VECTRA
SECURITY THAT THINKS.®

PRÉSENTATION DE SOLUTION

Une visibilité inégalée pour les SOC

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*).

Comme expliqué dans ce rapport :

« Le niveau de sophistication croissant des menaces oblige 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]. »

Figure 1. Modèle « SOC Visibility Triad »

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

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, 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.

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.

3. Les fonctions de **détection et résolution des incidents axées réseau (NDR) (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.

Détection et aide à la résolution des incidents réseau (NDR) 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.

Une solution NDR 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. Elle crée des modèles qui reflètent les comportements normaux et les enrichit grâce à des métadonnées historiques et en temps réel.

Une solution NDR offre une vue globale des interactions qui existent entre les différents équipements du réseau. Les attaques en cours sont détectées, classées en fonction de leur niveau de gravité et mises en corrélation avec les systèmes compromis.

Une solution NDR offre une visibilité à 360° à l'échelle de l'entreprise, des charges de travail dans les centres de données privés et les clouds publics aux équipements IoT et terminaux des utilisateurs.

Détection et aide à la résolution des incidents pour terminaux (EDR)

Les compromissions de terminaux ne sont que trop fréquentes, qu'elles soient le fruit de malwares, de vulnérabilités non corrigées 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. Il est bien connu que les équipements de l'Internet des objets (IoT) ne sont pas sécurisés.

Une solution EDR propose des fonctions plus avancées qu'un antivirus traditionnel. Elle permet notamment un suivi détaillé des activités malveillantes sur un terminal ou un système. Elle offre une vue globale en temps réel des processus s'exécutant sur un système ou un équipement, ainsi que des interactions entre ceux-ci.

Une solution EDR capture l'exécution des processus, de la mémoire et d'autres activités et modifications système. 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 du système.

Solutions SIEM d'entreprise

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 fonctions d'analyse de données, de corrélation des événements, d'agrégation et de génération de rapports.

L'intégration des fonctions de détection des menaces des solutions EDR et NDR peut renforcer davantage la puissance des solutions SIEM et permettre aux analystes en sécurité de bloquer les attaques plus rapidement. Lorsqu'un incident se produit, les analystes peuvent identifier rapidement les 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 prévenir les attaques.

Approche intégrée de la détection et de la neutralisation des cyberattaques

Les équipes de sécurité déployant la triade de solutions NDR, EDR et SIEM peuvent répondre à un plus large éventail de questions lorsqu'elles interviennent sur un incident ou qu'elles traquent des menaces. En voici des exemples :

- 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 ?

Ces solutions permettent conjointement d'apporter des réponses rapides et coordonnées, d'améliorer l'efficacité des opérations de sécurité et de réduire les durées d'implantation, sources de risques pour l'entreprise.

Selon le Forum économique mondial, les pertes économiques imputables aux cyberattaques devraient atteindre 3 000 milliards de dollars d'ici 2020. Bien que le nouveau monde numérique sans frontières soit du pain béni pour les groupes à la solde d'États et les cyberpirates, en adoptant une triade nucléaire de visibilité, les SOC peuvent protéger les données sensibles et les opérations critiques des entreprises.

Pour plus d'informations, veuillez contacter l'un de nos représentants à l'adresse sales-inquiries@vectra.ai.

E-mail : info_france@vectra.ai / info_dach@vectra.ai vectra.ai/fr