Faire face à la complexité

Comment gérer les cyberincidents complexes

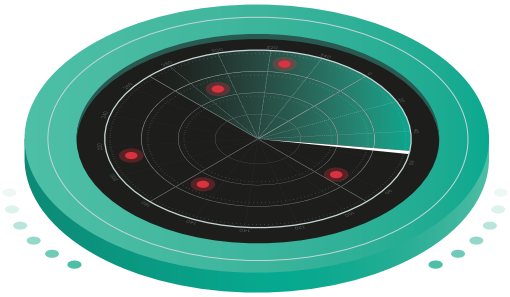
kaspersky BRING ON THE FUTURE

S'il n'est pas toujours possible de stopper une attaque avant qu'elle ne pénètre votre périmètre de sécurité, il est cependant possible de limiter ou d'exclure les dommages qui en résultent et d'éviter sa propagation. Lorsqu'il s'agit d'attaques ciblées complexes, la rapidité de la réponse est essentielle.

Cependant, les incidents complexes présentent des défis très particuliers, car ils impliquent généralement de nombreux aspects du système de l'organisation attaquée. Comment savoir où commencer quand tout semble important ?

Dans ce document, nous nous penchons sur les cinq principaux obstacles à la résolution efficace des incidents complexes. Définissons tout d'abord le concept de complexité et ce qu'il implique pour les professionnels de la cybersécurité.

C'est quoi, exactement, un incident complexe ?



Un incident complexe peut être plus clairement défini en opposition à un incident simple. Par exemple, la pandémie de Covid-19 est l'incarnation d'un incident complexe car elle implique de multiples systèmes : pays, organisations (gouvernementales et professionnelles), communautés, écoles, secteurs, familles et individus. Sans parler du fait que le virus agit comme un incident complexe pour la santé des individus qui tombent malades. Les effets du Covid-19 vont au-delà du système respiratoire pour atteindre les fonctions cardiovasculaires, rénales, dermatologiques, neurologiques, immunitaires, voire psychiatriques.

Cyberespace complexe, panorama des cybermenaces complexes, cyberincidents complexes. Une évolution normale ?

La complexité accrue des cyberincidents est directement liée à celle des systèmes informatiques des entreprise et, par conséquent, au cyberespace lui-même. Selon le rapport Panorama des cybermenaces et tendances émergentes de janvier 2019 à avril 2020 de l'ENISA (European Union Agency for Cybersecurity, Agence de l'Union européenne pour la cybersécurité), « le caractère interconnecté des différents systèmes et réseaux permet aux cyberincidents de se propager rapidement et largement, compliquant l'évaluation et l'atténuation des cyberrisques ». En d'autres termes, plus l'infrastructure informatique d'une entreprise est complexe, plus elle s'expose à des cyberattaques complexes, augmentant le risque d'incidents complexes pour les grandes organisations ou entreprises complexes par nature.

La corrélation naturelle entre environnements et incidents complexes s'étend au-delà du système professionnel complexe spécifique. Le cyberespace lui-même est défini par la norme ISO/IEC 27032:2012 comme un « environnement complexe résultant de l'interaction des gens, des logiciels et des services sur Internet au moyen d'appareils technologiques et de réseaux qui y sont connectés et n'existant sous aucune forme physique ». Nous faisons donc face à trois niveaux de complexité : le cyberespace, l'environnement informatique de l'entreprise et les cyberincidents. Ce panorama se complique lorsque les trois niveaux sont interconnectés et

interdépendants, chacun gagnant en complexité pour atteindre ses propres objectifs :

Le cyberespace : confiance accrue dans les appareils interconnectés, les systèmes et les processus pour l'activité professionnelle comme pour les loisirs, menant à un environnement plus complexe

L'environnement informatique de l'entreprise : expérimentation d'une surface d'attaque qui s'élargit en raison de la multiplication des appareils interconnectés, systèmes et processus (y compris la chaîne d'approvisionnement) et brusque hausse simultanée de la complexité des cyberincidents qui y surviennent et des configurations de cybersécurité nécessaires pour s'en protéger

Le panorama des cybermenaces et ses acteurs : d'un côté, en réponse à la complexité accrue à la fois au niveau du cyberespace et de l'environnement des entreprises, et de l'autre, exploitation spécifique de cette complexité pour lancer des attaques avancées hautement sophistiquées (impliquant un mouvement latéral impossible avec des systèmes cibles plus simples)

La vérité, c'est que ce sont les cybercriminels qui ont trouvé le plus rapidement les moyens de réduire la barrière de la complexité en ayant recours, entre autres, aux programmes malveillants :

> « Aujourd'hui, les barrières auxquelles se heurtent les cybercriminels aspirants tombent puisqu'ils disposent d'une foule de capacités (techniques) et de ressources substantielles depuis que les programmes malveillants et les programmes malveillants en tant que services sont disponibles plus facilement et à moindre coût par le biais de divers moyens et sources (comme le Dark Web et le Deep Web). En conséquence, une variété de techniques et d'outils sophistiqués (comme les techniques d'ingénierie sociale et les programmes d'exploits zero-day) sont disponibles et peuvent être utilisés par les cybercriminels pour lancer des attaques ciblées avancées. »
>
> Papastergiou, S., Mouratidis, H. & Kalogeraki, EM. **Gestion des menaces persistantes avancées et des incidents complexes dans les infrastructures TIC de santé, de transport et d'énergie.**Systèmes en évolution (2020).

La bonne nouvelle, c'est qu'il existe des moyens permettant aux entreprises de réduire considérablement, efficacement et une bonne fois pour toutes la barrière de la complexité. Ce sont ces moyens que nous allons évoquer dans ce document. Avant toute chose, penchons-nous sur les cinq principaux obstacles à la résolution efficace des incidents complexes.

Les cinq principaux obstacles à la résolution des incidents complexes

Il est possible de stopper la progression des menaces complexes et de limiter les dommages qu'elles provoquent, même une fois qu'elles ont franchi le périmètre de l'entreprise. Pour commencer, rappelons que la majorité des tactiques 'Initial Access' de MITRE ATT&CK sont encore relativement traditionnelles.

Que le phishing ciblé soit toujours une tactique 'Initial Access' fondamentale, même pour les APT, dans le contexte du chaos créé par la pandémie, doit nous faire réfléchir. Premièrement, nous devrions considérer le nombre d'attaques susceptibles d'être évitées en automatisant les tâches de cybersécurité routinières qui bloquent l'accès initial. Cela dit, ce n'est pas la pénétration des attaques (avec des exceptions comme les exploits zero-day) qui rend un incident *complexe*.

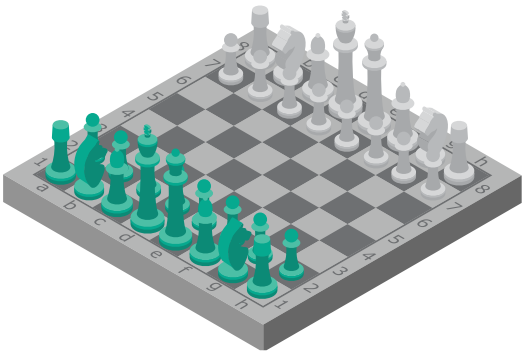
La complexité commence par des tactiques telles que le mouvement latéral, l'établissement de portes dérobées, différents modes de transmission de charge utile et la discrétion. Mais qu'est-ce qui empêche les équipes de sécurité informatique d'éviter qu'un incident ne devienne complexe ? Et une fois que l'incident est catégorisé, pourquoi est-il souvent très difficile de l'atténuer et de le résoudre efficacement ?

Obstacle n° 1 : La complexité inhérente aux systèmes de cybersécurité

Pour un non-initié, la configuration d'une cybersécurité d'entreprise moyenne est aussi déconcertante que le cockpit d'un avion de chasse furtif. Non qu'il existe des entreprises moyennes ou des configurations de cybersécurité moyennes, mais plutôt de multiples outils pour exécuter des tâches de sécurité spécifiques hautement spécialisées, un éventail de consoles de contrôle et un nombre incalculable d'alertes. C'est la résultante directe d'une complexité accrue de l'infrastructure de sécurité informatique pour faire face à la complexité du panorama des cybermenaces.

Il est donc ironique et terrible que la complexité de la configuration de la cybersécurité devienne trop souvent un réel obstacle à la résolution efficace des incidents très complexes. Cette complexité a plusieurs impacts :

- Les équipes sont submergées d'outils et consacrent un temps précieux à jouer les « interprètes » entre des solutions distinctes. Les piles technologiques de cybersécurité (et les piles technologiques en général) deviennent souvent des tours de Babel virtuelles, avec un fonctionnement freiné par les différents « langages » parlés par les différents outils.
- Si les données issues du cyberincident sont collectées dans de petits échantillons provenant de différents capteurs de données non intégrés sur les points de pénétration potentiels, les équipes n'ont généralement pas accès à une vue d'ensemble et ne peuvent prendre conscience qu'un incident complexe est en cours avant que n'apparaissent des signes tangibles de pénétration. En d'autres termes, l'incident n'est pas pleinement compris, ce qui risque d'entraîner des dommages.
- Un traitement manuel continu issu de la gestion d'un processus non systématique et non cohérent d'alertes et de réponse aux incidents demande beaucoup d'énergie, ce qui amène à manquer des alertes majeures et à consacrer trop d'attention aux faux positifs.



Obstacle n° 2 : Des informations insuffisantes ou non pertinentes sur les menaces

La Threat Intelligence doit passer une épreuve de vérité en trois étapes pour tenir sa promesse de visibilité approfondie sur les cybermenaces ciblant votre entreprise :

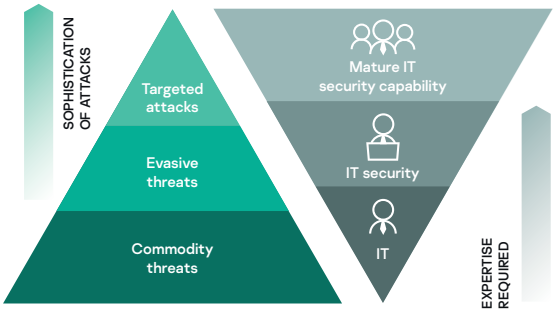
- Est-ce complet ?
- Est-ce précis ?
- Est-ce à jour ?

Passer cette épreuve n'est que la première étape. La barrière que rencontrent trop d'entreprises aujourd'hui est la suivante : même si elles ont accès à des données de Threat Intelligence complètes, précises et à jour, la pièce maîtresse, la pertinence, leur manque toujours. Tout professionnel de la sécurité informatique maîtrisant l'ensemble des flux d'informations de Threat Intelligence disponibles aujourd'hui en est tout à fait conscient.

La pertinence peut être un moyen de dire que la qualité prévaut sur la quantité, mais ce n'est pas tout à fait vrai. La Threat Intelligence doit provenir d'une source offrant les deux et doit être canalisée ou traitée par le biais d'un système de cybersécurité holistique, qui créé lui-même la pertinence pour cette entreprise, ce moment et cet environnement en particulier. La pertinence n'est pas un comportement exceptionnel, mais un processus continu qui implique une boucle de rétroaction entre les éléments intégrés dans une configuration de cybersécurité.

La Threat Intelligence pertinente contextuellement, intégrée à d'autres mécanismes de détection et de recherche de menaces, permet de trouver automatiquement une signification et un contexte, pour un gain de temps et une vue claire dès le départ.

Obstacle n° 3 : Tendance à se focaliser sur les menaces « basiques »



Les menaces « basiques » représentent toujours un pourcentage très élevé de l'ensemble des menaces visant les entreprises. Cette tendance est endémique même au sein des grandes entreprises matures sur le plan informatique.

Néanmoins, le coût des incidents liés à ces menaces est négligeable par rapport à celui des assauts complexes dévastateurs comme les attaques ciblées.

La raison pour laquelle certaines équipes de sécurité informatique se concentrent toujours trop sur les menaces simples (au détriment des incidents complexes) est assez évidente. Il est humain de vouloir se focaliser sur un problème simple et facile à résoudre. De plus, l'une des raisons pour lesquelles les menaces simples sont si faciles réside dans le fait que même la configuration de cybersécurité la plus basique et à la structure la moins robuste peut toujours fonctionner efficacement et les détecter automatiquement, mais sans proposer suffisamment d'automatisation pour les éliminer. Ainsi, les menaces simples peuvent occuper beaucoup d'espace et requérir une attention inutile au détriment des incidents complexes, beaucoup plus dangereux.

Obstacle n° 4 : La pénurie de talents en cybersécurité

La carte Cyberseek Heat Map, lancée par l'US National Initiative for Cybersecurity Education (NICE), illustre l'étendue de la pénurie de talents en cybersécurité. Même si l'outil Cyberseek pointe uniquement la pénurie sur le sol américain, il fournit un aperçu très utile (et qui fait froid dans le dos) de la situation mondiale.

Depuis le 30 janvier 2021, 521 617 postes en cybersécurité sont vacants aux États-Unis, contre un effectif global de 941 904 salariés. Cela représente un ratio d'offre par rapport à la demande de 1,8.

Même si ces chiffres mettent en lumière la sécurité d'emploi pour les professionnels de la cybersécurité (et il serait temps d'encourager vos enfants à l'aube de leurs études à faire carrière dans ce secteur), ils sont aussi porteurs de mauvaises nouvelles quant à la qualité et l'efficacité de la vie professionnelle.

La plupart des analystes concluent que la pénurie de talents en cybersécurité est due aux dysfonctionnements au niveau des formations, une information qui n'aidera en rien les entreprises concernées. Tant que ces dysfonctionnements ne sont pas résolus (en partie par des initiatives comme l'outil Cyberseek), les entreprises doivent surmonter cet obstacle en optimisant les capacités de leurs équipes de sécurité informatique existantes, en leur fournissant des outils, du support, des conseils et le support dont elles ont besoin pour résoudre efficacement les incidents complexes.

Obstacle n° 5 : Le problème de la vitesse

Ce dernier frein à la résolution efficace des incidents complexes est lié aux quatre obstacles précédents. Face aux défis complexes tels que les exploits zero-day, les attaques de programmes malveillants et les attaques hors sol, la vitesse fait toute la différence.

Un incident complexe ne commence pas nécessairement de façon complexe, comme nous l'avons vu avec le recours continu au phishing ciblé en tant que tactique d'accès initial. Les conséquences désastreuses (et onéreuses) des incidents ultra-complexes peuvent être évitées si l'équipe en question parvient à y répondre suffisamment vite.

Il ne s'agit naturellement pas de suggérer qu'il y a toujours un moment dans l'évolution d'un incident complexe où c'est « trop tard » et où le niveau de complexité monte d'un cran. Cependant, la vitesse fait souvent toute la différence avec les incidents complexes.

La vitesse n'implique pas un combat permanent ou le fait d'avoir la gâchette sensible et de répondre rapidement à n'importe quelle alerte sollicitant notre attention, mais d'exécuter rapidement et avec précision tous les processus essentiels de détection et de réponse, fermement et invariablement. Une telle exécution inclut entre autres une recherche proactive des menaces, une analyse rétrospective des causes profondes, une résolution, une atténuation et une réponse aux incidents.

Qu'est-ce que l'avenir réserve aux entreprises exposées à des incidents complexes ?

Le début de l'année 2021 semble être la période la pire, de mémoire d'homme, pour prévoir l'avenir. Après tout, la pandémie est en elle-même un incident complexe pour lequel nos outils, systèmes et professionnels ne sont pas équipés. Mais nous avons tout de même quelques certitudes. Par exemple, nous savons que les APT et autres attaques complexes continueront d'évoluer et que le télétravail ne va cesser de croître, même après la fin de la crise. Notre équipe GReAT (Global Research and Analysis Team) composées des meilleurs chercheurs au monde en matière de cybersécurité, a fait les prévisions suivantes concernant les APT en 2021 :

- Les attaques False flag (comme Olympic Destroyer) vont atteindre un niveau plus élevé
- Des ransomwares de plus en plus ciblés
- De nouveaux vecteurs d'attaque de banques et de paiement en ligne
- La hausse des attaques d'infrastructures et des attaques contre des cibles non-PC
- L'augmentation des attaques dans les régions situées le long des routes commerciales entre l'Asie et l'Europe
- La hausse de la sophistication des méthodes d'attaque
- La réorientation vers les attaques mobiles
- L'abus d'informations personnelles : des deepfakes aux fuites de données sur l'ADN

Le risque de tels incidents complexes planant sur les professionnels de la sécurité informatique n'est pas forcément dramatique.

Le rapport de recherche de l'ENISA nous donne une lueur d'espoir et une astuce pour concentrer nos efforts sur la résolution efficace des incidents complexes : la dimension humaine :

« La cybersécurité est toujours considérée comme une pratique de protection des réseaux, des systèmes d'informations et des données (NIS). Cette définition doit aller au-delà des problèmes techniques pour inclure les obstacles sociologiques, comportementaux et économiques, ainsi que les différents rôles occupés par les parties impliquées. Ceci doit constituer une priorité dans la recherche future liée à la cybersécurité et les discussions autour de l'innovation. Une meilleure compréhension de la dimension humaine est primordiale dans la définition de n'importe quelle stratégie de cybersécurité pour pouvoir prendre les décisions en fonction des besoins, des compétences et des attentes. »

Dans cette optique, les « parties » susmentionnées font référence aux professionnels de la sécurité informatique, ainsi qu'aux chefs d'entreprises dont ils dépendent. Nous ne sommes pas en mesure de recruter tous les talents en cybersécurité dont nous avons besoin. La question est : comment soutenir ceux qui travaillent pour nous ?

Une technologie experte entre des mains d'experts

La première étape consiste à comprendre que même les entreprises les plus matures sur le plan informatique ne peuvent pas lutter seules contre les attaques complexes et les APT. Il s'agit d'un problème global, qui sévit constamment d'une région et d'un secteur à l'autre. Trop d'équipes sont dans l'incapacité de résoudre efficacement les incidents complexes à cause des obstacles évoqués dans ce document.

C'est pourquoi nous encourageons l'ensemble de nos clients professionnels à s'assurer qu'ils traitent rapidement ce que nous considérons comme les trois piliers d'une stratégie efficace de résolution des incidents complexes. Les équipes de sécurité doivent être :

- **Correctement équipées :**
  la cybersécurité est un domaine dans lequel même un expert peut légitimement jeter la faute sur ses outils. La protection contre les attaques multi-vecteurs et autres incidents complexes nécessite une plateforme unifiée et consolidée qui procure une visibilité totale, élimine les silos obstructifs et empêche la lassitude face à un grand nombre d'alertes et autres tâches de routine pendant le processus de réponse aux incidents.

- **Informées :**
  l'expertise avancée des entreprises matures sur le plan informatique ne doit jamais être prise pour acquise. Après tout, l'horizon du cybercrime se transforme et s'étend constamment. Il est essentiel d'assurer une formation continue et d'obtenir des informations pertinentes sur les menaces en matière de cybersécurité auprès d'un partenaire fiable.

- **Renforcées :**
  si un incident complexe ou une APT est détecté(e), même les analystes de sécurité informatique les plus expérimentés doivent avoir accès à une aide externe pour obtenir un avis tiers, une évaluation de la sécurité, une recherche gérée des menaces et une réponse aux incidents. Même si les incidents complexes résultant des APT sont généralement hautement ciblés, ils ciblent rarement une seule victime. L'expertise externe peut apporter un éclairage global multi-secteurs sur les chemins probables d'une APT et prodiguer des conseils applicables sur le moyen le plus efficace de l'éliminer du système.

Kaspersky Expert Security révolutionnera la façon dont vos experts en sécurité informatique prennent le contrôle d'incidents complexes.

Révolutionnez la façon dont vos experts en sécurité informatique prennent le contrôle d'incidents complexes à l'aide de Kaspersky Expert Security : un concept défensif complet qui équipe, informe et guide votre équipe dans sa lutte contre les cyberattaques les plus complexes et les plus ciblées. Il s'agit d'une plateforme Extended Detection and Response (XDR) qui offre une combinaison optimale de technologies, de Threat Intelligence, d'expertise humaine, de formation et de services, le tout soutenu par des experts reconnus en cybersécurité. Notre approche holistique renforce les compétences de votre équipe sur le plan de la cybersécurité grâce à la découverte multidimensionnelle des menaces, à des enquêtes efficaces, à la chasse proactive des menaces et à une réponse rapide et centralisée à l'ensemble des menaces modernes.

Pour en savoir plus, rendez-vous sur go.kaspersky.com/fr_expert

Actualités sur les cybermenaces : www.securelist.com
Actualités sur la sécurité informatique : www.kaspersky.fr/blog
Portail de Threat Intelligence : opentip.kaspersky.com
Technologies en bref : www.kaspersky.fr/enterprise-security/wiki-section/home
Prix et distinctions : go.kaspersky.com/awards_b2b.html
Interactive Portfolio Tool (outil de portefeuille interactif) :
media.kaspersky.com/fr/business-security/enterprise/KL-Enterprise-Catalogue.pdf

www.kaspersky.fr

kaspersky BRING ON THE FUTURE