

The background of the slide features a complex isometric network diagram. It includes various server racks, network switches, and routers, all interconnected by a web of blue lines representing data connections. Some components are highlighted with orange triangles, suggesting active or critical nodes in the network. The overall style is technical and modern, with a light blue grid background.

L'Architecture de Télémétrie du SOC

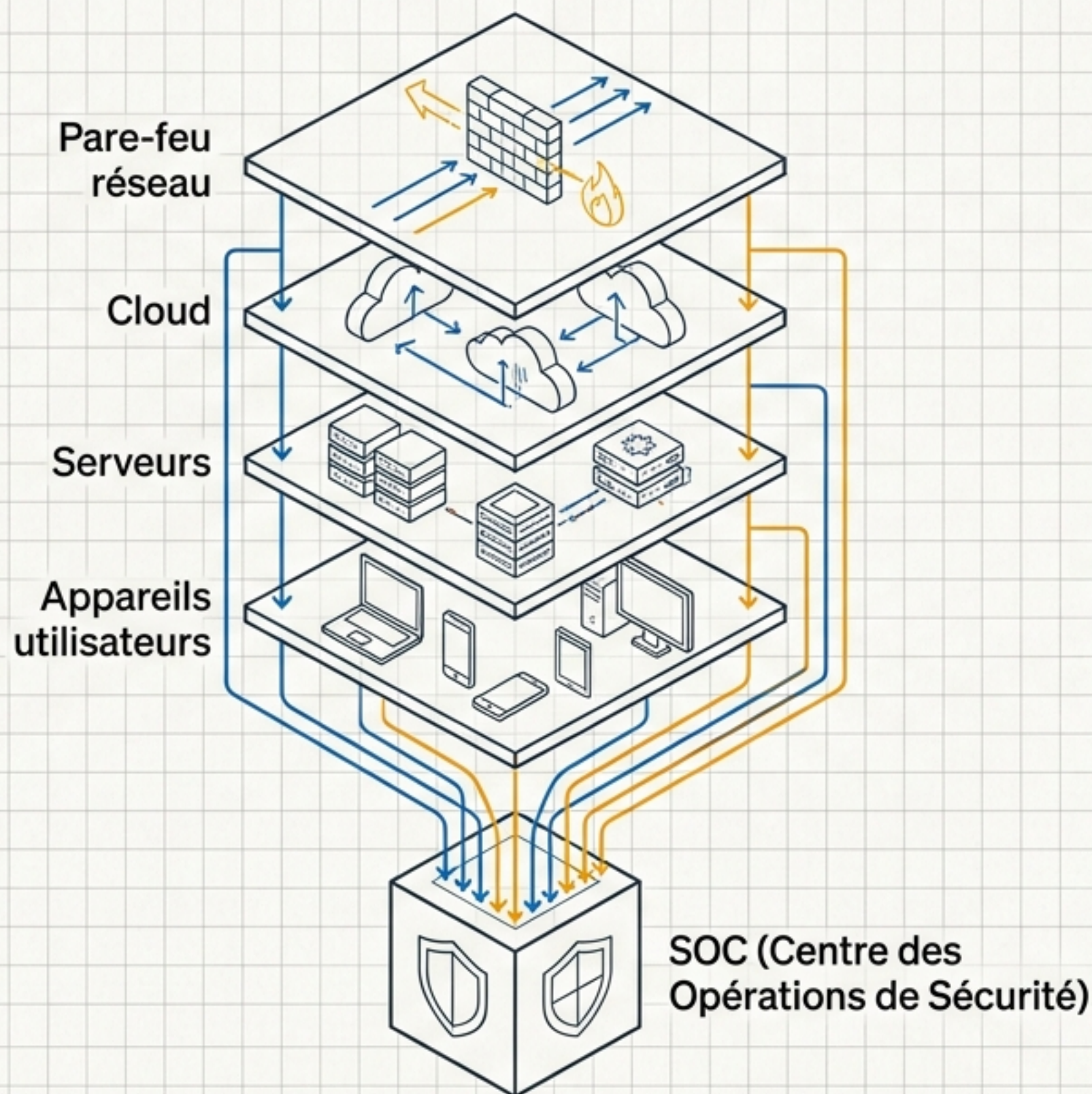
Le guide tactique de **génération, collecte** et corrélation d'événements de sécurité.

« Vous raterez les meilleures choses si vous gardez les yeux fermés. »

— Dr. Seuss

Éliminer les Angles Morts par la Collecte en Couches

Un angle mort, même minime, ouvre la voie à une attaque. La meilleure pratique consiste à déployer des points de surveillance en couches successives et à centraliser les événements.

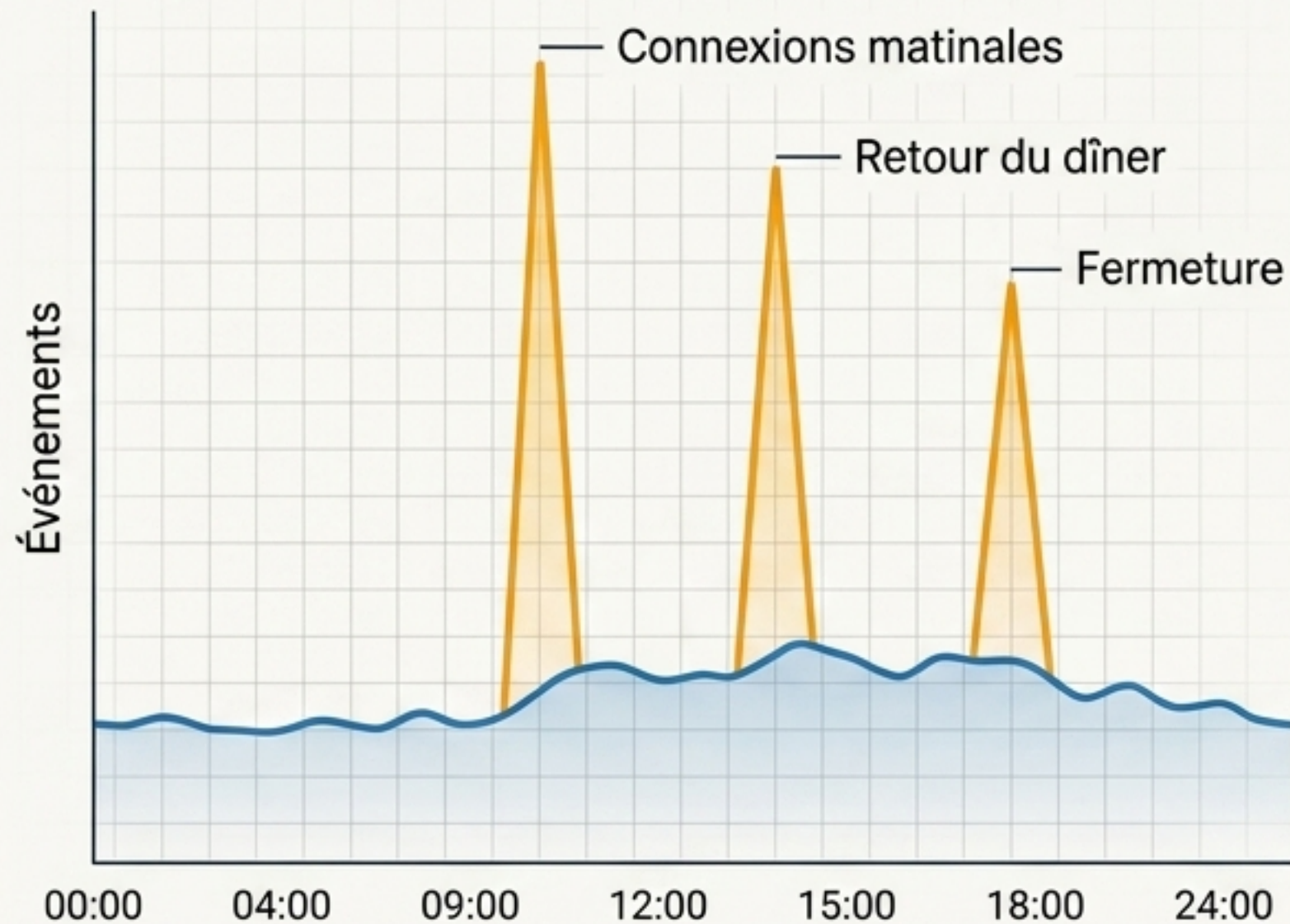


Objectif Principal :

- Corréler les données disparates pour obtenir une visibilité rapide et détecter les menaces sophistiquées.

Dimensionner le Cœur : Le Calcul de l'EPS (Événements Par Seconde)

Trafic Réseau sur 24 Heures

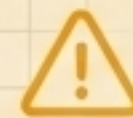


Trafic Normal

$$\text{EPS} = \frac{\text{Nombre d'événements système}}{\text{Période en secondes}}$$

Trafic de Pointe

$$\text{EPS de pointe} = \frac{(\text{EPS normal} \times \text{Nombre de pics} \times \text{Durée du pic} \times \text{Facteur d'écart})}{86\,400}$$



Règle d'or : Toujours intégrer une marge de sécurité d'au moins 20 % pour éviter la perte de journaux critiques lors d'un incident majeur.

Établir une Ligne de Base : Serveur Syslog Ubuntu

```
sudo apt-get install syslog-ng
sudo nano /etc/syslog-ng/syslog-ng.conf
```

```
# Configuration du pare-feu source (ex: 192.168.1.50)
```

```
source source_example { udp(ip(192.168.1.200) port(514));};
```

```
filter filter_example { host( "192.168.1.50" ); };
```

```
destination destination_example { file("/var/log/eventdata.log"); };
```

```
log { source ( source_example ); filter( filter_example );
      destination ( destination_example ); };
```

```
sudo /etc/init.d/syslog-ng restart
```



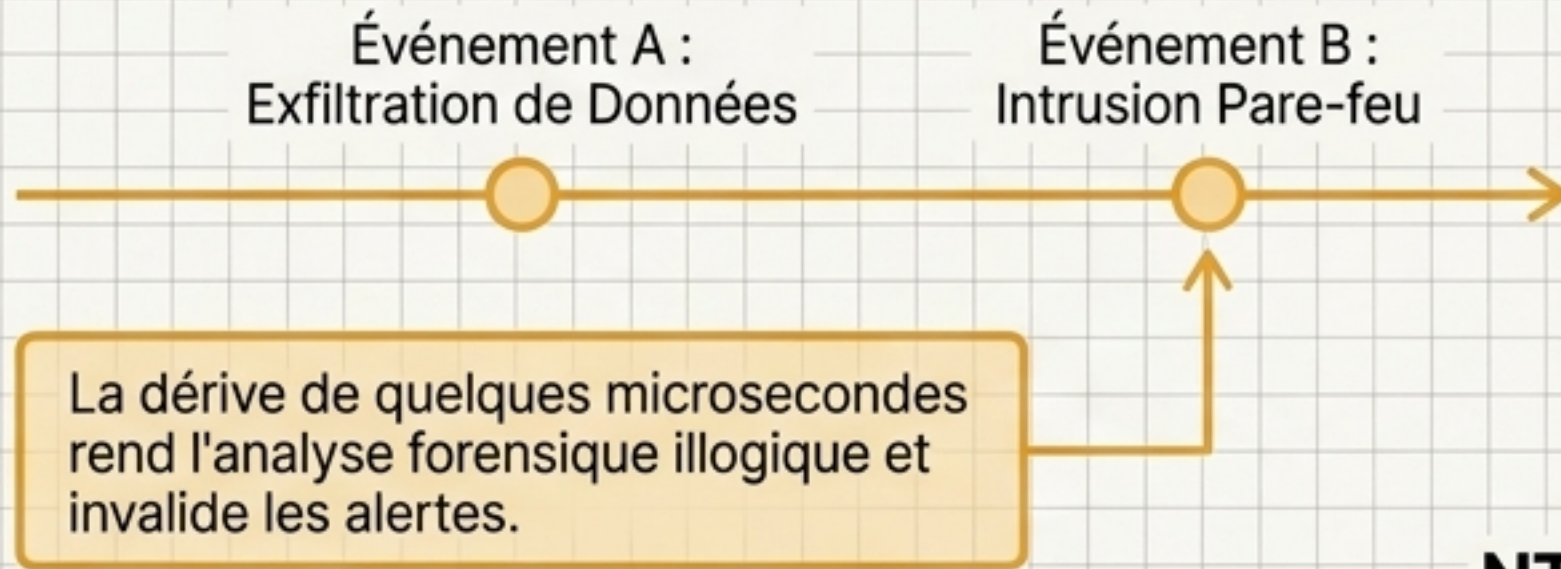
Port d'écoute UDP 514

IP du pare-feu autorisé

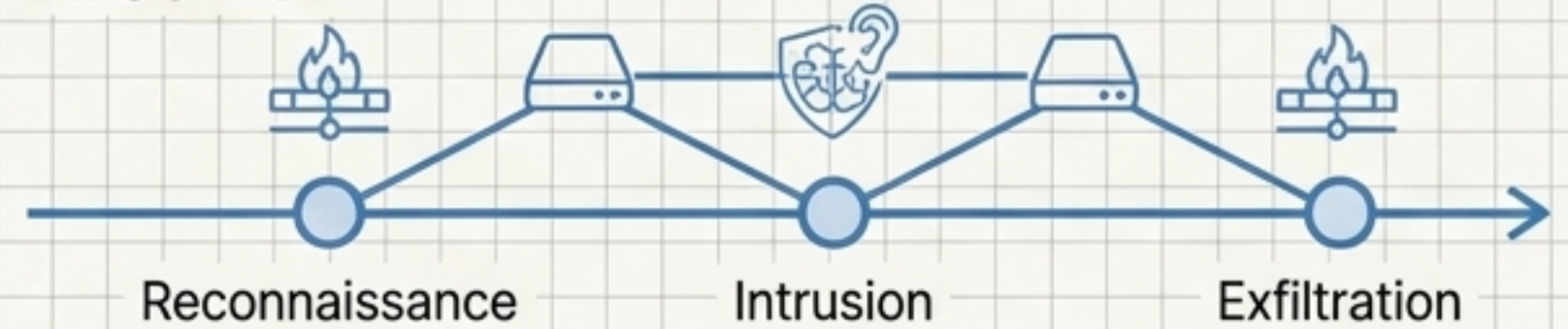
Fichier de stockage local

L'Impératif de Corrélation : Le Danger Le Danger de la Dérive Temporelle

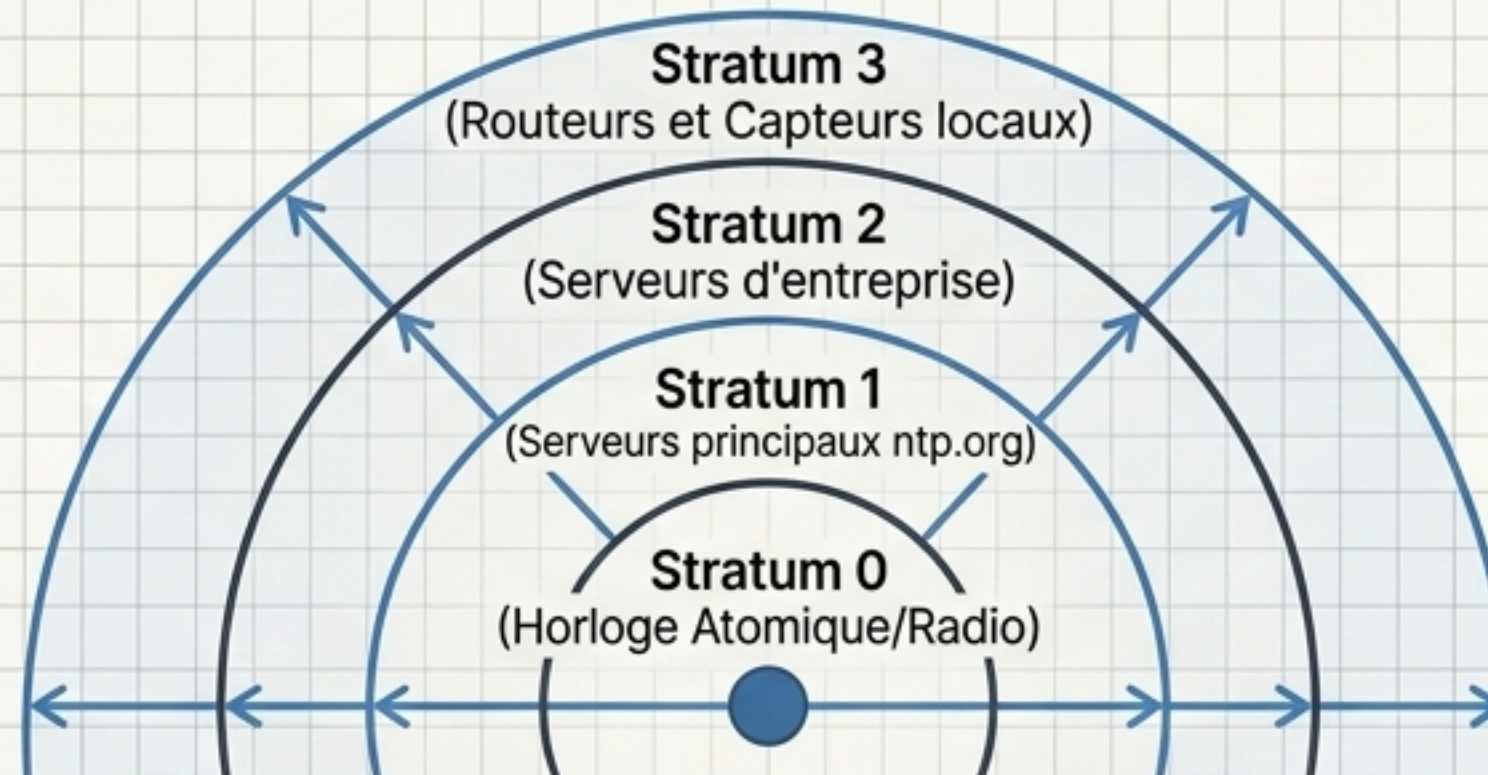
Sans NTP



Avec NTP



NTP Radar



Déploiement Tactique : Configuration NTP Maître et Client

Serveur NTP Maître - Cisco IOS

```
clock timezone EST -5
clock summer-time EST recurring

ntp master 3
ntp source loopback0
ntp authentication-key 1 md5 cisco
ntp trusted-key 1_
```

Pare-feu Client - ASA5520

```
ntp authenticate
ntp server 1.1.1.1

show ntp associations_
```

Authentication requisite : NTP sans authentication par clé (MD5) expose le réseau à l'usurpation d'identité et aux attaques temporelles.

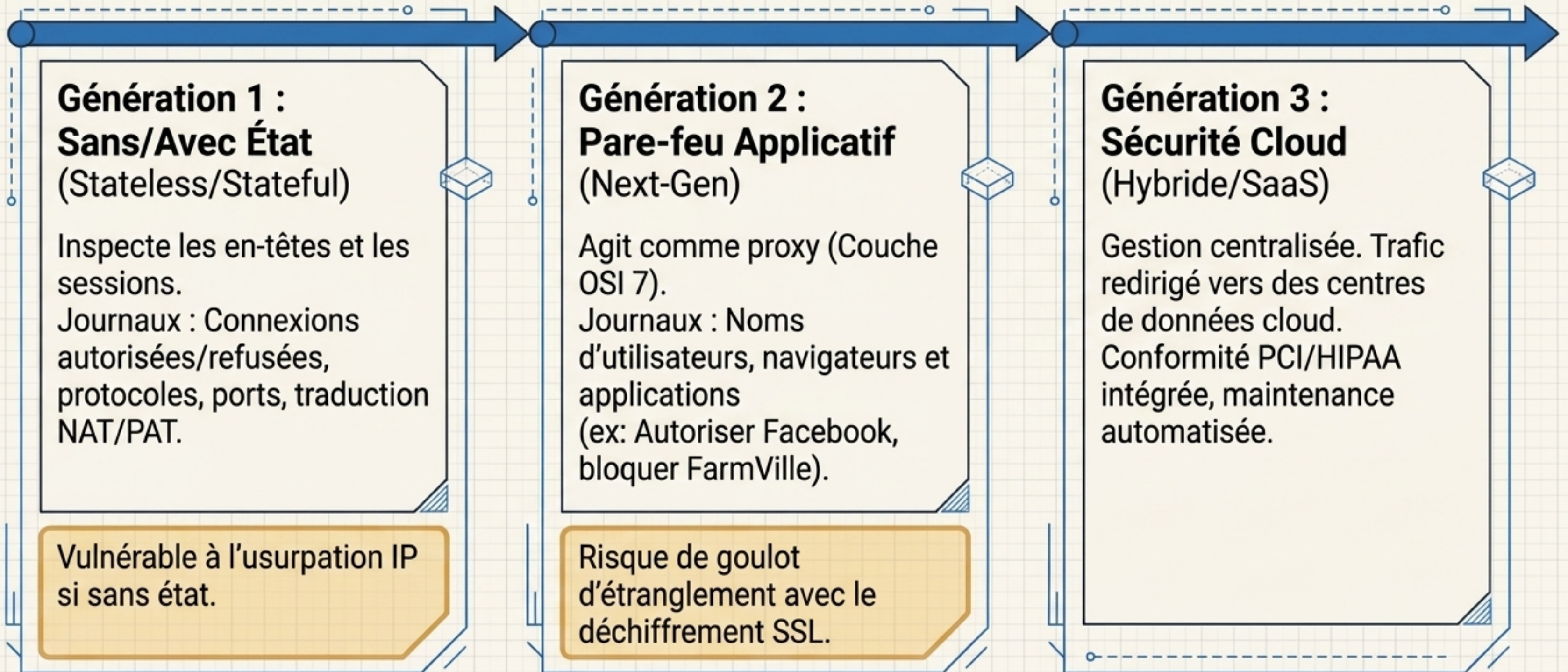
Le Cerveau du SOC : Évaluation de la Matrice SIEM

SIM (Security Information Management)	SEM (Security Event Management)	SIEM (Le standard hybride)
Accent sur les journaux, la recherche, l'archivage, les rapports historiques et l'investigation forensique.	Accent sur l'analyse des menaces en temps réel, la corrélation, l'agrégation, la visualisation et la réponse aux incidents.	Combine l'exploration approfondie des données et la réponse en temps réel aux incidents.

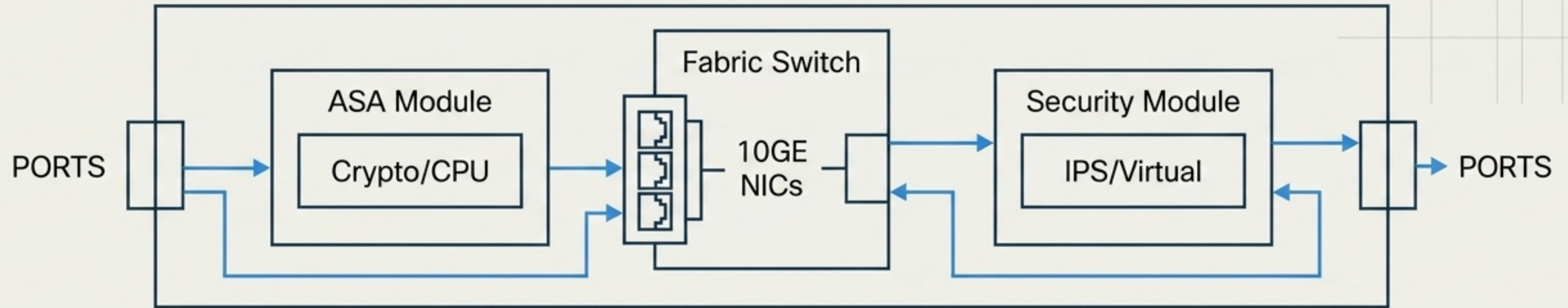
Critères de Sélection d'un Fournisseur SIEM :

- ✓ Architecture et Licence (Appliances vs SaaS, coût total sur 5 ans)
- ✓ Limitations et Capacité EPS
- ✓ Conformité (PCI DSS, JITC, directives NIS)
- ✓ Interface Utilisateur (Contrôle d'accès basé sur les rôles)

L'Évolution des Capteurs : Matrice des Pare-feu



Télémétrie Périphérique : Cisco ASA



```
Terminal
logging buffered 4
logging host inside 192.168.1.15
logging trap debugging
logging list Critical_Syslogs level 2
logging destination Critical_Syslogs
```

Capture
les
niveaux
0 à 4

Table 6-1 *Security Logging Level Values*

Level Number	Severity Level	Description
0	Emergencies	System is unusable.
1	Alert	Immediate action is needed.
2	Critical	Critical conditions.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notification	Normal but significant editions.
6	Informational	Informational messages only.
7	Debugging	Debugging messages only.

Visibilité Profonde : Cisco FirePOWER (FMC)

Capacités Clés



AVC (Application Visibility & Control) :
Plus de 3 000 contrôles d'applications.



Filtrage d'URL : Plus de 280 millions de domaines catégorisés.

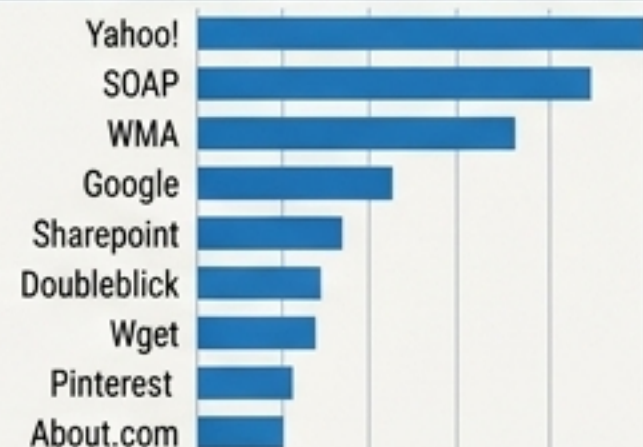


IPS & AMP : Protection anti-malware et détection d'intrusions.

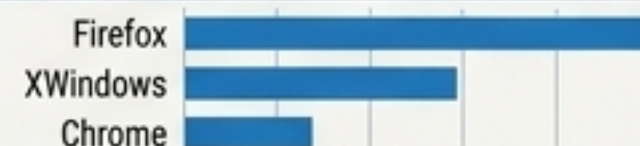
Tableau de bord

Tableau de bord
Tableau de bord session alert

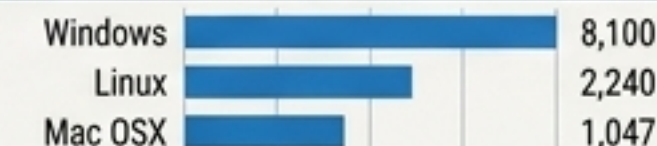
Top Web Applications Seen ▼ Total Bytes (KB)



Top Client Applications Seen ▼ Total Bytes (KB)



Top Operating Systems Seen ▼ Count



Top Server Applications Seen

Vendor	Count
Microsoft-IIS	11,382
Apache	982
ngins	107
Computer Associates	73
Apache-Coyote	58
AmazonS3	21
PWS	17
Omniture DC	16
service.brightcloud.com	11
NNM Release 8.07.53	11

Top Operating Systems Seen

OS Name	Count
Windows	8,100
Linux	2,340
Mac OSX	1,047
+1 Unix	187
-1 Android	185
Chromium	113
Windows Phone	86
AIX	51
FreeBSD	20
ESX	16

Flux d'Exportation

1

Créer une Réponse à une alerte (Syslog, SNMP, Email).

— Paramètres:
Spécifier la réponse (ex: 5514),
et la gravité (ex: ALERT, DEBUG).
Associer ...

2

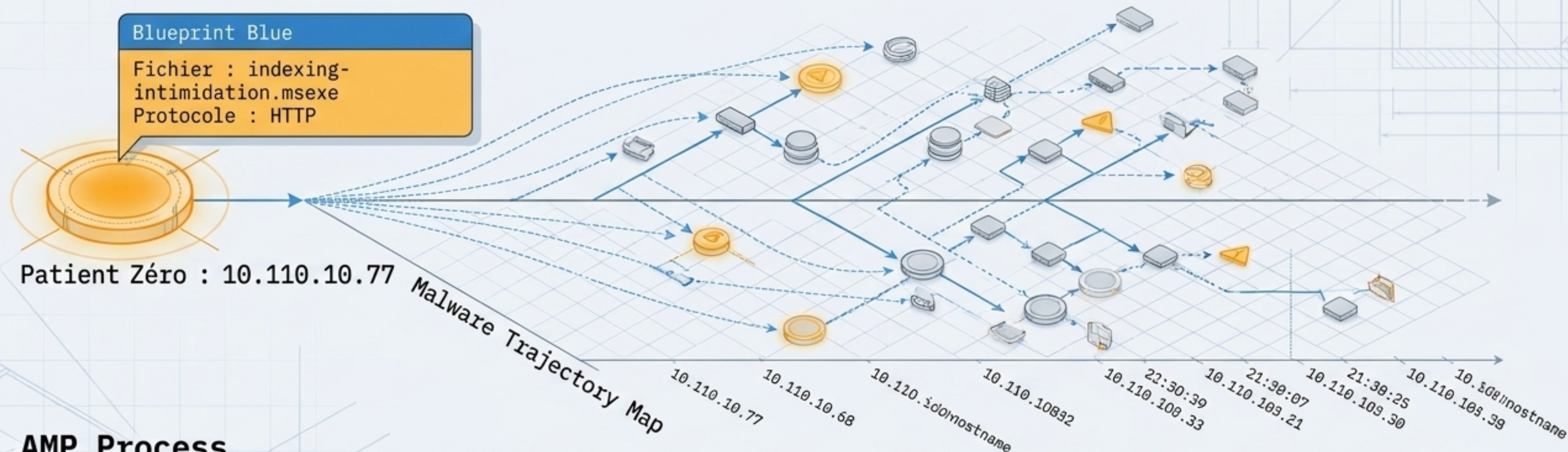
Spécifier le port (ex: 514) et la gravité (ex: ALERT, DEBUG).

— Paramètres:
Spécifier le port (ex: 514),
gravité (ex: ALERT, DEBUG).
Associer ...

3

Associer l'alerte à une politique de contrôle d'accès (onglet Journalisation).

Rétrospection des Menaces : Trajectoire du Patient Zéro



Note : Exporter les événements rétrospectifs vers le SIEM via SNMP/Syslog pour une alerte SOC instantanée.

Sécurité Cloud Hybride : Architecture Cisco Meraki

Les Avantages du Cloud



Déploiement simplifié : Configuration avant réception du matériel.



Mises à jour automatiques : Maintenance du firmware transparente.



Gestion centralisée : Interface web unique (meraki.cisco.com).



Conformité : Chiffrement SSL et certification PCI niveau 1.

Configuration de l'Exportation

○ ○ ○

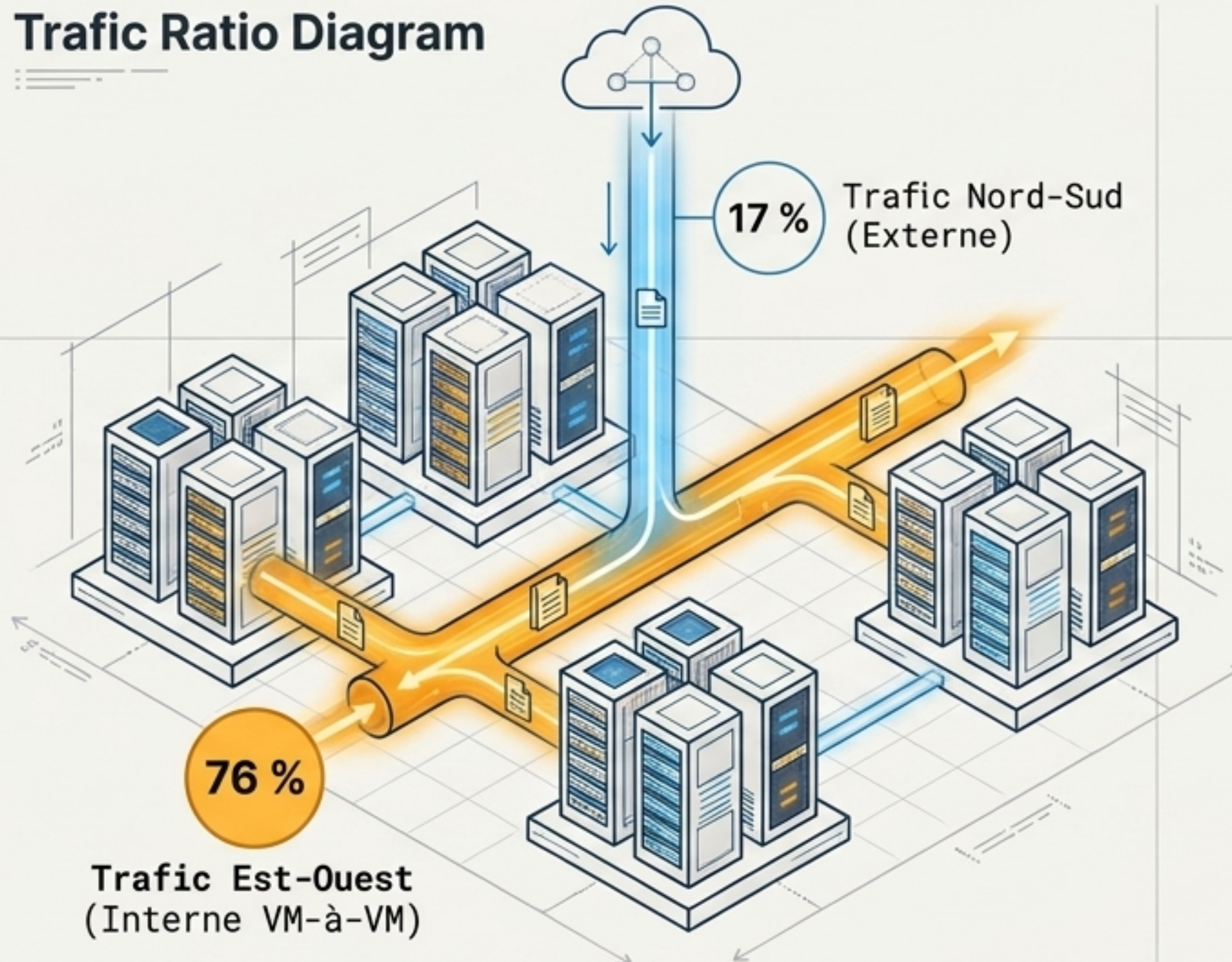
Reporting

Syslog servers

Server IP	Port	Roles	
192.168.1.200	514	Journal des événements Alertes IDS (Sourcefire) URLs ✓ Flux	×

Le Cœur du Centre de Données : Trafic Est-Ouest et Pare-Feu Virtuels

Traffic Ratio Diagram



Attention : La négligence de la sécurité du calcul interne est la faille la plus courante. Un pare-feu de périmètre ne voit pas le trafic Est-Ouest.

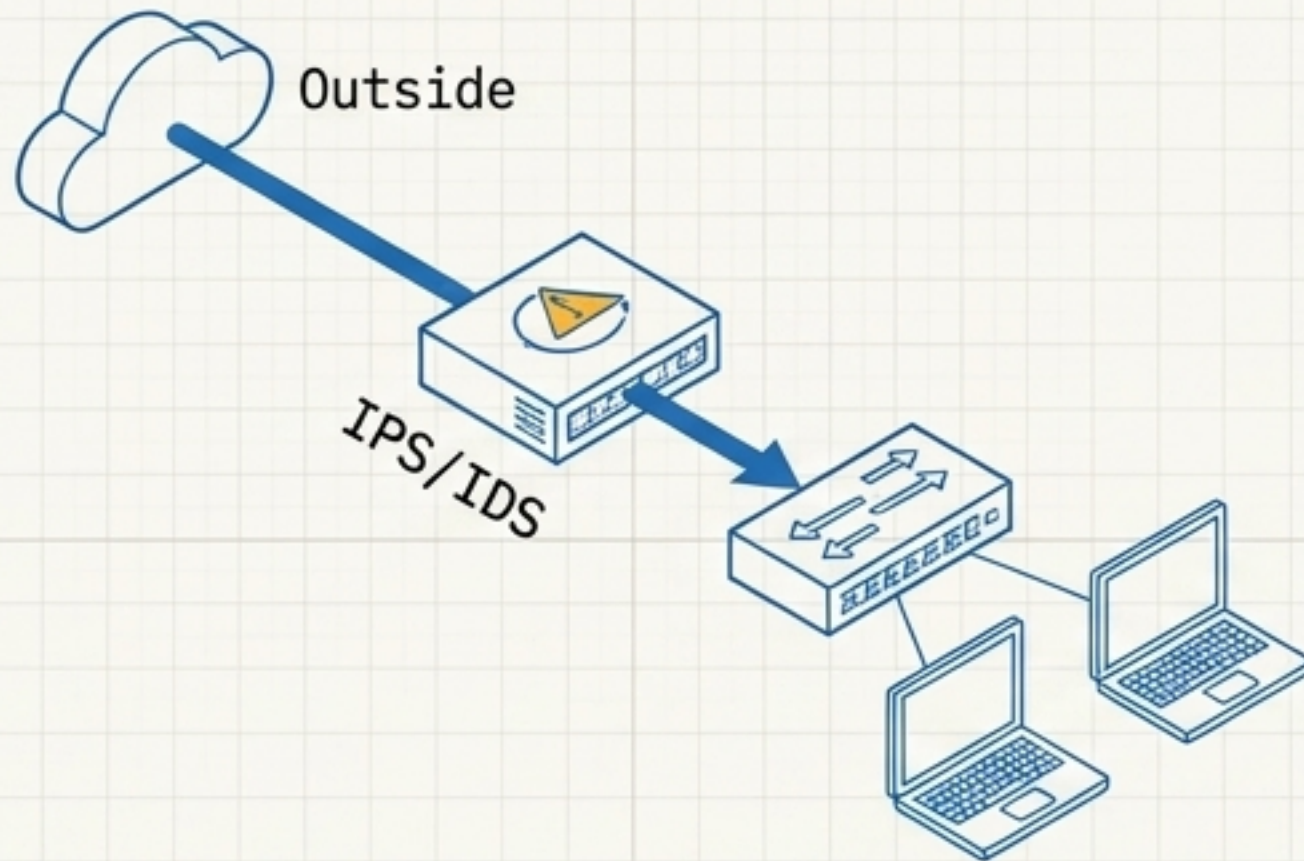


Solutions (Pare-feu Virtuels)

- **Cisco ASAv :** Les capacités complètes de l'ASA optimisées pour les hyperviseurs.
- **Cisco VSG (Virtual Security Gateway) :** Intégré aux commutateurs virtuels (ex: Nexus 1000v) pour segmenter jusqu'au niveau de la machine virtuelle. Exportation gérée via Prime Network Services Controller.

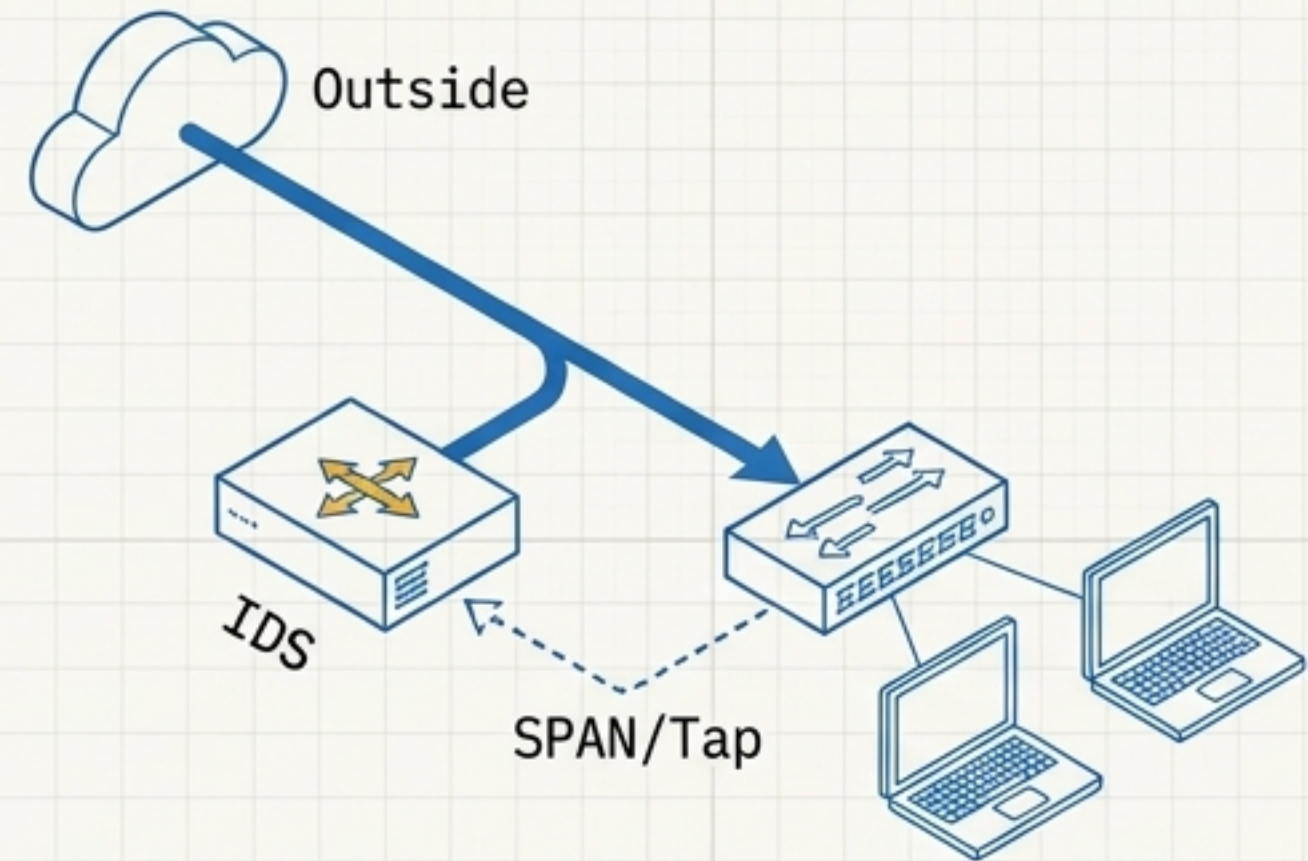
Matrice de Déploiement : IPS vs. IDS

Configuration En Ligne (IPS - Prévention)



Action : Bloquer et alerter. Requis pour stopper les menaces avant pénétration.

Configuration Hors Bande (IDS - Détection)



Action : Surveiller et alerter uniquement.

Moteurs de Détection :

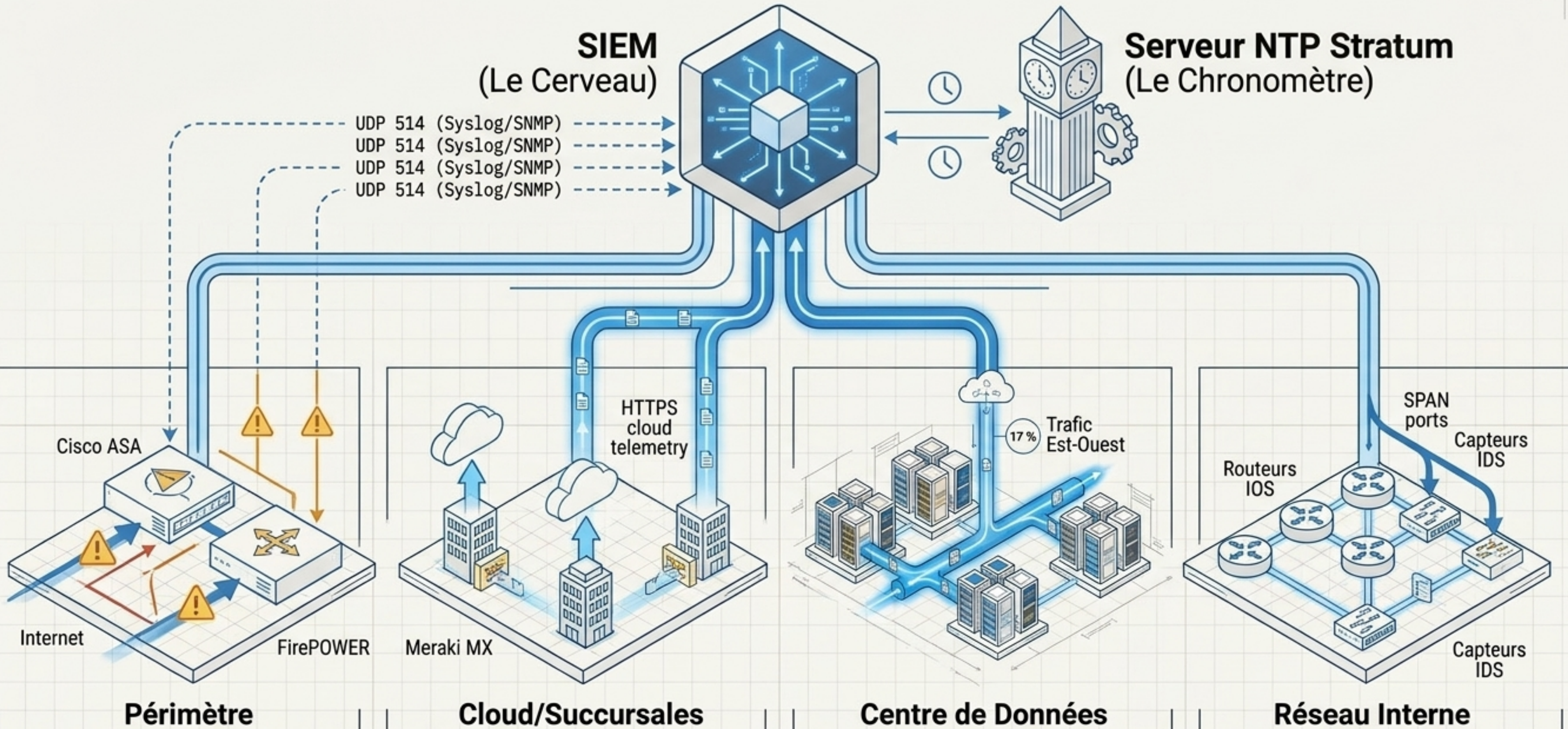
Signature : Modèles d'attaques connus (vulnérable au trafic inconnu/zéro-jour).

Anomalies Statistiques : Écarts par rapport à la ligne de base. (Nécessite un paramétrage fin pour éviter la fatigue des alertes).

SIEM (Le Cerveau)

Serveur NTP Stratum (Le Chronomètre)

UDP 514 (Syslog/SNMP)
UDP 514 (Syslog/SNMP)
UDP 514 (Syslog/SNMP)
UDP 514 (Syslog/SNMP)



La visibilité totale n'est pas un produit, c'est une architecture. L'intégration de la capacité (EPS), de la précision temporelle (NTP) et de capteurs distribués est la seule défense contre l'obscurité du réseau.