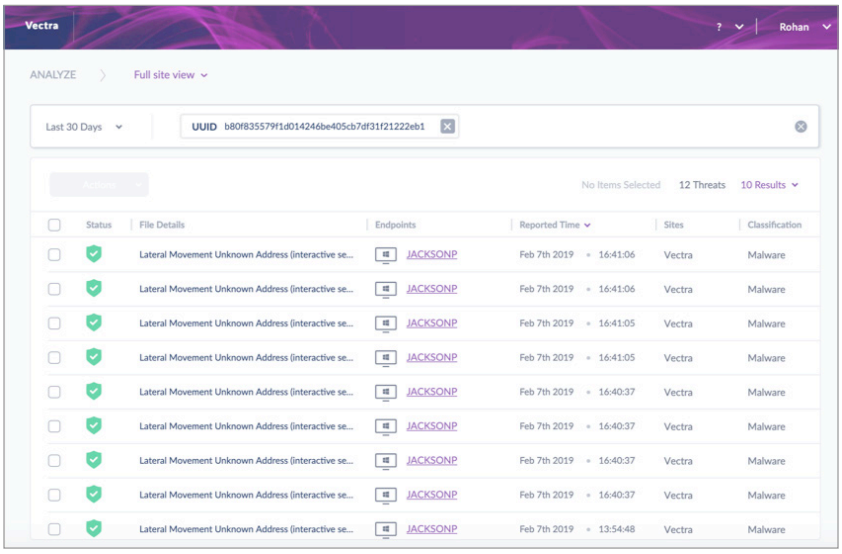
Vectra + Sentinel One

Détecter et neutraliser les cyberattaques grâce à l'IA comportementale

FONCTIONNALITÉS-CLÉS

- Une prévention autonome multi-niveaux couvrant tous les vecteurs d'attaque, même hors ligne.
- Une visibilité complète, en local et cloud, du réseau jusqu'aux postes de travail.
- Recours au machine learning : technologie sans signatures, ne nécessitant pas de mises à jour quotidiennes/hebdomadaires. Un volume réduit d'alertes pour une gestion plus attentive, plus efficace.
- Déclenchement de différentes actions en fonction du type de menace, du risque et du degré de certitude.

En misant à la fois sur la surveillance du réseau et des postes de travail, Vectra et Sentinel One offrent une visibilité complète et fiable sur les cyberattaques.
Vectra analyse le trafic réseau pour détecter automatiquement les comportements suspects et les hiérarchiser en fonction des risques.
De son côté, la plateforme de protection des postes de travail (EPP) Sentinel One assure la prévention et la détection des attaques menées via tous les principaux vecteurs. Sentinel One élimine rapidement les menaces grâce à des mesures de réponse totalement automatisées, définies par des politiques de sécurité. Cette solution offre une visibilité complète sur les postes de travail grâce à des analyses forensiques contextualisées, menées en temps réel.
L'ampleur et la sophistication des menaces réseau ne cesse de croître. Les entreprises ont besoin d'une plus grande visibilité sur les menaces, sur leurs appareils et sur les différents comptes. Elles doivent s'appuyer sur des renseignements automatisés et exploitables pour alléger la charge de travail du SOC et réduire au maximum le temps de présence d'un pirate informatique sur le réseau.



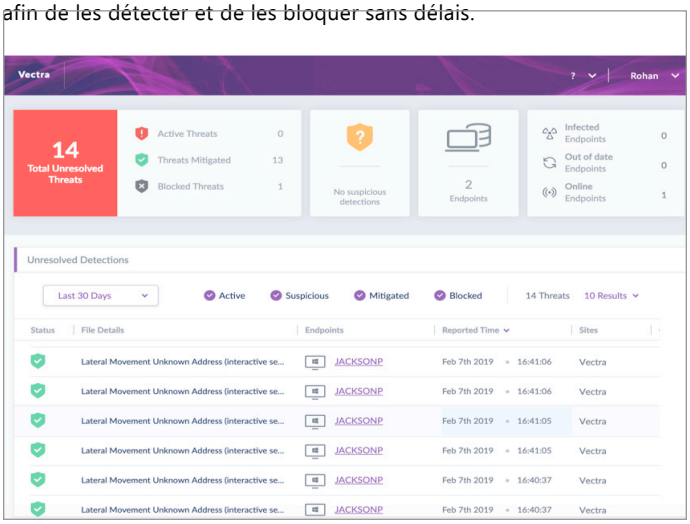
En déployant des solutions NDR et EDR, les équipes de sécurité acquièrent des données précieuses. Ces informations peuvent être exploitées en cas d'incident ou au cours d'opérations de Threat Hunting, pour répondre aux questions suivantes :

- L'appareil a-t-il commencé à présenter des comportements suspects après avoir communiqué avec un autre appareil potentiellement piraté ?
- Quels services et protocoles ont été utilisés ?
- Quels autres dispositifs ou comptes peuvent être impliqués ?
- Un autre système a-t-il contacté la même adresse IP externe de Command-and-Control ?
- Le compte utilisateur a-t-il été utilisé de manière inattendue sur d'autres appareils ?

Ensemble, ces deux solutions permettent d'apporter des réponses rapides et coordonnées, couvrant l'ensemble des actifs de l'entreprise. Elles permettent d'optimiser l'efficacité des opérations de sécurité et de réduire les délais de traitement, dans un contexte où chaque minute compte.

Technologie et produit Sentinel One

Les outils traditionnels de sécurité des postes de travail sont truffés de problèmes. Ils présentent des angles morts, proposent des détections basées sur des signatures facilement contournables et nécessitent souvent des mises à jour constantes ou des cycles d'exécution programmés. Ces solutions ne permettent pas de voir ou de stopper les cybermenaces avancées. Sentinel One surveille en permanence l'activité de tous les postes de travail et analyse les données en temps réel, pour procéder à l'identification automatique des cybermenaces, afin de les détecter et de les bloquer sans délais.

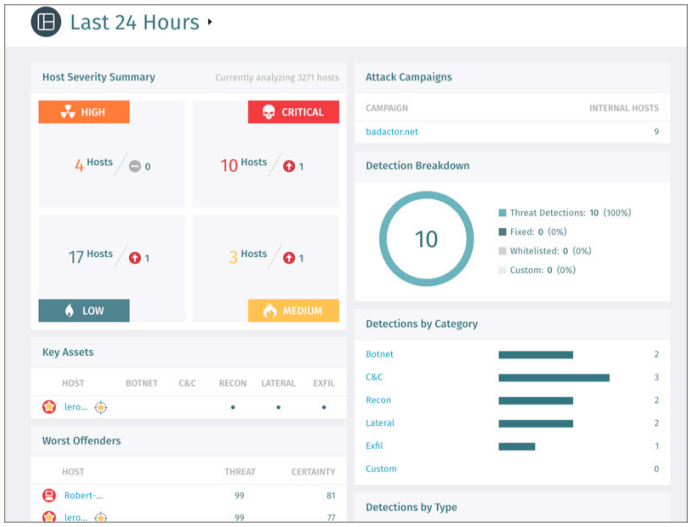


Une contextualisation optimale, à partir du réseau et des postes de travail

Lorsqu'une menace est détectée, les équipes de sécurité accèdent instantanément à des informations précises, afin de mener les opérations de vérification et d'investigation qui s'imposent.

Les identificateurs d'hôte et autres données fournies par Sentinel One s'affichent automatiquement sur l'interface utilisateur de Vectra Cognito. Elles viennent ainsi compléter les informations de détection réseau fournies par Vectra.

Sentinel One incorpore les détections et les scores de risque de Vectra. Ces données sont ensuite corrélées avec les détections internes relatives à des comportements suspects, uniquement visibles depuis l'hôte lui-même. Les fonctionnalités de réponse automatisées, reposant sur des politiques de sécurité, permettent ensuite d'éliminer rapidement les menaces.



Avec cette solution mixte, Vectra et Sentinel One créent un nouveau type de cyberdéfense. En combinant la science des données et le machine learning, Vectra fournit une détection des menaces intra-réseau, et apporte ainsi un niveau de défense supplémentaire au sein de l'infrastructure de sécurité. Grâce à une IA comportementale sophistiquée, Sentinel One permet une réponse automatisée instantanée permettant d'empêcher les communications entre un appareil infecté et un serveur C&C. Vous êtes ainsi protégé contre un plus large spectre des cybermenaces.

Vectra, société d'intelligence artificielle, transfigure la cybersécurité. Sa plateforme Cognito est le moyen le plus rapide et efficace de détecter et répondre aux cyberattaques : elle réduit par 34 le volume de travail des équipes de sécurité. Cognito effectue un Threat Hunting en temps réel, en analysant les métadonnées du trafic réseau, les logs pertinents et les événements cloud. Cet outil détecte les activités suspectes enregistrées sur le cloud, au sein des datacenters, sur les appareils et les objets connectés. Cognito corrèle les menaces, hiérarchise les hôtes en fonction des risques et fournit une contextualisation détaillée pour permettre une réponse efficace. Cette plateforme s'intègre à la sécurisation des postes de travail, des NAC et des firewalls, pour automatiser les confinements et fournir une base solide aux recherches menées via les SIEM et les outils forensiques.

SentinelOne offre une protection autonome des postes de travail grâce à un agent unique capable de prévenir, de détecter et de répondre aux attaques menées via les principaux vecteurs de piratage. Particulièrement intuitive, la plateforme S1 permet aux clients de recourir à l'IA pour éliminer automatiquement les menaces en temps réel, à la fois en environnement on-premise et sur le cloud. Il s'agit de la seule solution à offrir une visibilité totale sur les réseaux, directement depuis les postes de travail.

VECTRA®
Security that thinks®

E-mail : info@vectra.ai
Téléphone : +1 408-326-2020 vectra.ai