

**"Détection , supervision et traitement  
des évènements de sécurité".**

# Quelle est votre couleur préférée ?

Une "**Red Team**" est concentrée sur les tests de pénétration des systèmes d'informations en mode éthique. Elle n'est pas incluse dans le fonctionnement du système d'informations et ne connaît pas les défenses en place.

Une "**Blue Team**" est concentrée sur l'amélioration continue de la sécurité du S.I. dans laquelle elle est incluse. Elle est impliquée dans la recherche des menaces et l'analyse d'incident.

Les deux sont complémentaires dans leurs actions et inter-agissent.

# Non merci, je préfère le violet

Une "**Purple Team**" a pour ambition d'améliorer le travail des Red et des Blue Team. Elles peuvent être temporaires et jouer un rôle de médiation ou d'oeil extérieur avec les deux autres équipes. Elle se focalise sur les évolutions des menaces, des technologies mais aussi des métiers des clients dans un rôle de vigie.

Ce cours est orienté "Blue Team".

# Deux grands domaines de la supervision et la détection des incidents.

- Le "**Network Security Monitoring**"\*\* est une discipline mêlant les aspects instrumentation réseau (collecte de trafic) et détection d'intrusions, essentiellement via des NIDS (**Network Intrusion Detection Systems**).
- Le "**Host Intrusion Detection S** est orienté "machine" et s'appuie sur les traces (logs) de ces dernières.

# Définitions

- "**Threat Hunting**" ou chasse aux cyber-menaces est une activité de défense active. Il s'agit de détecter des "**Advanced Persistent Threats**" ou menaces sophistiquées et persistantes dans la durée.
- "**Network FORENSICS**": cette activité désigne l'étude postmortem des traces réseaux après un incident de sécurité.
- **Détection d'intrusion**: il s'agit en temps réel de détecter et identifier des attaques déjà connues ou des anomalies.

# Deux modes de détection:

- Par **scénario**: il s'agit de reconnaître la signature d'une attaque en recherchant des chaînes de caractères dans les flux des données transitant sur le réseau. On peut choisir de "reconnaître et/ou de bloquer" (**Intrusion Detection System** versus **Intrusion Prevention System**).
- Par **comportement**: Il s'agit de détecter des changements dans le trafic (par exemple par analyse en composantes principales ou à l'aide des outils de type "machine learning").

# Méthodologie avec OSCAR

- Obtain Information: Réunion des informations factuelles (dates, heures, personnes, lieux...)
- Strategize: Priorisation des acquisitions des ressources pour l'analyse post-mortem et des moyens humains et informatiques alloués.
- Collect evidence: Les preuves sont collectées des sources priorisées mais avec méthode. Les traces doivent permettre de retrouver sa source, avec un horodatage et des mesures pour éviter les corruptions...

# Méthodologie avec OSCAR (suite)

- **Analyse:** C'est la période où on utilise divers outils et méthodes en fonction des traces recueillies.
- **Report:** Il s'agit de produire un rapport pour le client, mais intelligible par une personne non experte (juges par exemple).

Il faut réaliser une "**timeline**" comme dans la série "ColdCase", afin de bien clarifier les lieux et le déroulement des actions et comprendre ce qu'il s'est passé.

# Les bonnes questions pour créer sa "timeline"

- "Quand est ce cette machine a été infectée?"
- "Combien de fois cet utilisateur a-t-il accédé ou tenté d'accéder à ce service ?"
- "Quand est ce que cet utilisateur a-t-il accédé à ce fichier ?"
- "Depuis combien de temps ce fichier est-il dans la directory ? le stockage est-il compatible avec le niveau de confidentialité ?"
- "Quand est-ce que l'attaquant a-t-il pénétré notre réseau ?"
- "Combien de temps l'attaquant as-t-il mis pour s'introduire dans ce système ?"

# Les questions auxquelles on veut répondre lors de l'analyse

- Qui est impliqué ?
- Que s'est il passé ?
- Dans quels endroits?
- Pourquoi est-ce arrivé ?
- Comment est-ce arrivé ?

# Les conséquences que l'on veut mesurer

- Depuis quand l'activité malveillante s'exerce-t-elle ?
- Cette activité malveillante est-elle terminée ?
- Quels systèmes ont été corrompus ou infiltrés ?
- Quelles sont les données récupérées ou modifiées ?
- Parmi ces données lesquelles sont importantes ou confidentielles ?

# Les sources de détection

- Sniffing & PCAP & Netflow (Utilisation de TAP)
- Table CAM d'un switch
- Table de routage
- Logs DHCP, DNS et service réseaux...
- Logs systèmes (EVT, Rsyslog)
- Log IPS/IDS
- Logs des firewall
- Logs des proxy

...

# Les outils historiques de "*threat hunting*"

**Sniffers:** Wireshark, tcpdump

**Collecteurs & aggrégateurs** NetFlow: nfsen,  
**nfpcap, argus** 😊

# Définition des IDS et IPS

Un IDS détecte des "motifs d'attaques" dans les trames réseaux et implémentés sous forme de signature. L'IPS est le pendant armé de l'IDS et va bloquer les IP qui ont levé une alerte.

Ce type d'outil est moins efficace avec la généralisation du chiffrement mais est capable de donner des éléments sur les flux réseaux des attaquants. A ce titre il est toujours utile.



## Outils IDP/IPS: **Snort!**

C'est un IDS historique. A ce titre le format de ses règles est un standard y compris pour son concurrent Suricata. Racheté par Cisco, il a été ré-écrit (version 3) pour des raisons de performance (multi-threading et inspection http entre autre).



## Outils IDP/IPS: Suricata

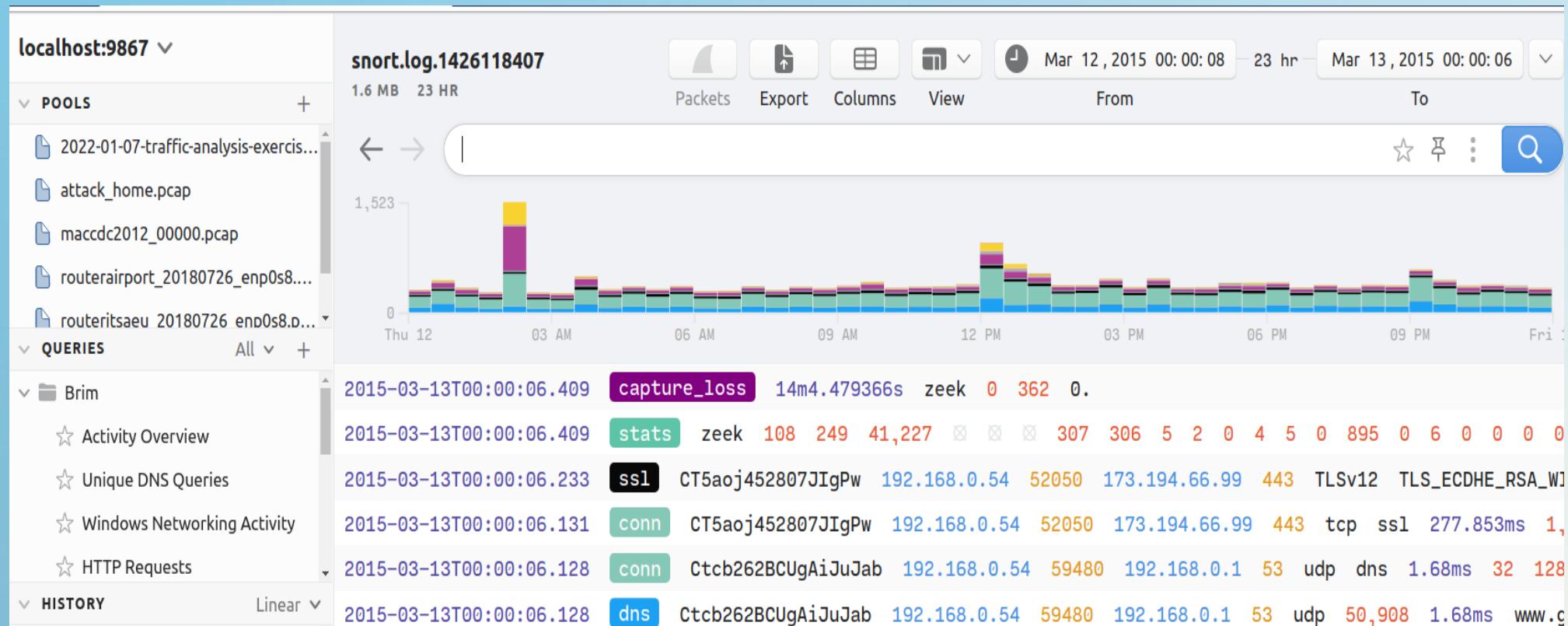
Plus récent (2009) que SNORT il a bénéficié d'une architecture modulaire et multi-threadé dès sa conception. C'est un outil intégré dans beaucoup d'autres du fait de son positionnement "opensource". Il ne sert pas qu'à la détection mais il capable aussi



## **ZEEK est un analyseur comportemental du trafic**

Zeek (ex Bro) est un peu à part des deux précédents IDS/IPS. Il est capable d'analyse protocolaire. Programmable (conception évènementielle), il est hautement adaptable. IMHO un bon complément aux deux autres.

# Brim ❤️ est un client qui lit et "parse" rapidement de gros fichiers au format pcap



# Brim embarque Suricata et affiche ses alertes

The screenshot shows the Brim application interface. On the left, there is a sidebar with a dropdown menu set to "localhost:9867". Below it are two sections: "POOLS" containing files like "2022-01-07-traffic-analysis-exercis...", "attack\_home.pcap", and "maccdc2012\_00000.pcap"; and "QUERIES" containing star icons and labels such as "HTTP Post Requests", "Show IP Subnets", "Suricata Alerts by Category", "Suricata Alerts by Source and ...", and "Suricata Alerts by Subnet".

The main area is titled "snort.log.1426118407" and shows a log entry from March 12, 2015, at 00:00:08. The log file size is 1.6 MB and has been analyzed for 23 hours. There are four buttons: "Packets", "Export", "Columns", and "View". A timestamp "Mar 12, 2015 00:00:08" is also present.

A search bar contains the query: `event_type=="alert" | alerts := union(alert.category) by src_ip, dest_ip`.

The results table has columns: "src\_ip", "dest\_ip", and "alerts". The data is as follows:

src_ip	dest_ip	alerts
108.160.162.76	192.168.0.54	[[Potential Corporate Privacy Violation]]
95.154.26.34	192.168.0.2	[[Generic Protocol Command Decode]]
108.160.170.50	192.168.0.54	[[Potential Corporate Privacy Violation]]
192.168.0.54	65.55.54.42	[[Misc activity, Unknown Traffic]]
108.160.165.211	192.168.0.54	[[Potential Corporate Privacy Violation]]
108.160.165.84	192.168.0.54	[[Potential Corporate Privacy Violation]]
108.160.167.35	192.168.0.54	[[Potential Corporate Privacy Violation]]

# "Open Source", Brim s'appuie sur des données super-structurées formant un "data-lake", "parsable" avec un outil zq (modèle en "pipe" comme jq)

snort.log.1426118407  
1.6 MB 23 HR

Packets Export Columns View Mar 12 , 2015 00:00:08 - 23 hr Mar 13 , 2015 00:00:06 From To

← → method=="POST" | cut ts, uid, id, method, uri, status\_code | sort id.resp\_p

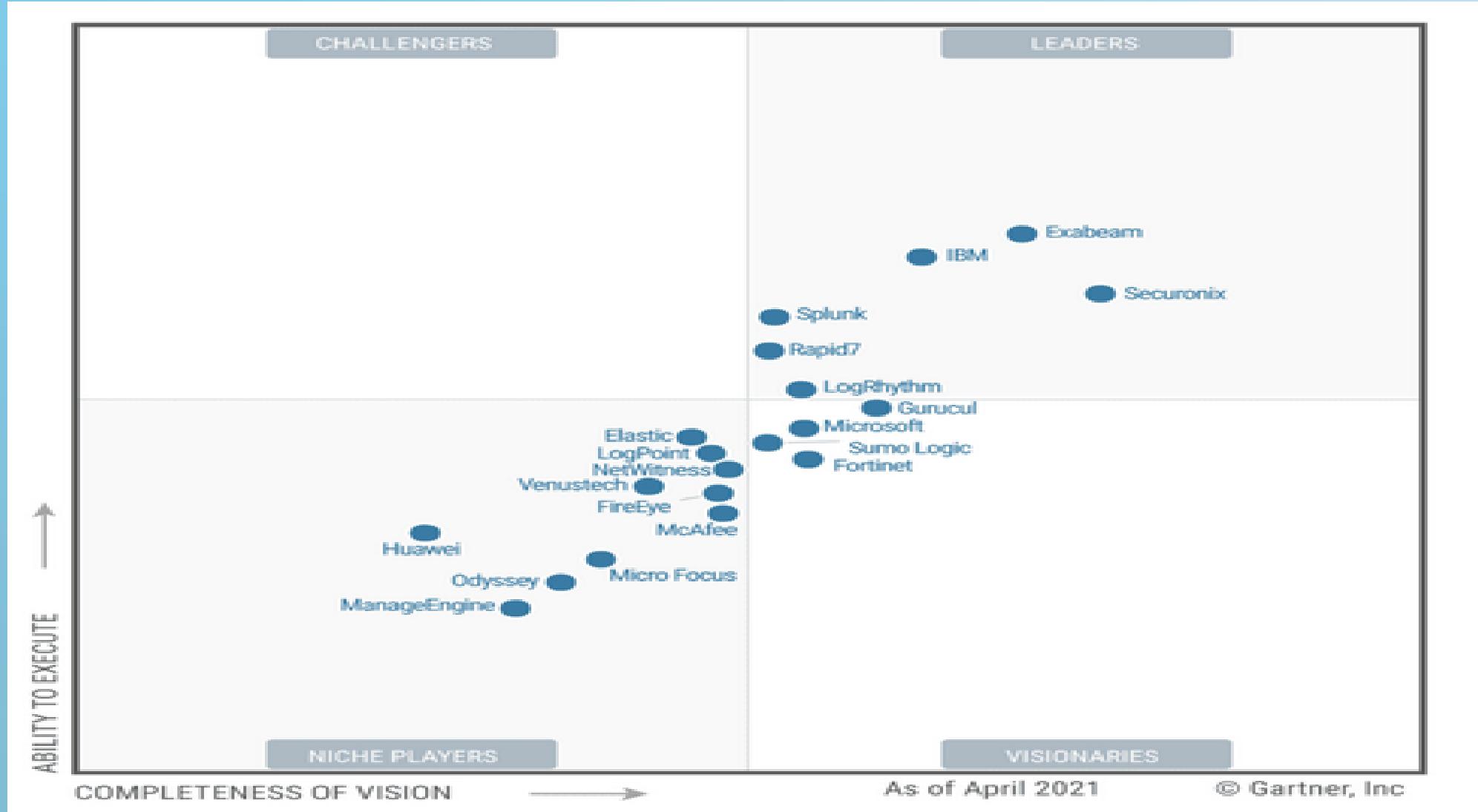
Star Print More Search

uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	method	uri
CI0Tqn2MKb8heZrczh	217.195.49.146	54331	192.168.0.2	80	POST	/skyblue/index.php?pid=4
Cn6gUH1nt3CNrLncj1	217.195.49.146	54314	192.168.0.2	80	POST	/skyblue/index.php?pid=4
ChgT0tHLen9zgs8c1	217.195.49.146	54312	192.168.0.2	80	POST	/skyblue/index.php?pid=4
CE4RNT2M4Wj3JbS04k	217.195.49.146	54311	192.168.0.2	80	POST	/skyblue/index.php?pid=4
C16Tvmeq98ydW4xo8	217.195.49.146	54304	192.168.0.2	80	POST	/skyblue/index.php?pid=4
CR1cH5AzLKIrx9r	217.195.49.146	54302	192.168.0.2	80	POST	/skyblue/index.php?pid=4

# Les SIEM (Security Information and Event Management)

- La détection et la neutralisation des menaces demandent de corrélérer les informations de multiples sources.
- C'est la promesse du **SIEM** qui est utile en particulier dans les S.O.C ("Security Operation Center"). L'évolution des SIEM se fait comme dans d'autres secteurs de l'I.T. vers le **CLOUD** et l'**I.A.**.

# La concurrence est rude sur ce segment



# Les "10 commandements du SIEM"

(source "no limit sécu" épisode 334 avec Etienne Ladent et Thomas Burnouf)

1. Des relais de collecte de logs indépendants tu mettras => pour avoir un tampon de données avant le SIEM et éviter le DOS involontaire , la perte, filtrer et diminuer les coûts)
2. Les "regex" tu apprendras" => pour retrouver efficacement des motifs. Un savoir-faire des analystes.
3. Le "zéro alerte" tu viseras => "Trop d'alertes tue l'alerte". Paradigme bien connu en supervision et ailleurs.

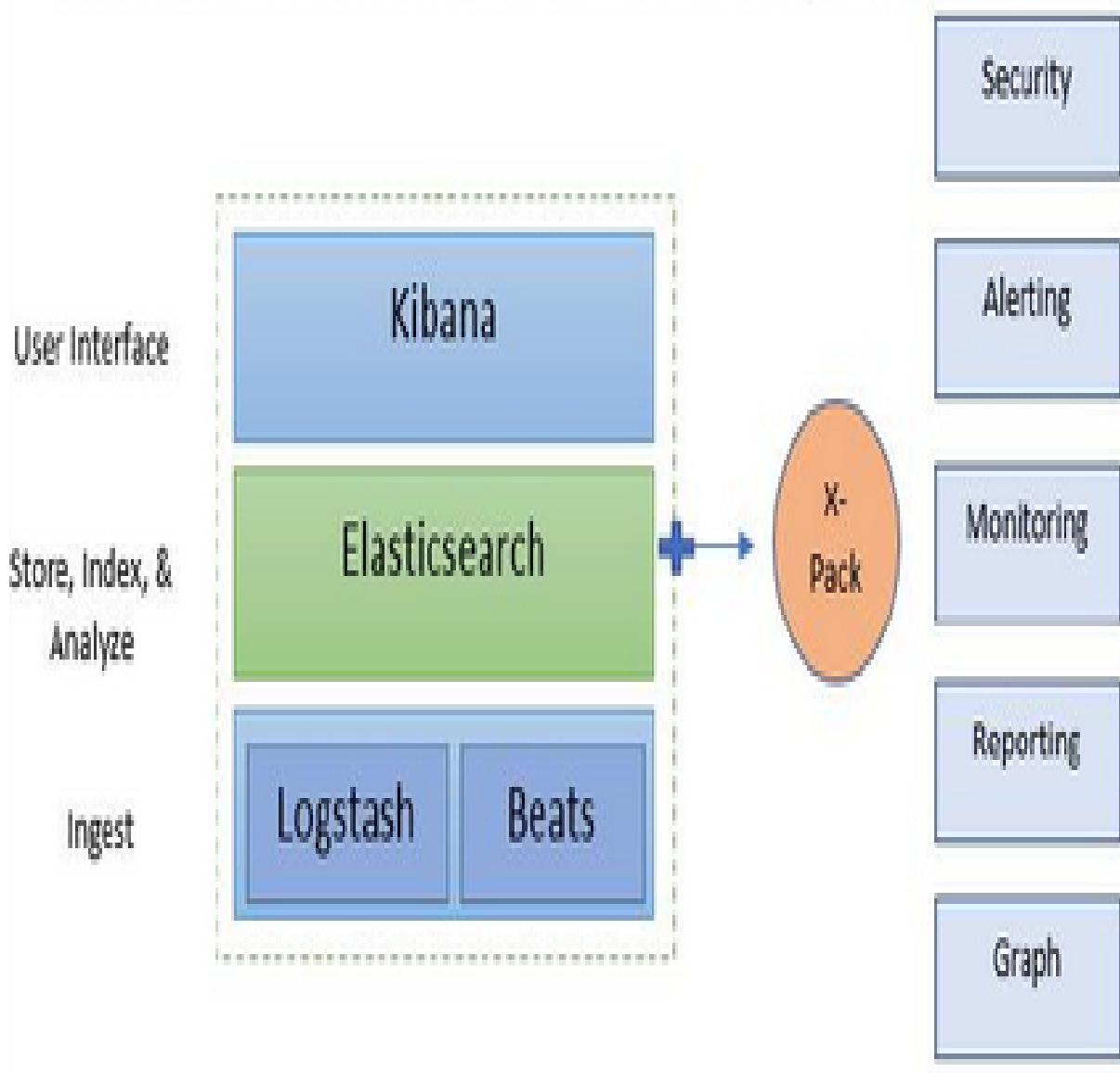
## Les "10 commandements du SIEM"

4. Tes données d'inventaire tu collecteras => un analyste a besoin de ces données d'inventaire pour être efficace.
5. Sur tes données utilisateurs tu formeras => Il faut comprendre les métiers).
6. Sur tes alertes tu contextualiseras => (Dans l'esprit d'EBIOS le métier oriente l'analyste et peut donner du sens à l'attaque).
7. Sur tes recherches tu refléchiras => les ressources sont limitées et un analyste ne doit pas les monopoliser.

## Les "10 commandements du SIEM"

8. Tes alertes régulièrement tu contrôleras => revue des alertes suite à l'évolution du SI et des formats logs qui les rendent obsolètes == MCO
9. Tes données tu documenteras => évident.
10. Tes noms de données tu nommeras. (Un modèle de référence "Splunk Information Model" ) pour nommer de façon cohérente.

# **Wazzuh & OSSEC**



## Stack "Elastic"

- Elastic Search stocke les données sur un cluster de plusieurs noeuds
- La suite beats extrait des informations des fichiers de Log (Filebeat), du processus d'audit (Auditbeat), du traffic réseau (Packetbeat), ...

# "Elastic Search"

- C'est un moteur de recherche et d'analyse , accessible en mode "RESTfull" et distribué.
- IL stocke des informations au format JSON.
- Il est performant pour des recherches textes et permet l'indexation de documents non structurées.
- Ses capacités permettent à son utilisateur de trouver des informations via Curl ou au travers de son API.

# Logstash versus Beats

- C'est aussi un composant "Server Side" historique comme "Elastic Search". Écrit en JRuby (lent au démarrage et gourmand), il est important dans fonction ETL (transformation des données avec des regex standardisées).
- Les composants de Beats sont orientés "Client Side" et peuvent alimenter directement "Elastic Search". La "LibBeat" sert de base commune.

## X-Pack

- Il ajoute les fonctions de sécurité, de monitoring , de supervision , de reporting et de "machine learning". Cette dernière fonction est payante et a pour but de détecter des comportements anormaux.
- Complété par "Elastic Agent" qui permet d'enrouler un client et FLEET qui permet de les gérer de façon centralisé on a une solution de type SIEM.

## "Endpoint Protection Platform" et les "Endpoint Detection and Response"

Ces composants permettent de combiner la protection du poste de travail avec la détection et la remédiation en cas d'alerte virale. Ils sont chargés de la protection des équipements terminaux (pc, smartphone ..):

- Les **EPP** sont des antivirus avec des fonctionnalités de prévention des menaces.
- Les **EDR** sont orientés sur le détection comportementale via l'**IA**, la surveillance de la mémoire et la présence d' "Indicateurs de Compromissions" (**IoC**).

## "Dans la famille acronyme il y a":

- SOC: "**S**ecurity **O**peration **C**enter.
- NDR: "**N**etwork **D**etection and **R**esponse.
- EDR: "**e**xtended **D**etection et **R**esponse".
- CIRT: "**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam.
- SOAR: "**S**ecurity **O**rchestration **A**utomation and **R**esponse".
- MDR: "**M**anagement **D**etection and **R**esponse".

## Si vous voulez être incompris par les "moldus"

- Le **NDR** est le processus de haut niveau qui apporte une visibilité à l'échelle du réseau aux équipes **CSIRT** du **SOC** afin de détecter les comportements malveillants au niveau des infrastructures. Il ne s'occupe donc pas des points terminaux dévolus aux **EPP/EDR**.
- Le **XDR** réunit **NDR** et **EPP**.
- Le **MDR** regroupe les solutions managées qui permettent d'automatiser et de fluidifier au travers du **SOAR** la réponse aux incidents.

# Elastic Siem fait partie de Kibana

**Kibana** est le front end de la suite Elastic et permet de déployer des tableaux de bord. Certains sont orientés sécurité et constituent un SIEM.

La corrélation est possible par adjonction d'une TimeLine.

## R5.cyber.11 Supervision de la sécurité

**MA TIMELINE** Autosaved 21 seconds ago

Processes: 0 Users: 0 Hosts: 0 Source IPs: 1 Destination IPs: 1.168k

Add to favorites Attach to case

MA TIMELINE

Query 333338 Correlation Analyzer Notes 1 Pinned

Feb 25, 2022 @ 22:15:52.341 → Feb 26, 2022 @ 22:15:52.341 Refresh Data view

( \_id: "8QPjN38BKJEtSBKk2SMz" )

OR ( source.ip: "192.168.1.25" )

OR ( ) + Add field

Filter Search KQL

+ Add filter

UI icons: @timestamp ↓ 1 message event.category event.action host.name source.ip

# Comment tester son SIEM ?

En se basant sur framework Mitre des techniques d'attaques observées.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (2/8)	Account Manipulation (2/4)	Abuse Elevation Control Mechanism (2/4)	Abuse Elevation Control Mechanism (2/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1/15)	Boot or Logon Autostart Execution (1/15)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (1/5)	Boot or Logon Initialization Scripts (1/5)	Build Image on Host
Gather Victim Org Information (0/4)	Establish Persistence (0/4)	Extract Data (0/1)	File Raise Privileges (0/1)	File Replace (0/1)	File Replace (0/1)	Deobfuscate/Decode Files or Information (0/1)

```
> pwsh
PowerShell 7.2.1
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS /root> Invoke-AtomicTest T1046
PathToAtomicsFolder = /root/AtomicRedTeam/atomics

Executing test: T1046-1 Port Scan
Done executing test: T1046-1 Port Scan
```

- On utilise des outils comme ceux d'**Atomic RedTeam** qui vont tester les défenses d'un hôte afin d'en vérifier la conformité.
- On peut aussi rejouer des pcaps qui contiennent des traces des tentatives d'intrusion.

# HoneyPot qui mal y pense...

- Une façon de détecter les intrusions réseaux et d'analyser les évolutions des attaques c'est de mettre en place un **Honeypot**.
- Les honeypots à faible interaction offrent de faux services et n'offrent que peu de privilèges à l'attaquant.  
L'interaction avec l'attaquant est faible. Simple à mettre en oeuvre ils sont limités et recueillent les attaques automatisées et sans intelligence.
- Au contraire les honeypots à forte interaction permettent à l'attaquant d'aller loin dans son parcours, avec à la clef une analyse en profondeur du mode d'attaque.

**TPOT** combine de nombreux honeypots implémentés sous forme de containers Docker. Il donne des renseignements comme ici une URI de téléchargement d'un logiciel malveillant:

The screenshot shows the TPOT dashboard interface. At the top, there's a navigation bar with a menu icon, a teal 'D' button, a 'Dashboard' button, the current section 'Cowrie', and a refresh icon. Below the navigation is a search bar with a magnifying glass icon and the placeholder 'Search'. Underneath the search bar is a filter input field containing the text 'url.keyword: http://179.43.175.170/putkite/quickr1n.sh' with a close button 'X' and a '+ Add filter' link. The main area is titled 'Cowrie Attacks Bar' and features a large red rectangular bar. To the right of the bar is a legend with two items: a pink circle next to 'Attacks' and a blue circle next to 'Unique Src IPs'. The bottom right corner of the slide contains the number '39'.

# "Only for your eyes"



## Bibliographie:

- Hands-On Network Forensic - auteur Nipun Jaswal- Packt
- Learning Elastic Stack 7.0 - Second Edition Shukla, Pranav Kumar M N, Sharath Packt
- Introduction to Network Forensics FINAL VERSION 1.1 ENISA
- Définitions [soc-siem-xdr-mdr](#) par Orange Cyberdéfense