CROWDSTRIKE

Next-Gen SIEM RFP Checklist

Evolve your SOC to achieve superior security outcomes, reduce complexity and slash costs

The Keys to Modernizing Your SOC

Legacy security information and event management (SIEM) solutions have failed the SOC. They are too slow, complex and costly, and they were designed for an age when data volumes, adversary speed and attack sophistication were a fraction of what they are today. As your organization becomes more complex, data sources continue to proliferate, forcing your team to spend more time and resources setting up, maintaining and trying to extract effective security outcomes from your SIEM rather than stopping breaches.

As you embark on your journey to evolve your SOC, you need a solution that's orders of magnitude faster, easier to deploy and more cost-effective than legacy SIEMs. This new approach should unify all threat detection, investigation and response in one cloud-native, AI-native platform for unrivaled efficiency and speed. By breaking down silos and consolidating tools, you can slash complexity and costs. Plus, you can overcome one of the toughest challenges of legacy SIEMs — getting data in — because your key security data is already in the platform. CrowdStrike Falcon® Next-Gen SIEM was built to empower you to achieve full visibility and help you dispel the challenges associated with legacy SIEMs. Falcon Next-Gen SIEM was built by CrowdStrike to deliver on our core mission: stopping the breach.

This request for proposal (RFP) checklist provides you with CrowdStrike's point of view on next-gen SIEM to help you identify the best solution vendor or partner to solve your unique security challenges and align with your goals and objectives. It provides you with a starting point to kick off your evaluation process, compare vendors and ultimately make an informed decision to evolve your SOC.

Requirements Checklist

SIEM Architecture and Deployment

- □ Software-as-a-service (SaaS) deployment model to keep costs low and simplify upgrades
- □ Truly cloud-native architecture — not a lift-and-shift process — to ensure scalability
- □ Multi-tenancy deployment options for complex and geographically spread organizations
- □ Granular role-based access control (RBAC) to restrict permissions and access
- □ Smooth migration process with reasonable timeline, clear expectations and customized configuration options
- □ Flexible training options to help your team ramp up, gain confidence and achieve mastery to operate your new SIEM deployment
- □ Effortless maintenance and timely updates to protect against emerging threats and address any issues
- □ Reliable support services with skilled personnel and service-level agreement (SLA) terms
- □ Regular cadence of new product releases that prioritize efficiency and user experience

Data Onboarding, Processing and Management

- □ Built upon existing high-fidelity endpoint data and extended to third-party data for full visibility
- □ Variety of data connectors available out-of-the-box across IT and security domains
- □ Readily available data parsers to ensure access and readability for faster analysis
- □ HTTP event collector (HEC) to easily onboard custom data sources and leverage parsers to normalize data ingest
- □ Unified fleet management for log collectors to easily monitor data ingest and health
- □ Robust API capabilities to ensure secure, easy data sharing with applications

- □ Support for data pipelines to move data efficiently and route it into your SIEM
- □ Petabyte-scale data ingestion to onboard new data into your SIEM fast
- □ Index-free ingestion to speed up data retrieval and efficiently use available resources
- □ Data normalization for different information fields and data formats for faster analysis
- □ Out-of-the-box parsers to convert data into a suitable format to structure data
- □ Native ecosystem components to reduce interoperability friction across siloed tools, such as:
  - □ Extended detection and response (XDR)
  - □ Endpoint detection and response (EDR)
  - □ Threat intelligence
  - □ Cloud-native application protection platform (CNAPP)
  - □ Identity threat detection and response (ITDR)
  - □ Next-generation antivirus (NGAV)
  - □ Data protection
  - □ Exposure management
- □ Sub-second latency to process logs, alert on threats and make data actionable in real time
- □ Freedom to access your data whenever, wherever and in any way you need it
- □ Multiple search options, from free-text search to advanced RegEx search for patterns
- □ Lightning-fast, scalable search across large datasets and growing data volumes
- □ Single, cross-platform query language that is user-friendly to overcome the entry barrier
- □ Metrics dashboard to assess system health, manage data and predict usage

Analytics

- □ Sensible, high-fidelity correlation rules — available out-of-the-box — that are continuously tested and easy to tune
- □ Wide range of ready-to-use detections across various security domains, such as:
  - □ Endpoint
  - □ Cloud
  - □ Identity
  - □ Network
  - □ Email
  - □ Application
- □ Support for open detection sharing, such as Sigma, YARA and Snort rules
- □ Use of generative AI (GenAI) to allow analysts of all skill levels to do more with less by answering analyst questions in plain language
- □ GenAI-powered analysis to sift through large data volumes and detect anomalies
- □ Behavioral analytics that leverage statistical analysis and machine learning (ML) like user and entity behavior analytics (UEBA)
- □ AI-driven anomaly detection to identify abnormal users by creating dynamic peer groups
- □ Contextual enrichment with techniques and tactics from the MITRE ATT&CK® framework
- □ Ability to tag and enrich parsed data with high-quality threat intelligence that provides confidence-rated indicators of compromise (IOCs), malware context, campaign information and adversarial names
- □ Detection coverage mapping against the MITRE ATT&CK framework for quick action
- □ Out-of-the-box popular use case dashboard visualizations for at-a-glance visibility

- □ Customizable dashboards and preferential views that can build on any query to analyze and display your data
- □ Inclusion of documented threat hunting queries — regularly updated and extracted from the latest threat intelligence insights — to discover the most advanced adversaries
- □ Analytics workflow to operationalize threat hunting processes and reduce the manual effort needed to create, validate, tune and operationalize threat queries
- □ Third-party testing of detection and protection capabilities, such as MITRE Engenuity ATT&CK and SE Labs evaluations, with superior results

Incident Investigation and Response

- □ Alert prioritization based on severity and grouping to sift through the noise faster
- □ Comprehensive incident management that enables incident creation from a detection — or a group of related detections — to keep incident information organized
- □ Fully integrated security orchestration, automation and response (SOAR) capabilities included standard
- □ Intuitive, no-code workflow builder to automate any use case and carry out any task
- □ Many out-of-the-box workflow templates for popular use cases with customizable options
- □ Workflow automation triggered based on events or detections, scheduled or on demand
- □ Broad integrations ecosystem across security domains and IT tools, such as IT service management (ITSM) tools
- □ Bidirectional integration between SIEM and SOAR to ensure information sharing
- □ Ability to automate routine investigative tasks such as correlations and data collection
- □ Integration with industry-leading, adversary-focused threat intelligence for threat reports, threat profiles, technical reports, malware sandbox and daily IOC reports on emerging threats
- □ Threat intelligence spanning over 230 distinct adversaries based on analysis of trillions of endpoint-related events per week

- □ Advanced investigation visualizations, such as graph views to understand entity relationships and attacker paths, and timeline views to understand the progression of an attack
- □ Real-time collaboration for analysts to share and document findings
- □ Ability to send notifications via your preferred communication method, such as email or Slack
- □ Flexibility to automate any use case with numerous prebuilt response actions
- □ Tight EDR agent integration to execute any action on the endpoint, such as network isolation, quarantine, real-time response and more
- □ Integration with any HTTP-based API to create actions in low-code or full-code
- □ Historical data access to enable threat hunting use cases across large volumes of data
- □ Ability to create custom applications to deploy more use cases and bridge product gaps
- □ Ability to customize your existing security operations platform with a purpose-built, integrated low-code application platform (LCAP)
- □ GenAI-powered investigation engine that allows analysts to generate summaries of incidents in plain language with recommended next steps

Data Retention, Privacy and Compliance

- □ Flexible long-term data retention options for data that is always accessible and always high-speed
- □ Scheduled on-demand reporting capabilities for audits and compliance and the ability to keep a security system of record
- □ Masking and obfuscation capabilities to meet privacy and protection requirements

Services

- □ 24/7 expert-led managed detection and response (MDR) coverage across critical attack vectors: endpoint, cloud, identity and third-party data, such as email, network detection and response (NDR), firewall and more
- □ Certified security analyst team with in-depth technology knowledge
- □ Integrated threat intelligence for full attack context and the latest IOCs
- □ Proactive human-led threat hunting to uncover sophisticated adversary tradecraft
- □ Surgical threat remediation in true end-to-end fashion, including full cleanup to original state without costly reimaging or downtime
- □ Breach prevention warranty without red tape to cover the costs of a breach should one ever occur within a protected environment
- □ Efficacy of attack detection coverage as denoted by MITRE ATT&CK evaluations
- □ Industry and analyst recognition to validate expert-driven protection through services
- □ Implementation and operational services to accelerate configuration and tuning
- □ Wide ecosystem of service providers for additional strategic support

Pricing

- □ Transparent and simple-to-understand pricing to enable predictability in planning
- □ Flexible pricing that adapts to growing data volumes without breaking the bank

Vendor Profile

- □ Cybersecurity maturity with validation from customers and analysts
- □ Expertise managing numerous customers that vary in size, geographic regions and industries to benefit from community immunity
- □ Tightly integrated cybersecurity product and services portfolio that fosters product innovation, deepens expertise and widens offering choices

☐ Long-term vision to capitalize on industry trends and a fast-developing roadmap to support execution

☐ Relevant awards and certifications from analyst firms and the security industry, including leadership in threat intelligence, endpoint security, cloud workload protection, managed detection and response, and risk-based vulnerability management

CrowdStrike is pioneering the future of AI-native security operations by offering a complete SOC platform to help customers stop breaches, achieve compliance and solve any security challenge they face. Extending the industry's most dominant EDR, threat intelligence and expert services to all data sources, Falcon Next-Gen SIEM gives you full visibility and protection.

Your team will get immediate insights with the key data you need already built in. A growing set of data connectors unlocks the power of your entire ecosystem so you can spend more time fighting threats and less time onboarding data.

Built from the ground up around a modern security analyst experience, Falcon Next-Gen SIEM amplifies the speed and efficiency of incident response so you can swiftly root out adversaries while slashing SOC costs.

Request a demo →
to see Falcon Next-Gen SIEM in action

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise
risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.