

CONCEPTEUR,
INTÉGRATEUR,
OPÉRATEUR
DE SYSTÈMES
CRITIQUES



Prelude SIEM

Prelude SIEM

Supervision de la sécurité

Seul SIEM (Security Information & Event Management) Français et Européen, **Prelude SIEM** vous offre une vision unifiée de la sécurité de votre système d'information. Il vous protège et vous alerte en temps réel des risques et menaces. Il stocke et archive toutes les traces pour l'analyse, l'enquête et la preuve en cas de cyberattaques. Ses capacités combinées de Big Data, de Smart Data ainsi que les nombreuses possibilités d'analyse graphique lui permettent de détecter les menaces les plus complexes (APT).



Caractéristiques

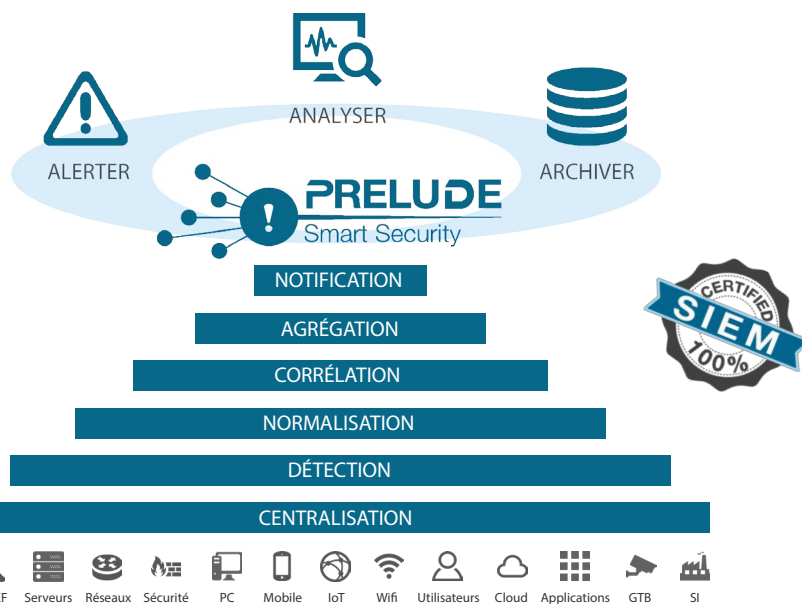
- > Cœur open-source
- > Standards : ISI (ETSI), IDMEF, IODEF (IETF, RGI v2)
- > Client léger Web 2.0
- > Big Data : Log et Netflow
- > Smart Data : corrélation intelligente
- > Rapport et conformité PCI DSS, ISO 27 002 et PDIS
- > Threat intelligence, rejeu, multi-entité, MSSP
- > Log source : Syslog, JSON, CEF, LEEF, etc.
- > Architecture modulaire
- > Confidentialité, anonymisation intégrité, traçabilité



Références

- > Administration, Défense, Finance, Energie, Transport, Santé
- > France et International

www.c-s.fr



ALERTER

Le SmartData au service de l'efficacité en temps réel

Prelude SIEM identifie les comportements suspects, puis les affiche dans une interface qui propose des fonctions avancées de filtrage, de tri, de corrélation et d'agrégation. Un module de gestion de tickets permet d'associer une alerte à un workflow ainsi qu'à une base de connaissances. Ce module s'appuie sur les formats standards IDMEF et IODEF.

ANALYSER

Des interfaces simples pour des analyses complexes

Plusieurs fonctions d'analyse sont disponibles. D'une part l'analyse en temps réel des données pour mesurer le niveau de criticité de la situation, d'autre part l'analyse en temps différé des informations à la recherche d'informations «cachées» dans la masse de données, enfin un module unique permet le forensic visuel à partir de graphiques originaux.

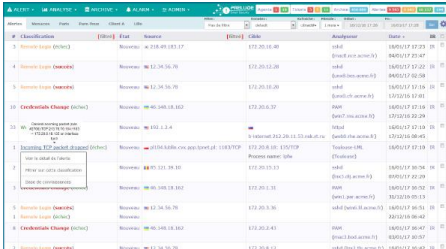
ARCHIVER

Le BigData pour le stockage à long terme

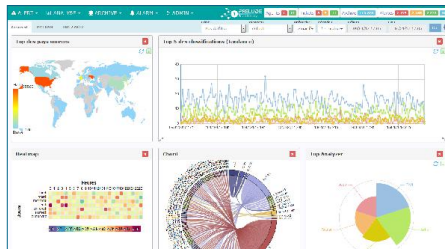
Ce module archive la totalité des traces dans une base de données NoSQL. Une interface avancée permet ensuite de naviguer dans ces données pour mener des analyses post-mortem ou investiguer sur une alerte en cours grâce à des filtres standards ainsi qu'un langage de requêtes avancées «Google-Like».

Des interfaces intuitives et ergonomiques

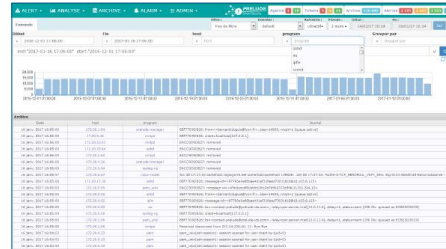
Un travail important a été effectué sur les interfaces Prelude SIEM pour faciliter la tâche des exploitants au quotidien. Les puissants moteurs de corrélation assistent l'exploitant dans l'identification des menaces au sein des volumes importants de données. L'analyse, le forensic et la recherche d'APT (Advanced Persistent Threat) sont aujourd'hui à la portée de tous.



ALERTER



ANALYSER



ARCHIVER

Nos services



PLAN

Spécification et conception architecture, planning, ressources.



DEPLOY

Mode assistance ou «clé en main» sur le déploiement.



RUN

Externalisé ou à distance. Suivi des alertes. Reporting.



TRAINING

Formation, configuration et exploitation. Transfert de compétences



SERENITY

Assistance à la prise en main et à la configuration. Points périodiques.



EMERGENCY

Assistance en cas d'incidents. Escalade.

www.prelude-siem.com
contact.prelude@c-s.fr

À PROPOS DE CS

Concepteur et intégrateur de systèmes clés en main performants et innovants, CS intervient sur l'ensemble de la chaîne de valeur de ses clients. Avec 170 M€ de chiffre d'affaires et 2000 collaborateurs, CS s'impose aujourd'hui comme un fournisseur de confiance, reconnu par ses grands clients en raison de l'expertise, de l'engagement et du sens du service de ses collaborateurs.



CS Communication & Systèmes
 22, avenue Galilée - 92350 Le Plessis Robinson
 tél : +33 (0)1 41 28 40 00 - fax +33 (0)1 41 28 40 40