

**RAPPEL**

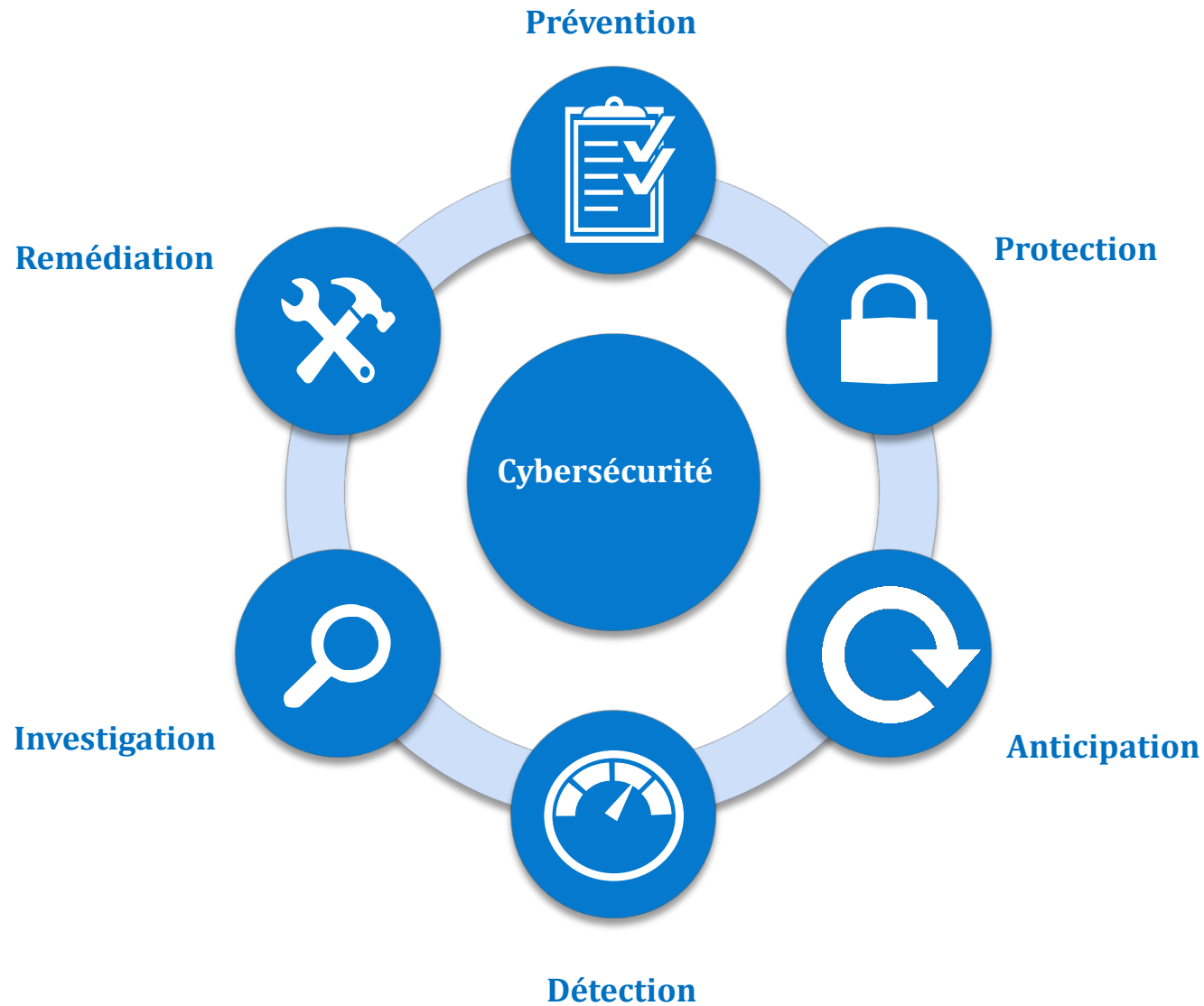
# Connaître les menaces : *Cyber Threat Intelligence*



Nicolas Pierson

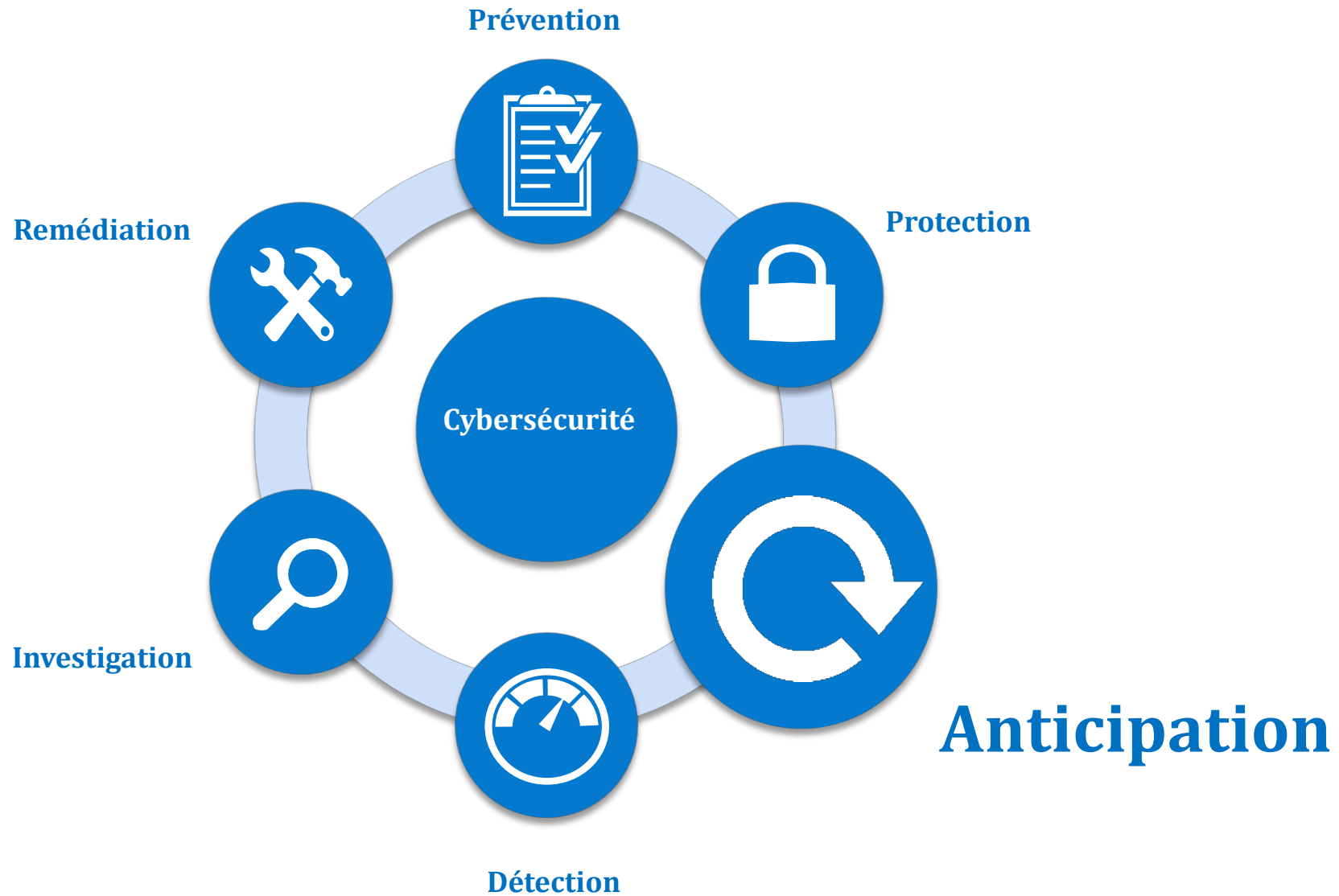
# I. Contexte général

---



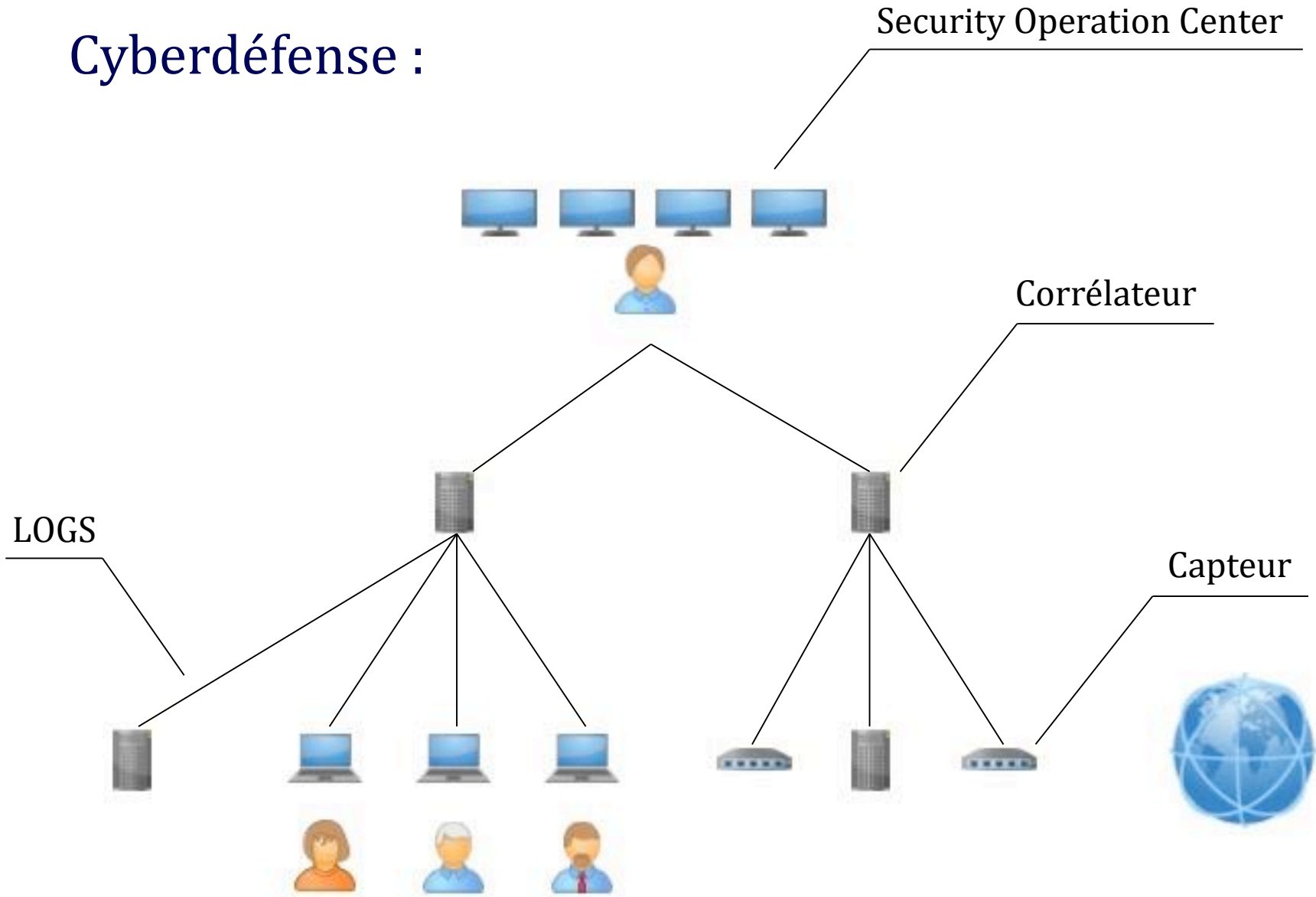
# I. Contexte général

---



# I. Contexte général

Cyberdéfense :



# I. Contexte général

---

**SOC (*Security Operation Center*) ou centre opérationnel de sécurité ou service de détection des incidents de sécurité (PDIS) :**

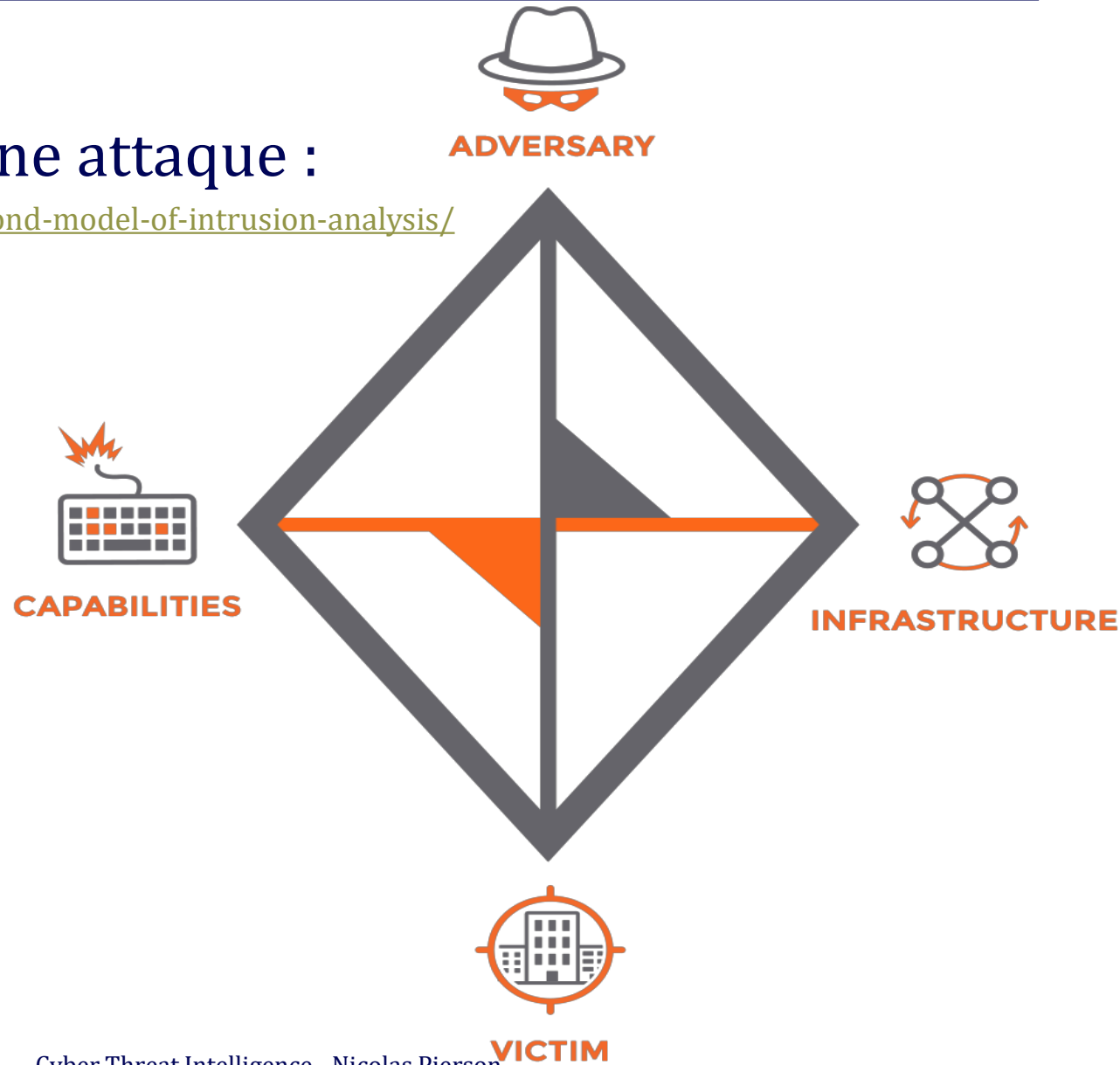
Dispositif de supervision et d'administration de la sécurité des systèmes d'information permettant de détecter et d'analyser les menaces internes et externes et de répondre aux intrusions dans le SI.



# I. Contexte général

## Caractérisation d'une attaque :

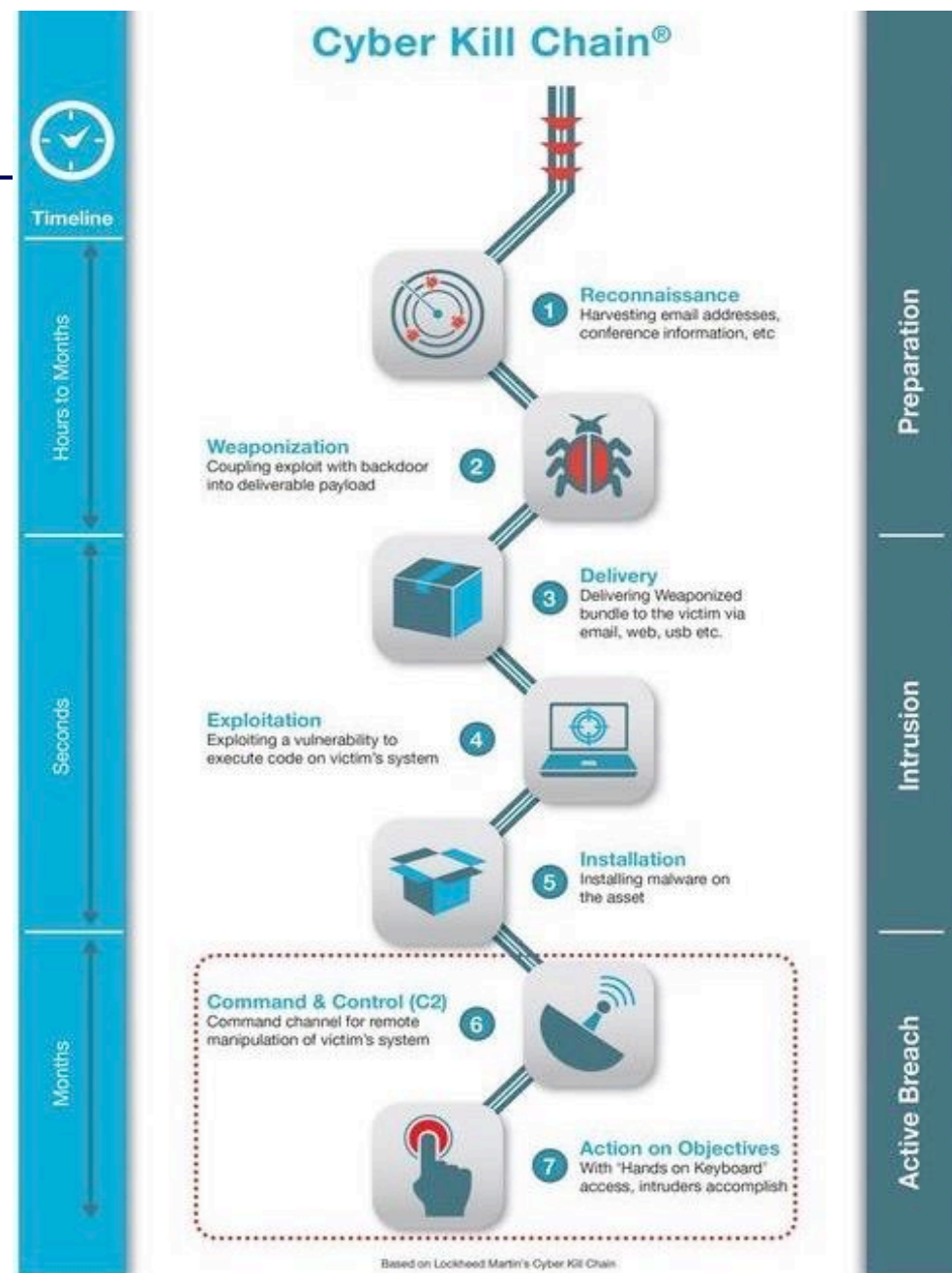
<https://threatconnect.com/tag/diamond-model-of-intrusion-analysis/>



# I. Contexte général

## Cyber Kill Chain :

- ✓ Reconnaissance
- ✓ Préparation
- ✓ Livraison
- ✓ Exploitation
- ✓ Installation
- ✓ Contrôle
- ✓ Action

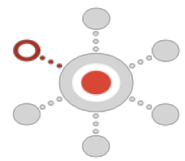


<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>



# II. Cyber Threat Intelligence

---



## Quoi ?

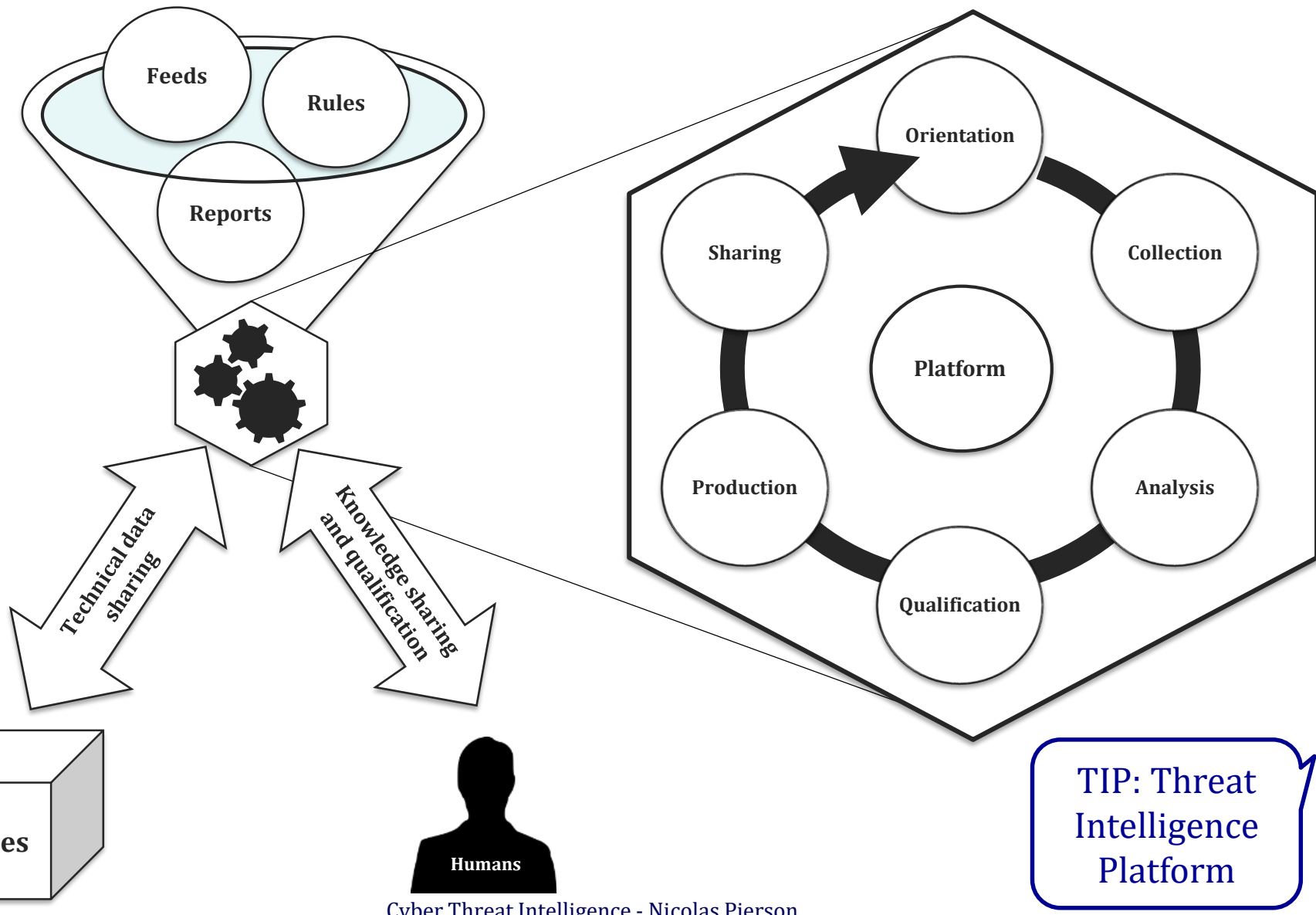
Définition de la Threat Intelligence :

Ensemble des informations et des actions issues de la collecte et de l'analyse des menaces en provenance du cyberspace.

L'objectif de la Threat Intelligence est de connaître les menaces pour s'en défendre efficacement.

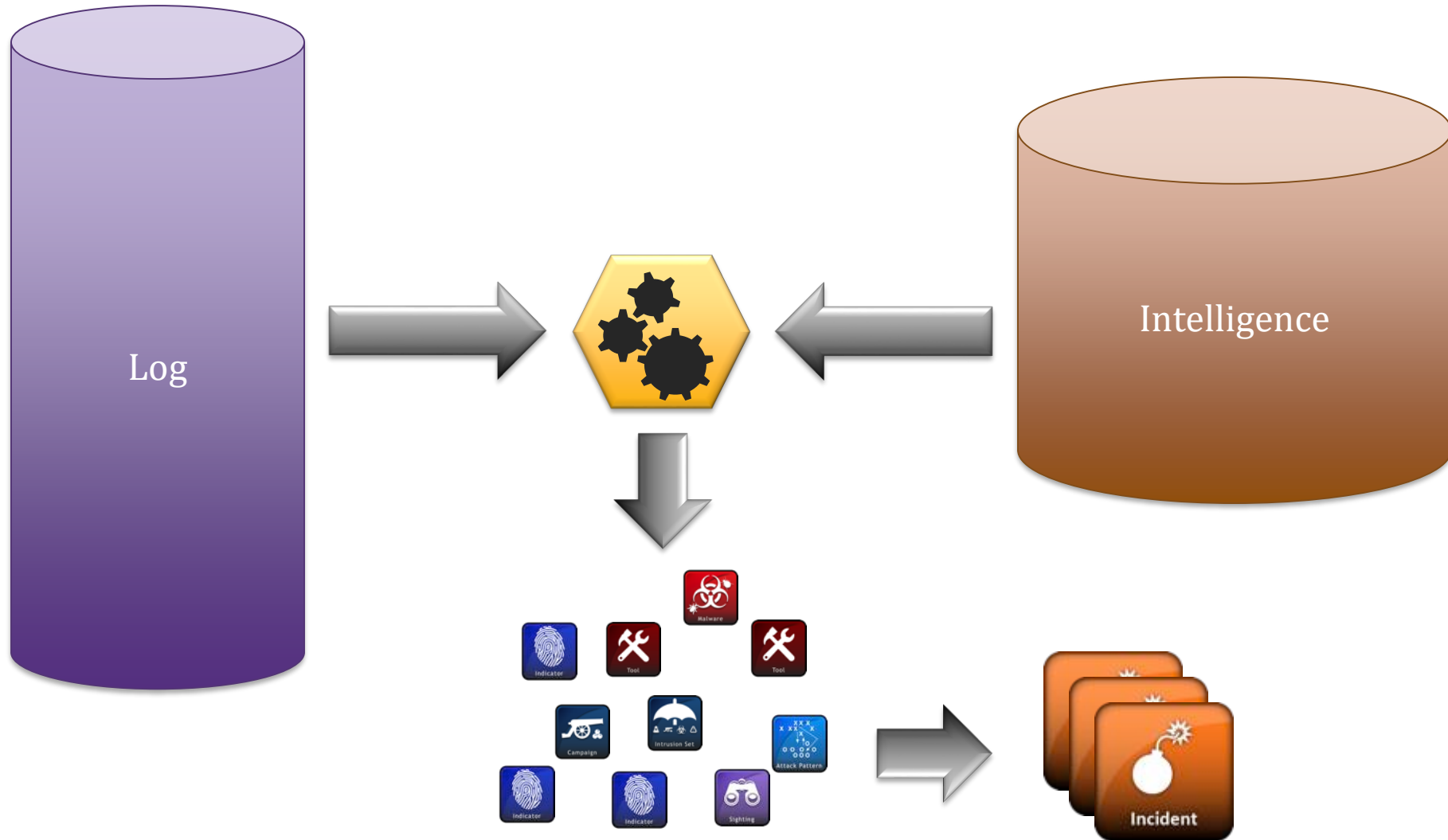


# II. Cyber Threat Intelligence



# III. Perspectives

Recherche/hunting :



# Conclusion

---

- ✓ **Cyber Threat Intelligence =**  
**Des outils + des hommes + des processus**
  
- ✓ **Cyber Threat Intelligence = ART :**
  - **Accurate**
  - **Reliable**
  - **Timely**

# TP :

---

## **Objectif :**

Utiliser & produire de la Threat Intelligence

## **Scénario :**

Vous êtes analystes au sein d'un SOC du ministère des armées.

Le centre d'analyse et de lutte informatique défensive vous a envoyé par mail un rapport d'analyse sur une campagne en cours : Banacry

Sur la base de ce compte rendu, vous mènerez une investigation et produirez, le cas échéant, un rapport d'analyse.








# Modalités pratiques

---

- Accès au SIEM du SOC (instance Splunk)
- Par binôme
- Production d'un rapport d'incident (noté)
  - ✓ Résumé de l'attaque
  - ✓ Détail de l'analyse
  - ✓ Annexe contenant les IOC identifiés
- Échéance pour le rapport : 18 février 2020
- CR à [nicolas.pierson@for-cyb.com](mailto:nicolas.pierson@for-cyb.com)

# Découverte des logs

Bluecoat : Proxy web  
cisco:esa : Passerelle Mail  
fgt\_traffic : Firewall réseau  
linuxsecure : Infos  
d'authentification Linux  
portcontrol : Branchement  
support amovible  
streammysql : Ecoule  
réseau et interprétation  
protocolaire de SQL  
winhostmon : Infos de  
création de process  
Windows

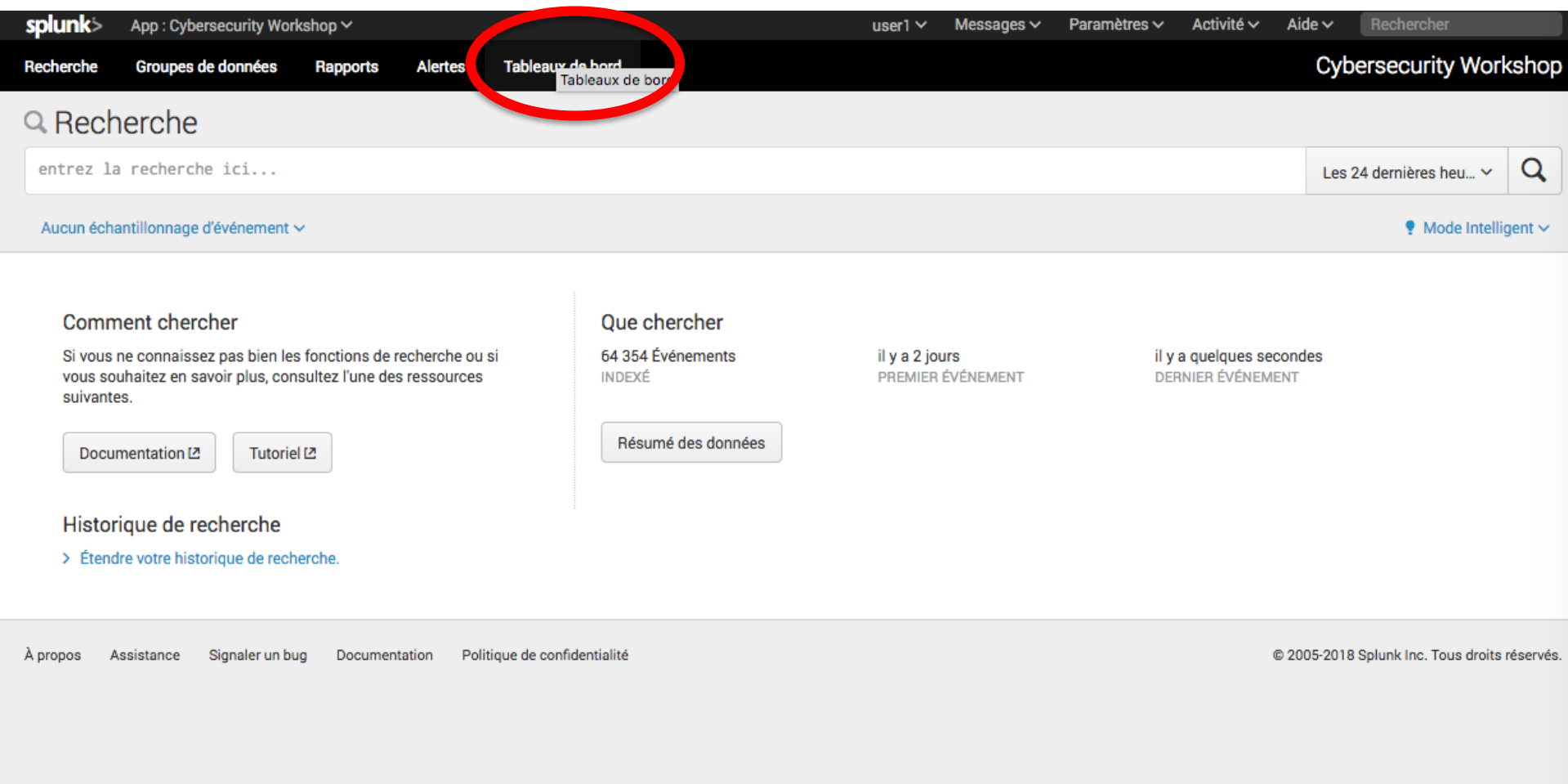
Résumé des données			
Hôtes (6)	Sources (1)	Sourcetypes (7)	
filtre			
Type de source		Nombre	Dernière mise à jour
bluecoat		97,395	15/02/17 16:33:44,000
cisco:esa		13,458	15/02/17 16:33:04,000
fgt_traffic		167,057	15/02/17 16:33:45,000
linuxsecure		29,719	15/02/17 16:33:39,000
portcontrol		1,109	15/02/17 16:33:04,000
streammysql		7,776	15/02/17 16:33:25,000
winhostmon		31,552	15/02/17 16:33:40,000

# Création de tableaux de bord

The screenshot displays the Splunk Enterprise web interface. At the top, a navigation bar includes the 'splunk' logo, a user dropdown (user1), and links for Messages, Paramètres, Activité, Aide, and a search bar (Rechercher). The left sidebar contains a list of applications: 'Apps' with a gear icon, 'Search & Reporting' with a right arrow icon, and 'Cybersecurity Workshop' with a headset icon, which is circled in red. Below these is a dashed box with a plus sign. The main content area is titled 'Explorer Splunk Enterprise' and features four green circular icons with corresponding text: 1. 'Présentations des produits' (New on Splunk? Discover our presentations.) 2. 'Ajouter des données' (Add or transmit data to Splunk Enterprise. You can then [extract fields](#).) 3. 'Explorer les données' (Explore the data and define how Hunk analyzes the data.) 4. 'Splunk Apps' (Applications and extensions develop Splunk Enterprise capabilities.) At the bottom, a large dashed box contains faint icons of various data visualizations like bar charts, line graphs, and tables. A 'Fermer' button is located in the top right corner of the main content area.



# Création de tableaux de bord



splunk> App : Cybersecurity Workshop ▾ user1 ▾ Messages ▾ Paramètres ▾ Activité ▾ Aide ▾ Rechercher

Recherche Groupes de données Rapports Alertes **Tableaux de bord** Tableaux de bord

Cybersecurity Workshop

Recherche

entrez la recherche ici...

Les 24 dernières heures ▾ 🔍

Aucun échantillonnage d'événement ▾ Mode Intelligent ▾

**Comment chercher**

Si vous ne connaissez pas bien les fonctions de recherche ou si vous souhaitez en savoir plus, consultez l'une des ressources suivantes.

Documentation 🔗 Tutoriel 🔗

**Que chercher**

64 354 Événements INDEXÉ

il y a 2 jours PREMIER ÉVÉNEMENT

il y a quelques secondes DERNIER ÉVÉNEMENT

Résumé des données

**Historique de recherche**

> Étendre votre historique de recherche.

À propos Assistance Signaler un bug Documentation Politique de confidentialité

© 2005-2018 Splunk Inc. Tous droits réservés.

# Création de tableaux de bord

Créer un nouveau tableau de bord

Titre

facultatif

ID?

Ne peut contenir que des lettres, des nombres et des underscores.

Description

facultatif

Permissions

Privé

Partagé dans l'...

Annuler

Créer un tableau de bord

# Au travail !

---





Contact : [nicolas.pierson@for-cyb.com](mailto:nicolas.pierson@for-cyb.com)