

SOC Event Detection and Incident Response Strategies

Ce texte détaille le fonctionnement opérationnel d'un **centre opérationnel de sécurité (SOC)** lors de la détection et du traitement des menaces informatiques. Il met en lumière l'importance d'une **définition inclusive des événements**, soulignant que les signalements humains sont souvent plus efficaces que les seuls outils automatisés comme le **SIEM**. À travers l'exemple d'une cyberattaque par hameçonnage, l'ouvrage illustre la transition critique entre un simple signalement et l'ouverture d'une **enquête formelle**. La gestion d'incidents majeurs y est présentée comme un effort collectif exigeant une **collaboration étroite** entre les analystes, la direction et divers services internes tels que les réseaux ou les ressources humaines. Enfin, l'auteur insiste sur la nécessité de processus structurés et de **systèmes de gestion de cas** pour maintenir la cohésion de l'équipe sous pression.

Quelle est la différence entre un événement et un incident ?

Selon les sources, la différence fondamentale entre un événement et un incident réside dans la **gravité**, la **nature des conséquences** et la **décision d'un analyste** suite à une enquête.

Voici les distinctions clés :

- **L'événement** : Il s'agit d'une **observation de base** ou de n'importe quel artefact observable indiquant qu'un phénomène s'est produit. Les événements peuvent être des traces dans des journaux (logs) automatisés, des alertes générées par un SIEM, ou même un signalement humain (par exemple, un employé signalant un lien suspect par courriel). Un événement en soi n'est pas nécessairement néfaste ; il retrace simplement une action récente ou ancienne.
- **L'incident** : Un incident est une **décision formelle** prise par un enquêteur. On considère qu'il y a incident lorsqu'une série d'événements entraîne des **conséquences néfastes** réelles. Un

rapport d'incident est généralement créé pour signaler qu'un événement jugé **grave** s'est produit, justifiant ainsi une enquête approfondie.

- **Le processus de distinction** : Le rôle d'un SOC est d'analyser les événements pour déterminer s'ils indiquent un incident potentiel. C'est l'analyste, et non le système automatisé, qui détermine généralement si un rapport d'incident constitue un **incident réel** ou un **faux positif**. Un événement peut ne pas atteindre le seuil défini pour être qualifié d'incident (par exemple, s'il n'y a pas de dommages financiers ou si les conditions spécifiques à l'organisation ne sont pas remplies).

En résumé, l'événement est le **fait brut observé**, tandis que l'incident est la **confirmation d'une situation préjudiciable** nécessitant une intervention.

Quels outils sont utilisés pour transformer un événement en incident ?

Selon les sources, la transformation d'un événement en incident n'est pas un processus purement automatisé ; elle repose sur l'utilisation de plusieurs outils technologiques qui permettent à un analyste de qualifier la situation.

Voici les principaux outils utilisés dans ce processus :

- **Le SIEM (Gestion des informations et des événements de sécurité)** : C'est l'outil central de détection. Il collecte et regroupe les journaux (logs) provenant de sources variées et applique des règles pour automatiser la détection d'incidents de sécurité **potentiels**. Il hiérarchise ensuite ces alertes pour qu'un analyste les examine plus en profondeur. Dans certains cas, le SIEM peut même générer automatiquement un rapport d'incident.
- **Les systèmes de gestion des cas (ou systèmes de gestion des enquêtes)** : Ces outils servent à coordonner les investigations. Lorsqu'un analyste estime qu'un événement est grave, il crée un **rapport d'incident** dans ce système. Des solutions spécifiques comme **RTIR (Request Tracker for Incident**

Response) sont mentionnées comme des alternatives pour gérer ces dossiers.

- **Les solutions de gestion des journaux de sécurité (Log Management)** : Utilisées en complément du SIEM, elles permettent de stocker et de récupérer des données d'événements sur le long terme pour mener des investigations approfondies sur des événements qui n'auraient pas été initialement captés par le SIEM.
- **Les plateformes de communication et de collaboration** : Puisque la majorité des incidents sont signalés par des humains, les outils comme le **courriel**, la **téléphonie**, la **messagerie instantanée sécurisée** ou les **portails intranet** sont essentiels pour capturer les événements initiaux.
- **Les outils d'investigation spécialisés** : Pour confirmer qu'un événement est bien un incident, les analystes utilisent des solutions d'**analyse forensique d'entreprise** (recherche d'indicateurs de compromission) et des systèmes d'**analyse des vulnérabilités** pour vérifier si les failles détectées sont exploitables.

En définitive, bien que le SIEM automatise une partie de la détection, c'est généralement l'analyste qui, en s'appuyant sur ces outils, prend la **décision formelle** de qualifier un événement (ou une série d'événements) d'incident réel.

Qu'est-ce qu'une plateforme d'analyse forensique d'entreprise ?

Selon les sources, une **plateforme d'analyse forensique d'entreprise** est une solution technologique déployée sur les actifs d'une organisation (souvent les plus critiques) pour mener des investigations numériques approfondies.

Ses principales fonctions et caractéristiques sont les suivantes :

- **Investigations et recherche d'indices** : Elle permet de réaliser des **investigations ponctuelles** suite à une alerte et de mener une **recherche active d'indicateurs de compromission (IOC)** au sein du parc informatique. Cela aide les analystes à confirmer si un système a été réellement compromis.

- **Intégration technologique** : Ces plateformes sont généralement intégrées aux **systèmes de gestion des cas (enquêtes)** et aux SIEM pour rationaliser le processus de réponse aux incidents.
- **Capacités avancées** : Dans des contextes plus complexes, l'analyse forensique peut inclure l'**analyse de logiciels malveillants** (malware), la collecte de preuves numériques certifiées pour des procédures judiciaires ou l'analyse de la mémoire vive (via l'hibernation des machines) pour éviter la perte de données volatiles.
- **Déploiement ciblé** : Bien qu'idéalement étendue, elle est parfois limitée aux actifs jugés les plus sensibles par l'organisation en raison de contraintes techniques ou de coûts.

En résumé, cet outil transforme le SOC d'une simple surveillance passive à une capacité d'**investigation active**, permettant de comprendre précisément comment et quand une intrusion a eu lieu.

Quels sont les avantages de l'hibernation pour l'analyse mémoire ?

L'hibernation présente un avantage stratégique majeur pour l'analyse mémoire lors d'une investigation numérique :

- **Préservation des données volatiles** : Contrairement à un arrêt complet de la machine, l'hibernation permet de sauvegarder le contenu de la mémoire vive, qui risquerait autrement d'être définitivement perdu.
- **Analyse approfondie de l'état du système** : En conservant cet état, les analystes du SOC peuvent effectuer une analyse beaucoup plus poussée de ce qui se passait sur la machine au moment précis de l'incident.

Dans le scénario décrit dans les sources, cette technique est privilégiée par rapport à une extinction simple pour permettre aux enquêteurs de capturer un maximum d'indices sur l'activité malveillante en cours.

Quelles données la mémoire vive contient-elle après l'hibernation ?

Selon les sources, l'hibernation permet de sauvegarder l'intégralité de la **mémoire de la machine** (mémoire vive) telle qu'elle se trouvait au moment précis du déclenchement de l'action.

Voici ce que cette sauvegarde contient et permet :

- **Données volatiles** : Elle contient toutes les informations qui **risqueraient d'être définitivement perdues** si l'ordinateur était complètement éteint.
- **État du système** : En conservant le contenu de la mémoire vive, l'hibernation permet aux analystes de réaliser une **analyse plus poussée** de ce qui se passait sur le système au moment de l'incident.
- **Indices d'activité** : Bien que les sources ne listent pas de manière exhaustive chaque type de donnée technique, elles indiquent que cette capture mémoire est essentielle pour mener une investigation numérique approfondie sur une machine suspecte (comme celle de Robert dans le scénario) afin de comprendre les actions malveillantes en cours.

En résumé, l'hibernation transforme le contenu temporaire de la RAM en un état statique consultable ultérieurement par les experts en criminalistique numérique.

Comment fonctionne l'analyse forensique de la mémoire vive ?

Selon les sources, l'analyse forensique de la mémoire vive (ou criminalistique numérique de la RAM) fonctionne en capturant et en examinant l'état volatil d'un ordinateur pour identifier des activités malveillantes qui ne seraient pas visibles sur le disque dur.

Voici les étapes et principes de fonctionnement décrits dans les sources :

- **Préservation par l'hibernation** : Plutôt que d'éteindre complètement une machine suspecte, ce qui effacerait les données de la mémoire vive, on utilise l'**hibernation**. Cela permet de sauvegarder l'intégralité du contenu de la RAM dans un fichier statique, préservant ainsi des indices précieux qui risqueraient d'être perdus en cas d'arrêt.

- **Utilisation de plateformes spécialisées** : Les analystes utilisent des **solutions d'analyse forensique d'entreprise** déployées sur les actifs critiques. Ces outils permettent de mener des investigations ponctuelles et de rechercher activement des **indicateurs de compromission (IOC)** directement dans la mémoire capturée.
- **Recherche de traces d'activité en cours** : L'analyse de la mémoire permet de reconstituer précisément ce qui se passait sur le système au moment de l'incident. Cela inclut l'identification de processus malveillants, comme des **chevaux de Troie** ou des logiciels permettant un accès à distance, même s'ils sont inconnus des antivirus traditionnels.
- **Analyse de logiciels malveillants** : Une partie de ce travail peut être confiée à des prestataires spécialisés pour effectuer une **analyse forensique avancée**. Ils examinent des échantillons de code malveillant extraits de la mémoire pour comprendre leur fonctionnement, comme la communication avec des **serveurs de commande et de contrôle (C2)**.
- **Identification de l'exfiltration** : En croisant l'analyse mémoire avec d'autres données (comme la capture de paquets réseau), les experts peuvent déterminer si des informations confidentielles ont été exfiltrées via l'accès compromis.

En résumé, cette technique "gèle" l'état de l'ordinateur pour permettre une investigation approfondie sur les processus, les connexions et les codes malveillants actifs au moment de l'attaque.

Comment l'analyse de la RAM détecte-t-elle les chevaux de Troie ?

Selon les sources, l'analyse de la mémoire vive (RAM) permet de détecter les chevaux de Troie en examinant l'état actif du système pour y trouver des traces logicielles qui ne sont pas visibles sur le stockage permanent.

Voici comment ce processus fonctionne concrètement :

- **Préservation des preuves volatiles** : L'analyse commence par la mise en **hibernation** de la machine suspecte. Cette étape est cruciale car elle sauvegarde l'intégralité du contenu de la RAM

dans un fichier, évitant ainsi la perte des données volatiles qui s'effaceraient lors d'un arrêt complet.

- **Extraction et analyse d'échantillons** : Les enquêteurs extraient de la mémoire des **échantillons de code potentiellement malveillant**. Ces échantillons sont ensuite soumis à une **analyse forensique avancée** (souvent réalisée par des spécialistes externes) pour identifier la nature exacte du logiciel.
- **Identification des comportements caractéristiques** : L'analyse permet de détecter des variantes de chevaux de Troie, même si elles sont jusqu'alors inconnues des antivirus. Les experts recherchent spécifiquement des fonctions permettant un **accès à distance** et des communications avec des **serveurs de commande et de contrôle (C2)**.
- **Recherche active d'indicateurs de compromission (IOC)** : Les plateformes d'analyse forensique d'entreprise permettent de scanner la mémoire à la recherche d'**IOC** spécifiques. Ces indicateurs (comme des adresses IP suspectes ou des signatures de fichiers) sont souvent partagés par des fournisseurs de renseignements sur les menaces ou des partenaires du secteur.
- **Génération de signatures de détection** : Une fois le cheval de Troie identifié dans la RAM, les informations recueillies permettent de mettre à jour les solutions de sécurité (comme les antivirus) pour **détecter et bloquer le code malveillant** sur l'ensemble du parc informatique.

En résumé, l'analyse de la RAM "fige" l'activité du cheval de Troie en plein vol, permettant de disséquer son code et ses connexions réseau pour confirmer l'infection.

Comment l'analyse RAM aide-t-elle à identifier l'exfiltration de données ?

Selon les sources, l'analyse de la mémoire vive (RAM) est une étape cruciale pour identifier l'exfiltration de données, car elle permet de capturer l'activité malveillante en temps réel qui ne laisse pas forcément de traces sur le disque dur.

Voici comment elle aide spécifiquement à identifier l'exfiltration :

- **Identification des vecteurs d'exfiltration** : L'analyse de la RAM permet d'extraire des échantillons de **codes malveillants** (comme des variantes de chevaux de Troie) qui servent à établir un accès à distance. Dans le scénario décrit, c'est cette analyse qui a permis d'identifier un logiciel permettant de prendre le contrôle d'un système pour en extraire des données.
- **Détection des serveurs de commande et de contrôle (C2)** : L'analyse mémoire aide à découvrir les connexions actives vers des **serveurs C2**. Ces serveurs sont les destinations vers lesquelles les données volées sont généralement envoyées. Connaître ces adresses IP permet de retracer le flux de l'exfiltration.
- **Préservation des preuves de transfert** : En utilisant l'**hibernation** plutôt que l'extinction, les enquêteurs préservent l'état volatil de la machine. Cela inclut les processus de transfert de fichiers en cours, les sessions réseau actives et les clés de chiffrement qui pourraient être utilisées pour masquer l'exfiltration, autant d'éléments qui seraient perdus lors d'un redémarrage.
- **Confirmation de la compromission des données** : Dans le cas pratique cité, l'expertise judiciaire (incluant l'analyse forensique avancée) a permis de conclure qu'une **quantité limitée d'informations confidentielles** avait effectivement été exfiltrée via l'accès compromis d'un administrateur.
- **Corrélation avec le trafic réseau** : L'analyse de la RAM fonctionne de pair avec l'isolation et la **capture des données brutes du réseau**. En comparant ce qui est présent en mémoire (processus suspects) avec ce qui sort de la machine (trafic réseau vers l'extérieur), les analystes peuvent confirmer si des données quittent l'organisation.

En résumé, l'analyse de la RAM fournit le contexte technique (quel logiciel, vers quelle destination) qui permet de confirmer si un incident de sécurité a mené à une fuite de données réelle.

Quels sont les indicateurs de compromission typiques recherchés dans la RAM ?

Selon les sources, l'analyse de la mémoire vive (RAM) permet de rechercher des **indicateurs de compromission (IOC)** volatils qui ne sont pas nécessairement visibles sur le disque dur.

Voici les indicateurs typiques recherchés lors d'une investigation dans la RAM :

- **Échantillons de codes malveillants** : La RAM permet d'extraire des morceaux de code actifs. Dans le scénario étudié, cela a permis d'identifier des **variantes de chevaux de Troie** jusqu'alors inconnues des antivirus traditionnels.
- **Connexions aux serveurs de commande et de contrôle (C2)** : L'analyse mémoire aide à identifier les processus qui tentent de communiquer avec des infrastructures externes malveillantes. On y cherche des **adresses IP suspectes** et des détails sur la rotation des serveurs de commande utilisés par les attaquants.
- **Traces d'accès à distance** : On recherche des indicateurs montrant qu'un logiciel permet un **accès à distance** frauduleux à la machine. Cela permet de confirmer si un attaquant a pris le contrôle d'un système pour, par exemple, exfiltrer des données.
- **Processus et artefacts système actifs** : L'analyse de la RAM "gèle" l'état des processus en cours d'exécution au moment de l'**hibernation**. Cela inclut des indicateurs sur les actions d'un compte compromis (comme celui de l'administrateur Robert dans l'exemple) sur des ressources critiques.
- **Signatures et indicateurs fournis par le renseignement** : Les analystes utilisent des plateformes forensiques pour scanner la mémoire à la recherche d'**IOC spécifiques** (signatures de fichiers, adresses e-mail associées à des campagnes de phishing, etc.) partagés par des partenaires de confiance ou des fournisseurs de renseignement sur les menaces.

Ces indicateurs sont précieux car ils permettent de transformer une simple alerte en une **confirmation technique** de l'étendue d'une compromission.

Pourquoi est-il crucial de détecter les serveurs de commande C2 ?

La détection des **serveurs de commande et de contrôle (C2)** est une étape critique de la réponse aux incidents, car ces serveurs constituent le "centre nerveux" permettant aux attaquants de piloter une intrusion. Selon les sources et les éléments du scénario analysé, voici pourquoi leur détection est cruciale :

- **Identifier la prise de contrôle à distance** : Les serveurs C2 sont utilisés par des logiciels malveillants, comme certaines variantes de chevaux de Troie, pour établir et maintenir un **accès à distance** aux systèmes compromis. Sans la détection de ces serveurs, l'attaquant conserve la capacité de diriger ses outils malveillants depuis l'extérieur.
- **Obtenir des indicateurs de compromission (IOC)** : L'identification des adresses IP associées aux serveurs C2 fournit des **IOC précieux**. Ces informations permettent au SOC de vérifier si d'autres machines au sein de l'organisation communiquent avec la même infrastructure malveillante, révélant ainsi l'étendue réelle de l'attaque.
- **Confirmer l'exfiltration de données** : Les serveurs C2 servent souvent de destination pour les informations volées. Dans le cas étudié, l'analyse de l'accès compromis a permis de conclure que des **informations confidentielles ont été exfiltrées** via l'accès malveillant établi. Détecter le serveur C2 permet de retracer où les données ont été envoyées.
- **Permettre la remédiation et le blocage** : Une fois les serveurs C2 et les échantillons de code associés identifiés, les équipes de sécurité peuvent collaborer avec des fournisseurs d'antivirus pour créer des **mises à jour de détection spécifiques**. Cela permet de bloquer les communications malveillantes et de nettoyer l'ensemble du parc informatique pour éviter toute réinfection.

En résumé, détecter un serveur C2 permet de briser la chaîne de communication de l'attaquant, d'évaluer l'ampleur des dégâts (comme la fuite de données) et de mettre en œuvre des mesures de défense globales pour protéger l'organisation.

Quel est le rôle de Vicki Vale dans l'équipe ?

Dans l'équipe du SOC fictif présenté dans les sources, **Vicki Vale** occupe le rôle de **responsable des incidents** (Incident Manager).

Ses fonctions principales sont les suivantes :

- **Coordination des interventions** : Elle est chargée de coordonner les opérations lors de la gestion d'un dossier. Dans le cas d'un **incident majeur**, c'est elle qui pilote les actions des différentes équipes de support mobilisées.
- **Évaluation de l'analyse forensique** : Vicki examine les options d'**analyse forensique d'entreprise** disponibles sur les actifs critiques de l'organisation. Elle peut notamment effectuer des recherches actives d'**indicateurs de compromission (IOC)** sur certains systèmes.
- **Gestion de l'information** : Elle se familiarise avec les dossiers d'enquête (cas) ouverts par les analystes (comme Dan) et reçoit les mises à jour techniques pour les communiquer aux dirigeants et autres parties prenantes.

En résumé, tandis que les analystes comme Dan et Sarah se concentrent sur l'investigation technique, Vicki Vale assure la **gestion opérationnelle et stratégique** de la réponse à l'incident.

Comment Vicki Vale coordonne-t-elle la réponse aux incidents majeurs ?

Vicki Vale occupe le rôle de **gestionnaire d'incidents** (Incident Manager) et son action est déterminante lorsque la situation bascule d'une simple enquête à un **incident majeur**.

Selon les sources, elle coordonne la réponse à travers les actions suivantes :

- **Mobilisation des équipes de support** : Lorsqu'un incident majeur est déclaré (comme dans le scénario de la brèche de sécurité), c'est Vicki qui centralise la coordination. Elle déclenche des actions qui permettent de mobiliser, en moins de 15 minutes, la

plupart des **ressources d'astreinte** et des équipes de support internes via une téléconférence.

- **Pilotage opérationnel et stratégique** : Pendant que les analystes techniques (comme Dan et Sarah) expliquent les détails de l'intrusion, Vicki **dirige les opérations**. Elle se concentre sur l'ensemble des actions à mener et sur la communication de l'état d'avancement aux dirigeants et aux parties prenantes clés.
- **Gestion échelonnée des ressources** : Pour éviter l'épuisement de l'équipe lors d'incidents de longue durée, elle veille à ce que les ressources critiques soient déployées de manière **échelonnée**. Cela évite de mobiliser tous les experts dès le début et préserve la cohésion de l'équipe sur le long terme.
- **Exploration des capacités d'investigation** : Sur le plan technique, elle examine les options d'**analyse forensique d'entreprise** disponibles. Elle peut mener elle-même des recherches actives d'**indicateurs de compromission (IOC)** sur certains systèmes critiques pour évaluer l'étendue des dégâts.
- **Utilisation des outils de collaboration** : Elle s'appuie sur le système de **gestion des cas** (ou de gestion des tickets) pour assurer la coordination globale, car dans un incident majeur, le SOC ne contrôle plus seul la gestion de la crise.

En résumé, son rôle est de transformer l'expertise technique des analystes en une réponse organisée à l'échelle de toute l'entreprise, tout en protégeant l'équipe contre la fatigue et la surcharge.

Comment l'équipe de Dan collabore avec la direction ?

L'équipe de Dan (analyste CSIRT de niveau 3) collabore avec la direction de plusieurs manières, principalement par l'entremise de la gestionnaire d'incidents, **Vicki Vale**, et via des processus de signalement (reporting) formels.

Voici les points clés de cette collaboration selon les sources :

- **Rattachement hiérarchique** : L'équipe SOC dont Dan fait partie relève directement du **Responsable de la Sécurité des Systèmes d'Information (RSSI)**.
- **Rôle d'interface de la gestionnaire d'incidents** : Vicki Vale assure le pont entre la technique et la stratégie. Elle est chargée

de **communiquer l'état d'avancement des incidents aux dirigeants** et aux autres parties prenantes clés, leur permettant de prendre des décisions éclairées sans s'enliser dans les détails techniques.

- **Implication lors d'incidents majeurs** : Lorsqu'un incident est qualifié de « majeur » (comme la brèche de sécurité détectée par Dan et Sarah), le SOC ne contrôle plus seul la situation. La coordination s'effectue via le processus de gestion des incidents de l'entreprise, où les **responsables fonctionnels, voire la direction, peuvent piloter les opérations** selon la gravité de l'événement.
- **Reporting et analyse des tendances** :
 - Pour les **incidents majeurs**, l'équipe prépare des rapports variés, allant du résumé d'une page pour les décideurs à des analyses détaillées de plusieurs centaines de pages.
 - Les **incidents mineurs** sont compilés dans des rapports de gestion destinés à la direction pour présenter les tendances à court et à long terme.
- **Pression pour la clôture des dossiers** : Les sources mentionnent que la direction exerce souvent une **forte pression** pour clore les dossiers rapidement, bien que l'équipe technique doive parfois maintenir un dossier ouvert tant que le problème sous-jacent n'est pas résolu pour éviter toute récurrence.
- **Aide à l'amélioration continue** : Le reporting sert également à identifier des axes d'amélioration pour **rationaliser et optimiser les processus** de l'organisation, une information cruciale pour la direction dans sa gestion des risques opérationnels.

En somme, la direction intervient comme un superviseur stratégique et un soutien opérationnel lors des crises, tout en étant la destinataire finale des analyses qui orientent les investissements en sécurité.

Comment l'équipe de Dan prépare-t-elle les rapports pour la direction ?

L'équipe de Dan prépare les rapports pour la direction en suivant des processus de clôture rigoureux et en adaptant le format du document à la gravité de l'incident et au public visé.

Voici les principales étapes et caractéristiques de cette préparation selon les sources :

- **Consignation exhaustive des faits** : Avant la clôture d'un dossier, l'équipe s'assure que toutes les informations pertinentes recueillies (événements SIEM, captures d'écran, résultats d'analyses forensiques) sont intégralement consignées. Cela permet d'éviter que les détails ne s'estompent avec le temps.
- **Adaptation selon la gravité de l'incident** :
 - **Incidents majeurs** : Les rapports peuvent varier considérablement en longueur, allant d'un **résumé d'une page** destiné aux décideurs à une **analyse détaillée de plusieurs centaines de pages** pour un public technique ou d'audit.
 - **Incidents mineurs** : Bien que moins médiatisés, ils sont regroupés dans des **rapports de gestion et de direction complets** qui présentent les tendances à court et à long terme de l'organisation.
- **Contenu stratégique du rapport** : L'accent n'est pas mis uniquement sur ce qui s'est passé, mais sur l'**amélioration continue**. Le rapport doit identifier des axes d'amélioration pour rationaliser, optimiser ou repenser les processus du SOC afin d'éviter la récurrence des problèmes.
- **Formalisation et modèles** : Les communications internes et les rapports d'activité sont généralement **formalisés** et suivent des **modèles existants** au sein de l'entreprise pour garantir la cohérence des informations transmises.
- **Rôle de la gestionnaire d'incidents** : C'est Vicki Vale qui assure principalement la **communication de l'état d'avancement** et des conclusions aux dirigeants et autres parties prenantes clés. Elle utilise le système de gestion des cas (comme RTIR) pour coordonner ces signalements de bout en bout.
- **Gestion de la pression temporelle** : L'équipe doit parfois résister à une **forte pression de la direction** pour classer les dossiers rapidement. Elle doit s'assurer que le problème sous-jacent est

bien résolu avant de finaliser le rapport, car un incident peut être résolu alors que le dossier d'enquête reste ouvert pour une analyse rétrospective plus approfondie.

Quels sont les modèles de rapports utilisés par le SOC ?

Selon les sources, le SOC utilise une variété de modèles et de formats de rapports qui s'adaptent à la gravité de la situation, au type d'événement et au public visé.

Voici les principaux modèles de rapports utilisés :

- **Modèles pour événements récurrents** : Pour faciliter le travail des analystes et garantir que toutes les informations critiques sont saisies, le SOC utilise des modèles standardisés pour les cas fréquents, tels que les **signalements de phishing** et de **logiciels malveillants**.
- **Formats pour incidents majeurs** : La forme de ces rapports varie considérablement selon le destinataire :
 - **Résumé d'une page** : Destiné aux décideurs et à la direction pour une compréhension rapide des enjeux stratégiques.
 - **Analyse détaillée** : Un document pouvant atteindre **plusieurs centaines de pages** pour un public technique, des auditeurs ou des experts en criminalistique.
- **Rapports de gestion et de direction** : Les incidents mineurs sont compilés dans des rapports complets qui mettent en lumière les **tendances à court et à long terme** de la sécurité au sein de l'organisation.
- **Rapports automatisés et techniques** :
 - Le **SIEM** peut générer automatiquement des rapports d'incidents ou des tickets dans le système de gestion des cas.
 - Les **systèmes de gestion des cas** offrent la possibilité de produire des rapports sur des incidents individuels ou des analyses de tendances globales.
- **Rapports de conformité et d'éthique** : Certains outils permettent de générer des rapports spécifiques pour les incidents de

conformité ou pour le **signalement anonyme** de violations éthiques.

- **Modèles institutionnels** : De manière générale, les rapports d'activité et les communications internes sont formalisés et suivent les **modèles existants de l'entreprise** afin d'assurer une coordination fluide avec les autres services.

L'un des objectifs centraux de ces rapports, au-delà de la simple documentation, est de servir de base à l'**amélioration continue** en identifiant des pistes pour rationaliser ou repenser les processus du SOC.

Comment le SOC collabore-t-il avec le RSSI ?

Selon les sources, la collaboration entre le SOC et le **RSSI** (Responsable de la Sécurité des Systèmes d'Information) s'articule autour d'un lien hiérarchique direct, d'une communication stratégique en temps de crise et d'un processus de reporting continu pour l'amélioration de la sécurité.

Voici les principaux aspects de cette collaboration :

- **Rattachement hiérarchique** : Dans l'organisation type décrite, **l'équipe SOC relève directement du RSSI**. Bien que le SOC dispose d'une grande autonomie sur la configuration de ses propres systèmes, il reste sous la supervision stratégique de ce responsable.
- **Communication lors d'incidents majeurs** : En cas de crise, le rôle de l'**Incident Manager** (comme Vicki Vale) est crucial pour faire le pont avec la direction. Cette personne se concentre sur la **communication de l'état d'avancement aux dirigeants** et aux autres parties prenantes clés, permettant au RSSI d'avoir une vision claire de la situation sans s'impliquer dans les détails techniques de l'investigation.
- **Pilotage stratégique des opérations** : Pour les incidents les plus graves, le SOC ne contrôle plus seul la gestion de la crise. Les **responsables fonctionnels, voire la direction**, peuvent piloter les opérations selon la gravité de l'incident via le processus de gestion des incidents de l'entreprise.

- **Reporting et aide à la décision** : Le SOC prépare différents types de rapports pour le RSSI et la direction :
 - **Résumés d'une page** pour les décideurs lors d'incidents majeurs afin d'offrir une visibilité immédiate sur les risques.
 - **Rapports de gestion complets** présentant les tendances à court et à long terme, ce qui aide le RSSI à orienter la stratégie de sécurité globale.
- **Amélioration continue** : La collaboration vise également à identifier des **axes d'amélioration**. Les retours d'expérience après chaque incident permettent au RSSI de justifier des changements dans les processus ou de nouveaux investissements technologiques pour rationaliser ou repenser les méthodes du SOC.
- **Gestion des pressions opérationnelles** : Il existe parfois une tension entre les impératifs techniques et les attentes de la direction. Par exemple, une **forte pression** peut être exercée par la direction pour clore les dossiers rapidement, tandis que le SOC peut juger nécessaire de les maintenir ouverts pour résoudre des défauts sous-jacents. Dans ces situations, les analystes sont encouragés à discuter des enjeux politiques et opérationnels avec leur responsable.

Quels sont les défis politiques mentionnés lors de la collaboration ?

Selon les sources, la collaboration au sein d'une organisation lors d'un incident de sécurité soulève plusieurs **défis politiques et structurels** importants :

- **La pression pour la clôture des dossiers** : Une **pression généralement forte** de la part de la direction s'exerce souvent pour classer les dossiers rapidement. Or, il est parfois inapproprié de le faire tant que le défaut sous-jacent n'est pas résolu, car cela pourrait entraîner une récurrence de l'incident.
- **La résistance des propriétaires d'actifs** : Lors d'un incident majeur, les responsables des systèmes critiques (comme les systèmes bancaires) peuvent se montrer **extrêmement réticents**

à mettre leurs services hors ligne pour les réparer. Cela crée un conflit politique entre les impératifs de sécurité (confinement de la brèche) et les impératifs financiers liés à l'indisponibilité des services.

- **La perte de contrôle du SOC** : Lorsqu'une procédure d'intervention formelle est activée pour un incident majeur, **le SOC ne contrôle plus la gestion de l'incident**. La coordination bascule vers le processus de gestion des incidents de l'entreprise, où des **responsables fonctionnels ou la direction** peuvent piloter les opérations selon la gravité, ce qui modifie la dynamique d'autorité habituelle.
- **Les enjeux interservices** : La collaboration avec des services variés (Juridique, RH, Audit, etc.) fait intervenir des **enjeux politiques** spécifiques. Les sources recommandent d'ailleurs aux analystes de ne pas hésiter à discuter de ces tensions politiques avec leur responsable pour mieux les gérer.
- **La confidentialité des outils partagés** : L'utilisation d'un système de gestion des incidents commun à toute l'entreprise (DSI) pour des enquêtes de sécurité confidentielles peut poser problème. Des contrôles d'accès insuffisants ou des API trop ouvertes risquent de **compromettre la sécurité et la confidentialité** des investigations menées par le SOC.

Quels sont les enjeux de sécurité liés au système de tickets commun ?

L'utilisation d'un système de gestion des incidents d'entreprise (système de tickets commun) pour mener des investigations de sécurité présente des enjeux majeurs, principalement centrés sur la **confidentialité** et la **protection des données sensibles** liées aux enquêtes.

Voici les principaux risques de sécurité identifiés dans les sources :

- **Contrôles d'accès défaillants** : Bien que ces systèmes puissent techniquement prendre en charge des files d'attente fermées et des **contrôles d'accès basés sur les rôles**, ces fonctionnalités sont fréquemment **insuffisamment configurées ou non mises en place**. Cela peut permettre à des personnes non autorisées au

sein de l'organisation d'accéder à des détails confidentiels sur une intrusion en cours.

- **Exposition via le reporting et les API** : L'accès ouvert aux fonctions de **reporting** et aux **API du backend** du système de tickets peut malheureusement compromettre la sécurité des enquêtes en permettant l'extraction de données sensibles par des utilisateurs ou des processus tiers.
- **Interception des communications** : Pour garantir que les échanges entre analystes ne soient pas interceptés et lus par des tiers (ce qui est crucial lors d'une investigation), les systèmes doivent offrir une **authentification robuste** et des **fonctionnalités cryptographiques**. Un système de tickets d'entreprise standard peut ne pas répondre à ces exigences de sécurité élevées.

Pour pallier ces risques, il est souvent recommandé d'utiliser des outils de gestion de cas spécialisés et sécurisés, comme **RTIR**, ou de déployer des plateformes de collaboration web sécurisées spécifiquement dédiées au SOC.

Quel est le rôle du RSSI vis-à-vis du SOC ?

Selon les sources, le **RSSI** (Responsable de la Sécurité des Systèmes d'Information) occupe une position de supervision stratégique et hiérarchique par rapport au SOC.

Voici les détails de son rôle et de sa relation avec l'équipe :

- **Lien hiérarchique direct** : Dans l'organisation type présentée, **l'équipe SOC relève directement du RSSI**. Cela place le SOC au cœur de la stratégie de sécurité pilotée par ce responsable.
- **Supervision et autonomie** : Bien que le SOC dispose d'une **grande autonomie** sur la configuration et l'exécution de ses propres systèmes et contenus, il reste sous l'autorité du RSSI pour assurer la cohérence des missions de surveillance, d'investigation et de réponse aux incidents.
- **Arbitrage des enjeux politiques** : Le RSSI joue un rôle de soutien lors de situations complexes. Les sources recommandent aux analystes de ne pas hésiter à **discuter des enjeux politiques** (comme les tensions avec d'autres services ou la résistance des

propriétaires d'actifs) avec leur responsable (le RSSI ou son représentant direct) afin de débloquent des situations critiques.

- **Destinataire du reporting stratégique** : Le RSSI est l'un des principaux destinataires des analyses produites par le SOC. Il utilise les **rapports de gestion et de direction** (présentant les tendances à court et long terme) ainsi que les bilans d'incidents majeurs pour orienter la stratégie de défense de l'entreprise et identifier les axes d'amélioration continue.
- **Coordination transverse** : Le RSSI assure le lien avec les autres fonctions de sécurité qui ne sont pas forcément intégrées au SOC, comme la **gestion des vulnérabilités**, la conformité ou l'ingénierie de la sécurité.

En résumé, le RSSI agit comme le **pilote stratégique** qui définit le cadre de mission du SOC, le soutient face aux pressions internes de l'organisation et utilise ses résultats pour renforcer la posture de sécurité globale.

Quels sont les avantages de l'outil open source RTIR ?

Selon les sources, l'outil **RTIR** (Request Tracker for Incident Response) est une alternative open source performante pour la gestion des cas (enquêtes) au sein d'un SOC.

Ses principaux avantages incluent :

- **Coût avantageux** : En tant qu'outil **open source**, il représente une alternative crédible et performante aux solutions commerciales coûteuses, ce qui est particulièrement bénéfique pour les organisations où le budget est un facteur déterminant.
- **Spécialisation CSIRT** : Il a été spécifiquement développé pour la gestion des cas et est déjà adopté par de **nombreuses équipes CSIRT** à travers le monde.
- **Coordination de bout en bout** : Comme les autres systèmes de gestion de cas, il permet de coordonner la réponse, l'investigation et le signalement des incidents de sécurité de manière complète.
- **Collaboration sécurisée** : Il offre une **plateforme de collaboration web sécurisée** permettant à plusieurs analystes et

parties prenantes de travailler ensemble sur un même rapport d'incident.

- **Analyse des tendances** : L'outil permet non seulement de gérer les incidents individuels, mais aussi de fournir des **données de tendances** essentielles pour une analyse de sécurité à plus long terme.
- **Capacités d'intégration** : Bien qu'il puisse nécessiter une personnalisation pour l'intégration, RTIR peut être relié à d'autres briques technologiques comme les **SIEM**, les plateformes d'analyse forensique ou les systèmes de gestion d'incidents d'entreprise pour rationaliser les opérations.

En résumé, RTIR combine la puissance des outils de gestion professionnelle avec la flexibilité et l'accessibilité du modèle open source.

Comment le SOC collabore-t-il avec les équipes réseau ?

Selon les sources, la collaboration entre le SOC et les équipes réseau est essentielle car le personnel du SOC possède généralement une **connaissance limitée du réseau** et des flux de données qui y circulent. Cette collaboration se manifeste de plusieurs manières concrètes :

- **Expertise et visibilité** : Les administrateurs réseau apportent une compréhension approfondie de l'infrastructure que le SOC n'a pas forcément en interne. Ils aident à interpréter les flux de données et la télémétrie réseau pour identifier des comportements anormaux.
- **Accès à des outils spécialisés** : L'équipe réseau fournit au SOC des capacités techniques cruciales lors d'une enquête, telles que :
 - L'**analyse du trafic** en temps réel.
 - La **capture de paquets bruts** (données entrantes et sortantes), ce qui est parfois indispensable lorsque les outils propres au SOC ne permettent pas de le faire directement.
- **Gestion de la sécurité périmétrique** : Dans de nombreuses organisations, les administrateurs réseau gèrent des éléments clés de la sécurité, notamment les **pares-feux** (firewalls) et les

serveurs proxy. Le SOC doit donc collaborer avec eux pour obtenir les journaux de ces dispositifs ou pour faire appliquer des règles de filtrage.

- **Actions de confinement lors d'un incident :** Lorsqu'une machine est suspectée d'être compromise, le SOC travaille avec l'équipe réseau pour **isoler le trafic** associé à cette machine. Cela permet de bloquer l'attaquant tout en continuant de capturer des données brutes pour l'analyse forensique, sans pour autant éteindre le système.
- **Support lors d'incidents majeurs :** En cas de crise (comme une brèche de sécurité), les équipes réseau font partie des ressources d'astreinte mobilisées pour participer aux téléconférences de coordination et mettre en œuvre les mesures correctives décidées par le gestionnaire d'incidents.

En résumé, l'équipe réseau agit comme un **partenaire technique indispensable** qui fournit au SOC la "vue" et les "leviers" nécessaires sur l'infrastructure réseau pour mener à bien les investigations et le confinement des menaces.

Pourquoi privilégier l'adéquation au poste plutôt que la technique ?

Selon les sources, il est recommandé de privilégier **l'adéquation au poste** plutôt que les seules compétences techniques pour constituer une équipe de SOC performante pour plusieurs raisons fondamentales liées à la nature du travail en cybersécurité :

- **L'impossibilité de l'action individuelle :** Il est extrêmement difficile pour un analyste de réagir seul à un incident, même simple, en raison de nombreuses contraintes de temps et de ressources.
- **La nécessité d'une collaboration étroite :** Un analyste doit pouvoir collaborer efficacement avec une équipe élargie incluant d'autres membres du SOC, différents services de l'organisation et des partenaires externes. Une équipe performante repose avant tout sur des **individus compatibles** qui se soutiennent mutuellement et partagent des **valeurs communes**.

- **La gestion du stress et de la fatigue** : Les compétences techniques ne garantissent pas la capacité à gérer la pression intense d'un incident majeur. Une équipe soudée permet de mieux répartir la charge de travail et d'éviter que les experts techniques ne s'épuisent rapidement.
- **La pérennité de l'équipe (cohésion)** : Mobiliser toutes les meilleures ressources techniques dès le début d'une crise est une erreur fréquente qui nuit à la cohésion sur le long terme. Une bonne adéquation au poste permet au responsable de la gestion des incidents de déployer les ressources de manière **échelonnée**, préservant ainsi l'efficacité globale.
- **La communication avec les non-techniciens** : Une équipe trop axée sur la technique peut souffrir d'une mauvaise coordination ou d'une communication déficiente, particulièrement avec les parties prenantes moins techniques (dirigeants, autres services).

En résumé, si la technique s'apprend, les **qualités interpersonnelles**, la capacité à travailler en équipe sous pression et le partage de valeurs communes sont les véritables piliers de l'efficacité d'un SOC sur la durée.

Comment RTIR s'intègre-t-il aux SIEM ?

L'intégration de **RTIR** (Request Tracker for Incident Response) avec les systèmes **SIEM** s'inscrit dans une volonté globale de **rationaliser les investigations et les réponses** aux incidents de sécurité.

Voici comment cette intégration fonctionne et ce qu'elle permet, selon les sources :

- **Automatisation de la création de tickets** : Les SIEM peuvent être configurés pour effectuer des actions automatisées ou scriptées. Ainsi, lorsqu'un incident potentiel est détecté par le SIEM, il peut **générer automatiquement un ticket ou un rapport d'incident** directement dans le système de gestion des cas comme RTIR.
- **Coordination de bout en bout** : Une fois l'alerte du SIEM transférée dans RTIR, l'outil permet de coordonner l'enquête, la réponse et le signalement de l'incident de manière centralisée.

Cela permet aux analystes de disposer d'une plateforme de collaboration sécurisée pour travailler sur les données issues du SIEM.

- **Nécessité de personnalisation** : Bien que la plupart des SIEM prennent en charge l'intégration directe avec des systèmes de gestion d'incidents, les sources précisent que pour un outil open source comme RTIR, une **personnalisation spécifique** peut être nécessaire pour mettre en œuvre ces mécanismes d'intégration.
- **Enrichissement des investigations** : L'intégration permet de lier les événements bruts et les alertes du SIEM aux dossiers d'enquête (cas) dans RTIR. Par exemple, un analyste peut joindre des événements SIEM spécifiques à un rapport d'incident pour documenter ses conclusions initiales.

En résumé, l'intégration du SIEM vers RTIR transforme une alerte technique automatisée en un **processus d'enquête structuré**, bien que la mise en place technique puisse exiger des ajustements manuels par rapport aux solutions commerciales clés en main.

Quels sont les exemples concrets de sources d'enrichissement ?

Selon les sources, les données d'enrichissement permettent d'ajouter des informations supplémentaires aux éléments clés d'un événement pour aider l'analyste dans son travail.

Voici des exemples concrets de sources d'enrichissement cités dans les documents :

- **Données de réputation IP** : Ces sources, qu'elles soient gratuites ou commerciales, indiquent si une adresse IP capturée lors d'un événement est associée à une **activité malveillante connue** ou si elle provient d'une **zone géographique suspecte**.
- **Données internes sur les actifs** : Des informations propres à l'organisation peuvent être utilisées pour enrichir un événement, comme l'**emplacement physique** d'un actif particulier (ordinateur, serveur, etc.).
- **Résultats d'analyse des vulnérabilités** : Bien que non listés explicitement comme « source d'enrichissement » dans la section dédiée, le scénario montre que l'analyste Dan utilise les résultats

d'analyses de vulnérabilités intégrés au SIEM pour enrichir sa compréhension de l'état des systèmes ciblés.

De nombreux SIEM exploitent automatiquement ces sources de données d'enrichissement pour fournir un contexte immédiat à l'analyste SOC lors de la réception d'une alerte.

Quels sont les avantages des sources d'enrichissement internes ?

Selon les sources, les sources d'enrichissement internes offrent plusieurs avantages déterminants pour l'efficacité des analyses menées au sein d'un SOC :

- **Apport de contexte précis** : Elles permettent d'ajouter des **informations supplémentaires relatives aux éléments clés** d'un événement. Par exemple, l'intégration de données internes comme **l'emplacement physique d'un actif particulier** permet d'enrichir les alertes et de donner une dimension géographique concrète à une activité numérique.
- **Vérification de la légitimité des activités** : Le croisement avec des sources internes permet de confirmer ou d'infirmer des soupçons. Dans le scénario de Sarah, l'accès aux **données d'accès physique** (parking, badges d'entrée) a permis de confirmer que l'administrateur système était bien présent dans son bureau au moment des faits, ce qui aide à orienter l'enquête.
- **Évaluation de la vulnérabilité des cibles** : L'utilisation interne de **résultats d'analyse des vulnérabilités** intégrés au SIEM permet à l'analyste de constater immédiatement si les systèmes visés par une activité suspecte présentent des failles exploitables ou des niveaux de correctifs obsolètes.
- **Confirmation par les outils de support** : L'accès aux systèmes internes comme la **billetterie (ticketing)** permet de vérifier si une activité inhabituelle correspond à une demande d'assistance réelle formulée par un utilisateur, évitant ainsi de classer trop vite un incident comme un faux positif ou une attaque.
- **Vision multi-dimensionnelle de l'incident** : En extrayant des événements provenant d'endroits variés (journaux réseau, systèmes natifs, accès physiques), l'analyste peut **reconstituer**

l'étendue réelle d'un incident, ce qui serait impossible en se basant uniquement sur des alertes automatisées.

En résumé, ces sources internes transforment une alerte technique brute en un scénario compréhensible et vérifiable, facilitant la prise de décision rapide lors d'un incident.

Pourquoi l'humain reste la meilleure source de détection ?

Selon les sources, l'humain est considéré comme la meilleure source de détection au sein d'un SOC car les systèmes automatisés ne parviennent à identifier qu'une minorité d'incidents et manquent de la flexibilité nécessaire pour interpréter des contextes complexes.

Voici les raisons principales expliquant pourquoi l'humain reste indispensable :

- **Limites de l'automatisation** : Un rapport de l'Economist Intelligence Unit indique que **seul un tiers des incidents de sécurité mondiaux sont détectés par les SIEM** (systèmes de gestion des informations et des événements de sécurité). Les systèmes automatisés ne fonctionnent que de manière partielle et sont souvent limités à la recherche de scénarios spécifiques pour lesquels ils ont été configurés.
- **Signalements directs par les employés** : La grande majorité des incidents sont signalés par les employés eux-mêmes ou lors de contrôles de routine. Une définition inclusive d'un « événement » doit inclure les informations fournies par les utilisateurs finaux par téléphone ou courriel, par exemple lorsqu'ils rencontrent un problème inhabituel ou cliquent sur un lien suspect.
- **Capacité de vérification et de contextualisation** : Contrairement aux machines, les humains peuvent croiser des informations provenant de sources hétérogènes. Par exemple, l'analyste peut **appeler directement un utilisateur** pour vérifier la légitimité d'une action ou consulter les **données d'accès physique** (badges, parking) pour confirmer la présence d'une personne à son bureau.
- **Discernement entre incident et faux positif** : C'est l'analyste, et non le système, qui possède la compétence nécessaire pour

déterminer si un rapport d'incident constitue un **incident réel** ou un **faux positif** résultant d'une mauvaise configuration.

- **Détection des attaques inédites** : En se concentrant uniquement sur le SIEM, une organisation risque de détecter les incidents beaucoup trop tard ou de passer à côté d'attaques qui ne génèrent pas de journaux automatisés traditionnels.

En résumé, l'humain apporte une **vision multi-dimensionnelle** et une capacité d'enquête qui permettent de transformer des signaux faibles ou des comportements suspects en une réponse structurée,.

Pourquoi le SOC ne contrôle-t-il plus la gestion lors d'un incident majeur ?

Lorsqu'un incident est qualifié de **majeur**, le SOC ne contrôle plus seul la gestion de la situation car la coordination bascule vers le **processus global de gestion des incidents de l'entreprise**.

Voici les raisons précises de ce changement de gouvernance selon les sources :

- **Activation d'une procédure formelle** : Une fois qu'une procédure d'intervention formelle est déclenchée, la gestion dépasse le cadre strict de la sécurité informatique piloté par le SOC pour s'intégrer dans une structure de réponse à l'échelle de toute l'organisation.
- **Implication de la direction et des responsables fonctionnels** : En raison de la gravité de l'incident, ce sont les **responsables fonctionnels**, voire la **direction**, qui peuvent piloter les opérations. Les décisions à prendre (comme mettre hors ligne des systèmes critiques) ont des conséquences qui dépassent les compétences techniques et touchent à la stratégie d'entreprise.
- **Arbitrage des impacts financiers et opérationnels** : Dans le cas d'un incident majeur, les propriétaires d'actifs peuvent être très réticents à arrêter des systèmes bancaires ou critiques en raison des pertes financières importantes que cela engendrerait. Ces arbitrages entre sécurité et continuité d'activité doivent être tranchés par des instances supérieures au SOC.

- **Rôle des gestionnaires d'incidents d'entreprise** : Les responsables de la gestion des incidents de l'entreprise sont alors impliqués pour assurer la liaison entre les équipes techniques (Dan, Sarah) et les parties prenantes clés, garantissant une communication formalisée et cohérente via le système de gestion des tickets de la DSI.

En résumé, le SOC redevient un **contributeur technique essentiel** qui explique la situation et propose des mesures (comme le confinement), mais la **responsabilité décisionnelle et la gestion de crise** sont transférées aux instances de direction de l'organisation.

Quelles sont les limites du SIEM dans la détection des menaces ?

D'après les sources, bien que le SIEM soit un investissement technologique majeur pour les SOC, il présente plusieurs limites fondamentales dans la détection des menaces :

- **Une faible capacité de détection globale** : Un rapport de l'Economist Intelligence Unit souligne que **seul un tiers des incidents de sécurité mondiaux** sont détectés par les SIEM. La majorité des incidents sont signalés par des employés ou lors de contrôles de routine.
- **Une visibilité parcellaire** : Les alertes générées par les SIEM ne représentent qu'une **petite partie des événements pertinents** pour les incidents de sécurité. De nombreux systèmes ne fournissent pas de journaux au SIEM, ce qui crée des lacunes de visibilité. Par exemple, dans le scénario étudié, le SIEM ne collectait pas les journaux des postes utilisateurs.
- **Une focalisation sur le temps réel** : Les SIEM sont avant tout des systèmes d'analyse en temps réel axés sur les événements récents (allant de quelques jours à quelques mois). Ils analysent rarement des informations plus anciennes sans une réimportation complexe de données archivées.
- **Des contraintes techniques et de format** : Les SIEM peuvent être limités par :
 - **La compatibilité** : Ils n'acceptent parfois que des formats de journaux spécifiques provenant de fournisseurs ou de versions précises.

- **Le besoin de parseurs** : Chaque source nécessite un analyseur syntaxique pour interpréter les données.
- **La performance** : Ils sont conçus pour traiter un nombre moyen d'**événements par seconde (EPS)** au-delà duquel ils peuvent devenir instables ou surchargés.
- **Un filtrage restrictif (cas d'utilisation)** : La plupart des SIEM sont configurés pour rechercher des **cas d'utilisation spécifiques** et ignorent ou filtrent les données qui ne leur ont pas été signalées comme pertinentes. Cela évite la surcharge de l'analyste mais risque de masquer des signaux faibles.
- **Le risque de faux positifs** : Un SIEM peut être **configuré de manière incorrecte**, déclenchant ainsi des alertes inappropriées qui nuisent à l'efficacité de l'équipe.
- **Une détection potentiellement tardive** : Se concentrer uniquement sur le SIEM fait courir le risque de détecter les incidents **beaucoup trop tard**. Les humains restent souvent plus rapides pour identifier des anomalies comportementales ou contextuelles que les systèmes automatisés.

Comment isoler le trafic réseau d'une machine compromise ?

L'isolation du trafic réseau d'une machine compromise est une mesure de confinement critique qui repose sur une coordination étroite entre les analystes du SOC et les administrateurs réseau de l'organisation.

Voici la procédure et les principes clés pour réaliser cette isolation selon les sources :

- **Collaboration avec l'équipe réseau** : Comme le SOC possède souvent une connaissance limitée du réseau, l'analyste doit contacter les **administrateurs réseau**. Ces derniers ont accès aux outils d'analyse du trafic et de télémétrie nécessaires pour agir sur l'infrastructure (comme les pare-feux).
- **Isolation logique plutôt que déconnexion physique** : Au lieu de simplement éteindre l'ordinateur ou de débrancher le câble, l'équipe réseau travaille pour **isoler le trafic réseau associé à la machine spécifique**. Cela permet de neutraliser la capacité de

l'attaquant à communiquer tout en gardant le système "vivant" pour l'observation.

- **Capture des données brutes** : Simultanément à l'isolation, l'objectif est de **capturer un maximum de données brutes entrantes et sortantes** de la machine compromise. Ces paquets bruts sont essentiels pour comprendre les actions de l'attaquant et identifier d'éventuelles exfiltrations de données.
- **Préservation de la mémoire vive (RAM)** : Il est crucial de ne pas éteindre complètement la machine, car cela effacerait les preuves volatiles présentes en mémoire. Une fois la capture réseau effectuée, la machine peut être mise en **hibernation** avant d'être remise physiquement au SOC. L'hibernation permet de sauvegarder l'état de la mémoire sur le disque, facilitant une analyse forensique ultérieure approfondie.

Cette approche permet de **contenir la brèche de sécurité** tout en collectant les preuves techniques indispensables pour déterminer l'étendue réelle de la compromission.

Comment l'hibernation aide-t-elle l'analyse forensique ?

L'**hibernation** joue un rôle crucial dans l'analyse forensique car elle permet de **préserver l'état de la mémoire vive (RAM)** d'un système compromis, ce qui est impossible avec un arrêt complet.

Voici comment elle facilite spécifiquement le travail des enquêteurs :

- **Préservation des données volatiles** : Contrairement à un arrêt traditionnel qui efface le contenu de la mémoire vive, l'hibernation sauvegarde l'image de la RAM sur le disque dur. Ces données sont "volatiles" et contiennent des preuves critiques qui seraient autrement définitivement perdues.
- **Analyse approfondie de la mémoire** : Une fois l'image de la mémoire sauvegardée via l'hibernation, les experts en criminalistique numérique peuvent mener une **analyse plus poussée** pour identifier des processus malveillants, des connexions réseau actives ou des fragments de code qui ne laissent aucune trace sur le disque dur.

- **Maintien de la chaîne de preuves** : Dans le scénario étudié, l'analyste Dan a spécifiquement demandé à l'utilisateur (Robert) de mettre son ordinateur en hibernation avant de le remettre physiquement au SOC. Cela garantit que l'état exact de la machine au moment de la détection de l'incident est "gelé" pour l'investigation.

En résumé, l'hibernation constitue un compromis idéal : elle interrompt l'activité de l'attaquant sur la machine tout en capturant l'ensemble des preuves numériques présentes en mémoire vive pour une analyse rétrospective détaillée.

Comment Dan a-t-il confirmé la présence de Robert au bureau ?

Dans le scénario présenté dans les sources, ce n'est pas Dan, mais sa collègue **Sarah Connor** (analyste de niveau 2) qui a initialement confirmé la présence physique de Robert au bureau.

Voici comment cette vérification a été effectuée et comment Dan en a été informé :

- **Appel au bureau de sécurité** : Sarah a contacté le bureau de sécurité de l'entreprise pour vérifier les données d'accès physique.
- **Données de parking et d'accès** : Le bureau de sécurité a confirmé que Robert était arrivé au **parking du bâtiment à 20h12** et qu'il se trouvait dans son **bureau à 20h25**.
- **Transmission à Dan** : Dan a pris connaissance de cette confirmation en examinant le **rapport d'incident** que Sarah lui a transmis lors de l'escalade du dossier au niveau 3. Ce rapport incluait une synthèse des vérifications faites par Sarah, notamment les journaux du SIEM et les données d'accès physique obtenues auprès de l'équipe de sécurité.

Cette démarche a permis à l'équipe de confirmer que Robert n'agissait pas à distance (via un VPN par exemple), mais qu'il s'agissait bien d'une connexion locale effectuée alors qu'il était présent sur site pour une fenêtre de maintenance planifiée.

Comment Sarah a-t-elle identifié l'e-mail de phishing suspect ?

Sarah Connor a identifié l'e-mail de phishing suspect en combinant l'analyse technique et les informations obtenues directement auprès de l'utilisateur concerné, Robert.

Voici les étapes clés de cette identification selon les sources :

- **L'alerte initiale** : Sarah a d'abord été alertée par le SIEM d'une activité inhabituelle sur le compte de Robert, qui tentait de se connecter à plusieurs systèmes critiques qu'il n'administrerait pas habituellement.
- **L'appel direct à l'utilisateur** : En appelant Robert, elle a appris que celui-ci avait reçu un e-mail lui demandant de **mettre à jour son profil RH**. Robert a expliqué qu'il avait tenté de se connecter au lien fourni, sans succès, et qu'il avait même créé un ticket d'assistance à ce sujet.
- **L'examen de la copie de l'e-mail** : Sarah a demandé à Robert de lui transmettre une copie de l'e-mail pour l'analyser. Elle a alors relevé deux anomalies majeures qui rendaient le message suspect :
 - **Lien externe incohérent** : Bien que l'e-mail ressemble à un message interne de l'entreprise, le lien vers le « système RH » pointait vers une **adresse sur Internet** plutôt que vers une adresse réseau interne.
 - **Technique de Spear Phishing** : L'analyse ultérieure avec Dan a confirmé que l'e-mail était probablement une attaque de **spear phishing** ciblée.
- **Vérification croisée** : Elle a également confirmé la légitimité du récit de Robert en vérifiant l'existence réelle du **ticket de service** dans le système de billetterie de l'entreprise.

Cette approche a permis à Sarah de confirmer que l'incident n'était pas un faux positif et qu'une compromission réelle était en cours, ce qui l'a menée à créer un rapport d'incident formel.

Quelles sont les preuves trouvées sur la copie de l'e-mail ?

L'examen de la copie de l'e-mail par Sarah Connor, puis par Dan Kaminsky, a révélé plusieurs preuves indiquant qu'il s'agissait d'une tentative de **phishing** (hameçonnage) ciblée :

- **Une apparence trompeuse** : L'e-mail avait l'apparence d'un **message interne** légitime de l'entreprise.
- **Une URL externe suspecte** : Le lien contenu dans l'e-mail, censé diriger l'utilisateur vers le « système RH » pour une mise à jour de profil, pointait en réalité vers une **adresse sur Internet** (URL externe) plutôt que vers une adresse réseau interne à l'organisation.
- **Un prétexte classique** : Le contenu du message demandait à l'utilisateur de mettre à jour son **profil RH**, une technique courante pour inciter la victime à cliquer sur un lien malveillant.
- **Une attaque ciblée (Spear Phishing)** : L'analyse a conclu qu'il s'agissait probablement d'une attaque de **spear phishing** dirigée spécifiquement contre Robert et potentiellement d'autres administrateurs système.
- **Une diffusion large auprès des administrateurs** : L'enquête ultérieure sur les journaux de messagerie a confirmé que des e-mails similaires avaient été envoyés à **tous les administrateurs système** de l'environnement au cours des dernières 24 heures.

Ces éléments ont permis à l'équipe du SOC de confirmer que l'incident n'était pas un faux positif et qu'une compromission réelle était en cours.

Comment Robert a-t-il pu accéder à des systèmes critiques ?

Selon les sources, Robert n'a pas accédé intentionnellement à ces systèmes critiques ; c'est un **attaquant** qui a utilisé son compte et sa machine après une compromission réussie par **phishing**.

Voici le mécanisme qui a permis cet accès :

- **Le point d'entrée (Phishing)** : Robert a reçu un courriel de type « spear phishing » l'invitant à mettre à jour son profil RH sur un site Web. Ce site, bien que d'apparence interne, était une **URL externe** conçue pour capturer ses informations ou infecter son poste.
- **Infection par un cheval de Troie** : L'analyse technique a révélé que l'ordinateur de Robert a été infecté par une variante jusqu'alors inconnue d'un **cheval de Troie**. Ce logiciel malveillant

permettait un **accès à distance** à sa machine via des serveurs de commande et de contrôle (C2).

- **Utilisation de privilèges légitimes** : En tant qu'administrateur système, le compte de Robert possédait des **privilèges élevés**. L'attaquant a pu utiliser ces droits pour tenter de se connecter à divers systèmes de l'entreprise.
- **Exploitation de vulnérabilités** : L'enquête menée par Dan a démontré qu'au moins la moitié des systèmes critiques visés présentaient des **failles hautement exploitables** et des **niveaux de correctifs obsolètes**. Ces vulnérabilités ont permis à l'attaquant de compromettre réellement plusieurs serveurs critiques en utilisant les accès de Robert.

En résumé, l'accès a été rendu possible par la combinaison d'une **erreur humaine** (clic sur un lien de phishing), de l'**infection du poste de travail** et de l'**exploitation de failles de sécurité** sur des serveurs qui n'étaient pas à jour.

Comment a-t-on découvert que Robert était victime de spear phishing ?

La découverte que Robert était victime d'une attaque de **spear phishing** (hameçonnage ciblé) s'est faite en plusieurs étapes, mêlant alertes automatisées, communication directe et analyse technique approfondie :

- **L'alerte initiale du SIEM** : Tout commence par une alerte automatisée du SIEM signalant une activité inhabituelle : le compte de Robert, administrateur système, tentait de se connecter à plusieurs systèmes critiques qu'il n'administrait pas habituellement.
- **L'échange direct avec l'utilisateur** : L'analyste Sarah Connor appelle Robert pour vérifier cette activité. Robert nie avoir accédé à ces systèmes, mais mentionne avoir reçu un e-mail lui demandant de **mettre à jour son profil RH**.
- **L'analyse de la copie de l'e-mail** : Robert transmet une copie de l'e-mail à Sarah. L'examen révèle que si le message ressemble à une communication interne, le lien vers le « système RH » pointe

en réalité vers une **URL externe sur Internet** plutôt que vers une adresse interne.

- **La confirmation du caractère ciblé (Spear Phishing) :** En examinant le rapport d'incident, l'analyste de niveau 3 Dan Kaminsky conclut rapidement qu'il s'agit d'une attaque de **spear phishing**. Cette conclusion est renforcée par deux faits :
 - La cible est un profil à hauts privilèges (administrateur système).
 - Une enquête ultérieure dans les journaux de messagerie confirme que des e-mails similaires ont été envoyés à **tous les administrateurs système** de l'organisation au cours des dernières 24 heures.
- **La preuve de l'infection :** L'analyse de l'ordinateur de Robert par des prestataires spécialisés confirme ensuite la présence d'une variante inconnue d'un **cheval de Troie** permettant un accès à distance via des serveurs de commande et de contrôle, expliquant comment l'attaquant a pu agir après le clic sur le lien de phishing.

Quelles mesures ont été prises pour réduire les risques ?

Pour réduire les risques suite à la détection de l'incident, plusieurs mesures tactiques et stratégiques ont été déployées, allant du confinement immédiat à la remédiation technique approfondie :

Mesures de confinement et d'urgence

- **Désactivation des accès :** Le compte administrateur de Robert a été immédiatement **désactivé** pour empêcher l'attaquant de s'en servir pour compromettre d'autres systèmes.
- **Isolation réseau :** Plutôt que d'éteindre simplement l'ordinateur, le SOC a collaboré avec l'équipe réseau pour **isoler le trafic** de la machine compromise tout en capturant les données brutes pour l'analyse.
- **Préservation des preuves :** Robert a reçu l'instruction de mettre son ordinateur en **hibernation** afin de sauvegarder l'état de la mémoire vive (RAM) pour une analyse forensique ultérieure, évitant ainsi la perte de données volatiles.

- **Restauration des systèmes** : Profitant de la virtualisation des actifs, l'organisation a avancé une fenêtre de maintenance pour **restaurer les serveurs affectés** à partir de sauvegardes saines, après en avoir conservé des copies pour investigation.

Mesures techniques et investigations

- **Analyse des vulnérabilités** : Dan a lancé de nouvelles séries d'analyses sur l'ordinateur de Robert et les ressources critiques pour identifier les **failles exploitables** et les retards de correctifs.
- **Mise à jour de la protection** : Suite à l'envoi d'échantillons de code malveillant au fournisseur de l'antivirus, une **mise à jour spécifique** a été déployée pour détecter cette nouvelle variante de cheval de Troie sur l'ensemble du parc informatique.
- **Recherche d'indicateurs de compromission (IOC)** : Le SOC a utilisé des flux de renseignements externes et des échanges avec des pairs du secteur pour identifier d'autres adresses IP et e-mails suspects associés à l'attaque.

Mesures organisationnelles et de remédiation

- **Gestion de crise** : Un **incident majeur** a été déclaré, permettant de mobiliser les ressources d'astreinte de plusieurs services (réseau, serveurs, direction) via une téléconférence de coordination.
- **Recours à l'expertise externe** : Des prestataires spécialisés ont été engagés pour l'**analyse forensique avancée** et l'étude du logiciel malveillant, complétant les capacités internes du SOC.
- **Correction des failles** : Des modifications ont été mises en œuvre pour **corriger les vulnérabilités** qui avaient permis l'exfiltration initiale des données.
- **Amélioration continue** : Le processus prévoit qu'après la clôture, un rapport identifie les **axes d'amélioration** pour optimiser ou repenser les processus du SOC afin d'éviter la récurrence de tels incidents.

Quels étaient les indicateurs de compromission identifiés ?

Dans le cadre du scénario de l'incident chez Wereabank, plusieurs **indicateurs de compromission (IOC)** techniques et comportementaux ont été identifiés par l'équipe du SOC et ses partenaires :

- **Alertes comportementales (SIEM) :** Le premier indicateur a été une alerte signalant qu'un compte administrateur (Robert) tentait de se connecter à plusieurs **systèmes critiques** qu'il n'avait jamais consultés auparavant.
- **Caractéristiques de l'e-mail de phishing :**
 - L'e-mail utilisait un prétexte interne (mise à jour du profil RH) pour tromper l'utilisateur.
 - Il contenait un lien malveillant pointant vers une **URL externe sur Internet** plutôt que vers une adresse réseau interne légitime.
 - Des **adresses e-mail d'expédition** spécifiques associées à cette campagne d'attaque ont été identifiées et partagées par des pairs du secteur.
- **Traces du logiciel malveillant (Malware) :**
 - L'analyse a révélé la présence d'une **variante inconnue d'un cheval de Troie** sur l'ordinateur de Robert.
 - Ce code malveillant communiquait avec un ensemble de **serveurs de commande et de contrôle (C2)** fonctionnant selon un système de rotation pour éviter la détection.
- **Indicateurs réseau et externes :**
 - Des **adresses IP suspectes** liées à des attaques similaires sur d'autres institutions financières de la région ont été fournies par des fournisseurs de renseignements et des collègues d'autres banques.
 - Le fournisseur de renseignements sur les menaces a suggéré d'autres IOC spécifiques à surveiller suite à l'analyse de la campagne en cours.
- **Exploitation de vulnérabilités :**
 - La présence de **correctifs obsolètes** et de failles hautement exploitables sur les serveurs ciblés a été confirmée, expliquant comment l'attaquant a pu progresser après l'infection initiale.

L'identification de ces indicateurs a permis de lancer une recherche active (Hunting) sur l'ensemble du parc informatique, menant à la découverte de deux serveurs supplémentaires compromis.

Quels systèmes n'étaient pas surveillés par le SIEM ?

Selon les sources, plusieurs systèmes et types de données ne sont pas surveillés ou intégrés directement dans le SIEM, que ce soit par choix de configuration ou par limitation technique :

- **Les postes utilisateurs** : Dans le scénario de Wereabank, il est explicitement mentionné que le SIEM ne collecte généralement pas les journaux provenant des **postes de travail des utilisateurs**.
- **Les journaux de messagerie (Email)** : Bien que cruciaux pour détecter les attaques de phishing, les journaux de courrier électronique ne sont pas intégrés au SIEM dans l'exemple étudié, nécessitant une investigation manuelle séparée de la part de l'analyste.
- **Les plateformes de communication et de collaboration** : Les événements provenant des **appels téléphoniques**, de la **messagerie instantanée** ou des **échanges directs par courriel** ne sont pas automatisés dans le SIEM et dépendent de signalements humains.
- **Les services fournis par des tiers** : Les données de certains services externes ne sont souvent accessibles que via des portails spécifiques et ne sont pas intégrées au SIEM. Cela inclut :
 - Les protections contre les **attaques par déni de service (DoS)** fournies par les FAI ou les fournisseurs de cloud.
 - Les services de **protection de la marque**.
 - Les plateformes de communication externes comme **Twitter**.
- **Les systèmes aux contraintes spécifiques** : Certains systèmes ne partagent pas leurs données avec le SIEM pour des raisons de **confidentialité** ou pour éviter des **impacts négatifs sur leurs performances**.

- **Les données filtrées** : Même pour les sources compatibles, le SIEM est souvent configuré pour **ignorer ou filtrer** les données qui ne correspondent pas à des "cas d'utilisation" spécifiques afin d'éviter la surcharge du système ou des analystes.

De manière générale, les sources soulignent que les alertes du SIEM ne représentent qu'une **petite partie** des événements pertinents pour la sécurité, et que de nombreux systèmes restent en dehors de son périmètre de surveillance directe.

Comment le SOC a-t-il restauré les systèmes virtualisés ?

Selon les sources, la restauration des systèmes virtualisés lors de l'incident a été facilitée par plusieurs facteurs et décisions stratégiques :

- **Restauration à partir de sauvegardes** : Après avoir envisagé plusieurs options, l'équipe a choisi de procéder à une **restauration à partir de sauvegardes** saines.
- **Ajustement du calendrier** : Pour limiter les interruptions de service, les responsables ont accepté d'**avancer la fenêtre de maintenance** qui était initialement planifiée, permettant ainsi une intervention immédiate sur les systèmes affectés.
- **Agilité technique** : Le fait que les systèmes soient virtualisés a permis aux équipes d'**agir rapidement** pour remettre les services en ligne.
- **Conservation des preuves** : Un avantage majeur de la virtualisation a été la capacité de **sauvegarder des copies complètes des systèmes compromis** avant leur restauration. Cela a permis au SOC de disposer de preuves intactes pour mener une analyse forensique approfondie tout en rétablissant la continuité d'activité.

Une fois cette restauration rapide effectuée, le SOC a pu poursuivre ses activités d'investigation et de remédiation à plus long terme sur les copies sauvegardées.

Comment Wereabank a-t-elle géré la fenêtre de maintenance ?

Dans le cadre de l'incident de sécurité survenu chez Wereabank, la gestion de la fenêtre de maintenance a évolué selon l'urgence de la situation :

- **Planification initiale** : L'administrateur système, Robert, était initialement revenu au bureau pour effectuer une modification approuvée durant la fenêtre de maintenance normale, prévue pour **minuit**.
- **Arbitrage lors de la crise** : Face à la détection de systèmes critiques compromis, les propriétaires des actifs étaient d'abord très réticents à mettre les services hors ligne pour réparation, en raison des conséquences financières importantes liées à l'indisponibilité des systèmes bancaires.
- **Avancement de la fenêtre** : Après discussion entre les parties prenantes, il a été décidé d'**avancer la fenêtre de maintenance planifiée**. Cette décision a permis d'intervenir plus tôt que prévu pour restaurer les systèmes affectés sans attendre l'heure initialement fixée.
- **Facilitation par la virtualisation** : La gestion de cette fenêtre a été facilitée par le fait que tous les systèmes touchés étaient **virtualisés**. Cela a permis aux équipes :
 - D'agir **rapidement** pour la restauration.
 - De **sauvegarder des copies** des systèmes compromis avant leur remise à zéro, garantissant ainsi la conservation des preuves pour une analyse approfondie ultérieure.

Cette approche a permis de concilier les impératifs de sécurité (confinement et restauration) avec les contraintes de disponibilité de l'entreprise.

Comment former le personnel du SOC à la technique ?

Bien que les sources privilégient **l'adéquation au poste** (compatibilité, valeurs communes) plutôt que les seules compétences techniques lors du recrutement, elles soulignent plusieurs leviers pour développer et structurer le savoir-faire technique du personnel au sein du SOC.

Voici comment, selon les documents, le personnel monte en compétence et se perfectionne techniquement :

- **L'apprentissage par l'expérience** : C'est une méthode fondamentale citée pour progresser au-delà de la formation initiale. Chaque incident traité est une occasion d'identifier des **pistes d'amélioration** permettant de rationaliser ou de repenser les processus techniques.
- **L'utilisation d'une base de connaissances et de guides pratiques (Playbooks)** : Le SOC s'appuie sur une **base de connaissances** commune et des **guides pratiques** (comme celui utilisé par Dan pour la mobilisation). Ces outils fournissent des méthodes reproductibles et des modèles qui garantissent la cohérence des enquêtes techniques et servent de référence aux analystes.
- **La collaboration avec des experts externes** : Pour les domaines très pointus comme l'**analyse forensique avancée** ou l'**analyse de logiciels malveillants**, le SOC fait appel à des prestataires spécialisés. Travailler avec ces tiers permet aux équipes internes de gérer des situations exceptionnelles tout en bénéficiant d'une expertise qu'il serait difficile de maintenir totalement en interne.
- **L'encadrement par des analystes expérimentés** : Le fonctionnement en niveaux (Level 1, 2, 3) favorise le transfert de connaissances. Par exemple, les analystes les plus expérimentés (niveau 2 ou 3) traitent les événements complexes et les signalements humains, tandis que les procédures documentées guident le travail des échelons inférieurs.
- **L'évaluation et l'amélioration continue** : Le SOC doit régulièrement évaluer ses programmes et identifier les domaines récurrents où des améliorations techniques seraient les plus bénéfiques, notamment pour réduire les taux de faux positifs et de faux négatifs.

En résumé, la formation technique dans un SOC tel que décrit dans les sources repose moins sur des cours théoriques que sur une **immersion pratique encadrée par des procédures strictes**, une collaboration avec des experts et une analyse rétrospective systématique des incidents passés.

Quelles vulnérabilités Dan a-t-il découvertes sur les serveurs ?

En examinant les résultats des analyses qu'il a lancées, Dan Kaminsky a découvert plusieurs vulnérabilités critiques sur les serveurs de Wereabank :

- **Faibles hautement exploitables** : Au moins la moitié des systèmes critiques auxquels le compte de Robert s'était connecté présentaient des failles majeures. Ces failles étaient d'autant plus dangereuses qu'elles étaient accessibles avec des **privileges d'administrateur** comme ceux détenus par Robert.
- **Niveaux de correctifs obsolètes** : Dan a d'abord remarqué dans le SIEM que certains systèmes n'avaient pas été analysés depuis longtemps et que d'autres présentaient des **retards de mise à jour** (correctifs obsolètes).
- **Vulnérabilités résiduelles sur les systèmes à jour** : Même les serveurs ayant bénéficié de correctifs récents comportaient encore des **vulnérabilités exploitables**, bien que celles-ci nécessitent un niveau de compétence technique plus élevé de la part de l'attaquant pour être utilisées.

Ces découvertes ont été déterminantes pour confirmer que l'incident était bien réel et ont conduit Dan à recommander la déclaration d'un **incident majeur** afin de mobiliser les ressources nécessaires au confinement de la brèche