Club de la sécurité de l'information français

Conférence CLUSIF

SI Industriels en 2017 :
Incidents, enjeux et… parades

Club de la sécurité de l'information français

CLUSIF

Le SI Industriel, Panorama des cyber-menaces et stratégie de réponse

Faiz Djellouli
Head of CITI Cybersecurity Services / CISO
ENGIE – Global Business Consulting

Sommaire

- Cybersécurité et Cyber-Menaces
- Une menace bien réelle…
- Quelles approches à préconiser ?
- REX d'un Centre de compétences interne

Club de la sécurité de l'information français

CLUSIF

Cybersécurité et Cyber-Menaces

Qu'est-ce que la cybersécurité ?

DISPONIBILITE

Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

INTEGRITE

Empêcher les altérations, suppressions ou ajouts d'informations non autorisées

CONFIDENTIALITE

Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

TRACABILITE

Garder les traces des accès, actions ou échanges réalisés, afin d'assurer la possibilité d'un contrôle systématique ou a posteriori, d'apporter des preuves

La **cybersécurité** consiste à préserver la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT) des informations et des systèmes physiques/logiques sous-jacents

La confiance est indispensable à la Digitalisation

Contexte et Enjeux

- **Le risque Cybersecurité** (IT&OT) est souvent classé dans le **TOP10 des risques des Groupes Industriels et tertiaires français.**
- Dans le contexte de digitalisation, la **Cybersecurité** est d'autant plus nécessaire pour atteindre la **confiance numérique**.
- De plus, le risque **Cybersécurité des SCI (Systèmes de Contrôle Industriels)** devient **un sujet d'intérêt majeur** dans l'Industrie.

Approche observée

- La Cybersécurité doit bénéficier d'un **engagement Corporate** à travers toutes ses entités afin d'addresser à la fois IT et OT.
- Cependant, la Cybersécurité des ICS doit prendre en compte les **spécificités du monde industriel** et ses contraintes.
- Les **ressources** compétentes en Cybersécurité sont **rares** et plus spécifiquement sur les ICS. Des **centres de compétences** doivent émerger pour partager les bonnes et **accompagner** ses entités dans leurs démarches de sécurisation.

Des différences de contexte entre SI et SCI

Systèmes d'Information traditionnels	Critères	Systèmes de Contrôle Industriels
Confidentialité > **Intégrité** > Disponibilité	Priorité pour la sécurité	**Disponibilité** > **Intégrité** > Confidentialité
Fonctionnel durant les heures de bureaux (Le reboot est acceptable)	Disponibilité	Fonctionnement stable **24x365** (Aucun reboot autorisé)
Impacts financiers (espionnage industriel, vol de données, fraude) et d'image	Conséquence d'un incident	Dommages aux personnes ou à l'environnement, interruption de la continuité de service, détérioration des équipements
3-5 ans	Durée de vie	**10 - 20 ans**
Moins d'impacte pour **un retard de réponse (délai)**	Vitesse de traitement des données	**Réponses en temps réels**
Souvent et régulier	Cycle pour la gestion et l'application des patchs	**Irrégulier** dépends de chaque fournisseur ICS, **Assez long terme** (un tous les 1~4 ans)
Département de sécurité informatique	Gestion opérationnelle des équipements et de la sécurité	**Service technique terrain**
Sécurisation des postes via de **nombreux outils** : antivirus, firewalls, IPS, etc.	Standard de sécurité	**Problèmes de compatibilité** des applications avec les antivirus, firewalls, IPS, etc.

Les cyber-attaques en 2015

+ de 64K

- C'est le nombre d'incidents de cyber-sécurité
- Dans **82 pays, c**oncernant différentes sociétés

- **3 min 40''**
  - C'est le temps nécessaire pour obtenir le **premier clic** sur une **pièce-jointe** ou URL malveillante dans le cadre d'une tentative de **phishing**
- **1 minute**
  - Dans **93%** des cas, il faut **moins d'une minute** pour que les **premières compromissions d'une fuite de données** apparaissent

Moyen de locomotion #1 des malware

- La **pièce-jointe** d'email est le **1er moyen de transmission de malware**

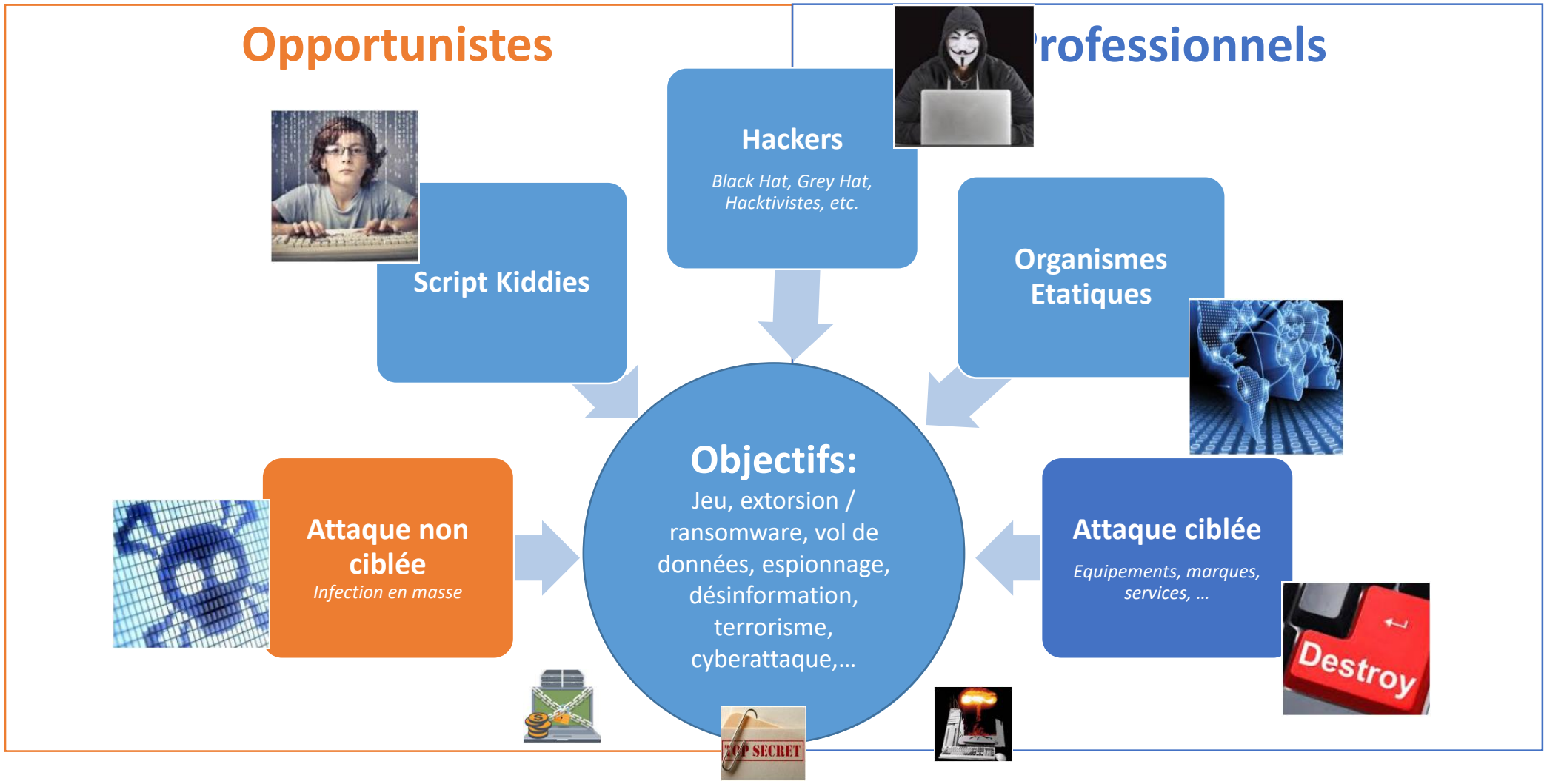
Seulement **10 vulnerabilités** représentent **85% des exploitations réussies**

50% des exploitations d'une vulnérabilité donnée apparaissent entre 10 et 100 jours après la publication des vulnérabilités

63% des fuites de donnée ont impliqué des **mot-de-passe faibles**, par défaut ou subtilisés

37% des fuites de données sont attribuées à des **attaquants internes** et les exploitants et mainteneurs

Attaquants : qui sont-ils ? A qui s'en prennent-ils ? Que veulent-ils ?

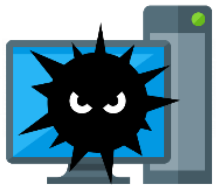


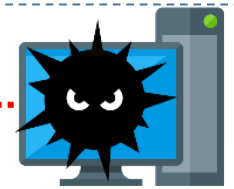
Des attaques de plus en plus sophistiquées

2. Primo Infection
Exploitation de vulnérabilité : PDF
(dissimulation)

3. Social Engineering
Le hacker envoie une facture factice au service
Comptabilité

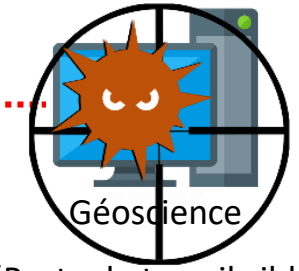
4. Propagation
Vol de compte
/ périphérique amovible


Compatibilité


Ventes


Direction


Logistique


Géoscience
(Poste de travail cible)

1. Création du malware
Ciblant une technologie précise
(du poste cible)

5. Voler ou Détruire
Exfiltration de données sensibles
ou Chiffrement de données

CLUSIF

Une menace bien réelle…

Des 1er signaux de cyber-attaques sur les SCI

L.A. NOW

SOUTHERN CALIFORNIA -- THIS JUST IN

Engineers who hacked into L.A. traffic signal computer, jamming streets, sentenced

December 1, 2009 | 7:17 am

Two L.A. traffic engineers who pleaded guilty to hacking into the city's signal system and slowing traffic at key intersections as part of a labor protest have been sentenced to two years' probation.

Authorities said that Gabriel Murillo, 40, and Kartik Patel, 37, hacked into the system in 2006 despite the city's efforts to block access during a labor action.

Fearful that the strikers could wreak havoc, the city temporarily blocked all engineers from access to the computer that controls traffic signals.

But authorities said Patel and Murillo found a way in and picked their targets with care -- intersections they knew would cause significant backups because they were close to freeways and major destinations.

The engineers programmed the signals so that red lights for several days starting Aug. 21, 2006 would be extremely long on the most congested approaches to the intersections, causing gridlock. Cars backed up at Los Angeles International Airport, at a key intersection in Studio City, at access onto the clogged Glendale Freeway and throughout the streets of Little Tokyo and the L.A. Civic Center area, sources told The Times at the time. No accidents occurred as a result.

As part of their plea deal, the engineers agreed to pay $6,250 in restitution and completed 240 hours of community service.

-- Sholby Grad

Deux employés mécontents ont désactivé les feux de signalisation, causant une saturation complète du centre-ville de Los Angeles [sabotage interne]

Un adolescent a transformé une télécommande de télévision en un boîtier capable d'envoyer des signaux au système de gestion du trafic des tramways en Pologne (protocole de communication ancien et non sécurisé).

The Telegraph

Home News World Sport Finance Comment Culture Travel

USA Asia China Europe Middle East Australasia Africa Nels

HOME » NEWS » WORLD NEWS

Schoolboy hacks into city's tram system

The boy, described as a 'genius'and some of the equipment he used

By Graeme Baker

12:01AM GMT 11 Jan 2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

…Mais néanmoins, avant 2010, le sujet des attaques sur les SCI était « impossible » à évoquer, jusqu'à…

… jusqu'au cas STUXnet en 2010…

Mail Online

Computer super-virus 'targeted Iranian nuclear power station' but who made it?

By NIALL FIRTH FOR MAILONLINE
UPDATED: 01:14 GMT, 24 September 2010

BBC Sign in | News | Sport | Weather | Shop | Earth | Travel | Mc

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

Stuxnet worm hits Iran nuclear plant staff computers

Stuxnet est un virus découvert en 2010 qui :

- ***A ciblé*** *les centrales nucléaires iraniennes d'enrichissement d'uranium, entraînant un arrêt de la production*
- *Touche les* ***équipements Siemens*** *: automates et IHM (avec les logiciels WinCC Simatic et Step 7) entraînant une reprogrammation partielle de ces automates*
- ***Plusieurs vulnérabilités*** *exploitées sur le seul cas Stuxnet*
  - *Infection via les ports USB*
  - *Elévation de privilèges*
  - *Exploitation de vulnérabilités critiques affectant Windows*
- *Stuxnet a démontré la faisabilité d'une* ***attaque ciblée et très sophistiquée***

D'autres cas depuis…

theguardian

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company

Smokestacks in Dniprodzerzhynsk, Ukraine. Photograph: John Mcconnico/AP

A power blackout in Ukraine over Christmas and a destructive cyberattack on a major Ukrainian media company were caused by the same malware from the same major hacking group, known as Sandworm, according to security researchers at Symantec.

80,000 to 1.4 million de personnes impactées. 6 heures – blackout.

L'attaque a débutée par du "Social Engineering" : fichier Excel infecté en pièce jointe d'un mail
Le malware s'est propagé sur le réseau permettant ainsi de prendre contrôle et d'arrêter la centrale, causant un blackout.

Les hackers ont utilisés des emails et le "social engineering" pour s'infiltrer et prendre contrôle de la chaîne de production de métal…

Dommages directs évalués à 10-20 M€ alors que le coût d'une acierie est de l'ordre de 100 M€.

BBC NEWS TECHNOLOGY

22 December 2014 Last updated at 13:01 GMT

Share

Hack attack causes 'massive damage' at steel works

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

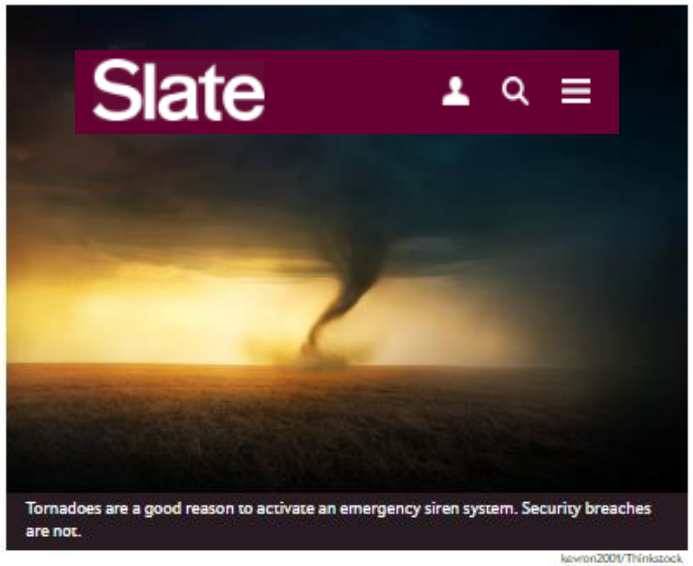
A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI).

It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.

Ainsi que des défis lancés aux initiatives de type « digitale »

*Deux chercheurs ont prouvé l'extrême vulnérabilité des compteurs intelligents espagnols de « M**** and M**** » qui équipent ENDESA. Risques de Black-Out, Usurpation, fraude, malveillance ciblée sur un compteur donné …*



Many computer security breaches are designed to stay under the radar, so they remain undetected and unmitigated for as long as possible. But every once and a while we see a breach that is meant to draw as much attention and wreak as much havoc as possible. If ever a security breach was designed to be difficult to ignore, it was the one that was exploited in Dallas last week to set off 156 emergency sirens—typically used to warn residents about tornadoes and other serious weather events—for more than an hour and a half on Friday night and into early Saturday morning, until the city finally unplugged and shut off the entire alert system.

*L'attaque **aurait** été facilitée par la présence de faiblesses introduites par **l'intégration mal maîtrisée du « digital » dans les SI Industriels** contrôlant les sirènes (interconnexions multiples, accès internet …)*

156 sirènes d'alarme se sont mises à sonner à plein volume entre 23h et 1h du matin, déclenchant panique et nuisances.

Eteindre l'électricité chez son voisin, envoyer des faux rapports de consommation, provoquer une panne générale… Certains compteurs intelligents sont facilement piratables, comme viennent de le montrer deux chercheurs en sécurité.

La belle promesse des « smarts cities » - ou villes intelligentes - ne serait-elle qu'une illusion? A l'occasion de la conférence Black Hat Europe 2014, deux hackers espagnols ont montré que l'interconnexion des infrastructures urbaines cachent aussi d'énormes risques. Javier Vazquez Vidal et Alberto

CLUSIF

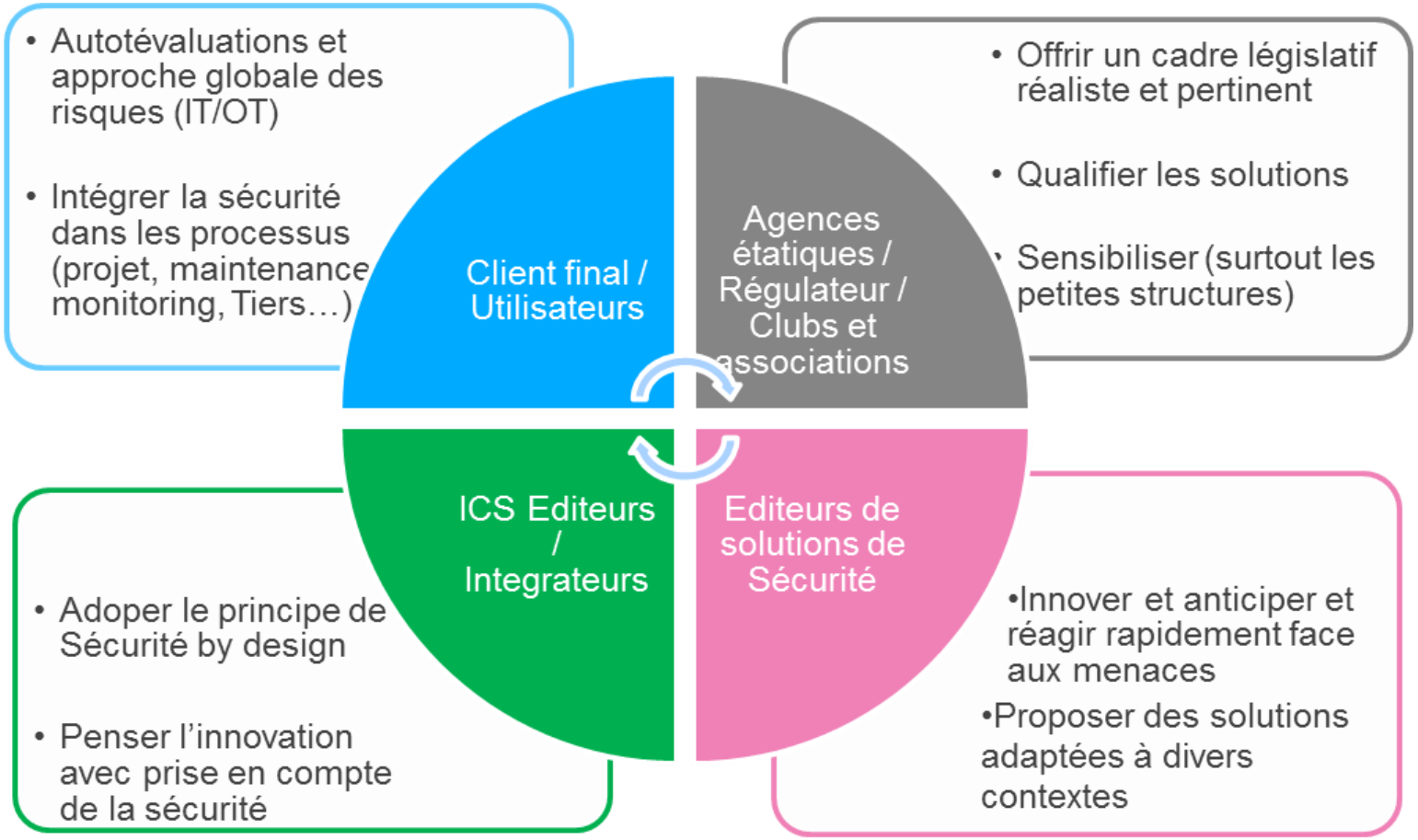
Quelles approches préconiser ?

1 - Se doter d'une Stratégie Cybersécurité

- Débute par une prise de conscience au plus haut niveau de l'entreprise, suivie d'une mise en œuvre d'une gouvernance spécifique prenant le sujet dans sa globalité (IT&OT)

- Identifier et organiser les fonctions importantes de manière inclusive et transverse

2 - Penser la Cybersécurité dans un ensemble d'acteurs inter-dépendants



3 - Réaliser des diagnostics approfondis « Security Expedition » et proposer des solutions qualifiées :

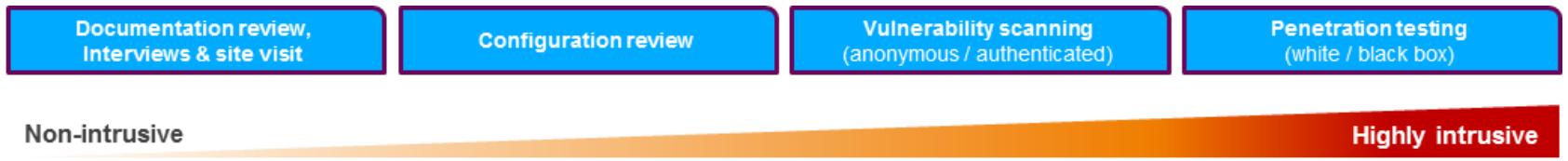
Définition et objectifs

- Réaliser un audit 360° de cybersécurité des sites industriels, selon plusieurs axes (techniques, organisationnel, humain) incluant un gap analysis avec la politique en vigueur
- Proposer et implémenter des solutions adaptées au regard des risques évalués (quickwins, solutions du catalogue de service, sensibilisation, bonnes pratiques, etc.)

Approche

- Double approche Risques / Conformité afin de couvrir la problématique sous divers angles :

- Approche progressive :

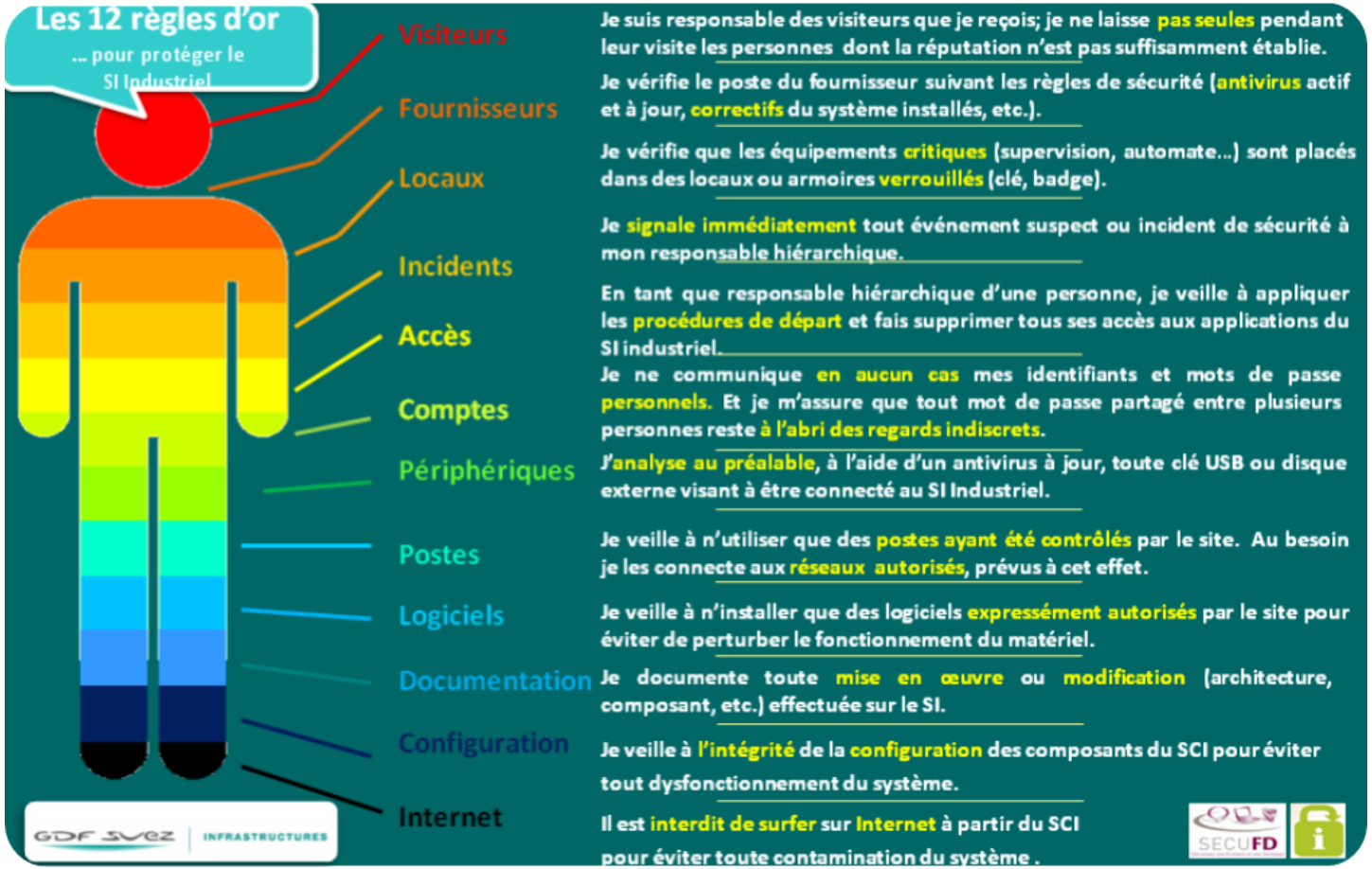


Secure Expedition Service Catalog :

- Administration Bastion
- ICS USB/PC Protection
- Whitelisting/hardening
- Awareness materials
- Industrial probes
- Supervision
- Generic procedures
- ...

4 - Sensibiliser le personnel intervenant sur les ICS

- Les 12 règles d'or SCI visent à sécuriser le comportement du personnel travaillant sur les systèmes de contrôle industriels.
- Réaliser des démonstrations de hacking pour marquer les esprits
- Des tests (ex. **de Social Engineering**) permettent d'évaluer la bonne application de certaines règles.



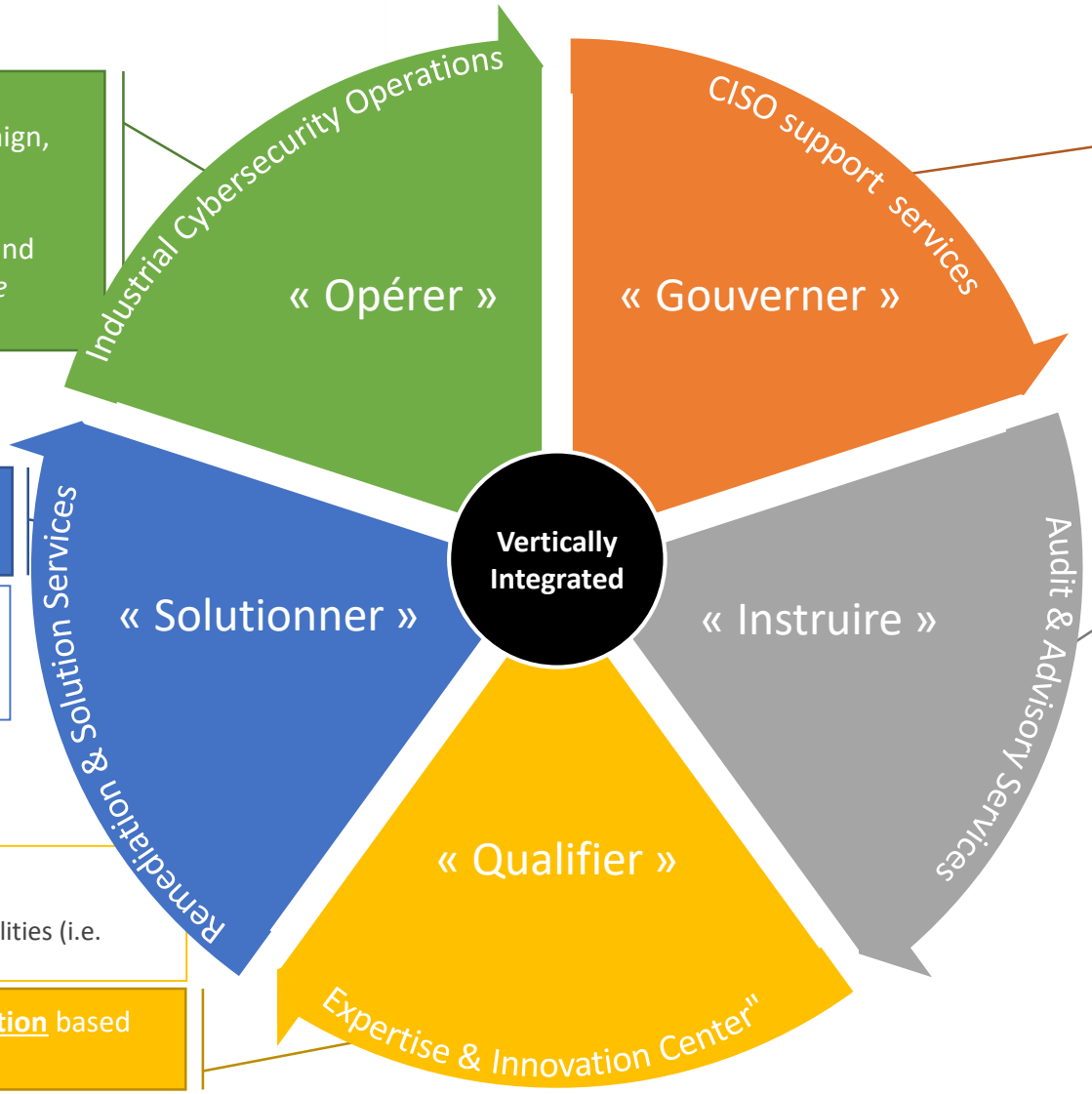
CLUSIF

REX d'un Centre de compétences interne

CITI Cybersecurity Services

5 piliers pour une maîtrise de la chaine de valeur Cybersécurité

- **CISO Back-office operations & Controls:** authorization management, IAM review campaign, security watch, etc.
- **Solutions maintenance**
- **Industrial CSIRT** (incident management, alert and vulnerability treatment, forensics, etc.), *in close coordination with Corp. Global SOC*



CISO support services for small and medium operational entities needing cybersecurity governance and management

- Contribution to the Group Security Governance (Group Security Program, Policies, Best practices …)
- CISO Run and Project activities

Security Expeditions that can include **cybersecurity audits**, **pentests**, **risk analysis**, framework/standard **compliancy gap analysis** (ICS Framework, LPM), **advisory**, remediation plan **recommendation**, and also **solution quick-win implementation**

- Methodology Development
- Identify cybersecurity and business process features depending on plant typology and market technologies
- Regulatory watch and gap analysis between referential

Solutions packaging
Solutions implementation

- Cybersecurity solution and tools packaging and standardization (with business models)
- Implementation project

- Cybersecurity watch activity
- Tests bench, POC incubator and Sand Box
- Cartography of unaddressed Cybersecurity functionalities (i.e. remediation needs)

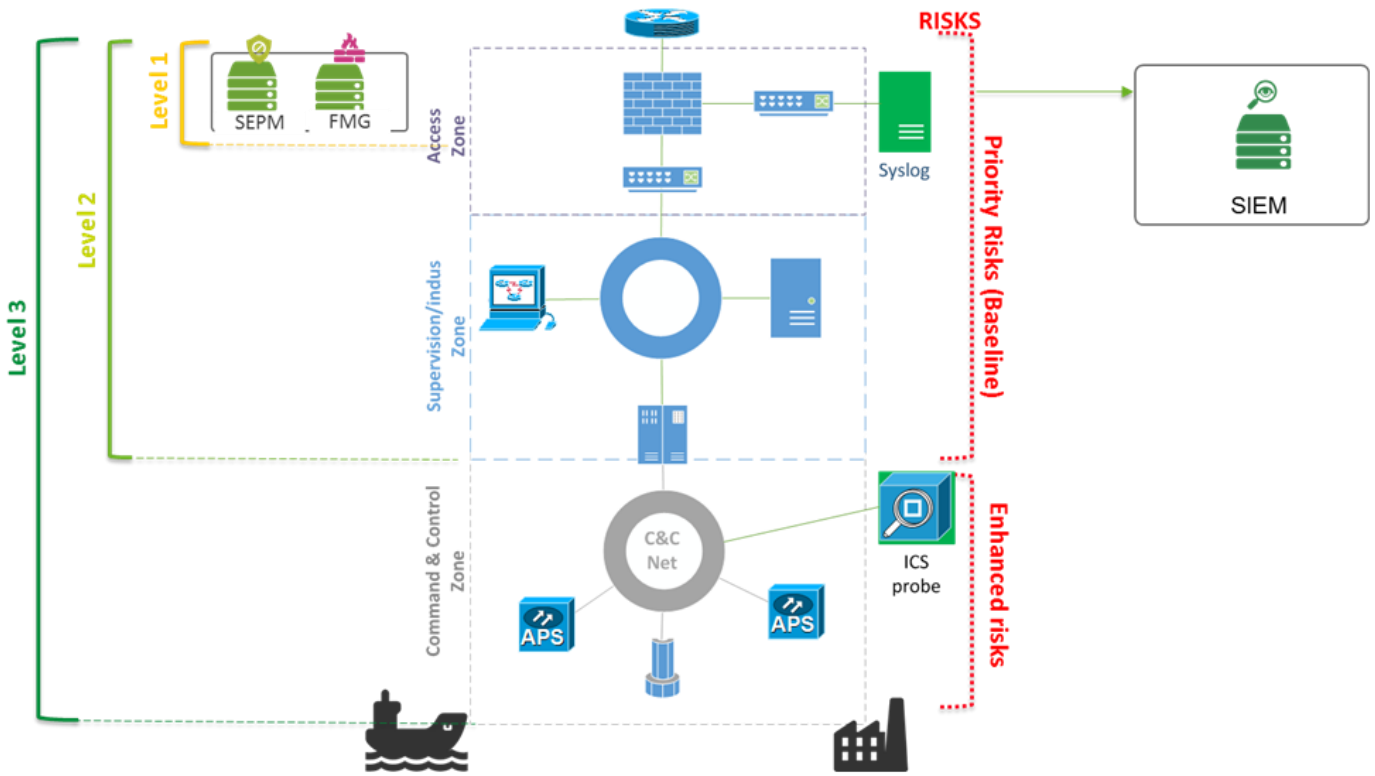
Solutions and methodology study and certification based on tangible and operational needs

Exemple 1 : Tester les solutions supposées être sécurisées mais ne disposant pas de certification sécurité

- Peripheral capable of transmission or reception of radio signals + 2.4Ghz antenna : **HackRF** used.
- Open source software

#	vulnérabilité	Risque	Priorité	Description
V-01	Attaque par rejeu possible	Elevé	★★★☆	Un attaquant peut rejouer les trames capturées. L'id d'incrémentation présent dans la trame n'est pas vérifié côté serveur.
V-02	Prise en compte des messages non chiffrés	Elevé	★★☆☆	Une trame non chiffrée envoyée par un capteur censé chiffrer ses messages est correctement interprété et traité côté serveur.
V-03	Prise en compte des messages d'un capteur non enregistré	Elevé	★★★★	Une trame provenant d'un capteur non référencé est prise en compte. L'id du capteur présent dans la trame n'est pas vérifié côté serveur.

Exemple 2 (1/2) : Mettre en œuvre une supervision du SI Industriel – *Quel niveau choisir ?*



La Baseline a été définie sur la base du rejeu des Cyber-attaques « **Ukraine** » et « **German Steelworks** » * avec la préconisation pour cette baseline d'être en mesure de détecter l'attaque suffisamment tôt pour réagir et protéger les actifs industriels.

(modèle générique, délicat à mettre en œuvre et pas toujours réalisable en l'état)

Phases des attaques :

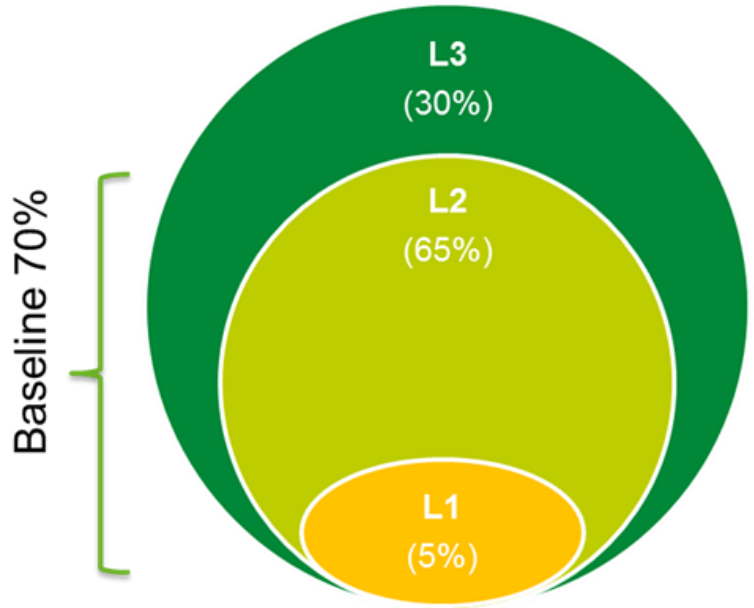
- ciblage fishing **L1****
- vol d'identifiants **L1****
- découverte (netsat…) **L2**
- mouvement latéral (SSH, RDP…) **L2**
- Exécution de l'attaque (écriture sur automates) **L3**
- Destruction de preuves **L2**

* https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf & https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

** : détection possible en amont du L1 si corrélation des postes et réseau bureautique et des accès internet

Exemple 2 (1/2) : Mettre en œuvre une supervision du SI Industriel – *Quelles menaces peut-on couvrir ?*

Use case repartition by connection level



Detailed threat use case repartition by **Level** & by **Impact**

Top 10 RISKS	GSOC connection level	Impact 0	Impact 1	Impact 2	Impact 3	TOTAL
R2.ICS cyber attack (direct)	***Level 1***	0	0	0	0	**0**
	Level 2	0	4	2	17	**23**
	Level 3	0	1	3	9	**13**
R3.ICS impacted IT cyber attack (indirect)	***Level 1***	0	0	1	1	**2**
	Level 2	1	3	0	2	**6**
	Level 3	0	0	0	0	**0**
TOTAL		**1**	**8**	**6**	**29**	**44**

Exemple 3 : Infrastructure centralisée d'administration des sites industriels

Usual unsecured remote access

Secured remote access through Admin Bastion

Industrial sites

Industrial Control System
(SCADA, Command-control)

Security appliance
(Antivirus managers, FW manager, etc.)

ICS Network assets
(switches, firewall)

Administration Bastion

Mainly generic account

Administrators and external third-party with privileged access

1. Personal credentials

5. Target devices credential mgt
6. Protocol intermediation

4. Validation workflow

ICS Owners/Operators

2. Authentication imputability

marc@192.168.56.1	root@ubuntu:22	SSH/SSH_X11_SESSION	2013-09-30 17:47:17	2013-09-30 17:58:16
marc@192.168.56.1	root@VMware_ESX	APP/RDP	2013-09-30 17:50:47	2013-09-30 17:51:30
marc@192.168.56.1	administrateur@win2008R2:3389	RDP/RDP	2013-09-30 17:53:28	2013-09-30 17:54:04

3. Fine-grained access management

Show 10 entries

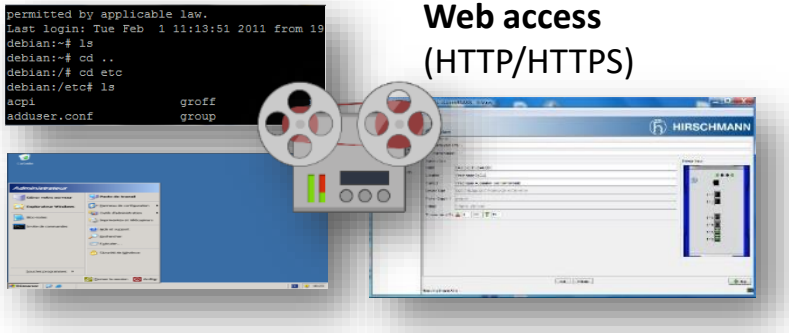
	Target	Protocols / Ports	Timeframe
RDP file / Direct access	admin@win7:RDP	RDP:3389	allthetime
WABPutty file / Direct access	root@ubuntu:SSH	SSH_SHELL_SESSION:22 SSH_REMOTE_COMMAND:22 SSH_SCP_UP:22 SSH_SCP_DOWN:22 SSH_X11_SESSION:22 SFTP_SESSION:22	allthetime

7. Action traceability and imputability

Command line
(SSH, TELNET, FTP, SCP…)

Graphic session
(RDP, VNC …)

Web access
(HTTP/HTTPS)



CLUSIF

Merci de votre attention