|  |  |  |
| --- | --- | --- |
| **Funcionalidades** | **Nombre de la Solución: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **Si** | **No** |
| Bloqueo de un dominio identificado como malicioso |  |  |
| Bloqueo de dominios potencialmente maliciosos / sospechosos |  |  |
| Almacena registro de todas las peticiones DNS detectadas (maliciosas, sospechosas y legítimas) |  |  |
| Almacena registro de todas las peticiones DNS maliciosas detectadas |  |  |
| Generación de alertas o algún indicador visual de un potencial incidente / detección de petición DNS para los analistas |  |  |
| Configuración personalizable de alertas o indicador visual ante la detección de una determinada petición DNS a un determinado dominio. |  |  |
| Envío de alertas o notificaciones a través mensajes de correo electrónico |  |  |
| Almacena registros de peticiones durante \_\_\_\_\_\_\_\_\_ días o \_\_\_\_\_\_\_\_ MB (dejar en blanco si no lo hace) | | |
| Manejar múltiples Organizaciones (Multi-tenant) |  |  |
| Administrar redes, segmentos y políticas de otras organizaciones de manera centralizada |  |  |
| Filtrar registros de petición de DNS por IP |  |  |
| Filtrar registros de DNS por organización |  |  |
| Elaborar zonas DNS customizables |  |  |
| Exportación de logs o registros de peticiones DNS |  |  |
| Se integra o incluye al menos una fuente de listas de dominios maliciosos conocidos, mantenida por una organización o comunidad de inteligencia de amenazas |  |  |
| Integración con fuentes externas existentes de Listas de dominios maliciosos conocidos (URL Haus, Talos, etc.) |  |  |
| Integración con fuentes personalizadas a través de APIs |  |  |
| Integración con herramientas tipo SIEM (Elastic, Splunk, etc) |  |  |
| Dashboard de Visualización General y global para todas las organizaciones |  |  |
| Dashboard segmentado por organización, con accesos/roles por organización |  |  |