Secureworks

5 principales raisons de remplacer votre solution SIEM par Secureworks® Taegis™ XDR

Quels sont les attributs les plus problématiques de la solution SIEM pour votre organisation ?

1 Coûts

Taegis XDR		SIEM existant
Diminution du coût total de possession • La technologie Cloud native simplifie le déploiement, réduit les coûts de maintenance et accélère le délai de rentabilisation. • Les outils d'orchestration et d'investigation améliorent la productivité des SecOps • L'analytique de sécurité et l'intelligence sur les menaces appliquée réduisent les besoins de produits de sécurité complémentaires.	CONTRE	**Le coût total de possession reflète la complexité de possession de la solution SIEM** • La technologie sur site nécessite un investissement matériel en amont et au fil du temps. • Licences supplémentaires ou produits tiers requis pour les fonctionnalités d'orchestration. • Produits de sécurité supplémentaires et abonnement à des fonctionnalités d'intelligence sur les menaces requis pour générer des alertes plus fiables.

Augmentation de la désensibilisation aux alertes

70 % des analystes de sécurité enquêtent sur plus de 10 alertes par jour (augmentation par rapport à 45 % l'an dernier)[1]

78 % déclarent que l'examen de chaque alerte leur prend plus de 10 minutes (augmentation par rapport à 64 % l'an dernier)[1]

2 Temps et main d'œuvre

Taegis XDR		SIEM existant
Alertes fiables Réduisez le volume d'alertes sur les menaces en limitant le nombre de faux positifs grâce à une analytique puissante, pour que votre équipe ne voie que les informations qui comptent vraiment	VS	**Désensibilisation aux alertes** Détectez les volumes élevés d'alertes sans contexte fourni, lesquelles augmentent le risque de passer à côté de violations et demandent plus de temps et de ressources pour être analysées

La possibilité de détecter les menaces inconnues est une nécessité

80 % En moyenne, 80 % des violations réussies sont le fruit d'attaques « zero-day » nouvelles ou inconnues[2]

X2 Les attaques zero-day nouvelles ou inconnues devraient plus que doubler au cours de l'année à venir[3]

3 Détection des menaces

Taegis XDR		SIEM existant
Détection des menaces sophistiquées Reconnaissez vos adversaires en fonction de leur comportement, soyez alerté des menaces connues et émergentes et rendez rapidement compte si votre organisation a été victime dans le passé d'une attaque qui vient d'être découverte	VS	**Désensibilisation aux alertes** • Les indicateurs de compromission et les règles de base ne suffisent pas pour détecter les menaces modernes • Les moteurs d'analytique rajoutés augmentent la complexité et les coûts

Les professionnels de la sécurité révèlent les trois principales problématiques liées à la complexité des SIEM

38,5 % Administration[4]

32 % Déploiement[4]

29,5 % Opérations[4]

4 Complexité

Taegis XDR		SIEM existant
Simplifie les opérations de sécurité • Consolidation de plusieurs outils de sécurité en une solution unique de détection des menaces et de réponse • Comme XDR est une solution Cloud native, sa mise en œuvre ne demande que quelques jours, et non en plusieurs semaines	VS	**Conséquences de la complexité** Des experts en sécurité difficiles à recruter vont continuer à effectuer les tâches de gestion administrative des plates-formes requises par la plupart des solutions SIEM au lieu de se consacrer à la défense contre les menaces

5 Cas d'utilisation

Taegis XDR		SIEM existant
XDR a ajouté les cas d'utilisation des SIEM suivants : • Collecte et rétention des journaux • Recherche et création de rapports • Prise en charge des cas d'utilisation personnalisés **et d'autres qui ne sont pas couverts par les solutions SIEM existantes :** • Analyse du comportement de l'utilisateur • Surveillance de sécurité du Cloud • Investigations efficaces des incidents	VS	**Les principaux cas d'utilisation des SIEM sont notamment :** • Surveillance de sécurité de base • Surveillance de la conformité et du contrôle • Recherche et création de rapports de base À mesure que les volumes de données ont augmenté et sont passés dans le Cloud, la couverture des cas d'utilisation dans cet environnement par les outils SIEM est devenue de moins en moins efficace

[1] Enterprise Strategy Group | The Impact of XDR in the Modern SOC, nov 2020
[2] CriticalStart | The Impact of Security Alert Overload, 3e trimestre 2019
[3] Forrester Institute, The Third Annual Study on the State of Endpoint Security Risk, Janvier 2020
[4] SUMO Logic - SIEM Complexity Challenges Survey 2020

Découvrez XDR en action

Commencez par vous rendre sur le site secureworks.com pour en savoir plus

Secureworks