

# HACK YOUR FUTURE

**JEUDI 13 OCTOBRE**

**14h - Amphithéâtre Vinci**

**Présentation RSO, SOC, CTI/VOC et Pentest  
Questions/Réponses**

# Introduction

**RSO, SOC, CTI et Pentest**, ces acronymes sonnent extra-terrestre ?

**Vous avez envie de participer à la protection de systèmes complexes contre des attaques innovantes ?**

**Alors vous êtes au bon endroit avec nos experts !**



**Gaëlle AKEBOUE**  
RSO/Gouvernance  
@SSG depuis Sept. 2016  
INSA AE 2000



**Kevin MARTIN**  
Analyste SOC  
@SSG depuis Mars. 2021



**Constance JOURDAN**  
CTI  
@SSG depuis Fev. 2021



**Dorian PELUSO**  
Pentester  
@SSG depuis Unknown



**Mathilde JOLY**  
Chargée de Recrutement  
Cyber  
@SSG depuis Sept. 2021

# L'Agenda

- **Quels sont les enjeux de la cybersécurité et comment Sopra Steria y répond ?**
- **Retour d'expérience sur vécu de consultants (le métier, les enjeux, les compétences, etc.) :**
  - **RSO (Responsable Sécurité Opérationnelle)**
  - **SOC (Security Operation Center)**
  - **CTI (Cyber Threat Intelligence)**
  - **Pentesting**
- **Quelques petits conseils de sécurité**
- **Découverte des offres de stages et alternances pour ceux qui en cherchent**
- **Questions/Réponses**

# Quels sont les enjeux de la cybersécurité et comment Sopra Steria y répond ?



# L'ETAT DE LA MENACE

**55%**

Des entreprises ont été **victimes d'une cyberattaque** au moins une fois au cours des 12 derniers mois.

**85 %**

Des violations de la cybersécurité sont causées par une **erreur humaine**.

**500 Mds \$/mois**

**Coûts mondiaux** des dommages liés à la cybercriminalité

## Principales sources de risque pour les entreprises :



### L'humain

**85%** des violations de la cybersécurité sont causés par une erreur humaine



### Les réseaux criminels

**71 %** de toutes les cyberattaques sont motivées financièrement



### Le contexte géopolitique



### La supply chain

Sources : CERT Sopra Steria et étude PAC Teknowlogy juin 2022

## Difficultés rencontrées par les organisations pour maîtriser leur risque cyber :

**50%**  
LA COMPLEXITÉ  
DU PAYSAGE  
INFORMATIQUE

**44%**  
LA PÉNURIE DE  
TALENTS



**31%**  
LES DIFFICULTÉS  
DE GESTION DES  
PARTENAIRES EN  
CYBERSÉCURITÉ

**31%**  
LE BUDGET  
INSUFFISANT

**37%**  
LA RÉSISTANCE AU CHANGEMENT  
DES COLLABORATEURS AUX  
DIFFÉRENTS NIVEAUX

# ... ET LE DILEMME DU RSSI

Comment accélérer la transformation digitale en conformité avec la réglementation ?

## TRANSFORMATION DIGITALE

Mobilité

Social

IoT

Cloud & SaaS

Big Data & Analytics

Réalité virtuelle augmentée

Intelligence Artificielle

## RÈGLEMENTATIONS



En favorisant la mise en œuvre de la stratégie d'entreprise tout en réduisant les potentiels impacts négatifs sur les métiers de l'entreprise.

# LEADER EUROPEEN DE LA CYBERSECURITE

**01. Partenaire de confiance numérique des entreprises**  
du CAC 40 et grands comptes de tous secteurs d'activité.



**02. Offreur global** capable d'adresser la sécurité de **bout en bout, du conseil aux services managés, en passant par l'intégration.**

**03. Expert en cybersécurité reconnu par les Analystes :**



Les services de sécurité stratégique et services d'infogérance de sécurité pour les grandes organisations de Sopra Steria classés parmi les leaders dans la dernière étude ISG Provider Lens™



Sopra Steria sélectionné par Forrester dans le rapport *"Now Tech : European Cybersecurity Consulting Providers, Q1 2021"*



**N° 3**  
européen en cyber



**700**  
experts en France



**1 400**  
Consultants & experts  
dans le monde

# SECURISATION DE TOUTE LA CHAÎNE DE VALEUR CYBER

Nous intervenons sur l'ensemble de la chaîne de valeur cyber avec 3 principes clés :

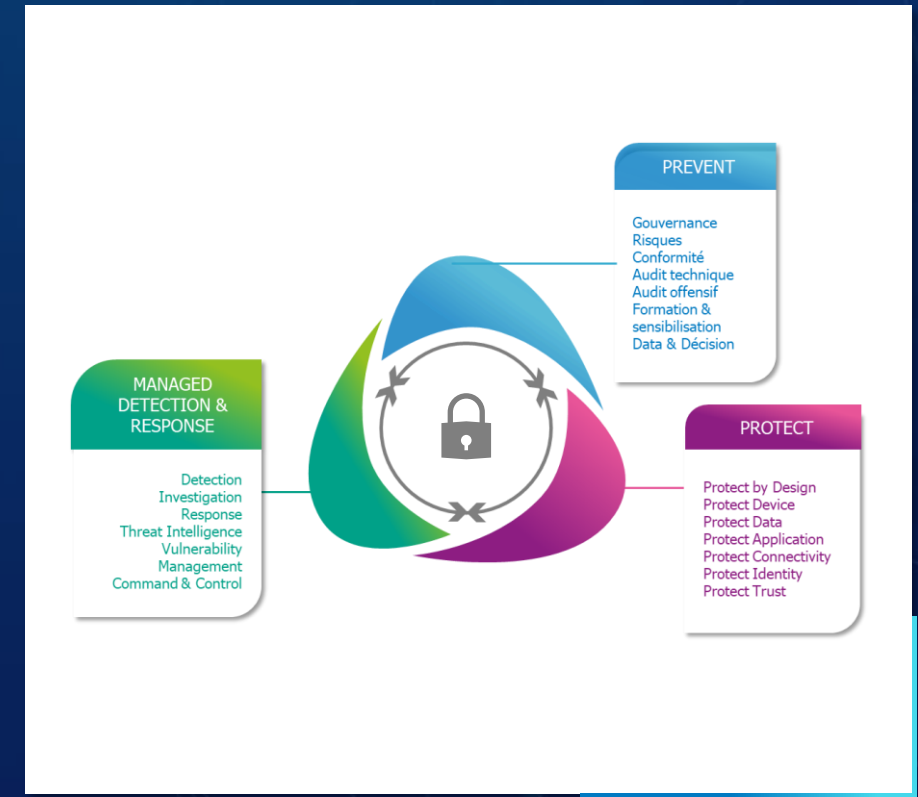
## 01. Maximiser la valeur apportée à nos clients :

- Une compréhension des enjeux sectoriels et des contraintes de nos clients, croisée à une connaissance fine de l'état de la menace cyber.

## 02. Accompagner de bout-en-bout :

- **Prevent** : élaborer, adapter une stratégie et évaluer la maturité cyber de l'entreprise
- **Protect** : apporter une réponse complète et adaptée sur l'ensemble des composants de sécurité
- **Detect & Respond** : connaître la menace à laquelle l'entreprise est exposée et se doter de moyens de détection et de réponse aux incidents de sécurité

## 03. Mettre en œuvre l'excellence opérationnelle via des offres transverses adaptées aux enjeux d'actualité.





# Parole d'experts !



**Gaelle AKEBOUE**

RSO/Gouvernance

@SSG depuis Sept. 2016

INSA AE 2000

# LA SÉCURITÉ OPÉRATIONNELLE, KÉSAKO ?

La sécurité opérationnelle c'est l'ensemble des processus opérationnels qu'il faut mettre en place et évaluer au quotidien afin réduire la surface d'exposition du système d'information aux risques.

La sécurité opérationnelle adresse plusieurs facettes et aspects du système.

Dans ce cadre, la mission de la Gouvernance Sécurité est de :

- Vérifier la conformité du dispositif en place par rapport aux exigences de sécurité applicables
  - PSSI clientes et Sopra Steria
  - Normes et réglementations
- Conseiller, accompagner le RSSI dans l'amélioration de ce dispositif

## Chapitres de l'ISO 27001 : 2013

- Politique de sécurité
- Organisation de la sécurité
- Sécurité des RH
- Gestion des actifs
- Contrôle d'accès
- Cryptographie
- Sécurité physique et environnementale
- Sécurité liée à l'exploitation
- Sécurité des communications
- Acquisition, développement et maintenance des SI
- Relations avec les fournisseurs
- Gestion des incidents liés à la sécurité de l'information
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Conformité

# LES ACTIVITÉS DU RESPONSABLE SÉCURITÉ OPÉRATIONNELLE

Le RSO est le garant de la gouvernance sécurité en appui du RSSI client.

Il fait une revue du respect des règles de sécurité et accompagne également son client dans l'amélioration du dispositif de sécurité.

## Gouvernance

Les équipes CERT opèrent le service Scan de Vulnérabilités et produisent le rapport de scan. Le RSO suit la mise en œuvre du dispositif, déclenche la réalisation des scans et soumet au RSSI un plan d'actions de remédiation.

## Gestion des vulnérabilités

Le RSO suit le nombre de comptes administrateurs et de comptes à privilèges sur les assets du périmètre.

## Gestion des habilitations

Le RSO réalise une action de veille sécurité en s'appuyant sur les sources du CyberCentre.

## Veille sécurité

Le RSO accompagne les auditeurs mandatés par son client dans la compréhension du système de sécurité et dans la recherche de preuves.

## Accompagnement d'audit externe

## Gestion du PAS

Colonne vertébrale des activités du RSO, le Plan d'Assurance Sécurité met en relation les exigences sécurité client et les moyens que SopraSteria s'engage à mettre en œuvre pour y répondre.

## Gestion du patch management

Le RSO propose au RSSI client une sélection de patches à appliquer et suit leur mise en œuvre.

## Gestion des produits de sécurité

Les équipes Produits de Sécurité gère les outils tels que l'antimalware (MCO, incidents...). Le RSO monitora la gestion de ces produits.

## Gestion des incidents de sécurité

Le RSO relaie les incidents auprès de son client, définit le plan d'actions et en assure le suivi. Il sollicite les experts du Cybercentre pour des investigations avancées.





**Kevin MARTIN**  
Analyste SOC  
@SSG depuis Mars. 2021



# QUI SUIS-JE ?



**Kevin MARTIN**

Analyste SOC

@SSG depuis Mars. 2021

Mail: [kevin.martin3@soprasteria.com](mailto:kevin.martin3@soprasteria.com)

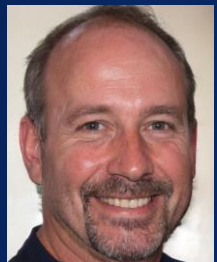
LinkedIn: [linkedin.com/in/martinke](https://www.linkedin.com/in/martinke)

## Parcours académique

- **ENSEEIH – SN** | 2018 – 2021
  - Spécialisation Infrastructure Big Data et IOT
  - UEs optionnelles cybersécurité

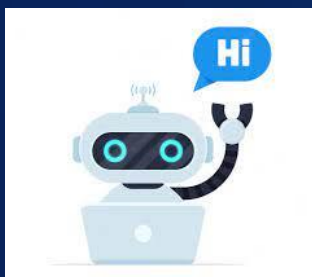
## Parcours professionnel

- **Analyste SOC L1** | Mars 2022 – Septembre 2022
  - Traitement d'une alerte de sécurité
  - Outils et méthodes de recherche pour les logs
- **Analyste forensique** | Depuis septembre 2022
  - Traitement en direct d'un incident de sécurité
  - Recherche et analyses poussées de systèmes informatique et de logs



### Roger, 48 ans, département comptabilité:

- Télécharge Dofus sur son PC
- Clique sur le lien d'un mail lui promettant de gagner 2 000 000 d'euros



### Bot, Ecume internet 24h/24

- Lance des attaques simples et/ou automatisables (injections SQL, path traversal, vulnérabilités avec procédures d'exploitations publiques, ...)



### Attaquant humain

- Attaques lentes, simples et ou complexes avec une capacité d'adaptation

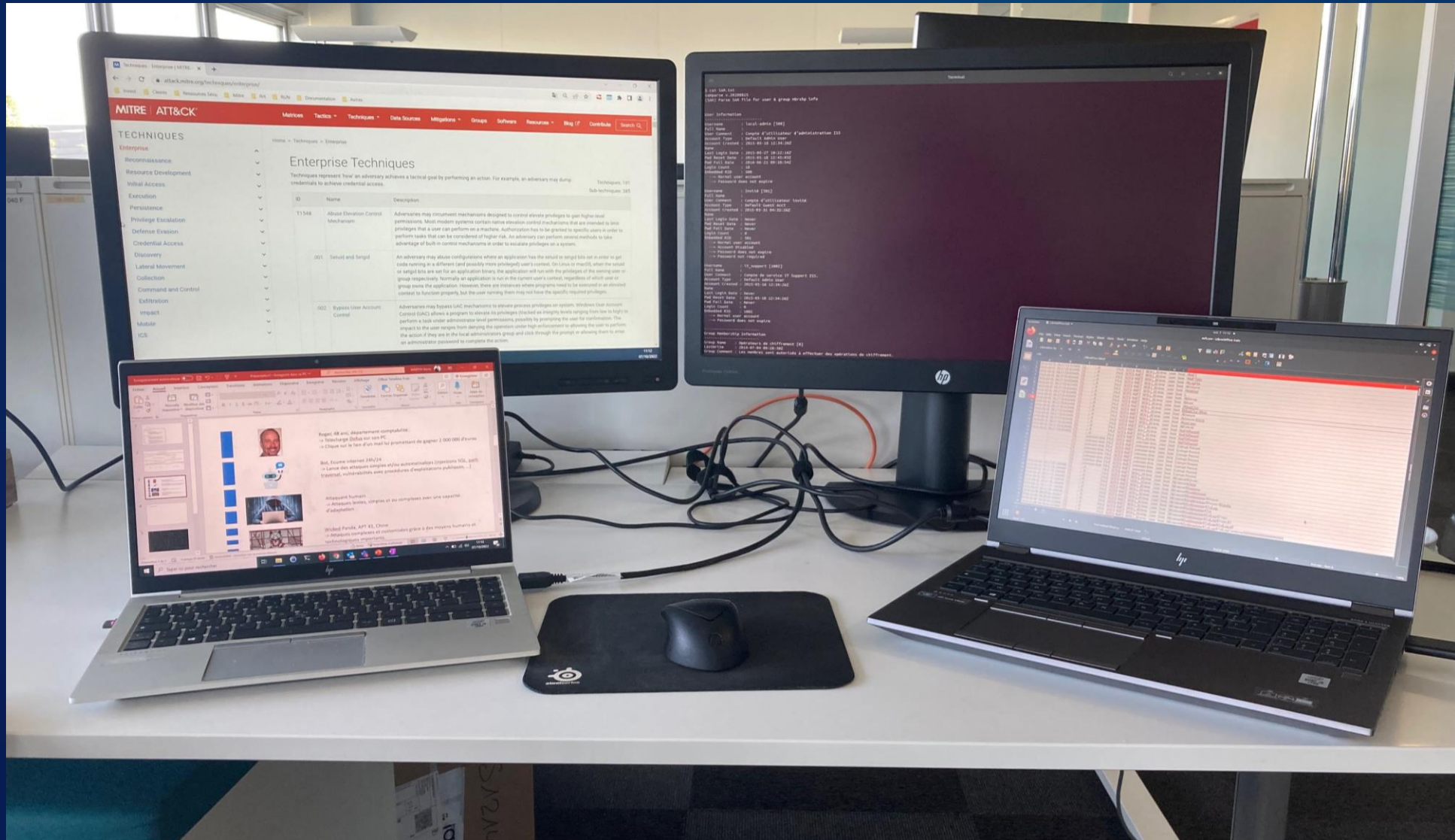


### Wicked Panda, APT 41, Chine

- Attaques complexes et customisées grâce à des moyens humains et technologiques importants.
- Affiliés à un état



# MON BUREAU ET MON MATERIEL DE TRAVAIL





```
rrypi su[2085]: Successful su for pihole by root
rrypi su[2085]: + ??? root:pihole
rrypi su[2085]: pam_unix(su:session): session opened for user pihole by (uid=0)
rrypi systemd-logind[1007]: New session c1 of user pihole.
rrypi systemd: pam_unix(systemd-user:session): session opened for user pihole by (uid=0)
rrypi su[2085]: pam_unix(su:session): session closed for user pihole
rrypi login[2084]: pam_unix(login:session): session opened for user pi by LOGIN(uid=0)
rrypi systemd-logind[1007]: New session c2 of user pi.
rrypi systemd: pam_unix(systemd-user:session): session opened for user pi by (uid=0)
rrypi sshd[2245]: Accepted password for pi from 192.168.1.199 port 40040 ssh2
rrypi sshd[2245]: pam_unix(sshd:session): session opened for user pi by (uid=0)
rrypi systemd-logind[1007]: New session c3 of user pi.
rrypi CRON[1077]: pam_unix(cron:session): session closed for user root
rrypi sudo: www-data : TTY=unknown ; PWD=/var/www/html/admin ; USER=root ; COMMAND=/usr/local/b
rrypi sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
rrypi sudo: pam_unix(sudo:session): session closed for user root
rrypi sudo: www-data : TTY=unknown ; PWD=/var/www/html/admin ; USER=root ; COMMAND=/usr/local/b
rrypi sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
rrypi sudo: pam_unix(sudo:session): session closed for user root
rrypi sudo: www-data : TTY=unknown ; PWD=/var/www/html/admin ; USER=root ; COMMAND=/usr/local/b
rrypi sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
rrypi sudo: pam_unix(sudo:session): session closed for user root
rrypi CRON[2509]: pam_unix(cron:session): session opened for user root by (uid=0)
rrypi CRON[2509]: pam_unix(cron:session): session closed for user root
rrypi sudo: pi : TTY=pts/0 ; PWD=/home/pi ; USER=root ; COMMAND=/home/pi/.kodi/userdata/a
ome/pi/.kodi/userdata/addon_data/program.plexus/acestream/androidfs /system/bin/sh -c cd /system
stem/bin/acestream.sh -
```



```
rrypi su[2085]: Successful su for pihole by root
rrypi su[2085]: + ??? root:pihole
rrypi su[2085]: pam_unix(su:session): session opened for user pihole by (uid=0)
rrypi systemd-logind[1007]: New session c1 of user pihole.
rrypi systemd: pam_unix(systemd-user:session): session opened for user pihole by (uid=0)
rrypi su[2085]: pam_unix(su:session): session closed for user pihole
rrypi login[2084]: pam_unix(login:session): session opened for user pi by LOGIN(uid=0)
rrypi systemd-logind[1007]: New session c2 of user pi.
rrypi systemd: pam_unix(systemd-user:session): session opened for user pi by (uid=0)
rrypi sshd[2245]: Accepted password for pi from 192.168.1.199 port 40040 ssh2
rrypi sshd[2245]: pam_unix(sshd:session): session opened for user pi by (uid=0)
rrypi systemd-logind[1007]: New session c3 of user pi.
rrypi CRON[1077]: pam_unix(cron:session): session closed for user root
rrypi sudo: www-data : TTY=unknown ; PWD=/var/www/html/admin ; USER=root ; COMMAND=/usr/local/b
rrypi sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
rrypi sudo: pam_unix(sudo:session): session closed for user root
rrypi sudo: www-data : TTY=unknown ; PWD=/var/www/html/admin ; USER=root ; COMMAND=/usr/local/b
rrypi sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
rrypi sudo: pam_unix(sudo:session): session closed for user root
rrypi sudo: www-data : TTY=unknown ; PWD=/var/www/html/admin ; USER=root ; COMMAND=/usr/local/b
rrypi sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
rrypi sudo: pam_unix(sudo:session): session closed for user root
rrypi CRON[2509]: pam_unix(cron:session): session opened for user root by (uid=0)
rrypi CRON[2509]: pam_unix(cron:session): session closed for user root
rrypi sudo:      pi : TTY=pts/0 ; PWD=/home/pi ; USER=root ; COMMAND=/home/pi/.kodi/userdata/a
ome/pi/.kodi/userdata/addon_data/program.plexus/acestream/androidfs /system/bin/sh -c cd /system
stem/bin/acestream.sh -
```



# ETUDE DE CAS PRATIQUE

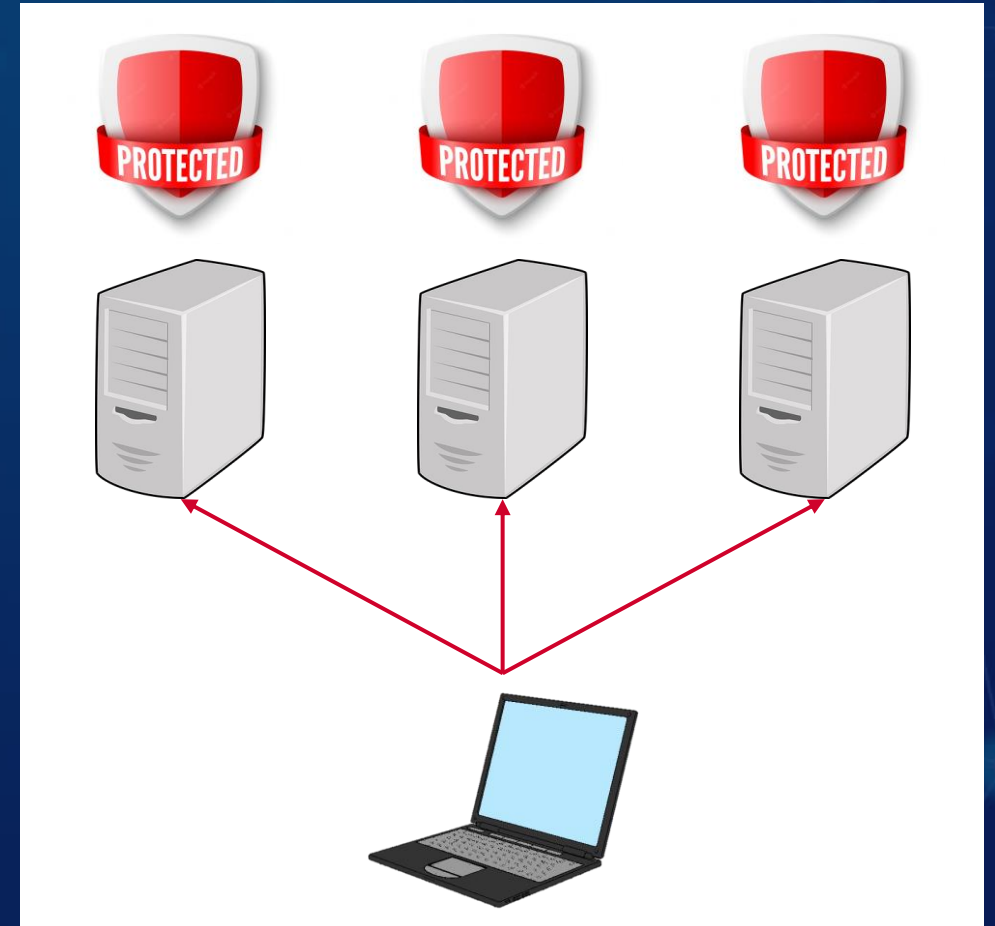


Un **rançongiciel** a tenté de se propager dans mon système informatique. L'**EDR** des machines de mon SI a permis d'empêcher la propagation de la menace et de déterminer la source de l'attaque.

## Matériel de travail

- Disque dur de la workstation
- Logs EDR/antivirus
- Témoignage utilisateur

**Contexte** --> Infection le 10/02 par Lockbit, 210 PC infectés



kevmartin@siftworkstation: /mnt/windows\_mount/Windows

\$ ls

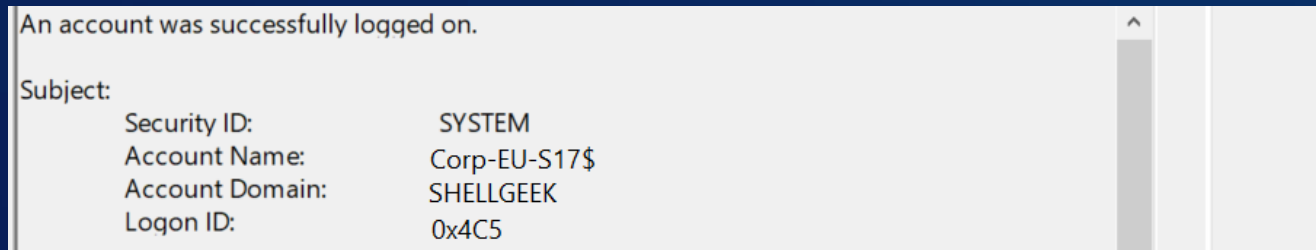
addins	HPMPProp.INI	PolicyDefinitions	System32
AppCompat	IE10_main.log	Prefetch	system.ini
AppPatch	IME	Professional.xml	SysWOW64
assembly	inf	qeriuwjhrf	TAPI
ativpsrm.bin	Installer	RegBootClean64.CFG	Tasks
bfsvc.exe	ISS	RegBootClean64.exe	tasksche.exe
Boot	IsUn040c.exe	RegBootClean.CFG	Temp
bootstat.dat	L2Schemas	RegBootClean.exe	TMFilter.log
Branding	LiveKernelReports	regedit.exe	tracing
cfgall.ini	Logs	Registration	TSSysprep.log
CSC	Media	rescache	twain_32
Cursors	MEMORY.DMP	Resources	twain_32.dll
debug	mib.bin	SchCache	twain.dll
diagnostics	Microsoft.NET	schemas	twunk_16.exe
DigitalLocker	Migration	security	twunk_32.exe
'Downloaded Program Files'	Minidump	ServiceProfiles	vmgcoinstall.log
DtcInstall.log	ModemLogs	servicing	Vss
ehome	msdfmap.ini	Setup	Web
en-US	mssecsvc.exe	setupact.log	WindowsShell.Manifest
explorer.exe	mssecsvr.exe	setuperr.log	WindowsUpdate.log
Fonts	notepad.exe	ShellNew	winhlp32.exe
fr-FR	'Offline Web Pages'	smsts.ini	win.ini
fveupdate.exe	Panther	SoftwareDistribution	winsxs
Globalization	PCHEALTH	Speech	WMSysPr9.prx
Help	Performance	splwow64.exe	write.exe
HelpPane.exe	PFR0.log	Starter.xml	
hh.exe	PLA	system	

# ARTEFACTS FORENSIQUE

- Master File Table (MFT): Tableau récapitulant les dates d'arrivées des fichiers sur le système et leur chemin d'accès

2022-08-18	08:17:37.415733	FILE	NTFS \$MFT	user	host	/users/martinke/Pictures/001.jpg
------------	-----------------	------	------------	------	------	----------------------------------

- Events ID (EVTX): Journalisation de l'ensemble des événements systèmes suivant leur catégorie et leur cible.




- HIVE système (HIVE): Journalisation de l'état des registres et du système (SECURITY, SOFTWARE, SYSTEM, ...)

C:\WINDOWS\tasksche.exe	2022-01-11	06:05:45	Executed
C:\WINDOWS\tasksche.exe	2022-01-17	09:37:31	Executed
C:\WINDOWS\mssecsvc.exe	2020-01-22	13:27:25	Executed
C:\WINDOWS\mssecsvc.exe	2020-01-22	14:01:17	Executed

# WANNACRY

869a8da45f4d8a9afc7a31e0494cebb3f5d962185b68b6b85a07328914e1d85e mssecsvc.exe



63  
/ 70

Community Score

⚠ 63 security vendors and 1 sandbox flagged this file as malicious

869a8da45f4d8a9afc7a31e0494cebb3f5d962185b68b6b85a07328914e1d85e  
869a8da45f4d8a9a\_mssecsvc.exe

cve-2017-0147 exploit peexe

BitDefender	⚠ Trojan.Ransom.WannaCryptor.H
ClamAV	⚠ Win.Ransomware.WannaCry-6313787-0
Comodo	⚠ TrojWare.Win32.WannaCry.jet@714um4

- Rançongiciel **auto-répliquant** massivement déployé en mai 2017
- Accès initial via la vulnérabilité CVE-2017-0144 (**EternalBlue**) affiliée au service SMB v1.0

Quand est-il arrivé sur le système ?

2019-11-05	12:11:24.031301	FILE	NTFS \$MFT	user	host	/Windows/mssecsvc.exe
------------	-----------------	------	------------	------	------	-----------------------

2019-11-05	12:12:37.117428	FILE	NTFS \$MFT	user	host	/Windows/tasksche.exe
------------	-----------------	------	------------	------	------	-----------------------

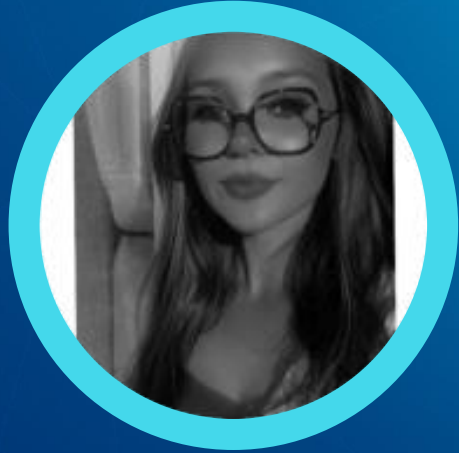
# CONCLUSION

Encore beaucoup de choses à déterminer :

- Méthode de persistance de Wannacry ?  
--> Via un **service** dans le système nommé **mssecsvc2.1**
- Quel accès initial ?  
--> Présence du **driver et du service SMB v1.0** sur la machine
- Fonctionnement précis des deux exécutables ?  
--> Lancement en **sandbox**

**Merci de votre écoute !**





**Constance JOURDAN**

CTI

@SSG depuis Fev. 2021

# CTI: TROIS NIVEAUX D'ANALYSE

## CTI actionnable



### Strategic

#### *Who & Why ?*

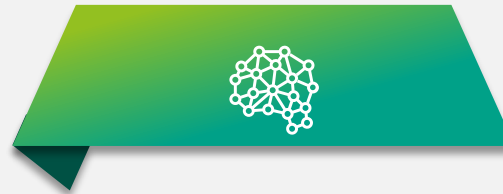
Attacker profile  
Campaigns : focus on sectors and geographic areas (Exec reports)



### Tactical

#### *How ?*

Focus on *modus operandi*  
(TTPs & tools & ops reports)



### Operational

#### *What & Where ?*

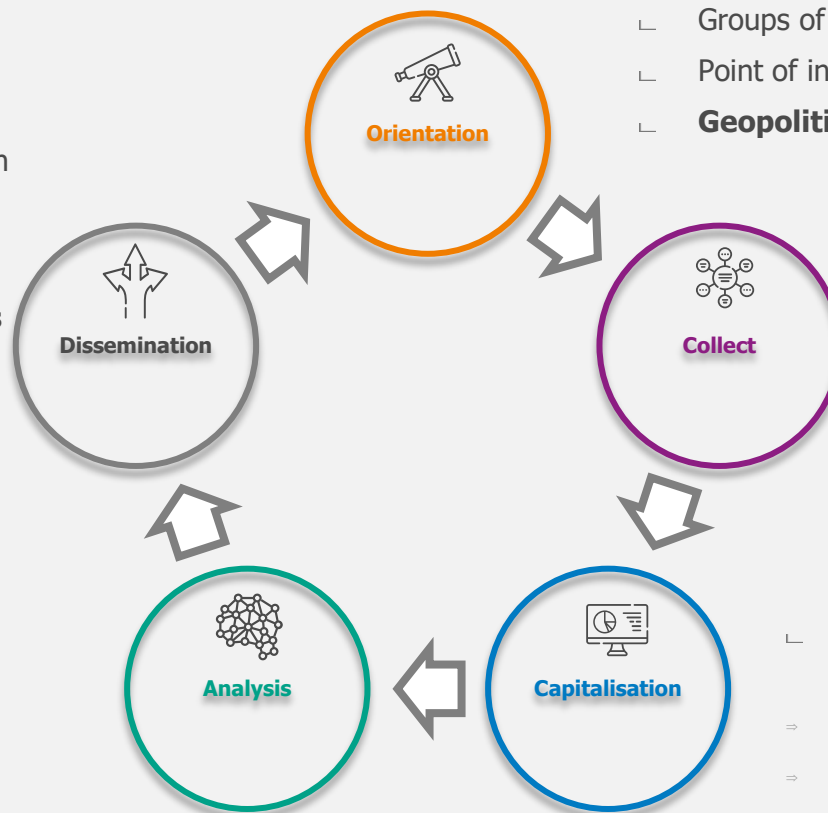
Focus on technical issues or artifacts observed  
(IOCs, Yara & Snort Rules)

# CTI: LE RENSEIGNEMENT D'INTERET CYBER

## Cinq étapes du renseignement

- └ Production of **report / deliverables**
- └ Sent of **contextualized IoC** to Detection / Protection tools (after that **sighting** based on MSSP datas with anonymisation)
- └ Creation of **own detection capabilities** (exploits)

- └ Definition of value of information :
  - First seen, last seen.
  - Impacts
- └ **Enrichment** (through SOAR or TIP)
- └ **Pivot** for product MDR &/or customers
  - TTPs coverage
  - **Fine behaviour**



- └ Groups of Threat actors followed
- └ Point of interest on Ransomware
- └ **Geopolitical / Economic approach**

- └ Public Feeds. Quality process based on **admirability code** (A to F depending freshness, reputation & False positive)
- └ Private Feeds
- └ Blogs
- └ Communities
- └ **Data management** with TLP & PAP

- └ All information **gathered in Threat Intelligence Platform** : MISP & EcleticIQ

### CTI Taxonomy

- Use of **STIX format** (Sopra Steria membership of Oasis Organisation)
- └ Information classified and correlated
- └ **Datavisualisation & reports** available quickly



**Dorian PELUSO**  
Pentester  
@SSG depuis Unknown



# Quelques petits conseils de sécurité





## Thomas ne partage pas tout

Et vous ?

- Protégez l'accès à vos données confidentielles
- N'utilisez pas de clés USB personnelles ou inconnues
- Utilisez un filtre d'écran de confidentialité



## Sandra est aussi étrange que ses mots de passe

Pas vous ?

- Créez des mots de passe longs et inhabituels
- Gardez les secrets
- Utilisez-en plusieurs différents
- Utilisez un gestionnaire de mot de passe pour ne pas tous les mémoriser



## Carlos se méfie de l'ingénierie sociale\*

Pas vous ?

- Signalez tous les emails suspects
- Sachez avec qui vous communiquez
- Soyez prudent sur les réseaux sociaux

\* L'ingénierie sociale est l'art de manipuler les personnes pour les inciter à transmettre des informations confidentielles.



1. Gardez à jour vos logiciels et votre antivirus.



2. N'agissez pas avec précipitation et prenez le temps d'examiner le mail : adresse de l'émetteur, fautes d'orthographe ou de grammaire, demande suspecte, etc.



3. Ne répondez jamais aux mails qui vous paraissent suspects.



4. Ne cliquez pas sur les liens et ne téléchargez pas les pièces jointes.



# Découverte des offres de stage



## Mathilde JOLY

Chargée de Recrutement Cyber  
@SSG depuis Sept. 2021

Mail: [mathilde.joly@soprasteria.com](mailto:mathilde.joly@soprasteria.com)

Téléphone : 07 85 98 17 24

## Campagne de Stage 2022-2023

- **TOULOUSE | PARIS | RENNES**
- Stages de fin d'études ( 5<sup>ème</sup> année)
- Analyste SOC, Analyste CTI, Analyste VOC, Analyse de Risques, RSO, Ingénieur EDR, Ingénieur Systèmes et réseaux, Ingénieur Infrastructure, Sécurité Applicative etc...
- Retrouvez nos offres de stages sur notre site dédié : [etudiants.soprasteria.fr](https://etudiants.soprasteria.fr)

## Campagne d'Alternance 2023

- *Lancement en Mars 2023*

## Offres d'emplois

- Disponible depuis le site carrière de Sopra Steria

# Questions/Réponses