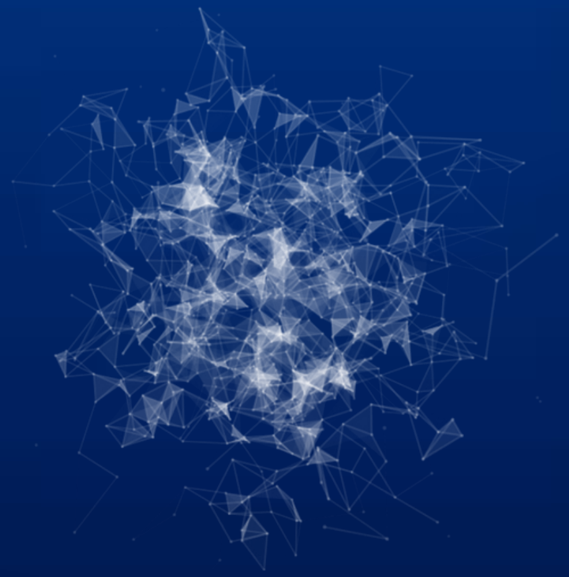
BLUE INFO.

Plaquette - 2025

Jérôme Sanchez - www.blueinfo.fr



SYSTEM - NETWORK AND CYBERSECURITY IT/OT

Table des Matières

Chapitre 1.
La société BLUE INFO.

Le business modèle est la qualité et non celui de la quantité.
Donc, je suis très fier de pouvoir présenter les avantages de BLUE INFO :

IMPLANTATION LOCALE
Le siège se trouve à Thonon-les-Bains et dispose d'une très forte couverture de la région du Léman et du Genevois. Le MeltingSpot 8 avenue du Général de Gaulle 74200 THONON-LES-BAINS

METIERS IT
Administrator | Consulting | Training | Book Author | Speaker
System, Network and Cybersecurity iT/oT

AUTEUR IT
Livre disponible aux éditions ENI : Les fondamentaux de la cybersécurité avec WatchGuard

CONNAISSANCES THÉORIQUES / PRATIQUES
BLUE INFO dispose de +40 certifications sur les technologies les plus pointues. Certifications à renouveler régulièrement permettant d'offrir le meilleur niveau de service aux clients.
https://www.blueinfo.fr/certifications/

EXPÉRIENCE
Depuis 2003 dans les SI (système information) et couvrant tous type de secteurs.

LONGÉVITÉ
Existe depuis 2010 (+15 ans) sur la région du Léman et du Genevois

DISPONIBILITÉ
24h/24 & 7j/7 (en fonction du contrat)

RAPIDITÉ
Contact possible par SMS, MAIL, TÉLÉPHONE (avec une réactivité d'instantanée à maximum 7h)

SOUPLESSE
Le client est décideur, il est toujours informé et c'est lui qui décide de qui, quoi, ou, quand, comment.

TRANSPARENCE
Le client apprend à connaitre les points forts et faibles de son SI (système d'information).
Après chaque intervention, des rapports sont réalisés par mail, ceux-ci contiennent de précieux conseils.

SUIVI
Un interlocuteur diplômé et certifié (disponible 90% du temps) pour les échanges commerciaux et techniques. Permettant ainsi la mise en place de stratégies et de tactiques avec des résultats tangibles.

SÉCURITÉ
Utilisation systématique du "PoLP" en francais on parle "Principe du Moindre Privilège".
Cette approche Admin/User place nos clients dans une démarche de mise en conformité ISO 27001.

FORMATIONS
La société dispose de son propre centre de formation inscrit au DATADOCK.

AUDITS/CONSEILS
Notre équipe est certifiée par l'organisme certificateur PECB « auditeur RGPD / ISO 27001 / Risk Manager ».
Cela permet à chaque moment de respecter les cadres LCR (Légal, Contractuel et réglementaire).

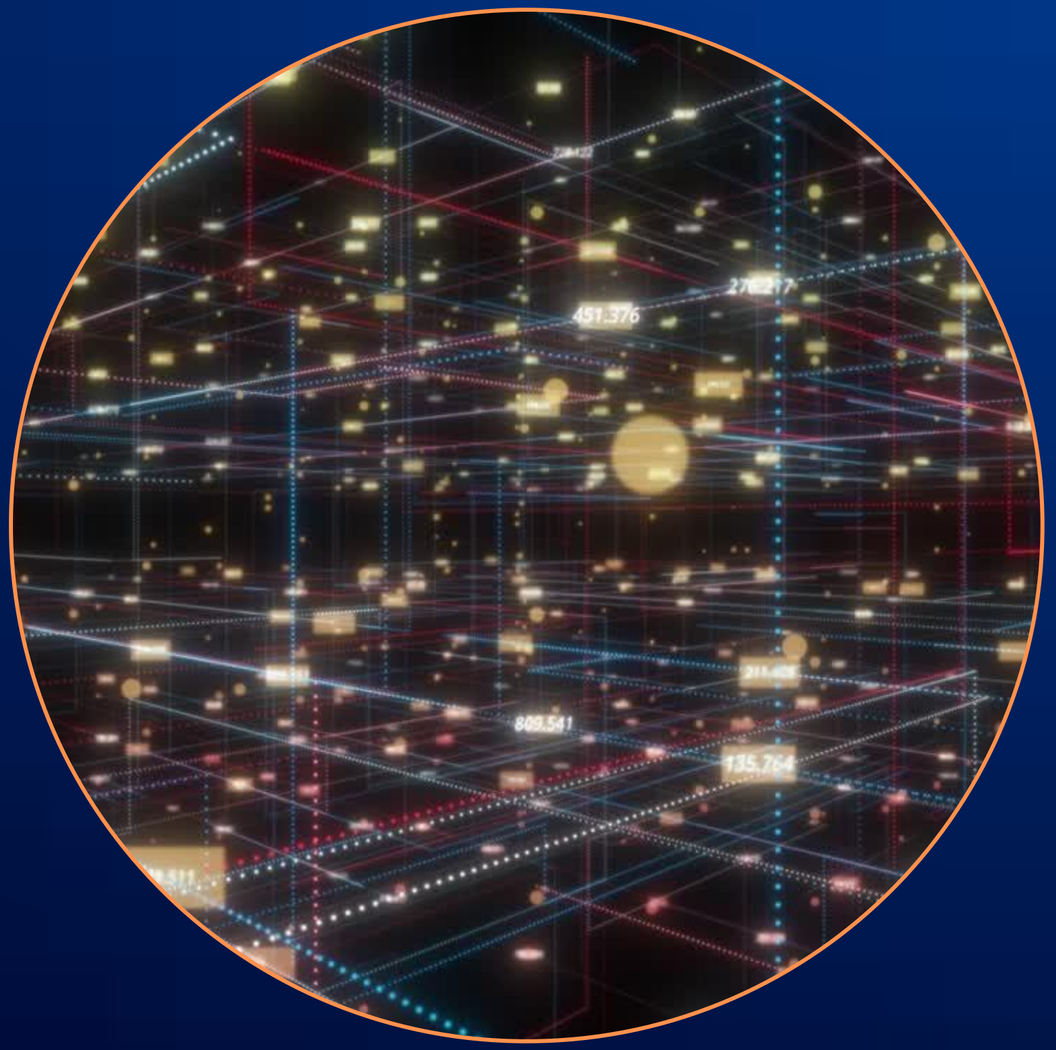
Chapitre 2.
Les certifications

Les certifications (+40)

La formation sur les dernières TECHNOLOGIES et une obligation dans l'iT/oT :
(La liste complète sur www.blueinfo.fr/certifications)

- Microsoft Cybersecurity Architect
- Azure Solutions Architect Expert
- DevOps Engineer Expert
- M365 Enterprise Administrator Expert
- MCSE Core Infrastructure
- MCSA Windows Server 2003/2016
- PECB ISO 27001 Lead Auditor
- PECB ISO 27001 Lead Implementer
- PECB ISO 27005 Risk Manager
- PECB EBIOS Risk Manager (2018)
- PECB ISO 27035 Lead Incident Manager
- PECB Lead SCADA Security Manager
- PECB Certified Data Protection Officer
- PECB Lean Management Black Belt
- IASSC Lean Six Sigma Black Belt
- WatchGuard Certified UTM, EDR, MFA

Chapitre 3.
Les services iT/oT



Les services iT/oT

Si & CYBERSECURITE - iT/oT -

- ADMINISTRATION RESEAUX iT/oT (contrat GOLD sur la base d'un forfait)
- DÉPANNAGE (contrat SILVER sur la base d'heures prépayées).
- MISSION (objectif à définir : cybersécurité etc..) - 875€ HT/jour

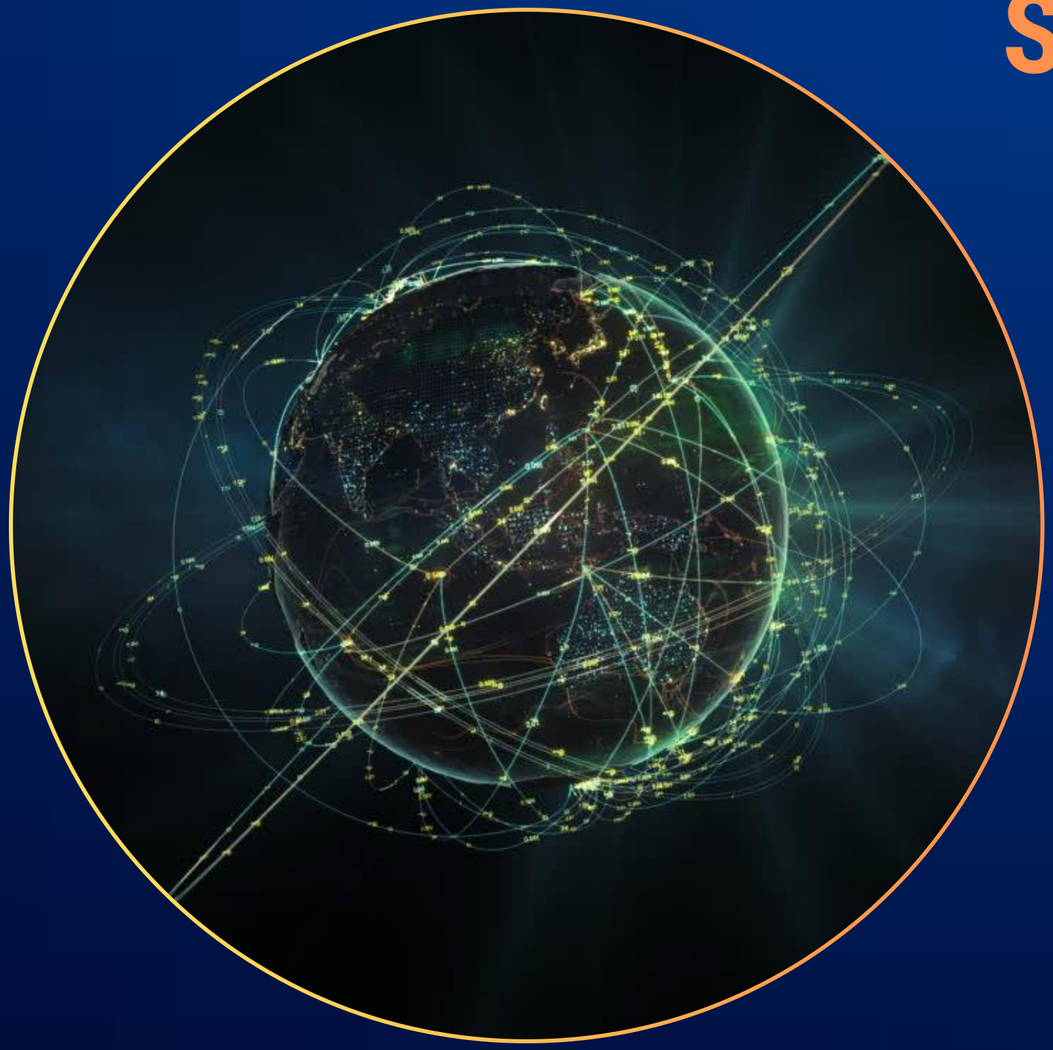
AUDITS (Auditeur ou implémenteur) & CONSEILS - GRC - 875€ HT/jour

- CONSEILS (objectif à définir)
- RGPD (règles strictes de collecte, traitement et conservation des informations privées)
- NIS2 (obligations de cybersécurité et de notification des incidents)
- COBIT (cadre de gouvernance qui aligne iT et stratégies tout en maîtrisant les risques)
- ITIL (meilleures pratiques pour la gestion des services iT)
- ISO27001 (norme internationale qui définit les exigences pour proteger un SI)

FORMATIONS

- PERSONNALISE (objectif à définir)
- MICROSOFT : WS2025 / CLOUD AZURE (AZ) / M365 (MS) / SECURITY (SC)
- CYBERSECURITY iT / oT (SCADA) : introduction / débutant / intermédiaire / avancé
- *Le centre de formation est DATADOCK depuis 2019

Chapitre 3.1
SI & Cybersécurité - iT/oT -



Système d'information (Si)

Définition

« Le SI est un ensemble de ressources humaines (personnel, formation, procédures, etc.) et de ressources techniques (matériel, logiciel, données, réseau, etc.) permettant, à travers plusieurs processus, de collecter, regrouper, classer, traiter et diffuser l'information. »

Son objectif est de créer de la Valeur Ajoutée (VA) pour l'entreprise dans :

- Le monde physique
- Le cyberespace virtuel

Cybersécurité

Définition

« La cybersécurité est la combinaison de personnes, de politiques, de processus et de technologies mises en œuvre par une entreprise pour protéger ses actifs numériques. Elle est optimisée selon les niveaux définis par les dirigeants, en équilibrant les ressources nécessaire entre la facilité d'utilisation/gestion et le niveau de risque compensé. Les sous-domaines de la cybersécurité incluent la sécurité informatique (IT), la sécurité de l'Internet des objets (IoT), la sécurité de l'information et la sécurité des technologies opérationnelles (OT). »

La cybersécurité peut être explorée à travers 3 facettes différentes :

- Normative
- Défensive
- Offensive

Protection SI - Les bases

Pour simplifier à l'extrême, le SI est composé d'actifs à protéger. En Cybersécurité défensive on peut décomposer le SI en 2 parties, la brique « Sureté » et la brique « Sécurité » :

- La Sureté correspondant à la protection des actifs contre les dysfonctionnements involontaires.
- La Sécurité correspond à la protection des actifs contre les actions malveillantes volontaires.

Pour garantir la brique « Sureté », il faut au minimum :

- Avoir un contrat valide.
- Remplacer le matériel obsolète (fin de cycle de vie)
- Maintenir les équipements redondants (HDD/SSD, RAID, Onduleur, etc.)
- Toujours garder vos systèmes à jour (OS Windows & applications)
- Réaliser et vérifier vos sauvegardes régulièrement
- (Attention le contrat SILVER n'inclut pas de sauvegarde ni de vérification)
- Faire un point annuellement (pour cela il faut me contacter et prendre RDV)

Pour garantir la brique « Sécurité », il faut au minimum :

- idem Sureté +
- Respecter le principe AAA (Authentification, Autorisation, Audit)
- Mise en place de PoLP (principe du moindre privilège)
- Changer vos MDP fort régulièrement + activer le MFA (Windows, applications, mails etc..)
- Toujours garder les équipements à jour AV/EDR, UTM, VPN, MFA, WIFI/WIPS, xDR + NDR & MDR
- Approfondir les questions de cybersécurités en vous formant et en réalisant des audits

Pour aller plus loin :

Afin de protéger votre SI, il faut avoir une **DÉFENSE EN PROFONDEUR** (ANSII).
L'ANSII propose un guide de 42 mesures en 10 chapitres pour renforcer son SI :

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
N'hésitez pas à me contacter pour faire le point sur vos SI.

Menaces

Définition

Dans le monde de la cybersécurité, une menace est la cause d'une action, d'un événement ou d'une circonstance pouvant compromettre la sécurité.

Les menaces exploitent les vulnérabilités des actifs.

Les menaces peuvent provenir de sources internes ou externes :

- Actes intentionnels tels que des attaques malveillantes
- Evénements non intentionnels tels que des pannes

Les sources de menaces par vecteur informatique sont les suivantes :

- Attaques connues avec fichiers ou sans fichiers
- Attaques inconnues avec fichiers ou sans fichiers

Exemples

Menaces humaines

Phishing : usurpation d'identité par e-mail pour voler des données

Ingénierie sociale : manipulation psychologique pour obtenir un accès

Erreurs humaines : mauvaise configuration, clics sur des liens malveillants...

Menaces logicielles

Malwares : virus, vers, chevaux de Troie.

Ransomwares : blocage des données contre rançon.

Spywares / Keyloggers : logiciels espions qui collectent des données

Menaces réseau

Attaques DDoS : surcharge d'un service pour le rendre indisponible.

Sniffing / Spoofing : interception ou falsification de données réseau.

Man-in-the-Middle (MitM) : interception de communications

Menaces physiques

Vol de matériel : ordinateurs, disques durs, smartphones.

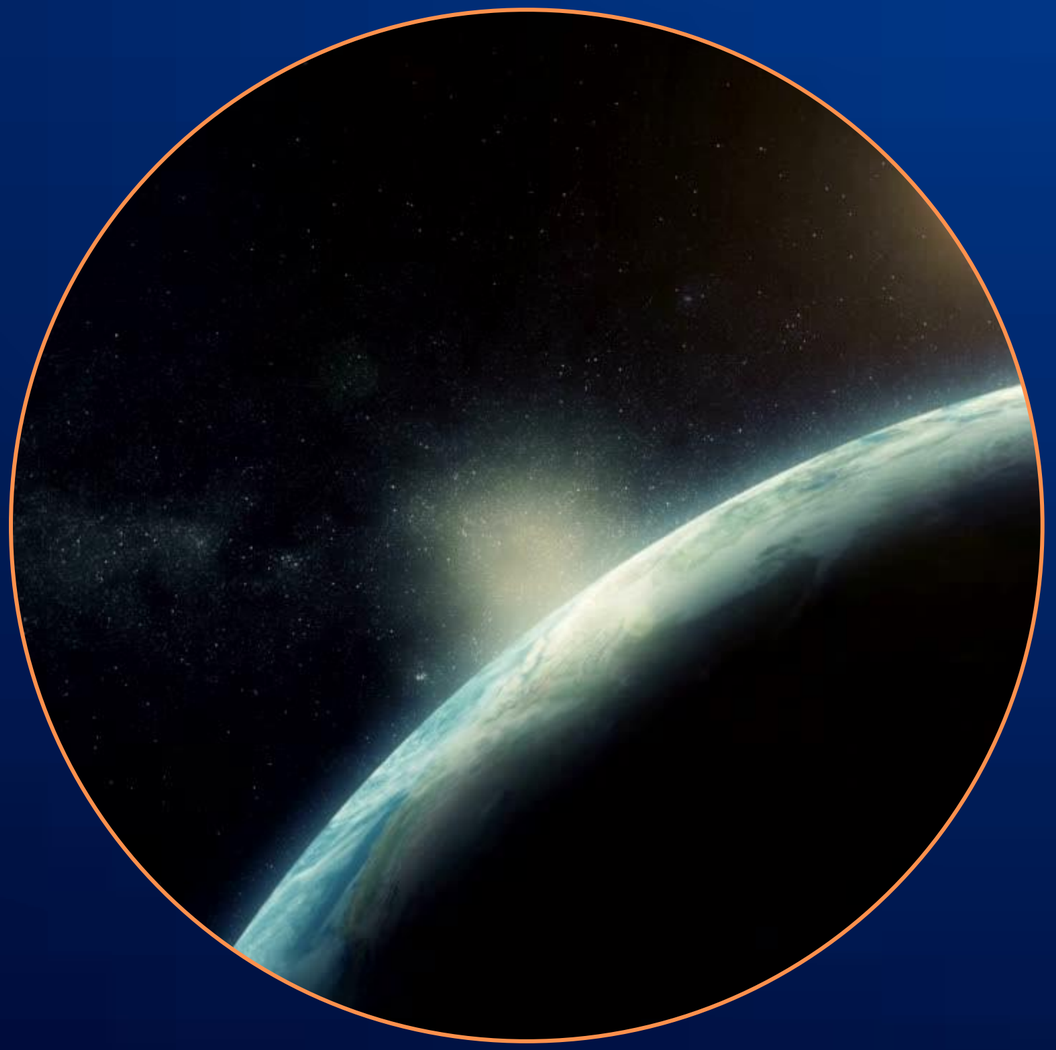
Intrusion physique : accès non autorisé à des locaux sensibles.

Catastrophes naturelles : incendies, inondations, tremblements de terre.

Menaces liées aux tiers

Fournisseurs compromis : attaque via un prestataire ou un partenaire.

Chaîne d'approvisionnement : introduction de vulnérabilités Soft/Hard.

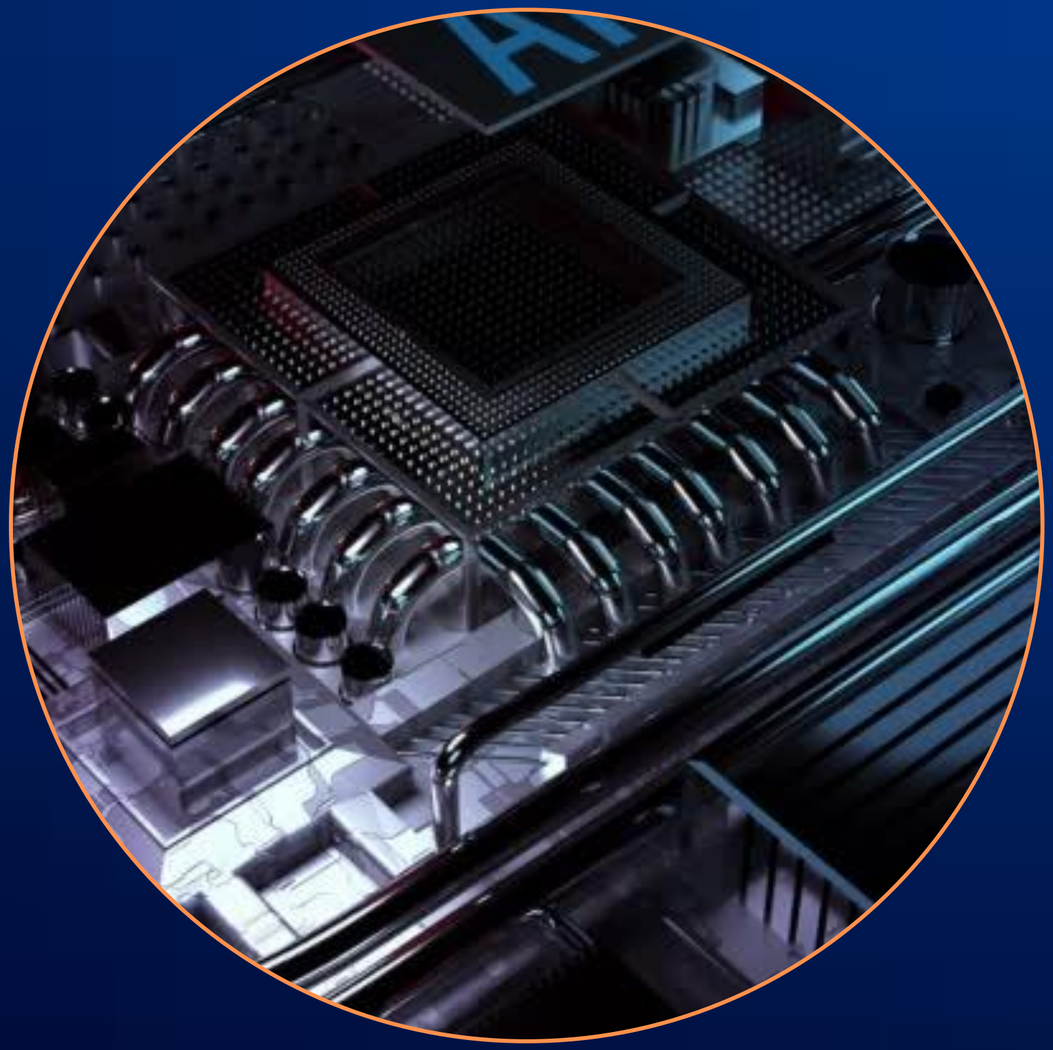


Impacts

Définition

Les menaces si elles se réalisent, sont la « cause » d'un ou plusieurs « impacts » sur « l'organisation ». Les « Impacts Potentiels » ou « Potentiel Conséquences » sont le résultat d'évènement ou de situation qui affecte les objectifs.

- Pertes financières
- Perte d'actifs
- Perte de clients
- Procédures judiciaires
- Perte avantage concurrentiel
- Physique (pouvant parfois entrainer la mort… ICS, SCADA, DCS)
- etc.



intelligence Artificielle

Définition

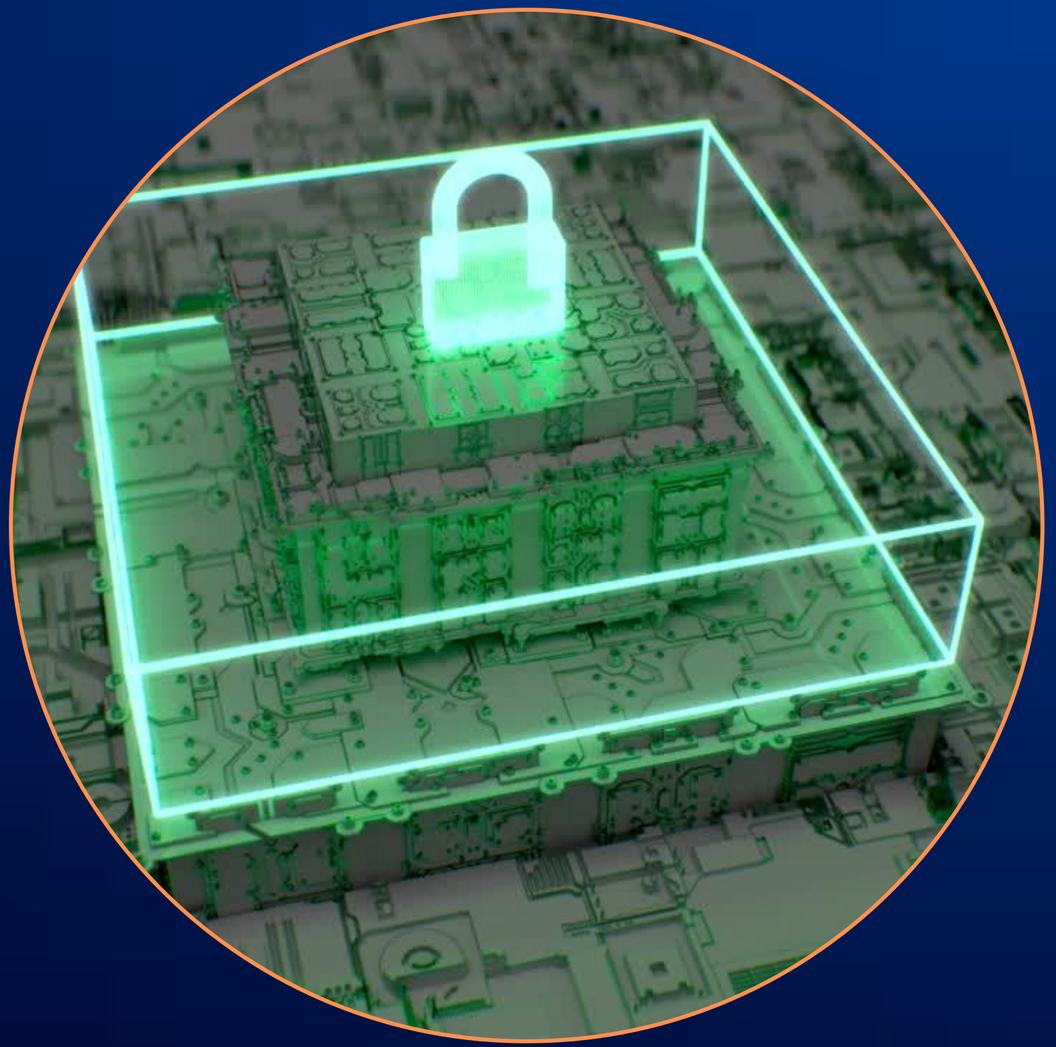
L'intelligence artificielle utilise des techniques d'analyse avancées et basées sur la logique pour interpréter des événements, soutenir et automatiser les décisions.

L'IA utilise les statistiques et de l'optimisation pour fournir des prédictions rapides, de la classification, du regroupement et ainsi définir les meilleures stratégies.

Dans la cybersécurité, voici quelques exemples d'IA répandus :

- Machine Learning (ML) algorithmes qui apprennent à partir de données
  - Neural Network (NN) algorithme inspiré des neurones biologiques
    - Deep Learning (DL) NN avec plusieurs profondeur (+3)

Chapitre 3.2
Audits & Conseils - GRC -



GRC

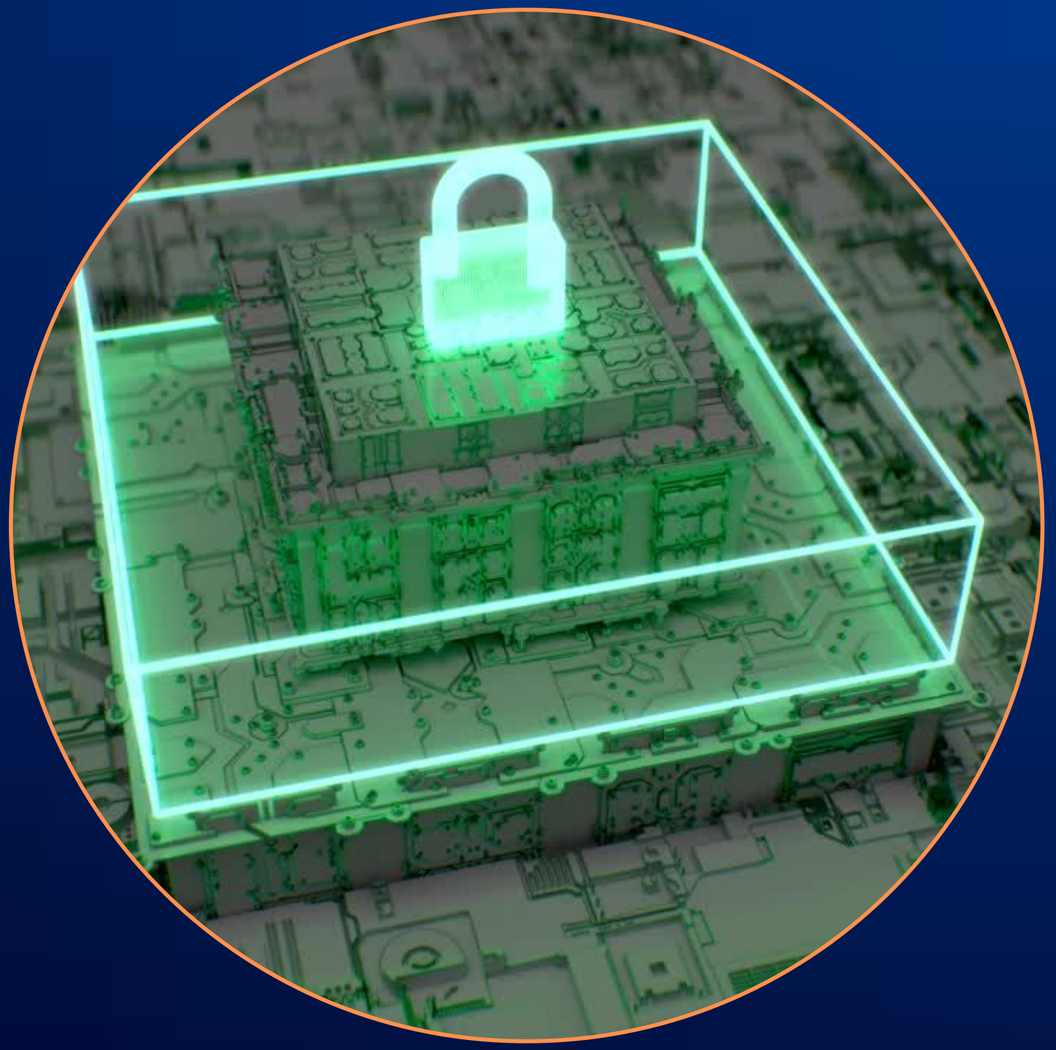
Gouvernance, Risques et Conformité

De nombreuses nouvelles obligations Européennes sont désormais en place, avec des impacts variés, tant positifs que négatifs. Ces régulations visent à améliorer la sécurité, la résilience et la concurrence dans l'environnement numérique. Cependant, dans la pratique, elles peuvent parfois devenir complexes et coûteuses, et dans certains cas, affecter la liberté d'expression.

Comme le dit le proverbe, "l'enfer est pavé de bonnes intentions".

Nos services sont là pour simplifier ces démarches et vous accompagner dans la conformité avec ces normes et réglements obligatoires.

- RGPD
- NIS2



NIS2 (Directive on Security of Network and Information Systems)
Étends les exigences de cybersécurité à un plus grand nombre de secteurs.
Renforçant les normes de sécurité et les obligations de notification des incidents.

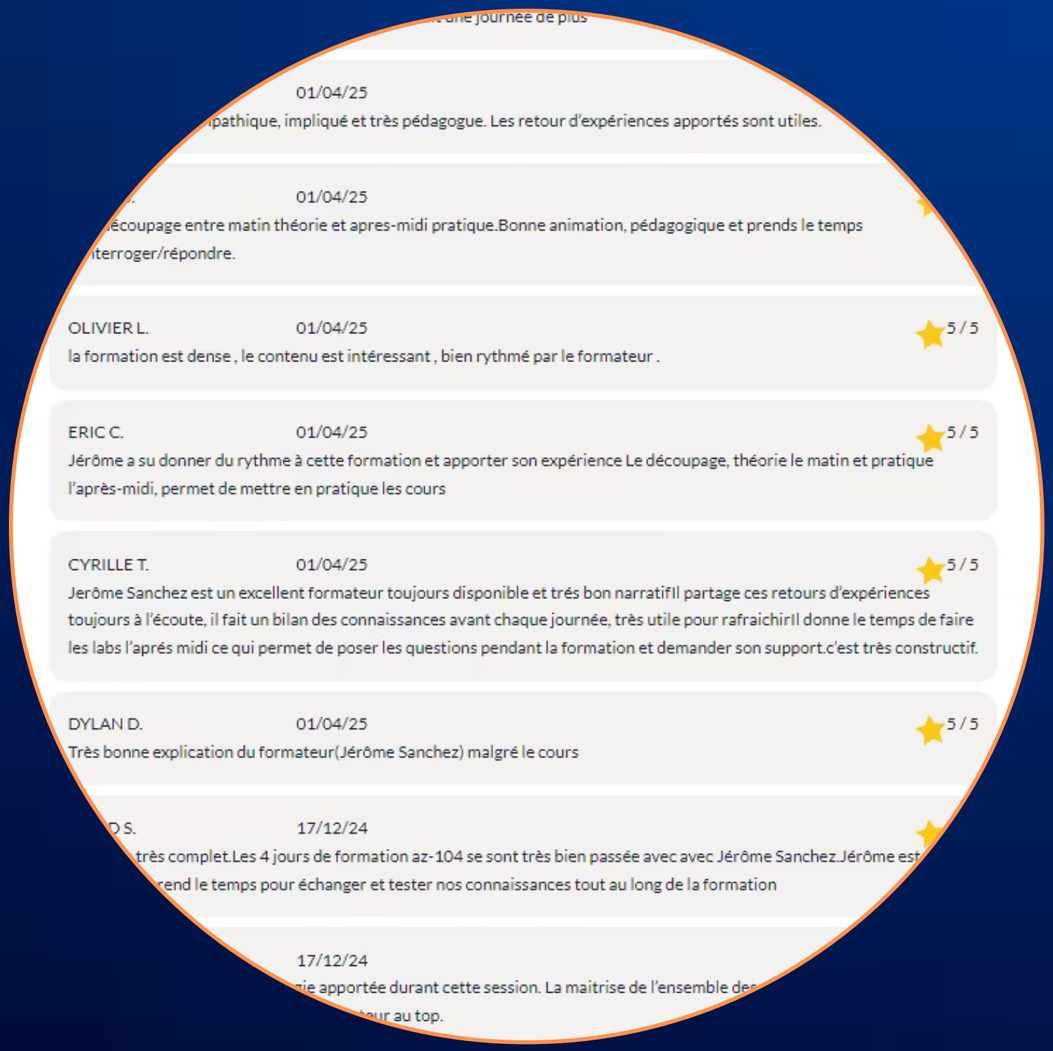
La directive NIS2 a été adoptée le 10 novembre 2022 et est entrée en vigueur le 16 janvier 2023. Les États membres de l'UE doivent transposer NIS2 dans leur législation nationale d'ici le 17 octobre 2024.

Les amendes peuvent atteindre jusqu'à 10 millions d'euros ou jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'organisation, selon le montant le plus élevé. Le montant exact des amendes dépendra de la gravité de la non-conformité et de l'impact des incidents de cybersécurité.

RGPD (Règlement Général sur la Protection des Données)
Depuis le 25 mai 2018, le RGPD (le Règlement Général sur la Protection des Données) est en vigueur. Le site de la CNIL rappelle les bonnes pratiques en matière de traitement des données.

Les amendes peuvent atteindre jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'organisation, selon le montant le plus élevé. Les amendes sont calculées en fonction de la gravité de l'infraction et du degré de négligence.

Chapitre 3.3
Formations



Formations

MCT (Microsoft Certified Trainer) & PCT (PECB Certified Trainer)

Les centres de formation de renommée internationale comme Orsys (France, Belgique, Suisse, Luxembourg, Monaco) s'appuient sur nos services pour proposer des formations pointues sur les dernières technologies et cadres réglementaires.

À droite, découvrez quelques-uns de nos clients qui nous font confiance pour former leurs équipes.
Nos formations : Azure, M365, ISO27001, RGPD, SCADA...
(noté **+18/20** par les stagiaires en 2024/2025)

Indicateur de performance sur la qualité de la prestation de formation :
Moyenne générale des animations 2024
Pour société, société unipersonnel (indépendant) et intervenant d'une société

Notes *	Indice d'évaluation de la prestation	Indice obtenu
≥ à 18	Très satisfaisant	
≥ à 16	Satisfaisant	
≥ à 15	Moyennement satisfaisant	
< à 15	Insuffisant	

** Moyenne calculée sur l'item « satisfaction générale de la session » des évaluations participants de l'ensemble des sessions réalisées sur l'année de référence.*

AUDEMARS PIGUET
NAVAL GROUP
SAFRAN
La Poste
OCSIN
RATP
ARCELOR
CMA-CGM
SUEZ
EXAKIS NELITE
ALTEN
KP1
ONF
A3IS
UNSYS
BANQUE DE FRANCE
NEO SOFT
SITEC
BOURSORAMA
NRJ
etc...

Chapitre 4.
Livre

Livre sur la Cybersécurité

Les Fondamentaux de la Cybersécurité avec WatchGuard (Edition ENI en vente sur Amazone, Fnac et Cultura)

Ce livre est destiné aux informaticiens dotés de connaissances de base en réseau et désireux de découvrir comment mettre en œuvre la cybersécurité à travers les services et produits WatchGuard.

Il a pour double objectif d'exposer les concepts fondamentaux du Système d'Information et de la cybersécurité tout en explorant une vaste gamme de technologies incontournables pour la sécurisation des systèmes modernes.

La puissance de cet ouvrage réside dans sa capacité à rendre les concepts complexes accessibles à tous.

Table des matières (980 pages) :

Chapitre 5.
Conférences

Conférences Cyber + iA

Depuis 2024, nous avons l'honneur de partager notre expertise à travers des salons ou des séminaires. En partenariat avec des leaders du secteur de la formation comme ORSYS, nous mettons l'accent sur les Si, la Cybersécurité et l'Intelligence Artificielle.

Chapitre 6.
RESPONSABILITÉS & ASSURANCES

RESPONSABILITÉS & ASSURANCES

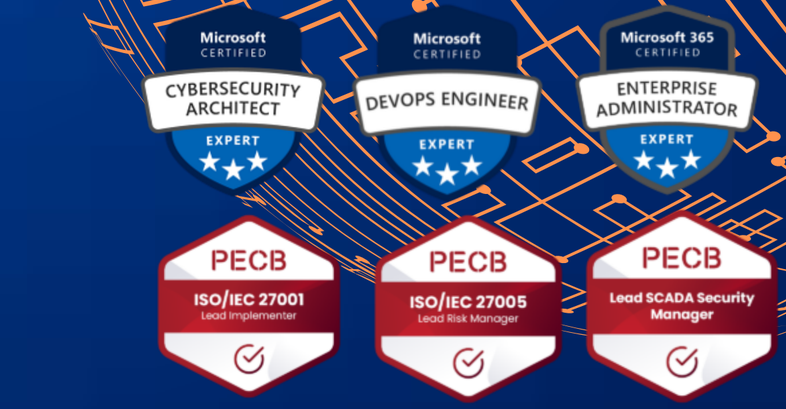
Le client à travers ses décisions et actions est responsable de la « Sureté » et de la « Sécurité » de son SI :

- Il incombe au client la réalisation et le test de ses sauvegardes, sauf en cas de mission spécifique confiée à BLUE INFO.
- Le contrat SILVER ne couvre pas les sauvegardes, ni leurs tests.
- BLUE INFO s'engage à informer ses clients des risques potentiels et à formuler des recommandations de sécurité tout au long de l'année.
- Dans ces conditions, BLUE INFO ne peut être tenue responsable des incidents affectant le réseau du client.
- BLUE INFO recommande vivement la souscription d'une assurance couvrant toutes les menaces informatiques telles que le vol, la détérioration, le piratage ou la suppression de données etc...

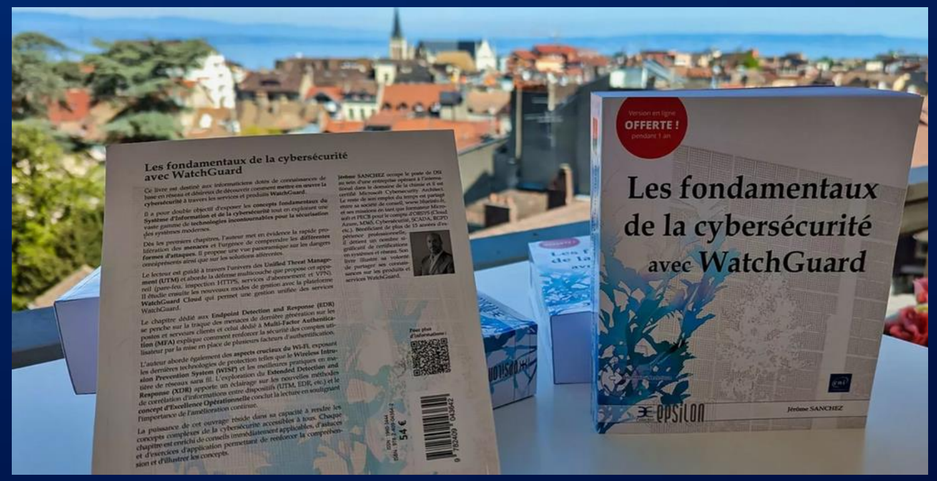
Jérôme Sanchez
Administrator | **Consulting** | **Training**
Book Author | **Speaker**
System, Network and Cybersecurity iT/oT

commercial@blueinfo.fr
+33 7 86 09 22 00
www.blueinfo.fr

blue
INFORMATIQUE



- **MCT (Microsoft Certified Training)**
  - Microsoft Cybersecurity Architect
  - Azure Solutions Architect Expert
  - DevOps Engineer Expert
  - M365 Enterprise Administrator Expert
  - MCSE Core Infrastructure
- **PCT (PECB Certified Training)**
  - PECB 27001 LA, LI, RM, CDPO
  - PECB Lead SCADA Security Manager
  - PECB Lean Management Black Belt
- **IASSC** Lean Six Sigma Black Belt
- **WatchGuard certified** UTM, EDR, MFA
- **ENI** Les fondamentaux de la cybersécurité avec WatchGuard



retrouvez moi sur Linkedin

+4 500 personnes déjà connectées !!