CYBERWEEK 2024

LES DÉFIS DE LA CYBERSÉCURITÉ DANS L'INDUSTRIE 4.0

14 OCTOBRE 2024

LIÈGE

Agence du Numérique · Cyberwal by digital wallonia · Industrie du Futur digital wallonia · CENTRE FOR CYBERSECURITY BELGIUM · expleo · Microsoft · SIAPARTNERS · Life Is On Schneider Electric · Cresco. Cybersecurity · Wallonie Relance

Programme

8h30 : Accueil petit-déjeuner.
9h00 : Introduction - Nina Hasratyan et Jeremy Grandclaudon, responsables du programme Cyberwal by Digital Wallonia à l'Agence du Numérique.
9h15 : La Directive NIS2 et sa loi de transposition et le Cyber Resilience Act : Quel impact sur l'industrie ? - Yann Caldor du Centre pour la Cybersécurité Belgique (CCB).
10h30 : Démo live d'une cyber-attaque sur un drone - Expleo.
11h00 : Pause-café.
11h15 : Démo : Utilisation d'un simulateur numérique pour mener une cyber-attaque sur un système industriel virtuel - SIA Partners.
12h00 : Comprendre et appliquer l'IEC 62443 pour une sécurité optimale - Geoffroy Moens, Schneider Electric.
12h25: AI in Threat & Incident Response - Bart Gabriëls, Microsoft.
12h45 : Conclusion - Jessica Miclotte, responsable du programme Industrie du Futur Digital Wallonia à l'Agence du Numérique.
13h00 : Networking lunch. Animation HackingLab par Cresco.

Cyberwal
by digital
wallonia

Nina Hasratyan

Agence du Numérique

Jeremy Grandclaudon

Agence du Numérique

Cyberwal
by digital
wallonia

Cyberwal by digital wallonia

Cyberweek – 14/10/2024

Les défis de la cybersécurité dans l'industrie 4.0

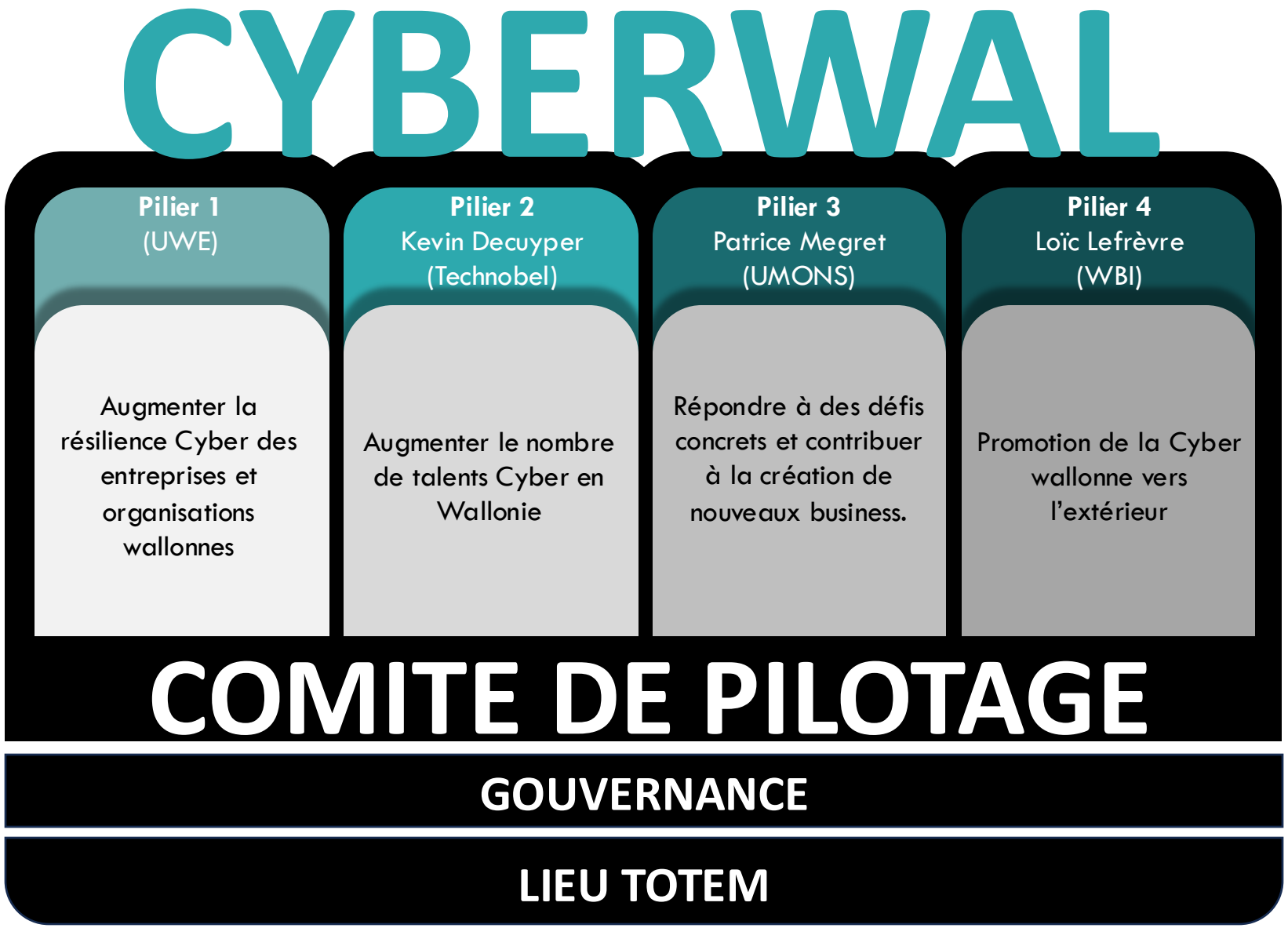
Jeremy Grandclaudon

Nina Hasratyan

Agence du Numérique


QUATRE
PILIERS

VUE D'ENSEMBLE



USAGES

COMPETENCES

RECHERCHE

RAYONNEMENT

Cyberwal by Digital Wallonia : des actions dédiées à l'Industrie 4.0

Cyberwal
by digital
wallonia

Chèques entreprise Cyber

Mobiliser & Accompagner

Objectifs :

- Fournir des **aides accessibles aux PME** (sens européen : 250 ETP / 50 Moi € de CA)
- **Améliorer le niveau et la maîtrise de la sécurité informatique** des entreprises wallones
- Soutenir la **création et la diffusion d'un label Cyber-sécurité** en Wallone (KIS)

Cyberwal by digital wallonia

- **Principes :**
  - **Procédure en ligne** (www.cheques-entreprise.be)
  - Champ d'application élargi : favoriser la **transformation numérique des acteurs économiques** sous toutes ses formes
  - Obtention rapide (**réponse en 5 jours ouvrables**)
  - Cibles privilégiées : **starters et TPE**
  - Vision "portefeuille électronique d'entreprise" (100.000€ d'aides par année civile, 200.000€ maximum sur trois ans)
- **Prestations éligibles :**
  - **Conseil et accompagnement** : audit, analyse des risques, définition d'une politique de cyber-sécurité, mise en œuvre, labellisation
- **Plafonds et taux d'intervention :**
  - 50.000€ sur 3 ans (75% de subsides)

Boîte à outils de cybersécurité pour PME

Mobiliser & Accompagner

Objectifs :

- Contribuer à améliorer la cyber-protection des entreprises
- Fournir une vidéo d'introduction, des outils gratuits, et des ressources complémentaires
- Aider les entreprises en matière de cyber-hygiène essentielle

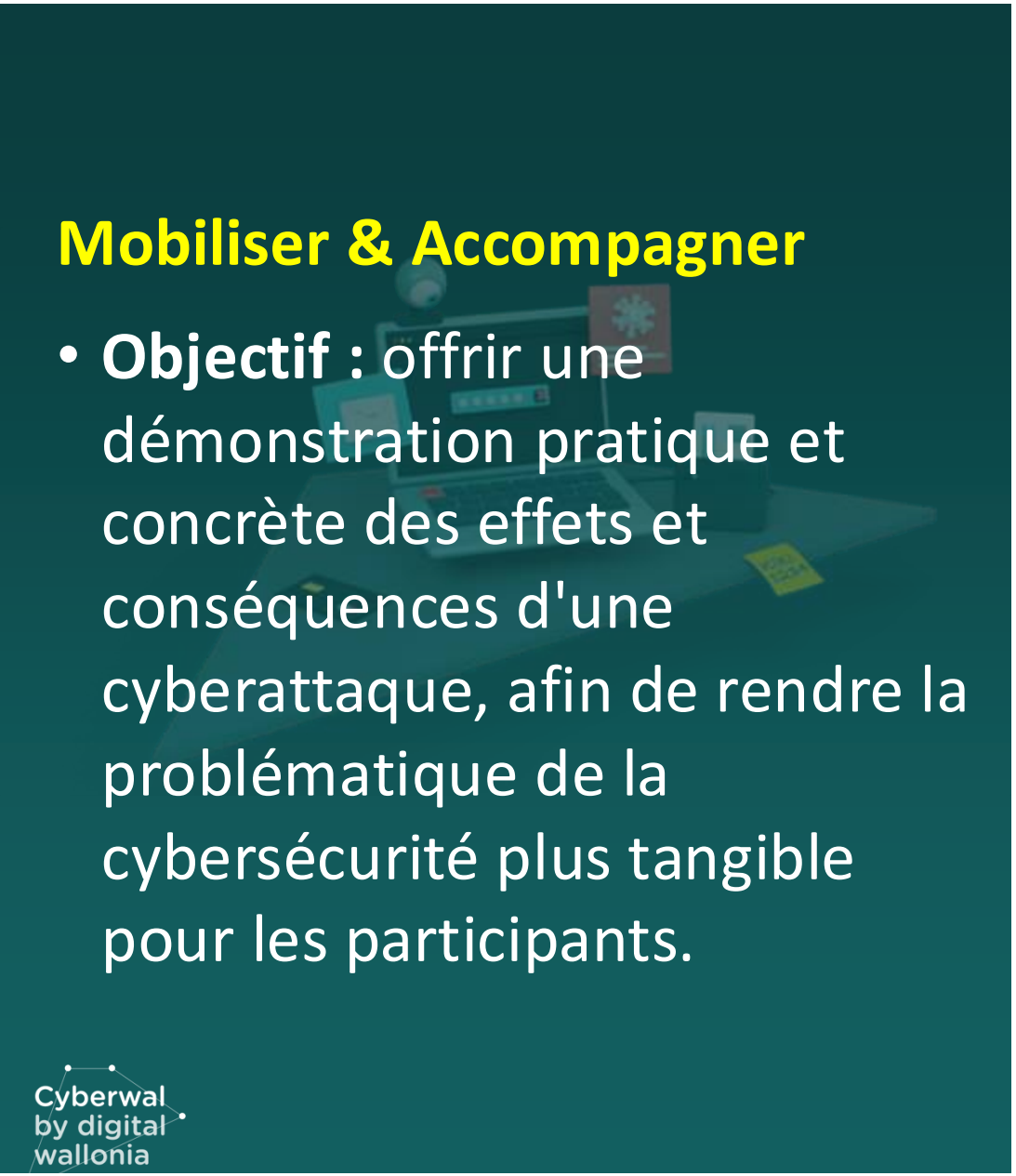
Cyberwal by digital wallonia

- **Partenariat avec le Global Cyber Alliance (GCA)**

1. Identifier vos appareils et applications
   L'Inventaire
2. Mettre à jour vos défenses
   Mettre à jour vos appareils et applications, Chiffrer vos données Sécuriser vos sites web
3. Éviter l'emploi de mots de passe simples
   Mots de passe forts, 2FA
4. Prévenir l'hameçonnage et les logiciels malveillants
   Antivirus, Sécurité DNS (Quad9)
5. Sauvegarder et récupérer
   Configurer et planifier des sauvegardes
6. Protéger vos emails et votre réputation
   DMARC et vérifications du site Web

SCAN ME

Simulateur numérique



Mobiliser & Accompagner

- **Objectif :** offrir une démonstration pratique et concrète des effets et conséquences d'une cyberattaque, afin de rendre la problématique de la cybersécurité plus tangible pour les participants.

Cyberwal by digital wallonia

- Un environnement virtuel offrant différents scénarios de cyberattaques.
- Des scénarios avec une variété de processus, de cibles, de vulnérabilités et de conséquences.
- Disponible de manière itinérante à partir de 2025.
- **Pour qui ?**
  - Preneurs de décision.
  - Tout type de public, technique ou non.
  - Utilisé lors d'événements et de conférences pour les publics cibles.

DIGITAL WALLONIA
www.digitalwallonia.be
info@digitalwallonia.be
@digitalwallonia

AGENCE DU NUMERIQUE
Av. Prince de Liège, 133
5100 Jambes
+32 (0)81 778080
www.adn.be

STÉPHANE VINCE
Directeur,
Pôle Technologie et
Administration Numérique
Stephane.vince@adn.be

JEREMY GRANDCLAUDON
Jeremy.grandclaudon@adn.be

NINA HASRATYAN
Nina.Hasratyan@adn.be

WE LOVE DIGITAL

WE KNOW DIGITAL

WE MAKE DIGITAL

Wallonie Relance

AdN

Yann Caldor

Centre pour la Cybersécurité Belgique (CCB)

Cyberwal
by digital
wallonia

Transposition de la Directive NIS2 en Belgique

Directive(UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

NIS Team CCB

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Que signifie TLP Green ?

TRAFFIC LIGHT PROTOCOL (TLP)

Green (TLP GREEN)

Limited disclosure, recipients can spread this within their community.

TLP:GREEN peut être utilisé quand l'information est utile pour augmenter les connaissances au sein de leur communauté élargie.

Les destinataires peuvent partager des informations **TLP:GREEN** avec leurs pairs et leurs organisations partenaires au sein de leur communauté mais pas via des canaux accessibles au public (par exemple des sites web, LinkedIn, …). Les informations **TLP:GREEN** ne peuvent pas être partagées en dehors de ces communautés. Note: lorsque « communauté » n'est pas défini, assumez la communauté de cybersécurité/de défense.

Agenda

1. NIS2 – Pour qui, pourquoi?
2. Scope NIS2
3. Obligations – Enregistrement
4. Obligations – Mesures de Cybersécurité
5. Obligations – Notification d’incident
6. Autorités compétentes & supervision
7. Next steps

CENTRE FOR CYBERSECURITY BELGIUM

NIS2 – Pour qui ? Pourquoi ?

01

CENTRE FOR CYBERSECURITY BELGIUM

NIS 2 : POUR QUI ? POURQUOI ?

QUOI ?

La directive n° 2022/2555 (« NIS2 ») est une révision de la directive n° 2016/1148 (« NIS1 ») (Network and Information Security). Il s'agit d'une législation de l'UE en matière de cybersécurité.

QUELLES OBLIGATIONS ?

1. S'enregister auprès du CCB (Safeonweb@work).
2. Prendre des mesures de cybersécurité adéquates.
3. Notifier au CCB les cyberincidents significatifs.
4. Effectuer des évaluations régulières de la conformité vérifiées par un organisme de contrôle de la conformité (entités essentielles).

POURQUOI ?

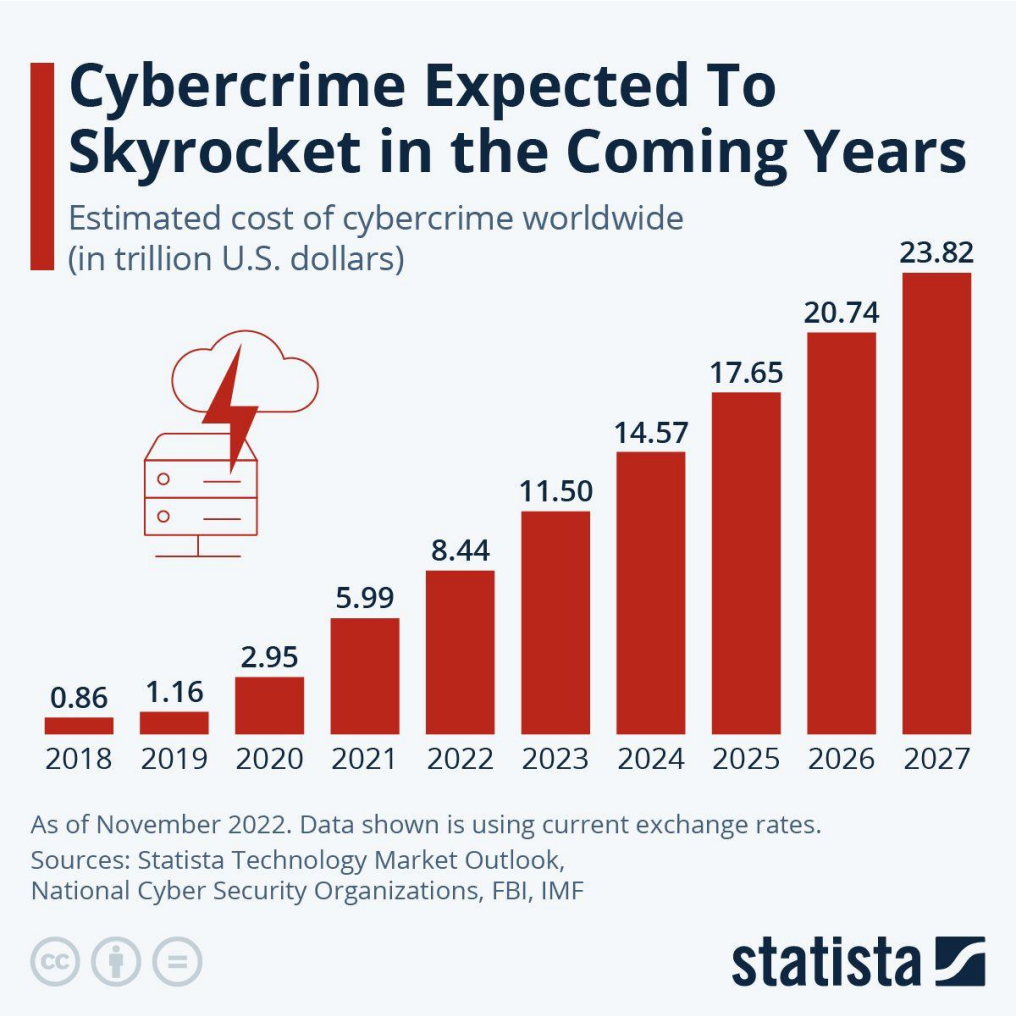
NIS 2 vise à établir un niveau élevé et commun de cybersécurité dans l'UE en imposant des exigences de gestion des risques de cybersécurité et de notification des incidents aux entités actives dans différents secteurs critiques.

POUR QUI ?

Les entités (essentielles ou importantes) fournissant des services dans les secteurs repris aux annexes I ou II.

Pourquoi NIS2?

- **RANSOMWARE**
  - Augmentation de 57.8% année après année
- **ONLINE FRAUD**
  - Double de l'année passée
- **DDOS**
  - En Moyenne 10/mois en BE
- **ESPIONAGE**
- **NEW TECHNOLGIES**
  - Artificial Intelligence

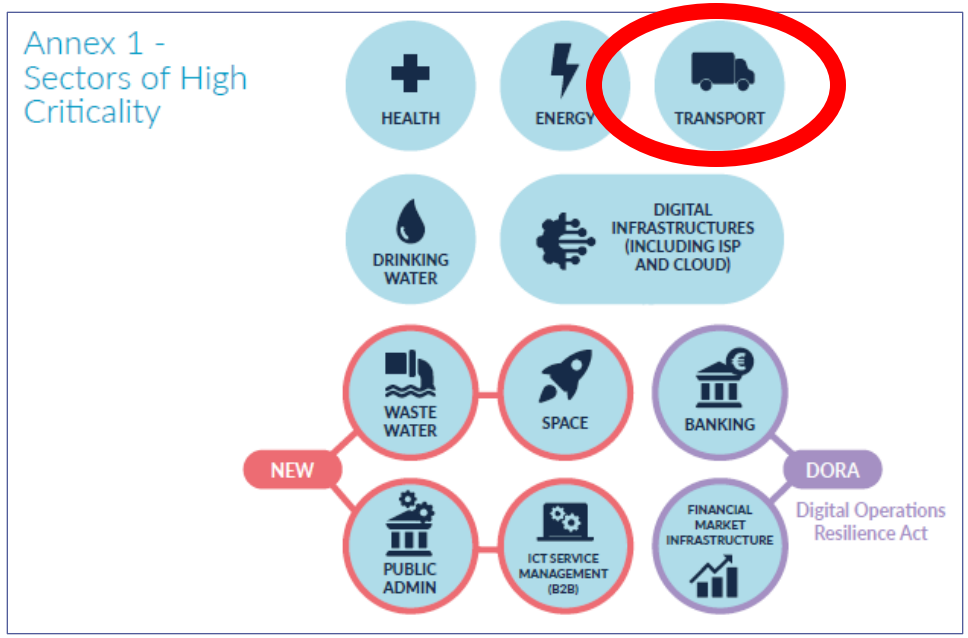


CENTRE FOR CYBERSECURITY BELGIUM

Scope NIS2

02

Scope NIS2 – Vue d'ensemble



Source: www.ncsc.gov.ie

- **Correspondre à un des types d'entités visés aux annexes I et II**
- **Être d'une certaine taille ("size-cap")**

Exceptions :

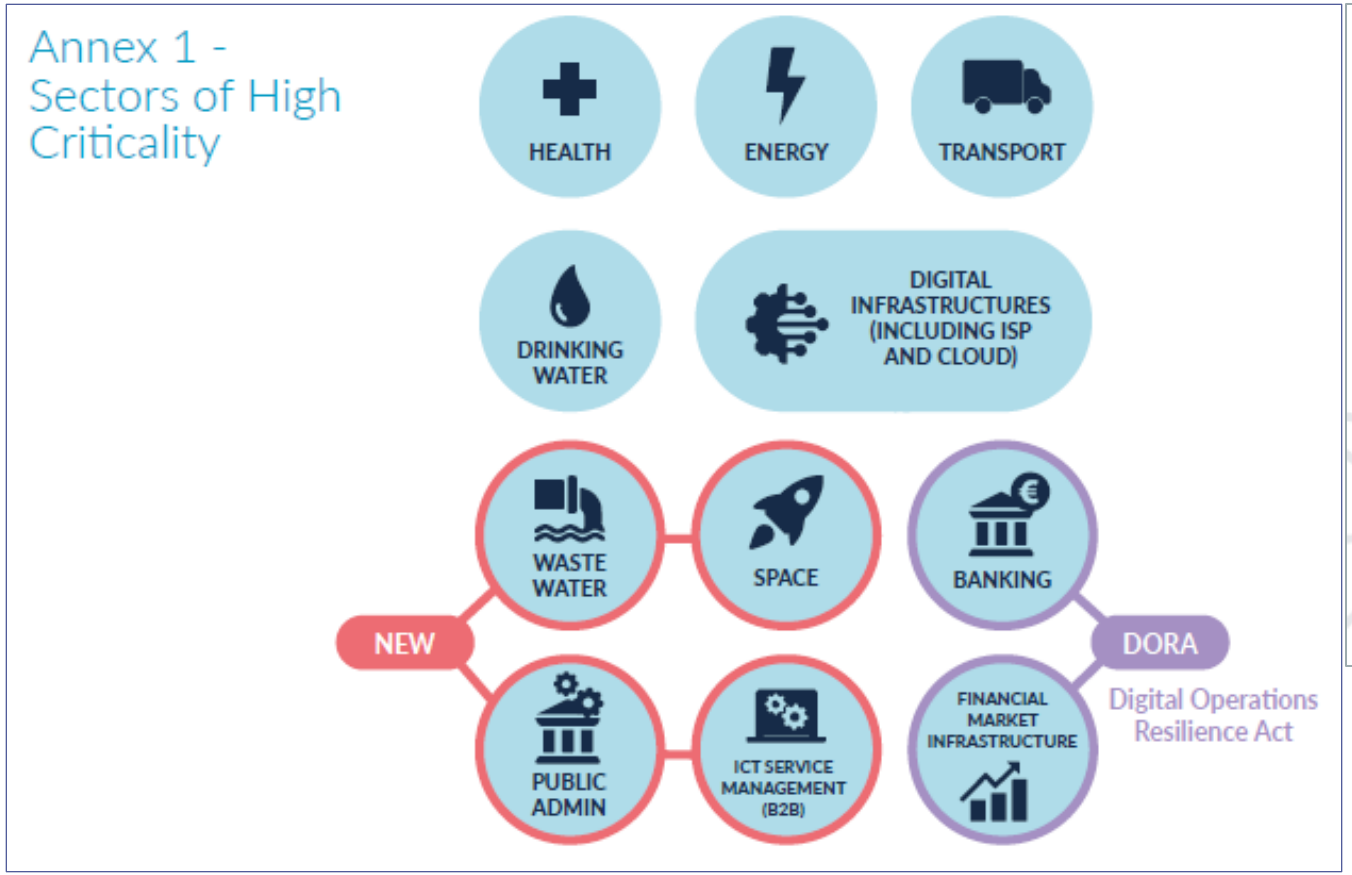
- Application d'une *Lex specialis* : Règlement DORA (Digital Operations Resilience Act – secteurs bancaires/financiers)

- Identification nationale (CER ou NIS2) + administrations publiques des entités fédérées

- Pas de critère de taille pour certains types d'entités

Scope NIS2 – Vue d'ensemble

CENTRE FOR CYBERSECURITY BELGIUM



Entités **essentielles** ou **importantes**

Entités **importantes**

Annex I : sectors of high criticality

SECTOR	SUB-SECTOR and/or ENTITY TYPE		LARGE ENTERPRISES *staff headcount of at least 250 FTEs, or > € 50m annual turnover and € 43m annual balance sheet total*	MEDIUM ENTERPRISES *staff headcount of at least 50 FTEs, or > € 10m annual turnover / annual balance sheet total*	SMALL & MICRO ENTERPRISES
1. Energy	Electricity	Electricity undertakings; Distribution system operators; Transmission system operators; Producers; Nominated electricity market operators; Market participants; Operators of a recharging point	Essential	Important*	Only if identified*
	District heating & cooling	Operators of district heating or district cooling			
	Oil	Operators of oil transmission pipelines; Operators of oil production, refining and treatment facilities, storage and transmission; Central stockholding entities			
	Gas	Supply undertakings; Distribution system operators; Transmission system operators; Storage system operators; LNG system operators; Natural gas undertakings; Operators of natural gas refining and treatment facilities			
	Hydrogen	Operators of hydrogen production, storage and transmission			
2. Transport	Air	Air carriers used for commercial purposes; Airport managing bodies, airports, and entities operating ancillary installations contained within airports; Traffic management control operators providing air traffic control (ATC) services			
	Rail	Infrastructure managers; Railway undertakings			
	Water	Inland, sea and coastal passenger and freight water transport companies; Managing bodies of ports and entities operating works and equipment contained within ports; Operators of vessel traffic services (VTS)			
	Road	Road authorities responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity; Operators of Intelligent Transport Systems			
3. Banking	Credit institutions *[DORA Lex specialis]*				
4. Financial Market Infrastructure	Operators of trading venues; Central counterparties *[DORA Lex specialis]*				
5. Health	Healthcare providers; EU reference laboratories; research and development activities of medicinal products; manufacturing of basic pharmaceutical products and pharmaceutical preparations; manufacturing of medical devices considered to be critical during public health emergency				
6. Drinking Water	Suppliers and distributors of water intended for human consumption, **only if** essential part of their general activity				
7. Waste Water	Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water, **only if** essential part of their general activity				
8. Digital Infrastructure	Qualified trust service providers		Essential		
	DNS service providers [excluding root name servers]				
	TLD name registries				
	Providers of public electronic communication networks or electronic communication services available to the public		Essential		Important*
	Non-qualified trust service providers				
	Internet Exchange Point providers		Essential	Important*	Only if identified*
	Cloud computing service providers				
	Data centre service providers				
	Content delivery network providers				
9. ICT-service management	Managed (Security) Service Providers				
10. Public Administration (excluding judiciary, parliaments, central banks; national security, public security, defence or law enforcement).	Public administrations depending on the federal State		Essential		
	Public administrations depending on the federated entities (only after identification following a risk-based assessment of the criticality of the services provided)		Important*		
	Emergency zones (including the Firefighting and emergency medical assistance service of the Brussels Capital Region)				
11. Space	Operators of ground-based infrastructure that support the provision of space-based services, excluding providers of public electronic communications networks		Essential	Important*	Only if identified*

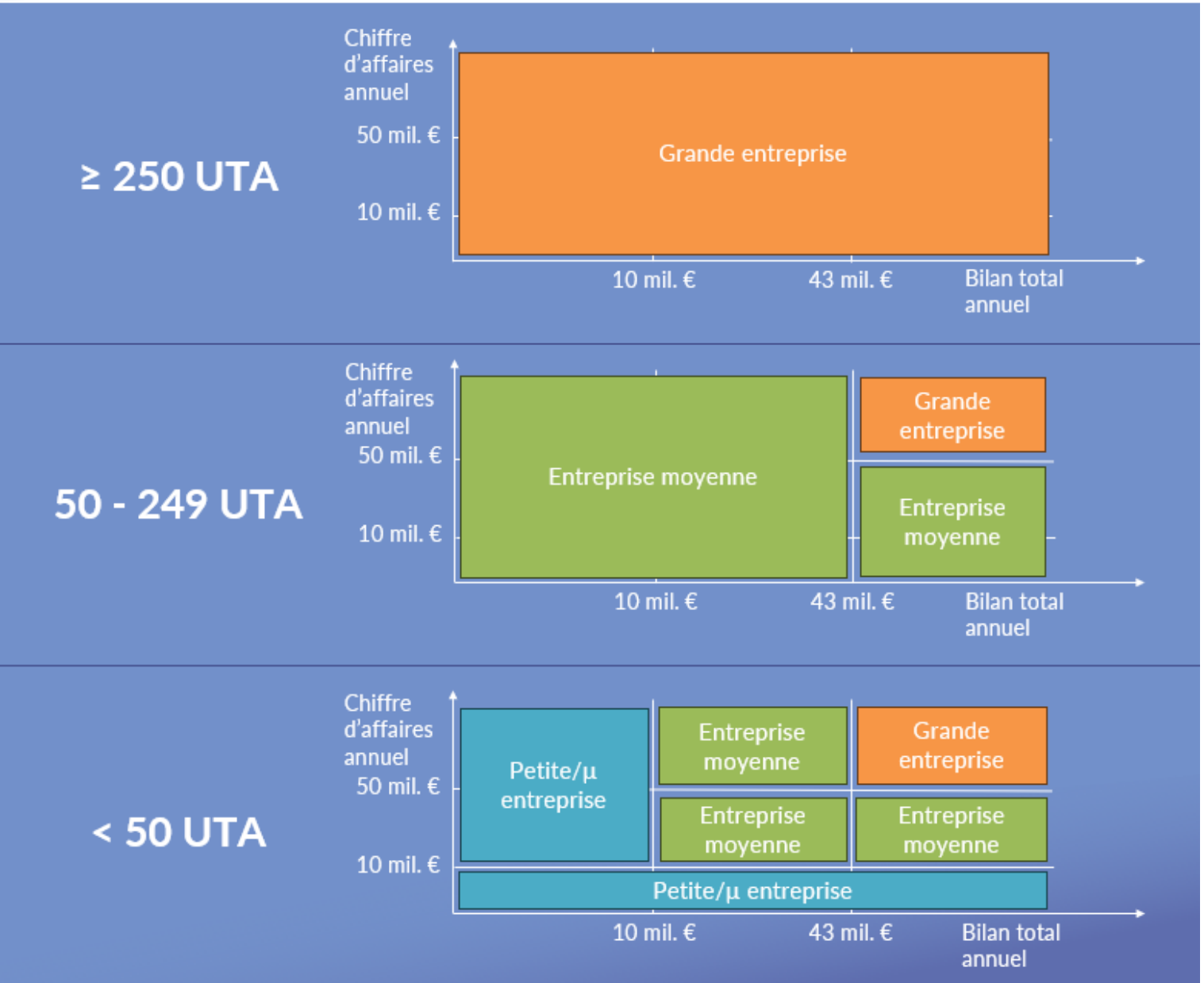
Scope NIS2 – Types d'entités

- **Exploitants de systèmes de transport intelligents**: systèmes dans lesquels des technologies de l'information et de la communication sont appliquées, dans le domaine du transport routier, y compris les infrastructures, les véhicules et les usagers, et dans la gestion de la circulation et la gestion de la mobilité, ainsi que pour les interfaces avec d'autres modes de transport
- **Prestataires de services postaux**: services qui consistent en la levée, le tri, l'acheminement et la distribution des envois postaux;
- **Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques**, sur base de la nomenclature NACE rev. 2
- **Fabrication de produits informatiques, électroniques et optiques**: Sur base de la nomenclature NACE rev. 2 (section C, division 26) **Fabrication de machines et équipements n.c.a.**: Sur base de la nomenclature NACE rev. 2 (section C, division 28)
- **Construction de véhicules automobiles, remorques et semi-remorques**: Sur base de la nomenclature NACE rev. 2 (section C, division 29)
- **Etc**

Scope NIS2 = même les activités accessoires. En principe, sauf si spécifié autrement, l'activité concernée ne doit pas forcément être à titre principal

CENTRE FOR CYBERSECURITY BELGIUM

Taille d'une entreprise selon la Recommandation 2003/361/CE



L 124/36 EN Official Journal of the European Union 20.5.2003

COMMISSION

European Commission

COMMISSION RECOMMENDATION
of 6 May 2003
concerning the definition of micro, small and medium-sized enterprises
(notified under document number C(2003) 1422)
(Text with EEA relevance)

(2003/361/EC)

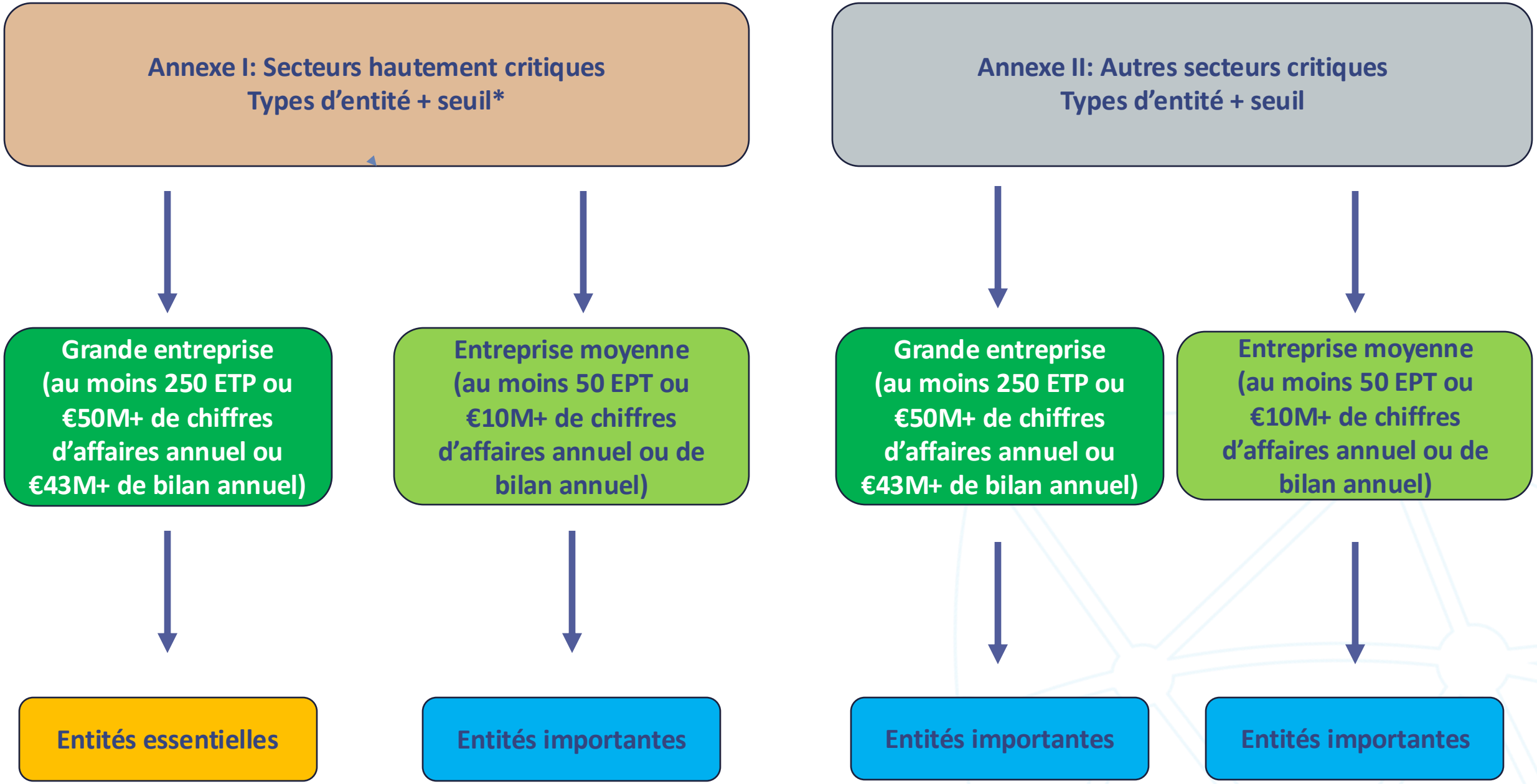
THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European

economic developments, pursuant to Article 2 of the Annex thereto, consideration must be given to a number of difficulties of interpretation which have emerged in its application, as well as the observations received from

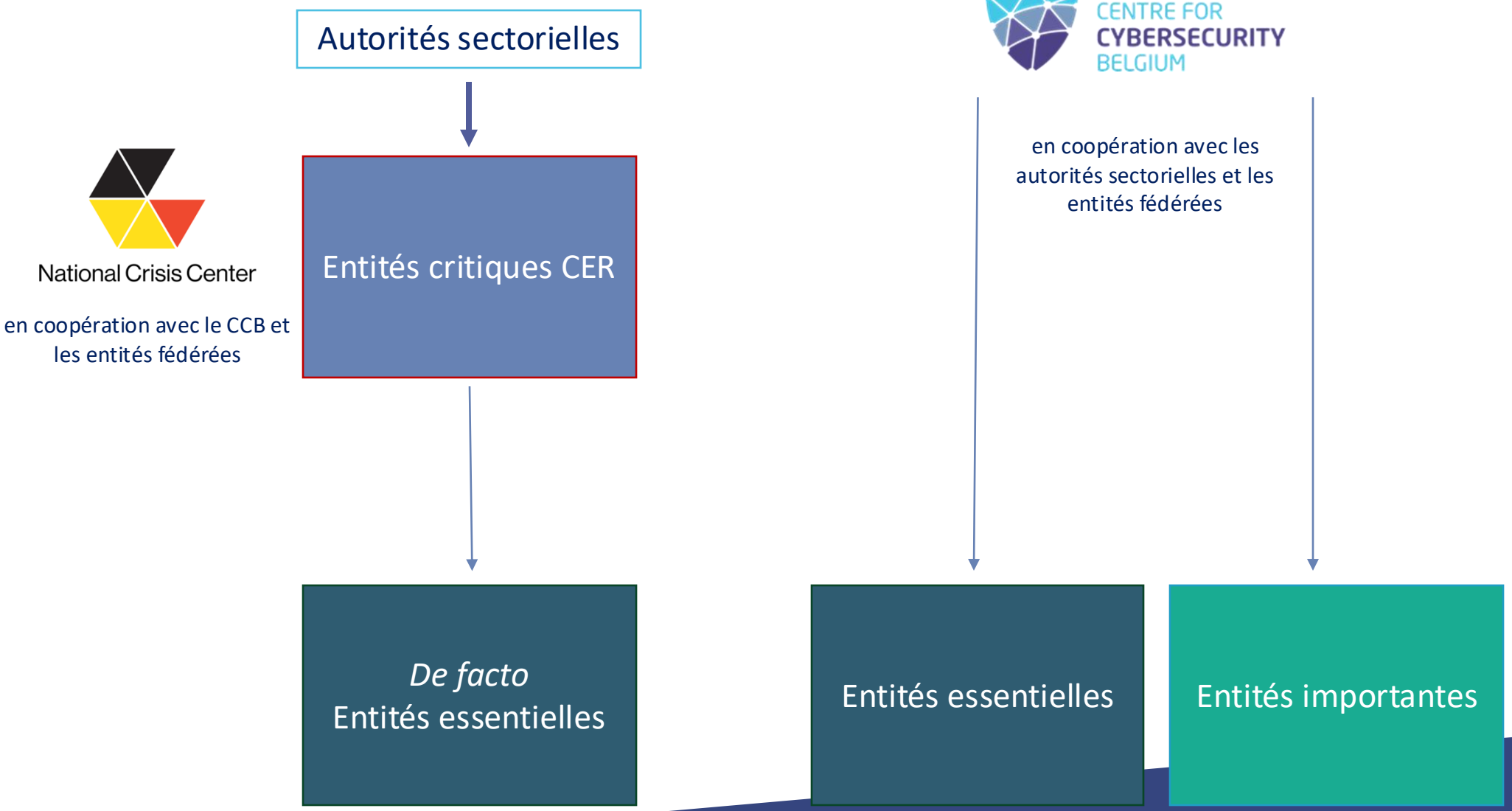
[Guide de l'utilisateur pour la définition des PME (EU)]

[Outil en ligne pour déterminer la taille d'une entreprise (EU)]



(*) Rappel, il existe des exceptions pour lesquelles les seuils ne s'appliquent pas

Identification nationale additionnelle



CENTRE FOR CYBERSECURITY BELGIUM

Obligations – Enregistrement

03

Obligations – Enregistrement

CENTRE FOR CYBERSECURITY BELGIUM

S'enregistrer auprès de l'autorité nationale de cybersécurité dans les 5 mois suivant l'entrée en vigueur de la loi ou suivant l'identification

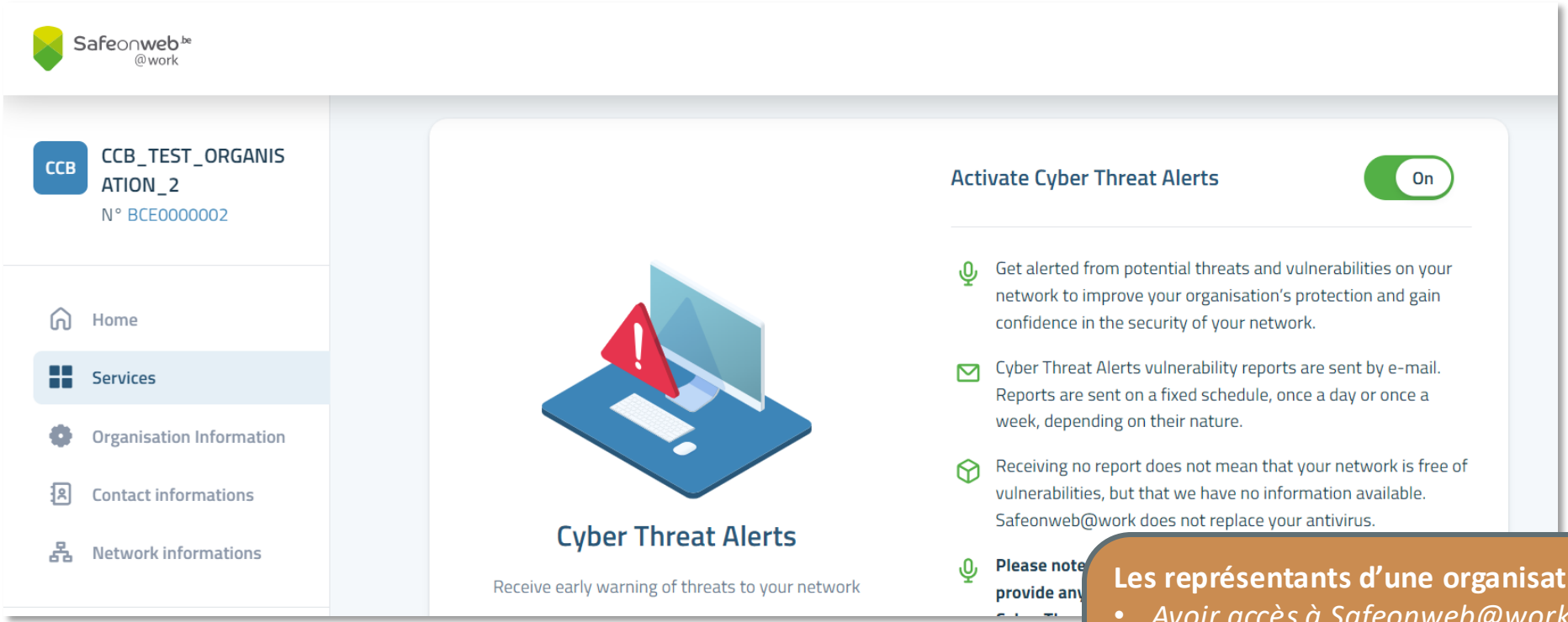
Fournir les informations suivantes

- La dénomination de l'entité et son numéro BCE
- L'adresse et les coordonnées actualisées, y compris l'adresse de courrier électronique, les plages d'IP et le numéro de téléphone
- Le secteur et sous-secteur auquel l'entité appartient
- Le cas échéant, la liste des Etats membres dans lesquels l'entité fournit des services relevant du champ d'application de NIS2

Communiquer les modifications apportées aux informations ci-dessus endéans les deux semaines

L'enregistrement en pratique

Usage des données existantes auprès des administrations publiques relatives aux entités NIS2 (principe administratif "only once")



Les représentants d'une organisation pourront:

- *Avoir accès à Safeonweb@work*
- *Enregistrer les données de contact et les informations relative à leur réseau*
- *Enregistrer l'organisation en tant qu'entité NIS2*
- *Indiquer le(s) secteur(s) d'activité*

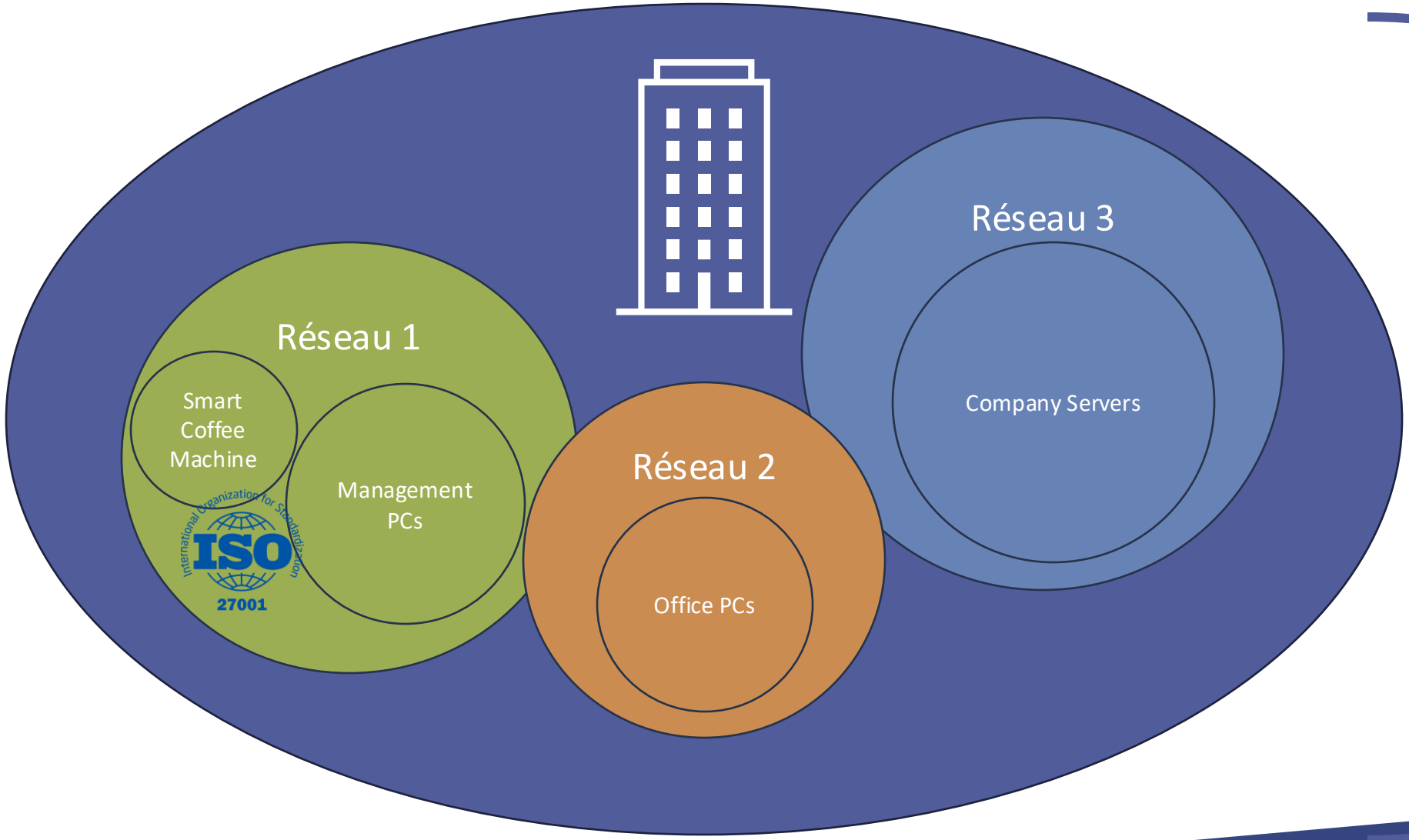
Deadline 18 mars 2025 (en principe)

Deadline 18 décembre 2024 (certaines entités du secteur des infrastructures digitales)

Obligations – Mesures de Cybersécurité

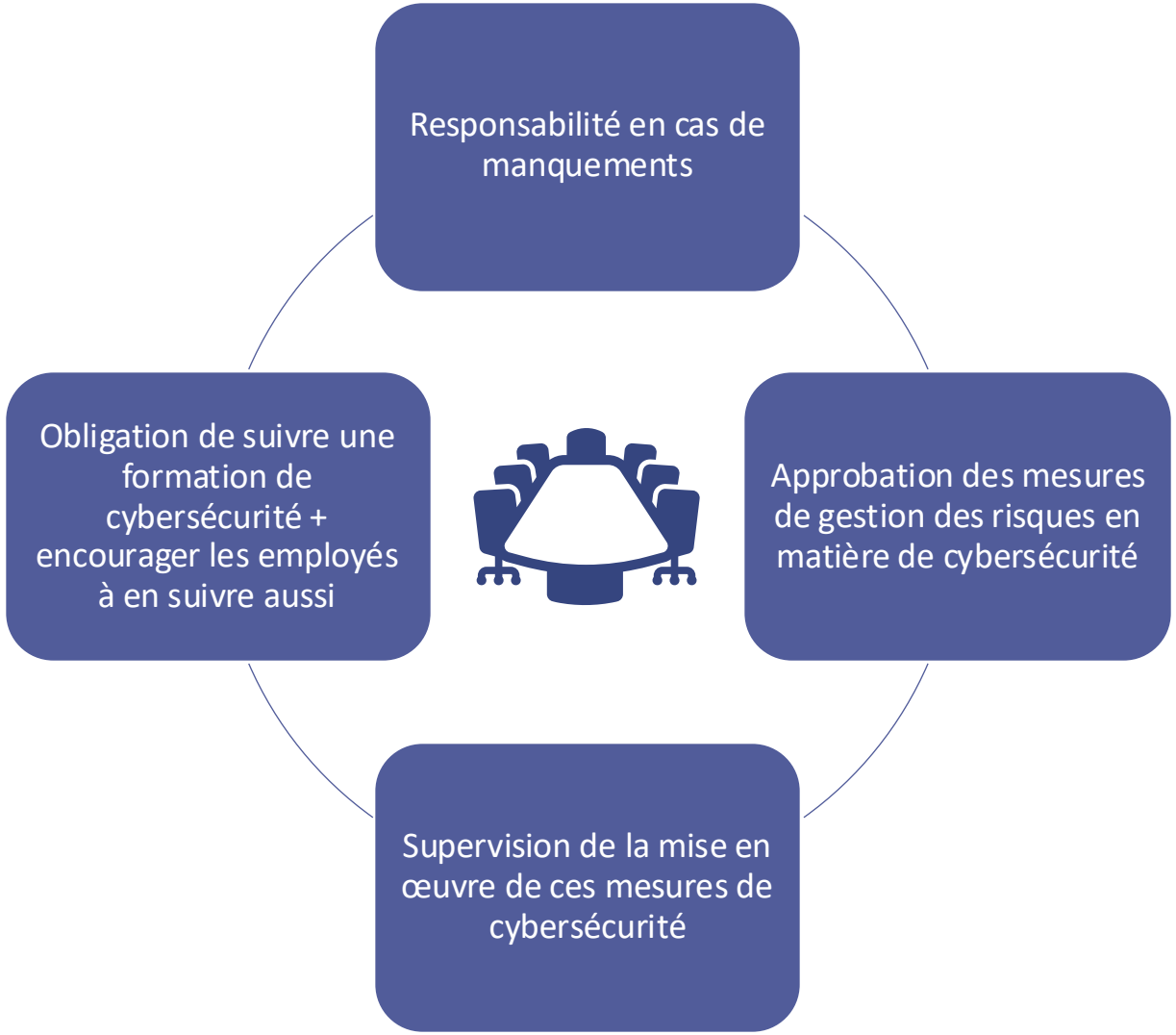
04

Scope des mesures



NIS2 scope = l'entièreté de l'entité

Responsabilité des organes de gestion



La notion de “membre d’un organe de direction” signifie toute personne physique ou morale qui:

(i) exerce une fonction au sein d’une entité ou en relation avec celle-ci l’autorisant (a) à **administrer et à représenter l’entité** en question ou (b) à **prendre des décisions au nom et pour le compte de l’entité qui sont juridiquement liantes** pour celle-ci ou à participer, au sein d’un organe de l’entité, à la prise de telles décisions, ou

(ii) exerce un **contrôle** de l’entité en question, soit le pouvoir de droit ou de fait d’exercer une influence décisive sur la désignation de la majorité des administrateurs ou gérants de celle-ci ou sur l’orientation de sa gestion.

Lorsque l’entité en question est une société de droit belge, tel contrôle est déterminé conformément aux articles 1:14 à 1:18 du Code des sociétés et des associations.

Lorsque la personne dont le rôle est examiné est une personne morale, la notion de “membre d’un organe de direction” est examinée de façon récursive et recouvre tant la personne morale en question que tout membre d’un organe de direction de ladite personne morale.

Caractéristiques des mesures de gestion des risques en matière de cybersécurité

d'ordre **techniques, opérationnelles et organisationnelles**

Appropriées et **proportionnées**

Gèrent les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services

Eliminent ou réduisent les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services

Prennent en compte les **coûts d'implémentation**

Prennent en compte **l'état de l'art** et, si applicable, les **standards européens et internationaux** pertinents

Proportionnalité : degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques

Analyse de risques

→ Adaptées à la situation concrète de l'entité NIS2

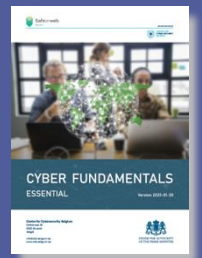
CENTRE FOR CYBERSECURITY BELGIUM

LES MESURES DE CYBERSÉCURITÉ À METTRE EN OEUVRE

NIS 2 : approche « tous risques (*all hazards*) » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents. La loi impose de prendre des mesures appropriées et proportionnelles en fonction de l'analyse de risques de l'entité. Ces mesures portent au moins sur :

- Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information
- La gestion des incidents
- La continuité des activités et la gestion des crises
- La sécurité de la chaîne d'approvisionnement
- La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités.
- Une politique de divulgation coordonnée des vulnérabilités
- Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité
- Cyberhygiène et la formation à la cybersécurité
- Des politiques et des procédures sur la cryptographie et, le cas échéant, du chiffrement
- La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
- Des solutions d'authentification à plusieurs facteurs, de communications sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins

Ces mesures de sécurité peuvent être implémentées avec les référentiels CyberFundamentals (CyFun®) ou ISO 27001.



ISO 27001

Obligation dans la chaîne d'approvisionnement

CENTRE FOR CYBERSECURITY BELGIUM

Entité NIS2

- Imposer des mesures de gestion des risques en matière de cybersécurité
- Contrôle du respect de ces mesures

Prendre des mesures de gestion des risques en matière de cybersécurité appropriées et proportionnées

Fournisseur direct
Fournisseur de service

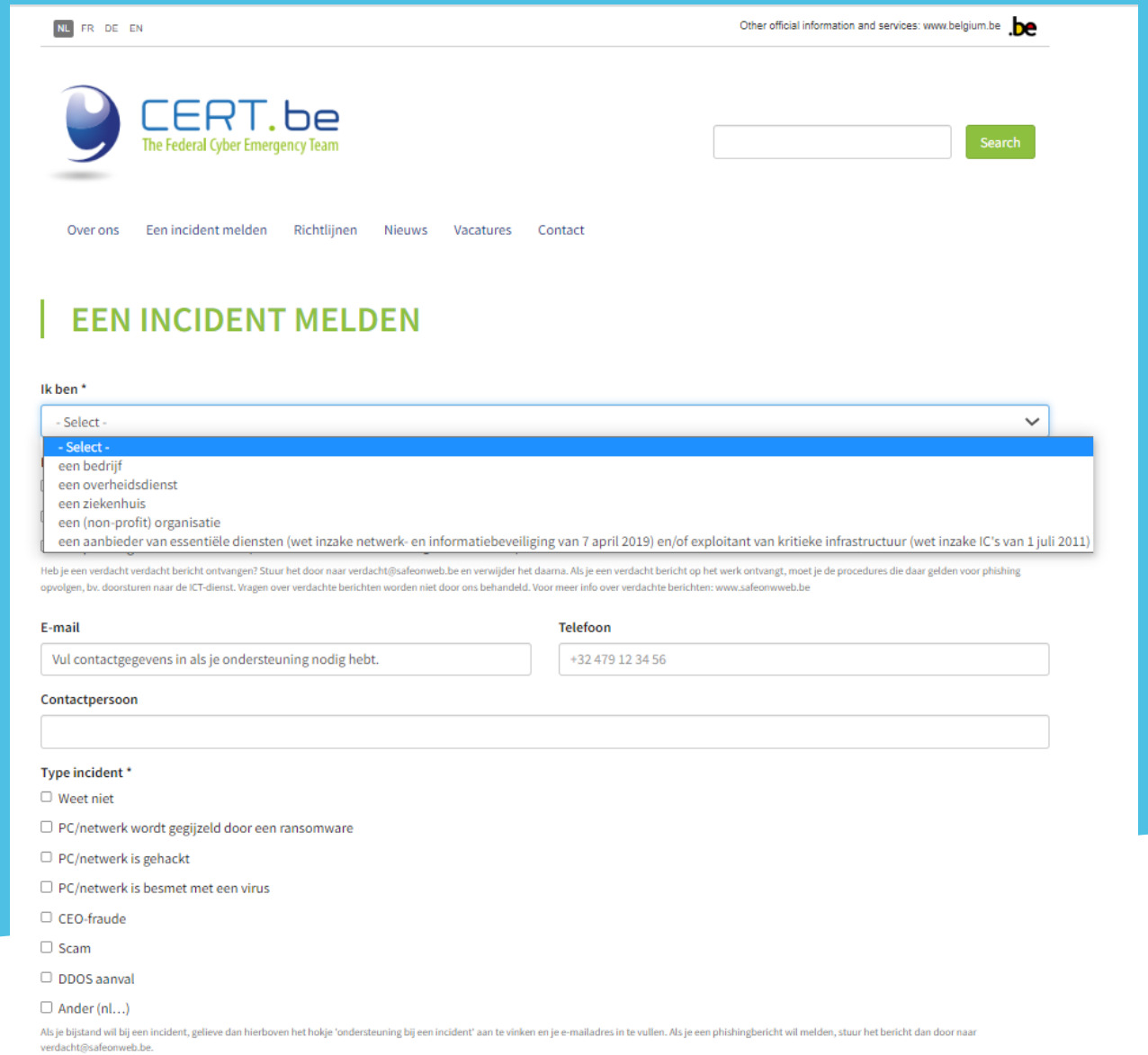
Potentielle entité non-NIS2

La loi NIS2 détermine la sécurité de la supply chain comme une mesure de cybersécurité minimale mais n'explique pas comment cela doit être effectué en pratique.

Le CCB recommande l'usage du cadre CyberFundamentals (CyFun®)

Obligations – Notification d'incident

05



Incidents – que notifier ? A qui?

Les entités essentielles et importantes doivent notifier les **incidents significatifs**

- "**Incident**" signifie tout événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles

- Un incident est **significatif** si :
  Il a causé ou est susceptible de causer une perturbation opérationnelle grave de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II ou des pertes financières pour l'entité concernée **ou**
  Il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables

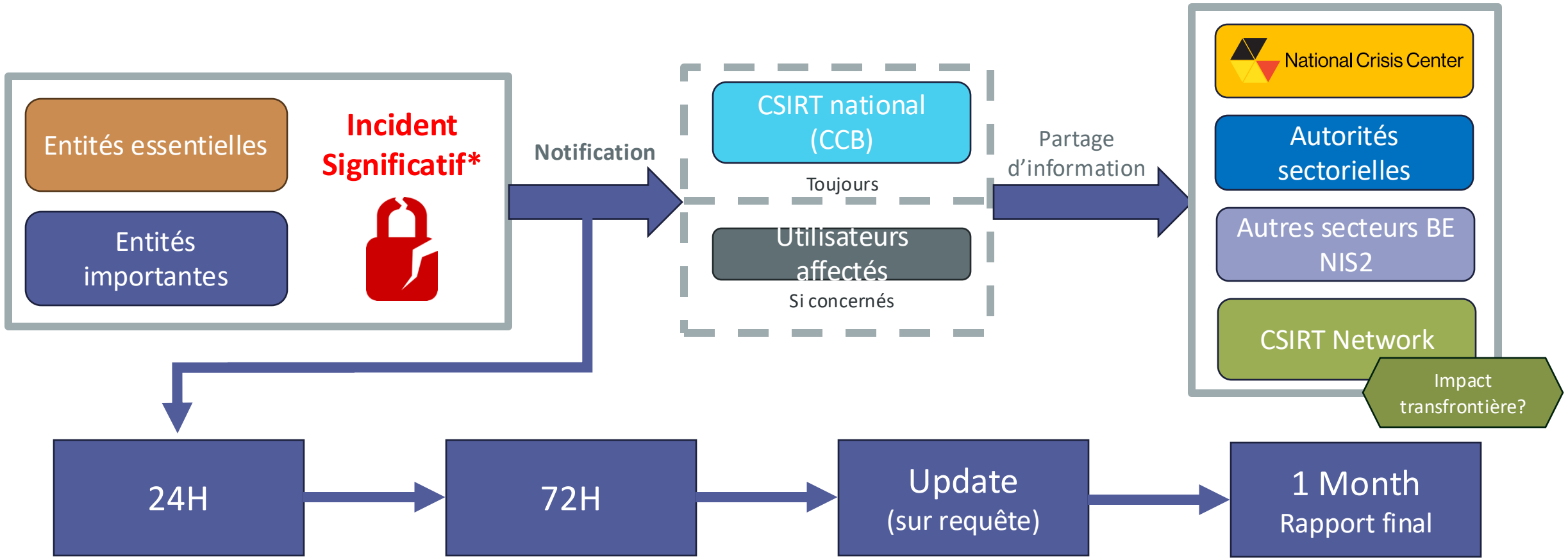
Les entités essentielles notifient au **CSIRT national** et, le cas échéant, aux **destinataires de leurs services**

- **Au CSIRT national**, tout incident significatif + toute information permettant de déterminer si l'incident a un impact transfrontière (voir slide suivant)

- **Au destinataire**, les incidents significatifs susceptibles de nuire à la fourniture des services repris à l'annexe I et II + les mesures/corrections que ces destinataires peuvent appliquer + la cybermenace importante elle-même

Guidance du NIS CG & CCB à venir

Notification au CSIRT - Etapes et délais



Alerte précoce (téléphone, mail) + information sur une potentielle nature malveillante/illicite **+ potentiel impact transfrontière**

- **Evaluation initiale de l'incident**, sa gravité, son impact, si possible, des indicateurs de compromission
- **Mise à jour des informations fournies dans les 24h**

- **Description détaillée** de l'incident, sa gravité et son impact
- **Type de menace ou cause profonde** qui a probablement déclenché l'incident
- **Mesures d'atténuation** appliquées et en cours

* Susceptible d'affecter la fourniture des services NIS2

CENTRE FOR CYBERSECURITY BELGIUM

Autorités compétentes & supervision

06

Autorité nationale de cybersécurité

Le Centre pour la Cybersécurité Belgium (CCB) sera désigné comme **Autorité nationale de cybersécurité**

L'autorité nationale de cybersécurité a les taches suivantes:

- Superviser et coordonner l'implémentation de la loi NIS2
- Superviser son implémentation par les entités NIS2
- Gérer les crises et incidents de cybersécurité

L'autorité nationale de cybersécurité a les rôles suivants:

- Autorité compétente en principe pour la supervision des entités NIS2 (en coopération avec les autorités sectorielles)
- CSIRT national
- SPOC pour l'implémentation de NIS2
- Représentant de la Belgique dans différents groupes européens

Autorité nationale de cybersécurité

Le Centre pour la Cybersécurité Belgique (CCB) est désigné comme **Autorité nationale de cybersécurité**.

Nos rôles:

Autorité compétente pour la supervision des entités NIS2

CSIRT national

Point de contact unique (SPOC) pour l'implémentation de NIS2

Représentant BE dans le CSIRTs network

Représentant BE dans le NIS cooperation group

Représentant BE dans le European Cyber Crisis Liaison Organisation Network (EU-

Nos tâches:

Superviser et coordonner l'implémentation de la loi NIS2

Superviser son implémentation par les entités NIS2

Gérer les crises et incidents de cybersécurité

Autorités sectorielles

CENTRE FOR CYBERSECURITY BELGIUM

- Energy
- FSMA Finance
- bipt Digital infastructure
- Transport
- Health
- Digital service providers
- National Bank of Belgium Banking
- National water Committee
- belspo Space & Research
- AFCN Nuclear

...

Supervision des entités NIS2

Entités importantes

Supervision *ex-post* : Après incident ou suspicion de violations de la loi

Entités essentielles

Supervision *ex-post* & *ex-ante*

Mesures de supervision:

- Inspections sur site et à distance
- Audits ad hoc
- Scans de sécurité
- Requête d'information et de preuve

Evaluation périodique de la conformité **volontaire** sous CyFun® ou ISO 27001

Evaluation périodique de la conformité **obligatoire** sous CyFun® ou ISO 27001 ou inspection

Evaluation périodique de la conformité

Certification/Vérification: CyberFundamentals par un organisme d'évaluation de la conformité (CAB) autorisé (avec un scope pertinent) **CyFun®**

Mesures sectorielles additionnelles

Certification: ISO 27001 par un organisme d'évaluation de la conformité (CAB) autorisé (avec un scope et un *statement of applicability* pertinent)

Mesures sectorielles additionnelles

Inspection par le CCB (rétributions pour l'entité)

CENTRE FOR CYBERSECURITY BELGIUM

Mesures sectorielles additionnelles

Présomption de conformité

Mesures et sanctions administratives

CENTRE FOR CYBERSECURITY BELGIUM

Avertissements

Déclaration publique/information aux utilisateurs

Instructions contraignantes

Inspections ciblées et ad-hoc

Recommendations
Monitoring

Amendes

Mesures et sanctions administratives

CENTRE FOR CYBERSECURITY BELGIUM

Avertissements ou **instructions contraignantes**		Ordre de **mettre un terme à une violation** ou de **garantir la conformité**	Ordre de **rendre public** les aspects de violations constatées
Désigner, pour une période déterminée, **un responsable du contrôle** [essentiel]	Ordre de mettre en œuvre les **recommandations** formulées	**Suspendre temporairement** une certification ou une autorisation concernant tout ou partie des services fournis [essentiel]	**Interdiction temporaire d'exercice de responsabilités dirigeantes** [essentiel]

500 à 125 000 € si non-conformité avec les obligations d'information de l'art. 12 (identification)

500 à 200 000 € si représailles contre un employé ou sous-contractant qui exécute une obligation de la loi NIS2 en toute bonne foi et dans le cadre de ses fonctions

500 à 200 000 € si non-conformité avec les obligations de supervision

Amendes doublées en cas de "récidives" dans les 3 ans

500 à 7 000 000 € ou 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu [**important entities**]

500 to 10 000 000 € ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu [**essential entities**]

Next steps
07

Next steps


DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Adoption de la Directive NIS2 14/12/2022

Approbation de l'avant-projet de loi par le CMR 10/11/2023

Janvier/Février 2024 Review/2ème lecture

Juin 2024 (Elections)

Entrée en vigueur de la loi NIS 2 18/10/2024

Groupes de travaux √

Consultation publique/ avis formels √

Discussion/ adoption de la loi au Parlement √

Préparation

Exécution loi

Arrêté royal approuvé par le CMR 10/11/2023

Début de la présidence Belge EU 2024

Entrée en vigueur AR NIS 2 18/10/2024

Avis formel AR

Adoption AR √

Préparation

Exécution AR

Entrée en vigueur de la loi NIS2

Les obligations NIS2 (Loi et arrêté royal) sont applicables à partir du 18 octobre 2024:

- Mesures de gestion des risques en matière de cybersécurité
- Notification d'incident
- Supervision (avec un délai spécifique pour les premières évaluations périodiques de la conformité pour les entités essentielles)
- Etc.

En cas d'identification, les délais (voir slide suivante) commencent à courir à partir de la notification de la décision administrative

Délais d'implémentation: **entités essentielles**

CENTRE FOR CYBERSECURITY BELGIUM

2024 | 2025 | 2026 | 2027

Jun Jul Aug Sep **Oct** Nov **Dec** Jan Feb **Mar** Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar **Apr** May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar **Apr**

18 18 18 18

Délai d'enregistrement principal*

Sur Safeonweb@work

Délai d'enregistrement – Secteur digital*

*en cas d'identification, le délai commence à partir de la notification de la décision administrative

Mesures de sécurité & notification d'incident

Mesures de gestion des risques en matière de cybersécurité
Notifications obligatoires des incidents significatifs
Notifications volontaires d'autres incidents, cybermenaces & near misses

Amélioration des mesures après incidents
Formation de cybersécurité

Implémentation & supervision progressive

- Choix du framework
- Début de l'implémentation ou complementing cybersecurity measures

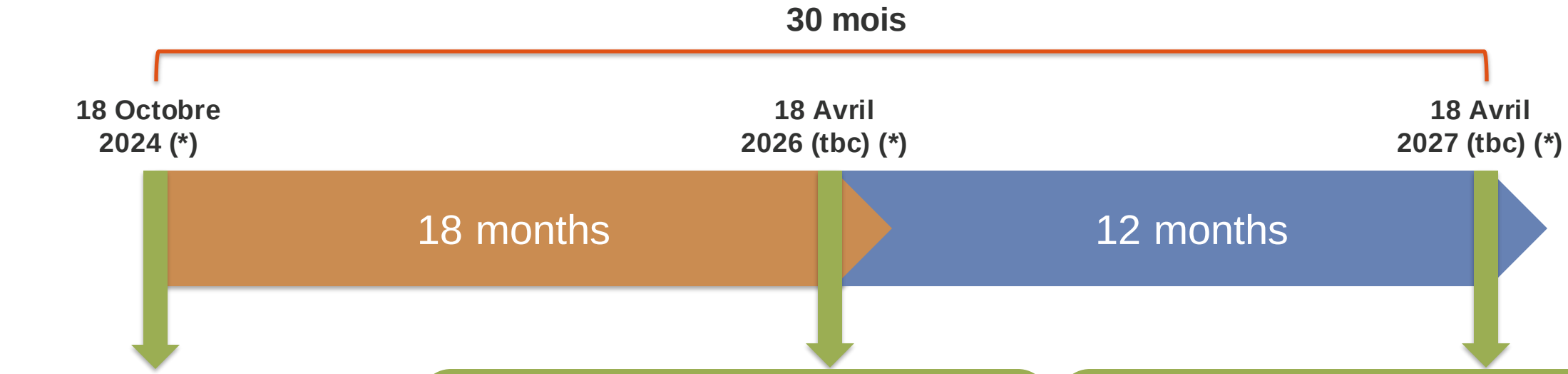
CyberFundamentals ESSENTIAL version 2023-03-01
CyberFundamentals IMPORTANT version 2023-03-01
CyberFundamentals BASIC version 2023-03-01

ISO 27001

Get CyFun Basic or Important label (or equivalent inspection)

Get CyFun Essential label (or equivalent inspection)

Délai spécifique pour l'évaluation périodique de la conformité des **entités essentielles**



Entrée en vigueur de la loi NIS2

Objectif: Niveau d'assurance Cyfun *Basic* ou *Important* (*)
- Deadline pour la *vérification* par un CAB **ou**
- ISO 27001 *Scope & Statement of Applicability* équivalent

Objectif: Niveau d'assurance Cyfun *Essential* (*)
- Deadline pour la *certification* CyFun par un CAB **ou**
- *Certification* ISO 27001 *Scope & Statement of Applicability* équivalent

Alternative (inspection CCB):
Check du statut du processus de conformité NIS2 :
- CyFun Self-Assessment **ou**
- ISO 27001 *Scope & SoA* (+I.B.B./P.S.I.)

*(en cas d'identification formelle, le délai commence àpd la notification de la décision administrative)

CENTRE FOR
CYBERSECURITY
BELGIUM

NIS Team CCB
nis@ccb.belgium.be

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

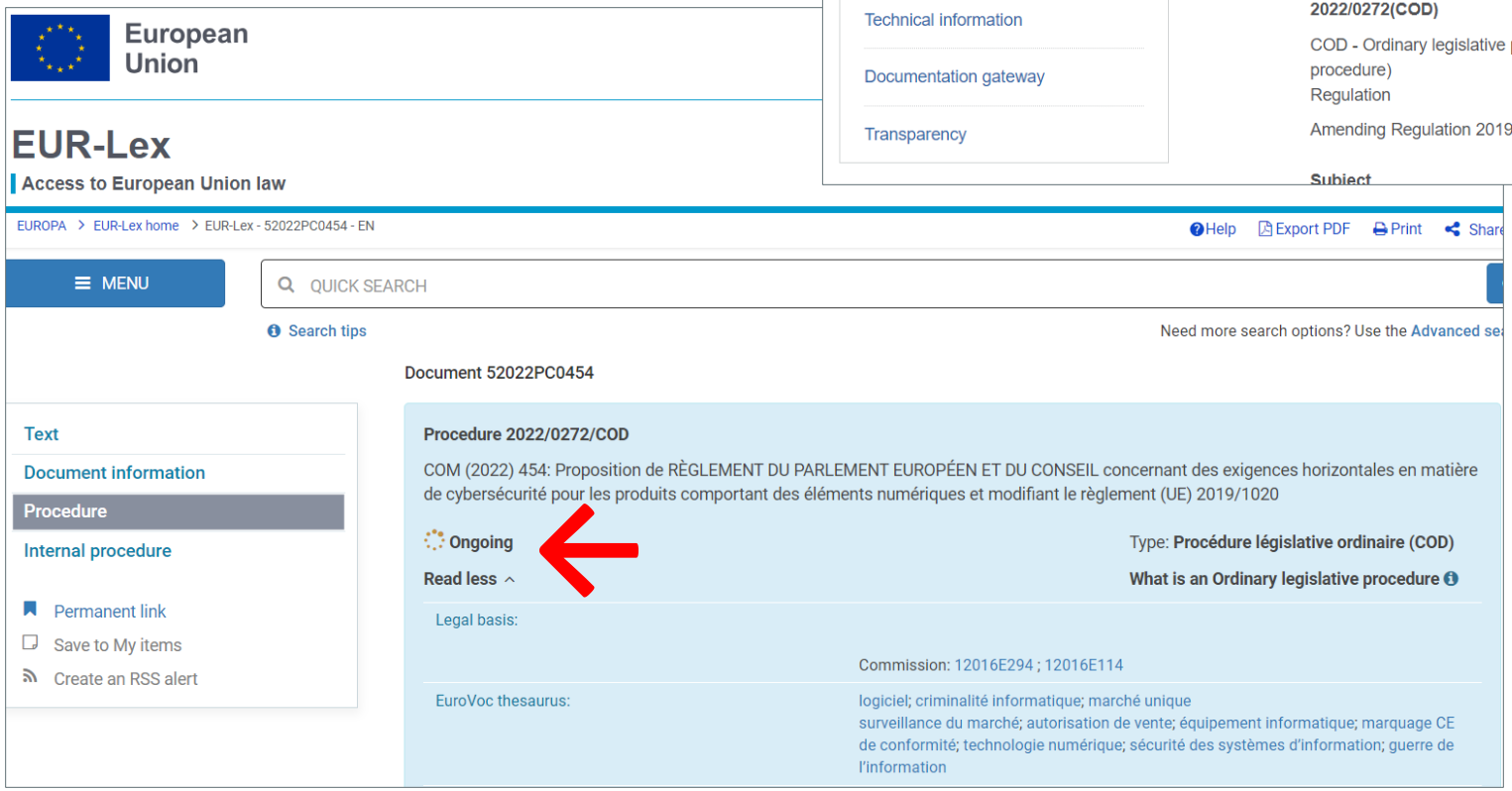
Cyber Resilience Act

Présentation générale

NIS Team CCB

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Disclaimer



Bien qu'il soit à peu près certain que le règlement sera adopté en l'état, il est encore susceptible d'être modifié, recalé, amendé, …

Les éléments présentés ci-après sont à prendre au conditionnel

Agenda

1. Introduction et scope
2. Mesures
3. Implémentation

CENTRE FOR CYBERSECURITY BELGIUM

Introduction et scope

01

CRA, c’est quoi?

CENTRE FOR CYBERSECURITY BELGIUM

Le problème: Trop de produits connectés (**IoT**) avec des standards de cybersécurité bas & des **vulnérabilités connues** sont mis sur le marché.
→ Des attaques auraient pu être évitées avec un simple patching
→ Les utilisateurs ne connaissent souvent pas les risques & les fabricants du produit devraient faire en sorte qu’il soit aussi facile que possible pour leur produit de rester sécurisé.

Le **Cyber Resilience Act (CRA)** est un nouveau règlement UE qui imposes des obligations minimales de cybersécurité pour tous les produits comportant des éléments numériques (IoT, software):

- avant qu’ils soient mis sur le marché UE (**security by design & by default, transparence utilisateur, etc**)
- durant l’entièreté du cycle de vie (**gestion des vulnérabilités, màj documentation, etc**)
- avec des **évaluations de la conformité** & une surveillance du marché fondée sur le cadre existant de régulation des produits (marquage CE et autorités de marchés

Scope CRA

Le CRA **s'applique aux produits comportant des éléments numériques mis à disposition sur le marché:**

- Incl. **hardware, software & composants,**
- Incl. les **produits pour consommateurs, pour B2B** systèmes industriels complexes (*ex* : laptops, home cameras, système d'exploitation, apps mobile, modems, VPNs, gestionnaires de mdp, smart meters...)

Pour autant que leur utilisation comprenne une connexion à un dispositif ou un réseau

Les fabricants mettant ces produits sur le marché UE doivent respecter le CRA, même s'ils sont établis dehors de l'UE (ex: Fabricant chinois de panneaux solaires sont *in scope*).

Scope CRA - Out of scope

CENTRE FOR CYBERSECURITY BELGIUM

Le CRA ne s'applique pas:

- **aux produits faisant déjà l'objet de régulations suffisantes (**dispositifs médicaux, dont diagnostic in vitro, composants de véhicules à moteurs, aviation civile, équipements marins, etc)

- **aux produits développés ou modifiés exclusivement à des fins de sécurité nationale ou de défense** (en ce compris la gestion d'informations classifiées)

CENTRE FOR CYBERSECURITY BELGIUM

Mesures

02

Proportionnalité des obligations CRA

Les exigences de cybersécurité imposées par le CRA **sont les mêmes pour tous les produits *in scope***, mais…

- …**différents niveaux de contrôle,** selon la **"criticité"** (standard vs. important vs. "very" important vs. critical products), de l'auto-évaluation à la certification.

- **Régime de conformité plus léger pour les logiciels open source** (lorsqu'ils sont commercialisés sous le modèle de la **fondation** cf. Eclipse, Linux…). Si la fondation agit comme "steward", elle n'est **pas responsable** du travail de développeurs individuels *mais*:
  - elle doit documenter sa politique de cybersécurité
  - elle doit notifier les incidents graves et vulnérabilités exploitées dont elle a connaissance
  - elle est encouragée à participer à des programmes volontaires d'attestation de sécurité

Les exigences du CRA

CENTRE FOR CYBERSECURITY BELGIUM

Annexe I.1. Exigences de cybersécurité

- **Security by design**
- **Secure by default** configuration (ex. Màj de sécurité automatique, refus de mdp faible, etc)
- Mesures de protection contre les accès non-autorisés
- **Protection de la confidentialité** des données, par exemple en les chiffrant
- Limitation de la surface d'attaque
- **Mise à disposition sans vulnérabilités connues**
- etc.

Annexe I.2. Gestion des vulnérabilités

- **Documenter** les vulnérabilités
- Effectuer des tests de sécurité réguliers
- Mettre en place une politique de divulgation coordonnée des vulnérabilités (CVDP)
- etc.

+ Annexe II Informations utilisateurs

- Mention claire de la **fin de la période d'assistance** (qui correspond à la durée de vie prévue du produit)
- Informations sur le fabriquant
- Identification du produit
- Installation des màj de sécurité
- etc.

Comment effectuer l'évaluation de la conformité?

	Auto-évaluation sur base du CRA Annex I	**Auto-évaluation sur base de normes harmonisées CRA**	**Evaluation de la conformité par un tiers** (CAB)	**Certification européenne de cybersécurité** (qui couvre le CRA)
Produits connectés	**Y**	Y	Y	Y
Produits importants (classe I)	N	**Y**	Y	Y
Produits importants (classe II)	N	N	**Y**	Y
Produits critiques	N	N	(pour autant qu'il n'y ait pas de certification EU de cybersécurité disponible)	**Y**

Après cette évaluation → Déclaration de conformité à émettre pour obtenir le marquage CE

Exemple: smart watch

Avant de pouvoir être mise sur le marché EU, le fabricant doit:

- Effectuer une analyse de risques de cybersécurité
- Se mettre en conformité avec les exigences du CRA (ex. Pas de vulnérabilités connues, refus de mdp faible, maj automatique par défaut, date de fin de support claire, etc)
- Créer et mettre à disposition les instructions utilisateurs
- Créer et mettre à disposition la documentation technique
- Faire procéder à l'évaluation de la conformité (par ex. par un CAB)
- Emettre une déclaration de conformité → apposer le marquage CE

Durant toute la durée de vie du produit (5 ans min. sauf si le produit a un cycle de vie plus court), le fabricant doit:

- Gérer les vulnérabilités, par ex. en fournissant des màj de sécurité
- notifier les vulnérabilités activement exploitées & les incidents graves (early warning dans les 24h, notification dans les 72h, rapport final dans les 14j/le mois).

CENTRE FOR CYBERSECURITY BELGIUM

Implémentation

03

CRA implementation prevue (EU level)

- ~~**Septembre 2024 (tbc)**~~: Adoption formelle par le Conseil
  → octobre 2024?
- **Octobre 2024 (tbc)**: Publication dans le Journal officiel UE & entrée en vigueur 20 jours après publication
- **18 mois plus tard (~printemps 2026):** notification des organismes d'évaluation de la conformité (CABs)
- **21 mois plus tard (~été 2026):** Obligation de notifier **les vulnérabilités & et les incidents** pour les fabricants
- **3 ans plus tard (~automne 2027):** Le CRA est entièrement applicable (**security by design & by default** avant la mise sur le marché d'un produit connecté, **transparence utilisateur** et gestion des **vulnérabilités** Durant tout le cycle de vie du produit)

CENTRE FOR
CYBERSECURITY
BELGIUM

NIS Team CCB
nis@ccb.belgium.be

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

[expleo]

Démo live d'une cyber-attaque sur un drône

Cyberwal
by digital
wallonia

Drone Security

& Life Hacking

#securingthefuture

expleo

Think bold, act reliable

Agenda

- **Hacks & Stats**
- **ExpleoSmeeta Project**
- **Demo**
- **Key Takeaways**

Hacks & Stats

#securingthefuture

exploeo

Think bold, act reliable

Hacks & Stats

7.6M 

Drone flight hours in 2023 (in the world)

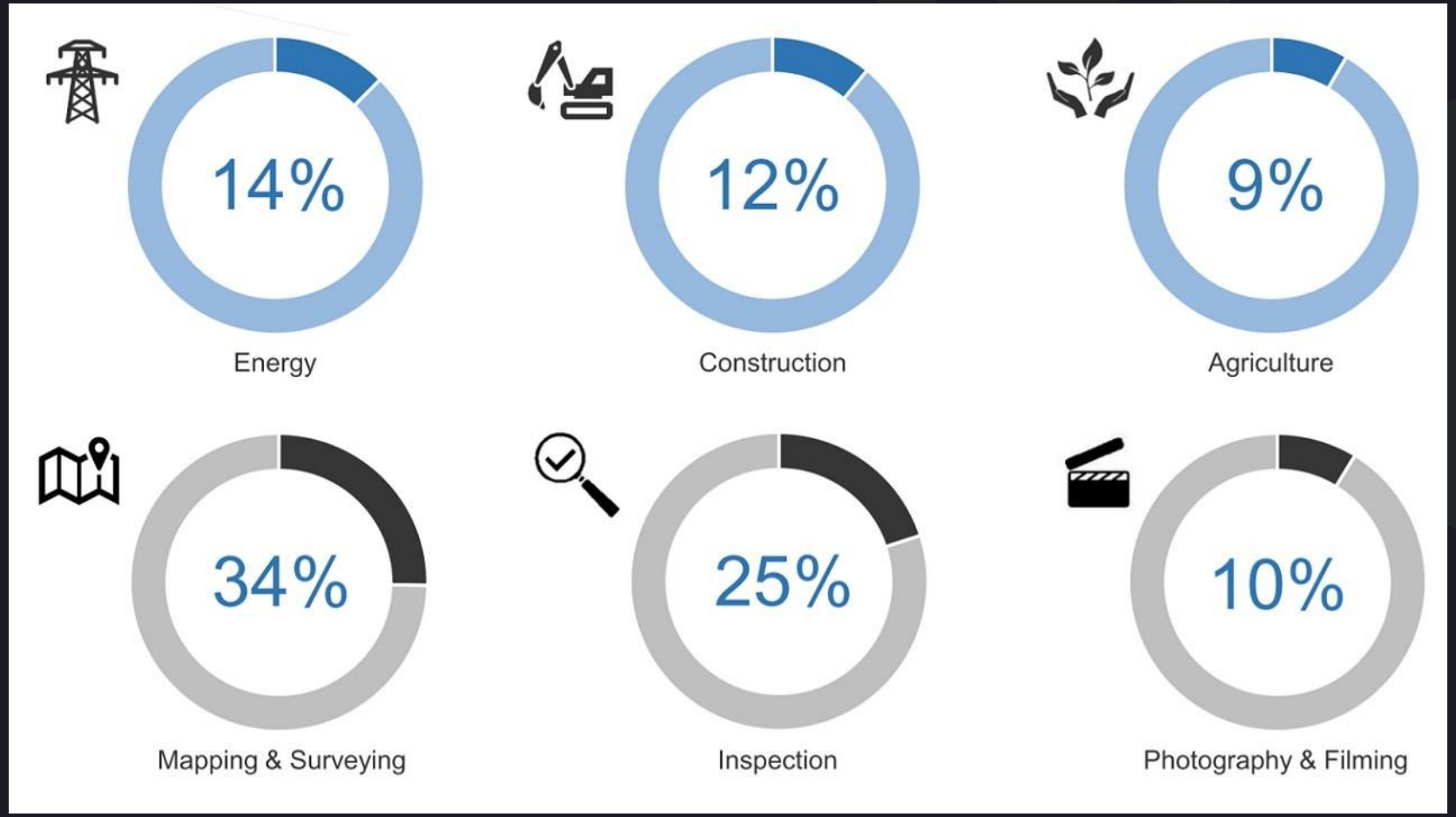
x7 

Growth of Vulnerabilitie's number affecting Drones products between 2022 & 2023

Drone Cybersecurity Market
USD 55 Billion in 2023
USD 106.03 Billion by 2031

Drones Application

Credit: Drone Industry Insights



expleo

Hacks & Stats

Forbes

FORBES > BUSINESS > AEROSPACE & DEFENSE

Ukrainian Marines Hacked A Russian Drone To Locate Its Base—Then Blew Up The Base With Artillery

David Axe Forbes Staff

David Axe writes about ships, planes, tanks, drones and missiles.

Follow

26 Nov 30, 2023, 05:45pm EST

A 36th Marine Brigade drone-operator with his quadcopter drone. 36TH MARINE BRIGADE PHOTO

sudo apt-get update cyber_news

Followed by 4.50+ million

The Hacker News

Subscribe – Get L

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Expert Insights Contact

TIDRONE Espionage Group Targets Taiwan Drone Makers in Cyber Campaign

Sep 09, 2024 Ravie Lakshmanan Cyber Attack / Threat Intelligence

A previously undocumented threat actor with likely ties to Chinese-speaking groups has predominantly singled out drone manufacturers in Taiwan as part of a cyber attack campaign that commenced in 2024.

Trend Micro is tracking the adversary under the moniker **TIDRONE**, stating the activity is espionage-driven given the focus on military-related industry chains.

The exact initial access vector used to breach targets is presently unknown, with Trend Micro's analysis uncovering the deployment of custom malware such as CXCLNT and CLNTEND using remote

— Trending News

5 Must-Have Tool
Dynamic Malware

Hacks & Stats

AIRSIGHT
UAS & Drone Pilot Detection

Software

Flying the Phantom 3 over Facebook's Data Center

The Geek Pub
LET'S MAKE STUFF

Hacking capabilities of drones

Post Share Share 0

New Data Center Security Threats: An Overview of the Hacking Capabilities of Drones

BlackBerry Cybersecurity Automotive & IOT Critical Communications

The Drone Cyberattack That Breached a Corporate Network

CYBERSECURITY / 10.21.22 / Bruce Sussman

No one at the investment firm must have noticed the whirring of drone
– if they made any noise at all.

But once there, the attack drones began carrying out their secret missio

This is the true story of a drone attack that led to a corporate data brea

Greg Linares
@Laughing_Mantis

This lead the team to the roof, where a 'modified DJI Matrice 600' and a 'modified DJI Phantom' series were discovered.

The Phatom was carring a 'modified Wifi Pineapple Device'

It appeared neatly landed and was not damaged

Greg Linares
@Laughing_Mantis

During their investigation they determined that the DJI Phantom drone had originally been used a few days prior to intercept a workers credentials and WIFI.

This data was later hard coded into the tools that was deployed with the Matrice.

{ expleo }

Hacks & Stats

yahoo!tech Search the web News Finance

Today in Tech The 15 best Prime Day tech deals Best Prime Day Apple deals Best Prime Day deals on Amazon

GIZMODO

Researchers Spin up Terrifying Hacker Drone That Can 'See Through Walls' With Wifi

Lucas Ropek
November 5, 2022 · 3 min read

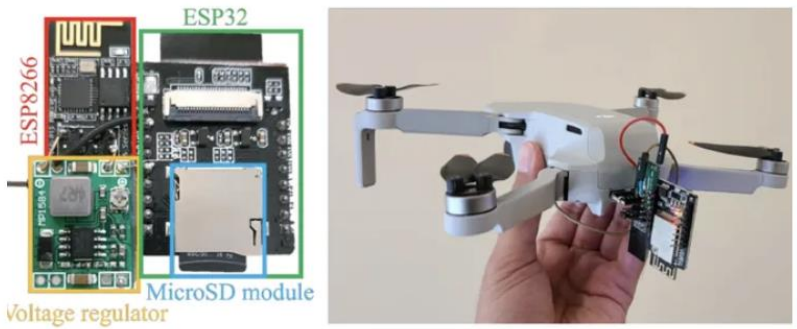


Figure 2: Wi-Peep [1]

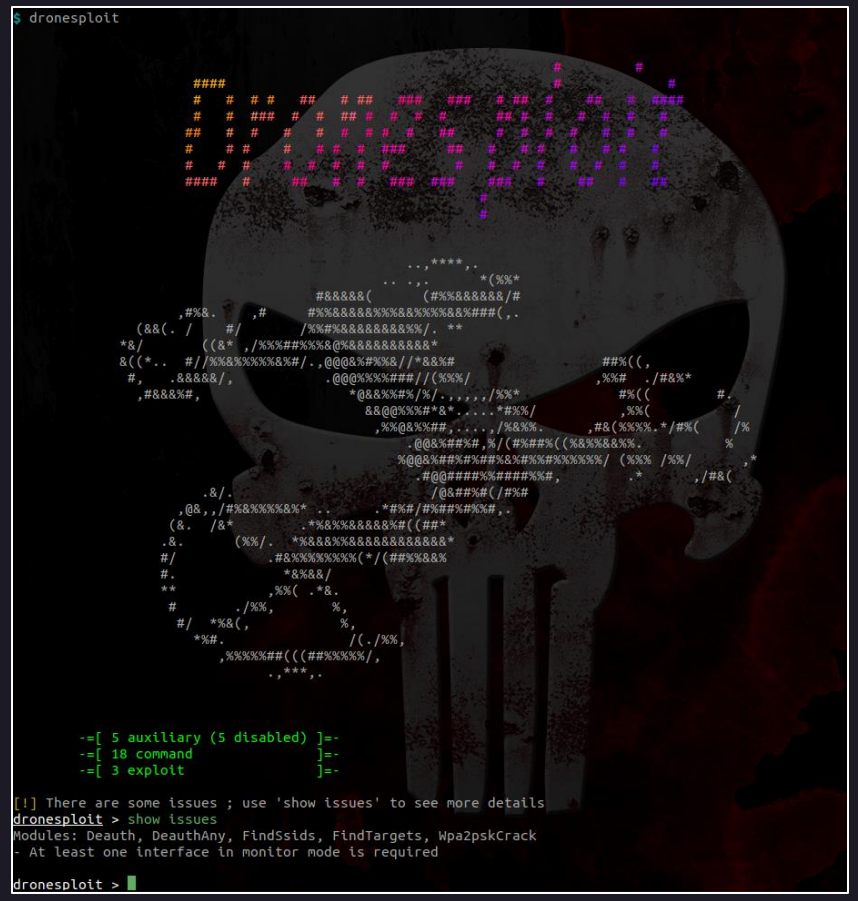
WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH PRIME DAY

This Hacker Tool Can Pinpoint a DJI Drone Operator's Exact Location

Every DJI quadcopter broadcasts its operator's position via radio—unencrypted. Now, a group of researchers has learned to decode thos

expleo

Hacks & Stats



README MIT license

Drone Hacking Tool

Drone Hacking Tool is a GUI tool that works with a USB Wifi adapter and HackRF One for hacking drones.

license MIT

Overview

Drones, as a high mobility item that can be carried around easily and launched, are becoming cheaper and more popular among the public, they can be seen almost anywhere nowadays.

However, the drone built-in flying cameras could use for illegal usage like candid photos on private property. This shows drones clearly present risks to public safety and personal privacy.

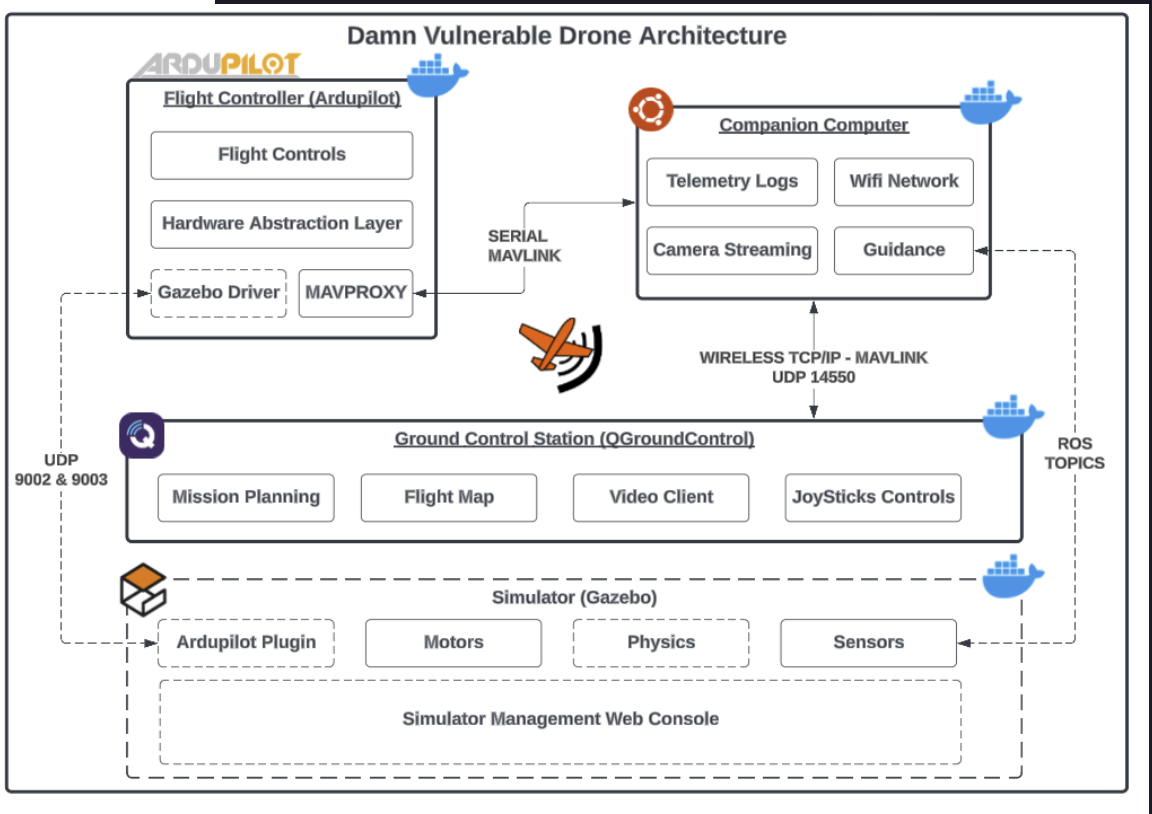
Therefore, we are working on using wireless connection methods (Wi-Fi, GPS) to hack it and take over. In this project, our goal is to capture drones to stop users with malicious intent for proof of concept and a sense of accomplishment.

expleo

Hacks & Stats

Damn Vulnerable Drone

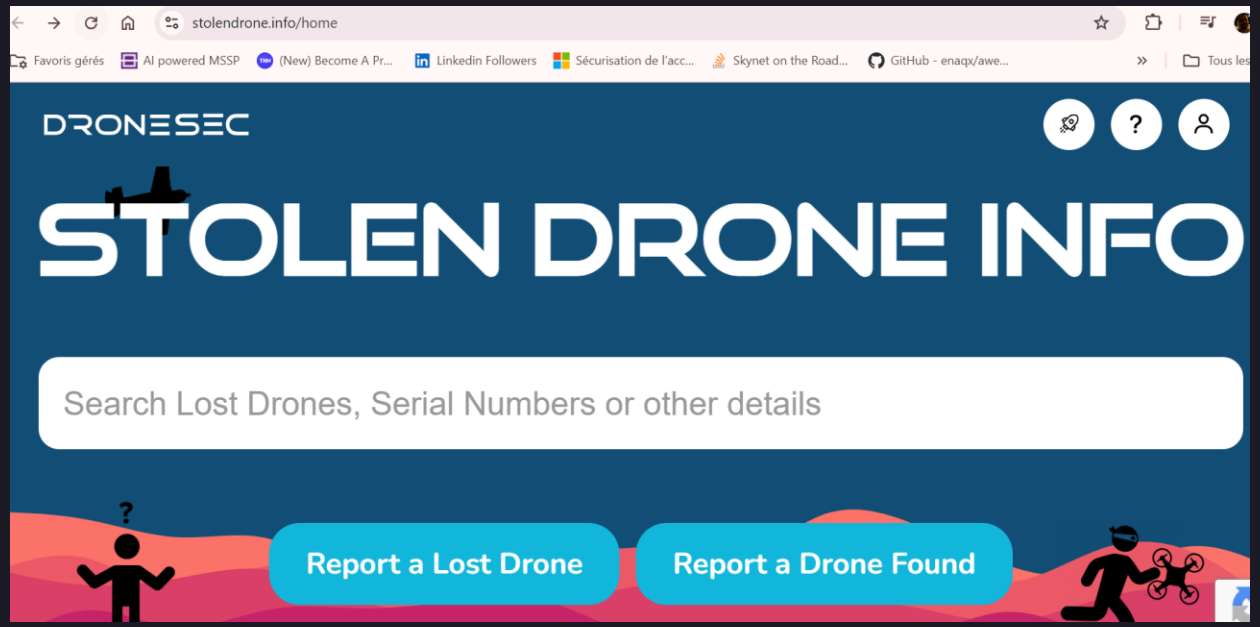
The Damn Vulnerable Drone is an intentionally vulnerable drone hacking simulator based on the popular ArduPilot/MAVLink architecture, providing a realistic environment for hands-on drone hacking.

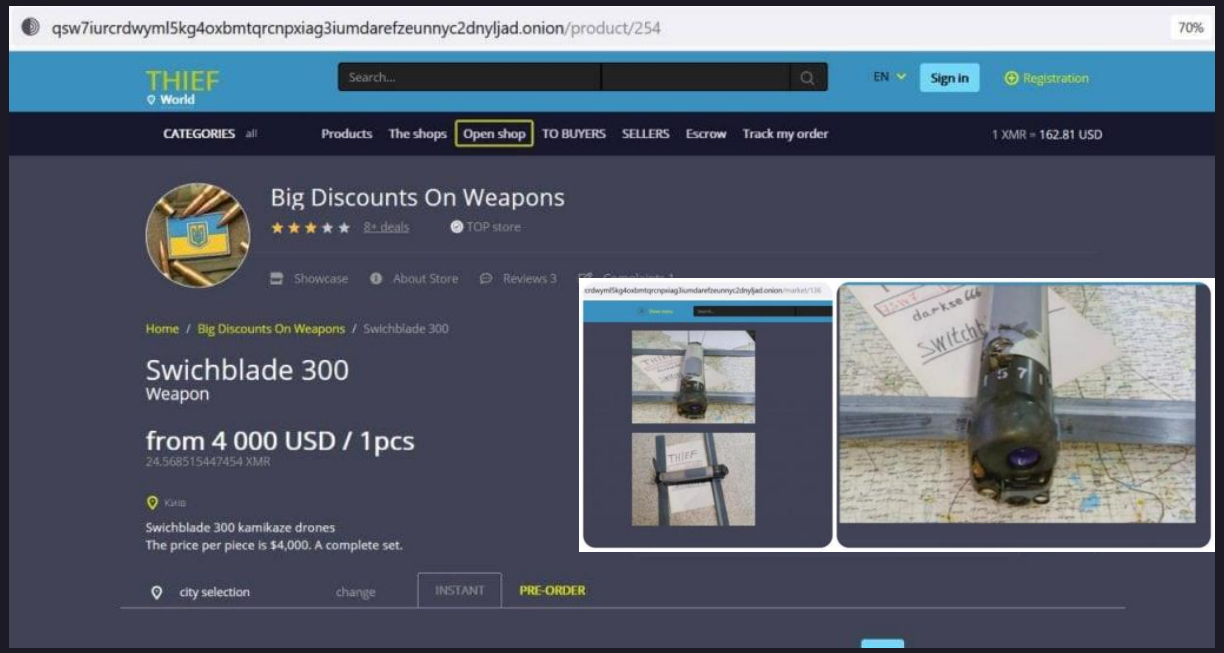


expleo

Hacks & Stats

FAKE?





expleo

ExpleoSmeeta

#securingthefuture

expleo

Think bold, act reliable

ExpleoSmeeta
Briefcase

- **All-in-one Framework**
- **Simple to use**
- **Portable Solution**
- **Totally customizable**
- **Several versions**

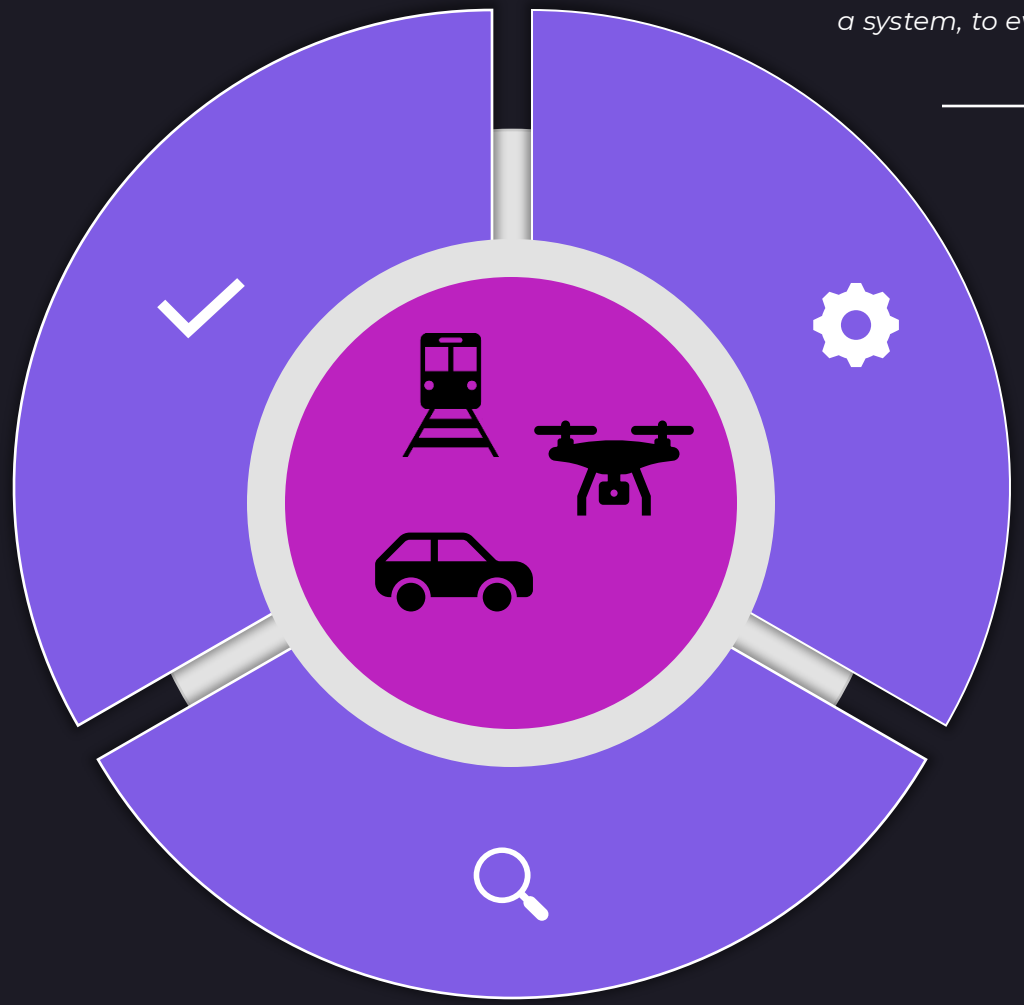
Ensuring the security of connected vehicles

PENETRATION TESTING

Authorised simulated cyberattack on a system, to evaluate its security

VULNERABILITY ASSESSMENT

Identify, quantify and prioritise the vulnerability



FORENSICS

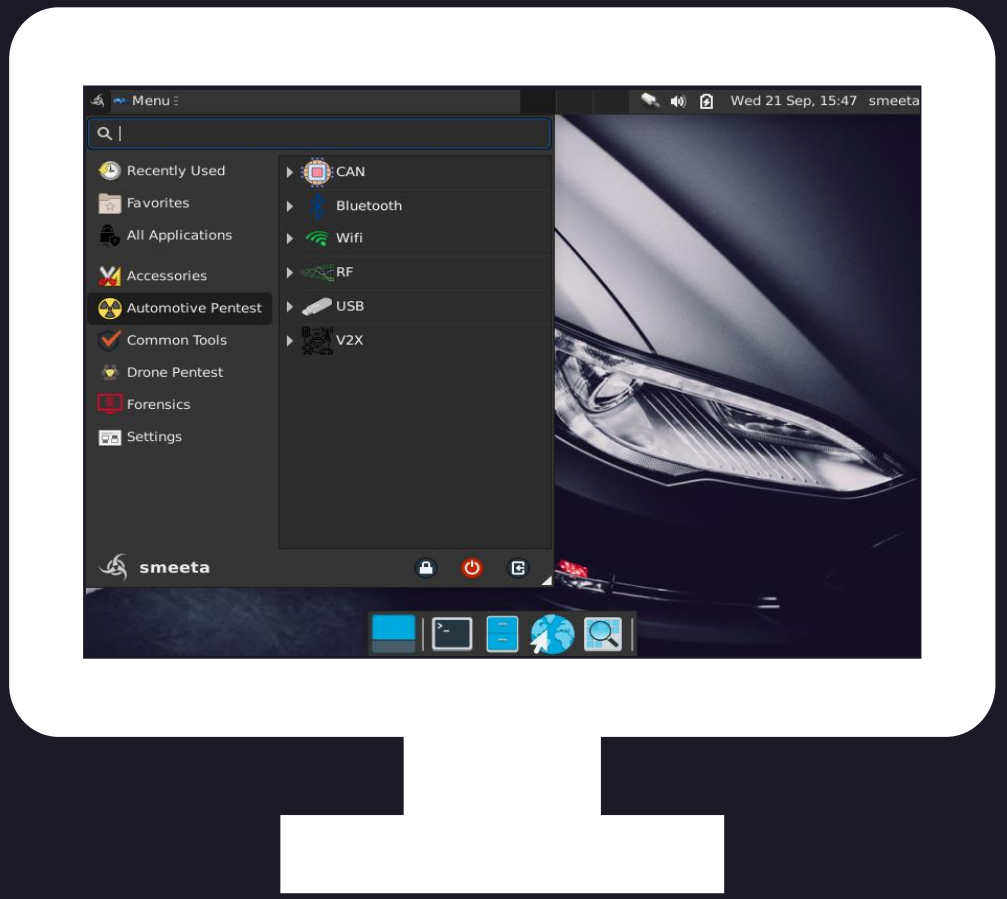
Tools to assist during the phases of the digital investigation

expleo

ExpleoSmeeta OS

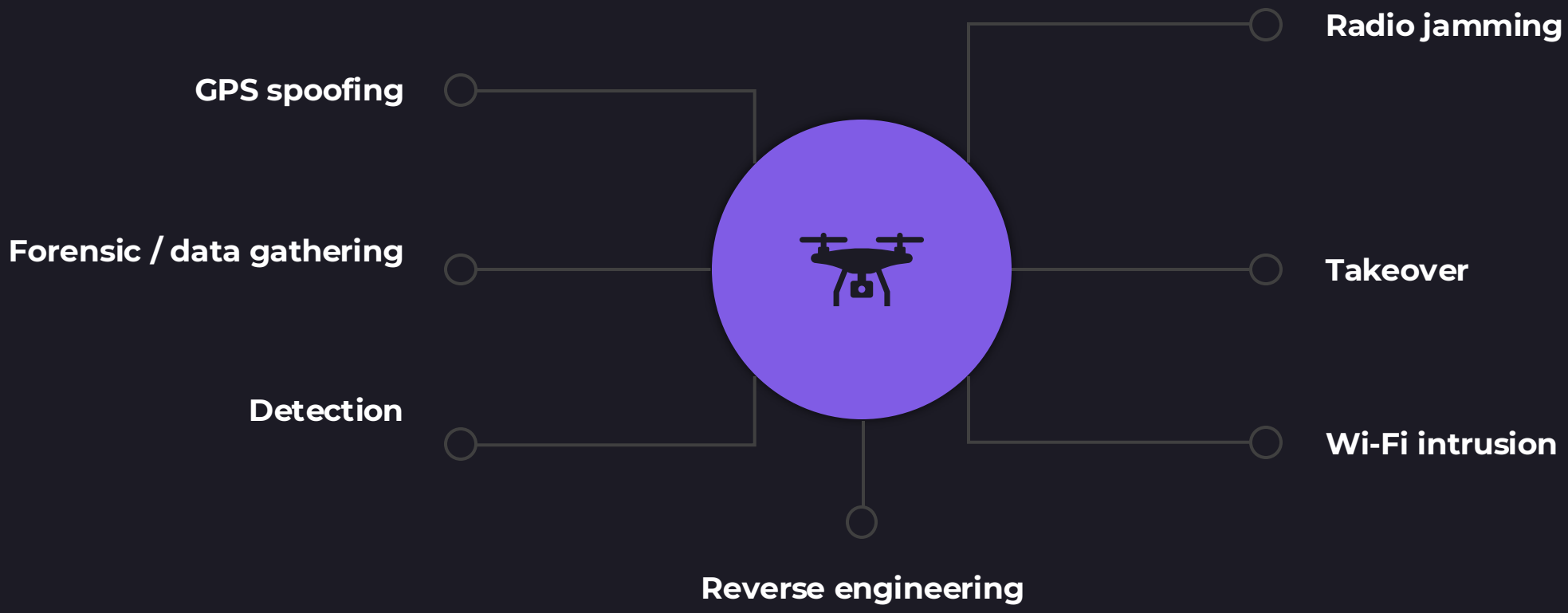
A Linux distribution derived from Debian (version 11 "Bullseye") and specialized in **vehicle security** assessment.

Debian modules not useful for this purpose have been removed while **specific tools** for vehicle attacks were added. The user interface has been designed in graphical and organisational ways to **optimise the use** of this operating system and highlight the most relevant menus.



expleo

Drone attacks

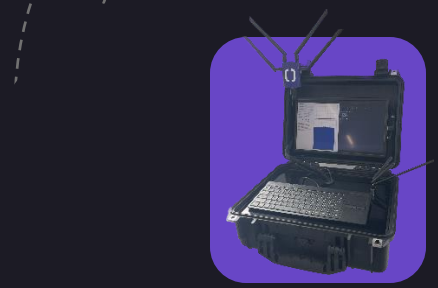


Demonstrations planned.

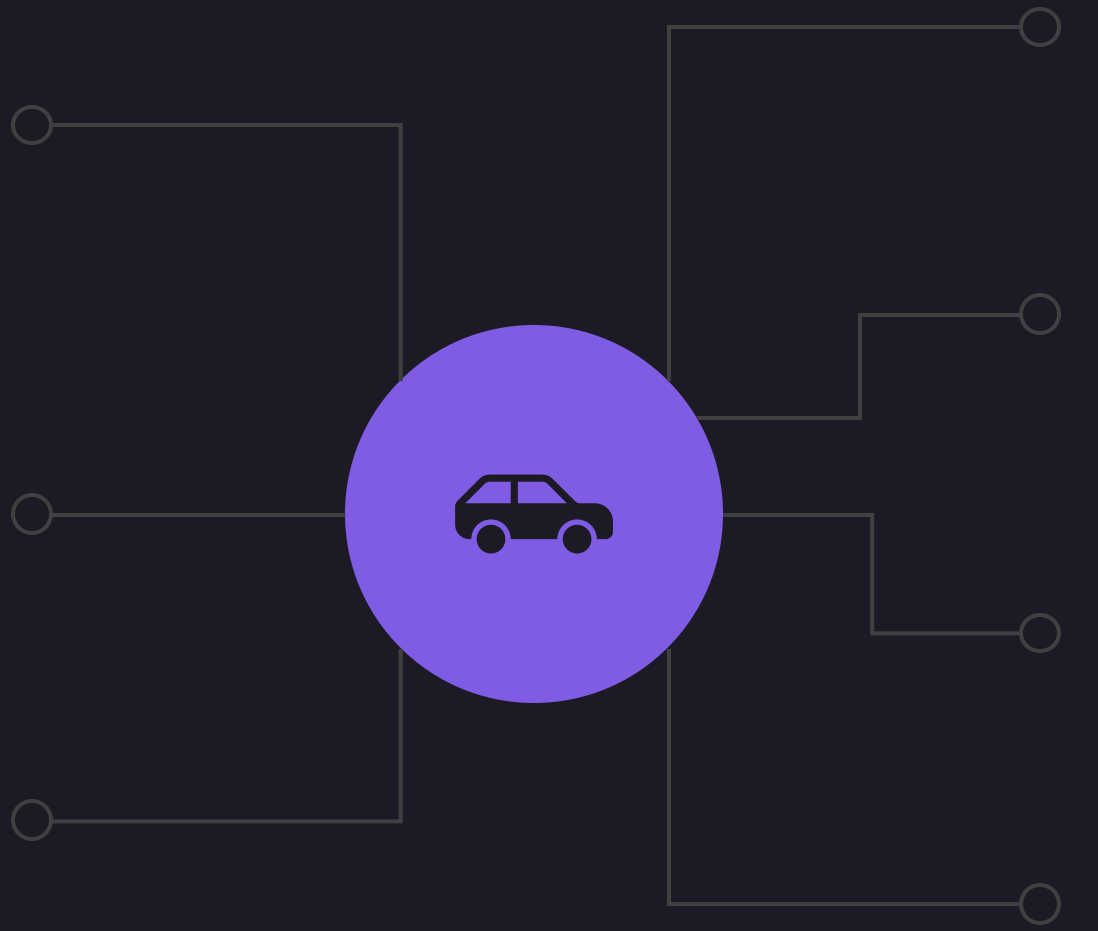
expleo

Use Cases

- **Drone Detection & Jamming**
- **Takeover a Drone and turn it to facial recognition engine**
- **Intercept Drone-to-Drone communication**
- **Compromise Privacy and collect personal data**
- **Trick a drone into landing and reverse engineer the technology**



Other attacks



RADIO FREQUENCY

Replay
Relay
RollJam
RollBack
GPS tracking
GPS Spoofing

CELLULAR, WIFI, BLUETOOTH, TELEMATICS

Malicious firmware updates
V2X attacks

SENSORS

Blind spot exploitation
Sensor interference
Spoofing (TPMS)
Jamming

CAN BUS

Frame attacks
Eavesdropping
Fuzzing
Replay
Spoofing
Flooding
Reverse Eng.

PROTOCOLS ATTACK

Bus-off attack
Janus attack
Error attack
Double receive attack

UART- JTAG

Firmware extract
Root shell access

USB, CD and SD Cards

Malicious code injection
Theft of sensitive data

expleo

Quick Demo

#securingthefuture

expleo

Think bold, act reliable

Key Takeaways

#securingthefuture

exploro

Think bold, act reliable

Drones Empower Hackers

Drones become a “payload” to carry out :

- **Information Gathering**
- **Data Stealing**
- **Surveillance**
- **Network Disruption**
- **Network Intrusion**
- **Etc.**

Hacking Drones Scenarios

Reconnaissance	Protocol Tampering	Denial of Service	Injection	Exfiltration	Firmware Attacks
Wifi Analysis & Cracking	Telemetry Spoofing	Battery Drain Attack	MAVLink Command Injection	Flight Log Extraction	Firmware Decompile
Drone Discovery	Flight Mode Spoofing	Communication Link Flooding	Camera Gimbal Takeover	Parameter Extraction	Firmware Modding
Packet Sniffing	Drone State Spoofing	Denial-of-Takeoff	Waypoint Injection	Mission Extraction	
Protocol Fingerprinting	GPS Spoofing	Geo-Squeezing	Sensor Data Injection	FTP Eavesdropping	
GPS & Telemetry Analysis		Altitude Limiting	Flight Mode Injection	Camera Feed Eavesdropping	
Payload Detection		GPS Jamming			
		Wireless Deauthentication			

Deploy Drones Securely within your information system

Build a Risk Based Stratregy

Network Segregation and Zero Trust Architecture

Consider this Subnet as an External

Access Control

limit of one for the number of devices that can connect to your base station.

Monitor and Detect Suspicious Activities

Controller, Access Point, Drones

Drones Hardening before deployment

Strong Password

Ensure activation of "Return to Home" (RTH) mode.

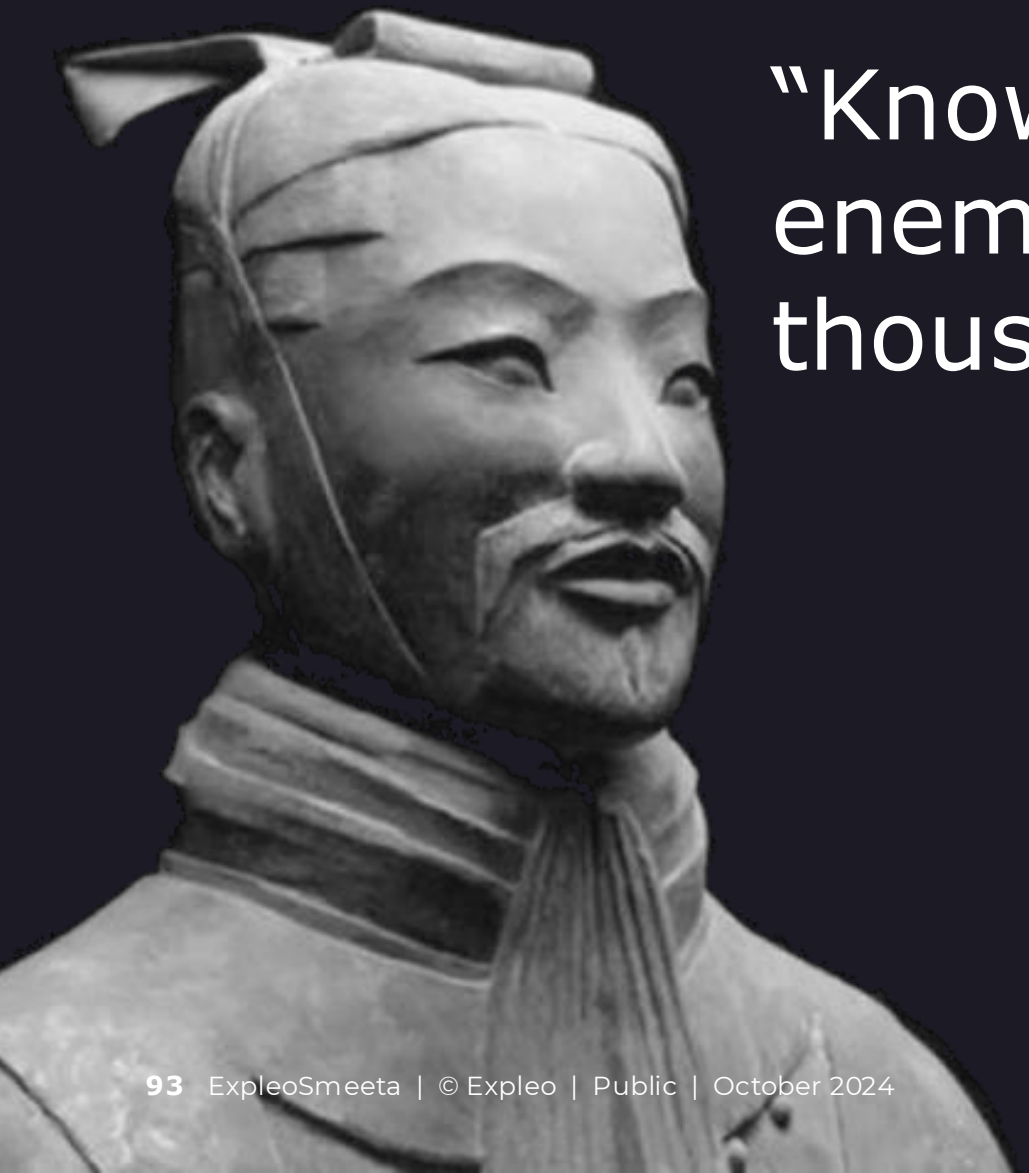
Vulnerability and Obsolescence Management

Firmware, Controller, Access Point, Drones

Asset Management

Ensure that this OT Device is managed

expleo



"Know thy self, know thy enemy. A thousand battles, a thousand victories."

Sun Tzu, The Art of War

[expleo]

[expleo]

Think bold, act reliable

L’événement reprendra dans 15 minutes.

Cyberwal by digital wallonia

SIAPARTNERS

Démo -

Utilisation d'un simulateur numérique pour mener une cyber-attaque sur un système industriel virtuel

Cyberwal
by digital
wallonia

Cyber Crisis Awareness Platform

Digital simulator

Cyberwal by digital wallonia

Wallonie Relance

SIAPARTNERS

Speakers

Nina Hasratyan
Agence du Numérique

nina.hasratyan@adn.be

Jeremy Grandclaudon
Agence du Numérique

jeremy.grandclaudon@adn.be

News

Cyberattaques en Belgique : les sites de services bancaires visés ce jeudi

Une nouvelle salve de cyberattaques a visé des sites internet belges ce jeudi 10 octobre 2024. Cette fois-ci, ce sont ceux de Febelfin (la fédération du service bancaire) et du SPF Economie qui ont été ciblés, confirme le Centre pour la cybersécurité Belgique (CCB).

BELGIQUE

Cyberattaques de sites d'autorités belges : "L'objectif est de décrédibiliser les autorités à quelques jours des élections"

RTL info ACTU SP

Le secteur de la santé belge de plus en plus ciblé par des cyberattaques: "Cela permet de pouvoir négocier une rançon"

Publié le 04/08 à 11h05 Par RTL info avec Cath

LE SOIR

24 Opinions Podcasts Politique Société Monde Économie Vidéos Sports

ACCUEIL • SOCIÉTÉ

Nouvelle cyberattaque en Belgique : plusieurs sites communaux et portuaires visés

Le groupe de hackers qui a attaqué des sites gouvernementaux lundi a visé des ports et des communes ce mardi.

Cyberattaque à l'hôpital d'Armentières : une réouverture des urgences espérée lundi dans la journée

remière fois que
attaque.

Technologie

Belgique : 200 sites gouvernementaux victimes d'une vaste cyberattaque

L'attaque a eu lieu au moment où une commission parlementaire belge, chargée de déterminer s'il convient d'accuser la Chine de génocide à propos du traitement des ouïghours, se réunissait.

DUVEL, LA CHOUFFE: STOPPÉE APRÈS UNE CYBERATTAQUE, LA PRODUCTION DES BIÈRES BELGES REPREND

Data breach CYBERSÉCURITÉ \ DONNÉES PERSONNELLES \ BELGIQUE

Un fournisseur de la ville de Bruxelles visé par une cyberattaque, des données personnelles dérobées

Presentation of the cyber crisis awareness platform

In a context where cyber threats are omnipresent, awareness of risks and best practices is becoming imperative for organizations. In an environment where cyber threats are omnipresent, organizations must prioritize understanding risks and adopting best practices. To enhance awareness among Walloon institutions and businesses regarding cyber risks and effective IT hygiene, L'Agence du Numérique sought to develop a cyber crisis awareness platform. This innovative tool allows for the simulation of various cyber-related crisis scenarios, by staging incidents, their impacts, and the solutions to address them, thus offering an immersive experience that prepares organizations to face these threats.

48 **Engaging, multidimensional crisis scenarios crafted to enhance cybersecurity awareness in a crisis context.**

4 **strategic sectors of activity representative of the Walloon economic and social fabric: Health , Industry 4.0 , Public Sector , SMEs .**

3 **levels of complexity that involve more or less sophisticated attacks.**

Cyberwal by digital wallonia · Wallonie Relance · SIAPARTNERS

An immersive platform promoting dynamic interactions

Dynamic interactions
Participants can engage in real-time through their smartphones, promoting active participation and interaction..

Knowledge development
Open to all participants, regardless of their cybersecurity knowledge level, this enriching experience allows everyone to enhance their skills.

Diversity of questions
Questions are tailored to various participant profiles based on their expertise, including legal teams, human resources, information security, communications, and specific professions.

“Coach” facilitator
The facilitator guides discussions, shares feedback and provides context and a broader perspective on the events unfolding in the scenario.

Chronological consistency
The scenarios progress chronologically, presenting realistic situations, diverse stimuli, and a mini-informant that offers insights into key concepts.

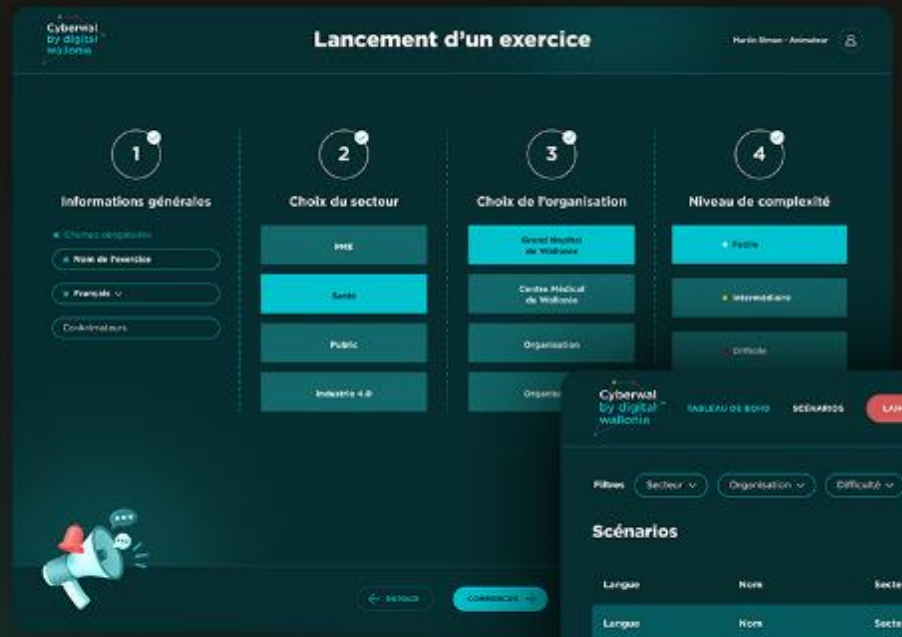
Realistic Cyber Attacks
The scenarios feature a range of proven cyber attacks grounded in real-world experiences.

Collaborative scenarios

With a **scripted approach**, the platform is tailored to different audiences, providing a clear and contextualized understanding of **cybersecurity** issues relevant to each specific sector.

During the simulation, participants **engage actively** through a variety of stimuli that encourage deeper thinking by answering both multiple-choice and open-ended questions. **Facilitated discussions** will emphasize best practices and incorporate feedback, providing participants with a practical perspective that is directly relevant to their professional environments.

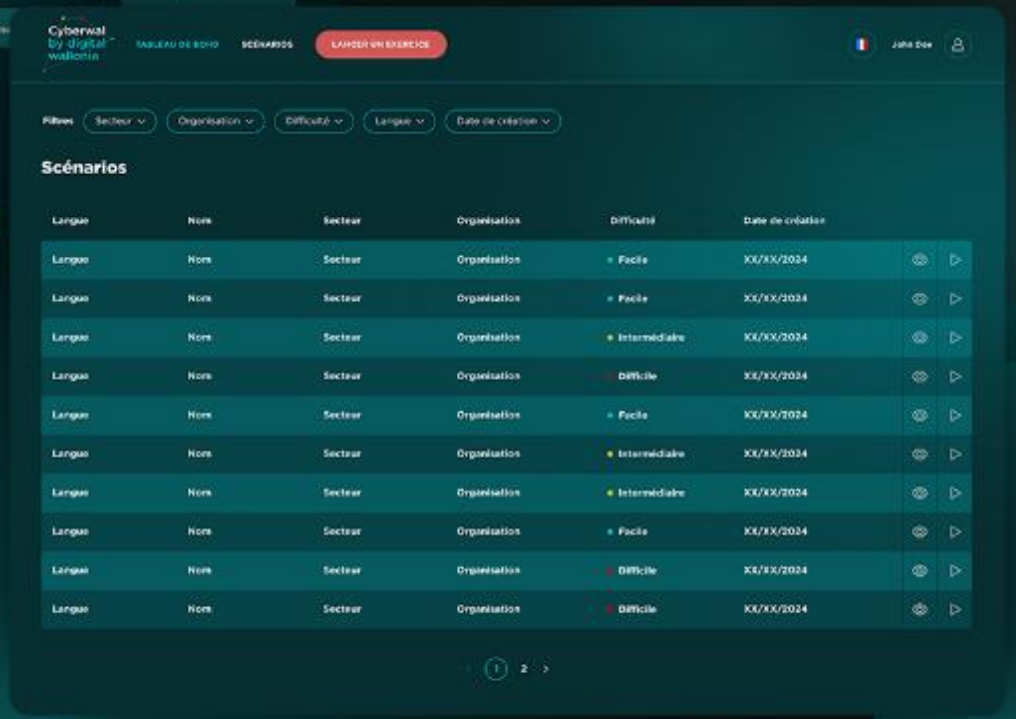

Cyberwal
by digital
wallonia
ANIMATEUR
PARTICIPANT
Identifiant
Mot de passe
Mot de passe oublié ?
Connexion
Se connecter avec
LA SENSIBILISATION SUR LA
cybersécurité pour
la Wallonie
Powered by SIAPARTNERS


Cyberwal by digital wallonia
Lancement d'un exercice
1
Informations générales
2
Choix du secteur
3
Choix de l'organisation
4
Niveau de complexité


Nom de l'exercice
SECTEUR PUBLIC.
Cible privilégiée des attaquants :
Les PME, vecteur d'attaque de grands organismes

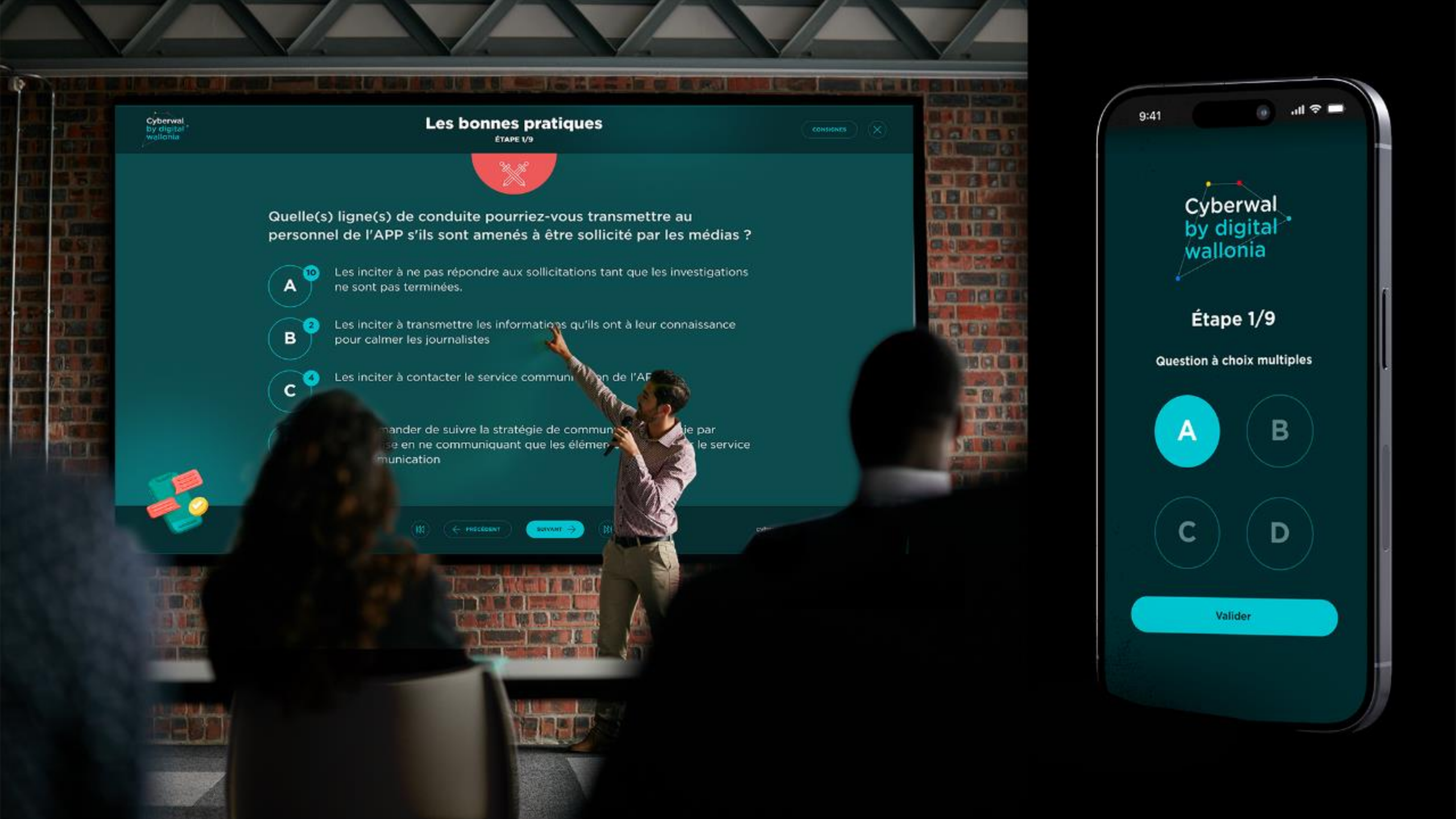

Cyberwal by digital wallonia
LA SENSIBILISATION SUR LA
cybersécurité pour la Wallonie
ANIMATEUR
PARTICIPANT
Code de la session
Accéder
Powered by SIAPARTNERS


Cyberwal by digital wallonia
Étape 1/9
Question ouverte
Vous pouvez soumettre 3 réponses !
Exemple 1
Réponse
Réponse
Valider


Cyberwal by digital wallonia
TABLEAU DE BORD
SCÉNARIOS
LANCER UN EXERCICE
John Doe
Filtres
Secteur
Organisation
Difficulté
Langue
Date de création
Scénarios
Langue
Nom
Secteur
Organisation
Difficulté
Date de création
Facile
Intermédiaire
Difficile
XX/XX/2024


Êtes-vous sûr de vouloir quitter ?
Attention, vous ne pourrez pas reprendre la session en cours.


Nom de l'exercice
ÉTAPE 1/9
Un des magasiniers a contacté les médias afin de les alerter des conditions de travail déplorables. Plusieurs journalistes se sont donc déplacés sur les lieux et tentent de s'introduire dans les locaux pour obtenir des informations et des séquences vidéo.


Cyberwal by digital wallonia
Les bonnes pratiques
ÉTAPE 1/9
CONSIGNES
Quelle(s) ligne(s) de conduite pourriez-vous transmettre au personnel de l'APP s'ils sont amenés à être sollicité par les médias ?
A
Les inciter à ne pas répondre aux sollicitations tant que les investigations ne sont pas terminées.
B
Les inciter à transmettre les informations qu'ils ont à leur connaissance pour calmer les journalistes
C
Les inciter à contacter le service communi on de l'AP
mander de suivre la stratégie de commun ie par
e en ne communiquant que les élémen le service
munication
PRÉCÉDENT
SUIVANT
9:41
Cyberwal by digital wallonia
Étape 1/9
Question à choix multiples
A
B
C
D
Valider

Cyberwal by digital wallonia

TABLEAU DE BORD SCÉNARIOS LANCER UN EXERCICE

Martin Simon - Animateur

Filtres Date Secteur (Santé) Difficulté Statut Langue EXPORTER

Vos scénarios par secteur

Évolution du score moyen/niveau

2024

Total de participants

379

15 animateurs

Total d'exercices

13

3 4 6

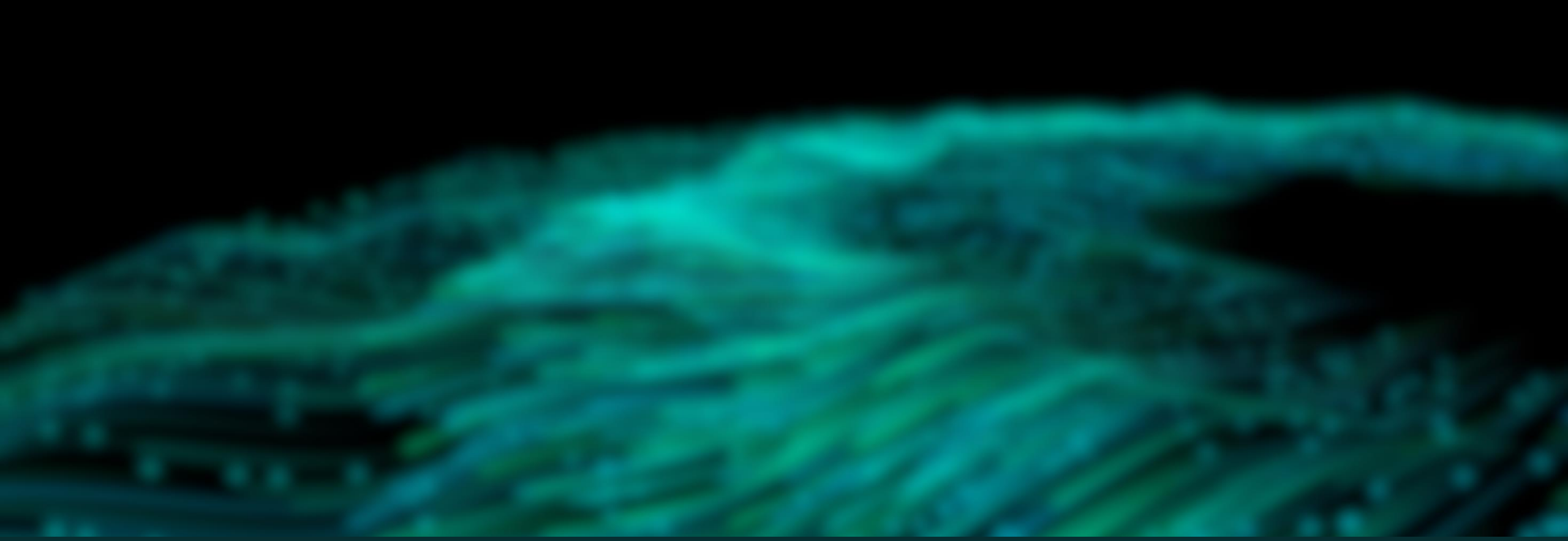
Score

50%

Min 35%
Max 65%

Vos exercices

Nom	Participants	Date	Difficulté	Scénarios	Statut
Nom	Participants	XX/XX/2024	Facile	Scénarios	REPRENDRE



Any questions?

Cyberwal by digital wallonia

Wallonie Relance

SIAPARTNERS

Geoffroy Moens

Schneider Electric

Cyberwal
by digital
wallonia

Welcome

Comprendre et Appliquer l’IEC 62443 pour une Sécurité Optimale

Speaker’s Biography

Geoffroy Moens
Cybersecurity Architect
Energy Management
Schneider Electric

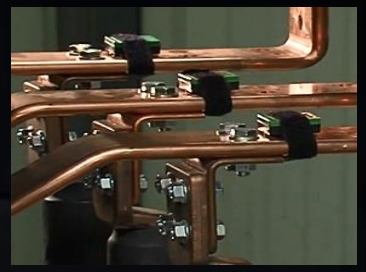
Why a Cybersecurity Standard for OT Environment

Facilities are "smart" and everything is connected.

All systems are comprised of more and more intelligent & connected equipment



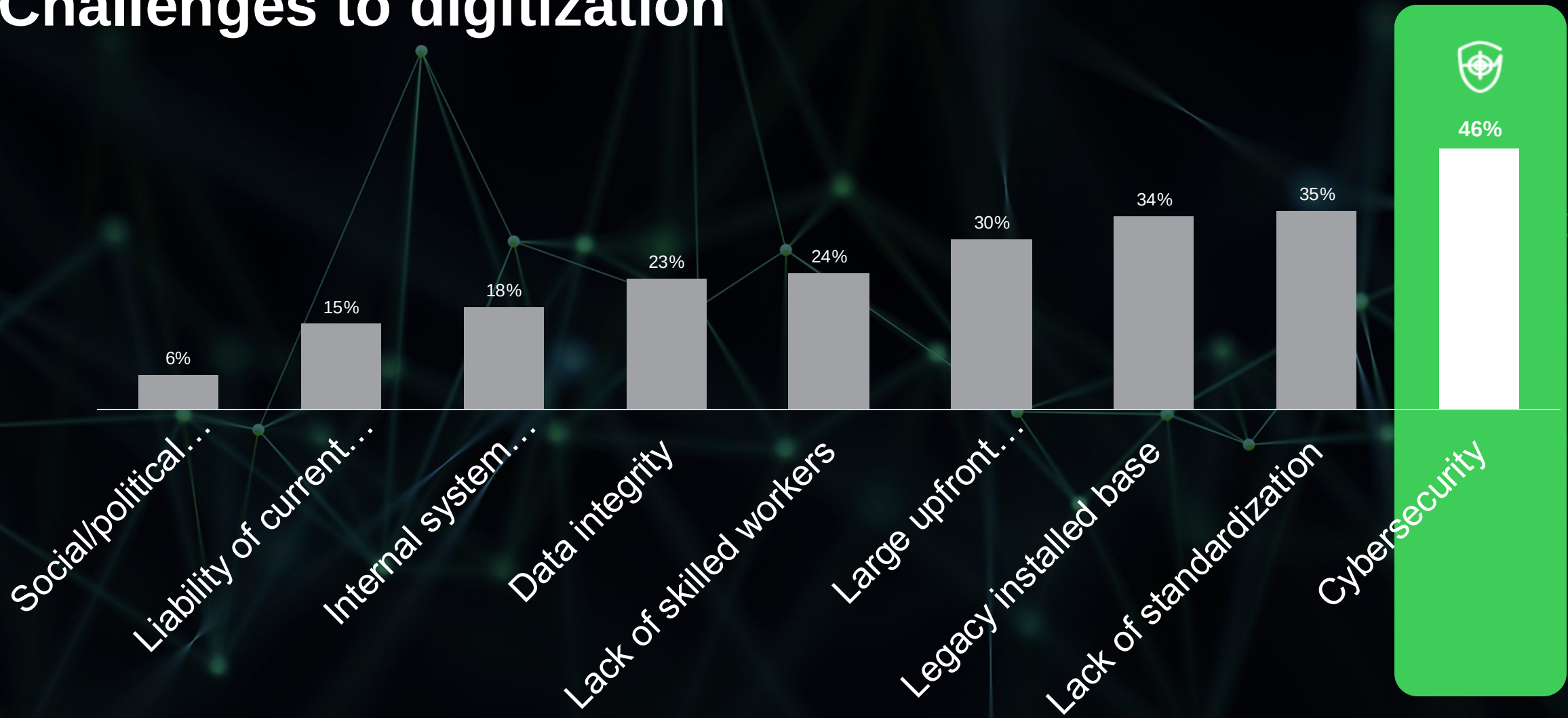






Life Is On Schneider Electric

Challenges to digitization



Source: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

What is the risk?

Likelihood X Impact = Risk

Likelihood is rising

Stuxnet
Iran nuclear plan

45,000 machines infected
PLC modified and destroyed

Uncontrollu
a blast furna
control componen
breakdowns

2024 - Water Supply & Treatment USA, France, Poland
Sandworm group manipulated chemical levels in water supplies

2010 2015

The impact of downtime is massive

Cost of disruption

Semiconductor production	**€ 3,800,000** per event
Financial trading	**€ 6,000,000** per hour
Data center	**€ 750,000** per event
Telecommunications	**€ 30,000** per minute
Steel works	**€ 350,000** per event
Glass industry	**€ 250,000** per event
200 room hospital	**€ 1,000,000** per 8 hour event
Off-shore O&G platform	**€ 30,000,000** per day

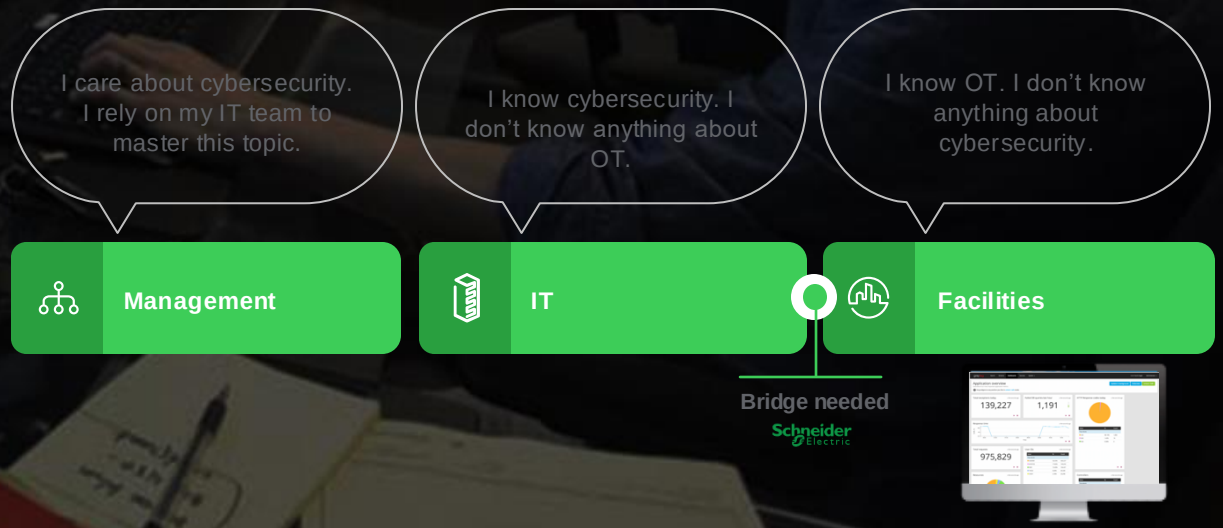
Source: Copper Development Association, Allianz Global Corporate & Specialty, & Customer testimony

Everyone has a role

IEC 62443 – Overview of the Standard

IT standards are not appropriate for Operational Technology environments. For example, they have different performance and availability requirements, and equipment lifetime.

Moreover, cyber-attacks on IT systems have essentially economic consequences, while cyber-attacks on critical infrastructure can also be heavily environmental or even threaten public-health and lives.



Why ISA / IEC 62443

World's only consensus-based standard automation and control system applications

Defines requirements and procedures for implementing electronically secure systems

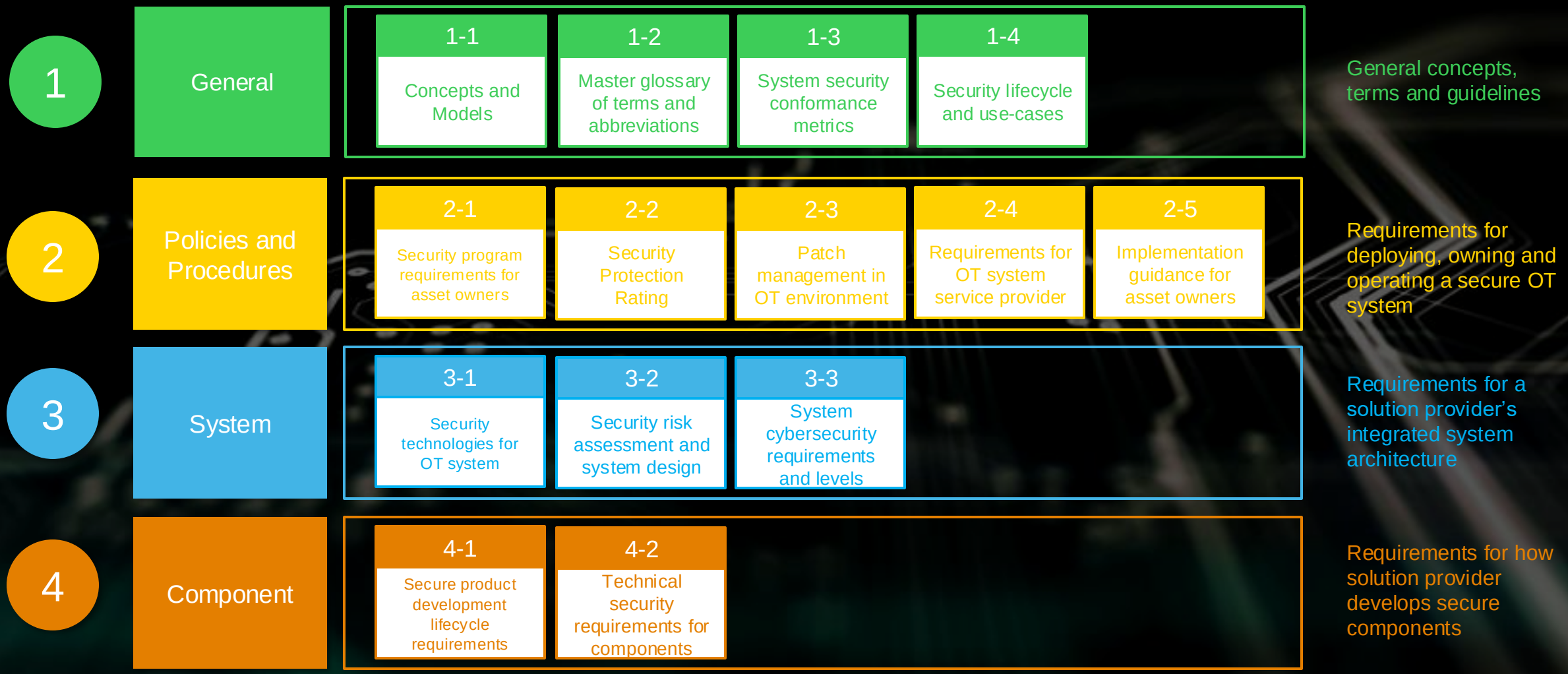
Leverage industry standards, increase productivity, lower costs & keep facilities safe

Flexible framework to address and mitigate current and future security vulnerabilities

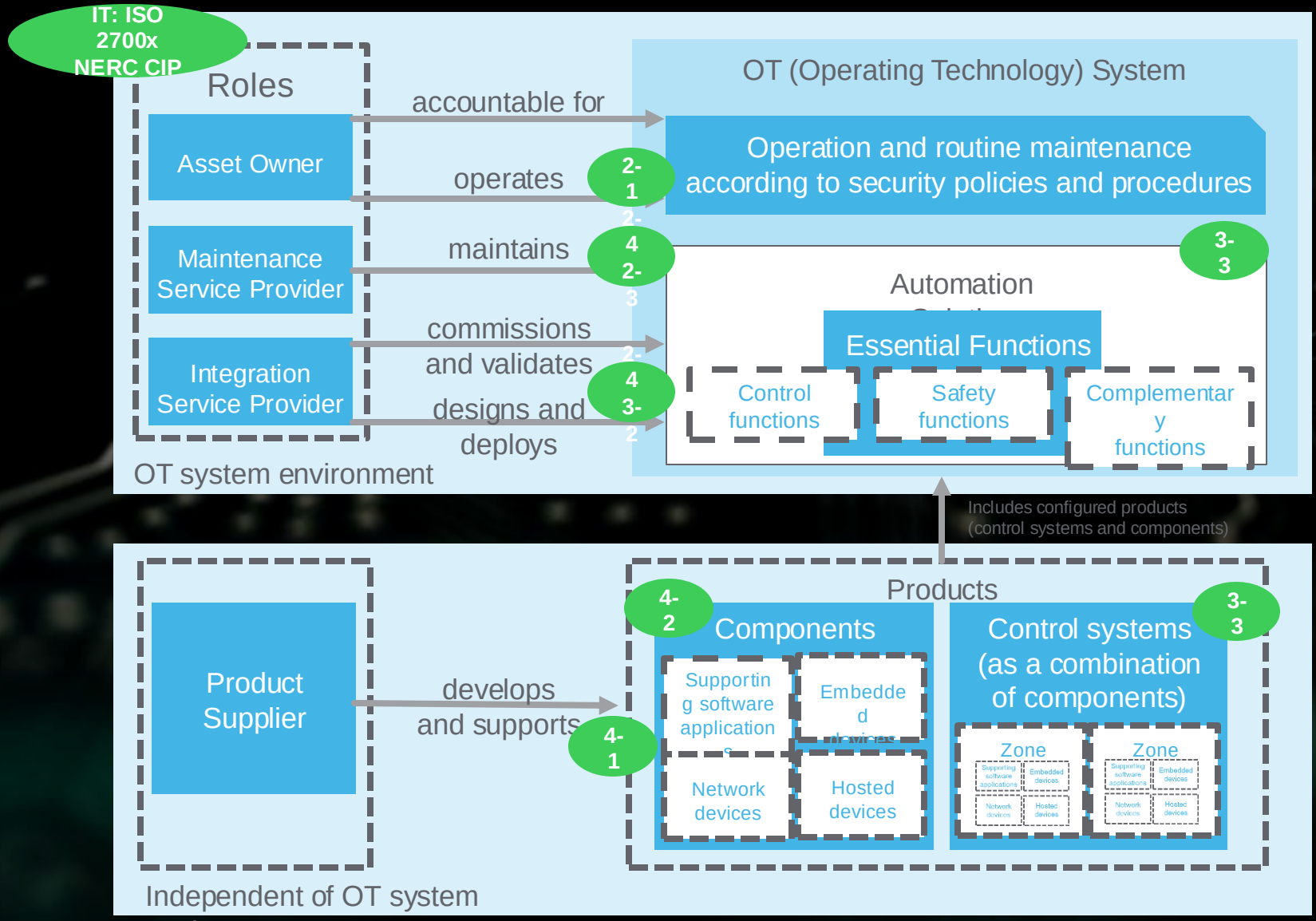
Leverages a holistic approach, bridging the gap between operation and information technology, as well as between safety and cybersecurity

Information Source ISA GCA

IEC62443 addresses People, Processes and Technology

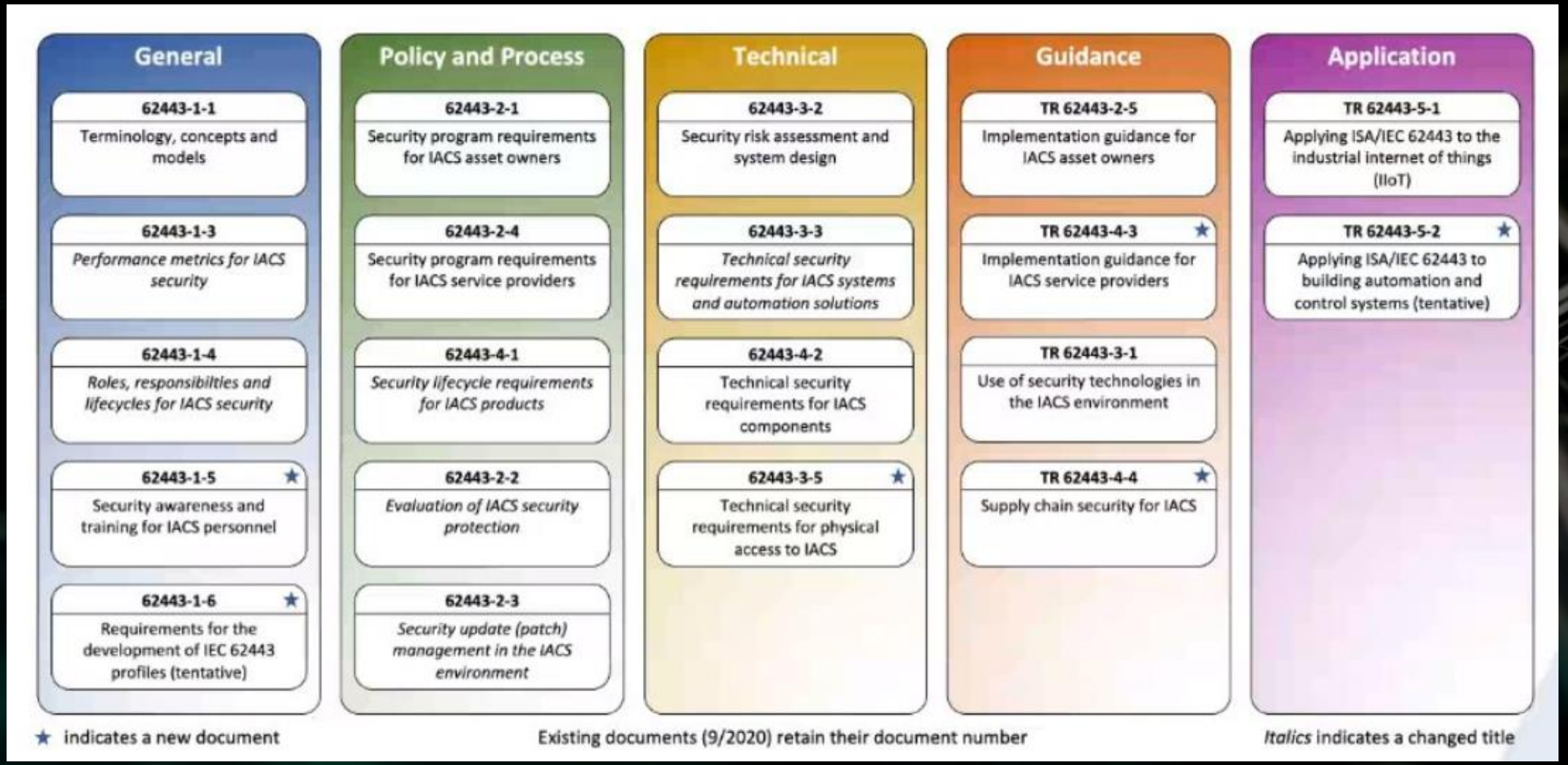


The main players in the lifecycle of a system



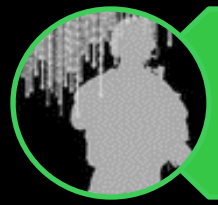
Life Is On Schneider Electric

New and updated ISA/IEC 62443 Series documents



Information Source ISA

ISA/IEC Security Levels

Nation-states Governments	 Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation	SL 4
Terrorists, Hacktivists, Professionals, Competitors	 Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation	SL 3
Disgruntled Employees, Thrill-Seekers, Hobbyist	 Protection against intentional violation using simple means with low resources, generic skills and low motivation	SL 2
Well-intentioned, Careless Employees	 Protection against casual or coincidental violation	SL 1

IEC 62443 Foundational Requirement Categories

4-2	3-3
Technical security requirements for components	System cybersecurity requirements and levels

These seven FRs are the foundation for system (and components) capability security levels

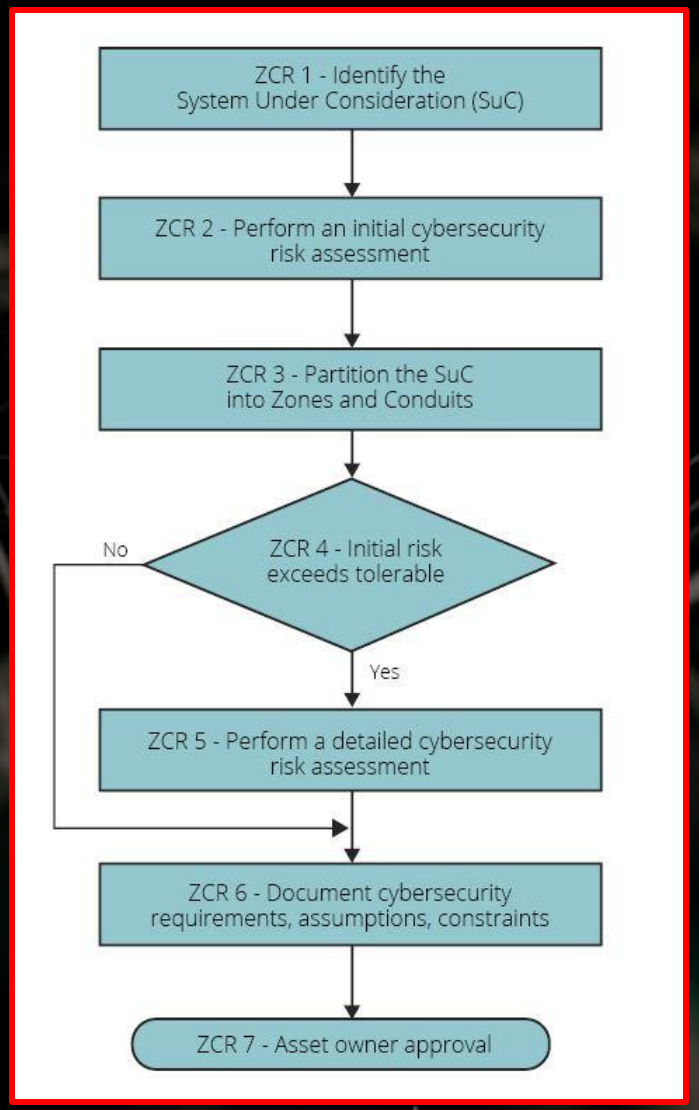
FR 1 - IAC Identification and Authentication Control	FR 2 - UC Use Control	FR 3 - SI System Integrity	FR 4 - DC Data Confidentiality	FR 5 - RDF Restricted Data Flow	FR 6 - TRE Timely Response to Events	FR 7 - RA Resource Availability
Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the system	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the system and monitor the use of these privileges	Ensure the integrity of the system to prevent unauthorized manipulation	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	Segment the control system via zones and conduits to limit the unnecessary flow of data	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered	Ensure the availability of the system against the degradation or denial of essential services

Security Risk Assessment for System Design (IEC 62443-3-2)

A key step in the Risk Assessment process is to partition the System Under Consideration into separate Zones and Conduits. The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk.

Partitioning the System Under Consideration into Zones and Conduits can also reduce overall risk by limiting the scope of a successful cyberattack. Part 3-2 requires or recommends that some assets are partitioned as follows:

- Shall separate business and control system assets
- Should separate temporarily connected devices
- Should separate wireless devices
- Should separate devices connected via external networks



IEC62443-3-2 suggests to break down system into Zones & Conduits

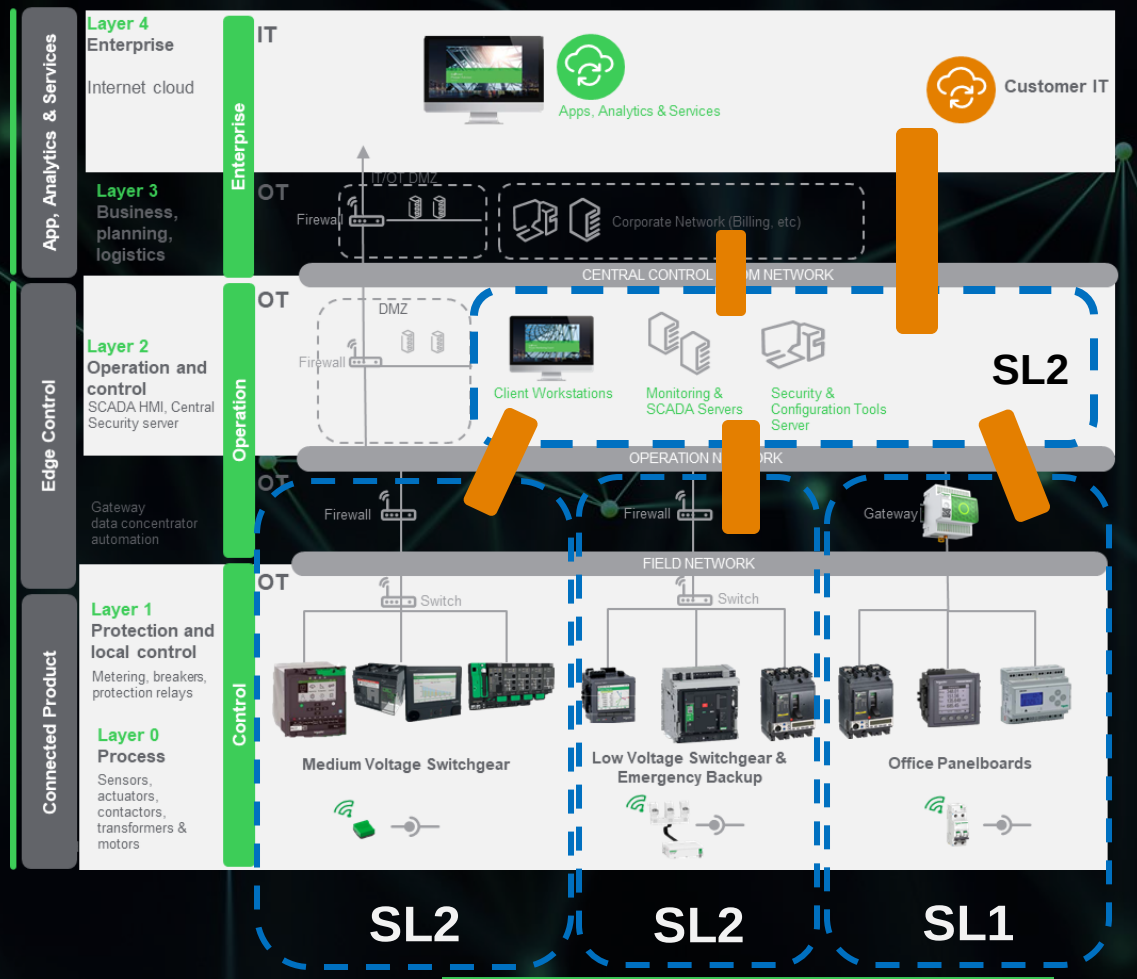
3-2

Security risk assessment and system design

Zone: consists of the grouping of connected assets that share the same cybersecurity requirements

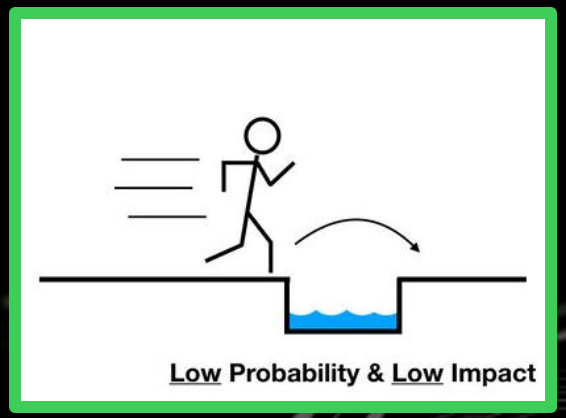
Conduit: consists of the grouping of connected assets dedicated exclusively to communications, and which share the same cybersecurity requirements

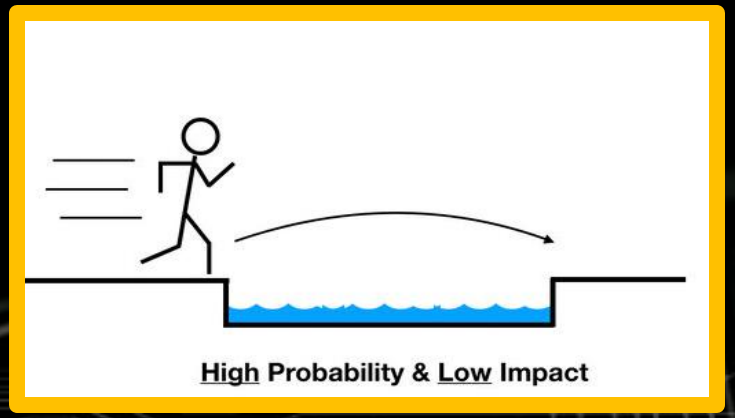
Zone and Conduit analysis yields a **“Security Level Target SL-T”** helps determine what Cybersecurity measures will be required to secure the system.

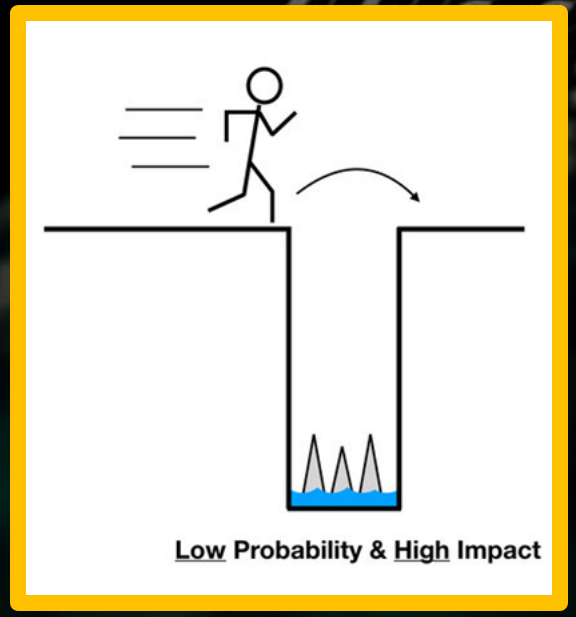


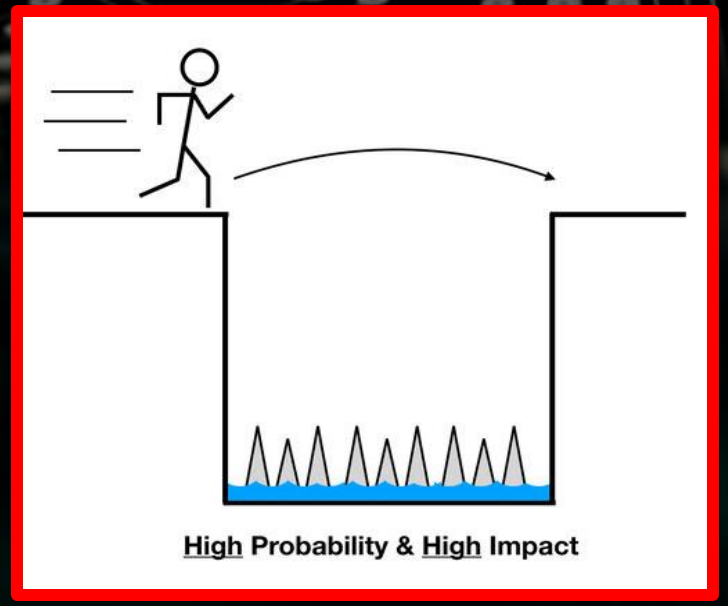
Life Is On Schneider Electric

First understand the risks to your business



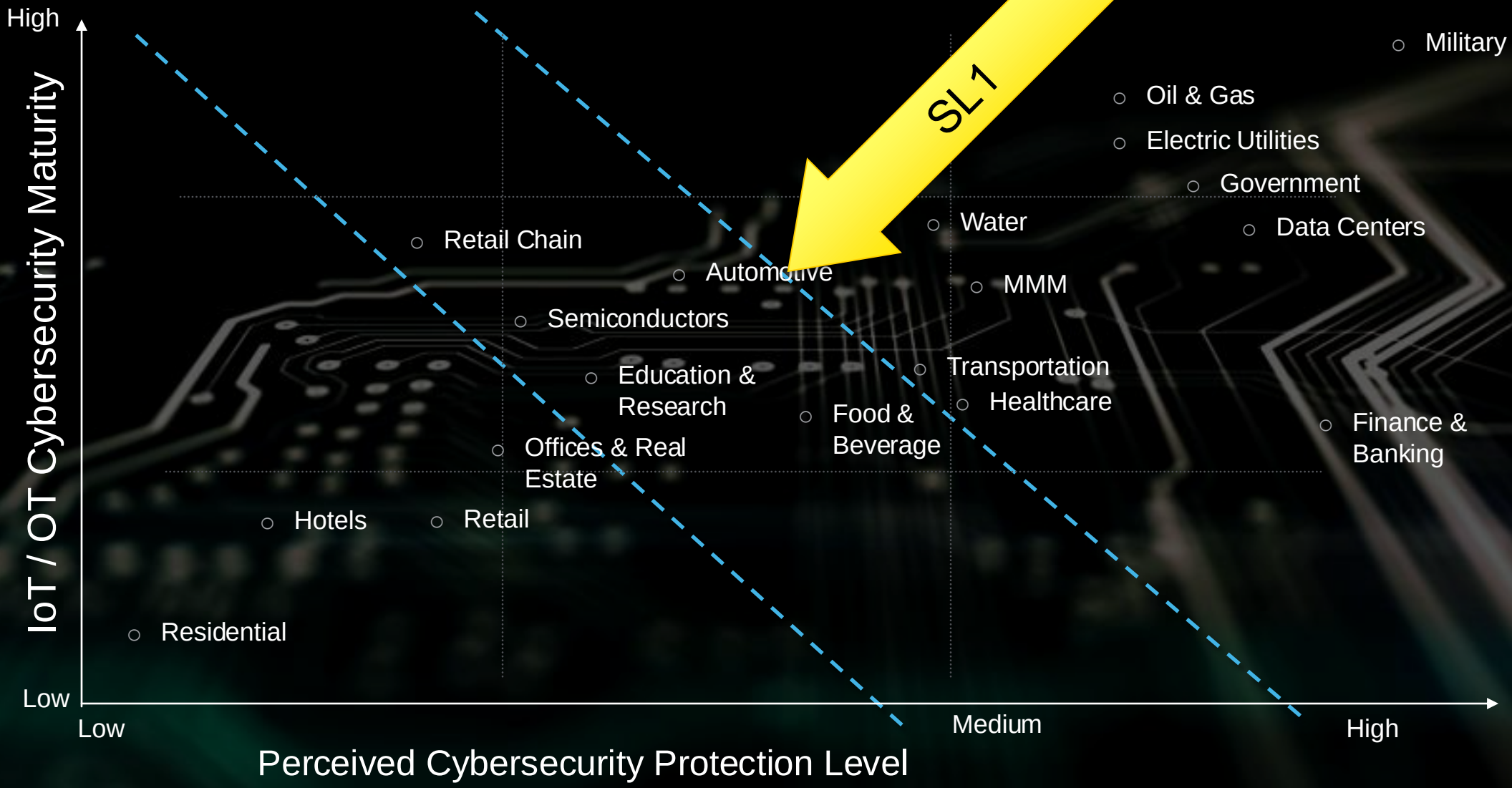






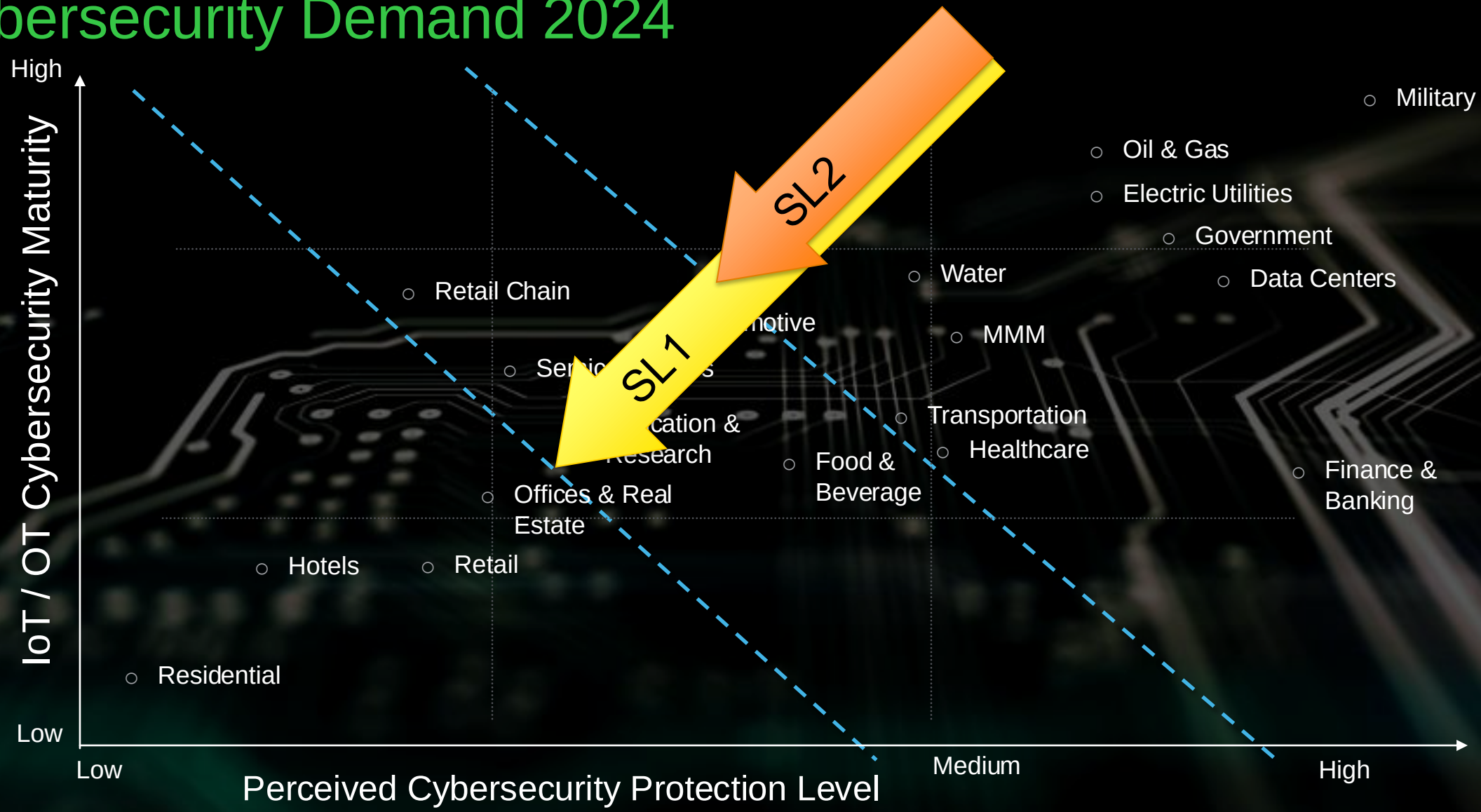
		Likelihood				
		Remote	Unlikely	Possible	Likely	Certain
Impact	Trivial	SL-0	SL-1	SL-1	SL-1	SL-1
	Minor	SL-1	SL-1	SL-2	SL-2	SL-2
	Moderate	SL-1	SL-2	SL-2	SL-3	SL-3
	Major	SL-1	SL-2	SL-3	SL-4	SL-4
	Critical	SL-1	SL-2	SL-3	SL-4	SL-4

Cybersecurity Demand 2023



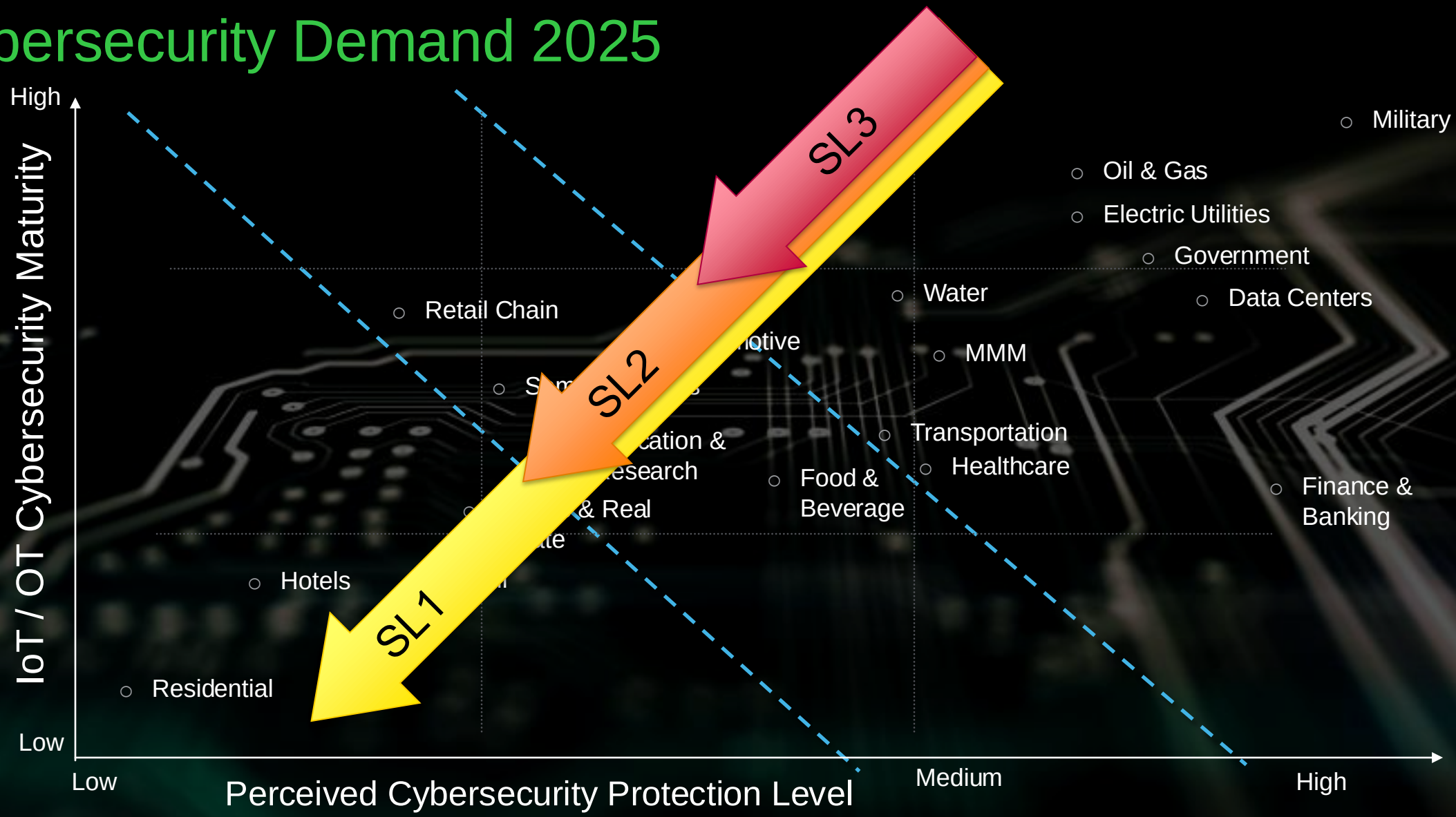
Life Is On Schneider Electric

Cybersecurity Demand 2024



Life Is On Schneider Electric

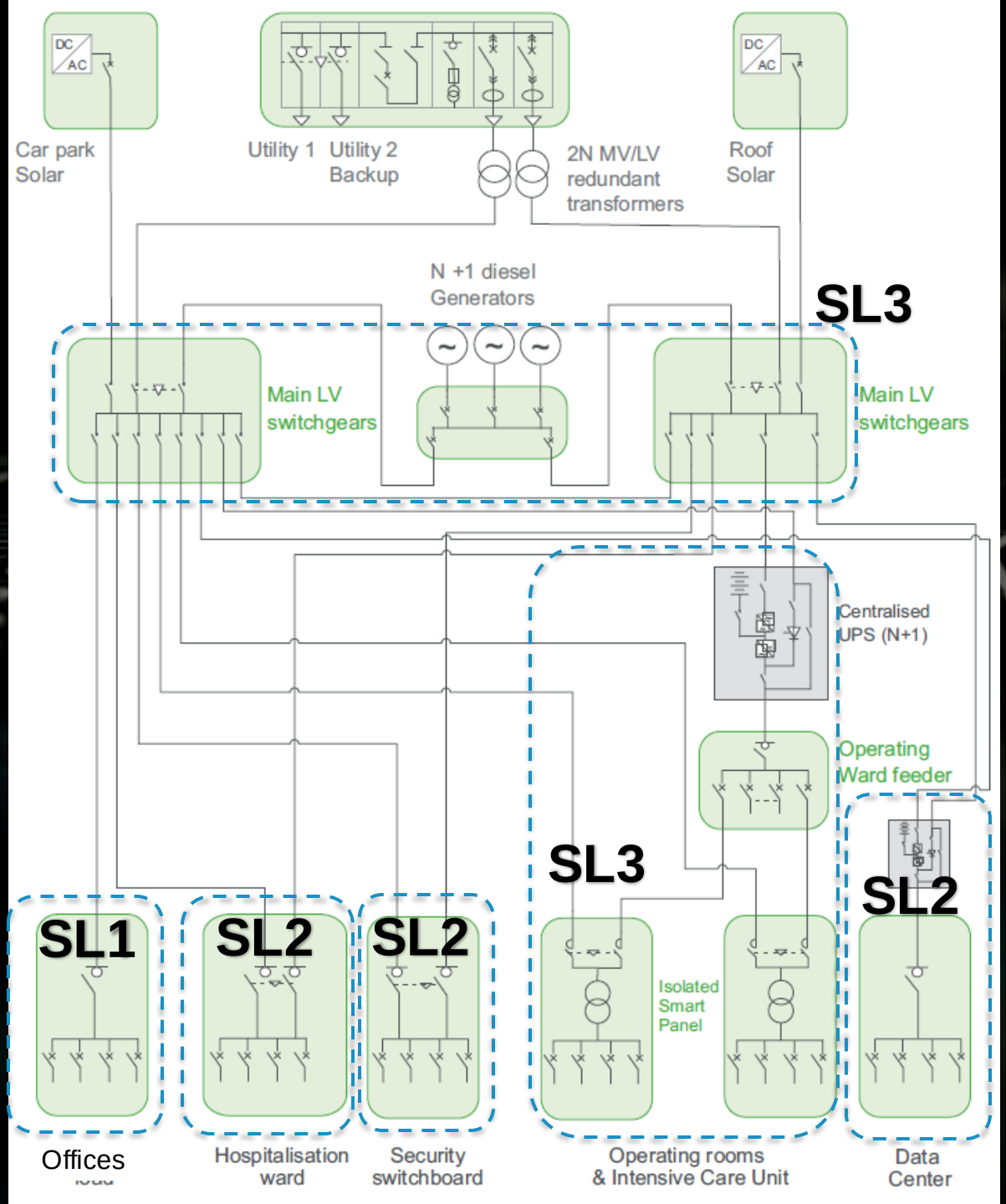
Cybersecurity Demand 2025



Practical Example for a Hospital

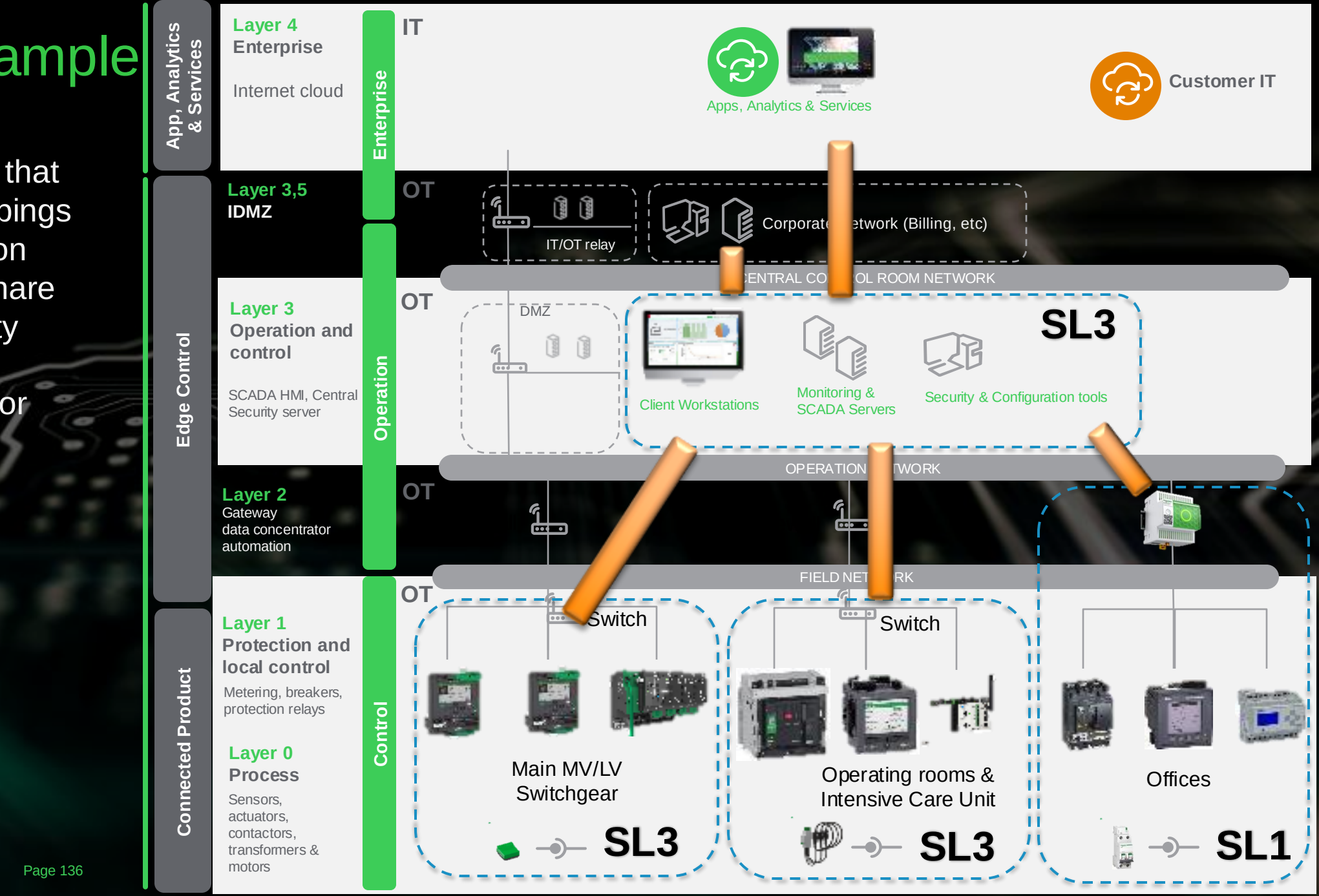
Hospital Example

1. Partition the system into Zones based on risk or criteria such as criticality of assets, operational function, physical or logical location, access or organizational requirements.
2. Identify assets which share common security characteristics and define a security level target for each zone.
3. Develop a high-level digital network architecture.



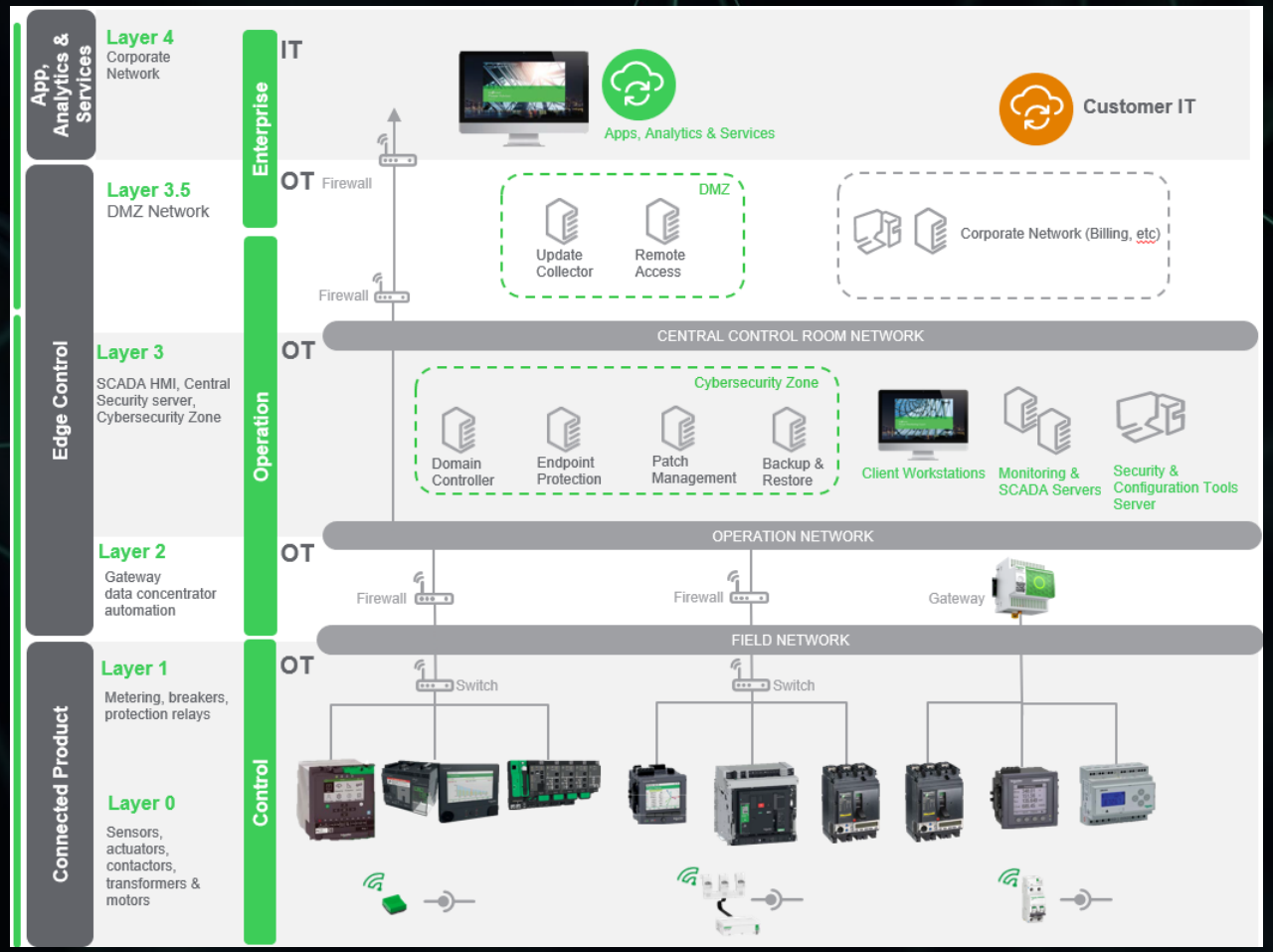
Hospital Example

4. Define conduits that are logical groupings of communication channels that share common security requirements connecting two or more zones.



Example of an SL1 System Including Compensating Measures

What can you expect to budget for beyond the CS capabilities in our offers



Security Solutions Including Compensating Measures according to IEC62443-3-3

Identification, Authentication and Use Control FR- 1 & 2, Cryptography FR-4

- User management and cryptography accomplished with inherent capabilities in connected products and edge control software
- User management and role-based access control managed with Cybersecurity Admin Expert (CAE)

System Integrity FR-3

- End-Point Protection (McAfee anti-virus and end-point protection)
- Patch Management (typically performed on a dedicated security server and through regular maintenance

Restricted Data Flow (Network Segmentation) FR-5

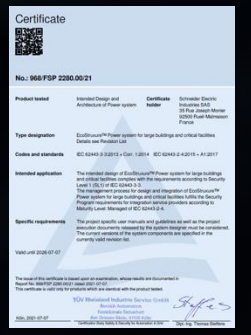
- Network Firewalls (Palo Alto Networks PA-220)

Timely Response to Events FR-6

- Access to audit log – CAE SysLog

Resource Availability FR-7

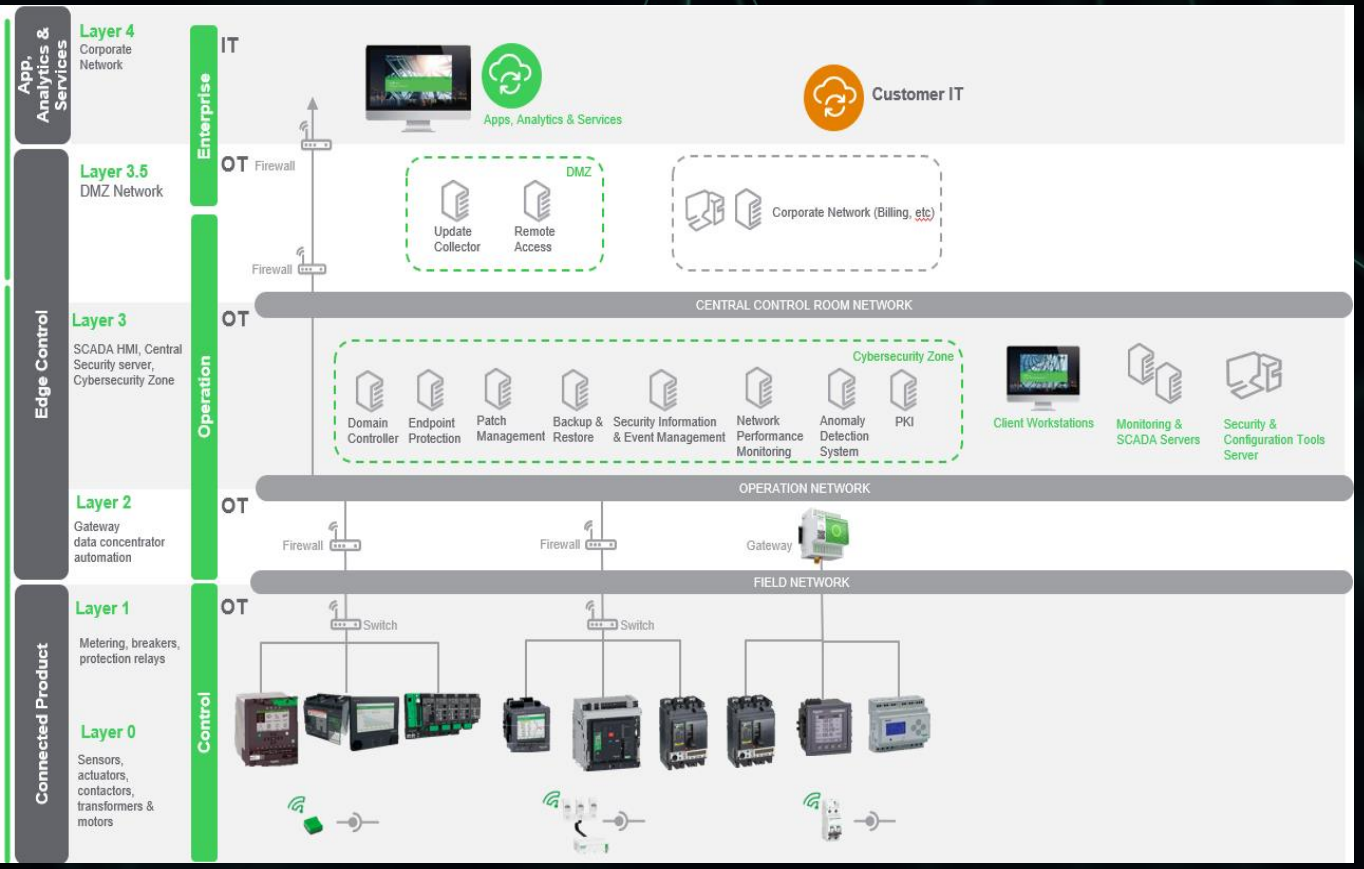
- Backup & Restore (data backups and restore managed by Veritas Backup Exec – run as a VM on same server as patch management)



Life Is On Schneider Electric

Example of an **SL2** System Including Compensating Measures

What can you expect to budget for beyond the CS capabilities in our offers



Security Solutions for SL2 In addition to SL1 requirements

Identification, Authentication and Use Control FR-1 & 2, Cryptography FR-4

- Application Allow Lists, Multi- Factor Authentication (McAfee Application Control, Yubi-Key)

System Integrity FR-3

- Secure communication via VPN
- Anomaly / Intrusion Detection System (IDS) – CAP (Nozomi)

Restricted Data Flow (Network Segmentation) FR-5

- Remote Access (VPN)

Timely Response to Events FR-6

- Logging
- SysLog/SIEM / Network Performance Monitoring

Certifications

IEC62443: Schneider Electric Certifications

1 General

- 1-1 Con… M…
- 1-2 Master glossary
- 1-3 System security conformance metrics
- 1-4 Security lifecycle and use-cases

2 Policies and Procedures

- Secu… requi… ass…
- 2-3 Patch management in OT environment
- 2-4 Requirements for OT system service provider

3

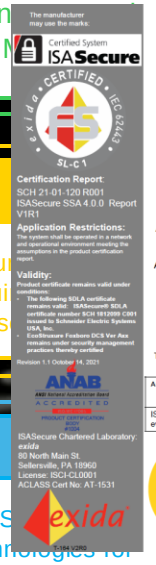
- S… technologies for OT system
- assessment and system design
- 3-3 System cybersecurity requirements and levels

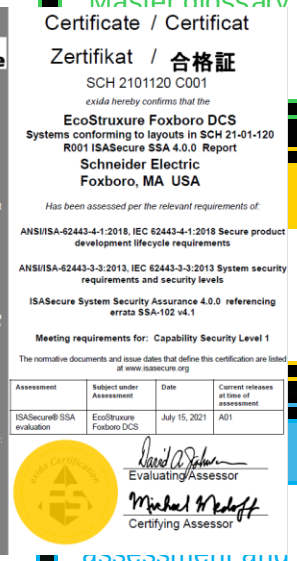
4

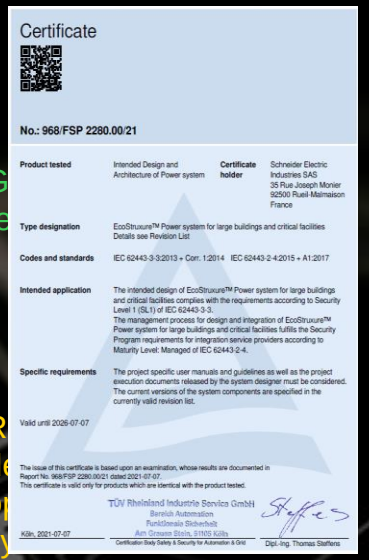
- 4-1 Secure product development lifecycle requirements
- 4-2 Technical security requirements for components

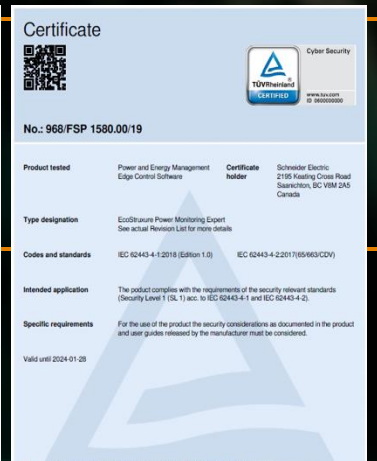
Requirements for a solution provider's integrated system architecture

Requirements for how solution provider develops secure components









Life Is On | Schneider Electric

Take Aways

IEC 62443 – Takeaways

1. **Why – IEC 62443 addresses physical consequences, including safety and environmental.**

2. **For whom – IEC 62443 applies for Asset Owner, Service Provider and Products Supplier.**

3. **How – IEC 62443 provides Security Requirements based on Foundational Requirements and Security Levels.**

4. **And the most important: IEC 62443 addresses Cybersecurity Lifecycle for Systems – Cybersecurity is a continuous process !**

Thank you!

Some graphics provided by and used with the permission of the ISA Global Cybersecurity Alliance

Microsoft

Bart Gabriëls

Microsoft

Cyberwal
by digital
wallonia

Microsoft Security

AI for Threat Detection and Incident Response

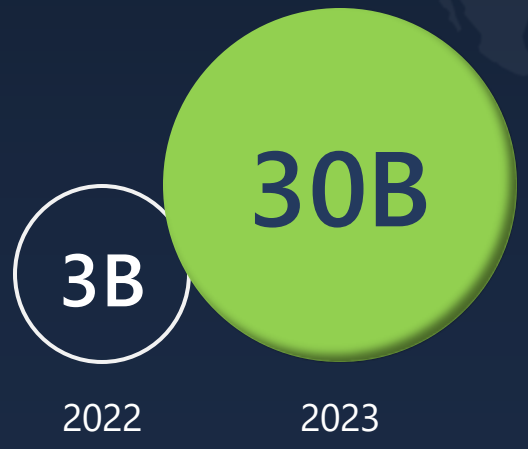
Bart Gabriëls
Sr. Solution Specialist
Security,Compliance and Identity Management

Setting the scene

We live in the most complex threat landscape in history

Speed, scale, and sophistication of attacks

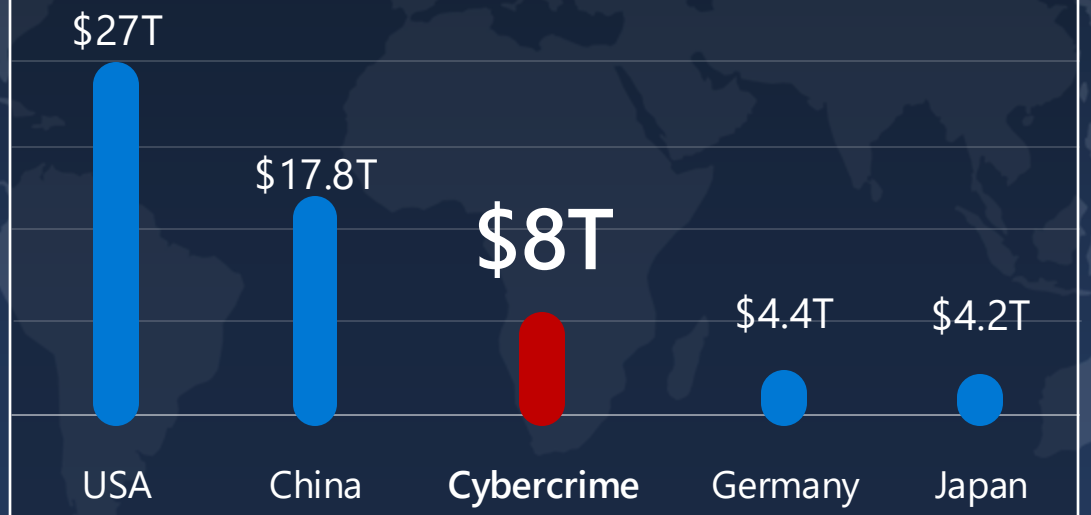
Password attacks per month



Source: Microsoft

Rapidly growing cyber economy

Annual GDP



Source: Statista

Growing regulatory environment

250

new regulatory updates tracked every day

Source: Microsoft

AI Powered
Threat Protection

By the numbers

323

MTTD - Days to Detect an attack is happening without automated detection in place (Best of Breed)

249

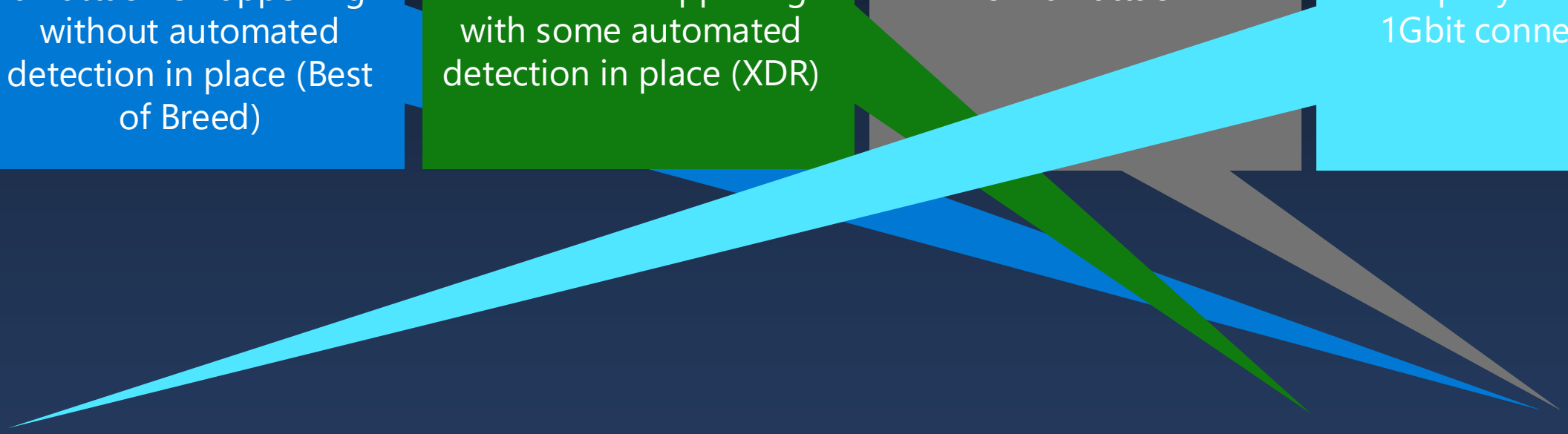
MTTD -Days to Detect an attack is happening with some automated detection in place (XDR)

7

MTTR - Days to recover from an attack

2,5

hours to download 1TB of company data over a 1Gbit connection



By the numbers

323

MTTD - Days to Detect an attack is happening without automated detection in place (Best of Breed)

249

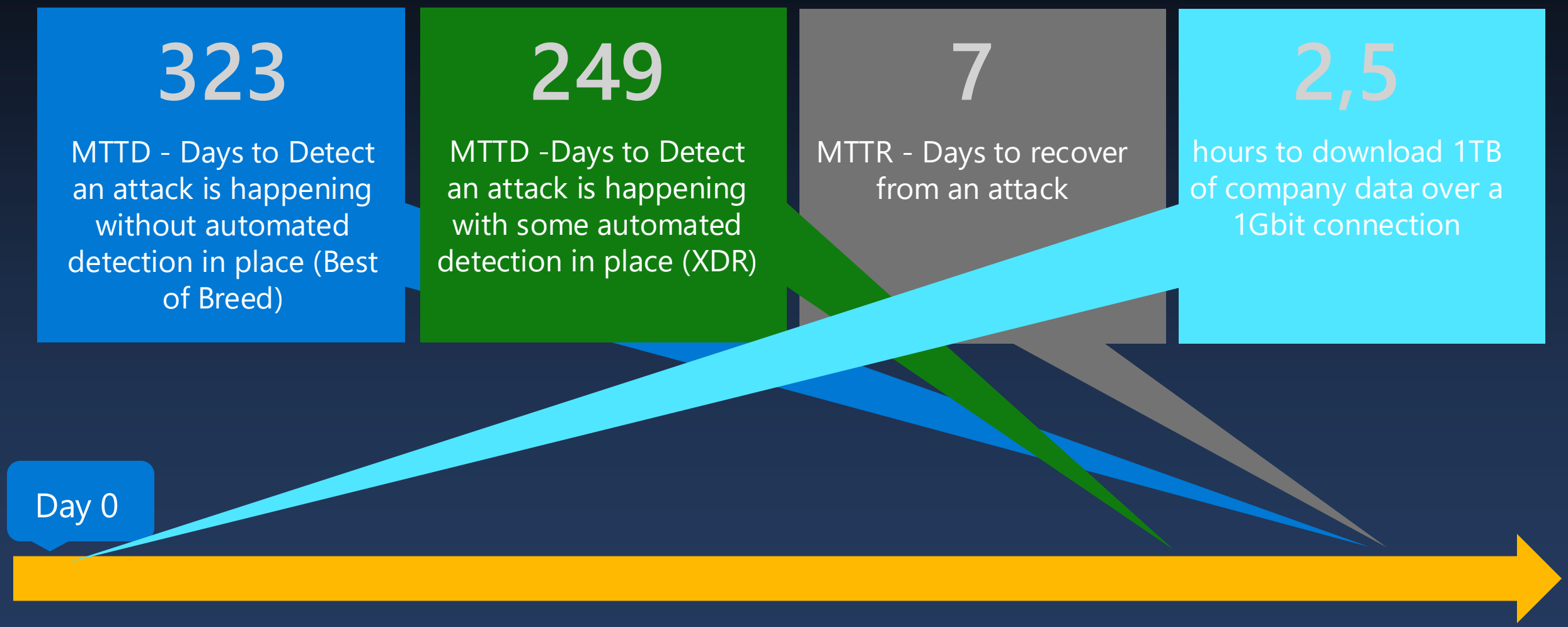
MTTD -Days to Detect an attack is happening with some automated detection in place (XDR)

7

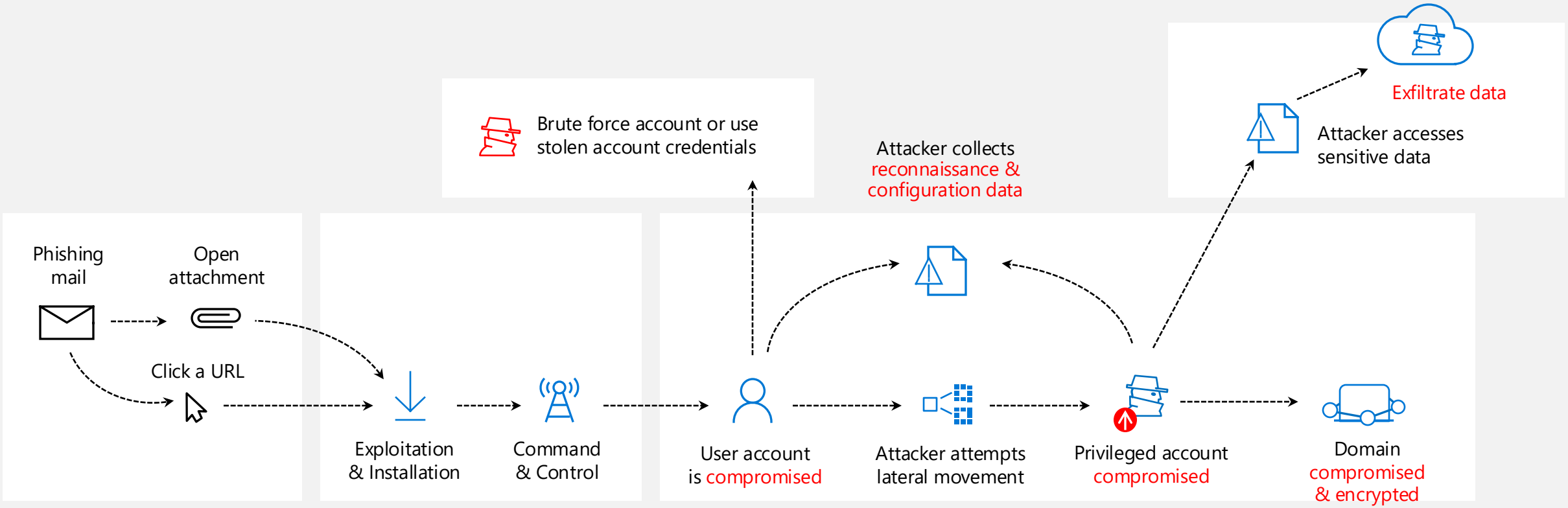
MTTR - Days to recover from an attack

2,5

hours to download 1TB of company data over a 1Gbit connection



The pattern


Brute force account or use stolen account credentials
Attacker collects reconnaissance & configuration data
Exfiltrate data
Attacker accesses sensitive data
Phishing mail
Open attachment
Click a URL
Exploitation & Installation
Command & Control
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised & encrypted

The pattern

Email ATP

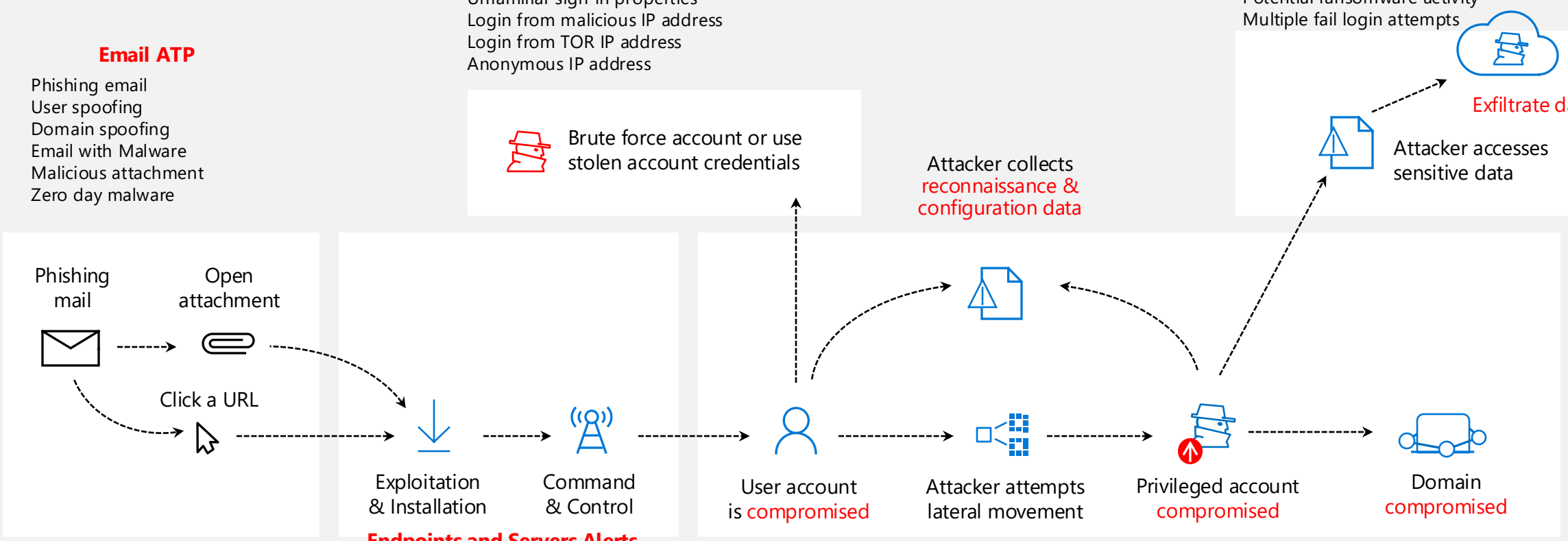
Phishing email
User spoofing
Domain spoofing
Email with Malware
Malicious attachment
Zero day malware

Identity Protection Alerts

Password spray
Unfamiliar sign-in properties
Login from malicious IP address
Login from TOR IP address
Anonymous IP address

Cloud Apps Security Broker Alerts

Mass downloads
Shadow IT Apps
Impossible travel activity,
Activity from infrequent country
Potential ransomware activity
Multiple fail login attempts



Endpoints and Servers Alerts

Suspicious files
WMI execution
Event log clearance
Privilege escalation
Suspicious base64 decoding
Suspicious service registered
Malicious use of built in SQL account

User Profiling and Lateral Movement

Account enumeration reconnaissance

Preventing Pass-the-Ticket ,Pass-the-Hash, Skeleton key malware, Golden ticket

The pattern

Email ATP

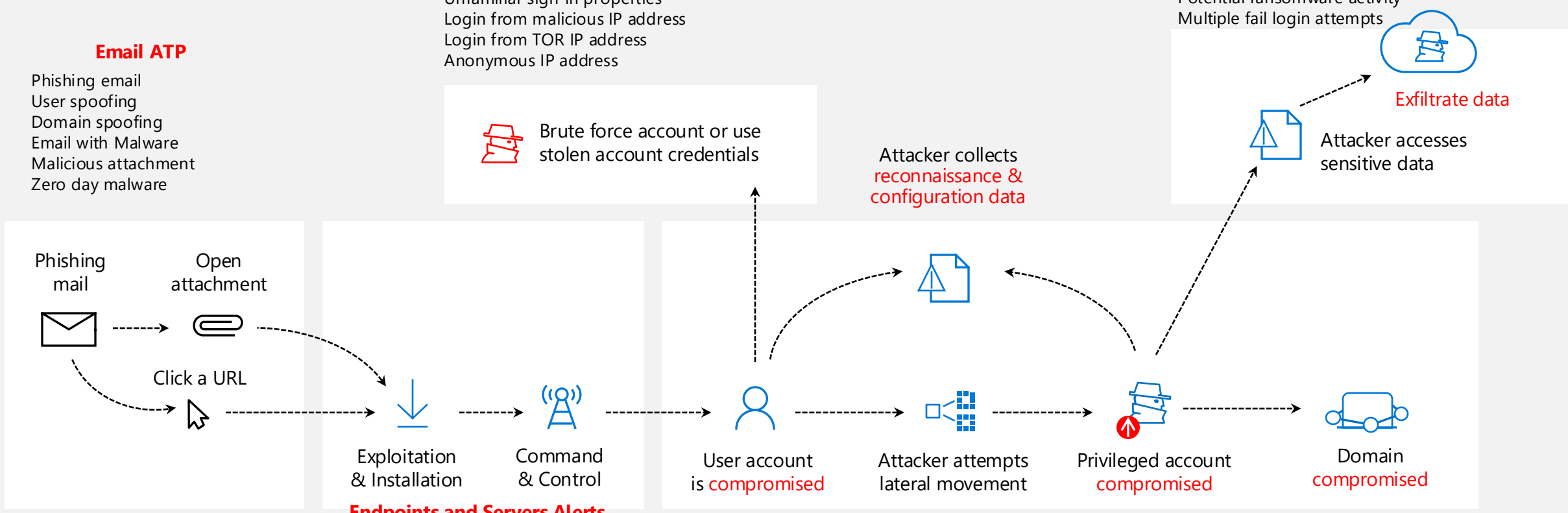
Phishing email
User spoofing
Domain spoofing
Email with Malware
Malicious attachment
Zero day malware

Identity Protection Alerts

Password spray
Unfamiliar sign-in properties
Login from malicious IP address
Login from TOR IP address
Anonymous IP address

Cloud Apps Security Broker Alerts

Mass downloads
Shadow IT Apps
Impossible travel activity,
Activity from infrequent country
Potential ransomware activity
Multiple fail login attempts



Endpoints and Servers Alerts

Suspicious files
WMI execution
Event log clearance
Privilege escalation
Suspicious base64 decoding
Suspicious service registered
Malicious use of built in SQL account

User Profiling and Lateral Movement

Account enumeration reconnaissance

Preventing Pass-the-Ticket ,Pass-the-Hash, Skeleton key malware, Golden ticket

AI Powered Incident Response

By the numbers

3,2 mil

Open vacancies for skilled Cyber Security Professionals in 2023

300

Number of threat actors (Nation State Sponsored, Ransomware Groups …) Microsoft is currently tracking

4,45 mil

Average cost of a breach

Making organizations more secure

Increasing volume and sophistication of threats

Critical vulnerabilities surfaced before damage is done; **mean time to detect and respond** reduced to contain incidents sooner

Inability to adequately staff, train, and retain top security talent

Improved **operational efficiency** with increased team skills and productivity

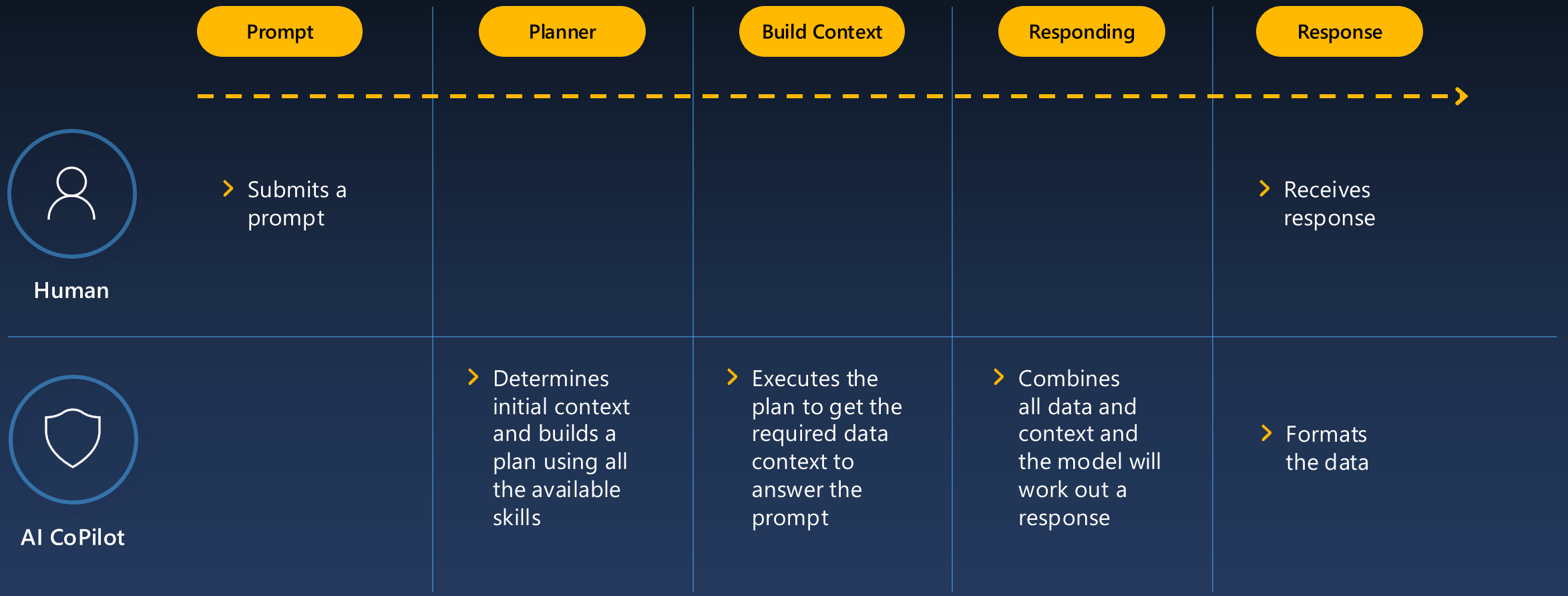
Overworked, fatigued staff unable to focus on what matters

Shift **from reactive to proactive:** ability to focus on high priority problems and critical tasks

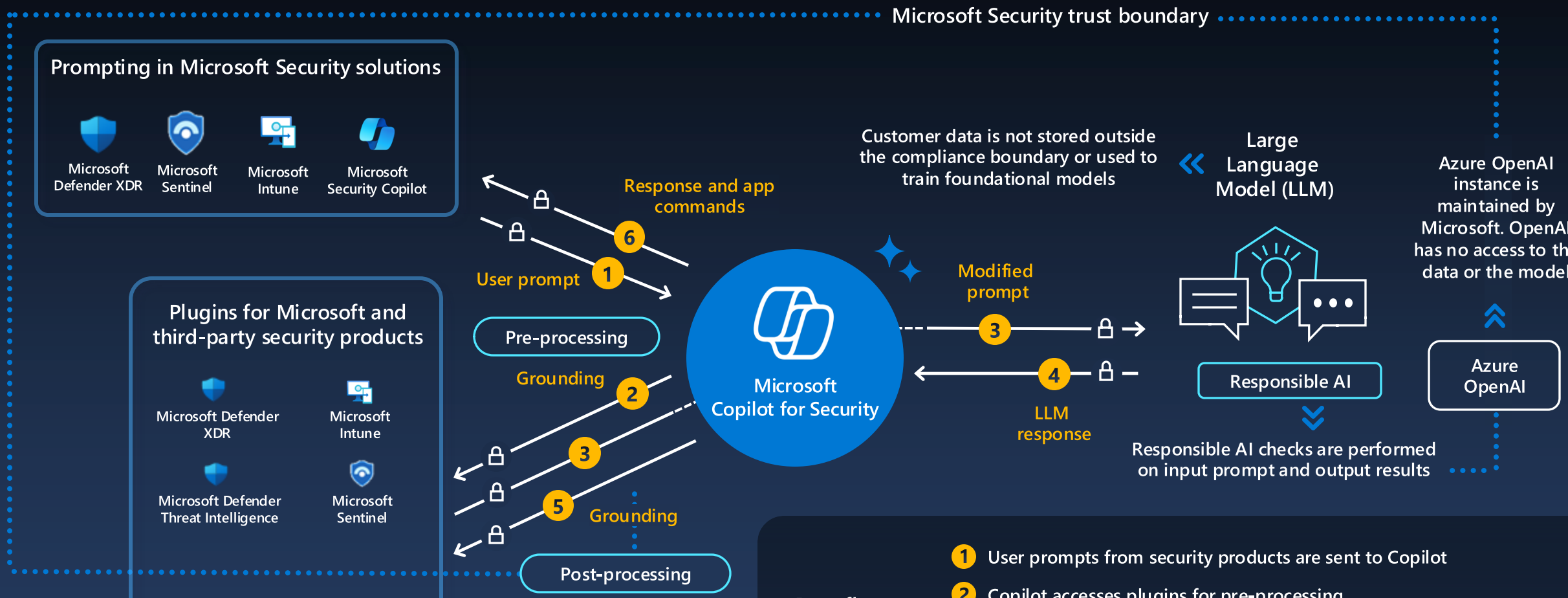
Reactive security operation poorly adjusted to risk and business priorities

Improved understanding of **business risk and executive and board-level reporting**

Operated with simple natural language queries



Data flow for Microsoft Copilot for Security



Data flow

(🔒 = all requests are encrypted via HTTPS)

1. User prompts from security products are sent to Copilot
2. Copilot accesses plugins for pre-processing
3. Copilot sends modified prompt to LLM
4. Copilot receives LLM response
5. Copilot accesses plugins for post-processing
6. Copilot sends the response, and app command back to security products

Incident Summarization

SOC analysts face numerous complex security alerts daily. Efficient summarization is essential for quick and effective response, minimizing potential threats and improving overall security posture.

Prompt Example: Summarize this incident in bullets.

Challenge

SOC analysts find it challenging to quickly understand and respond to incidents due to the high volume and complexity of alerts.

Solution

Copilot for Security uses AI to summarize incidents by distilling up to 100 alerts into a concise, actionable report. These summaries include critical information such as the start time, affected assets, timeline of events, indicators of compromise, and involved threat actors, providing SOC analysts with a clear and comprehensive view of the incident.

Key Benefits

- **Efficient Summarization:** Quickly condense alerts into coherent summaries.
- **Enhanced Context:** Detailed insights including timelines and affected assets.
- **Improved Response:** Facilitates faster and more informed decision-making.

Learn more:

- **Youtube:** Link 1
- **MS Learn:** Link 1

Impact Analysis

Leverage AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritize response efforts effectively.

Prompt Example: What systems were affected by this incident?

Challenge

SOC analysts struggle to assess the impact of security incidents and prioritize response efforts due to lack of clear insights into affected systems and data.

Solution

Copilot for Security uses AI-driven analytics to assess the potential impact of incidents, providing insights into affected systems and data. It also performs vulnerability assessments, describing CVEs, their severity, mitigation steps, and affected products, significantly speeding up the process.

Key Benefits

Insightful Impact Assessment: Quickly determine the potential impact of incidents.

Detailed Vulnerability Assessment: Provides severity, mitigation steps, and affected products.

Efficient Resource Allocation: Helps prioritize response efforts effectively.

Learn more:

- **Youtube:** Link 1 | Link 2

Reverse Engineering of Scripts

Automate the reverse engineering of malware, enabling analysts to comprehend attacker actions. Translate complex scripts into natural language, linking indicators to affected entities efficiently.

Prompt Example: Is this script malicious?

Challenge

SOC analysts find it difficult to understand complex and obfuscated scripts, which are time-consuming to analyze and hard to link to affected entities.

Solution

Copilot for Security utilizes AI to automatically inspect and translate complex scripts into clear, actionable insights. This helps determine if scripts are malicious or benign and links indicators to affected entities, aiding in quicker and more accurate analysis.

Key Benefits

Simplified Analysis:
Quickly and accurately analyze complex scripts.

Enhanced Understanding:
Translate scripts into natural language for better clarity.

Improved Efficiency:
Link indicators to affected entities, speeding up investigations.

Learn more:

- **Youtube:** Link 1 | Link 2
- **MS Learn:** Link 1 | Link 2

Guided Response

Receive detailed, step-by-step guidance for incident response, from triage to remediation, with deep links to recommended actions for faster and more effective responses.

Where to find: Guided responses are available in the Microsoft Defender portal or in the standalone experience through the Defender XDR plugin. Cards with recommended actions will appear on the Copilot pane when an incident page is opened.

Challenge

SOC analysts often lack clear, actionable steps for efficiently managing incidents, leading to inconsistencies and delays in triage, investigation, containment, and remediation.

Solution

Copilot for Security provides AI-driven guided responses with step-by-step instructions for triage, investigation, containment, and remediation. These responses ensure consistent and efficient incident management by offering clear, actionable steps for each phase.

Key Benefits

Clear, actionable steps: Provides detailed instructions for each phase of incident response.

Accelerated incident resolution: Faster and more effective handling of incidents

Improved consistency: Ensures standardized response procedures for all team members

Learn more:

- MS Learn: Link 1

Making organizations more secure

"It's a time saver. **I don't have to go into 50 different tools** to do an investigation."

SOC Director, Fortune 100 Chemicals

"When we need to check for IOCs, it takes **10-15 minutes** for an analyst to do it. It took Security Copilot **3 minutes** to do the same."

CISO, Global Ecommerce

"Generating reports would be a **huge time saver.** It is probably our most time-consuming function at this time."

Head of Security, Global Consultancy

"I use Security Copilot as a sanity check. The generated KQL query gets **me 80% of the way there."**

CISO, Fortune 500 Construction

"We've been using it during actual incidents. **It gave a great explanation of 537 lines of code in about a minute."**

SOC Director, Fortune 100 Chemicals

Questions ?

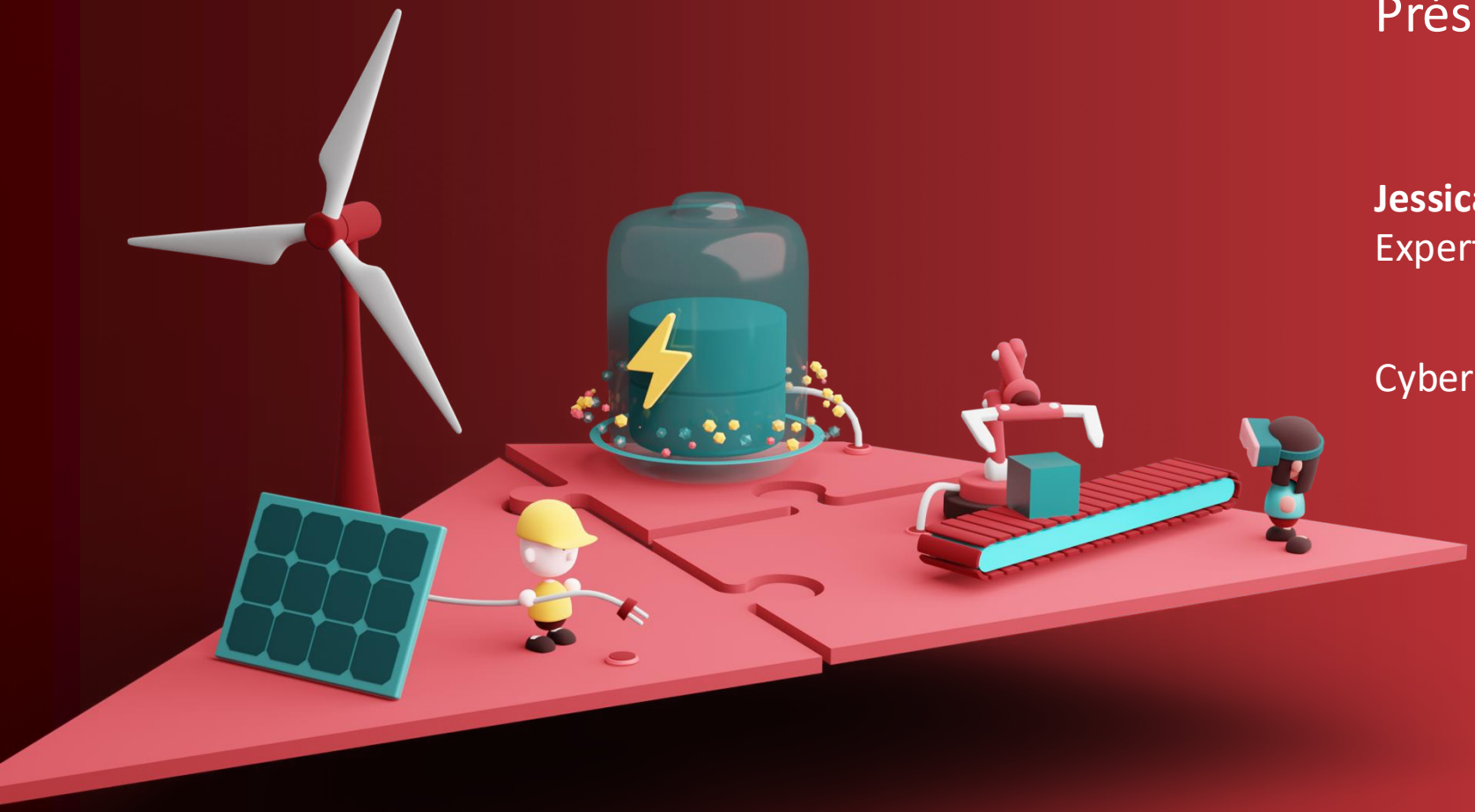
Bart Gabriëls
bartgabriels@microsoft.com

Jessica Miclotte

Agence du Numérique

Cyberwal
by digital
wallonia

Industrie du Futur digital wallonia



Programme Industrie du Futur
Présentation de l'offre

Jessica Miclotte
Experte Industrie du Futur

CyberWeek - 14/10/2024

Agence du Numérique

Wallonie Relance

Industrie du Futur digital wallonia

La Wallonie a de l'ambition

Accélérer la transformation numérique des 2300 entreprises manufacturières wallonnes et améliorer leur compétitivité

Agir sur les méthodes de production et l'usage de technologies numériques clés, permettant aux entreprises d'innover, de renforcer leur position concurrentielle et de développer un écosystème porteur d'emplois locaux

Wallonie Industrie du futur | digital wallonia .be

Les 38 partenaires

Un accompagnement à chaque étape de votre projet

Sensibilisation

- Evénements
- Démonstrateurs
- Digiscore
- 'Factory of the Future'

Accompagnement

- Approches, méthodes et outils, bonnes pratiques génériques et sectorielles
- Un consortium Industrie du Futur avec l'Agence du Numérique et 38 partenaires métiers et technologiques complémentaires
- Intégré dans l'initiative Digital Wallonia

Formations

- Développement de compétences numériques et opérationnelles

Financement

- Subsides Industrie du Futur
- Wallonie Entreprendre
- Aides Région Wallonne et Européennes

Réflexion | **Initiation** | **Planning** | **Exécution** | **Clôture** | **Maintenance**

Diagnostic

- Analyse de maturité 360° sur 7 piliers
- Identification des opportunités
- Plan d'Actions

Proof of Concept

- Hébergement et Réalisation de 'Proof of Concept' (IA, Circulaire, technologique)

Wallonie
Industrie du futur
digital wallonia .be

WALHUB brings together the expertise of 9 leading digital strategy players in Wallonia.

DISCOVER
EXPERIENCE
CONNECT
GET STARTED

Need a digital boost?

Experts of our EDIH advise manufacturing companies on how to optimize the use of digital technologies, whatever their digital maturity level.

TEST BEFORE INVEST	EMPOWER WORK FORCE
GROW YOUR NETWORK	FIND INVESTMENT

#IoT #AI
#SUPERCOMPUTER
#CYBERSECURITY
#MANUFACTURING
#DIGITALISATION
#INDUSTRY4.0
#PRODUCTION
#SUPPLYCHAIN

Collective approach

Find inspiration at WalHub free events!
Do not miss any, join EDIH-WalHub.

Individual approach

Unlock digital! Activate 1 to 3 days free custom support with an expert.

www.walhub.be

Industrie du Futur digital wallonia

Co-funded by the European Union

Wallonie

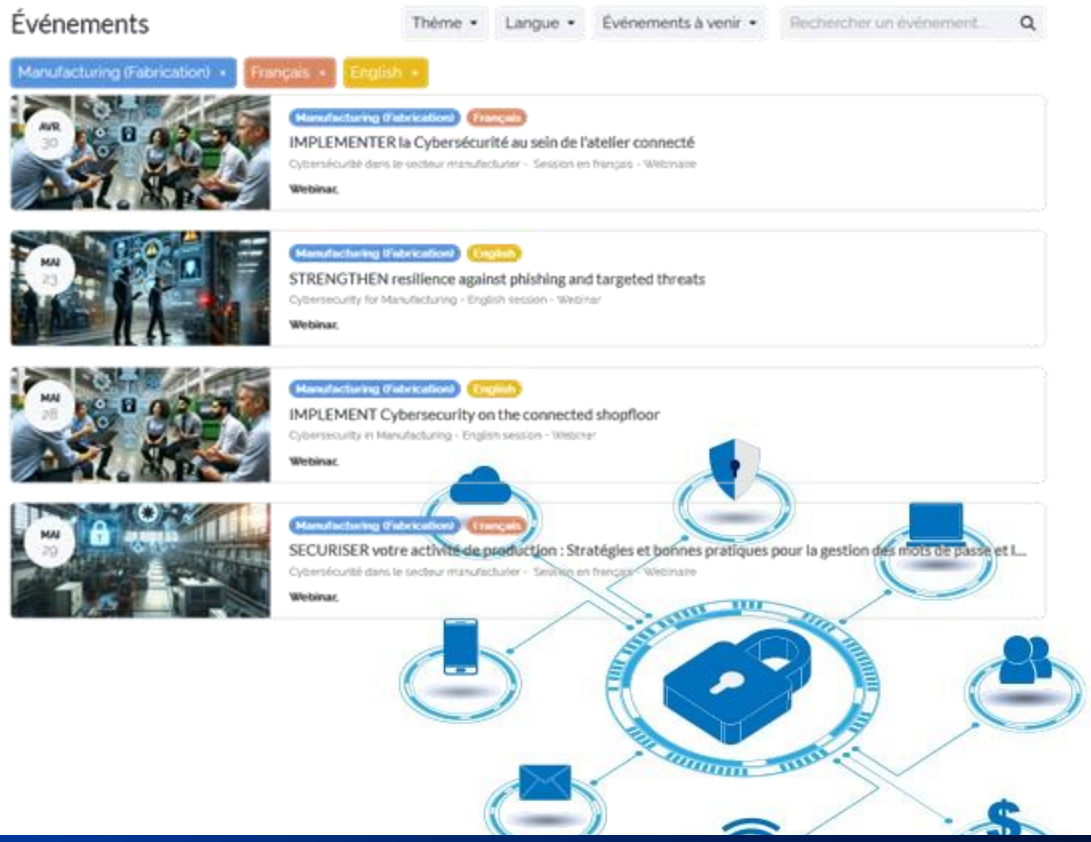
CyberActive

Strengthening Cybersecurity Skills

Vous êtes une PME ou un indépendant actif dans l'industrie manufacturière ?
Bénéficiez gratuitement de contenus d'experts adaptés à vos besoins et aux challenges relatifs à la cybersécurité :

- **Sessions de formation courtes - max 2h (Web/Live)**
- **Vidéos instructives**
- **Ressources didactiques (« cheat sheets »,…)**

Site web : https://www.cyberactive.be
Sessions de formations : https://event.cyberactive.be



Funded by
economie
Funded by the European Union
NextGenerationEU

Cyberboost

Accélérons la cybersécurité de votre PME

Un **e-learning gratuit** et complet pour protéger votre PME contre les cyberattaques les plus courantes.

Des outils et des connaissances pratiques pour vous guider pas à pas dans la mise en œuvre des mesures de sécurité.

Spécialement conçu pour les PME,
sur base du cadre CyFun de notre autorité nationale, le Centre pour la Cybersécurité Belgique (CCB).

- ✓ 5 modules, à votre rythme (4 à 6 heures)
- ✓ Des exercices interactifs et des plans d'actions
- ✓ Des modèles et des checklists pratiques
- ✓ Un certificat de réalisation en fin d'apprentissage
- ✓ Disponible en néerlandais et en français

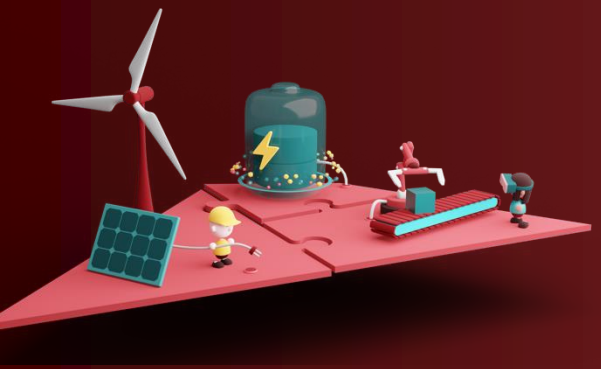
Participez
agoria.be/cyberboost

WALHUB

Co-funded by the European Union

Avec le soutien de la Wallonie

Industrie du Futur digital wallonia

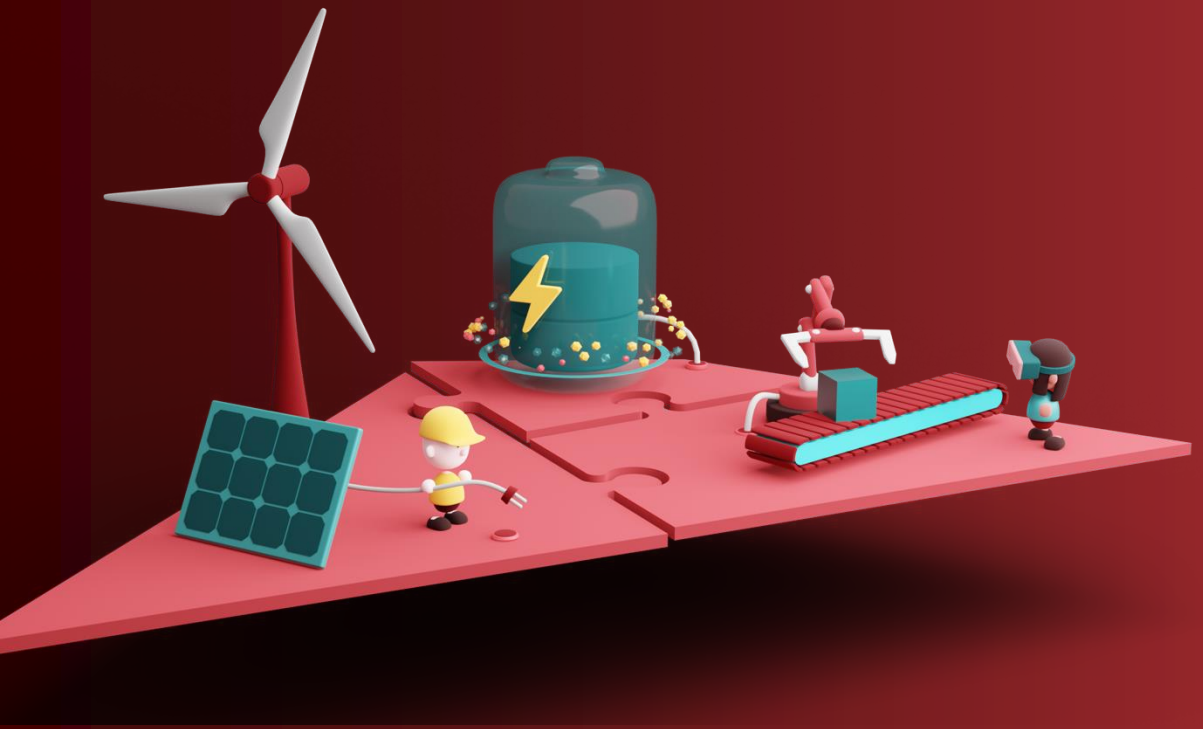


45 champions industriels	>1.200 entreprises informées	>800 entreprises accompagnées
27 leviers d'accompagnement	15 démonstrateurs technologiques	38 partenaires à votre disposition !

Agence du Numérique

Wallonie Relance

Industrie du Futur digital wallonia



Jessica Miclotte
Experte Industrie du Futur
Jessica.miclotte@adn.be
0474/39 60 09
www.digitalwallonia.be/industriedufutur

Agence du Numérique

Wallonie Relance

Plus d’infos sur

digitalwallonia.be/cyber

Cyberwal by digital wallonia

Wallonie Relance