Solicitud de Propuesta Plataforma de Protección de Cargas de Trabajo en la Nube

Índice

1. Introducción

Esta solicitud de propuesta (RFP) busca una plataforma de protección de la carga de trabajo en la nube (CWPP). Las CWPP son soluciones de seguridad especializadas diseñadas para salvaguardar cargas de trabajo -como aplicaciones, bases de datos y servicios- en diversos entornos de nube, incluidas nubes públicas, privadas e híbridas. Estas plataformas ofrecen una visibilidad completa, detección de amenazas y respuestas automatizadas para garantizar la integridad y seguridad de las operaciones basadas en la nube.

2. Beneficios clave

La solución propuesta debe ofrecer las siguientes ventajas clave:

1. Postura de seguridad reforzada
    - Protección integral frente a amenazas
    - Medidas de seguridad proactivas
    - Inteligencia avanzada sobre amenazas
2. Eficiencia operativa
    - Operaciones de seguridad racionalizadas
    - Procesos de seguridad automatizados
    - Reducción de la intervención manual
3. Escalabilidad
    - Compatibilidad con entornos de nube en crecimiento
    - Optimización del rendimiento
    - Gestión de recursos
4. Garantía de cumplimiento
    - Gestión del cumplimiento de la normativa
    - Control automatizado del cumplimiento
    - Informes de conformidad
5. Gestión entre nubes
    - Seguridad unificada en todas las plataformas en nube
    - Aplicación coherente de las políticas
    - Gestión centralizada

3. Características principales

Los proveedores deben demostrar su capacidad en las siguientes áreas básicas:

1. Descubrimiento y visibilidad automatizados
    - Descubrimiento de activos en tiempo real

- Visibilidad completa de todos los entornos
- Asignación de recursos

2. Detección de amenazas y respuesta
    - Detección avanzada de amenazas
    - Capacidad de respuesta automática
    - Gestión de incidentes
3. Endurecimiento de la carga de trabajo
    - Gestión de la configuración de seguridad
    - Gestión de vulnerabilidades
    - Endurecimiento del sistema
4. Descubrimiento de activos
    - Supervisión continua de activos
    - Clasificación de los activos
    - Gestión de existencias
5. Detección de anomalías
    - Análisis del comportamiento
    - Reconocimiento de patrones
    - Generación de alertas
6. Seguridad de los datos
    - Protección de datos
    - Gestión del cifrado
    - Control de acceso
7. Gobernanza

- Gestión de políticas
- Control del cumplimiento
- Evaluación de riesgos

8. Registro e informes
    - Registro exhaustivo
    - Informes personalizados
    - Cuadros de mando analíticos

4. 4. Requisitos funcionales

4.1 Recogida y agregación de datos

Consejo: La recopilación y agregación eficaz de datos constituye la base de su solución CWPP. Céntrese en las capacidades integrales de recopilación de datos en todos los entornos de nube teniendo en cuenta el impacto en el rendimiento y los requisitos de almacenamiento. Busque soluciones capaces de procesar grandes volúmenes de datos en tiempo real.

Requisito	Subrequisito	S/N	Notas
Recogida y agregación de datos	Recogida en varios proveedores de nube (AWS, Azure, GCP)		
	Recopilación de datos en tiempo real de cargas de trabajo en la nube		
	Recogida y agregación de registros		
	Recopilación de métricas de rendimiento		
	Recopilación de datos de configuración		
	Supervisión del tráfico de red		
	Recogida de datos a nivel de API		

4.2 Detección de amenazas

Consejo: Las funciones avanzadas de detección de amenazas deben combinar varios métodos de detección para ofrecer una protección completa. Considere soluciones que aprovechen tanto la detección tradicional basada en firmas como los modernos análisis basados en ML para minimizar los falsos positivos y mantener al mismo tiempo altos índices de detección.

Requisito	Subrequisito	S/N	Notas
Detección de amenazas	Detección basada en firmas		
	Análisis de aprendizaje automático		
	Análisis del comportamiento		
	Exploración de vulnerabilidades		
	Detección de malware		
	Detección de amenazas de día cero		
	Detección de amenazas persistentes avanzadas (APT)		

4.3 Respuesta a incidentes

Consejo: Las capacidades automatizadas de respuesta a incidentes son cruciales para mantener la seguridad en entornos de nube en los que las amenazas pueden propagarse rápidamente. Asegúrese de que la solución ofrezca opciones de respuesta automatizadas y manuales con flujos de trabajo y registros de auditoría claros.

Requisito	Subrequisito	S/N	Notas
Respuesta a incidentes	Contención automatizada de amenazas		
	Capacidad de aislamiento del sistema		
	Mecanismos de bloqueo del tráfico		

	Flujos de trabajo de corrección automatizados		
	Ejecución del libro de jugadas de incidentes		
	Opciones de respuesta manual		
	Herramientas de análisis posterior al incidente		

4.4 Priorización de alertas

Consejo: La priorización eficaz de las alertas es esencial para gestionar las operaciones de seguridad a escala. Busque soluciones que utilicen algoritmos inteligentes para reducir la fatiga de las alertas y garantizar al mismo tiempo que las amenazas críticas no pasen desapercibidas.

Requisito	Subrequisito	S/N	Notas
Priorización de alertas	Clasificación de alertas en función del riesgo		
	Capacidad de correlación de alertas		
	Reglas de alerta personalizadas		
	Opciones de supresión de alertas		
	Clasificación automática de alertas		
	Enriquecimiento del contexto de alerta		
	Análisis histórico de alertas		

4.5 Gestión del cumplimiento

Consejo: Las funciones integrales de gestión del cumplimiento deben ser compatibles tanto con los marcos normativos estándar como con las políticas de cumplimiento personalizadas. Considere las soluciones que automatizan la supervisión del cumplimiento y la elaboración de informes para reducir los requisitos de supervisión manual.

Requisito	Subrequisito	S/N	Notas

Gestión del cumplimiento	Cumplimiento de la normativa del sector		
	Funciones de supervisión de políticas		
	Herramientas de información sobre el cumplimiento		
	Creación de políticas personalizadas		
	Controles de conformidad automatizados		
	Alertas de infracción		
	Mantenimiento de registros de auditoría		

4.6 Escalabilidad

Consejo: La escalabilidad es fundamental para los entornos de nube en crecimiento. Evalúe las soluciones en función de su capacidad para escalar horizontal y verticalmente manteniendo el rendimiento y la eficacia en todas las cargas de trabajo protegidas.

Requisito	Subrequisito	S/N	Notas
Escalabilidad	Admite un volumen de carga de trabajo cada vez mayor		
	Capacidad de escalado entre nubes		
	Funciones de optimización del rendimiento		
	Eficiencia en el uso de los recursos		
	Mecanismos automáticos de escalado		
	Capacidad de equilibrio de carga		
	Compatibilidad multirregión		

4.7 Integración con los sistemas existentes

Consejo: Una sólida capacidad de integración garantiza que su solución CWPP funcione a la perfección con su infraestructura de seguridad existente. Céntrese en la compatibilidad con API estándar y en las integraciones prediseñadas con herramientas de seguridad comunes.

Requisito	Subrequisito	S/N	Notas
Capacidades de integración	Integración de la API de la herramienta de seguridad		
	Integración SIEM		
	Integración de la plataforma SOAR		
	Integración de la gestión de identidades		
	Opciones de desarrollo de API personalizadas		
	Compatibilidad con webhooks		
	Compatibilidad con plugins de terceros		

4.8 Gestión de la privacidad de los datos

Consejo: Las funciones de privacidad de datos deben cumplir tanto los requisitos normativos como las políticas de seguridad internas. Considere soluciones que proporcionen un control granular sobre el manejo de datos sensibles y sólidas capacidades de cifrado.

Requisito	Subrequisito	S/N	Notas
Gestión de la privacidad de los datos	Tratamiento de datos sensibles		
	Aplicación del cifrado		
	Funciones de control de acceso		
	Funciones de enmascaramiento de datos		

	Cumplimiento de la política de privacidad		
	Herramientas de clasificación de datos		
	Informes sobre el cumplimiento de la privacidad		

4.9 Capacidades impulsadas por la IA

Consejo: Las capacidades de IA deben mejorar tanto las operaciones de seguridad como la detección de amenazas. Busque soluciones que demuestren aplicaciones prácticas de IA/ML más allá de las palabras de moda de marketing, con beneficios claros para los resultados de seguridad.

Requisito	Subrequisito	S/N	Notas
Capacidades basadas en IA	Supervisión de la seguridad de la carga de trabajo con IA		
	Medidas correctoras generadas por IA		
	Optimización de políticas IAM		
	Descripciones de alertas generadas por IA		
	Detección inteligente de anomalías		
	Detección de modelos/paquetes de IA		
	Análisis de rutas de ataque mejorado por IA		
	Gestión de inventarios con IA		
	Políticas de ejecución específicas de la IA		

5. Requisitos de integración

La solución CWPP debe integrarse con:

- Sistemas de detección y respuesta para puntos finales (EDR)
- Software de seguridad para centros de datos

- Plataformas de gestión en nube
- Software de cumplimiento en la nube

6. Tendencias emergentes

Los vendedores deben abordar su enfoque de:

- Integración de IA y aprendizaje automático para mejorar la detección y respuesta ante amenazas
- Cambio a la izquierda Prácticas de seguridad
- Integración con Cloud Security Posture Management (CSPM)

7. Aplicación y apoyo

Los vendedores deben facilitar información detallada sobre:

- Proceso y calendario de aplicación
- Formación y apoyo a la incorporación
- Asistencia técnica permanente y acuerdos de nivel de servicio
- Actualizaciones periódicas y gestión de parches

8. Conformidad y certificaciones

Los vendedores deben especificarlo:

- Certificaciones sectoriales pertinentes (por ejemplo, ISO 27001, SOC 2)
- Cumplimiento de la normativa sobre protección de datos (por ejemplo, GDPR, CCPA)

9. Modelo de precios y licencias

Los vendedores deben proporcionar:

- Estructura detallada de precios
- Modelos de licencia (por usuario, por carga de trabajo o para toda la empresa)
- Costes adicionales por funciones premium o asistencia

10. Casos prácticos y referencias

Los vendedores deben incluir:

- Estudios de casos pertinentes que demuestren el éxito de la aplicación del CWPP
- Referencias de clientes de sectores similares o con entornos de nube comparables

11. 11. Criterios de evaluación

Las propuestas se evaluarán en función de

- Completitud de las características
- Facilidad de uso y gestión
- Escalabilidad y rendimiento
- Capacidad de integración
- Capacidades de IA y aprendizaje automático
- Precios y coste total de propiedad
- Reputación del proveedor y calidad de la asistencia

Información de contacto: security@company.com

12. Cronología

- Fecha de publicación de la RFP: [Fecha]
- Preguntas Plazo: [Fecha]
- Fecha límite para la presentación de propuestas: [Fecha]
- Presentaciones de proveedores: [intervalo de fechas]
- Fecha de selección: [Fecha]
- Fecha de inicio del proyecto: [Fecha]