar.

Splunk est la plateforme commerciale de référence pour la collecte, l'indexation et
de données machine massives, positionnée comme leader incontesté du Magic Q
Gartner SIEM depuis plus d'une décennie. Fondée en 2003 et acquise par Cisco e
2024 pour 28 milliards de dollars — la plus importante opération de l'histoire de C
solution combine désormais un SIEM premium (Splunk Enterprise Security), une p
d'orchestration et d'automation (Splunk SOAR, ex-Phantom), un module Mission C
unifiant SIEM/SOAR/UEBA, et une suite Observability
Real User Monitoring et logs. Son langage de requêt

Language), associé au Common Information Model et à plus de 2 400 applications disponibles sur Splunk Base, en fait l'outil privilégié des SOC de grandes entrepris banques, agences gouvernementales et opérateurs d'importance vitale. Splunk es FedRAMP High, FIPS 140-2 et ISO 27001, ce qui justifie son adoption massive dan environnements régulés malgré un coût élevé qui en limite l'usage aux organisatio disposant d'un budget cybersécurité conséquent.

À RETENIR

L'essentiel à retenir

Leader Gartner SIEM depuis 11 années consécutives, racheté par Cisco en 2024 pour 28 Md$.

SPL (Search Processing Language) : langage propriétaire de pipelines de recherche, puissant mais à courbe d'apprentissage marquée.

Trois éditions : Splunk Enterprise (on-prem), Splunk Cloud Platform (SaaS) Splunk Edge Hub (IoT/OT).

Modules clefs : Enterprise Security (SIEM), SOAR (SOAR/Phantom), MLTK Observability Cloud (APM/RUM/logs).

Pricing workload-based depuis 2023, avec dimensions Ingest, Edge, Stora Activity.

Conformité : FedRAMP High, FIPS 140-2, ISO 27001, SOC 2 Type II — adop DoD, NSA, GCHQ, banques tier 1.

Coût élevé : entre 150 000 et 800 000 € annuels pour 1 To/jour selon éditio modules.

Réponse sous 24h

Devis gratuit →