TLP:CLEAR

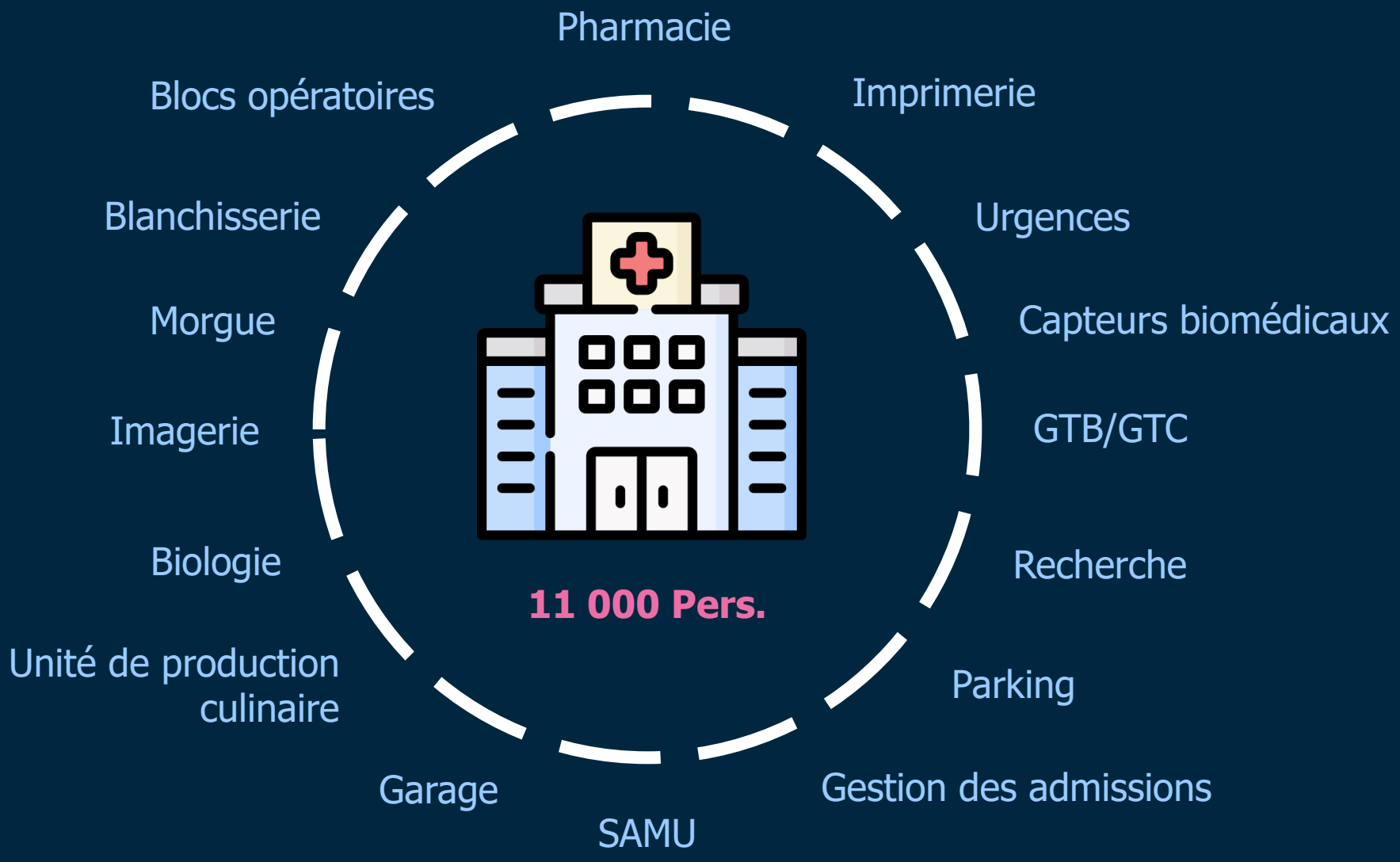
L'EDR, de la réponse à incident, à la pierre angulaire de la cybersécurité du CHU de Brest

Agrégation Rhône-Auvergne des Métiers de l'Informatique dans le Supérieur (ARAMIS)

Jean-Sylvain CHAVANNE
Responsable de la sécurité des systèmes d'information (RSSI) – CHU Brest

L’Hôpital, une petite ville dans la ville

TLP:CLEAR



Quelques chiffres pour le CHU de Brest

TLP:CLEAR

- **2 500 lits et places** sur 7 sites géographiques
- **210 000** venues en imagerie médicale par an
- **800 000** dossiers d'analyses de biologie médicale par an

300 applications métiers

3 Po taille des bases de données

34k mails ext reçus / jour

800 serveurs virtuels

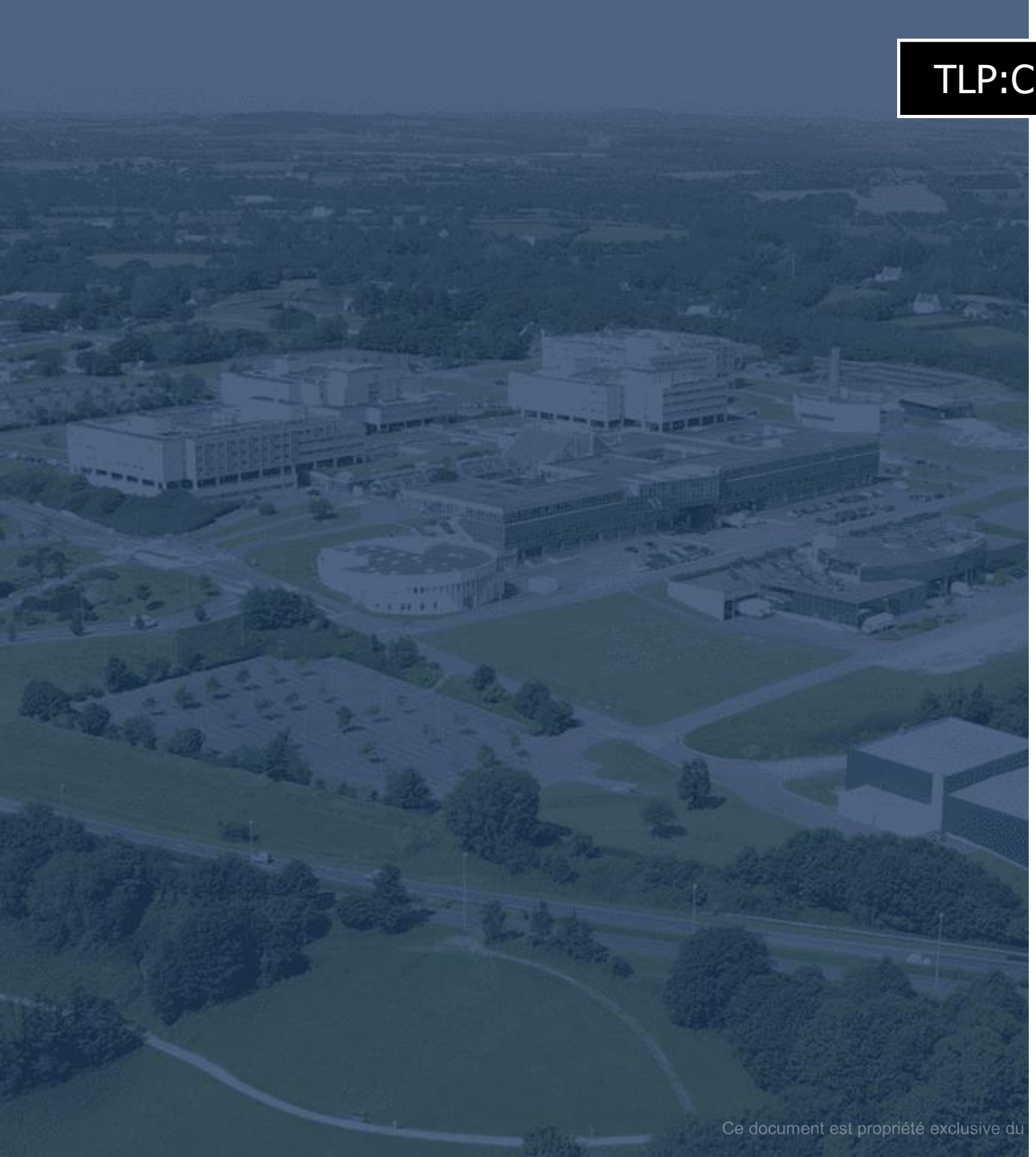
20k équipements biomédicaux

12 Phishing Par heure

160 bases de données

20 applications exposées

60' charges malveillantes



TLP:CLEAR

1

Le contexte du CHU en 2022

Le choix de l'EDR

TLP:CLEAR

- Choix d'HarfangLab par le CHU : Juillet 2022
- Financement de France Relance
- Décommissionnement de Kaspersky et mise en œuvre de Windows Defender avec MECM
- EDR HarfangLab supervisé par un prestataire de service

- Début de la mise en place : octobre 2022
  - Phase des postes de travail
    - D'abord avec MaJ via MECM mais mauvaise idée.
  - Phase des serveurs Linux
  - Phase des serveurs Windows
  - Le tout en phase de détection et non de **blocage** car la DTSN était réticente sur les effets de bord potentiels.

Cela concerne uniquement le domaine AD, géré par la DTSN.

Les étapes du déploiement

TLP:CLEAR

TEST

- Installation manuelle sur quelques postes (3 à 5 – équipe projet ou IT)
- Recette technique (Console EDR ou support Advens)

PILOTE

- Création des packages à déployer sur le parc (5 à 10% du parc)
- Installation sur un lot pilote représentatif (PdT, serveurs)
- Recette technique (validation de déploiement)
- Recette métier (validation de bon fonctionnement et validation des cas d'usage – ex : blocage par un proxy etc.)

GENERALISATION

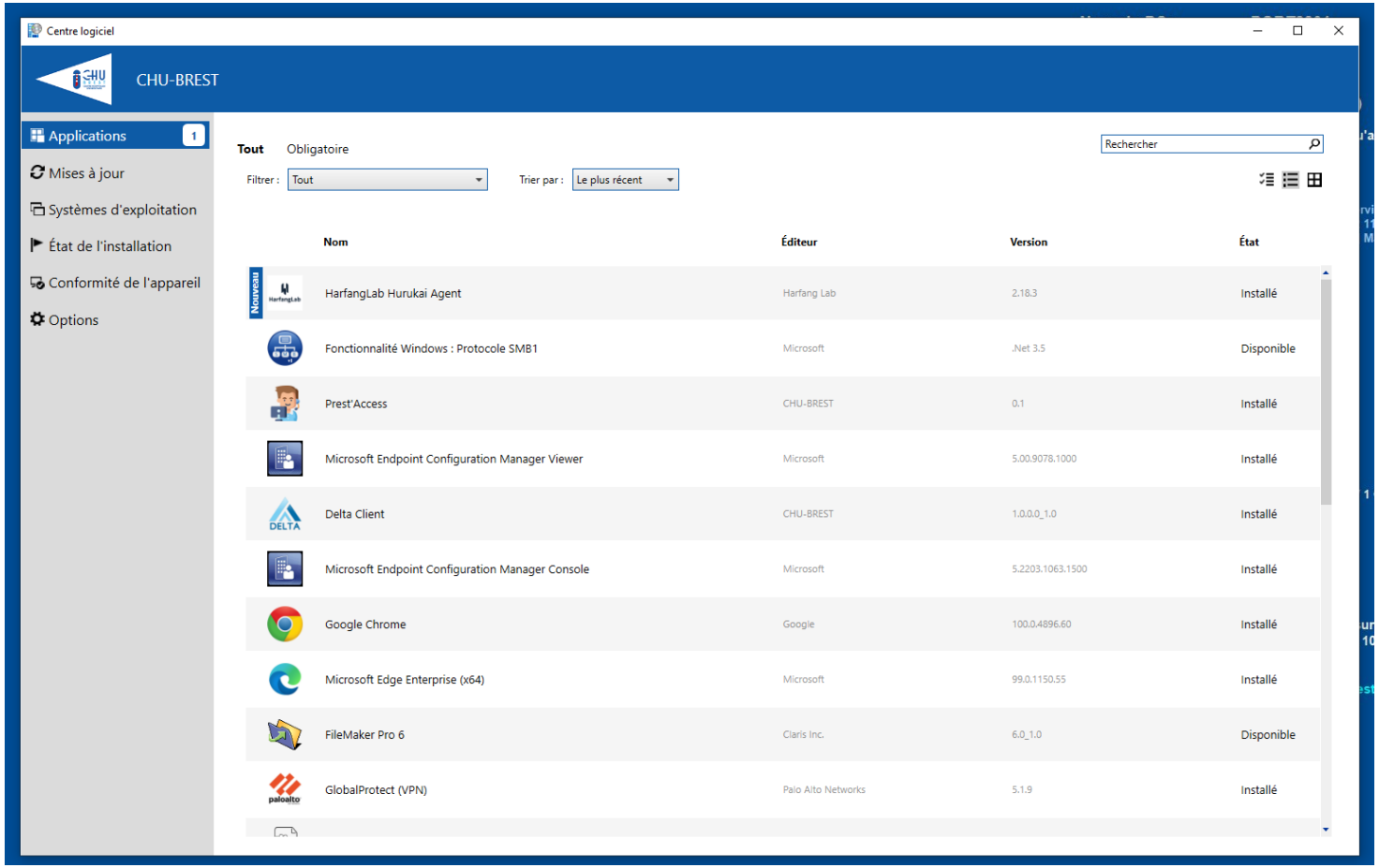
- Définition de lots de déploiement (campagnes)
- Déploiement par lot selon un calendrier défini
- Support au déploiement
- Validation d'aptitude au bon fonctionnement (VABF)

Les modes de déploiement choisis

TLP:CLEAR

Le CHU de Brest va déployer :

- Sur les postes de travail via MECM de Microsoft
- Sur les serveurs Windows par GPO
- Sur les serveurs Linux à la main
- Sur les serveurs relevant du biomédical
  - Difficile politiquement
- Sur les serveurs relevant de la DTA
  - Difficile politiquement



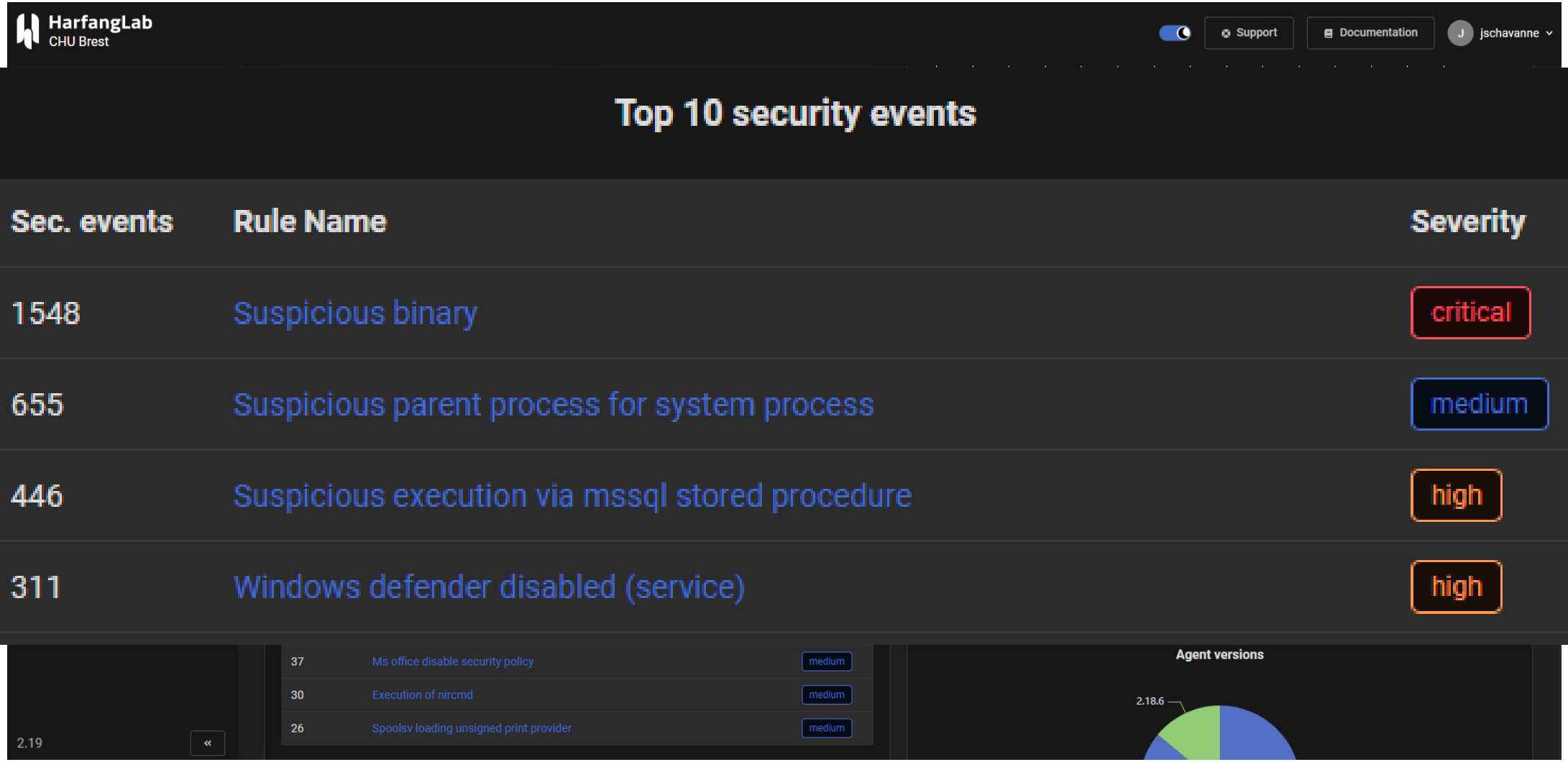
Les premières dates au CHU de Brest

TLP:CLEAR

- 10/10/2022 : Décommissionnement de Kaspersky + Installation et paramétrage de Windows Defender
- 14/10/2022 : Réception des éléments techniques par aDvens :
- 17/10/2022 : Création du package MSI par l'équipe Poste de Travail :
- 17/10/2022 : Déploiement sur les PC de test du CHU (4 PdT)
- 18/10/2022 : Passage en CAB (Comité des changements)
- 18/10/2022 : Déploiement sur les PdT de la DSI (60 PdT)
- 24/10/2022 : Réunion avec aDvens pour les problèmes avec HarfangLab (accès console, MàJ automatique)
- 10/11/2022 : Passage en CAB :
- 14/11/2022 : Déploiement sur le tout le parc IT (8 500 PdT)
- 01/12/2022 : Déploiement sur l'ensemble des serveurs Windows
- 01/12/2022 : Déploiement sur les serveurs Linux

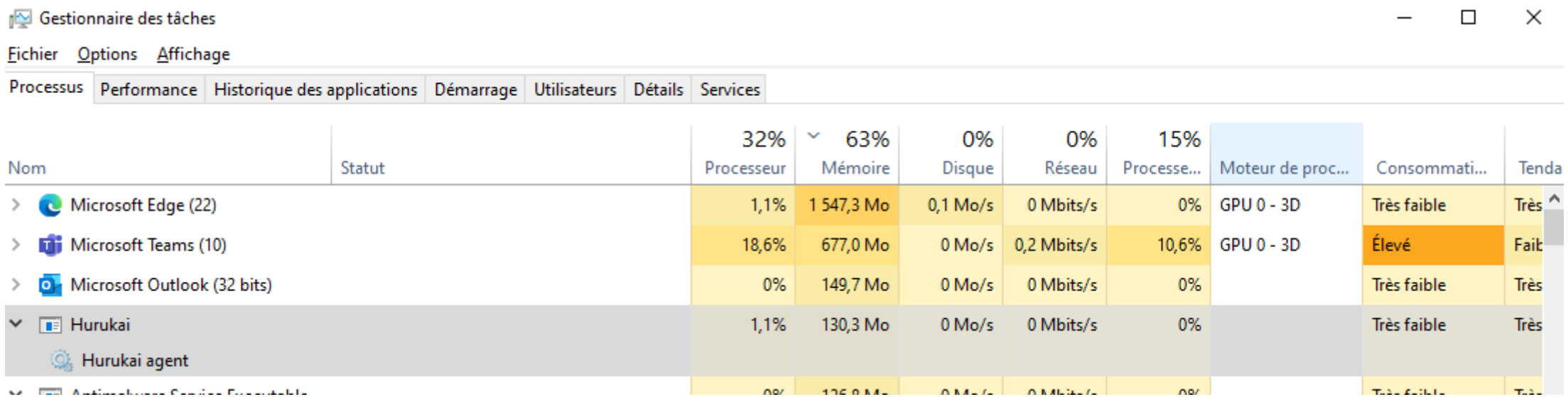
Le premier accès au dashboard

TLP:CLEAR



En parallèle, on a surveillé la consommation des ressources

TLP:CLEAR

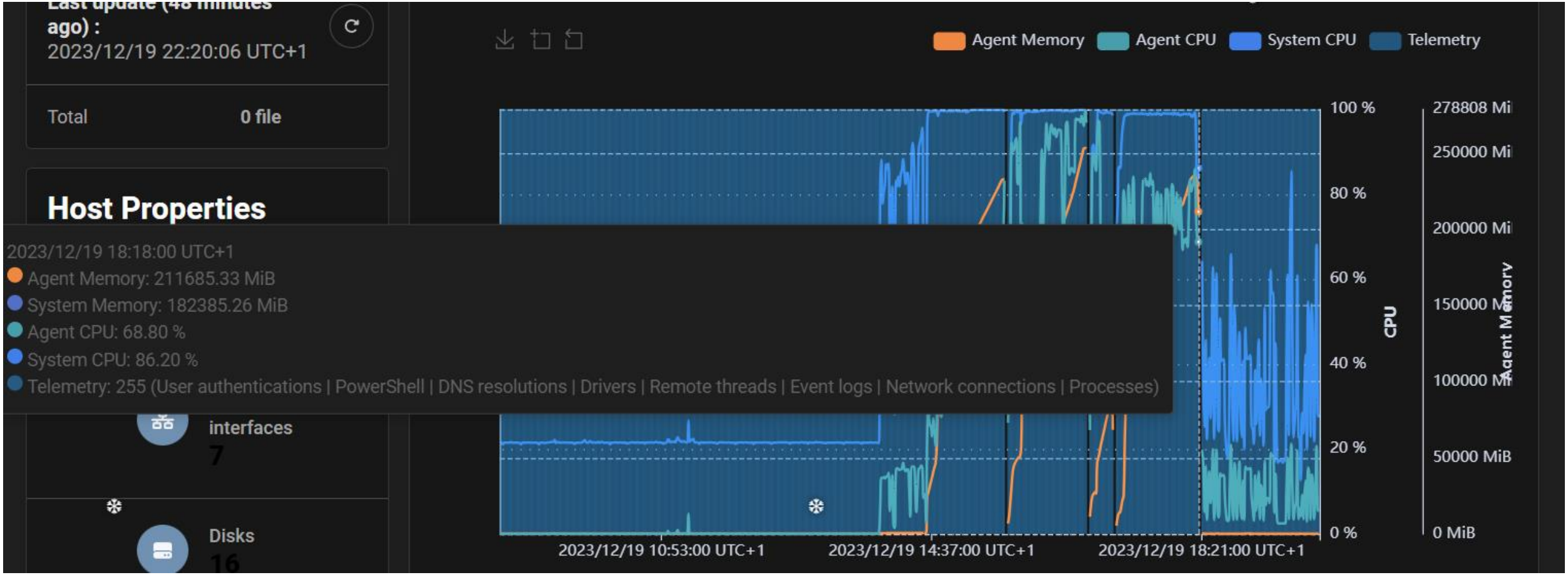


Nom	Statut	32% Processeur	63% Mémoire	0% Disque	0% Réseau	15% Processe...	Moteur de proc...	Consommati...	Tenda
Microsoft Edge (22)		1,1%	1 547,3 Mo	0,1 Mo/s	0 Mbits/s	0%	GPU 0 - 3D	Très faible	Très
Microsoft Teams (10)		18,6%	677,0 Mo	0 Mo/s	0,2 Mbits/s	10,6%	GPU 0 - 3D	Élevé	Faib
Microsoft Outlook (32 bits)		0%	149,7 Mo	0 Mo/s	0 Mbits/s	0%		Très faible	Très
Hurukai		1,1%	130,3 Mo	0 Mo/s	0 Mbits/s	0%		Très faible	Très
Hurukai agent									

En parallèle, on a surveillé la consommation des ressources

TLP:CLEAR

Depuis le déploiement, nous avons eu **2 cas de surutilisation** des ressources d'HarfangLab



En parallèle, on a surveillé la consommation des ressources

TLP:CLEAR

Mais cela s'explique car les serveurs avaient une très grande quantité d'I/O (serveurs de recherche)

TLP:CLEAR

Et la suite…

Situation en mars 2023

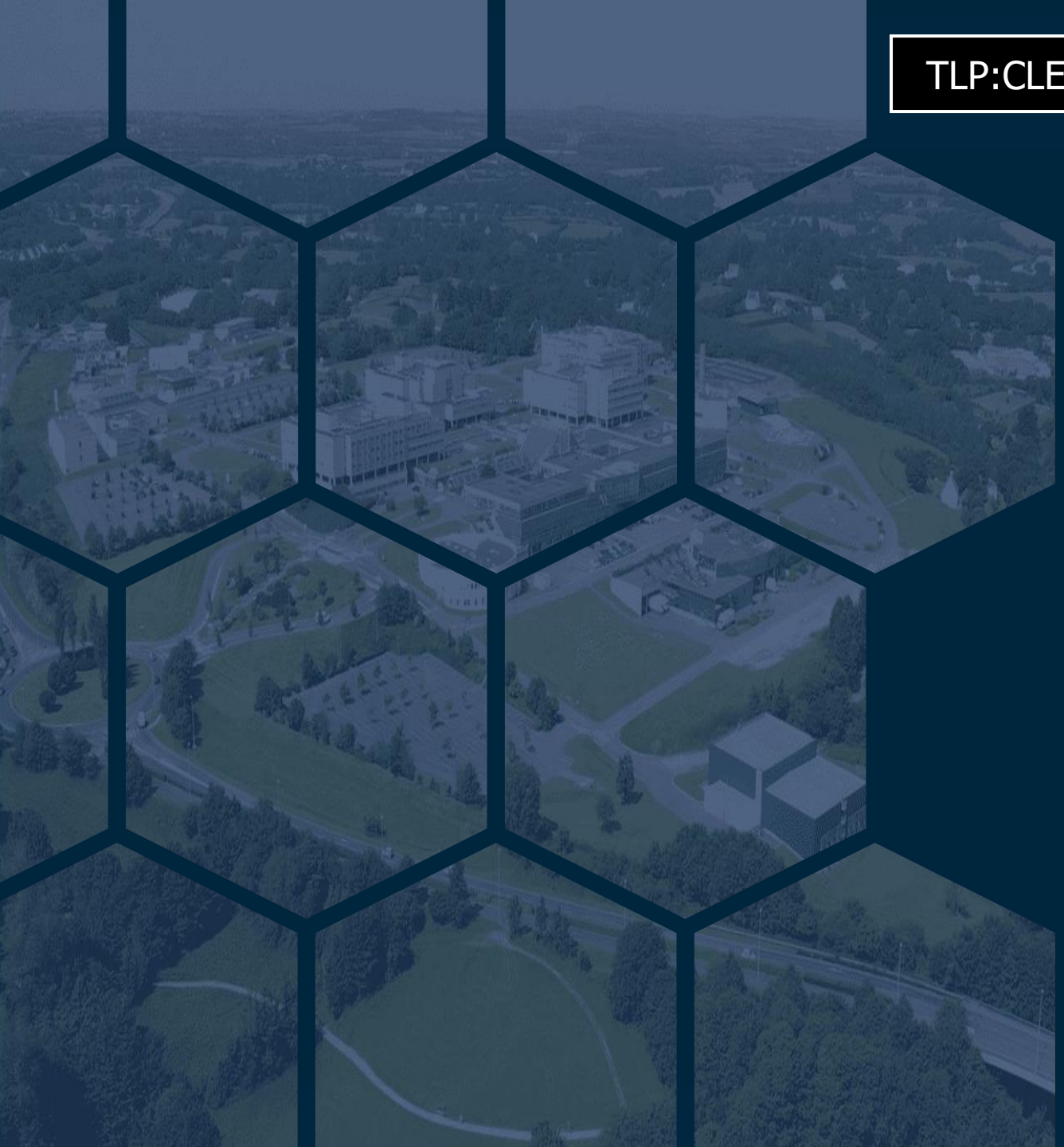
TLP:CLEAR

Début mars 2023, l'EDR était donc déployé sur l'ensemble des postes de travail et une grande partie des serveurs, en mode de détection uniquement.

Puis le 9 mars 2023 arriva…

mars 2023

	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi	Dimanche
9			1	2	3	4	5
10	6	7	8		10	11	12
11	13	14	15	16	17	18	19
12	20	21	22	23	24	25	26
13	27	28	29	30	31		



TLP:CLEAR

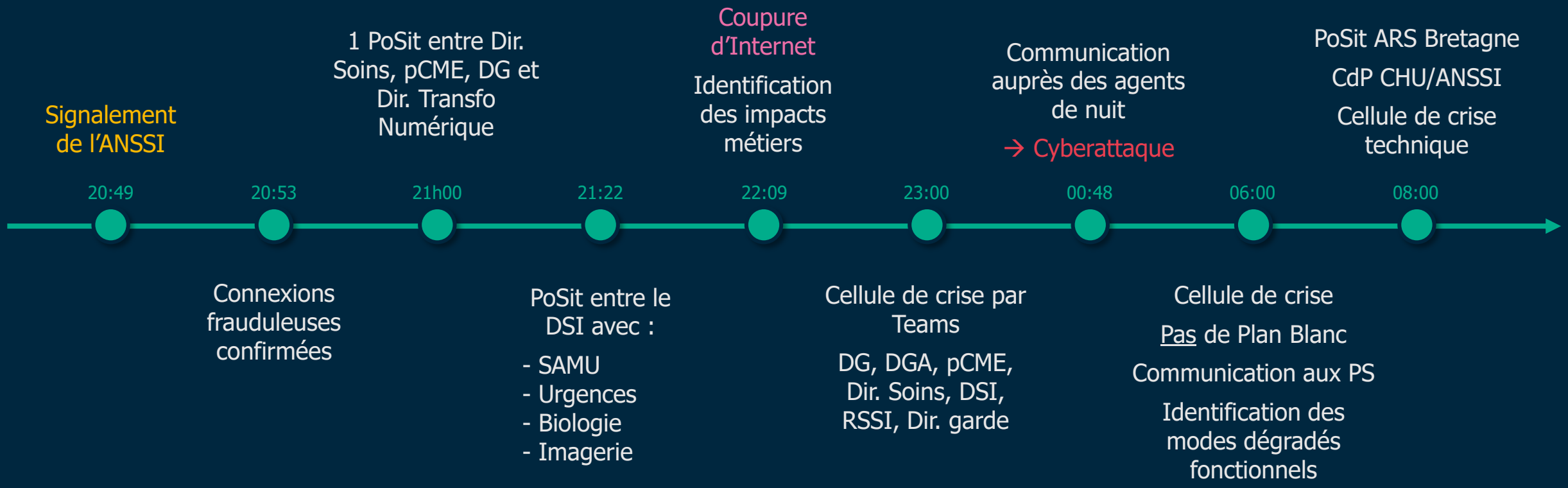
1

Que s’est-il passé ?

Le 9 mars 2023

Les premières heures de la cyberattaque

TLP:CLEAR



Risques identifiés

TLP:CLEAR

Prise de contrôle à distance du SIH

Compromission du domaine du CHU

Possibilité de déploiement d'un rançongiciel

Vol de données sensibles des patients et/ou des collaborateurs.

Perte irréversible des données et des ressources

notamment biomédicales

Intervention du CSIRT

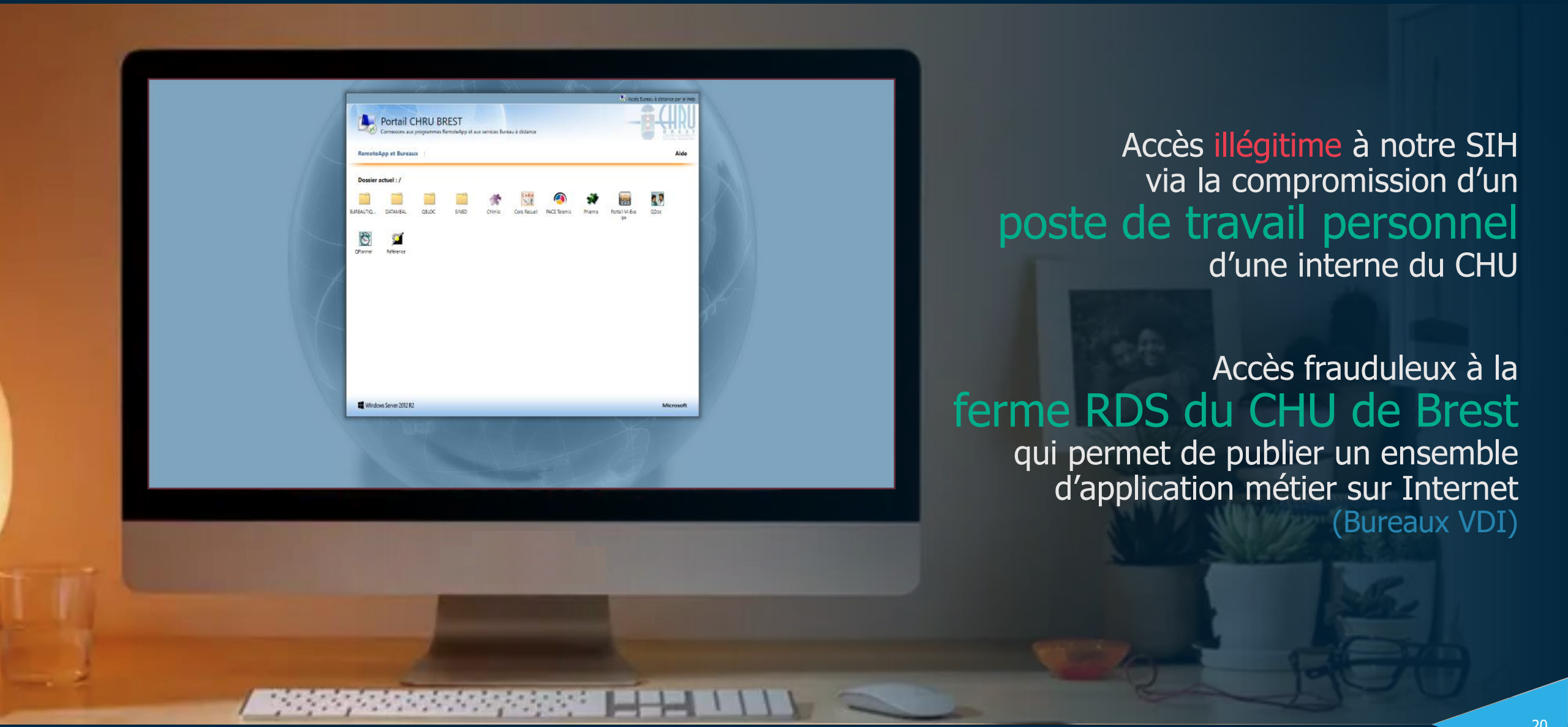
TLP:CLEAR

Dès le vendredi 10 mars 2023, le CSIRT a mis à disposition des ressources afin de conduire les investigations nécessaires à identifier :

- le périmètre de la compromission
- la *root cause*.

La porte d'entrée

TLP:CLEAR

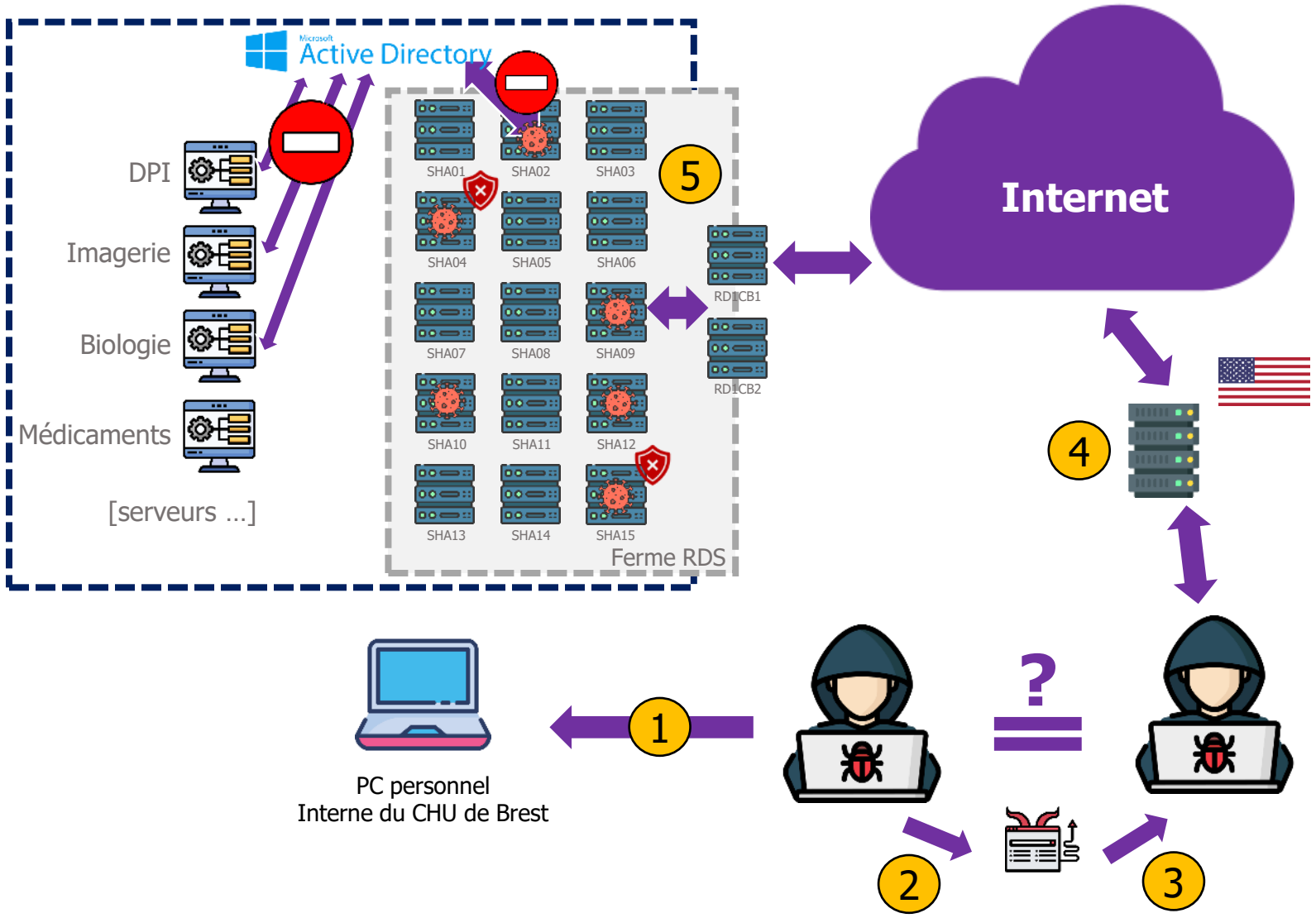


Accès illégitime à notre SIH
via la compromission d'un
poste de travail personnel
d'une interne du CHU

Accès frauduleux à la
ferme RDS du CHU de Brest
qui permet de publier un ensemble
d'application métier sur Internet
(Bureaux VDI)

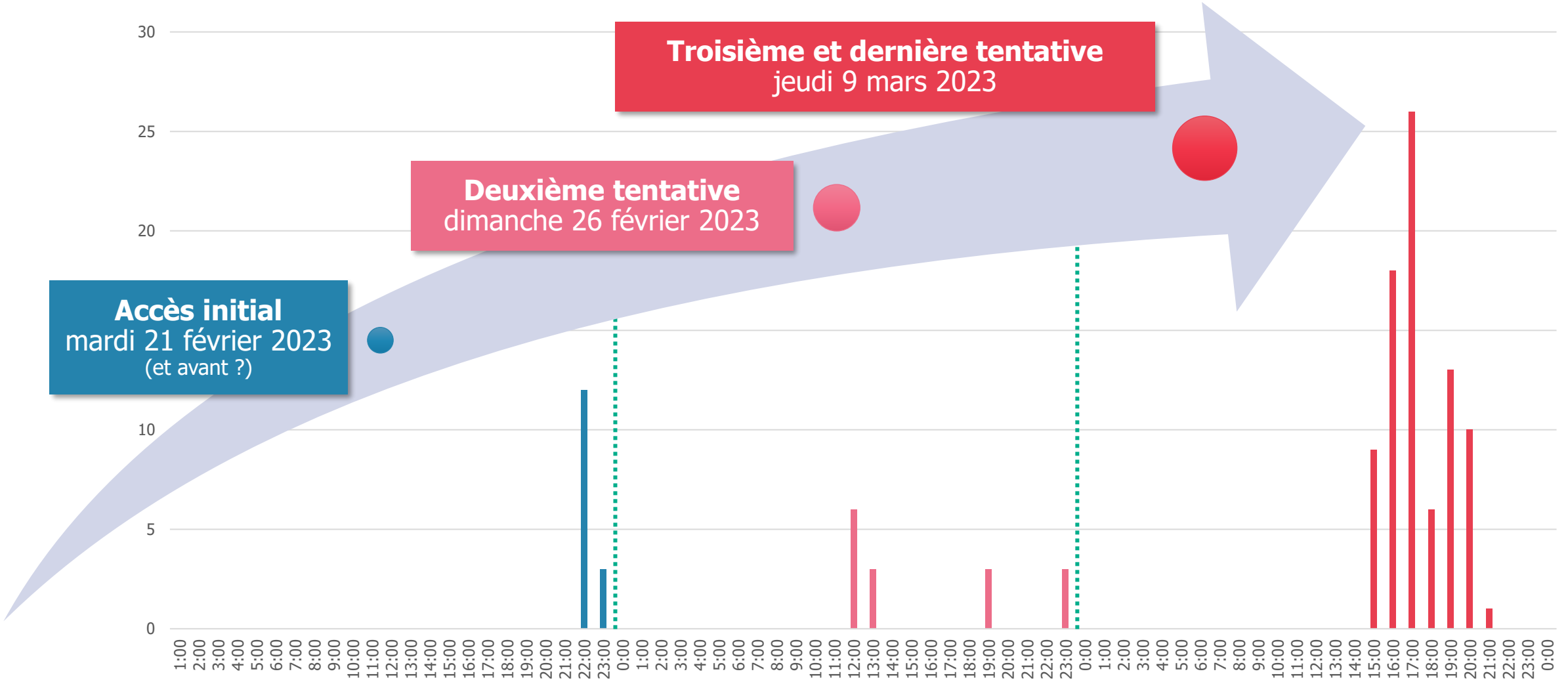
La nature de l'attaque

TLP:CLEAR



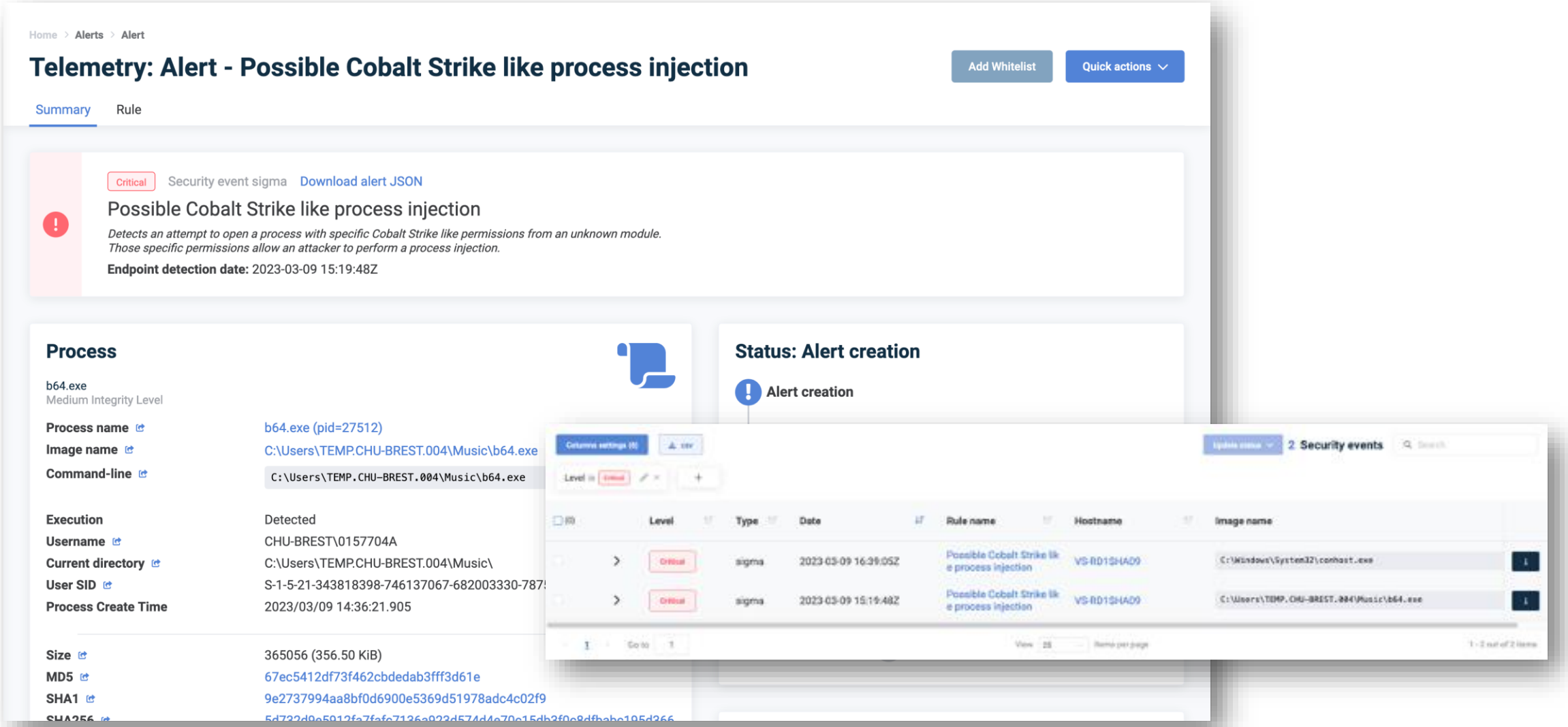
Répartition des actions illégitimes par heure

TLP:CLEAR



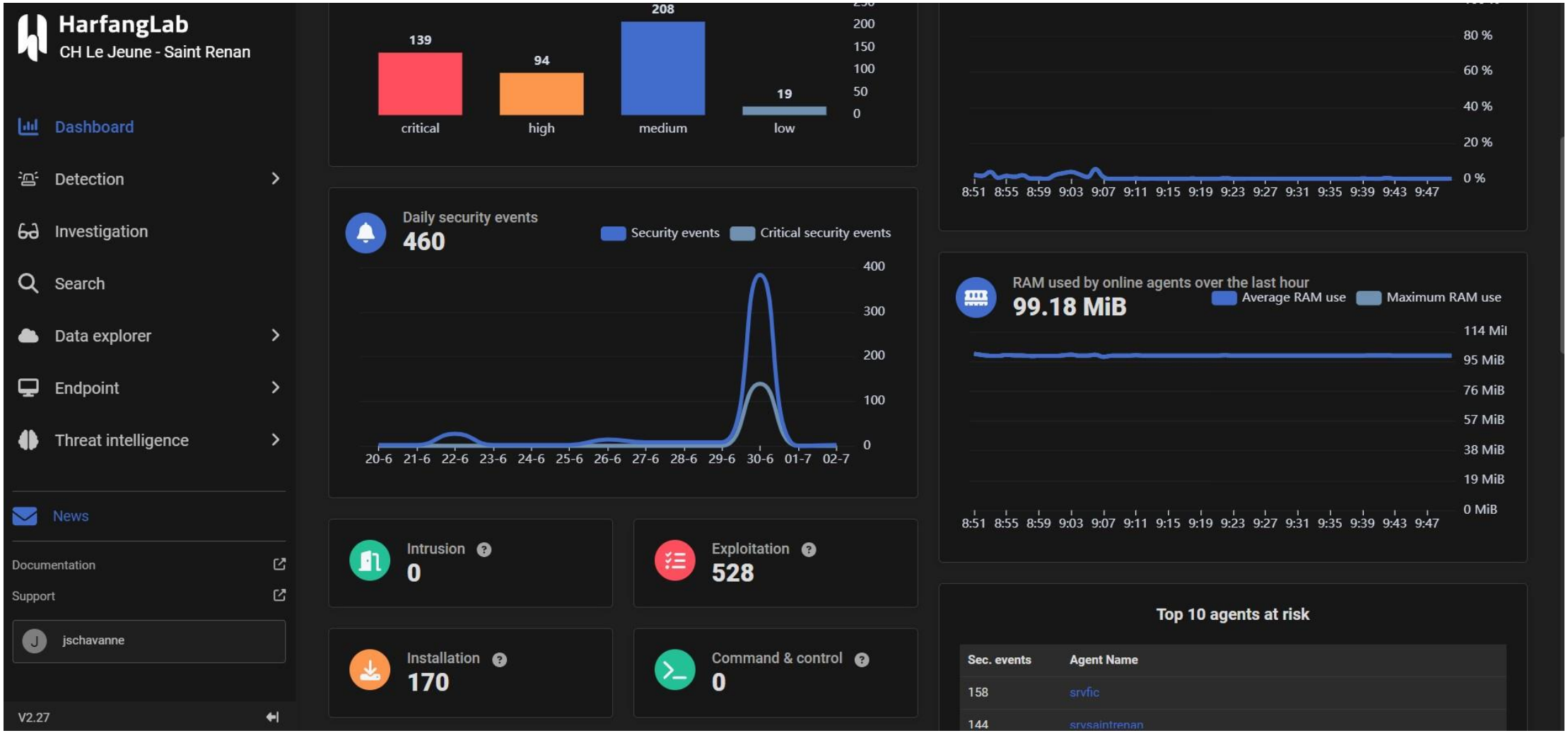
L'EDR me permet de qualifier rapidement l'alerte

TLP:CLEAR



Autre exemple : le CH de Saint-Renan

TLP:CLEAR



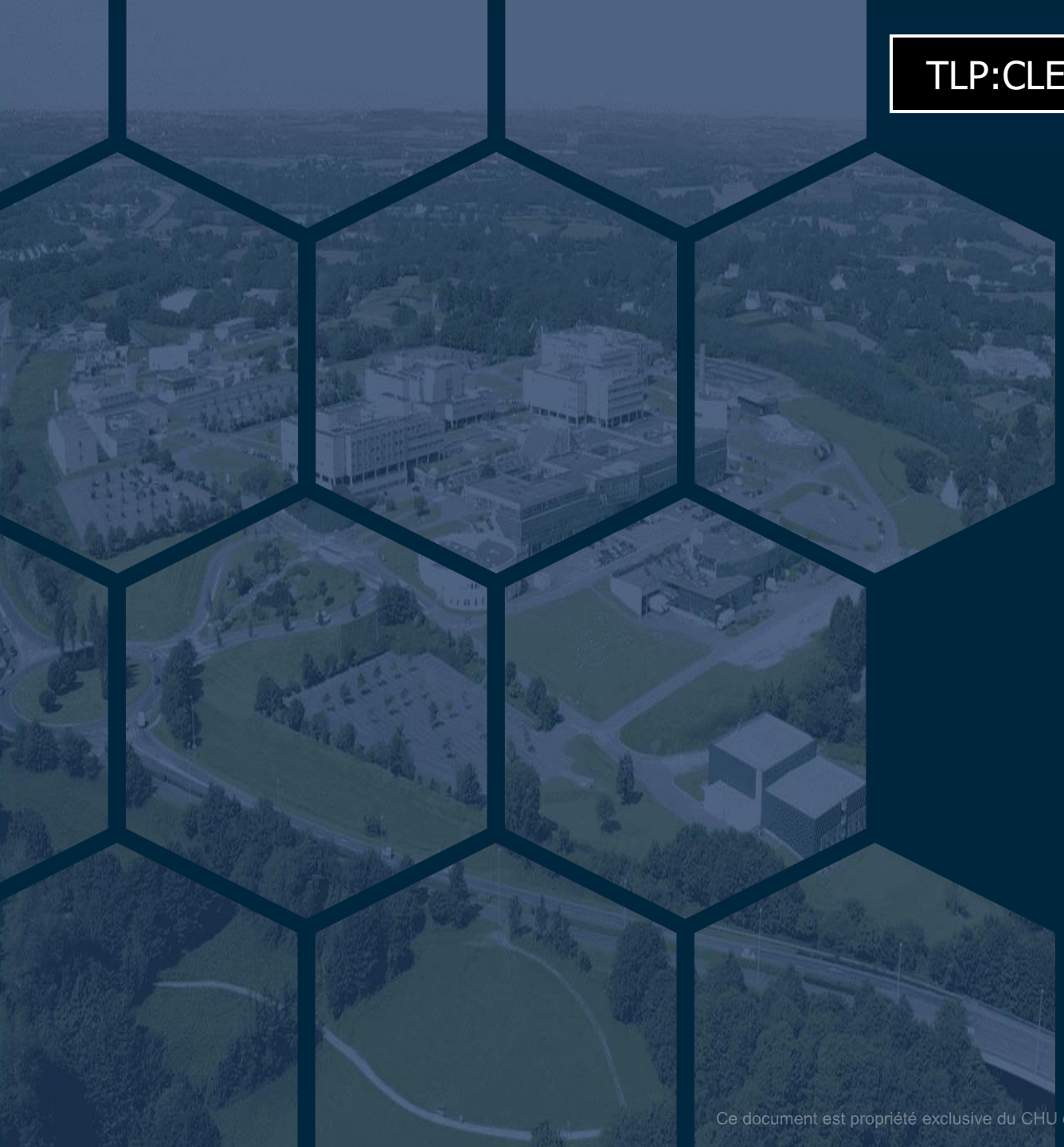
Le passage en crise

TLP:CLEAR

Une fois que l'alerte est qualifiée → les investigations commencent.

Le principal outil à disposition : l'EDR.

TLP:CLEAR



3

Les investigations avec un EDR

Les propriétés d'un EDR

TLP:CLEAR

L'EDR permet de réaliser un grand nombre d'actions comme des prélèvements sur les équipements compromis.

- Identification des commandes passées par l'utilisateur
- Voir les connexions réseaux entre les équipements
- Télécharger de charges actives
- Collecter la mémoire vive de l'équipement
- Collecter la MFT
- Collecter les journaux
- Télécharger des binaires suspects
- Télécharger des scripts malveillants
- …

Si on reprend le CH de Saint-Renan

TLP:CLEAR

Le SIH est entièrement chiffré le vendredi 30/06 à 23h30.

- Les équipes de la DTSN du CHU, le responsable technique ainsi que le RSSI arrivent le matin à 8h pour investiguer.

Sauf que…

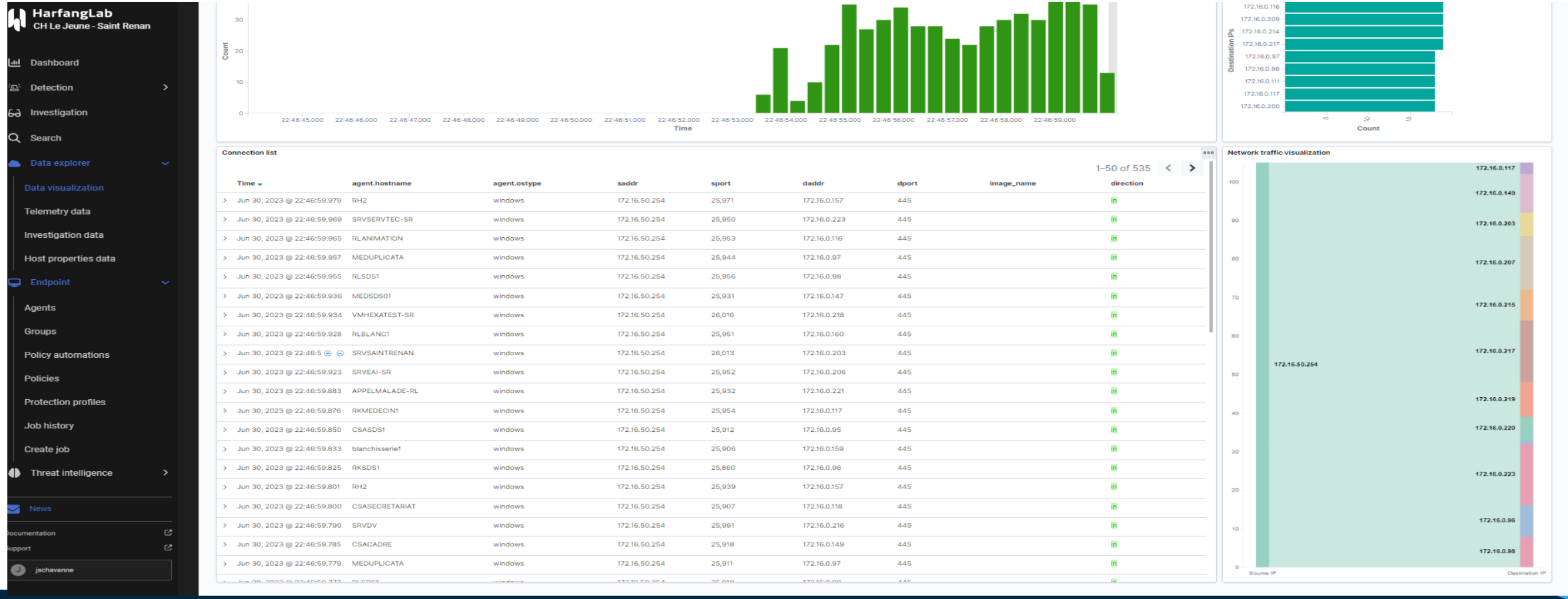
- Aucun accès à l'hyperviseur.
- Le mot de passe du compte **`administrateur`** a été changé par l'attaquant !
- Heureusement, l'EDR enregistre les commandes, notamment les commandes Powershell.

2023-06/30 21:30:28	SRVSAINTRENAN	[edr/process] Exécution de la ligne de commande « psexec.exe -accepteula -nobanner -s \\172.16.0.159 -u HOPITALLEJEUNE\administrateur -p Abc123Abc! -c openrdp.bat »

Les connexions réseaux vues par l'EDR

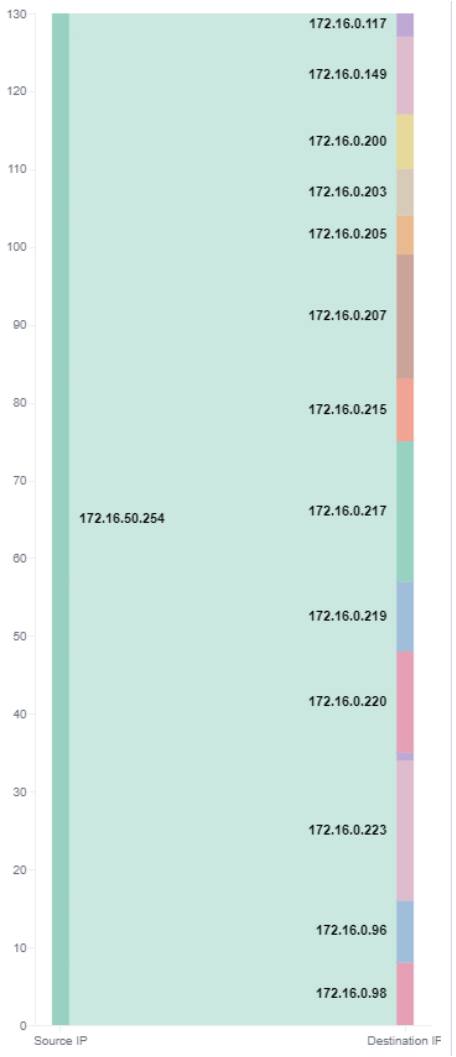
TLP:CLEAR

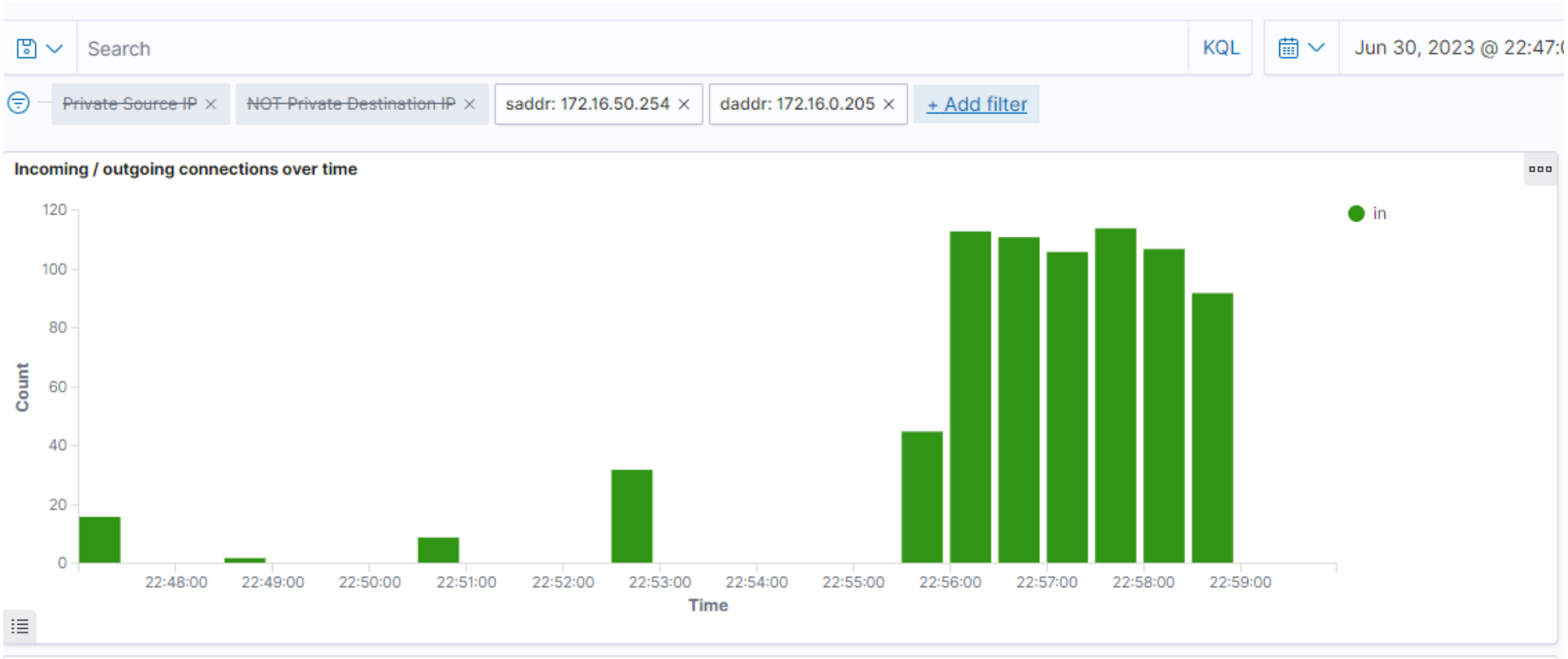
30/06 à 22h46 Scan SMB (port 445 et 3389) sur quasiment 610 IP.



Les connexions réseaux vues par l'EDR

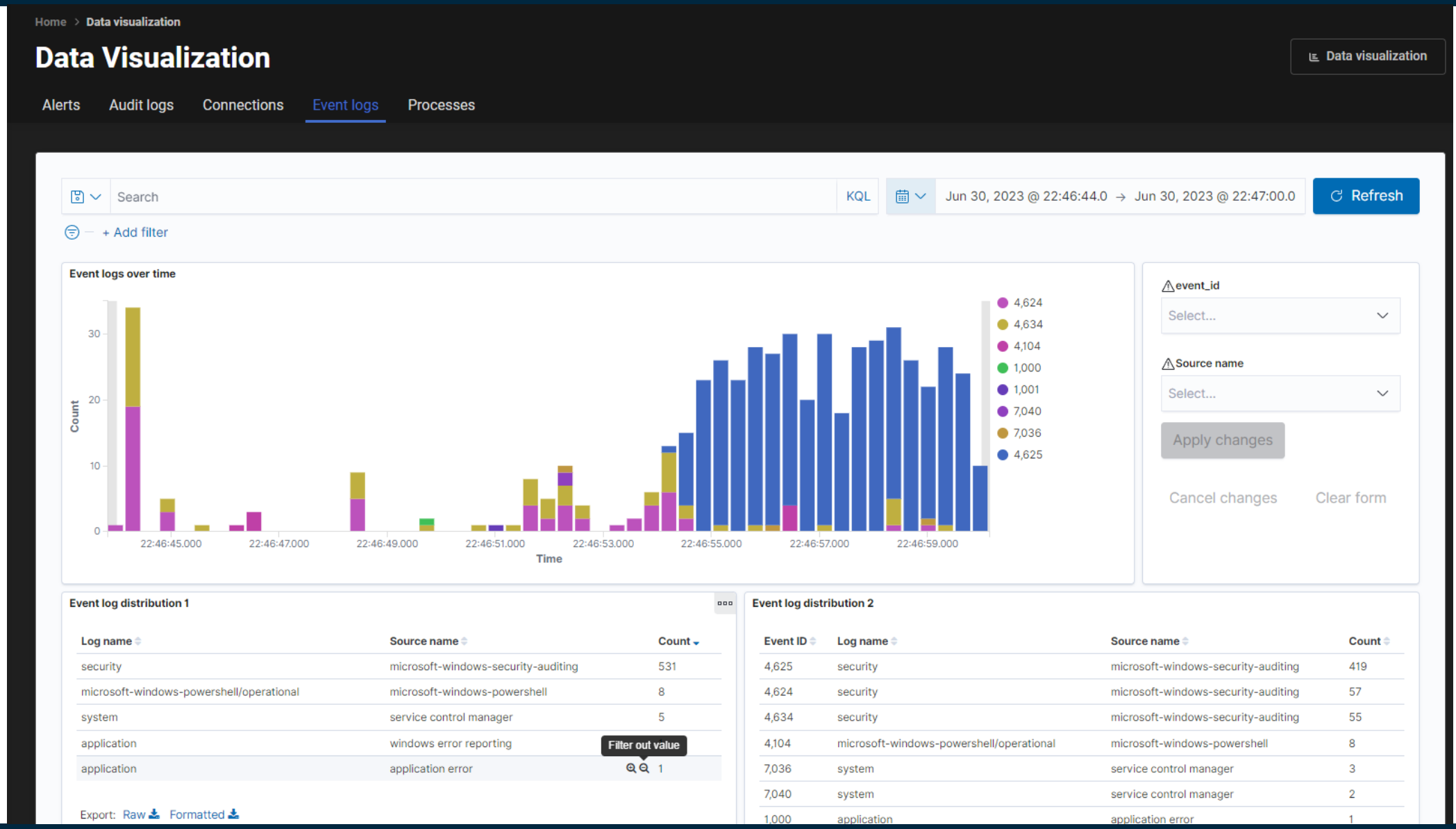
TLP:CLEAR





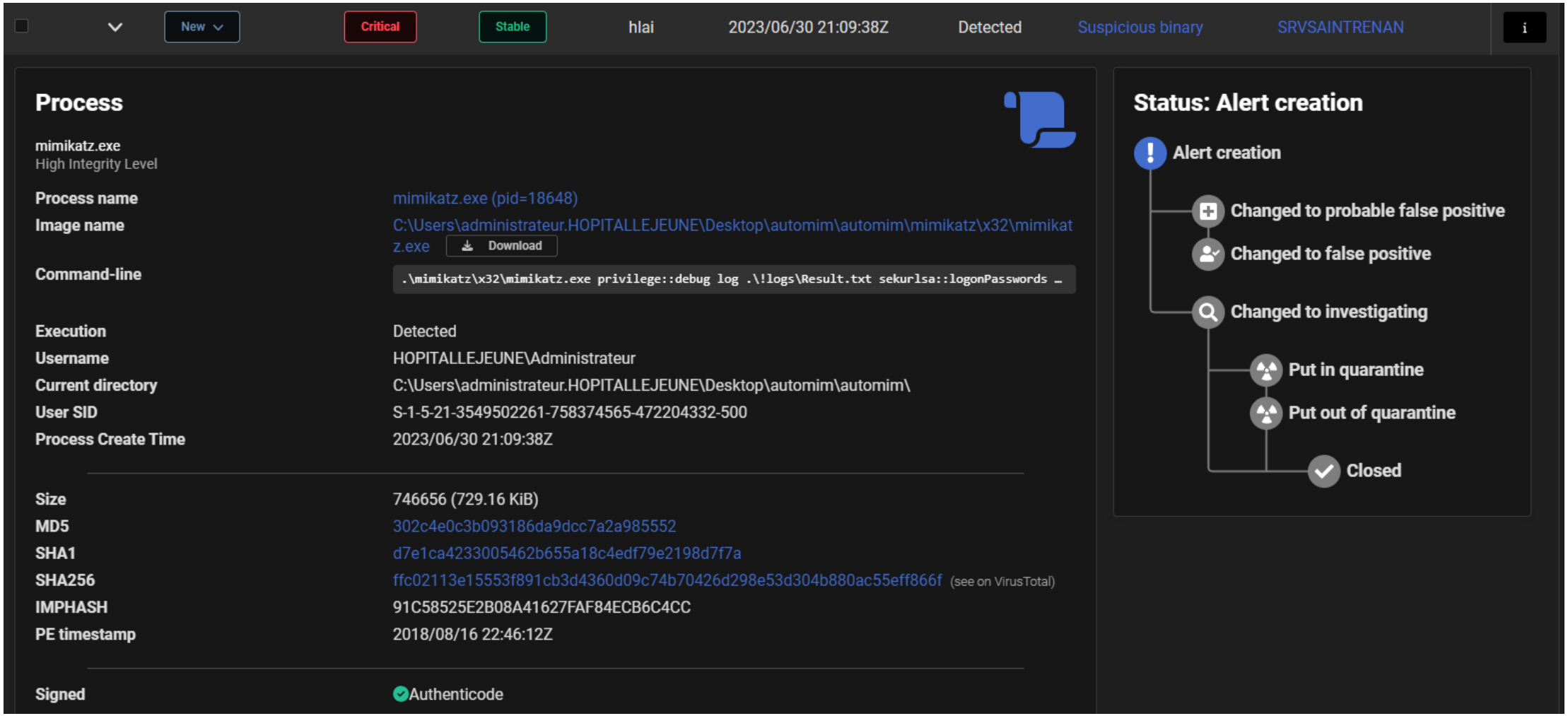
Les journaux Windows vus par l'EDR

TLP:CLEAR



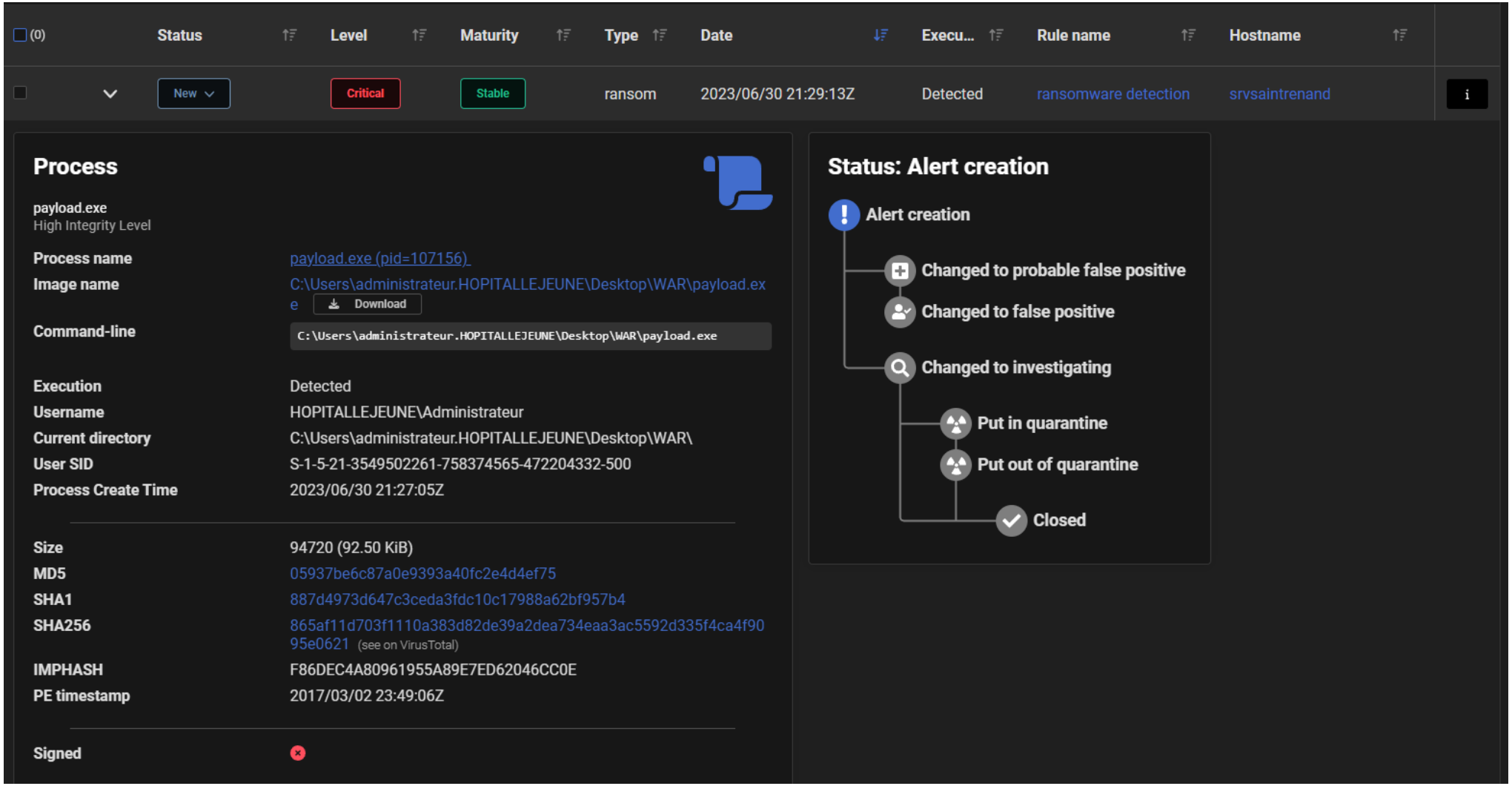
Les alertes de l'EDR

TLP:CLEAR



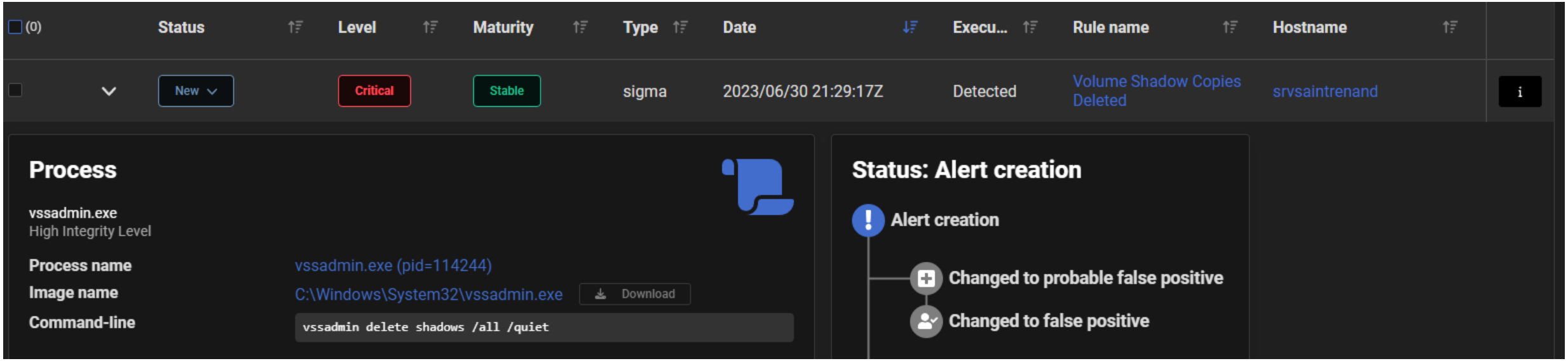
Les alertes de l'EDR

TLP:CLEAR



Les alertes de l'EDR

TLP:CLEAR



Les alertes de l'EDR

TLP:CLEAR

L'EDR permet de commencer à retracer le chemin réalisé par l'attaquant grâce à l'historique des commandes passées et des connexions réseaux.

Concernant les alertes de l'EDR :

- Elles n'ont pas eu le temps d'être traité par le SOC (30 min)
- Elles n'ont pas permis de bloquer l'attaque car l'EDR était en mode « DETECT » et non en mode « PREVENT ».

Conséquence : 1 semaines d'interruption des systèmes d'information hospitaliers pour un CH de 230 lits (205 agents).

L'EDR en mode « BLOCK » aurait probablement pu éviter cet incident.

TLP:CLEAR

Revenons à l’exemple du CHU.

Revenons à l'exemple du CHU : Récupérer de l'information

TLP:CLEAR

5d732d9e5912fa7fafc7136a923d574d4e70c15db3f0c8dfbabc195d3660d4d9 - details

Binary | Security events | Processes | Drivers | Telemetry processes | Persistence | IOC | YARA

Columns settings (7) | csv | Update status | 2 Security events | Search

+ Filter

Status	Level	Type	Execution	Rule name	Hostname	Command-line	
Investigating	Critical	sigma	Detected	Possible Cobalt Strike like process injection	VS-RD1SHA09	C:\Users\TEMP.CHU-BREST.004\Music\b64.exe	i
Investigating	Critical	sigma	Detected	Possible Cobalt Strike like process injection	VS-RD1SHA10	C:\Users\Public\Music\b64.exe	i

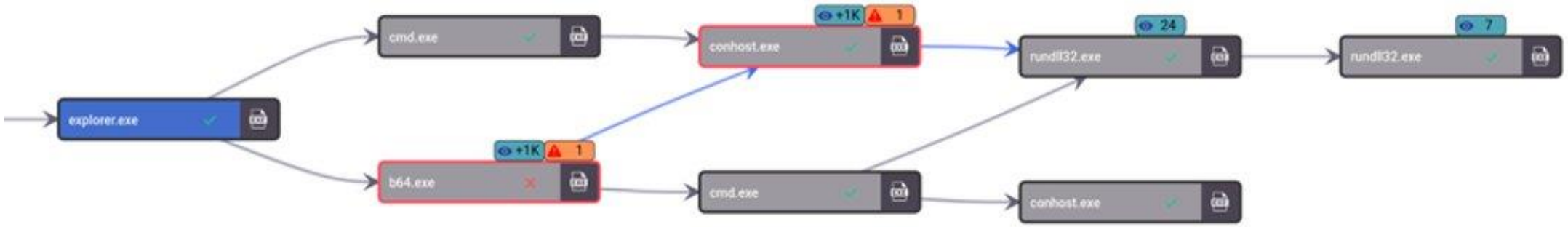
1 | Go to 1 | View 25 Items per page | 1 - 2 out of 2 items

Récupérer de l'information

Beacons Cobalt Strike

VS-RD1SHA09
15h36 GMT+01

MARS
9



- SetUnhandledExceptionFilter detected (possible anti-debug)
- Dynamic (imported) function loading detected
- CAPE extracted potentially suspicious content
- Creates RWX memory
- Performs some HTTP requests
- Network activity detected but not expressed in API logs
- CAPE detected the CobaltStrikeBeacon malware
- Yara rule detections observed from a process memory dump/dropped files/CAPE

Command & Control

youthconscience[.]com

hxxps:*youthconscience[.]com/Remove/x/996NV95ZCC*
*hxxps:*youthconscience[.]com/activate/v3.45/JAIUN0X5L

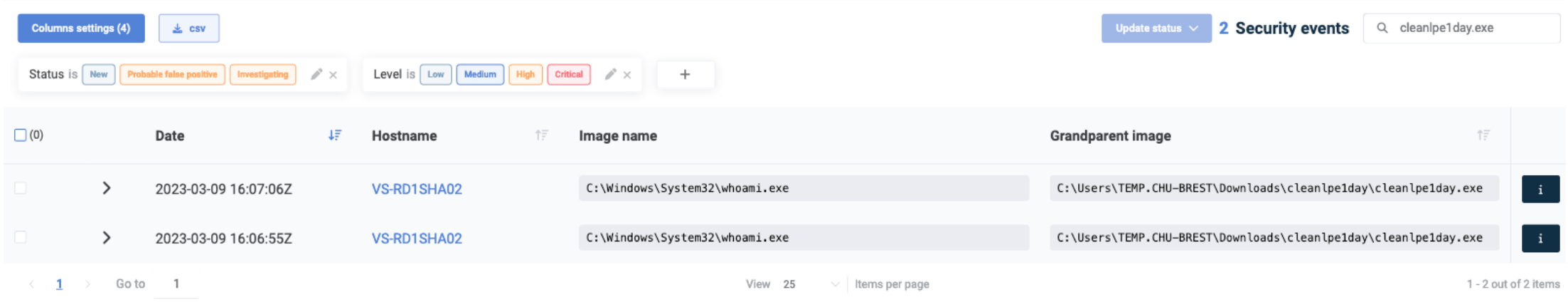
147[.]78[.]47[.]242

Récupérer de l'information

cleanlpe1day.exe

VS-RD1SHA02
17h06 GMT+01

MARS
9



- SetUnhandledExceptionFilter detected (possible anti-debug)
- A file with an unusual extension was attempted to be loaded as a DLL.
- Dynamic (imported) function loading detected
- Creates RWX memory
- Yara rule detections observed from a process memory dump/dropped files/CAPE

Arguments manquants

CVE-2022-24521
Windows Common Log File System

Trigger CLFS bug to overwrite usermode process token to elevate to system privileges

https://www.pixiepointsecurity.com/blog/nday-cve-2022-24521.html

AccountRestore (svchost.exe)

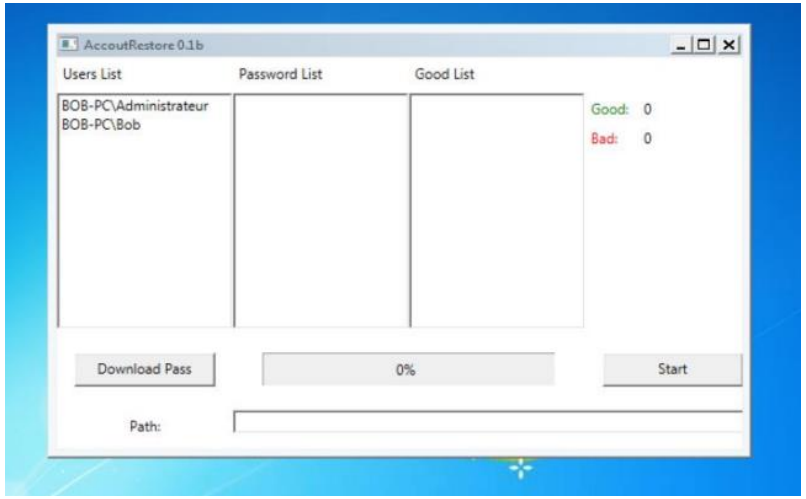
VS-RD1SHA02
17h09 GMT+01
MARS 9

Columns settings (7) | csv | Update status | 2 Security events | Search

+ Filter

Status	Level	Type	Execution	Rule name	Hostname	Command-line	
Investigating	Medium	sigma	Detected	Suspicious match of legitimate executable name	VS-RD1SHA02	C:\Users\TEMP.CHU-BREST\Downloads\svchost\svchost.exe	i
Investigating	Medium	sigma	Detected	Suspicious parent process for system process	VS-RD1SHA02	C:\Users\TEMP.CHU-BREST\Downloads\svchost\svchost.exe	i

- Collects and encrypts informations about the computer likely to send to C2 server
- SetUnhandledExceptionFilter detected (possible anti-debug)
- Guard pages use detected – possible anti-debugging
- Dynamic (imported) function loading detected
- Access the NetLogon registry key, potentially used for discovery or tampering
- Creates RWX memory
- Exhibits possible ransomware or wiper file modification behavior: overwrites_existing_files



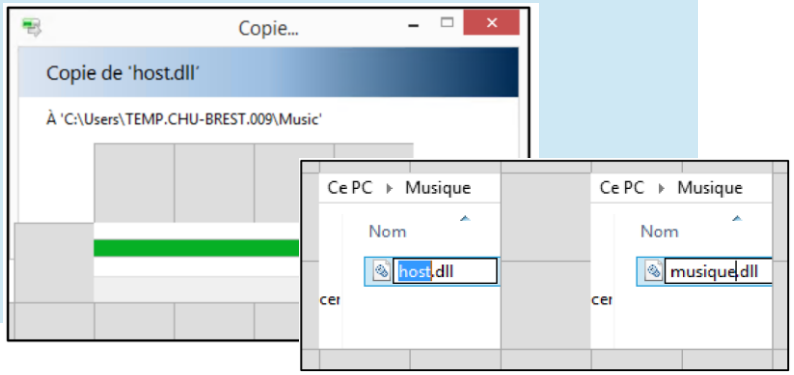
Comprendre les opérations de l'attaquant

VS-RD1SHA09/02
Entre 15h30 et 17h20 GMT+01

MARS
9

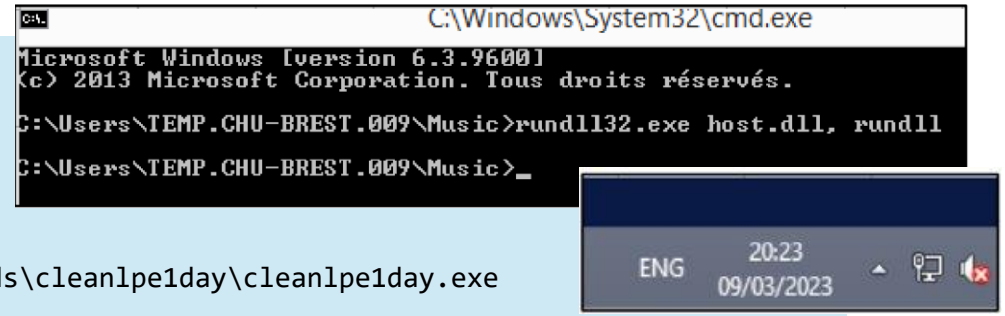
Historique de commande SHA09

```
2023-02-26 22:29:54.227     CHU-BREST\0157704A      net group /domain
2023-02-26 22:30:23.963     CHU-BREST\0157704A      net group Admins du domaine /domain
2023-03-09 14:31:45.243     CHU-BREST\0157704A      nslookup google.com
2023-03-09 14:32:03.840     CHU-BREST\0157704A      nltest /dclist:chu-brest.fr
2023-03-09 14:49:49.385     CHU-BREST\0157704A      net local admin access /domain
2023-03-09 14:50:37.496     CHU-BREST\0157704A      net user 0157704A /domain
2023-03-09 14:58:31.947     CHU-BREST\0157704A      rundll32.exe host.dll, rundll
2023-03-09 14:58:31.962     CHU-BREST\0157704A      rundll32.exe host.dll, rundll
2023-03-09 15:05:15.812     CHU-BREST\0157704A      ping RD1.chu-brest.fr
```



Historique de commande SHA02

```
2023-03-09 16:04:17.792     CHU-BREST\0157704A      cleanlpe1day.exe
2023-03-09 16:04:52.749     CHU-BREST\0157704A      net user supp Supp@123 /add
2023-03-09 16:05:01.438     CHU-BREST\0157704A      mmc
2023-03-09 16:05:54.140     CHU-BREST\0157704A      net user SinedCron Supp@111!
2023-03-09 16:06:40.689     CHU-BREST\0157704A      net user SinedCron Supp@111!
2023-03-09 16:06:55.226     CHU-BREST\0157704A      whoami
2023-03-09 16:07:01.429     CHU-BREST\0157704A      C:\Users\TEMP.CHU-BREST\Downloads\cleanlpe1day\cleanlpe1day.exe
2023-03-09 16:07:06.260     CHU-BREST\0157704A      whoami
2023-03-09 16:07:14.212     CHU-BREST\0157704A      C:\Users\TEMP.CHU-BREST\Downloads\cleanlpe1day\cleanlpe1day.exe
2023-03-09 16:07:20.043     CHU-BREST\0157704A      whoami
2023-03-09 16:07:22.965     CHU-BREST\0157704A      C:\Users\TEMP.CHU-BREST\Downloads\cleanlpe1day\cleanlpe1day.exe
2023-03-09 16:07:38.385     CHU-BREST\0157704A      net user supp @Supp11@32 /add
```



Retrouver la confiance dans son SI

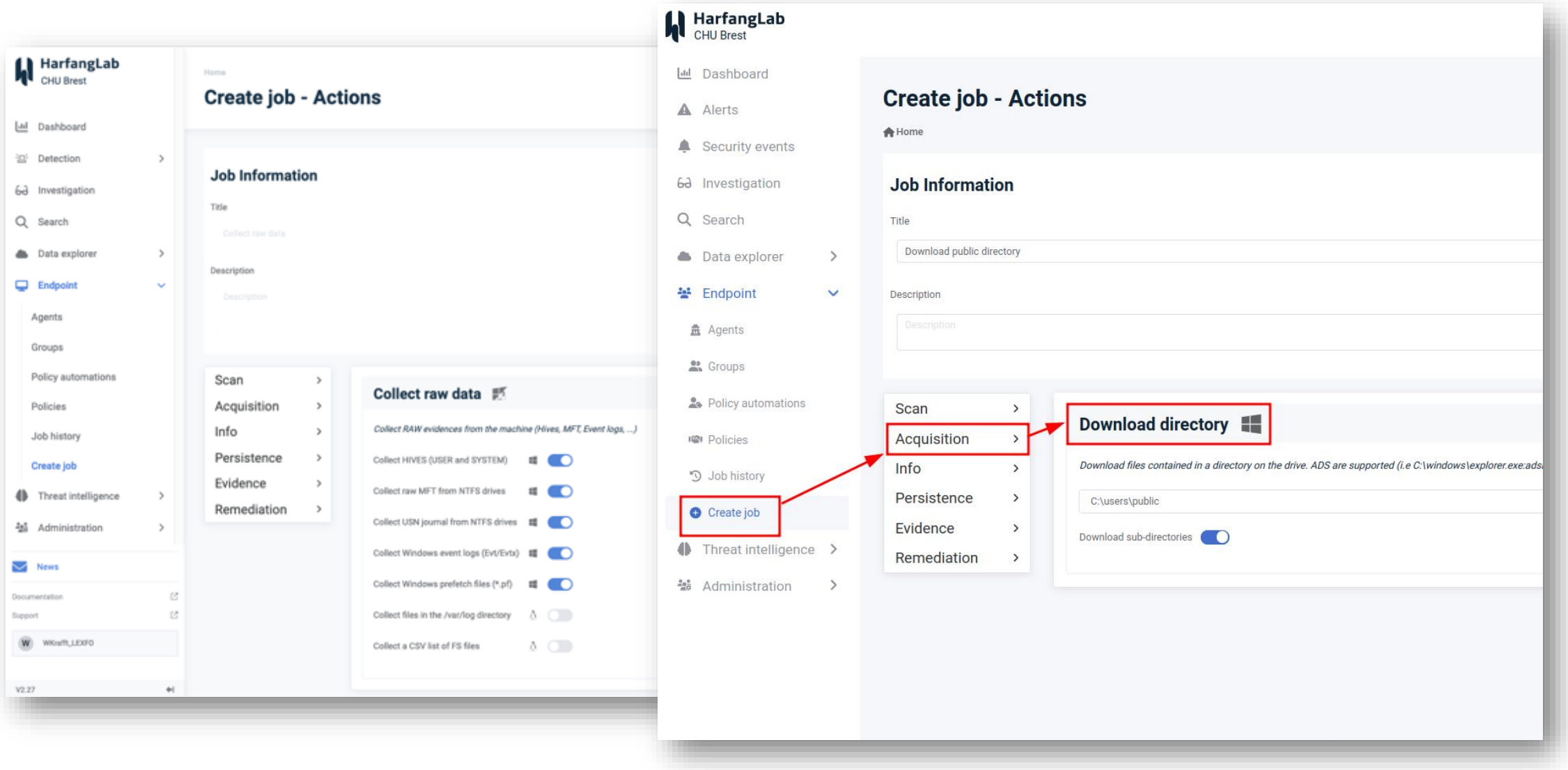
TLP:CLEAR

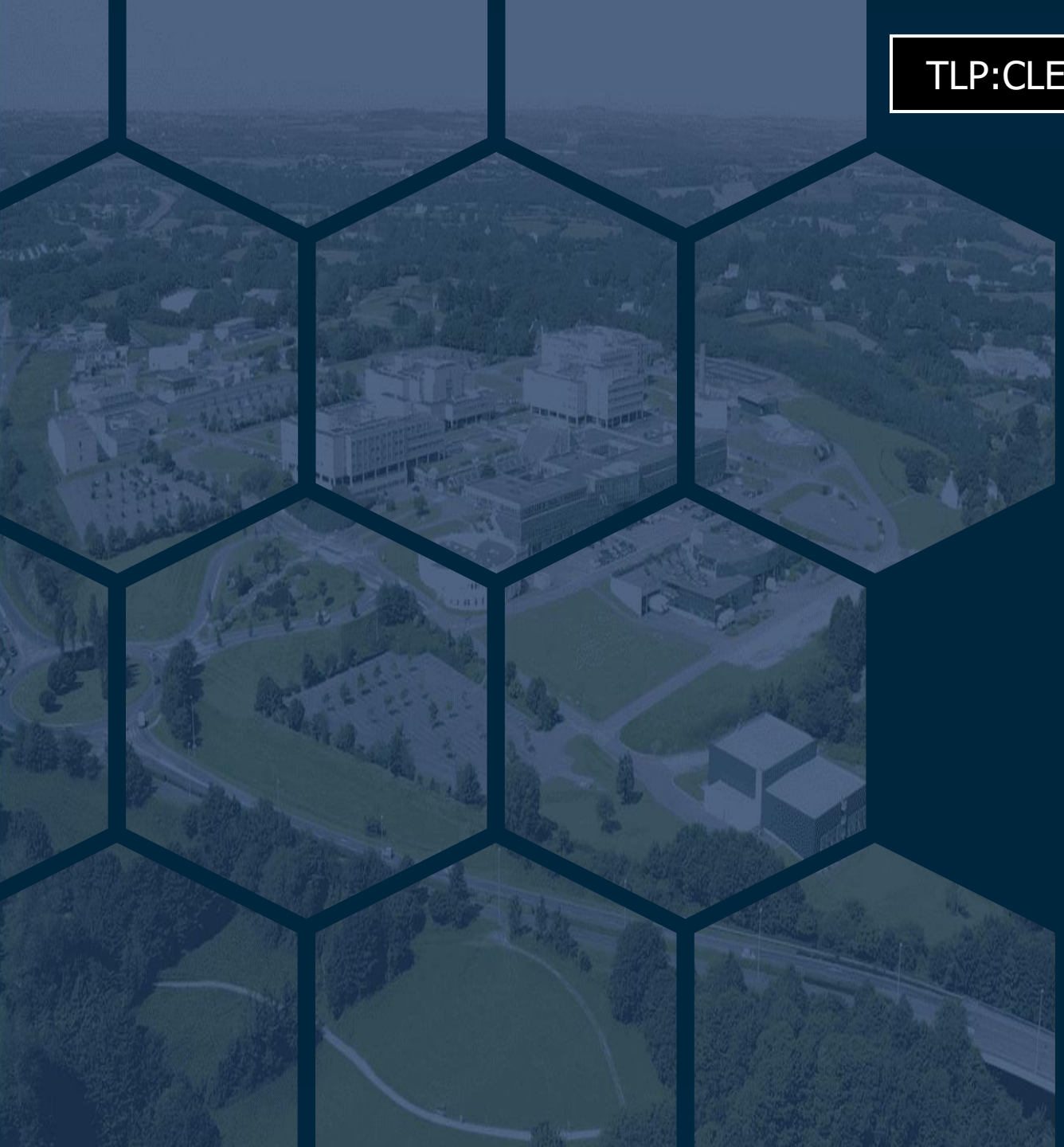
- L'EDR permet également de s'assurer que les attaquants n'ont pas disséminé de code malveillant sur l'ensemble du parc.

- Grâce à des « jobs », il est possible de scanner l'ensemble du parc à la recherche :
  - D'entrées malveillantes dans la base de registre
  - De fichiers déposés sur les postes de travail etc.

Puis explorer l'ensemble du parc.

TLP:CLEAR





TLP:CLEAR

2

Les mesures de remédiation

TLP:CLEAR

Mais comment s’assurer que le menace n’est plus là si l’EDR n’est pas installé sur l’ensemble des équipements ?

Il faut couvrir les angles morts

Il manque des serveurs et des PdT !

TLP:CLEAR

En effet, notamment dans le domaine biomédical, les éditeurs sont très réticents à mettre des AV / EDR sur leurs serveurs et pdt qui sont déployés au sein du CHU de Brest.

Donc…

Angles morts.

La phase de remédiation

TLP:CLEAR

- Pour reprendre une activité nominale et faire que le RSSI soit en confiance, l'ensemble des équipements biomédicaux pouvant accueillir l'EDR l'ont installé.

- Résultat : Aucun effet de bord sur les équipements.

- L'incident de sécurité a donc permis d'augmenter mon niveau de visibilité sur l'ensemble des équipements.

Passage en mode prévention (PREVENT)

TLP:CLEAR

- Il s'agit d'une **politique de blocage** identique pour les établissements de santé.

- Règle **SIGMA**
  - Permet de détecter un malware sur ce qu'il fait (se base sur l'analyse de logs) – Ex : exécution d'un script powershell
  - Import depuis un MISP (1 324 règles)
  - *Paramètre :* Alerte et bloque
- Règle **IoC**
  - Permet de détecter des fichiers provenant d'IoC de CERT par exemple
  - *Paramètre :* Alerte et bloque
- Règle **YARA**
  - Détecte les malwares sur sa structure (modèles textuels ou binaires)
  - Règles locales (163 règles) et import depuis un MISP (190 règles)
  - *Paramètre :* Alerte et bloque
- Règle **HL-AI**
  - Le moteur HL-AI est le moteur de détection à base d'intelligence artificielle développé par HarfangLab.
  - *Paramètre :* Alerte et bloque (bloque uniquement les alertes CRITIQUE)
- Règle **Ransomguard**
  - Il crée des fichiers canaris et surveille toute modification, chiffrement ou supression anormale de ces fichiers qui peut intervenir pendant une attaque par ransomware.
  - *Paramètre :* Alerte et bloque

Les enseignements d'un tel incident

TLP:CLEAR

La cyberattaque a accéléré drastiquement la mise en œuvre des mesures de cybersécurité qui étaient prévues à la suite d'une analyse de risque

Plan de sécurisation sur 3 ans réalisé en 6 mois

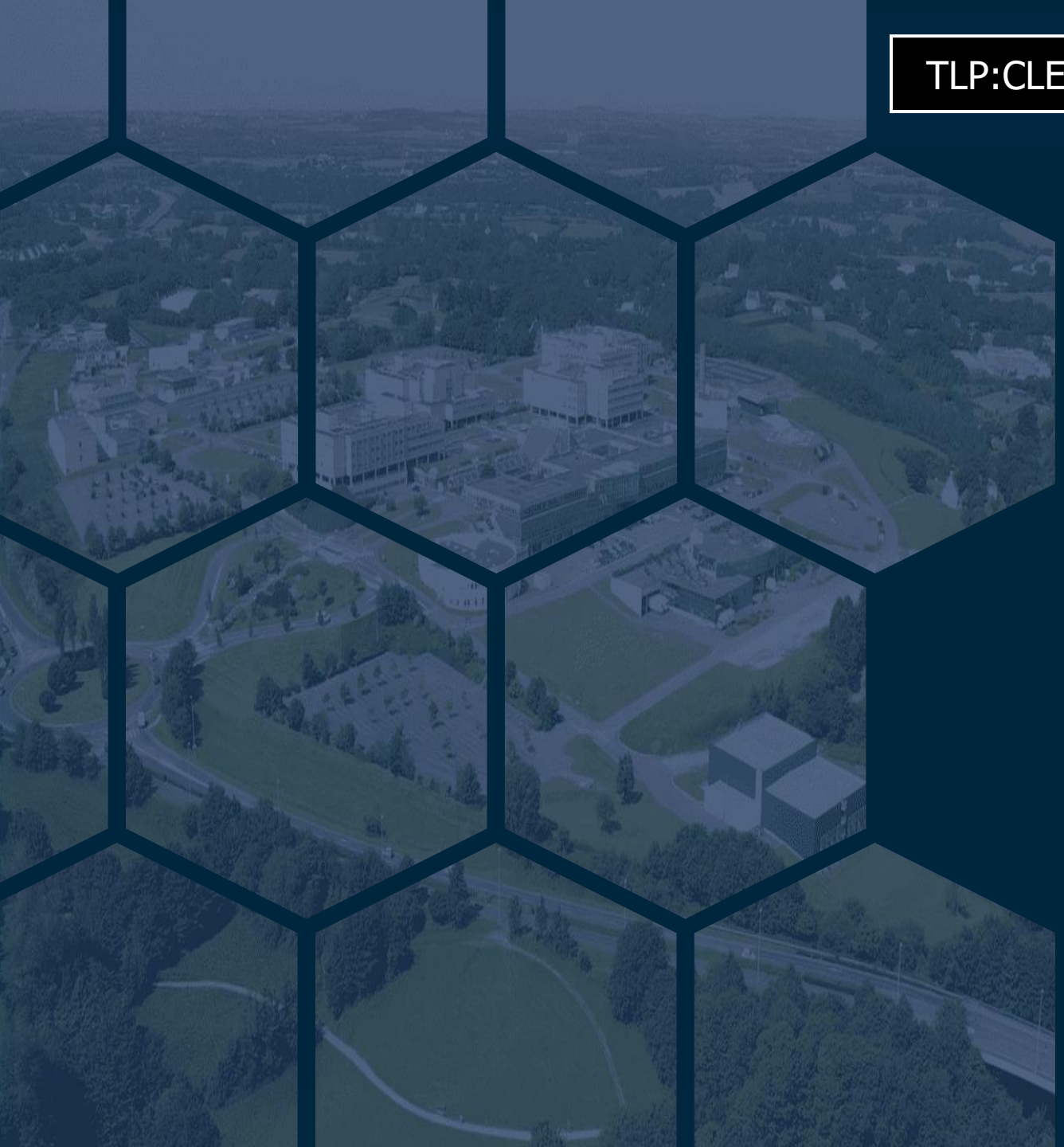
L'incident a permis de mettre en exergue la possibilité de faire des changements structurels qui semblaient impossibles à cause des répercussions potentielles

Changement de proxy/reverse proxy

Suppression des comptes Domain Admin

EDR sur les équipements biomédicaux

L'ensemble de ces mesures a pu se faire grâce à l'implication de l'ensemble des équipes de la DSI (qui était sensibilisées aux cybermenaces) et à l'aide des établissements de santé du territoire



TLP:CLEAR

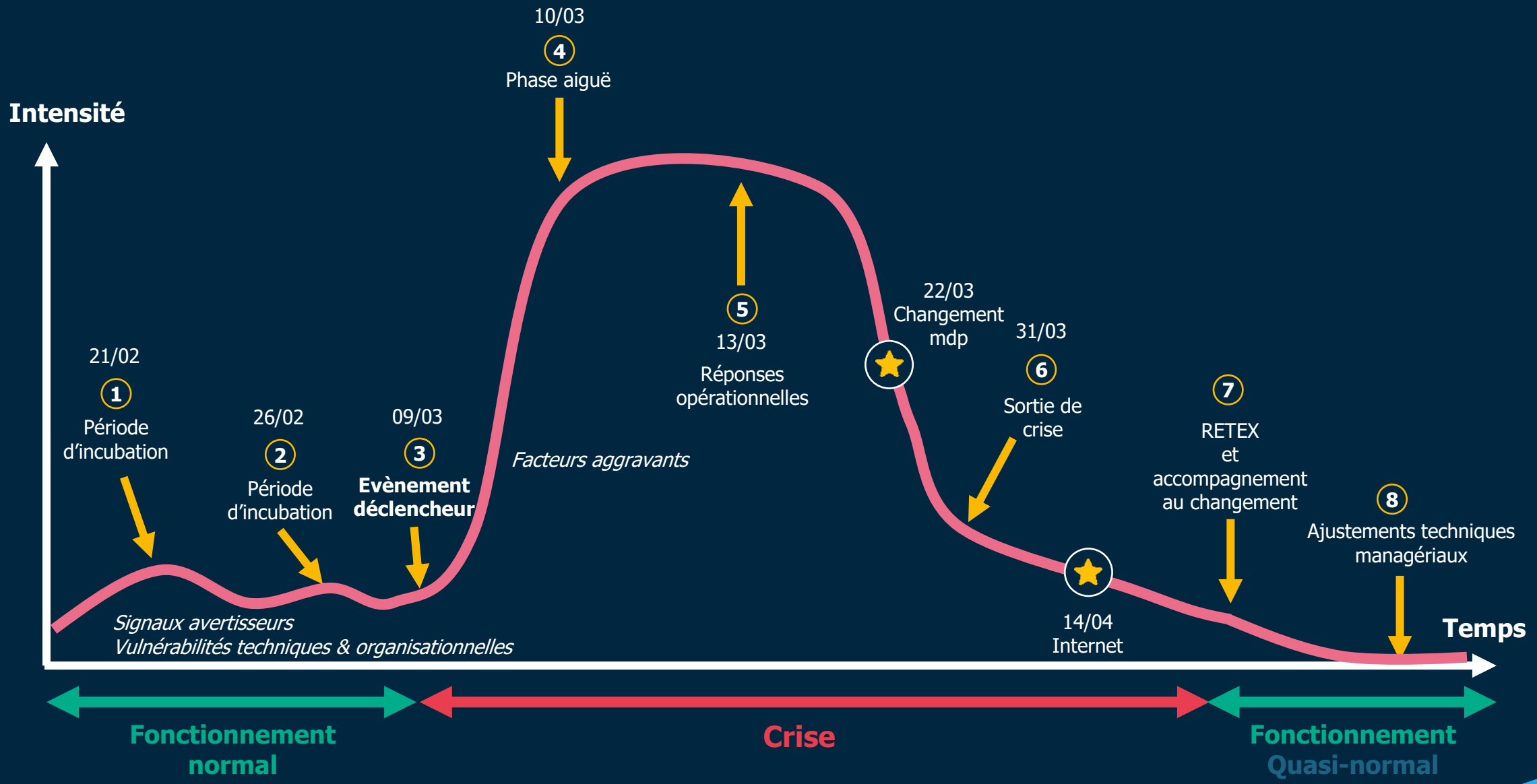
4

Conclusion

L’EDR, un outil central pour la réponse à incident

Les étapes de la gestion de crises numérique

TLP:CLEAR



Conclusion du retour d'expérience

TLP:CLEAR

- **J-16 :** Premières opérations des attaquants
- **J-11 :** Deuxième tentative des attaquants
- **J :** Elément déclencheur de la crise – coupure Internet. Début des mesures de remédiation de l'ANSSI/CHU.
- **J+1 :** Début des investigations du PRIS.
- **J+8 :** Fin des investigations. Identification du périmètre compromis terminé.
- **J+22 :** Fin officielle de la gestion de crise.
- **J+36 :** Réouverture d'Internet au CHU

Résultats et éléments clés

Réaction rapide du CHU de Brest grâce à l'alerte de l'ANSSI

Identification rapide du mode opératoire et du périmètre de compromission par LEXFO

Réouverture des services validés collégialement

Compromission effective grâce à une identification simple facteur

Utilisation d'outil grand public pour les opérations de reconnaissance

Compromission stoppée car les mises à jour de correction des vulnérabilités sont appliquées

Points à retenir

Importance de la collaboration dans la réponse à incident (ANSSI, CSIRT, ARS et le CHU).

Collaboration sur les investigations entre le CHU / ANSSI / LEXFO (via l'EDR HarfangLab)

Identification rapide du périmètre de compromission permet de donner une perspective de reprise aux services de soins et administratifs

Entraîner les équipes IT à réaliser des relevés de journaux et à réaliser les premiers gestes (isolation de sauvegardes par exemple) sur les outils à disposition

Mise en place d'un canal unique de communication pour les agents pour identifier les effets de bord.

Conclusion

TLP:CLEAR

Les différents rôles de l'EDR sur le système d'information hospitalier du CHU

- Avant une cyberattaque :
  - Permet d'empêcher les attaquants d'exécuter les charges malveillantes et de récupérer des informations
  - Permet de s'assurer que les éditeurs respectent bien les bonnes pratiques de cybersécurité
  - Permet de supprimer les logiciels pirates des utilisateurs

- Pendant une cyberattaque :
  - Permet de récupérer de l'information sur le mode opératoire de l'attaquant (d'effectuer de passe des comptes à privilèges)
  - Permet d'effectuer des recherches sur un large périmètre (via règles YARA notamment)

- Après une cyberattaque :
  - Permet de s'assurer que les modes opératoires repérés précédemment seront immédiatement détectés et bloqués.

TLP:CLEAR

Merci pour votre attention.

Jean-Sylvain CHAVANNE
RSSI du CHU de Brest
rssi@chu-brest.fr

C.H.U Brest - Site de Morvan
2 avenue Foch
29609 BREST Cedex

CHU BREST
CENTRE HOSPITALIER UNIVERSITAIRE