LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE
No. JEMPP-CEDE6-DIPCO-ET-2686/ COMUN-04

CONTENIDO

Elaboró	Revisó	Aprobó
SV. OLGUERG BARRIOS NIÑO Suboficial Analista Respuesta Cibernética	MY. BAHENA VASQUEZ FABIAN ANDRES Ejecutivo y Segundo CDTE BACCI DRA GLORIA CECILIA CORREA. Asesora jurídica CEDE6	TC. RAMIRO ESTEBAN SILVA GUTIÉRREZ Comandante BACCI

1. OBJETO

Establecer los requisitos técnicos necesarios para contar con el licenciamiento de la plataforma DARKTRACE, con la que cuenta en la actualidad el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

- **ANTIGENA**: es una solución de respuesta autónoma desarrollada por Darktrace, una empresa de ciberseguridad. Antigena utiliza inteligencia artificial y aprendizaje automático para detectar y responder a amenazas cibernéticas en tiempo real. Actualmente la solución se conoce como "Darktrace Respond Network"

- **APPLIANCE**: se refiere a un componente hardware o dispositivo que está diseñado específicamente para proporcionar una función o recurso de computación determinado. Un appliance se presenta como un elemento hardware cerrado, lo que significa que está diseñado para realizar una tarea específica y no se espera que sea modificado o personalizado por el usuario final.

- **DARKTRACE:** Es una plataforma basada totalmente en IA (Inteligencia Artificial) la cual maneja maching learning no supervisado, es una tecnología que no necesita ningún tipo de training de datos, o comparación de firmas, políticas o reglas. Cuenta con un cyber analist que realizadas investigaciones 7x24 de manera autónoma, su funcionamiento se basa en autoaprendizaje, detecta patrones raros e inéditos en la información, con la habilidad de realizar bloqueo autónomo sobre conexiones, todo basado en el ruido que genera la actividad diaria de los sistemas digitales de la red.

- **IA (INTELIGENCIA ARTIFICIAL):** La IA se refiere a un campo de la informática que se enfoca en la creación de máquinas y sistemas que pueden funcionar y reaccionar de manera similar a los seres humanos. La IA utiliza algoritmos y técnicas de aprendizaje automático para realizar tareas que normalmente requerirían inteligencia humana, como el reconocimiento de imágenes, el procesamiento del lenguaje natural y la toma de decisiones.

2.2 APLICACIÓN

Contar con un enfoque proactivo para la ciberseguridad integral haciendo uso de IA (Inteligencia Artificial) que busca proteger la infraestructura de red ante cualquier evento de seguridad, que proporcione visibilidad para una postura preventiva, detección en tiempo real y respuesta autónoma a amenazas conocidas y desconocidas.

3. REQUISITOS

3.1 REQUISITOS GENERALES

Realizar todas las tareas de licenciamiento de la plataforma con sus módulos, herramientas, y/o servicios con los que cuenta el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, relativas a la plataforma DARKTRACE garantizando la disponibilidad al 100% de la herramienta.

3.2 REQUISITOS ESPECÍFICOS

<table>
<tr><th>N°</th><th>REQUISITOS</th></tr>
<tr><td>3.2.1</td><td>TIPO LICENCIAMIENTO:

• Darktrace Detect Network
• Darktrace Respond Network

Licenciar todos los equipos de la red de sensores Darktrace desplegados en las diferentes unidades del Ejército Nacional así:
<table><tr><th>TIPOS DE EQUIPOS A LICENCIAR</th></tr><tr><td>Appliance DCIP-Z</td></tr><tr><td>Appliance DCIP-X2</td></tr><tr><td>Appliance DCIP-M</td></tr><tr><td>Appliance DCIP-S</td></tr><tr><td>Vsensor</td></tr></table></td></tr>
<tr><td>3.2.1.1</td><td>Darktrace Detect Network: Darktrace realiza una inspección profunda a todas la conexiones y paquetes haciendo uso de la IA y del autoaprendizaje, analizando datos en milisegundos y en tiempo real, destacando cualquier métrica inusual y emitiendo una puntuación que Darktrace Respond Network recoge y prioriza en el momento adecuado.</td></tr>
</table>

	La solución de Darktrace está basada en hardware de propósito específico para optimizar y reforzar continuamente la seguridad de la organización en cada etapa del ciclo de vida de un ataque, cuenta con componentes de monitoreo para detección y respuesta donde debe englobar un conjunto interconectado de productos de IA y machine learning no supervisado; ofreciendo capacidades de ciberseguridad proactiva con el fin que permita la detección y respuesta frente a amenazas desconocidas en las redes físicas y virtuales de la organización, incluyendo nubes públicas y privadas contratadas por la organización para soportar sus operaciones. Este enfoque tecnológico está basado en varios componentes que retroalimentan constantemente el sistema en su conjunto, manteniendo la estabilidad cibernética de la organización, mejorando continuamente el estado de la ciberseguridad, comprendiendo el entorno y detectando cualquier desviación.
	Darktrace Respond Network: Darktrace Respond contiene y desarma las amenazas de forma autónoma, todo ello respaldado por la toma de microdecisiones impulsada por la IA, La respuesta autónoma toma datos de eventos, los combina con el contexto general del entorno, así como con guías humanas para determinar en milisegundos la mejor respuesta posible sin interrumpir el negocio.
3.2.1.2	Darktrace Respond/Network controla las conexiones entre dispositivos de red enviando paquetes de restablecimiento de TCP a ambos puntos finales de una conexión de red no deseada. Estos paquetes se forman a partir de propiedades de los paquetes capturados; contienen encabezados IP y TCP falsificados. Darktrace Respond/Network enviará una cantidad de paquetes a cada punto final, variando el encabezado TCP e IP de las propiedades para aumentar la probabilidad de recepción exitosa en el punto final y la interrupción exitosa de la Conexión TCP.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque. OMITIDO

3.3.2 Rotulado. OMITIDO

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

OMITIDO

4.1.1 Muestreo. OMITIDO

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado. OMITIDO

4.2 TOMA DE MUESTRAS Y CRITERIOS DE ACEPTACIÓN O RECHAZO PARA EVALUAR REQUISITOS ESPECÍFICOS.
OMITIDO

4.2.1 Muestreo. OMITIDO

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos. OMITIDO

5. MÉTODOS DE ENSAYO

OMITIDO

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia.
- Código Civil.
- Código General del Proceso.
- Código de Comercio.
- Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 80 de 1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública" y las demás normas que la modifiquen o aclaren.
- Ley 816 de 2003 "Por medio de la cual se apoya a la industria nacional a través de la contratación pública" y las demás normas que la modifiquen o aclaren.
- Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos" y las demás normas que la modifiquen o aclaren.
- Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de

Espectro y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.

- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" y las demás normas que la modifiquen o aclaren.
- Decreto Ley 19 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública" y las demás normas que lo modifiquen o aclaren.
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Decreto 1082 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional" y las demás normas que lo modifiquen o aclaren.
- Decreto 103 del 20 de enero de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones" y las demás normas que lo modifiquen o aclaren.
- Resolución 4223 del 23 de junio de 2022 "Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, unas funciones de carácter administrativo y se dictan otras disposiciones".
- Resolución No. 4130 del 16 de junio de 2022 "MANUAL DE CONTRATACIÓN Y DE CONVENIOS" del Ministerio de Defensa Nacional y las demás normas que la modifiquen o aclaren.
- Resolución 2710 del 03 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones "Por la cual se establecen lineamientos para la adopción del protocolo IPv6", modificada por la Resolución 1126 de 2021 "por la cual se establecen lineamientos para la adopción del protocolo IPv6" y las demás normas que la modifiquen o aclaren.
- Resolución 7870 del 26 de diciembre de 2022, por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digita, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al sector defensa, y se dictan otras disposiciones".
- Directiva permanente 00201 de 2017 "Lineamiento de ciberseguridad y Ciberdefensa para el Ejercito Nacional" y las demás normas que la modifiquen o aclaren.
- Directiva permanente 00221 de 2017 "Seguridad de la información para el Ejercito Nacional" y las demás normas que la modifiquen o aclaren.
- Procedimiento documentos Técnicos Normativos P-JEMPP-CEDE4-348.

LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE No. JEMPP-CEDE6-DIPCO-ET-2686/ COMUN-04

6.2 ANTECEDENTES

OMITIDO

7. ANEXOS

No se relacionan anexos

8. CONTROL DE REVISIONES

Debe contener un cuadro de control de revisiones, cada especificación técnica debe llevar un registro denominado control de revisiones el cual permite asegurar que se identifiquen los cambios realizados y el estado de revisión actual del documento.

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación de la especificación técnica ACTUALIZACIÓN DEL LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE No. No. JEMPP-CEDE6-DIPCO-ET-2686/ COMUN-01	1/10/2021
01	Se realizan cambios por creación de unidad de GAOCC/CIBERDEFENSA a Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional. Se incluyeron en el numeral 1.12 los temas específicos de la Transferencia Tecnológica. Por lo anterior, queda sin validez la anterior versión y a partir del momento rige la presente versión.	09/06/2022
02	Se incluyeron en el numeral 1.2 la totalidad de los dispositivos a licenciar de la herramienta. Por lo anterior, queda sin validez la anterior versión y a partir del momento rige la presente versión.	06/03/2023
03	Se realizan cambios en el ítem 1.2, eliminando las cantidades de los dispositivos a licenciar. Se realizan cambios en las normas que deben consultarse ítem 6.1 Por lo anterior, queda sin validez la anterior versión y a partir del momento rige la presente versión.	01/08/2023
04	Se realizaron las siguientes modificaciones a la especificación técnica ACTUALIZACIÓN DEL LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE No. JEMPP-CEDE4-DIETE-ET-2686/ COMUN-03. Se actualiza la Especificación técnica en atención al oficio No. 2024574001567841 de fecha 17 de junio de 2024 elaborado por el BACCI, en cumplimiento a la circular 2023218004540933 del 09 de marzo y el boletín 030 del 17 de febrero de 2023 emitido por JEMPP, acogiéndose al numeral 05. Se modifica el nombre, quedando como: LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE	28/06/2024

LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE No. JEMPP-CEDE6-DIPCO-ET-2686/ COMUN-04

	Se modifica la línea de mando quedando como: No. JEMPP-CEDE6-DIPCO-ET-2686/ COMUN-04 Se eliminan los ítems 1, 1.1, 1.2 agregando nuevas características técnicas relacionadas al licenciamiento. Se eliminan los ítems 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12 que hacen parte del documento Anexo técnico de la especificación técnica de obligatorio cumplimiento. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza la pluralidad de oferentes. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. El Batallón de Ciberdefensa y Ciberseguridad BACCI, técnica garantiza que la presente especificación fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional. Por lo anterior, queda sin validez la especificación técnica ACTUALIZACIÓN DEL LICENCIAMIENTO PARA LA PLATAFORMA DARKTRACE No. JEMPP-CEDE4-DIETE-ET-2686/ COMUN-03 y a partir del momento rige la presente versión.	