Microsoft et Vectra parviennent à réaliser le modèle de la triade SOC (SOC Visibility Triad)

Face à l'augmentation sans précédent de la cybercriminalité, force est de constater que les solutions de protection traditionnelles ont perdu de leur efficacité. Les menaces sont devenues furtives, s'exécutant sur des périodes prolongées, dissimulées au sein de trafic chiffré ou dans des tunnels. Confrontées à des menaces de plus en plus sophistiquées, les équipes de sécurité ont besoin d'une visibilité immédiate sur les cybermenaces qui pèsent sur leurs environnements.

Dans le rapport Gartner consacré à l'application d'une approche axée réseau (*Applying Network-Centric Approaches for Threat Detection and Response*), publié le 18 mars 2019 (ID : G00373460), Augusto Barros, Anton Chuvakin et Anna Belak ont introduit le concept du modèle de la triade SOC (SOC Visibility Triad).

D'après Gartner, « par leur niveau croissant de sophistication, les menaces obligent les entreprises à s'appuyer sur plusieurs sources de données pour la détection des menaces et la résolution des incidents. Les technologies réseau permettent aux responsables techniques de bénéficier d'une visibilité immédiate sur les menaces, et ce, sur l'ensemble de leur environnement et sans l'intervention d'agents[1]. »

Cette étude montre que « les outils modernes spécialisés dans les opérations de sécurité peuvent également être comparés à une triade nucléaire, ce fameux concept qui a vu le jour durant la Guerre froide. Cette triade était alors constituée de bombardiers stratégiques, de missiles balistiques intercontinentaux et de sous-marins lanceurs d'engins. Tel qu'illustré par la figure 1 (à droite), les SOC modernes disposent eux aussi de leur propre triade nucléaire de visibilité :

1. Les solutions **SIEM/UEBA** permettent de rassembler et d'analyser les fichiers journaux générés par les applications, l'infrastructure informatique et autres outils de sécurité. (Pour plus d'informations, voir *SIEM Technology Assessment*.)
2. Les technologies de **détection et résolution des incidents pour terminaux (EDR)** permettent quant à elles de capturer l'exécution des processus, les connexions locales, les modifications apportées au système, les activités mémoire et autres opérations réalisées sur les terminaux. (Pour plus d'informations, voir *Endpoint Detection and Response Architecture and Operations Practices*.)
3. Les fonctions de **détection et résolution des incidents axées réseau (analyse du trafic réseau, outils d'investigation numérique du réseau et systèmes IDPS)** sont assurées par les outils dévolus à la capture et à l'analyse du trafic réseau, tel que présenté dans cette étude[2]. »

Cette approche triple permet aux SOC de bénéficier d'une amélioration de la visibilité, de la détection, de la résolution des incidents, des investigations et de la correction.

Figure 1. Modèle de la triade SOC.

Source : Gartner, Applying Network-Centric Approaches for Threat Detection and Response, Augusto Barros et al., 18 mars 2019, ID : G0037346

Microsoft Defender Advanced Threat Protection

Les compromissions de terminaux ne sont que trop fréquentes, qu'elles soient le fruit de malwares, de vulnérabilités non corrigées, d'erreurs de configuration ou d'erreurs d'inattention de la part des utilisateurs. Les équipements mobiles peuvent facilement être compromis sur les réseaux publics. Il suffit alors qu'ils se reconnectent au réseau de l'entreprise pour que l'infection se propage.

Microsoft Defender ATP (Advanced Threat Protection) est une plate-forme unifiée de sécurité pour terminaux garantissant une protection préventive, une détection post-compromission, des investigations automatisées et la résolution des incidents.

Basées sur le comportement et optimisées par le cloud, ses technologies de protection contre les menaces et les malwares empêchent les cybermenaces inédites et les plus sophistiquées d'avoir un impact sur les équipements. Microsoft Defender ATP offre une visibilité approfondie sur le système d'exploitation (mémoire et noyau y compris) et contribue à la détection des menaces jour zéro, des attaques avancées et des violations de données.

---

1 Source : Gartner, Applying Network-Centric Approaches for Threat Detection and Response, Augusto Barros et al., 18 mars 2019, ID : G00373460
2 Ibid.

Cette visibilité accrue aide les analystes en sécurité à identifier les comportements, les indicateurs de compromission et autres indices cachés. Les données peuvent être associées à d'autres flux de données de cyberveille afin de détecter les menaces susceptibles d'être uniquement visibles à l'intérieur de l'hôte.

Détection et aide à la résolution des incidents réseau Vectra

Les métadonnées réseau constituent la source la plus sûre en matière de détection des menaces. Seul le trafic réseau permet de déceler les menaces cachées avec un niveau optimal de fiabilité et d'objectivité. Les sources basse résolution, comme les analyses de fichiers journaux, ne répertorient que ce que vous avez déjà vu ; elles n'intègrent pas les comportements caractéristiques des opérations de reconnaissance, propagation et exfiltration exécutées par les cyberpirates, impossibles à dissimuler.

La plate-forme Vectra offre une vue globale des interactions qui existent entre les différents équipements du réseau. S'appuyant sur les recherches en sécurité et la science des données, les modèles comportementaux optimisés par l'intelligence artificielle de Vectra sont capables de détecter les attaques en cours, classées en fonction de leur niveau de gravité et mises en corrélation avec les systèmes compromis. La plate-forme collecte et stocke les métadonnées réseau pertinentes et les enrichit grâce à l'apprentissage automatique et aux analyses avancées, de façon à détecter les activités suspectes sur les réseaux d'entreprise.

Grâce à l'intégration native de la plate-forme avec Microsoft Defender ATP, les équipes de sécurité peuvent allier la vue globale de Vectra à la vue opérationnelle de Microsoft Defender ATP. Les analystes peuvent ainsi obtenir des informations de contexte grâce à Microsoft directement sur la plate-forme Vectra, et désactiver automatiquement certains comptes ou exécuter un isolement de l'hôte Microsoft Defender ATP depuis le console Vectra. Les équipes de sécurité peuvent également accélérer les investigations en basculant immédiatement vers Microsoft Defender ATP, tout en bénéficiant du contexte local de Vectra utilisé pour définir les paramètres de portée et d'échelle de Microsoft Defender ATP.

Microsoft Azure Sentinel

Depuis plusieurs décennies, les équipes de sécurité utilisent les solutions SIEM en tant que tableau de bord pour centraliser leurs activités de sécurité dans l'ensemble de leur environnement informatique. Les solutions SIEM recueillent les informations des journaux d'événements à partir d'autres systèmes et proposent des fonctionnalités d'analyse de données, de corrélation des événements, d'agrégation et de génération de rapports.

Azure Sentinel est capable d'intégrer des journaux syslog aussi bien à partir de Vectra Cognito que de Microsoft Defender ATP. Lorsqu'un incident se produit, les analystes peuvent utiliser des applications intégrées et les widgets de tableau de bord Vectra afin d'identifier rapidement les comptes et systèmes compromis. Ils peuvent également mener des investigations plus facilement pour déterminer la nature d'une attaque et sa réussite ou son échec.

Les solutions SIEM sont par ailleurs capables de communiquer avec d'autres contrôles de sécurité réseau, comme les pare-feux ou les systèmes NAC de contrôle d'accès réseau, de sorte à leur donner l'instruction de bloquer les activités malveillantes détectées. Les flux de données de cyberveille peuvent aussi aider les solutions SIEM à empêcher les attaques de manière proactive.

Microsoft et Vectra, ou comment réaliser le modèle de la triade SOC

Les équipes de sécurité sont en mesure de réaliser le modèle de la triade SOC grâce à des intégrations natives entre la plate-forme Vectra Cognito, Microsoft Defender ATP et Azure Sentinel. Elles peuvent ainsi répondre à plus de questions différentes, ce qui aurait été impossible si les solutions fonctionnaient de manière compartimentée. À titre d'exemple :

- Le comportement d'une autre ressource a-t-il changé de manière inhabituelle après avoir communiqué avec une ressource potentiellement compromise ?
- Quels services et protocoles étaient utilisés ?
- Quels autres comptes ou ressources pourraient être touchés ?
- Une autre ressource a-t-elle établi un contact avec la même adresse IP C&C externe ?
- Le compte utilisateur a-t-il été utilisé de manière inattendue sur d'autres équipements ?

Grâce aux intégrations natives qui centralisent les contextes de toutes les sources de données, aux stratégies de mise en œuvre intégrées (comme la désactivation de compte ou l'isolement d'hôte) et aux tableaux de bord de visibilité des SOC, ces solutions permettent conjointement d'apporter des réponses coordonnées, d'améliorer l'efficacité des opérations de sécurité et de réduire les durées d'implantation, sources de risques pour votre entreprise.

VECTRA®
Security that thinks®

E-mail : info_france@vectra.ai / info_dach@vectra.ai **Téléphone :** +33 62 912 4119 / +41 44 551 0143 vectra.ai/fr

© 2020 Vectra AI, Inc. Tous droits réservés. Vectra, le logo Vectra Networks et le slogan « Security that thinks » sont des marques commerciales déposées ; Cognito, Cognito Detect, Cognito Stream, Vectra Threat Labs et Threat Certainty Index sont des marques commerciales de Vectra Networks. Les autres noms de marque, de produit ou de service sont des marques commerciales, des marques commerciales déposées ou des marques de service de leurs propriétaires respectifs.