Solicitud de Propuesta: Software de Gestión de Postura de Seguridad en la Nube (CSPM)

Índice

1. Introducción

1.1 Objetivo

Esta RFP busca propuestas para una solución de gestión de la postura de seguridad en la nube (CSPM) que mejore la postura de seguridad en la nube de nuestra organización, garantice el cumplimiento y gestione los riesgos en todos nuestros entornos en la nube.

1.2 Antecedentes

El software CSPM está diseñado para supervisar, detectar y responder continuamente a los riesgos de seguridad y a los problemas de cumplimiento en las infraestructuras de nube, incluidos los entornos IaaS, PaaS y SaaS.

2. Requisitos de la solución

2.1 Funciones básicas

2.1.1 Control continuo

- Vigilancia en tiempo real de los recursos de la nube
- Detección de errores de configuración y vulnerabilidades

2.1.2 Corrección automatizada

- Corrección automática de los problemas detectados
- Reducción del error humano en la gestión de la seguridad

2.1.3 Gestión de la conformidad

- Control del estado de cumplimiento
- Generación de informes de cumplimiento
- Asistencia en el cumplimiento de las normas y reglamentos del sector

2.1.4 Evaluación de riesgos

- Evaluación y priorización de los riesgos de seguridad
- Centrarse en las amenazas de alto impacto

2.1.5 Capacidades de integración

- Perfecta integración con las herramientas de seguridad existentes
- Compatibilidad con varias plataformas en la nube

2.2 Requisitos funcionales

2.2.1 Recogida y agregación de datos

Consejo: Un sistema sólido de recopilación de datos constituye la base de un CSPM eficaz. Tenga en cuenta el volumen, la variedad y la velocidad de las fuentes de datos que su organización necesita supervisar, y asegúrese de que la solución puede gestionar sus requisitos de ingesta de datos actuales y previstos, manteniendo el rendimiento.

Subrequisito	S/N	Notas
Recopilar datos de los registros de la nube		

Recopilar datos del tráfico de red		
Recopilar datos de la actividad del punto final		
Proporcionar una visibilidad completa del entorno de nube		

2.2.2 Detección de amenazas

Consejo: la combinación de varios métodos de detección proporciona la cobertura de amenazas más completa. Evalúe cómo cada método de detección complementa a los demás y tenga en cuenta las tasas de falsos positivos junto con la eficacia de la detección.

Subrequisito	S/N	Notas
Utilizar la detección basada en firmas		
Utilizar algoritmos de aprendizaje automático		
Utilizar el análisis del comportamiento		
Identifique posibles amenazas en tiempo real		

2.2.3 Capacidades de respuesta a incidentes

Consejo: La rapidez y eficacia de la respuesta a incidentes repercute directamente en la contención de los incidentes de seguridad. Busque capacidades de automatización que puedan reducir los tiempos de respuesta, manteniendo al mismo tiempo una supervisión humana adecuada para las decisiones críticas.

Subrequisito	S/N	Notas
Permitir el aislamiento de los sistemas afectados		
Permitir el bloqueo del tráfico malicioso		
Facilitar el inicio de investigaciones		
Apoyo a la gestión de las investigaciones		

2.2.4 Gestión de alertas

Consejo: La fatiga por las alertas puede afectar significativamente a la eficacia del equipo de seguridad. Céntrese en soluciones que ofrezcan correlación y priorización inteligente de alertas para garantizar que las alertas críticas de reciban la atención adecuada al tiempo que se reduce el ruido de los falsos positivos.

Subrequisito	S/N	Notas
Priorizar las alertas en función de su criticidad		
Priorizar las alertas en función de su impacto potencial		
Gestión inteligente de alertas		
Reducir la fatiga por alerta		

2.2.5 Escalabilidad y adaptabilidad

Consejo: Los entornos de nube pueden crecer rápidamente y cambiar con frecuencia. Asegúrese de que la solución puede escalarse horizontal y verticalmente para adaptarse al crecimiento manteniendo el rendimiento, y adáptese a los nuevos servicios en la nube y patrones arquitectónicos.

Subrequisito	S/N	Notas
Escala para adaptarse a organizaciones de todos los tamaños		
Adaptarse a entornos de nube complejos		
Admite la asignación dinámica de recursos		
Gestione eficazmente los picos de carga		

2.2.6 Gestión de la privacidad de los datos

Consejo: Los requisitos de privacidad de datos varían según el sector y la región. Compruebe que la solución es compatible con sus requisitos de cumplimiento específicos y proporciona controles granulares para el acceso, almacenamiento y transmisión de datos en diferentes entornos de nube.

Subrequisito	S/N	Notas

Gestione de forma segura la información confidencial		
Implantar medidas sólidas de protección de datos		
Soporta despliegues multi-nube		
Proporcionar pistas de auditoría para el acceso a los datos		

2.3 Funciones basadas en IA

2.3.1 Gestión de las posturas de seguridad de la IA (AI-SPM)

Consejo: La gestión de la postura de seguridad de la IA requiere una visibilidad especializada de las cargas de trabajo y la infraestructura de IA/ML. Asegúrese de que la solución comprende los retos de seguridad específicos de los sistemas de IA y puede proporcionar información significativa sobre el estado de seguridad de su pila de IA.

Subrequisito	S/N	Notas
Proporcionar visibilidad de la seguridad de los servicios GenAI		
Ofrecer inventario de la pila de IA (modelos, datos, infraestructura)		
Identificar las vulnerabilidades específicas de la IA		
Trazar posibles rutas de ataque en entornos de IA		

2.3.2 Detección mejorada con IA y aprendizaje automático

Consejo: La detección mediante IA debe complementar los métodos tradicionales y minimizar los falsos positivos. Busque soluciones que demuestren claras ventajas en cuanto a precisión y velocidad de detección en comparación con los métodos convencionales.

Subrequisito	S/N	Notas
Utilizar algoritmos avanzados para la detección de patrones		
Utilizar algoritmos avanzados para la detección de anomalías		
Detección en tiempo real de amenazas complejas		

2.3.3 Priorización de riesgos mediante IA

Consejo: La priorización eficaz de los riesgos es crucial para la asignación de recursos. El sistema de IA debe proporcionar una justificación clara de sus evaluaciones de riesgos y permitir la personalización en función de la tolerancia al riesgo específica de su organización.

Subrequisito	S/N	Notas
Analizar el radio de explosión de los activos de riesgo		
Descubra riesgos complejos de forma eficaz		
Priorizar los riesgos identificados		

2.3.4 Análisis predictivo

Consejo: Las capacidades de predicción deben proporcionar información práctica en lugar de meras posibilidades teóricas. Céntrese en soluciones que demuestren un historial de predicciones precisas con recomendaciones claras de mitigación.

Subrequisito	S/N	Notas
Anticipar posibles vulnerabilidades antes de su explotación		
Habilitar estrategias proactivas de gestión de riesgos		

2.3.5 Copiloto AI para CSPM

Consejo: Los asistentes de IA deben mejorar la eficiencia de los operarios sin sustituir el juicio humano. Evalúe lo bien que se integra el copiloto en los flujos de trabajo existentes y si ofrece explicaciones claras de sus recomendaciones.

Subrequisito	S/N	Notas
Permitir consultas en lenguaje natural para interactuar con el sistema		
Proporcionar información rápida sobre el estado de la seguridad		
Ofrecer recomendaciones correctoras		

Sugerir flujos de trabajo óptimos		

2.3.6 Control automatizado del cumplimiento con IA

Consejo: La supervisión del cumplimiento impulsada por IA debe adaptarse a los cambios normativos manteniendo la precisión. Verifique la capacidad de la solución para interpretar los nuevos requisitos de cumplimiento y traducirlos en controles procesables.

Subrequisito	S/N	Notas
Adaptarse a los cambios normativos con una intervención humana mínima		
Supervisión en tiempo real de una amplia gama de normativas		
Generar informes de cumplimiento		

2.3.7 Previsión de amenazas basada en IA

Consejo: la previsión de amenazas debe combinar la información sobre amenazas globales con el contexto local. Busque soluciones que puedan demostrar la precisión de sus predicciones y ofrecer un razonamiento claro para sus previsiones.

Subrequisito	S/N	Notas
Utilizar el aprendizaje automático para mejorar la capacidad de predicción		
Permitir una previsión precisa de las amenazas		
Detección de anomalías		

2.3.8 Seguridad de las aplicaciones de IA generativa

Consejo: La seguridad de la IA generativa requiere un conocimiento especializado de las vulnerabilidades de los modelos de IA y de los riesgos de la cadena de suministro. Asegúrese de que la solución puede supervisar y proteger eficazmente tanto los modelos de IA como su infraestructura de apoyo.

Subrequisito	S/N	Notas
Descubrir y evaluar los riesgos de seguridad en las aplicaciones de IA generativa		
Identificación de vulnerabilidades en las dependencias de las bibliotecas de IA		
Análisis del código fuente en busca de errores de configuración de la Infraestructura como Código		

3. 3. Requisitos técnicos

3.1 Compatibilidad con plataformas en nube

- Compatibilidad con los principales proveedores de nube (AWS, Azure, Google Cloud)
- Compatibilidad con entornos de nubes múltiples y nubes híbridas
- Integración basada en API con las herramientas de seguridad existentes
- Compatibilidad con sistemas comunes de gestión de eventos e información de seguridad (SIEM)

3.2 Capacidades de integración

- Integración basada en API con las herramientas de seguridad existentes
- Compatibilidad con sistemas comunes de gestión de eventos e información de seguridad (SIEM)

3.3 Escalabilidad

- Capacidad para gestionar implantaciones en la nube a gran escala
- Optimización del rendimiento para el tratamiento de grandes volúmenes de datos

3.4 Gestión de datos

- Almacenamiento y tratamiento de datos seguros
- Capacidad de conservación y archivo de datos

4. Informes y análisis

4.1 Cuadros de mando y visualización

- Cuadros de mando personalizables para diferentes funciones de usuario
- Visualización en tiempo real de la postura de seguridad

4.2 Capacidad de elaboración de informes

- Generación automática de informes con fines de cumplimiento y auditoría
- Plantillas de informes personalizables

5. Apoyo y mantenimiento

5.1 Asistencia técnica

- Asistencia 24 horas al día, 7 días a la semana
- Múltiples canales de asistencia (teléfono, correo electrónico, chat)

5.2 Actualizaciones y mejoras

- Actualizaciones periódicas de software y parches de seguridad
- Ruta de actualización clara para futuras versiones

6. Formación y documentación

6.1 Formación de usuarios

- Amplio programa de formación para administradores y usuarios finales
- Opciones de formación en línea y presencial

6.2 Documentación

- Manuales de usuario y guías de administración detallados
- Actualizaciones periódicas de la documentación

7. Precios y licencias

7.1 Modelo de fijación de precios

- Explicación clara de la estructura de precios (por usuario, por activo, etc.)
- Descuentos por volumen o compromisos a largo plazo

7.2 Condiciones de la licencia

- Flexibilidad en las opciones de licencia

- Cualquier restricción o limitación de uso

8. 8. Información sobre proveedores

8.1 Perfil de la empresa

- Breve historia y antecedentes de la empresa
- Estabilidad financiera y posición en el mercado

8.2 Referencias

- Proporcione al menos tres referencias de organizaciones de tamaño similar
- Casos prácticos de éxito

9. 9. Criterios de evaluación

Las propuestas se evaluarán en función de

- Integridad de la solución para cumplir los requisitos establecidos
- Funciones innovadoras, sobre todo de inteligencia artificial
- Facilidad de uso e integración
- Escalabilidad y rendimiento
- Precios y coste total de propiedad
- Reputación del proveedor y capacidad de asistencia

10. Instrucciones de presentación

Las propuestas deben incluir:

- Respuesta detallada a todos los requisitos
- Plan y calendario de aplicación
- Información sobre precios
- Información y referencias de la empresa
- Ejemplos de informes y documentación