CROWDSTRIKE

Checklist d'appel d'offres pour le SIEM nouvelle génération

Optimisez votre SOC pour améliorer les performances en sécurité, simplifier la gestion et réduire les coûts

Les clés de la modernisation de votre SOC

Les solutions traditionnelles de gestion des événements et des informations de sécurité (SIEM) ont failli à leur mission dans les SOC. Elles sont trop lentes, complexes et onéreuses, et ont été conçues pour une époque où les quantités de données, la rapidité des cyberadversaires et la sophistication des cyberattaques étaient bien inférieures à ce qu'elles sont aujourd'hui. Alors que votre entreprise devient plus complexe, les sources de données se multiplient. Par conséquent, votre équipe doit investir davantage de temps et de ressources dans la configuration et la maintenance de votre SIEM. Elle tente d'obtenir des résultats de sécurité efficaces au lieu de se concentrer sur la prévention des compromissions.

Dans le cadre de la modernisation de votre SOC, vous avez besoin d'une solution plus rapide, plus facile à déployer et plus rentable que les anciens SIEM. Cette nouvelle approche doit centraliser la détection, l'investigation et la réponse aux cybermenaces au sein d'une seule plateforme cloud native et IA native pour garantir une efficacité et une rapidité inégalées. En éliminant les silos et en consolidant les outils, vous pouvez réduire la complexité et les coûts. De plus, vous pouvez surmonter l'un des principaux défis liés aux anciens SIEM, à savoir l'intégration des données, car vos données de sécurité essentielles sont déjà présentes dans la plateforme. CrowdStrike Falcon® Next-Gen SIEM a été conçu pour offrir une visibilité totale et pour vous aider à relever les défis posés par les anciens SIEM. Développé par CrowdStrike, Falcon Next-Gen SIEM répond à notre mission fondamentale : bloquer les compromissions.

Cette checklist pour appels d'offres (RFP) vous donne le point de vue de CrowdStrike sur le SIEM de nouvelle génération. Son but est de vous aider à identifier le meilleur fournisseur de solutions ou partenaire pour répondre à vos défis de sécurité spécifiques et aligner vos initiatives avec vos objectifs stratégiques. Elle constitue un point de départ pour lancer votre processus d'évaluation, comparer les différents fournisseurs et, en fin de compte, prendre une décision éclairée pour faire évoluer votre SOC.

Liste de contrôle des exigences

Architecture et déploiement du SIEM

- [ ] Modèle de déploiement SaaS (Software-as-a-Service) pour maintenir les coûts à un niveau bas et simplifier les mises à niveau
- [ ] Architecture véritablement cloud native, et non un simple processus de réhébergement, pour assurer l'évolutivité
- [ ] Options de déploiement multitenant pour les entreprises complexes et géographiquement dispersées
- [ ] Contrôle d'accès granulaire basé sur les rôles (RBAC) pour restreindre les autorisations et les accès
- [ ] Processus de migration fluide avec un calendrier raisonnable, des attentes claires et des options de configuration personnalisées
- [ ] Options de formation flexibles pour aider votre équipe à monter en puissance, à gagner en confiance et à maîtriser le fonctionnement de votre nouveau déploiement SIEM
- [ ] Maintenance sans effort et mises à jour régulières pour assurer la protection contre les cybermenaces émergentes et remédier à tout problème
- [ ] Services d'assistance fiables avec du personnel qualifié et des accords de niveau de service (SLA)
- [ ] Lancement régulier de nouvelles versions de produits axées sur l'efficacité et l'expérience utilisateur

Intégration, traitement et gestion des données

- [ ] Solution qui s'appuie sur les données existantes de haute fidélité des endpoints et qui s'étend aux données de tiers pour une visibilité totale
- [ ] Variété de connecteurs de données disponibles prêts à l'emploi dans les domaines de l'informatique et de la sécurité
- [ ] Analyseurs de données facilement disponibles pour garantir l'accès et la lisibilité des données en vue d'une analyse plus rapide
- [ ] Collecteur d'événements HTTP (HEC) pour intégrer facilement des sources de données personnalisées et utiliser des analyseurs pour normaliser l'ingestion de données
- [ ] Gestion unifiée des collecteurs de logs pour surveiller facilement l'ingestion et l'intégrité des données
- [ ] Fonctionnalités API robustes pour assurer un partage sécurisé et facile des données avec les applications

- [ ] Prise en charge des pipelines de données pour déplacer efficacement les données et les acheminer vers votre SIEM
- [ ] Ingestion de données à l'échelle du pétaoctet pour une intégration rapide des nouvelles données dans votre SIEM
- [ ] Ingestion sans index pour accélérer la recherche de données et utiliser efficacement les ressources disponibles
- [ ] Normalisation des données pour divers champs d'information et formats de données afin d'accélérer l'analyse
- [ ] Analyseurs syntaxiques prêts à l'emploi pour convertir les données en un format structuré approprié
- [ ] Composants natifs de l'écosystème pour réduire les frictions liées à l'interopérabilité entre des outils cloisonnés. Par exemple :
    - [ ] Détection et réponse étendues (XDR)
    - [ ] Solution de détection et d'intervention sur les endpoints (EDR)
    - [ ] Recherche de menaces
    - [ ] Plateforme de protection des applications cloud native (CNAPP)
    - [ ] Détection et réponse aux cybermenaces liées à l'identité (ITDR)
    - [ ] Antivirus de nouvelle génération (NGAV)
    - [ ] Protection des données
    - [ ] Gestion de l'exposition
- [ ] Latence inférieure à une seconde pour traiter les logs, alerter sur les cybermenaces et rendre les données exploitables en temps réel
- [ ] Liberté d'accéder à vos données à tout moment, où que vous soyez et de la manière dont vous le souhaitez
- [ ] Plusieurs options de recherche (p. ex. recherche en texte libre ou recherche avancée de schémas par RegEx)
- [ ] Recherche évolutive et ultra rapide sur des jeux de données massifs et des volumes de données en constante expansion
- [ ] Langage de requête unique, multiplateforme et convivial pour surmonter les problèmes de saisie des données
- [ ] Tableau de bord de mesures pour évaluer l'intégrité du système, gérer les données et prévoir l'utilisation

Analyses

- [ ] Règles de corrélation précises et de haute fidélité, prêtes à l'emploi, continuellement testées et facilement adaptables
- [ ] Vaste gamme de détections prêtes à l'emploi couvrant divers aspects de la sécurité. Par exemple :
  - [ ] Endpoint
  - [ ] Cloud
  - [ ] Identité
  - [ ] Réseau
  - [ ] E-mail
  - [ ] Application
- [ ] Prise en charge du partage de détection ouvert, tel que les règles Sigma, YARA et Snort
- [ ] Utilisation de l'IA générative (GenAI) pour répondre aux questions des analystes en langage simple, quel que soit leur niveau de compétences, et pour optimiser leur productivité avec des ressources réduites
- [ ] Analyse pilotée par l'IA générative pour passer au crible d'importants volumes de données et détecter les anomalies
- [ ] Analyses comportementales tirant parti de l'analyse statistique et du Machine Learning (ML) comme l'analyse du comportement des utilisateurs et des entités (UEBA)
- [ ] Détection des anomalies pilotée par l'IA pour identifier les utilisateurs anormaux en créant des groupes de pairs dynamiques
- [ ] Enrichissement contextuel grâce aux techniques et tactiques du cadre MITRE ATT&CK®
- [ ] Possibilité d'annoter et d'enrichir les données analysées avec des renseignements sur les menaces de haute qualité qui fournissent des indicateurs de compromission (IOC) assortis d'une cote de confiance, des informations contextuelles sur les logiciels malveillants, des détails sur les campagnes, ainsi que les noms des cyberadversaires
- [ ] Mappage de la couverture de détection au cadre ATT&CK de MITRE pour une action rapide
- [ ] Visualisations prêtes à l'emploi de tableaux de bord de cas d'usage populaires pour une visibilité rapide

- [ ] Tableaux de bord personnalisables et vues préférentielles pouvant s'appuyer sur n'importe quelle requête pour analyser et afficher vos données
- [ ] Inclusion de requêtes documentées pour le Threat Hunting (régulièrement mises à jour et extraites des derniers renseignements sur les cybermenaces) afin de détecter les cyberadversaires les plus avancés
- [ ] Workflow analytique pour opérationnaliser les processus de Threat Hunting et réduire les efforts manuels nécessaires pour créer, valider, ajuster et opérationnaliser les requêtes sur les cybermenaces
- [ ] Tests de détection et de protection effectués par des tiers, tels que les évaluations MITRE Engenuity ATT&CK et SE Labs, avec des résultats supérieurs

Enquêtes et réponses aux incidents

- [ ] Priorisation des alertes en fonction de leur gravité et de leur corrélation pour filtrer plus rapidement le bruit
- [ ] Gestion complète des incidents permettant la création d'un incident à partir d'une détection (ou d'un groupe de détections liées) afin d'assurer une organisation structurée des informations relatives à l'incident
- [ ] Fonctionnalités d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR) entièrement intégrées, incluses en standard
- [ ] Générateur de workflows intuitif et sans code pour automatiser une variété de cas d'usage et exécuter des tâches diverses
- [ ] Nombreux modèles de workflow prêts à l'emploi pour les cas d'usage courants, avec des options personnalisables
- [ ] Automatisation des workflows en fonction d'événements ou de détections, planifiée ou à la demande
- [ ] Vaste écosystème d'intégration entre les domaines de sécurité et les outils informatiques, tels que les outils de gestion des services informatiques (ITSM)
- [ ] Intégration bidirectionnelle entre le SIEM et le SOAR pour assurer le partage des informations
- [ ] Capacité à automatiser les tâches d'investigation de routine telles que les corrélations et la collecte de données
- [ ] Intégration avec les meilleurs renseignements sur les menaces du secteur, axés sur les cyberadversaires, pour les rapports sur les menaces, les profils de menaces, les rapports techniques, l'analyse antimalware en environnement sandbox et les rapports quotidiens sur les indicateurs de compromission relatifs aux cybermenaces émergentes
- [ ] Renseignements sur les cybermenaces couvrant plus de 230 cyberadversaires différents, basés sur l'analyse de plusieurs billions d'événements liés aux endpoints par semaine

- [ ] Visualisations d'investigation avancées, telles que des vues graphiques pour comprendre les relations entre les entités et les parcours des cyberattaquants, ainsi que des vues chronologiques pour comprendre la progression d'une cyberattaque
- [ ] Collaboration en temps réel pour les analystes afin de partager et de documenter les résultats
- [ ] Possibilité d'envoyer des notifications via votre méthode de communication préférée, par exemple des e-mails ou Slack
- [ ] Possibilité d'automatiser n'importe quel cas d'usage grâce à de nombreuses actions de réponse prédéfinies
- [ ] Intégration étroite de l'agent EDR pour exécuter n'importe quelle action sur l'endpoint, comme l'isolation du réseau, la mise en quarantaine, la réponse en temps réel, etc.
- [ ] Intégration avec n'importe quelle API basée sur HTTP pour créer des actions en low code ou en full code
- [ ] Accès aux données historiques pour permettre des cas d'usage de Threat Hunting sur de grands volumes de données
- [ ] Possibilité de créer des applications personnalisées pour déployer davantage de cas d'usage et combler les lacunes des produits
- [ ] Possibilité de personnaliser votre plateforme d'opérations de sécurité existante avec une plateforme d'applications low code (LCAP) intégrée et conçue à cet effet
- [ ] Moteur d'investigation optimisé par l'IA générative permettant aux analystes de générer des résumés d'incidents en langage clair et de recommander les étapes suivantes

Rétention des données, confidentialité et conformité

- [ ] Options flexibles de rétention des données à long terme pour des données toujours accessibles et toujours à haut débit
- [ ] Fonctionnalités de création de rapports planifiés à la demande pour les audits et la conformité et possibilité de conserver un système d'enregistrement de la sécurité
- [ ] Fonctionnalités de masquage et de dissimulation pour répondre aux exigences en matière de protection et de confidentialité

Services

- [ ] Couverture de la détection et de l'intervention managées (MDR) dirigée par des experts 24 heures sur 24 et 7 jours sur 7 sur les vecteurs d'attaques stratégiques : endpoints, cloud, identité et données de tiers, comme les e-mails, la détection et l'intervention managées (NDR), les pare-feu, etc.
- [ ] Équipe d'analystes de sécurité certifiés ayant une connaissance approfondie des technologies
- [ ] Renseignements intégrés sur les menaces pour un contexte complet des cyberattaques et les derniers indicateurs de compromission
- [ ] Threat Hunting proactif assuré par une équipe d'experts pour découvrir les techniques d'attaque sophistiquées des cyberadversaires
- [ ] Correction chirurgicale des cybermenaces de bout en bout, y compris le nettoyage complet à l'état d'origine sans processus coûteux de restauration d'une image système ni temps d'arrêt
- [ ] Garantie de prévention des compromissions sans charge administrative pour couvrir les coûts d'une éventuelle brèche dans un environnement protégé
- [ ] Efficacité de la couverture de la détection des cyberattaques, comme indiqué dans les évaluations ATT&CK de MITRE
- [ ] Reconnaissance du secteur et des analystes pour valider la protection assurée par des experts à l'aide des services
- [ ] Services de mise en œuvre et d'exploitation pour accélérer la configuration et le réglage
- [ ] Large écosystème de prestataires de services pour un soutien stratégique supplémentaire

Tarifs

- [ ] Tarification transparente et simple à comprendre pour permettre une planification prévisible
- [ ] Tarification flexible qui s'adapte à l'augmentation du volume de données sans grever votre budget

Profil du fournisseur

- [ ] Maturité en matière de cybersécurité validée par les clients et les analystes
- [ ] Expertise dans la gestion de clients de tailles variées, répartis dans différentes régions géographiques et différents secteurs, pour optimiser l'immunité communautaire
- [ ] Portefeuille de produits et services de cybersécurité étroitement intégrés qui stimule l'innovation produit, renforce l'expertise et diversifie les offres disponibles

- [ ] Vision à long terme pour tirer parti des tendances du secteur et feuille de route agile pour faciliter l'exécution
- [ ] Récompenses et certifications pertinentes décernées par des cabinets d'analystes et le secteur de la sécurité, attestant de bonnes performances dans les domaines suivants : renseignements sur les menaces, sécurité des endpoints, protection des workloads dans le cloud, détection et intervention managées, et gestion des vulnérabilités basée sur les risques

CrowdStrike se positionne à la pointe des opérations de sécurité IA natives, notamment grâce à une plateforme SOC intégrée. Celle-ci permet aux clients de bloquer les compromissions, d'assurer la conformité et de relever tous les défis de sécurité auxquels ils sont confrontés. En intégrant l'EDR, les renseignements sur les menaces et les services d'experts les plus performants du secteur à toutes les sources de données, Falcon Next-Gen SIEM vous assure une visibilité et une protection complètes.

Votre équipe obtiendra des informations immédiates grâce aux données clés dont vous avez besoin et qui sont déjà intégrées. Un nombre croissant de connecteurs de données libère le potentiel de l'ensemble de votre écosystème. Vous pourrez ainsi consacrer plus de temps à la lutte contre les cybermenaces et moins de temps à l'intégration des données.

Conçu autour d'une expérience moderne d'analyste de sécurité, Falcon Next-Gen SIEM amplifie la vitesse et l'efficacité de la réponse à incident afin que vous puissiez rapidement éradiquer les cyberadversaires tout en réduisant les coûts du SOC.

Demandez une démo
pour découvrir Falcon Next-Gen SIEM en action

À propos de CrowdStrike

CrowdStrike (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une intelligence artificielle de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, le renseignement sur les cybermenaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike : We stop breaches.