

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

**U6 – CYBERSÉCURITÉ DES SERVICES
INFORMATIQUES**

SESSION 2024

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 19 pages, numérotées de 1/19 à 19/19.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 1 sur 19

Cas MARTIN

Ce sujet comporte 18 pages dont un dossier documentaire de 13 pages.

Barème

DOSSIER A	Gestion et réduction du risque d'attaque par rançongiciel	52 points
DOSSIER B	Audit de sécurité de l'annuaire <i>Active Directory</i>	28 points
	TOTAL	80 points

Dossier documentaire

Documents communs	7
Document 1 : Schéma et description de l'infrastructure réseau envisagée	7
Document 2 : Sigles couramment utilisés dans les documents	7
Documents associés au dossier A	8
Document A1 : Événements redoutés	8
Document A2 : Niveau de gravité EBIOS	8
Document A3 : Extrait du guide « Attaques par rançongiciels, tous concernés » publié par l'Agence nationale de la sécurité des systèmes d'information en septembre 2020.....	9
Document A4 : Schéma d'une attaque classique par rançongiciel	10
Document A5 : Traitement des règles de filtrage et de sécurité concernant les flux HTTP et HTTPS sur un pare-feu UTM.	11
Document A6 : Extrait des recommandations de sécurité concernant l'analyse des flux HTTPS publiées par l'ANSSI en 2014.....	12
Document A7 : Messages d'erreur émis par le navigateur internet du poste client de test .	13
Documents associés au dossier B	14
Document B1 : Notions d'annuaire « Active Directory »	14
Document B2 : Présentation du programme PingCastle	14
Document B3 : Extraits du rapport PingCastle	15
Document B4 : Extraits du rapport PingCastle - suite.....	16
Document B5 : Les utilisateurs protégés dans l'annuaire Active Directory	17
Document B6 : Utiliser le transfert d'événements Windows (Windows event forwarding : WEF) pour optimiser la détection d'intrusion	18

Présentation du contexte

La clinique MARTIN est un établissement de santé privé à but lucratif créé en 1986, dans l'agglomération bordelaise, par deux chirurgiens orthopédiques. Après une fusion avec un autre établissement en 1997, la clinique a ensuite regroupé l'ensemble de son activité en 2004 sur son site historique de Pessac (Gironde) où elle compte désormais un effectif de 450 salariés dont 118 médecins. Elle est désormais exploitée sous la forme d'une société par actions simplifiée.

Dans un souci d'amélioration constante de l'offre de soins et du perfectionnement du parcours de santé des patients, la société s'est engagée en février 2016 dans un processus de certification du respect de la norme ISO 9001:2015 sur le management de la qualité.

Les avantages obtenus par cette certification, notamment en matière de communication avec les tiers (fournisseurs de matériel médical et de produits de santé, organismes de sécurité sociale et professionnels de l'assurance santé complémentaire, etc.), ont convaincu l'équipe de direction et plus particulièrement son directeur, monsieur Jean-Marc GALLOIS, de poursuivre l'effort en 2019 avec l'obtention de la certification ISO 27799 sur le management de la sécurité de l'information relative à la santé.

De fait, au cours des 30 dernières années, au gré des transformations successives de son système d'information, la clinique a été confrontée à de multiples défaillances, qui ont conduit à une réflexion sur les efforts à entreprendre pour l'amélioration de la performance et de la sécurité du système d'information. Des efforts qui n'ont jamais été minimisés compte tenu du caractère hautement confidentiel des données médicales liées aux patients.

Ainsi, en 2003, un salarié a été licencié pour avoir transmis à une société de promotion immobilière des informations médicales sur des patients âgés.

En 2009, la clinique a subi un défaçage¹ de son site *web* par des auteurs qui n'ont pu être identifiés et qui aurait pu avoir des conséquences plus graves sur la réputation de l'établissement en l'absence de réaction rapide.

En 2011, ce sont deux incidents qui ont manqué, coup sur coup, de mener à une erreur médicale. Ces erreurs ont été évitées de justesse et ont conduit à modifier en profondeur le protocole préopératoire.

Enfin, en 2020 et 2021, dans le contexte de crise sanitaire mondiale liée à l'épidémie de COVID 19, et du fait de son expérience dans le traitement des affections respiratoires et de ses infrastructures permettant de rapidement mettre en œuvre une trentaine de lits de réanimation, la clinique a été mise à contribution pour accueillir des patients affectés par cette pathologie. La clinique a alors dû mener un travail de collecte de données à transmettre à l'agence régionale de santé afin de suivre l'évolution de l'épidémie.

Les contraintes du RGPD, ainsi que la crise COVID, ont induit une surcharge de travail durable pour la direction des systèmes d'information (DSI) et les projets s'enchaînent. Les données médicales sont des données très sensibles qui nécessitent une politique de sécurité stricte.

Vous avez été nouvellement embauché(e) comme technicien(ne) junior pour renforcer les équipes infrastructures de la clinique MARTIN, sous l'autorité de la responsable de la sécurité des systèmes d'information (RSSI), madame Florence DODIER.

Vous participez à des projets prioritaires ou urgents :

- projet de réduction du risque d'attaque par rançongiciel ;
- projet d'audit de conformité du système d'information.

Vous vous appuyerez sur les dossiers documentaires mis à votre disposition.

¹ Attaque qui consiste à pirater un site *web* de manière à modifier des pages, le plus souvent la page d'accueil.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 3 sur 19

Dossier A – Gestion et réduction du risque d’attaque par rançongiciel

Mission A1 – Analyser et réduire les risques liés à une attaque informatique de type « rançongiciel (*ransomware*) ».

Les infections des systèmes d’information par rançongiciels ont connu une croissance exponentielle depuis 2020. Un rapport de l’entreprise spécialisée en cybersécurité Check Point Research (CPR) fait état d’une augmentation de 28 % de ces attaques au niveau mondial par rapport à la même période l’année dernière. En 2022, plusieurs établissements de santé français ont été la cible d’attaques de type rançongiciel, comme le centre hospitalier Sud Francilien de Corbeil-Essonnes ou celui de Versailles.

La RSSI de la clinique MARTIN, madame Florence DODIER, souhaite donc se pencher sur cette question à travers une analyse de risques. Dans un second temps, elle vous demande d’être force de proposition afin de les réduire.

Les premières analyses font apparaître des failles et des opportunités de sécurisation prioritaires ou urgentes.

Question A1.1

- Identifier le principal risque associé à une attaque de type rançongiciel.
- Indiquer le niveau de gravité EBIOS correspondant à ce risque. *Justifier la réponse.*
- Proposer et détailler quatre mesures permettant d’éviter une attaque par rançongiciel ou de réduire son impact.

Le directeur des systèmes d’information souhaite obtenir des précisions concernant un certain nombre de points soulevés dans le guide de l’ANSSI.

Question A1.2

Répondre aux interrogations suivantes :

- Indiquer quel est l’intérêt d’effectuer des sauvegardes déconnectées du système d’information et quelle solution matérielle permettrait de les mettre en place.
- Préciser comment il est possible de s’informer régulièrement des dernières failles de sécurité découvertes afin de gagner en réactivité.
- Justifier l’intérêt d’un réseau local virtuel (VLAN) dédié à l’administration réseau dans l’optique du cloisonnement du système d’information.
- Expliquer pourquoi il est recommandé que le ou les poste(s) d’administration n’aient pas accès à internet.

Un schéma caractérisant le fonctionnement d’un rançongiciel a été créé par la RSSI afin de mieux appréhender ce type d’attaque.

Question A1.3

Proposer au moins deux contre-mesures efficaces pour chaque phase de l’attaque.

Mission A2 – Mettre en œuvre un déchiffrement des flux HTTPS pour lutter plus efficacement contre les rançongiciels (*ransomwares*).

Madame DODIER constate que les protocoles HTTP et HTTPS constituent les principaux vecteurs d'attaques des rançongiciels au même titre que les courriels. Ainsi, elle envisage de mettre en place une solution de déchiffrement des flux HTTPS au sein de la clinique.

Question A2.1

Expliquer pourquoi le protocole HTTPS complexifie la lutte contre les rançongiciels pour la clinique.

La RSSI vous demande, dans un premier temps, de réaliser une maquette de cette solution de déchiffrement des flux HTTPS. Elle souhaite notamment que toute l'équipe comprenne bien le rôle du service mandataire (*proxy*) SSL proposé par les solutions de pare-feu Stormshield Network Security (SNS).

Question A2.2

Schématiser l'utilisation du service mandataire (*proxy*) SSL entre une station cliente présente dans le réseau interne de la clinique et un serveur *web* (externe), lorsque le déchiffrement des flux HTTPS est activé correctement sur le boîtier Stormshield.

Vous mettrez en évidence les différentes zones chiffrées et non chiffrées lors d'un échange de ce type.

Question A2.3

a) Déterminer pourquoi un message d'avertissement est apparu sur le pare-feu lors de la première phase de tests.

b) Expliquer l'absence de message d'avertissement lors du second test.

Question A2.4

Justifier les avantages et les inconvénients pour la clinique d'utiliser une technologie permettant de déchiffrer les flux HTTPS.

Lorsque vous vous connectez sur un poste client afin de valider le bon fonctionnement de la technologie de déchiffrement HTTPS, un message d'erreur apparaît sur le navigateur.

Question A2.5

a) Identifier la cause de ce message d'erreur.

b) Proposer une solution de remédiation.

Lors de la dernière réunion avec la RSSI et le DSI, l'encadrement juridique du déchiffrement a été évoqué et madame DODIER vous demande de fournir des informations précises à ce sujet.

Question A2.6

Déterminer quelles sont les obligations légales de la clinique concernant l'utilisation de cette technologie vis à vis de ses employés et de la CNIL.

Dossier B – Audit de sécurité de l'annuaire *Active Directory*

Mission B1 – Analyser un audit de sécurité de l'annuaire *Active Directory* (première partie)

La RSSI de la clinique MARTIN a été alertée d'une recrudescence des attaques à destination des établissements de santé.

Certaines de ces attaques utilisent les potentielles vulnérabilités de l'annuaire *Active Directory*.

Dernièrement l'outil *PingCastle* lui a été recommandé. Elle décide de vous confier une première analyse de cet outil, dans sa version gratuite, avant de s'engager éventuellement sur son acquisition.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 5 sur 19

Vous générez un premier rapport, dont un extrait est fourni dans le dossier documentaire.

Question B1.1

Lister au moins deux éléments de sûreté pertinents déjà mis en œuvre pour le service d'annuaire *Active Directory*. Justifier la réponse.

Question B1.2

Analyser la politique de mot de passe mise en œuvre pour assurer une bonne sécurité, en indiquant au moins trois éléments judicieux et deux éléments discutables de cette politique.

Suite à une sensibilisation à la sécurité effectuée récemment par un partenaire auprès de la majorité des utilisateurs de votre organisation, monsieur Denis BRODIER, responsable des ressources humaines, vous alerte de la fuite de son mot de passe. Le site *web haveibeenpwned.com* a confirmé ce vol et sa publication. Cette fuite impacte la sécurité de l'établissement par le statut de cet utilisateur avec pouvoir (il possède des droits supplémentaires) et la réutilisation du même mot de passe auprès de différentes entités dont la clinique MARTIN.

Votre hiérarchie vous demande de rappeler certaines bonnes pratiques rattachées à la gestion des mots de passe, ces préconisations seront diffusées par la suite à l'ensemble du personnel.

Question B1.3

- a) Expliquer par un exemple concret le danger d'utiliser un mot de passe même complexe de manière répétée.
- b) Proposer un outil aidant les utilisateurs à respecter la logique « un site = un mot de passe unique » tout en maintenant un bon niveau de sécurité.

Mission B2 – Analyser un audit de sécurité de l'annuaire *Active Directory* (deuxième partie)

Le rapport d'audit fourni par l'outil *PingCastle* fait apparaître la présence de machines disposant d'un système d'exploitation considéré comme obsolète et potentiellement dangereux pour la sécurité.

Question B2.1

- a) Expliquer pourquoi la présence de machines utilisant un système d'exploitation trop ancien pose des problèmes de sécurité.
- b) Préciser le critère que peut utiliser l'outil *PingCastle* pour considérer les machines comme vulnérables d'après l'obsolescence des systèmes d'exploitation

Le rapport d'audit généré par l'outil *PingCastle* fait également apparaître la problématique de la mise en cache des informations d'authentification pour les comptes administrateurs, comme étant un élément de vulnérabilité pour le système d'information.

Question B2.2

- a) Expliquer pourquoi la mise en cache des informations d'identification sur les postes clients est particulièrement problématique pour les administrateurs.
- b) Proposer une solution à cette problématique pour les différents administrateurs amenés à s'authentifier sur le réseau de la clinique MARTIN. Justifier la réponse.

Mission B3 : Centraliser les journaux d'événements (logs)

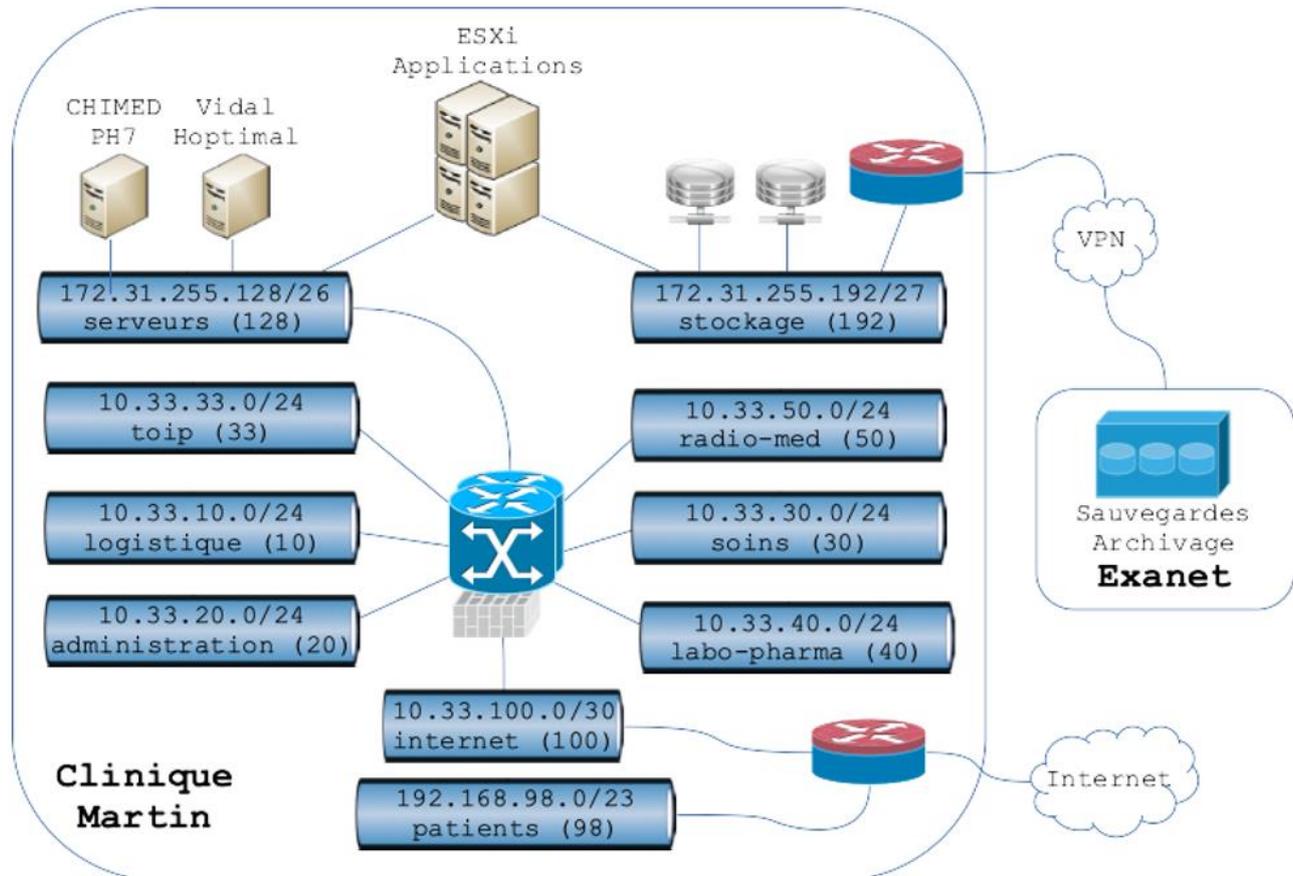
Parmi les anomalies, ou points de vigilance, l'outil *PingCastle* évoque la possibilité d'utiliser l'outil WEF (*Windows event forwarding*) de centralisation des journaux d'événements (logs).

Question B3.1

- a) Indiquer si le service WEF est utilisé actuellement dans l'infrastructure.
- b) Indiquer si l'utilisation de ce système vous paraît pertinente dans le contexte de la clinique MARTIN. Justifier la réponse.
- c) Préciser les avantages et la limite de ce système de centralisation.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 6 sur 19

Document 1 : Schéma et description de l'infrastructure réseau envisagée



L'infrastructure réseau est déployée sur l'ensemble des quatre bâtiments de la clinique, reliés par des dorsales fibre. Les bureaux de la DSI ainsi que la salle serveur sont dans le bâtiment [D] Logistique et pharmacie. Les autres bâtiments sont dédiés à [A] Accueil et consultations ; [B] Radiologie et laboratoire ; [C] Blocs et chambres.

Les passerelles ont pour adresse IP la dernière de leur sous-réseau.

Les serveurs d'annuaire Active Directory appartiennent au réseau 172.31.255.128/26. La ferme de virtualisation ESXi héberge le contrôleur de domaine Windows 2019, ainsi que les applications principales suivantes :

- **Administratif** PASTEL (dossier administratif patient) ; CDR (consultation droits carte vitale)
- **Médical** Cariatides (dossier médical patient) ; Superdoc (archives médicales)
- **Logistique** Hospitalis (commandes de médicaments) ; AGIRH (planning des services)

Document 2 : Sigles couramment utilisés dans les documents

- AD : *active directory*, service Windows d'authentification centralisée.
- ANSSI : agence nationale de la sécurité des systèmes d'information.
- DSI : direction des systèmes d'information.
- HDS : hébergeur de données de santé.
- HIDS (*host-based intrusion detection system*) : système de détection des intrusions basé sur l'hôte, logiciel qui surveille un système informatique sur lequel il est installé. Il s'agit d'un système permettant de détecter une intrusion et/ou une utilisation abusive.
- RGPD : règlement général sur la protection des données.
- RSSI : responsable de la sécurité des systèmes d'information.
- TLS (*transport layer security*) : sécurité de la couche de transport ; protocole de sécurisation des échanges.
- TOIP (*telephony over internet protocol*) : protocole de téléphonie sur IP, service de communications – public ou privé – qui utilise le protocole de réseau Internet.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 7 sur 19

Documents associés au dossier A

Document A1 : Événements redoutés

N°	Risque
1	Vol de données patient
2	Modification d'informations médicales
3	Non accès aux données
4	Perte des connexions réseaux
5	Applications administratives indisponibles
6	Applications de visioconférence indisponibles
7	Application de supervision réseaux indisponible
8	Vol de matériel informatique (ordinateurs portables, tablettes, imprimantes, etc.)

Document A2 : Niveau de gravité EBIOS

NIVEAU DE L'ÉCHELLE	DÉFINITION
G5 CATASTROPHIQUE	Conséquences sectorielles ou régaliennes au-delà de l'organisation. Écosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables. Et/ou : difficulté pour l'État, voire incapacité, d'assurer une fonction régalienne ou une de ses missions d'importance vitale. Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d'infrastructures essentielles, etc.).
G4 CRITIQUE	Conséquences désastreuses pour l'organisation avec d'éventuels impacts sur l'écosystème. Incapacité pour l'organisation d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. L'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels elle opère seront susceptibles d'être légèrement impactés, sans conséquences durables.
G3 GRAVE	Conséquences importantes pour l'organisation. Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. L'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique.
G2 SIGNIFICATIVE	Conséquences significatives mais limitées pour l'organisation. Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. L'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Conséquences négligeables pour l'organisation. Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. L'organisation surmontera la situation sans trop de difficultés.

Source : d'après https://www.ssi.gouv.fr/uploads/2018/10/fiches-methodes-ebios_projet.pdf

Document A3 : Extrait du guide « Attaques par rançongiciels, tous concernés » publié par l'Agence nationale de la sécurité des systèmes d'information en septembre 2020.

Réduire le risque d'attaque : Les mesures qui suivent permettront d'éviter qu'une attaque par rançongiciel atteigne l'organisation ou réduiront les pertes liées à une telle attaque.

I. Sauvegarder les données

Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques doivent être réalisées. Ces sauvegardes, au moins pour les plus critiques, doivent être déconnectées du système d'information pour prévenir leur chiffrement, à l'instar des autres fichiers.

II. Maintenir à jour les logiciels et les systèmes

Les vulnérabilités non corrigées des systèmes d'exploitation ou des logiciels présents sur le système d'information peuvent être utilisées pour infecter le système ou favoriser la propagation de l'infection. De la même manière, les ressources exposées sur internet non mises à jour sont régulièrement exploitées par les attaquants. Il est donc essentiel de porter une attention toute particulière à l'application de correctifs de sécurité dans les plus brefs délais. Enfin, assurer une veille permanente permet de rester informé de la découverte des vulnérabilités logicielles et matérielles.

III. Cloisonner le système d'information

Sans mesure de protection et à partir d'une seule machine infectée, le rançongiciel peut se propager sur l'ensemble de votre système d'information et infecter la plupart des machines accessibles. Pour limiter le risque de propagation, il convient de mettre en place un ou plusieurs dispositifs de filtrage permettant un cloisonnement entre les différentes zones réseaux plus ou moins critiques du système d'information.

IV. Limiter les droits des utilisateurs et les autorisations des applications

Une première bonne pratique consiste à vérifier que les utilisateurs ne sont pas administrateurs de leur poste de travail. Ainsi, l'installation de logiciels et l'exécution involontaire de codes malveillants seront impossibles par défaut. Une autre bonne pratique consiste à dédier et à limiter les comptes d'administration sur les ressources du système d'information et à mettre en place des postes de travail dédiés à l'administration, sans accès à internet. Parmi les règles de sécurité supplémentaires applicables, les stratégies de restriction d'exécution logicielle (*HIDS type Windows Defender ATP et Applocker sous Windows*) permettent de limiter l'exécution de logiciels malveillants.

V. Sensibiliser les collaborateurs

Le plus souvent, l'attaque par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page *web* malveillante. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace même si elle ne constitue pas un rempart absolu. L'objectif est également de faire naître ou de renforcer certains réflexes chez les utilisateurs en les invitant à signaler au service informatique de l'organisation tout élément suspect (exemple : pièce-jointe ou courriel douteux, clé USB offerte, requêtes inhabituelles, etc.).

VI. Mettre en œuvre un plan de réponse aux cyberattaques

La spécificité des attaques par rançongiciel est leur potentiel effet déstabilisateur sur les organisations. Il est donc crucial pour les organisations de définir un plan de réponse aux cyberattaques associé au dispositif de gestion de crise, quand il existe, visant à assurer la continuité d'activité puis son retour à un état nominal. La mise en œuvre d'un plan de continuité informatique doit permettre à votre organisation de continuer à fonctionner quand survient une altération plus ou moins sévère du système d'information.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 9 sur 19

Document A4 : Schéma d'une attaque classique par rançongiciel

Phase 1

- Le pirate envoie un courriel malveillant ;
- La victime ouvre le courriel.

Phase 2

- La victime télécharge la pièce-jointe contenue dans le courriel ;
- Le rançongiciel contacte le serveur du pirate pour obtenir une clé de chiffrement ;
- Les données présentes sur le disque dur de la victime sont chiffrées.

Phase 3

- Un message s'affiche sur l'ordinateur de la victime lui demandant de payer une rançon pour récupérer ses données ;
- Si la victime paie, le pirate peut transmettre à la victime la clé privée permettant de déchiffrer ses données ;
- Si la victime ne possède pas cette clé privée, elle perd l'ensemble des données concernées.

Document A5 : Traitement des règles de filtrage et de sécurité concernant les flux HTTP et HTTPS sur un pare-feu UTM.

Premier test effectué

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
<input checked="" type="checkbox"/> on	passer	Network_internals	Internet	http		IPS Antivirus Filtrage URL : Blacklist-categories-URL
<input checked="" type="checkbox"/> on	passer	Network_internals	Internet	https		IPS Antivirus Filtrage URL : Blacklist-categories-URL

VÉRIFICATION DE LA POLITIQUE

 [Règle 2] Une inspection appliquée sur un protocole SSL nécessite d'être précédée d'une règle déchiffrant ce trafic.

Second test après la prise en compte du message d'avertissement

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
<input checked="" type="checkbox"/> on	passer	Network_internals	Internet	http		IPS Antivirus Filtrage URL : Blacklist-categories-URL
<input checked="" type="checkbox"/> on	déchiffrer	Network_internals	Internet	https		IPS Antivirus Filtrage URL : Blacklist-categories-URL
<input checked="" type="checkbox"/> on	passer	Network_internals via Proxy SSL	Internet	https		IPS Antivirus Filtrage URL : Blacklist-categories-URL

NB : L'objet *Network_internals* représente l'ensemble des réseaux privés de la clinique MARTIN.

Filtrage URL sous forme de listes noires

(1) Blacklist-categories-URL		Editer		Fournisseur de base URL : Base URL embarquée	
+ Ajouter		x Supprimer		↑ Monter	
		↓ Descendre		Couper	
		Copier		Coller	
	État	Action	Catégorie d'URL	Commentaire	
1	<input checked="" type="checkbox"/> on	Bloquer	ads		
2	<input checked="" type="checkbox"/> on	Bloquer	entertainment		
3	<input checked="" type="checkbox"/> on	Bloquer	illegal		
4	<input checked="" type="checkbox"/> on	Bloquer	online		
5	<input checked="" type="checkbox"/> on	Bloquer	pornography		
6	<input checked="" type="checkbox"/> on	Bloquer	proxy		
7	<input checked="" type="checkbox"/> on	Bloquer	warez		
8	<input checked="" type="checkbox"/> on	Passer	any	default rule (pass all)	

Catégories d'URL : Publicité (*ads*), culture et loisirs (*entertainment*), contenu illicite (*illegal*), jeux en ligne, paris, radio, réseaux sociaux et partage de fichiers (*online*), contenu pornographique ou érotique (*pornography*), proxys anonymes (*proxy*), piratage informatique et violation des droits d'auteurs (*warez*).

Document A6 : Extrait des recommandations de sécurité concernant l'analyse des flux HTTPS publiées par l'ANSSI en 2014

Avant de mettre en place des mécanismes de déchiffrement au niveau d'un serveur mandataire (*proxy*) *web*, il est nécessaire de bien comprendre les avantages, les inconvénients et les problématiques que cela induit.

La possibilité de disposer du trafic HTTPS en clair au niveau d'un serveur mandataire (*proxy*) *web* procure plusieurs avantages :

- il est possible d'analyser le trafic HTTPS afin de protéger le client de menaces émanant du serveur *web* cible : contenus inappropriés, fichiers malveillants, etc. ;
- il est possible de contrôler le contenu des données échangées entre le client et le serveur afin de s'assurer que les flux HTTPS ne sont pas utilisés pour faire sortir du système d'information des données confidentielles. L'analyse doit être réalisée en limitant autant que possible l'exposition des données à caractère personnel des usagers ;
- il est possible d'appliquer la même politique de journalisation que celle mise en œuvre pour les flux HTTP non sécurisés. La journalisation doit être réalisée en accord avec le respect de la vie privée des usagers ;
- le serveur mandataire (*proxy*) a la possibilité de mettre en cache du contenu qu'il peut resservir à plusieurs clients qui souhaitent accéder au même serveur cible.

Cependant, le déchiffrement présente plusieurs inconvénients :

- des données normalement chiffrées sont présentes en clair au niveau du serveur mandataire (*proxy*). Si ce dernier est compromis, des informations sensibles peuvent être exposées ;
- l'authentification du client à l'aide d'un certificat n'est plus possible auprès d'un site *web* qui requerrait ce mode d'authentification. En effet, le serveur mandataire (*proxy*) étant placé en coupure, le client ne dialogue pas directement via le protocole TLS avec le site *web* ; il ne reçoit donc pas les demandes d'authentification par certificat formulées par ce dernier. Les sites qui requièrent une authentification par certificat doivent donc être placés dans une liste blanche pour laquelle le déchiffrement n'est pas effectué ;
- le niveau de sécurité du tunnel TLS établi sur internet avec le serveur cible ne dépend plus du navigateur *web* du client. Celui-ci n'est donc pas en mesure de connaître les risques qu'il prend. La sécurisation des tunnels TLS établis avec le monde extérieur repose uniquement sur les possibilités offertes par le serveur mandataire (*proxy*) en tant que client, celui-ci étant potentiellement plus laxiste au niveau du protocole TLS que les navigateurs *web* les plus récents ;
- une autorité de certification interne doit être employée pour générer les certificats que le serveur mandataire (*proxy*) présente à ses clients.

En résumé, si le déchiffrement des flux HTTPS permet un meilleur contrôle des données échangées entre un système d'information et le monde extérieur, ce processus complexifie l'architecture d'accès à internet et déporte la sécurisation du canal de communication avec l'extérieur sur le serveur mandataire (*proxy*). Ce type d'équipement devient ainsi très critique. L'attaque de l'homme du milieu repose sur un principe très similaire à celui du fonctionnement d'un serveur mandataire (*proxy*) dans ce cas de déchiffrement pour analyses diverses du contenu transporté (antivirus, filtrages divers, etc.).

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 12 sur 19

Document A7 : Messages d'erreur émis par le navigateur internet du poste client de test

Connexion bloquée : problème de sécurité potentiel

Firefox a détecté une menace potentielle de sécurité et a interrompu le chargement de www.google.com, car ce site web nécessite une connexion sécurisée.

Que pouvez-vous faire ?

www.google.com a recours à une stratégie de sécurité HTTP Strict Transport Security (HSTS), une connexion sécurisée est obligatoire pour y accéder. Vous ne pouvez pas ajouter d'exception pour visiter ce site.

Le problème vient probablement du site web, donc vous ne pouvez pas y remédier.

Si vous naviguez sur un réseau d'entreprise ou si vous utilisez un antivirus, vous pouvez contacter les équipes d'assistance pour obtenir de l'aide. Vous pouvez également signaler le problème aux personnes qui administrent le site web.

[En savoir plus...](#)

[Retour](#) [Avancé...](#)

Quelqu'un pourrait être en train d'essayer d'usurper l'identité du site. Vous ne devriez pas poursuivre.

Les sites web justifient leur identité par des certificats. Firefox ne fait pas confiance à www.google.com, car l'émetteur de son certificat est inconnu, le certificat est auto-signé ou le serveur n'envoie pas les certificats intermédiaires corrects.

Code d'erreur : [SEC_ERROR_UNKNOWN_ISSUER](#)

[Afficher le certificat](#)

Certificat

	www.google.com	pki.cliniquemartin.fr	SSL Proxy Trusted CA 5fce40f7
Nom du sujet			
Pays	FR		
État / Province	Gironde		
Localité	Bordeaux		
Organisation	Clinique Martin		
Unité organisationnelle	PKI		
Nom courant	www.google.com		
Adresse électronique	postmaster@cliniquemartin.fr		
Nom de l'émetteur			
Pays	FR		
État / Province	Gironde		
Localité	Bordeaux		
Organisation	Clinique Martin		
Unité organisationnelle	PKI		
Nom courant	SSL Proxy Trusted CA 5fce40f7		
Adresse électronique	postmaster@cliniquemartin.fr		
Validité			
Pas avant	30/11/2023 à 15:49:51 (heure normale d'Europe centrale)		
Pas après	14/12/2024 à 15:49:51 (heure normale d'Europe centrale)		

Document B1 : Notions d'annuaire « Active Directory »

Domaine et contrôleur de domaine

Le domaine représente une limite de sécurité où les utilisateurs sont définis.

Un domaine contient au moins un contrôleur de domaine. Néanmoins il est recommandé d'en avoir deux afin d'assurer l'authentification en cas de maintenance ou de panne d'un des serveurs d'annuaire. Si plus aucun serveur n'est en ligne, l'authentification ne pourra plus être assurée, ce qui va impliquer une perte de production pour l'ensemble des utilisateurs.

Un serveur ayant le rôle de contrôleur de domaine a la responsabilité de l'authentification des comptes utilisateurs et ordinateurs.

Il est possible de trouver différents types d'objets *Active Directory* : utilisateur, groupe, ordinateur, unité d'organisation, imprimante, [...]

Corbeille « Active Directory »

La suppression accidentelle d'un objet *Active Directory* peut avoir un impact plus ou moins important sur la production.

Lorsque la corbeille est activée, les attributs des objets *Active Directory* supprimés sont préservés. Il est donc possible d'effectuer la restauration de l'objet dans son intégralité.

Depuis Windows Server 2012, la fonctionnalité a été améliorée par l'ajout d'une interface graphique qui permet la restauration d'un objet supprimé. Une liste de tous les objets ayant été supprimés s'affiche. L'administrateur peut ainsi sélectionner ceux dont il souhaite la récupération.

Extraits de la source Editions ENI « Windows Server 2019 : Les bases indispensables pour administrer et configurer votre serveur »

Document B2 : Présentation du programme PingCastle

PingCastle : Dans quel état est votre annuaire Active Directory ?

L'annuaire *Active Directory* (AD) représente la colonne vertébrale de votre système d'information. Tous les utilisateurs, groupes, gestions de droits, etc. sont gérés dans l'annuaire AD. Comme toute solution, au fil des années les règles de sécurité changent et il faut maintenir son infrastructure.

Pour aider à avoir une vision plus claire, l'outil *PingCastle* permet d'analyser l'état de votre annuaire AD.

Qu'est-ce que l'outil PingCastle ?

C'est un programme autonome (pas besoin de l'installer), qui parcourt la configuration de votre annuaire AD et contrôle si toutes les règles préconisées par l'ANSSI sont appliquées.

En cas de mauvais réglage, vous avez des points "malus" répartis en 4 catégories (objets obsolètes, comptes privilégiés, relations d'approbation *Trusts* et anomalies). Le nombre de points varie en fonction de la gravité. Celle-ci peut varier de plusieurs dizaines de points pour les cas les plus critiques à 0 pour les règles d'informations.

Les points forts de l'outil :

- basé sur les préconisations de l'ANSSI ;
- analyse (*scan*) rapide et rapports clairs (format HTML et XML). La présentation est propre sans être surchargée ;
- pas besoin d'être administrateur du domaine pour faire un bilan de santé (*healthcheck*) ;
- disponible en plusieurs versions dont une gratuite qui donne déjà des pistes pertinentes ;
- pilotable en ligne de commande ;
- support très réactif même avec la version gratuite ;
- mise à jour régulière (tous les 6 mois environ) ;
- avoir dans les rapports les liens vers les documentations pour corriger le "problème", par exemple les recommandations ANSSI ainsi que les articles Microsoft ou les sources Github.

Source : <https://jerome-raymond.medium.com/pingcastle-dans-quel-%C3%A9tat-est-votre-active-directory-8e4d2afaef2b>

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 14 sur 19

cmartin.local - Analyse bilan de santé

Date : 2023-04-25 - Version moteur : 2.11.0.1

Indicateurs Active Directory

Cette section se concentre sur les indicateurs de sécurité de base. Localisez le sous-processus déterminant le score et fixez certaines règles dans cette zone pour obtenir une amélioration du score.

Indicateurs



Niveau de risque de domaine: 90 / 100

C'est le score maximum des 4 indicateurs et un score ne peut pas être supérieur à 100. Plus c'est bas, mieux c'est

[Comparer avec les statistiques](#)

[Avis de confidentialité](#)

<p>Bien périmé : 66 / 100 Il s'agit d'opérations liées à des objets utilisateur ou informatiques</p>	<p>7 règles appariées</p> <p>Fiducies : 0 / 100 Il s'agit de liens entre deux Active Directory</p>	<p>0 règles correspondantes</p>
<p>Comptes privilégiés : 65 / 100 Il s'agit des administrateurs d'Active Directory</p>	<p>5 règles appariées</p> <p>Anomalies : 90 / 100 Il s'agit de points de contrôle de sécurité spécifiques</p>	<p>13 règles appariées</p>

Informations sur l'utilisateur

Cette section fournit des informations sur les comptes d'utilisateurs stockés dans Active Directory

Analyse de compte

Nb Comptes d'utilisateurs	Nb activé	Nb Désactivé	Nb Actif	Nb Inactif	Nb verrouillé	Nb pwd n'expire jamais	Nb SidHistoire	Nb Bad PrimaryGroup	Nb Mot de passe non Req.	Nb Des activé.	Nb délégations sans contrainte	Nb Mot de passe réversible
77	64	13	60	4	0	34	0	23	54	0	0	0

[Objets inactifs \(dernière utilisation > 6 mois\)](#) [4]

[Objets avec un mot de passe qui n'expire jamais](#) [34]

[Objets dont l'attribut de groupe principal a été modifié](#) [23]

Stratégies de mot de passe

Remarque : Les PSO (Password Settings Objects) ne sont visibles que si l'utilisateur qui a collecté les informations a la permission de les consulter. L'OSP indiquée dans le rapport sera précédée du préfixe « PSO » :

Nom de la stratégie	Complexité	Âge maximal du mot de passe	Âge minimum du mot de passe	Longueur minimale du mot de passe
Stratégie de domaine par défaut	Vrai	270 jour(s)	1 jour(s)	7

Historique des mots de passe	Chiffrement réversible	Seuil de cadencage	Durée du cadencage	Réinitialiser le casier du compteur de compte après
24	Faux	15	5 minute(s)	5 minute(s)

Informations sur le domaine

Cette section présente les principales caractéristiques techniques du domaine.

Domaine	Nom Netbios	Niveau fonctionnel du domaine	Niveau fonctionnel de la forêt	Date de création	Nombre de DC	Version du schéma	Corbeille activée
cmartin.local	CMARTIN	Windows Server 2016	Windows Server 2016	2020-01-27 16:22:53Z	2	Windows Server 2019	VRAI

Systèmes d'exploitation

Système d'exploitation	Nb OS	Nb activé ?	Nb Désactivé ?	Nb Actif ?	Nb Inactif ?	Nb SidHistoire ?	Nb Bad PrimaryGroup
inconnu	1	1	0	1	0	0	
OperatingSystem non défini	5	5	0	3	2	0	
Windows Server 2016 1607	6	6	0	6	0	0	
Windows 10 1803	7	7	0	4	3	0	
Windows 10 21H1	55	55	0	55	0	0	
Windows 10 2004	2	2	0	1	1	0	
Windows 10 1809	1	1	0	0	1	0	
Windows Server 2003 SP2	1	1	0	1	0	0	
Windows 10 1703	1	1	0	1	0	0	
Windows 10 21H2	28	28	0	28	0	0	
Windows 10 1903	1	1	0	0	1	0	
Windows 10 20H2	2	2	0	2	0	0	
Windows Server 2019 1809	3	3	0	2	1	0	
Windows 10 1909	1	1	0	1	0	0	

Contrôleurs de domaine

Voici un zoom spécifique lié aux serveurs Active Directory : les contrôleurs de domaine.

[Contrôleurs de domaine](#)

[2]

Contrôleur de domaine	Système d'exploitation	Date de création ?	Temps de démarrage	Disponibilité	Propriétaire ?	Sessions nu
SRV-01	Windows 2019	2020-01-27 16:23:42Z	2022-06-19 16:43:06Z	115 jours	cmartin\Admins du domaine	NON
SRV-02	Windows 2019	2020-02-06 14:32:06Z	2021-10-27 13:01:15Z	351 jours	cmartin\Admins du domaine	NON

Anomalies

Transfert d'événements Windows (WEF)

Windows Event Forwarding est un mécanisme natif utilisé pour collecter des logs sur tous les postes / serveurs du domaine. Microsoft recommande [d'utiliser le transfert d'événements Windows pour faciliter la détection des intrusions](#). Voici la liste des serveurs configurés pour WEF trouvés dans GPO

Nombre de configuration WEF trouvée: 0

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 16 sur 19

Document B5 : Les utilisateurs protégés dans l'annuaire Active Directory

Un groupe de sécurité spécial, appelé « *ProtectedUsers* » (utilisateurs protégés), est présent dans le gestionnaire d'annuaire « *Active Directory* ». Il applique automatiquement des protections pour minimiser l'exposition des informations d'identification, à partir de Windows 8.1.

Pour les administrateurs, ce groupe de sécurité :

- désactive l'authentification NTLM (protocole d'authentification utilisé par Microsoft), réduit la durée de vie du ticket Kerberos, impose des algorithmes de chiffrement forts, tels que AES ;
- empêche la mise en cache des mots de passe sur les postes de travail, empêche tout type de délégation Kerberos.

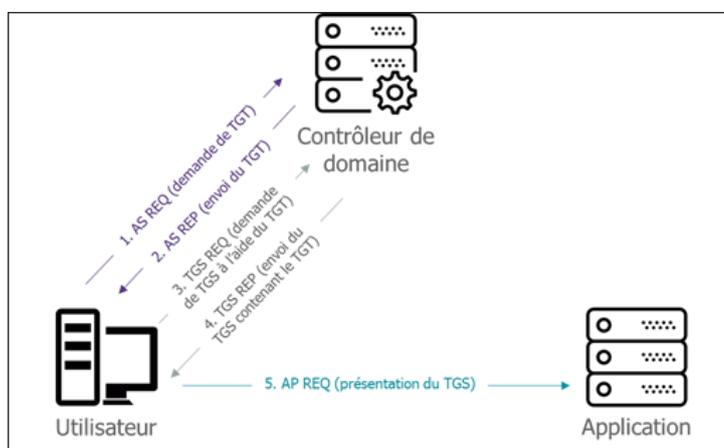
Toutefois, il est recommandé qu'au moins un compte soit conservé en dehors du groupe utilisateurs protégés, en cas de problème d'autorisation.

Source : D'après l'aide associée au rapport PingCastle

Rappels sur le protocole d'authentification Kerberos

Kerberos est un protocole d'authentification réseau reposant sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets. Il fait partie intégrante des systèmes d'exploitation Windows depuis la version Windows Serveur 2000. Différents termes spécifiques sont utilisés pour détailler ce protocole :

- KDC (*key distribution center*) : service installé sur les contrôleurs de domaine et permettant l'obtention des différents tickets par un utilisateur.
- TGT (*ticket-granting ticket*) : ticket attribué par le service KDC à un utilisateur. Ce ticket représente l'identité de l'utilisateur, et lui permet d'effectuer des demandes de tickets TGS auprès du service KDC.
- TGS (*ticket-granting service*) : ticket attribué par le service KDC pour représenter un utilisateur. Il permet à l'utilisateur de s'authentifier auprès d'un service spécifique, dont le nom est inscrit dans le ticket.



Le schéma d'une authentification Kerberos classique est représenté par l'illustration ci-contre.

Adapté du site <https://www.riskinsight-wavestone.com/2017/04/compromission-domaine-windows-delegation-kerberos/>

Mise en cache des informations d'identification de l'annuaire Active Directory

Pour comprendre l'objectif des informations d'identification mises en cache, examinons le processus normal de connexion en termes généraux. Lorsqu'un utilisateur se connecte sur un ordinateur relié à un domaine, ses informations d'identification sont transmises au contrôleur de domaine le plus proche dans l'environnement. Le contrôleur de domaine vérifie les informations d'identification, et soit authentifie l'utilisateur, soit rejette les informations d'identification saisies.

Les travailleurs distants qui utilisent des ordinateurs portables reliés à un domaine pour accéder aux ressources de l'entreprise ne se connecteront pas directement au réseau de l'entreprise. Par extension, ces utilisateurs n'auront pas accès à un contrôleur de domaine pour répondre aux demandes d'authentification. La solution à ce problème est la mise en cache des informations d'identification.

Comment fonctionnent les justificatifs d'identité mis en cache ?

Les informations d'identification mises en cache permettent à la station de travail ou à l'ordinateur portable distant de stocker la valeur hachée d'une connexion réussie dans un cache d'informations d'identification local qui permet à l'ordinateur de s'authentifier et de se connecter localement, qu'un contrôleur de domaine soit disponible ou non. Microsoft stocke la valeur hachée dans la clé de registre HKEY_LOCAL_MACHINE\SECURITY.

D'après un article du blog <https://specopssoft.com/fr/blog/>

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 17 sur 19

Document B6 : Utiliser le transfert d'événements Windows (Windows event forwarding : WEF) pour optimiser la détection d'intrusion

Le transfert d'événements Windows (WEF) lit tout journal des événements opérationnels ou administratifs sur un appareil de votre organisation et transfère les événements que vous choisissez à un serveur Windows Event Collector (WEC).

Pour accomplir cette fonctionnalité, deux abonnements différents sont publiés sur les appareils clients : l'abonnement de base et l'abonnement suspect. L'abonnement base de référence inscrit tous les appareils de votre organisation, et un abonnement Suspect inclut uniquement les appareils que vous avez ajoutés. L'abonnement Suspect collecte davantage d'événements pour aider à créer le contexte de l'activité du système et peut être rapidement mis à jour pour prendre en charge de nouveaux événements et/ou scénarios en fonction des besoins sans affecter les opérations de base.

Le transfert d'événements Windows (WEF) est-il de type envoyé (push) ou tiré (pull) ?

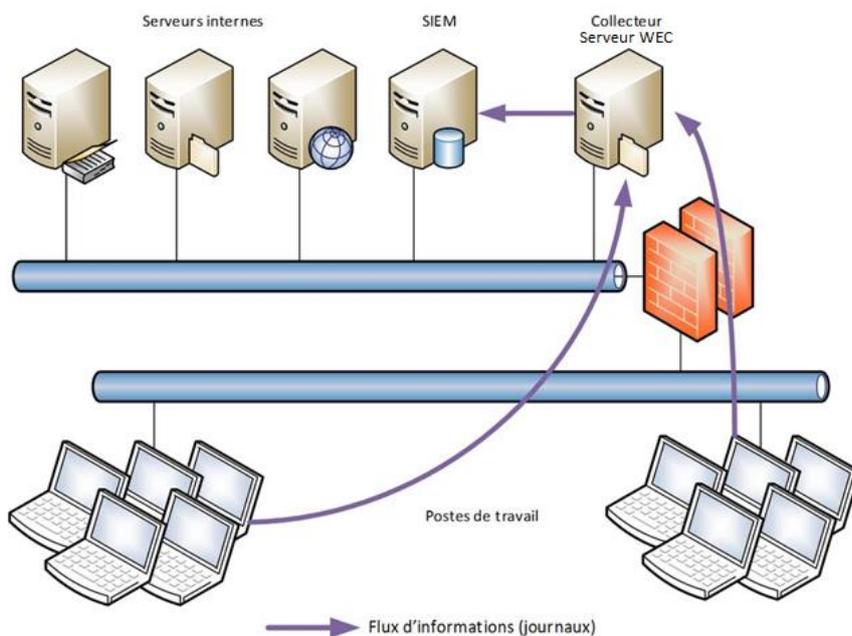
Un abonnement WEF peut être configuré pour être envoyé (push) ou tiré (pull), mais pas les deux. Le déploiement informatique le plus simple et le plus flexible avec la plus grande extensibilité (*scalability*) peut être obtenu à l'aide d'un abonnement push ou initié par la source. Les clients WEF sont configurés de manière automatique (à l'aide d'un objet de stratégie de groupe) et le client de transfert intégré est activé. Pour l'extraction lancée par le collecteur, l'abonnement sur le serveur WEC est préconfiguré avec les noms des appareils clients WEF à partir desquels les événements doivent être sélectionnés. Ces clients doivent être configurés à l'avance pour permettre aux informations d'identification utilisées dans l'abonnement d'accéder à distance à leurs journaux des événements (normalement en ajoutant les informations d'identification au groupe de sécurité local intégré « Lecteurs du journal des événements »). Un scénario utile : surveiller de près un ensemble spécifique de machines.

Adapté de <https://learn.microsoft.com/fr-fr/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

Intégration du transfert d'événements de Windows (WEF) avec un outil SIEM (security information and event management – gestion de l'information et des événements de sécurité)

Les environnements Windows (depuis Windows Vista/2008 server) proposent nativement l'outil WEF. Ce dernier permet le transfert réseau des journaux Windows au format syslog, largement utilisé dans le milieu de la sécurité.

La centralisation des journaux nécessite d'une part de mettre en place le collecteur destiné à recevoir les événements, et d'autre part de configurer les sources destinées à fournir leurs événements au collecteur. Ce dernier pourra mettre les journaux à disposition d'un serveur de supervision via d'autres moyens (partage de dossier réseau, syslog, agent spécifique, etc.).



Source : À partir d'une recherche utilisant docplayer.fr

Cette approche, qui permet de passer par un serveur Windows pour remonter les journaux d'événements (*logs*) des machines dans l'infrastructure, possède plusieurs avantages... [cf. page suivante].

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 18 sur 19

Avantages à l'utilisation du transfert d'événements Windows (WEF) :

- D'abord, elle évite l'installation d'un agent sur l'ensemble des postes informatiques. Ce qui est toujours intéressant du point de vue des performances, mais également pour la maintenance dans le temps de cet agent. Il faut en effet acquérir des compétences pour le gérer, le maintenir à jour et suivre ses vulnérabilités sur l'ensemble du parc.
- Ensuite, cela permet d'avoir une couche de collecte dédiée et distincte du service de centralisation et de recherche : le SIEM (Security Information and Event Management – Splunk, ELK, logpoint, greylog et Azure Sentinel en sont des exemples). Cette couche de collecte est très utile, car elle vous rend indépendant de votre SIEM. Le jour où vous souhaitez changer de SIEM, il suffira de « rerouter » les journaux d'évènements depuis ce serveur WEF (ou syslog) vers le nouveau SIEM. Vous n'aurez pas à modifier les configurations de toutes les machines du parc qui transmettent des messages.

Les journaux d'évènements des machines Windows ainsi centralisés peuvent être transférés vers un collecteur Syslog classique. Pourquoi syslog ? Parce que l'écrasante majorité des SIEM fonctionne aujourd'hui sous Linux et supporte très bien des entrées syslog par défaut, et à l'inverse celles sous Windows sont assez mal supportées. Une alternative à syslog consiste à faire exporter les évènements au collecteur sous forme de fichiers, à intervalles réguliers, pour les transmettre au SIEM, via un partage NFS ou SMB par exemple.

Il existe de nombreux services (parfois open source) pour convertir et transférer des journaux Windows vers du syslog. On citera notamment Rsyslog, Syslog-ng, Snare et NXLog.

Extraits de la source Editions ENI « Cybersécurité et PowerShell : De l'attaque à la défense du système d'information ».

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2024
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 24SI6SISR-M1	Page 19 sur 19