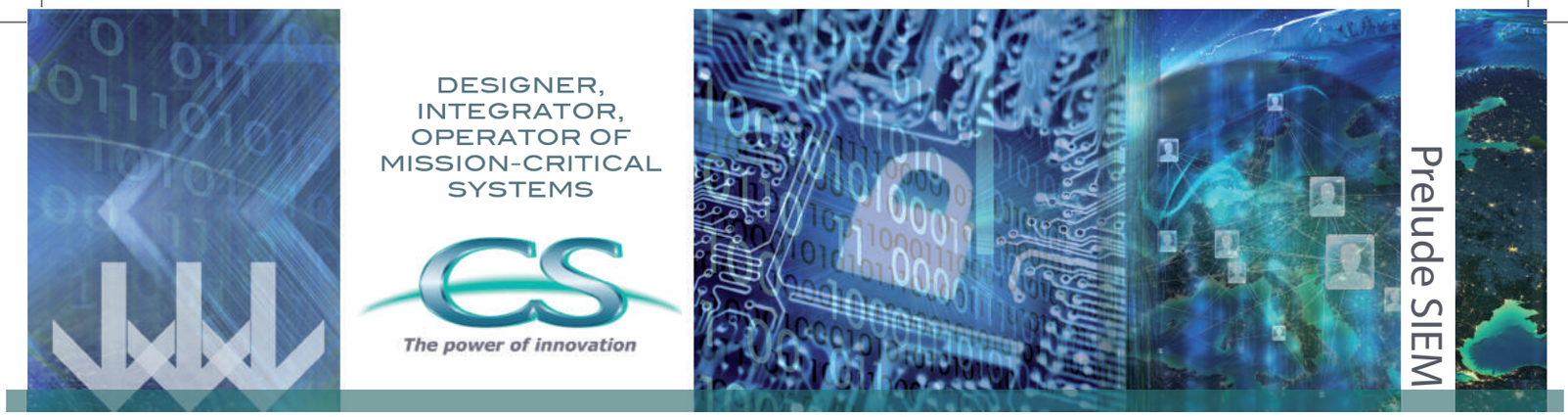
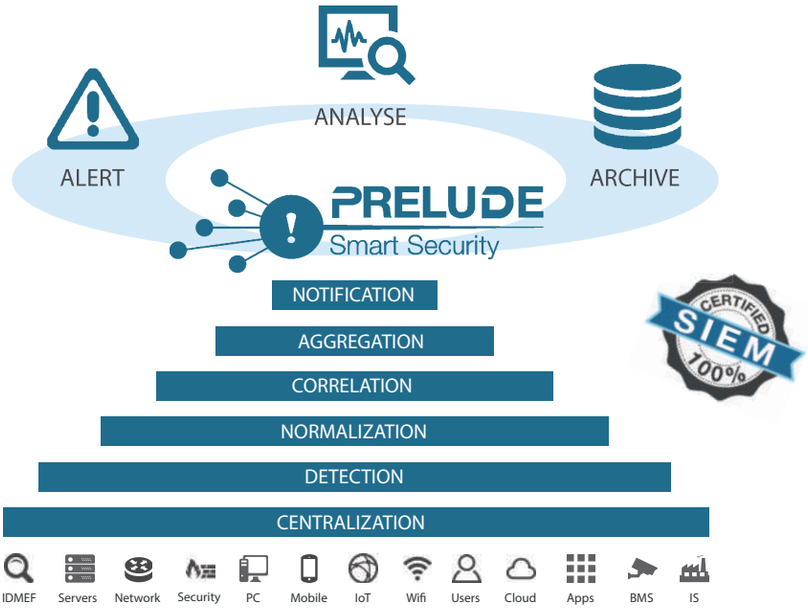


Prelude SIEM SIEM

Security Monitoring

Sole French and European SIEM, PRELUDE SIEM 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, MSSP

> Log source : Syslog, JSON, CEF, LEEF, etc.

> Modular architecture

> Confidentiality, anonymization, integrity and traceability

References

> Administration, Defense, Finance, Energy, Transportation, Healthcare

> France and International

ALERT

The SmartData service efficiency

Prelude SIEM 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

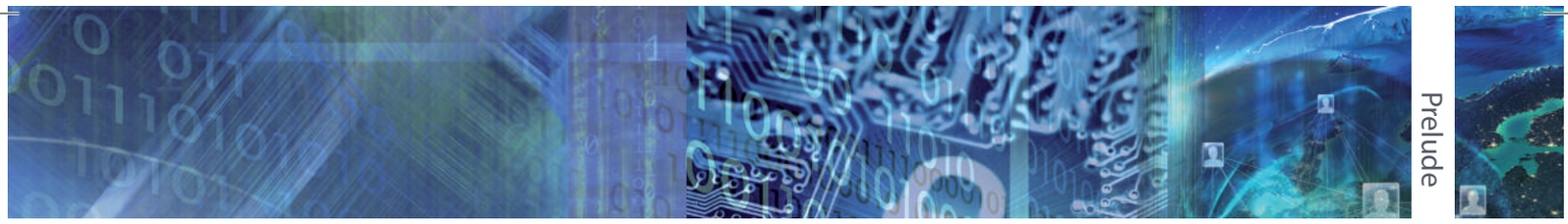
Several analysis functions are available. On the one hand, real-time data analysis to measure the level of criticality of the situation. On the other hand, the deferred time analysis of information to search for hidden information in the data mass. Finally, a single module enables the visual forensic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

ARCHIVE

Long-term storage of all your logs

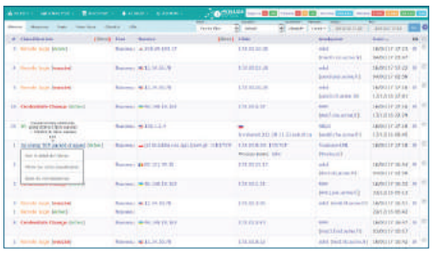
This module archives all logs in a NoSQL database. Thanks to the advanced interface, you can browse those data to conduct postmortem analysis or investigate on a current alert with standard filters and «Google-Like» advanced query language.

www.c-s.fr

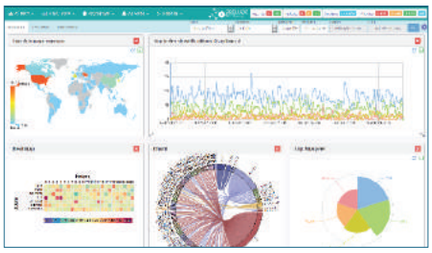


Intuitive and ergonomic interfaces

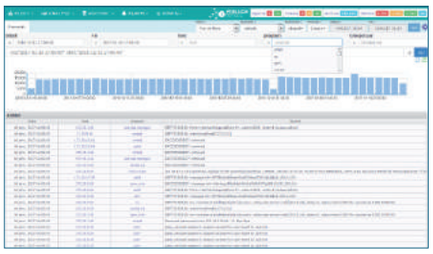
Significant work has been done on Prelude SIEM's interfaces to facilitate the operators daily work. The powerful correlation engines help the operators to identify threats in hudge volumes of datas. Analysis, forensic and research of APT (Advanced PersistantThreat) are now intuitive and fast.



ALERT



ANALYSE



ARCHIVE

Services

PLAN

Architecture specification and conception, planning, resources

DEPLOY

Assistance mode or «turnkey» on the deployment

RUN

Outsourced or remotely.
Alert tracking.

Reporting

TRAINING

Configuration and operation training.

Transfer of skills.

SERENITY

Assistance with handling and configuration

Periodic review

EMERGENCY

Assistance in case of incidents.

Escalation

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

ABOUT CS

As prime contractor in the design, integration and operation of mission-critical systems, CS is present all long the value chain for its customers. With a turnover of €170M and 2000 employees, CS is an established supplier acknoledged by its major customers thanks to the expertise & commitment of its staff.

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