ANEXO A1

SOLUCIONES PARA LA DETECCIÓN, RESPUESTA, ANÁLISIS E INVESTIGACIÓN DE PUNTOS FINALES, COLECCIÓN DE EVENTOS Y DETECCIÓN DE AMENAZAS AVANZADAS DE LA RED Y ACTUALIZACIONES Y DISTRIBUCIONES DE SOFTWARE.

1. SOLUCIÓN PARA LA DETECCIÓN, RESPUESTA, ANÁLISIS E INVESTIGACIÓN DE PUNTOS FINALES.

A. Características Generales

1. La solución para la detección, respuesta, análisis e investigación de puntos finales - Cortex XDR PRO per endpoint de la marca palo alto (marca estandarizada por la entidad), o equivalente[1] debe esta licenciada por un periodo de mil noventa y cinco (1095) días calendario.
2. Debe contar con la capacidad de realizar análisis e investigación de puntos finales como mínimo en 200 equipos mediante el Forencis add–on for Cortex XDR per Endpoint, por un periodo de mil noventa y cinco (1095) días calendario, permitiendo intercambiar esta capacidad entre los 3500 dispositivos según la necesidad.

Descripción	Marca	Cantidad
Cortex XDR PRO per endpoint de la marca Palo Alto (marca estandarizada por la entidad), o equivalente	Palo Alto	3500

2. SOLUCIÓN PARA LA COLECCIÓN DE EVENTOS Y DETECCIÓN DE AMENAZAS AVANZADAS DE LA RED.

A. Características Generales

1. La solución para la colección de eventos y detección de amenazas avanzadas de la red - Cortex XDR PRO per TB de la marca Palo Alto (marca estandarizada por la entidad), o equivalente[2], debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario según el siguiente detalle:

Descripción	Marca	Cantidad
Cortex XDR PRO per TB de la marca Palo Alto (marca estandarizada por la entidad), o equivalente	Palo Alto	10TB

3. SOLUCION PARA FILTRO DE NAVEGACIÓN.

A. Características Generales

1. La solución de seguridad de red para teletrabajo - Prisma Access for users de la marca Palo Alto (marca estandarizada por la entidad), o

[1] Informe Técnico de Estandarización N° 001-2022-EF/OGTI, aprobado mediante Resolución Directoral N° 181-2022-EF/43.01
[2] Informe Técnico de Estandarización N° 001-2022-EF/OGTI, aprobado mediante Resolución Directoral N° 181-2022-EF/43.01

equivalente[3] debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario según el siguiente detalle:

Descripción	Marca	Cantidad
Prisma Access for users de la marca Palo Alto (marca estandarizada por la entidad), o equivalente	Palo Alto	2500

4. SOLUCIÓN DE ORQUESTACIÓN DE SEGURIDAD, AUTOMATIZACIÓN Y RESPUESTA (SOAR)

1. Debe estar licenciada por un para un (01) analista por un periodo mil noventa y cinco (1095) días calendario.
2. Debe incluir una tecnología SOAR para la automatización de respuesta ante incidentes. Esta tecnología deberá ser totalmente integrable con soluciones SIEM.
3. Debe soportar investigaciones interactivas que permitan la colaboración, la revisión histórica y la documentación en tiempo real de todas las acciones.
4. Debe soportar flujos de trabajo y secuencias de comandos modulares.
5. Debe automatizar las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos.
6. Debe soportar investigaciones interactivas que permitan colaboración, revisión histórica y ejecución en tiempo real y documentación de todas las acciones.
7. Para cualquier acción de seguridad, debe ofrecer flexibilidad para automatizar o manualmente ejecutar en tiempo real según los requisitos del caso de uso.
8. La automatización se debe lograr utilizando flujos de trabajo modulares y scripts.
9. Las tareas automatizadas se deben visualizar en flujos de trabajo basados en interfaz gráfica y ser impulsadas por scripts de automatización en el backend.
10. Cualquier script puede ser adjunto a una tarea automatizada dentro de flujos o playbooks visuales. La cantidad de playbooks a configurar será de 10 aparte de los que vienen por defecto en la solución y las tecnologías a integrarse con el SOAR son las siguientes:

    - **Solución de gestión de identidades de la infraestructura tecnológica del MEF**

        - Software de gestión de identidades, provisionamiento y roles.
        - Software de autenticación Multifactor.

    - **Solución gestión de riesgos de seguridad de TI.**

        - Software de Gestión de Riesgo de seguridad de TI.

    - **Solución para el descubrimiento predictivo de amenazas avanzadas con fuentes de datos estructurados y no estructurados de la infraestructura del MEF**

[3] Informe Técnico de Estandarización N° 001-2022-EF/OGTI, aprobado mediante Resolución Directoral N° 181-2022-EF/43.01

- Solución para el descubrimiento predictivo de amenazas avanzadas con fuentes de datos estructurados y no estructurados.

- **Solución de ciberseguridad para la protección avanzada de correo de la infraestructura tecnológica del ministerio de Economía y Finanzas**

  - Servidor virtual Filtro para correo electrónico

- **Solución de ciberseguridad para la prevención de fuga de información de la infraestructura tecnológica del Ministerio de Economía y Finanzas.**
  - Software de fuga de información (DLP).
  - Sensor de red prevención de fuga de información (DLP).

- **Soluciones de ciberseguridad para la administración de dispositivos móviles, control acceso de cuentas privilegiadas y asistencia remota de la infraestructura tecnológica del Ministerio de Economía y Finanzas.**

  - Administración de Dispositivos Móviles (MDM)
  - Control de cuentas privilegiadas
  - Software de asistencia remota – Remote Support de la marca BeyondTrust (marca estandarizada por la entidad), o equivalente

- **Soluciones para la detección, respuesta, análisis e investigación de puntos finales, colección de eventos y detección de amenazas avanzadas de la red y actualizaciones y distribuciones de software.**

  - Solución para la detección, respuesta, análisis e investigación de puntos finales.
  - Solución para la colección de eventos y detección de amenazas avanzadas de la red.
  - Solución para filtro de navegación.
  - Solución de actualizaciones y distribuciones de software.

- **soluciones de ciberseguridad de balanceador de aplicaciones y HSM de la infraestructura tecnológica del Ministerio de Economía y Finanzas**

  - Solución balanceador de Aplicaciones
  - Solución HSM
  - Servidor de consola de administración

- **Soluciones de ciberseguridad para la protección de servicios web y base de datos de la infraestructura tecnológica del MEF**

  - Firewall de aplicaciones (WAF).
  - Firewall de Base de datos (DBF).
  - Servidor de consola de administración.

- **Soluciones de ciberseguridad para la protección de ambientes virtuales de la infraestructura tecnológica del MEF**

  - Sofware de ambientes SDDC(Firewall Virtual).
  - Sofware de Gestor de Contenedores.

- **Soluciones de ciberseguridad para el desarrollo seguro de aplicaciones en la infraestructura tecnológica del MEF**

  - Software gestión de código.

- Software escáner de vulnerabilidades de infraestructura.
- Software análisis de código estático.
- Análisis de seguridad aplicativo web.
- Software análisis de binarios.

- **Soluciones de ciberseguridad para la toma de evidencias digitales de la infraestructura tecnológica del MEF**

  - Software de extracción de datos de computadoras.
  - Equipo de extracción de datos dispositivos.
  - software de análisis de datos digitales extraídos.
  - Servidor de análisis de datos extraídos FRED.

11. Debe ser compatible con Python y JavaScript, debe tener la capacidad de exportar paquetes de Python a Dockers (de preferencia) o contenedores para que librerías de Python existentes puedan ser reutilizadas.
12. Debe incluir una función "BYOI" o similar que permita a los analistas escribir sus propias integraciones a través de un SDK interno y un wizard.
13. Debe incluir nuevas integraciones de productos y automatizaciones automáticas como parte de actualizaciones de contenido.
14. La herramienta debe contar con un mínimo de 100 casos de usos o playbooks de respuesta a incidentes
15. Los playbooks deben ser de código abierto.
16. Debe permitir crear playbooks copiando flujos existentes, debe poseer una interface sencilla de utilizar que permita realizar drag-and-drop de acciones u otros flujos/playbooks
17. Debe permitir embeber un playbook dentro de otro, de forma de que este sea reutilizado continuamente.
18. Un playbook puede contener acciones totalmente automatizadas o tareas manuales, tareas de collection de datos o tareas condicionadas.
19. Los playbooks pueden ser ejecutadas automáticamente al crear un incidente y asociadno al playbook correspondiente
20. Los playbooks también pueden ser ejecutados como tareas y ejecutados en tiempo real para casos de uso como health checks.
21. La ejecución de los playbooks y la actividad relacionada por el analista debe ser automáticamente documentada para cada incidente de seguridad.
22. La herramienta debe de tener la capacidad de ejecutar flujos/playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario.
23. Las acciones de los playbooks deben ser totalmente personalizables por el usuario y deben poder utilizarse para adherirse a cualquier requisito de proceso organizacional o industrial.
24. Debe poseer la capacidad de asignar a cualquiera de los usuarios disponibles en el sistema basado en las capacidades RBAC.
25. La herramienta debe tener un API capaz de ejecutar las mismas funciones que la interfaz gráfica.
26. Debe soportar un despliegue on-premise permitiendo que toda la data que se produzca en la organización no salga de las premisas
27. Debe soportar un despliegue permitiendo la integración con plataformas en la nube con la solución on-premise de SOAR.
28. Debe incluir una instancia donde usuarios puedan ver evidencia y documentación de incidentes anteriores, la herramienta debe agregar información de investigaciones pasadas.

29. Debe detectar alertas redundantes y agregar incidentes duplicados en uno solo, desplegando los datos de la agregación realizada.
30. Como parte de un incidente, la herramienta debe documentar cualquier cambio, los analistas parte del incidente, tareas terminadas, comandos de interacción, evidencia, chats (opcional), notas y tareas de playblooks.
31. Los usuarios pueden marcar resultados de comandos o notas como evidencia, o automatizar la recolección de evidencia dentro de un playbook.
32. Toda la información a recolectar debe ser inmutable y no debe ser modificada, la documentación debe ser exportable para producir un documento de cadena de custodia.
33. Los analistas deben poder ver todos los indicadores de compromiso y el detalle alrededor de ellos deben poder asociados a las distintas fases del ataque o kill chain.
34. Los analistas deben ser capaces de utilizar campos customizados para por ejemplo atribuir indicadores a campañas de ataque.
35. El producto debe proveer herramientas de colaboración entre usuarios, debe agrupar a todos los usuarios asociados a un incidente dentro del mismo o en un cuarto de guerra.
36. Los analistas deberán poder colaborar uno con otro usando la línea de comando dentro de la investigación de un incidente.
37. La colaboración puede ser extendida a grupos o equipos de trabajo terceros, como usuarios internos, grupos de recursos humanos, PR, o terceros.
38. Las tareas realizadas dentro de incidentes deben de ser respaldadas para que sirvan de documentación para entrenar a nuevos analistas
39. La herramienta debe incluir un Canvas de investigación dentro de la solución ofertada o como componente adicional que pueda integrarse, el cual mediante machine learning pueda crear un mapa de ataques en tiempo real.
40. Los resultados de los canvas deben ser exportados y compartidos por equipos ejecutivos e interesados.
41. El producto debe correlacionar bidireccionalmente indicadores e incidentes. Los usuarios deben poder ver todos los indicadores de un incidente y viceversa.
42. La plataforma debe incluir playbooks de threat hunting, que puedan ser ejecutados utilizando indicadores de compromiso, también se aceptará que el playbook de threat hunting pueda ser desarrollado y configurado por el proveedor, debiendo este contar un estándar de calidad y seguridad que deberá ser presentado en el plan de trabajo y sin ningún costo adicional.
43. Debe ser posible importar y exportar indicadores en archivos STIX.
44. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.

5. SOLUCIÓN DE ACTUALIZACIONES Y DISTRIBUCIONES DE SOFTWARE

A. Características Generales

1. Debe estar licenciada para 3500 dispositivos por un periodo mil noventa y cinco (1095) días calendario.
2. Debe realizar el despliegue remoto de software.
3. Debe realizar un inventario de licencias de software.
4. Debe construir un perfil detallado de software y hardware instalado, inventario de red, parches faltantes de Microsoft, estado del antivirus (opcional), criterios de seguridad.

5. Debe detectar actualizaciones pendientes como mínimo para los siguientes tipos de software:
    - Sistemas Operativos (Windows 7, Windows 8.1, Windows 10, Red Hat Enterprice Linux).
    - Debe reconocer por lo menos 44 aplicaciones diferente, mínimamente que incluyan las siguientes: Microsoft Office, Adobe Reader, Adobe Acrobat Professional ,Adobe Air, Adobe Flash, Adobe Reader, Adobe Shockwave, Apache Tomcat, Apple iTunes, Citrix Receiver para Windows Enterprise, FileZilla Client, Foxit Enterprise Reader, Foxit Reader, Google Chrome, Mozilla Firefox, Mozilla Thunderbird, Notepad++, Oracle Java, QuickTime Player para Windows, RealPlayer, Skype, VLC Media Player,7-Zip,WinRAR, WinZip, Wireshark. Se aceptarán protocolos alternativos a DSSP para el monitoreo de sitios globales o geográficos
6. Debe poder integrarse al servidor de directorio.
7. Debe poder integrarse a soluciones SIEMS. La Integración de la solución con el SIEM puede realizarse a nivel del sistema operativo donde se encuentra instalada la solución siempre y cuando los eventos generados por la solución y todos los componentes que la integren sean enviados al SIEM.
8. Debe soportar instalar el agente como mínimo en sistemas operativos Windows 8.1, 10 y versiones de servidor como Windows 2012, 2016, 2019.
9. Debe soportar instalar el agente como mínimo en sistemas Linux RHEL 6, 7 y superior. Se considera como opcional para sistemas Linux RHEL 6
10. Debe contar con una consola de administración centralizada para la gestión de políticas y tareas que realizaran los agentes. Se aceptará que la solución sea desplegada en una arquitectura de nodos distribuidos siempre y cuando se cumpla con las especificaciones técnicas solicitadas.
11. El MEF facilitara el componente de GPO para el despliegue de agentes.
12. La entidad brindará el entorno virtual incluyendo la licencia de virtualización, así como también la licencia del sistema operativo (Windows o Linux), todo licenciamiento adicional necesario para la implementación deberá ser proporcionado como parte de la solución.