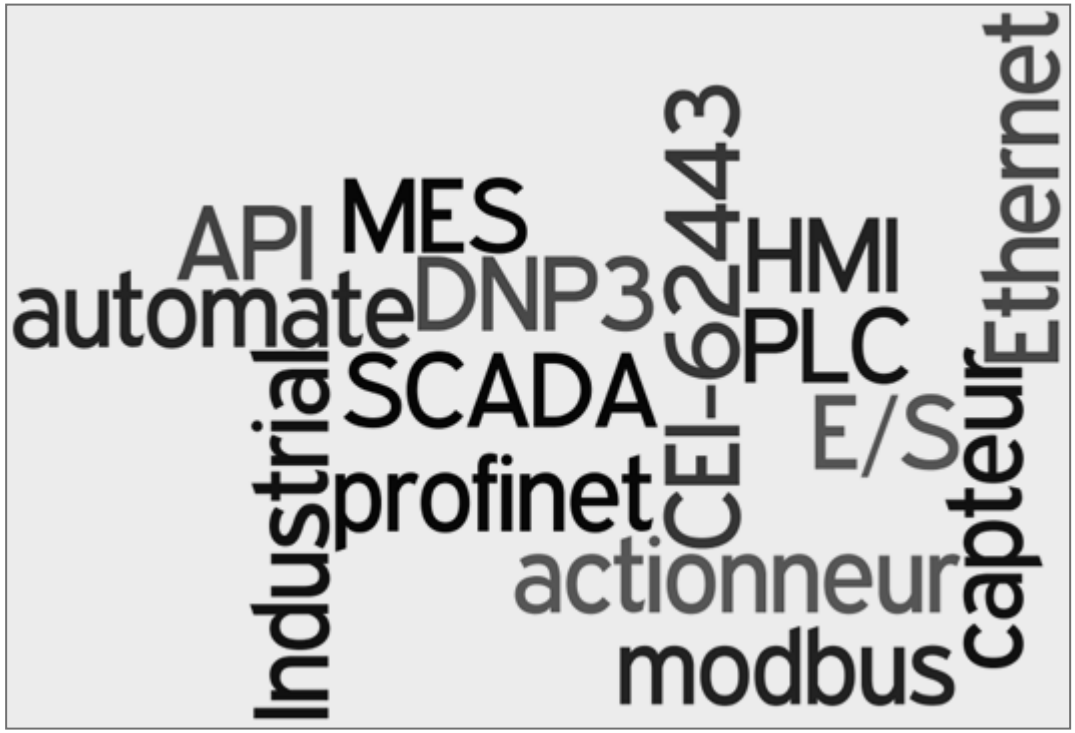
LEXSI

INNOVATIVE SECURITY. FOR BUSINESS

Conseil / Audit / Formations
Veille et lutte contre la cybercriminalité



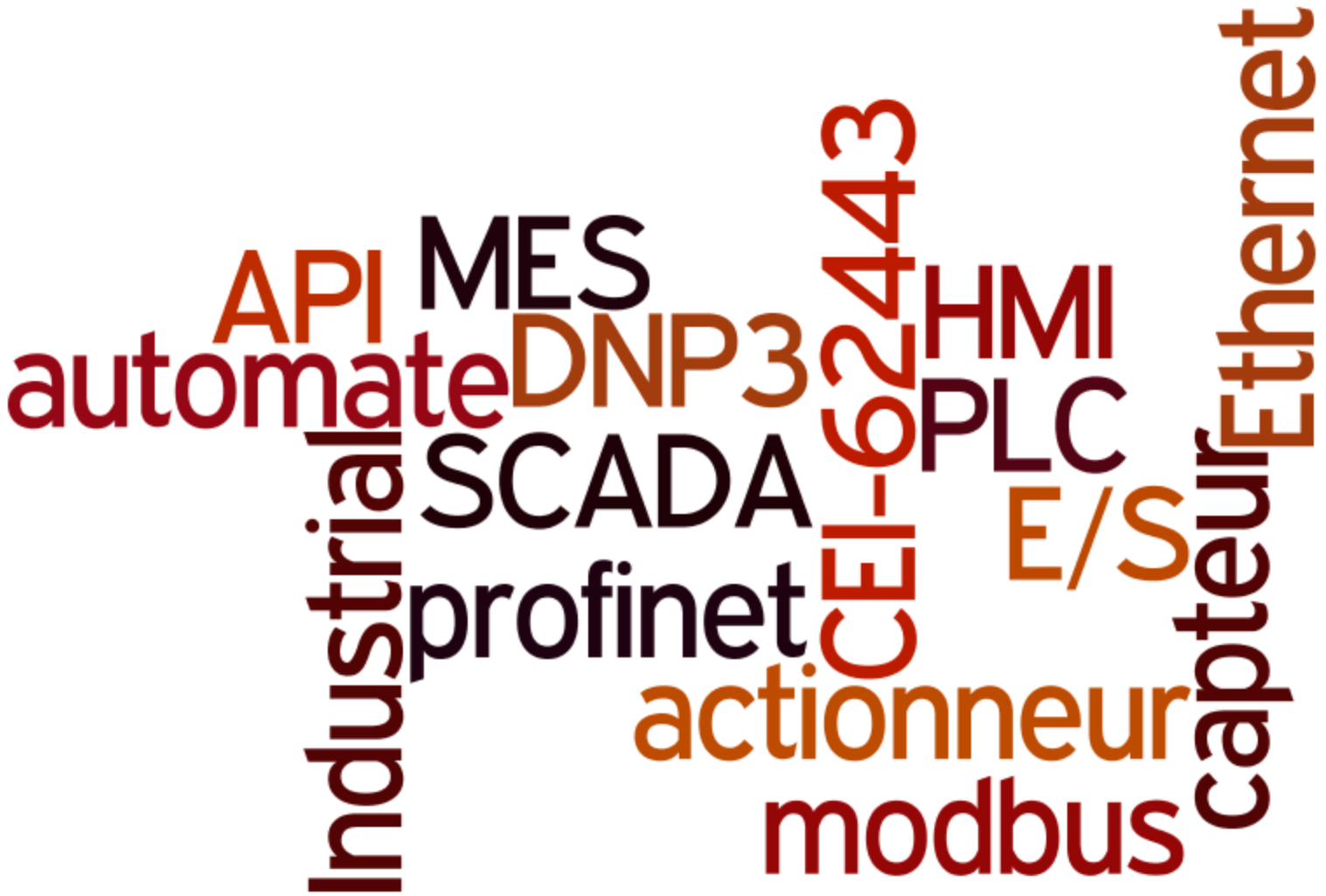
CYBERSÉCURITÉ INDUSTRIELLE

CONSTATS & SOLUTIONS

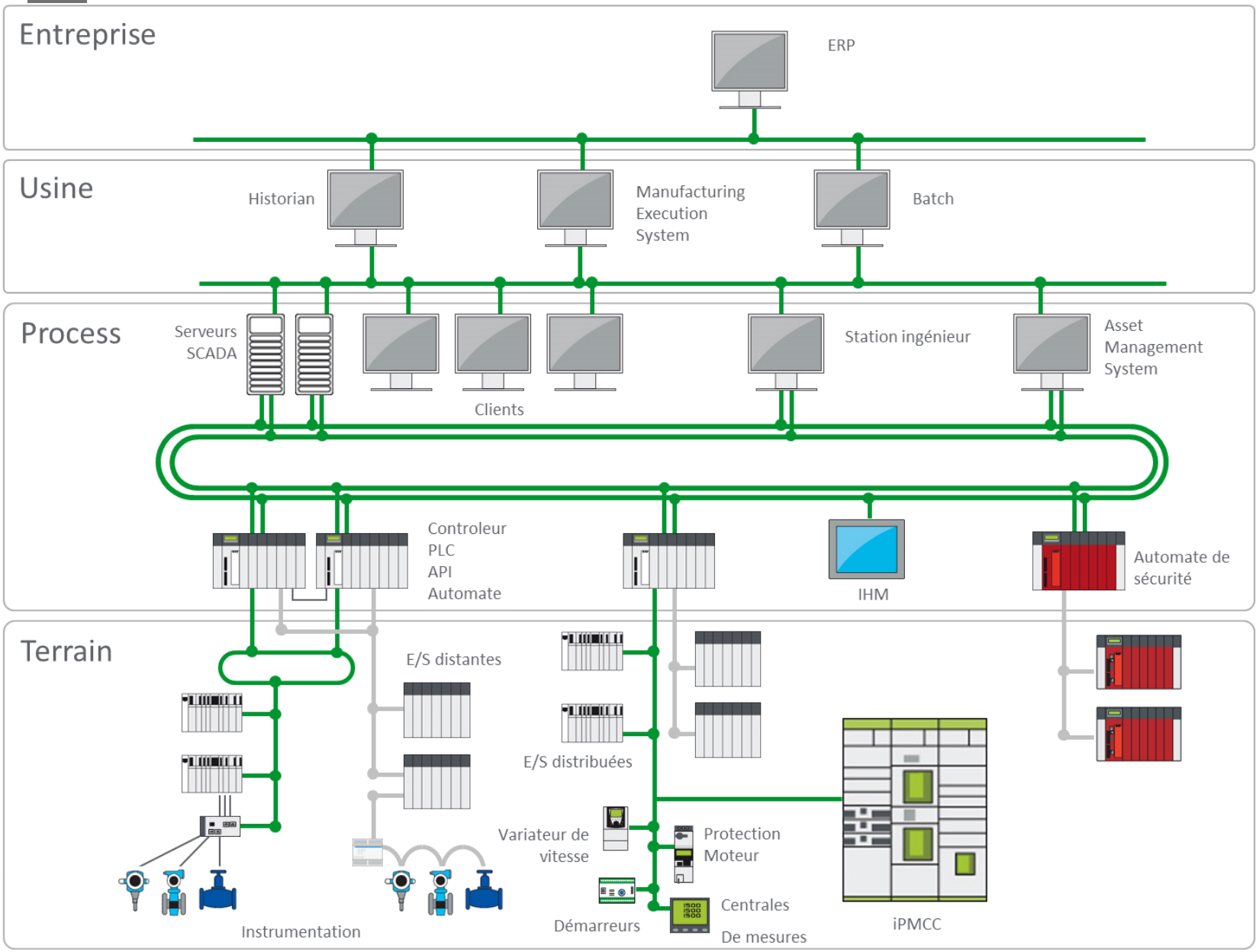
Thomas HOUDY

Manager Innovation & Stratégie
thoudy@lexsi.com

SCADA ? ICS ? CONTRÔLE COMMANDE ?



ARCHITECTURE « TYPE »



Source : Schneider

ENJEUX ET PROBLÉMATIQUES

- Sécurité physique
- Ancienneté des systèmes, réseaux, protocoles
- Insécurité « native » hardware, software, protocoles
- La tendance à l'interconnexion et aux accès distants
- Le risque humain : problématique centrale
- Le risque tiers / fournisseurs
- Les priorités budgétaires
- Convergence sécurité / sûreté : comment faire ?

CYBERSÉCURITÉ INDUSTRIELLE …
… une histoire de ponts

Constructeurs

DG

DSI

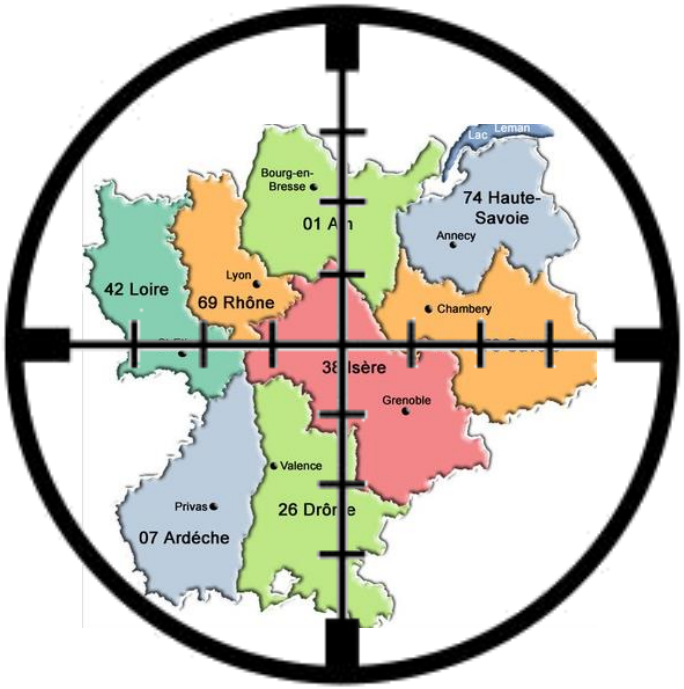
Achats

Moyens Généraux

Dir. Production
Dir. Exploitation
Automaticiens
Resp. Sureté
Resp automatismes
Autres profils ?

Distributeurs
Intégrateurs
Installateurs

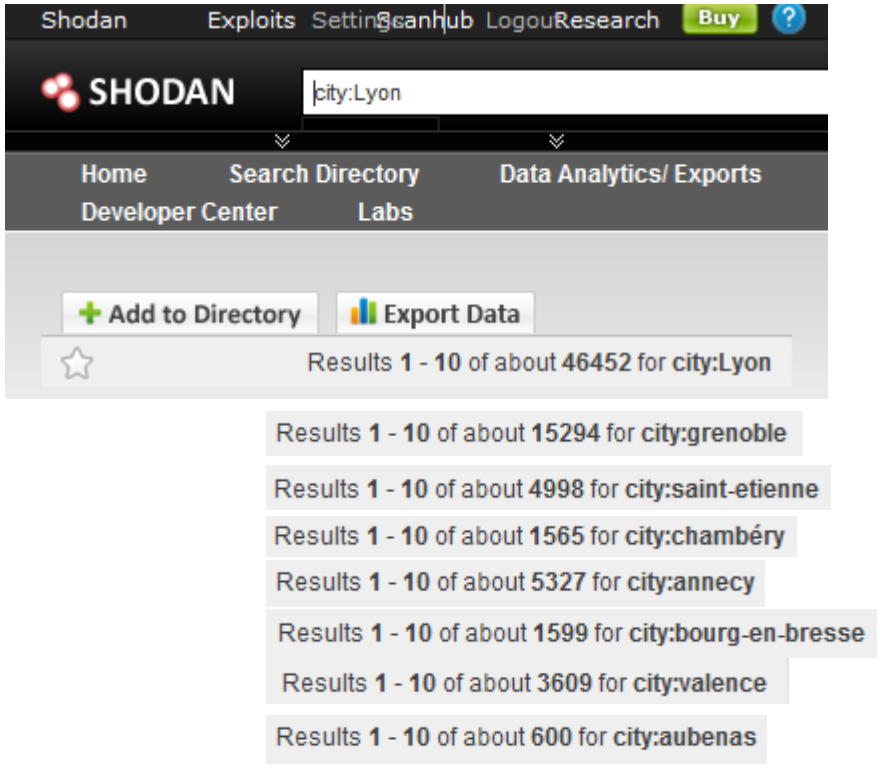
RÉGION RHÔNE ALPES

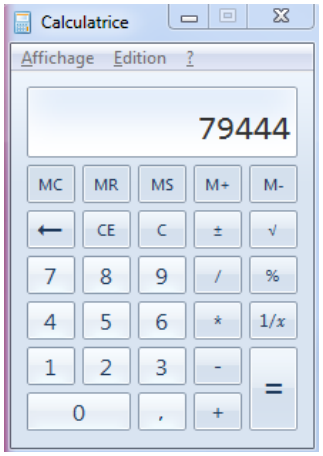


RHÔNE ALPES

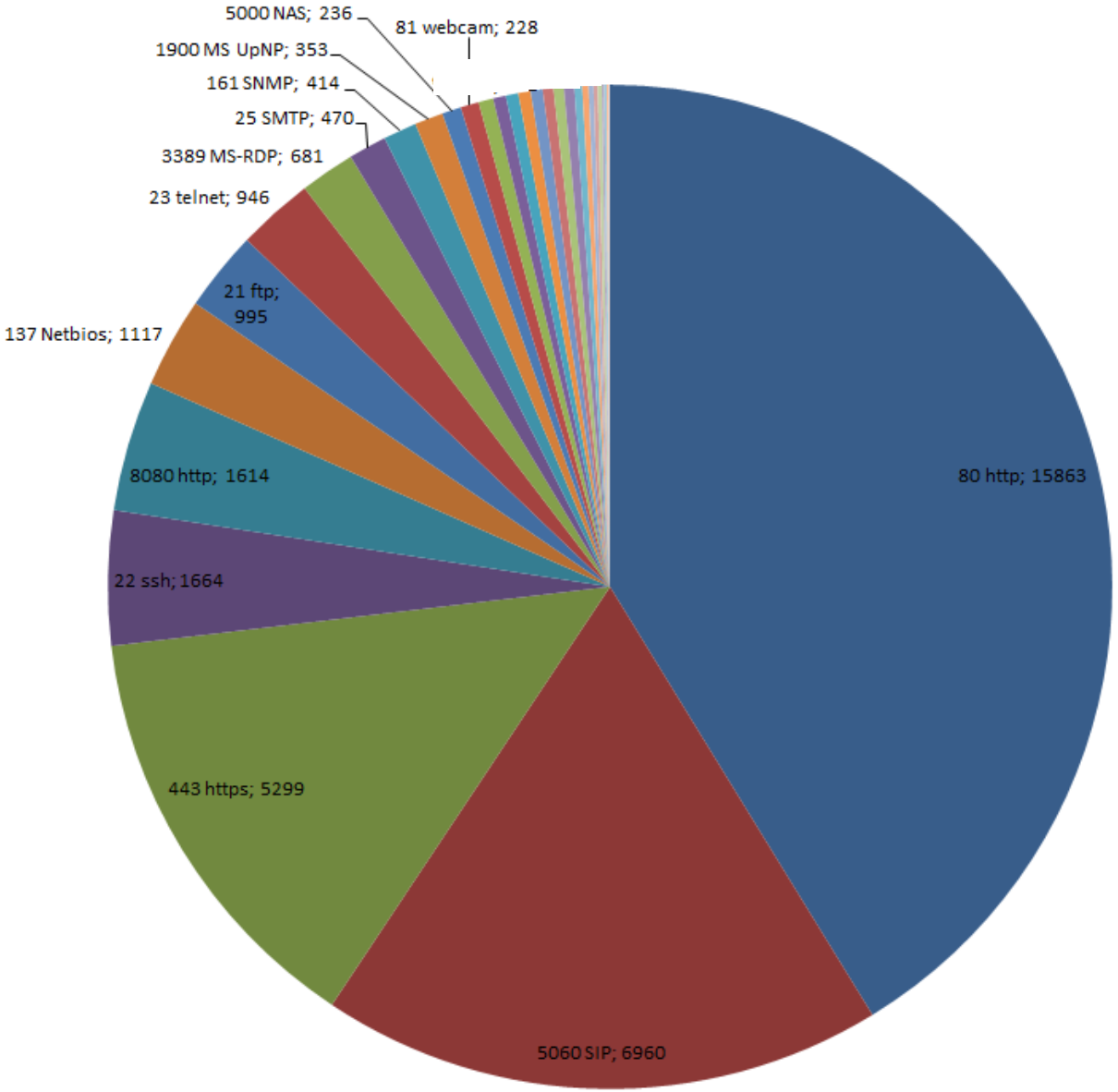
- 90 sites SEVESO
  - Nucléaire
  - Stockage de gaz
  - Raffineries
- 30000 entreprises industrielles
  - Chimie
  - Réseau routier
  - Pharmacie
  - Plasturgie
  - Aéronautique & défense
  - Smart Grid & Smart City
- Clusters et centres d'excellence : Aerospace, EDEN (Défense et sécurité), Axelera (chimie), Lyonbiopôle, Plastipolis
- Quelques PIV et beaucoup de PI *N* V

CYBERSÉCURITÉ CIBLES SÉCURITÉ EN RHÔNE-ALPES



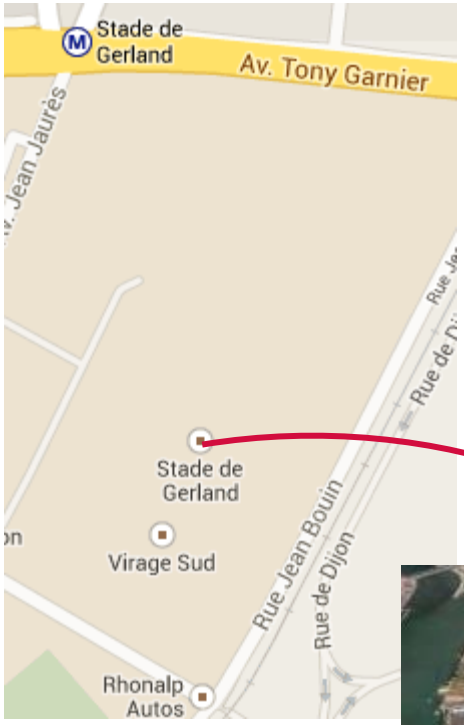


SHODAN « LYON »

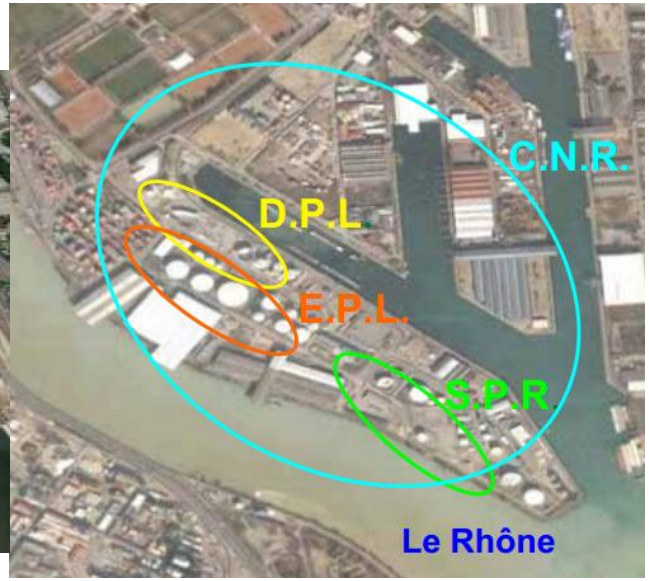


Port		Détail	Nb
	80	http	15863
★	5060	SIP	6960
	443	https	5299
	22	ssh	1664
	8080	http	1614
★	137	Netbios	1117
★	21	ftp	995
★	23	telnet	946
★	**3389**	**MS-RDP**	**681**
	25	SMTP	470
★	**161**	**SNMP**	**414**
	1900	MS UpNP	353
	5000	**NAS**	**236**
	81	webcam	228
	53	DSN	182
	110	pop3	157
★	**445**	**SBM/tcp**	**156**
	143	IMAP	153
★	**5432**	**PostgreSQL**	**148**
★	**3306**	**MySQL**	**131**
	993	IMAP SSL	129
	5353	Mcast DNS	127
	8443	https	97
	995	POP3 SSL	78
★	**5900**	**VNC**	**62**
★	**389**	**LDAP**	**51**
	123	NTP	49
★	**1434**	**MS-SQL**	**30**
	465	SMTP-SSL	30
★	**5632**	**PcAnywhere**	**22**
	7777	IPCamera	7
	8000	BarCode	6
	623	IMPI server r	4
	1023	Netopia	1

SCADA À LYON ?

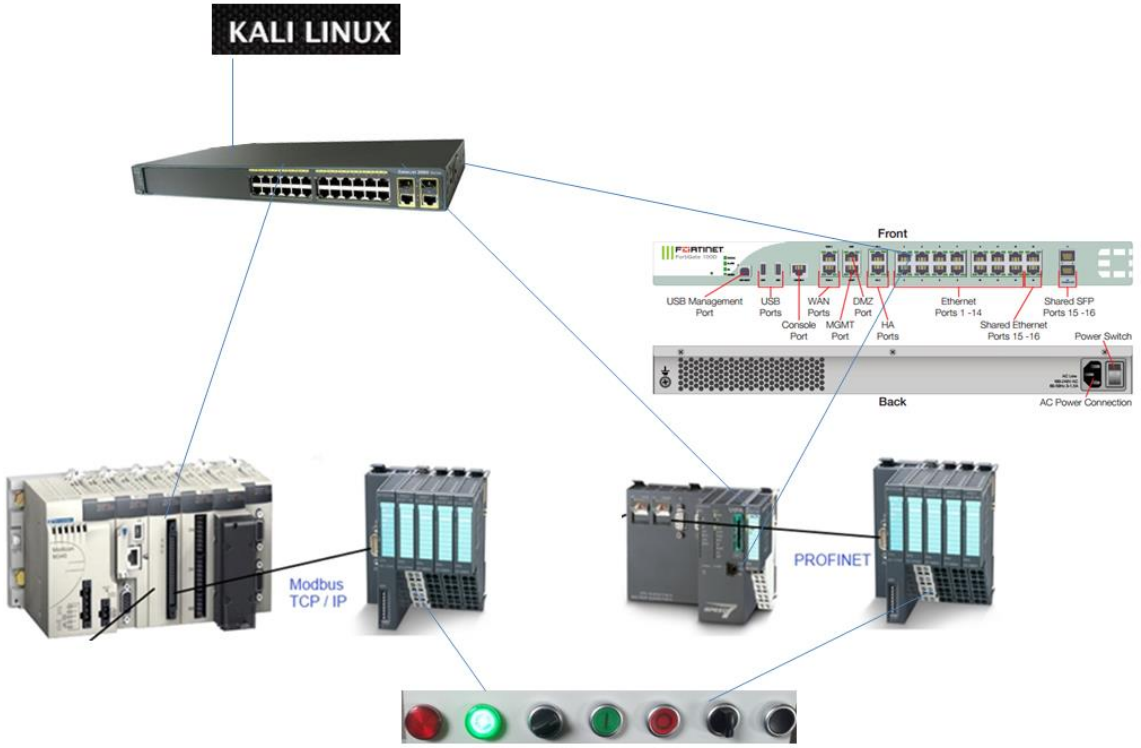


Dépôt pétrolier de Lyon
Entrepôts Pétroliers de Lyon
Stockage Pétrolier du Rhône



RAPIDE DÉMONSTRATION

- Simulation d'un malware (injecté par email ou clé USB) ou d'un pirate ayant accès à l'environnement contrôle commande.
- Simulation d'un hacker depuis Internet disposant de l'outil (téléchargeable) Unity



Cybersécurité industrielle

JUSQU'ICI, TOUT VA BIEN

LPM 2014-2019 : la loi instaure l'obligation de notification d'incidents affectant le fonctionnement ou la sécurité des systèmes d'information des opérateurs d'importance vitale.

PARANOÏA ?

Jihadist Cyber Terror Group to Target SCADA Systems

On June 11, 2011, a prominent Web Jihadist from the *Shumukh al-Islam* forum, *Yaman Mukhaddab*, launched a campaign to recruit male and female volunteers for a new Electronic Jihad group. The campaign, which takes place over the thread itself, begins with a clear definition of the group's tasks and priorities. *Mukhaddab* says:

> *Simply put, it is a cyber-terror base, for launching electronic terror attacks on major infidel powers, specifically the U.S., the U.K. and France, no others. This base is not going to attack, for instance, the sites of Shi'a, Christians, apostates, slanderers, liar sites and forums or anything else. I repeat: it will only target the U.S., the U.K. and France.*

Mukhaddab goes on to list the main targets for future attacks. SCADA systems are ranked as a top priority target, in order to "destroy power, water and gas supply lines, airports, railway stations, underground train stations, as well as central command and control systems" in these three countries. The second priority includes control systems of general financial sites, such as central savings organizations, stock markets and major banks. Third on the group's agenda are websites and databases of major corporations dominating the economies of these countries, while fourth and last are less specified "public sites affecting the daily routine of citizens, in order to maximize the terror effects on the population".

To date, close to a hundred volunteers have already signed on to *Mukhaddab*'s Electronic Jihad group. We have yet to see indications that this newly formed group has started to engage in online hacking activity, but given the enthusiasm it created among forum members, this is likely to occur in the near future.

PARANOÏA ? – ÇA N'ARRIVE (PAS) QU'AUX AUTRES !

Fri Jan 17, 2014 2:30

Israel Fires N. Researcher for Linking USB to Work Computer

An employee of Israel's Negev Nuclear Research Center is being sacked from his post after connecting a USB flash drive to a work computer – used for highly classified information – some 14 times, a disciplinary tribunal ruled.

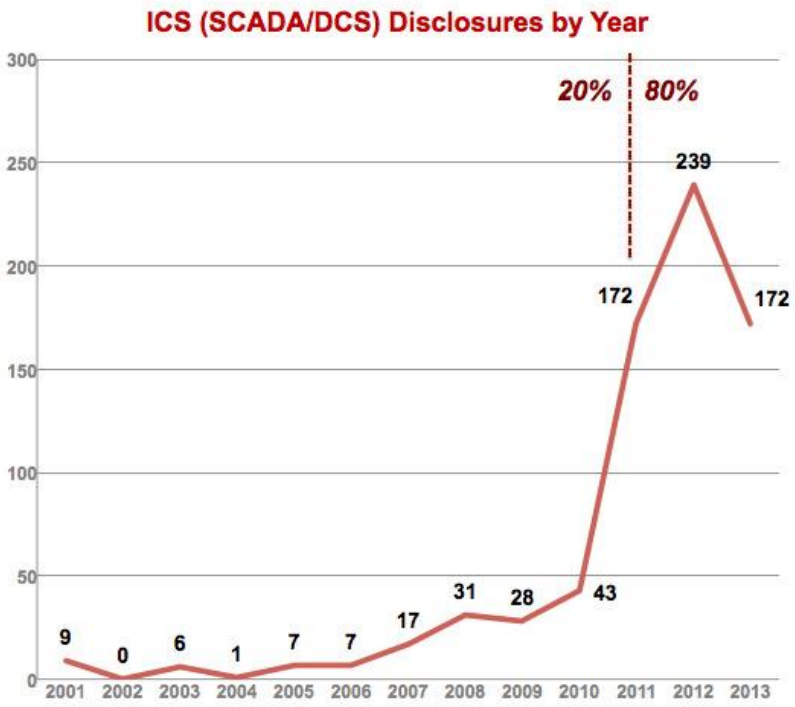
by Dennis Fisher

March 13, 2014 , 1:56 pm

A recent watering-hole attack targeted firms in the energy sector using a compromised site belonging to a law firm that works with energy companies and led victims to a separate site that used the LightsOut exploit kit to compromise their machines.

TOUT VA BIEN … JUSQU'À QUAND ?

(OU COMMENT RÉPONDRE À « ON N'A JAMAIS EU DE PROBLÈME JUSQU'À CE JOUR »)



Vulnerability Trend Data

BY YEAR	
2014	8
2013	172
2012	239
2011	172
2010	43
2009	28
2008	31
2007	17
2006	7
2005	7
2004	1
2003	6
2001	9
1983	1

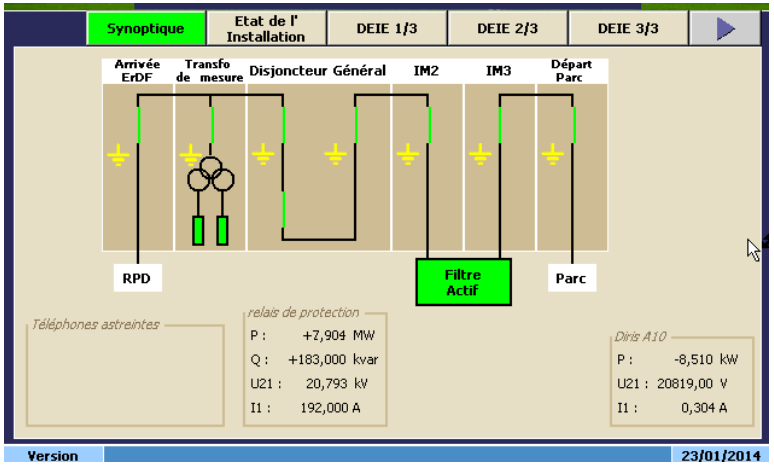
BY TYPE	
Other	251
Denial of Service (DoS)	155
Buffer Overflow	142
Code Execution	57
Cross-Site Scription (XSS)	31
Arbitrary File	31
SQL Database Injection	20
Information Disclosure	19
Privilege Escalation	16
Memory Corruption	13
Cross-Site Request Forgery	6

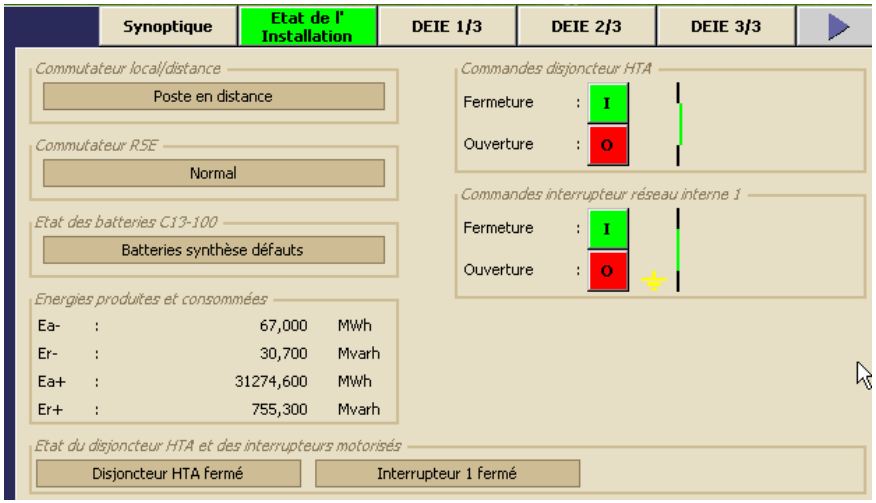
Last update: Feb. 1, 2014 (7:05UTC) - Open-Source Vulnerability Database (OSVDB)

Disc Date	Title
2014-03-20	Siemens SIMATIC S7-1200 CPU Random Number Generator Entropy Weakness Session Hijacking
2014-03-20	Siemens SIMATIC S7-1200 CPU Crafted PROFINET Traffic Handling Remote DoS
2014-03-20	Siemens SIMATIC S7-1200 CPU Crafted HTTPS Traffic Handling Remote DoS
2014-03-20	Siemens SIMATIC S7-1200 CPU Crafted HTTP Traffic Handling Remote DoS
2014-03-20	Siemens SIMATIC S7-1200 CPU Crafted TCP/IP Traffic Handling Remote DoS
2014-03-12	Siemens SIMATIC S7-1500 Controller Random Number Generator Session Hijacking Weakness
2014-03-12	Siemens SIMATIC S7-1500 Controller Crafted HTTPS Request Handling Remote DoS
2014-03-12	Siemens SIMATIC S7-1500 Controller Crafted HTTP Request Handling Remote DoS
2014-03-12	Siemens SIMATIC S7-1500 Controller Multiple Unspecified CSRF
2014-03-12	Siemens SIMATIC S7-1500 Controller Multiple Unspecified Reflected XSS
2014-03-12	Siemens SIMATIC S7-1500 Controller Multiple Unspecified HTTP Header Injection
2014-03-12	Siemens SIMATIC S7-1500 Controller Unspecified Open Redirect Weakness
2014-03-12	Siemens SIMATIC S7-1500 Controller Crafted Profinet Packet Handling Remote DoS
2014-03-12	Siemens SIMATIC S7-1500 Controller Crafted TCP/IP Packet Handling Remote DoS
2014-03-07	Yokogawa CENTUM CS 3000 BKBCopyD.exe Crafted Packet Handling Remote Stack Buffer Overflow
2014-03-07	Yokogawa CENTUM CS 3000 BKCLogSvr.exe Crafted Packet Sequence Handling Remote Heap Buffer Overflow
2014-03-07	Yokogawa CENTUM CS 3000 BKHOdeq.exe Crafted Packet Handling Remote Stack Buffer Overflow
2014-02-20	ICONICS GENESIS32 ActiveX Control Unspecified Insecure Method Arbitrary Code Execution
2014-02-18	RuggedCom Rugged Operating System (ROS) SNMP Packet Handling Unspecified Remote DoS
2014-02-14	CenturyStar ActiveX (CamW2000.dll) SetMyAddress Function Crafted Argument Handling Stack Buffer Overflow
2014-02-11	MatrikonOPC SCADA DNP3 OPC Server Malformed DNP3 Packet Handling Infinite Loop Remote DoS
2014-02-07	CenturyStar ActiveX (CamW2000.dll) SetMyAddress Function Argument Handling Buffer Overflow
2014-02-07	Microsys PROMOTIC ActiveX (PmTrends.dll) Start Method NULL Pointer Dereference DoS Weakness
2014-02-04	Rockwell Automation RSLogix 5000 Unspecified Customer-defined Password Compromise
2014-02-03	Siemens SIMATIC WinCC OA Project User Password Hash Remote Disclosure
2014-02-03	Siemens SIMATIC WinCC OA Crafted Packet Handling Unspecified Remote Code Execution
2014-02-03	Siemens SIMATIC WinCC OA Unspecified Traversal Remote File Access
2014-02-03	Siemens SIMATIC WinCC OA Malformed HTTP Packet Handling Remote DoS
2014-01-31	Schneider Electric OPC Factory Server (OFS) Test Client Configuration File Parsing Buffer Overflow
2014-01-30	Schneider Electric Telvent SAGE 3030 RTU DNP3 Driver IP-Based Crafted Packet Handling Remote DoS
2014-01-30	3S CoDeSys Runtime Toolkit Unspecified NULL Pointer Dereference Remote DoS
2014-01-24	Schneider Electric Multiple Products Citect.Platform.Transport.dll Multiple Functions Unhandled InvalidDataException Remote DoS
2014-01-24	Schneider Electric SCADA Expert / ClearSCADA PLC Driver ServerMain.exe Project File (PDF) Handling Multiple Buffer Overflows
2014-01-15	Schneider Electric Floating License Manager Unspecified Service Unquoted Service Path Local Privilege Escalation
2014-01-15	Ecava IntegraXor Unspecified Arbitrary DLL Handling Remote Buffer Overflow DoS
2014-01-14	WellinTech Multiple Product kxClientDownload.ocx ActiveX ProjectURL Property Arbitrary DLL Injection Code Execution
2014-01-14	WellinTech Multiple Product KAEClientManager Console Remote Authentication Credential Disclosure
2014-01-07	Sierra Wireless AirLink Raven X EV-DO Plaintext Credential Remote Disclosure

MULTIPLES PLATEFORMES EXPOSÉES

- Sofrel
- Passerelle IP – modbus
- VNC Siemens
- S7-300
- Hirschmann
- Schneider
- Yokogawa





- Siemens Scalance
- Exemple digi ... préoccupant

Entering the user name and password

You will be prompted to enter the user name and the password. The factory setting is as follows:

User name: admin (cannot be modified)
Password: scalance

Digi One SP Configuration and Management

Home
Configuration
Network
Serial Port
Security
System
Management
Serial Ports
Connections
Administration
Backup/Restore
Update Firmware
Factory Default Settings
Device Information
Reboot
Logout

Session Management

Active Network Connections

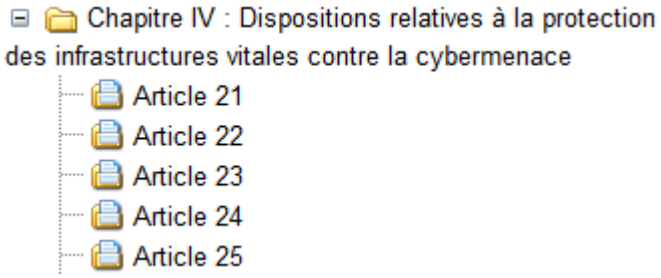
TTY	Username	Connected From	O...	IP Address	Network Name	Owner Name	Country
1	None	81.252.208.189	1	81.252.208.189	FR-VIVALE	Interconnection with RAEI backbone	France
2	None	213.85.186.114	2	213.85.186.114	Home-Mytishi	Russian Central Telegraph, Moscow	Russian Feder...
3	None	86.10.201.24	3	86.10.201.24	NTL	NTL Infrastructure - Leeds	United Kingd...
4	None	86.10.201.24	4	2.50.21.242	ETISALATADSL-EMIRNET	Emirates Telecommunications Corporation	United Arab E...
5	None	86.10.201.24	5	91.202.240.208	SC-VEKTOR-NET	Komertsiyno Virobnitcha Firma "VEKTOR"	Ukraine
6	None	2.50.21.242	6	202.159.194....	MTNL-ISP	MTNL INTERNET SERVICE PROVIDER IN THE CITY OF DELHI AND MUMBAI	India
7	None	70.113.8.2	7	151.217.31.249	EU-ZZ-151	RIPE NCC	EU # Country ...
8	None	24.175.221.119	8	62.195.159.184	UPC-NL	CPE Customers NL	Netherlands
9	None	91.202.240.208	9	187.178.74.220	MX-ARWI-LACNIC	Axtel - Recursos WiMAX	Mexico
10	None	202.159.194.131	1	37.8.53.227	HBSAGAZA	Hadara Gaza BSA	Palestinian Te...
11	None	151.217.31.249	1	112.214.22.131	CNM-KR	C&M Communication Co.,Ltd.	Korea, Republ...
12	None	62.195.159.184					
13	None	187.178.74.220	Logging In	0	Disconnect...		
14	None	37.8.53.227	Logging In	0	Disconnect...		
15	None	112.214.22.131	Logging In	0	Disconnect...		

BILAN 2010 - 2013

- Attaques ciblées sectorielles, mais … uniquement aux Etats Unis (?)
- Rebond à partir d'attaques « IT » vers des composants industriels
- Maladresses à répétition et infection de systèmes industriels
- Malversation, terrorisme ciblé sur les infrastructures vitales ?
- PRISM et les infrastructures critiques ?
- Prise de conscience ?
- Résultats des audits menés par LEXSI préoccupants.

LPM – OIV – OI *N* V - ANSSI

- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale
- Chapitre III – article 20 : Accès administratif aux données de connexion
- Chapitre IV



- Promulgation en décembre
- Groupe de travail de l'ANSSI en 2013, publication des outils en janvier 2014

LPM ET OIV : CONCRÈTEMENT

- Loi votée
- Déclinaison en 2014 => méthode d'accompagnement LEXSI
  - Mode projet, approche pluriannuelle modeste et pragmatique
  - Convergence sûreté / sécurité : informaticiens et automaticiens, **ensemble**
  - Audits maitrisés (pentest « de base » sans intérêt)
  - Formations et sensibilisations
- Chantiers ANSSI – labellisation produits et prestataires
- Applicabilité de la LPM et Audits en 2015 ?

Méthode de classification
et
mesures principales

Mesures détaillées

LEXSI

OI N V

solitude
nom féminin
(latin *solitudo*)

Définitions | Synonymes | Citations

- État de quelqu'un qui est seul momentanément ou habituellement : *Profiter d'un instant de solitude pour réfléchir. Aimer la solitude.*
- État de quelqu'un qui est psychologiquement seul : *Solitude morale.*
- Caractère d'un lieu où l'on se sent seul, isolé : *La solitude des forêts.*

pragmatisme
nom masculin
(allemand *Pragmatismus*, du grec *pragmatikos*, qui concerne l'action)

- Attitude de quelqu'un qui s'adapte à toute situation, qui est orienté vers l'action pratique.

débrouillardise
nom féminin

Définitions | Synonymes

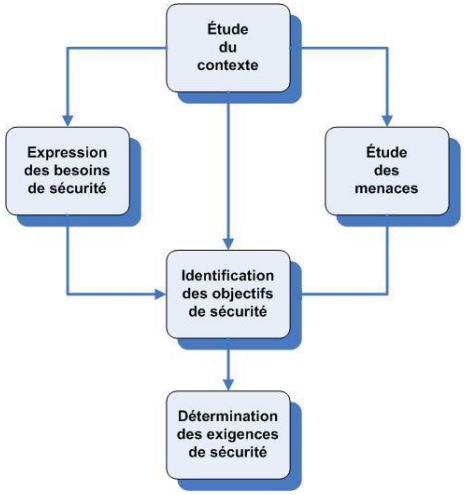
- Familier. Aptitude à se débrouiller.

ORGANISATIONNEL

Convergence sûreté - cybersécurité

ANSSI

- Classe 1/2/3
- Mesures organisationnelles et techniques
- Analyse de risque EBIOS



ISO 2700x

- ISO 27002 (mesures de sécurité IT)
- ISO 27005 (analyse de risques)

CEI-62443 & normes spécifiques

- Modélisation d'un site industriel avec mise en évidence de zones et conduits
- Normes sectorielles (eau, énergie, nucléaire, transports …)

LEXSI

ORGANISATIONNEL - SIMPLIFIÉ

- Sponsoriser et organiser la gouvernance sûreté + sécurité
- Prioriser : approche risk management
- Sensibiliser, former : populations IT et industrielle
- Maitriser au travers de standards de sécurité « quick-win » :
  - Inventaire
  - Accès distants
  - Prestataires et responsables maintenance
  - Durcissement
  - Cloisonnement
- Détecter, anticiper, réagir
  - Veille pastebin, veille Shodan
  - Sondes
  - Audits

SOLUTIONS TECHNIQUES

- Une fois le diagnostic posé
- Une fois le sponsoring identifié
- Une fois les équipes formées et sensibilisées
- Une fois le cadre de gouvernance sûreté – sécurité en place

SOLUTIONS – (« LABELLISABLES ? »)

INDUSTRIAL DEFENDER®

LOCKHEED MARTIN

HIRSCHMANN
A BELDEN BRAND

TOFINO™

Tofino Security Appliance
Zone Level Security for your control network.

Loadable Security Modules
Firmware modules that customize the security features on Tofino Security Appliances.

Tofino Central Management Platform
Configure and manage security for your entire control network from one place.

USB MALWARE CLEANER

LEXSI
INNOVATIVE SECURITY FOR BUSINESS

Sas de décontamination de périphériques USB

http://vimeo.com/80463870

WATERFALL®
One Way to Connect

ARKOON + NETASQ

StormShield
ENDPOINT SECURITY

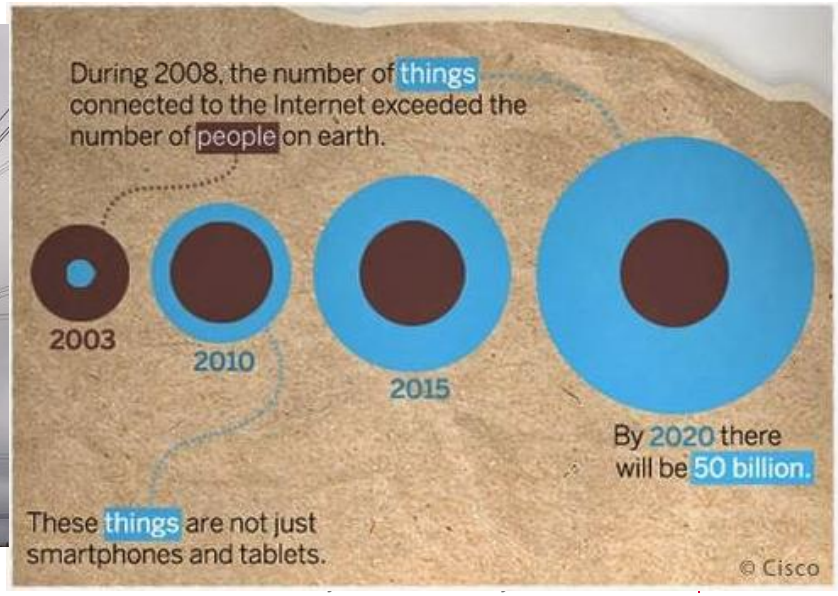
LEXSI

DEMAIN

« Scada BYOD »
Bring Your Own Disaster / Destruction

Smart Grid / Smart Cities …
Smart … peut être, sécurisé ?

Internet of everything …
Hacking everything on the Internet !



LEXSI

SMART SCADA

CONVERGENCE SÉCURITÉ IT & SÛRETÉ SYSTÈMES INDUSTRIELS

Cybersécurité SCADA

Machine to Machine

Internet of Things

Contrôle Commande

- EXPERTISES
- AUDITS & TESTS
- VEILLES CIBLÉES
- FORMATIONS

INNOVATIVE SECURITY

Pour vous aider à maîtriser vos risques

SIEGE SOCIAL

Tour Mercuriale Ponant
40 rue Jean Jaurès
93170 Bagnolet
Tél. (+33) 1 55 86 88 88

Thomas HOUDY

Manager Innovation & Stratégie
thoudy@lexsi.com

www.lexsi.com