Post-Mortem d'une cyberattaque : Méthodologie Forensic

30/01/2025

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS

technobel

TABLE DES MATIÈRES :

Introduction

Le projet Maker-Hub s'inscrit dans une démarche pédagogique et professionnelle visant à démontrer la maîtrise des compétences acquises au cours de la formation de consultant en cybersécurité orienté SecOps du centre de formation Technobel.

Ce projet, conçu pour un jury de professionnel, repose sur le choix d'une thématique technique : la méthodologie forensic.

L'objectif principal est la mise en place d'un réseau modulaire sécurisé, construit selon le principe du Security by Design. Cette approche garantit que la sécurité est intégrée dès les premières étapes de conception, réduisant ainsi les vulnérabilités exploitables.

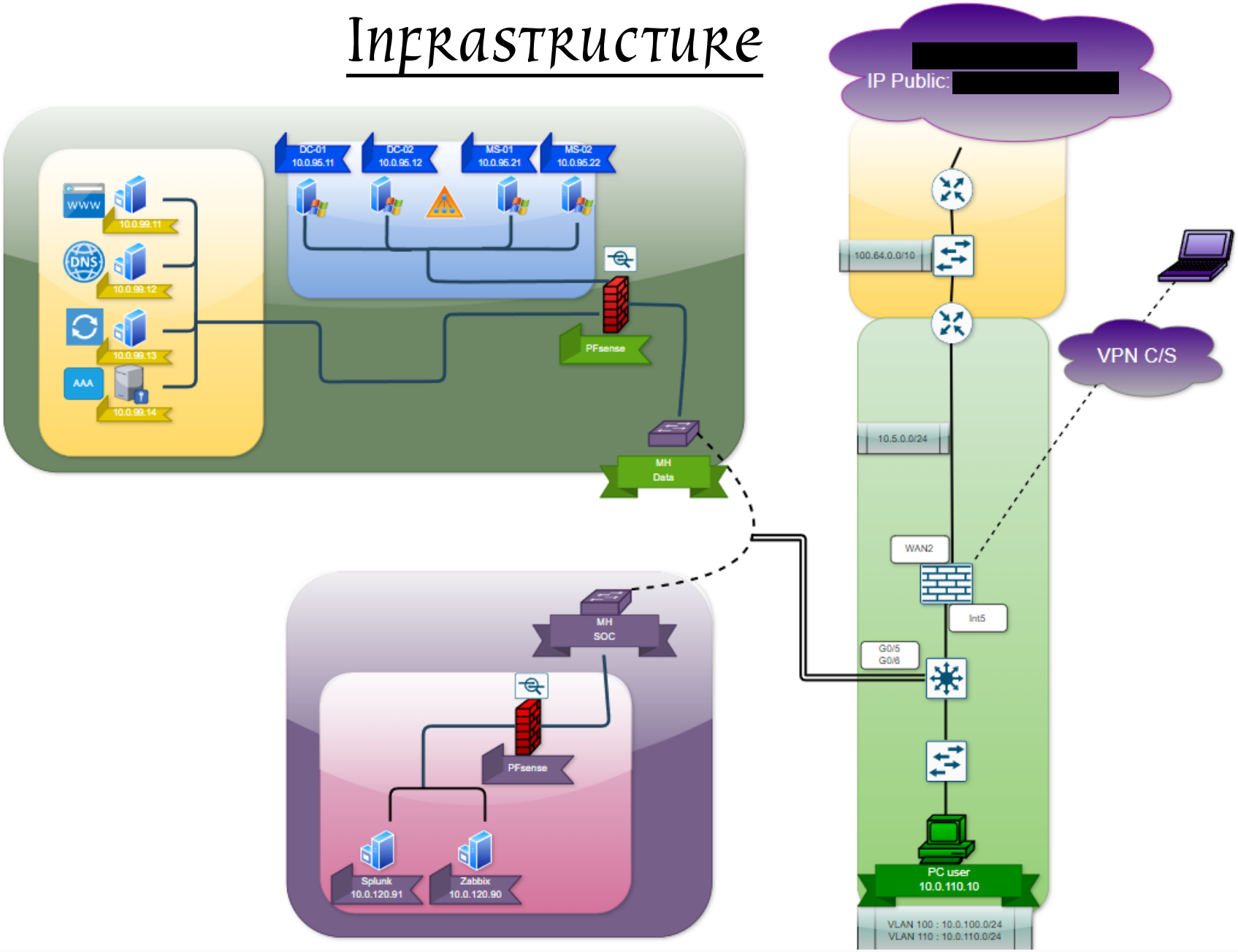
À travers ce projet, la méthodologie forensic est mise en pratique pour détecter, analyser et répondre à des incidents de sécurité simulés, ainsi que récolter des preuves de l'incident et les documenter tout en démontrant l'efficacité des processus de détection et de réponse aux menaces.

Le projet Maker-Hub reflète une intégration complète des compétences théoriques et pratiques acquises au cours de la formation. Il met en lumière des aspects fondamentaux du rôle de consultant en cybersécurité.

LLD

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Infrastructure



Réseau et segmentation

- Réseaux séparés de manière logique via des vlan (data, monitoring/gestion), meilleure pratique : séparer le réseau monitoring physiquement pour éviter les mélanges de flux au niveau matériel
- Mise en place d'ACL sur le switch MLS pour sécuriser l'accès aux différents réseaux interne (web, AD) et externe (SOC/NOC)
- Réseau SOC/NOC sur un réseau séparer, dans un site distant

Redondance et haute disponibilité

- Redondance appareils réseau non mise en place mais nécessaire
- Redondance DC et MS pour garder les services actifs même en cas de panne/mise à jour

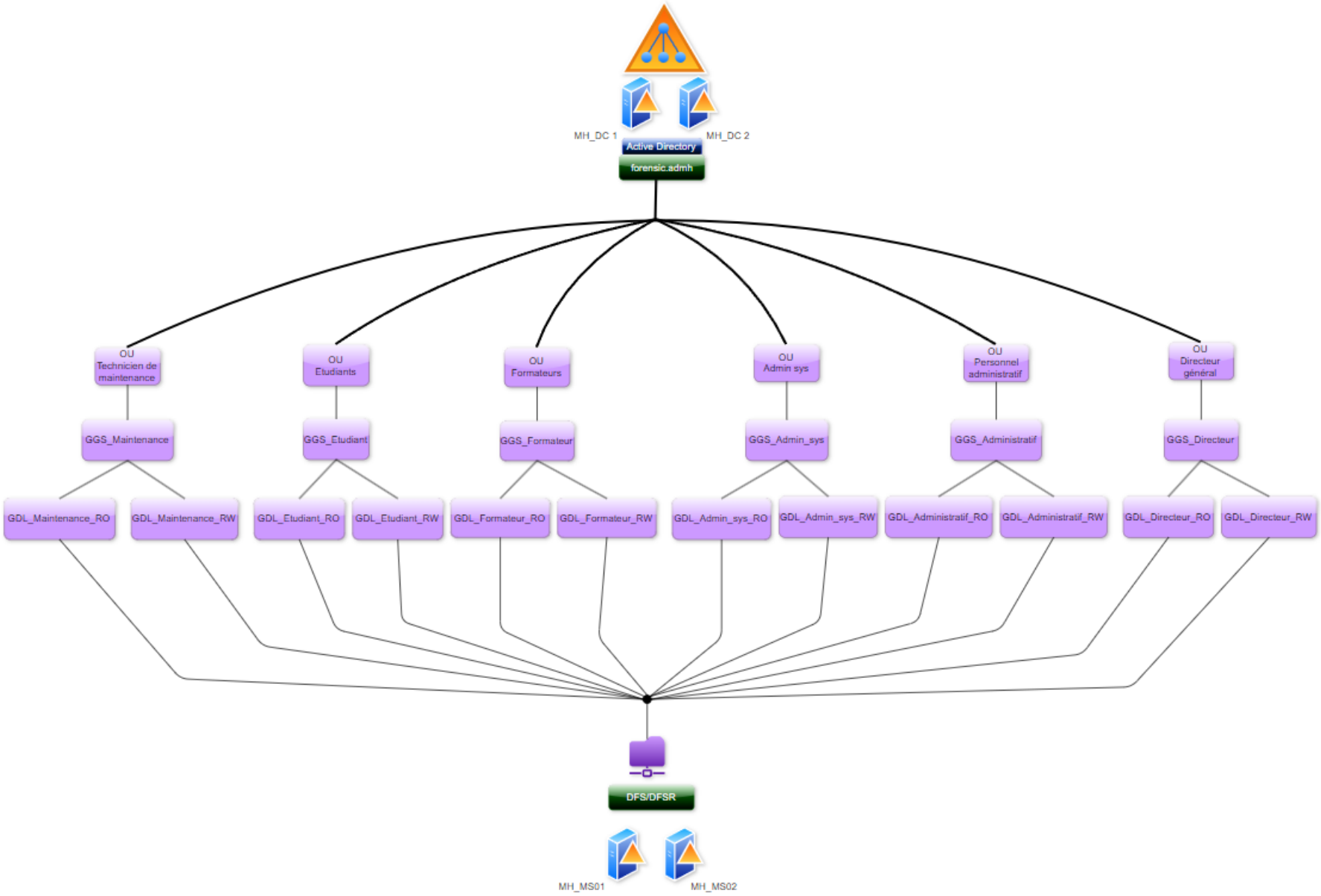
Sécurité et supervision

- Firewalls de marque différente pour pallier aux différentes vulnérabilités
- Reverse proxy web afin d'éviter les connexions directes au serveur web
- Mise en place d'un VPN SSL pour des raisons de rapidité de déploiement et de limitation du nombre de port forwarding de l'ip publique en IPSEC, meilleure pratique : mise en place d'un VPN IPSEC plus sécurisé
- IDS mis en place pour générer des alertes en cas de comportement suspect sur le réseau
- IDS transformé en IPS une fois la base-line définie
- IDS mis en place sur le PFSense pour des raisons pratiques et de limites de temps, meilleure pratique : le placer sur une machine à part d'où le réseau sera routé

Active Directory

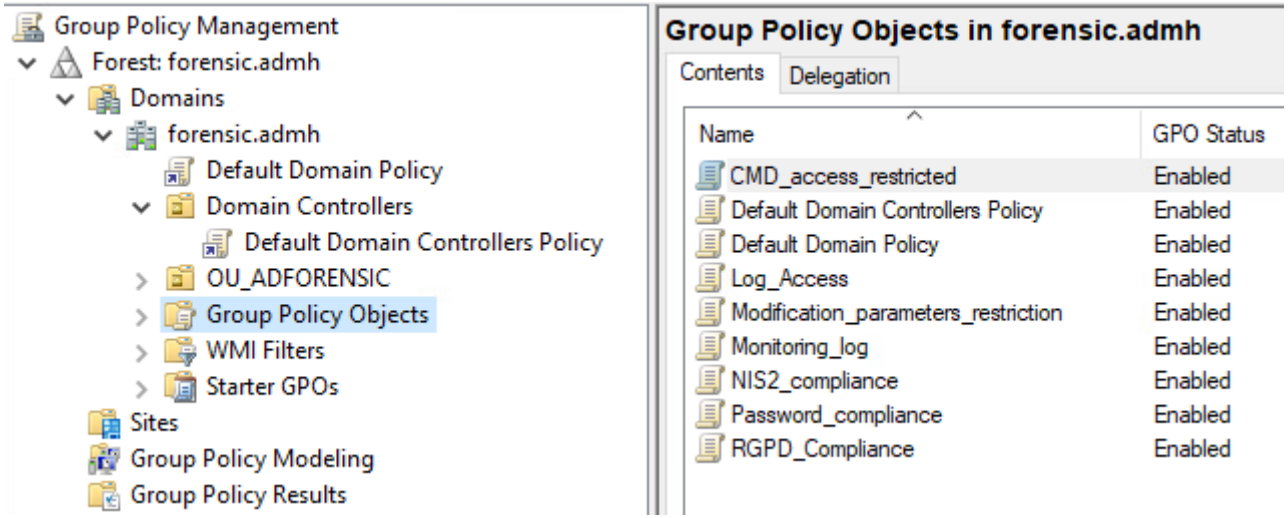
Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Schéma structurel



Liste des Users + Exemple GPO

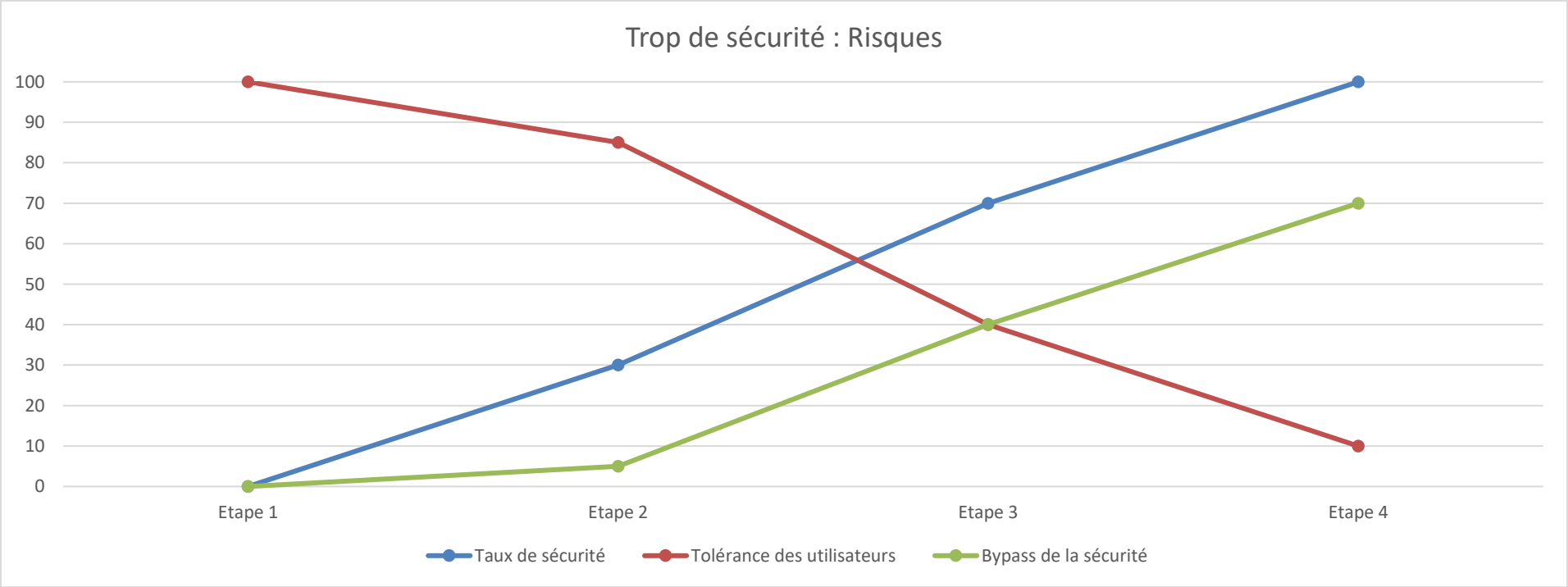
OU	Users
Etudiant	Lorianne Belvaux
	Thélio Carvot
	Amandra Duclerc
	Elio Gervais
	Mériane Lintier
Formateur	Izelin Vauber
	Rynan Devorel
	Héliona Leclercq
	Evron Montivon
	Sylième Dauvris
Technicien de maintenance	Tovan Larmois
	Zélia Sauvion
	Floran Triérat
	Alixor Vaupel
	Serena Belerin
Admin Sys	Orlan Siverot
	Martis Daubret
	Lunis Varten
	Delphée Givarel
	Corwin Clavon
Personnel Administratif	Faéline Derat
	Thyral Quennec
	Ysandra Belvéro
	Firis Lermont
	Eldrin Grévot
Directeur	Dir Gen



Analyse de risques

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Sécurité et Utilisateurs



La sécurisation à outrance peut être contre-productive, plus la sécurité est élevée et contraignante et plus les utilisateurs trouveront des moyens de la contournée, ce qui amène à des vulnérabilités non prévues.

Il est conseillé de mettre en place une sécurité en adéquation avec les normes en vigueur ainsi que les bons usages et de monitorer l'ensemble des appareils sur le réseau afin d'éviter le problème d'une sécurité trop envahissante pour l'utilisateur.

Analyse SWOT
Méthodologie Forensic

Forces

- Précision scientifique
- Applications variées
- Aide à la justice
- Technologies avancées
- Documentation rigoureuse

Faiblesses

- Coût élevé
- Temps d'analyse élévé
- Complexité des procédures
- Sensibilité aux erreurs humaines
- Dépendance technologique

Opportunités

- Croissance de la cybersécurité
- Innovations technologiques
- Collaboration internationale
- Sensibilisation accrue

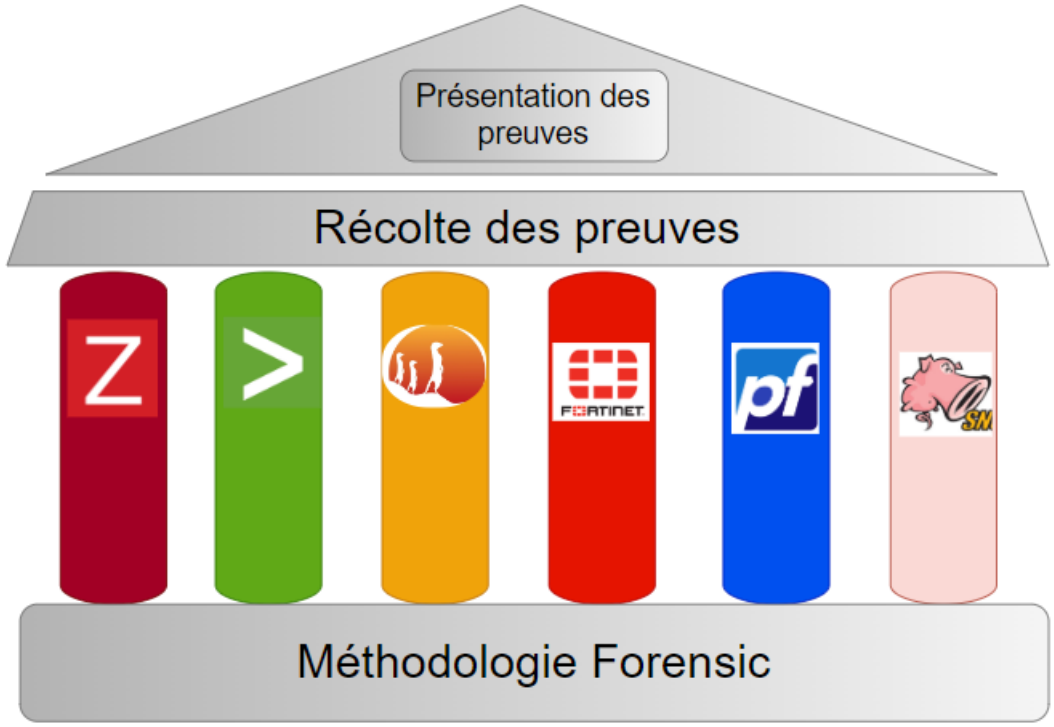
Menaces

- Évolution des technologies criminelles
- Risques juridiques et éthiques
- Manque de réglementation
- Compétition accrue

Les piliers de la méthodologie Forensic dans mon réseau

- Zabbix et Splunk (NOC/SOC) afin de récupérer les logs et les analyser
- Suricata et Snort (IDS/IPS) afin de relever toute activités suspectes sur le réseau et bloquer si nécessaire
- Fortigate et PFSense (firewall) permet de filtrer les réseaux via les règles

Tous ces piliers sont essentiels dans mon infrastructure afin d'utiliser la méthodologie forensic, sans cela les incidents passeront inaperçu et il sera impossible de retracer le chemin jusqu'à la source du problème.



Forensic : Histoire et Méthodologie

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

1) Définitions :

1) La **FORENSIC**, ou science forensique, désigne l'ensemble des méthodes scientifiques appliquées pour collecter, analyser et interpréter des preuves dans le cadre d'enquêtes judiciaires. Elle regroupe des disciplines variées comme la médecine légale, la toxicologie, la balistique, la criminalistique ou encore l'analyse ADN. Son objectif principal est de reconstituer les faits à partir de traces ou indices physiques laissés sur une scène de crime ou dans un contexte d'investigation.

2) La **FORENSIC NUMÉRIQUE**, ou **DIGITAL FORENSIC**, est une branche de la cybersécurité qui consiste à collecter, préserver, analyser et interpréter des données numériques afin de comprendre, documenter et prouver des activités malveillantes dans des systèmes informatiques, des réseaux ou des appareils numériques. Elle vise à répondre à des incidents de sécurité, détecter des intrusions, et fournir des preuves recevables en justice.

2) Histoire de la forensic de la science à la cybersécurité

2.1) Forensic scientifique

A) Antiquité et prémices de l'enquête scientifique :

- Les premières formes d'investigation datent de l'Antiquité, où l'observation et l'analyse étaient utilisées pour résoudre des crimes.
- En Chine, en 1248, le manuel judiciaire "Hsi Duan Yu" (Le Lavage des Injustices) a documenté des techniques rudimentaires pour examiner des blessures et des cadavres.

B) Émergence au XIXe siècle :

- Les techniques modernes forensiques prennent racine dans le développement de la médecine légale, de la chimie et de la criminologie.
- Le criminologue français Alphonse Bertillon a introduit l'anthropométrie (mesure du corps humain) pour identifier les criminels.
- En 1890, Francis Galton développe l'analyse des empreintes digitales (minuties).
- En 1910, Edmond Locard, fondateur du premier laboratoire de police scientifique à Lyon, formule son célèbre "principe d'échange de Locard" : « Tout contact laisse une trace. »

2.2) Évolution vers la forensic numérique :

A) Les premiers cas numériques (1970-1980) :

- Avec l'essor des ordinateurs dans les années 1970, des crimes liés à la technologie (fraudes informatiques, vols de données) commencent à apparaître.
- Les premières enquêtes numériques sont manuelles, nécessitant une expertise en informatique rudimentaire.

- Exemple notable : le cas Clifford Stoll en 1986, où un astronome découvre des intrusions dans des systèmes informatiques du gouvernement américain.

B) Formalisation des méthodologies (1990-2000) :

- Les années 1990 voient l'apparition des premières normes et outils dédiés à l'investigation numérique.
- Création de laboratoires forensiques informatiques par les gouvernements et les forces de l'ordre.
- Les logiciels comme EnCase (1997) permettent de créer des copies immuables de disques pour analyse.

C) Professionnalisation (2000-2010) :

- La montée d'Internet a amplifié les crimes numériques : attaques DDoS, ransomwares, espionnage industriel.
- Les organisations internationales comme l'INTERPOL et l'ICANN commencent à intégrer la forensic dans leurs processus d'enquête.
- Formation des experts forensiques spécialisés dans la cybersécurité.

D) Convergence cybersécurité et forensic (2010-présent) :

- Explosion des cyberattaques complexes (APT, menaces persistantes avancées) nécessitant des compétences spécialisées.
- La forensic numérique devient un pilier de la réponse aux incidents et de la gestion des crises cyber.
- Les organisations adoptent une approche proactive, intégrant forensic et cybersécurité dans les outils de détection et de prévention (SIEM, EDR, XDR).

3) Méthodologie de la forensic numérique

La méthodologie forensic en cybersécurité repose sur une série d'étapes clairement définies pour garantir la préservation, l'analyse et l'interprétation des preuves numériques de manière fiable et recevable en justice. Chaque phase est essentielle et doit être menée avec soin pour éviter la contamination des preuves et garantir la validité de l'enquête.

3.1) Préparation et planification

Objectif :

Créer un cadre organisationnel et technique avant de lancer une investigation pour maximiser l'efficacité des opérations forensic.

Étapes :

Définir les objectifs de l'enquête :

- Identifier la nature de l'incident (ex. intrusion, vol de données, ransomware).

- Déterminer les résultats attendus (identifier l'attaquant, récupérer des données, préparer des preuves pour un tribunal).

Assembler l'équipe :

- Inclure des experts forensic, des analystes cybersécurité, et des conseillers juridiques si nécessaire.
- Attribuer des rôles et responsabilités.

Préparer les outils :

- Vérifier que les logiciels forensic sont à jour et conformes aux standards (ex. EnCase, FTK, Volatility).
- Préparer des supports matériels, comme des disques externes et des systèmes isolés pour l'analyse.

Planifier les opérations :

- Identifier les ressources numériques à examiner (serveurs, postes de travail, réseaux, IoT).
- Évaluer les risques associés (perte de données, contamination des preuves).

3.2) Identification des preuves numériques

Objectif :

Localiser les données pertinentes pour l'enquête dans un environnement numérique.

Étapes :

Cartographier l'infrastructure concernée :

- Identifier les systèmes, réseaux et périphériques potentiellement impactés.
- Localiser les logs, les journaux d'événements et les fichiers système utiles.

Prioriser les sources :

- Réseaux : Paquets réseau, journaux de pare-feu, configurations de routeurs.
- Systèmes : Journaux système, fichiers de configuration, bases de données.
- Périphériques externes : Clés USB, disques durs externes.
- Clouds et environnements virtuels.

Utiliser des outils de détection :

- Utiliser des scanners (ex. Wireshark pour l'analyse réseau) pour détecter des activités anormales.

3.3) Collecte des preuves

Objectif :

Capturer les données numériques de manière à préserver leur intégrité.

Étapes :

Créer une image disque :

- Réaliser une copie exacte et immuable des disques ou partitions à analyser (bitstream).
- Utiliser des outils comme FTK Imager ou dd sous Linux.

Capturer les données volatiles :

- Collecter la mémoire vive (RAM) pour détecter les processus en cours, les sessions réseau actives et les données temporaires.
- Utiliser des outils comme Volatility ou DumpIt.

Exporter les journaux et logs :

- Sauvegarder les journaux d'événements système, les logs réseau et les journaux d'applications.

Établir la chaîne de conservation :

- Documenter chaque étape (qui, quoi, où, quand, comment) pour prouver l'intégrité des preuves.

3.4) Préservation des preuves

Objectif :

Garantir que les données collectées ne sont pas altérées et restent recevables en justice.

Étapes :

Isoler les preuves :

- Stocker les données sur des systèmes sécurisés, sans connexion au réseau, pour éviter toute contamination.

Vérification d'intégrité :

- Générer des hashs (MD5, SHA-256) des fichiers ou des disques capturés.
- Comparer les hashs avant et après l'analyse pour garantir que les données n'ont pas été modifiées.

Créer des copies de travail :

- Utiliser une copie des preuves pour l'analyse, en conservant l'original intact.

3.5) Analyse des preuves

Objectif :

Examiner les données collectées pour identifier des indices, reconstituer les événements et déterminer la cause de l'incident.

Étapes :

Analyse des fichiers et métadonnées :

- Rechercher des fichiers supprimés, cryptés ou cachés.
- Examiner les métadonnées pour obtenir des informations sur la création, la modification et l'accès aux fichiers.

Analyse des logs :

- Examiner les journaux système, réseau et applicatifs pour détecter des anomalies ou des événements suspects.
- Identifier les connexions réseau malveillantes ou non autorisées.

Analyse de la mémoire vive (RAM) :

- Identifier les processus actifs, les connexions établies et les données volatiles pertinentes.

Rétro-ingénierie de logiciels malveillants :

- Analyser les malwares pour comprendre leur fonctionnement, leurs objectifs et leur origine.

Corrélation des données :

- Croiser les informations issues de différentes sources pour reconstituer la chronologie de l'incident.

3.6) Documentation et rapport

Objectif :

Rassembler et présenter les résultats de l'enquête sous forme claire, détaillée et exploitable.

Étapes :

Rédiger un rapport détaillé :

- Inclure les objectifs, la méthodologie, les outils utilisés, les résultats et les conclusions.
- Documenter les preuves collectées et leur analyse.

Créer une chronologie des événements :

- Détailler les actions de l'attaquant et l'impact sur les systèmes.

Émettre des recommandations :

- Suggérer des mesures correctives pour éviter la répétition de l'incident.
- Conseiller sur les améliorations à apporter à la sécurité des systèmes.

3.7) Présentation des preuves

Objectif :

Communiquer les résultats aux parties concernées (direction, forces de l'ordre, tribunaux).

Étapes :

Présentation technique :

- Préparer un briefing pour les équipes techniques ou de gestion, avec des explications détaillées.

Présentation juridique :

- Traduire les conclusions techniques en éléments compréhensibles pour les avocats ou les juges.

Défense en justice :

- Si nécessaire, témoigner comme expert pour expliquer les résultats et garantir leur validité.

3.8) Rétroaction et amélioration

Objectif :

Tirer des leçons de l'incident pour améliorer la sécurité et les méthodologies futures.

Étapes :

Post-mortem :

- Identifier ce qui a fonctionné ou échoué dans l'enquête.

Mise à jour des processus :

- Améliorer les procédures internes et les outils utilisés.

Formation et sensibilisation :

- Partager les enseignements avec les équipes pour renforcer leur préparation.

3.9) Conclusion :

La méthodologie forensic en cybersécurité est un processus rigoureux et structuré qui nécessite des compétences techniques, organisationnelles et juridiques. Elle joue un rôle essentiel dans la réponse aux incidents et la prévention future des menaces en cybersécurité.

4) Limites de la forensic numérique :

Malgré ses capacités impressionnantes, la forensic en cybersécurité n'est pas une solution universelle. Ses limites techniques, juridiques et organisationnelles exigent une planification rigoureuse, des ressources adéquates, et une coordination interdisciplinaire pour maximiser son efficacité. Les organisations doivent également combiner la forensic avec des mesures proactives (prévention, surveillance) pour limiter les impacts des cyberattaques.

En voici quelques exemples :

4.1) Limites techniques :

A. Cryptographie et chiffrement :

- Les fichiers ou disques cryptés (ex : via BitLocker) peuvent être impossibles à analyser sans les clés de déchiffrement. Les messageries sécurisées (comme Signal ou WhatsApp) rendent difficile l'accès aux contenus échangés.

B. Volatilité des preuves numériques :

- Les données numériques peuvent être supprimées, modifiées ou écrasées (logs système, mémoire vive).
- Les informations volatiles (comme les processus en cours ou les données en mémoire RAM) nécessitent une intervention rapide pour être collectées.

C. Quantité et complexité des données :

- Les environnements modernes génèrent une immense quantité de données à analyser, ce qui peut être chronophage et nécessiter des outils coûteux.
- Les systèmes complexes (cloud computing, conteneurs, IoT) compliquent l'identification et l'accès aux données pertinentes.

D. Avancées des cyberattaques :

- Les techniques anti-forensic, utilisées par des attaquants, rendent l'enquête plus difficile :
  - Suppression de logs.
  - Effacement sécurisé des données (secure wipe).
  - Injection de fausses preuves (ex. falsification de timestamps ou de métadonnées).

4.2) Limites juridiques et réglementaires :

A. Respect de la vie privée :

- Lors d'une investigation, les experts doivent souvent traiter des données personnelles ou sensibles, ce qui peut soulever des problèmes éthiques et légaux (RGPD en Europe, HIPAA aux États-Unis).

B. Acceptabilité des preuves :

- Pour qu'une preuve soit recevable en justice, elle doit respecter des procédures strictes (chaîne de conservation, intégrité des données). Une simple erreur peut invalider une enquête.

C. Problèmes de juridiction :

- Les cyberattaques transcendent souvent les frontières nationales, rendant l'accès aux données ou la collaboration avec d'autres pays juridiquement complexe.

- Certaines juridictions peuvent refuser de coopérer ou imposer des restrictions sur la collecte des preuves numériques.

4.3) Limites organisationnelles :

A. Manque de ressources spécialisées :

- La forensic numérique requiert des experts formés ainsi que des outils et logiciels spécifiques, souvent coûteux, ce qui limite son accessibilité pour les petites organisations.

B. Temps et coûts élevés :

- Les investigations forensic peuvent être longues et coûteuses, surtout dans des environnements complexes ou en cas d'attaques sophistiquées.
- Dans certaines situations, le coût d'une analyse peut dépasser l'intérêt financier de l'enquête.

C. Conflits d'intérêts internes :

- Lorsque l'attaquant est un employé ou un partenaire interne, des pressions politiques ou organisationnelles peuvent freiner l'enquête.

4.4) Limites pratiques :

A. Temps de réaction :

- Une réaction tardive à un incident peut entraîner la perte irrémédiable de preuves importantes (logs écrasés, redémarrage des systèmes).

B. Manque de standards universels :

- Bien qu'il existe des standards (NIST, ISO/IEC 27037), ils ne sont pas uniformément appliqués et réglementés à l'échelle mondiale et européenne, ce qui peut compliquer la coordination et la documentation.

C. Difficulté d'identification de l'attaquant :

- Les cybercriminels utilisent des techniques pour masquer leur identité (proxy, VPN, réseaux TOR), ce qui rend leur identification complexe et coûteuse en ressources.

D. Dépendance aux outils :

- Les résultats d'une enquête forensic dépendent largement des outils utilisés. Une mauvaise configuration ou des limitations de ces outils peuvent biaiser les conclusions.

4.5) Limites liés à l'évolution technologique :

A. Environnements complexes (cloud, IoT, blockchain) :

- Les données hébergées sur des infrastructures cloud ou dispersées sur des appareils IoT sont souvent difficiles à localiser et à capturer.
- Les transactions blockchain, bien que traçables, sont anonymes par nature.

B. Obsolescence des compétences :

- Les techniques forensic doivent évoluer rapidement pour suivre les nouvelles technologies et méthodes d'attaque, ce qui nécessite une formation continue des experts.

5) Outils fréquemment utilisés en forensic

- ***EnCase*** : Suite d'utilitaires complète pour l'analyse de disques, le tri des données, l'analyse de fichiers et le déchiffrement de volumes
- ***FTK (Forensic ToolKit)*** : Apprécié pour son efficacité dans l'analyse de courriels, la recherche par mots-clés et sa stabilité
- ***Autopsy*** : Interface graphique du framework Sleuth Kit, permettant l'analyse de disques, la génération de timeline et l'analyse d'artefacts Windows
- ***Wireshark :*** Outil de capture et d'analyse de réseau, utile pour les enquêtes sur les incidents liés au réseau
- ***Magnet RAM Capture*** : Utilisé pour capturer et analyser la mémoire physique d'un ordinateur Windows
- ***SIFT (SANS Investigative Forensic Toolkit)*** : Suite d'outils forensics open source basés sur Ubuntu, largement utilisés pour la réponse aux incidents
- ***Volatility*** : Framework pour l'analyse de la mémoire vive
- ***Paladin*** : Distribution Linux contenant plus de 100 outils répartis en 29 catégories pour l'investigation forensique
- ***ExifTool*** : Outil pour lire, écrire et modifier les méta-informations de divers types de fichiers
- ***BlueBear LACE*** : Solution pour le traitement, la catégorisation et la gestion de gros volumes de supports visuels

6) Type de preuves collectées

6.1) Fichiers et données :

- Fichiers générés par les utilisateurs
- Fichiers système et logs
- Fichiers supprimés ou fragments de fichiers récupérés
- Métadonnées des fichiers (dates de création/modification)

6.2) Mémoire volatile :

- Capture de la mémoire vive (RAM) pour l'analyse "live forensics"

- Processus en cours d'exécution

6.3) Supports de stockage :

- Images forensiques des disques durs
- Données des appareils mobiles, clés USB, cartes mémoire
- Sauvegardes et archives

6.4) Données réseau :

- Logs de trafic réseau
- Historique de navigation internet
- Traces de communications (e-mails, messages)

6.5) Artefacts système :

- Journaux d'événements du système d'exploitation
- Registre Windows
- Traces d'installation ou d'exécution de logiciels malveillants

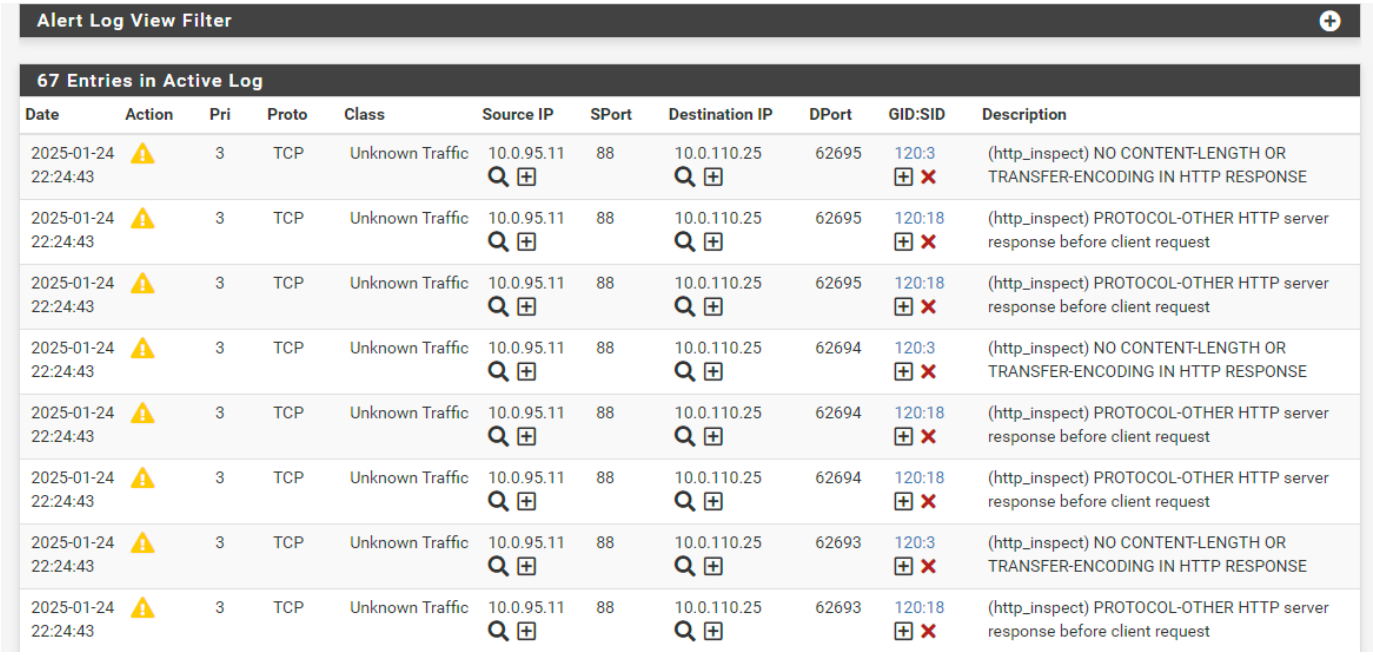
Ces preuves sont collectées en utilisant des méthodes et des outils spécialisés pour garantir leur intégrité et leur admissibilité juridique. L'objectif est de reconstituer la chronologie des événements, identifier les vulnérabilités exploitées et comprendre le déroulement de l'incident de sécurité.

Démonstration Méthodologie Forensic

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Étape 1 : Identification et analyse de l'alerte initiale

1. **Réception de l'alerte :**
   - Une alerte est émise par le système IDS (Intrusion Detection System).
   - Identifier l'appareil concerné, qui appartient à un domaine Active Directory, et noter l'heure de l'alerte (heure inhabituelle, par exemple 22h).
2. **Validation de l'alerte :**
   - Vérifier la légitimité de l'alerte en confirmant qu'il s'agit d'une activité inhabituelle et non d'un faux positif.



Alert Log View Filter

67 Entries in Active Log

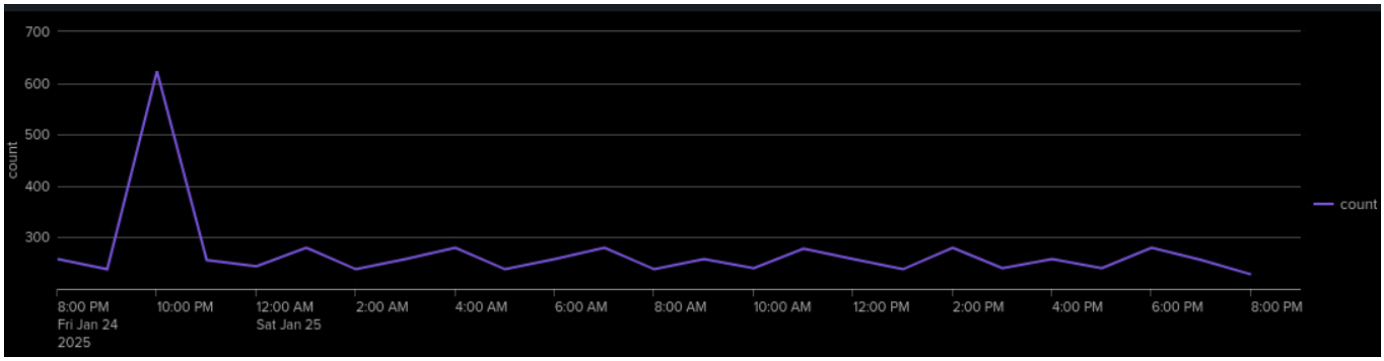
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62695	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62695	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62695	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62694	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62694	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62694	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62693	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2025-01-24 22:24:43	⚠	3	TCP	Unknown Traffic	10.0.95.11	88	10.0.110.25	62693	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request

Étape 2 : Analyse des logs du site web via Splunk

1. **Consultation des logs :**
   - Accéder aux logs du site web sur Splunk.
   - Utiliser le dashboard pour repérer des connexions ou des activités anormales autour de l'heure signalée par l'IDS.

2. **Validation de la suractivité :**

   - Identifier une suractivité des connexions vers le site à une heure étrange (22h).
   - Relever les adresses IP ou identifiants utilisateurs impliqués.



Étape 3 : Identification de l'attaque brute force

1. **Analyse approfondie des logs :**

   - Examiner les logs pour détecter des tentatives de connexion répétées ou automatiques.
   - Identifier des patterns correspondant à une attaque par force brute (tentatives multiples d'identifiants et mots de passe).

2. **Enregistrement des preuves techniques :**

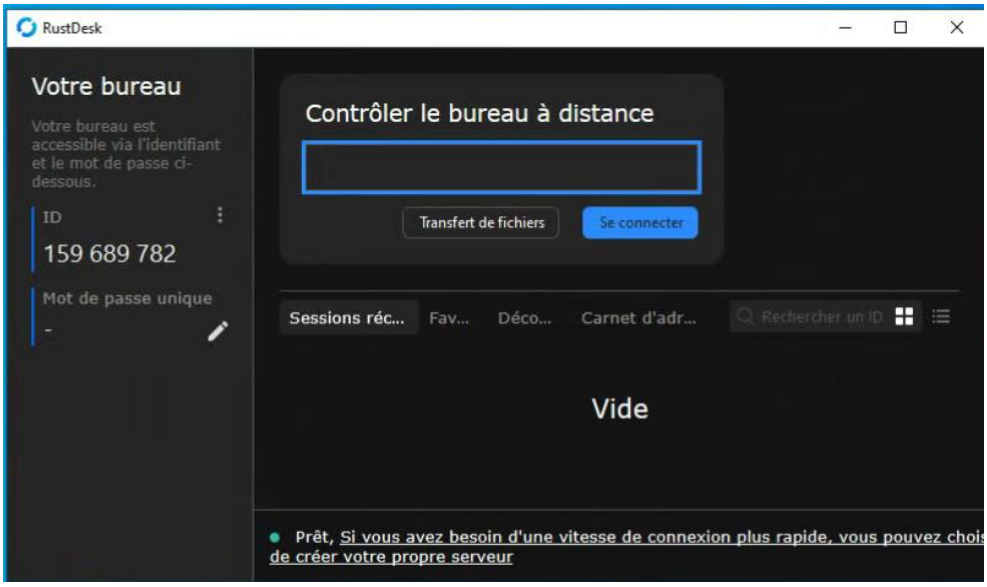
   - Sauvegarder les logs suspects, incluant les adresses IP sources, les timestamps, et les logs de connexions échouées.

i	Durée	Événement
›	24/01/2025 22:28:30,000	10.0.110.25 - - [24/Jan/2025:22:28:30 +0100] "GET /?nom=Orlan&password=3caa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:27,000	10.0.110.25 - - [24/Jan/2025:22:28:27 +0100] "GET /?nom=Orlan&password=2caa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:23,000	10.0.110.25 - - [24/Jan/2025:22:28:23 +0100] "GET /?nom=Orlan&password=1caa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:19,000	10.0.110.25 - - [24/Jan/2025:22:28:19 +0100] "GET /?nom=Orlan&password=0caa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:14,000	10.0.110.25 - - [24/Jan/2025:22:28:14 +0100] "GET /?nom=Orlan&password=zcaa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:11,000	10.0.110.25 - - [24/Jan/2025:22:28:11 +0100] "GET /?nom=Orlan&password=ycaa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:07,000	10.0.110.25 - - [24/Jan/2025:22:28:07 +0100] "GET /?nom=Orlan&password=xcaa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined
›	24/01/2025 22:28:03,000	10.0.110.25 - - [24/Jan/2025:22:28:03 +0100] "GET /?nom=Orlan&password=wcaa%3D HTTP/1.1" 200 3843 "http://data.forensic.mh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36" host = 10.0.99.13 source = /var/log/httpd/reverse-proxy-access.log sourcetype = access_combined

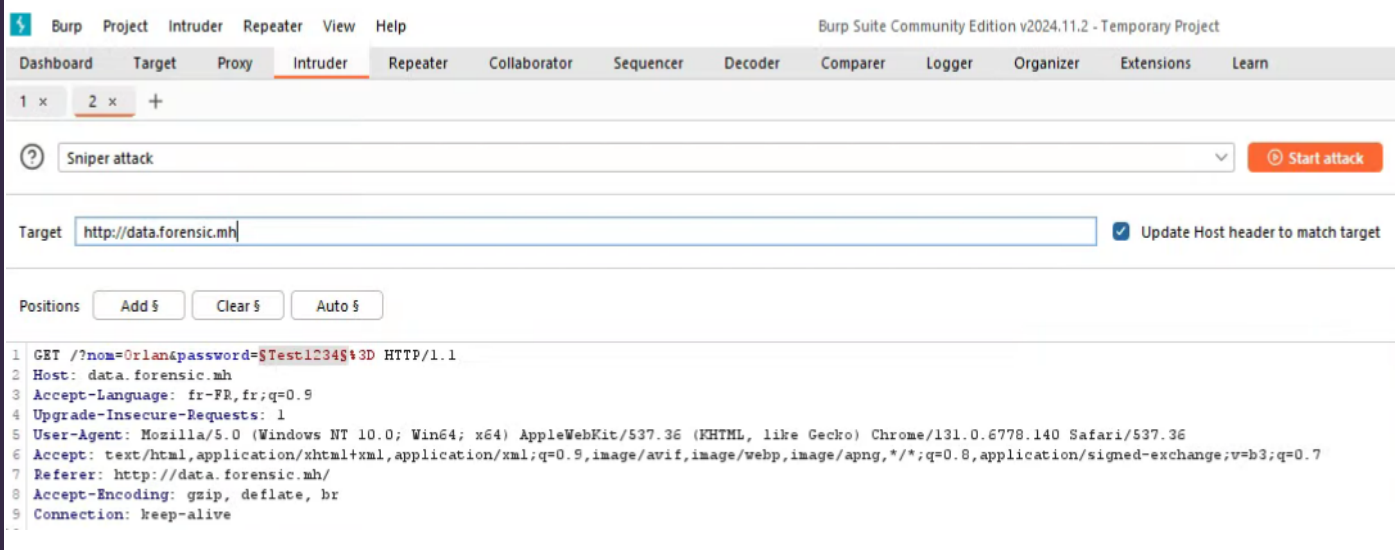
Étape 4 : Inspection de la machine compromise

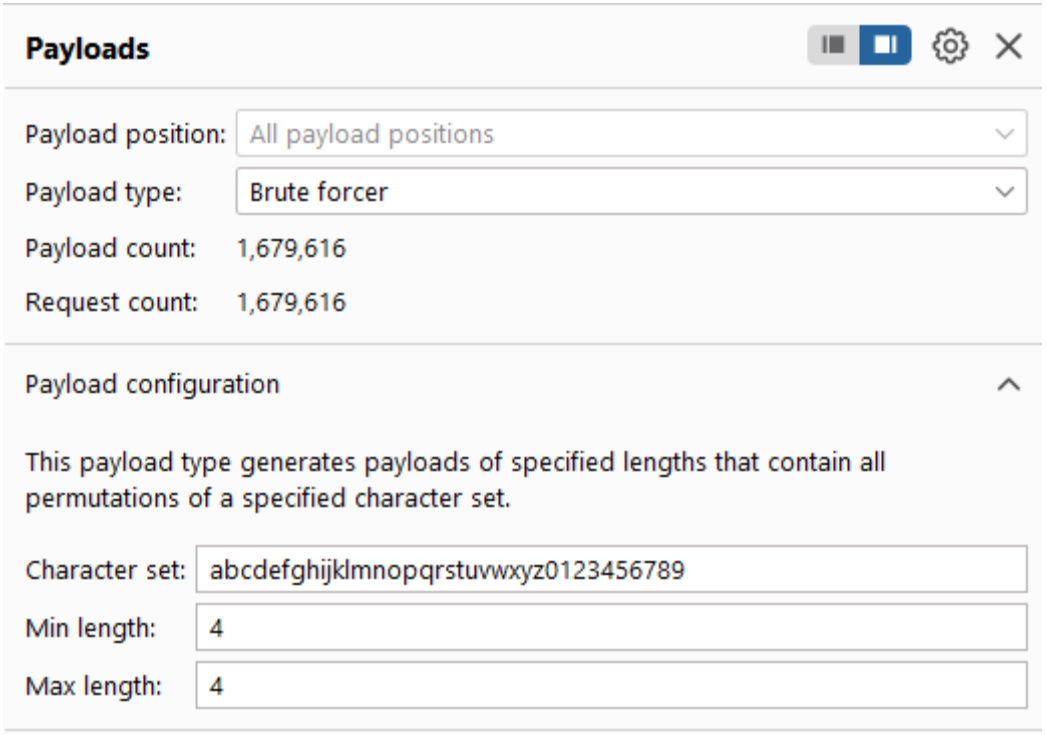
1. **Audit de la machine concernée :**
   - Accéder à la machine identifiée via l'IDS.
   - Vérifier les processus actifs, les applications installées, et la configuration réseau.

2. **Détection d'applications non autorisées :**
   - Repérer des outils tels que **RustDesk** et **Burp Suite**, qui ne sont pas autorisés selon les politiques de sécurité de l'entreprise.



3. **Capture des preuves :**
   - Réaliser des captures d'écran, exporter les données système et générer un rapport de l'état actuel de la machine.





Étape 5 : Investigation auprès de l'utilisateur concerné

1. **Contact de l'utilisateur :**
   - Identifier la personne propriétaire de la machine.
   - La convoquer pour une discussion sur l'usage de l'appareil et vérifier son alibi à l'heure de l'incident.
2. **Validation des réponses :**
   - Noter les explications fournies et les confronter aux preuves techniques collectées.
   - En cas de doute, collecter davantage de preuves liées à son activité.

Étape 6 : Synthèse des preuves et constitution du dossier

1. **Rédaction du rapport d'incident :**
   - Documenter tous les éléments récoltés, incluant :
     - Les logs du système IDS.
     - Les anomalies identifiées dans Splunk.
     - Les preuves de l'attaque brute force.
     - Les applications non autorisées découvertes.

- Les résultats de l'entretien avec l'utilisateur.

2. **Organisation des preuves :**
   - Préparer un dossier clair et chronologique permettant de retracer les étapes de l'incident.

Étape 7 : Mise en place des mesures correctives

1. **Actions techniques immédiates :**
   - Bloquer l'accès RDP via une GPO (Group Policy Object).
   - Désinstaller les applications non autorisées (RustDesk, Burp Suite) des systèmes concernés.
   - Renforcer les politiques de mot de passe et limiter les heures d'accès réseau.
2. **Sensibilisation des employés :**
   - Organiser une session de formation ou de sensibilisation pour rappeler les bonnes pratiques de cybersécurité.
3. **Renforcement de la sécurité globale :**
   - Mettre en place des solutions de détection des comportements anormaux.
   - Activer des mesures de limitation de tentatives de connexion (par exemple, verrouillage temporaire après 5 tentatives échouées).

Étape 8 : Prise de mesures légales si nécessaire

1. **Évaluation des preuves :**
   - Vérifier si les éléments collectés sont suffisants pour engager des actions légales.
   - Consulter l'équipe juridique ou un expert en cybersécurité pour validation.
2. **Constitution d'un dossier juridique :**
   - Préparer les éléments nécessaires pour une éventuelle action en justice contre la personne responsable ou un tiers malveillant.
   - Fournir un résumé clair des impacts financiers, techniques et organisationnels de l'incident.

Hypothèse et scénario d'attaque

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Hypothèse

Les paragraphes suivants sont une hypothèse émise par l'enquêteur forensic aux suites des différentes preuves récoltées après l'attaque afin de reconstituer les faits. En fonctions de ces preuves, il peut y avoir un recours à la justice.

Phase 1 : Social engineering

1.1. Identification de la cible

L'attaquant réalise des recherches approfondies sur l'entreprise et ses employés via :

- **LinkedIn** : pour identifier les employés en poste (techniciens ou administrateurs système).
- **Réseaux sociaux** : pour collecter des informations personnelles sur les habitudes et centres d'intérêt des employés.

1.2. Interaction directe avec la victime

- L'attaquant contacte un employé par téléphone en se faisant passer pour un membre du service informatique.
- Il évoque un **problème urgent** : « Votre accès au réseau interne expire bientôt. Pouvez-vous me donner votre login pour le réactiver ?».
- Il profite de la **panique** ou de la **bonne volonté** de la victime.

1.3. Obtention des identifiants et accès

- Une fois les identifiants obtenus, l'attaquant accède à l'ordinateur professionnel de la victime via des outils de bureau à distance (RustDesk).
- Il explore rapidement les configurations locales (navigateurs, mots de passe enregistrés).

Phase 2 : Attaque via Burp Suite

2.1. Installation et configuration de Burp Suite

- L'attaquant configure un proxy local avec Burp Suite pour capturer les requêtes entre l'application interne (site web) et le serveur.
- Il manipule le fichier hosts de la victime pour intercepter les connexions aux sites internes via Burp Suite.

2.2. Analyse des requêtes HTTP/S

- En explorant les requêtes interceptées, il tente un brute force sur ce qui ressemble à une page de login.

2.3. Exploitation des failles

- L’attaquant utilise l'outil **Intruder** de Burp Suite pour forcer des paramètres.
- Les outils **Repeater** et **Decoder** sont utilisés pour affiner et déchiffrer des données sensibles, mais l’attaquant se fait repérer avant d’avoir eu le temps d’utiliser ces outils.

Phase 3 : Détection par les systèmes de défense

3.2. Détection et réponse des systèmes de défense

- Les systèmes de sécurité (SIEM, WAF ou EDR) détectent une activité anormale, comme :
  - Une tentative de login multiple sur différents comptes.
  - Un flux inhabituel de données vers une adresse IP externe non autorisée.

3.3. Blocage et traçabilité

- Une alerte est déclenchée, et l'accès de l'attaquant est révoqué en temps réel.
- Une enquête est lancée pour identifier la source de l'attaque.
- Les journaux montrent des anomalies, notamment l’utilisation de Burp Suite comme proxy.

Conclusion et impact

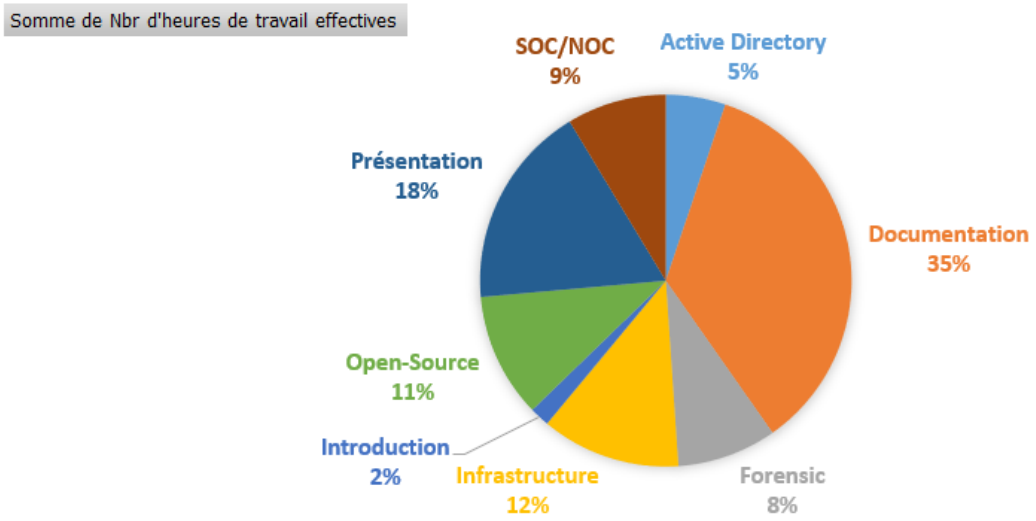
Bien que l’attaquant ait réussi à extraire certaines données initialement, sa tentative de brute force a permis aux systèmes de sécurité de détecter l’intrusion. L’entreprise renforce ses défenses, sensibilise ses employés contre le social engineering, et implémente une surveillance plus stricte (IPS) via une nouvelle base-line pour prévenir des attaques similaires.

Time-Sheet

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Global

Catégorie	Somme de Nbr d'heures de travail effectives	Prix "Tarif Playzone"
Active Directory	12	450
Documentation	81	3037,5
Forensic	20	750
Infrastructure	28	1050
Introduction	4	150
Open-Source	25	937,5
Présentation	41	1537,5
SOC/NOC	20	750
Total général	**231**	**8662,5**



Catégories

Introduction

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
17-12-24	Introduction	Présentation du Maker-Hub	1	Eric	
	Introduction	Choix du sujet	1	Non	
19-12-24	Introduction	Présentation du sujet à Eric	1	Eric	
20-12-24	Introduction	Présentation du sujet à Eric et Jean	1	Eric, Jean	

Total heures de travail effectives
4

Infrastructure

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
18-12-24	Infrastructure	Test et validations des scripts	2	Non	
	Infrastructure	Poussée des scripts	1	Non	
	Infrastructure	Test et validation des configurations réseau	4	Non	
19-12-24	Infrastructure	VPN	5	Adrien Bouillot	
20-12-24	Infrastructure	VPN	3	Adrien Bouillot	
	Infrastructure	Connexion ESXi (SOC/NOC)	2	Non	
02-01-25	Infrastructure	Implémentation PFSense	2	Non	
15-01-25	Infrastructure	Vérification et correction règles firewall	3	Non	
17-01-25	Infrastructure	Mise en place switch MLS	3	Non	
21-01-25	Infrastructure	Vérification routes et règles firewall	3	Non	

Total heures de travail effectives
28

Active Directory

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
03-01-25	Active Directory	Installation windows server	2	Non	
06-01-25	Active Directory	Configuration AD	2	Non	
08-01-25	Active Directory	Création des OU et users	1	Non	
09-01-25	Active Directory	Création GDL/GGS + DFS/DFSR	3	Non	
10-01-25	Active Directory	Config GPO	1	Non	
13-01-25	Active Directory	Implémentation GPO	1	Non	
15-01-25	Active Directory	Implémentation GPO	2	Non	

Total heures de travail effectives
12

Open-Source

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
03-01-25	Open-Source	Installation Rocky Linux Open-Source	2	Non	
04-01-25	Open-Source	Configuration server web	3	Non	
06-01-25	Open-Source	Config web + DNS	4	Non	
07-01-25	Open-source	Config DNS	1	Non	
08-01-25	Open-Source	Config web	3	Non	
09-01-25	Open-Source	Config web	2	Non	
19-01-25	Open-Source	Config reverse-proxy	2	Non	
21-01-25	Open-Source	Config reverse-proxy + waf	2	Non	
22-01-25	Open-Source	Config IDS/IPS	4	Non	
23-01-25	Open-Source	Config IDS/IPS	2	Non	

Total heures de travail effectives
25

SOC/NOC

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
06-01-25	SOC/NOC	Installation Splunk	2	Non	
07-01-25	SOC/NOC	Installation + config Zabbix	4	Non	
08-01-25	SOC/NOC	Implémentation log zabbix	1	Non	
10-01-25	SOC/NOC	Implémentation log zabbix	2	Non	
11-01-25	SOC/NOC	Config forwarder Splunk	1	Non	
14-01-25	SOC/NOC	Config forwarder Splunk + Zabbix	5	Non	
15-01-25	SOC/NOC	Config Splunk	3	Non	
20-01-25	SOC/NOC	Vérification zabbix	2	Non	

Total heures de travail effectives
20

Forensic

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
06-01-25	Forensic	Document introduction forensic	1	Non	
07-01-25	Forensic	Documentation histoire et limites forensic	3	Non	
08-01-25	Forensic	Documentation et template	4	Non	
	Forensic	Utilisation de Burp suite	1	Non	
09-01-25	Forensic	Template doc	1	Non	
10-01-25	Forensic	Template doc	2	Non	
16-01-25	Forensic	Config burp suite	2	Non	
	Forensic	Analyse des logs Splunk	3	Non	
17-01-25	Forensic	Relecture scénario d'attaque	3	Non	

Total heures de travail effectives
20

Présentation

Dates	Catégorie	Tâches	Nbr d'heures de travail effectives	Aide extérieure	
13-01-25	Présentation	Mise en place scénario de présentation	2	Non	
17-01-25	Présentation	Présentation de l'avancement	1	Eric, Jean	
19-01-25	Présentation	Préparation simulation jury	1	Non	
20-01-25	Présentation	Préparation simulation jury	6	Non	
21-01-25	Présentation	Simulation jury	1	Non	
22-01-25	Présentation	Mise à jour Powerpoint	1	Non	
24-01-25	Présentation	Rédaction Powerpoint	3	Non	
25-01-25	Présentation	Rédaction Powerpoint	4	Non	
26-01-25	Présentation	Rédaction Powerpoint	2	Non	
27-01-25	Présentation	Rédaction Powerpoint	12	Non	
28-01-25	Présentation	Rédaction Powerpoint	8	Non	

Total heures de travail effectives
41

Documentation

Dates	Catégorie	Tâches	Nbr d'heures de travail effectiv	Aide extérieu	
17-12-24	Documentation	Conception des scripts de configuration	3	Non	
	Documentation	Rédaction du LLD	4	Non	
18-12-24	Documentation	Mise à jour LLD	2	Non	
19-12-24	Documentation	Conception agenda inversé	2	Non	
	Documentation	Conception Time-Sheet et filtre	3	Solenne François	
	Documentation	Mise à jour LLD	2	Non	
20-12-24	Documentation	Mise à jour Time-Sheet	1	Non	
	Documentation	Adressage IP	2	Non	
02-01-25	Documentation	Adressage IP	1	Non	
04-01-25	Documentation	Documentation web + DNS + Reverse proxy	3	Non	
06-01-25	Documentation	Documentation web + DNS + Splunk	1	Non	
07-01-25	Documentation	Documentation	2	Non	
09-01-25	Documentation	Doc AD	2	Non	
10-01-25	Documentation	HLD/LLD	3	Non	
11-01-25	Documentation	Documentation Forensic	4	Non	
13-01-25	Documentation	Documentation	6	Non	
14-01-25	Documentation	Documentation	3	Non	
16-01-25	Documentation	Soft-skills	1	Frédérique	
	Documentation	Mise à jour doc générale	2	Non	
19-01-25	Documentation	Doc IDS	1	Non	
22-01-25	Documentation	Mise à jour doc générale	3	Non	
23-01-25	Documentation	Rédaction doc finale	5	Non	
24-01-25	Documentation	Rédaction doc finale	5	Non	
25-01-25	Documentation	Rédaction doc finale	8	Non	
26-01-25	Documentation	Rédaction doc finale	12	Non	

Total heures de travail effectives
81

Agenda Inversé

Semaine	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi	Dimanche
16/12-22/12				Rédaction agenda inversé; LLD; Time-Sheet; Adressage ip	Implémentation infra physique; Connexion ESXi depuis l'infra; VPN C/S	Rédaction doc	Rédaction doc
23/12-29/12	REPOS	REPOS	REPOS	REPOS	Début implémentation AD + Open-source	AD + Open-Source	Fin implémentation AD
30/12-05/01	Open-Source	Début implémentation SOC/NOC	REPOS	SOC/NOC + Open-Source	SOC/NOC + Open-Source	SOC/NOC + Open-Source	Fin implémentation Opens-source + SOC/NOC
06/01-12/01	FORENSIC	FORENSIC	FORENSIC	FORENSIC	FORENSIC	FORENSIC	FORENSIC
13/01-19/01	FORENSIC	FORENSIC	FORENSIC	FORENSIC	FORENSIC	FORENSIC	FORENSIC
20/01-26/01	Préparation simulation	Simulation jury	FORENSIC + Analyse de risque	FORENSIC + Analyse de risque	FORENSIC + Analyse de risque	FORENSIC + Analyse de risque	FORENSIC + Analyse de risque
27/01-31/01	Remise doc technique	Simulation jury	Préparation jury	Présentation jury	Débrief	REPOS	REPOS

Bibliographie

- Eccouncil : C|HFI v10
- Social Engineering : The science of human hacking (Christopher Hadnagy)
- Incident Response & computer forensics (Jason T. Luttgens, Matthew Pepe, Kevin Mandia)
- Solenne François : cours Management DD (M.Reyners)
- Documents playzone cyber 2024

Culot Jonathan
CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS
technobel

Remerciements

- Jury
- Formateur : Eric Houtevelt , Jean Thomas
- RH et équipe d'accompagnement : Frédérique Renault
- L'équipe CyberOps
- Technobel
- Solenne François

Culot Jonathan

CONSULTANT EN CYBERSÉCURITÉ ORIENTÉ SECOPS

technobel