AJUNTAMENT DE CALVIÀ
MALLORCA

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA ADQUISICIÓN SISTEMA PARA ANALIZAR DOCUMENTACIÓN EN FORMATO DIGITAL, MEDIANTE TÉCNICAS DE SANDBOXING

PRIMERA.- OBJETO DEL CONTRATO.

El Ajuntament de Calvià, en pleno proceso de digitalización, necesita adquirir un sistema para analizar (mediante técnicas de sandboxing) la documentación en formato digital aportada por la ciudadanía. Además, el sistema a adquirir debe posibilitar la integración nativa con la infraestructura de seguridad perimetral existente.

CPV.: 48731000-1 Paquetes de software de seguridad de archivos

SEGUNDA.- REQUERIMIENTOS TÉCNICOS

En la actualidad, el Ajuntament dispone de 5 firewalls Fortigate del fabricante Fortinet, cuyos logs se centralizan en un dispositivo Fortianalyzer.

El sistema de sandbox a adquirir ha de proporcionar una capa de seguridad contra amenazas avanzadas (malware, URL y amenazas desconocidas, incluyendo las Zero day), pudiendo también compartir esta información con otros equipos. Ha de utilizar técnicas de IA, sandboxing en VM personalizadas y técnicas antievasión para conseguir identificar todo tipo de código malicioso (malware).

Ha de proporcionar los servicios y características siguientes:

- Análisis bajo demanda de URL y ficheros.
- Capacidad de conexión de forma proactiva a carpetas compartidas para buscar código malicioso y enlaces maliciosos.
- Capacidad de sniffer para todo el tráfico PCAP.
- Capacidad de MTA integrada para SMTP.
- Sandboxing en diferentes sistemas operativos.
- La solución deberá disponer de certificaciones y recomendaciones de NSS Labs e ICSA Labs.
- Se deberá poder desplegar en un entorno VMware ESXi, a proporcionar por parte del Ajuntament.
- Funcionalidades ATP (Advanced Threat Protection):
    - Inspección de nuevas amenazas, incluido ramsonware y mitigación de malware protegido por contraseña.
    - Análisis de código estático impulsado por aprendizaje automático (ML) que identifica posibles amenazas dentro del código que no se ejecuta.
    - Análisis heurístico/basado en patrones/reputación.
    - Perfil de escaneo adaptable inteligente que optimice los recursos de la zona de pruebas en función de los envíos.
    - Tasa de escaneo de VM para una utilización eficiente de las VM.
    - Módulo de escaneo dinámico impulsado por Deep Learning (Pexbox) para emular códigos ejecutables de Windows.
    - Escaneo paralelo para ejecutar varios tipos distintos de VM.

- Integración nativa con FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM y sus versiones equivalentes encriptadas con SSL.
- Servicios OT compatibles: tftp, modbus, s7comm, http, snmp, bacnet, ipmi.
- Detección de amenazas de red en modo Sniffer: identificación de las actividades de la botnet y los ataques a la red y visita de URL maliciosas.
- Escaneo manual o programado de recursos compartidos de almacenamiento SMB / NFS, AWS S3 y Azure Blob y cuarentena de archivos sospechosos.
- Escaneo de URL incrustadas dentro de archivos de documentos.
- Capacidad para configurar prioridades de inspección.
- Capacidad de aislamiento del tráfico de imágenes de VM del tráfico del sistema.
- Soporte de, como mínimo, los siguientes tipos de ficheros:
  - Ejecutables: BAT, CMD, DLL, EML, EXE, JAR, JSE, MSI, PS1, UPX, WSF y VBS.
  - Compresión: 7Z, ARB, BZIP, BZIP2, CAB, ISO, EML, GZIP, LZW, RAR, TAR, XZ, ZIP y variantes. Debe tener capacidad para extraer hasta un mínimo de 6 niveles de compresión anidados.
  - Toda la suite de MS Office: Word, Excel, Powerpoint, Outlook, etc.
  - Otros: PDF, SWF, HTML, JS, LNK, APK, DMG, AP, MACH-O, APP, MSI.
- Sandbox de SO virtual:
  - Análisis de comportamiento impulsado por ML que aprende constantemente nuevas técnicas de malware y ransomware o instancias concurrentes.
  - Tipo de sistema operativo compatible: sistemas Windows 10, Windows 8.1, Windows 7, macOS, Linux, Android e ICS.
  - Posibilidad de personalización de las máquinas virtuales con aplicaciones propias y sistemas operativos Windows y Linux.
  - Técnicas anti-evasión: llamadas de suspensión, procesos, consultas de registro y más.
  - Detección de devolución de llamada: visita de URL maliciosa, comunicación de C&C de botnet y tráfico de atacantes de malware activado.
  - Descargar paquetes de captura, archivo original, registro de seguimiento y captura de pantalla.
  - Modo interactivo Sandbox o grabación de video de la interacción del malware

- Integraciones
  - API JSON para automatizar la carga de muestras y la descarga de indicadores de malware procesables para remediar.
  - Entrada de envío de archivos de FortiGate.
  - Ingesta de IOC (hashes, Yara Rules, etc.)
  - Compartición centralizada de IOC (hashes, URL, Threat Intelligence, MITRE ATT&CK Matrix, etc.)
  - Integración con ICAP con proxies y balanceadores.
  - Integración nativa con Fortianalyzer.
- Administración
  - Admitirá configuraciones de GUI y CLI.
  - Permitirá la creación de múltiples cuentas de administrador.
  - Ha de permitir copia de seguridad y restauración del archivo de configuración.

  - Capacidad de notificación por correo electrónico cuando se detecta un archivo malicioso.
  - Capacidad de envío de informes periódicos a listas de correo electrónico.
  - Página de búsqueda centralizada que permita a los administradores crear condiciones de búsqueda personalizadas.
  - Actualizaciones automáticas frecuentes de firmas.
  - Comprobación y descarga automática de nuevas imágenes de VM.
  - Supervisión del estado de la máquina virtual.
  - Autenticación Radius para administradores.
  - Gestión de clústeres para administrar HA-Cluster.
  - Sistema de alerta para la verificación del estado del sistema.
- Visibilidad y dashboard:
  - Debe proporcionar gráficas y tablas de visibilidad, tanto del conjunto de equipos como del detalle de las amenazas.
  - Debe disponer de un dashboard donde se muestre información global de la plataforma, por ejemplo la distribución de código malicioso detectado.
  - Informes detallados con información forense de cada muestra.
  - Información en tiempo real de amenazas y conexión a herramientas de gestión.
  - Debe disponer de informes detallados de los ficheros inspeccionados, incluyendo todas las categorías. Del mismo modo, se debe poder acceder a los informes detallados y descargar el informe en formato PDF.
  - Se ha de disponer del detalle de todo el proceso de análisis temporal y mostrar el ataque con la matriz MITRE ATTA&CK, así como el detalle del IOC creado.
  - Disponer, en tiempo real, de:
    - Información categorizada.
    - Todas las amenazas ordenadas por fecha y tipo.
    - Fuentes del sandbox y ordenar el código malicioso según su origen (mail, proxy, firewall, etc.) y localización geográfica.

- Deberá reunir las siguientes capacidades:
  - Deberá tener capacidad para ejecutar, como mínimo, 8 VM simultáneas.
  - Se deberá incluir el licenciamiento correspondiente a 2 VM con sistema operativo licenciado.
  - Capacidad de 1 Gbps de sniffer.

Se debe incluir el licenciamiento necesario para que se pueda desplegar el sistema de sandbox en el entorno VMware del Ajuntament, cumpliendo con todas las características descritas y con derecho a actualizaciones de firmas y a nuevas versiones de firmware durante un periodo mínimo de 12 meses

TERCERA. DOCUMENTACIÓN.

Las empresas presentarán la siguiente documentación técnica:

- Características técnicas del servicio de mantenimiento ofertado.
- Cualquier otra documentación que se considere de interés.
- Oferta económica, detallando los precios por equipos.

CUARTA.- PRESUPUESTO Y FORMA DE PAGO.

El presupuesto máximo de licitación, para la totalidad del servicio será de doce mil seiscientos euros (12.600€ euros), base imponible, al que corresponde dos mil seiscientos cuarenta y seis euros (2.646 €) como 21% de IVA, lo que asciende a un total de quince mil doscientos cuarenta y seis euros (15.246 €), que irán con cargo a la partida 202/92201/6260001 "Adquisición aplicaciones informáticas" correspondiente al ejercicio 2022.

El pago del precio acordado se realizará contra la presentación de la correspondiente factura, debiendo estar conformada por el técnico responsable del contrato.

QUINTA- CRITERIOS DE VALORACIÓN.

El criterio de adjudicación del presente contrato menor será el económico.

Los licitadores deberán especificar en sus ofertas: los precios por equipos, y el importe total del servicio desglosado, detallando la base imponible, el importe de IVA correspondiente y el importe total de su oferta con el IVA incluido.

La valoración de las ofertas se efectuará de la siguiente manera:
Mejor oferta económica: hasta 100 puntos. Se valorará en función de la oferta efectuada, adjudicándose la totalidad de los puntos a la empresa que oferte el importe más económico, y puntuando al resto de las ofertas de forma proporcional, mediante la siguiente fórmula, la cual se aplicará sobre el importe total sin IVA:

Puntuación = 100 x (Importe de la oferta más económica / Importe de la oferta)

SEXTA- PLAZO DE EJECUCIÓN

Los productos serán entregados telemáticamente en un plazo máximo de 15 días a contar desde la fecha de la firma del contrato.

SÉPTIMA.- INSPECCIÓN Y DIRECCIÓN DE LOS TRABAJOS.

La prestación del suministro se realizará bajo la dirección e inspección del Jefe del Servicio de Informática y Nuevas Tecnologías o persona en quien delegue.

Calvià,

Francisco Javier Mir Jaume
Jefe de Servicio de Informática y Nueva Tecnologías