PERCEPTION POINT

Guía de requisitos RFP – Seguridad del correo electrónico

Proteción del correo electrónico.		Sí / No	Respuesta detallada
Escaneo de correos	¿La solución analiza el 100 % de los correos electrónicos de forma dinámica?		
	¿La solución analiza todas las URL y los archivos adjuntos de los correos electrónicos entrantes?		
	¿Puede la solución escanear dinámicamente correos electrónicos a una velocidad promedio de aproximadamente 15 segundos?		
	¿Puede un administrador de cliente acceder por sí mismo a los detalles de escaneo para ver los motivos exactos por los que se marca un correo electrónico malicioso?		
	¿La solución protege activamente contra el spam?		
	Si la solución identifica amenazas después de la entrega, ¿puede notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente?		
Identificación de amenazas	¿La solución utiliza fuentes de Threat Intelligence para identificar amenazas conocidas?		
	¿La solución utiliza capacidades internas de búsqueda de amenazas asistidas por humanos?		
	¿La solución escanea correos electrónicos estáticamente usando motores AV?		
	¿La solución utiliza herramientas para identificar firmas altamente complejas?		
Amenazas avanzadas	¿La solución protege de los ataques de phishing mediante el reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación?		
	¿La solución protege de los ataques BEC al realizar comprobaciones de SPF, DKIM y DMARC?		
	¿La solución protege de los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres para mostrar y las suplantaciones de VIP?		
	¿La solución protege contra ataques de día cero y día N al inspeccionar los datos de nivel de CPU?		
	¿Puede la solución detectar ATO al observar anomalías en el comportamiento del usuario?		
Manejo de URL	¿La solución hace clic y escanea activamente las URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final? (Zona de pruebas de URL)		

	¿La solución tiene capacidades de reescritura de URL?		
Sandbox	¿La solución escanea utilizando la tecnología Sandbox para identificar archivos maliciosos?		
	¿La solución utiliza datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos?		
	¿Puede la solución mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos?		
	¿Puede la solución identificar exploits de corrupción de memoria?		
	¿Puede la solución detectar errores lógicos y macros dentro de los documentos?		
Manejo de archivos	¿Puede la solución escanear cientos de tipos de archivos diferentes?		
	¿La solución permite al usuario escanear manualmente archivos y enlaces con una herramienta de arrastrar y soltar?		
	¿La solución descomprime el contenido recursivamente, buscando enlaces y archivos incrustados para escanear?		
	¿La tecnología de la solución para escanear enlaces y archivos incrustados es capaz de tener al menos 10 capas de profundidad?		
	¿La solución puede escanear contenido protegido por contraseña?		
	¿Puede la solución escanear archivos comprimidos/comprimidos?		
Situación del mercado	¿Se ha incluido la solución en la Guía de mercado para la seguridad del correo electrónico de Gartner?		
	¿La solución ocupó el primer lugar cuando un analista externo conocido la probó con otros competidores del mercado?		
	¿Es la empresa un socio avanzado de AWS?		
Usabilidad.			
Servicio alojado en la nube	¿La solución es nativa de la nube y está totalmente alojada en la nube?		
	¿La solución se actualiza automáticamente?		
	¿Puede la solución satisfacer las necesidades de escalado de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales?		
Instalación	¿Se puede implementar la solución en modo de prevención de amenazas, previniendo las amenazas antes de que lleguen a los usuarios finales?		
	¿Se puede implementar la solución en modo BCC/Registro en diario, así como en línea para una protección completa?		
	¿Se puede implementar la solución para los usuarios a través de una invitación por correo electrónico?		

	¿Se puede implementar la solución automáticamente con la integración de Office 365?		
Integración	¿Puede la solución conectarse mediante API a otras aplicaciones?		
	¿La solución se integra sin problemas con Office 365 a través de API sin necesidad de cambiar el registro MX?		
	¿El sistema se ajusta a las políticas y SIEM existentes y no requiere cambios de infraestructura?		
	¿Es posible exportar registros en tiempo real al SIEM de una organización?		
	¿La solución se integra con la gestión de identidad de la organización a través de SAML?		
	¿Se asignan automáticamente a los usuarios permisos para roles y grupos en función de un esquema RBAC?		
	¿Puede la solución escanear las bandejas de entrada locales?		
	¿La empresa ofrece servicios adicionales para proteger el uso del almacenamiento compartido, las herramientas de colaboración y el navegador por parte del cliente?		
Manejo de datos	¿La solución cifra los datos en reposo con AES-256 y en tránsito con TLS 1.2+?		
	¿Las claves de cifrado están protegidas con AWS KMS?		
	¿Cumple la solución con todo lo siguiente: SOC2, RGPD, HIPAA, CCPA?		
	¿La solución aloja datos en servidores separados ubicados en Europa, EE. UU. y APAC?		
Manejabilidad	¿La solución proporciona un tablero de administración informativo que muestra datos, informes y políticas de incidentes?		
	¿La solución puede incluirse en la lista blanca/negra en función de IP, URL, dominios, remitentes, tipos de archivo y más?		
	¿El sistema registra las acciones de los usuarios, como los intentos de inicio de sesión, los cambios de veredicto, la publicación de correos electrónicos y las solicitudes de investigación?		
	¿Puede el cliente personalizar pancartas y alertas de advertencia y traducir a otros idiomas además del inglés?		
	¿Puede un usuario reportar fácilmente una sospecha de falso positivo o falso negativo para que el sistema la revise?		
	¿La solución envía informes de acción y resúmenes a los usuarios?		
Servicio.			

Respuesta a incidentes	¿Cuenta la empresa con un equipo de IR interno que refuerce los servicios de detección y remediación?		
	¿La solución brinda servicios de equipo de IR complementarios como parte de su oferta sin cargo adicional?		
Atención al cliente	¿La solución ofrece atención al cliente y capacitación ilimitadas según sea necesario sin cargos adicionales?		
	¿La atención al cliente está disponible las 24 horas, los 7 días de la semana por correo electrónico, chat y teléfono?		