CROWDSTRIKE

Angebots-Checkliste für SIEM-Systeme der nächsten Generation

Entwickeln Sie Ihr SOC weiter, um überragende Sicherheitsergebnisse zu erzielen, Komplexität zu reduzieren und die Kosten zu senken

So modernisieren Sie Ihr SOC

Herkömmliche SIEM-Lösungen (Sicherheitsinformations- und Ereignismanagement) sind im SOC gescheitert. Sie sind zu langsam, zu komplex und kostspielig und wurden für ein Zeitalter entwickelt, in dem Datenvolumen, Geschwindigkeit des Angreifers und Raffinesse der Angriffe nur einen Bruchteil dessen ausmachten, was sie heute sind. Da Ihr Unternehmen immer komplexer wird, nehmen auch die Datenquellen immer weiter zu, sodass Ihr Team mehr Zeit und Ressourcen für die Einrichtung, Wartung und den Versuch aufwenden muss effektive Sicherheitsergebnisse aus Ihrem SIEM zu extrahieren, anstatt Kompromittierungen zu verhindern.

Auf dem Weg zur Weiterentwicklung Ihres SOC benötigen Sie eine Lösung, die um ein Vielfaches schneller, einfacher zu implementieren und kostengünstiger ist als herkömmliche SIEMs. Dieser neue Ansatz soll die gesamte Bedrohungserkennung, -untersuchung und -reaktion in einer cloudnativen, KI-nativen Plattform vereinen und so für unübertroffene Effizienz und Geschwindigkeit sorgen. Durch das Aufbrechen von Silos und die Konsolidierung von Tools können Sie Komplexität und Kosten senken. Darüber hinaus können Sie eine der größten Herausforderungen älterer SIEMs meistern – die Einbindung von Daten –, da sich Ihre wichtigsten Sicherheitsdaten bereits in der Plattform befinden. CrowdStrike Falcon® Next-Gen SIEM wurde entwickelt, um Ihnen vollständige Transparenz zu bieten und Sie bei der Bewältigung der Herausforderungen zu unterstützen, die mit herkömmlichen SIEMs verbunden sind. Falcon Next-Gen SIEM wurde von CrowdStrike entwickelt, um unsere zentrale Mission erfolgreich umzusetzen: Kompromittierungen zu verhindern.

Diese Angebots-Checkliste informiert Sie über CrowdStrikes Sichtweise auf die nächste Generation von SIEM-Systemen, um Ihnen dabei zu helfen, den besten Lösungsanbieter oder -partner zu finden, der Ihre individuellen Sicherheitsherausforderungen löst und mit Ihren Zielen im Einklang steht. Sie bietet Ihnen einen Ausgangspunkt, um Ihren Evaluierungsprozess zu starten, Anbieter zu vergleichen und letztendlich eine fundierte Entscheidung zur Weiterentwicklung Ihres SOC zu treffen.

Anforderungs-Checkliste

SIEM-Architektur und -Bereitstellung

- [ ] Software-as-a-Service (SaaS)-Bereitstellungsmodell, um Kosten niedrig zu halten und Upgrades zu vereinfachen
- [ ] Eine echte cloudnative Architektur – kein Lift-and-Shift-Prozess – zur Gewährleistung der Skalierbarkeit
- [ ] Mulit-Tenant-Bereitstellungsoptionen für komplexe und geografisch verteilte Organisationen
- [ ] Granulare rollenbasierte Zugriffssteuerung (role-based access control, RBAC) zur Einschränkung von Berechtigungen und Zugriff
- [ ] Reibungsloser Migrationsprozess mit angemessenem Zeitrahmen, klaren Erwartungen und maßgeschneiderten Konfigurationsoptionen
- [ ] Flexible Schulungsoptionen, mit denen Ihr Team die neue SIEM-Bereitstellung in Betrieb nehmen, üben und dann problemlos bedienen kann
- [ ] Mühelose Wartung und zeitnahe Updates zum Schutz vor zukünftigen Bedrohungen und zur Behebung von Problemen
- [ ] Zuverlässige Support-Services mit qualifiziertem Personal und Service-Level-Agreement-Bedingungen (SLA)
- [ ] Regelmäßige Veröffentlichung neuer Produkte, bei denen Effizienz und Benutzererfahrung im Vordergrund stehen

Datenübernahme, -verarbeitung und -verwaltung

- [ ] Aufbauend auf vorhandenen High-Fidelity-Endgerätedaten und erweitert um Daten von Drittanbietern für vollständige Transparenz
- [ ] Vielzahl von sofort einsatzbereiten Datenkonnektoren für IT- und Sicherheitsdomänen
- [ ] Leicht verfügbare Datenparser, um den Zugriff und die Lesbarkeit für eine schnellere Analyse zu gewährleisten
- [ ] HTTP-Ereignissammler (HTTP Event Collector, HEC) zur einfachen Einbindung benutzerdefinierter Datenquellen und Nutzung von Parsern zur Normalisierung der Datenerfassung
- [ ] Einheitliches Flottenmanagement für Log-Sammler zur einfachen Überwachung der Datenerfassung und Leistung
- [ ] Robuste API-Funktionen für einen sicheren und einfachen Datenaustausch mit Anwendungen

- [ ] Unterstützung für Datenpipelines, um Daten effizient zu übertragen und in Ihr SIEM zu leiten
- [ ] Datenerfassung im Petabyte-Bereich, um neue Daten schnell in Ihr SIEM zu integrieren
- [ ] Indexfreie Erfassung zur Beschleunigung der Datenabfrage und effizienten Nutzung verfügbarer Ressourcen
- [ ] Datennormalisierung für verschiedene Informationsfelder und Datenformate für eine schnellere Analyse
- [ ] Sofort einsatzbereite Parser zur Umwandlung von Daten in ein geeignetes Format zur Strukturierung von Daten
- [ ] Native Ökosystemkomponenten zur Verringerung von Interoperabilitätskonflikten zwischen isolierten Tools, wie z. B.:
    - [ ] Erweiterte Erkennung und Reaktion (XDR)
    - [ ] Endpunktbasierte Detektion und Reaktion (EDR)
    - [ ] Bedrohungsanalysen
    - [ ] Cloud-Native Application Protection Platform (cloudnative Plattform für Anwendungsschutz, CNAPP)
    - [ ] Identity Threat Detection and Response (ITDR)
    - [ ] Virenschutz der nächsten Generation (NGAV)
    - [ ] Datenschutz
    - [ ] Schwachstellenverwaltung
- [ ] Latenzzeiten von unter einer Sekunde, um Protokolle zu verarbeiten, vor Bedrohungen zu warnen und Daten in Echtzeit verwertbar zu machen
- [ ] Freiheit, auf Ihre Daten zuzugreifen, egal wann, wo und auf welche Art und Weise
- [ ] Mehrere Suchoptionen, von der Freitextsuche bis zur erweiterten RegEx-Suche nach Mustern
- [ ] Blitzschnelle, skalierbare Suche in großen Datenbeständen und wachsenden Datenmengen
- [ ] Einheitliche, plattformübergreifende Abfragesprache, die benutzerfreundlich ist, um die Einstiegshürde zu überwinden
- [ ] Metrik-Dashboard zur Bewertung des Systemzustands, zur Datenverwaltung und zur Vorhersage der Nutzung

Analysen

- [ ] Sofort einsatzbereite, sinnvolle und hochpräzise Korrelationsregeln, die kontinuierlich getestet werden und einfach anzupassen sind
- [ ] Große Auswahl an sofort einsatzbereiten Erkennungsfunktionen für verschiedene Sicherheitsbereiche, wie z. B.:
  - [ ] Endgeräte
  - [ ] Cloud
  - [ ] Identität
  - [ ] Netzwerke
  - [ ] E-Mail
  - [ ] Anwendung
- [ ] Unterstützung für die gemeinsame Nutzung offener Erkennungsdaten, wie z. B. Sigma-, YARA- und Snort-Regeln
- [ ] Einsatz generativer KI (GenAI), damit Analysten aller Qualifikationsstufen mit weniger mehr erreichen können, indem Fragen von Analysten in normaler Sprache beantwortet werden
- [ ] GenAI-gestützte Analyse, um große Datenmengen zu durchsuchen und Anomalien zu erkennen
- [ ] Verhaltensanalysen, die statistische Analysen und maschinelles Lernen (ML) nutzen, wie z. B. die Analyse des Verhaltens von Benutzern und Entitäten (User and Entity Behavior Analytics, UEBA)
- [ ] KI-gesteuerte Anomalieerkennung zur Identifizierung abnormaler Benutzer durch die Erstellung dynamischer Peer-Gruppen
- [ ] Kontextuelle Anreicherung mit Techniken und Taktiken aus dem MITRE ATT&CK®-Framework
- [ ] Fähigkeit, analysierte Daten zu kennzeichnen und mit hochwertiger Threat Intelligence anzureichern, die vertrauenswürdige Indikatoren für Kompromittierungen (Indicators of Compromise, IOCs), Malware-Kontext, Kampagneninformationen und Namen von Angreifern bereitstellt
- [ ] Erfassung der Abdeckung anhand des MITRE ATT&CK-Framework für schnelles Handeln
- [ ] Sofort einsatzbereite, beliebte Dashboard-Visualisierungen für Anwendungsszenarien für eine übersichtliche Darstellung auf einen Blick

- [ ] Anpassbare Dashboards und bevorzugte Ansichten, die auf jeder Abfrage aufbauen können, um Ihre Daten zu analysieren und anzuzeigen
- [ ] Einbeziehung dokumentierter Threat Hunting-Abfragen, die regelmäßig aktualisiert und aus den neuesten Threat Intelligence-Einblicken extrahiert werden, um die fortschrittlichsten Angreifer zu entdecken
- [ ] Analyse-Workflow zur Operationalisierung des Threat Hunting-Prozesses und zur Reduzierung des manuellen Aufwands für die Erstellung, Validierung, Abstimmung und Operationalisierung von Bedrohungsabfragen
- [ ] Unabhängige Tests der Erkennungs- und Schutzfunktionen, wie z. B. MITRE Engenuity ATT&CK und SE Labs-Bewertungen, mit hervorragenden Ergebnissen

Untersuchung und Behebung von Zwischenfällen

- [ ] Priorisierung von Warnmeldungen nach Schweregrad und Gruppierung, um die Flut an Informationen schneller zu sichten
- [ ] Umfassendes Vorfallmanagement, das die Erstellung von Zwischenfällen aus einer Erkennung oder einer Gruppe verwandter Erkennungen ermöglicht, um Ereignisinformationen zu organisieren
- [ ] Integrierte Sicherheitsorchestrierung, Automatisierung und Reaktionsfähigkeit (Security Orchestration, Automation and Response, SOAR) als Standardfunktionen
- [ ] Intuitiver, codierungsfreier Workflow-Builder zur Automatisierung beliebiger Anwendungsszenarien und zur Ausführung beliebiger Aufgaben
- [ ] Viele sofort einsatzbereite Workflow-Vorlagen für beliebte Anwendungsszenarien mit anpassbaren Optionen
- [ ] Workflow-Automatisierung, die auf der Grundlage von Ereignissen oder Erkennungen ausgelöst wird
- [ ] Umfassendes Integrations-Ökosystem über Sicherheitsdomänen und IT-Tools hinweg, wie z. B. IT-Service-Management-Tools (ITSM)
- [ ] Bidirektionale Integration zwischen SIEM und SOAR zur Gewährleistung des Informationsaustauschs
- [ ] Möglichkeit zur Automatisierung routinemäßiger Untersuchungsaufgaben wie Korrelationen und Datenerfassung
- [ ] Integration mit branchenführender, angreiferorientierter Threat Intelligence für Bedrohungsberichte, Bedrohungsprofile, technische Berichte, Malware-Sandbox und tägliche IOC-Berichte über zukünftige Bedrohungen
- [ ] Threat Intelligence, die über 230 verschiedene Angreifer umfasst und auf der Analyse von Billionen von Endgeräte-bezogenen Ereignissen pro Woche basiert

- [ ] Fortgeschrittene Untersuchungsvisualisierungen, wie z. B. Diagrammansichten zum Verständnis von Entitätsbeziehungen und Angreiferpfaden, und Zeitachsenansichten zum Verständnis des Verlaufs eines Angriffs
- [ ] Echtzeit-Zusammenarbeit für Analysten zum Teilen und Dokumentieren von Ergebnissen
- [ ] Möglichkeit, Benachrichtigungen über Ihre bevorzugte Kommunikationsmethode zu senden, z. B. per E-Mail oder Slack
- [ ] Flexibilität zur Automatisierung jedes Anwendungsfalls mit zahlreichen vorgefertigten Reaktionsmaßnahmen
- [ ] Enge Integration von EDR-Agenten (Endgeräte-Erkennung und Reaktion) zur Ausführung beliebiger Aktionen auf dem Endgerät, wie z. B. Netzwerkisolierung, Quarantäne, Echtzeitreaktion und mehr
- [ ] Integration mit jeder HTTP-basierten API zur Erstellung von Aktionen in Low-Code oder Full-Code
- [ ] Zugriff auf historische Daten, um Anwendungsszenarien für das Threat Hunting in großen Datenmengen zu ermöglichen
- [ ] Möglichkeit, benutzerdefinierte Anwendungen zu erstellen, um mehr Anwendungsszenarien bereitzustellen und Produktlücken zu schließen
- [ ] Möglichkeit, Ihre vorhandene Sicherheitsbetriebsplattform mit einer speziell entwickelten, integrierten Low-Code-Anwendungsplattform (LCAP) anzupassen
- [ ] GenAI-gestützte Untersuchungs-Engine, die es Analysten ermöglicht, Zusammenfassungen von Zwischenfällen in normaler Sprache mit empfohlenen nächsten Schritten zu erstellen

Datenspeicherung, Datenschutz und Compliance

- [ ] Flexible langfristige Datenspeicherung Option für Daten, die immer zugänglich und immer mit hoher Geschwindigkeit verfügbar sind
- [ ] Geplante On-Demand-Berichterstattungsfunktionen für Audits und Compliance sowie die Möglichkeit, ein Sicherheitsprotokoll zu führen
- [ ] Funktionen zur Maskierung und Obfuskation, um Datenschutz- und Schutzanforderungen zu erfüllen

Services

- [ ] Rund um die Uhr von Experten verwaltete Erkennung und Reaktion (Managed Detection and Response, MDR) für kritische Angriffsvektoren: Endgeräte, Cloud, Identitäten und Daten von Drittanbietern, wie E-Mail, Netzwerkerkennung und -reaktion (Network Detection and Response, NDR), Firewall und mehr
- [ ] Zertifiziertes Team von Sicherheitsanalysten mit fundierten technischen Kenntnissen
- [ ] Integrierte Threat Intelligence für den vollständigen Angriffskontext und die neuesten IOCs
- [ ] Proaktives, von Menschen geführtes Threat Hunting, um ausgeklügelte Angreifertaktiken aufzudecken
- [ ] Umfassende, chirurgisch genaue Behebung von Bedrohungen, einschließlich vollständiger Wiederherstellung des Originalzustands ohne kostspieliges Re-Imaging oder Ausfallzeiten
- [ ] Unbürokratische Garantie zur Verhinderung von Kompromittierungen, die die Kosten einer Kompromittierung abdeckt, sollte es jemals in einer geschützten Umgebung zu einer solchen kommen
- [ ] Wirksamkeit der Angriffserkennungsabdeckung gemäß MITRE ATT&CK-Bewertungen
- [ ] Anerkennung durch Branche und Analysten zur Validierung von fachkundigem Schutz durch Services
- [ ] Implementierungs- und betriebliche Services zur Beschleunigung der Konfiguration und Abstimmung
- [ ] Umfangreiches Ökosystem von Service-Anbietern für zusätzliche strategische Unterstützung

Preis

- [ ] Transparente und leicht verständliche Preisgestaltung für eine bessere Planbarkeit
- [ ] Flexible Preisgestaltung, die sich an wachsende Datenmengen anpasst, ohne das Budget zu sprengen

Anbieterprofil

- [ ] Reife der Cybersicherheit mit Validierung durch Kunden und Analysten
- [ ] Expertise in der Betreuung zahlreicher Kunden unterschiedlicher Größe, geografischer Regionen und Branchen, um von Herdenimmunität zu profitieren
- [ ] Eng integriertes Portfolio an Produkten und Services für Cybersicherheit, das Produktinnovationen fördert, Fachwissen vertieft und die Auswahlmöglichkeiten erweitert

- [ ] Langfristige Vision, um von Branchentrends zu profitieren, und eine sich schnell entwickelnde Roadmap zur Unterstützung der Umsetzung

- [ ] Relevante Auszeichnungen und Zertifizierungen von Analystenfirmen und der Sicherheitsbranche, darunter Führungspositionen in den Bereichen Threat Intelligence, Endgerätesicherheit, Schutz der Cloud-Auslastung, verwaltete Erkennung und Reaktion sowie risikobasiertes Schwachstellenmanagement

CrowdStrike ist Vorreiter bei der Zukunft KI-nativer Sicherheitsmaßnahmen und bietet eine vollständige SOC-Plattform, die Kunden dabei unterstützt, Kompromittierungen zu stoppen, Compliance zu erreichen und alle Sicherheitsherausforderungen zu bewältigen. Falcon Next-Gen SIEM erweitert die branchenweit führenden EDR (Endgeräte-Erkennung und Reaktion)-, Threat Intelligence- und Expertenservices auf alle Datenquellen und bietet Ihnen vollständige Transparenz und Schutz.

Ihr Team erhält mit den bereits integrierten Schlüsseldaten unmittelbare Einblicke. Eine wachsende Anzahl von Datenkonnektoren erschließt die Leistungsfähigkeit Ihres gesamten Ökosystems, sodass Sie mehr Zeit für den Kampf gegen Bedrohungen und weniger Zeit für die Datenerfassung aufwenden können.

Falcon Next-Gen SIEM wurde von Grund auf für moderne Sicherheitsanalysten entwickelt und erhöht die Geschwindigkeit und Effizienz der Reaktion auf Zwischenfälle. So können Sie Angreifer schnell aufspüren und gleichzeitig die SOC-Kosten reduzieren.

Fordern Sie eine Demo an: →
Sehen Sie Falcon Next-Gen SIEM in Aktion

Über CrowdStrike

CrowdStrike (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich Cybersicherheit, hat mit der weltweit fortschrittlichsten cloudnativen Plattform zum Schutz kritischer Bereiche des Unternehmensrisikos – Endgeräte und Cloud-Workloads, Identität und Daten – die moderne Sicherheit neu definiert.

Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde für den Cloud-Einsatz entwickelt und nutzt einen einzigen schlanken Agenten, um schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite zu ermöglichen.

CrowdStrike: We stop breaches.