

ANEXO I-A

TÉRMINOS DE REFERENCIA DE CIBERSEGURIDAD

SOLUCIÓN INTEGRAL DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD PASIVA/ACTIVA (COCS) CON SOLUCIÓN ESPECIALIZADA DE DETECCIÓN Y ANÁLISIS

Contenido

I. OBJETIVO	2
II. CONSIDERACIONES GENERALES PARA LA PROPUESTA ECONÓMICA	2
III. CONCEPTOS A PRESUPUESTAR.....	3
1. Identificación y control de Amenazas Persistentes Avanzadas – APTs	3
2. Gestión continua de vulnerabilidades.....	3
3. Ciberpatrullaje.....	3
4. Pentest y análisis de vulnerabilidades	3
5. Solución especializada de detección y análisis.....	3
IV. ALCANCE Y CARACTERÍSTICAS DE LOS CONCEPTOS.....	3
1. Identificación y control de Amenazas Persistentes Avanzadas - APTs..	3
2. Gestión continua de vulnerabilidades	5
3. Ciberpatrullaje	9
4. Pentest y análisis de vulnerabilidades	10
5. Solución especializada de detección y análisis.....	12
V. PROCESO DE ATENCIÓN A VULNERABILIDADES Y/O DE HALLAZGOS RESULTANTES.....	16
VI. PERFILES QUE DEBE CUBRIR EL LICITANTE.....	17

I. OBJETIVO

El Centro de Operaciones de Ciberseguridad tiene como objetivo detectar las vulnerabilidades de la Red Internet Libre para la Gente, es decir, medir los niveles de seguridad perimetral de la red, esto por medio del personal de Gobierno del Estado y acompañado y capacitados durante un periodo de 12 meses por una empresa especializada en Ciberseguridad.

II. CONSIDERACIONES GENERALES PARA LA PROPUESTA ECONÓMICA

- Tiempo de implementación: EL LICITANTE ganador deberá llevar a cabo la implementación de las plataformas de software y hardware relacionadas con el presente servicio integral, en un tiempo máximo de 5 semanas contados a partir de la notificación del fallo.
- Tiempo de ejecución del Servicio: 12 meses a partir de la implementación.
- EL LICITANTE deberá considerar en su propuesta la capacitación a 5 colaboradores de Gobierno del Estado de Guanajuato, en cada uno de los conceptos que conforman el presente servicio integral, con el objetivo de fortalecer las capacidades e incrementar el nivel de especialización del personal de gobierno, responsable de las actividades en materia de ciberseguridad, para mejorar la prevención, detección, respuesta y recuperación en casos de eventualidades; dicha capacitación tendrá una duración total de 60 horas (12 horas para cada concepto), la cual deberá de ser impartida durante el segundo trimestre de la vigencia del servicio y podrá llevarse a cabo de manera virtual (online) o presencial en las oficinas de la Secretaría de Obra Pública, ubicadas en México 110, San José de Tránsito, Silao, Gto.
- El servicio tiene como alcance el monitoreo en al menos 4,000 dispositivos de acceso a la Red Internet Libre para la Gente.
- El servicio de monitoreo y administración de las plataformas se llevará a cabo 24x7x365 vía remota VPN site to site.
- EL LICITANTE deberá considerar que tanto las licencias ofertadas como el equipo de cómputo, serán propiedad de Gobierno del Estado al término de contrato a valor \$0.00 M.N. (cero pesos 00/100 M.N.) para las facturas correspondientes.

III. CONCEPTOS A PRESUPUESTAR

- 1. Identificación y control de Amenazas Persistentes Avanzadas – APTs**
- 2. Gestión continua de vulnerabilidades**
- 3. Ciberpatrullaje**
- 4. Pentest y análisis de vulnerabilidades**
- 5. Solución especializada de detección y análisis**

IV. ALCANCE Y CARACTERÍSTICAS DE LOS CONCEPTOS

1. Identificación y control de Amenazas Persistentes Avanzadas - APTs

La solución debe ser capaz de llevar a cabo protecciones en la dirección "Norte-Sur", para el tráfico entrante y saliente de la red estatal, y "Este-Oeste", para el tráfico interno de la red estatal.

Para el escenario de análisis de tráfico E-W (Este-Oeste), la solución debe proporcionar la detección de la actividad del atacante en la fase posterior a la exploración y el robo de datos/información que ocurre en redes internas o privadas. Debe admitir la funcionalidad NTA.

Debe ser capaz de detectar "Pasar el hash", sin archivos, enumeración de red, host y ataques de servicio, proporcionando así capacidades para la búsqueda de amenazas.

La solución debe tener, de forma predeterminada, una variedad de reglas de detección para el nivel de análisis de tráfico Este-Oeste.

La solución debe tener un motor de correlación avanzado, un motor analítico y utilizar técnicas de aprendizaje automático para detectar movimientos laterales sigilosos.

La solución debe escalarse para admitir Mbps de rendimiento definidos por la entidad.

La solución debe incluir reglas e inteligencia de amenazas.

La solución debe incluir un paquete de reglas estándar. Estos deben ser alimentados automáticamente directamente por el fabricante sin afectar la solución o incluir la intervención de los analistas.

La solución debe incluir la descripción de las familias de malware.

La solución debe proporcionar detalles sobre las alertas con asignaciones de marcos de seguridad de ATT&CK de MITRE.

EL LICITANTE debe tener expertos en seguridad que estén monitoreando las amenazas actuales y generen paquetes de reglas para ayudar a la solución ofrecida con la detección.

Debe tener la capacidad de enviar registros al equipo de soporte directamente desde la solución, sin necesidad de envíos externos, facilitando así el tiempo de respuesta y la resolución en caso de problemas.

La solución debe permitir que la ingesta de fuentes de terceros para integraciones de api, feeds (dominios, URLs y hashes) también deba importarse manualmente, en función de las fuentes importadas debe ser posible elegir una acción de bloqueo o supervisión.

Debe permitir que el software y el firmware se actualicen sin costo adicional

Debe contar con firmas de detección basadas en vulnerabilidades y también detección de ataques desconocidos mediante el análisis de anomalías en el tráfico de red, sin necesidad de firmas específicas.

Debe poseer la capacidad de operar en modo sigiloso, sin dirección IP asociada con los puertos de detección.

Debe tener la capacidad de crear suscripciones definidas por el usuario mediante expresiones regulares.

Debe permitir la actualización de las suscripciones y sus tratamientos de forma manual y automática.

Debe permitir la identificación de ataques en protocolos que utilizan puertos aleatorios.

Debe permitir el desarrollo de firmas de ataques descubiertos con el fin de evitar su recurrencia.

El equipo debe tener mecanismos de lista blanca y lista negra que permitan el control de excepciones y listas de detecciones personalizadas para bloqueos en tiempo real.

El sistema de protección contra malware debe detectar malware de día cero, malware polimórfico, Botnets y otras amenazas persistentes avanzadas (APT) en la red interna y en las comunicaciones por Internet (tráfico entrante y tráfico saliente) La plataforma también debe tener la capacidad de detectar software malicioso que se aprovecha de vulnerabilidades conocidas.

La solución debe registrar y almacenar evidencia de ejecución de malware en el entorno de inspección, almacenando al menos: direcciones IP, puertos y protocolos utilizados por malware, y todo el proceso de ejecución y comunicación del ciclo de vida del malware detectado.

Debe permitir crear reglas para determinar qué tráfico se debe descifrar, incluida la IP de origen y destino, el puerto de destino, la aplicación, la zona, el usuario y cualquier combinación de estos.

Debe permitir crear reglas de excepción para el análisis de tráfico por categoría de direcciones URL de destino.

La consola de administración debe poder implementarse en hardware dedicado, en una solución virtualizada o en la nube, escalada para satisfacer todas las necesidades técnicas.

La solución debe tener motores de búsqueda en su consola de administración, de modo que sea más fácil buscar detecciones.

Debe tener una interfaz WEB segura (HTTPS).

Debe emitir informes gráficos y de texto, lo que permite la ejecución periódica automáticamente.

Debe tener un módulo de informes que emita al menos informes sobre alertas clave (actividad actual o histórica) por intervalo de fechas/direcciones IP, etc.

La solución debe ser capaz de admitir la retención de registros durante al menos 90 días. Los informes y registros deben exportarse a al menos formatos PDF y CSV.

Se deberá proporcionar licenciamiento del software para la identificación y control de amenazas persistentes avanzadas – APTs con una duración de un (1) año, la licencia será propiedad de Gobierno del Estado.

Entregables:

- Informe técnico de manera mensual que especifique los hallazgos y estrategias de mitigación
- Informe ejecutivo

Cartas requeridas:

- Para las Herramientas de identificación y control de amenazas persistentes avanzadas – APTs, EL LICITANTE deberá integrar en su propuesta técnica carta emitida por el fabricante de la solución, en original, en hoja membretada y firma autógrafa, indicando que EL LICITANTE está autorizado para distribuir la solución que soporta el servicio de Herramientas de Identificación y control de Amenazas Persistentes Avanzadas – APTs.

2. Gestión continua de vulnerabilidades

EL LICITANTE debe realizar una gestión continua de vulnerabilidades a los componentes tecnológicos que hacen parte del alcance del servicio, para tal fin debe utilizar herramientas de gestión de vulnerabilidades.

Debe realizar procesos continuos de análisis de vulnerabilidades.

El oferente debe utilizar una herramienta licenciada de gestión de vulnerabilidades durante la duración de los servicios, no se aceptan soluciones free u open source.

La herramienta debe contar con Administración de Activos: Identificación y clasificación de activos automatizadas.

La verificación se debe realizar a los activos de información definidos por la entidad.
Se deben generar recomendaciones para el cierre de vulnerabilidades.

Se debe gestionar todo el ciclo de vida de las vulnerabilidades presentes en los activos.

Requerimientos Técnicos

La solución de gestión de vulnerabilidades debe contar con la capacidad de realizar descubrimiento de activos.

Debe permitir priorización automática de Amenazas.

La herramienta debe generar Informes de resultados de la evaluación de vulnerabilidades.

La solución de gestión de vulnerabilidades debe contar con procesos de actualización periódicos de su base de firmas de vulnerabilidades para analizar sobre los activos.

La solución de gestión de vulnerabilidades debe contar con la capacidad de identificar y analizar vulnerabilidades, como mínimo a sistemas operativos, equipos de comunicaciones, bases de datos, dispositivos de seguridad.

La solución de gestión de vulnerabilidades debe contar con la capacidad de realizar tareas de definición de prioridades de las vulnerabilidades a remediar.

La solución de gestión de vulnerabilidades debe contar con la capacidad de programar tareas de ejecución de análisis de vulnerabilidades sobre los activos identificados de forma automática.

La solución de gestión de vulnerabilidades debe contar con la capacidad de clasificar alertas de vulnerabilidades de acuerdo con la prioridad estimada por los fabricantes de sistemas, aplicaciones y módulos de los activos de información analizados.

La solución de gestión de vulnerabilidades debe contar con la capacidad de proveer información del CVSS v2 y v3 (COMMON VULNERABILITY SCORING SYSTEM) y/o CVE (Common Vulnerability Exposure) de las vulnerabilidades encontradas a través de los análisis de vulnerabilidades efectuados.

La solución de gestión de vulnerabilidades debe clasificar la criticidad de las vulnerabilidades encontradas.

La solución de gestión de vulnerabilidades debe permitir exportar la información de inventario con el detalle de los activos, incluyendo la programación del escaneo.

El sistema de gestión centralizada, logs y reportes debe presentar la consola de gestión y la información gráfica (dashboards) de las vulnerabilidades.

Ser accesible de inmediato en cualquier momento y ubicación a través de cualquier explorador Web.

Contar con una suite integral de productos nativos del fabricante que permitan el análisis de vulnerabilidades basado en: Sistemas Operativos, Servicios WEB, Puertos TCP y UDP, Servicios, Aplicaciones, Bases de Datos, Versiones de Firmware.

Analizar en profundidad aplicaciones web, al menos las contenidas en los principales listados de seguridad actuales como son: Open Web Application Security Project (OWASP) Top 10.

La herramienta debe permitir la ejecución de las pruebas a nivel de red usando escáner Appliance, escáner virtual y/o mediante el uso de agentes.

La herramienta debe identificar vulnerabilidades a nivel de aplicación web e infraestructura cómo servidores, bases de datos y dispositivos de red.

Debe contar con Integración con tecnologías SIEM para el monitoreo de eventos de seguridad.

Debe contar con capacidades para consultar de manera unificada todos los activos gestionados y sus vulnerabilidades.

Brindar Integración nativa con información de fuentes de inteligencia que permita dar prioridad basado en riesgos.

La información recopilada debe poderse correlacionar fácilmente al activo asociado.

Debe correlacionar automáticamente las vulnerabilidades y parches para hosts específicos, disminuyendo el tiempo de respuesta de corrección, buscando los CVE e identificando los últimos parches reemplazantes.

Debe permitir la gestión centralizada de los activos, generación de etiquetas fijas y dinámicas para organizarlos y categorizarlos.

Debe tener la capacidad de monitorear y alertar en tiempo real o basado en los escaneos ejecutados las vulnerabilidades presentes en los activos, así como amenazas y cambios inesperados antes de que se conviertan en problemas.

Contar con dashboards y cuadros de mando de manera unificada.

Debe contar con manejo de roles y perfiles de acuerdo a funciones.

Brindar Integración con bases de conocimiento e identificación de vulnerabilidades como CVE y calificación CVSS.

Debe gestionar integralmente las vulnerabilidades.

Debe contar con la funcionalidad de etiquetar host con el fin de obtener una mejor administración de los Host y/o IPs.

Debe detectar una amplia gama de vulnerabilidades e indicar su relación con contenido malicioso como Virus, Troyanos y Malware.

Debe generar dashboards y reportes de priorización de riesgos y amenazas.

Contar una base actualizada al día de los cambios más recientes en el panorama de las nuevas amenazas.

Cubrir de manera activa y pasiva todos los activos de la red.

Manejar opciones de implementación simple o en múltiples sistemas.

Debe analizar automáticamente las aplicaciones web y dar informes concisos de las vulnerabilidades localizadas.

La solución propuesta debe permitir la administración centralizada vía acceso directo (tipo servidor) por interfaz gráfica o vía WEB utilizando HTTPS.

La solución debe permitir definir diferentes niveles de usuario de administración.

Debe proporcionar un panel de estado de dispositivo que incluya la información más relevante sobre los dispositivos analizados.

Generar reportes ejecutivos y detallados

Generar reportes mediante IP, Grupo o Tags

La solución propuesta debe incluir:

- La actualización del licenciamiento de software y firmware.
- Actualizaciones automáticas de la base de datos de vulnerabilidades o el método de detección de vulnerabilidades que utilice el sistema propuesto.
- Actualizaciones automáticas del sistema vía Internet".

Se deberá proporcionar licenciamiento Qualys para Patch Management (PM), Custom Assessment and Remediation (CAR) y CyberSecurity Asset Management (CAM) para al menos 4,000 equipos con una duración de un (1) año, con soporte 24x7x365 por parte de fabricante, la licencia será propiedad de Gobierno del Estado.

Entregables:

- Informe técnico de manera mensual que especifique los hallazgos y estrategias de mitigación.
- Informe ejecutivo.

Cartas requeridas:

- EL LICITANTE deberá integrar en su propuesta técnica, carta emitida por el fabricante de la herramienta, en original, en hoja membretada y firmada por el representante legal donde indique que el Licitante está autorizado para distribuirlas.

3. Ciberpatrullaje

EL LICITANTE debe brindar servicios de Ciberpatrullaje en SurfaceWeb, DeepWeb y DarkWeb, como mínimo el servicio debe identificar:

- Identificación de suplantaciones: phishing, blackseo, sitios similares con fines maliciosos
- Monitoreo del servicio DNS y certificados digitales
- Identificación de ciber criminales que atenten contra ellos o lo estén planeando (recolección evidencia forense + apoyo jurídico)
- Identificación de fugas de información en Internet
- Monitoreo de redes sociales para asuntos que puedan llevar a delitos informáticos
- Alerta temprana sobre vulnerabilidades en su infraestructura"
- "Identificación en más de 30 fuentes de análisis identificadas y que no se limitan a las fuentes disponibles para OSINT, las fuentes de OSINT son fuentes públicas (Surface Web) y las fuentes que se busca en el servicio se ubican entre otras en:
 - SurfaceWeb.
 - DeepWeb.
 - DarkWeb.
 - Redes Sociales.
 - Leaks.
 - Phishing.
 - Dominios DNS.
 - Marcas.
- EL LICITANTE debe contar con una herramienta que permita visualizar los resultados y debe entregar a la entidad acceso para consultar la información

Se deberá proporcionar licenciamiento para protección de aplicaciones Web y API's para el dominio principal y hasta 600 subdominios y/o IPs con una duración de un (1) año con soporte 24x7x365 por parte del fabricante, la licencia será propiedad de Gobierno del Estado.

Entregables:

Reporte mensual, como mínimos los siguientes puntos:

- Resumen ejecutivo.
- Objetivos del análisis.
- Hallazgos de ciberinteligencia.
- Actividades de ciber actores y grupos de ciber crimen.
- Conclusiones.
- Ciberactores.
- Recomendaciones.

4. Pentest y análisis de vulnerabilidades

Dentro del servicio se deberá evaluar el nivel de riesgo de la red Internet Libre para la Gente, en términos de seguridad de la información, emitiendo una opinión que permita identificar y eventualmente con base en esta, permitir a la LA CONTRATANTE eliminar la causa raíz del problema, reduciendo el riesgo asociado al proceso que soporta.

Pruebas Dinámicas de sistemas

Se evaluará el nivel de riesgo de los sistemas, permitiendo identificar el riesgo asociado al proceso de negocio. Esta revisión proporcionará un reporte detallado de los hallazgos incluyendo medidas de recomendación de mitigación y de solución a los problemas detectados en los diferentes tipos de pruebas, de manera enunciativa más no limitativa como son:

- Vulnerabilidades inherentes a la arquitectura de la aplicación.
- Riesgos introducidos durante las fases de desarrollo, integración, despliegue y procesos operacionales.
- Vulnerabilidades técnicas inherentes a la plataforma en las diversas capas, incluyendo los servicios de middleware y de bases de datos.
- El riesgo de la aplicación y la infraestructura a diversos ataques como Cross Site Scripting (XSS), SQL Injection, Buffer Overflow, Command Injection, etc.

Las pruebas dinámicas podrán realizarse usando una combinación de herramientas automatizadas y métodos manuales, ejecutando de forma enunciativa más no limitativa:

- Análisis de métodos de autenticación
- Pruebas de seguridad a configuraciones de la aplicación
- Análisis de seguridad de datos de entrada
- Verificación de parámetros
- Pruebas de seguridad conforme a metodología OWASP top 10

Pruebas de penetración

A través del servicio se comprobará la seguridad de la infraestructura de los sistemas que determine LA CONTRATANTE, al ejecutar el servicio en busca de problemáticas que pudieran transformarse en ataques, pérdida del servicio o afectación a la imagen de LA CONTRATANTE, sin entrar en el análisis de los sistemas mismos.

Se deberán realizar las pruebas de seguridad, hackeo ético, y en su caso explotación de vulnerabilidades a los servidores de la red Internet Libre para la Gente desde internet a través de un punto externo a la red Internet Libre para la Gente.

- a) El diagnóstico de vulnerabilidades y las pruebas de seguridad serán realizadas a partir de la metodología “Open Source Security Testing Methodology Manual” (OSSTMM) del organismo internacional “Institute for Security and Open Methodologies” (ISECOM) en versión 3. Las siguientes actividades son enunciativas más no limitativas:
 - Escaneo de Puertos
 - Identificación de Servicios
 - Identificación de Sistemas
 - Identificación e investigación de vulnerabilidades
 - Pruebas y/o Explotación de vulnerabilidades.
- b) Se deberá presentar documento donde se describa la forma o reglas mediante las cuales se llevará a cabo el diagnóstico de vulnerabilidades y pruebas de seguridad, es decir, describir de forma detallada las actividades a realizar, los límites, riesgo, alcances, herramientas a utilizar y resultados esperados, dentro de los primeros 3 días hábiles posteriores a la firma del contrato, el cual deberá ser aprobado por las áreas correspondientes de LA CONTRATANTE.
- c) Realizar un análisis de la infraestructura crítica, con la finalidad de identificar los servicios de los sistemas, así como generar la búsqueda de vulnerabilidades en la infraestructura tecnológica de LA CONTRATANTE: aplicación de parches, debilidad de contraseñas, permisos de archivos, barridos de puertos, SNMP, RPC, correo electrónico, FTP y servicios habilitados, etc.
- d) Una vez concluida la búsqueda de vulnerabilidades, se deberá realizar la documentación de cada una de las vulnerabilidades identificadas; y no importando si las vulnerabilidades fueron o no explotadas, se generarán las recomendaciones que apliquen.
- e) Para cada vulnerabilidad importante identificada, se establecerá el nivel de riesgo que tendría si la vulnerabilidad en cuestión fuera explotada, identificando el impacto al negocio en función del cumplimiento normativo y asignando una calificación de riesgo.

Por tal motivo se considerarán las siguientes actividades de manera enunciativa más no limitativa:

- Escaneo de Puertos
- Identificación de Servicios
- Identificación de Sistemas
- Identificación e investigación de vulnerabilidades
- Pruebas y/o Explotación de vulnerabilidades

- f) Elaboración de reportes de resultados conforme lo establecido en la sección de entregables, el cual contendrá al menos lo siguiente: Introducción, Objetivo, Alcance, Resumen de Actividades realizadas, Ambiente evaluado, Hallazgos obtenidos por criticidad (indicando en que equipos se detectó ese hallazgo), resumen por tipo de hallazgos basándose en la escala de la OSSTMM.

Entregables:

Reporte, como mínimos los siguientes puntos:

- Resumen ejecutivo.
- Metodología.
- Objetivos del análisis.
- Hallazgos.
- Elementos vulnerados.
- Conclusiones.
- Recomendaciones.

5. Solución especializada de detección y análisis

El gobierno de Guanajuato requiere contar con una solución para el fortalecimiento de la seguridad en la red de datos mediante técnicas especializadas de detección y análisis, teniendo al menos las siguientes características:

- La solución deberá tener capacidad de identificar movimiento lateral.
- La solución deberá tener capacidad de identificar amenazas en el tráfico cifrado.
- La solución deberá tener capacidad de identificar conexiones a dominios DGA generados automáticamente.
- La solución deberá tener capacidad de identificar incumplimiento de las políticas de seguridad.
- La solución deberá tener capacidad de identificar uso de herramientas de hackers.
- La solución deberá tener capacidad de identificar explotación de vulnerabilidades de red.
- La solución deberá tener capacidad de identificar análisis retrospectivo del tráfico.
- La solución deberá tener capacidad de identificar actividad de malware.
- La solución deberá tener capacidad de identificar signos de ataques previamente inadvertidos.

- La solución deberá tener capacidad de identificar actividades ocultas a las herramientas de seguridad.
- La solución deberá tener capacidad de revelar explotación de vulnerabilidades en la red.
- La solución deberá tener capacidad de revelar ocultación de la actividad de los medios de protección.
- La solución deberá tener capacidad de revelar movimientos de los atacantes dentro del perímetro.
- La solución deberá tener capacidad de revelar dominios generados automáticamente.
- La solución deberá tener capacidad de revelar herramientas de hackers.
- La solución deberá tener capacidad de revelar signos de ataques no detectados previamente.
- La solución deberá tener capacidad de revelar violación de las normas de seguridad.

Características Generales de la solución especializada de detección y análisis

- **Detección de actividad maliciosa tanto en el perímetro como en el interior de la red**
Al analizar el tráfico externo e interno, deberá ser capaz de detectar anomalías de red movimientos laterales, intentos de explotar vulnerabilidades y ataques contra usuario de la red Internet Libre para la Gente o servicios internos.
- **Detección de ataques y sus consecuencias incluso en tráfico cifrado**
El análisis en profundidad debe permitir detectar con precisión el malware cifrado con TL u otros protocolos personalizados diseñados para ocultar la actividad de piratería.
- **Búsqueda de amenazas**
Deberá mostrar la imagen completa de la red al equipo de seguridad, cubriendo mas aspectos que otras herramientas de seguridad, y ayudar a reconstruir la línea de tiempo del ataque. Almacenar metadatos y una copia de tráfico capturada, lo que debe permitir a los equipos de seguridad encontrar rápidamente sesiones sospechosas y volver sobre los pasos del atacante.

Fuentes de Datos para Análisis Múltiples Niveles de Abstracción

- Base de datos con direcciones IP de muchos países.
- Detección de archivos transferidos a nivel de aplicación.
- Análisis de solicitudes de DNS.
- Cuentas de usuario de solicitudes Kerberos.
- 3,000 reglas de tránsito definidas por expertos de ESC basadas en forenses de incidentes y pen tests.
- ICC de listas de reputación basadas en inteligencia de amenazas.
- Firmas de IDS.
- Encapsulación: GRE, VLAN, MPLS, VXLAN, TEREDO, ERSPAN, GENEVE.
- Análisis: 1200 parámetros de aplicación.
- Identificación de la aplicación.
- Grabación de todos los paquetes de red.

Funcionalidad requerida:

Captura de tráfico de red.

- Capturar el tráfico de una interfaz de red seleccionada por el usuario
- Registro del tráfico de red capturado en archivos PCAP.
- Importación de tráfico de red de archivos PCAP.
- Uso de filtros de red para capturar y registrar tráfico de red La captura del tráfico de red se debe filtrar según los siguientes parámetros:
 - Protocolo de capa de transporte.
 - Puerto o grupo de puertos de red.
 - Subred IP o grupo de subredes IP.
 - Dirección IP o grupo de direcciones IP.
- Registro de solo una parte de la sesión al archivo PCAP. El filtro debe restringir la sesión guardando según los siguientes parámetros:
 - Protocolo de capa de aplicación.
 - Tamaño de la parte de la sesión que se guardó en PCAP (en bytes).

Manipulación de tráfico de red.

- Registro y almacenamiento del tráfico de red capturado y posterior reescritura automática de los archivos de tráfico de red.
- Registro y almacenamiento de resultados del tráfico de red capturado (índices).

Almacenamiento de tráfico de red

- Análisis del tráfico de red, incluidas las capas de red y de transporte (protocolos TCP y UDP).
- Definición y análisis de los protocolos de capa de aplicación.
- Recuperación de archivos e información transferidos vía protocolos de capa de aplicación (HTTP, SMTP, FTP, SMB, TFTP, POP3, IMAP4, NFS).
- Revisión de todos los nombres de dominio detectados, direcciones IP y URL contra listas blancas y negras.
- Indexación continua en tiempo real del tráfico capturado (registro en la base de datos).

Procesamiento de tráfico de red.

- Búsqueda de una conexión de red en la información de sesión almacenada.
- Identificación de las conexiones de red entre servidores (usando filtros).
- Creación de gráficos de conexiones identificadas según los filtros del usuario.
- Exportación de sesiones en PCAP.
- Acceso vía interfaz Web.
- Mensajes sobre los ataques y los indicadores de compromiso detectados enviados a un sistema externo a través de webhooks.
- Informes proporcionados en DOC y PDF.
- Información de la sesión proporcionada en CSV y JSON.

Detección de ataques a la red.

- Respaldo de las reglas de detección de ataques a la red.
- Creación de reglas personalizadas.
- Registro de desencadenantes de reglas.
- Notificación de las herramientas de seguridad de la información del cliente cada vez que se desencadena una regla syslog.
- Actualización automática de los métodos de detección de ataques y las listas de reputación.
- Supervisión del servidor de red, detección de nuevos dispositivos en la red.

Supervisión.

- Supervisión del estado de todos los subsistemas del sistema. El subsistema reinicia el servicio infractor si se detecta alguna anomalía.
- Notificaciones para el usuario de LA CONTRATANTE sobre el estado actual del sistema a través de la interfaz web.

Gestión.

- Gestión basada en roles de los privilegios de acceso del usuario.
- Gestión de asignación de usuario y rol: se le puede asignar más de un rol a cada usuario de LA CONTRATANTE.
- Configuración del sistema y cambios a los ajustes del sistema.

Se deberá proporcionar el licenciamiento para la detección y análisis especializado de ciberseguridad en la red de datos del segmento principal mediante el análisis del tráfico, con una duración de un (1) año, con soporte 24x7x365, la licencia será propiedad del Estado.

Características mínimas que deberá tener el equipo de cómputo requerido en el cual se implementará la licencia:

- AMD Número de núcleos indistinto, familia de proc. Ryzen 7 serie 7000 o superior, velocidad de frecuencia base indistinto, Cache total mínimo indistinto, TDP Indistinto, chipset indistinto o INTEL número de núcleos indistinto, familia de proc. Core i7 de decimotercera generación o superior, velocidad de frecuencia base indistinto, Cache total mínimo indistinto, TDP indistinto, chipset Intel Q670;
- Sistema Operativo Libre;
- MEMORIA: Mínimo 32GB DDR4 entregada en dos módulos de 16GB en configuración de doble canal, expandible a 64GB. Con al menos dos ranuras libres para expansión. (Debe soportar Quad Channel si se utilizan 4 dimms); Velocidad mínimo 3200MHz; MONITOR: Led de 23.8", Resolución mínima 1920 x 1080. Panel IPS. Conexión Display Port;
- DISCO DURO 1: En ranura M.2 PCI NVMe de estado sólido mínimo 512 GB y DISCO DURO 2: Mecánico rotacional SATA mínimo 2 TB, 7200 RPM mínimo;
- TECLADO: En español;
- MOUSE ÓPTICO: Con dos botones y scroll;
- PUERTOS USB: Mínimo 4 puertos posteriores y 4 frontales, al menos uno del tipo C;
- AUDIO Y VIDEO: Audio integrado a la tarjeta madre, tarjeta de video independiente de 8GB DDR6 mínimo;

- RED ETHERNET: 10/100/1000 e INALÁMBRICA 802.11 ax (Wifi 6), Antena 2x2 / Bluetooth 5.1 mínimo;
- GABINETE: Volumen indistinto;
- RANURAS DE EXPANSIÓN: Mínimo 1 PCI Express libre, conector indistinto;
- GARANTÍA: 3 años en partes, mano de obra y en sitio (incluye PC y Monitor) por parte del fabricante;
- FUENTE DE PODER: 500 Watts Máximo con una eficiencia energética de al menos 92%

El hardware requerido será instalado en las oficinas de la Secretaría de Obra Pública del Estado de Guanajuato, ubicadas en **México 110, San José de Tránsito, Silao, Gto.**, el cual será propiedad del Estado de Guanajuato a la conclusión del servicio.

Entregables:

Reporte mensual, como mínimos los siguientes puntos:

- Resumen ejecutivo.
- Objetivos del análisis.
- Hallazgos de del análisis

Cartas requeridas:

- EL LICITANTE deberá integrar en su propuesta técnica, carta emitida por el fabricante de la herramienta, en original, en hoja membretada y firmada por el representante legal donde indique que el Licitante está autorizado para distribuirlas.

V. PROCESO DE ATENCIÓN A VULNERABILIDADES Y/O DE HALLAZGOS RESULTANTES

Para todos los conceptos anteriormente descritos dentro de los alcances del servicio integral, se deberá considerar el siguiente proceso de atención a las vulnerabilidades, amenazas detectadas y/o de hallazgos resultantes de dichas funciones:

- Dependiendo del caso detectado, deberá de mitigarse, controlarse o contener la persistencia identificada.
- Notificar mediante correo electrónico al personal designado de Gobierno del Estado, las incidencias detectadas que supongan un riesgo potencial a los bienes del gobierno en la materia, y que estén directamente relacionados a los alcances del presente servicio.
- Asesorar al personal del gobierno para que se efectúen las correcciones necesarias de las vulnerabilidades o amenazas detectadas, ya sea a través del personal de gobierno o a través de un tercero.
- Verificar que las correcciones se hayan efectuado de manera correcta y confirmar que se haya mitigado de manera efectiva el hallazgo detectado.

VI. PERFILES QUE DEBE CUBRIR EL LICITANTE

A continuación, se listan las credenciales y capacidades que deberán cubrir los recursos asignados.

Líder de Proyecto.

ROL	PERFIL Y CERTIFICACIONES QUE DEMOSTRAR	NÚMERO DE RECURSOS
Líder de proyecto	Formación: Ingeniería o licenciatura en sistemas o computación titulado, o carrera afín, certificaciones requeridas: • PMP PROJECT MANAGER PROFESIONAL • AUDITOR LÍDER ISO 27001 • COBIT 5 FUNDAMENTOS • ITIL V3 O V4 FUNDAMENTOS • CISM	1 recurso

Consultor de Monitoreo de Soluciones de Ciberseguridad

ROL	PERFIL Y CERTIFICACIONES QUE DEMOSTRAR	NÚMERO DE RECURSOS
Consultor de Monitoreo de Soluciones de Ciberseguridad	Formación: Ingeniería o licenciatura en sistemas o computación, o carrera afín, certificaciones requeridas: • CERTIFIED INCIDENT HANDLER	2 recursos

Consultor en implementación de soluciones de evaluación y análisis de vulnerabilidades

ROL	PERFIL Y CERTIFICACIONES QUE DEMOSTRAR	NÚMERO DE RECURSOS
Consultor en Pruebas de Penetración	Formación: Ingeniería o licenciatura en sistemas o computación, o carrera afín, certificaciones requeridas: • Certified Ethical Hacker, • Certified OSSTMM 3.0 Professional Security Analyst OPSA • Comptia security+	2 recursos

Arquitecto en soluciones de ciberseguridad

ROL	PERFIL Y CERTIFICACIONES QUE DEMOSTRAR	NÚMERO DE RECURSOS
Consultor en tácticas de ataques Red Team	Formación: Ingeniería o licenciatura en sistemas o computación titulado, o carrera afín, certificaciones requeridas: • CompTIA Security+ • Certified Ethical Hacker (Master) • Offensive Security Certified Professional (OSCP) • Certified OSSTMM 3.0 Professional Security Analyst OPSA • Web Application Penetration Tester (GWAPT) • Penetration Tester Certification (GPEN) • Red Team Operator	1 recurso

“EL LICITANTE” debe incluir como parte de su propuesta técnica un escrito firmado por el representante legal en papel membretado donde indique el nombre del personal y el perfil asignado, acompañado del currículum vitae.

Para garantizar la calidad, seguridad de la información, continuidad de las operaciones y niveles del servicio, se requiere que “**EL LICITANTE**” cuente con las siguientes certificaciones vigentes: ISO 9001:2015, ISO/IEC 27001:2022, ISO 37001:2016, ISO 22301:2019 e ISO/IEC 20000-1:2018 en al menos seis (6) de los siguientes procesos:

- i. Forense Digital
- ii. Centro de Operaciones de Redes y Seguridad "NOC" y "SOC" con Detección, Análisis y Respuesta Gestionada "MDR" para la atención con el Equipo de Respuesta ante Emergencia Informáticas
- iii. Inteligencia de Análisis de Información Digital
- iv. Análisis de Ciberseguridad en Entornos de Nube
- v. Mesa de Ayuda Especializada en la Atención y Gestión de Incidentes de Seguridad de la información
- vi. Análisis y Monitoreo Externo de la Información para el Alertamiento de Riesgos y Ciber amenazas
- vii. Gobierno de Seguridad y Cumplimiento Normativo
- viii. Protección Digital de la Identidad Corporativa mediante el Análisis de Ciber amenazas

Se requiere que “**EL LICITANTE**” cuente con un convenio de colaboración con el Grupo de Trabajo de las Américas de INTERPOL, OEA, CERT MEX o algún otro organismo internacional del mismo ámbito y reconocimiento, con un alcance similar al siguiente:

- Compartir información relevante sobre incidentes y cualquier otro tipo de información que se considere de utilidad en materia de ciberseguridad.
- Compartir información de ataques recientes que afecten a infraestructuras críticas
- Generar estrategias de protección y defensa de la infraestructura crítica cibernética
- Compartir las investigaciones científicas para la prevención e investigación de los delitos cibernéticos.

BIENES QUE SE ENTREGARÁN A GOBIERNO DEL ESTADO AL TÉRMINO DEL CONTRATO

Nº	DESCRIPCIÓN
1	Licenciamiento del software para la identificación y control de amenazas persistentes avanzadas – APTs con una duración de un (1) año.
1	Licenciamiento de Qualys para Patch Management (PM), Custom Assessment and Remediation (CAR) y CyberSecurity Asset Management (CAM) para al menos 4,000 equipos con una duración de un (1) año.
1	Licenciamiento para protección de aplicaciones Web y API's para el dominio principal y hasta 600 subdominios y/o IPs con una duración de un (1) año.
1	Licenciamiento para la detección y análisis especializado de ciberseguridad en la red de datos del segmento principal mediante el análisis del tráfico, con una duración de un (1) año.
1	Equipo de cómputo requerido, conforme a las características descritas en los presentes términos de referencia.