DESIGNER,
INTEGRATOR,
OPERATOR OF
MISSION-CRITICAL
SYSTEMS

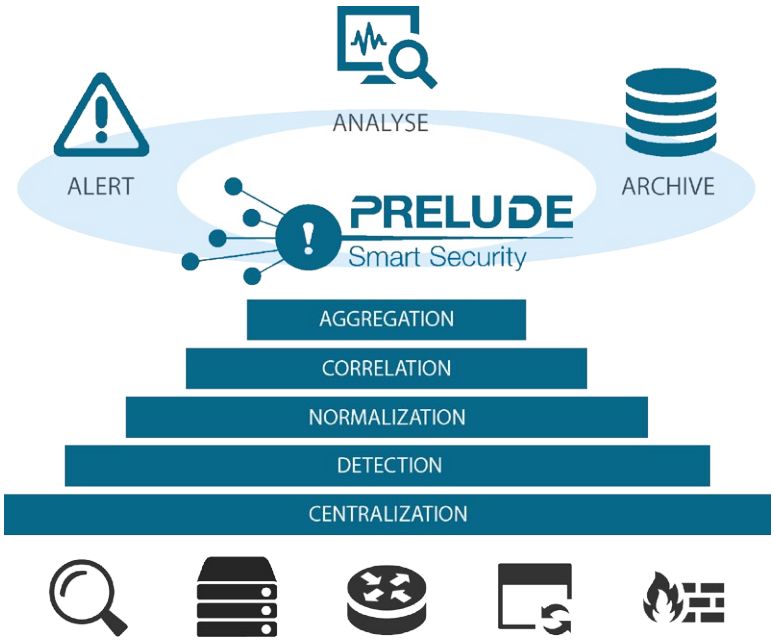
The power of innovation

PRELUDE

PRELUDE SIEM

Security Monitoring

Sole French and European SIEM, PRELUDE offers a unified view of your information system security. It protects and alerts you in real time about the risks and threats. It stores and archives all the traces for analysis, investigation and evidence. Finally, it provides many possibilities for graphical and mathematical analysis to search for complex advanced persistent threats (APT).



Features

> Based on Open Source Software

> IDMEF, IODEF standards

> Lightweight web client 2.0

> Big Data: Log and Netflow

> Smart Data: intelligent correlation

> Reporting and compliance PCI DSS, ISO 27 002 and PDIS

> Threat intelligence: replaying and multi-tenancy

> Modular architecture

> Confidentiality, anonymization, integrity and traceability

References

> Administration, Defense, Finance, Energy, Transportation

> France, Europe, Canada, USA, South America, Africa, Asia, Russia

ALERT

The SmartData service efficiency

PRELUDE identifies suspicious behaviors then displays them in an interface with advanced sorting and aggregation filter functions. A ticket management module allows association of an alert with a workflow and a knowledge base. This module uses the IDMEF and IODEF standard formats.

ANALYSE

Simple interfaces for complex analysis

Several analysis functions are available. On the one hand, real-time data analysis to measure the level of criticality of the situation. On the other hand, the deferred time analysis of information to search for hidden information in the data mass. Finally, a single module enables the visual forensic based on original graphics.

ARCHIVE

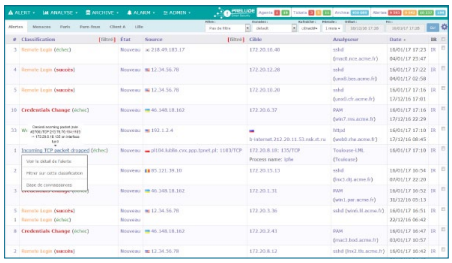
Long-term storage of all your logs

This module archives all logs in a NoSQL database. Thanks to the advanced interface, you can browse those data to conduct postmortem analysis or investigate on a current alert with standard filters and «Google-Like» advanced query language.

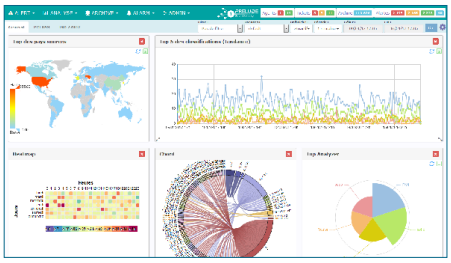
www.c-s.fr

Intuitive and ergonomic interfaces

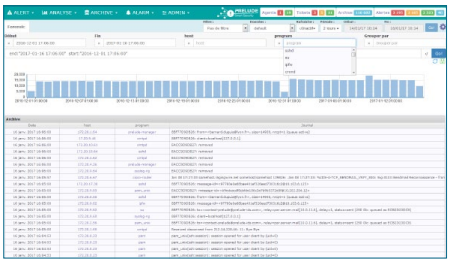
Significant work has been done on PRELUDE's interfaces to facilitate the operators daily work. The powerful correlation engines help the operators to identify threats in hudge volumes of datas. Analysis, forensic and research of APT (Advanced PersistantThreat) are now intuitive and fast.



ALERT



ANALYSE



ARCHIVE

Services

PLAN	DEPLOY	APPS
Assistance in the specification and design phase of your deployment: architecture, planning, resources, timing.	In assistance form or «turnkey» mode, we support you during the deployment phase of your SIEM.	Customization or development of specific business functions for your own needs.

TRAINING	SERENITY	EMERGENCY
Training for the configuration and operation of PRELUDE, scenario-based sessions for operators. Awareness sessions for your employees.	Personalized support for the handling of your SIEM followed periodic meeting points to assist you in the tool's sharp tuning.	Our team of experts assists you in case of incident or intrusion to recover your activity as soon as possible.

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

ABOUT CS

CS's expertise in mission critical applications and systems makes it the best partner in sectors with strong growth potential, such as defense, space and security, aeronautics, energy and transportation. With € 162 million in revenues and 1.730 employees worldwide, CS is an established provider, acknowledged by major customers for its expertise and commitment of service to customers.

The power of innovation

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