Solicitud de Propuesta Software de Monitoreo y Análisis de Seguridad en la Nube

Índice

1. 1. Introducción y antecedentes

La organización necesita una solución integral de supervisión y análisis de la seguridad en la nube para mejorar la infraestructura de ciberseguridad. Esta RFP describe los requisitos de un sistema robusto que proporcione supervisión continua, detección de amenazas y análisis exhaustivo de eventos de seguridad en entornos en la nube.

1.1 Organización

- Infraestructura multicloud utilizando servicios de AWS, Azure y GCP
- Arquitectura de nube híbrida con centros de datos locales
- Operaciones globales en múltiples regiones geográficas
- Requisitos de implantación a escala empresarial
- Necesidades críticas de protección de datos

1.2 Postura actual en materia de seguridad

- Herramientas SIEM y de gestión de registros existentes
- Sistemas de supervisión de la seguridad de las redes
- Plataformas de protección de puntos finales
- Herramientas de seguridad nativas de la nube
- Retos actuales de la integración

1.3 Objetivos del proyecto

- Mejorar la visibilidad de la infraestructura de la nube y los eventos de seguridad
- Mejorar las capacidades de detección de amenazas y respuesta en todos los entornos
- Garantizar el cumplimiento de los reglamentos y normas del sector
- Optimice las operaciones de seguridad mediante análisis avanzados
- Implantar la automatización de la seguridad basada en IA
- Establecer una vigilancia exhaustiva de la seguridad

2. Objetivos del proyecto

2.1 Objetivos básicos de seguridad

- Implantar una supervisión exhaustiva de la seguridad en la nube en todos los entornos
- Establecer capacidades de detección de amenazas y respuesta en tiempo real
- Mejorar las funciones de control e información sobre el cumplimiento
- Mejorar la investigación de incidentes de seguridad y los análisis forenses
- Implantar análisis de seguridad avanzados
- Respuesta automatizada a las amenazas

2.2 Objetivos de análisis e inteligencia

- Implantación de análisis avanzados para la correlación de eventos de seguridad
- Implantar la detección y el análisis de amenazas basados en IA
- Establecer capacidades de seguridad predictivas
- Respuesta automatizada a incidentes de seguridad
- Desarrollar la integración de la inteligencia sobre amenazas
- Obtenga información práctica sobre seguridad

2.3 Objetivos operativos

- Agilice las operaciones de seguridad mediante la automatización
- Reduzca la fatiga de las alertas mediante la priorización inteligente de las mismas
- Mejorar la eficacia de las investigaciones de seguridad
- Habilitar funciones proactivas de caza de amenazas
- Mejorar los flujos de trabajo de respuesta a incidentes
- Optimizar la utilización de los recursos

3. 3. Alcance del trabajo

3.1 Servicios de implantación

- Evaluación completa del entorno y análisis de carencias
- Diseño y documentación de la arquitectura de la solución
- Integración con las herramientas y plataformas de seguridad existentes
- Procedimientos de prueba y validación del sistema
- Despliegue y optimización de la producción
- Transferencia de conocimientos y formación

3.2 Implementación de las funciones básicas

- Sistemas de recogida y agregación de datos

- Marcos de supervisión de la seguridad
- Sistemas de gestión de alertas
- Flujos de trabajo de respuesta a incidentes
- Herramientas de control del cumplimiento
- Plataformas de informes y análisis

3.3 Aplicación de análisis avanzados

- Despliegue de modelos de IA y aprendizaje automático
- Capacidades de análisis predictivo
- Sistemas de respuesta automática
- Integración de inteligencia sobre amenazas
- Aplicación del análisis del comportamiento
- Desarrollo de análisis personalizados

4. 4. Requisitos técnicos

4.1 Recogida e integración de datos

- Capacidades de ingestión de datos en múltiples nubes para AWS, Azure y GCP
- Agregación y normalización de registros en tiempo real
- Completo marco de integración de API
- Capacidad de tratamiento de datos en tiempo real
- Compatibilidad con fuentes de datos personalizadas
- Soluciones escalables de almacenamiento de datos

4.2 Vigilancia de la seguridad

- Supervisión continua de la postura de seguridad
- Análisis del tráfico de red en tiempo real
- Análisis avanzados del comportamiento de usuarios y entidades

- Configuración de la nube y supervisión del cumplimiento
- Localización de activos y seguimiento de inventarios
- Seguimiento y evaluación de la vulnerabilidad

4.3 Detección de amenazas

- Detección multicapa basada en firmas
- Análisis avanzados del comportamiento
- Detección de amenazas basada en el aprendizaje automático
- Identificación de amenazas de día cero
- Vigilancia de las amenazas internas
- Creación de reglas de detección personalizadas

5. 5. Requisitos funcionales

5.1 Funciones básicas

5.1.1 Recogida y agregación de datos

La recopilación y agregación eficaz de datos constituye la base de la supervisión de la seguridad en la nube. Céntrese en una cobertura completa de todos los activos de la nube y en la capacidad de normalizar datos de diversas fuentes para un análisis unificado.

Requisito	Subrequisito	S/N	Notas
Fuentes de recogida de datos	Recopilar datos de los registros de la nube		
	Recopilar datos del tráfico de red		
	Recopilar datos de la actividad del punto final		
	Integración de fuentes de datos personalizadas		

Visibilidad	Proporcionar una visibilidad completa del entorno de nube		
	Habilitar capacidades de supervisión en tiempo real		
	Análisis de datos históricos		
Tratamiento de datos	Normalización de datos en tiempo real		
	Permitir el filtrado y la clasificación de datos		
	Proporcionar capacidades de enriquecimiento de datos		

5.1.2 Detección de amenazas

La detección eficaz de amenazas requiere un enfoque multicapa que combine la detección basada en firmas, el análisis del comportamiento y el aprendizaje automático.

Requisito	Subrequisito	S/N	Notas
Métodos de detección	Aplicar la detección basada en firmas		
	Utilizar algoritmos de aprendizaje automático		
	Habilitar el análisis del comportamiento		
	Admite reglas de detección personalizadas		
Cobertura de amenazas	Identificar las amenazas conocidas		
	Detectar amenazas de día cero		
	Vigilancia de las amenazas internas		
	Seguimiento de las amenazas persistentes avanzadas		
Aplicación	Admite un enfoque de detección polifacético		

	Habilitar las funciones de caza de amenazas		
	Integrar la información sobre amenazas		

5.1.3 Respuesta a incidentes

La rapidez y eficacia de la respuesta a incidentes repercute directamente en su postura de seguridad. Céntrese en las capacidades de automatización manteniendo la supervisión humana de las decisiones críticas.

Requisito	Subrequisito	S/N	Notas
Acciones de respuesta	Activar el aislamiento del sistema		
	Bloqueo del tráfico		
	Permitir el inicio de una investigación		
	Ofrezca opciones de respuesta automática		
	Activar la reparación remota del sistema		
Libros de jugadas	Compatibilidad con guías de respuesta personalizadas		
	Automatización del flujo de trabajo		
	Proporcionar capacidades de prueba de libros de jugadas		
Documentación	Seguimiento del ciclo de vida de los incidentes		
	Mantener registros de auditoría de las respuestas		
	Generar informes de incidentes		

5.1.4 Priorización de alertas

La priorización inteligente de las alertas es crucial para gestionar eficazmente las operaciones de seguridad y reducir la fatiga de las alertas.

Requisito	Subrequisito	S/N	Notas
Sistema de prioridades	Establecer prioridades basadas en la criticidad		
	Considerar el valor de los activos en la priorización		
	Incluir el contexto de la amenaza en la evaluación		
	Soporte de reglas de priorización personalizadas		
Gestión de alertas	Filtrado inteligente de alertas		
	Enrutamiento y escalado de alertas		
	Correlación de alertas		
	Permitir categorías de alerta personalizadas		

5.1.5 Gestión de la conformidad

Para mantener el cumplimiento de la normativa y las normas de seguridad en todos los entornos de nube, es esencial disponer de funciones completas de gestión del cumplimiento.

Requisito	Subrequisito	S/N	Notas
Gestión de políticas	Aplicar las políticas de cumplimiento		
	Compatibilidad con múltiples marcos de cumplimiento		
	Habilitar la creación de políticas personalizadas		
	Proporcionar capacidades de comprobación de políticas		
Supervisión	Implantar un control continuo del cumplimiento		

	Seguimiento de las infracciones		
	Generar alertas de cumplimiento		
	Apoyo a las evaluaciones automatizadas		
Informes	Crear informes de cumplimiento automatizados		
	Mantener registros de auditoría detallados		
	Generación de informes personalizados		
	Activar informes programados		

5.1.6 Escalabilidad

Las soluciones de seguridad en la nube deben escalar eficientemente con el crecimiento de la organización, manteniendo al mismo tiempo el rendimiento y la fiabilidad en todas las regiones y entornos.

Requisito	Subrequisito	S/N	Notas
Ampliación de infraestructuras	Admite escalado horizontal		
	Activar la escala vertical		
	Gestión de mayores volúmenes de datos		
	Apoyo a la implantación multirregional		
Rendimiento	Mantener la velocidad de procesamiento bajo carga		
	Apoyo al procesamiento distribuido		
	Activar el equilibrio de carga		
Apoyo al crecimiento	Adaptarse al crecimiento de la organización		
	Modelo de licencia a escala		

	Apoyo a la integración de nuevas tecnologías		

5.1.7 Capacidades de integración

La perfecta integración con la infraestructura y las herramientas de seguridad existentes es crucial para mantener la eficacia operativa y una cobertura de seguridad completa.

Requisito	Subrequisito	S/N	Notas
Integración de herramientas de seguridad	Conexión con sistemas SIEM		
	Integración con plataformas EDR		
	Apoyo a la integración SOAR		
	Integración de la gestión de identidades		
Integración del desarrollo	Apoyo a la integración de canalizaciones CI/CD		
	Habilitar flujos de trabajo DevSecOps		
	Proporcionar interfaces de automatización		
Soporte API	Ofrecer API REST completas		
	Implementación de webhooks		
	Permitir el desarrollo de integraciones personalizadas		

5.1.8 Gestión de la privacidad de los datos

Una sólida gestión de la privacidad de los datos es esencial para proteger la información confidencial y mantener el cumplimiento de la normativa en los entornos de nube.

Requisito	Subrequisito	S/N	Notas

Protección de datos	Cifrado de datos en reposo		
	Activar el cifrado en tránsito		
	Admite enmascaramiento de datos		
	Habilitar la anonimización de datos		
Clasificación	Apoyo a la clasificación automatizada de datos		
	Habilitar reglas de clasificación personalizadas		
	Proporcionar informes de clasificación		
Control de acceso	Implantar un control de acceso basado en funciones		
	Activar el control de acceso basado en atributos		
	Apoyar el principio del menor privilegio		
	Seguimiento de las actividades de acceso a los datos		

5.2 Capacidades potenciadas por la IA

5.2.1 Asistentes de IA generativa

Los asistentes de IA deben mejorar las operaciones de seguridad mediante la interacción con el lenguaje natural y la automatización inteligente, manteniendo al mismo tiempo la precisión y la pertinencia.

Requisito	Subrequisito	S/N	Notas
Tratamiento del lenguaje	Gestión de consultas en lenguaje natural		
	Respuestas adaptadas al contexto		
	Activar la compatibilidad multilingüe		
Tareas de seguridad	Automatizar las operaciones rutinarias		

	Obtener información sobre seguridad		
	Proporcionar orientación para la reparación		
Integración	Integración de flujos de trabajo		
	Activar la automatización personalizada		
	Mantener registros de auditoría		

5.2.2 Integración de inteligencia sobre amenazas

La integración de la inteligencia avanzada sobre amenazas debe proporcionar información procesable al tiempo que correlaciona automáticamente los datos de múltiples fuentes para mejorar las capacidades de detección y respuesta a las amenazas.

Requisito	Subrequisito	S/N	Notas
Análisis de inteligencia	Procesar múltiples fuentes de amenazas		
	Correlacionar los indicadores de amenazas		
	Generar perfiles de actores		
	Proporcionar una evaluación de impacto		
Automatización	Automatizar la ingesta de alimentos		
	Apoyo a la creación de inteligencia personalizada		
	Actualización automática de las reglas de detección		
Integración	Conectar con plataformas externas		
	Compatible con los formatos STIX/TAXII		
	Habilitar la capacidad de compartir amenazas		

5.2.3 Análisis de códigos

El análisis de código impulsado por IA debe proporcionar capacidades de evaluación de seguridad completas, al tiempo que minimiza los falsos positivos y ofrece una orientación clara para la corrección.

Requisito	Subrequisito	S/N	Notas
Análisis Características	Realizar análisis estáticos de código		
	Activar el análisis dinámico del código		
	Compatible con varios idiomas		
	Identificar las vulnerabilidades de seguridad		
Automatización	Automatice la programación de las exploraciones		
	Integración CI/CD		
	Generar medidas correctoras		
Informes	Proporcionar resultados detallados		
	Seguimiento de las tendencias de vulnerabilidad		
	Informes personalizados		

5.2.4 Detección y respuesta inteligente en la nube (CDR)

Las capacidades CDR deben aprovechar la IA para la detección temprana de amenazas, al tiempo que permiten acciones de respuesta automatizadas y proporcionan una visualización clara de la cadena de ataque.

Requisito	Subrequisito	S/N	Notas
Capacidad de detección	Permitir la detección precoz de ataques		
	Supervisar los servicios en la nube		

	Identificar patrones de ataque		
	Movimiento lateral de la vía		
Características de la respuesta	Automatizar la respuesta inicial		
	Compatibilidad con playbooks personalizados		
	Permitir la contención de incidentes		
Analítica	Correlacionar eventos de seguridad		
	Proporcionar visualización de ataques		
	Generar análisis de impacto		

5.2.5 Seguridad adaptable

Los marcos de seguridad adaptables deben evolucionar continuamente para hacer frente a las amenazas emergentes, al tiempo que ajustan automáticamente los controles de seguridad en función de la evaluación de riesgos en tiempo real.

Requisito	Subrequisito	S/N	Notas
Marco adaptativo	Implantar controles dinámicos		
	Control en tiempo real		
	Apoyar la adaptación de las políticas		
	Ajuste en función del riesgo		
Capacidades de aprendizaje	Activar el reconocimiento de patrones		
	Apoyar el aprendizaje del comportamiento		
	Actualización de las bases de seguridad		

Automatización	Ajustar las normas de seguridad		
	Modificar los controles de acceso		
	Actualizar los criterios de detección		

5.2.6 Análisis predictivo

Las capacidades de análisis predictivo deben aprovechar los datos históricos y la información actual sobre amenazas para prever posibles incidentes de seguridad y permitir una mitigación proactiva.

Requisito	Subrequisito	S/N	Notas
Previsión	Predecir incidentes de seguridad		
	Identificar posibles amenazas		
	Calcular las puntuaciones de riesgo		
	Tendencias en los ataques a proyectos		
Análisis	Procesar datos históricos		
	Analizar las pautas de las amenazas		
	Evaluar los factores de riesgo		
Informes	Generar informes de previsiones		
	Proporcionar análisis de tendencias		
	Crear evaluaciones de riesgos		

5.2.7 Operaciones de seguridad automatizadas

La automatización de la seguridad debe agilizar las operaciones manteniendo la transparencia y permitiendo la supervisión humana de las decisiones críticas.

Requisito	Subrequisito	S/N	Notas

Automatización de tareas	Automatizar tareas rutinarias		
	Gestionar las alertas de seguridad		
	Gestionar la respuesta a incidentes		
	Gestión de la vulnerabilidad de los procesos		
Gestión del flujo de trabajo	Crear flujos de trabajo automatizados		
	Activar la automatización personalizada		
	Apoyar la supervisión humana		
Informes	Seguimiento de acciones automatizadas		
	Mantener registros de auditoría		
	Generar informes de eficacia		

5.2.8 Control de acceso inteligente

Los sistemas de control de acceso deben aprovechar la IA para tomar decisiones dinámicas manteniendo el equilibrio entre seguridad y usabilidad.

Requisito	Subrequisito	S/N	Notas
Análisis del comportamiento	Supervisar las actividades de los usuarios		
	Seguir las pautas de acceso		
	Detectar anomalías		
	Perfil del comportamiento del usuario		
Gestión de accesos	Establecer permisos dinámicos		
	Acceso basado en el riesgo		
	Acceso justo a tiempo		

Protección	Impedir el acceso no autorizado		
	Bloquear actividades sospechosas		
	Aplicar políticas de acceso		

5.2.9 Prevención de Pérdida de Datos Mejorada con IA

Las capacidades de DLP deben utilizar la IA para identificar y proteger con precisión los datos confidenciales, minimizando al mismo tiempo las interrupciones de la actividad empresarial.

Requisito	Subrequisito	S/N	Notas
Detección de datos	Identificar los datos sensibles		
	Clasificar los tipos de información		
	Supervisar el movimiento de datos		
	Seguimiento del uso de datos		
Prevención	Bloquear el uso compartido no autorizado		
	Cifrar datos sensibles		
	Aplicar políticas de DLP		
Gestión	Crear reglas personalizadas		
	Generar informes de DLP		
	Seguimiento de las infracciones		

5.2.10 Gestión de la postura de seguridad de la IA (AI-SPM)

AI-SPM debe proporcionar una visibilidad completa de la seguridad de los servicios de IA y permitir al mismo tiempo la corrección automatizada de los problemas detectados.

Requisito	Subrequisito	S/N	Notas

Seguridad de los servicios de IA	Supervisar las cargas de trabajo de IA		
	Evaluar la seguridad del LLM		
	Seguimiento del acceso al modelo de IA		
	Evaluar el uso de datos de IA		
Gestión	Automatizar los controles de seguridad		
	Activar acciones correctoras		
	Mantener líneas de base de seguridad		
Informes	Generar informes de postura		
	Seguimiento de las métricas de seguridad		
	Documentar el estado de cumplimiento		

5.2.11 Seguridad SaaS potenciada por GenAI

La seguridad SaaS debe aprovechar la IA generativa para mejorar la protección, manteniendo al mismo tiempo una visibilidad y un control exhaustivos.

Requisito	Subrequisito	S/N	Notas
Protección SaaS	Supervisar las aplicaciones SaaS		
	Controlar el acceso a los datos		
	Proteger la información sensible		
	Seguimiento de las actividades de los usuarios		
Integración	Apoyar las funciones CASB		

	Habilitar la integración de DLP		
	Garantizar la seguridad de la API		
Gestión	Obtener información sobre seguridad		
	Automatizar la aplicación de políticas		
	Crear informes de cumplimiento		

6. 6. Cualificación de los proveedores

6.1 Información sobre la empresa

- Mínimo 5 años de experiencia en seguridad en la nube
- Experiencia demostrada en soluciones de seguridad empresarial
- Sólida estabilidad financiera y crecimiento
- Certificaciones y asociaciones industriales
- Capacidad de asistencia mundial

6.2 Conocimientos técnicos

- Amplia experiencia en seguridad en la nube
- Capacidades avanzadas de análisis e inteligencia artificial
- Experiencia en integración con las principales plataformas
- Capacidad de desarrollo y personalización
- Capacidades de investigación sobre seguridad e inteligencia sobre amenazas

6.3 Capacidades de apoyo

- Asistencia técnica 24 horas al día, 7 días a la semana, 365 días al año
- Múltiples canales de asistencia
- Amplios programas de formación
- Disponibilidad de servicios profesionales
- Actualizaciones y mejoras periódicas de los productos

7. 7. Criterios de evaluación

7.1 Mérito técnico (40%)

- Solución completa
- Innovación técnica
- Capacidades AI/ML
- Capacidad de integración
- Escalabilidad y rendimiento
- Eficacia de la seguridad

7.2 Capacidades funcionales (30%)

- Funciones básicas de seguridad
- Análisis avanzados
- Capacidades de automatización
- Informes y visibilidad
- Experiencia del usuario
- Opciones de personalización

7.3 Cualificación de los proveedores (20%)

- Experiencia de la empresa
- Conocimientos técnicos
- Referencias de clientes
- Infraestructura de apoyo
- Hoja de ruta de la innovación
- Posición en el mercado

7,4 Coste (10%)

- Solución de precios
- Costes de aplicación

- Mantenimiento continuo
- Gastos de formación
- Servicios adicionales
- Coste total de propiedad

8. Requisitos de presentación

Los vendedores deben presentar:

1. Descripción detallada de la solución técnica
2. Metodología de aplicación e integración
3. Calendario del proyecto con los principales hitos
4. Estructura completa de precios
5. Cualificaciones y experiencia de la empresa
6. Un mínimo de tres referencias de empresas
7. Planes de asistencia y mantenimiento
8. Formación y transferencia de conocimientos
9. Ejemplos de informes y documentación
10. Hoja de ruta de productos y planes de desarrollo futuro

9. Cronología

- Liberación de la RFP:
- Preguntas vencidas:
- Presentación de propuestas:
- Periodo de evaluación:
- Presentaciones de proveedores:
- Selección de proveedores:
- Inicio del proyecto:

- Fase de aplicación 1:
- Fase de aplicación 2:
- Finalización del proyecto:

Envíe todas las propuestas a

Contacto técnico:

Contacto para adquisiciones: