Sécurité IT, SOC et analyse UEBA: comment apporter une réponse globale

Si les menaces sont mieux cernées, elles ne diminuent pas pour autant. Les dispositifs de sécurité doivent être déployés de façon globale alors que les analyses du comportement des entités et des utilisateurs (UEBA) apportent des éléments de réponse intéressants.

Qu'observe-t-on depuis quelques mois ? Les attaques DDOS (Distributed Denial of Service) se seraient stabilisées depuis 2017, mais elles perdurent avec, notamment, un retour du malware Pbot. On cite également Mirai et des variantes plus sophistiquées (Reaper, IOTroop…).

Le mode opératoire vise toujours à bloquer des accès réseaux ou des sites web en les bombardant de tentatives de connexions à un débit très élevé. Des flux records ont été atteints, dépassant le tera-octets par seconde en provenance de milliers de systèmes attaquant simultanément !

Autre menace qui perdure : les ransomwares (rançongiciels) se sont révélés très effaces ces derniers mois pour extorquer de coquettes sommes d'argent. Leurs signatures sont aujourd'hui généralement bien repérées par les logiciels anti-malwares mais la menace subsiste, comme le notifient les rapports de sécurité de Symantec, Sophos ou Kaspersky.

1 – Menace sur les identifiants

Autre menace récurrente : les vols de mots de passe, utilisant des techniques de phishing avec de faux sites web, restent également très présents.

Même la double authentification peut être détournée par une parade des hackers, comme, par exemple, EvilGinx2 – un proxy qui capture automatiquement les identifiants, les victimes ayant été conduites vers un vrai compte Microsoft.

Dans son rapport 2018 sur la sécurité, Symantec épingle également les malwares qui attaquent la chaîne d'approvisionnement de logiciels. L'infiltration s'opère lors des mises à jour de packages logiciels.

La poussée du crypto-jacking

Une autre menace se développe depuis ces deux dernières années : le crypto-jacking exploite la puissance de calcul de l'ordinateur piraté pour « miner » les crypto-monnaies et actifs tels que Bitcoin, Monero ou Ethereum.

Selon Symantec, ces attaques ont augmenté de 8.500 % ces derniers mois et leur nombre peut friser les 2 millions d'attaques par mois : « En moyenne, les pirates volent 1,5 million de dollars de crypto-monnaie chaque mois. La majeure partie des vols est due à du phishing».

Les smartphones dans le viseur

« Dans les transactions bancaires, on voit de plus en plus d'attaques sur des campagnes de vol

d'identités sur smartphone, à partir de 'rogue apps' », observe Bernard Montel, chez RSA (Dell-EMC). De fait, les 'rogue apps' se comptent par milliers sur les sites de téléchargements. Sous couvert d'apporter un service, elles permettent d'installer des malwares sur le smartphone.

Bref, les menaces sont toujours là : « Les nouvelles cyberattaques sont plus ciblées et à multiples facettes. Or, les entreprises ne bénéficient la plupart du temps que d'une visibilité limitée et en silos », constate Bernard Montel.

2 – Des solutions contre les cyber-menaces

Sur les postes de travail, beaucoup de malwares ne sont pas détectés par les outils traditionnels. Alors comment faire face au nombre et à la variété des types de menaces ?

« Il faut s'interroger sur les limites du tryptique constitué du suivi des logs, du contrôle du réseau et du contrôle des postes. Ce n'est plus la seule bonne approche, constate Bernard Montel (RSA). « Il faut certes savoir se servir de l'analyse des logs, tout en reconnaissant leurs limites. Il faut également déterminer quoi faire pour limiter les faux-positifs », ajoute-t-il.

SIEM et analyse des flux

Le recours à un centre d'opération sécurité ou SOC (Security Operation Center) reste une bonne réponse, car sa mission principale est la détection des principales menaces.

« Le SOC est bien souvent équipé d'une solution de SIEM (Security information and event management) permettant de collecter, d'agréger et de corréler l'ensembles des logs issus du Systèmes d'Information (SI) afin de constituer une vue holistique de la sécurité du SI », observe Arnaud Delande, CTO Sécurité d'IBM France.

Aussi, faut-il considérer plus en détail les données issues des flux réseau dans l'environnement de l'entreprise : « L'analyse des flux offre en effet une visibilité en profondeur indispensable et en temps réel. Elle permet d'aider les équipes de sécurité à détecter les attaques les plus sophistiquées en rapprochant ces données avec celles issues des journaux de logs, tout en éliminant les alertes « faux-positifs ».

L'apport de l'IA

Les solutions d'Intelligence Artificielle apportent un complément très salutaire.
« Une solution d'IA, comme IBM QIRadar Watson, met à disposition un expert en sécurité qui lit le Web 24x7x365, garde tout en mémoire, formule des hypothèses sur les attaques en s'appuyant sur sa base de connaissances hautement dynamique. Elle permet également de réduire drastiquement le temps d'investigation des incidents de sécurité en éliminant rapidement les faux-positifs pour laisser les analystes se concentrer sur les incidents les plus critiques », explique Arnaud Delande chez IBM.

Prévenir le Social Engineering

Chez Microfocus, on souligne également la nécessité de dépasser le triptyque » logs + réseau + postes de travail » même s'il reste essentiel pour la défense du périmètre, pour la protection

extérieure du SI.

« C'est le premier rempart pour détecter et repousser les attaques ». Cependant, les études montrent que plus de 80% des attaques démarrent avec une forme de « social engineering » permettant à un hacker de s'accaparer des comptes utilisateurs. « C'est pourquoi nous proposons un autre tryptique : utilisateurs + applications + données », explique Louis Vieille-Cessay, responsable avant-ventes chez Microfocus.

Des considérations particulières s'imposent alors en termes de durcissement, de suivi, d'audit et de contrôles des accès utilisateurs : « Au-delà du périmètre, il faut un niveau de défense et une compréhension du contexte particulier plus profond, similaire à ce que l'on fait pour le réseau» poursuit-il.

Autre constat : l'objectif des d'attaquants est d'atteindre les données sensibles : « Ce sont les données personnelles et les données de propriété intellectuelle qui ont de la valeur. Il faut donc adapter sa sécurité informatique en conséquence ».

En clair, les environnements contenant des données sensibles et critiques doivent être mieux protégés : « Il faut des protections renforcées autour de certaines applications et aussi du chiffrement pour les données critiques. Les environnements à risque doivent donc être très surveillés afin de mieux comprendre le contexte d'utilisation, d'exploitation, d'accès, etc », ajoute Louis Vieille-Cessay.

3 – Limiter les interfaces et écouter les métiers

« Aujourd'hui le tryptique « logs, réseau, poste » reste crucial. Mais les logs ne suffisent plus. Il faut également limiter le nombre des interfaces et les outils. C'est la raison pour laquelle nous avons unifié les interfaces afin de faciliter le travail des analystes du SOC », confirme Bernard Montel.

Capturer des logs, dans différents contextes et en faire des rapports est donc aujourd'hui insuffisant. Des analyses de corrélation s'imposent entre les différents niveaux contextuels. Elles viennent alimenter des indicateurs et spécifient les anomalies en temps réel.

Tous les faux positifs ne seront pas évités pour autant. « C'est pourquoi Il doit rester une place à l'analyse par des spécialises (rôle du SOC). C'est encore plus vrai pour les enquêtes post-incident », résume Bernard Montel (RSA) qui ajoute : « Faire le lien entre le risque métier et le SOC est également très important : le SOC ne peut pas tout surveiller tout azimut. Le métier doit guider les priorités des RSSI. Et il faut donc orchestrer et gouverner les risques métier / IT et redescendre ceux-ci vers le pilotage du SOC ».

4 – SOC : externaliser ou automatiser ?

Les compétences qu'impose un SOC (Security Operation Center) n'existent pas dans toutes les entreprises. Faut-il se résoudre à en externaliser l'exploitation ? Et jusqu'où peut-on l'automatiser ? « Il existe aujourd'hui une réelle pénurie de ressources compétentes en matière de cybersécurité et cette tendance va s'accélérer dans les années à venir », observe Arnaud Delande (IBM).

Certaines organisations s'orientent vers l'option d'un SOC « hybride » – en partie interne et en

partie externe.

A un prestataire spécialisé, on délègue généralement la partie détection, l'analyse et l'évaluation des menaces, la qualification et l'investigation de premiers niveaux des incidents de sécurité. C'est le rôle du SOC de définir les schémas de réponse automatisés pour chaque type d'incident de sécurité, en impliquant des personnes, des processus, des solutions, tout en tenant compte de la réglementation. Il faut également une vue centralisée.

SOC : des compétences rares

Le rôle premier du SOC est de sécuriser, faciliter et stabiliser l'organisation qu'il surveille : «La mise en place d'un SOC exige un éventail de compétences rares et très demandées, telle qu'une expertise sur les processus de sécurité et d'analyse de risques au moment de la mise ne place mais aussi de suivi ; une expertise technique sur l'outillage utilisée pour en assurer le bon fonctionnement ; enfin, une expertise en sécurité pour comprendre, veiller et analyser ce qui se passe dans le SI pour détecter les attaques », explique Louis Vieille-Cessay .

L'externalisation est une solution « mais il faut que cela s'inscrive dans une certaine démarche ; car certains logs contiennent de données très personnelles ». Des questions se posent alors – y compris règlementaires – concernant l'accès que l'on en donne à un prestataire. Il faut trouver la bonne démarche, bien équilibrée entre compétences internes et externes.

Que peut-on automatiser ?

Les capacités d'automatisation du SOC deviennent cruciales : elles concernent notamment les plans de réponses aux incidents de sécurité. « Idéalement, il faut un juste équilibre entre l'automatisation et les prises de décision humaines » – observe Arnaud Delande.

« Il est inconcevable aujourd'hui d'automatiser l'intégralité du fonctionnement d'un SOC. L'analyse d'incidents nécessite une forte contextualisation de ce qu'il se passe mais aussi une forte réactivité et créativité, ces décisions complexes ne sont pas toujours prises de manière optimale par les machines… », explique Louis Vieille-Cessay. Même avis chez RSA : « l'automatisation apporte beaucoup en efficacité, mais n'est pas la réponse à toutes les situations. » affirme Bernard Montel.

5 – Les solutions UEBA et leurs limites

Depuis quelques mois, les experts en sécurité débattent sur l'UEBA, c'est à dire l'ensemble les fonctions d'analyse avancées et d'analyse du comportement des entités et des utilisateurs. Quels sont les enjeux ?

Selon le cabinet d'étude Gartner, d'ici à deux ans, au moins 60 % des principaux éditeurs de solutions CASB (Cloud Access Security Broker), et 25 % des principaux éditeurs de solutions SIEM (Security Information and Event Management) et DLP (Data Loss Prevention), intégreront des fonctions d'analyse avancées UEBA dans leurs produits.

Ces fonctions sont proposées, soit en natif ou à travers des partenariats ou alliances technologiques. Elles assurent la sécurité via un profilage statistique et une détection des anomalies basés sur l'IA ou 'machine learning' (apprentissage machine). Se méfier des systèmes

complexes, coûteux

Ces technologies peuvent être très performantes pour identifier les menaces internes ou externes, « mais il ne s'agit là que d'un cas d'utilisation, et non d'un besoin d'une solution de sécurité dédiée qui nécessite le plus souvent le déploiement d'agents sur les systèmes rendant complexe et coûteux leurs déploiements », objecte Arnaud Delande (IBM France.)

Il est vrai qu'une solution SIEM peut suffire à apporter une base solide pour la surveillance, tout en permettan d'évoluer en fonction des besoins. L'enjeu, c'est de corréler les données des journaux de logs, les informations sur les menaces, les coordonnées de géolocalisation, les données d'analyse des vulnérabilités et les activités des utilisateurs internes et externes. « Les applications UEBA, avec le 'machine learning' peuvent être avantageusement associées à des alertes basées sur des règles comportementales », constate Arnaud Delande.

Une réponse partielle

« Il faut reconnaitre ce type de solutions pour ce qu'elle est : un niveau et un contexte analytique supplémentaire qui permettra à un analyste de sécurité dans un SOC de mieux comprendre ce qui est en train de se passer quand les systèmes soupçonnent une attaque », observe Louis Vieille-Cessay, responsable avant-ventes chez Microfocus.

Pourtant, ce n'est pas la panacée. Car il faut que la solution soit bien implémentée, avec un niveau contextuel et de corrélation suffisant. « La plupart des attaques commencent par des mots de passes de comptes compromis. Une attention particulière sur ces sujets peut donc être très utile pour identifier les attaques en phase amont et réduire les risques d'un SI compromis », souligne -t-il.

Privilégier une approche globale

Tout dispositif de sécurité doit donc être, par nature, un sujet global. « C'est un exercice d'équilibriste entre l'efficience métier et l'acceptation du risque qui y est associe. Cet équilibre se joue également sur les terrains de jeux proactifs et réactifs », ajoute Louis Vieille-Cessay.

Idéalement il convient de combiner les dispositifs réactifs – dont l'analyse de logs et le SOC ainsi que les dispositifs proactifs : firewall, chiffrement, analyse de code, classification de données, gestion des accès et des identités…

En pratique, un bon environnement de sécurité présuppose une stratégie bien adaptée à la culture interne de l'organisation, à son métier, sa maturité et à ses moyens. « Ça commence donc par des personnes qui mettent en place des processus et qui s'équipent des bons outils pour appliquer cette stratégie », ponctue Louis Vieille-Cessay.

« Pour développer une approche globale efficace, il faut pouvoir combiner deux composants importants, résume Bernard Montel (RSA) : d'une part l'analyse comportementale – et là, effectivement le machine learning apporte une contribution intéressante (cf. RSA NetWitness) – et, d'autre part, une augmentation de la capacité de décision et d'organisation du SOC, avec de l'automatisation (cf. NetWitness Orchestrator).
On touche ici au domaine du SOAR (Common security orchestration, automation and response).