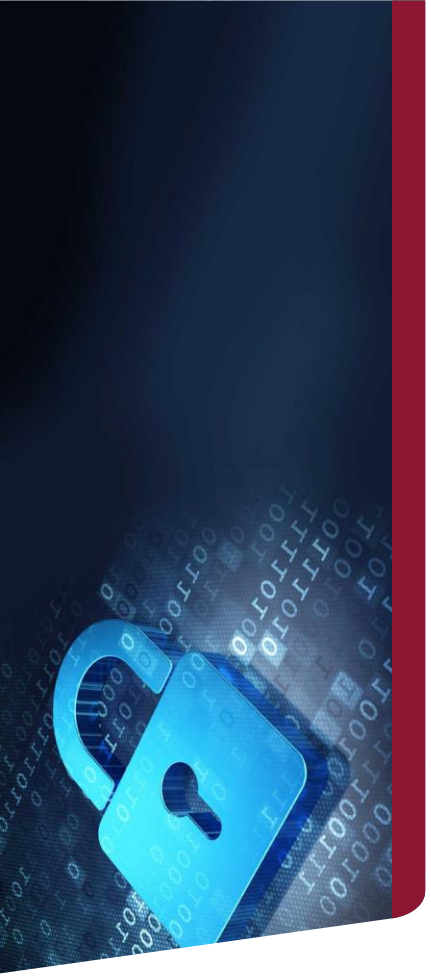
Cybersécurité
Protégez vos produits et les données associées

Jeudi 1er février 2018

CAP'TRONIC



PROGRAMME DE LA JOURNEE

ACCUEIL

1. L'univers de la Cybersécurité
2. Législation actuelle et Référentiels existants

COMMENT SE PROTEGER

1. Guides SW100 et SW200
2. Analyse de Risques
3. Les attaques par interfaces

UNE SOLUTION COMMUNE

1. Partenariat CEA – Bureau Veritas
2. Présentation P-Scan

DEJEUNER

DATA PROTECTION OFFICER

1. Le DPO, pourquoi, quel rôle ?
2. Les tâches du DPO
3. DPO externalisé, une solution pour les TPE/PME

CAP'TRONIC

BUREAU VERITAS

leti ceatech

BUREAU VERITAS LCIE

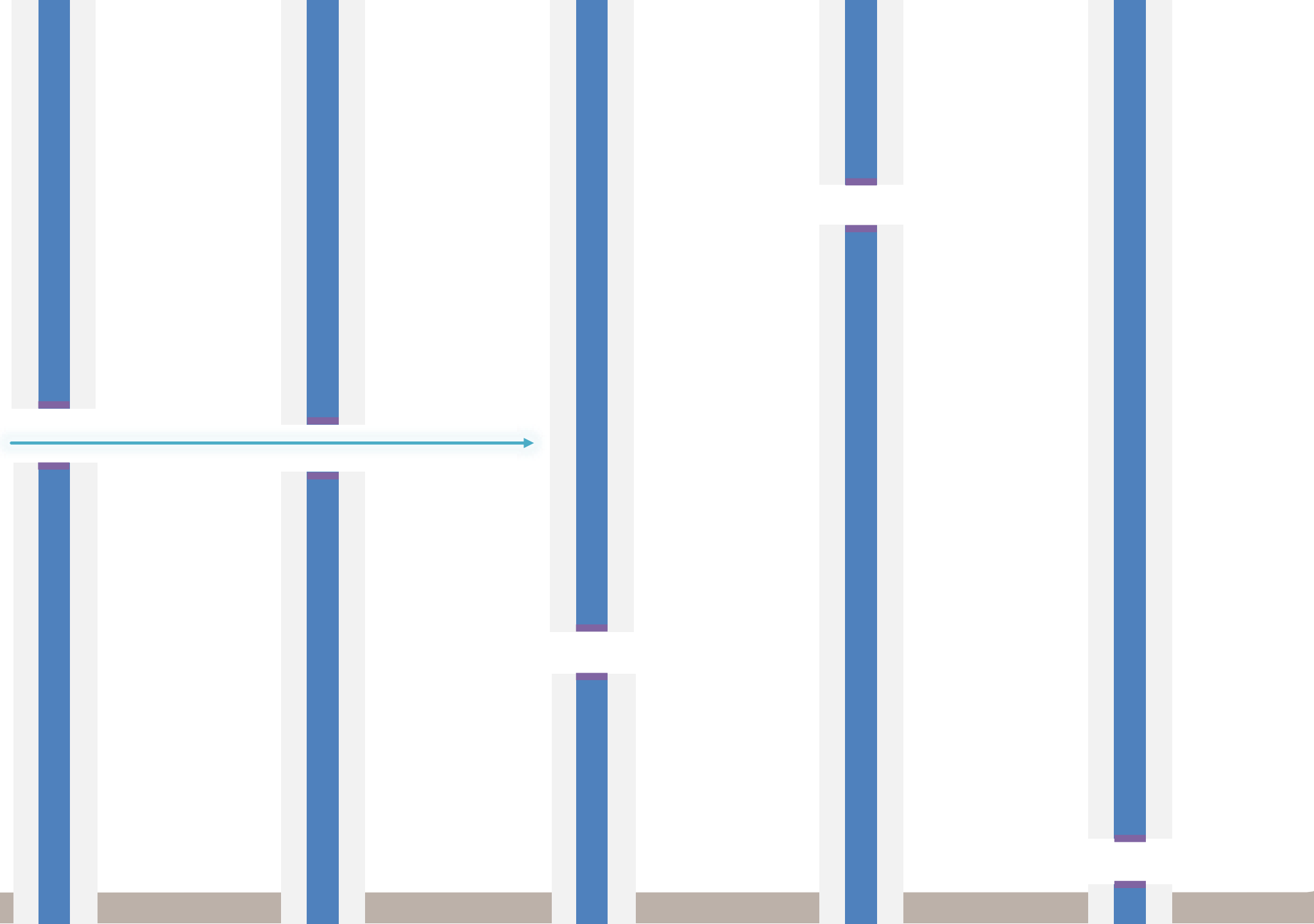
AKANT

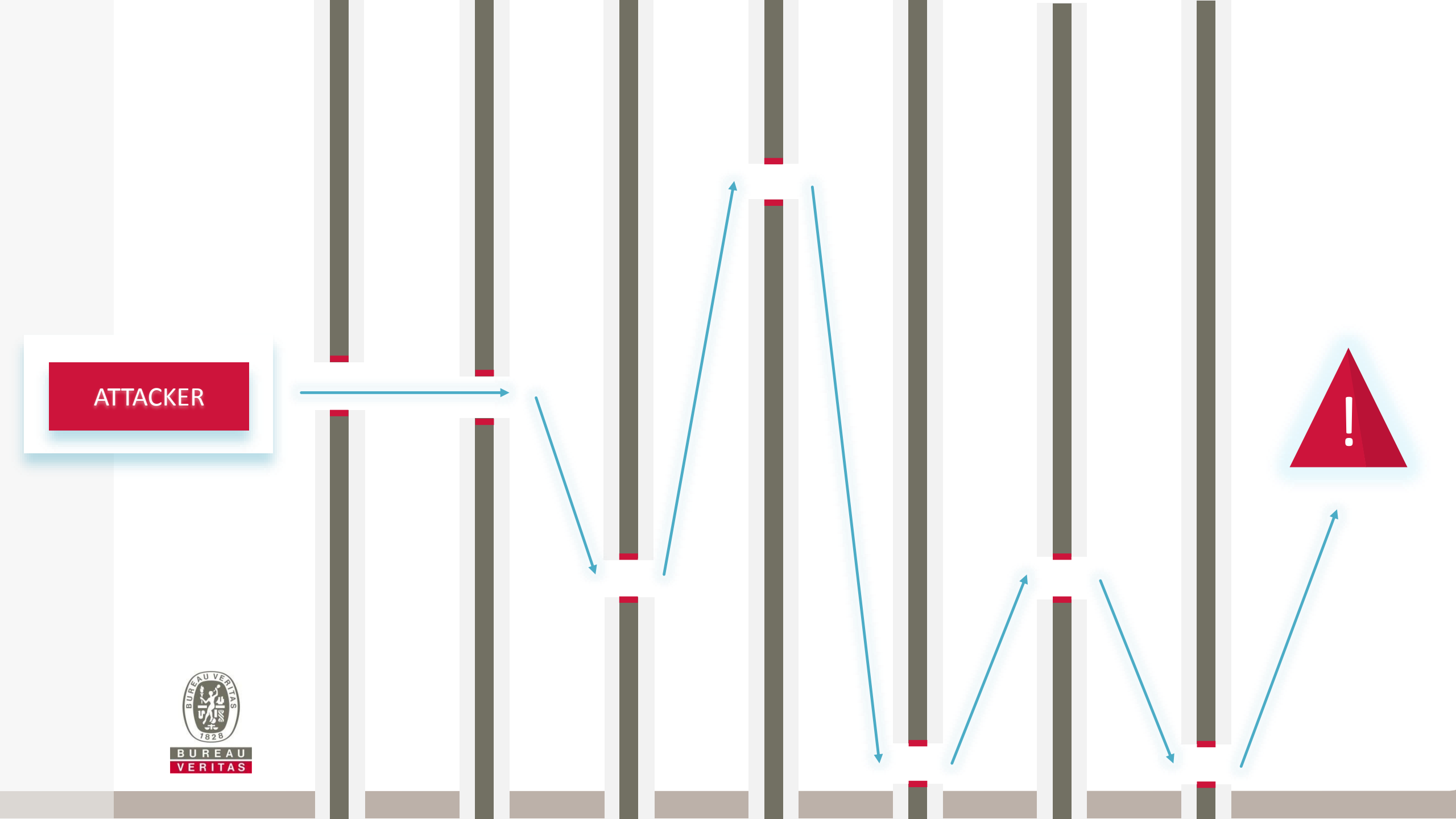
L'UNIVERS DE LA CYBERSECURITE

Laurent Midrier

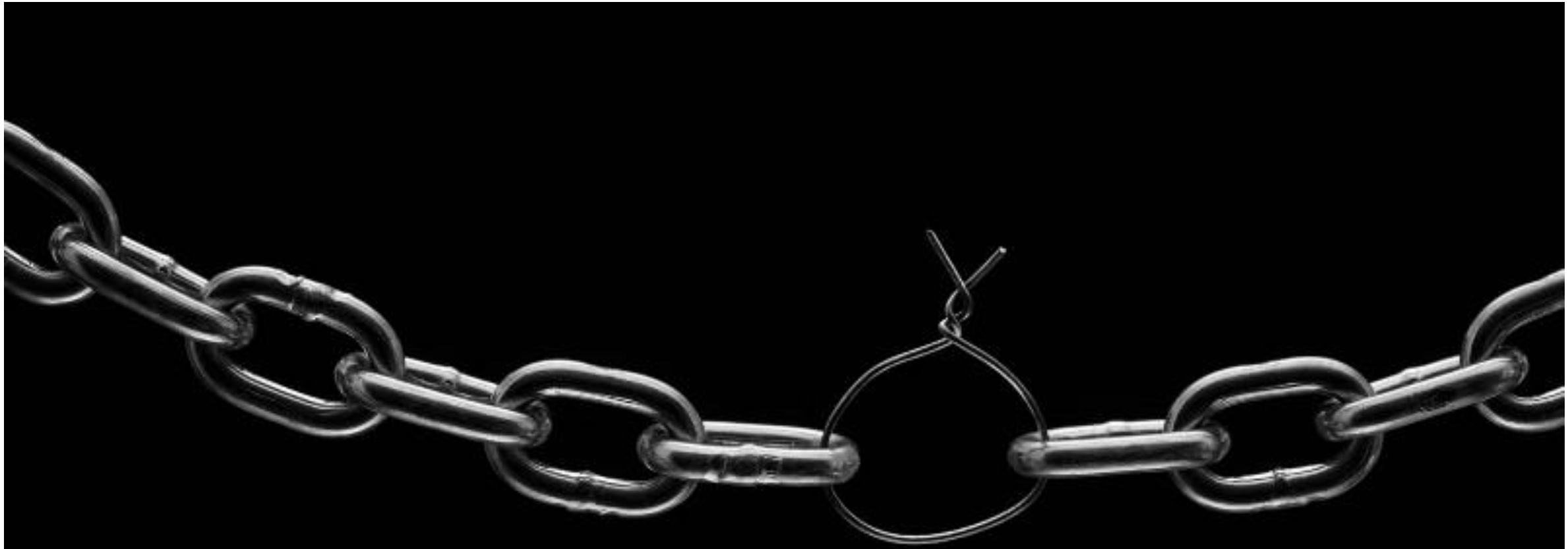
Vice-Président Innovation – Bureau Veritas

BUTTERFLY




ATTACKER

La Cybersécurité n’est pas probabiliste



- Le niveau de sécurité global d’un système repose sur son maillon faible
- La sécurité doit être cohérente sur l’ensemble des composants du système !

La diffusion de l'IoT augmente les surfaces d'attaques et est le vecteur pour atteindre le monde physique

15x

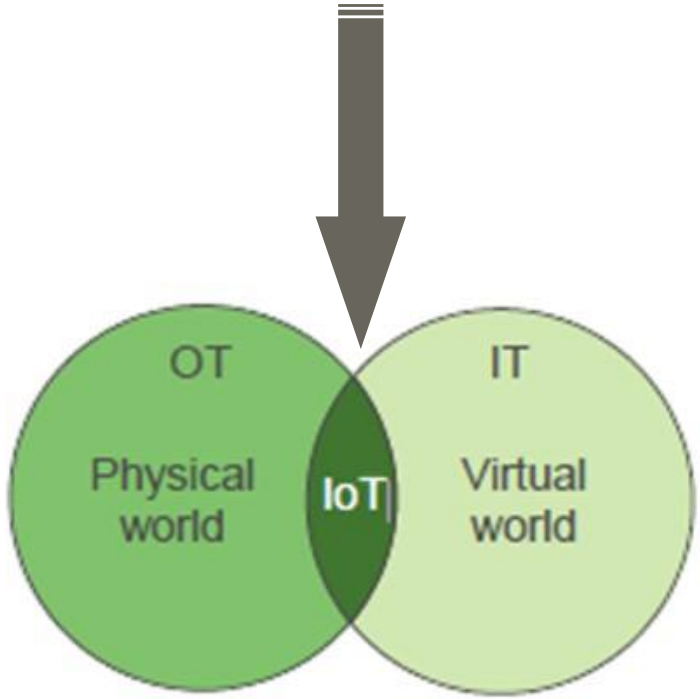
- Les périphériques intégrés sont 15 fois plus vulnérables aux attaques que les points de terminaison d'entreprises traditionnelles. (McAffee)

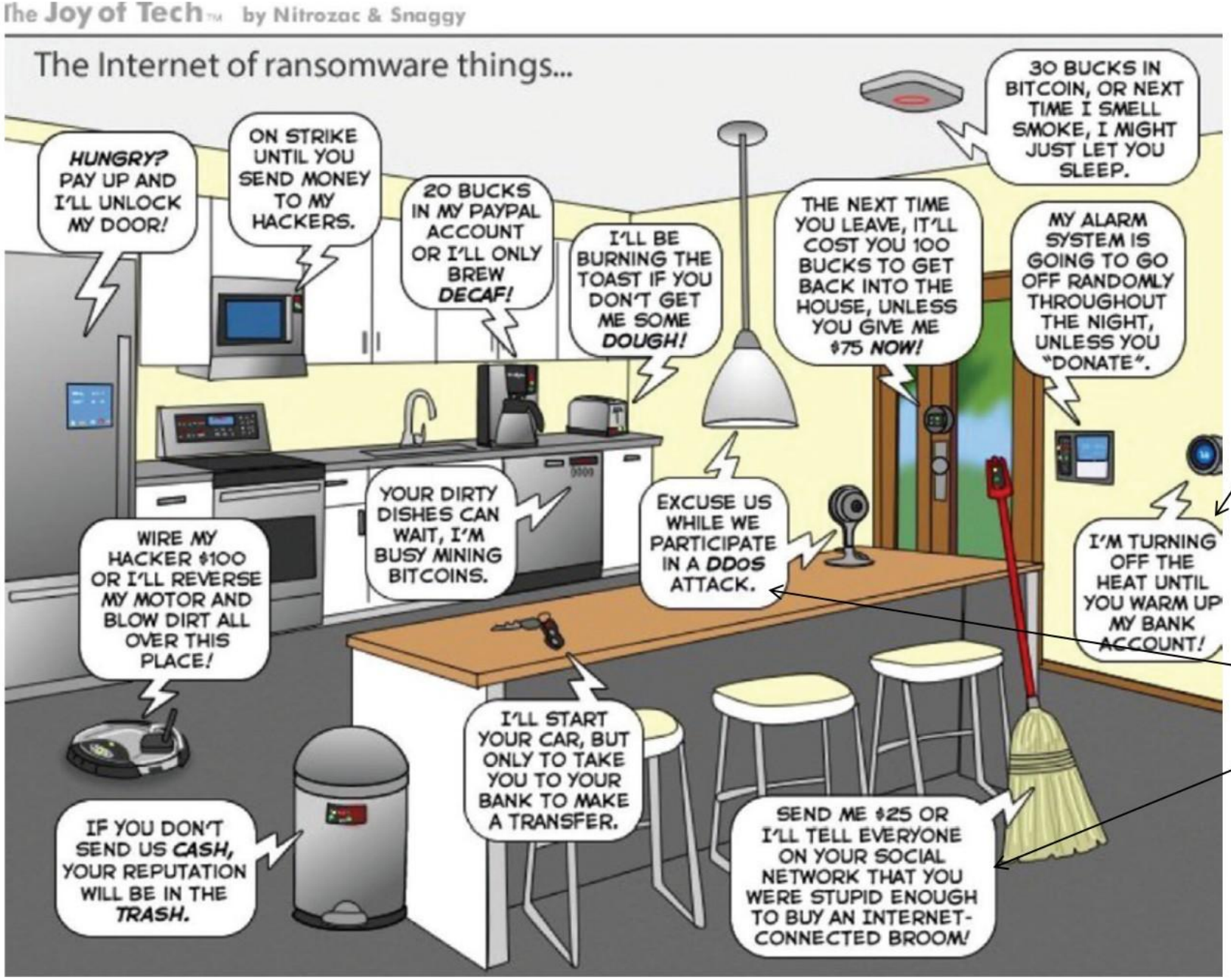
7x

- Augmentation des incidents de cybersécurité IoT sur les infrastructures industrielles et critiques depuis 2015 (CEA, Intel)

70%

- En 2014, environ 70% de tous les IoT devices étaient vulnérables aux attaques (Université Columbia, HP)





Intégrité

Disponibilité

Confidentialité

Source
REE IOT2018

Définition

CYBERSÉCURITÉ :

Ensemble des technologies, des processus et des pratiques conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques & les dommages du cyber espace.

Logiciel

Heartbleed - corruption du protocole de communication de sécurité SSL

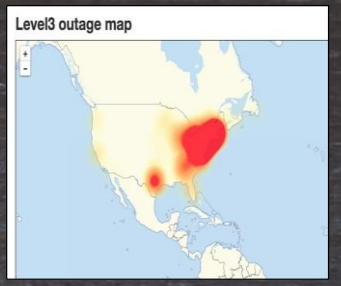
Système

Stuxnet – Propagation d'un virus dans une centrale nucléaire

Matériel

Clef USB corrompue laissée à portée de main

Réseau



Attaque DDOS sur DynDNS

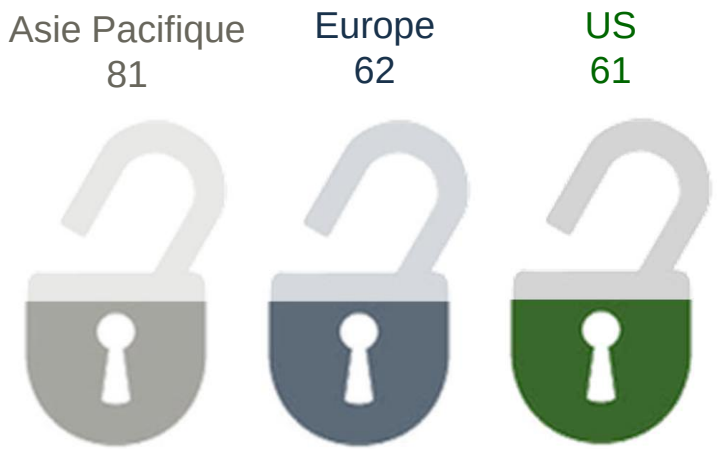
Les vulnérabilités

PRODUIT	VULNÉRABILITÉ / FAILLE (NON EXHAUSTIF)	ATTAQUE(S) CONNUE(S)
Matériel	Pas de durcissement matériel Protection physique	Attaque par canaux cachés, bit flipping, injections matérielles Attaques « cold boot » : extraction de clés par exploitation de la persistance en mémoire vive Attaque « Back door »: ajout de portes "malveillantes" durant la conception
Réseau	Absence de segmentation Mauvaise configuration des équipements de sécurité (firewalls, VPNs)	Déni de service : utilisation de botnets pour générer du trafic (cf. malware Miraï et l'attaque d'OVH) Espionnage des communications chiffrées par compromission des équipements de sécurité (Affaire Equation Group / ShadowBrokers)
Système	Architectures IT/OT non cloisonnées Faiblesse des défenses en profondeur Process de veille et de suivi des mises à jour non défini	Attaque de type Stuxnet sur les systèmes industriels connectés
Logiciel	Interactions non désirées avec le logiciel (élévation de privilège) Non-respect des bonnes pratiques de génie logiciel et de qualité logicielle	Exploitation de bugs à des fins malveillantes (use-after-free, buffer overflows, Injections, Hard Coded passwords, Return Oriented Programming)
Facteur Humain	Négligence matérielle porteuse de virus (Clés USB) Modification involontaire de réglages d'asservissements (mot de passe)	Conséquences sur la qualité des produits, services délivrés, l'environnement, la santé ou la sécurité des personnes.

Les risques pour l'entreprise

Risques	Description
Dommages matériels / Corporels	La modification des configurations nominales des installations peut provoquer des dégradations physiques avec le plus souvent des conséquences matérielles – mais parfois aussi humaines
Perte de chiffre d'affaires	L'interruption de la production génère des manques à gagner importants. La modification de paramètres de fabrication conduisant à des produits non conformes génère des coûts importants.
Vol de données	Perte de secret de fabrication, contrefaçons, avantage pour la concurrence
Impact sur l'environnement	La défaillance du système suite à une prise de contrôle malveillante peut générer un dysfonctionnement des installations (ouverture de vannes de produits polluants) et provoquer une pollution du site et de son environnement. Un tel incident s'est produit en Australie ces dernières années.
Responsabilité civile / pénale - Image et notoriété	L'indisponibilité du service comme la rupture de distribution d'électricité ou d'eau, ainsi que la fourniture de produits défectueux mettant en danger le consommateur peuvent aboutir à des poursuites pour les dommages occasionnés ou simplement dégrader l'image de l'entreprise (la satisfaction du client et sa confiance).

- Pertes de CA dues aux cyber- attaques (en Millions $)



Le cycle de la sécurité

Anticiper et Prévenir

- Analyse des risques (identification des périmètres)
- Gouvernance de la sécurité
- Systèmes d'information et de gestion des risques
- Prévention des vulnérabilités

Protéger

- Sécurité du Data Center
- Sécurité de l'IoT
- Sécurité des Mobiles
- Sécurité des Applications
- Sécurité du Réseau

Contrôler - Détecter - Réagir

- Assurer la continuité du service
- Détecter les comportements anormaux
- Déclenchement de contre-mesures
- Gestion du Centre Opératoire de Sécurité
- Gestion des mises à jour

Evaluation tierce partie : Revues de code – Essais de sécurité – Gestion de la documentation

La cybersécurité tout au long de la supply chain

	TOE	Conception (Ingénierie & constructeur)	Intégration de système (Systémier/Intégrateur)	Production (Fabricant)	Exploitation (Exploitant)
Analyse de risques Identification des biens à protéger	Hardware / Matériel	• Security by Design • Analyse de la conception • Tests des interfaces physiques et de communication • Durcissement des composants	• Tests des interfaces physiques et de communication (BV-HW-XXX)	• Suivre règle d'utilisation	
	Système / Réseau	• Définition d'architecture / réseau adapté • Segmenter le réseau	• Concept Secure by Design • Evaluation des COTS • Système de détection d'intrusion	• Additional class notation SYS-COM	• Gestion des logs • Gestion des incidents
	Cloud / Données		• RGPD • Privacy by design	• RGPD	• RGPD • Move Forward With Privacy
	Système d'exploitation	• Utilisation d'OS sécurisé	• Paramétrage système d'exploitation • Mettre en place une Gestion des accès logiques	• Suivre règle d'utilisation • Appliquer politique de MdP	• Gestion des mises à jour
	Application Software	• Concept Secure by Design • Bonnes pratiques (BV-SW-200 Conception) • Analyse du code source • Test boite blanche	• Paramétrage correct de l'application • Utilisation selon recommandations constructeurs • Mettre en place une Gestion des accès logiques		• Gestion des mises à jour
	Personnes & Procédures	• SMSI • ISO 27k	• SMSI • ISO 27k	• SMSI • ISO 27k	• SMSI • ISO 27k

Etat des lieux

Pourquoi ?

Confidentialité

Intégrité

Disponibilité

Quoi ?

Produit / (device)

Système/Réseau

Cloud /Data

Applications

Personnes

Quand ?

Identifier

Protéger

Détecter

Réagir

Remédier

Qui ?

Concepteur

Fabricant

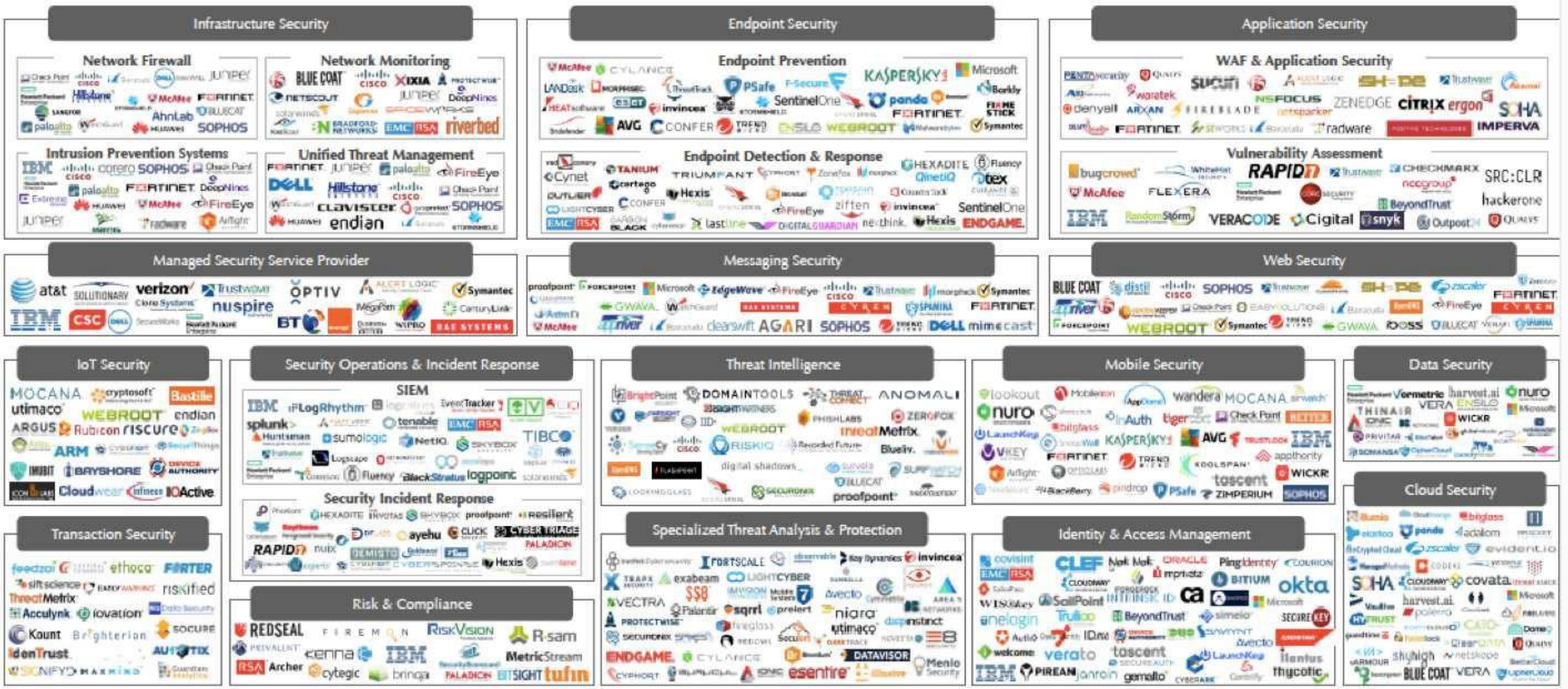
Intégrateur

Opérateur/exploitant

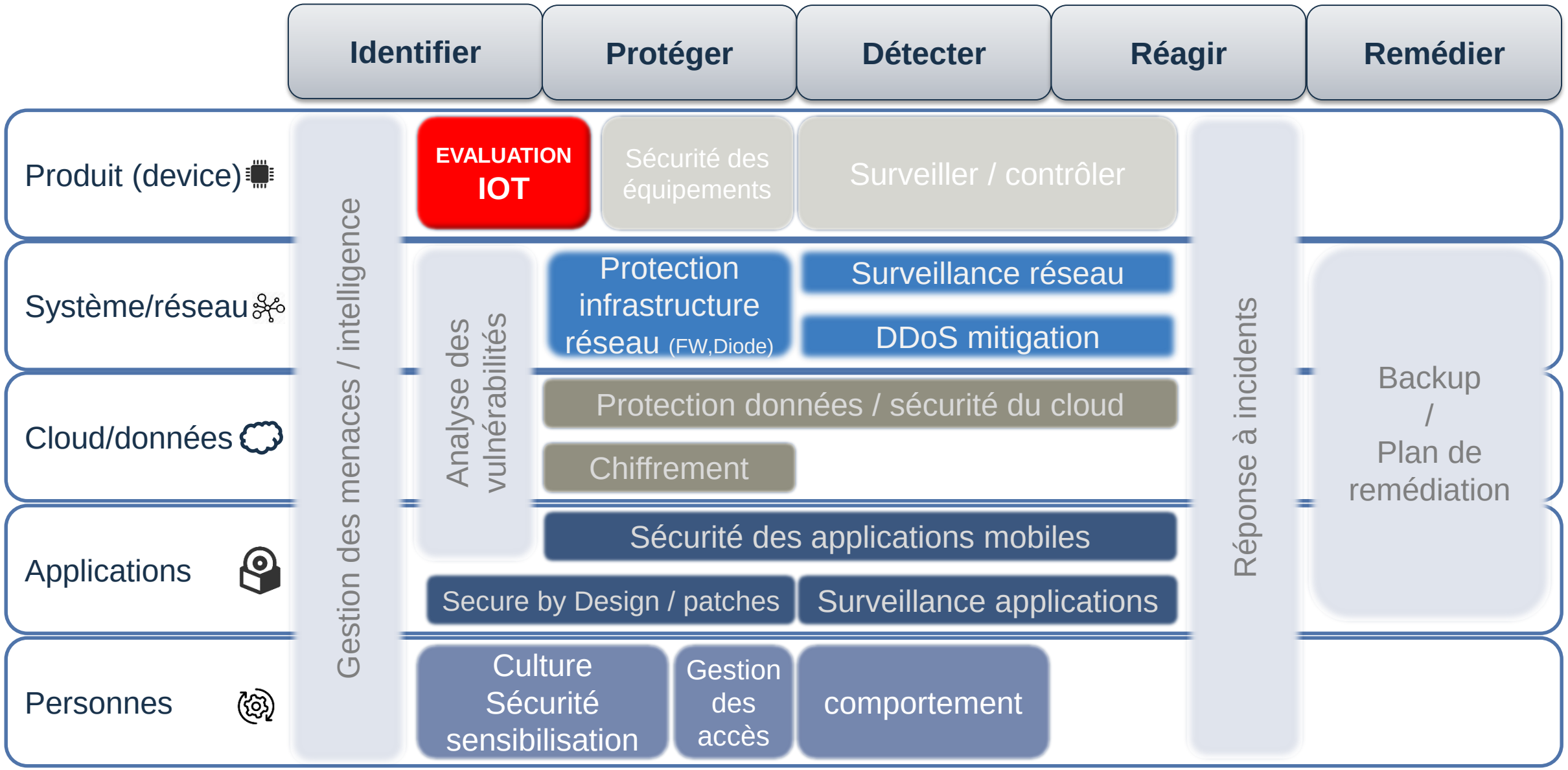
Service de confiance

…

Le marché de la cybersécurité est actif



Offre de services



Questions ?

BUREAU VERITAS

LÉGISLATION ACTUELLE & RÉFÉRENTIELS EXISTANTS

Laurent Midrier

Vice-Président Innovation – Bureau Veritas

Les trois directives clefs en Europe

Directive on security of network and information systems (NIS Directive)

Security | Août 2016

Appliquée aux opérateurs économiques essentiels qui exploitent les infrastructures critiques

- énergie,
- transport,
- bancaire,
- santé
- services numériques
- ... *

Ces entreprises sont tenues de se conformer aux normes minimales de cybersécurité et de notifier les incidents graves

Cibler les industriels / opérateurs et sociétés de services

"Cybersecurity act"

Security | Fin 2018

- Concerne tous les produits vendus dans l'UE
- Demander la certification du produit avec 3 niveaux
- Devrait compléter le marquage CE avec une évaluation spécifique de la cybersécurité

Fabricants d'appareils cibles

General Data Protection Regulation

Security | Data privacy and compliance | Mai 2018

- Appliquée à toutes les entreprises traitant avec les citoyens de l'UE. Données de mai 2018
- Traite de la protection des données personnelles et de la conformité
- Demande une "sécurité par conception" pour tout type de services traitant des données personnelles et d'une organisation spécifique
- Demande des processus spécifiques en cas de violation de données
- Forte amende en cas de non-conformité

Cibler toutes les entreprises

Tendances : EU / échelle / certification

Coopération européenne, certifications, contre-attaques : l'ANSSI expose ses ambitions au FIC 2018

L'Agence nationale de la sécurité des systèmes d'information a fait le point sur ses dossiers en cours à l'occasion du forum international de la cybersécurité (FIC) de Lille. L'occasion pour son directeur général Guillaume Poupard d'exposer ses ambitions en matière de coopération européenne, de certification des produits et acteurs de la cybersécurité, mais aussi de pouvoir agir auprès des fournisseurs de services numériques pour prévenir ou court-circuiter des attaques.

L'USINE DIGITALE

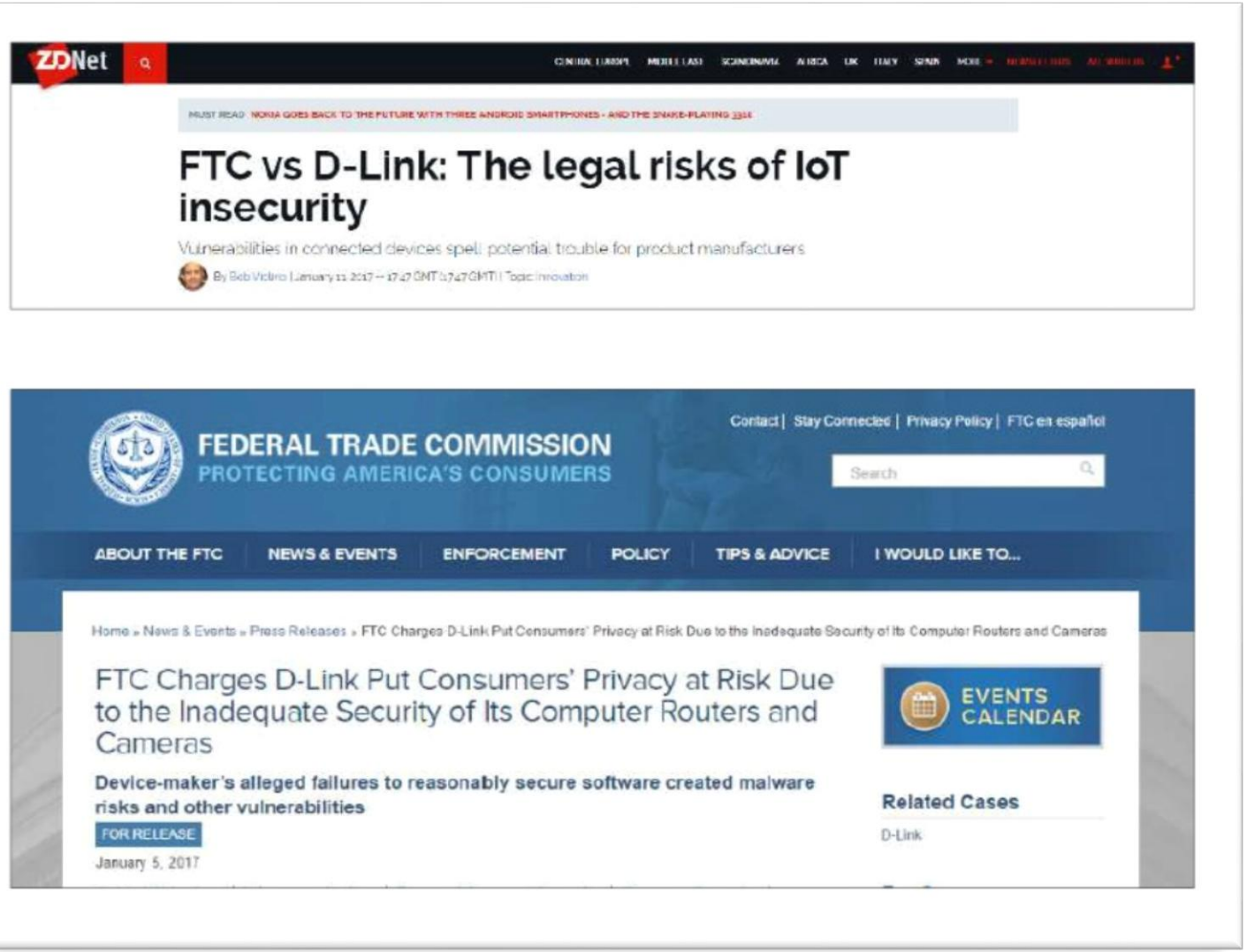
24 janvier 2018

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

31 octobre 2017

Pour Philippe Blot, au niveau européen 300 à 400 produits seraient certifiés chaque année ce qui est insuffisant. C'est pour cela que l'approche européenne avec l'aide de bureaux certificateurs du monde privé comme Bureau Veritas ou le CNPP, pourrait être précieuse. En effet, ces organismes pourraient certifier les produits qu'ils évaluent déjà sur d'autres domaines. Ces certifications seraient plus automatisées avec des bancs de tests et un processus plus légers nécessitant seulement une « dizaine d'hommes jours » pour obtenir une certification.

La sécurité générale des produits



- La responsabilité du fait du produit (product liability) :

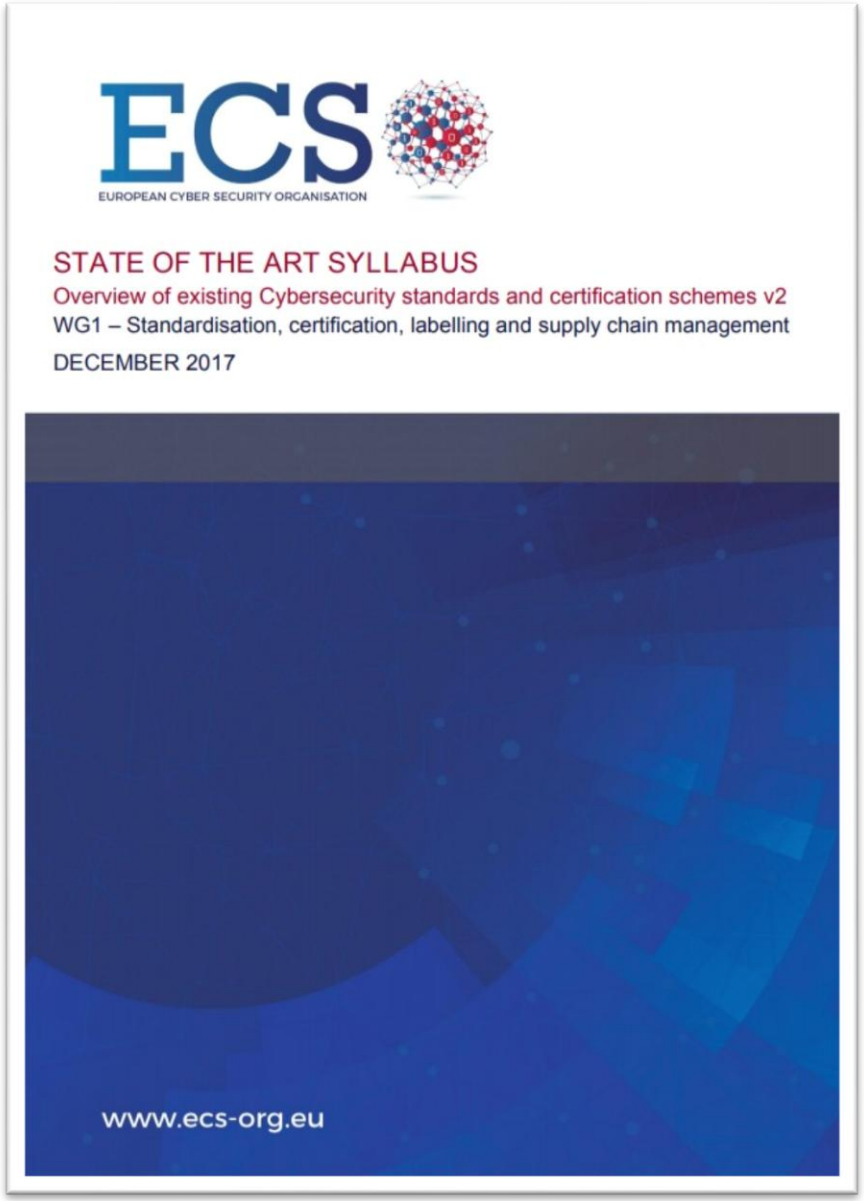
Un produit est défectueux lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre

… la cybersécurité fait partie de la sécurité

Le fabricant /importateur est responsable de cette sécurité en particulier pour des failles connues

Base de données CE de vulnérabilité connue CVE.mitr.org

Les référentiels existants



Produits / composants
- Smart grid
- ICS
- …

Services / organisations
- Général
- Banque / assurances
- Services de confiance

Personnes
- Personnels de sécurité

Technologies
- Cryptographie
- Signature
- Protocoles
- …

Référentiels existants

Certification

IEC 27001
IEC 62443
CSPN / Critères communs

Normes

Générique (IT)
ISO / IEC 2700, …
Cyberessential
EBIOS (ANSSI)

Industrie (OT)
Série IEC 62443
Guides ANSSI

Normes domaine Energie & Nucléaire
- IEC 62645
- AIEA NSS17
- IEC 62351

Normes domaine Automobile
- IEC 26262 (Safety)
- XXX (à venir)

Normes domaine Marine
- Série IEC 61162-450/460

Gouvernance
Produit (device)
Réseau / Infra

Today Vs Tomorrow

AUJOURD'HUI

Applications hautement critiques

Process de certification à long terme

Cas par cas

DEMAIN

Applications standard

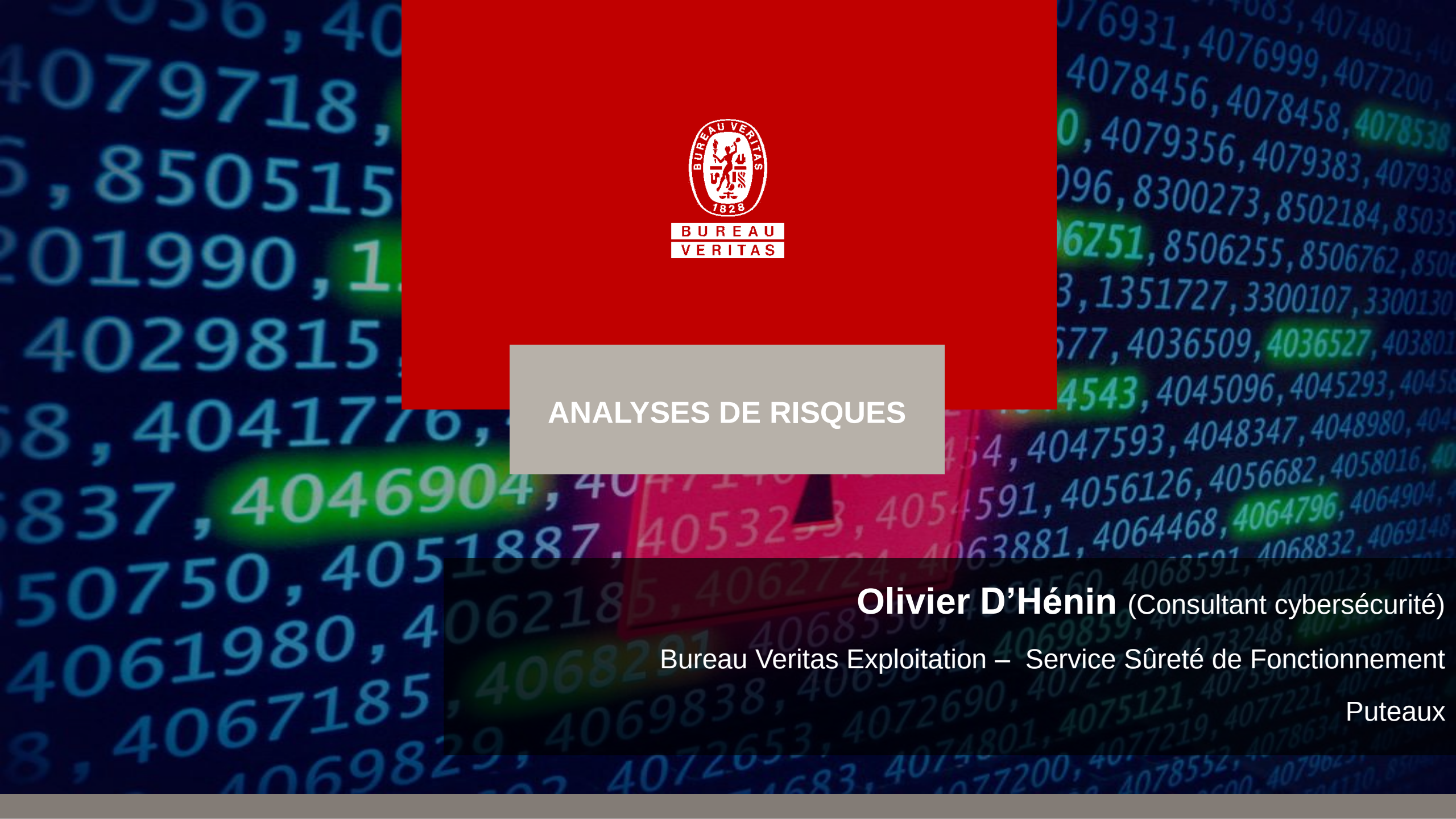
Possibilité de spécifier le niveau de sécurité pour chaque composant

Approche holistique

- matériel + logiciel
- fiabilité + sécurité

Questions ?

BUREAU VERITAS



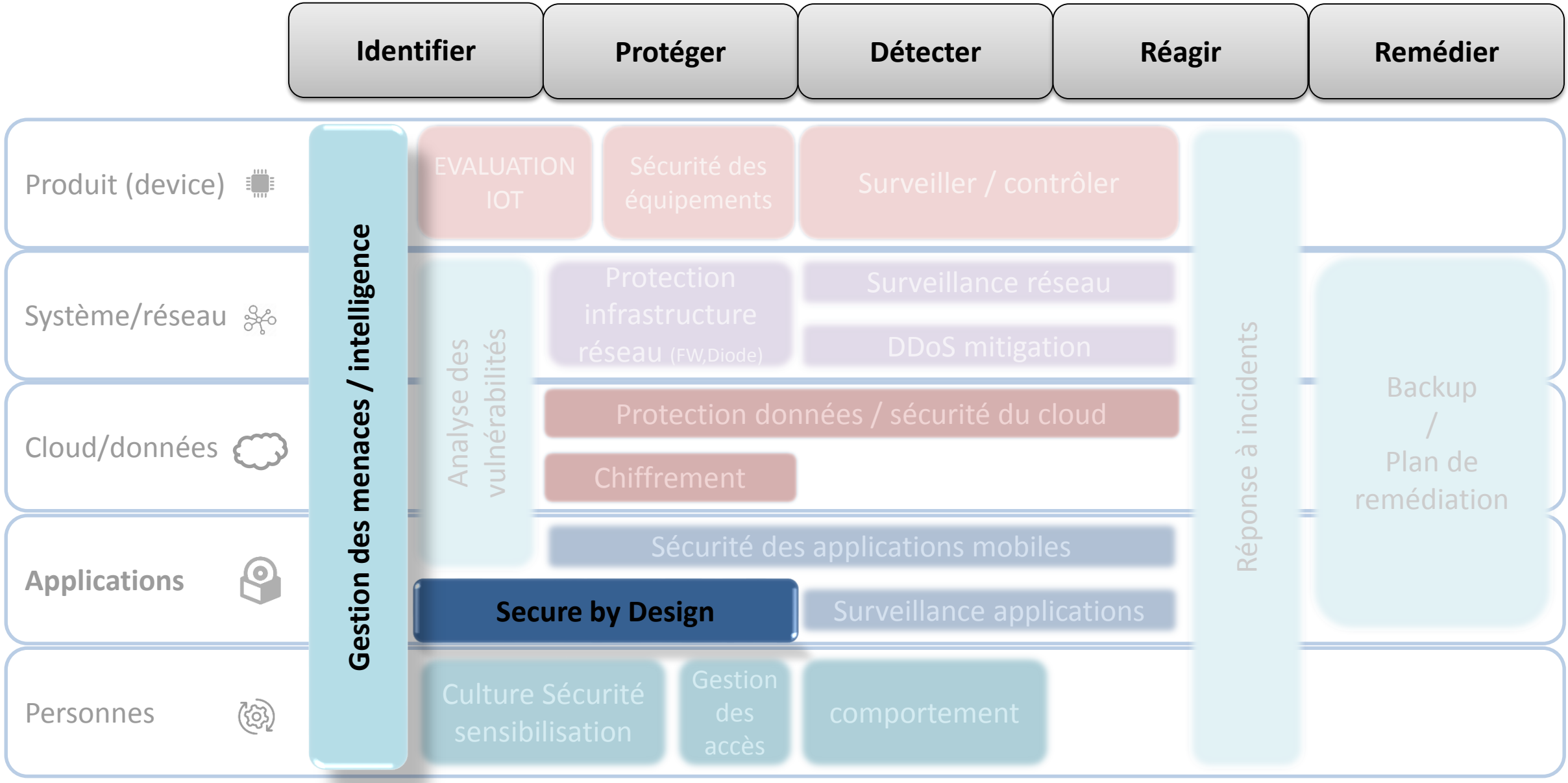
ANALYSES DE RISQUES

Olivier D'Hénin (Consultant cybersécurité)

Bureau Veritas Exploitation – Service Sûreté de Fonctionnement

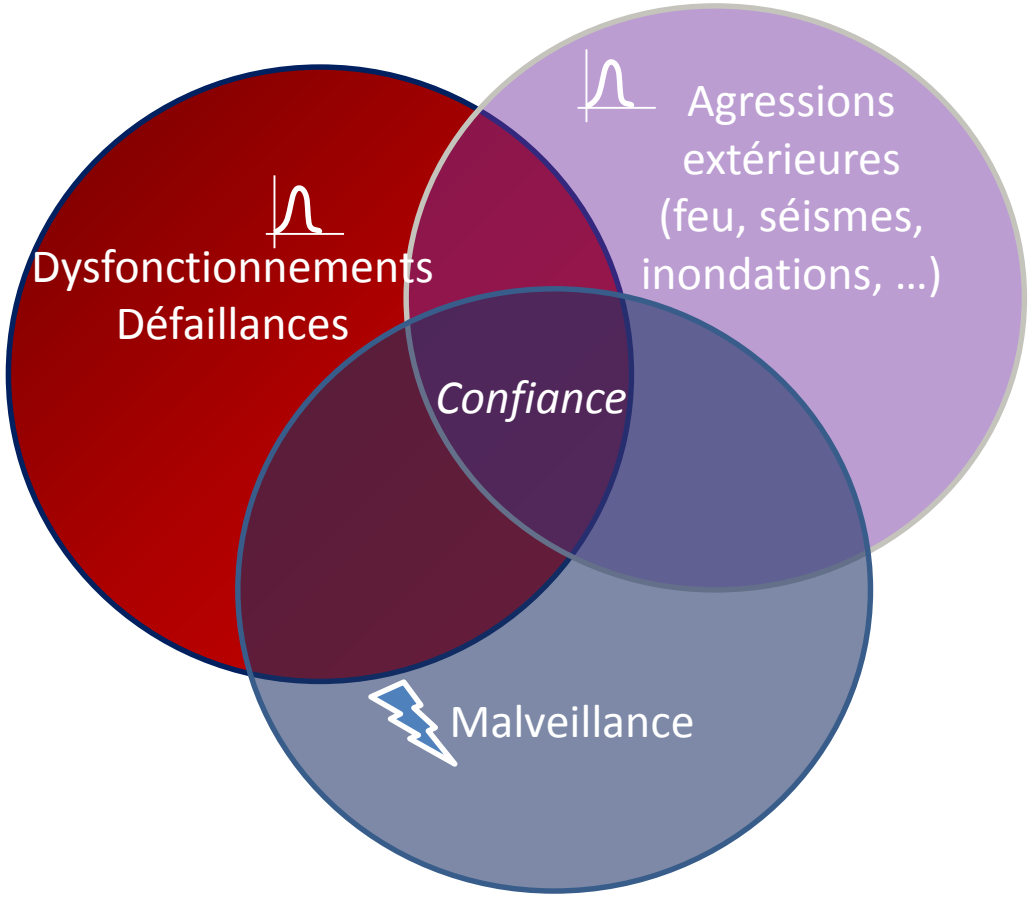
Puteaux

1. Le périmètre de la Cybersécurité



No Safety without Security, reversely

SDF / Cyber ont un but commun :
confiance



Pour le **logiciel**, les deux démarches vont s'accorder :
Qualité, traçabilité, maitrise des développements, tests type boite blanche, etc.

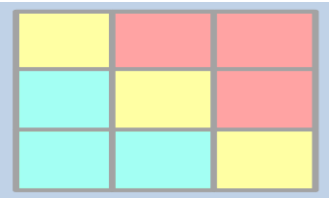
Mais certains concepts sont en opposition :

Sureté de fonctionnement (Safety)	CyberSecurity
Quête de la stabilité	Problématique des patches
Quête de la performance	Certains mécanismes cyber peuvent ralentir les traitements
Quête de la Simplicité	L'ajout de mécanismes cyber peut compliquer la qualification
Quête de l'accessibilité	Limiter les accès (besoin d'en connaitre)

Analyses de risques

Analyse de risques - généralités

- Le BUT
  - La base : Estimer un risque à partir du produit Probabilité x Impact
  - Identifier : Identifier et quantifier les risques, puis les hiérarchiser par niveau de criticité
  - Gérer le risque : Accepter / Réduire / Eviter / Transférer



- Référentiel cyber
  - C'est l'ISO 27005 qui adresse le sujet des analyses de risques sans toutefois préciser le « comment »
- Méthodes
  - Méthode « maison »
    - Outil Excel et déploiement des concepts de l'ISO 27005
  - EBIOS
    - Expression des Besoins et Identification des Objectifs de Sécurité
    - Méthode élaborée par L'ANSSI et le Club EBIOS / Dernière version : 2010

Analyse de risques –

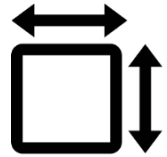
- Mener une analyse de risques

  - PRODUIT / SYSTÈME / APPLICATION / INFRASTRUCTURE / ACTIVITES

  - Garder en tête l’objectif : Mettre en place des mesures efficaces pour réduire le risques.

  - La plupart des valorisation étant qualitatives, il est nécessaire d’impliquer plusieurs intervenants (de plusieurs horizons) pour obtenir une valorisation pertinente et consensuelle.

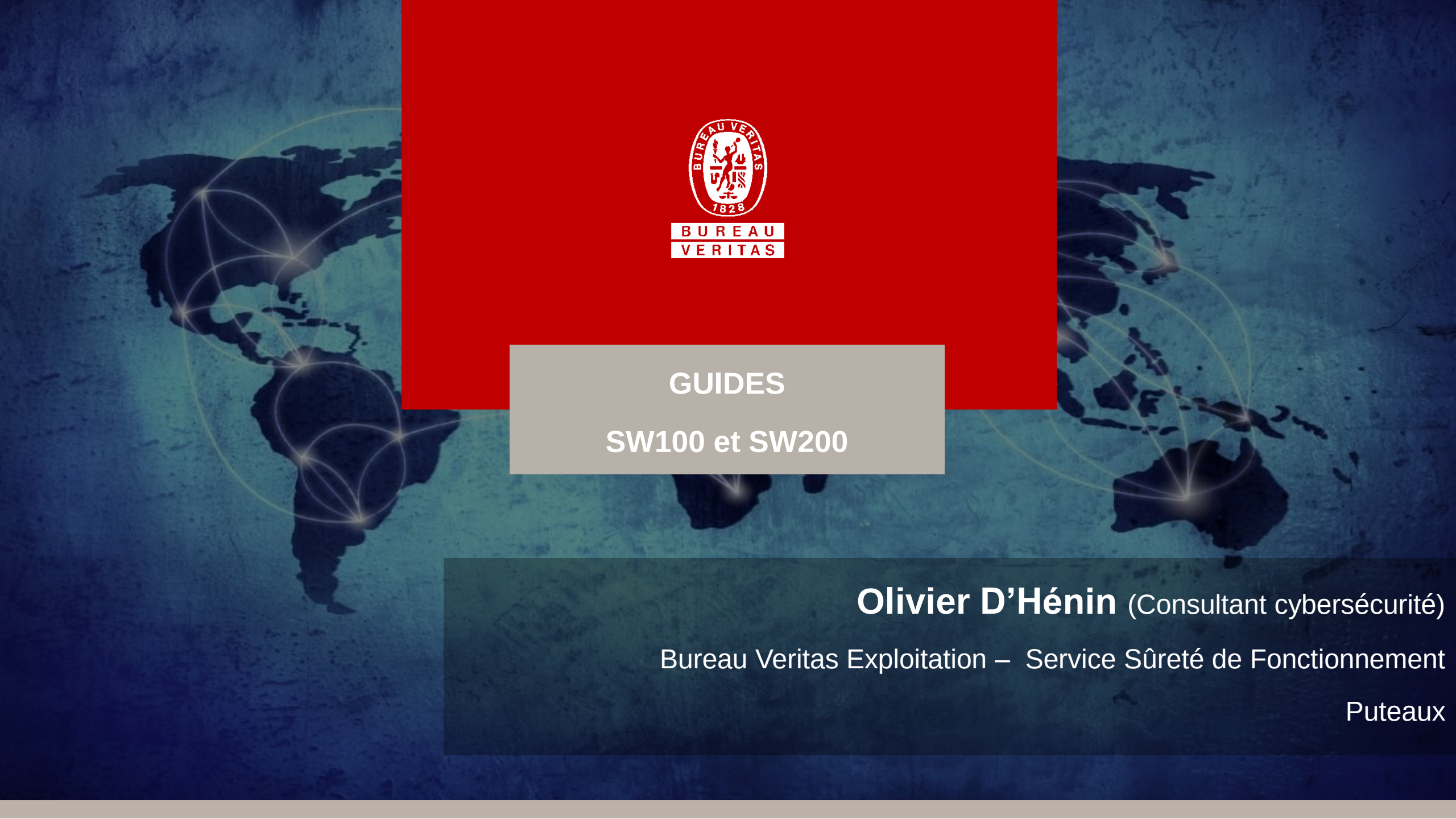
  - Impliquer/informer le porteur du risque (propriétaire du risque)



Analyse de risques – Ebios

- Avantages :
  - Méthode Reconnue
  - Plus ou moins adaptable
  - Bien cadrée
  - Bien documentée.
    https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

- Inconvénients / Limites:
  - Lourdeur
    - Temps a passer à mener l'analyse
    - Manque de vision Synthétique
  - Manque d'outillage (gratuit / libre)
  - Pas adaptée pour de la conception d'architecture (l'analyse porte sur de l'existant)



GUIDES

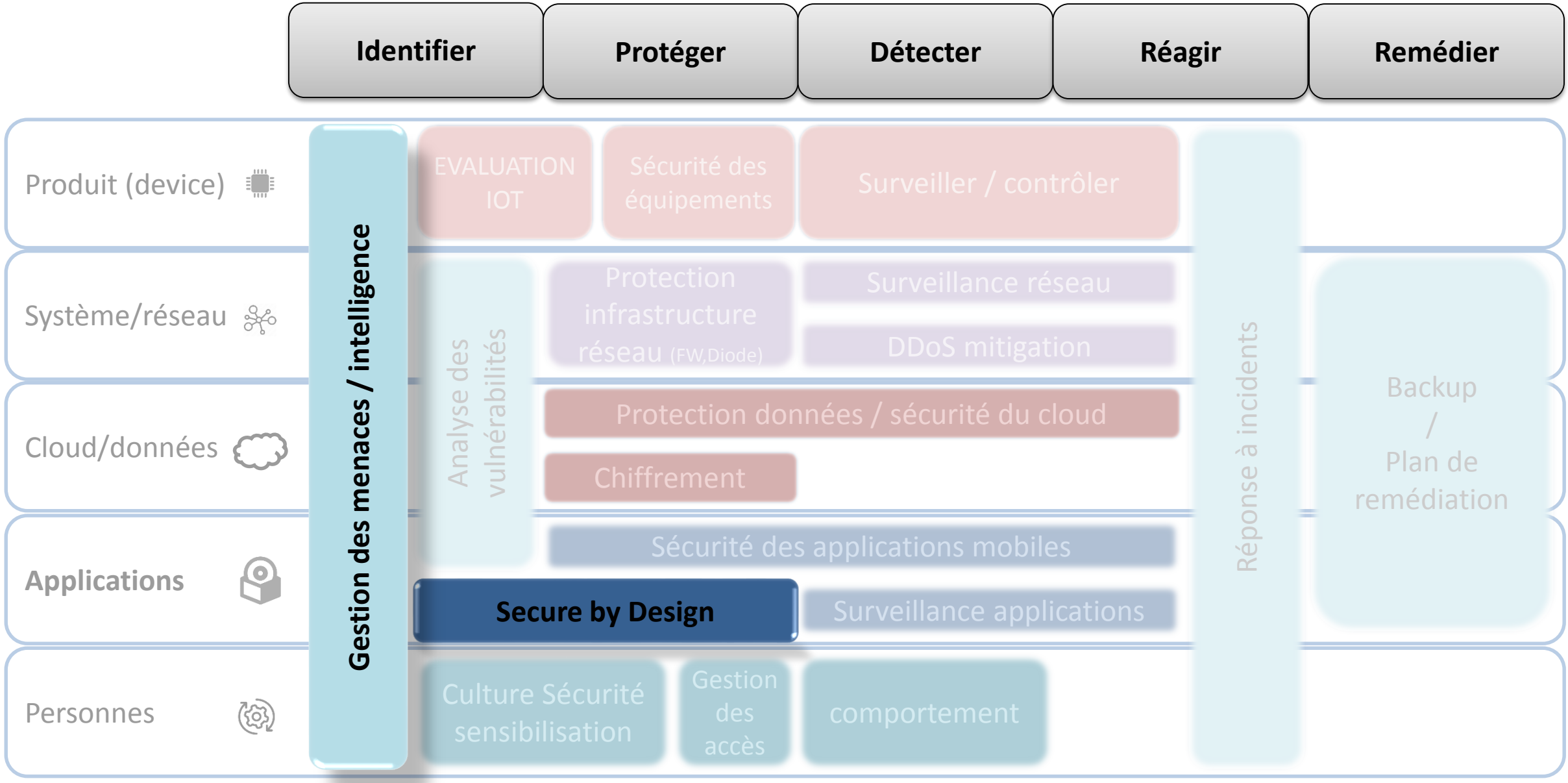
SW100 et SW200

Olivier D'Hénin (Consultant cybersécurité)

Bureau Veritas Exploitation – Service Sûreté de Fonctionnement

Puteaux

1. Le périmètre de la Cybersécurité

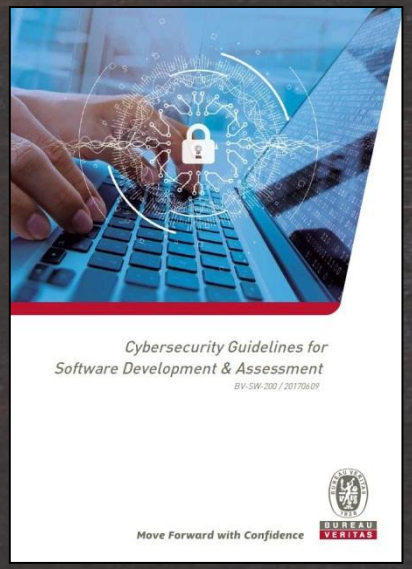


1. Guides BV

Pourquoi ces guides ?

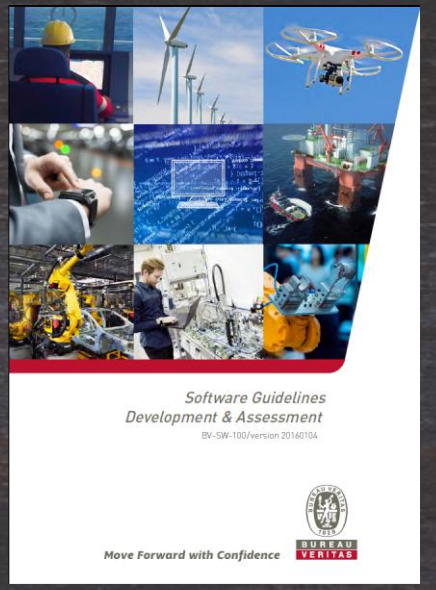
Attente clients :

- Difficulté à appréhender l'ensemble des standards de cybersécurité / sureté de fonctionnement.
- Aucun standard ne traitant spécifiquement du sujet du Logiciel (informations disséminées).



BV-SW200
Cybersécurité des développements logiciels

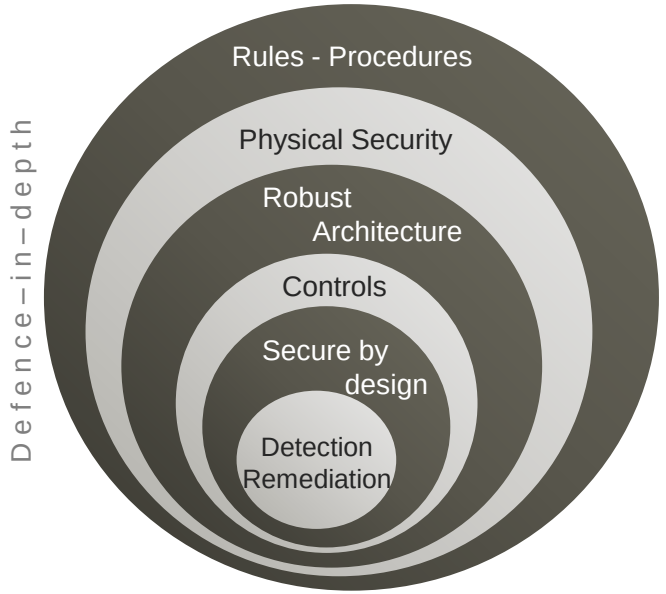
BV-SW100
Développements de logiciels sûrs



Approche graduée

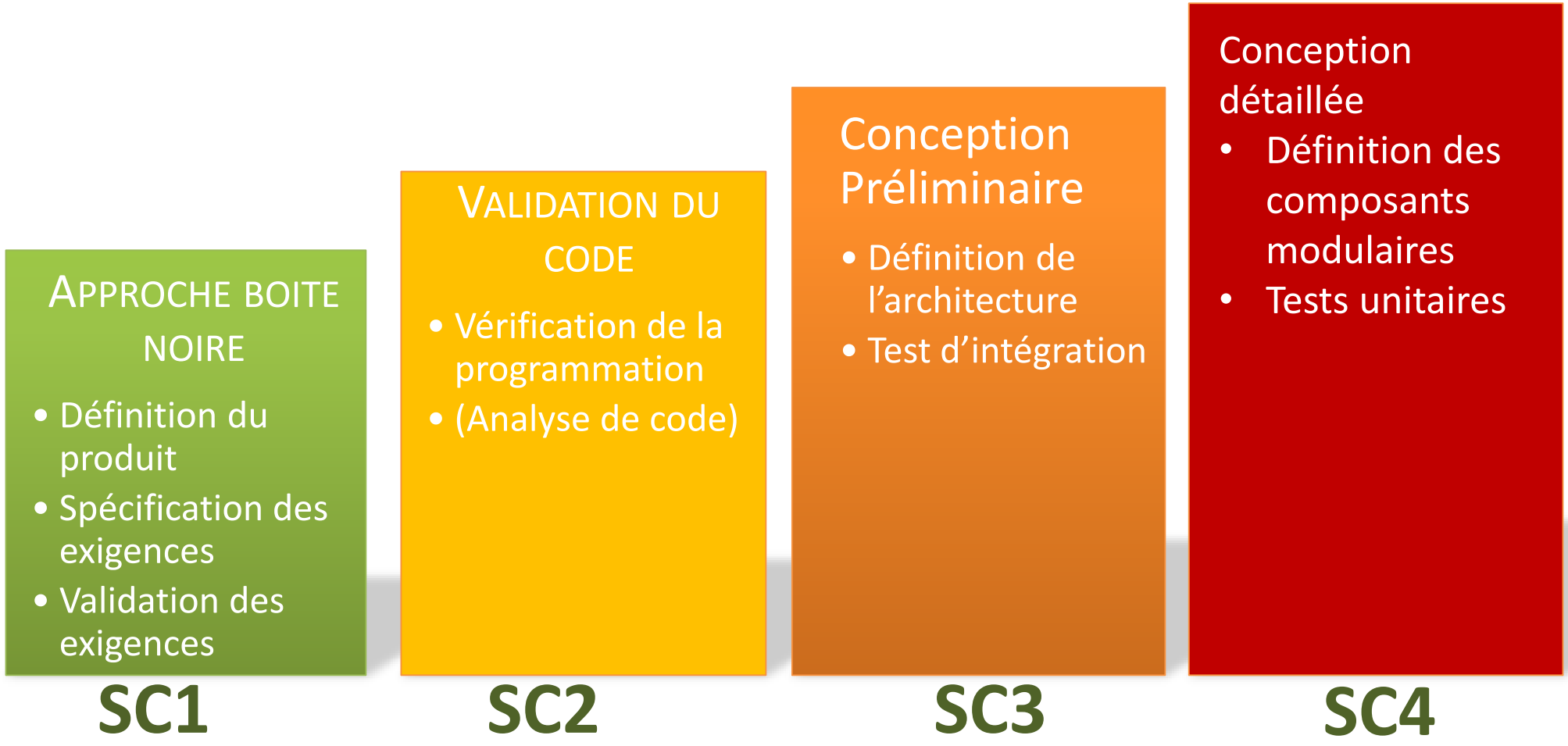
Suis-je obligé d'appliquer le concept du SECURE by DESIGN:

- **Défense en profondeur :** le concept de défense en profondeur signifie que les divers composants d'une infrastructure ou d'un système d'information ne font pas confiance aux autres composants avec lesquels ils interagissent [(1)].
- **Approche par niveau :**
  - 4 niveaux pour le BV SW100 (Safety) SC1 à SC4
  - 2 niveaux pour BV SW200 (cyber sécurité) SC0 à SC1

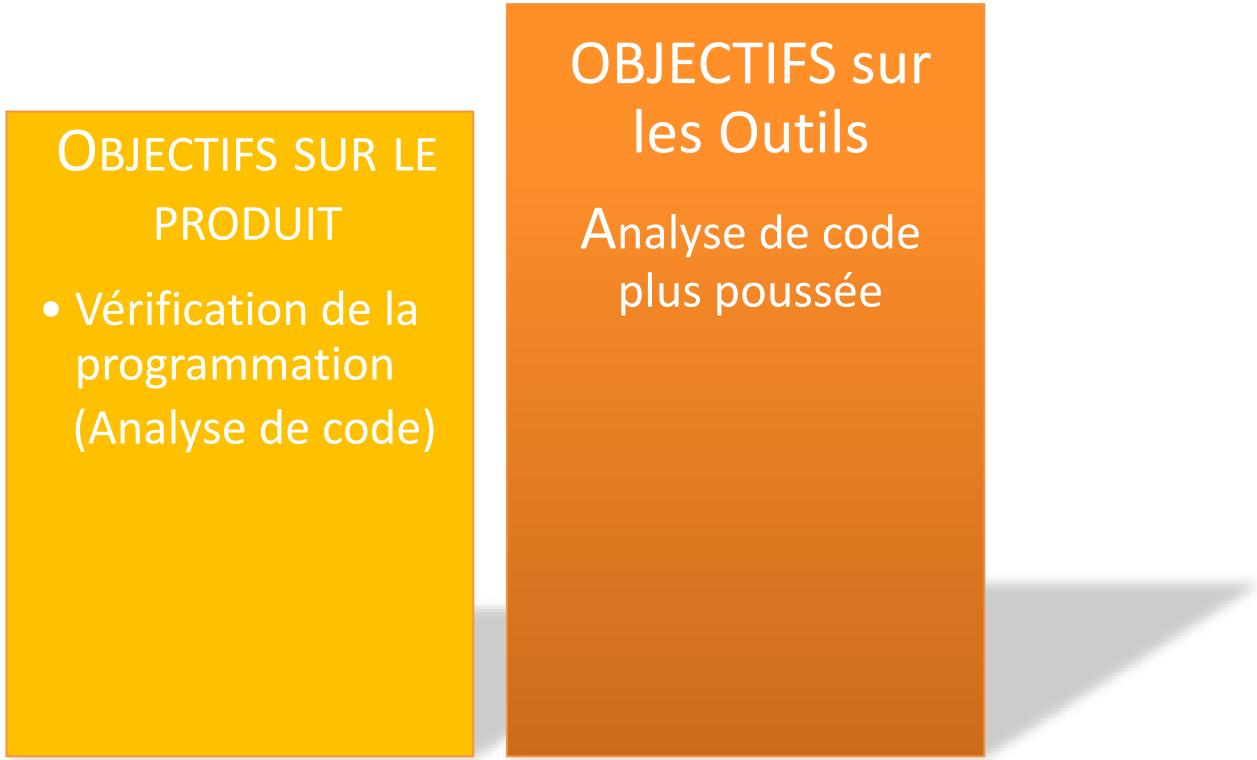


(1) : wikipedia

Les 4 niveaux du BV SW100 (Safety)



Les 2 niveaux du BV SW200 (Cyber)



Security Categories….

Analyse statique de code / Analyse des menaces

ANALYSE STATIQUE DE CODE

- **1 Pierre 2 coups :**

  L' analyse de code est efficace pour tracker les défaillances logicielles (**Safety**) et identifier certaines vulnérabilités (**Cyber**).

- **Frama- C :**

  Supporté par le CEA-List (Saclay)

ANALYSE des MENACES

- **STRIDE :**

  SPOOFING, TAMPERING, REPUDIATION, INFORMATION DISCLOSURE, DENIAL of SERVICE , ELEVATION of PRIVILEGES

Le contenu des guides

Présentation des Objectifs

- **Notation : ex: OBJ_COTS_040.**
- **Objectifs typés :**
  - **TOOLS_ ,** (sur outillage)
  - **DES_ ,** (sur le Design)
  - **DEV_,** (sur le développement)
  - **COTS_,** (sur l'intégration de logiciel tiers)
- **Critères d'acceptations :**
  - Ce qu'il faut mettre en œuvre pour satisfaire l'objectif.

CONCLUSION sur les guides

- **BENEFICES**
  - Aide aux développeurs
  - Accompagnement par BV dans votre démarche
  - ATTESTATION de CONFORMITE
- **Téléchargeables GRATUITEMENT**
  - Suffisamment génériques pour être applicables à tous les domaines
  - Votre retour (REX) nous est précieux.

Questions ?

EBIOS : Expression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité –
Expression of Needs and Identification of Security Objectives

Created by the ANSSI

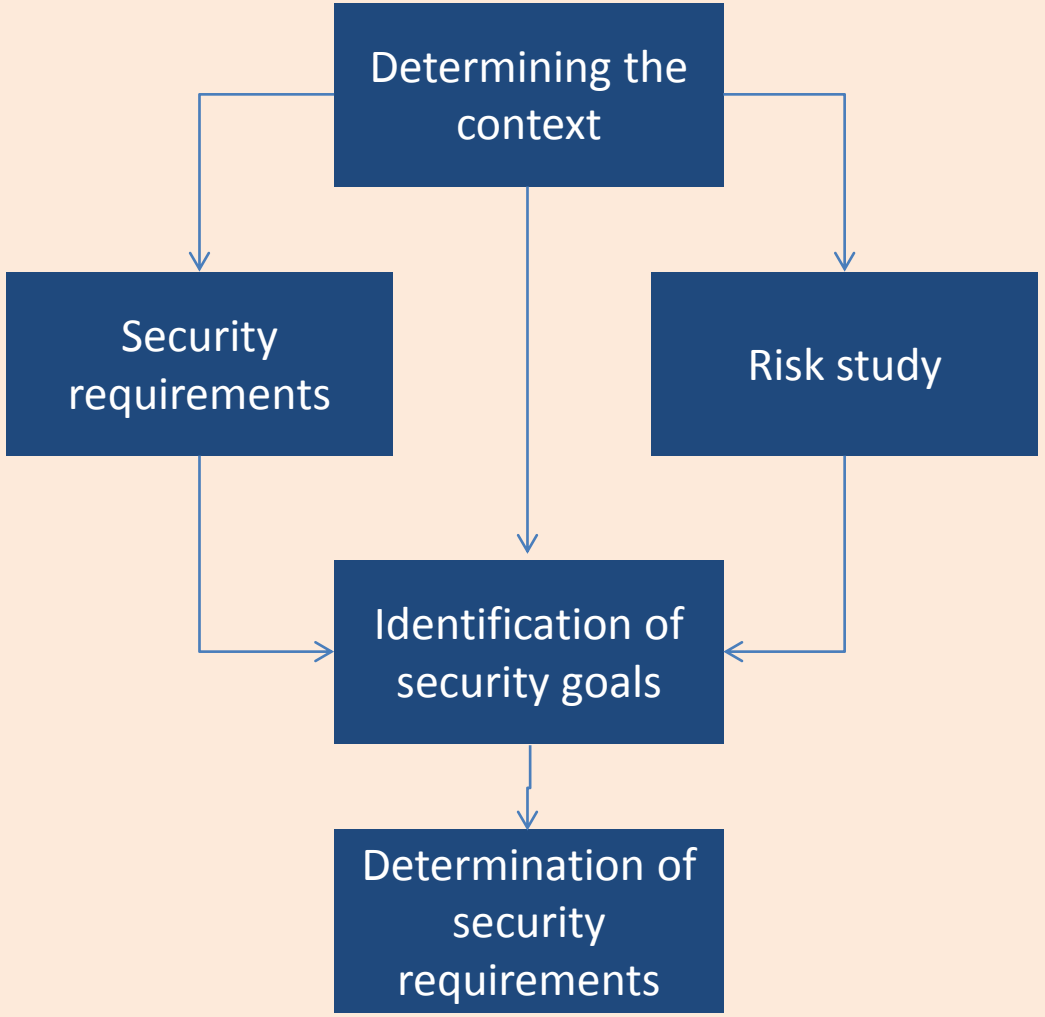
Method to evaluate risk related to information systems

- allows determining a security policy adapted to the risk
- Specifies security actions

The objective are to

- assess and prepare for possible future situations and identify
- respond to deficiencies.

The risk analysis is a base for our security service



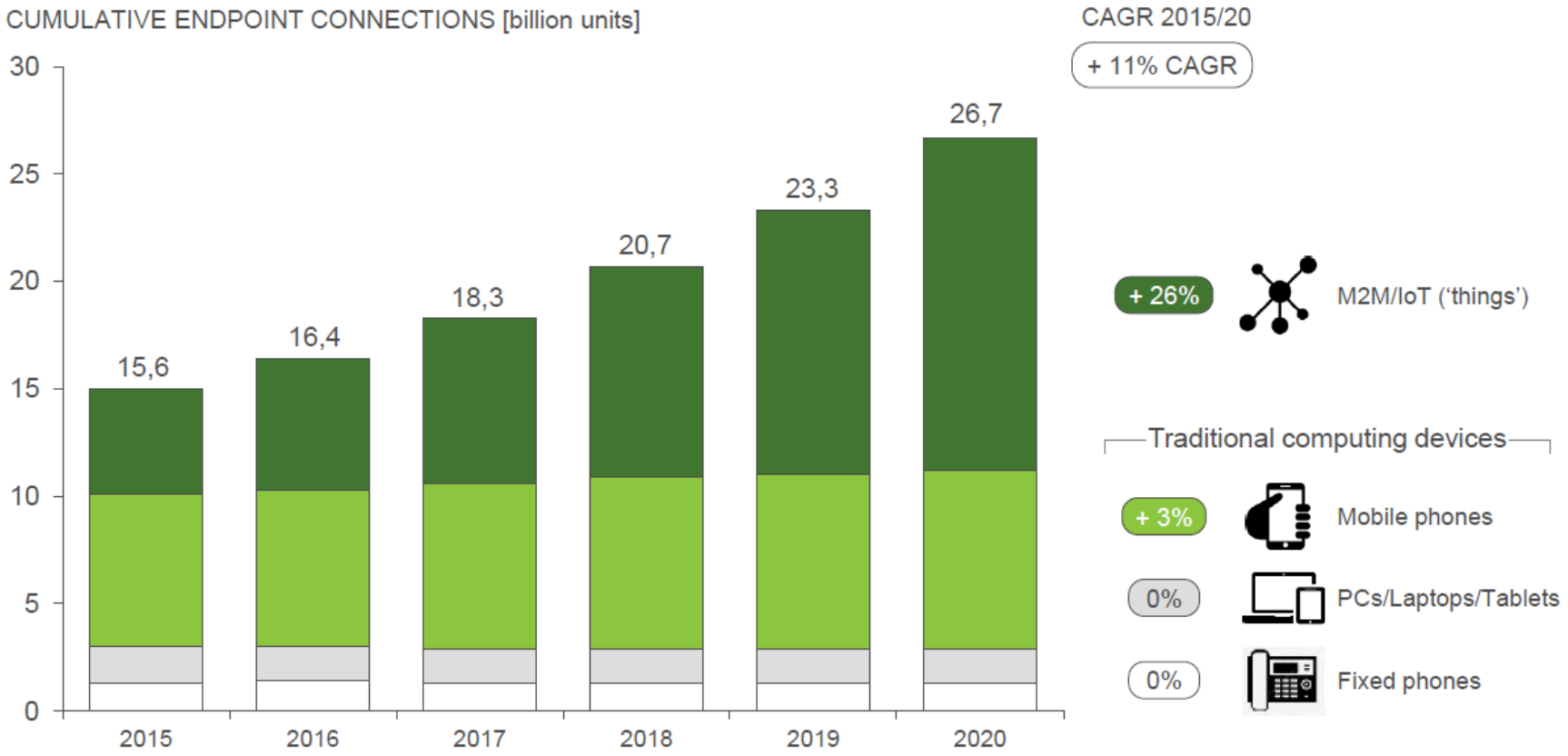
LES ATTAQUES PAR INTERFACES OU CANAUX DE COMMUNICATION

Philippe SISSOKO

Directeur des Opérations LCIE Bureau Veritas

Plus de 70% de tous les appareils IoT seront connectés en utilisant une technologie à courte portée d'ici 2020.

Part des connexions M2M / IoT par type de connectivité, 2015..2020



Un potentiel en plein essor

- Sécurité
- Logistique
- Mobilité à tous les niveaux
- Automobile
- Lecture automatique du compteur d'électricité
- Dispositifs médicaux connectés

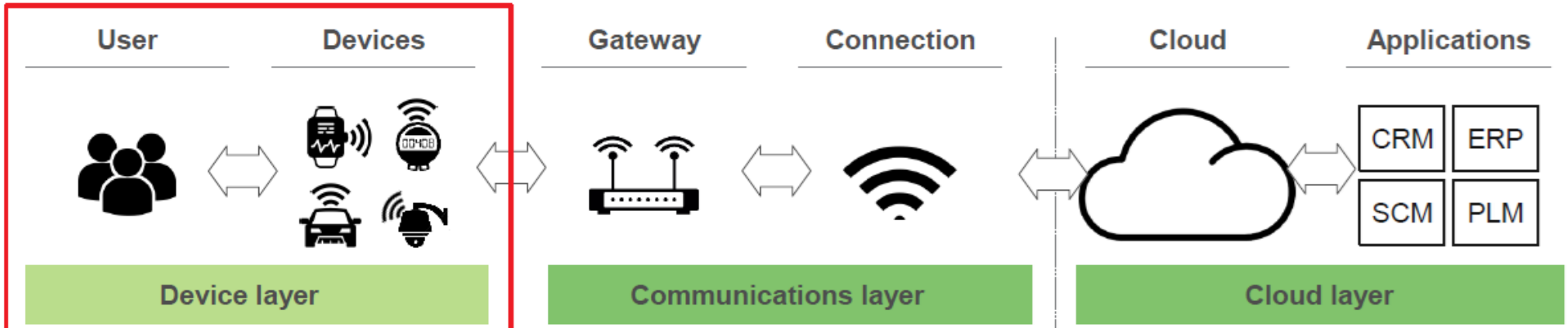
Les plus grands segments nécessitent des technologies sans fil autres que cellulaires

- Appareils électrodomestiques
- Domotique
- Compteurs intelligents
- Energie & Automation

Sources: Machina Research (2014), Ericsson (2016), HIS (2014), Gartner (2015) + SBEM analysis

Combler l'écart de sécurité de l'IoT ...

LETI/BV strategic focus



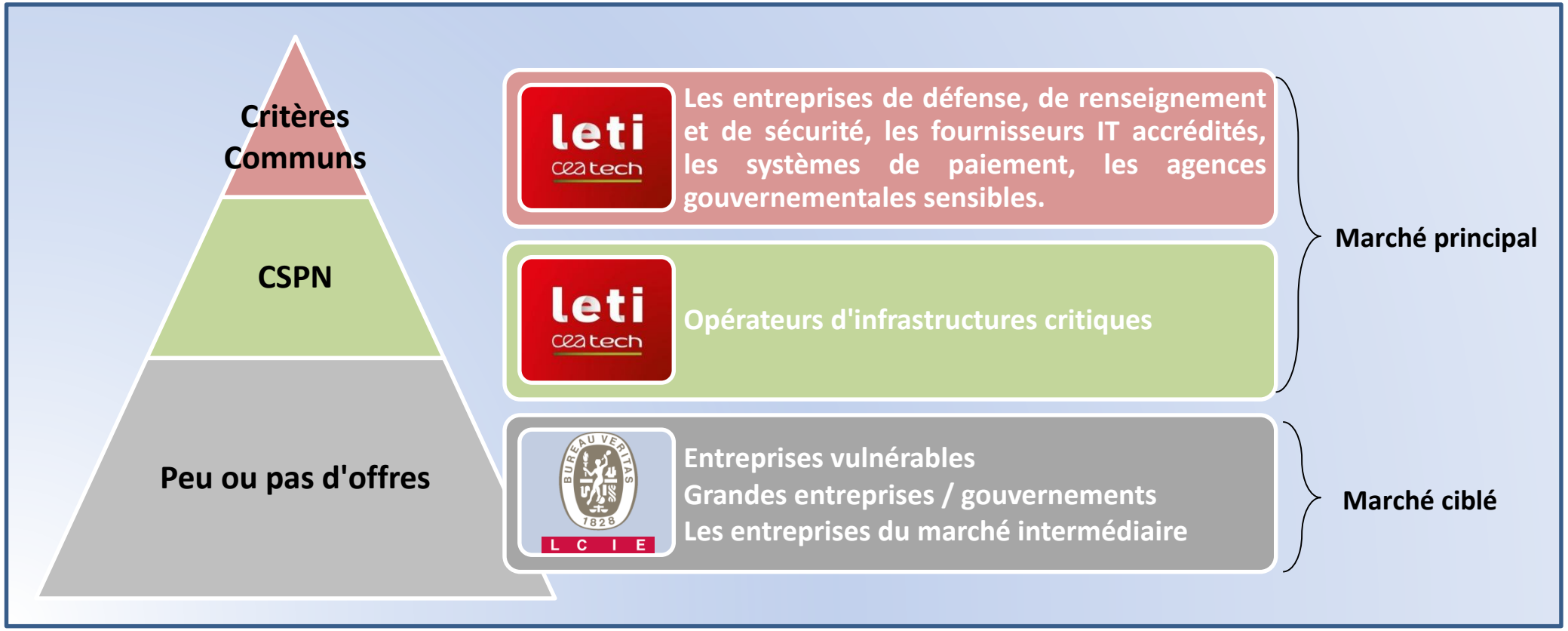
- Designing a secured network-connectable product is not trivial
- There is no easy solution but to implement a secure development process
- Though based on similar architecture & components, security designs must be validated on a case by case basis
- LETI and BV together bring consistent expertise to evaluate and validate IoT security architectures

Sources: LETI/BV

Contexte du projet

LCIE BUREAU VERITAS & CEA LETI ont convenu de développer conjointement une activité de tests et de certification pour les objets connectés.

- **Segmentation simplifiée du marché de la certification de la cybersécurité**



Test et certification de cybersécurité: Concept

1 Attaques par logiciels

- Approche « White Box »
- Basé sur les normes de sécurité
- Axé sur le développement, la validation et l'exploitation de logiciels
- Tirer parti de l'analyse du code source Y compris l'analyse de la communication (protection des données et protocole sécurisé)
- Convient dans tous les domaines (IoT, Automobile, Industrie, ...)

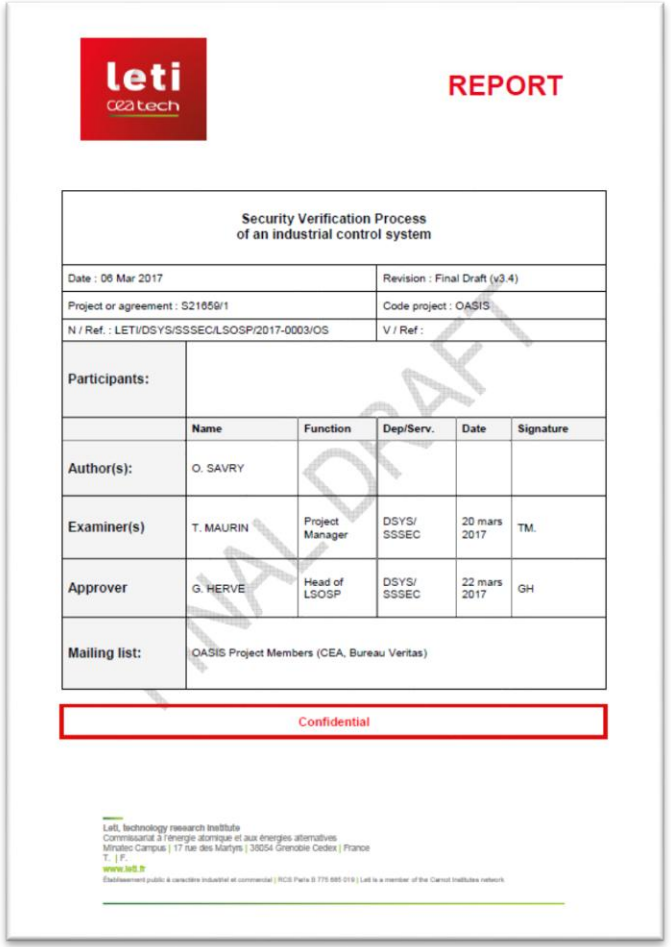
2 Attaques par interfaces

- Approche « Black Box »
- Convient à tous les secteurs
- Basé sur les normes de sécurité
- Axé sur les développeurs
- Axé sur les attaques d'interfaces
- Test de conformité automatisé

Processus d'évaluation de la sécurité

L1 2017-0003 Spécifications Techniques Final Draft

- ✓ Processus de vérification de la sécurité d'un système de contrôle industriel
- ✓ Ce document décrit une méthodologie permettant de fournir un plan de tests pour évaluer la sécurité d'un système de contrôle industriel sur ses différents canaux de communication (WiFi, Bluetooth, Zigbee, Ethernet, USB…)



leti cea tech

REPORT

Security Verification Process
of an industrial control system

Date : 06 Mar 2017			Revision : Final Draft (v3.4)		
Project or agreement : S21659/1			Code project : OASIS		
N / Ref. : LETI/DSYS/SSSEC/LSOSP/2017-0003/OS			V / Ref :		
Participants:					
	Name	Function	Dep/Serv.	Date	Signature
Author(s):	O. SAVRY				
Examiner(s)	T. MAURIN	Project Manager	DSYS/ SSSEC	20 mars 2017	TM.
Approver	G. HERVE	Head of LSOSP	DSYS/ SSSEC	22 mars 2017	GH
Mailing list:	OASIS Project Members (CEA, Bureau Veritas)				

Confidential

FINAL DRAFT

Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 rue des Martyrs | 38054 Grenoble Cedex | France
T. | F.
www.leti.fr

Le processus de certification va plus loin que le simple test

Testing & certification process

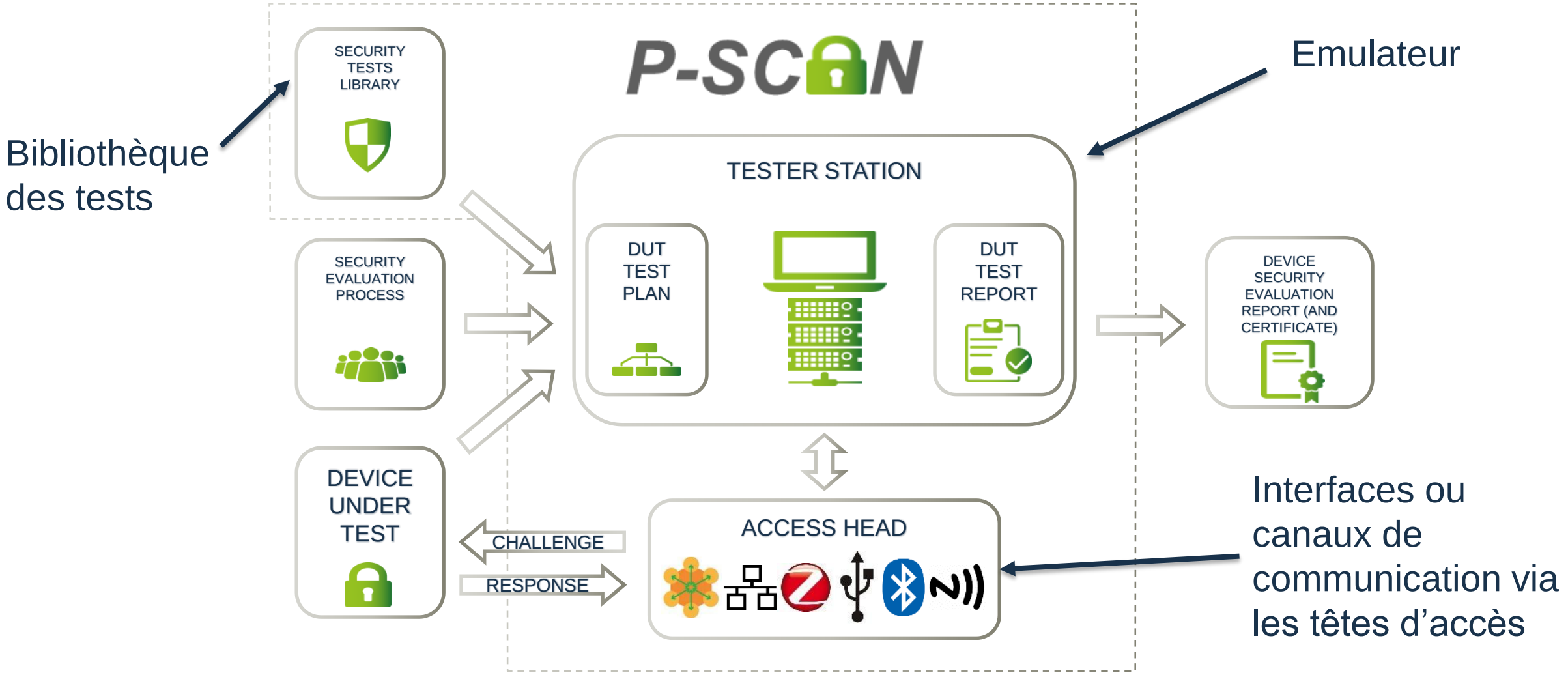




Reception of test objectives & documentation	Laboratory testing	Test report	Lifecycle monitoring	Certification
> Process guidance: checklist of all items to be tested (system, components, architecture, development procedures, lifecycle management) and the corresponding minimum requirements > Issue test plan	> Accredited testing methodology and testing tools > Verify and validate the absence of known vulnerabilities and effective implementation of security controls > Provide pass/fail details on all tested items and corresponding documentation		> Follow-up examination > Monitor changes along with product evolutions > Implement testing of new versions	> Issue certificate based on test report score and lifecycle monitoring report > Monitor validity periods

Sources: BV + SBEM analysis

Les tests de sécurité IoT nécessitent des outils automatisés



Valeur de P-Scan par rapport aux pratiques actuelles

	P-SCAN	Pratiques actuelles
Capacité d'essai	Capacité de tester la Cybersécurité à travers des canaux de communication basée sur un référentiel technique spécifique. Bureau Veritas sera en mesure d'ajouter les tests IEC 62443-4-2.	Pas encore de vision claire ou norme claire pour ce type de test : Approche CSPN spécifique à certains produits, IEC 62443-4-2: spécifique aux automates
Efficacité	Pour les produits à interfaces multiples: deux semaines de test	Approche Test CSPN: 40 jours d'essais (avec 50% de chances d'obtenir la certification)
Complémentarité avec évaluation & test du logiciel Bureau Veritas	Nous pouvons modifier nos plans de tests pour répondre à des profils de tests spécifiques pour des menaces identifiées	Des guides et référentiels existent de façon plus générique

Questions ?

BUREAU VERITAS