Solicitud de Propuesta: Plataforma de Protección de Aplicaciones Nativas en la Nube (CNAPP)

Tabla de Contenidos

1. Descripción General

Estamos buscando propuestas para una Plataforma de Protección de Aplicaciones Nativas en la Nube (CNAPP) integral para proteger nuestras aplicaciones nativas en la nube durante todo su ciclo de vida. La solución debe proporcionar funciones de seguridad integradas, ofreciendo visibilidad completa, aplicación consistente de políticas y protección robusta en todos nuestros diversos entornos en la nube.

2. Componentes Clave

La solución propuesta debe incluir los siguientes componentes clave:

2.1. Gestión de Postura de Seguridad en la Nube (CSPM)

2.2. Plataforma de Protección de Cargas de Trabajo en la Nube (CWPP)

2.3. Gestión de Derechos de Infraestructura en la Nube (CIEM)

2.4. Integración DevSecOps

2.5. Protección en Tiempo de Ejecución

3. Requisitos Funcionales

3.1. Visibilidad Unificada

Consejo: Una solución de visibilidad unificada robusta es crucial para mantener una supervisión integral de la seguridad. Busque soluciones que proporcionen capacidades de monitoreo en tiempo real y puedan integrar datos de múltiples fuentes en una vista única y coherente. Considere la profundidad de visibilidad en diferentes servicios en la nube y la capacidad de personalizar vistas según las necesidades de diferentes partes interesadas.

Requisito	Sub-Requisito	S/N	Notas
Visibilidad Unificada	Vista centralizada de seguridad en todos los recursos y servicios en la nube		
	Visibilidad en configuraciones		
	Visibilidad en activos		
	Visibilidad en permisos		
	Visibilidad en código		
	Visibilidad en cargas de trabajo		

3.2. Cumplimiento Automatizado

Consejo: Las capacidades de cumplimiento automatizado deben reducir la supervisión manual mientras aseguran el cumplimiento regulatorio continuo. Evalúe las soluciones según su capacidad para detectar, informar y remediar automáticamente las violaciones de cumplimiento en múltiples marcos regulatorios.

Requisito	Sub-Requisito	S/N	Notas
Cumplimiento Automatizado	Evaluación continua del cumplimiento con estándares de la industria		
	Aplicación continua del cumplimiento con estándares de la industria		

	Adhesión simplificada a requisitos regulatorios a través del monitoreo		
	Adhesión simplificada a requisitos regulatorios a través de informes		

3.3. Detección y Respuesta a Amenazas

Consejo: Las capacidades avanzadas de detección y respuesta a amenazas deben aprovechar métodos tanto tradicionales como mejorados por IA. Busque soluciones que puedan detectar amenazas en tiempo real y proporcionar recomendaciones de respuesta accionables.

Requisito	Sub-Requisito	S/N	Notas
Detección y Respuesta a Amenazas	Identificación en tiempo real de amenazas durante el ciclo de vida de la aplicación		
	Mitigación en tiempo real de amenazas durante el ciclo de vida de la aplicación		
	Detección de amenazas mejorada por IA usando análisis avanzado		
	Detección de amenazas mejorada por IA usando análisis predictivo		
	Implementación de Detección y Respuesta en la Nube (CDR) inteligente		
	Detección de amenazas en tiempo real con análisis de intención		

3.4. Gestión de Políticas

Consejo: La gestión efectiva de políticas requiere tanto consistencia como inteligencia. Evalúe las soluciones según su capacidad para mantener políticas de seguridad uniformes en diversos entornos mientras aprovecha la IA para optimizar y adaptar políticas basadas en amenazas emergentes y necesidades organizacionales.

Requisito	Sub-Requisito	S/N	Notas
Gestión de Políticas	Definición consistente de políticas de seguridad en todos los entornos		
	Aplicación consistente de políticas de seguridad en todos los entornos		
	Capacidades de gestión de políticas mejoradas por IA		
	Recomendaciones inteligentes de políticas		

3.5. Escalabilidad

Consejo: La escalabilidad es esencial para organizaciones en crecimiento. Busque soluciones que puedan escalar sin problemas con su infraestructura mientras mantienen el rendimiento. Considere tanto las capacidades de escalado horizontal como vertical, así como la capacidad de manejar picos repentinos en la carga de trabajo.

Requisito	Sub-Requisito	S/N	Notas
Escalabilidad	Capacidad de adaptarse a entornos dinámicos en la nube		
	Soporte para cargas de trabajo crecientes		
	Mantenimiento del rendimiento al escalar		

3.6. Capacidades de Integración

Consejo: Las capacidades de integración son cruciales para crear un ecosistema de seguridad cohesivo. Evalúe las soluciones según su capacidad para integrarse con su cadena de herramientas existente y la facilidad de implementar nuevas integraciones.

Requisito	Sub-Requisito	S/N	Notas
Capacidades de Integración	Integración perfecta con herramientas de desarrollo existentes		

	Integración perfecta con herramientas de seguridad		
	Integración perfecta con herramientas de gestión en la nube		
	Fácil integración con ecosistemas SecOps para alertas en tiempo real		

3.7. Cobertura de Seguridad Multi-Nube

Consejo: La seguridad multi-nube integral es esencial en los entornos de nube diversos de hoy. Busque soluciones que proporcionen controles de seguridad consistentes en todos los principales proveedores de nube mientras mantienen la conciencia de las particularidades específicas de cada proveedor.

Requisito	Sub-Requisito	S/N	Notas
Cobertura de Seguridad Multi-Nube	Visibilidad en entornos IaaS		
	Visibilidad en entornos PaaS		
	Visibilidad en entornos serverless		
	Soporte para AWS		
	Soporte para Azure		
	Soporte para Google Cloud		

3.8. Escaneo de Infraestructura como Código (IaC)

Consejo: Las capacidades de escaneo de IaC deben detectar problemas de seguridad temprano en el ciclo de vida del desarrollo. Busque soluciones que se integren con su flujo de trabajo de desarrollo y proporcionen orientación de remediación accionable.

Requisito	Sub-Requisito	S/N	Notas

Escaneo de Infraestructura como Código	Detección de vulnerabilidades de seguridad en código de infraestructura antes del despliegue		
	Soporte para múltiples marcos de IaC		
	Validación previa al despliegue		
	Aplicación de mejores prácticas de seguridad		

3.9. Escaneo de Contenedores y Kubernetes

Consejo: La seguridad de contenedores requiere un escaneo integral durante todo el ciclo de vida del contenedor. Evalúe las soluciones según su capacidad para escanear imágenes de contenedores, detectar vulnerabilidades en tiempo de ejecución y proporcionar controles de seguridad específicos para Kubernetes.

Requisito	Sub-Requisito	S/N	Notas
Escaneo de Contenedores y Kubernetes	Identificación de vulnerabilidades dentro de aplicaciones containerizadas		
	Monitoreo de seguridad de contenedores en tiempo de ejecución		
	Evaluación de seguridad de clústeres Kubernetes		
	Escaneo de imágenes de contenedores		

3.10. Protección de Datos

Consejo: Las capacidades de protección de datos deben cubrir datos en reposo y en movimiento. Busque soluciones que proporcionen controles de seguridad de datos integrales, incluyendo clasificación, cifrado y monitoreo de acceso.

Requisito	Sub-Requisito	S/N	Notas
Protección de Datos	Monitoreo de datos para posible exfiltración		

	Capacidades de clasificación de datos		
	Capacidades de inspección de datos		
	Prevención de exfiltración de datos		

3.11. Priorización de Riesgos

Consejo: La priorización efectiva de riesgos ayuda a enfocar los esfuerzos de seguridad en las amenazas más críticas. Busque soluciones que utilicen IA para analizar riesgos en el contexto de su entorno e impacto empresarial.

Requisito	Sub-Requisito	S/N	Notas
Priorización de Riesgos	Análisis de riesgos impulsado por IA		
	Priorización de riesgos impulsada por IA		
	Correlación de vulnerabilidades		
	Análisis de contexto a través del ciclo de desarrollo		
	Mapeo de relaciones a través del ciclo de desarrollo		

3.12. Seguridad Impulsada por IA para Aplicaciones de IA Empresariales

Consejo: La seguridad para aplicaciones de IA requiere capacidades especializadas. Busque soluciones que entiendan los patrones de carga de trabajo de IA/ML y puedan proteger contra amenazas específicas de IA.

Requisito	Sub-Requisito	S/N	Notas
Seguridad de Aplicaciones de IA	Postura de seguridad para aplicaciones GenAI		
	Protección contra amenazas para aplicaciones GenAI		
	Gestión de postura de seguridad de IA (AI-SPM)		

	Capacidades de descubrimiento de cargas de trabajo de IA		
	Capacidades de seguridad de cargas de trabajo de IA		

3.13. Remediación Impulsada por GenAI

Consejo: La remediación GenAI debe proporcionar soluciones accionables y conscientes del contexto. Evalúe la calidad y practicidad de las sugerencias de remediación generadas por IA.

Requisito	Sub-Requisito	S/N	Notas
Remediación Impulsada por GenAI	Sugerencias de remediación conscientes del contexto usando IA generativa		
	Generación de guías de consola		
	Generación de comandos CLI		
	Generación de fragmentos de código		

3.14. Clasificación y Priorización de Alertas Impulsada por IA

Consejo: La gestión de alertas debe reducir efectivamente el ruido mientras asegura que los problemas críticos sean atendidos. Busque soluciones que utilicen IA para categorizar y priorizar alertas de manera inteligente.

Requisito	Sub-Requisito	S/N	Notas
Clasificación y Priorización de Alertas	Modelos de IA/ML para análisis de alertas		
	Modelos de IA/ML para categorización de alertas		
	Modelos de IA/ML para priorización de alertas		
	Capacidades de reducción de fatiga por alertas		

3.15. Enriquecimiento Contextual con IA

Consejo: El enriquecimiento contextual debe proporcionar información significativa para una mejor toma de decisiones. Busque soluciones que puedan combinar inteligentemente múltiples fuentes de datos para proporcionar un contexto más rico.

Requisito	Sub-Requisito	S/N	Notas
Enriquecimiento Contextual	Enriquecimiento de datos de alertas impulsado por IA		
	Soporte para toma de decisiones informada		
	Integración de análisis de impacto empresarial		
	Mejora de procesos de priorización		

3.16. Aprendizaje Adaptativo de IA

Consejo: Las capacidades de aprendizaje adaptativo aseguran la mejora continua de las medidas de seguridad. Busque soluciones que puedan aprender de su entorno y adaptarse a nuevas amenazas.

Requisito	Sub-Requisito	S/N	Notas
Aprendizaje Adaptativo de IA	Mejora continua de recomendaciones de IA		
	Implementación de bucles de retroalimentación		
	Aprendizaje contextual entre CNAPP		
	Integración rápida de nueva cobertura de seguridad		

3.17. Consulta de Gráfico de Seguridad

Consejo: Las capacidades de consulta de gráfico de seguridad deben proporcionar herramientas de análisis potentes pero fáciles de usar. Busque

soluciones que ofrezcan interfaces tanto visuales como programáticas para el análisis de datos de seguridad.

Requisito	Sub-Requisito	S/N	Notas
Consulta de Gráfico de Seguridad	Búsqueda integral a través de proveedores de nube		
	Herramientas de visualización de datos de seguridad		
	Creación de políticas de seguridad desde el constructor de consultas		
	Capacidades de gestión de políticas de seguridad		

4. Requisitos Técnicos

4.1. Arquitectura de la Plataforma

- Diseño nativo en la nube
- Arquitectura de microservicios
- Infraestructura escalable
- Alta disponibilidad

4.2. Capacidades de Integración

- Diseño API-first
- Integración con herramientas DevOps
- Integración SIEM
- Soporte de integración personalizada

4.3. Estándares de Rendimiento

- Procesamiento en tiempo real
- Latencia mínima
- Rendimiento escalable

- Optimización de recursos

4.4. IA y Aprendizaje Automático

- Modelos ML avanzados
- Análisis en tiempo real
- Capacidades predictivas
- Aprendizaje continuo

5. Requisitos Adicionales

5.1. Interfaz de Usuario

- Interfaz web intuitiva
- Paneles personalizables
- Control de acceso basado en roles
- Accesibilidad móvil

5.2. Opciones de Implementación

- Implementación SaaS
- Opciones de implementación híbrida
- Soporte multi-región
- Recuperación ante desastres

5.3. Soporte y Capacitación

- Soporte técnico 24/7
- Documentación completa
- Recursos de capacitación
- Servicios profesionales

5.4. Rendimiento y Escalabilidad

- Soporte a escala empresarial
- Garantías de rendimiento

- Métricas de escalabilidad
- Adaptación al crecimiento

6. Criterios de Evaluación del Proveedor

Criterio	Peso	Descripción
Completitud de Solución CNAPP	20%	Cobertura integral de la funcionalidad requerida
Capacidades de IA/ML	15%	Fortaleza de las características de IA y aprendizaje automático
Soporte Multi-Nube	15%	Cobertura e integración entre proveedores de nube
Escalabilidad	10%	Rendimiento a escala empresarial
Experiencia de Usuario	10%	Usabilidad y accesibilidad de la interfaz
Analítica	10%	Capacidades de informes e insights
Cumplimiento	10%	Cobertura regulatoria y certificaciones
Soporte	5%	Soporte técnico y servicios profesionales
Costo	5%	Costo total de propiedad

7. Requisitos de Presentación

7.1. Propuesta Técnica

- Arquitectura detallada de la solución
- Matriz de cobertura de características
- Capacidades de integración
- Capacidades de IA/ML
- Controles de seguridad

7.2. Plan de Implementación

- Metodología de implementación

- Cronograma
- Requisitos de recursos
- Mitigación de riesgos

7.3. Estructura de Precios

- Modelo de licenciamiento
- Costos de implementación
- Costos de soporte
- Costos de capacitación

7.4. Información de la Empresa

- Experiencia
- Casos de estudio
- Referencias
- Plan de innovación

7.5. Detalles de Soporte

- Términos del SLA
- Niveles de soporte
- Enfoque de capacitación
- Servicios profesionales

8. Cronograma

- Fecha de Publicación del RFP: [Fecha]
- Fecha Límite para Preguntas: [Fecha]
- Fecha de Entrega de la Propuesta: [Fecha]
- Presentaciones de Proveedores: [Rango de Fechas]
- Fecha de Selección: [Fecha]
- Fecha de Inicio del Proyecto: [Fecha]

Información de Contacto

Por favor envíe propuestas y preguntas a:

- [Nombre de Contacto]
- [Correo Electrónico]
- [Número de Teléfono]