Corresponde al expediente N° EX-2021-27239710-GDEBA-DPTAARBA

PROCESO DE COMPRA N° 382-0126-CDI22

ANEXO I - ESPECIFICACIONES TÉCNICAS BÁSICAS

CARACTERÍSTICAS TÉCNICAS:

- Detección de ataques mediante analítica avanzada, combinando análisis de comportamiento, técnicas de Inteligencia Artificial y reglas modificables por el usuario.
- Agrupamiento automático de alertas relacionadas, para disminuir el esfuerzo manual de análisis de problemas.
- Herramientas de investigación rápida, que permitan encontrar y visualizar la causa raíz del problema detectado.
- Agente liviano con bajo consumo de recursos de procesamiento y memoria.
- Detección de amenazas aún no clasificadas, basada en comportamiento, con análisis local en el agente más procesamiento adicional en servidores.
- Generación local de perfiles de comportamiento típicos en el puesto de trabajo, para detectar desvíos sospechosos en el comportamiento del software.
- Agente con distribución sencilla a través de la nube, sin configuración por parte del usuario.
- Aplicación de técnicas de Machine Learning sobre el comportamiento del puesto de trabajo, con datos compartidos dentro de la organización y aportes de aprendizaje adquirido por el fabricante, para descubrir ataques del tipo encubierto.
- Clasificación y de-duplicación de información de alertas presentadas a los administradores, para facilitar la gestión de grandes números de incidentes con características similares.
- Capacidad en el agente de recolección de información adicional y control centralizado, para que los administradores puedan diagnosticar efectivamente los incidentes y tomar acciones remotas de remediación.
- Integración con base de datos de conocimiento en línea del fabricante (Wildfire), para complementar las capacidades locales de detección y prevención, y para recibir actualizaciones en tiempo real durante la vigencia de la suscripción
- Agente nativo único, con capacidades de prevención de exploits, malware, ransomware, ataques fileless y recolección de datos, y análisis de comportamiento

con correlación entre procesos activos.

- Aplicación centralizada de políticas con control granular de uso de dispositivos USB, basado en múltiples criterios, y posibilidad de integración con información de Active Directory.
- Gestión centralizada de firewall tipo Host y de encripción de discos.
- Capacidad de aplicación de alertas generadas por terceros para ampliar la base de conocimientos relacionada con protección y detección de amenazas.
- Capacidad de recolección de logs a nivel servidor, para complementar la información utilizada para detectar ataques, incluyendo análisis de tráfico de red, detección en puesto de trabajo y análisis de comportamiento de usuario.
- Capacidad de administración de las tareas dentro de un equipo de trabajo definido por el usuario, con asignación de problemas a distintos administradores o agentes, y su posterior seguimiento hasta la resolución o cierre.
- Reportes a nivel consola central, con distintos criterios de selección y lenguaje de consultas, con posibilidad de guardar las consultas elaboradas para posterior uso.
- Consola de administración accesible a través de la nube, con autenticación y autorización definible por el usuario, que contenga paneles configurables para cada agente y con herramientas para trabajo colaborativo.
- Agente con capacidades de ejecución remota desde la consola central, comandada por los administradores, con compatibilidad para ejecutar remotamente scripts de
- PowerShell, Python o comandos del sistema operativo, gestor de archivos gráfico remoto con capacidad de lectura y escritura, y gestor de procesos en ejecución.
- Capacidad de búsquedas desatendidas en puestos de trabajo, disparadas desde la consola central con criterios definidos por el usuario.
- Almacenamiento en nube para la recolección de datos asociados a ataques, logs y demás información de utilidad disponible en las herramientas.
- Posibilidad de aislamiento preventivo de puestos de trabajo, sin perder el acceso desde la consola central.
- Terminal interactiva en línea para acceso remoto a puestos de trabajo.
- Disponibilidad de APIs para respuesta a incidentes y recolección de datos.
- Protección contra robo de credenciales.

- Escaneos de malware programados o inmediatos.
- Actualizaciones de agentes comandada desde la consola de administración
- Capacidad de recibir e interpretar logs de dispositivos de Cisco, Fortinet, CheckPoint, PaloAlto y Windows Event Collector.
- Gestión centralizada de agentes de puestos de trabajo.
- Paneles de control y reportes configurables.