Enpresa-Garapenerako Euskal Agentzia
Agencia Vasca de Desarrollo Empresarial
Business Development Basque Agency
www.spri.eus

SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL

PLIEGO PRESCRIPCIONES TECNICAS

SUMINISTRO DE LICENCIAS Y PRESTACIÓN DEL SERVICIO DE SEGURIDAD DETECCIÓN Y RESPUESTA ENDPOINT

SUMARIO

1. OBJETO DEL CONTRATO 3
2. SITUACIÓN ACTUAL 3
3. ESPECIFICACIONES TÉCNICAS 3
S1: Suministro anual de licencias de agentes EDR 3
S2: Servicio de monitorización, análisis y contención de incidentes 4
S3: Servicio de instalación y mantenimiento de agentes EDR 4

1. OBJETO DEL CONTRATO

SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL (en adelante, "**SPRI**") actualmente dispone de un contrato para el suministro de un servicio de seguridad detección y respuesta endpoint (*Endpoint Detection and Response as a Service* - EDRaaS -) cuya fecha fin es el 31 de marzo de 2023.

El objeto de la presente licitación es la contratación del servicio de seguridad detección y respuesta endpoint (*Endpoint Detection and Response as a Service* - EDRaaS -) para el parque de dispositivos del Grupo SPRI como continuación del servicio disponible actualmente.

Para ello, se proveerán los siguientes suministros y servicios, que en cada caso corresponda y cuya descripción técnica se desarrolla en apartados posteriores:

- SUMINISTRO1: suministro anual de licencias de agentes EDR (en adelante, "**SUMINISTRO 1" o "S1".**
- SERVICIO 2: servicio de instalación y mantenimiento de agentes EDR (en adelante, "**SERVICIO 2**" o "**S2**").
- SERVICIO 3: servicio de monitorización, análisis y contención de incidentes (en adelante, "**SERVICIO 3**" o "**S3**")).

2. SITUACIÓN ACTUAL

SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL dispone actualmente de un agente EDR (*Endpoint Detection and Response*) de la marca *FireEye (FireEye Endpoint Security Agent*) instalado en el parque de equipos de trabajo (equipos portátiles y PCs de sobremesa), y servidores, sumando estos un total de 400 equipos.

Los equipos de uso personal y determinados servidores disponen actualmente de un antivirus (como complemento al agente EDR). En el caso de los servidores se valorará la posibilidad de la desinstalación del antivirus actual y activar el módulo de antivirus disponible con FireEye.

Adicionalmente, se dispone de un servicio EDRaaS el cual dispone de un despliegue de una tecnología Endpoint Detection & Response (EDR), monitorización 7x24 y operación de la herramienta que detecta amenazas basada en comportamiento. Todos los equipos están registrados (a través de ese agente EDR), y monitorizados en consola del fabricante (FireEye Hx).

3. ESPECIFICACIONES TÉCNICAS

SUMINISTRO1: Suministro anual de licencias de agentes EDR

Licencias *FireEye* hasta 500 dispositivos, siendo los requisitos mínimos de versión soportada:

Sistema Operativo	Versión
Windows	Win 10 (32-bit and 64-bit)
	Server 2003 R2 SP2 (32-bit and 64-bit)

	Server 2008 (32-bit and 64-bit) Server 2008 R2, R2 SP1, R2 SP2 (64-bit) Server 2012 (32-bit and 64-bit) Server 2012 R2 (32-bit and 64-bit) Server 2016 (32-bit and 64-bit)
Linux	RHEL 6.8+, 7.2+, 8 (64-bit) CentOS 6.9+, 7.2+, 8 (64-bit) Ubuntu 14.04, 16.04, 18.04, 19.04 Oracle Linux 6.10, 7.6

A continuación, ofrecemos los códigos *part number* del fabricante de los productos a suministrar:

part number	Descripción de licencia
EP-E-P-2W-PTM-999-1Y	Endpoint Security Ent Pwr Ed 2- Way w/PTM sppt, per Endpoint
EP-P-C-1Y	Endpoint Security Cloud Power Edition

SERVICIO 2: Servicio de instalación y mantenimiento de agentes EDR

Será responsabilidad de la empresa adjudicataria el despliegue de los agentes EDR, así como las actualizaciones de estos, dotándose al servicio a tal efecto de una bolsa de horas (en las condiciones descriptas en pliego de cláusulas administrativas).

Como se indica en el apartado 2, correspondiente a la "SITUACIÓN ACTUAL", los equipos se encuentran registrados (a través de los agentes EDR) en una consola única del fabricante. El despliegue de nuevos agentes EDR, en su caso, debe realizarse en la consola actual del fabricante.

Se valorará la activación del módulo de antivirus disponible para el agente EDR en los equipos de tipo servidor, siendo responsabilidad de la empresa adjudicataria la desinstalación de la solución de antivirus instalada en la actualidad, y la activación del nuevo módulo de antivirus.

SERVICIO 3: Servicio de monitorización, análisis y contención de incidentes

Se deberá proveer un servicio de monitorización, análisis y contención de incidentes para los agentes EDR FireEye instalados con los siguientes requerimientos mínimos:

- Gestión centralizada desde la consola del fabricante FireEye Hx Cloud (no se admitirá el despliegue de la solución en nube de la empresa licitadora).
- Monitorización 24x7 de todos los activos (hasta 500 *endpoints*).
- Definición de un conjunto de equipos críticos para análisis en 24x7.

- Análisis 8x5 de todos los activos (un mínimo 20 análisis).
- Análisis 24x7 de activos críticos (al menos 2 análisis para un mínimo del 10% de activos).
- Contención de dispositivos afectados por una amenaza dentro del alcance del servicio, y contención automática de activos no críticos en menos de 5 minutos.
- Inyección de inteligencia específica:
    - Inyección de IOCs (indicadores de compromiso) en consola de FireEye Hx.
    - Extracción de IOCs propios derivados de las investigaciones.
- Análisis proactivo de amenazas y *malware*.
- Gestión de incidencias, peticiones y seguimiento de tickets a través de un Centro de Operaciones de Seguridad (SOC).

Se deberá desarrollar, al menos, las siguientes actividades de seguimiento:

- Elaboración de informes técnicos de los servicios mensualmente.
- Reuniones mensuales de seguimiento de servicio.
- Reuniones de trabajo técnicas trimestrales para tratar temas relacionados con el servicio determinados por SPRI.