Solution EDR de Cybereason

ATTÉNUEZ LES MENACES AVANT QU'ELLES NE DEVIENNENT DES VIOLATIONS

PRINCIPAUX AVANTAGES

- **Comprenez** l'attaque dans son intégralité en quelques secondes
- **Contrôlez** votre environnement grâce à une visibilité complète et à des outils de résolution intégrés
- **Remédiez** aux menaces en un seul clic
- **Renforcez** votre équipe de sécurité existante
- **Etablissez** des règles de détection dans Windows, macOS, Linux, Android et iOS

Une Détection En Quelques Secondes Pour Une Résolution En Quelques Minutes

Étant donné que les attaquants développent des méthodes de plus en plus sophistiquées, il est d'autant plus difficile de faire face aux menaces en toute confiance. Lors d'un incident, chaque seconde compte. Les équipes de sécurité et informatique sont souvent ralenties en raison du manque de contexte des alertes, du travail manuel excessif requis pour les investigations, d'une capacité limitée d'automatisation et de l'effort de longue haleine requis pour résoudre le problème. Ces défis provoquent souvent une incertitude accrue et beaucoup de fatigue.

La solution EDR de Cybereason regroupe toutes les informations relatives à chaque attaque en une représentation visuelle unique appelée Malop (opération malveillante). Chaque Malop organise les données pertinentes sur les attaques dans une interface graphique interactive, facile à lire, en indiquant une chronologie complète de l'attaque, la circulation des malwares entre les processus et les utilisateurs, ainsi que toutes les communications entrantes et sortantes pour les machines affectées. Les mesures de résolution peuvent être automatisées ou exécutées à distance en un clic.

Intervenez Instantanément Pour Remédier Aux Attaques À Grande Échelle

La Cybereason Defense Platform permet aux analystes, quel que soit leur niveau de compétence, d'explorer rapidement les détails d'une attaque, sans élaborer de requêtes complexes et en intervenant directement, qu'il s'agisse d'examiner un Malop ou de remédier sur les machines affectées. Grâce à la solution EDR de Cybereason, les analystes peuvent appliquer une série complète de mesures de résolution, qu'il s'agisse de l'isolation des machines, de l'élimination de processus ou de la suppression de mécanismes de persistance, tout cela dans une interface conviviale et intuitive.

Traquez Les Menaces De Façon Proactive

La solution EDR de Cybereason permet de traquer les menaces de façon proactive et automatisée afin de détecter les indicateurs de compromissions et de comportements cachés dans votre environnement. Notre plateforme avancée de traque des menaces transforme les données non filtrées des terminaux en renseignements exploitables et fournit une interface utilisateur intuitive pour les investigations sans syntaxe permettant aux analystes des niveaux 1 et 2 d'être aussi efficaces qu'un analyste de niveau 3.

Détectez Les Attaques Sophistiquées

La Cybereason Defense Platform collecte des données à partir de tous les terminaux dans tous les systèmes d'exploitation. Elle utilise des analyses comportementales et une corrélation des données au niveau de tous les terminaux pour donner un aperçu complet de l'activité dans votre environnement. La corrélation des données en temps réel sur toutes les machines vous permet de prendre en compte les informations les plus critiques concernant une attaque avec un taux faible de faux positifs. Cela se traduit par des données détaillées, corrélées et enrichies provenant de chaque terminal afin de réduire les manquements de détection potentielles.

Une Suite Complète De Mesures De Résolution

Grâce aux outils de résolution de la Cybereason Defense Platform, les analystes peuvent appliquer une série complète de mesures de résolution, qu'il s'agisse de l'isolation des machines ou de l'interruption de processus, afin de mettre fin à la persistance, tout cela à partir de l'interface conviviale de la console. La Cybereason Defense Platform dote les utilisateurs de de toutes les compétences nécessaires pour agir. Les analystes peuvent passer directement de l'examen d'une attaque à la remédiation de toutes les machines affectées en un clic, ce qui permet de gagner du temps et de créer un flux de travail plus efficace pour votre équipe.

La Sécurité Pour Tous

Grâce à la solution EDR de Cybereason, aucune compétence spéciale n'est requise. Les nouveaux membres de l'équipe peuvent examiner et résoudre les attaques sans faire appel à des membres de l'équipe expérimentés, et les équipes avancées peuvent tirer parti d'outils d'analyse et de résolution intuitifs pour passer d'une attaque à une autre, et consacrer ainsi plus de temps à la traque et moins au triage. L'IU intuitive de la solution EDR de Cybereason a été conçue pour améliorer l'efficacité des SOC en automatisant les tâches fréquentes et en permettant à leurs analystes de comprendre rapidement l'ampleur et les répercussions des menaces afin de pouvoir agir immédiatement

Systèmes d'exploitation recommandés pour la version 20.1 de l'agent de la plateforme Cybereason

WINDOWS	MAC	LINUX	ANDROID
Windows 10	macOS Catalina (10.15)	CentOS 8	Android 7
Windows 8.1	macOS Mojave (10.14)	CentOS 6 et 7	Android 8
Windows 8	macOS High Sierra (10.13)	RedHat Enterprise Linux 8	Android 9
Windows 7 SP1	macOS Sierra (10.12)	RedHat Enterprise Linux 6 et 7	Android 10
Windows 11, 21, H2		Oracle Linux 6 et 7	
Windows Server 2019	**IOS**	Debian 8 et 9	
Windows Server 2016	iOS 11	Amazon Linux AMI 2017.03	
Windows Server 2012 R2	iOS 12		
Windows Server 2012	iOS 13		
Windows Server 2008 R2 SP1			
Windows Server 2022			

Pour obtenir une liste complète des systèmes d'exploitation pris en charge, y compris les systèmes d'exploitation plus anciens tels que Windows XP, veuillez envoyer un e-mail à sales@cybereason.com

À PROPOS DE CYBEREASON :

Cybereason est le champion actuel des défenseurs contre les cyberattaques et offre une protection pérenne contre les attaques s'étendant des terminaux à l'ensemble de l'entreprise, et partout ailleurs. La Cybereason Defense Platform allie les meilleures compétences du secteur en matière de détection et de réponse (EDR et XDR), un antivirus de nouvelle génération (NGAV) ainsi qu'une traque proactive des menaces pour fournir une analyse contextualisée complète de chaque élément d'une opération malveillante (Malop). Résultat : les défenseurs peuvent mettre fin aux cyberattaques, au niveau des terminaux et partout ailleurs.

CYBEREASON.COM/DEMO