

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

Problématique

"L'interconnexion croissante des réseaux et les besoins de dématérialisation exposent les systèmes d'information à des cyberattaques. Ainsi les points d'interconnexion avec l'extérieur et en particulier avec internet sont autant d'accès qu'un attaquant peut tenter d'exploiter pour s'introduire et se maintenir au sein d'un système d'information pour dérober, dénaturer ou détruire son patrimoine informationnel"

source: référentiel ANSSI des Prestataire de Détection des Incidents de Sécurité (PDIS)**

La réponse aux attaques externes et internes.

- Il faut donc détecter les attaques en dédiant des ressources matérielles et humaines à cette tâche: c'est le but du "**Security Operation Center**" ou "*centre *opérationnel de cybersécurité*".

Security Operation Center: définitions

- L'exploitation de systèmes de détection "**d'incidents de sécurité**" concourt à la protection d'un système d'information face aux menaces de cyberattaques. Les moyens humains, techniques et organisationnels peuvent se concentrer au sein d'un "**centre opérationnel de cybersécurité**" dédié à la détection des incidents de sécurité.
- C'est une entité **opérationnelle**, centrale dans la cyberdéfense d'une organisation.
- Le **S.O.C.** se doit de connaître le S.I. de l'entreprise (applications, réseaux, matériels de sécurité...).

Organisation du S.O.C.

- Le S.O.C peut être interne à l'entreprise ou externalisé vers un prestataire de service.
- Son infrastructure peut être dans le Cloud ou "on premise".
- Ses équipes sont constituées d'analystes, d'ingénieurs et d'experts en sécurité.
- Il doit être un bastion de sécurité et être lui-même protégé contre les attaques.
- Il doit avoir une vue globale du S.I. de l'entreprise. (inventaire, CMDB, cartographie applicative et systèmes...)

Finalités du S.O.C.

- Il permet de **prévenir des incidents de sécurité** graves ou lorsqu'ils surviennent d'en **limiter les conséquences**, en permettant des actions de remédiation rapides pouvant être menées par un prestataire de réponse aux incidents de sécurité (PRIS) ou (CERT) qualifié.
- Son métier est de **valoriser les données brutes** en informations exploitables par les équipes de réponse aux incidents de sécurité (CERT/CSIRT) et les opérationnels de la DSi.
- Ses domaines de responsabilités et ses domaines d'actions sont **variables** d'une entité à l'autre en fonction du partage des activités avec les CERT/CSIRT et les équipes de productions.

Processus de services du S.O.C.

Actions: Alerter, détecter, qualifier, analyser, traiter, communiquer, prévenir, réagir, administrer.

- Déetecter et de qualifier des incidents de sécurité.
- Analyser des incidents de sécurité.
- DéTECTER les menaces au travers des "Indicateurs de Compromission" (I.O.C.).
- Gérer les vulnérabilités.
- Gérer la conformité.(normes, réglementations, lois...)
- Communiquer avec les équipes cyber (CERT/CSIRT).

SOC versus CERT

- SOC et le CSIRT/CERT travaillent en étroite collaboration et s'auto-alimentent mutuellement.
- Le SOC est plus focalisé sur l'opérationnel et la détection des incidents de sécurité.
- Le CSIRT/CERT a un horizon de réflexion plus lointain. Il est focalisé sur la réponse aux incidents, la gestion de crise cyber et la veille autour des cybermenaces.

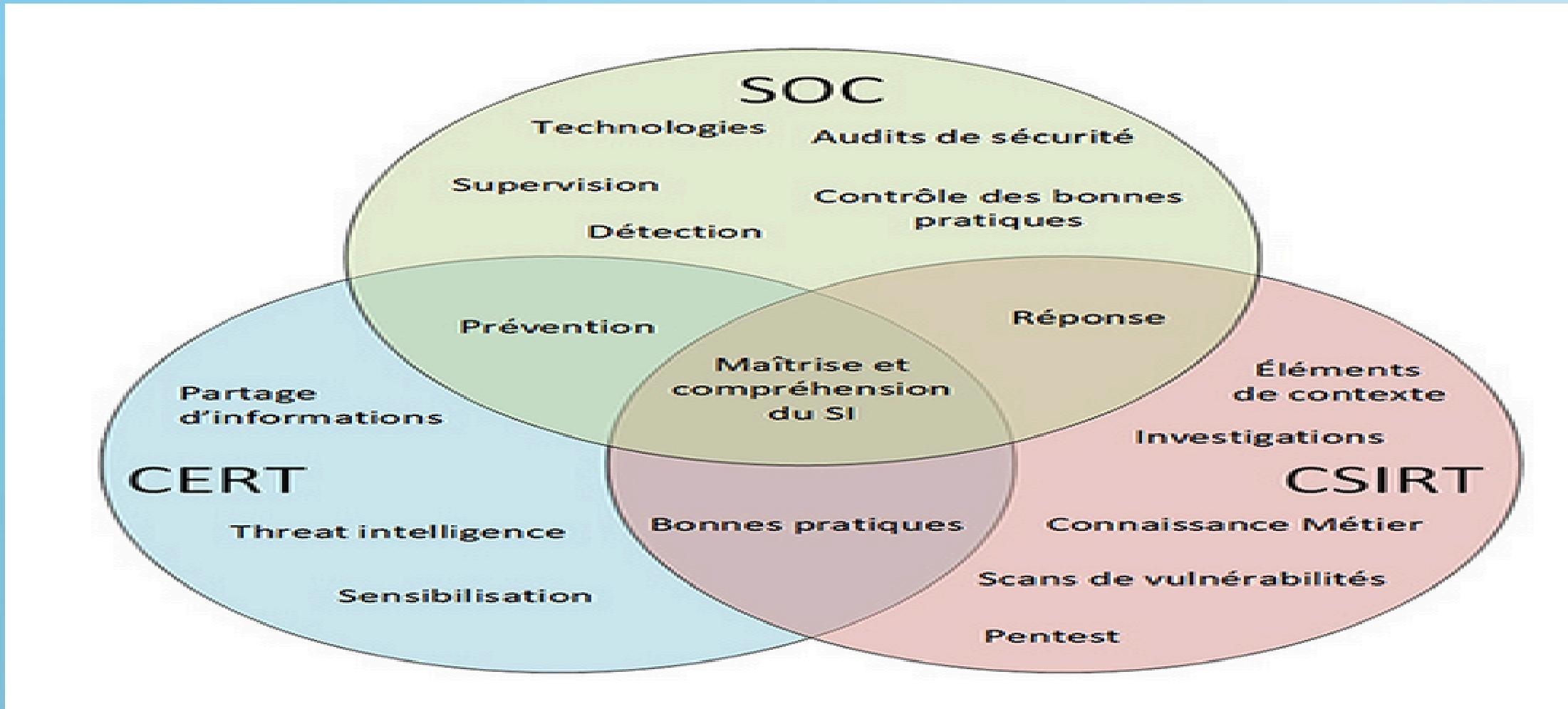
RACI - SOC versus CSIRT dans le domaine bancaire (source "www.forum-des-competences.org")

	SOC	CSIRT
Gestion des vulnérabilités sur le périmètre	Responsable	Contribue (cf. Veille)
Collecte des événements sur le périmètre	Responsable	
Gestion des règles de corrélation d'événements	Responsable	
Pondération des événements => émission d'alertes	Responsable	
Qualification de l'incident (instruction)	Responsable/Contribute	Responsable/Contributeur
Pilotage de la remédiation	Contribue	Responsable. Veille à l'industrialisation de la remédiation.
Remédiation technique	Acteur primaire (escalade N1 > N2 > N3)	Acteur sollicité sur escalade depuis N2 ou N3
Clôture de l'incident	Responsable	
Gestion de cybercrise	Contribue	Responsable
Veille technologique / Veille menaces		Responsable
Analyse post-mortem		Responsable

Deux très bons schémas de "Microsoft Learn" sur les SOC:

- "Modern Security Operations"
- "Modèles d'opérations de sécurité"

SOC versus CSIRT/CERT (Source MISC 120)



Organisation du S.O.C.: équipes "build & Run"

- L'équipe "**build**" se concentre sur la conception et la construction de l'infrastructure" de sécurité du SOC.(Déploiement d'outils de sécurité, de sondes, de capteurs, de S.I.E.M., de plateformes d'analyse de logs, de plateformes de Threat Intelligence, de plateformes de Threat Hunting...)
- L'équipe "**run**" s'occupe de la supervision, de la maintenance, de l'administration des équipements de sécurité, de la réponse aux incidents bref de l'exploitation quotidienne du SOC.

Organisation du S.O.C. : équipes des "analystes"

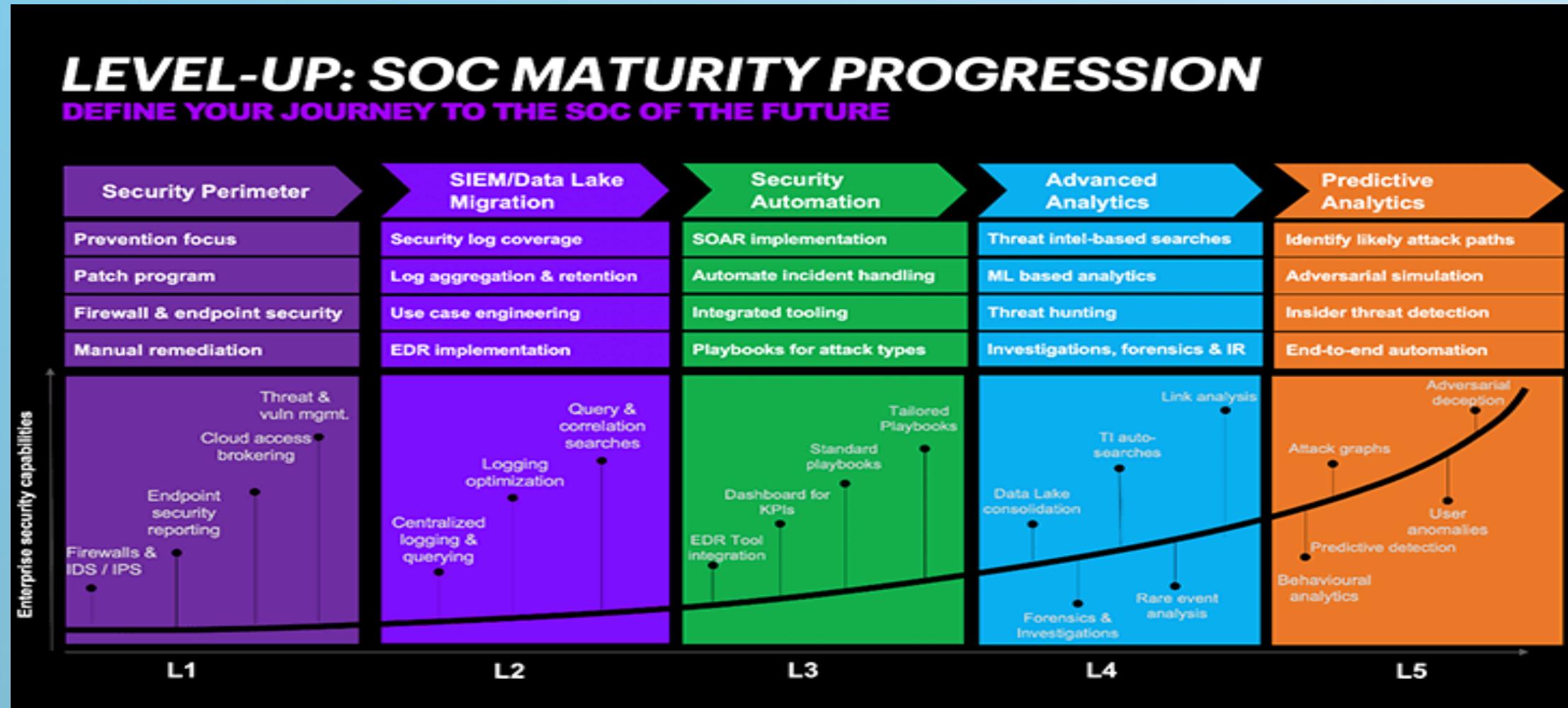
- L'*analyste S.O.C.* a une vision **holistique** de la sécurité de l'entreprise. Son but est de détecter les incidents de sécurité, les corrélérer avec des événements suspects provenant de systèmes différents, et analyser l'un incident de sécurité.
- Les analystes sont parfois répartis en équipes de niveau **1, 2 et 3**. L'équipe 3 prend en charge les incidents les plus complexes. Cela permet aussi une évolution de carrière pour les analystes.

Key Performance Indicators (K.P.I.) pour le S.O.C.

Un S.O.C. coûte cher ($3 \times 8 + \text{des cyber-spécialistes}$). Il est important d'avoir des métriques pour prouver son efficacité et son utilité:

- Nombre d'équipements surveillés ;
- Durée du processus d'investigation ;
 - M.T.T.D. (Mean Time to Detect) : durée nécessaire pour avoir connaissance d'un potentiel incident de sécurité.
 - M.T.T.R. Mean Time To Respond : durée nécessaire pour contrôler, remédier ou éradiquer une menace.

Pour améliorer ses KPI il faut augmenter la maturité de son S.O.C. (Source Accenture)



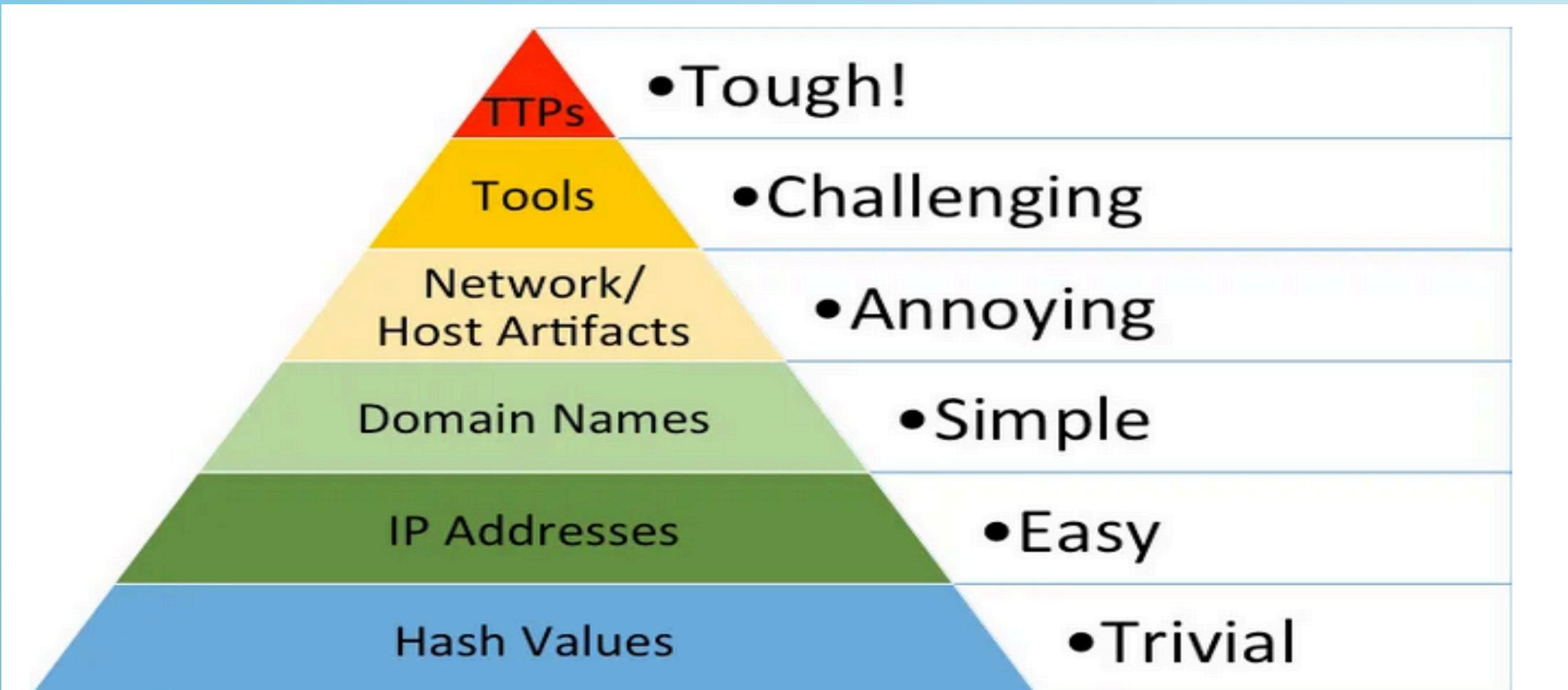
Indicateurs de Compromission (I.o.C.)

- Un I.o.C. est une donnée (fichiers, logs, registre, hashes, I.P. , URL..) ou un comportement (processus,accès, requêtes, volumétrie...) dont les caractéristiques sont inhabituelles et qui peut indiquer un problème de sécurité (malware, fuite de données, intrusions...).
- "Indicators of Compromise (I.o.C.) is an artifact observed on a network or in an operation system that with **high** confidence indicates a computer intrusion" (source Wikipedia)

Indicateurs de Compromission (I.O.C.)

- Ces indicateurs sont **statiques** et donc **facilement contournables** par les attaquants. (exemple : changer le hash d'un malware, changer l'adresse IP d'un serveur de commande et contrôle...)
- Plus l'effort de l'attaquant pour se rendre "invisible" est important et mieux c'est. (cf "Pyramid of Pain" de David Bianco SANS institute)
- Ils restent utiles néanmoins mais insuffisants pour détecter les attaques les plus sophistiquées.

"Pyramid of Pain" (Source blog de David Bianco 2013)



Advance Persistent Threats (A.P.T.)

- As the name "advanced" suggests, an advanced persistent threat (APT) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences. (Source Kaspersky)
- Il est judicieux d'avoir des modèles d'analyse des actions des attaquants pour détecter les A.P.T. (ex: "Cyber Kill Chain" de Lockheed Martin, Matrice "MITRE ATT&CK"...) et y repérer chronologiquement les I.o.C.

"Cyber Kill Chain"

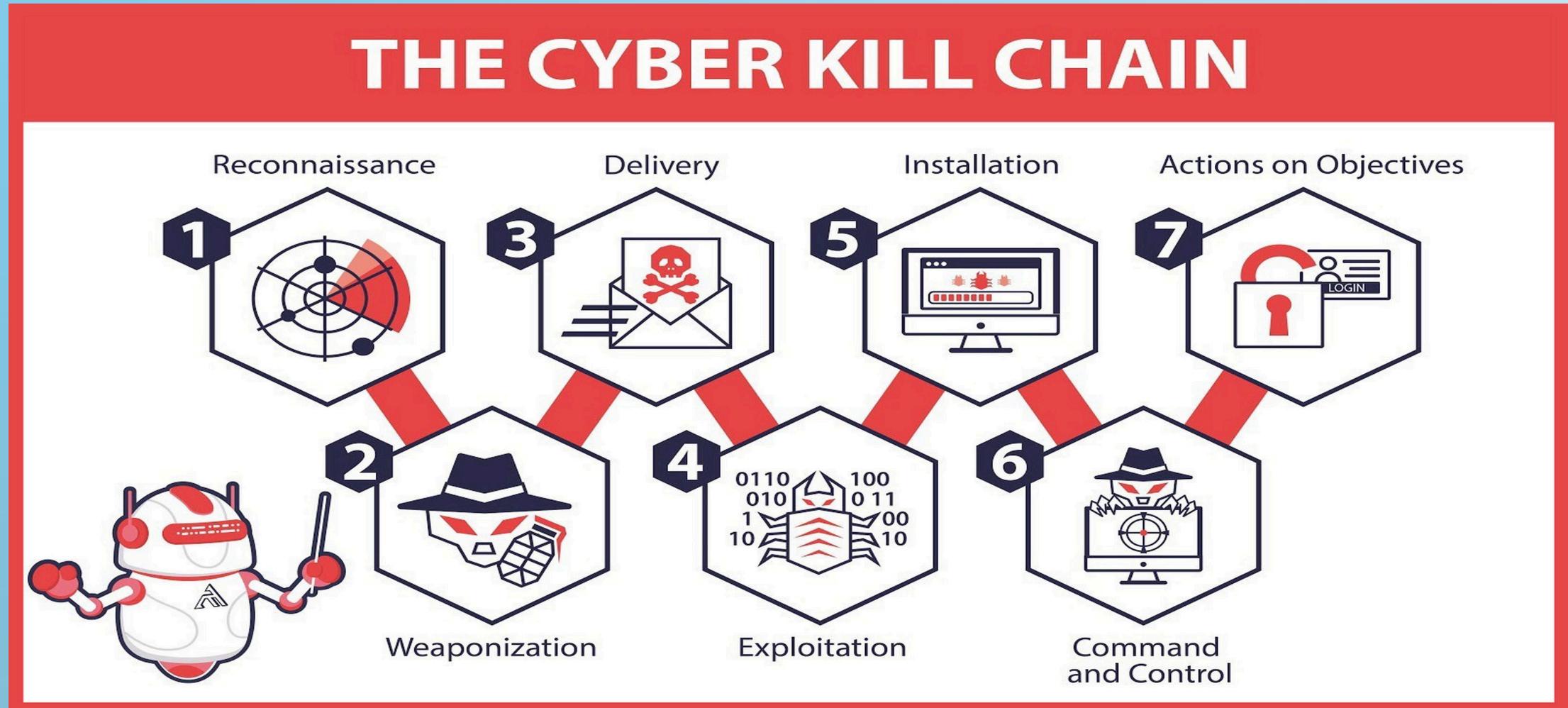
Le référentiel “Cyber Kill Chain” a été publié en 2011 par la société Lockheed Martin. Dans la “Cyber Kill Chain”, on décompose une cyber attaque en 7 étapes chronologiques :

- **Reconnaissance** (dont OSINT).
- **Weaponization** (constitution d'un armement adapté aux résultats de la reconnaissance).
- **Delivery** (Phishing, Exploit, Social Engineering pour implanter ses outils).
- **Exploitation** (exécution du code malveillant pour une pénétration initiale du système de la victime).

"Cyber Kill Chain"

- **Installation** (immédiatement après la phase d'exploitation, le vecteur d'attaque (logiciel malveillant ou autre) est installé sur le système de la victime. Il s'agit d'une étape décisive dans le cycle de vie de l'attaque : le cybercriminel s'est introduit dans le système et peut désormais en prendre le contrôle.)
- **Command & Control** (contrôle à distance, déplacement latéraux, escalade de privilèges...)
- **Actions on Objectives** (but final de l'"Advance Persistent Threats", exfiltration de données, destruction de données...)
- **Monetization** ?

"Cyber Kill Chain" (Source Lockheed Martin)



"Cyber Kill Chain Actions Matrix" (Source Lockheed Martin)

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

TTP: Tactics, Techniques and Procedures (Mitre Attack)

Le rattachement des I.O.C. aux TTP permet de mieux comprendre les attaques et de les détecter plus facilement.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 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 Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (1/4)	Deobfuscate/Decode Files or Information
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (1/2)	Deploy Container
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Scheduled Task/Job (4/6)		Domain Policy Modification (1/2)		Direct Volume Access
Search Open Technologies	Obtain Object					Domain Policy Modification (1/2)

Bibliographie:

- [PDIS ANSSI](#)
- 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
- SOC - Stratégie de détection par Maurugeon Cédric Menelet Alain Misc 120

Bibliographie:

- [Awesome SOC](#)
- [Etat de l'art de l'activité d'un S.O.C. WELAN OSSIR 2022](#)
- ["Pyramid of Pain David Bianco SANS institute"](#)
- ["CyberKillChain blog crowdstrike"](#)