



**VOTRE PARTENAIRE  
TECHNOLOGIQUE  
POUR DES INFRASTRUCTURES IT  
SÉCURISÉES ET PERFORMANTES**



**EXPERTISE**

Des solutions adaptées  
à chaque environnement



**CONFIANCE**

Un partenaire fiable  
à vos côtés



**PERFORMANCE**

Des infrastructures  
sécurisées et évolutives



**SUPPORT**

Un accompagnement  
technique de qualité



**HAFS**

*Distributeur à valeur ajoutée*

Des solutions IT innovantes pour  
un monde connecté et sécurisé



**WIRELESS  
RADIO**

Connectivité sans fil  
haute performance



**RÉSEAUX &  
SÉCURITÉ IT**

Des réseaux fiables  
et sécurisés



**VIRTUALISATION  
CLOUD**

Des solutions Cloud  
flexibles et évolutives



**CYBERSECURITY**

Protéger vos données  
et vos systèmes



**VIDÉO  
PROTECTION**

Solutions de vidéosurveillance  
intelligentes



**HCI STOCKAGE  
SAUVEGARDE**

Stockage, sauvegarde  
et haute disponibilité

SOLUTIONS IT

CYBERSÉCURITÉ

CLOUD

INFRASTRUCTURE RÉSEAU

STOCKAGE

PROTECTION

# Hillstone Network Detection and Response (NDR) Solution



**Integrative Cybersecurity**  
Visionary. **AI-powered.** **Accessible.**

# Agenda

La situation actuelle de la sécurité sur l'intranet

---

Proposition de valeur du NDR de Hillstone

---

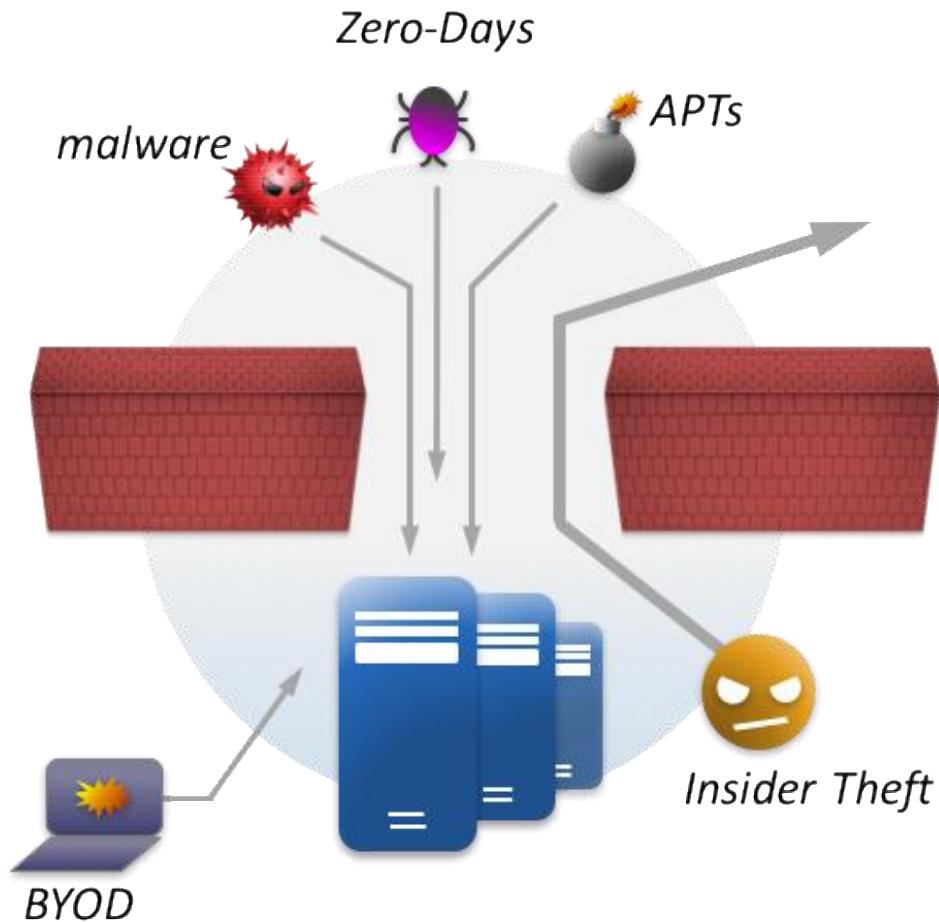
Liste des produits NDR de Hillstone

---

Études de cas et scénarios de déploiement

# La situation actuelle de la sécurité sur l'intranet

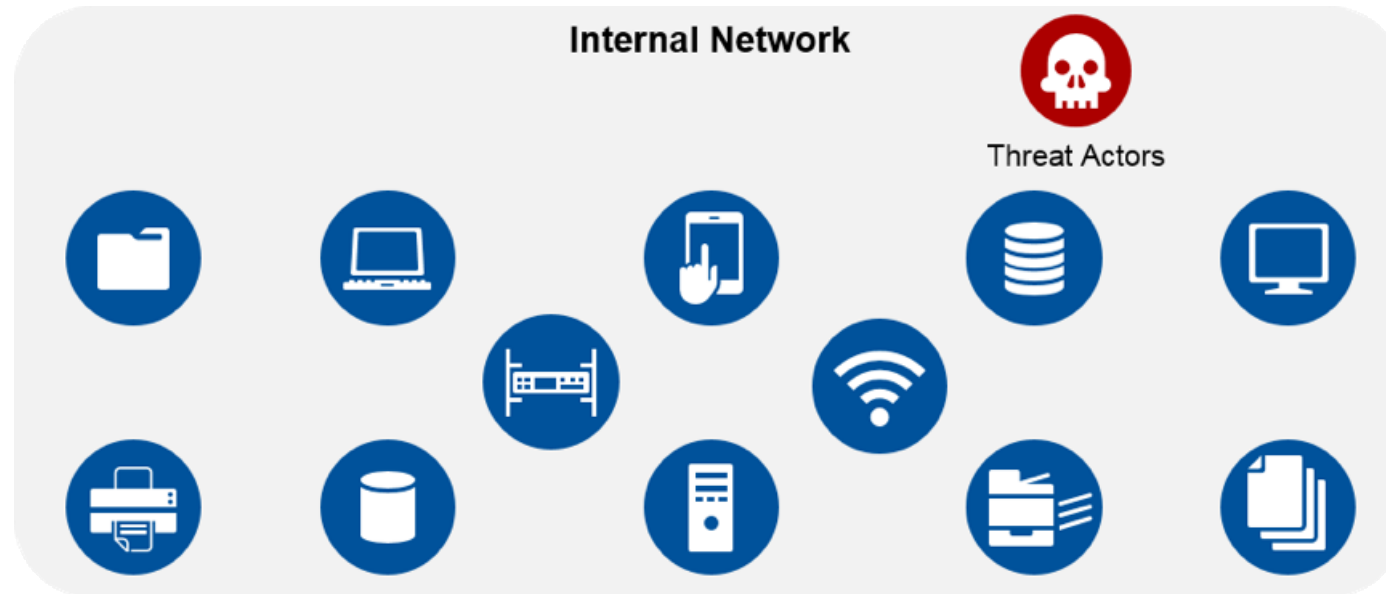
# Les violations de réseau interne se produisent à un taux alarmant



- Seules les défenses de signature traditionnelles peuvent mettre fin aux anciennes attaques **'amateur'**.
- De nouvelles attaques **sophistiquées** pour pirater chaque réseau.
- “Dans 60% des cas, les attaquants sont capables de compromettre une organisation en quelques minutes.”

– Verizon 2015 DBIR

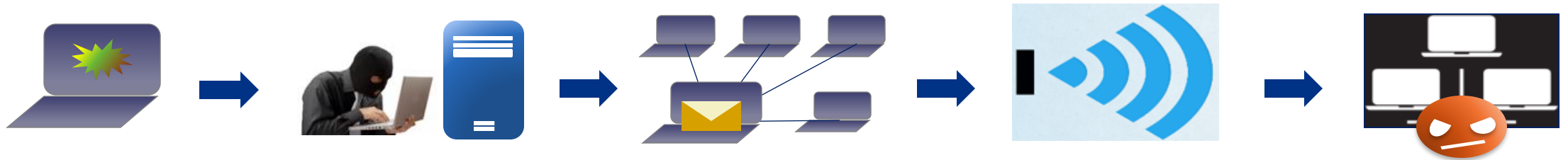
# La menace se propage facilement dans les réseaux internes plats...



*“... quelle que soit leur motivation, si les adversaires prennent pied sur votre réseau interne, ils peuvent pivoter et accéder à tout ce qui se trouve sur votre réseau interne. C’est la principale raison pour laquelle les violations modernes sont si dévastatrices en termes de quantité de données perdues et de temps passé sur le réseau d’une organisation avant d’être découvertes. En conséquence, la détection/prévention des mouvements latéraux est devenue un domaine d’intérêt considérable ”*

*-Source: Gartner (September 2016)*

# Interrompre les serveurs critiques et la continuité de l'activité



- Le phishing se produit lorsque le personnel surfe sur Internet

- C&C
- Le hacker contrôle complètement l'hôte.

- Un faux e-mail interne et une pièce jointe propagent des dommages en interne
- De plus en plus d'hôtes sont vulnérables

- L'hôte perd le contrôle
- Démarre une attaque DDoS de l'intérieur

- Resultats : Provoque une défaillance du serveur et du pare-feu
- En fin de compte, le réseau et l'entreprise sont hors service

# Violation de données sensibles via un hôte compromis



- Le phishing se produit lorsque le personnel surfe sur Internet

- Injecter des logiciels malveillants avec des signatures logicielles antivirus fausses ou expirées

- Le logiciel antivirus ne parvient pas à détecter les logiciels malveillants
- Le logiciel malveillant est activé

- C&C
- Téléchargements Fichier PE
- Le hacker contrôle complètement l'hôte.

- Le serveur de base de données est piraté à travers l'hôte compromis

# Proposition de valeur du NDR de Hillstone

# Hillstone NDR Produit BDS



Hillstone utilise son produit **NDR**, le **BDS**, pour repérer et réagir aux menaces réseau avancées.

Détection de Menaces	Une Visibilité Approfondie	Analyse de la criminalistique numérique	Réponse efficace
ABD/ATD/WEB	IOCs	Chaîne d'attaque	Actions de l'administrateur
NTA/Deception	Tableaux de bord	MITRE ATT&CK	Liste noire / Liste blanche
Correlation des menaces	Risque/Menace/Trafic	Expertise Forensique Avancée	Bloquer avec un pare-feu
...	...	...	...

# Analyse comportementale basée sur le Machine Learning (ML) pour détecter les anomalies

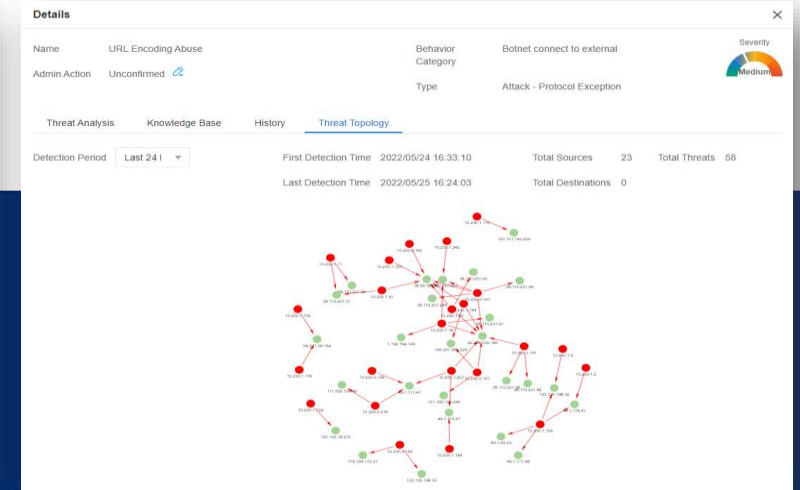
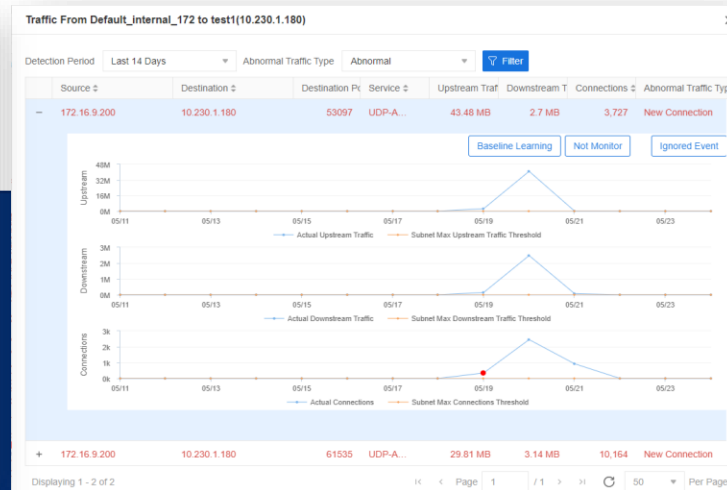
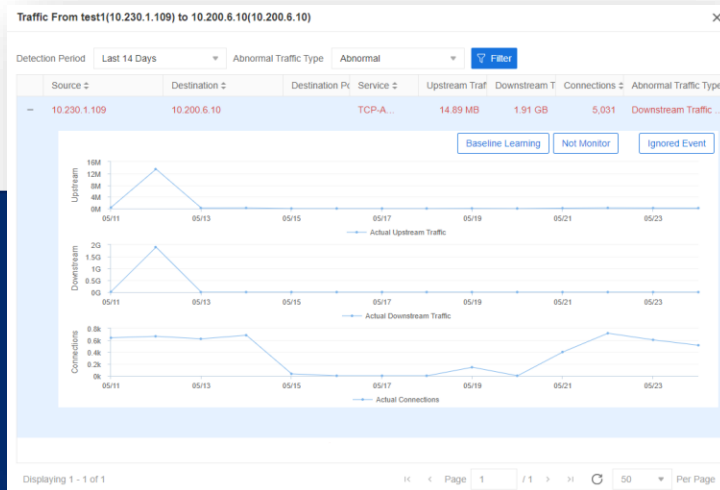


Apprendre et établir une ligne de base et un seuil de trafic normal

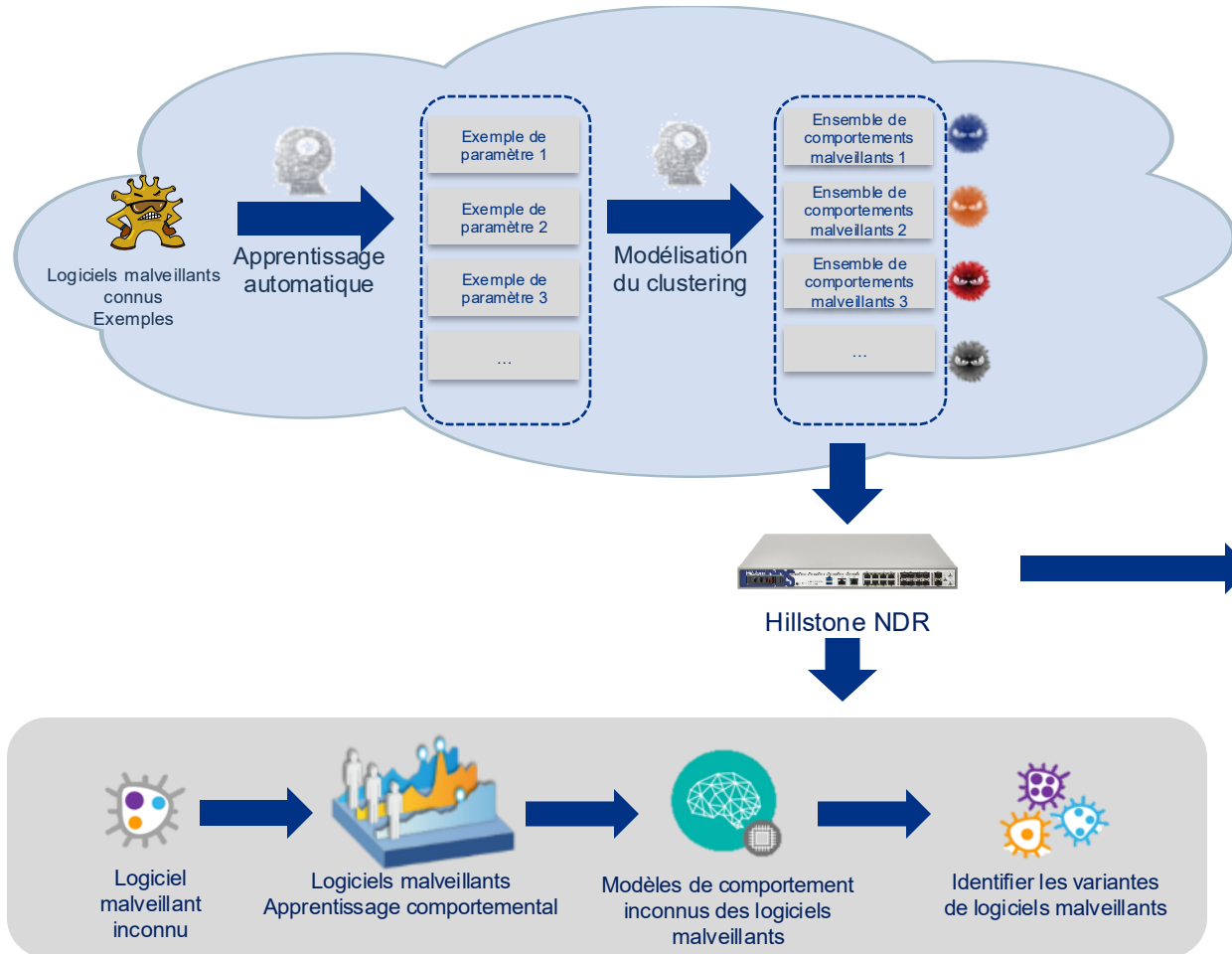
Détecter les tendances du trafic et identifier les comportements de trafic anormaux

Surveiller le trafic normal et anormal pour chaque serveur/hôte

Analyse du comportement basée sur le ML pour les URL, l'UEBA, les corrélations de menaces, etc.



# Détection : Détection avancée des menaces (ATD)



**Logiciel malveillant inconnu détecté par ATD**

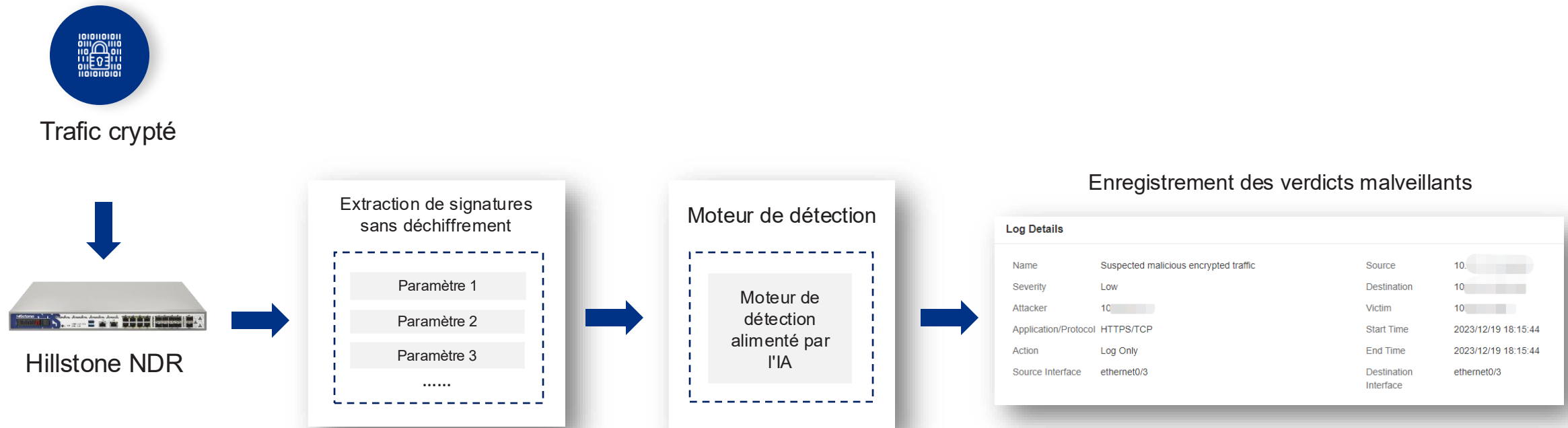
**Gravité de la menace** (Severity: Critical)

Details		Behavior Category	Severity
Name	Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain	Botnet connect to external	Critical
Admin Action	Unconfirmed	Type	Malware - Trojan

**Informations sur les logiciels malveillants connus**

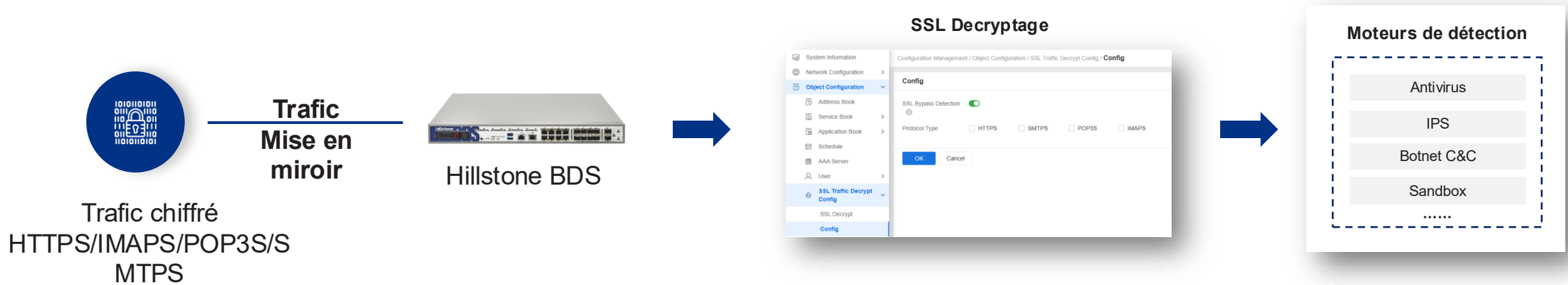
Application/Protocol DNS/UDP	
Source	Destination
Endpoint Name/IP: 192.168.1.37	Endpoint Name/IP: 8.8.8.8
Port: 53608	Port: 53
Interface: ethernet0/1	Interface: ethernet0/1
Zone: tap-bds	Zone: tap-bds
Action: Log Only	

# Detection: Abnormal Encrypted Traffic Detection



Exploitez la technologie basée sur l'IA pour détecter le trafic chiffré anormal sans déchiffrement

# Détection : détection des menaces pour le trafic chiffré avec déchiffrement SSL en mode TAP



Détection complète des menaces pour le trafic chiffré avec déchiffrement SSL en mode TAP

# Détection : Détection des attaques WEB

Règles WAF  
Utilisation du jeu de règles de sécurité OWASP  
ModSecurity Core (CRS) 3.3



Détecter et analyser les menaces pour les serveurs et applications WEB

## Détection des attaques WEB

Attaque DDoS

Attaque par injection

Cross-site Attack

HTTP anormal

Attaque de vulnérabilité spéciale

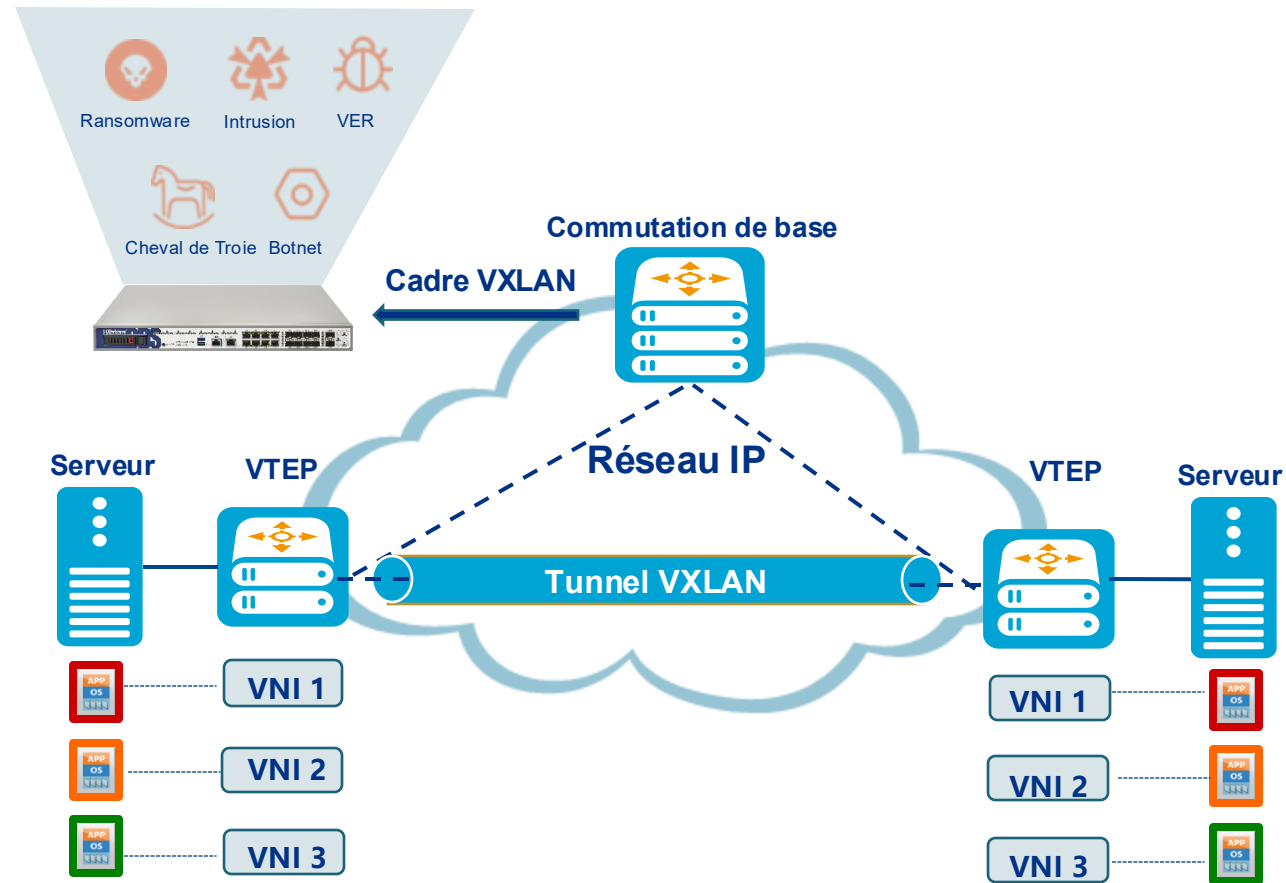
Fuite d'informations

Logiciels malveillants

Accès illégal aux ressources

Analyse des réseaux malveillants

# Détection : détection de trame VxLAN



Détecter les trames VXLAN dont le port UDP 4789 est le port de destination  
Ne pas détecter le trafic non VXLAN dont le port de destination est UDP 4789

# Détection : technologie de tromperie

Accès HTTP non autorisé détecté par le moteur de détection par leurre

**Details**

Name: Un authorized HTTP access | Behavior Category: Botnet connect to external | Severity: Critical

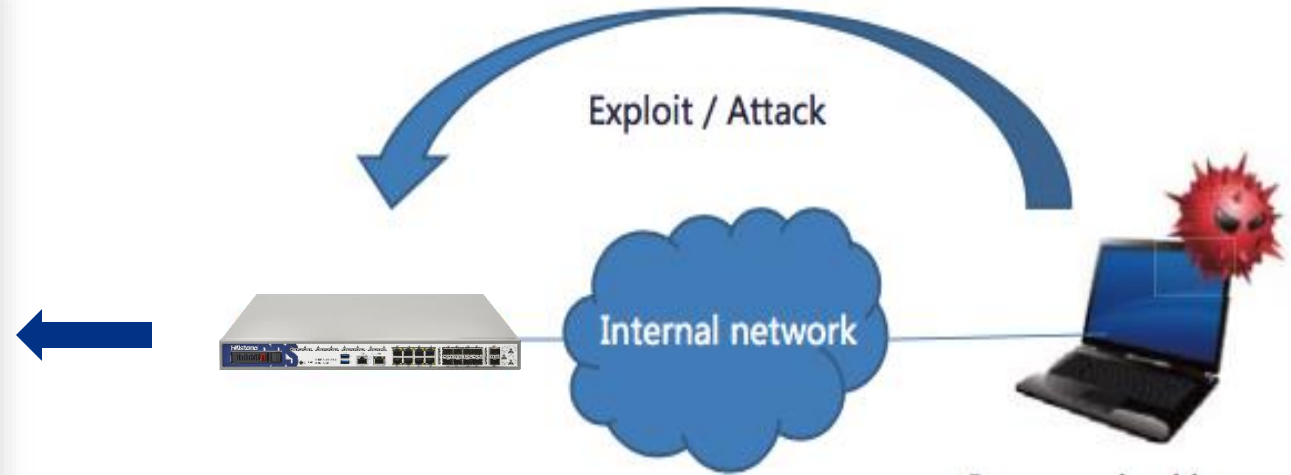
Admin Action: Unconfirmed | Type: Malware - Trojan

Application/Protocol: DNS/UDP

Source	Destination
Endpoint Name/IP: 192.168.1.37	Endpoint Name/IP: 8.8.8.8
Port: 53608	Port: 53
Interface: ethernet0/1	Interface: ethernet0/1
Zone: Deception	Zone: Deception

Action: Log Only  
Start Time: 2023/04/21 07:57:08  
End Time: 2023/04/21 07:57:28  
Attacks: 1  
Duration: 10seconds  
Profile: predef\_1

Service HTTP/TCP configuré dans la zone de déception



Simulez des services dans la zone de déception ,lorsqu'un hacker accède à ces services, l'attaque est détectée.

# Détection : moteur de détection antivirus double



## Détection basée sur le hachage

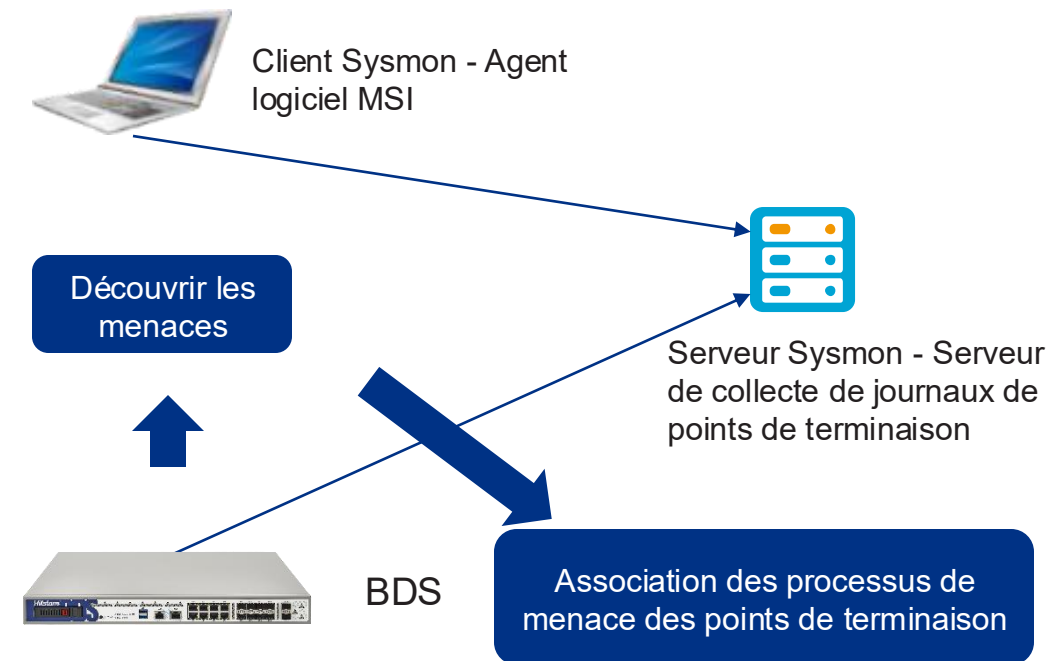
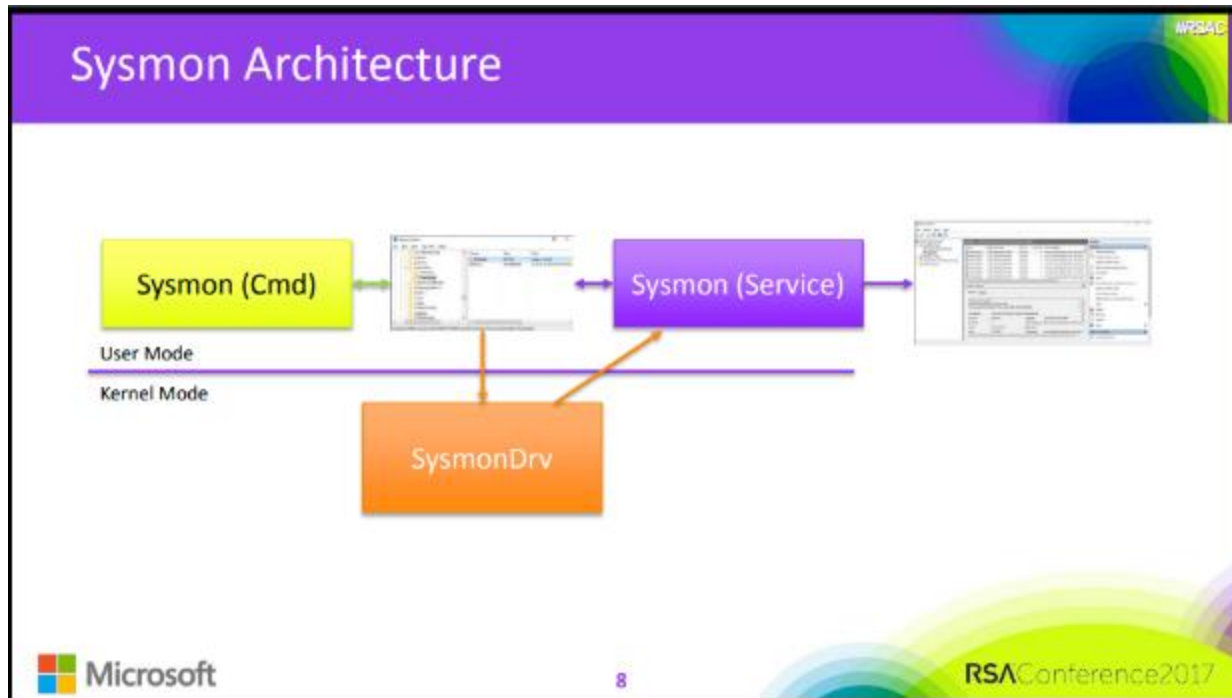
- Basé sur le hachage de fichier MD5
- Prend en charge tous les fichiers
- Cas d'utilisation : détection de virus connus



## Détection alimentée par l'IA

- Analyse des caractéristiques des fichiers
- Prise en charge des fichiers PE/PDF/Office/ELF
- Cas d'utilisation : détection de virus inconnus/variants

# Détection : intégration du service de point de terminaison Sysmon



# Détection : efficacité de détection et faible taux de faux positifs

**Details** [X]

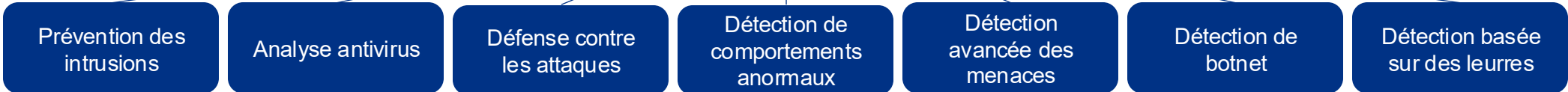
Name Ransomware Activity: TeslaCrypt/AlphaCrypt Variant ⓘ Behavior Category Botnet connect to external .onion Proxy Domain Severity

Admin Action Unconfirmed ⓘ Type Malware - Trojan

Threat Analysis Knowledge Base MITRE ATT&CK® Tactic Details ATT&CK® Technique Details History Threat Topology

	Source ⇅	Source Zone ⇅	Source Interface ⇅	Destination ⇅	Destination Zone ⇅	Detected at ⇅
1	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/21 07:57:28

## Analyse de corrélation des menaces

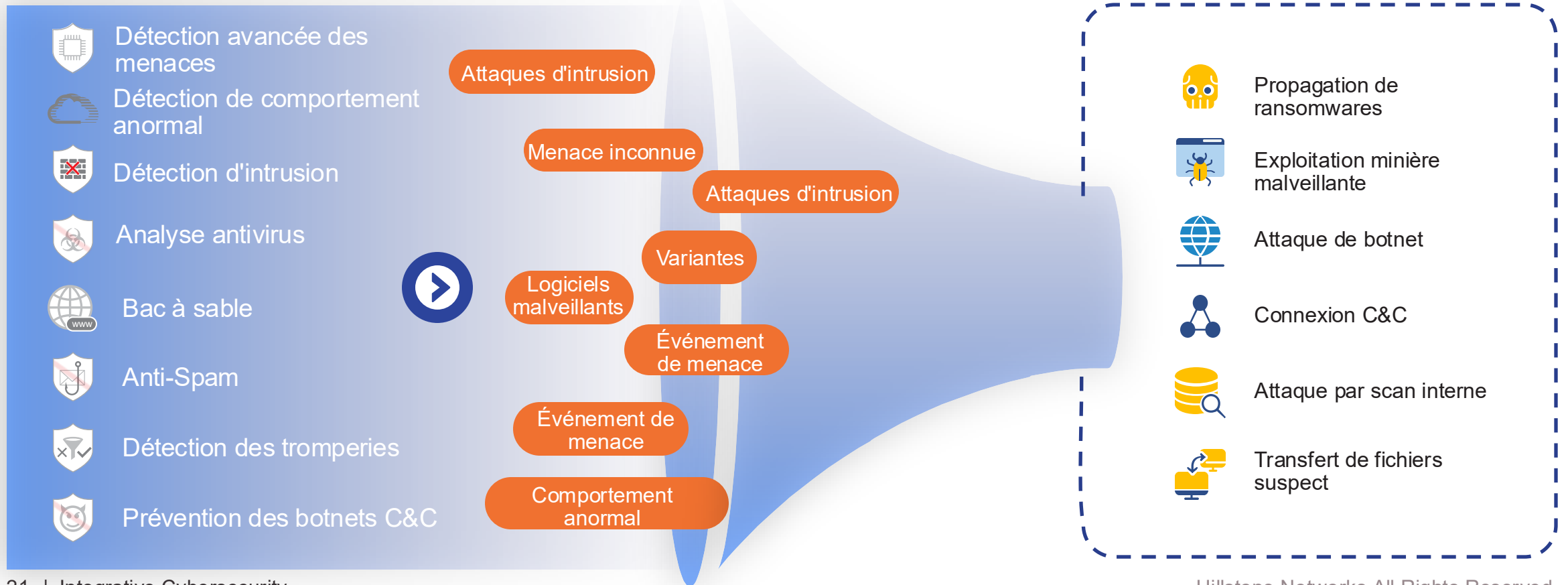


# Visibilité : menaces basées sur des Indicateurs de Compromission (IoC)

Les moteurs de détection de menaces identifient les événements liés aux menaces

Analyse de corrélation des menaces

IOCs (Indice de compromission)



# Visibilité : vue globale des menaces intranet

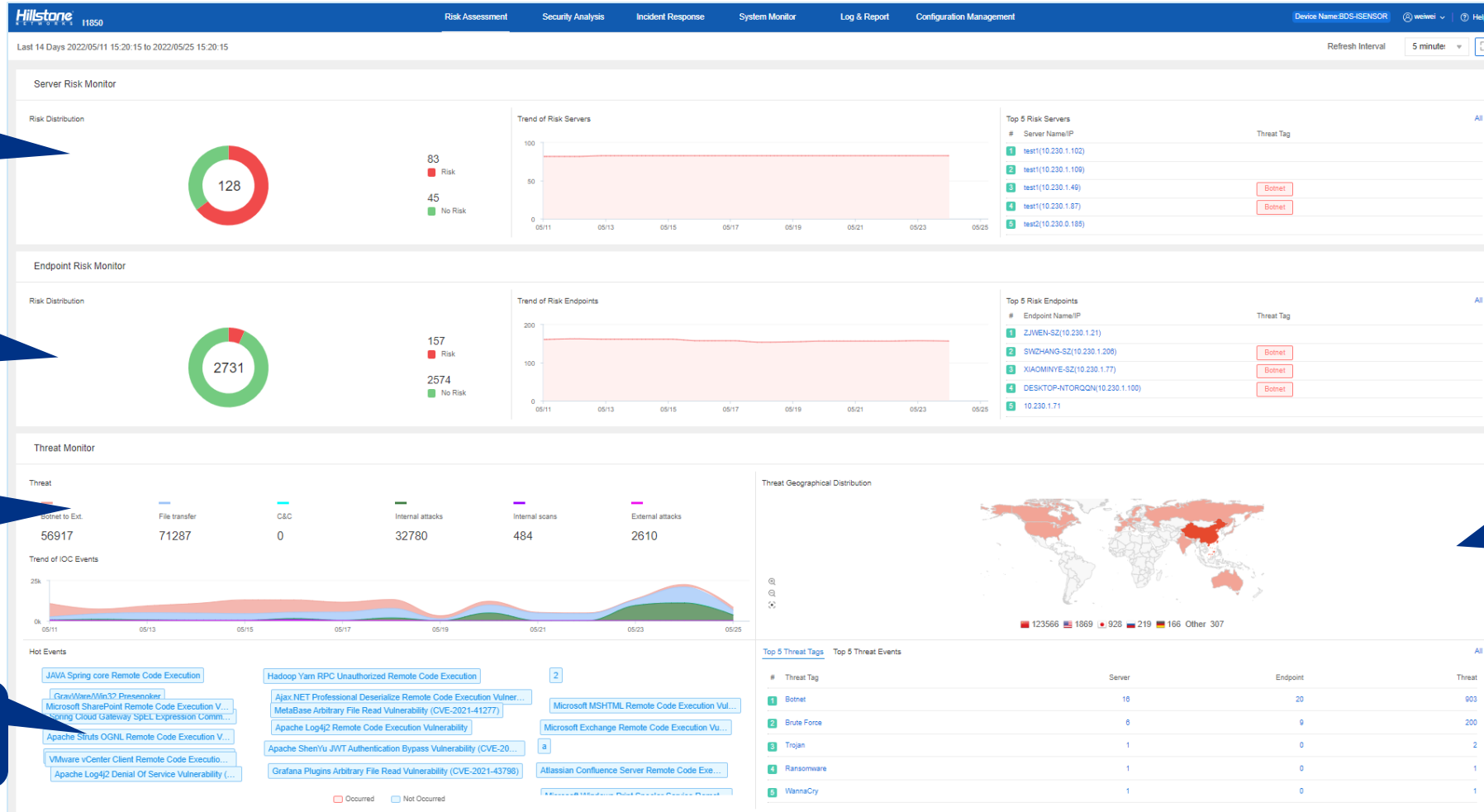
Aperçu des serveurs critiques et du niveau de risque

Aperçu de l'hôte interne et du niveau de risque

Type de menace, statistique, distribution historique, etc.

Événements critiques nécessitant une attention

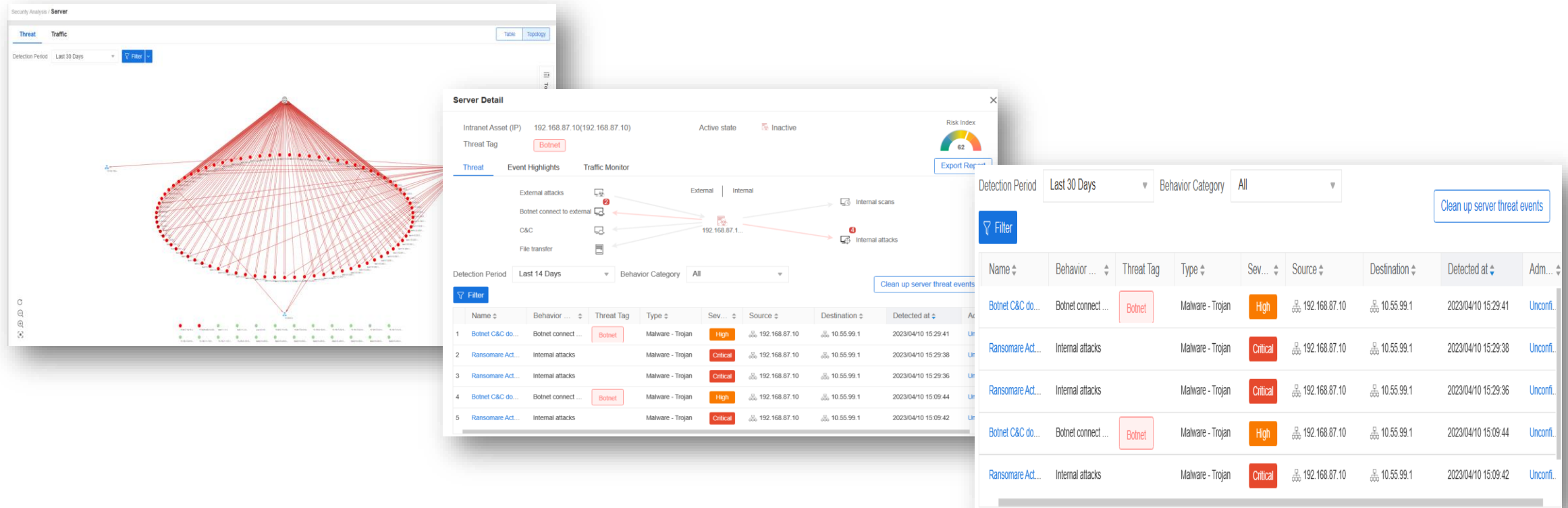
Répartition géographique des menaces et principale menace



# Visibilité : tableau de bord de surveillance des risques intranet

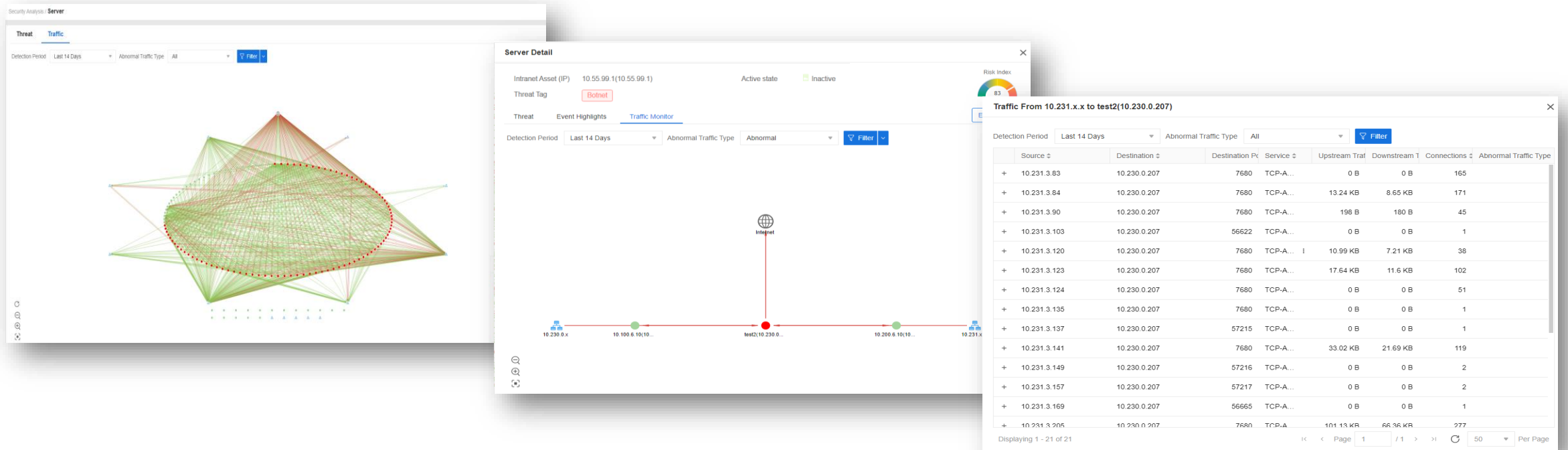


# Visibilité : surveillance des menaces sur les serveurs



- Topologie des menaces pour les serveurs intranet : direction, gravité et relations des attaques
- Analyse des menaces pour chaque serveur : 6 types de chaînes d'attaque
- Liste des événements de menace

# Visibilité : surveillance du trafic du serveur



- Topologie du trafic du serveur pour tous les serveurs intranet : toutes les relations de trafic entre tous les serveurs intranet
- Diagramme de trafic du serveur pour un serveur individuel : trafic entrant/sortant d'un serveur individuel
- Liste des activités de trafic : toutes les activités de trafic entre les serveurs

# Visibilité : topologie des menaces

The image displays three overlapping screenshots from a security dashboard, illustrating threat visibility and topology.

**Top Left Screenshot: Threat Details**

Name: Ransomare Activity: TeslaCrypt/AlphaCrypt Variant  
Behavior Category: Botnet connect to external  
Admin Action: Unconfirmed  
Type: Malware - Trojan  
Severity: Critical

Application/Protocol: DNS/UDP

Source		Destination	
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

Action: Log Only  
Start Time: 2023/04/21 07:57:08  
End Time: 2023/04/21 07:57:28  
Attacks: 1  
Duration: 10seconds  
Profile: predef\_1

**Top Middle Screenshot: Threat Topology**

Name: illegal downloading  
Behavior Category: File transfer  
Admin Action: Unconfirmed  
Type: Attack - Suspicious File Operation  
Severity: High

Detection Period: Last 14 | First Detection Time: 2022/05/17 15:21:39 | Total Sources: 214 | Total Threats: 44  
Last Detection Time: 2022/05/25 18:47:03 | Total Destinations: 5

The topology diagram shows a complex network of nodes (IPs) connected by lines, representing interactions between various active elements involved in the threat event.

**Bottom Right Screenshot: Endpoint Detail**

Endpoint Name/IP: 192.168.1.37  
Active state: Active  
Risk Index: 24  
Export Report

Event Highlights:

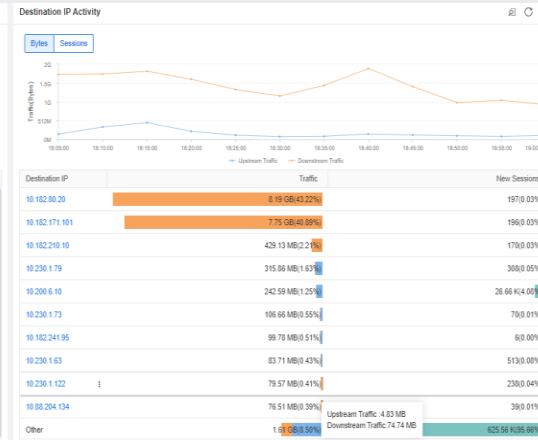
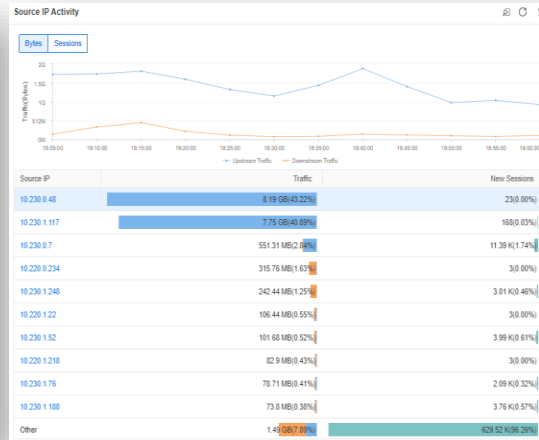
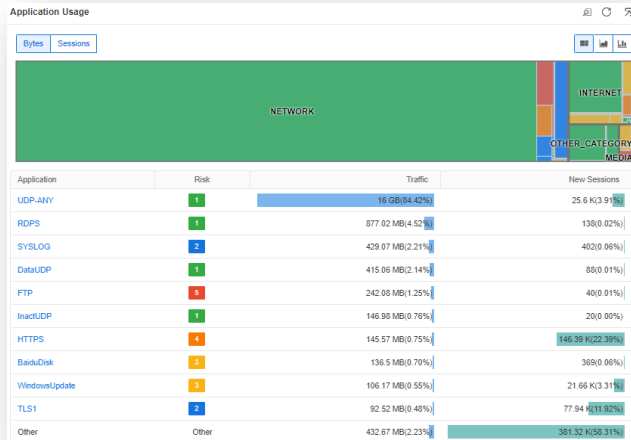
- External attacks
- Botnet connect to external
- C&C
- File transfer
- Internal scans
- Internal attacks

Detection Period: Last 14 Days | Behavior Category: Botnet connect to exten

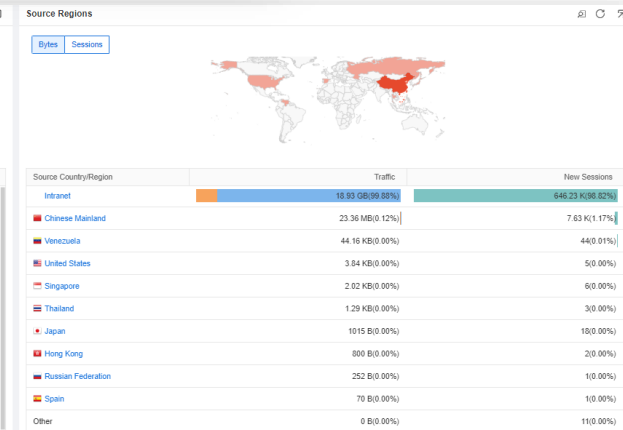
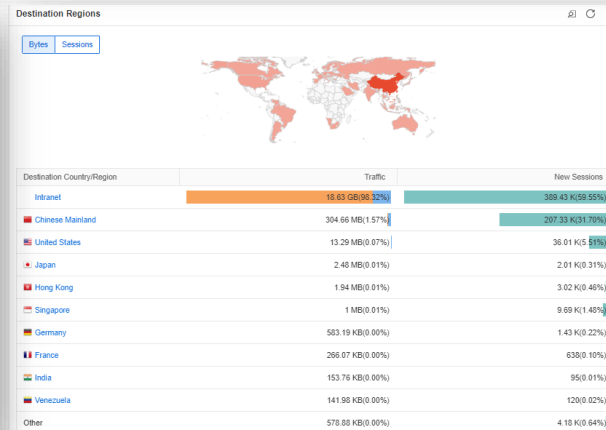
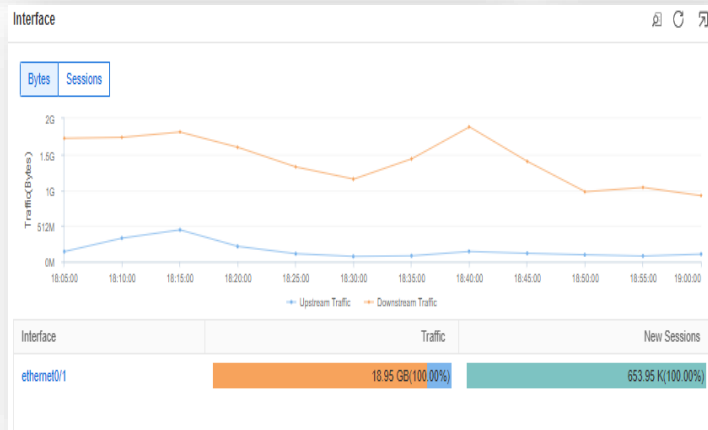
Name	Behavior	Threat Tag	Type	Sev	Source	Destination	Detected at	Adm
1 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/21 07:57:28	Unconfi...
2 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:15:36	Unconfi...
3 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:15:26	Unconfi...
4 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:14:22	Unconfi...
5 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/15 13:37:18	Unconfi...

- Détails d'une menace
- Topologie des menaces qui montre les interactions entre les actifs impliqués dans cet événement de menace
- Vue des activités détaillées d'une IP spécifique dans cette topologie de menace

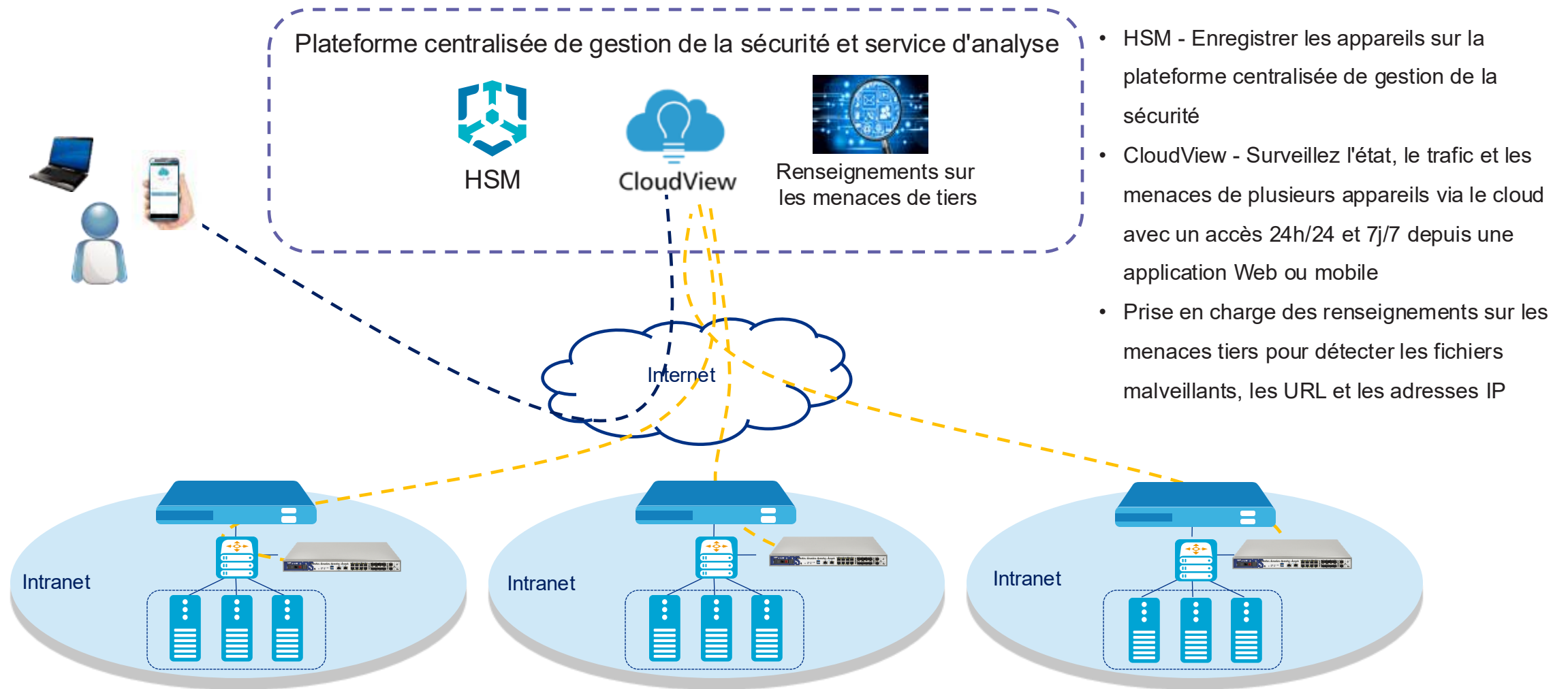
# Visibilité : Analyse des applications intranet



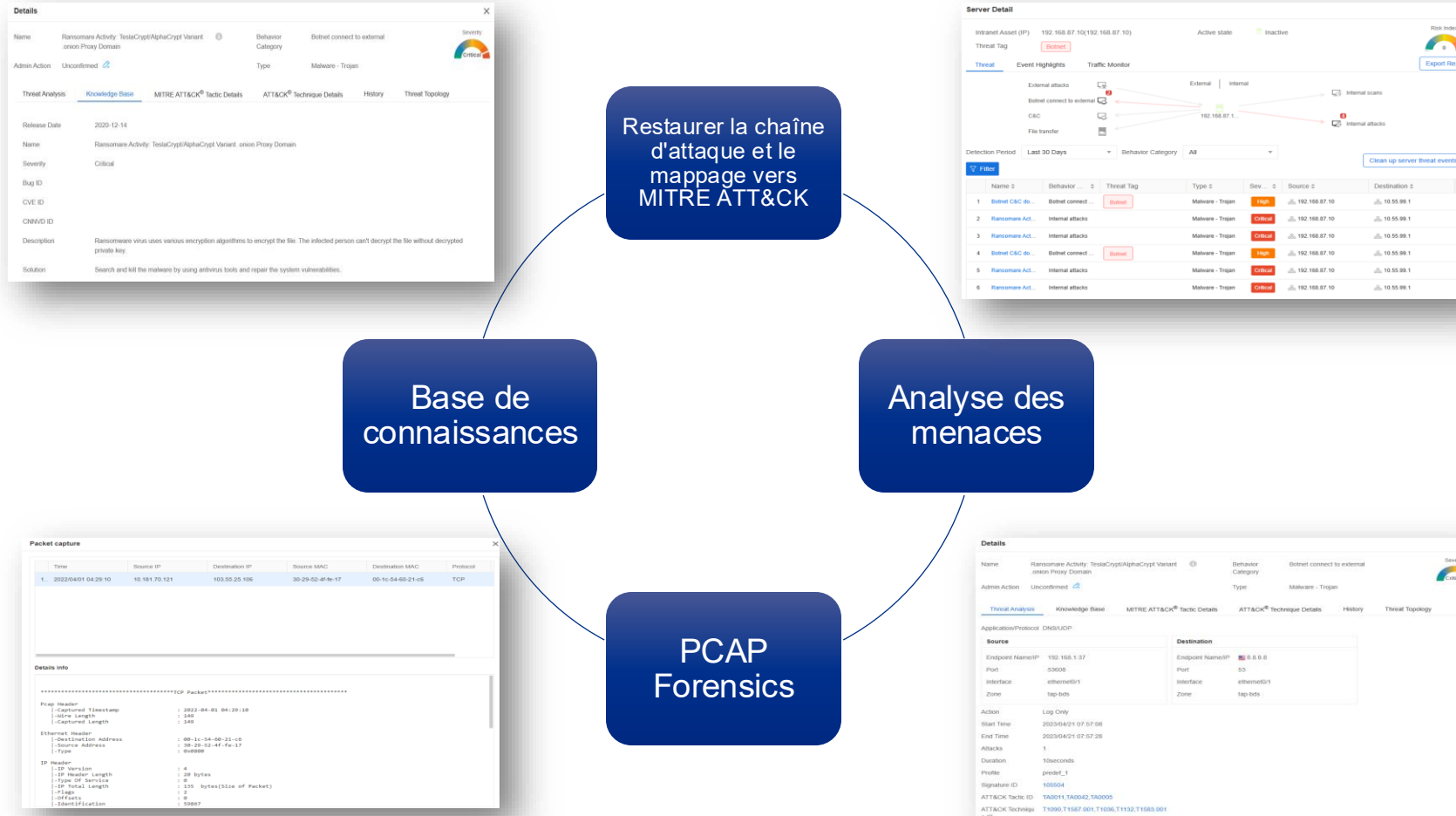
- Utilisation/Classement des applications
- Classement du trafic IP source/destination
- Classement du trafic d'interface
- Géolocalisation des menaces



# Visibilité : gestion centralisée de la sécurité



# Analyse forensique numérique : une analyse forensique riche permet une évaluation des risques



# Analyse médico-légale numérique : cartographie du cadre MITRE ATT&CK

## MITRE ATT&CK®

Acronyme de *Adversarial Tactics, Techniques, and Common Knowledge*, c'est un cadre de référence mondialement reconnu, développé par la MITRE Corporation, pour classifier et décrire les comportements potentiels liés aux menaces..

The screenshot shows the 'MITRE ATT&CK® Tactic Details' page for TA0042. The page includes a navigation bar with 'Threat Analysis', 'Knowledge Base', 'MITRE ATT&CK® Tactic Details', 'ATT&CK® Technique Details', 'History', and 'Threat Topology'. The main content area is enclosed in a red box and contains the following information:

ATT&CK ID	TA0042	TA0043
Name	Resource Development	
Create Time	2020/09/30 16:11:59	
Last Modified Time	2020/09/30 16:31:36	
Source	ATT&CK	
Official Link	<a href="https://attack.mitre.org/tactics/TA0042">https://attack.mitre.org/tactics/TA0042</a>	
Description	The adversary is trying to establish resources they can use to support operations. Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.	

The screenshot shows the 'ATT&CK® Technique Details' page for T1587.001. The page includes a navigation bar with 'Threat Analysis', 'Knowledge Base', 'MITRE ATT&CK® Tactic Details', 'ATT&CK® Technique Details', 'History', and 'Threat Topology'. The main content area is enclosed in a red box and contains the following information:

ATT&CK ID	T1587.001	T1590.002
ATT&CK Version	1.2	
Name	Malware	
Create Time	2020/10/01 01:33:01	
Last Modified Time	2022/01/14 17:14:27	
Source	ATT&CK	
Permission Requirement	-	
System Requirement	-	
Network Requirement	-	

### Détails de la technique ATT&CK sur les événements de menace

### Détails des tactiques ATT&CK sur les événements de menace

# Analyse forensique numérique : détails sur le comportement des menaces

**Details** [Close]

Name: Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain  ⓘ Behavior Category: Botnet connect to external  Severity: Critical

Admin Action: Unconfirmed  ⓘ Type: Malware - Trojan

Threat Analysis Knowledge Base MITRE ATT&CK<sup>®</sup> Tactic Details ATT&CK<sup>®</sup> Technique Details **History** Threat Topology

	Source	Source Zone	Source Interface	Destination	Destination Zone	Detected at
1	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/21 07:57:28
2	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/18 16:15:36
3	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/18 16:15:26
4	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/18 16:14:22
5	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/15 13:37:18
6	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/10 15:29:41
7	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/10 15:09:35

Displaying 1 - 7 of 7  ⏪ < Page 1 / 1 > ⏩ ↻ 50 Per Page

## Suivi des informations sur les événements de menace :

- IP, balayage des ports
- Craquage par force brute de services courants tels que FTP, LDAP et MySQL
- Réponse d'accès HTTP anormale
- Connexion C&C

# Réponse : Atténuer les attaques avec Hillstone et des dispositifs de sécurité tiers



Hillstone NDR



Hillstone NGFW/NIPS



Pare-feu de nouvelle génération tiers

- Détecter et identifier la menace
- Configurer la liaison avec Hillstone NGFW/NIPS ou NGFW tiers
- Ajouter les attaques confirmées à la liste de blocage



- Lié à Hillstone NDR
- Synchroniser la liste de blocage depuis Hillstone NDR
- Bloquer les attaques

# Réponse : Détectez et répondez aux menaces avec Hillstone XDR



## Dans le cadre d'une intégration avec Hillstone XDR :

- NDR télécharge les données\* (journal des menaces/paquets de preuves/métadonnées/netflow) vers XDR
- NDR peut effectuer une tâche d'analyse des actifs actifs fournie par XDR et télécharger les résultats vers XDR
- Prend en charge divers types de détection et d'analyse des menaces et attaques avancées, notamment la détection basée sur la signature, l'analyse de corrélation, NTA, etc.
- Fournir une visibilité complète et une réponse automatisée aux produits de sécurité intégrés tels que les NGFW

\* Remarque : le journal des menaces, les métadonnées et le flux net peuvent être téléchargés vers iSource V2.0R4-R8 ; le journal des menaces, les paquets de preuves et le flux net peuvent être téléchargés vers iSource V2.0R9 ou version ultérieure.

# Rapport : Évaluation des risques pour l'hôte

**Server Detail**

Intranet Asset (IP) 192.168.87.10(192.168.87.10) Active state  Inactive

Threat Tag **Botnet**

Threat | Event Highlights | Traffic Monitor

**Endpoint Detail**

Endpoint Name/IP 192.168.1.37 Active state  Inactive

Threat | Event Highlights

**1. Security Assessment**

1.1 Overview of Security Assessment

The risk index of server test1(10.230.1.165) is 48. The server is at low risk level. The following lists the threat behaviors detected on the server:

Threat Behavior	Frequency
The server tries to connect to the C&C server	0
The server conducts an internal network attack	0
The server performs an internal network scans	0
The server is involved in botnet activities	10
The server tries to transmit suspicious files	238
The server downloads malware	2

1. The server is at low risk level. No threat event of high reliability is detected.  
The threat event of low reliability listed in the second section may be normal. Please check whether it's a real threat.  
2. According to historical traffic statistics, the network traffic of the server is found abnormal. For details, refer to the third section.  
It is necessary to note that the abnormal traffic of the server may have the following potential risks:  
1) Threat Spread Risk: The malware, viruses and malicious plug-ins may exploit new connections with small traffic to spread threats.  
2) Data Leakage Risk: The latest malware may leak sensitive data to the external with normal traffic.  
3) Bandwidth Consumption Risk: The large number of abnormal traffic may cause bandwidth consumption, which will affect server performance.

**2. Threat Event**

2.1 Typical Threat Events

No data to display

**3. Abnormal Traffic**

The following lists the abnormal traffic of the server:

3.1 Traffic From Client To Server

Source Address	Service/Port	Upstream Traffic	Downstream Traffic	Connections	Anomaly Reason
10.230.3.225	TCP-4444(748)	26.55KB	2.12MB	866	New Connection
101.226.232.201	HTTP(80)	55.37KB	2.68MB	13	New Connection
10.182.142.116	SSH(22)	110.49MB	1.93MB	1	New Connection
10.182.142.81	SSH(22)	1.77MB	55.64MB	5	New Connection
10.88.15.114	TCP-4444(748)	76.62KB	1.91MB	20	New Connection

3.2 Traffic From Server

Destination Address	Service/Port	Upstream Traffic	Downstream Traffic	Connections	Anomaly Reason
10.230.3.225	TCP-4444(748)	26.55KB	2.12MB	866	New Connection
101.226.232.201	HTTP(80)	55.37KB	2.68MB	13	New Connection
10.182.142.116	SSH(22)	110.49MB	1.93MB	1	New Connection
10.182.142.81	SSH(22)	1.77MB	55.64MB	5	New Connection
10.88.15.114	TCP-4444(748)	76.62KB	1.91MB	20	New Connection

Anomaly Info:

- #1: Latest Abnormal Traffic Info: 2022-05-24 12:00:00 New Connection
- #2: Latest Abnormal Traffic Info: 2022-05-24 17:00:00 New Connection
- #3: Latest Abnormal Traffic Info: 2022-05-24 10:00:00 New Connection
- #4: Latest Abnormal Traffic Info: 2022-05-24 11:00:00 New Connection
- #5: Latest Abnormal Traffic Info: 2022-05-24 12:00:00 New Connection

**3.3 Analysis and Recommendations**

The following analyzes the reason of abnormal traffic and offers related recommendations:

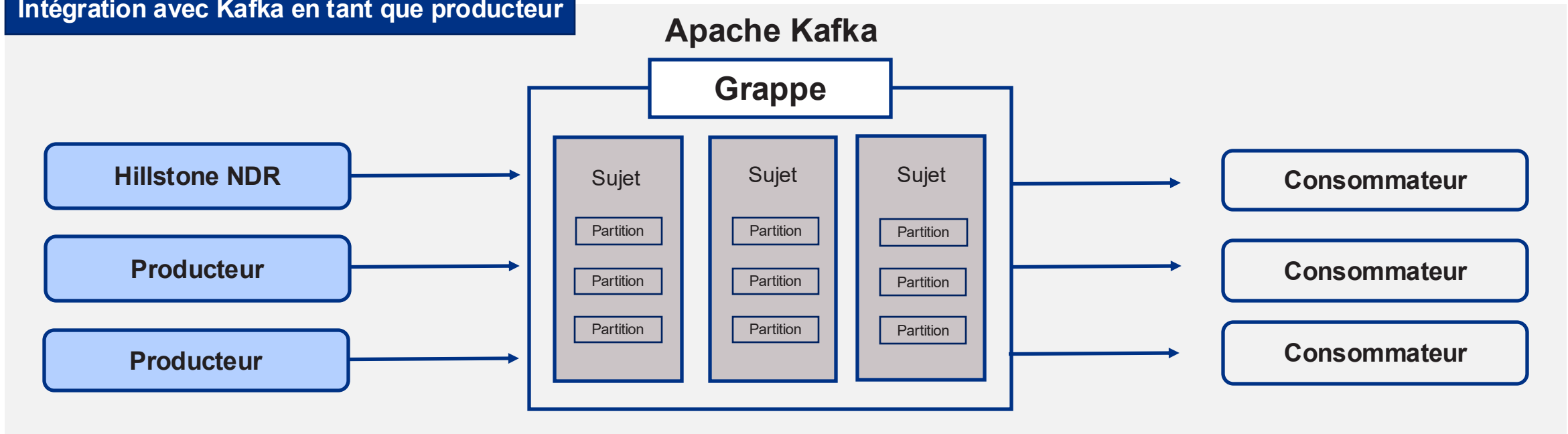
- New Connection**  
An unknown new connection was detected. Please check whether there is a new network service or whether the connection is conducted by malware.
- Upstream Traffic Exceeds Threshold**  
The upstream traffic of certain connection exceeded the threshold. Please check whether the upstream traffic is normal or whether the malware conducted content leakage.
- Downstream Traffic Exceeds Threshold**  
The downstream traffic of certain connection exceeded the threshold. Please check whether the downstream traffic is normal or whether the malware conducted content download.
- Connections Exceeds Threshold**  
The number of connections exceeded the threshold. Please check whether the connection frequency is normal or whether the number of connections conducted by the malware exceeded the threshold.

Sur la page du serveur de risques ou du point de terminaison de risques, les informations sur les menaces et le trafic correspondant aux conditions de filtrage d'interface actuelles sont exportées. Un rapport PDF est généré, contenant les informations suivantes :

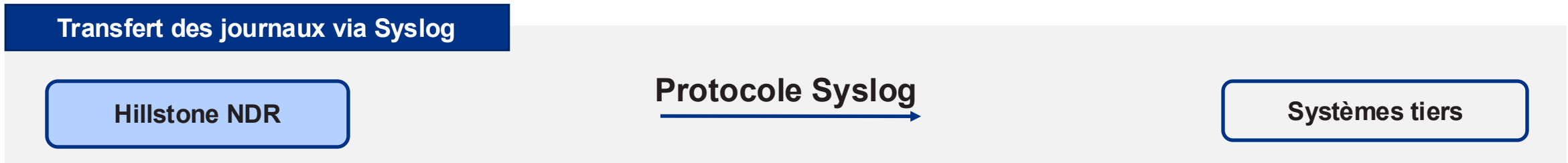
- Informations sur le serveur/point de terminaison
- Évaluation de l'état de sécurité
- Événement menaçant
- Trafic anormal
- Recommandations d'analyse et d'élimination

# Intégration tierce

## Intégration avec Kafka en tant que producteur



## Transfert des journaux via Syslog



# Cycle fermé : détection et réponse du réseau

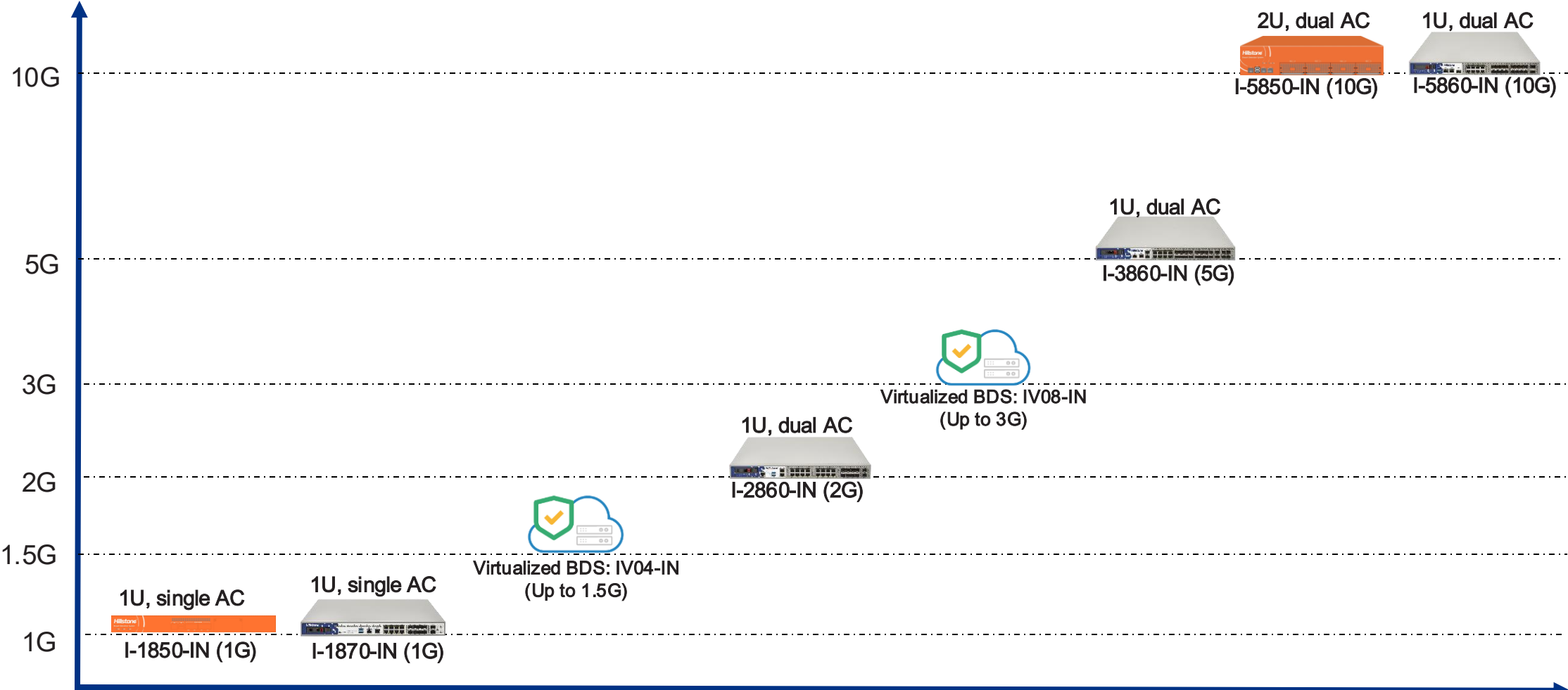


# Portefeuille de produits Hillstone NDR

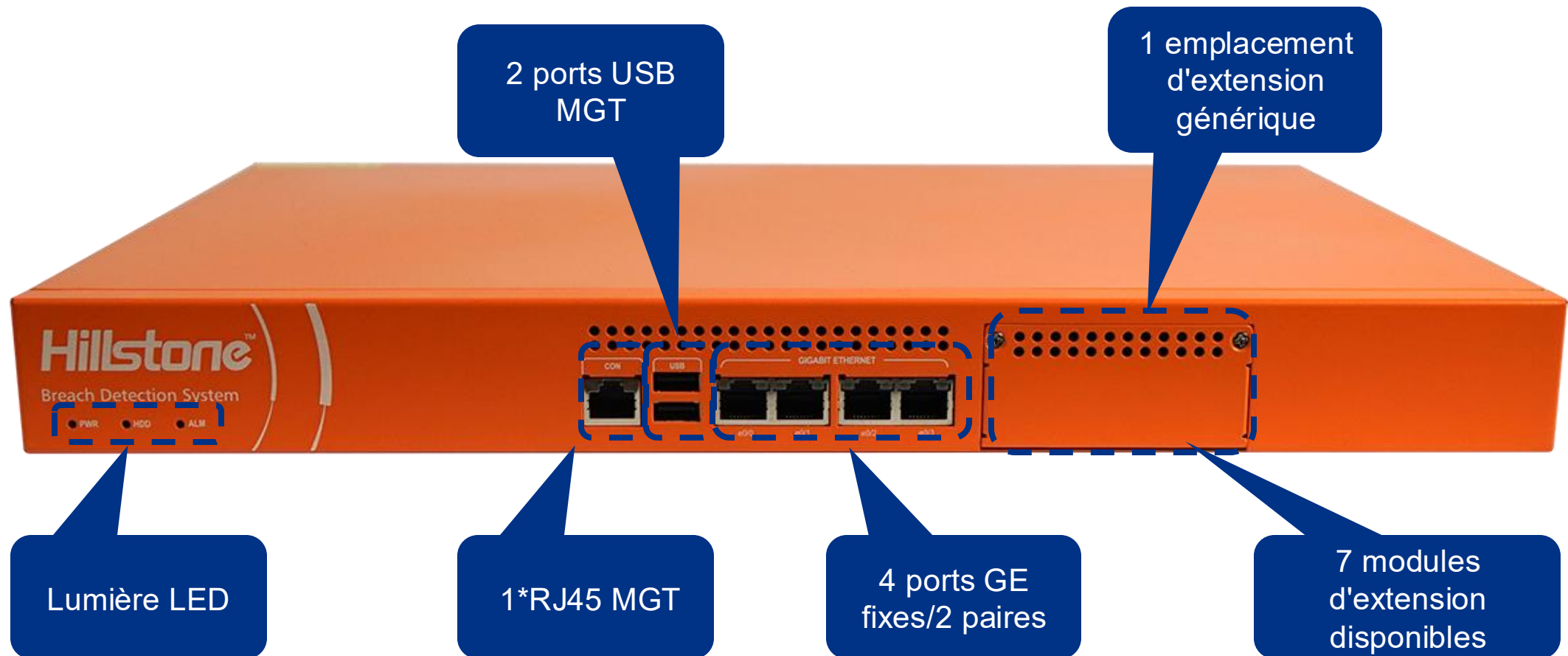
# Hillstone NDR Product Portfolio



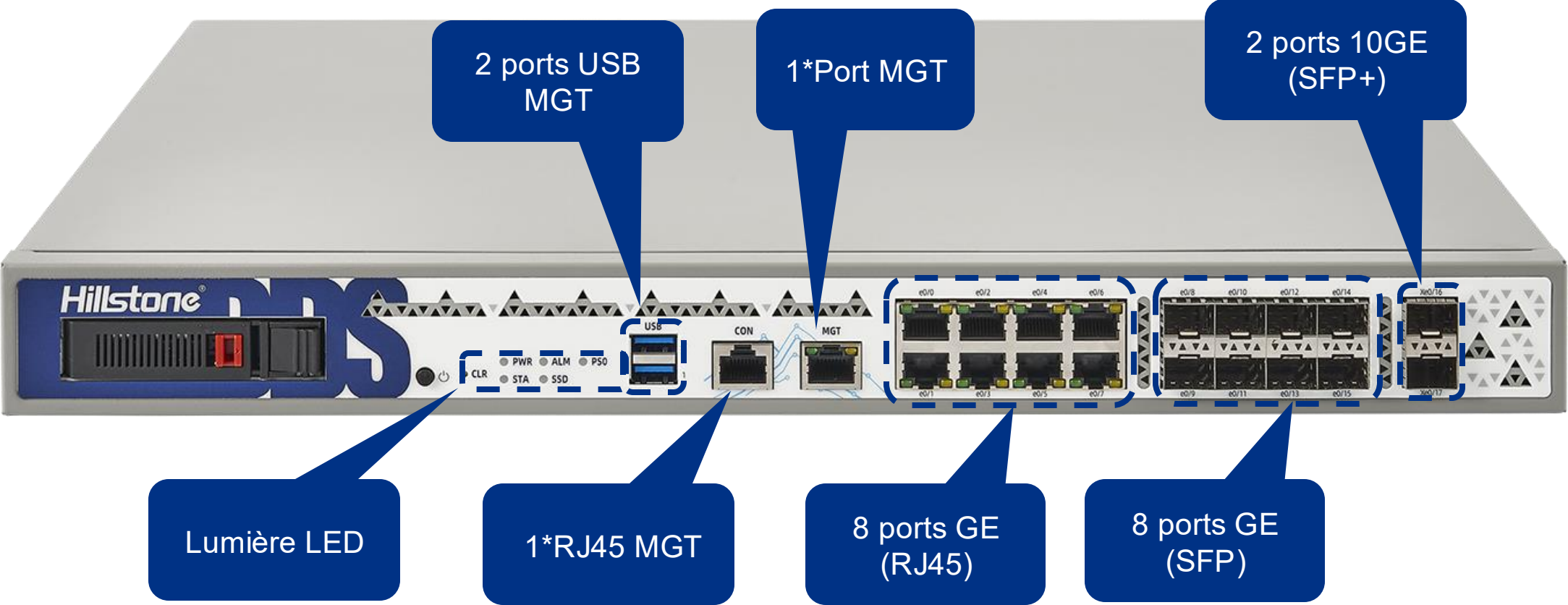
Débit de détection des violations



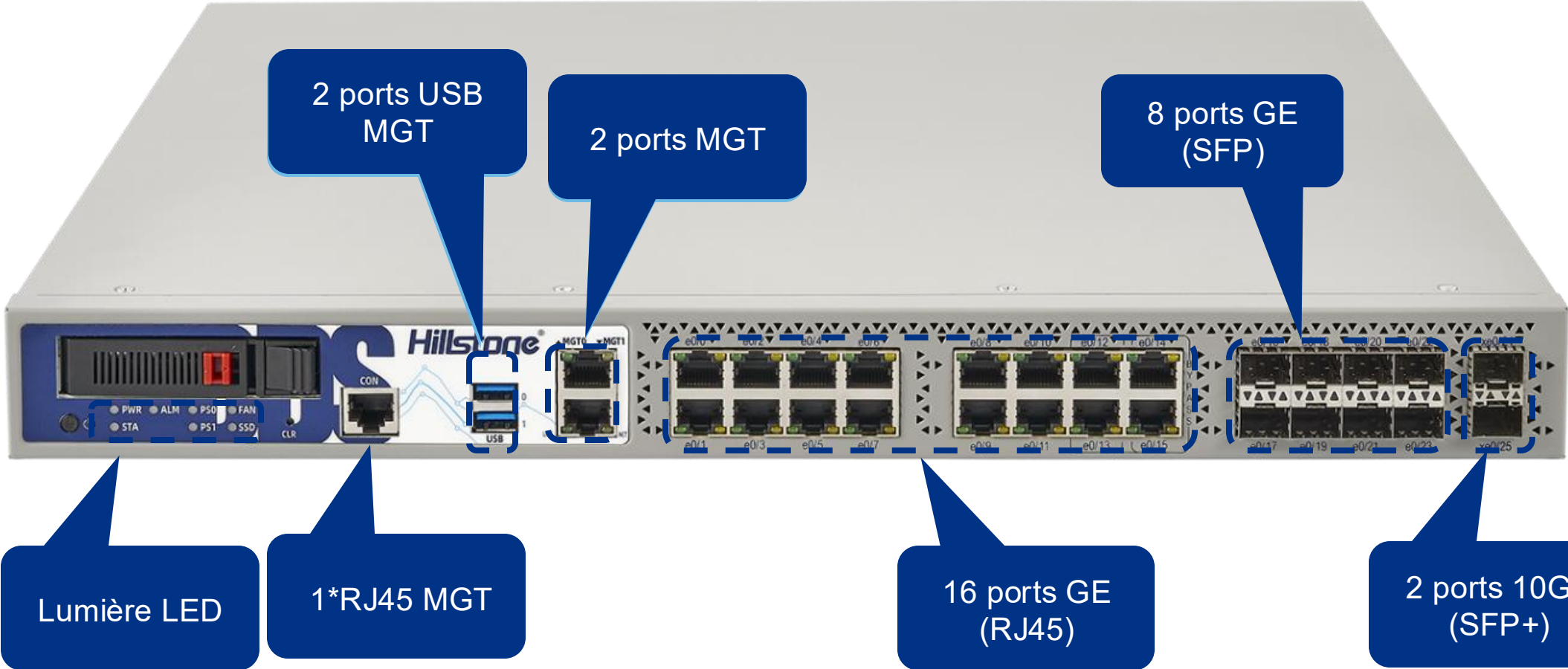
# Spécifications matérielles I-1850



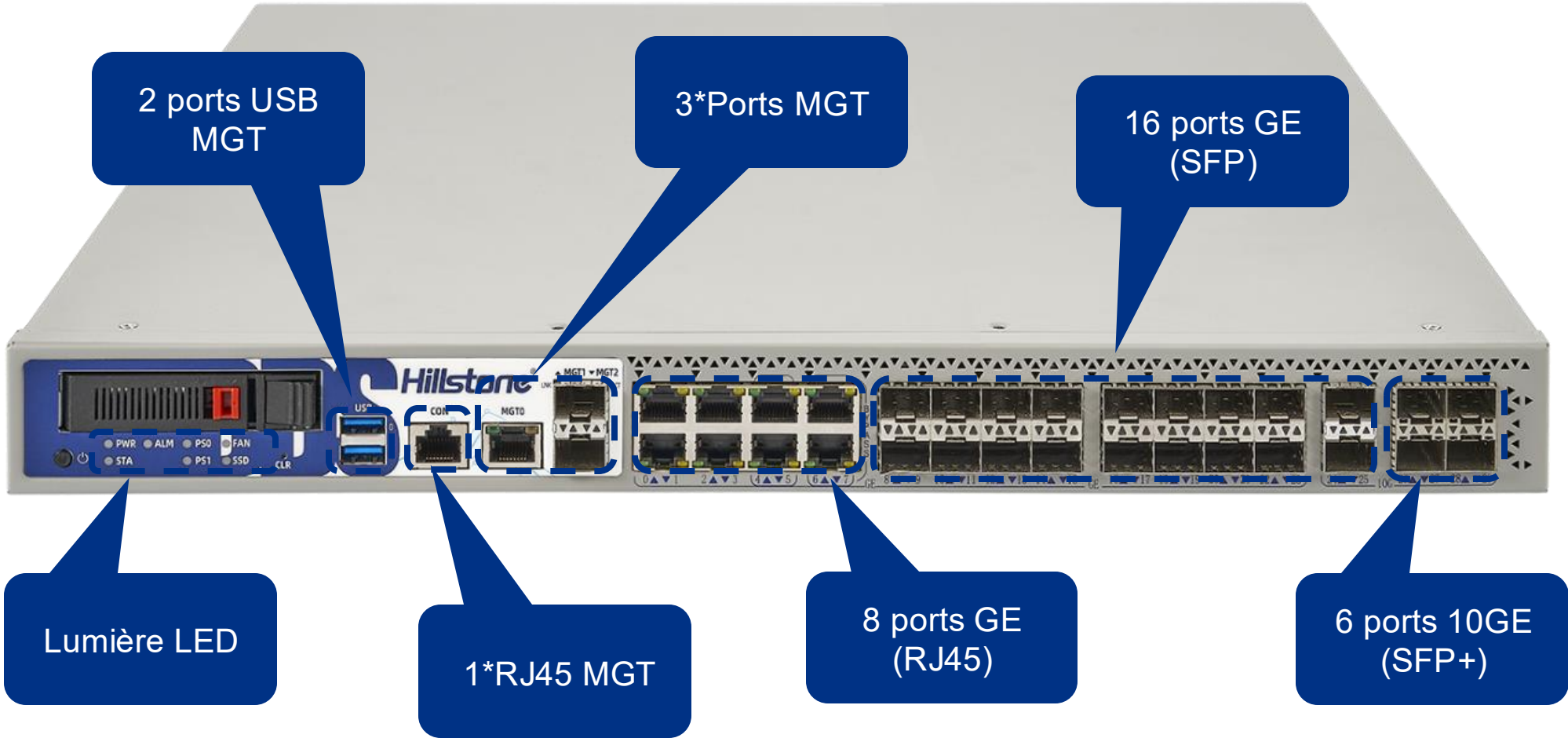
# Spécification matérielle I-1870



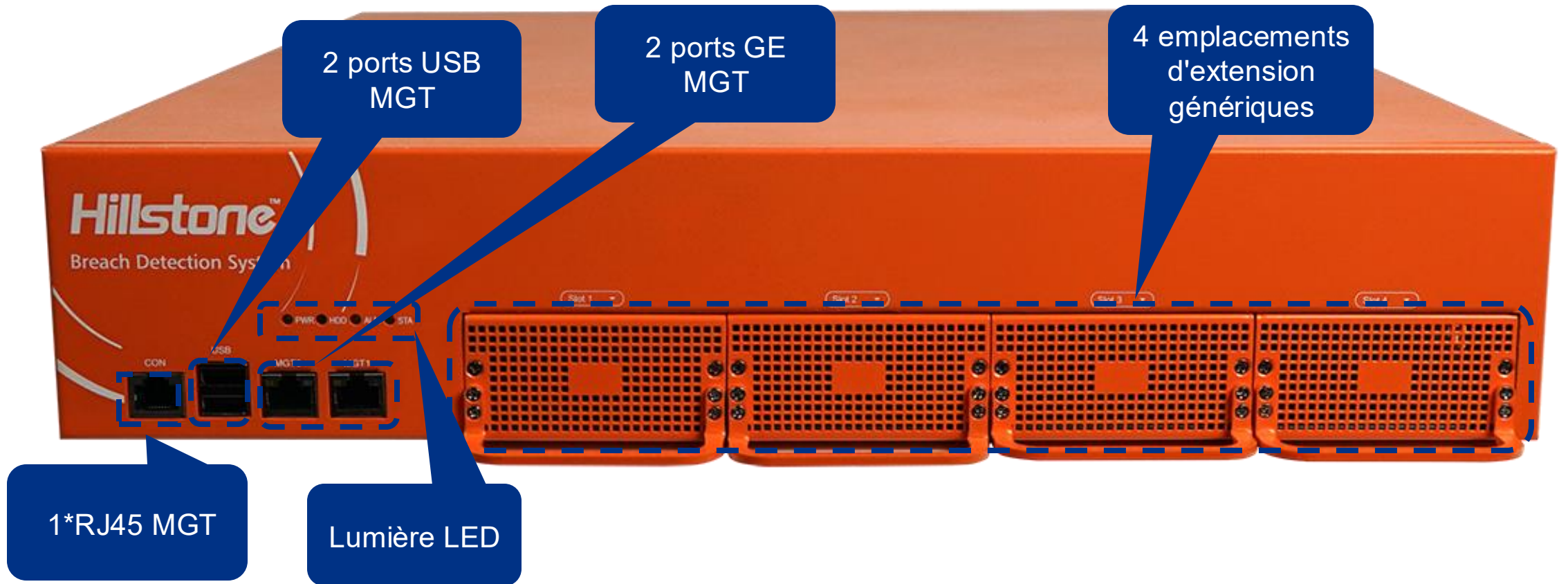
# Spécifications matérielles I-2860



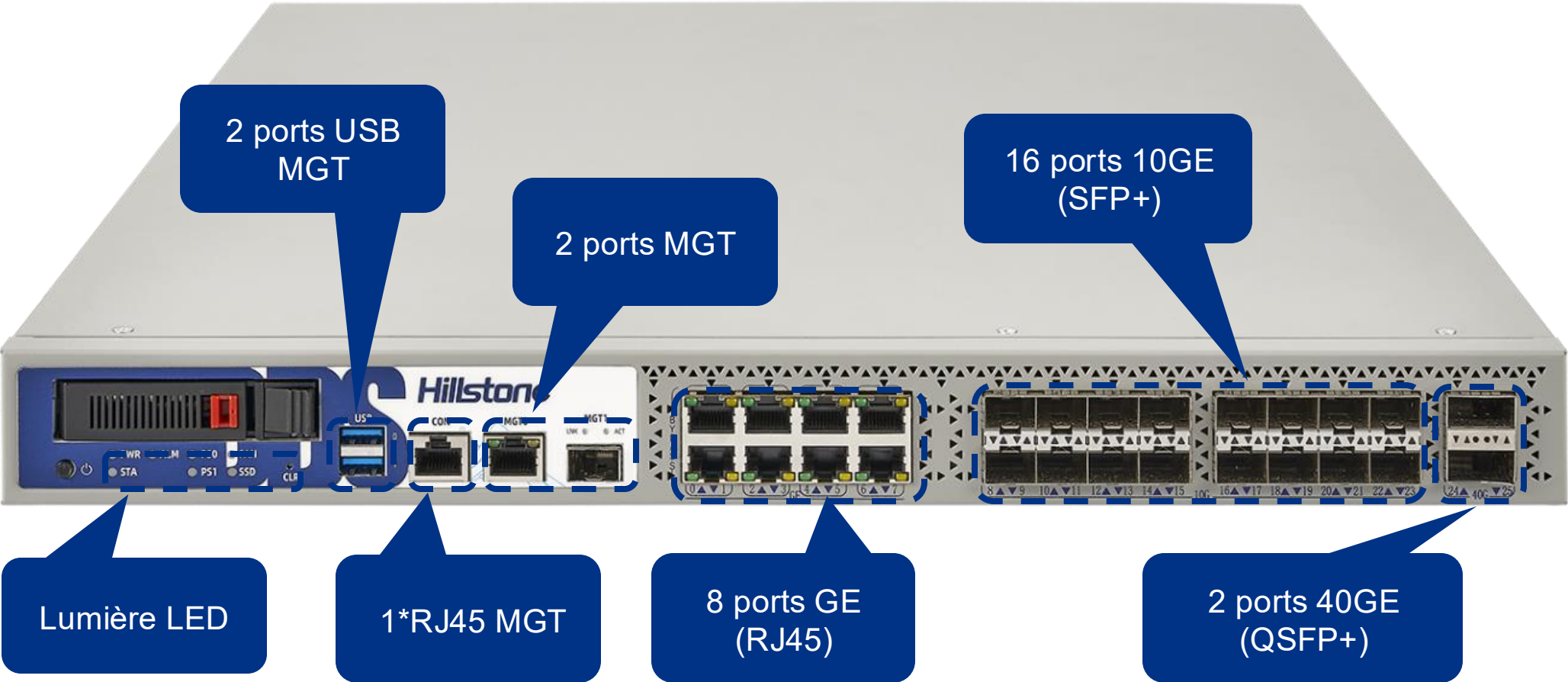
# Spécifications matérielles I-3860



# Spécifications matérielles I-5850



# Spécifications matérielles I-5860



# Spécifications matérielles NDR

Modèle	I-1850-IN	I-1870-IN	I-2860-IN	I-3860-IN	I-5850-IN	I-5860-IN
Débit de détection des violations	1 Gbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	10 Gbps
Nouvelles sessions	20,700	32,000	75,000	210,000	250,000	500,000
Nombre maximal de sessions simultanées	750,000	750,000	1,500,000	3,000,000	6,000,000	6,000,000
Facteur de forme	1 U	1 U	1 U	1 U	2 U	1 U
Stockage	1T HDD	1T SSD	1T SSD	1T SSD	1T HDD	2T SSD
Ports de gestion	2 x USB port 1 x RJ45 port	2 x USB port 1 x RJ45 port 1 x MGT	2 x USB port 1 x RJ45 port 2 x MGT	2 x USB port 1 x RJ45 port 3 x MGT	2 x USB port 1 x RJ45 port 2 x MGT	2 x USB port 1 x RJ45 port 2 x MGT
Ports d'E/S fixes	4 (2 Pairs) GE ports	2x10GE (SFP+) 8 x GE (SFP) 8 x GE (RJ45)	2x10GE (SFP+) 8 x GE (SFP) 16 x GE (RJ45)	6x10GE (SFP+) 16xGE (SFP) 8xGE (RJ45)	N/A	8xGE (RJ45) 16x10GE (SFP+) 2x40GE (QSFP+)
Emplacements disponibles pour les modules d'extension	1	N/A	1	1	4	1
Option de module d'extension	IOC-S-4SFP-L-IN	N/A	IOC-A-4SFP+-IN	IOC-A-4SFP+-IN	IOC-BDS-8GE-H-IN, IOC-BDS-8SFP-H-IN, IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN

# Spécification et configuration du produit virtualisé



Spécifications et configuration matérielle minimale :

Modèle	IV04-IN	IV08-IN
Débit de détection des violations*	Jusqu'à 1,5 Gbit/s	Jusqu'à 3 Gbit/s
Prise en charge du processeur	4 Core	8 Core
Mémoire	8G	16G
Stockage	100G	100G
Configuration requise	KVM / VMware ESXi version 6.5 ou supérieure	
Prise en charge du cloud public	Alibaba Cloud / Tencent Cloud	

\* Les données de débit de détection de violation dépendent de la configuration matérielle

Carte d'interface réseau prise en charge :

	SR-IOV	All NICs except SR-IOV
KVM	√ (seul SR-IOV X710 peut être pris en charge)	√
VMware	x	√

# Modules d'extension



Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN	IOC-BDS-8GE-H-IN	IOC-BDS-8SFP-H-IN	IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN
I/O Ports	4 x ports SFP	4 x Ports GE	8 x Ports GE	8 x Ports SFP	4 ports SFP+	4 x SFP+, SFP+ module non inclus
Dimension	1U (Occupe 1 emplacement générique)	1U (Occupe 1 emplacement générique)	1U (Occupe 1 emplacement générique)	1U (Occupe 1 emplacement générique)	1U (Occupe 1 emplacement générique)	1U
Poids	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.44 lb (0.2 kg)	2.09 lb (0.96 kg)

# Configuration Sysmon



Spécification	Serveur Sysmon	Client Sysmon
CPU	4 Core	\
Mémoire	16G	1G
Stockage	Disque dur 1T, extensible	40G HDD
Pack d'installation	Miroir OVF	Programme de service MSI
Logiciel	VMware ESXi	Windows 7 / Windows Server 2007 ou supérieur

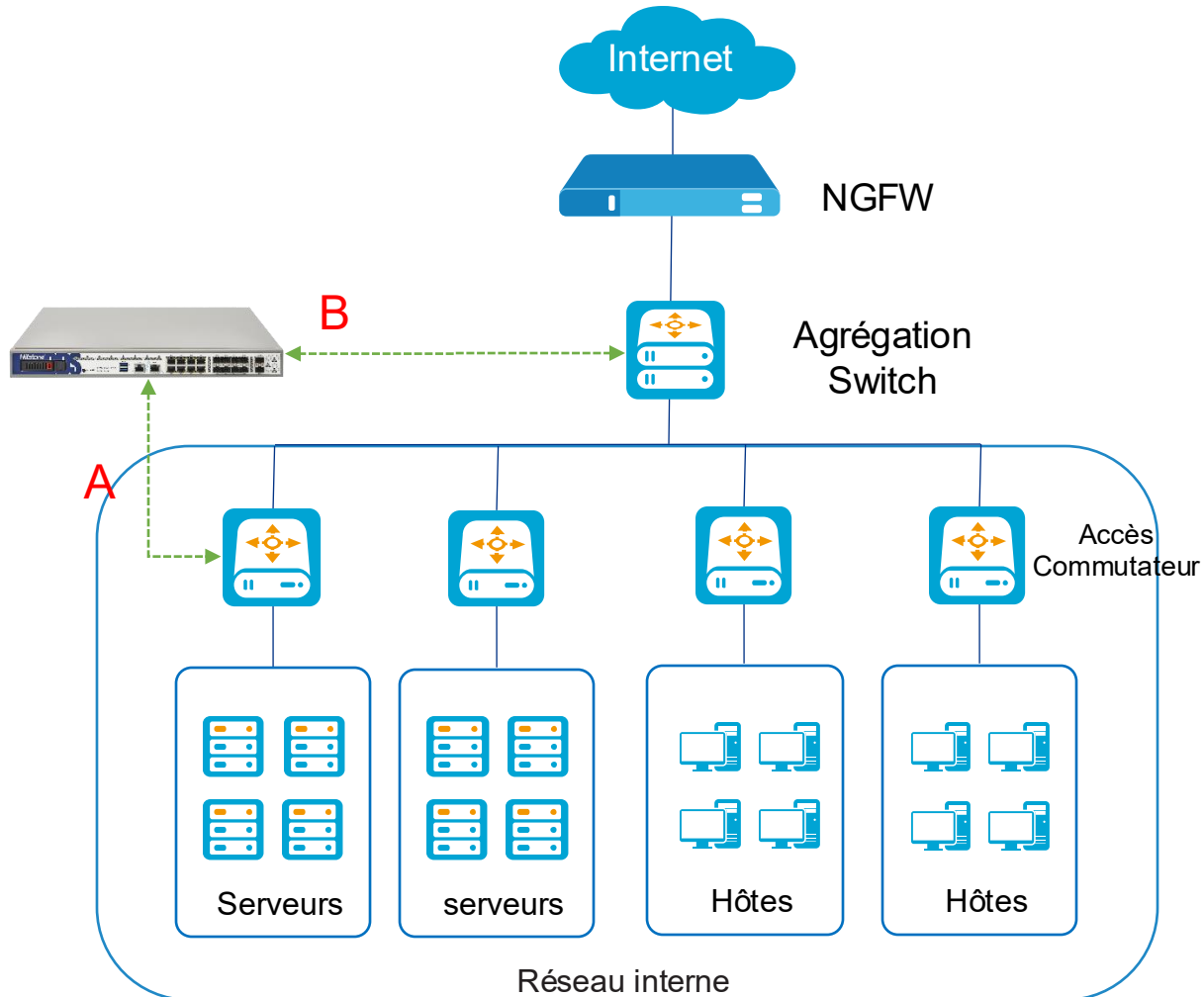
- La configuration par défaut prend en charge le stockage des journaux de 1 000 PC.
- Le serveur Sysmon stocke jusqu'à 90 jours de données. Les données sont automatiquement supprimées (nettoyées) après 90 jours. Lorsque l'utilisation du disque (/data) dépasse 85 %, le système supprime automatiquement les données les plus anciennes.
- Le système Sysmon Server a activé le service de réception de journaux (Logstash) et le service de requête (Elasticsearch), en utilisant respectivement les ports 5044 et 9200.

Deux méthodes d'installation sont disponibles :

- installation directe par l'utilisateur
- installation par lots via le logiciel de distribution de domaine Windows Active Directory

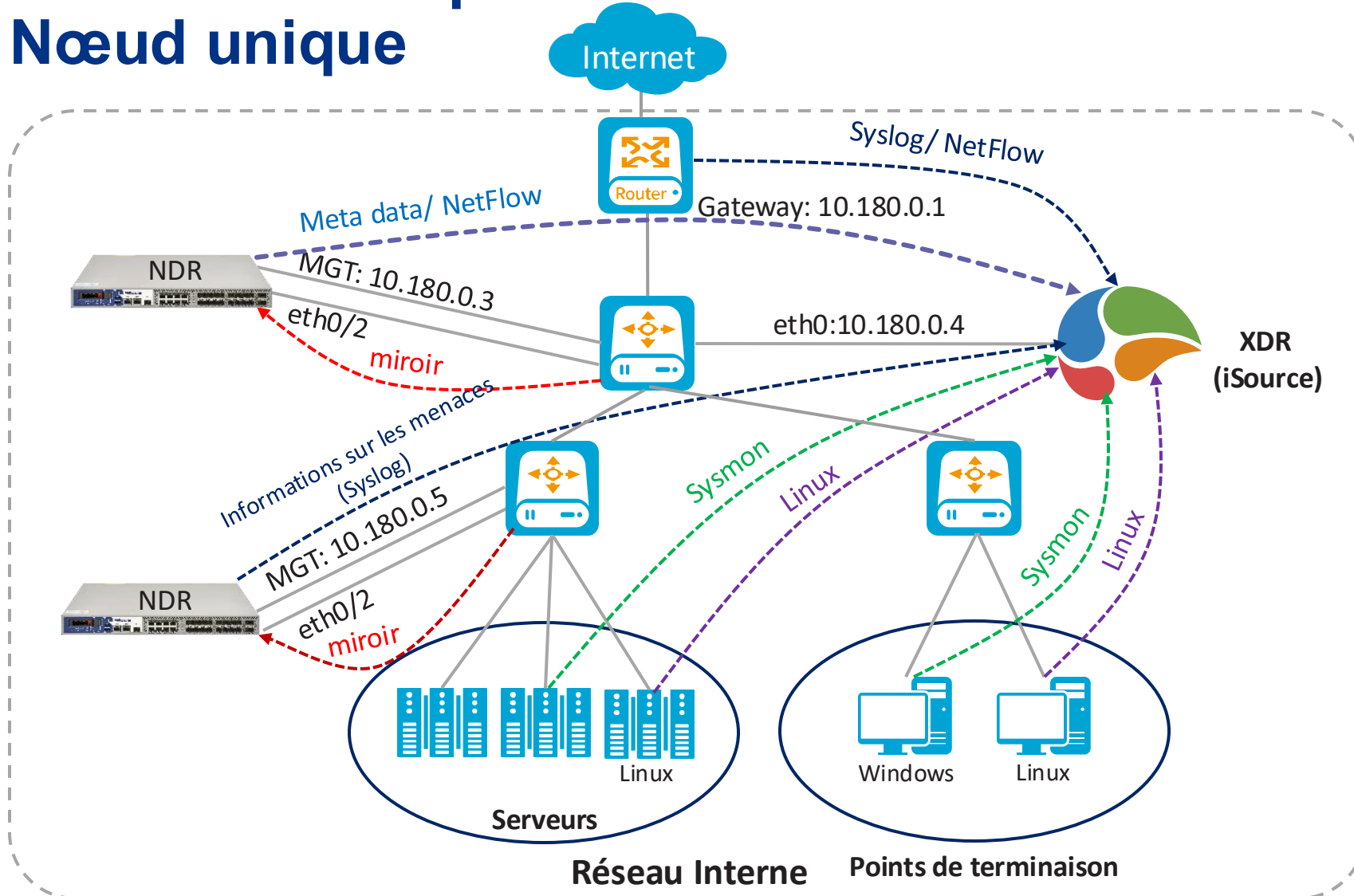
# Scénarios de déploiement et études de cas

# Scénarios de déploiement du NDR Hillstone : BDS et NGFW



- **Scénario A : Commutateur d'accès se connectant à des serveurs ou à des groupes de serveurs**
  - Surveiller le trafic entre les serveurs au sein du même segment ; les serveurs dans différents segments ; le serveur et Internet ; les serveurs et autres hôtes.
- **Scénario B : Commutateur d'agrégation entre commutateurs d'accès**
  - Surveiller le trafic entre les serveurs dans différents segments ; serveurs et Internet ; serveurs et autres hôtes ; hôtes et Internet.
- **Scénario C : Combinaison des scénarios ci-dessus**

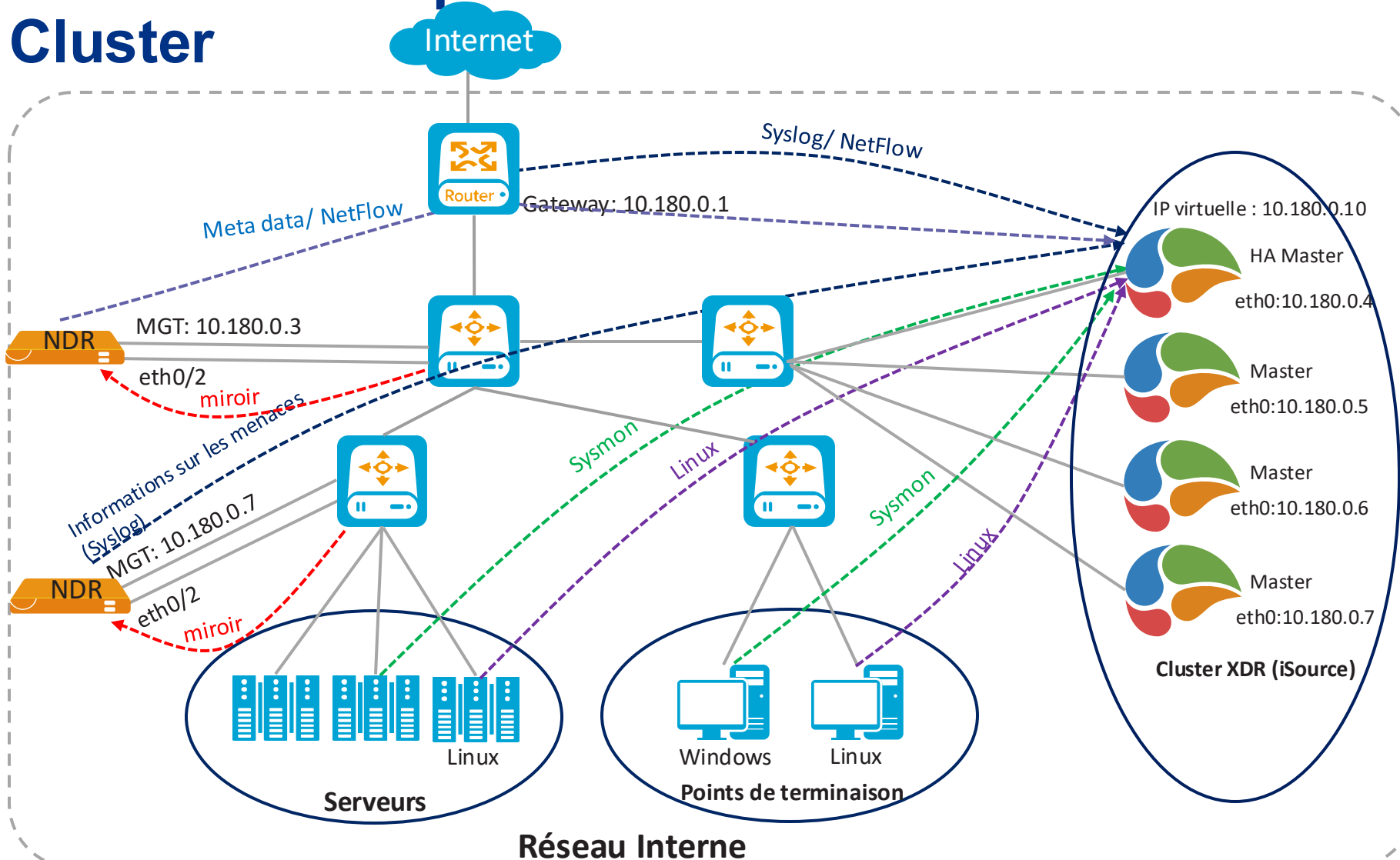
# Scénario de déploiement Hillstone NDR et XDR - Nœud unique



## Déploiement d'un nœud unique

- NDR déployé en mode TAP
- Le déploiement XDR a peu d'impact sur l'environnement réseau existant
- Solution économique

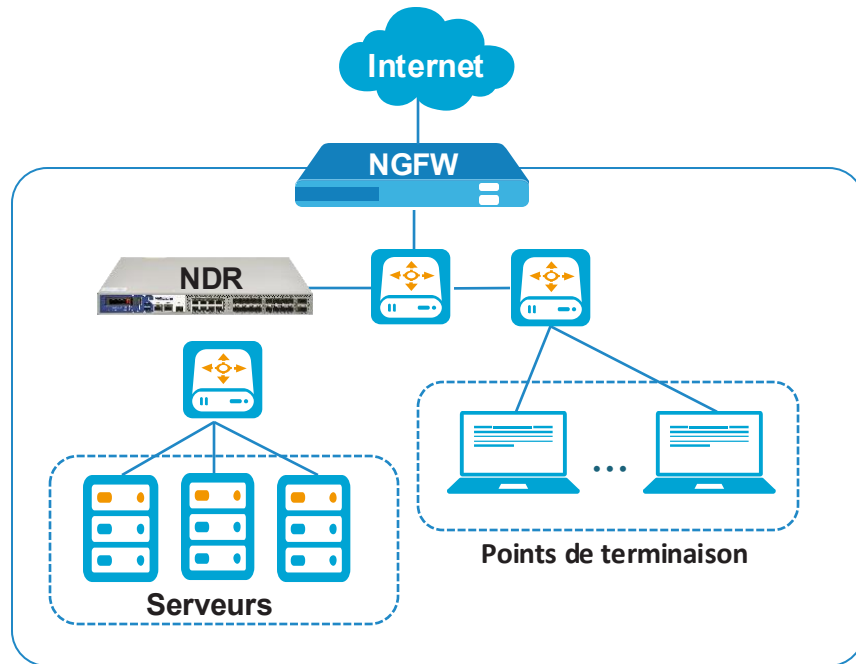
# Scénario de déploiement Hillstone NDR et XDR - Cluster



## Cluster Deployment

- NDR déployé en mode TAP
- Cluster jusqu'à 5 nœuds
- Le déploiement XDR a peu d'impact sur l'environnement réseau existant
- Solution hautement évolutive

# Étude de cas 1 : Protéger les informations critiques pour une grande université



## Profil client

- Une grande université privée comptant plus de 10 000 étudiants, située en Amérique du Sud

## Challenges

- Un nombre important d'utilisateurs se connectent ou accèdent aux réseaux à partir de divers appareils, compromettant souvent la sécurité du périmètre et générant des violations qui pourraient mettre en danger des informations critiques.
- Les cyberattaques potentielles pourraient avoir un impact sur la continuité des activités, interrompant l'accès aux propriétés Web de l'Université.

## Solution Hillstone

- Le client a déployé Hillstone NDR en conjonction avec les pare-feu intelligent de nouvelle génération Hillstone T-Series (iNGFW).
- Les fonctionnalités de sécurité du renseignement de Hillstone BDS et d'iNGFW – détection du comportement et des menaces basée sur le ML, ont permis de réaliser la détection et la prévention du périmètre au réseau interne
- Une attaque critique a été détectée par cette solution déployée, qui aurait provoqué une énorme brèche dans les services internes, ainsi que des données compromises.

# Étude de cas 2 : Sécuriser les actifs critiques d'un gouvernement régional en Amérique latine



## Profil client

- Un gouvernement régional doté d'une autonomie administrative, politique et économique en Amérique du Sud

## Challenges

- Les organisations effectuent constamment leurs opérations et leurs procédures en ligne, gérant un flux massif d'informations et d'argent. Face à la vague croissante de cyberattaques dans le monde, il est impératif de protéger ces informations et ces actifs.
- Le client doit minimiser la menace pesant sur les services qu'il fournit, ainsi que garantir la disponibilité des applications utilisées par le personnel.

## Solution Hillstone

- Le client a déployé Hillstone NDR pour protéger pleinement son réseau interne. Ce système permet d'identifier efficacement les menaces avancées qui se cachent au sein d'un réseau interne et qui sont liées au BYOD (apportez votre propre appareil) des employés de l'entreprise.
- La solution déployée a protégé le client des menaces en détectant l'utilisation d'appareils et l'accès aux données anormales sur son réseau. Elle lui a également permis de prendre des mesures pour éviter les attaques.

# Étude de cas 3 : Détecter le rançongiciel Locky pour une société pharmaceutique



## Challenges

- Le client a déployé des solutions de sécurité viables, notamment des solutions de pare-feu/IPS/antivirus, mais il n'a pas pu détecter les variantes de ransomware à un stade précoce et protéger ses serveurs contre le verrouillage.
- Le client essayait également d'embaucher des professionnels de la sécurité pour désinfecter ses systèmes verrouillés, mais le processus prend des jours, à un coût bien plus élevé que la rançon.

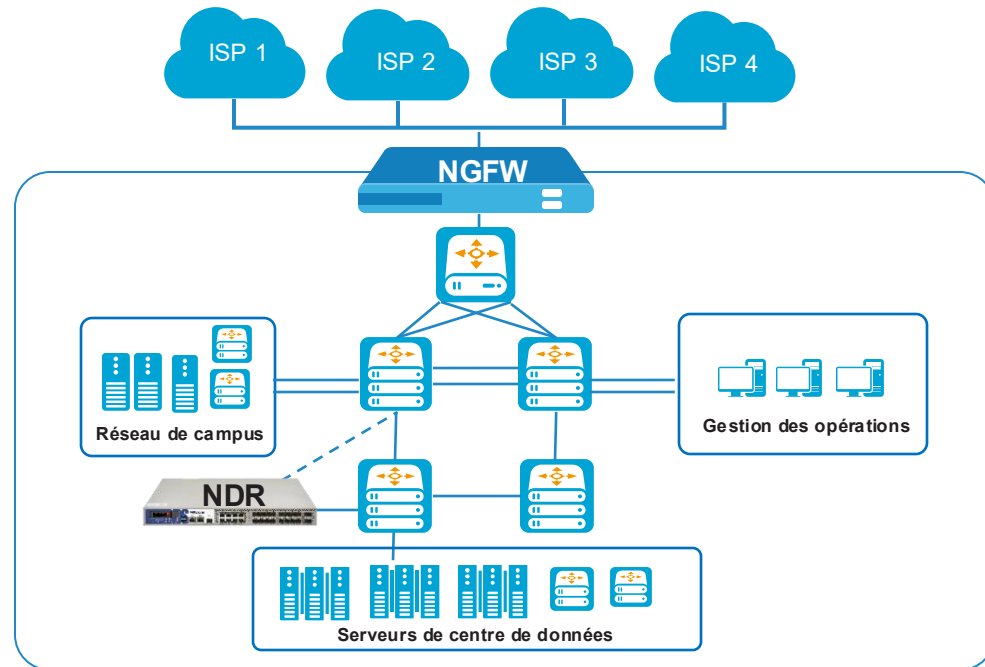
## Solution Hillstone

- Le client a déployé le produit Hillstone NDR devant la zone des serveurs, en mode Tapping par commutateur d'accès, avec Hillstone NGFW et IPS dans la sortie réseau.
- Le produit Hillstone NDR exploite ses moteurs de détection en couches (ABD/ATD/IPS/AV) pour détecter et identifier le ransomware Locky et d'autres attaques avancées et alerter l'équipe informatique afin qu'elle prenne rapidement des mesures pour bloquer ces blocages.

## Profil client :

- Une grande entreprise pharmaceutique compte plus de 2 000 employés dans 5 pays.

# Étude de cas 4 : Protéger les serveurs critiques d'une grande université



## Profil client :

Une université de premier plan avec 25 000 étudiants accédant au réseau et aux ressources du campus

## Challenges

- Impossible d'identifier et de détecter l'hôte interne compromis
- Aucune solution dédiée pour les serveurs critiques dans le centre de données
- Le NGFW et l'IPS actuels ne peuvent pas détecter les menaces inconnues avancées

## Solution Hillstone

- La solution NDR de Hillstone est conçue pour détecter les menaces internes et les attaques sophistiquées qui contournent la défense périmétrique traditionnelle.
- En se concentrant sur les actifs à haut risque et en fournissant un contrôle granulaire, Hillstone garantit que les données les plus précieuses sont protégées contre les menaces externes et internes.
- La solution NDR de Hillstone offre une surveillance continue, la détection des menaces et la capacité de répondre efficacement aux incidents de sécurité.

# Références clients



Centre d'information sur les réseaux  
Informatiques Gouvernement,  
Chine



China Telecom  
ISP,  
China



Datatell  
Communication,  
Costa Rica



Groupe d'énergie électrique  
régional du Shaanxi  
Énergie, Chine



Gouvernement régional  
d'Amazonas, Pérou



Woori Bank  
Finance,  
S.Korea



Administration métropolitaine de  
Bangkok  
Gouvernement,  
Thaïlande



Camel  
Industrie manufacturière, Chine



Groupe d'investissement du secteur  
ferroviaire du Sichuan  
Finance, Chine



Credimatic  
Finance,  
Ecuador



Xiangnan University  
Education,  
Chine



École professionnelle de la ville de Nanjing  
Éducation,  
Chine



École professionnelle d'agro-élevage  
du Jiangsu  
Éducation, Chine



Institut de technologie de Changchun  
Éducation, Chine



Département Commercial

WCA

 **HAFS**  
Distributeur à valeur ajoutée **WCA**

***Vous accompagne***



[www.hafs-networks.com](http://www.hafs-networks.com)  
Visitez notre site web



[sales-ci@hafs-networks.com](mailto:sales-ci@hafs-networks.com)  
Envoyez-nous un e-mail



(+225) 07 69 32 13 55  
Contact commercial 1



(+225) 07 59 05 85 82  
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

