CROWDSTRIKE

Lista de verificación de solicitud de propuestas para la SIEM de nueva generación

Transforma tu centro de operaciones de seguridad para conseguir excelentes resultados de seguridad y reducir la complejidad y los costes

Claves para modernizar tu centro de operaciones de seguridad

Las soluciones de gestión de eventos e información de seguridad (SIEM) tradicionales no están a la altura de las necesidades de los centros de operaciones de seguridad (SOC). Son demasiado lentas, complejas y costosas, y fueron diseñadas para una época en la que los volúmenes de datos, la velocidad de los ciberdelincuentes y la sofisticación de los ataques eran una fracción de lo que son hoy. A medida que tu organización se vuelve más compleja, las fuentes de datos siguen proliferando, por lo que tu equipo se ve obligado a dedicar más tiempo y recursos a la configuración, el mantenimiento y a intentar conseguir resultados de seguridad eficaces de tu SIEM, en lugar de concentrarse en detener las brechas.

Cuando te embarcas en un proyecto de mejora de tu SOC, necesitas una solución que sea más rápida, más fácil de desplegar y más rentable que las soluciones SIEM tradicionales. Este nuevo enfoque debe aunar la detección, la investigación y la respuesta a las amenazas en una única plataforma de IA nativa de la nube para alcanzar una velocidad y eficiencia sin igual. Al acabar con los silos y unificar las herramientas, podrás reducir la complejidad y los costes. Además, podrás superar uno de los retos más difíciles de las soluciones SIEM tradicionales (la introducción de los datos) gracias a que tus datos clave de seguridad ya estarán en la plataforma. CrowdStrike Falcon® Next-Gen SIEM ha sido concebido para que puedas lograr una visibilidad total y superar las dificultades asociadas a las soluciones SIEM tradicionales. Con esta solución, CrowdStrike puede cumplir su misión primordial: detener las brechas.

Esta lista de verificación para solicitudes de propuestas presenta el punto de vista de CrowdStrike sobre la SIEM de nueva generación para que puedas identificar al proveedor o socio con la mejor solución que te permita resolver tus problemas de seguridad particulares en consonancia con tus metas y objetivos. Te ofrecemos un punto de partida con el que poner en marcha tu proceso de evaluación, comparar a los proveedores y, en última instancia, tomar decisiones fundamentadas para desarrollar tu centro de operaciones de seguridad.

Lista de verificación de requisitos

Arquitectura y despliegue de la SIEM

- [ ] Modelo de implementación de software como servicio (SaaS) para contener los costes y simplificar las actualizaciones
- [ ] Arquitectura realmente nativa de la nube (no un proceso de realojamiento) para garantizar la escalabilidad
- [ ] Opciones de despliegue multiempresa para organizaciones complejas distribuidas geográficamente
- [ ] Control de acceso pormenorizado basado en roles para restringir los permisos y el acceso
- [ ] Proceso de migración sencillo con plazos razonables, expectativas claras y opciones de configuración personalizadas
- [ ] Opciones de formación flexibles para que tu equipo pueda redoblar esfuerzos, ganar confianza y dominar la implementación de tu nueva SIEM
- [ ] Mantenimiento sin esfuerzo y actualizaciones oportunas para protegerte de las nuevas amenazas y afrontar cualquier problema
- [ ] Servicios de soporte fiables con personal cualificado y condiciones establecidas en acuerdos del nivel de servicio
- [ ] Lanzamientos periódicos de nuevos productos para priorizar la eficiencia y la experiencia del usuario

Incorporación, procesamiento y gestión de datos

- [ ] Crecimiento a partir de datos precisos sobre endpoints, ampliados con datos de terceros, para conseguir una visibilidad total
- [ ] Amplia variedad de conectores de datos preconfigurados para su uso en ámbitos informáticos y de seguridad
- [ ] Analizadores de datos fácilmente disponibles para garantizar el acceso y la legibilidad y ofrecer análisis más rápidos
- [ ] Recopilador de eventos HTTP para incorporar fácilmente fuentes de datos personalizados y aprovechar los analizadores para normalizar la ingesta de datos
- [ ] Gestión uniforme de la flota para que los recopiladores de archivos de registro controlen fácilmente la ingesta y el estado de los datos
- [ ] Capacidades robustas de API para compartir datos con aplicaciones de forma fácil y segura

- [ ] Soporte para la canalización de datos que permita transferir la información de forma eficiente y dirigirla a tu sistema SIEM
- [ ] Capacidad de ingesta de varios petabytes de datos para incorporar rápidamente nuevos datos a tu SIEM
- [ ] Ingesta sin índices para acelerar la recuperación de los datos y usar eficientemente los recursos disponibles
- [ ] Normalización de los datos para distintos campos de información y formatos que permita ofrecer análisis más rápidos
- [ ] Analizadores preconfigurados para convertir los datos en un formato adecuado para su estructuración
- [ ] Componentes nativos del ecosistema para reducir los problemas de interoperabilidad en herramientas aisladas como:
    - [ ] Detección y respuesta ampliadas (XDR)
    - [ ] Detección y respuesta para endpoints (EDR)
    - [ ] Inteligencia sobre amenazas
    - [ ] Plataforma de protección de aplicaciones nativas de la nube
    - [ ] Detección y respuesta de amenazas de identidad
    - [ ] Antivirus de nueva generación
    - [ ] Protección de datos
    - [ ] Gestión de la exposición a riesgos
- [ ] Latencia inferior a un segundo para procesar los registros, alertar de las amenazas y obtener datos procesables en tiempo real
- [ ] Libertad para acceder a tus datos en el momento, lugar y forma que necesites
- [ ] Múltiples opciones de búsqueda que van desde la búsqueda sin texto a la búsqueda avanzada de patrones mediante expresiones regulares
- [ ] Búsqueda escalable ultrarrápida en grandes conjuntos de datos y volúmenes de datos en aumento
- [ ] Un único lenguaje de consulta sencillo y multiplataforma para superar la barrera de entrada
- [ ] Panel con parámetros para evaluar el estado del sistema, gestionar los datos y predecir el uso

Análisis

- [ ] Reglas de correlación lógicas de gran calidad (listas para su uso) que se someten a pruebas continuamente y son fáciles de ajustar
- [ ] Amplia variedad de detecciones listas para su uso en diversos ámbitos de la seguridad como:
  - [ ] Endpoint
  - [ ] Nube
  - [ ] Identidad
  - [ ] Red
  - [ ] Correo electrónico
  - [ ] Aplicación
- [ ] Soporte para un uso compartido abierto de las detecciones, como las reglas Sigma, YARA y Snort
- [ ] Uso de IA generativa para que analistas de todos los niveles puedan hacer más con menos respondiendo a las preguntas de los analistas en un lenguaje sencillo
- [ ] Análisis mediante IA generativa para filtrar grandes volúmenes de datos y detectar anomalías
- [ ] Análisis de comportamiento que aprovechan estadísticas y capacidades de aprendizaje automático, como los análisis de comportamiento de los usuarios y las entidades
- [ ] Detección de anomalías con IA para identificar a usuarios inusuales creando grupos de peers dinámicos
- [ ] Enriquecimiento contextual con técnicas y estrategias del marco MITRE ATT&CK®
- [ ] Capacidad de etiquetar y enriquecer los datos analizados con inteligencia sobre amenazas de gran calidad que ofrece indicadores de compromiso según el nivel de confianza, el contexto del malware, la información de la campaña y los nombres de los ciberdelincuentes
- [ ] Mapeo de las detecciones cubiertas con el marco MITRE ATT&CK para una actuación rápida
- [ ] Visualización de casos de uso populares para mostrar información de forma rápida

- [ ] Paneles personalizables y vistas preferentes basadas en los análisis realizados y los datos consultados
- [ ] Inclusión de consultas de Threat Hunting documentadas, las cuales se actualizan y extraen periódicamente de la última información de inteligencia sobre amenazas, para descubrir a los ciberdelincuentes más avanzados
- [ ] Flujo de trabajo de análisis para poner en funcionamiento procesos de Threat Hunting y reducir el esfuerzo manual necesario para crear, validar, ajustar y poner en marcha las consultas de amenazas
- [ ] Pruebas externas de las capacidades de detección y protección, como las evaluaciones MITRE Engenuity ATT&CK y de SE Labs, con excelentes resultados

Investigación y respuesta a incidencias

- [ ] Priorización de las alertas en función de la gravedad y el tipo para filtrar el ruido con mayor rapidez
- [ ] Gestión integral de incidencias que permite crear incidencias desde la detección, o un grupo de detecciones relacionadas, para mantener organizada la información sobre las incidencias
- [ ] Capacidades de organización, automatización y respuesta de seguridad (SOAR) totalmente integradas (estándar incluido)
- [ ] Creador de flujos de trabajo intuitivos sin código para automatizar cualquier caso de uso y realizar cualquier tarea
- [ ] Múltiples plantillas de flujos de trabajo listas para casos de uso populares con opciones personalizables
- [ ] Automatización del flujo de trabajo que se activa con eventos o detecciones, tanto programados como bajo demanda
- [ ] Amplio ecosistema de integraciones en ámbitos de seguridad y herramientas informáticas, como las herramientas de gestión de servicios informáticos
- [ ] Integración bidireccional entre SIEM y SOAR para garantizar el uso compartido de información
- [ ] Capacidad de automatizar tareas de investigación rutinarias como las correlaciones y la recopilación de datos
- [ ] Integración con la mejor inteligencia sobre amenazas y ciberdelincuentes para acceder a informes de amenazas, perfiles de amenazas, informes técnicos, entornos de prueba de malware e informes diarios sobre los indicadores de compromiso de las nuevas amenazas
- [ ] Inteligencia sobre amenazas que abarca más de 230 ciberdelincuentes distintos, basada en el análisis de billones de eventos relacionados con endpoints a la semana

- [ ] Visualizaciones avanzadas de las investigaciones, como gráficos, para entender las relaciones entre las entidades y las rutas de los atacantes, así como visualizaciones temporales para conocer la evolución de un ataque
- [ ] Colaboración en tiempo real para que los analistas compartan y documenten sus hallazgos
- [ ] Capacidad de envío de notificaciones a través del método de comunicación preferente, como el correo electrónico o Slack
- [ ] Flexibilidad a la hora de automatizar cualquier caso de uso con numerosas medidas de respuesta predefinidas
- [ ] Integración estrecha con los agentes de EDR para ejecutar cualquier acción en el endpoint, como el aislamiento de la red, la cuarentena, la respuesta en tiempo real y mucho más
- [ ] Integración con cualquier API HTTP para crear acciones con o sin codificación
- [ ] Acceso a los datos históricos para habilitar casos de uso de Threat Hunting en grandes volúmenes de datos
- [ ] Capacidad de crear aplicaciones personalizadas para implementar más casos de uso y reducir las lagunas de los productos
- [ ] Capacidad de personalización de tu plataforma de operaciones de seguridad existente con una plataforma de aplicaciones integradas con poco código diseñada con un objetivo específico
- [ ] Motor de investigación mediante IA generativa con el que los analistas pueden generar resúmenes de incidencias en un lenguaje sencillo con recomendaciones para los siguientes pasos

Conservación de datos, privacidad y cumplimiento normativo

- [ ] Opciones flexibles de conservación a largo plazo para que los datos sean accesibles rápidamente en todo momento
- [ ] Capacidades de generación de informes programados bajo demanda para las auditorías y el cumplimiento normativo, así como para mantener un sistema de registro sobre seguridad
- [ ] Capacidades de enmascaramiento y ofuscación para cumplir los requisitos de privacidad y protección

Servicios

- [ ] Detección y respuesta gestionadas por expertos 24/7 en vectores de ataque críticos: endpoints, nube, datos de identidad y de terceros como el correo electrónico, detección y respuesta de red, firewalls y mucho más
- [ ] Equipo de analistas de seguridad certificados con vastos conocimientos tecnológicos
- [ ] Inteligencia sobre amenazas integrada para ofrecer un contexto completo sobre los ataques y los últimos indicadores de compromiso
- [ ] Threat Hunting proactivo guiado por humanos para descubrir técnicas de ataque sofisticadas
- [ ] Corrección integral de las amenazas con gran precisión que incluya una limpieza total para restablecer el estado original, sin formateos ni interrupciones que supongan un alto coste
- [ ] Garantía de prevención de brechas sin trámites excesivos para cubrir los costes de una brecha en caso de que se produzca una dentro de un entorno protegido
- [ ] Eficacia de la cobertura de detección de ataques, de conformidad con las evaluaciones MITRE ATT&CK
- [ ] Identificación de los sectores y analistas para validar la protección guiada por expertos a través de los servicios
- [ ] Servicios operativos y de implementación para acelerar la configuración y los ajustes
- [ ] Amplio ecosistema de proveedores de servicios para ofrecer un apoyo estratégico extra

Precio

- [ ] Precios transparentes y fáciles de entender para disfrutar de predictibilidad en la planificación
- [ ] Precios flexibles que se adaptan a los crecientes volúmenes de datos sin ser excesivos

Perfil de los proveedores

- [ ] Madurez en términos de ciberseguridad con validación de clientes y analistas
- [ ] Experiencia en la gestión de numerosos clientes de distintos tamaños, regiones y sectores para beneficiarse de la inmunidad de rebaño
- [ ] Cartera de productos y servicios de ciberseguridad bien integrados que promueve la innovación, profundiza en los conocimientos y amplía la oferta

- [ ] Visión a largo plazo para capitalizar las tendencias del sector y desarrollar rápidamente un plan que ayude en la ejecución

- [ ] Premios y certificaciones relevantes de analistas y del sector de la seguridad, incluido el liderazgo en la inteligencia sobre amenazas, la seguridad de endpoints, la protección de la carga de trabajo de la nube, la detección y respuesta gestionadas, y la gestión de vulnerabilidades en función de los riesgos

CrowdStrike está dando forma al futuro de las operaciones de seguridad con IA nativa al proporcionar una plataforma completa de SOC donde los clientes pueden detener las brechas, cumplir las normativas y superar cualquier desafío de seguridad. Falcon Next-Gen SIEM amplía funcionalidades líderes del sector para llevar los servicios de EDR, inteligencia sobre amenazas y asesoramiento especializado a cualquier fuente de datos, y así ofrecer una visibilidad y una protección totales.

Tu equipo obtendrá información práctica al instante con los datos clave que necesitas. Un conjunto de conectores de datos en aumento explota todo el potencial de tu ecosistema al completo para que puedas dedicar más tiempo a combatir las amenazas y menos tiempo a incorporar datos.

Falcon Next-Gen SIEM, que se ha desarrollado para ofrecer una experiencia moderna a los analistas, potencia la velocidad y la eficiencia de la respuesta a incidentes para que puedas erradicar rápidamente a los ciberdelincuentes al tiempo que reduces los gastos en SOC.

Solicita una demo
y descubre Falcon Next-Gen SIEM en acción

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa de la nube más avanzada del mundo para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, una protección y un rendimiento superiores, una menor complejidad y una rentabilidad inmediata.

CrowdStrike: We stop breaches.