ITRC

CARACTERÍSTICAS Y/O ESPECIFICACIONES TÉCNICAS DE LOS BIENES A CONTRATAR

A continuación, se relacionan las especificaciones técnicas de los artefactos y componentes que se van a adquirir por parte de entidad, para suplir la necesidad de mejorar la velocidad de conectividad:

ITEM	A. SISTEMA DE DETECCIÓN DE AMENAZAS
1	La suscripción a la solución de CiberDefensa debe ser capaz de identificar cualquier amenaza anómala en la red y en tiempo real mediante aprendizaje automático e inteligencia artificial.
2	Certificación del fabricante o su representante donde autorice la comercialización de la solución.
3	El oferente y/o contratista deberá entregar un licenciamiento total de la solución para 250 dispositivos por (1) un año.
5	La solución debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo sobre la red de la Agencia.
6	La solución debe basarse en el análisis de comportamiento y correlación inteligente con la capacidad de detectar: a. Toda conectividad inusual en la red. b. Todas las actividades anómalas en la red. c. Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de dirección IP, uso del protocolo DHCP, etc. d. Tener la capacidad de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a unas determinadas credenciales. e. Identificar un volumen de conexiones significativamente inusual. f. Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo.
7	La solución debe alertar automáticamente sobre todas las actividades inusuales y anómalas en la red
8	La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: a. La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno b. Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y/o firmas

9	La solución debe utilizar modelos matemáticos de estimación recursiva bayesiana o similares con el fin de validar los comportamientos anómalos en la red.
10	La solución debe proporcionar visibilidad completa de la red, incluidas las tecnologías tradicionales y no tradicionales
11	La solución debe poder identificar cualquier comportamiento anómalo en el entorno y alertar sobre estos comportamientos en tiempo real
12	El servicio debe ser capaz de identificar cualquier dispositivo nuevo en la red
13	Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube.
14	Debe basarse en métodos matemáticos probabilísticos, analizando y correlacionando múltiples dimensiones distintas dentro del paquete
15	La solución debe poder realizar una captura de paquetes en tiempo real que permita un análisis exhaustivo del incidente en el momento de su ocurrencia, así como ofrecer la opción de analizar el paquete tanto en herramientas como Wireshark y dentro de su propia interfaz de usuario.
16	La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red de la Agencia ITRC
17	Ser completamente automatizada, no debe requerirse de reglas o intervención humana para instruir a la solución sobre cómo utilizar los logs y flows recolectados para correlacionar y determinar ataques en tiempo real.
18	Debe poder realizar investigaciones autónomas basadas en inteligencia artificial, sea por demanda a través de la interfaz gráfica y/o a través de la integración vía API, esta investigación debe incluso poder realizarse sin intervención humana y generar un reporte donde se evidencia al menos un resumen ejecutivo del incidente, las alertas que fueron investigadas que hacen parte de incidente e información técnica de cada uno de los eventos identificados, asociándolos a la fase del Cyber Kill Chain y a una posible TTP de framework ATT&CK Mitre.
19	La Investigación basada en Inteligencia Artificial debe generar un reporte como resultado del proceso investigativo que contenga como mínimo: a. Una reconstrucción cronológica de los eventos que hacen parte del Incidente. b. Un resumen del incidente con una narrativa basada en procesamiento de lenguaje natural que describa a alto nivel los comportamientos evidenciados durante el incidente. c. Detalles técnicos relevantes a la investigación realizada como direcciones Ips, Hostnames, cuentas de usuario involucradas, saltos de conexión, cantidad de transferencia de datos, destinos externos, rareza de los destinos, rareza de las conexiones y resúmenes de conexiones.
20	Debe realizar un análisis completo del tráfico (No análisis parciales de los paquetes p.e: sflow, jflow, netflow, Syslog)
21	La solución debe permitir la integración con LDAP o Directorio Activo

22	El sistema debe ser OPEN API, que admita integraciones con otros elementos de seguridad al menos en los formatos, CEF, LEEF, JSON, SYSLOG, entre otros.
23	La tecnología deberá proporcionar la capacidad de realizar procedimientos automatizados por parte del proveedor para encontrar amenazas, basados en inteligencia artificial con al menos las siguientes capacidades: a. Procesos de Threat Hunting basados en anomalías de comportamiento detectadas por la inteligencia artificial. b. Los procesos de Threat Hunting deberán indicar las fases del ciberataque en las que se hayan visto anomalías detectadas en el comportamiento. c. El proceso de Threat Hunting deberá tener la capacidad de correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo. Se deben validar con otras fuentes de información que llegan al correlacionador para dar mayor contexto a los hallazgos identificados por la inteligencia Artificial. d. Se deberá poder integrar el proceso de Threat Hunting automatizado para que otros servicios vía API puedan solicitar informes de cacería de amenazas de manera automatizada. e. Se deben poder solicitar investigaciones autónomas y a demanda a la inteligencia artificial, donde el disparador pueda ser una anomalía ya detectada o una simple investigación a demanda. f. El proceso de Threat Hunting deberá proporcionar un informe base entregado por la inteligencia artificial y uno adicional con la información de contexto y otras investigaciones adicionales realizadas por analistas humanos. g. El proceso deberá tener la capacidad de realizar investigaciones continuas 24/7 y en tiempo real de las anomalías detectadas por la inteligencia artificial h. Se deberán proponer los reportes estadísticos de la solución a nivel ejecutivo. i. Se deberán acordar los reportes de los Threat Hunting y sus respectivas evidencias con al menos un reporte por cada investigación realizada. j. Se deberán realizar procesos de Threat Hunting manuales basados en TTP's mitre de manera recurrente, identificando qué anomalías detectadas por la plataforma de Inteligencia Artificial hacen parte de las técinas buscadas para cada ejercicio de Treath Hunting propuesto.
24	La solución debe permitir la personalización avanzada de la tecnología, permitiendo considerar múltiples parámetros de datos al verificar un determinado comportamiento, entre los parámetros debe ser posible tener las siguientes opciones: Conexiones, conexiones externas, conexiones internas, transferencia de datos, datos externos transferencia, conexiones SMB, conexiones de puerto cerrado, difusiones, dispositivos conectados, transferencia de datos (cliente), transferencia de datos (servidor), entre otras métricas relevantes.
25	La solución debe utilizar varios algoritmos de inteligencia artificial, así como varias técnicas de Machine Learning como: Deep Learning, Machine Learning supervisado y Machine Learning no supervisado.

26	La tecnología de identificación de amenazas de la solución no debe basarse en firmas, ni reglas, ni heurística, ni sandboxing. Debe estar puramente basada en algoritmos avanzados de Machine Learning e Inteligencia Artificial.
27	La solución no debe depender de una conexión hacia Internet para realizar sus operaciones de inteligencia y análisis.
28	Debe funcionar completamente en función del comportamiento, donde no se permitirán las tecnologías que hacen uso de reglas, firmas y/o Indicadores de Compromiso (IoC's)
29	La solución debe tener la capacidad de modelar el comportamiento normal a nivel de usuario, dispositivos y red y a partir de estos, identificar de forma autónoma las anomalías que corresponden a brechas de seguridad.
30	La solución debe poder realizar un aprendizaje autónomo del comportamiento normal de la red sin requerir previo conocimiento del historial de comportamiento anómalo, con la posibilidad de identificar amenazas desde el primer día de instalación.
31	La solución nunca debe dejar de aprender autónomamente del comportamiento de red de la entidad, no se permiten soluciones con aprendizaje estático que sea configurado por la entidad.
32	La tecnología debe tener la capacidad de detectar amenazas internas y externas
33	La tecnología debe ser auto-configurable, es decir, debe tener la capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.
34	La solución debe tener capacidad de detectar como mínimo los siguientes tipos de brechas de seguridad: a. Ataques de tipo botnet b. Propagación de gusanos c. Ataques de ransomware d. Infiltración y exfiltración de datos e. Troyanos bancarios f. Credenciales comprometidas g. Minería de bitcoins h. Malware i. Ataques de DDoS a través de dispositivos IoT j. Amenazas avanzadas persistentes (APT)

35	La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente (Zero Day)
36	La tecnología ofertada deberá estar reconocida como líder en Gartner para NDR (ultimo cuadrante de Gartner) y como Líder en el informe IDC MarketScape (último informe) para Detección y Respuesta en Redes a nivel global, demostrando así liderazgo sostenido y validación independiente en el sector de seguridad avanzada.”
ITEM	**Visualización de red**
37	La solución debe poseer una interfaz de visualización amigable, que debe ser accesible vía web.
38	La interfaz de visualización debe permitir tener visibilidad gráfica de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real. No deberá necesitar compartir datos con una nube de seguridad global para obtener su inteligencia de seguridad
39	La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.
40	La solución debe ser capaz de agrupar automáticamente los dispositivos en grupos y/o grupos por su similitud de comportamiento
41	La solución debe tener una barra de búsqueda que permita buscar inmediatamente un dispositivo, IP, subred o host de red
42	La solución debe tener una interfaz de usuario donde se pueda consultar el estado completo del sistema, incluyendo:
43	a. La versión del software, el espacio en disco utilizado, el consumo de CPU y el consumo de memoria.
44	b. El detalle de todas las interfaces activas y el tráfico respectivo recibido a través de cada una de ellas
45	c. El ancho de banda total procesado, el ancho de banda promedio procesado hasta la fecha, el ancho de banda registrado en los últimos periodos de tiempo.
46	d. Un análisis detallado de todo el tráfico recibido en el dispositivo y la última vez que se identificaron los protocolos principales, entre ellos HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, etc.
47	La solución debe tener visibilidad en tiempo real de los siguientes datos correspondientes a la red: a. Cantidad de servidores b. Cantidad de estaciones cliente c. Cantidad de credenciales de usuario d. Tráfico de red

48	La interfaz de visualización debe poseer una barra de búsqueda que permita identificar de manera rápida cualquier elemento de la red bajo los siguientes criterios: a. Dirección IP b. Tipo de dispositivo c. Función o protocolo conocido. d. Tipo de dispositivo e. Nombre del dispositivo
49	Cuando se haga búsqueda de un dispositivo, la interfaz debe poder mostrar la información de éste en detalle incluyendo: dirección IP, dirección MAC, sistema operativo, logs de eventos, logs de brechas de seguridad identificadas, historial de conexiones, lista de dispositivos similares.
50	La interfaz debe permitir la visualización de todas las subredes, así como todos los dispositivos que las conforman. Debe permitir la visualización de la subred de manera gráfica en tiempo real, mostrando el esquema de conexiones entre los dispositivos
51	Las subredes deben poder visualizarse en un mapa global que permita conocer la ubicación real de cada una.
ITEM	**Visibilidad de amenazas**
52	La interfaz debe mostrar las amenazas que se van identificando en la red en tiempo real, con el detalle de eventos de cada amenaza generados por la herramienta, así como vistas gráficas que permitan ver el comportamiento de la amenaza en el tiempo.
53	La solución debe proporcionar filtros simples y rápidos para permitir el análisis de eventos informáticos por parte de Usuarios, Dispositivos y tipo de evento.
54	La interfaz debe poder mostrar la amenaza de manera gráfica y en tiempo real.
55	Las amenazas identificadas deben tener un nivel de clasificación según su criticidad y debe contar con un código de colores asociado a cada nivel.
56	La interfaz debe brindar la posibilidad de investigación de alertas en profundidad en tiempo real, de manera gráfica y mediante eventos.
57	La solución debe tener una función que permita el análisis retrospectivo de los registros del incidente, devolviendo la conexión en segundos, minutos, horas o días antes de que se haya identificado una anomalía
58	La interfaz debe poseer herramientas o funcionalidades que permitan la investigación forense al mayor nivel de detalle de cualquier amenaza identificada, sin necesidad de uso de herramientas externas.

59	La solución debe ser capaz de agrupar las anomalías de manera inteligente y por nivel de criticidad.
60	La solución debe contar dentro la su propia interface con herramientas tipo Punycode Convertor, RegEx Tester, Base64 Convertor, JS Beautifie, Epoch Converter, Facilitando el análisis de los incidentes.
61	La interfaz de visualización debe permitir tener visibilidad gráfica en 3D de cualquier elemento de la red con profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real.
62	La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.
ITEM	**Notificaciones**
63	La solución debe contar con la capacidad de poder notificar las amenazas a través de correos electrónicos.
64	Contar con una interfaz móvil disponible para Android y iOS, activa 7x24 que acelere las tareas de mitigación de riesgos mediante el envío de notificaciones push para dar aviso de amenazas en proceso y la posibilidad de confirmar acciones de respuesta autónoma.
ITEM	**Administración**
65	La herramienta debe ser capaz de realizar backup y restore de la configuración, permitiendo al administrador programar la realización de los backups en el momento deseado.
66	Los backups deben poder ser transferidos a un repositorio vía SFTP o alguna tecnología de transferencia equivalente, es decir, que considere las medidas de seguridad bajo protocolos aceptados por la industria
ITEM	**Contención**
67	Para la contención y bloqueos de ataques, se debe utilizar el mismo equipo ofertado en la solución de detección de amenazas, no se permite equipos (físicos o virtualizados) adicionales.
68	La solución debe estar en la capacidad de responder frente a incidentes de forma autónoma, esto es a partir del aprendizaje obtenido de la inteligencia artificial debe decidir qué debe bloquear y como debe hacerlo, no debe utilizar configuraciones ni políticas predefinidas para realizar el bloqueo y debe bloquear únicamente el tráfico asociado a la amenaza mientras permite que el tráfico restante (no anómalo) siga fluyendo.
69	Permitir integrarse con la infraestructura de seguridad existente, permitiendo optimizar la detección de amenazas y automatizando la mitigación de las mismas.
70	Las acciones de bloqueo deben ser generadas con la precisión necesaria para interrumpir exclusivamente el tráfico que corresponde a las acciones maliciosas detectadas, de manera que no se afecte al tráfico de las actividades normales de los dispositivos involucrados.

71	Capacidad para bloquear tráfico Norte-Sur y Este-Oeste de forma automática sin la instalación de dispositivos de control adicionales.
72	Capacidad de determinar automáticamente como bloquear el tráfico sin causar mayor impacto a la organización utilizando inteligencia artificial, bloqueando conexiones específicas a través del envío de TCP-RST sin necesidad de integraciones con la infraestructura de la entidad.
73	El bloqueo de conexiones a través de TCP-RST no debe necesitar más appliance físicos para su ejecución, se debe usar el mismo appliance de detección.
74	La solución debe poder ser configurada en modo pasivo-monitoreo o modo activo-bloqueo según la configuración predeterminada definida en conjunto con el personal de la entidad
75	Deberá ser gestionable desde la misma interfaz gráfica (GUI) de detección de la solución.
ITEM	**Periodo de vigencia**
76	La solución deberá ser licenciada y entregada por un periodo de **doce (12) meses**
ITEM	**Soporte del Fabricante incluido en la suscripción**
77	El fabricante deberá brindar las actualizaciones de software sin costo adicional durante el periodo de vigencia del contrato.
78	En caso de falla del equipo, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o en su defecto un equipo nuevo para el reemplazo sin costo adicional, modalidad RMA.
79	Se debe entregar junto con la oferta, un certificado del fabricante dirigido a la entidad, indicando que es un socio o partner aprobado para brindar las soluciones de este fabricante.
ITEM	**Capacitación incluida en la suscripción**
80	El fabricante debe tener un portal de capacitaciones sin costo adicional, donde se encuentren capacitaciones técnicas sobre la solución ofertada, estás capacitaciones deben ser en español, las personas de la entidad deben poder inscribirse a estos cursos y tomarlos en vivo y en directo con un capacitador del fabricante, el fabricante debe tener disponibilidad de estos cursos al menos 2 veces al mes dentro del portal de capacitaciones.
ITEM	**Certificación y fichas técnicas**
81	Se debe entregar junto con la propuesta, certificación emitida directamente por el fabricante de las soluciones ofertadas, donde se evidencie que el oferente es distribuidor o canal autorizado vigente.

82	El proponente deberá anexar las fichas técnicas y/o catálogos de los productos ofertados con la marca y referencia, y donde se pueda evidenciar el cumplimiento de cada una de las especificaciones técnicas solicitadas, frente a dudas que se presenten en este anexo técnico.
ITEM	**Servicios del oferente incluidos en la suscripción**
83	Soporte 7x24 por 12 meses por parte del contratista, para el sistema de detección de amenazas con inteligencia artificial para eventos no planeados que generan interrupción total o parcial del servicio.
ITEM	**TRANSFERENCIA DE CONOCIMIENTO**
84	El fabricante y/o proveedor debe contar dentro de su esquema de transferencia de conocimiento, un portal de capacitaciones sin costo adicional, donde se encuentre sesiones técnicas sobre la solución ofertada. Estás capacitaciones deben ser en español, las personas de la entidad deben poder inscribirse a estos cursos y tomarlos en vivo y en directo con un capacitador del fabricante, el fabricante debe tener disponibilidad de estos cursos al menos 1 vez al mes dentro del portal.
ITEM	**DLP**
85	Cobertura para 200 cuentas de Microsoft 365 durante el periodo contractual definido por la entidad.
86	Integración nativa con el entorno existente de Darktrace/Email y Microsoft Exchange Online.
87	Inspección del correo saliente antes de la entrega al destinatario final.
88	Implementación gradual, iniciando con un grupo piloto y ampliando la cobertura una vez verificadas la ruta de correo y las acciones.
89	Configuración de flujos de acción, notificaciones, operación, transferencia de conocimiento y soporte.
90	Entrega de evidencias de configuración, pruebas funcionales, plan de reversa y documentación final.
91	A nivel de arquitectura y despliegue la solucion DLP debera: integrarse de manera nativa con el entorno existente de Darktrace Email y Microsoft 365. analizar el tráfico de correo saliente antes de su entrega al destinatario final, permitiendo la prevención de fugas de información en tiempo real. operar mediante integración con Microsoft Exchange Online utilizando conectores y reglas de flujo de correo, sin requerir infraestructura local adicional. soportar entornos Microsoft 365 y permitir una implementación gradual por grupos de usuarios, dependencias o dominios. permitir la protección de correos electrónicos salientes sin afectar la continuidad operativa de los usuarios finales.

92	Análisis basado en Inteligencia Artificial La solución deberá utilizar Inteligencia Artificial y Machine Learning para analizar simultáneamente el contenido, contexto y comportamiento de los usuarios. La solución deberá identificar intentos de fuga de información sin depender exclusivamente de reglas estáticas, expresiones regulares o etiquetado manual. La solución deberá incorporar modelos de IA capaces de comprender entidades, relaciones contextuales, patrones de información sensible y comportamiento normal de los usuarios. La solución deberá crear perfiles de comportamiento por usuario, grupo y organización para identificar actividades anómalas relacionadas Sucon exfiltración de datos.
93	Protección de información sensible La solución deberá detectar intentos de envío de información sensible hacia: • Cuentas personales. • Direcciones de correo nunca antes utilizadas. • Servicios de correo gratuito. • Destinatarios externos inusuales. • Destinatarios con riesgo elevado según el contexto organizacional. • La solución deberá proteger archivos adjuntos y contenido embebido dentro del correo electrónico.
94	Prevención activa, retención y liberación • La solución deberá poder retener mensajes salientes antes de su entrega cuando un flujo de acción identifique un posible incidente de pérdida de datos. • La acción preventiva para correo saliente deberá implementarse mediante la acción Hold Message. • Los flujos de acción predeterminados deberán poder habilitarse individualmente y permanecer deshabilitados hasta que la entidad autorice su activación. • La solución deberá permitir la liberación de mensajes retenidos por personal autorizado desde la consola. • Para mensajes con múltiples destinatarios, la propuesta deberá explicar que una retención activada por un destinatario impide inicialmente la entrega a todos los destinatarios, aunque la liberación pueda gestionarse por destinatario. • La solución deberá permitir ajustar umbrales y lógica del flujo sin reemplazar el resultado preventivo requerido para el correo saliente. • La propuesta deberá indicar claramente que no es posible retener de forma retroactiva un correo que ya fue entregado.

95	Detección de amenazas internas y compromiso de cuentas • La solución deberá correlacionar información proveniente de actividad de usuarios, correos entrantes, correos salientes y señales de compromiso de cuenta para identificar posibles exfiltraciones de información. • La solución deberá detectar situaciones de error humano como: o Envío accidental a destinatarios equivocados. o Respuesta con adjuntos sensibles. o Reenvío indebido de información. o Compartición accidental de datos regulados.

_____

Contratista