Forum d'Aix-Marseille Université de la Cybersécurité - AMUSEC 2024

Segmenter pour mieux régner

... La segmentation réseau à l'épreuve des directives et normes

Conférence donnée le 23/02/2024

Qui sommes-nous ?

Cyberium

Robust security without isolation

Gilles Loridon
CEO

Stanislas Verley
VP Business Development

Laurent Pipitone
VP Marketing & Product Strategy

Société Française **experte en segmentation des réseaux** avec un portefeuille de solutions de sécurisation physique des communications **uni et bi-directionnelle** (**Data Diodes** / Cross-Domain) pour les **écosystèmes industriels** et gouvernementaux.

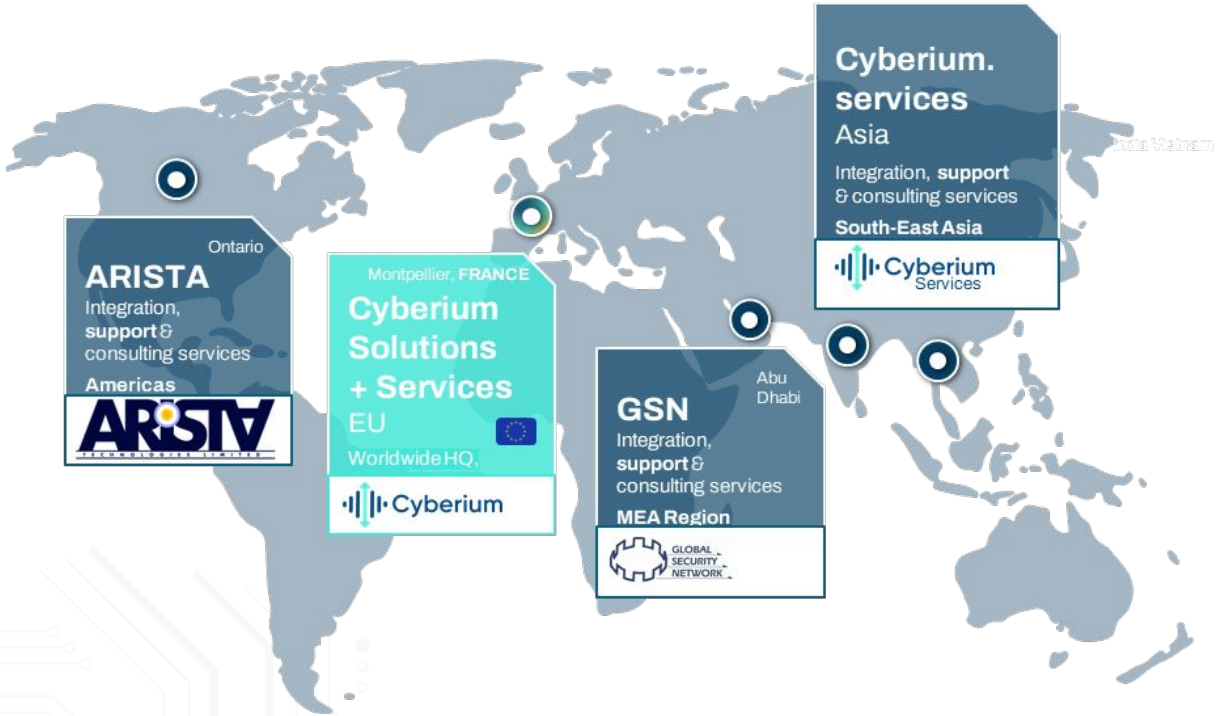
Fondée par **2 experts en Cybersécurité**.

Gilles est notamment référent de la **norme IEC-62443**(*) au Moyen-Orient et Stanislas a conduit de nombreux audits sur la base de cette norme internationale. Ils sont également **auteurs de brevets autour des technologies Data Diodes appliquées à l'OT**.

(*) Réseaux de communication industriels

Notre mission : libérer les EE et EI de pratiques cyber-isolationnistes, afin d'accélérer leur transformation digitale tout en préservant une sécurité absolue

International reach



> 300+

Deployed solutions

> 4

Main operating regions

Segmentation réseau ?

- **Segmentation :** protection “nord-sud” (externe)
- **Micro-segmentation :** protection “est-ouest” (interne)

Spécificités :

- Défense proactive
- **Physique** ou virtuelle

Valeur sécuritaire :

- Menaces externes & déplacement latéral
- Menaces internes & déplacement latéral
- Ségrégation interne / invité
- Protection / conformité pour les données réglementées

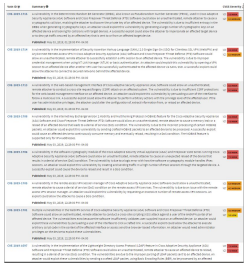
#Vulnérabilités Connues

Problème? les firewalls ne suffisent pas toujours…

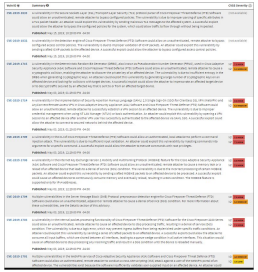
+ Impact en chaîne des mises à jour souvent complexes dans un contexte OT très contraint sur le “Change”

> “All Cisco devices with IOS XE and an internet facing HTTP server are vulnerable and there is no patch nor workaround but IoC are available.
>
> The vulnerability is easy to exploit and enables the attacker to get admin access and full control of the targeted devices. **- 2023**

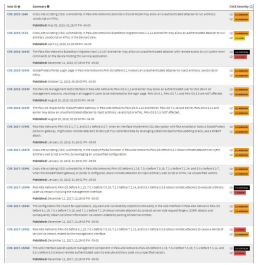
Cisco ASA CVE



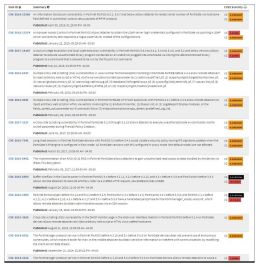
Cisco FTD CVE



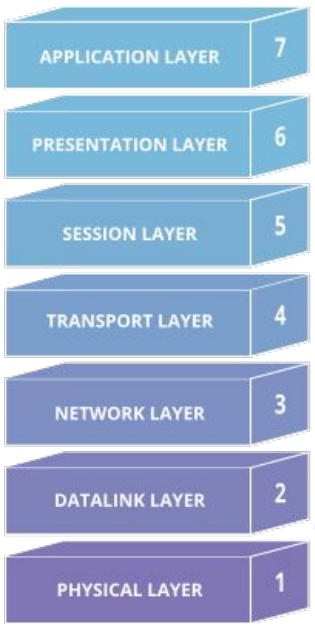
Palo Alto Networks



FORTINET CVE



When possible, make it one-way



OSI network layers

Surface of Attack (SoA)

Airgap

0 - way

More harm than good? Not real-time, manual transportation of data, increased risks on individuals, data fragmentation and more devices to sanitize

Firewalls

2 - way

Prone to bugs, mistakes and **hackers** or staff...

- Firewall is based on firmware, software and logic and is therefore vulnerable to attacks
- Is the Firewall setup properly?
- Back doors, covert channel / No guarantee of data traffic not going back to the external network.

True Data diodes

1 - way

Inviolability by physical law + “Blind” attacker

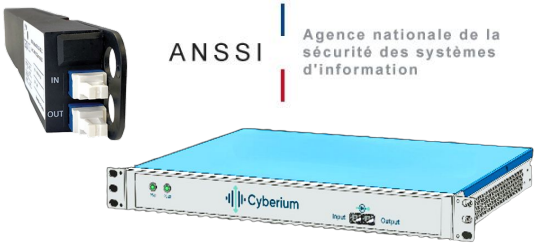
Light Emitter

Light Receiver

Don’t just take our word for it…

NIST	The National Institute of Standards and Technology – One direction gateway staves off all connection among domain traffic
enisa European Network and Information Security Agency	European Network and Information Security Agency- One direction gateway enables to realize superior protection to firewall.
ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM	Department of homeland security recommends one direction gateway at the security assessment. (Industry control system security organization)
ISA IEC	One direction gateway - Limits the spread of the malicious code. (ISA SP-99-3-3 /IEC 62443-3-3)
U.S.NRC NEI NUCLEAR ENERGY INSTITUTE	U.S. Nuclear Regulatory Commission and the Nuclear Energy Institute exonerate 21 cases from 26 cases of Cyber boundary rules at the protected site by one direction technology.
NERC CIP	At the site which is protected by one direction technology in critical infrastructure protection standard of North American Electric Reliability Corporation, more than 35 % requirements is exonerated.

Our Data Diode for critical verticals



Critical infrastructures need **unhackable security** without compromise whilst **transferring data from OT to IT,** either for commercial or industrial use.

Cross-domain data transfer and **data protection** add-ons built on top of the **most secure data diode** technology **in the world**.

Cross-domain data transfer technologies to empower **inviolable data bastion** or data lake for the most protected secrets.

Security Applications

Confidential networks need to send **OR** receive information from other networks **without** compromising isolation-grade security.

Gov & Secret defense

- **Lawful interception**
- **Secret Information protection**
- **E-Gate & Immigration**
- **Legacy CCTV isolation**
- **E-government asynchronous requests**

Industry 4.0 & Utilities

- **MES** (Manufacturing Execution System) / **Sync OT <> IT raw data** (Pi, Historian…)
- **Sync OT <> IT raw files** (Alarms & Events, backups…)
- **Preventive maintenance** (Potentially cloud + AI)
- **Production optimisation** (Potentially cloud + AI)

NIS2 : **directive EU en cours de transposition** dans la Loi FR

Impose :

- Qui est concerné par quoi ? (EI/EE)
- Proportionnalité
- **Sanctions**
- Déclaration d'incident
- Mesure de la mise en oeuvre

NIS2 : un catalyseur

- **≈ 150 000 organisations** (x10 - x30)
- **600 types d'entités, 18 secteurs, PME & CAC 40**
- **Sanctions = MAX (10 M€, 2% du CA)**

> Preamble (89) **Essential and important** entities should adopt a wide range of basic cyber hygiene practices, **such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness**, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

Conseil #1 : ne pas réinventer la roue dans la mise en oeuvre de NIS2 !

Industriels, utilisez l'opportunité de NIS2 pour implémenter le framework de référence pour la sécurité des réseaux industriels : ISA IEC-62443

NIS2 délègue l'implémentation :

Aux autres standards et frameworks, tels que IEC 62443 pour les réseaux industriels

Champs d'application croisés NIS2 ⨯ IEC-62443

Gouvernance

NIS2 : Votre roadmap pour Octobre 2025

1. Découvrir ce que vous avez déjà mis en place
2. Evaluer les risques de vos systèmes et processus
3. Agir sur les failles de sécurité principales
4. **Maintenez votre système de gestion de la cybersécurité**

Notion de CSMS (IEC 62443-3-2) ... voir ci-après.

Exécution

ISA IEC 62443

Standard international, robuste et efficace répondant aux attentes de NIS2 **sans crainte de requalification ultérieure**

Mapping complet de la NIS2 article 21.2…	… par l'usage de IEC 62443-2-1
a. Policies on risk analysis and information system security	**4.3.2.3** Organizing for security ; 4.3.2.6 Security policies and procedures ; **4.4.3** Review, improve and maintain the CSMS.
b. Incident handling	**4.3.4.5** Incident planning and response
c. Business continuity, such as backup management and disaster recovery, and crisis management	**4.3.2.5** Business continuity plan, **4.3.4.5** Incident planning and response
d. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	**4.3.2.2** CSMS scope, **4.3.2.3** Organizing for security ; **4.3.4.3** System development and maintenance ; **4.4.3** Review, improve and maintain the CSMS
e. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	**4.2.3** Risk identification, classification and assessment ; **4.3.3.4 Network segmentation** ; **4.3.4.3** System development and maintenance
f. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	**4.3.2.6** Security policies and procedures ; **4.2.3** Risk identification, classification and assessment ; **4.4.2** Conformance ; **4.4.3** Review, improve, and maintain the CSMS
g. Basic cyber hygiene practices and cybersecurity training	**4.3.2.4** Staff training and security awareness
h. Policies and procedures regarding the use of cryptography and, where appropriate, encryption	**4.3.4.3** System development and maintenance
i. Human resources security, access control policies and asset management	**4.3.2.4** Staff training and security awareness ; **4.3.3.2** Personnel security ; **4.3.3.5** Access control – account administration ; **4.3.3.6** Access control – authentication ; **4.3.3.7** Access control – authorization ; **4.3.4.4** Information and documentation management
j. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	**4.3.2.5** Business continuity plan ; **4.3.3.5** Access control – account administration ; **4.3.3.6** Access control - authentication

Conseil #2 : ne négligez pas la segmentation réseau !

L'extension du champ de la NIS2 à de nombreux acteurs amène un déport des technologies auparavant réservées aux OSE (LPM) vers les nouveaux EE / EI

Mais toutes les segmentations ne sont pas nées égales…

SR and RE	Firewalls	Two way gateway	Hardware DataDiode
FR 5 – Restricted data flow			
SR5.1 - Network segmentation	Yes	Yes	Yes
SR5.1 RE 1 Physical Network segmentation	No	Debatable	Yes
SR5.1 RE 2 Independence from non-control system networks	Maybe	Maybe	Yes
SR5.1 RE 3 Logical and physical isolation of critical networks	No	Debatable	Yes
SR5.2 - Zone boundary protection	Yes	Yes	Yes
SR5.2 RE 1 Deny by default, allow by exception	Maybe	Yes	Yes
SR5.2 RE 2 Island mode	?	?	Yes
SR5.2 RE 3 Fail close	Maybe	Yes	Yes
SR5.3 - General purpose person-to-person restriction	Possible	Possible	Yes
SR5.3 RE 1 Prohibit all general purpose person-to-person communication	Possible	Possible	Yes
SR5.4 - Application partitioning	Possible with exception	Possible with exception	Yes

Certains protocoles industriels tels que OPC DA sont **extrêmement difficiles à segmenter avec un Firewall classique**

Et toutes les Data Diodes ne se valent pas non plus

Les Data Diodes bi-directionnelles, logicielles ou basées FPGA **ne garantissent pas** l'imperméabilité aux attaques extérieures. Leur niveau de sécurité **équivaut à celui des Firewalls**. (CC.EAL 4+)

1 Garantie du vrai uni-directionnel

(= pas de http)

Inviolability by physical law
+ "Blind" attacker

Light Emitter Light Receiver

2 Reconnaissance par les certifications

Certification ANSSI Agence nationale de la sécurité des systèmes d'information

CC EAL 7+ Common Criteria

CC.EAL 7+

(>> aux firewalls certifiés au mieux 4+)

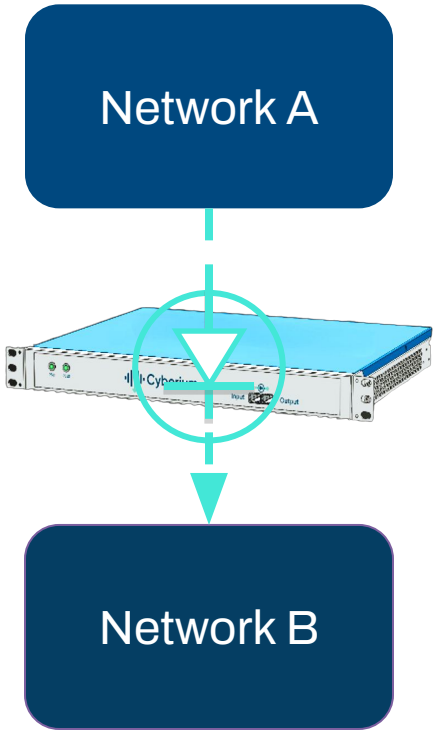
3 Capacités intrinsèques

- **Support des protocoles et bases de données OT**
- De 1 à 25 Gb /s (avec HA)
- Antivirus temp-réel (wire-speed)
- Fiabilité totale et reprise sur panne réseau (buffering)

Impossibilité d'une attaque menée depuis une position extérieure au réseau

True Data Diodes
top challenges

1. **UDP only**. Three-Way Handshake **impossible** e.g. **TCP** and SQL/FTP/...
2. **Data integrity issues**
3. **No control** over the **data flow** leading to repeated packet sending (poor for bandwidth...)
4. **Malware** can flow **through**



Target architecture

Internet

IT Network layer
> Level 4 (unsecured)

IT Data lake, Historian, A&E database

SIEM, A/V, WSUS, Backups

Proxy North

Proxy South

Data Diodes supercharged by proxies
At no security loss **by design!**
From 1 up to 10 Gbps

OT Network segmentation
Remote attacker **CANNOT** access the OT network

DCS / DMZ
> Level 3.5

3rd party
> Level 3

SIS
> Level 2.5

Proxy South

Proxy North

Safety network segmentation

Historian, A&E database

SIEM, Backups, A/V, WSUS

Scada

PLC

Historian

> Core OT network
Levels 1 to 2 (secured)

Data reliability up to 10 Gbps (SOON 25 GB) guaranteed by proxies

Detect & fix errors

Data is **hashed**, so any packet loss or change is detected, then corrected through **CRC** & **FEC** (Forward Error Correction)

Retry on bottleneck

Proxies are equipped with adequate **buffers** to allow data resending upon partial or complete destination unavailability.

Sanitize malware

Multiple **antivirus** engines operate at **wire speed** on the safe-side proxy. (avoids exposure)

High Availability

Multiple **architectural** options enable no-point of failure and **Load Balancing** across Data diodes.

0% packet loss and cost-effective strategy for 1+ Gbps as opposed to multiple packet sending attempts (classical Data Diode approach).

Unique IT/OT protocols support

Standard protocols (IT)

- TCP/UDP streaming
- FTP/SFTP/FTPS or Managed FTP (MFTP)
- Emails forwarding (SMTP)
- Database replication (Oracle, MSSQL, PgSQL)

Industrial protocols (OT)

- Logs forwarding
- OSIsoft PI 2 PI, Honeywell PHD 2 PHD,BN System 1, AspenTech IP21, AVEVA Historian...
- OPC UA, OPC DA, OPC A&E, Modbus...
- A/V and MS Windows update
- Splunk UF->SE
- Span Port
- IBM MQ and MQTT

Sources

- NIS2 : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022L2555
- ENISA : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0881
- jhttps://www.dnv.com/cybersecurity/cyber-insights/leverage-iec-62443-for-eu-nis2-directive-compliance.html
- https://industrialcyber.co/analysis/implications-of-the-nis2-directive-and-a-comparative-insight-with-iec-62443

,

Merci...