FORTINET

Faites appel à un analyste de sécurité virtuel basé sur l'IA pour moderniser votre SOC

L'Intelligence artificielle (IA) a la capacité d'identifier des modèles dans des quantités colossales de données, ce qui lui permet de détecter des tendances et de classifier les menaces beaucoup plus rapidement que les humains. Un (SOC) basé sur l'IA et utilisant un apprentissage approfondi tel que les réseaux neuronaux profonds peut aider à combler le manque de compétences croissant et à détecter et à répondre plus rapidement aux incidents de sécurité.

74% des professionnels de la sécurité affirment que le manque de compétences en matière de cybersécurité a eu un impact sur leur organisation.[1]

Un analyste du SOC virtuel basé sur un réseau neuronal profond contribue à atténuer les effets de ce déficit de compétences en aidant à effectuer des tâches de bas niveau et en assistant les analystes humains, ce qui leur permet d'opérer à un niveau plus élevé.

Un système d'IA doit présenter certaines caractéristiques pour être performant.

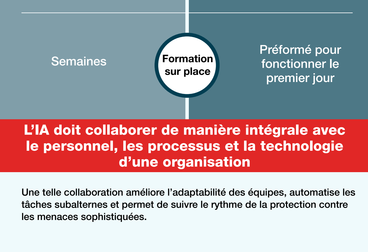
Un analyste de sécurité virtuelle piloté par l'IA doit apprendre par lui-même

Lorsqu'il s'agit d'**algorithmes d'apprentissage automatique**, le fait de disposer d'un analyste de sécurité virtuel basé sur un apprentissage approfondi et capable de travailler sans supervision et sans formation initiale sur place est une aubaine pour les équipes du SOC, qui comptent sur sa capacité à s'adapter à l'évolution du paysage des cybermenaces.

Apprentissage automatique	Modèle de formation	Apprentissage approfondi
Supervisé		Non supervisé
Domaine contrôlé par le fournisseur	Hébergé par l'IA	Partout, y compris dans les locaux des clients
Nécessite des mises à jour basées sur le Cloud	Maturité de l'IA (Formation continue)	Auto-apprentissage. Utilisation facultative de l'apprentissage global
Semaines	Formation sur place	Préformé pour fonctionner le premier jour

L'IA doit collaborer de manière intégrale avec le personnel, les processus et la technologie d'une organisation

Une telle collaboration améliore l'adaptabilité des équipes, automatise les tâches subalternes et permet de suivre le rythme de la protection contre les menaces sophistiquées.



La vitesse de la machine de l'IA doit accélérer la détection des menaces, les enquêtes et la réponse

Le SOC reçoit en moyenne **10000 alertes par jour**, mais ne dispose que de la main-d'œuvre et des ressources nécessaires pour traiter correctement une fraction d'entre elles.[2] Les deux tiers des analystes de sécurité enquêtent sur moins de 30 alertes par jour,[3] et la moitié d'entre elles sont probablement des faux positifs.[4]

Un analyste de la sécurité virtuelle basé sur l'IA peut accélérer le processus de détection et de classification précise des attaques potentielles, effectuer les enquêtes nécessaires pour identifier la source de la menace, les machines touchées et appliquer les mesures correctives appropriées.

Cela permet de réduire considérablement la charge de travail du personnel de sécurité et de diminuer le coût des incidents de sécurité.

Exemple de cycle de vie de la réponse à une menace

Avant : L'approche traditionnelle pour résoudre WannaCry avec uiquement les analystes de SecOps

Identifier (1+ heure)
- Supposons que sur 100 à 1000 alertes de menace sur un tableau de bord SOC, la menace sélectionnée est en fait un rançongiciel , ou
- Alerté directement par un utilisateur concerné

Enquêter (4+ heures)
- Se connecter au(x) produit(s) de sécurité
- Examiner les journaux/alertes
- Utiliser des outils intégrés et externes pour valider le rançongiciel
- Effectuer des recherches externes
- Se connecter au(x) produit(s) de sécurité pour rechercher le mouvement latéral de WannaCry
- Créer un plan de réduction des risques

Répondre (2+ heures)
- Dispositif(s) de quarantaine, segment de réseau
- Dispositif(s) correcteur(s)/restauration de la sauvegarde
- Appliquer les correctifs
- Fermer le billet

Après : Résoudre WannaCry avec un analyste de SecOps complété par des réseaux neuronaux profonds (IA)

Identifier (< 1 s)
- IA : rançongiciel validé en moins d'une seconde
- IA : auto-apprentissage des nouvelles fonctionnalités du rançongiciel

Enquêter (< 5 min)
- IA : la chaîne de mise à mort de WannaCry bénéficie d'une recherche contextuelle sur les menaces
- IA : identifier le mouvement latéral du patient 0 de WannaCry
- SecOps : créer un plan de réduction des risques

Répondre (< 30 min)
- L'IA intégrée aux contrôles de sécurité :
  - Dispositif(s) de quarantaine, segment de réseau
- Suivi du SecOps :
  - Dispositif(s) correcteur(s)/restauration de la sauvegarde
  - Appliquer les correctifs
- Fermer le billet

[1] Jon Oltsik, « The Life and Times of Cybersecurity Professionals 2018 (La vie et l'époque des professionnels de la cybersécurité 2018) », ESG et ISSA, avril 2019.
[2] How Many Daily Cybersecurity Alerts does the SOC Really Receive? (Combien d'alertes de cybersécurité le SOC reçoit-il réellement par jour ?) », Bricata, 2 octobre 2019.
[3] « SOCs still overwhelmed by alert overload, struggle with false-positives (Les SOC toujours débordés par la surcharge d'alertes, lutte contre les faux positifs) », Help Net Security, 29 août 2019.
[4] Idem.