la force de l'innovation

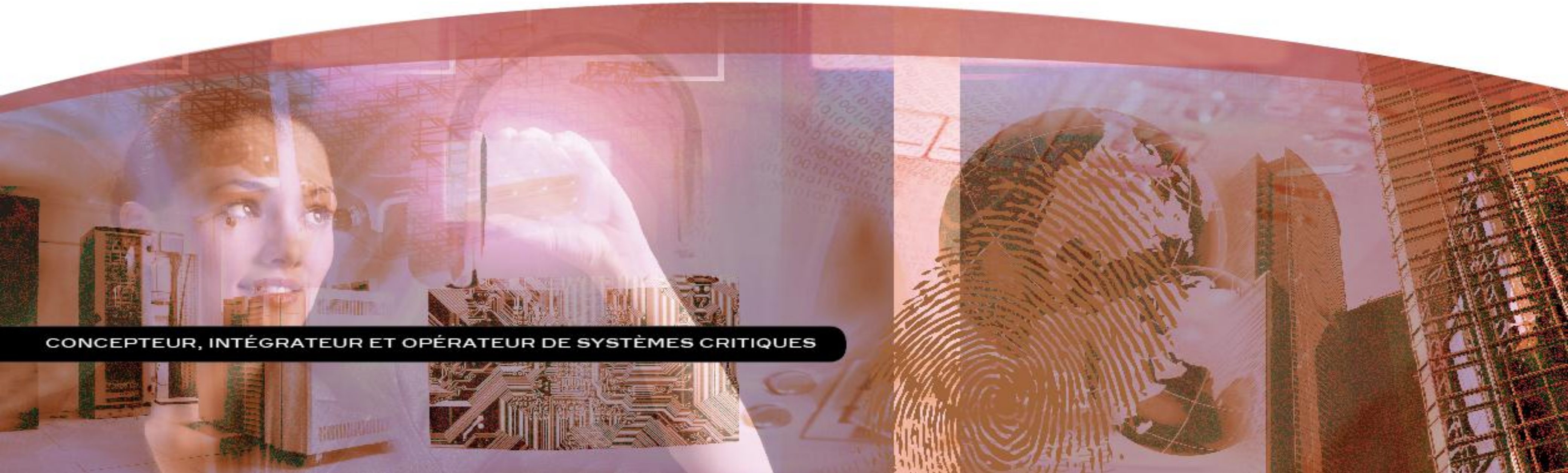
CS - Communication & Systèmes
R2GS – ETSI ISG ISI

14 May 2014

Towards European sovereign SOCs and SIEM

la force de l'innovation

- **Presentation of CS – Communication & Systèmes**
- The European and German Cybersecurity environment
- CS Security Business
- Offers: SOCs, SIEM, Industrial Control Systems (ICS) Security
- Some customer references



CONCEPTEUR, INTÉGRATEUR ET OPÉRATEUR DE SYSTÈMES CRITIQUES

CS Profile

Positioning

Designer, Integrator and Operator of Critical Systems

Our Motto

The Power of Innovation

Double competencies:
Clients' businesses & Technical IS

⬇

At the heart of the operational IS of our Clients

Excellent coverage of the value chain from Advisory services to System Operation

Innovating Products that contribute to our technology brand image + differentiating value

A combination of **Expertise and Teams** that are recognized for their talent

CS, designer, integrator & operator of mission critical systems

CS
la force de l'innovation

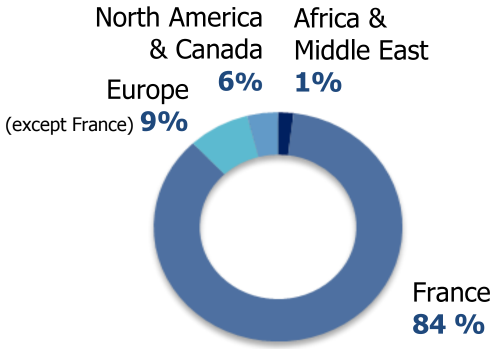
- → Prime contractor for turnkey systems, featuring innovation and performance
- → Active across the entire value chain: Consulting, Design, Build, Run
- → Culture of expertise & innovation

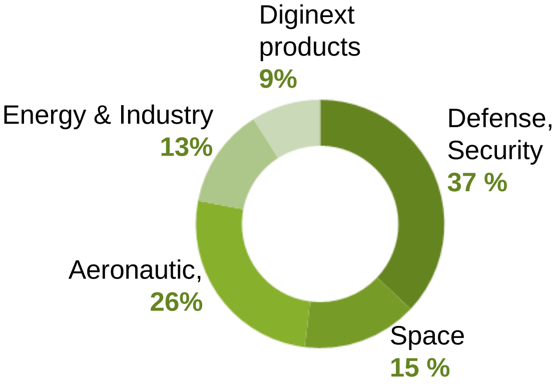
170 M
in revenues

1700
employees worldwide

1480
employees in France

220
employees abroad





Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

esa

EUMETSAT

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR
ET DE L'AMENAGEMENT DU TERRITOIRE

dgac
DSNA

TOTAL

france telecom

DCNS

EADS

THALES

SAFRAN

cea

EDF

IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE

Pratt & Whitney
A United Technologies Company

Fields of activities

DEFENSE & SECURITY

- Operations command information systems
- Command & control center
- Communication systems
- Support & logistics information system
- Armed forces training
- Area surveillance & intervention managment
- Information and communication systems safety & security
- › Authentification services
- › Cyberdefense

SPACE

- Space Software Systems & Services
- › Ground control & Simulation
- › Flight operation & planning
- Big Data Intelligence
- › Data processing, fusion & dissemination
- › Georeferenced services

AERONAUTICS

- Embedded systems
- Technical information systems
- › Enterprise content managment
- › Product lifecycle management
- Digital design

ENERGY

- Simulation & HPC
- Industrial information systems & nuclear
- Nuclear safety

Transverse Skills center

Secured Infrastructures

Image processing Geographical IS

PLM / ECM Real Time Software

High Performance Computing

DIGINEXT PRODUCTS

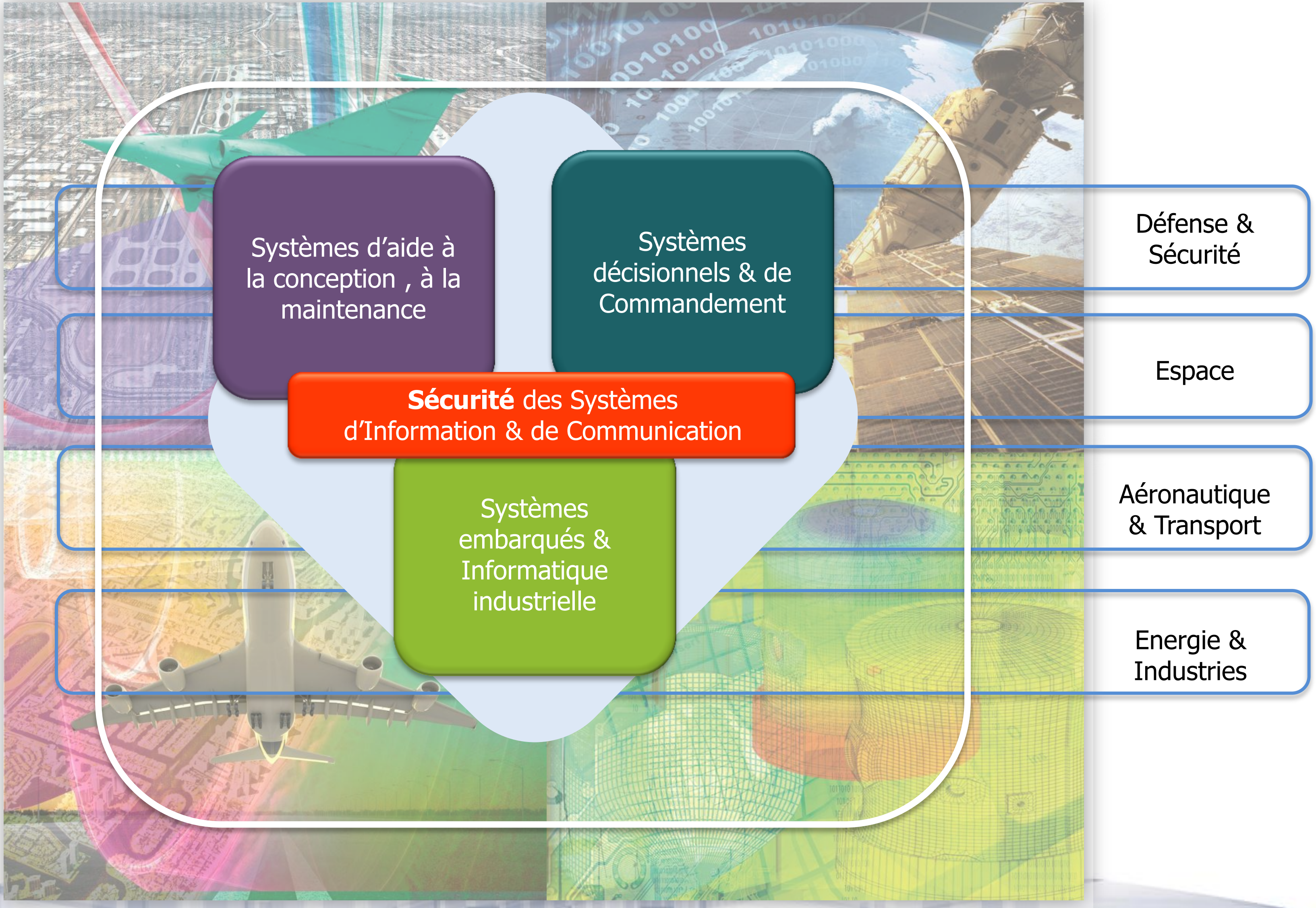
A CS group subsidiary, Diginext ensures product industrialization and marketing in the fields of :

- Tactical data links (TACTX, STARLINX, SOLSTICE)
- Simulation and vitual reality systems (Inscape, Vertigo, VirtualGeo, Indigo, VisualSim, CS Wave)
- Navigation, geolocalization and detection systems (MILGPS, LORANC, STRADIVARIUS…)
- Information systems for public transportation (MOBILITX…)

Transverse Skills center

Virtual reality / 3D

CS Profile
Domaines d'interventions



Systèmes d'aide à la conception , à la maintenance

Systèmes décisionnels & de Commandement

Sécurité des Systèmes d'Information & de Communication

Systèmes embarqués & Informatique industrielle

Défense & Sécurité

Espace

Aéronautique & Transport

Energie & Industries

Innovation & Expertise

la force de l'innovation

DEFENSE | **SECURITY** | **SPACE** | **AERONAUTICS** | **ENERGY** | **DIGINEXT PRODUCTS**

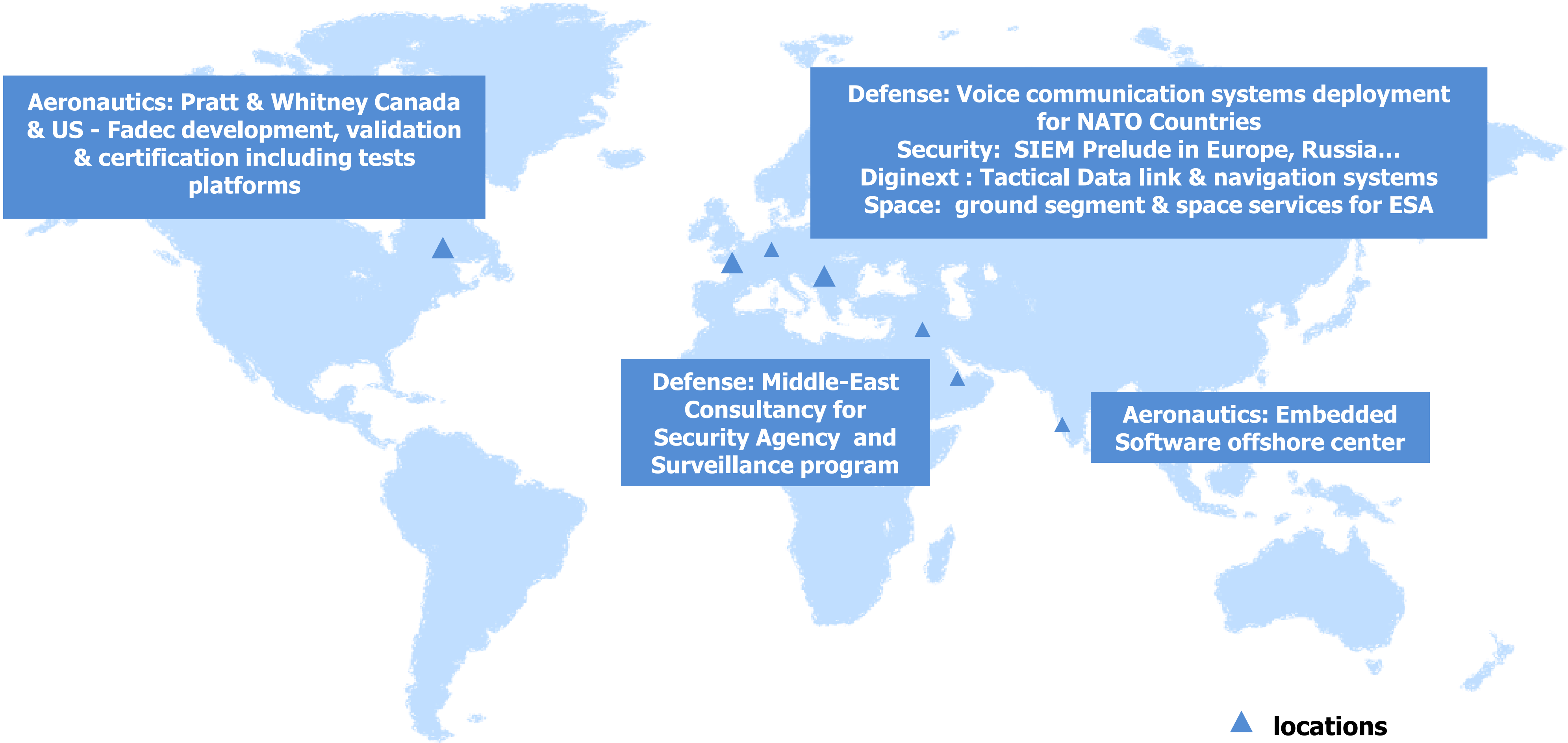
- Active participation to competitiveness clusters
  - System@tic; Minalogic; Aerospace Valley; Cancer research, Biotechnology and healthcare; Sea, Security, Safety and Sustainable Development; Secured Electronic Transactions
- Experts with state-of-the-art technology competencies: 220 technological & business oriented specialists federated in the company's experts network
  - Information systems network security, modeling & simulation, embedded systems, intelligence, open source software, software and systems engineering
- R&D: 9% of revenues
- Innovative components and products range
  - Command centers, tactical data links, communication and information systems security, electronic warfare, test & training, navigation systems, flight dynamics

CENTERS OF EXPERTISE

CS in brief

Global footprint

la force de l'innovation



Aeronautics: Pratt & Whitney Canada & US - Fadec development, validation & certification including tests platforms

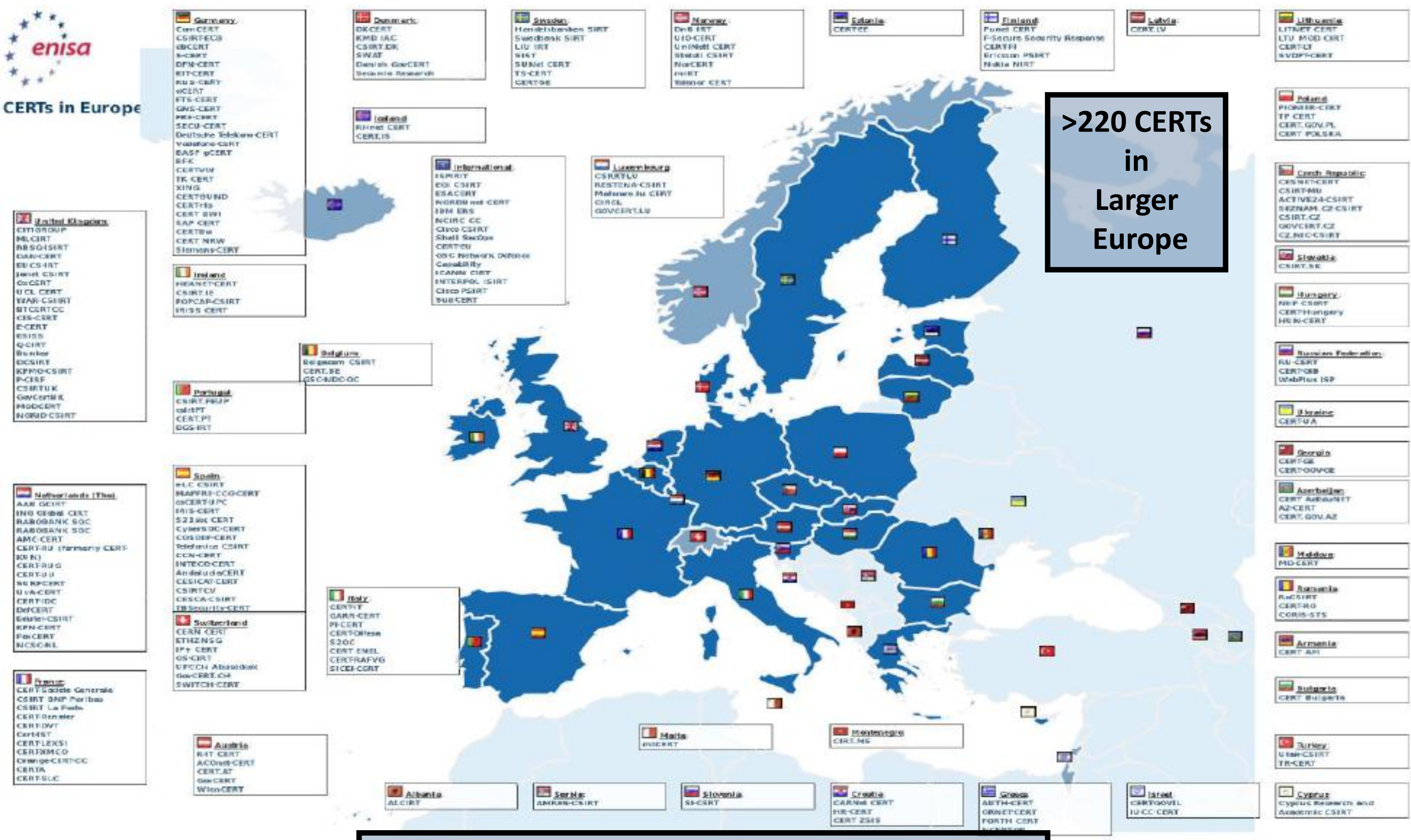
Defense: Voice communication systems deployment for NATO Countries
Security: SIEM Prelude in Europe, Russia…
Diginext : Tactical Data link & navigation systems
Space: ground segment & space services for ESA

Defense: Middle-East Consultancy for Security Agency and Surveillance program

Aeronautics: Embedded Software offshore center

▲ **locations**

- Presentation of CS – Communication & Systèmes
- **The European and German Cybersecurity environment**
- CS Security Business
- Offers: SOCs, SIEM, Industrial Control Systems (ICS) Security
- Some customer references



>220 CERTs in Larger Europe

CERT = Computer Emergency Response Team

Ranking of main countries in cyber-readiness (McAfee 2013)

1	**********	Finland, Israël, Sweden
2	*********	Denmark, Estonia, France, Germany, Netherlands, Spain, UK, USA
3	********	Australia, Austria, Canada, Japan
4	*******	China, Italy, Poland, Russia
5	******	Brazil, India, Romania
6	*****	Mexico

…

Cybersecurity is at the heart of the digital economy and enterprise

➔ Towards a knowledge economy, European plan

- e-Europe 2002, eEurope 2005, then in 2005: Initative i2010, and in 2010 « Strategy for a safer Information Society »
- **Communication 2010-245**: new **Digital Agenda for Europe**, 16 actions, of which : *reinforce digital trust, digital security, , cooperation between CERTS, and creation of the CERT of European Institutions …*
- **NIS Directive** voted in March 2014 and **European Ruling for Protection of Personal Data**, with the introduction of legal responsibility in case of breach, first **European Cousel Meeting** dedicated to Digital in October 2013
- **Horizon 2020 : European investment plan 2014-2020, Cybersecurity is in the stategy**
- **From IT Security to Industial Control Systems security**

➔ The cyberspace and security needs grow exponentially

- Global trafic of the **data centers**: X4 in the next 5 years, and from 2016 onwards: **2/3 in the cloud**
- **Connected objects**, IOE « Internet Of Everything », proliferation of intrusion sources
  - 2012: 7 MM of connected objects, 2015: 50 MM *(source Cisco),* home automation, meters, cars, planes, trains, industrial equipment, infrastructure equipment…, connections «any to any »…
- 07:Estonie, 10: Iran/ Stuxnet, 11: Sony, 13: USA/ NSA…, today, **cyberattacks hit the headlines everyday!**

➔ The cost of cybercrime is on the rise

- 2013: **between 300M$ and 1000MM$,** already higher that drug trafficking
- WEF expects the cost to rise to **3000MM$ in 2020**
- Work will all players of the ecosystem, so that **the cost of cybercrime is curbed, and never outpaces the benefits of the digital economy**

Main European Cybersecurity & Cyberdefense institutions

- **DG CONNECT (ex INFSO)** : Networks, IT, Technologies, Information Society, Media, Internet, digital signature, ENISA….
- **DG JUSTICE:** data protection issues…
- **DH HOME :** homeland security, cybercrime…
- **DG ENTR, Enterprises & Industries**: standardization, innovation in Cyberdefense…
- **DG HR & Security:** create global security policy for the ECommission…
- **DG JRC Joint Research Center**: cybersecurity and cyberdefense programmes..
- **EDPS:** European Data Protection Supervisor
- **ENISA:** dedicated to IS Security, and by extension SCADA and ICS security
- **EUROPOL:** main european force against cybercrime, coordination + operational teams
- **CERT-UE:** created in june 2011, open site on vulnerabilities, coordinates 60 CERTs in Europe
- **IS Security Audit Teams**
- **PCRD and Horizon2020:** mid term collaborative research programmes

European Strategy: Network & Information Security (NIS) directive – March 2014

➔ EU's vision of cyber-security with 5 priorities

- Achieving **cyber resilience,** resist, restart fast in case of problem
- Drastically **reduce cybercrime**
- Develop **cyber defence policy and capabilities** related to the Common Security and Defence Policy (CSDP)
- Develop the **industrial and technological resources** for cyber-security
- Establish a **coherent international cyberspace policy for the European Union** and promote core EU values

➔ 3 new requirements for the EU countries and the Operators of Critical Infrastructures (vital interest)

- Member States must **adopt a NIS strategy and designate a national NIS competent authority** with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents
- Creating a cooperation mechanism among Member States and the Commission to **share early warnings on risks and incidents** through a secure infrastructure, cooperate and organise regular peer reviews;
- Operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services and public administrations must adopt **risk management practices and report major security incidents on their core services.**

German Cybersecurity Strategy (feb. 2011)

1. Protection of critical information infrastructures

The protection of critical information infrastructures is the main priority of cyber security. They are a central component of nearly all critical infrastructures and become increasingly important.
The public and the private sector must create an enhanced strategic and organizational basis for closer coordination based on intensified information sharing.
To this end, cooperation established by the CIP implementation plan is systematically extended, and legal commitments to enhance the binding nature of the CIP implementation plan are examined.
With the participation of the National Cyber Security Council (cf. objective 5), the integration of additional sectors is examined and the introduction of new relevant technologies is considered to a greater extent.
Whether and where protective measures have to be made mandatory and whether and where additional powers are required in case of specific threats have to be clarified, too.
Furthermore we will examine the necessity of harmonizing rules to maintain critical infrastructures during IT crises.

German Cybersecurity Strategy (feb. 2011)

2. Secure IT systems in Germany

Infrastructure protection requires more security with regard to IT systems used by citizens and small and medium-sized businesses.
Users need appropriate and consistent information on risks related to the use of IT systems and on security measures they can take to use cyberspace in a secure manner.
We will organize joint initiatives with groups from society to pool information and advice consistently.

Furthermore we will examine whether providers may have to assume greater responsibility and make sure that a basic collection of appropriate security products and services are made available to users by providers.
We want to provide specific incentives and funds for basic security functions certified by the state (e.g. electronic proof of identity or De-mail) to be used by the vast majority of citizens.
To support small and medium-sized businesses in the secure use of IT systems, the Federal Ministry of Economics and Technology has set up a task force on “IT security in industry” with the participation of industry.

German Cybersecurity Strategy (feb. 2011)

3. Strengthening IT security in the public administration

The public administration will further enhance the protection of its IT systems. State authorities have to serve as role models for data security.
We will create **a common, uniform and secure network infrastructure in the federal administration ("federal networks")** as a basis for electronic audio and data communication.

We will continue to press ahead with the implementation plan for the federal administration. Should the IT security situation get worse, this plan may be aligned accordingly.
Effective IT security requires powerful structures in all federal authorities. For this reason resources must be deployed appropriately at central and local level.

To facilitate implementation through uniform action by authorities, joint investments into the Federal Government's IT security will be made regularly in line with budgetary possibilities.

Operational cooperation with the federal Länder, particularly with regard to **CERTs** (computer emergency response teams), will be further intensified by the IT planning council.

German Cybersecurity Strategy (feb. 2011)

4. National Cyber Response Centre

To optimize operational cooperation between all state authorities and improve the coordination of protection and response measures for IT incidents we will **set up a National Cyber Response Centre**. It will report to the Federal Office for Information Security (BSI) and cooperate directly with the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Civil Protection and Disaster Assistance (BBK).

Cooperation in the National Cyber Response Centre will strictly observe the statutory tasks and powers of all authorities involved on the basis of cooperation agreements. The Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the Bundeswehr and authorities supervising critical infrastructure operators all participate in this centre within the framework of their statutory tasks and powers.

Quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators enables the National Cyber Response Centre to analyse IT incidents and give consolidated recommendations for action. The interests of the private sector to protect itself against crime and espionage in cyberspace should also be adequately taken into account. At the same time respective responsibilities must be observed. Every stakeholder takes the necessary measures in its remit on the basis of the jointly developed national cyber security assessment and coordinates them with the competent authorities as well as partners from industry and academia.

Since security preparedness is best achieved by early warning and prevention, the Cyber Response Centre will submit recommendations to the National Cyber Security Council both on a regular basis and for specific incidents. If the cyber security situation reaches the level of an imminent or already occurred crisis, the National Cyber Response Centre will directly inform the crisis management staff headed by the responsible State Secretary at the Federal Ministry of the Interior.

German Cybersecurity Strategy (feb. 2011)

5. National Cyber Security Council

The identification and removal of structural causes for crises are considered an important preventive tool for cyber security. For this reason we want to establish and maintain cooperation within the Federal Government and between the public and the private sector within the responsibility of **the Federal Government Commissioner for Information Technology** more visible and set up a National Cyber Security Council.

The Federal Chancellery and a State Secretary from each the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Resarch and representatives of the federal Länder will participate. On specific occasions additional ministries will be included.

Business representatives will be invited as associated members. Representatives from academia will be involved, if required. The National Cyber Security Council is intended to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector. The National Cyber Security Council will complement and interlink IT management at federal level and the work of the IT Planning Council in the area of cyber security at a political and strategic level.

German Cybersecurity Strategy (feb. 2011)

6. Effective crime control also in cyberspace

The capabilities of law enforcement agencies, the Federal Office for Information Security and the private sector in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened.

To improve the exchange of know how in this area we intend to set up joint institutions with industry with the participation of the competent law enforcement agencies, which will act in an advisory capacity.

Projects to support partner countries with structural weaknesses will also serve the aim of combating cyber crime. To face up to the growing challenges of global cyber crime activities we will make a major effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention. Furthermore, we will examine whether additional conventions in this area may be necessary at UN level.

German Cybersecurity Strategy (feb. 2011)

7. Effective coordinated action to ensure cyber security in Europe and worldwide

In global cyberspace security can be achieved only through coordinated tools at national and international level.
At EU level we support appropriate measures based on the action plan for the protection of critical information infrastructures, **the extension and moderate enlargement of the mandate of the European Network and Information Security Agency (ENISA)** in view of the changed threat situation in ICT and the pooling of IT competences in EU institutions. The EU Internal Security Strategy and the Digital Agenda provide guidance for further activities.
We will shape our external cyber policy in such a way that German interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as the **United Nations, the OSCE, the Council of Europe, the OECD and NATO.** An increasingly multilateral approach must be brought in line with the necessity of sovereign evaluation and decision-making powers. In this context, a code for state conduct in cyberspace (cyber code) should be established, which is signed by as many countries as possible and includes confidence-building security measures. In the G8 framework we are currently working on intensifying anti-botnet activities.
NATO serves as the basis of transatlantic security. Hence, NATO must take cyber security appropriately into account in its entire range of responsibilities. We are in favour of the alliance's commitment to establishing uniform security standards, which Member States may also use for civilian critical infrastructures on a voluntary basis, as foreseen in NATO's new Strategic Concept.

German Cybersecurity Strategy (feb. 2011)

8. Use of reliable and trustworthy information technology

The availability of reliable IT systems and components must be ensured on a permanent basis. The development of innovative protection plans for improved security which take into account social and economic aspects is strongly supported. To this end, we will continue and intensify research on IT security and on critical infrastructure protection.

Furthermore we will strengthen Germany’s technological sovereignty and economic capacity in the entire range of core strategic IT competences, include them in our political strategies and develop them further. **Wherever it makes sense, we will pool our resources with those of our partners and allies, particularly in Europe.** We are in favour of diversity in technology. Our aim is to use components in critical security areas which are **certified against an international recognized certification standard**

German Cybersecurity Strategy (feb. 2011)

9. Personnel development in federal authorities

Given the strategic importance of cyber security, it must be examined as a priority whether additional staff is necessary in authorities in the interest of cyber security. Furthermore, intensified personnel exchange between federal authorities and appropriate **further training measures will enhance interministerial cooperation**.

German Cybersecurity Strategy (feb. 2011)

10. Tools to respond to cyber attacks

If the state wants to be fully prepared for cyber attacks, a coordinated and comprehensive **set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities**.
We will continue to assess the threat situation regularly and take appropriate protection measures. If necessary, we have to examine whether additional statutory powers must be created at federal or Länder level. Above all, the aims, mechanisms and institutions mentioned above must be internalized through a permanent exercise process with the relevant federal and Länder authorities as well as businesses.

- Presentation of CS – Communication & Systèmes
- The European and German Cybersecurity environment
- **CS Security Business**
- Offers: SOCs, SIEM, Industrial Control Systems (ICS) Security
- Some customer references

CS, a global offer to **PROTECT YOUR INFRASTRUCTURES AND YOUR DATA**

➔ cybersecurity: to fight against **CYBERCRIME** and create a **CYBERDEFENCE**

➔ trust services: to answer security needs in the **PAPERLESS DIGITAL ENTERPRISE,** through dematerialization

The new digital organization: what security for tomorrow?

Information System

Cloud security

Hyperconnected employees, customers, suppliers

New threats (APT…)

Mobility & BYOD

Big Data and external daya

Regulatory environment

New responsibilities: GRC

Key Issues

Extended IT & Network on multiple sites, proliferation of real time information sources

Increase and diversity of cyberthreats, how to manage cybersecurity globally

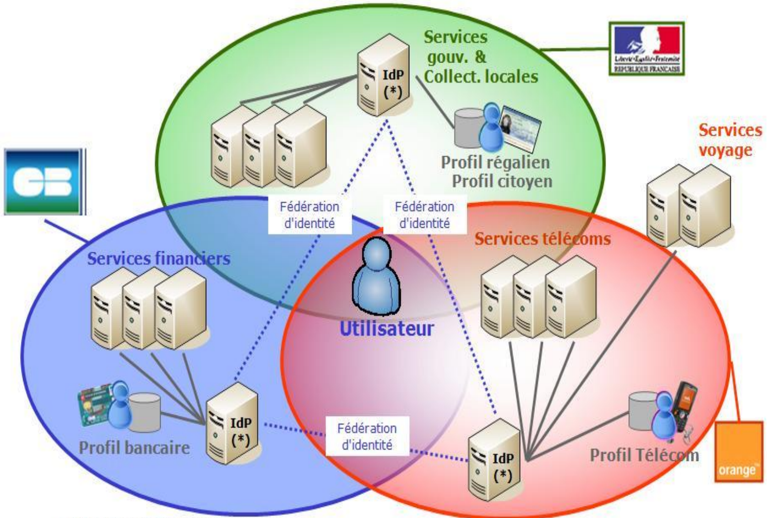
Time to detect, act, repair (and restart operations) much too long

How to prove compliance with regulations, how to reduce the business risk (confidentiality, integrity, availability, audit trails)

CS : Integrator and Operator of IT Security solutions

Cybersecurity

Trust Services

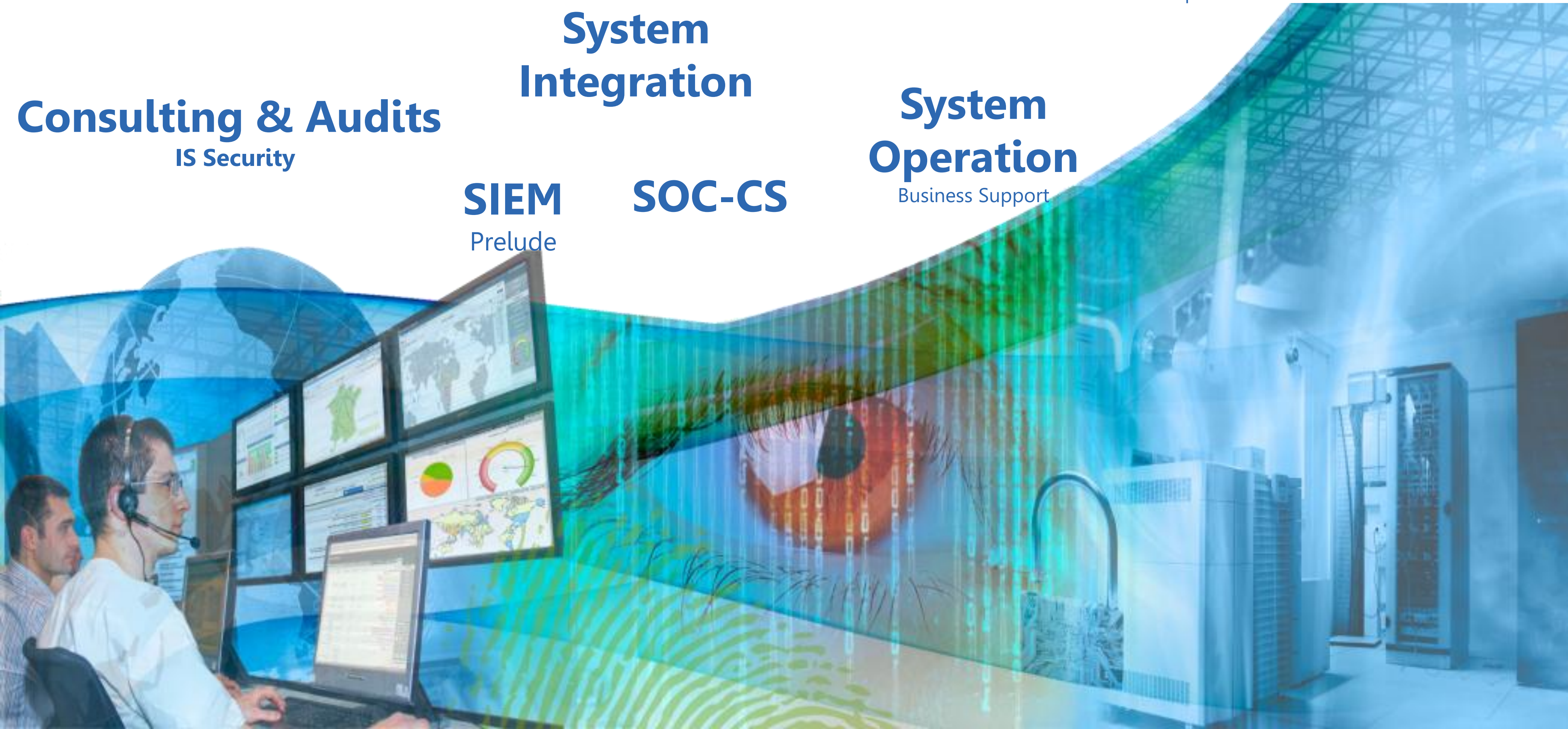


(*) IDP : Serveurs d'authentification

- Audit and Advisory Services in IT Security
- Security Operations Centers (SOC) / NOC
- Fast Intervention Group
- Secured Condition Maintenance (SCM)

- Trust Services Trusty
- Multi-level bridges
- Secured communications
- HSM

Cybersecurity



Consulting & Audits
IS Security

SIEM
Prelude

System Integration

SOC-CS

System Operation
Business Support

FIG
Fast Intervention Group

SCM
Secure Condition Maintenance

End-to-end security

Consulting and business support

Risk Analysis – Management of IS Security – IS Security Policy – Certifications – HPC – High Availability Computing

Security

Data	Users and workstations	Communications	Networks
Sign digitally Certify Protect & Cipher Archive Prove	Authenticate Manage Identity & Access (IAM) Sign digitally	Cipher Comunications Secure electronic messaging	Secure LAN and WAN Manage Multilevel communications

Security Governance

SIEM **Prelude** – Security Operation Centers (SOCs) – Maintenance in Secure Condition (MSC)

Network and Information System (IS) Governance

Network Operation Centers (NOC) – **Vigilo** Solution – IP networks, Voice VoIP **VCS** – Industrial Control Systems (ICS)

- Presentation of CS – Communication & Systèmes
- The European and German Cybersecurity environment
- CS Security Business
- **Offers: Audit, SOCs, SIEM, Industrial Control Systems (ICS) Security**
- Some customer references

Advisory Services and Management support

la force de l'innovation

World Class Expertise

- ➔Customer centric
- ➔Results driven

Risk Analysis
(Ebios, ISO 27005,…)

Security Audits
Penetration Tests

ISS Support (ISS Policies, key ceremonies, security docs writing like SSRS Otan…)

Maintenance in Security Condition MSC

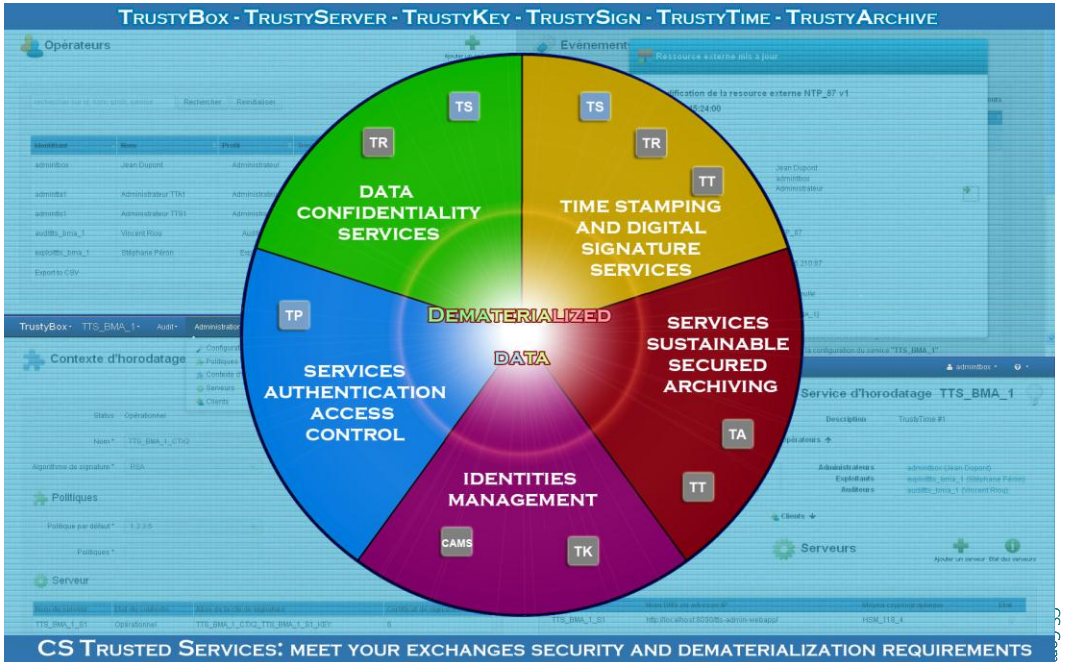
Certification support
(ETSI, ISO 27 0XX, Government listed supplier…)

Cyberdefence

Trust services : Trusty

➔ The Trust services

- Secured dematerialization
- Identity and Access management
- Delivery of baseline services: ciphering, PKI, signatures, time stamping, archival


TrustyBox - TrustyServer - TrustyKey - TrustySign - TrustyTime - TrustyArchive
TS
TR
DATA CONFIDENTIALITY SERVICES
TS
TR
TT
TIME STAMPING AND DIGITAL SIGNATURE SERVICES
TP
DEMATERIALIZED
DATA
SERVICES SUSTAINABLE SECURED ARCHIVING
SERVICES AUTHENTICATION ACCESS CONTROL
TA
TT
IDENTITIES MANAGEMENT
CAMS
TK
CS Trusted Services: meet your exchanges security and dematerialization requirements

➔ The Trusty products

- A product range to create solutions that enable digital trust
- Modular solution
- Common Criteria Certification
- Highly flexible according to customer needs

Trusty products

- **TrustyKey** : PKI
- **TrustyTime** : Time stamp server
- **TrustySign** : Digital signature, verification and ciphering
- **TrustyServer** : Digital signature, verification and ciphering server
- **TrustyArchive** : Long term archival with probating value
- **TrustyPass :** SSL/TLS authentication

Strategy for SOC-CS and Prelude : Europe, Vital Infrastructures Organizations (VIOs), LMP, ANSSI……

- **SRI/ NIS Directive in Europe (03/2014) and LPM in France (12/2013)**
  - **The EU countries must adapt the NIS Directive in 2014**
  - **The ANSSI in France will publish compliance rules effective 1 january 2015**
  - **2014: qualification rules for the SOCs serving the VIOs, and the build-in SIEMs**
  - **1st January 2015: LPM Law enforced in France**
- The future constraints imposed on VIOs in Europe will be applied (on certain perimeters**) to their own service providers:** *IT outsourcing, Managed Security Services, Managed SOCs, Cloud Services…*
- The new directive will allow the VIO to **invest in Security Systems in confidence**, because they will have been approved by ANSSI
- For France, the new regulation would impose that the **SOCs of the VIO be operated in Europe, with Data in France**

The **SOC-CS** will comply with the future obligations that relate to services to VIOs, in Europe and in France

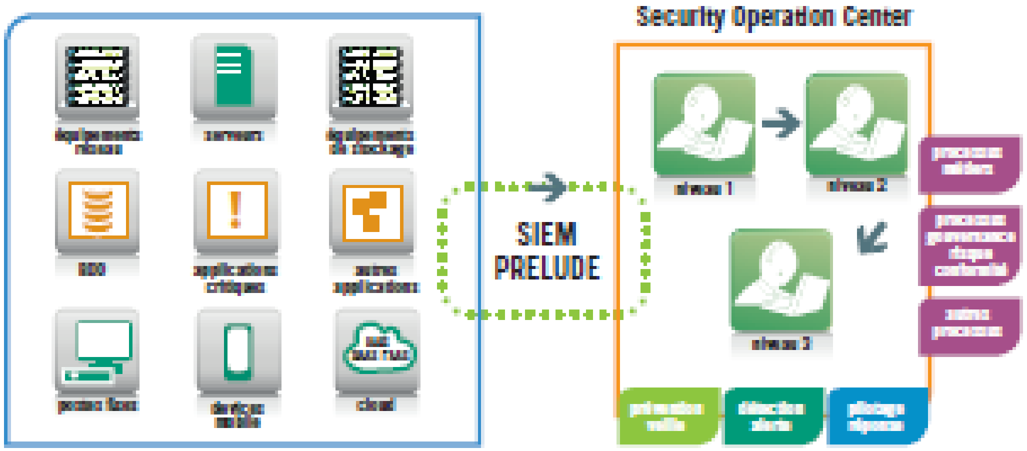
PRELUDE
The PRELUDE SIEM is supported by Europe, ANSSI, the Industry Ministry, the MOD, auditable and controlled software code, world class performance

Why a SOC, or several SOCs?

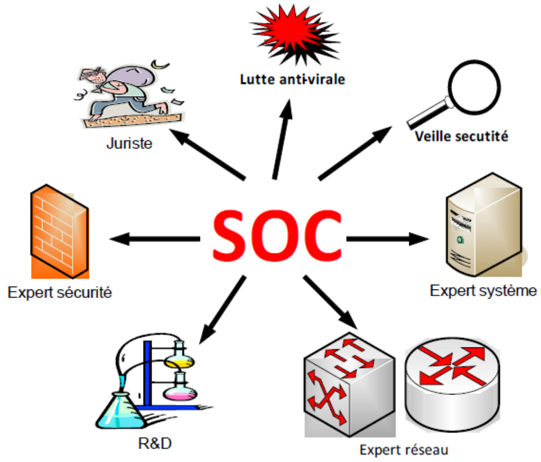
- Beyond data, **real time information security has become strategic**
  - Manage complex operations on a global scale
  - Manage global security, give real time visibility
  - Security supervision has to adapt to a fast changing organization (M&A, org change, new territories, new business models…): flexibility
- **Threats and vulnerabilities increase rapidly**
  - New vuln. per year: **IT: 8k to 10k** *(+10% trend),* **SCADA: 200+** *(from 20 only in 2008),* **Mobile : 300** *(+68% yoy)*
  - Prevention, Alert, Response & Remediation have become a must altogether
- **Centralisation**
  - Strategic view, Security management, visibility on system capabilities
- **Improve the Governance of Risk, Security and Compliance**
- **Establish proofs** in case of conflicts
- **Insure cyberrisk** (new insurance policies)
- Manage **a complex and changing** hierarchy of SOCS

What is a SOC?

- A SOC is an **information system**
  - *Processes*
  - *People*
  - *Technologies*



- It answers specific needs of an organization and it is tailor-made
- It provides
  - **Prevention and continuous threat intelligence**
  - **Detection and Alerts**
  - **Means for Action, Response, Remediation, Forensics…**
- Operations and experts work together hand in hand



CS : Designer, Integrator, Operator of SOCs (1/2)

la force de l'innovation

Customer centric SOCs

- **« Made to Order »: Planning, Design, Integration, Operating**
- State of the Art **Technologies**
- **Processes**
- **Human resources and Teams**

System Integrator

- Expecially for Critical IT Systems

SOC-CS

- Managed SOC Services
- Multiclients, multiservices

Editor of the only European SIEM : Prelude

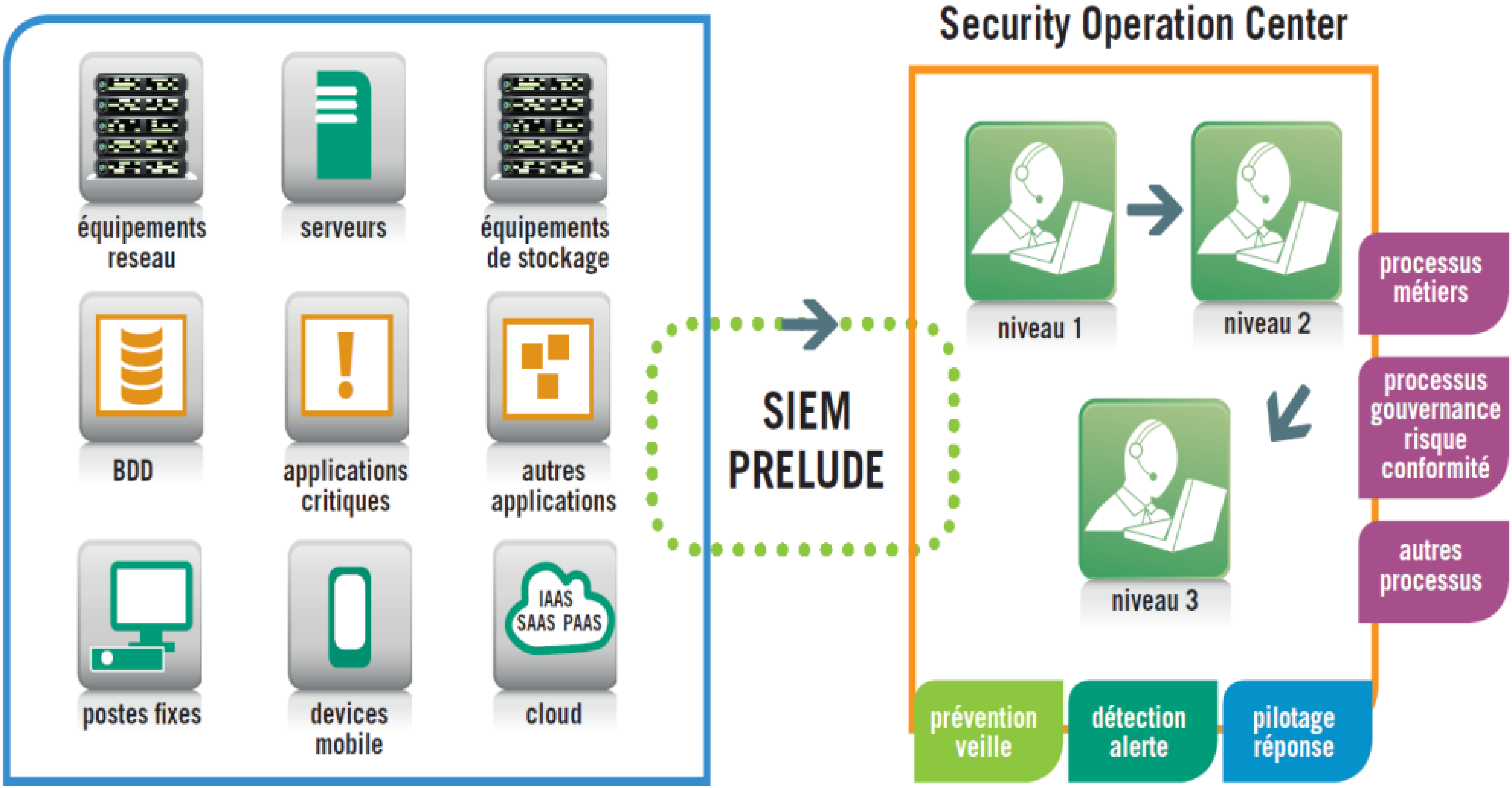
Core technologies of the SOC : **Prelude Entreprise**

Numerous Customer references in xOCs

- As **Opérateur** : SOC MTLID, SOC/NOC EPR Flamanville, NOC Renater…
- As **System Integrator**: SOCs of the IS of the French Armies, NOC Crédit Mutuel (Euro information/ CMEI)…
- As tant **Advisor:** ANSSI…
- Several refernces in **C2 Control & Command Centers**

CS : Designer, Integrator, Operator of SOCs (2/2)

la force de l'innovation



Security Operation Center

équipements reseau

serveurs

équipements de stockage

BDD

applications critiques

autres applications

postes fixes

devices mobile

IAAS SAAS PAAS

cloud

SIEM PRELUDE

niveau 1

niveau 2

niveau 3

processus métiers

processus gouvernance risque conformité

autres processus

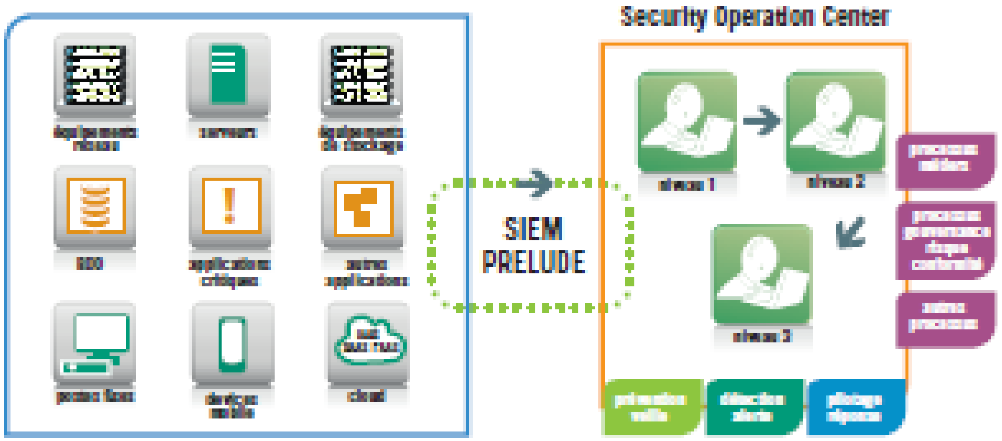
prévention veille

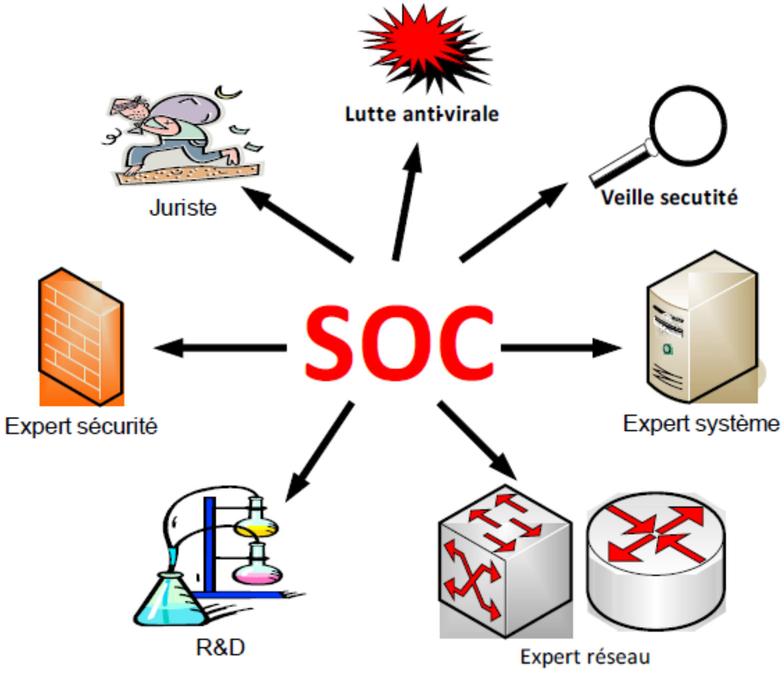
détection alerte

pilotage réponse

The SOC-CS

- **Information System**
  - Processes, Teams, Technologies
  - Securely integrated to the other IS of the organization : corporate, business
- It answers a need to supervise and manage globally the IT security of the organization as a whole
- It implements:
  - **Prevention and Intelligence**
  - **Detection and Alerting**
  - **Response and Security Management**
- Il relies on **a Operating Team** and **Security Experts**





Main services of the SOC

Prevention & Intelligence

- Threat and technology intelligence
- Announcements
- Product validation
- Consulting, coaching
- Training
- Incident classification
- Risk Analysis
- Security audits
- ...

Detection & Alert

- Event detection
- APT detection
- Behavioral analysis
- Threat info source integration
- Security Analytics
- Alert notification
- Intelligent correlation
- Rapid incident qualification
- ...

Response & Mngt

- Incident analysis, processing, support
- Fast Intervention group
- Vuln. Analysis/correction
- Processes with other departments, GRC, DR
- IS clean-up
- Forensics
- Administration
- Reporting
- ...

One SOC, many processes

➔ Business processes

- Admin, connection to Disaster Recovery, to Compliance management, to Risk management…
- KPI and reporting
- SOC management processes, continuous process improvement

➔ Technological processes

- Architectures, system admin
- Configuration management
- Maintainance in secure condition

➔ Operational processes

- Capacity Planning, shifts, on duty teams, daily operations
- Incident management, escalation procedures, crisis management
- HR management, competencies, training
- Equipment lifecycle management (enrolment -> decommissioning…)

➔ Security specific processes

- Intrusion analysis, incidents, reportings…
- Continuous threat intellligence, new threats and methods (APT…)
- Continuous security improvement (SOC and equipments)

One SOC, several Teams

The SOC Team

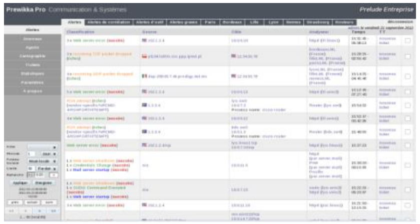
- Operators (N1)
- Security Analysts (N2)
- Security Experts (N3)
- System admin, SOC security and support staff
- Manager and HR
- Forensics analyst
- SIEM engineers
- Threat intelligence specialists
- Emergency Response Team

Core competencies

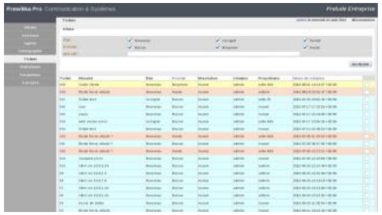
- ITIL
- Crisis management
- System and business expertise (forensics, DR…)
- …

Continuous training

One SOC, one SIEM, many technologies

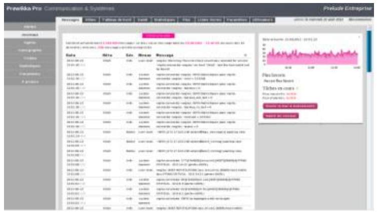


Events

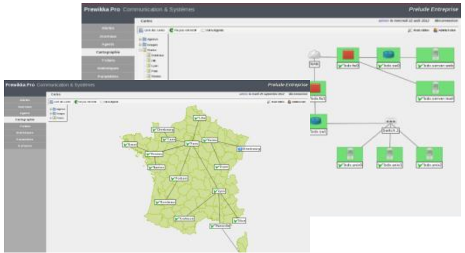


Tickets

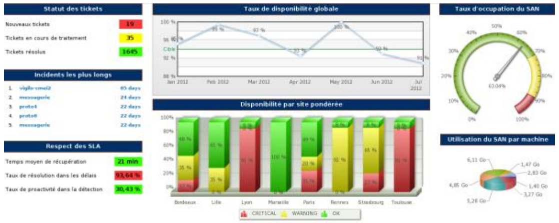
Statistics



Log Management



Maps



Statut des tickets

Nouveaux tickets	19
Tickets en cours de traitement	35
Tickets résolus	1645

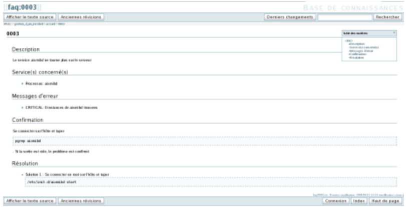
Incidents les plus longs

1.	vigile-cmei2	65 days
2.	messagerie	24 days
3.	proto4	22 days
4.	proto8	22 days
5.	messagerie	22 days

Respect des SLA

Temps moyen de récupération	21 min
Taux de résolution dans les délais	93,64 %
Taux de proactivité dans la détection	30,43 %

Reporting



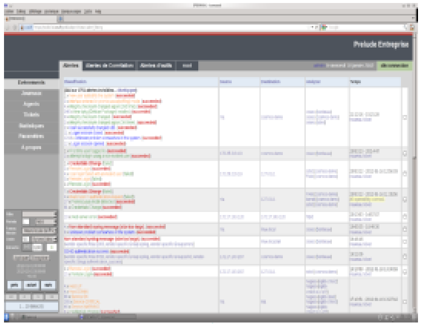
Knowledge base

Inventory

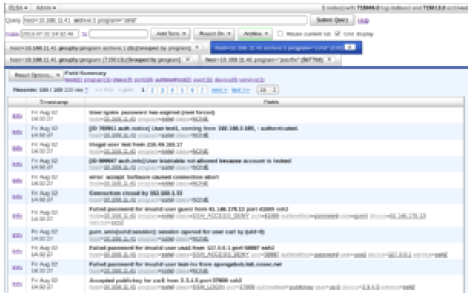
SIEM Prelude :core technology of the SOC

Security Governance: SIEM Prelude

ALERTING



ARCHIVING



ANALYSIS

PRELUDE

- Agregation
- Correlation
- Normalisation
- Selection
- Collect

Network
Systems
Applications
Probes

Prelude key benefits

Available in GERMAN

- **State of the art features, performance and usability**
  - Recognized solution even in **most demanding environments**
- **The only European SIEM solution**
  - Open source core, **guaranteed, controllable and auditable code**
  - Supported by **Europe, ANSSI, French MOD and Industry Minister**
  - An editor-integrator in a position to **support a complete SIEM project**
- **Stable and reliable solution**
  - **First SEM in the world**, as early as 1998, millions of users
- **Open standards compliance**
  - **IETF:** IDMEF natively interfaced to intrusion detection probes HIDS, NIDS (Snort, OSSEC, Samhain, ClamAV, etc.), and IODEF
  - SSL/TLS, HTTPS : **Web 2.0 standards compliance**, light client, Syslog, AMQP…
- **A highly modular, flexible and customisable solution**
  - Easily create a **hierarchy of SOCs, multilevel SOCs**
  - **Supports rapidly any organization change** (M&A, new territories, businesses, new initiatives…)
  - Web interface and **easy integration with any other module of the SOC**
  - Solution as **hardware, software, virtual or combination**

Customer testimonal Prelude - AlfaStrakhovanie Group - Russia – March 2013

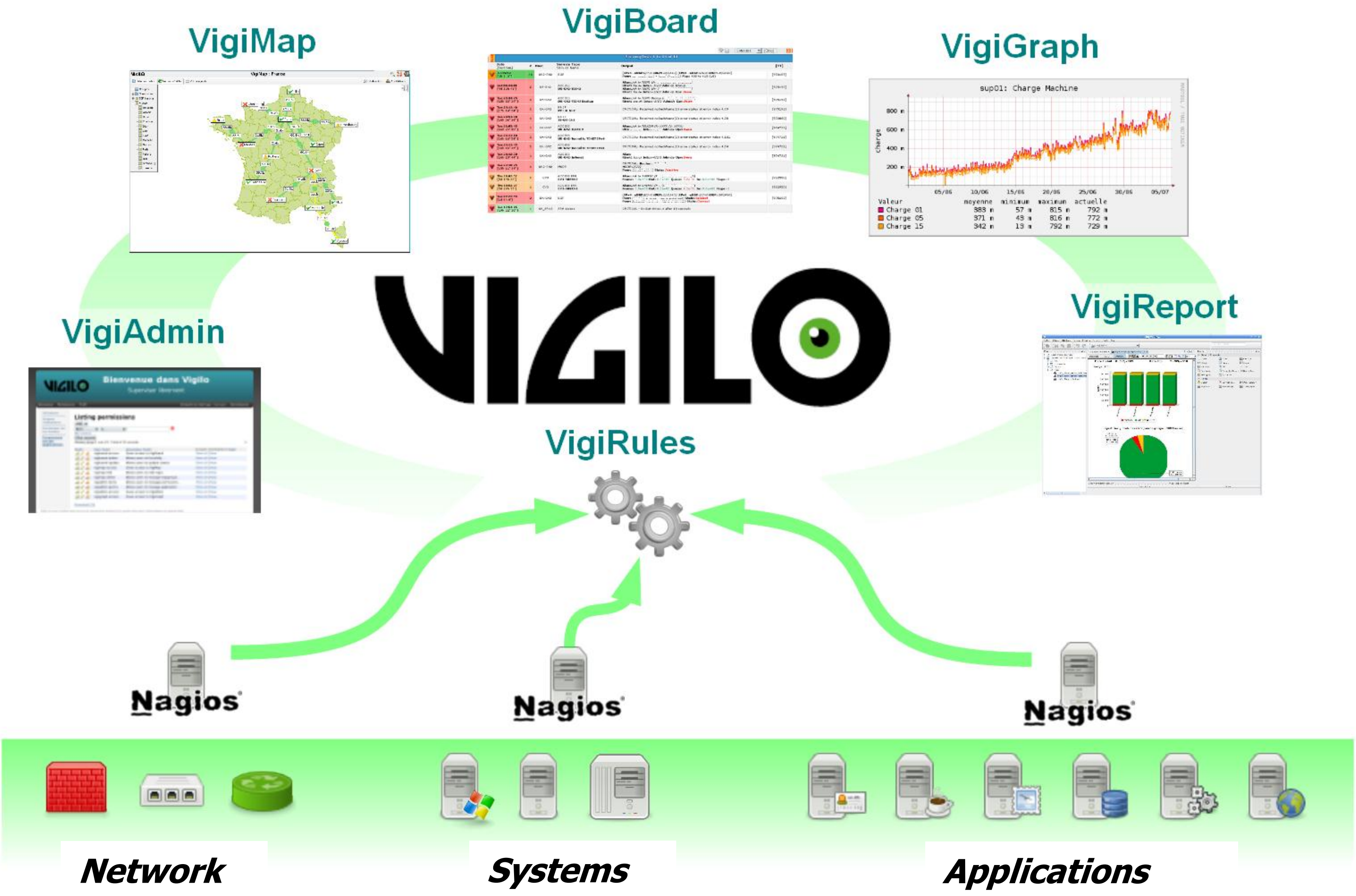
« AlfaStrakhovanie is a big insurance company with a large geographically distributed infrastructure: our network perimeter is stretched from Kaliningrad to Kamchatka.

- At the moment we have: **400 branch offices, 6000 employees, 2 data storage centers, 1 data processing center,**
- We have been using **Prelude for 3 years** and during this time it has become an indispensable tool for security event management, incident investigation and response
- Due to Prelude's **modularity** it easily handles with expansion and changes in our infrastructure without losing ability to collect and correlate critical security events
- For us is also very important to provide **compatibility with different types of systems** that should be monitored in one board. For now we have successfully integrated Prelude with:
  - *Antivirus for endpoints (on all employees PCs); OSSEC (Microsoft Active Directory and Windows event logs); Event log collection (*nix, BSD, AIX); Email DLP system; Removable media DLP system(on all employees PCs); Antivirus for Web-Gateways; IPS (at the beginning it was SNORT, for now it is a proprietary solution); Monitoring of network devices; VoIP Servers;*
- Prelude successfully handles with all this data sources and provides us with ability to add new ones in cost-effective manner. That in general gives us an ability to use **centralized approach** for managing our security solutions and provide the overall **high level of information security**. »

Head Department of Technical Security, AlfaStrakhovanie Insurance Moscow.

Network & IS Governance: Vigilo

➔ *Unified IS Supervision*



Vigilo key benefits

- **Powerful solution for very large installed bases**
- **Secure and auditable code**
- **Open source and based on reference solutions of the industry**
  - Nagios, RRDTool, Talend, TurboGears2, etc.
- **Open standards compliance**
  - SNMP, HTTP(S), SSH, XML, AMQP, etc.
- **Modular and highly flexible** for customized projects
- **Top grade solution for high volumes**
  - Scalability, performances, redundancy
- **Developed, distributed and maintained by a European team**
  - An editor-integrator in a position to support a complete NOC project
  - Speed and cooperation

Focus on IS Security & Industrial Systems Security

la force de l'innovation

➔ CS know how

- **Industrial Systems**
  - Systems engineering
  - Industrial IT
- **IT Security**

➔ Market situation

- In industrial environments, the Security of the Information system is not always a priority
- « Security » in industrial environments relates more to « Safety »

• CS develops an **Industrial IT an IS business**
• CS is already present in Security dedicated to Industrial Systems= **Industrial Systems Security**
• CS advocates taking into account **Information Security as a major driver of operational Safety**

Industrial IS and Industrial IS Security

SCADA and Industrial Control Systems (ICS)

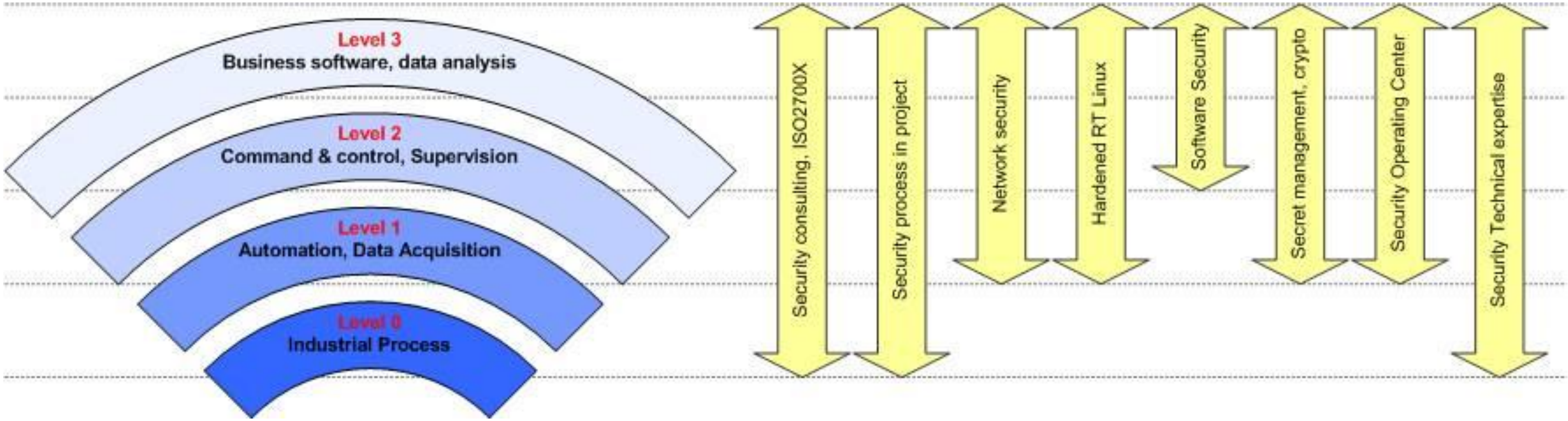
- Turnkey systems
- R&D around safety issues
  - Systems Safety
  - Systems Security
  - Sensors and Probes related issues

Industrial Information Systems Security – Cybersecurity

- **Advisory services** in Industrial IS Security
- **Project support** in Industrial IS Security projects
- **Evaluation & Integration of Security Solutions** for industrial systems, including solutions for IP networks, secure OS SEDUCS, new sensors and probes
- Developpement of **specific security solutions**
- Integration of **industrial network and security supervision** *(Prelude, Vigilo, integration in Panorama for example)*

Industrial IS Security

- **CS targets the generic IS Security to the specific needs of an industrial information system**


Level 3
Business software, data analysis
Level 2
Command & control, Supervision
Level 1
Automation, Data Acquisition
Level 0
Industrial Process
Security consulting, ISO2700X
Security process in project
Network security
Hardened RT Linux
Software Security
Secret management, crypto
Security Operating Center
Security Technical expertise

Integration of security solutions for industry specific protocols

➔ **Example: RadiFlow**

- Capability to secure communications in the various layers of a SCADA/ Industrial Control System, expecially between layers 0 and 1
  - Industrial Ethernet
  - RS232C, RS422
  - An extensive pack of security services is built in:
    - Router, VPN, Firewall
    - DPI (Deep Packet Inspection) and data inspection linked to each protocol *(Schneider MODBUS, Siemens PROFIBUS…)*
- Can be directly connected to the SOC-CS, Security Supervision Center through the SIEM Prelude

➔ *Under evaluation by CS*

- Presentation of CS – Communication & Systèmes
- The European and German Cybersecurity environment
- CS Security Business
- Offers: SOCs, SIEM, Industrial Control Systems (ICS) Security
- **Some customer references**

Industrial IS of the Flamanville Nuclear Plant (EPR) - France

la force de l'innovation

Customer: EDF

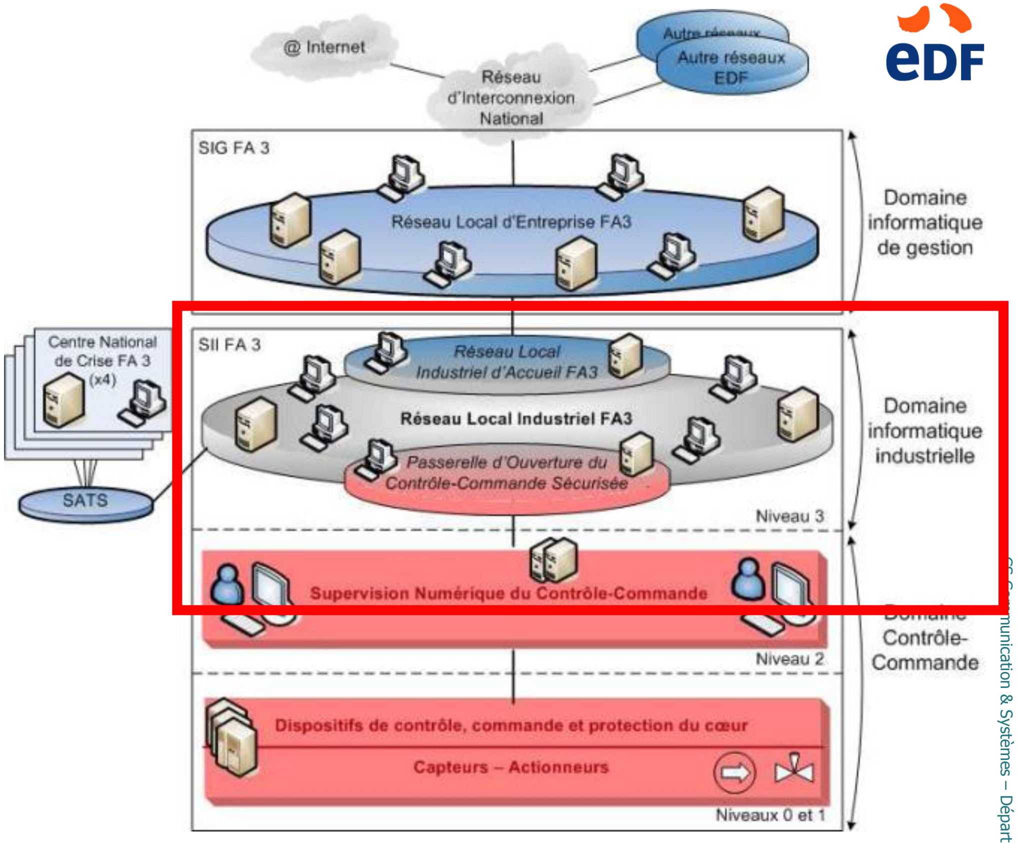
- Implementation of the network and IT infrastructure of the **Level 3** of the Industrial Control System

Objectives of EDF

- Facilitate the management of the plant
- Provide analysis of the status
- Publish data about lower levels
- Develop and integrate technical gateways for secure access to external networks

Stakes

- State of the art security and protection against cyberthreats
- Capability to open up to outside networks
- Supervision, and use of SIEM Technology
- Methodology/ quality
- Maintainance in Operational and Secure conditions
- Future proof technologies


@ Internet
Autre réseaux
Autre réseaux EDF
Réseau d'Interconnexion National
SIG FA 3
Réseau Local d'Entreprise FA3
Domaine informatique de gestion
Centre National de Crise FA 3 (x4)
SATS
SII FA 3
Réseau Local Industriel d'Accueil FA3
Réseau Local Industriel FA3
Passerelle d'Ouverture du Contrôle-Commande Sécurisée
Niveau 3
Domaine informatique industrielle
Supervision Numérique du Contrôle-Commande
Niveau 2
Domaine Contrôle-Commande
Dispositifs de contrôle, commande et protection du cœur
Capteurs – Actionneurs
Niveaux 0 et 1

Customer references, government (1/2)

MOD

IS of the joint forces

-Build the **NOCs/SOCs** embarking **SIEM** Prelude, **NOC** Vigilo
-Common foundation of **digital signatures**
-**Multi-tiered MSC**, **largest SIEM in Europe**
-Management and support of the **homologation process** (FR and NATO)

Government level IS

Security of communications

-**Communication bridges**
-***Top secret* grade secured electronic messaging**

Ministry of Justice

IS Security Consulting

-GISSIP Methodology
-Support of **homologation files**
-**Risk analysis**
-Support of the **Security Process formalization**

MOD

Vulnerability and Penetration Tests

-**Black Box/ White Box**
-**Specific tests**

Customer references, government (2/2)

Ministry of Home Affairs

ID Cards for civil servants

-**Public Key Infrastructure**
-**Digital signatures**
-**Strong authentication** with smart cards
-**200 000 cards in the field,** target: 400 000

MOD

Secured IS & Radiocommunications

Air defence system

-**Secured network**
-**Hardened OS**
-**Globalized MSC**

Middle-East State

IS Security at country level

-Build of a **PKI**
-Set up of the **processes of a National Security Agency**

Customer references, private and semi-private (1/2)

Alstom

IT Security of Electric Power Plants

- Support in writing the **System Security File**

EDF

Nuclear Plant Supervision

-**Secured network**
-Multi layer **communication bridges**
-**Data flow supervisio**n (SIEM)
-**Network, Industrial control and Sensor supervision**

Areva

IS Security Consulting
Industrial Control System – Nuclear power plant

-**Safety & Security requirements** of Finland
-Support in **methodology and compliance** with norms wrt implementation of ISS framework
- **Risk analysis**: ISO27001, IAEA, German, French and Finnish norms

Iter

Solution to manage cryptographic secrets

-Global analysis of the **end to end secured management of secrets**
-Expertise and architecture of **HSM**
-**Software implementation**
-Support in **organizing the « key exchange ceremony »**

Customer references, private and semi-private (2/2)

la force de l'innovation

International Insurance company

SOC managed by CS

-Support of a new **professional insurance offer against cyber risk**
- > 3000 customers in France
- **Prevention/ alert/ analysis and incident management**

La Poste

Registered electronic mail

-Support of the **requirements as government supplier**
-Time stamping with **probating value**
-**Training**

High Council of French Notaries

Paperless authentic instrument

Conseil Supérieur du Notariat

-**Digital signatures**
-**Time stamping**
-**Archival with probating value** for 99 years

GIE Cartes Bancaires

Authorization network for payment cards

-**Highly secured** network
-**Highly available** network
-Transaction **certification**
-Network **supervision**

la force de l'innovation

Please Visit us at

Assises de la Sécurité 2014

1-3 October 2014 – Monaco – Europe

Thank you

SIEM et Prelude

Positionnement CS sur le marché des SIEM

- Les éditeurs de SIEM sont quasiment tous similaires
  - Ce sont principalement des éditeurs américains, ayant racheté un produit SEM et un produit SIM
  - Ils proposent tous les mêmes boîtiers, aux mêmes capacités (en termes d'EPS notamment)
  - Chaque éditeur propose son format propriétaire et parfois ses propres sondes et collecteurs
- Pour déployer un SIEM, un Client doit
  - Traiter avec un éditeur pour acheter les produits / les boîtiers
  - Traiter avec un intégrateur pour personnaliser et déployer le produit
  - Traiter avec éventuellement des éditeurs de sondes

CS se positionne en temps qu'éditeur-intégrateur

- *Accompagnement du client jusqu'au système « clé en main »*
- *Prestation de mise en œuvre et de configuration ad-hoc du produit*
- *Proposition et installation de sondes open-source ou éditeurs*

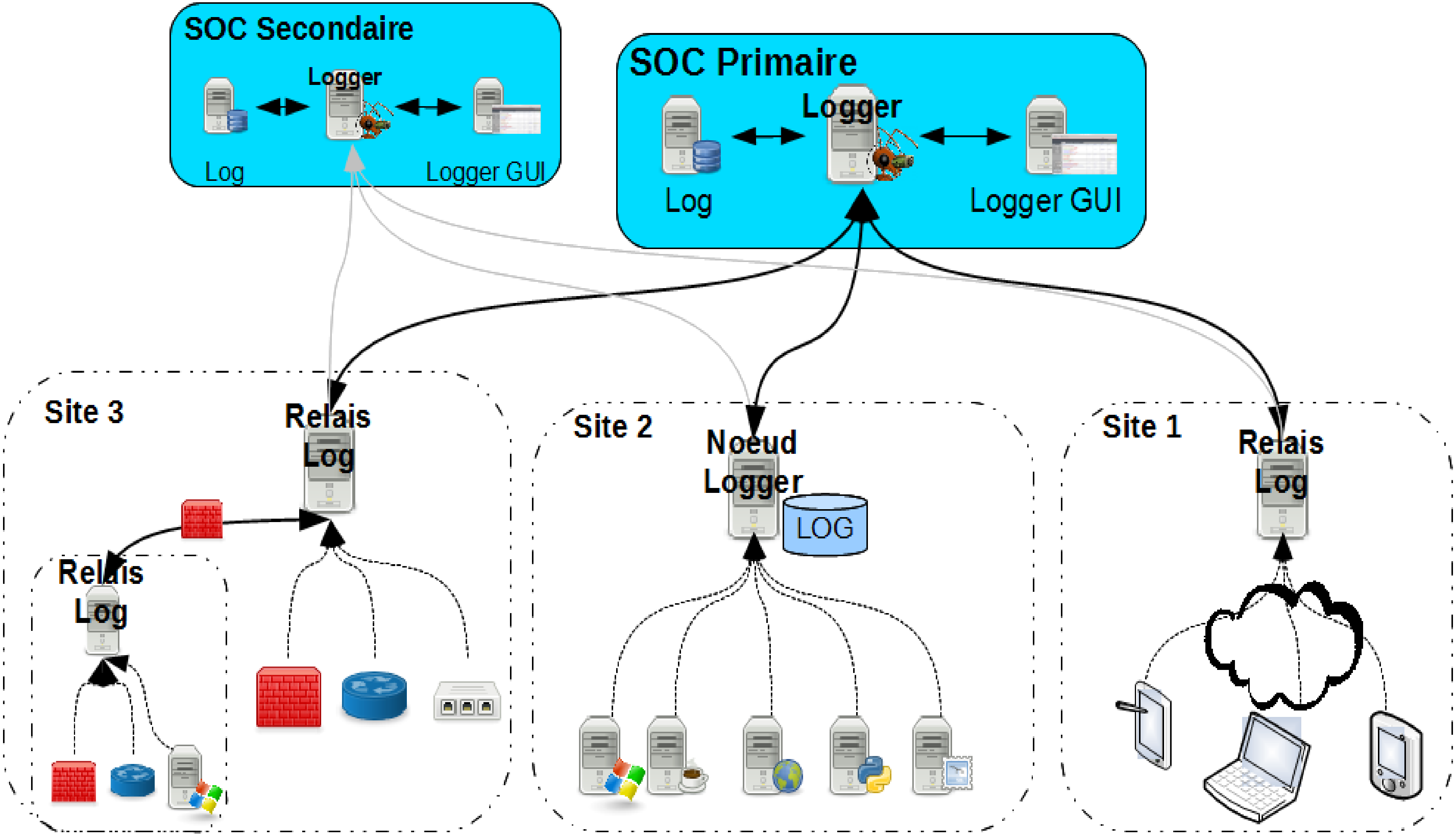
Points forts de Prelude

- **Fonctionnalités, performance et ergonomie à l'état de l'art mondial**
  - Solution reconnue même dans les environnement les plus exigeants
- **Seule solution de SIEM souveraine européenne et française**
  - Cœur Open Source, garantie d'une **maîtrise et une auditabilité du code**
  - Soutien de **l'ANSSI, de la DGCIS, de la DGA, et de l'Europe**
  - Fournie par un éditeur-intégrateur à même de **supporter l'intégralité du projet SIEM**
- **Stabilité et robustesse de la solution**
  - Premier SEM mondial : développements débutés en 1998
- **Respect des standards du marché**
  - Standards de **l'IETF**: IDMEF et IODEF pour les incidents
  - Nativement couplée avec diverses sondes de détection d'intrusion HIDS, NIDS
    - Snort, OSSEC, Samhain, ClamAV, etc.
- **Solution modulaire, flexible et personnalisable**
  - **Hiérarchisation simple des SOCs** multiniveaux, du petit SOC « terrain » à l'hyperviseur centralisé
  - **Accompagne facilement les transformations de l'organisation**
  - **Interface Web** et clients légers, liaison aisée avec d'autres modules d'un SOC
  - Solution **boîtier, logicielle, virtualisée ou une combinaison**

SIM : Archiver

- Fonctions
  - Centraliser, normaliser, stocker, indexer tous les journaux et traces d'un systèmes
- Objectifs
  - Légal
    - Sur le marché américain, conformité aux normes, etc.
  - Enquête
    - Technico-légales
    - Post-mortem
  - Reporting et Analyse des tendances
    - Aide à la décision
    - Justification de budget

Architecture de PRELUDE: SIM



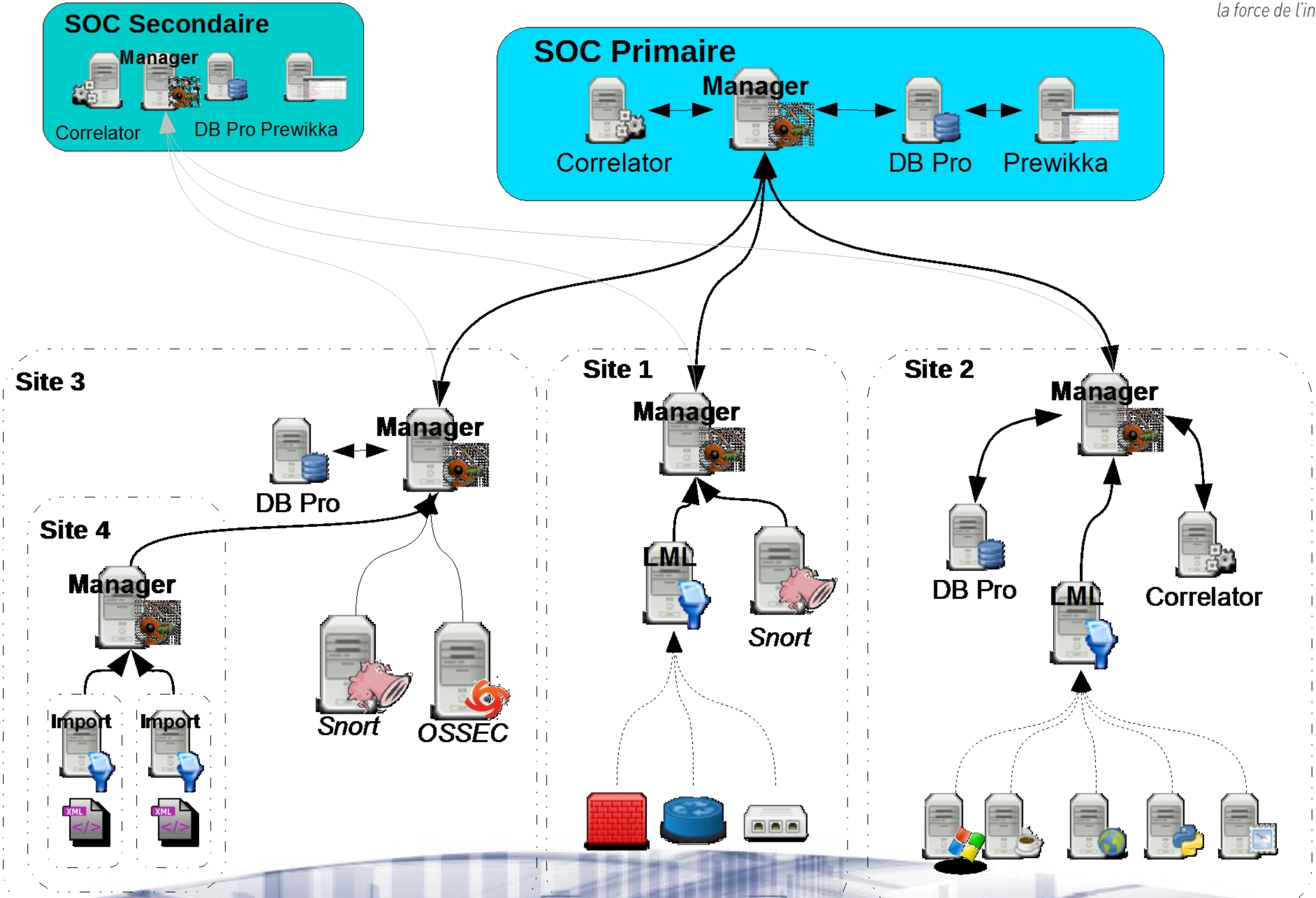
SEM : Alerter - Analyser

- Fonctions
  - Collecter, centraliser, normaliser, trier, agréger, corréler et afficher des événements de sécurité en temps réel

- Objectifs
  - Être **alerté** de comportements à surveiller
    - Comportements anormaux : attaques directes, indirectes, externes/internes, etc.
      - DoS, DDoS, Chevaux de Troie (APT, AET, etc.), virus, deface, injection, etc.
    - Comportements normaux : authentification d'un utilisateur, démarrage d'un service, etc.
  - **Analyser** ces comportements
    - Vis-à-vis d'une norme
      - Horaires, volumétrie, initiateur l'action, etc.
    - Disposer d'outils permettant la catégorisation de ceux-ci
      - Bac à événements, corrélateurs, tableau de bord, statistiques, tendances, etc.

- Doit être unique sur un même parc pour un maximum d'efficacité

Architecture de PRELUDE : SEM



Et demain ? La stratégie SOC de CS

- **Convergence NOC et SOC**
  - *Pourquoi ?*
    - Mutualisation des systèmes: sondes, log management
    - Mutualisation des moyens, au N1 par exemple
    - Rationalisation des coûts
  - Un NOC sert au SOC et inversement
    - Une alerte de performance est potentiellement un événement de sécurité
    - Un événement de sécurité peut impliquer une alerte de performance
  - Les processus d’exploitation sont proches
  - Hypervision commune à un certain niveau
- **SOC et Big Data** : corrélation haute définition avec données internes et externes (IAM, web 2.0…)
- **SOC et SI Industriel (SII)** : accompagnement du SOC sur la trajectoire d’urbanisation des SII
  - Technologies IP, présences d’OS complexes
  - Supervision des sondes, des équipements
  - Sécurité des interfaces SCADA
- **SOC et information**
  - Migration de la protection des assets vers la protection de l’information et de la connaissance