
22e édition
CARREFOUR des GESTIONS LOCALES de l'eau
5&6 MAI 2021
100 % DIGITAL
Rencontrez le monde de l'eau.
En direct. En vidéo.

5&6 MAI 2021

22e ÉDITION

CARREFOUR des GESTIONS LOCALES de l'eau

100 % DIGITAL

@CarrefourEau
#CGLE

Quels risques de cybercriminalité sur les services d'eau et d'assainissement ?

Modérateur
Bruno Nguyen
Académie de l'Eau

La cybersécurité

Une tâche sans relâche

Professeur Georges Ataya
Vice-Président de la Coalition belge de la Cybersécurité
Académique de l'Executive Master in Cybersecurity Management

Georges Ataya

Ville de Marseille

Retour d'expérience
Cyber-attaque du 14 Mars 2020

POGGI Jérôme / RSSI

Jérôme Poggi

Compagnie Intercommunale Liégeoi

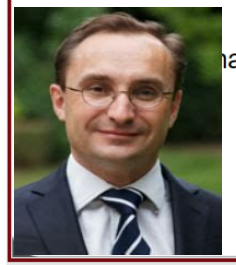
Retour d'expérience
Stratégie de cybersécurité

William De Angelis

LE POINT DE VUE DE L'ANSSI

Sylvie Andraud

Cyber menaces sur les SI Industriels



Franck Galland & Denis Pélanchon

Franck Galland

Denis Pélanchon

La cybersécurité

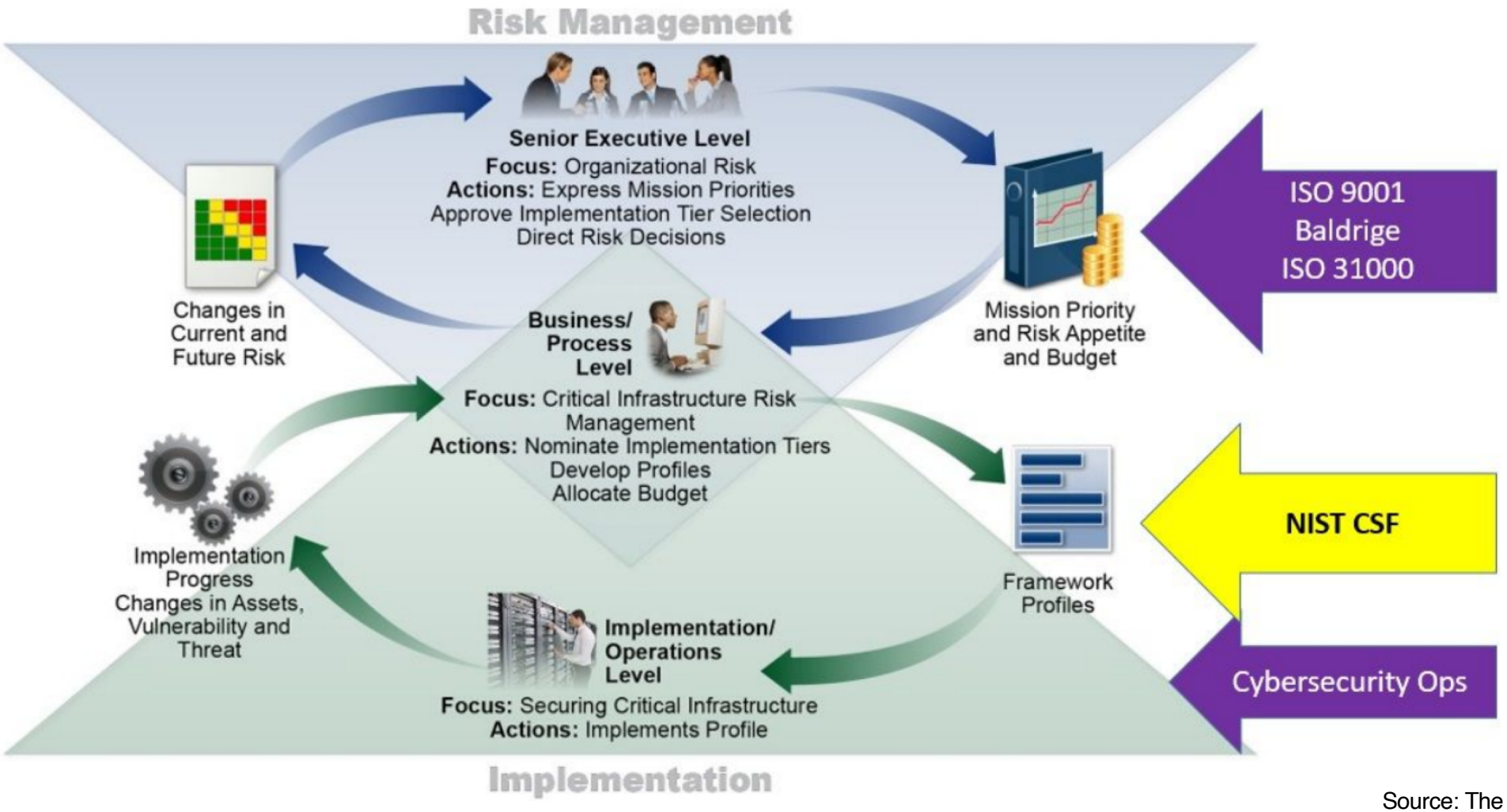
Une tâche sans relâche

Professeur Georges Ataya

Vice-Président de la Coalition belge de la Cybersécurité
Directeur Académique de l'Executive Master in Cybersecurity Management

Linkedin/ataya

Le paysage des menaces de cybersécurité change et évolue constamment à mesure que de nouvelles technologies sont développées et que les cyberattaques et les outils deviennent de plus en plus sophistiqués.



Source: The NIST Cybersecurity Framework


5&6 MAI 2021
22e ÉDITION
CARREFOUR des GESTIONS LOCALES de l'eau
100 % DIGITAL
@CarrefourEau
#CGLE
RISK
LEVEL
MAX
NO
LOW
MED
RETURN

5&6 MAI 2021

22e ÉDITION

CARREFOUR des GESTIONS LOCALES de l'eau

100 % DIGITAL

@CarrefourEau
#CGLE

Well-known cyber incident costs

(source: Deloitte.com)

- Customer breach notifications
- Post-breach customer protection
- Regulatory compliance (fines)
- Public relations/crisis communications
- Attorney fees and litigation
- Cybersecurity improvements
- Technical investigations

Source: Deloitte

Seven hidden costs of a cyberattack

(source: Deloitte.com)

- Insurance premium increases.
- Increased cost to raise debt.
- Operational disruption or destruction.
- Lost value of customer relationships.
- Value of lost contract revenue.
- Devaluation of trade name.
- Loss of intellectual property.


22e édition
CARREFOUR des GESTIONS LOCALES de l'eau
5&6 MAI 2021
100 % DIGITAL
Rencontrez le monde de l'eau.
En direct. En vidéo.

5&6 MAI 2021

22e ÉDITION CARREFOUR des GESTIONS LOCALES de l'eau

100 % DIGITAL

@CarrefourEau
#CGLE

Ville de Marseille

Retour d'expérience
Cyber-attaque du 14 Mars 2020

POGGI Jérôme / RSSI

Ville de Marseille

- Marseille : 240 km²
- 270 sites municipaux hors écoles
- 12 000 agents territoriaux
- 2 salles serveurs et un réseau en propre
  - Plus de 1000 serveurs
  - Plus de 5000 postes de travail

14 Mars 2020

- Veille du premier tours des élections municipales et du confinement
  - Compromission indirecte par rançongiciel
  - Perte de 90 % du système d'information
- Actions de réactions salvatrices
  - Les 24 premières heures les plus critiques

Bilan

- 3 jours pour comprendre ce qu'il venait de se passer
- 3 semaines pour avoir un redémarrage à minima
- 3 mois pour 80 % du SI opérationnel
- 3 ans de travail et de sécurisation
- Du budget et de la prise de conscience

Merci


22e édition
CARREFOUR des GESTIONS LOCALES de l'eau
5&6 MAI 2021
100 % DIGITAL
Rencontrez le monde de l'eau.
En direct. En vidéo.

Compagnie Intercommunale Liégeoise des Eaux CILE

Retour d'expérience
Stratégie de cybersécurité

William De Angelis
IT Manager

5&6 MAI 2021

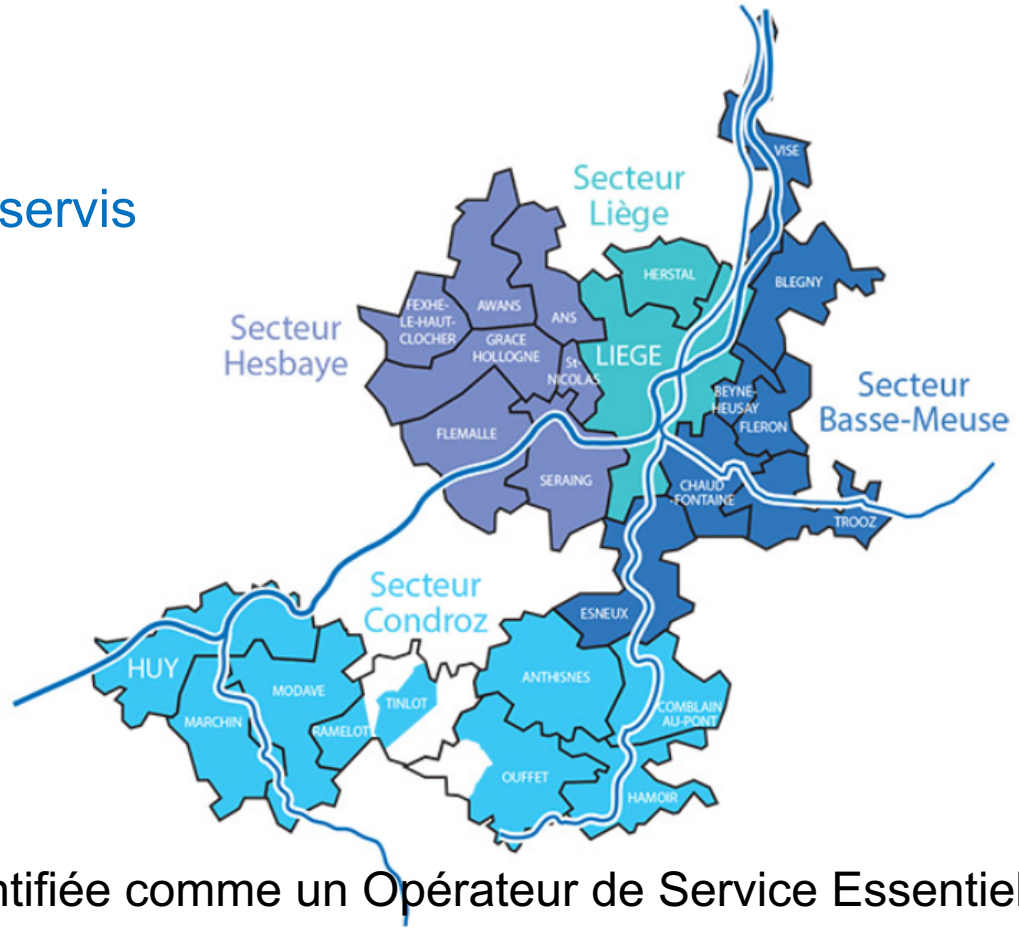
22e ÉDITION CARREFOUR des GESTIONS LOCALES de l'eau

100 % DIGITAL

@Carre

C.I.L.E. - Compagnie Intercommunale Liégeoise des Eaux SCRL

24 Communes
565.000 habitants désservis
260.000 compteurs
3600 km de conduites
350 automates
380 ETP
136 millions Euros CA



La CILE, votre distributeur d'eau dans les communes de :

- Ans
- Anthisnes
- Awans
- Beyne-Heusay
- Blegny
- Chaudfontaine
- Comblain-au-Pont
- Esneux
- Fexhe-le-Haut-Clocher
- Flémalle
- Fléron
- Grâce-Hollogne
- Hamoir
- Herstal (en partie)
- Huy
- Liège
- Marchin
- Modave
- Ouffet (en partie)
- Saint-Nicolas
- Seraing
- Tinlot
- Trooz
- Visé

La C.I.L.E est identifiée comme un Opérateur de Service Essentiel (OSE) au regard de la directive NIS.

Les déclencheurs

- La stratégie de cybersécurité Européenne
- La rencontre avec WSMART

2015
membre
WSMART

2016-2018
GDPR-RGPD

2016-2021
NIS-SRI

2021-2025?
NIS-SRI 2

Directive NIS-SRI et RGPD, nouvelles obligations légales

NIS art14 : Exigences de sécurité et notification d'incidents
RGPD art32 : Sécurité du traitement
… mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque…

ISO27001 comme moyen de mise en conformité

COBIT 5 AN ISACA® FRAMEWORK

ISO 27001

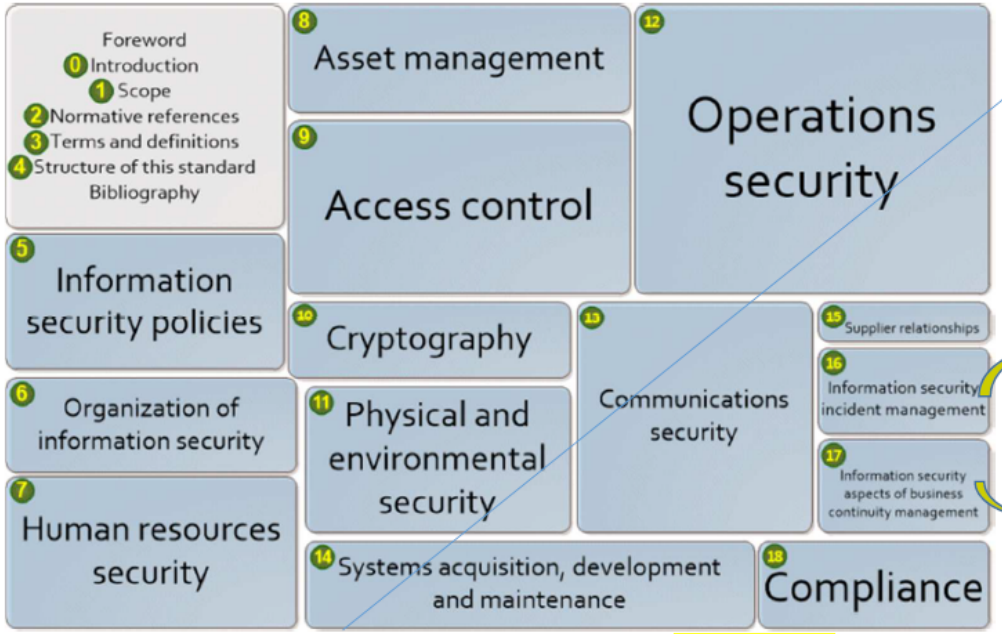
NIST CYBERSECURITY FRAMEWORK (CSF)

IDENTIFY PROTECT DETECT RESPOND RECOVER

Source : NIS Cooperation Group members.
Building upon answers provided by the Member States ENISA's questionnaire, the Group acknowledged that Member States m wish to use different sources or control frameworks for sec measures from European or International standards (e.g. ISO 27.000)6 to existing or new sets of security measures (e.g. France's cybersecurity measures for OES, Germany's IT-Grundschutz, Spain's National Security Framework, etc.).
6 Article 19 of the NIS Directive "Encourage the use of Europea and internationally accepted standards and specifications relev to the security of Network and Information Systems".

ISO27002-Control block

114 Exigences de sécurité



Art14.2

Art14.2 : les OSE prennent les mesures appropriées en vue de prévenir les incidents qui compromettent la SRI utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.

TRANSFORMATION DIGITALE

Directive NIS
RGPD

Gestion de crise

2015
CILE intègre WSMART

2017
BPMN
Cartographie processus et data

2018
Coopération WSMART-CILE
Sur la montée en maturité de la CILE en gestion de crise

2018
RGPD
Déploiement ISO27001

T3-2019
1er exercice de crise
Avec observateurs internationaux WSMART

2020
Certification ISO27001

2020-2021
démarche d'amélioration continue du dispositif de crise:
opportunités présentées par l'exercice de crise afin de s'améliorer

2021

T4 2021
2iem Exercice de crise

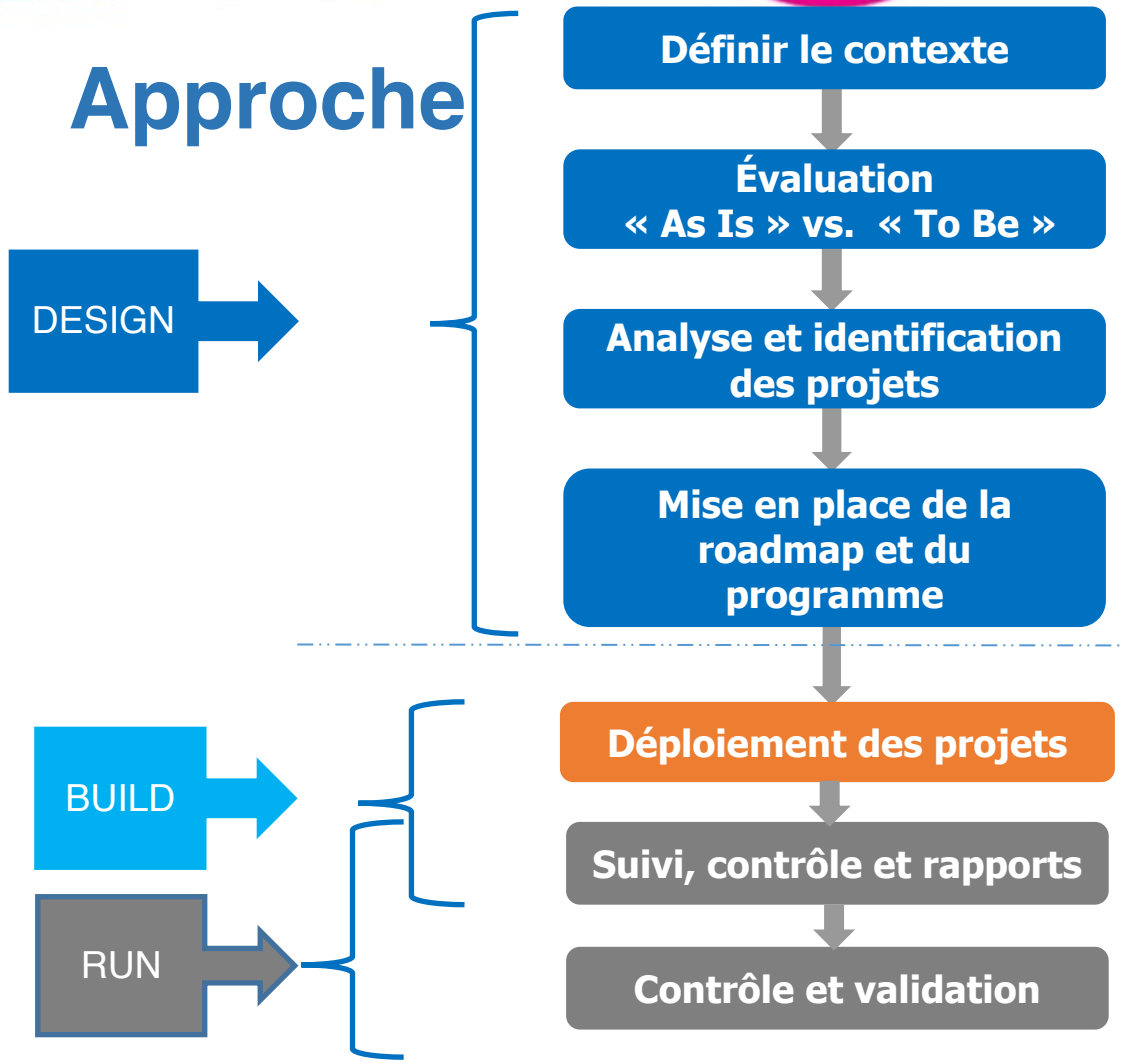
COVID

Roadmap Cybersécurité

Gestion de crise eau potable ISO 24518

Continuité (PCA COVID19) → ISO 22301

Construction de la roadmap de cybersécurité

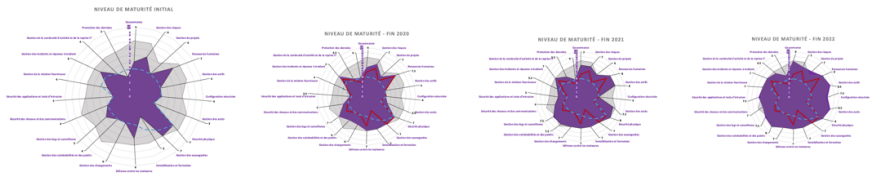


Définition des projets

Exemple avec un projet de gestion des vulnérabilités

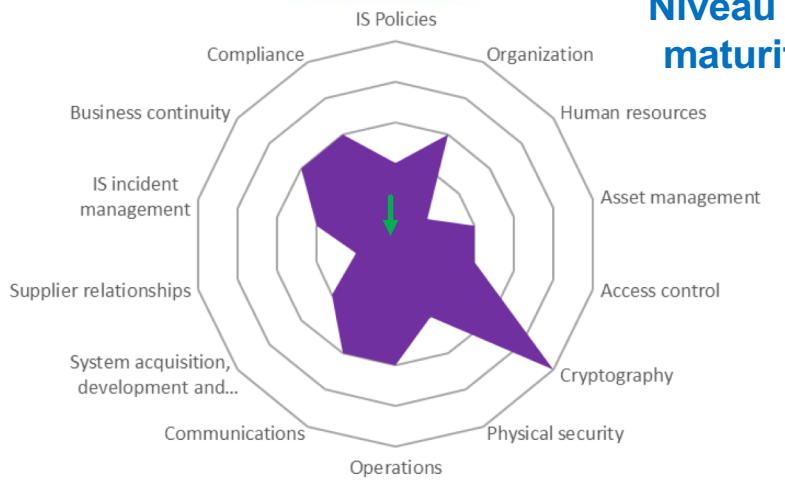
Vulnerability Management	
1	Run a vulnerability scan on most critical assets in order to identify, assess, prioritize and remediate known vulnerabilities.
2	Produce an remediation plan based on the assets criticality (exposure, hosted data, supported business process) and the vulnerability severity.
3	Follow up on the remediation plan.
4	Formalize a Vulnerability Management Policy, Processes and Procedures, including remediation strategy, timeframe, asset scope, KPIs and reports.
5	Deploy a solution for ensuring vulnerability watch and vulnerability scan in accordance with the VM Policy.
6	Formalize a Patch Management Procedure aligned with the VM Policy.
7	Choose and deploy a solution for ensuring vulnerability watch and vulnerability scan aligned with the VM Policy
8	Ensure appropriate training and handover to staff involved in the process.

From « **As Is** » to « **To Be** »

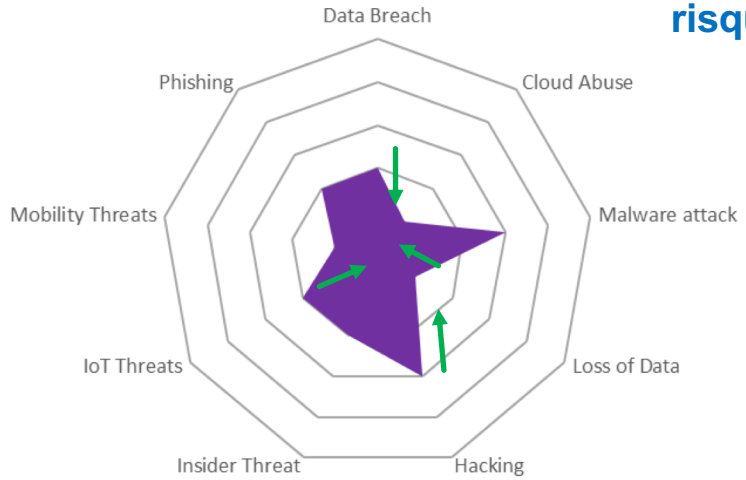


Existing | **End of 2020** | **End of 2021** | **End of 2022**

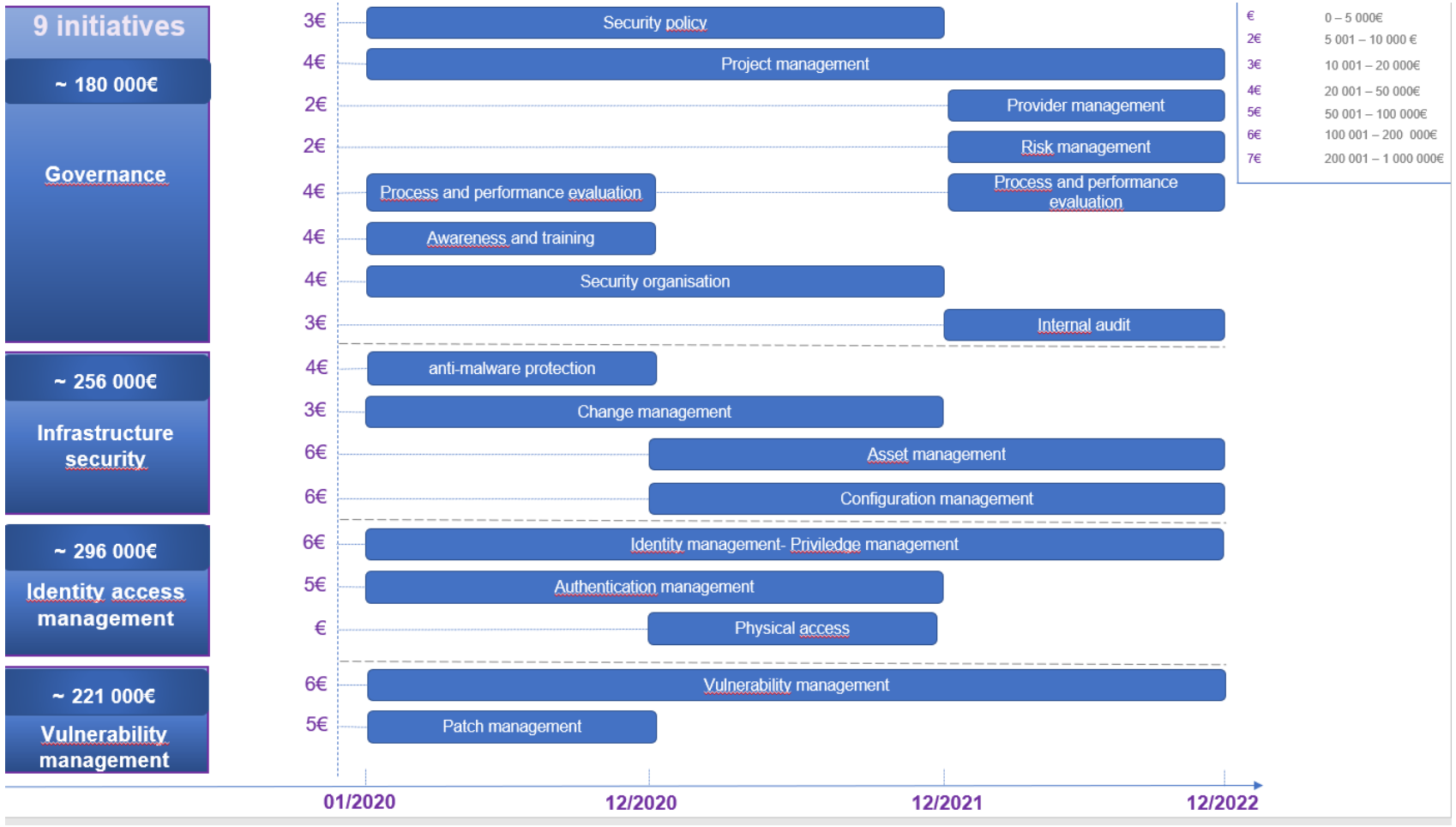
Niveau de maturité



Niveau de risque



Exemple de roadmap de cybersécurité




22e édition
CARREFOUR des GESTIONS LOCALES de l'eau
5&6 MAI 2021
100 % DIGITAL
Rencontrez le monde de l'eau.
En direct. En vidéo.

LE POINT DE VUE DE L'ANSSI

6 mai 2021

ETAT DE LA MENACE

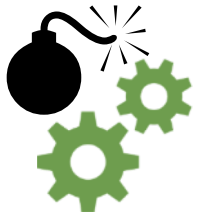
LES FINALITÉS

ATTEINTE À L'IMAGE

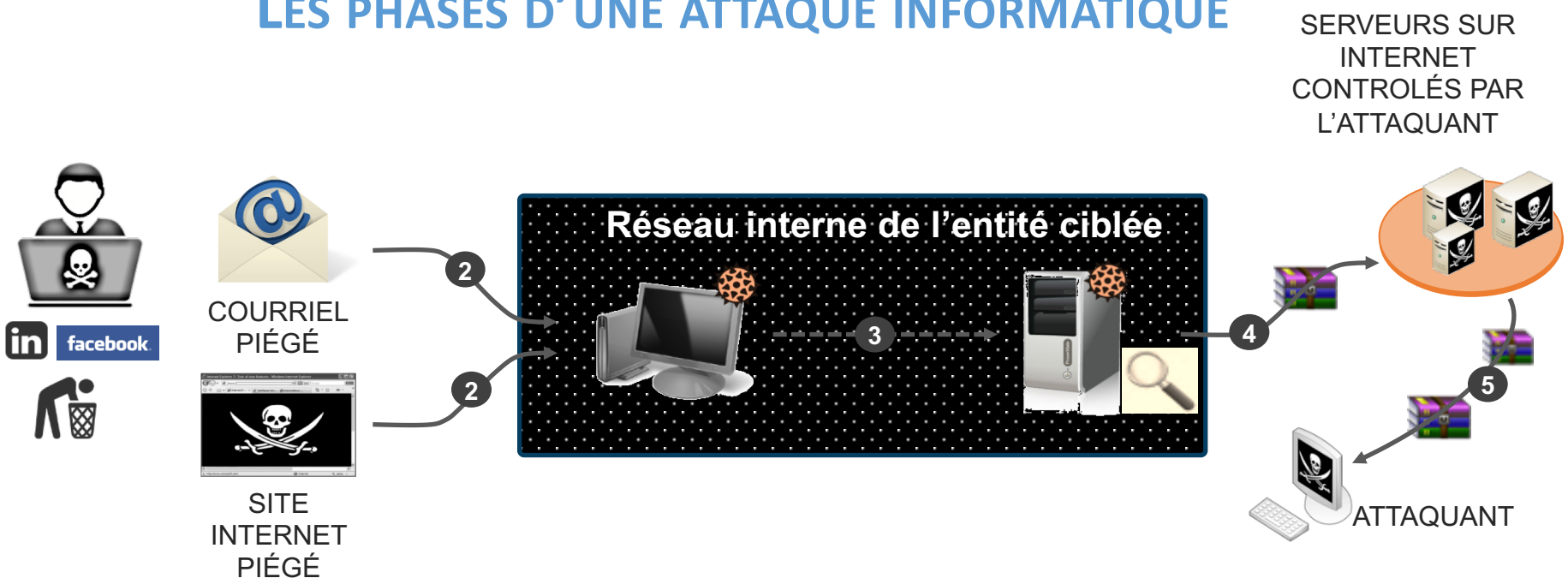
CYBER CRIMINALITÉ

ESPIONNAGE

SABOTAGE



LES PHASES D'UNE ATTAQUE INFORMATIQUE



Attaques récentes sur le secteur de l'eau

- **24 / 25 avril 2020 Israel**
  - ***Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran*** **(The Washington Post – 10/05/2020)**

    Quickly detected and thwarted before it could cause damage ; The intruders targeted "programmable logic" controllers that operate valves for water distribution networks. The two affected districts serve a variety of residential, medical and commercial customers, providing fresh water as well as wastewater removal and treatment. At the time, much of the population was under lockdown because of the pandemic.

  - ***Hackers Knew How to Target PLCs in Israel Water Facility Attacks*** ***(Securityweek.com – 30/04/2020)***

    The actions of the hackers who recently targeted water facilities in Israel show their sophistication and prove that they knew exactly what they were doing, according to people with knowledge of the attacks. The attacks targeted wastewater treatment plants, pumping stations and sewage facilities, and organizations in the water sector have been instructed by Israeli authorities to immediately take measures to prevent attacks, including changing passwords to internet-exposed control systems, reducing internet exposure, and ensuring that all software is up to date. Sources told SecurityWeek that the attackers targeted programmable logic controllers (PLCs) used to control valves. The changes made to the PLC logic were valid, which indicates that the attackers knew exactly what they were doing.

- **Juin 2020 Israel**
  - ***Two more cyber-attacks hit Israel's water system*** **(Zdnet – 20/07/2020)**

    Officials said the attacks took place last month, in June, and didn't cause any damage to the attacked organizations ; The first attack hit agricultural water pumps in upper Galilee, while the second one hit water pumps in the central province of Mateh Yehuda, local media reported last week. No harm or any real-world effects.

Attaques récentes sur le secteur de l'eau

- **1er décembre 2020 Israel**
  - ***Iranian Hackers Access Unprotected ICS at Israeli Water Facility*** **(securityweek.com – 04/12/2020)**

A group of Iranian hackers recently posted a video showing how they managed to access an industrial control system (ICS) at a water facility in Israel. According to industrial cybersecurity firm OTORIO, the hackers accessed a human-machine interface (HMI) system that was directly connected to the internet without any authentication or other type of protection. The target was apparently a reclaimed water reservoir. "This gave the attackers easy access to the system and the ability to modify any value in the system, allowing them, for example, to tamper with the water pressure, change the temperature and more. All the adversaries needed was a connection to the world-wide-web, and a web browser," OTORIO said.

- **8 février 2021 Floride**
  - **Hackers tried poisoning town after breaching its water facility (Bleepingcomputer.com – 08/02/2021)**

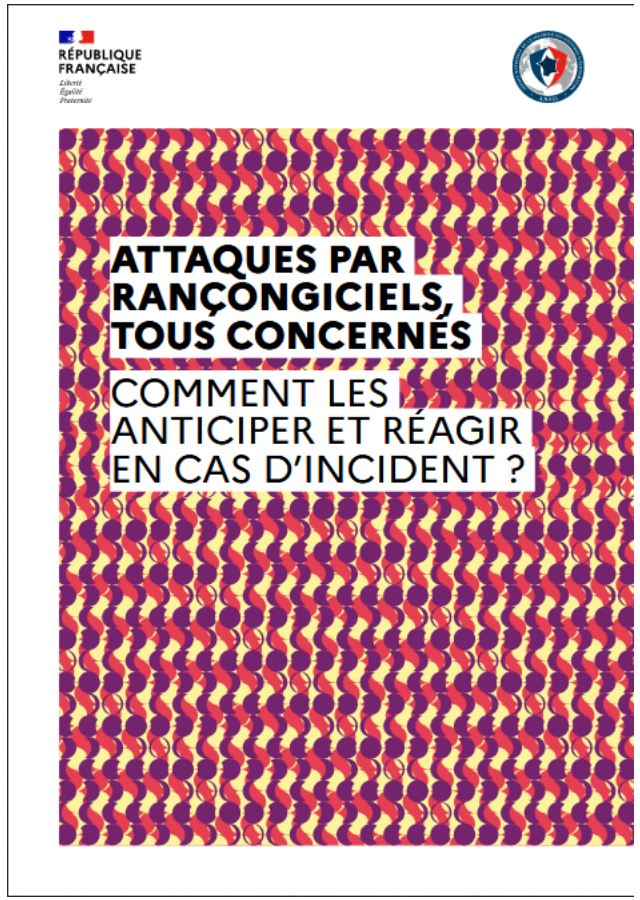
A hacker gained access to the water treatment system for the city of Oldsmar, Florida, and attempted to increase the concentration of sodium hydroxide (NaOH), also known as lye and caustic soda, to extremely dangerous levels. The hackers remotely gained access to a software program, named TeamViewer, on the computer of an employee at the facility to gain control of other systems. The intruder spent between three to five minutes inside the system and changed the the sodium hydroxide level from 100 parts per million to 11,100 parts per million. The change was immediately reverted by the operator and the population of Oldsmar was not at risk at any moment because the operator intervened immediately. The plant operator then cut off remote access to the system.

LES CONSTATS

- **Prolifération d'outils d'attaque informatique (Multitudes de techniques et d'outils malveillants réutilisables)**
- **Nombreuses publications de vulnérabilités sur les logiciels et leur exploitation par les cyber-attaquants**
- **Prolifération et professionnalisation des groupes d'attaquants**
- **Augmentation de la surface d'exposition aux attaques (télétravail, Internet des objets, numérisation et interconnexion croissantes, intégration des technologies (IT) au cœur des réseaux industriels (OT) …)**
- **Supply chain attack ; principe : atteindre une cible sécurisée par la compromission d'un prestataire (rebond vers la cible via l'interconnexion des réseaux) ou de la mise à jour d'un logiciel ;**

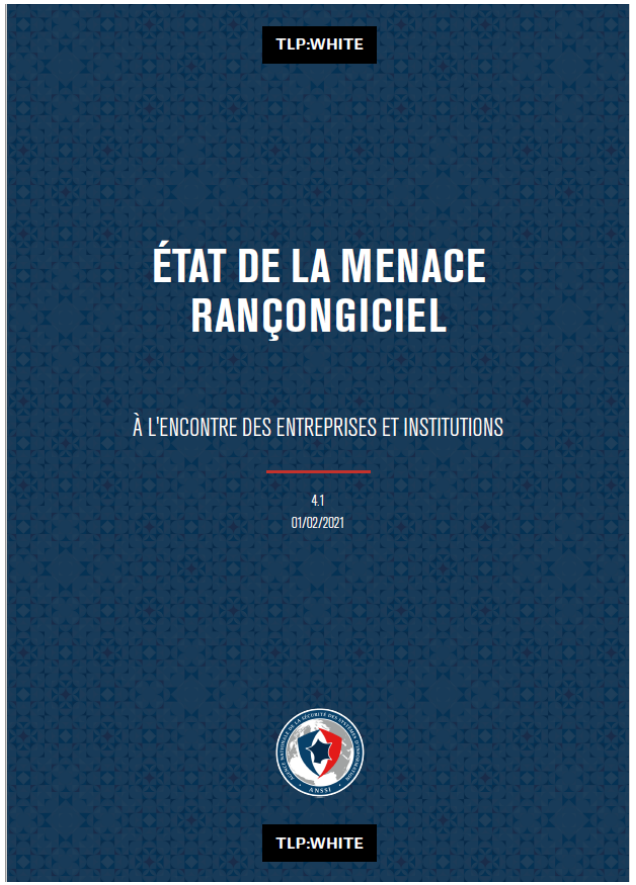
ATTAQUES PAR RANCONGICIELS, TOUS CONCERNES

SOMMAIRE



RANÇONGICIELS : UNE MENACE QUI EXPLOSE

- 2020 : augmentation de 255% des signalements d'attaque par rançongiciel par rapport à 2019
- *Ransomware-as-a-Service* (RaaS). Le modèle du RaaS consiste à proposer un véritable service de ransomware, prêt à l'emploi, et avec tout le support après vente
- Multiplication des techniques de chantage pour accroître la pression sur les victimes : en exfiltrant les données, avant le chiffrement, et en menaçant de les publier ; en revendant les accès obtenus à d'autres cybercriminels…
- Entités victimes incitées à payer la rançon qui représente souvent un coût inférieur aux coûts de remédiation



HAUSSE DE LA CYBERMENACE, EN PROPORTION DE LA NUMERISATION

- **Exposition accrue de nos sociétés (de plus en plus numérisées et interconnectées) au risque de crises cyber majeures**
- **Cyberattaques croissantes en nombre, intensité, sophistication et furtivité**

> **Explosion de la cybercriminalité ; le cybercrime devient une véritable industrie et constitue la principale menace cyber pour les entreprises et collectivités :**

  > **opérations lucratives, à très forte rentabilité (bien supérieure aux coûts de mise en œuvre)**

  > **Impunité des cybercriminels car difficilement identifiables, souvent hors de portée des mécanismes d'entraide pénale internationale, voire protégés par certains Etats**

- **Le risque d'espionnage demeure élevé (savoir-faire industriel, secteurs soumis à une forte compétitivité internationale)**

FOCUS SUR LES SYSTEMES INDUSTRIELS

LES TENDANCES

- Convergence IT / OT :
  - Besoins :
    - Optimisation des coûts : besoin de composants « sur étagère » (COTS), de télémaintenance
    - Amélioration de la productivité : besoin d'échanger des données entre les réseaux de gestion et les réseaux industriels, accéder aux données de production depuis le SI de gestion, pilotage centralisé et simultané de sites éloignés
  - Numérisation des activités industrielles
  - Tendance à l'externalisation et à l'intervention à distance
  - Intégration des technologies IT au cœur des réseaux OT
  - Interconnexion des réseaux OT et IT, parfois sans cloisonnement et/ou non maîtrisée
- Menace pesant sur les ICS pas nécessairement ciblée mais intérêt grandissant des attaquants
- Une attaque du SI de gestion peut compromettre les SI industriels ou impacter le processus industriel (sans compromission directe du réseau OT)
- Des systèmes de contrôle industriel non conçus pour faire face aux menaces liées à la cybersécurité
- Des ressources disponibles pour les attaquants
  - Moteurs de recherche spécialisés, référençant les ICS accessibles sur Internet (ex. SHODAN)
- Les systèmes de protection physique et les systèmes de type GTB sont aussi concernés par la menace cyber

Vulnérabilités fréquentes des SI industriels

- Protection :
  - Absence de durcissement et de sécurisation des OS et firmwares (services activés sans utilité fonctionnelle, emploi de services / protocoles non sécurisés, fonctions de sécurité non activées), favorisant l'augmentation de la surface d'attaque
  - absence de mécanisme de signature des *firmwares* (possibilité pour un attaquant de diffuser une mise à jour piégée)
  - OS et logiciels obsolètes
  - Absence / déficience du cloisonnement et du filtrage des flux, favorisant la propagation des attaques (notamment entre le SI de gestion et le SI industriel)
  - absence de politique de gestion des médias amovibles (ex. : blocage des ports USB) alors que les clés USB non maîtrisées sont autorisées
  - IHMs connectées en permanence
  - Absence de maintien en condition de sécurité (veille sur les vulnérabilités et patch management)
  - Non maitrise des accès distants, insuffisamment sécurisés (télédiagnostic, télémaintenance)
  - Absence / déficience des politiques de :
    - gestion des comptes (restent actifs après départ, comptes génériques, comptes par défaut…)
    - gestion des droits (droits administrateur aux utilisateurs, non respect du principe du moindre privilège)
    - gestion des mots de passe (mots de passe par défaut ou faibles, mots de passe en clair dans les codes sources, procédures d'exploitation, données sauvegardées …)

Vulnérabilités fréquentes des SI industriels (suite)

- Gouvernance
  - pas d'inventaire / cartographie du parc de SI industriel, pas d'inventaire des équipements, absence de vision des « générations » technologiques qui cohabitent et de leurs vulnérabilités intrinsèques
  - Absence d'analyse de risque et de PSSI sur le SI industriel
  - Défaut de sensibilisation du personnel
- Défense et résilience :
  - Fonctions de traçabilité non activées ; pas d'analyse des journaux
  - Absence de capacités de détection des incidents de sécurité
  - Absence / déficience (existante mais non testée) de la politique de sauvegarde / restauration
  - Pas de préparation à la gestion de crise cyber

- Déficience du contrôle d'accès physique permettant un accès physique direct au réseau industriel (ex. accès à une armoire informatique), voire l'installation d 'un composant physique étranger permettant un accès à distance

POUR ALLER PLUS LOIN …

- Guides ANSSI sur la cybersécurité des systèmes industriels
- Guide ANSSI sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection
- Analyse ANSSI : *Etat de la menace informatique liée aux Systèmes de contrôle industriel*
- Groupe de travail « Sécurité SCADA » du CLUSIF :
  - fiches incidents cyber – SI industriels ;
  - Panorama des référentiels
  - Guide cybersécurité des systèmes industriels
- Commission technique Cybersécurité des systèmes industriels de l'EXERA (journée technique annuelle fin septembre)
- CERTs dédiés aux systèmes de contrôle industriel, entre autres :
  - ICS CERT américain :
    - https://us-cert.cisa.gov/ncas/alerts/aa20-205a : **NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems**
  - Kaspersky ICS CERT
- Nombreuses publications des éditeurs

Au-delà des mesures purement techniques …

- Intégrer au bon niveau les enjeux de cybersécurité dans les organisations ; définir et appliquer une PSSI y compris sur le SI industriel
- Connaître son SI (inventaire / cartographie SI des installations industrielles, composants et flux, maintenue à jour) ;
- Connaître ses risques et faire accepter les risques résiduels par le bon niveau hiérarchique
- Auditer régulièrement son SI (connaître son niveau d'exposition sur Internet, le niveau de sécurité de l'AD Microsoft ; disposer d'une politique d'audit : tests d'intrusion, audit d'architecture, audit de configuration…)
- Sensibiliser
- Surveiller, détecter et réagir ; se préparer à la gestion de crise cyber
- Intégration de la cybersécurité dans les différentes phases du cycle de vie du système industriel ; exigences SSI dans les contrats et cahiers des charges pour les prestataires ; dans les contrats de maintenance
- Pour les projets de transformation numérique : évaluation des risques et mesures de réduction dès les phases de réflexion et à haut niveau

LA REGLEMENTATION

LA RÈGLEMENTATION

Loi de programmation militaire – article 22

Loi Française qui concerne les Opérateurs d'Importance Vitale (OIV) des 12 secteurs d'activité d'importance vitale, dont le secteur de la gestion de l'eau

Directive NIS (2016/1148 du 6 juillet 2016)

Directive européenne, transposée en droit national en 2018, qui concerne les Opérateurs de Services Essentiels (OSE), répartis par secteur / sous-secteur, dont :

- Fourniture et distribution d'eau potable
- Traitement des eaux non potables*

Règles de sécurité et délais d'application

OIV : **20 règles de sécurité** [Arrêté sectoriel du 17 juin 2016 applicable aux OIV du secteur « Gestion de l'eau »]

OSE : **23 règles de sécurité** [Arrêté du 14 septembre 2018]

OIV et OSE soumis à des contrôles de leur niveau de sécurité et **obligations de notification des incidents de sécurité**

* NIS V1 : secteur ajouté par la France ; NIS V2 : secteur retenu par la commission européenne

Merci pour votre attention

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

sylvie.andraud@ssi.gouv.fr

Division Coordination Sectorielle

Bureau Energie, Transport et Environnement


22e édition
CARREFOUR des GESTIONS LOCALES de l'eau
5&6 MAI 2021
100 % DIGITAL
Rencontrez le monde de l'eau.
En direct. En vidéo.

5&6 MAI 2021
22e ÉDITION
CARREFOUR des GESTIONS LOCALES de l'eau
100 % DIGITAL
@CarrefourEau
#CGLE

Cyber menaces sur les SI Industriels

Analyse des techniques utilisées

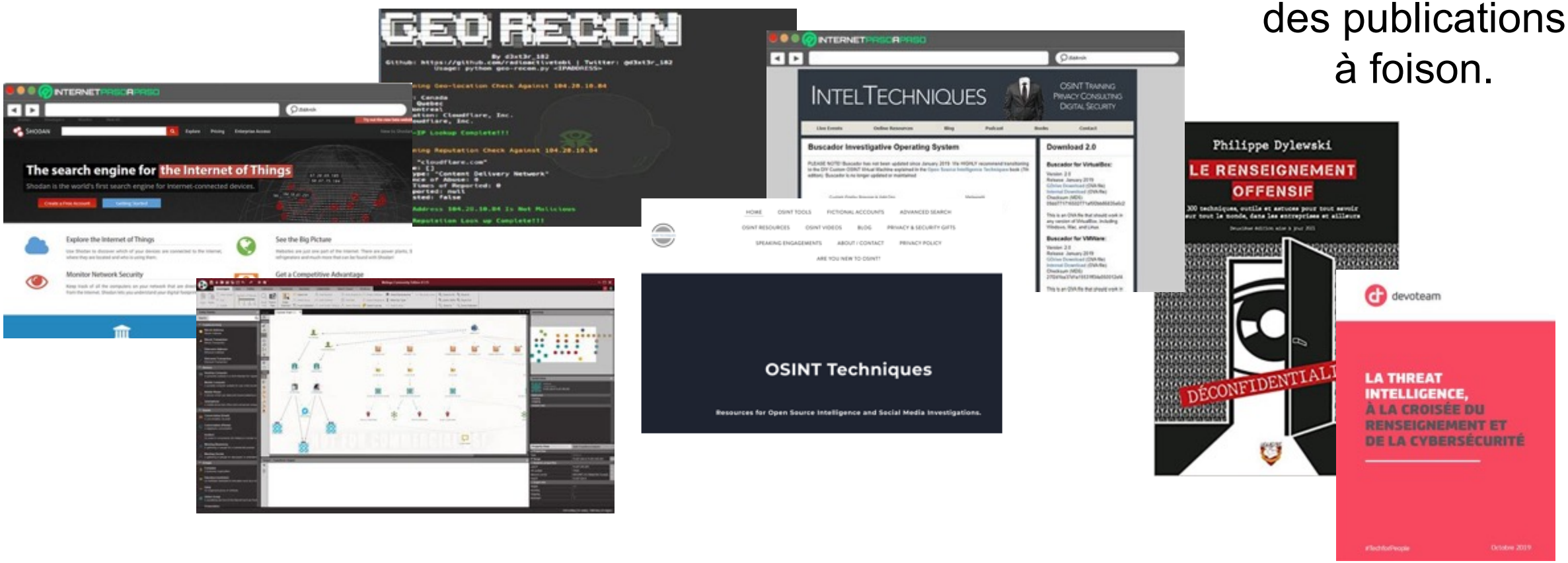
Franck Galland & Denis Pélanchon

es2 Environmental Emergency & Security Services

AXIS&CO

Open Source Intelligence

Des outils, des techniques et des publications à foison.

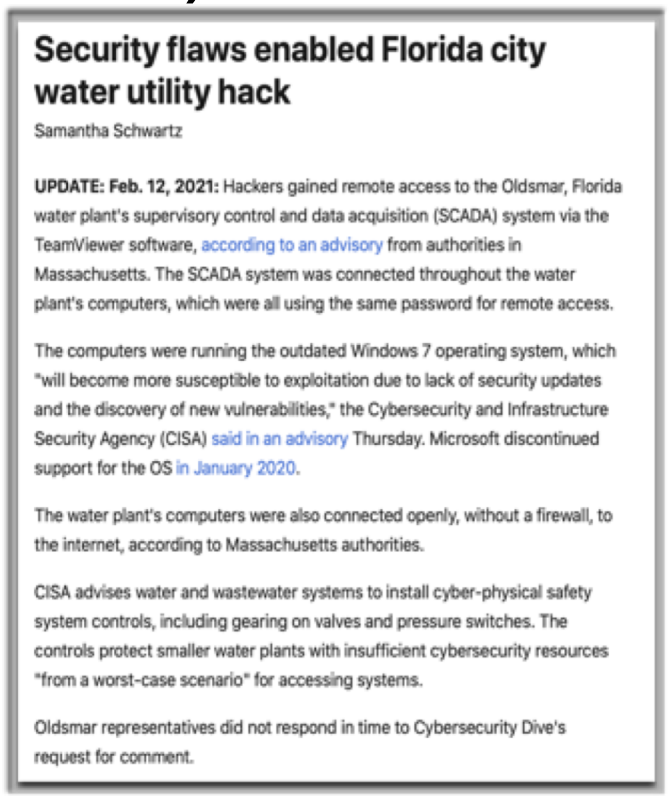


Oldsmar (février 2021)

all using the same password for remote access

outdated Windows 7

connected openly, without a firewall, to the internet



Security flaws enabled Florida city water utility hack

Samantha Schwartz

UPDATE: Feb. 12, 2021: Hackers gained remote access to the Oldsmar, Florida water plant's supervisory control and data acquisition (SCADA) system via the TeamViewer software, according to an advisory from authorities in Massachusetts. The SCADA system was connected throughout the water plant's computers, which were all using the same password for remote access.

The computers were running the outdated Windows 7 operating system, which "will become more susceptible to exploitation due to lack of security updates and the discovery of new vulnerabilities," the Cybersecurity and Infrastructure Security Agency (CISA) said in an advisory Thursday. Microsoft discontinued support for the OS in January 2020.

The water plant's computers were also connected openly, without a firewall, to the internet, according to Massachusetts authorities.

CISA advises water and wastewater systems to install cyber-physical safety system controls, including gearing on valves and pressure switches. The controls protect smaller water plants with insufficient cybersecurity resources "from a worst-case scenario" for accessing systems.

Oldsmar representatives did not respond in time to Cybersecurity Dive's request for comment.

https://www.cybersecuritydive.com/news/water-supply-cyber-attack-florida-ics-security/594764/

National water carrier Israël (avril et juin 2020)

Très peu de détails techniques.

Accès distants en cause.

Organisée et synchronisée.

Simple intimidation ?

Réplique de 2016 ?

Ukraine (décembre 2015)

Social engineering.

Malwares spécialisés.

Prise de main à distance.

Sabotage.

Absence de cloisonnement.

Armoires de rue

Serrures crochetables

Capteurs neutralisables

Ports physiques libres d'accès

Absence de règles de filtrage

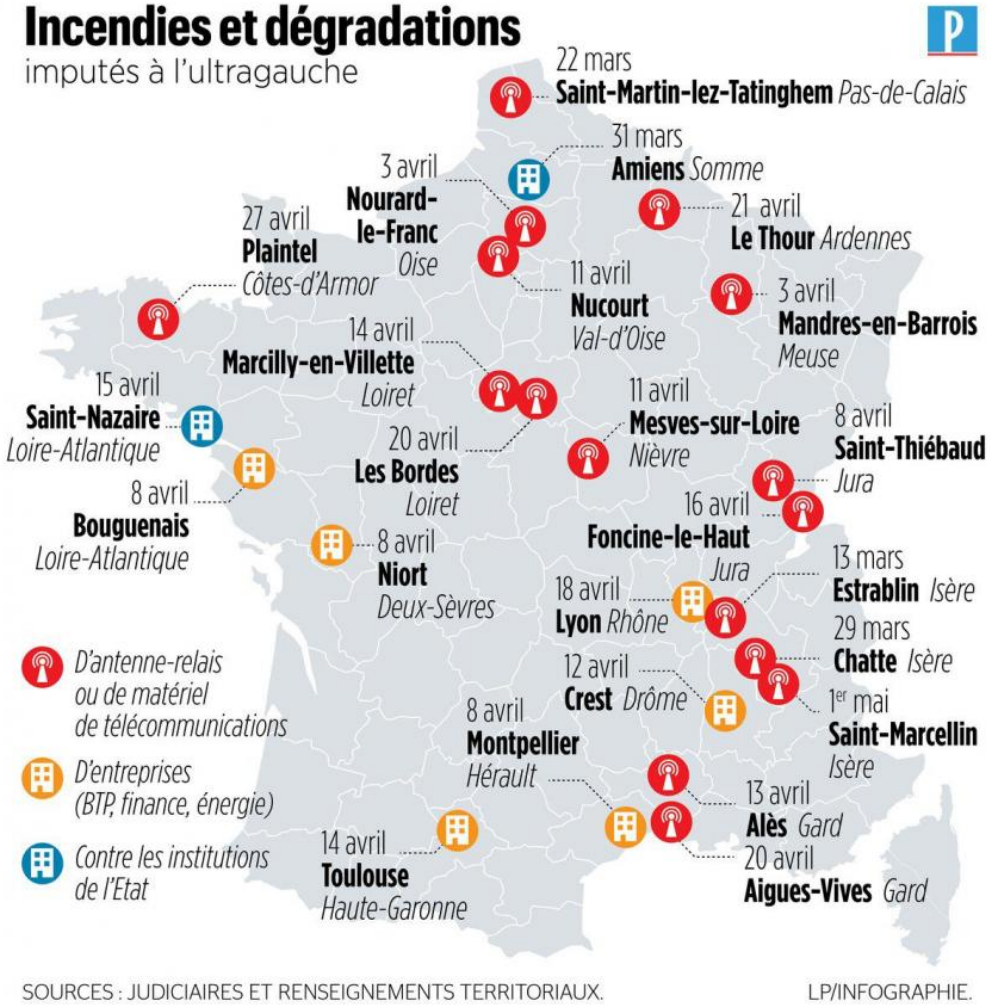
Surface d'attaque assez large

Remontée possible vers l'infrastructure centrale

Sabotage et malveillance

Menaces sur les antennes télécom et le secteur de l'énergie.

Risque d'indisponibilité



Défense dans la profondeur

1. **Accès distants :** uniquement pour des postes de confiance enrôlés.
2. **Cloisonnement et filtrage :** n'autoriser que le strict nécessaire.
3. **Politique de mots de passe :** ne peut être forte que si outillée.
4. **Journalisation :** basée sur les besoins d'investigation.
5. **Détection :** identifier les signaux faibles dès la phase de reconnaissance.
6. **Tests des équipes internes :** fausse campagne de fishing, exercice de crise cyber.


22e édition
CARREFOUR des GESTIONS LOCALES de l'eau
5&6 MAI 2021
100 % DIGITAL
Rencontrez le monde de l'eau.
En direct. En vidéo.

5&6 MAI 2021

22e ÉDITION

CARREFOUR des GESTIONS LOCALES de l'eau

100 % DIGITAL

@CarrefourEau
#CGLE