POINT DE VUE

Les étapes d'une stratégie SecOps efficace

Vers une cybersécurité proactive et résiliente

Résumé

Les équipes de sécurité font face à des menaces sophistiquées qui remettent en question leurs approches traditionnelles. Selon le rapport sur la pénurie d'expertise en cybersécurité de Fortinet, 53 % des organisations ont rapporté plus d'un million de dollars de pertes en 2023 suite à des violations de données. Elles ont donc besoin de solutions de sécurité plus efficaces.

Pour répondre aux besoins SecOps en constante évolution, disposer d'une stratégie de cybersécurité flexible est essentiel. Pour une sécurité proactive et résiliente, les organisations doivent d'abord miser sur des solutions fondamentales, puis mettre progressivement en place un centre d'opérations de sécurité (SOC) centralisé, piloté par l'IA et doté de capacités de réponse aux incidents. Ce parcours évolutif repose non seulement sur une gestion unifiée de la sécurité mais aussi sur l'assistance par l'IA, sur l'automatisation et sur une évaluation continue de la sécurité.

« Les attaques se produisent désormais à un rythme 43 % plus rapide qu'il y a six mois. Elles sont devenues plus ciblées, plus automatisées et exploitent davantage de canaux. »

Relever les défis de la cybersécurité grâce à l'IA et à l'automatisation

Accumuler les outils technologiques n'est pas toujours la solution la plus efficace. Chercher à connecter des produits disparates complique souvent le travail des équipes et surcharge les analystes. Les organisations ont besoin d'une gestion unifiée de la sécurité, capable d'offrir une vue d'ensemble claire et cohérente sur les menaces. Ainsi, elles peuvent mieux détecter et traiter les menaces dans des environnements variés. En simplifiant les processus, elles peuvent bénéficier d'une gestion plus efficace des ressources ; et en appliquant leurs politiques de manière uniforme, elles peuvent limiter les vulnérabilités exploitables par les pirates informatiques.

Les cybercriminels utilisent de plus en plus l'intelligence artificielle pour perfectionner leurs attaques. Il est donc essentiel que les organisations adoptent, elles aussi, des solutions basées sur l'IA. Ces technologies permettent d'analyser rapidement et avec précision d'immenses volumes de données pour détecter les menaces. Elles aident également à anticiper les attaques, pour une défense proactive renforcée. En automatisant les premières étapes de la réponse aux incidents, l'IA redonne du temps aux équipes humaines, qui peuvent se concentrer sur des problématiques plus complexes.

L'automatisation de la sécurité joue un rôle fondamental, compte tenu, notamment, de la pénurie de personnel qualifié. Face à l'avalanche d'alertes de sécurité, l'automatisation offre une gestion plus efficace : elle permet d'éliminer les faux positifs et donne la priorité aux menaces les plus sérieuses. Avec l'automatisation, les protocoles de réponse sont exécutés de manière systématique pour réduire les erreurs humaines ; et les opérations de sécurité peuvent se développer au rythme de la croissance de l'organisation.

En évaluant leur sécurité en continu, les organisations peuvent rapidement adapter leurs stratégies de sécurité aux menaces émergentes. Les évaluations régulières permettent d'allouer efficacement les ressources et d'optimiser la planification stratégique. Elles aident également à rester en conformité avec les normes juridiques et réglementaires en constante évolution, ce qui minimise les risques juridiques et financiers potentiels.

« Plus de 50 % des responsables informatiques considèrent que le manque de produits de cybersécurité de base est en partie responsable des violations de données. »

Vers une cybersécurité proactive et résiliente

Pour lutter efficacement contre les menaces en constante évolution, une approche SecOps structurée est essentielle. Pour détecter plus rapidement les menaces, les responsables en sécurité ont à leur disposition des technologies avancées telles que l'IA et le ML. Ils peuvent aussi mettre en place une surveillance centralisée pour accélérer les réponses aux attaques. Une stratégie SecOps efficace prend du temps. Il faut définir une approche qui puisse évoluer en même temps que les besoins en matière de sécurité. Le parcours SecOps peut être séquencé en trois étapes : opérations de sécurité essentielles, opérations de sécurité étendues et opérations de sécurité avancées. Chaque étape correspond à la résolution de problèmes spécifiques.

Opérations de sécurité essentielles

Pour commencer, les organisations doivent se doter d'une journalisation centralisée, de données analytiques, d'une automatisation de base et d'une assistance IA. Cette étape est cruciale. Les équipes manquent souvent de temps et de ressources pour élaborer et actualiser les cas d'utilisation. Elles doivent pouvoir assurer les opérations de sécurité de base sans perturber leurs opérations quotidiennes. Un outil prêt à l'emploi aux configurations minimales peut fournir toutes ces fonctions essentielles, sans compliquer les processus ou gaspiller les ressources.

Opérations de sécurité étendues

La deuxième étape consiste à s'appuyer sur des systèmes de gestion des informations et des événements de sécurité (SIEM) et des outils d'analyse du comportement des utilisateurs et des entités (UEBA). L'objectif, ici, est d'analyser plus finement les menaces. À mesure que les organisations se développent, elles ont besoin d'obtenir une vision plus précise de leur sécurité. Les solutions SIEM aident à gérer les multiples outils et sources de données diverses, tout en offrant une analyse renforcée grâce aux UEBA. Ce niveau d'analyse supplémentaire permet de détecter des menaces subtiles et sophistiquées en surveillant le comportement des utilisateurs et en identifiant des anomalies qui pourraient indiquer des menaces internes ou des identifiants compromis. Cette étape est particulièrement utile pour les équipes de sécurité spécialisées amenées à gérer un large éventail d'outils et de sources de données.

Opérations de sécurité avancées

Pour les organisations présentant des besoins accrus en sécurité, la troisième étape consiste à unifier l'orchestration, l'automatisation et la réponse (SOAR). L'intégration SOAR aux outils SecOps essentiels et étendus permet de gérer des incidents et des processus complexes. Elle facilite aussi la coordination des réponses au sein des infrastructures de sécurité sophistiquées. Grâce à l'automatisation des workflows complexes, l'approche SOAR garantit des réponses rapides et cohérentes face aux menaces, tout en facilitant la collaboration entre les différents outils de sécurité et les équipes, à grande échelle.

Renforcer les SecOps avec l'IA générative

L'intégration de l'IA générative (GenAI) à la cybersécurité représente une véritable révolution. L'IA générative interagit avec les autres solutions pour analyser de vastes ensembles de données, identifier des motifs et des anomalies, et offrir des éclairages approfondis sur les menaces potentielles. Elle vient aussi compléter les outils d'IA et de machine learning pour mieux automatiser les tâches répétitives, générer des rapports détaillés sur les menaces et suggérer des mesures proactives. Les opérations de sécurité deviennent donc à la fois réactives et prédictives, pour des détections et réponses plus rapides et plus précises. Avec l'aide de l'IA générative, les équipes peuvent se concentrer sur des tâches plus complexes liées à la résolution des menaces.

Amélioration progressive des SecOps

Le passage d'une gestion SecOps de base à une gestion avancée repose sur une progression stratégique, en accord avec les besoins de sécurité croissants de l'organisation. Ce parcours progressif et structuré permet d'établir un environnement sécurisé et de poser les bases d'un SOC résilient, alimenté par l'IA, pour anticiper les menaces complexes et multiformes. En progressant de l'automatisation de base vers l'orchestration avancée, et en se dotant de capacités d'IA et d'IA générative, les organisations peuvent affronter efficacement les cybermenaces en constante évolution, pour avancer en toute confiance.

Conclusion

La conception d'un cadre SecOps efficace nécessite une approche sur mesure, qui prend en compte la taille des équipes, la diversité des outils et la maturité des processus. En évaluant ces facteurs, les organisations peuvent identifier la stratégie dont elles ont besoin pour renforcer efficacement leur sécurité. Une approche stratégique des SecOps peut considérablement améliorer la capacité d'une organisation à détecter, répondre et neutraliser les menaces, et ce, qu'il s'agisse d'analyses et de gestion centralisée pour les équipes réduites, de SIEM pour les équipes de sécurité dédiées ou encore de SOAR pour les opérations avancées. En améliorant et en adaptant continuellement leur environnement SecOps, les organisations peuvent mieux appréhender les cybermenaces d'aujourd'hui.

[1] 2024 Cybersecurity Skills Gap Global Research Report, Fortinet, 20 juin 2024.

[2] Douglas Jose Pereira dos Santos, Key Findings from the 2H 2023 FortiGuard Labs Threat Report, Fortinet, 6 mai 2024.

[3] 2024 Cybersecurity Skills Gap Global Research Report, Fortinet, 20 juin 2024.

24 août 2024 18h47 PM / 2824932-0-0-EN