

STORMSHIELD

# Les systèmes DPI et la sécurité réseau

## La technologie IPS Stateful DPI dans les environnements OT

# Executive summary

Aujourd'hui, la segmentation des réseaux opérationnels constitue un premier niveau pour lutter contre les cyberattaques. Or, pour faire face aux nouvelles menaces de plus en plus sophistiquées, le déploiement de solutions d'analyse en profondeur (DPI - *Deep Packet Inspection*) des messages échangés s'avère également nécessaire pour anticiper la protection de ces réseaux sensibles.

Pour réussir ce pari dans l'OT, les solutions de sécurité déployées doivent répondre à des exigences fortes **de disponibilité, d'intégrité et de confidentialité**, émanant des différents enjeux métiers que supportent les réseaux opérationnels.

L'implémentation d'un système IPS (*Intrusion Prevention System*) au plus près des automates doit donc respecter ces aspects afin de pouvoir appliquer une politique de sécurité proactive et durable tout en garantissant la sûreté de fonctionnement des réseaux opérationnels.

Pour cela, quatre axes majeurs sont à prendre en considération :

- une **solution intégrée** qui assure une connaissance fine des protocoles industriels ;
- une **capacité à contrôler la conformité des messages opérationnels** pour mieux repérer les anomalies et préserver les actifs du réseau OT ;
- une **protection proactive face aux différentes variantes de menaces** pour contrer les attaques ciblées et éviter des arrêts dans la production ;
- une **approche contextuelle des échanges de messages** afin d'assurer la conformité vis-à-vis des processus opérationnels.

Ce livre blanc décrit les différents mécanismes qu'un système IPS doit exploiter pour mener à bien sa mission de détection et de protection. Il vous donnera également les éléments nécessaires qu'un IPS se doit d'intégrer pour s'adapter à vos besoins de sécurité.

Ce livre blanc s'adresse aux Responsables d'Exploitation, aux Responsables de maintenance, métier et opérationnel en charge des infrastructures critiques et aux Responsables de la Sécurité des Systèmes d'Information.

**Stormshield**

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin de s'appuyer sur des partenaires de confiance pour accompagner leur transformation numérique et assurer la cybersécurité de leurs infrastructures, de leurs utilisateurs et de leurs données. Les technologies Stormshield, certifiées au plus haut niveau européen (EU Restreint, OTAN Restreint, Critères Communs EAL3+/EAL4+, qualifications et visas ANSSI), répondent aux enjeux de l'IT et de l'OT afin de protéger vos activités. Nos solutions de sécurité vous redonnent la liberté d'entreprendre en toute sérénité.

## Sommaire


1. Contexte
2. Les risques cyber associés aux réseaux opérationnels
3. Systèmes de défense : sonde industrielle ou IPS ?
4. Les principes généraux de l'Intrusion Prevention System
   - Signature ou recherche protocolaire ciblée : deux approches pour le contrôle de conformité protocolaire
   - L'analyse contextuelle au cœur de la sécurité des échanges
   - La recherche des menaces réseau dans les échanges
   - Les nécessaires signatures personnalisées
5. Les critères pour bien choisir son IPS
6. Le moteur *Stateful DPI* Stormshield

# Contexte

Les cyberattaques contre les infrastructures opérationnelles sont de plus en plus sophistiquées. Séquencées en différentes étapes, elles deviennent virulentes et complexes à détecter par les différents systèmes de protection. Les *Advanced Persistent Threat* (APT) constituent des cyberattaques utilisant un ensemble de techniques et méthodes stratégiquement combinées afin d'atteindre une cible bien définie. Restant le plus longtemps sous les radars pour ne pas éveiller de soupçons, elles visent généralement l'exfiltration de données à fortes valeurs ajoutées (brevets, secrets industriels, etc.).

De ce fait, même si la plupart des entreprises et organisations se disent sensibilisées aux risques cyber et les implications que ceux-ci peuvent engendrer (perte ou vol de données, arrêts dans la production, etc.), elles sont bien souvent plus à risque qu'elles ne le pensent. Avec l'apparition, ces dernières années, de l'internet industriel des objets (IIoT), les cyberattaques ciblent des entreprises de différents secteurs comme l'aéronautique, le nucléaire, l'électricité, la santé… Des acteurs d'importance vitale pour la société qui deviennent des cibles privilégiées.

> L'enjeu est de concevoir l'architecture capable d'assurer la transmission, le traitement et **le maintien de l'intégrité des données** entre les systèmes.
>
> Cigref

Dans certains cas, ces acteurs savent pourtant où se trouvent les faiblesses de leurs systèmes, mais n'ont pas les moyens de remplacer les applications et/ou les équipements concernés. Ce cas de figure est fréquent dans les réseaux opérationnels et critiques, comme le secteur de la santé, qui utilisent des applications qui ne sont supportées que sur des anciens systèmes d'exploitation. Dans le domaine industriel, certains composants sont conservés alors même qu'ils sont obsolètes, ce qui accentue le risque d'être touché par une attaque implantée discrètement depuis un certain temps. Comme le révèle une étude de novembre 2019[1], certaines failles et vulnérabilités sont en effet utilisées depuis plus de dix ans par les cyberattaquants, et continuent d'être exploitées aujourd'hui.

Mais la cybersécurité industrielle reste une discipline relativement récente. L'expérience dans le domaine du monde de l'IT[2], comme l'analyse de risques par exemple, s'avère également utile pour apporter une réponse appropriée et efficace moyennant quelques ajustements.

Ce livre blanc a pour volonté de traiter et d'analyser les méthodes de protection réseau de type IPS ainsi que les enjeux associés dans la sécurisation des réseaux OT.

[1] Stormshield, www.stormshield.com/fr/actus/quelles-tendances-cybersecurite-pour-2020/
[2] Stormshield, www.stormshield.com/fr/actus/reseaux-it-ot-raisons-convergence-delicate/

# Les risques cyber associés aux réseaux opérationnels

Les dernières années, la transformation numérique marquée par la convergence IT/OT ou encore l'utilisation de l'Edge/Cloud Computing[3], conduit les réseaux d'entreprises industrielles, de toute taille, à une hyperconnectivité accrue. Des projets **d'excellence opérationnelle**, en lien avec l'Industrie 4.0 (comme l'optimisation avancée entre la chaîne de production et l'ERP de l'entreprise) rendent les réseaux opérationnels plus perméables aux risques cyber.

Récemment avec l'attaque EKANS (ou Snake), **nous avons (re)pris conscience de la dangerosité** des risques qu'une intrusion dans le réseau industriel peut provoquer. Il y a des facteurs qui peuvent favoriser ce type de risques : manque d'homogénéité entre les équipements mis en place et les postes de contrôle ou encore des composants industriels avec des normes et/ou des exigences distinctes. Ces éléments qui coexistent dans le même environnement peuvent provoquer des failles conduisant à la chute de tout le système.[4]

Force est de constater que dans l'univers OT, dès qu'il se produit des connexions des systèmes et machines jusqu'alors isolés du réseau, la possibilité de piratage augmente avec des lourdes conséquences : dégradation physique, interruption de production ou encore vol de procédés industriels.

Avec la convergence IT/OT qui s'opère, beaucoup d'industriels commencent à mettre en place une gouvernance globale de leurs sites afin de bénéficier d'une meilleure visibilité sur leurs réseaux opérationnels. De ce fait, pour arriver à une bonne observation des problématiques de cybersécurité industrielle, **les mondes de l'IT et de l'OT doivent dialoguer tout en analysant et en évaluant les risques afin de faciliter une mise en place efficace des processus d'administration et de gestion de la sécurité réseau.**

[3] Forbes, www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/#5f46307f24ae

[4] Stormshield, www.stormshield.com/fr/actus/industrie-manufacturiere-menace-cyber/

Comme le soulignait Vincent Riondet, Responsable des équipes Projets et Services Cybersécurité de Schneider Electric France, dans un précédent papier, sur la plupart des sites industriels « *on fait donc cohabiter des infrastructures qui sont plus ou moins anciennes, avec des architectures réseau et des systèmes d'exploitation plus ou moins récents, qui n'intègrent pas forcément des normes de sécurité avancées car les évolutions sont coûteuses* ».

L'application de multiples barrières de protection comme la segmentation, le contrôle de flux, la détection ou encore la prévention d'intrusion, peut s'avérer fortement utile pour lutter contre les menaces par les flux réseau. En outre, le contrôle d'accès seulement en autorisant ou non un protocole de communication (par son port) ne suffit plus ; il faut également analyser les commandes qui sont envoyées via les protocoles métier autorisés.

Par conséquent, la sécurisation de l'architecture réseau doit s'articuler autour de la protection et du maintien à jour de ces mesures de protection afin d'éviter les fuites de données ou la perturbation du processus opérationnel. Le but ? Mieux lutter contre les cyberattaques qui peuvent arriver à n'importe quel moment. **C'est pourquoi la mise en œuvre des systèmes de défense proactifs au plus proche des infrastructures critiques s'avère essentielle.**

# Systèmes de défense : sonde industrielle ou IPS ?

Même s'il est indispensable de surveiller l'infrastructure industrielle, il n'existe pas une grille d'évaluation technique unique applicable à toutes les architectures opérationnelles. L'une des questions à se poser : **qui traite les alertes générées et comment ?** En effet, au-delà des aspects techniques, la mise en place d'une sonde industrielle nécessite **une équipe d'exploitation formée** qui soit en mesure de gérer, d'analyser **une grande quantité d'information** pour identifier les événements critiques et escalader des potentiels problèmes de sécurité, le cas échéant.

Même si ces solutions peuvent être complémentaires, le choix éventuel entre une sonde industrielle et une solution IPS doit être basé sur un ensemble de paramètres, selon votre usage. Pour cela, il faut réaliser un examen détaillé de l'ensemble de votre architecture réseau opérationnelle. Selon vos besoins, **mesurez la criticité de la sûreté de chaque élément pour déterminer la protection adéquate**.

Il est également primordial de réfléchir à comment votre nouvelle solution va s'intégrer dans votre politique de cybersécurité globale ainsi que dans vos processus et organisation présents et futurs.

## LE SAVIEZ-VOUS ?

Les systèmes IPS proposent souvent les mêmes fonctionnalités IDS (*Intrusion Detection System*) que les sondes industrielles. N'apportant pas le même niveau de détail dans la capacité d'identification que ces sondes, les systèmes IDS assurent néanmoins la reconnaissance des flux traversant l'équipement.

Il est recommandé d'**effectuer une mise en place graduelle de l'IPS en passant par une phase d'analyse du trafic réseau en IDS**. Cette étape préparatoire permet de cartographier les flux et d'identifier les potentiels faux positifs avant d'activer la prévention active d'intrusion pour bloquer les flux illégitimes.

| **Une sonde industrielle** est un outil **passif** permettant de **détecter** les potentiels flux malveillants au sein du réseau | | **Un système IPS** est un outil de protection **actif** permettant d'**identifier** et de **bloquer** les potentiels flux malveillants au sein du réseau |
|---|---|---|
| • Ne bloque pas les paquets réseau | VS | • Agit en bloquant les paquets suspects |
| • A besoin d'une intervention humaine pour la gestion des incidents | VS | • Est autonome pour gérer les alarmes déclenchées |
| • Voit une copie complète du réseau | VS | • Se situe en coupure du réseau |
| • Fournit une grande quantité d'information | VS | • N'alerte qu'en cas de problème |
| • Est sensible aux actions de flooding | VS | • Arrête ce type d'attaques |
| • Est « transparent » dans le réseau en cas d'attaque | VS | • Peut être repéré plus facilement |

## LE SAVIEZ-VOUS ?

Il existe des solutions IPS qui intègrent un **mode de sûreté (fonction *bypass*) pour garantir, si nécessaire, la continuité de l'activité opérationnelle en cas de dysfonctionnement.**

# Les principes généraux de l'Intrusion Prevention System

## En bref

Le rôle principal des IPS consiste à **surveiller en temps réel les paquets réseau et leur contenu afin d'appliquer des règles prédéfinies selon l'attaque détectée et la cible visée**.

### NE PAS CONFONDRE

Il y a 2 types différents d'IPS :

- **HIPS (Host-Based Intrusion Prevention System)** : IPS surveillant les postes de travail.
- **NIPS (Network Intrusion Prevention System)** : IPS surveillant le réseau.

## Comment ça marche ?

Les systèmes de prévention d'intrusion sont placés en coupure du réseau qu'ils protègent. Ils analysent les paquets réseau pour vérifier dans un premier temps la conformité protocolaire et le contrôle des commandes.

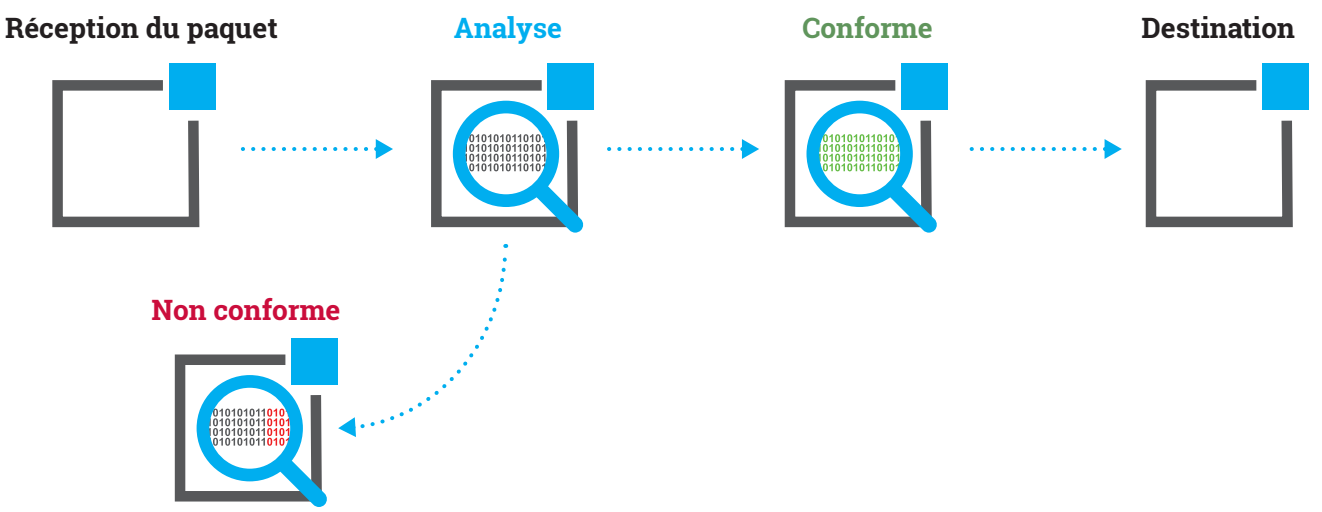
**Certains systèmes IPS sont même en mesure d'identifier les comportements anormaux.**

Les systèmes IPS recherchent ensuite si les paquets réseau ne contiennent pas un ensemble de données qui correspondent à la signature de malwares connus pour bloquer les tentatives d'attaques.

## Qu'apporte l'IPS ?

Cette technologie permet d'assurer la protection réseau d'une infrastructure informatique et / ou opérationnelle.

À ce titre, le support des protocoles métier exploités par l'organisation est un critère de sélection du système IPS à ne pas négliger afin d'assurer une bonne couverture dans la protection des commandes de contrôle.



## **Signature ou recherche protocolaire ciblée :** deux approches pour le contrôle de conformité protocolaire

Les meilleurs moteurs IPS assurent un décodage des protocoles utilisés et vérifient la conformité (longueur du paquet de données, type de protocole, etc.) de chacun des messages par rapport au format attendu, défini dans les standards normalisés de ces protocoles. Ils sont capables d'analyser très en détail les informations, d'où le terme fréquemment utilisé de ***Deep Packet Inspection*** **(DPI)**.

Le DPI (Deep Packet Inspection) évalue l'en-tête d'un paquet transmis et les données associées en éliminant toute non-conformité protocolaire

Prenons l'exemple d'un paquet réseau qui véhicule une commande :

| Entête | | Commande | Paramètres | | |
|---|---|---|---|---|---|
| 1100 | 0011 | 1101 | 1110 | 1110 | 1000 |

Dans le cas de la conformité protocolaire, un système IPS va rechercher des suites d'octets spécifiques pour deux raisons principales :

1. **Reconnaissance protocolaire** : dans un premier temps, reconnaître le protocole qui transite en cherchant des marqueurs caractéristiques
2. **Conformité protocolaire** : puis s'assurer que des suites d'octets, correspondant au protocole identifié, se trouvent bien dans le paquet réseau.

### LE SAVIEZ-VOUS ?

L'implémentation spécifique des protocoles dans le monde industriel utilise en majeure partie des valeurs de commande qui sont personnalisées (*custom command*). **L'analyse protocolaire par signature ne reconnaît pas ces valeurs générant ainsi des erreurs de détection.**

Dans ce cas de figure, une **analyse dite par signature** recherche la suite ***111101*** à n'importe quel endroit du paquet.

| Entête | | Commande | Paramètres | | |
|---|---|---|---|---|---|
| 1100 | 0010 | 1101 | 1110 | 1110 | 1000 |

Ici, les octets identifiés par cette approche sont présents mais pas à la bonne place dans le paquet. La technique par signature laisse quand même passer le paquet mal formé (conduisant ainsi à un faux négatif).

**L'approche ciblée va rechercher l'information souhaitée à l'emplacement correct, précisément où elle est censée se trouver,** afin d'éviter que des paquets mal formés (et potentiellement malveillants) puissent transiter.

Avec l'approche ciblée, le paquet mal formé est donc bloqué.

| Entête | | Commande | Paramètres | | |
|---|---|---|---|---|---|
| 1100 | 0010 | 1101 | 1110 | 1110 | 1000 |

Ainsi, l'**analyse protocolaire ciblée** apporte deux bénéfices majeurs :

1. **Conformité protocolaire exacte**
2. **Limitation des erreurs de détection**

# L'analyse contextuelle au cœur de la sécurité des échanges

Cette approche permet de bloquer les cyberattaques en contextualisant les messages échangés entre deux éléments du réseau. Pour cela, l'**analyse contextuelle** vérifie que la séquence des messages échangés suit la logique définie dans la norme du protocole et ne présente pas de comportement anormal.

L'analyse contextuelle examine et vérifie le message d'un échange entre deux dispositifs tout en prenant en compte les messages précédents. **Cette technologie avancée protège et garantit l'intégrité de vos actifs et environnements opérationnels.**

Prenons l'exemple d'un automate « A » qui peut être piloté par plusieurs contrôleurs. Un contrôleur « A » va demander la prise de contrôle en envoyant une requête adéquate. L'automate « A » va acquitter cette requête en envoyant l'acceptation de la commande sous réserve que celui-ci ne soit pas déjà piloté par un autre contrôleur. Dans l'exemple proposé, imaginons qu'un attaquant prenne le contrôle de l'automate « A ». Le système IPS voit un paquet envoyé spontanément par l'automate « A » qui accepte une demande de prise de contrôle qui n'a pas été identifiée par le système. Avec les éléments du contexte, l'IPS peut identifier ce comportement comme anormal et il peut le bloquer.

## BÉNÉFICES

Ce type de solution IPS, qualifiée de ***Stateful DPI***, permet de **renforcer le niveau de sécurité de l'infrastructure opérationnelle pour ainsi réduire la compromission des actifs du réseau.**

En effectuant l'**analyse contextuelle** des séquences de paquets transitant dans le réseau opérationnel, ce type d'IPS permet de considérer des informations concernant les échanges entre deux dispositifs. **Il prend en compte plusieurs paramètres du message en cours par rapport à ceux qui ont déjà été échangés**. Ces paramètres peuvent être : la direction de communication entre les deux dispositifs, le type de commande à exécuter ou encore les valeurs de commande à appliquer.

## IEC 104

La norme IEC 104 est un protocole utilisé pour le télécontrôle des sous-stations électriques. Dans ce protocole, les différentes sous-stations ne peuvent envoyer leurs mesures que si elles sont autorisées à le faire. Et dans les communications, certains attributs des protocoles peuvent être valides ou non selon le contexte (s'il s'agit d'une sous-station envoyant des mesures ou d'une station centrale envoyant des commandes).

## La recherche des menaces réseau dans les échanges

Le malware Triton illustre bien la faiblesse des réseaux OT et démontre l'importance d'un système IPS pour identifier les menaces par le réseau, même lorsque l'attaque respecte la conformité protocolaire et suit la logique définie dans la norme du protocole. Pour ceci, l'IPS recherche dans les données du paquet réseau si une suite d'octets correspond à une signature d'attaque connue.

Il faut noter également que certains malwares peuvent évoluer. Les variantes de ceux-ci nécessitent alors de nouvelles signatures spécifiques : si celles-ci ne sont pas déployées dans l'IPS, il ne sera pas en mesure de les détecter. **Pour cette raison, il est recommandé d'utiliser un IPS capable d'exploiter des signatures proactives qui engloberont les diverses variantes d'une attaque permettant leur détection.**

### BÉNÉFICES

La protection proactive présente un autre bénéfice non négligeable : le nombre de signatures requises en base étant plus réduit, **la recherche de motifs d'attaques connues dans le réseau est plus rapide et la latence réseau introduite par l'analyse amoindrie.**

Mieux encore, si le moteur de l'IPS est capable de profiter de l'analyse fine réalisée lors du contrôle de conformité protocolaire pour rechercher uniquement les signatures d'attaques pertinentes dans chaque partie des messages, **les performances sont encore accrues et le taux de faux positifs est drastiquement réduit.**

## Triton : une cyberattaque contre les ICS

*Le malware Triton a été conçu pour cibler les systèmes ICS d'une usine de pétrochimie saoudienne dans le but de provoquer une explosion. Heureusement, les attaquants ont commis une erreur déclenchant ainsi un arrêt d'urgence des systèmes critiques et révélant l'intrusion du réseau.*

## Stuxnet : illustration des variantes du ver

Stuxnet a été conçu pour attaquer les centrifugeuses iraniennes d'enrichissement d'uranium. La complexité de ce malware se base sur de fines connaissances en procédés industriels et en failles de l'OS Windows. Les cyberattaquants ont utilisé des exploits de type Zero-day sophistiqués et peu courants.

Des variantes de Stuxnet ont également été utilisées ensuite contre d'autres infrastructures industrielles.

Certaines organisations industrielles et des experts dans la matière ont publié des guides de bonnes pratiques pour la bonne gestion des systèmes de contrôle. Entre autres, ils évoquent la nécessité de segmenter le réseau, contrôler les accès, acquérir des systèmes durcis, implémenter des antivirus et des moteurs de prévention d'intrusion de type IPS.

Face à ce type de menaces, un système IPS proactif prenant en compte les potentielles variantes d'un même malware s'avère une aide essentielle voire vitale pour la survie du système industriel.

# Les nécessaires signatures personnalisées

Un système IPS doit connaître et gérer les messages échangés via les protocoles industriels pour bien protéger le système opérationnel. Chaque valeur envoyée dans les messages de commande se doit d'être correctement analysée et vérifiée car chaque communication réseau agît directement sur un processus opérationnel en particulier.

Un système IPS doit être capable d'offrir la personnalisation de signatures afin d'implémenter du contrôle des messages de commande en conformité avec les processus et les contraintes métier opérationnelles

Les solutions d'IPS peuvent assurer cette vérification par le biais de signatures personnalisées. L'objectif : contrôler les messages de commande pour qu'ils soient en conformité avec les processus et les contraintes métier opérationnels. Ce point est le plus critique dans un environnement opérationnel afin de bien s'assurer que les valeurs ne dépassent pas certaines limites qui pourraient mettre à mal l'ensemble du processus.

Prenons l'exemple simplifié d'un barrage hydraulique, où l'on doit s'assurer que les commandes de contrôle tiennent compte du débit supporté par une vanne (dans ce cas : capacité totale 50 à 5 000 $m^3/s$). Même si les nouveaux systèmes ICS/SCADA y sont moins sensibles, il est important pour les anciennes infrastructures que les valeurs envoyées au contrôleur respectent ces limites afin d'éviter des débits supérieurs entraînant de lourdes conséquences comme des inondations.

**Il est de plus primordial de pouvoir vérifier ces valeurs en temps réel.**

**700+**
**protocoles propriétaires**

UMAS, S7, TSAA, SAAT, HNZ, ...

**20+**
**protocoles standardisés**

Modbus, UMAS, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA...

## BÉNÉFICES

Les signatures personnalisées permettent de :

- **s'adapter** au contexte métier ;
- **implémenter** de l'analyse protocolaire sur des protocoles propriétaires ;
- **contrôler** les valeurs dites sensibles en lien avec la sûreté du système opérationnel ;
- **garantir** le bon fonctionnement du processus opérationnel.

# Les critères pour bien choisir son IPS

Le choix d'un système IPS peut sembler une tâche délicate et compliquée compte tenu des enjeux importants.

Le schéma ci-dessous vous permettra d'obtenir rapidement un aperçu des fonctionnalités les plus importantes.




## LE SAVIEZ-VOUS ?

Les systèmes de protection constitués de plusieurs composants complexifient leur intégration. Outre la multiplicité des outils de gestion, des licences et des formations, ces solutions augmentent généralement la latence sur le réseau.

**Optimisez la productivité de vos équipes en choisissant une solution IPS tout-en-un facile à déployer et simple d'utilisation. De même, une interface graphique claire permettra d'améliorer l'intégration et la gestion de l'IPS en offrant une meilleure visibilité sur les systèmes à protéger.**

# Le moteur *Stateful DPI* Stormshield

## Disposez d'un système de prévention d'intrusion et d'une segmentation de vos réseaux opérationnels de grande qualité assurant la disponibilité et l'intégrité de vos systèmes

### De puissantes analyses des flux

**CONTROLE DE CONFORMITÉ PROTOCOLAIRE**
alliant contrôle des paquets et conformité des protocoles applicatifs

**DPI sur 10+ Protocoles supportés**
Modbus, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFI-NET, IEC 61850 (MMS/GOOSE/SV), OPC UA, ...



### Un IPS industriel
se basant sur des multiples analyses pour apporter une réponse proactive, prévenant même les attaques Zero-day

### Analyse contextuelle
Etude du comportement selon un contexte métier



l'**optimisation de l'intégration de l'IPS** au sein de l'OS embarqué



la **recherche des signatures contextuelles** dans une base de données plus fine et ciblée



l'**analyse protocolaire ciblée et contextuelle** diminue le temps de latence et limite les faux-positifs

### Des performances supérieures grâce à...

SIGNATURE PERSONNALISÉE

**POURQUOI VOUS EN AUREZ BESOIN ?**

1. Contrôler la conformité aux processus opérationnels
2. Prévenir des dégâts sur l'outil industriel et l'environnement
3. S'adapter à une analyse protocolaire propre



**Prise en main intuitive**



**Solution tout-en-un**



**UI claire et simple d'utilisation**

**EXPERTISE DANS LA PROTECTION DES RÉSEAUX OT : CO-DESIGN AVEC LES ÉQUIPEMENTIERS, INTÉGRATEURS INDUSTRIELS ET CLIENTS**

www.stormshield.com

STORMSHIELD

Le choix européen de la cybersécurité

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin de s'appuyer sur des partenaires de confiance pour accompagner leur transformation numérique et assurer la cybersécurité de leurs infrastructures, de leurs utilisateurs et de leurs données. Les technologies Stormshield, certifiées au plus haut niveau européen (EU Restreint, OTAN Restreint, Critères Communs EAL3+/EAL4+, qualifications et visas ANSSI), répondent aux enjeux de l'IT et de l'OT afin de protéger vos activités. **Nos solutions de sécurité vous redonnent la liberté d'entreprendre en toute sérénité.** www.stormshield.com

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privée sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.