POSITIVA COMPAÑÍA DE SEGUROS	MACROPROCESO: GESTIÓN DE ABACTECIMIENTO PROCESO: GESTIÓN PRECONTRACTUAL SUBPROCESO: ANÁLISIS EXTERNO E INTERNO	Código:	APO_10_1_2_FR08
		Versión	01
		Clasificación	Pública clasificada
		Fecha:	15/07/2019
	FORMATO **ANÁLISIS DEL SECTOR Y ESTUDIO DE MERCADO**		

Aprobó:	Revisó:	Elaboró:
Luis Javier Castellanos Sandoval Gerente Abastecimiento Estratégico	**Martha Cecilia Florez Sanchez** Profesional Universitario	**Nicolás Martínez Benavides** Profesional Universitario

DESCRIPCIÓN DE LA NECESIDAD	
1. ASPECTOS GENERALES	
¿Cuál es su necesidad? Objeto	Prestación de servicios que permitan hacer correlación de eventos que puedan alertar, gestionar y brindar recomendaciones sobre incidentes de seguridad mediante la utilización de un SIEM.
Valor de la necesidad plan de contratación	$1.646.422.514

1.1 CONTEXTO ECONÓMICO

La transformación productiva, como una estrategia consolidada para su fomento y crecimiento, que en los últimos años han generado un ambiente adecuado para su reconocimiento a nivel mundial.

Con los programas de Gobierno en Línea, Fortalecimiento de la Industria TI y Vive Digital (Este programa tiene como objetivos generar crecimiento económico basado en el uso y apropiación de las TIC´s en la población colombiana y el desarrollo de un ecosistema digital nacional. A través de este programa, a cierre de 2013, se lograron conectar 1.048 municipios aumentando las conexiones a internet de 2.2 a 8.8 millones a nivel nacional), a través del Ministerio de Tecnologías de la Información, el Gobierno colombiano trabaja en la masificación del uso redes y el aprovechamiento de las mismas. Estos programas abren un amplio espectro de oportunidades para las industrias de Hardware y Servicios TI en el país por la masificación y acceso de la tecnología, un crecimiento en la demanda de la industria y los habitantes de estos bienes y servicios.

Por último, al evaluar el uso (impacto) de las TIC en el territorio colombiano, se evidencio que Colombia ha mejorado el acceso a servicios básicos y en el uso de las TIC para así mejorar la prestación de servicios a la ciudadanía.

El uso de las TIC ha permitido “cerrar brechas con la población económica o geográficamente marginada, al facilitar una eficiente provisión de información y reducir las diferencias en capacitación, en términos de contenidos. También posibilita a las Pymes mejorar su productividad y expandir sus mercados potenciales, multiplicando al tiempo su competitividad y el tamaño de la demanda.

Finalmente, acerca al Estado con el ciudadano, permitiendo mayor precisión en la ejecución de la política social”

1.2 CONTEXTO TÉCNICO

La gestión de eventos e información de seguridad (SIEM, por Security Information and Event Management) es un enfoque de gestión de la seguridad que busca proporcionar una visión holística de la seguridad de la tecnología de la información (TI) de una organización. El acrónimo se pronuncia "sim" con una e silenciosa.

El principio subyacente de un sistema SIEM es que los datos relevantes sobre la seguridad de una empresa se producen en múltiples ubicaciones, y al ser capaces de ver todos los datos desde un único punto de vista, es más fácil detectar tendencias y ver patrones fuera de lo común. SIEM combina funciones de SIM (gestión de información de seguridad) y SEM (gestión de eventos de seguridad) en un sistema de gestión de seguridad.

Un sistema SIEM recoge registros y otra documentación relacionada con la seguridad, para ser analizados. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación de forma jerárquica

para recopilar eventos relacionados con la seguridad de dispositivos de usuario final, servidores, equipos de red e incluso equipos de seguridad especializados como firewalls, antivirus o sistemas de prevención de intrusiones. Los recolectores envían eventos a una consola de administración centralizada, que realiza inspecciones y señala anomalías. Para permitir que el sistema identifique eventos anómalos, es importante que el administrador de SIEM cree primero un perfil del sistema en condiciones normales de evento.

Endpoint Detection and Response (conocida por sus siglas en inglés EDR) es una herramienta que proporciona monitorización y análisis continuo del endpoint (equipo de cómputo) y la red. La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad. El EDR en sus inicios estaba más pensado para grandes empresas con SOC dedicados. Hoy en día, la demanda de este tipo de soluciones se ha desplazado a empresas de todos los tamaños.

Evolución del mercado

La propia evolución del mercado ha llevado a que los distintos fabricantes vayan integrando en sus EPP (Endpoint Protection Plataform - Antivirus) funcionalidades EDR.

El objetivo es que la empresa esté protegida frente a cualquier posible incidente de seguridad.

Tanto si es una amenaza tradicional, una aplicación vulnerable o una amenaza desconocida. Proporciona herramientas adicionales para buscar amenazas desconocidas. Es posible realizar un análisis forense y responder de manera rápida y efectiva a los ataques. La tecnología EDR detecta ataques que nuestro antivirus ha pasado por alto. Monitoriza y evalúa todas las actividades de la red (eventos de los usuarios, archivos, procesos, registros, memoria y red). Detecta ataques informáticos en tiempo real, y permite tomar medidas inmediatas si es necesario.

EDR vs EPP

Un EPP (Antivirus) se centra únicamente en la prevención en el perímetro. Tiene como objetivo evitar que las amenazas ingresen en la red. El EDR está enfocado en amenazas avanzadas, las diseñadas para evadir la primera capa de defensa y que logran penetrar en la red. Detecta esa actividad y contiene al adversario antes de que pueda moverse lateralmente en la red.

Cómo funciona un EDR

El EDR es más efectivo que un antivirus en la detección del malware desconocido puesto que utiliza una serie de técnicas novedosas, como son:

- Machine learning y la analítica.
- Sandboxing.
- Alertas generadas por sistemas externos (IOC o indicadores de compromiso), categorización de los incidentes para actuar sobre los más críticos con rapidez.
- Investigación de los incidentes desde el punto de vista histórico: se rastrea el origen y evolución del malware para tomar medidas preventivas de cara a incidentes futuros.
- Herramientas de remediación para eliminar los ficheros infectados, poner en cuarentena y volver al estado anterior a la infección.

Características clave del EDR

a. Detección.

Utilizan la IA (inteligencia artificial) para reducir la tasa de falsos positivos.

Los equipos pueden optimizar los recursos clave y centrarse en tareas de TI importantes en lugar de revisar un gran volumen de alertas y falsos positivos.

Diseñados para vigilar y responder a una variedad de amenazas, no solo al malware.

Es una defensa contra un amplio rango de amenazas, como ransomware, malware, botnets y otras amenazas conocidas y desconocidas. Accesos no autorizados, ataques sigilosos para robo de datos, etc.

b. Contención.

Permite un bloqueo avanzado de amenazas.

No sólo es capaz de detectar rápido nuevas amenazas, sino que puede manejar ataques en directo y protegernos mientras éstos se producen.

c. Investigación.
Respuesta rápida frente a incidentes.
Cualquier empresa está expuesta a ser víctima de un ciberataque. El EDR permite una respuesta rápida y precisa a los incidentes. El objetivo es detener un ataque y volver a al trabajo cuanto antes.
d. Eliminación.
Reparación del endpoint a fondo.

Para que puedan recuperar el estatus anterior a ser infectados.

1.3 CONTEXTO REGULATORIO

El sector de sistemas de a información está regulado por el Ministerio de las Tecnologías de la Información y las Comunicaciones conforme a la 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"

- 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".

- Decreto 2618 de 2012 "Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones".

- LEY 1273 DEL 5 DE ENERO DE 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado de *la protección de la información y de los datos*-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- Circular externa 007 de 2018 de la Super Intendencia Financiera de Colombia.

- Manual para la Gestión de Abastecimiento de POSITIVA.

2. ESTUDIO DE LA OFERTA

En temas de Seguridad Informática existen múltiples herramientas para Auditoria de Bases de Datos y aplicaciones, algunas de código abierto y con licenciamiento como GNU GPL, que sirven al propósito requerido por la Entidad, pero presentan problemas de instalación, mantenimiento, versatilidad en la presentación de resultados y ningún tipo de soporte o garantías.

En la determinación del presupuesto aproximado de los servicios a adquirir, se tuvo en cuenta el estudio de mercado realizado con las cotizaciones presentadas por firmas que suministran y prestan los servicios requeridos. Las Empresas que atendieron la solicitud de cotización, fueron las siguientes:

- **INTERLAN SAS:** Organización con más de 25 años de experiencia en el mercado, especializada en suministrar, implementar y administrar soluciones de infraestructura y seguridad TI. En el ámbito de seguridad informática ofrecen servicios de consultoría en áreas como integridad, confidencialidad y continuidad de los sistemas de Información. Esto incluye soluciones antivirus, antimalware, antispam, respaldo, prevención en fuga de información, virtualización, gestión de dispositivos y continuidad del negocio. Partner de múltiples marcas entre ellas Aruba-HPE, Fortinet, Trend Micro, Palo Alto.

- **SONDA DE COLOMBIA:** SONDA es un grupo empresarial de Tecnologías de la Información, cuya casa matriz se encuentra en Chile y tiene 42 años de trayectoria, transformándose en el principal integrador y proveedor

de servicios de TI, siendo líder en América Latina con ingresos en el 2018 de US$1.151,7 millones y más de 18.000 colaboradores directos. SONDA tiene un extenso alcance en la región, con empresas en Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Perú y Uruguay.

- **WEXLER:** WEXLER S.A.S es una compañía de origen colombiano, con exigentes principios y valores éticos, que durante más de 10 años ha dedicado todos sus esfuerzos de Investigación y Desarrollo I+D al fortalecimiento de la Seguridad de la Información y Ciberseguridad de sus clientes; generando soluciones tecnológicas que se adaptan exactamente a las necesidades de las Organizaciones; respaldado en un equipo de trabajo que cuenta con el máximo nivel de certificación y experiencia en cada una de las soluciones que ofrece.

- **ADSUM:** Soluciones Tecnológicas con mas de 10 años en el mercado colombiano. Enfocados en las áreas de seguridad informática, conectividad empresarial y redes definidas por software, computo convergente e hiperconvergente y servicios de outsourcing TIC de nueva generación. Soluciones que desarrollan con un equipo humano especializado y certificado en cada una de las tecnologías y fabricantes que representan.

El resultado de las cotizaciones recibidas es el siguiente:

Tiempo cotizado: 33 meses

PROVEEDOR	VALOR MES	VALOR TOTAL
INTERLAN SAS	$63.218.244=	$2.086.202.060=
SONDA DE COLOMBIA	$49.891.591=	$1.646.422.514=
WEXLER SAS	$148.443.485=	$4.880.785.000=
ADSUM	$60.183.769=	$1.986.064.361=

Para la adquisición de los servicios del presente proceso se tuvieron en cuenta las siguientes variables que son parte importante de la toma de decisión para la contratación directa:

1. El proceso de implementación del servicio de ciberseguridad SOC Fase 1 tomó alrededor de 5 meses, donde se afinaron temas de monitoreo, conectividad, control de acceso y seguimiento del equipo Colector de logs para la infraestructura esencial de Positiva.
2. Se creó una base de conocimiento amplio y especializado acerca del comportamiento del tráfico de red al interior de la compañía donde se han ido identificando los eventos reconocidos como falsos positivos y dando prioridad a los que son eventos de seguridad como tal.
3. El cambio del proveedor actual implica reprogramar la implementación, estabilización y afinamiento del servicio durante 5 meses aproximadamente, lo que generaría dejar de contar con el servicio y un sobrecosto del proceso y avances en la ciberseguridad de Positiva.
4. Para la continuidad del servicio de ciberseguridad SOC fase 2, donde uno de los componentes importantes a implementar es el servicio de EDR, se solicitó una PoC (Prueba de concepto), la cual arrojó los siguientes resultados:

Prueba de Concepto herramienta de EDR (Endpoint Detection and Response)

Ficha Técnica
Fabricante: FORTINET
Solución: FortiEDR

Licencia de evaluación: 40 equipos de cómputo y 10 servidores

Installation ID: **8057280589** Name: **Positiva** Expiration Date: **25-Feb-2021**

License Status

Communication Control:	**Available**
Forensics:	**Available**
Threat Hunting:	**Available**
Content Updates:	**Available**
Vulnerability Management:	**Available**
License Capacity:	**40 workstations, 10 servers, 50 IoT devices**
In Use:	**37 workstations, 7 servers, 0 IoT devices**
Remaining:	**3 workstations, 3 servers, 50 IoT devices**

Equipos objetivo de la prueba de concepto

Para esta prueba de concepto se instaló el agente en 7 servidores que son utilizados en ambientes de pruebas, no productivos, con el fin de evitar cualquier impacto en la operación del negocio.

Para los equipos de cómputo con el apoyo de la OGIR se definieron los 40 equipos objetivo para la prueba de concepto, de éstos se realizó la prueba en 37 de ellos.

A continuación, se muestran las imágenes del dashboard con los insumos registrados previamente:

Para la prueba, la herramienta se configura en modo simulación, es decir, hace un análisis del comportamiento de cada equipo de cómputo, sus servicios y aplicaciones de red, sin afectar la operación de los equipos y servidores. De esta forma pudimos ver todos los procesos de máquina que se ejecutan y cuales son identificados como posible amenaza.

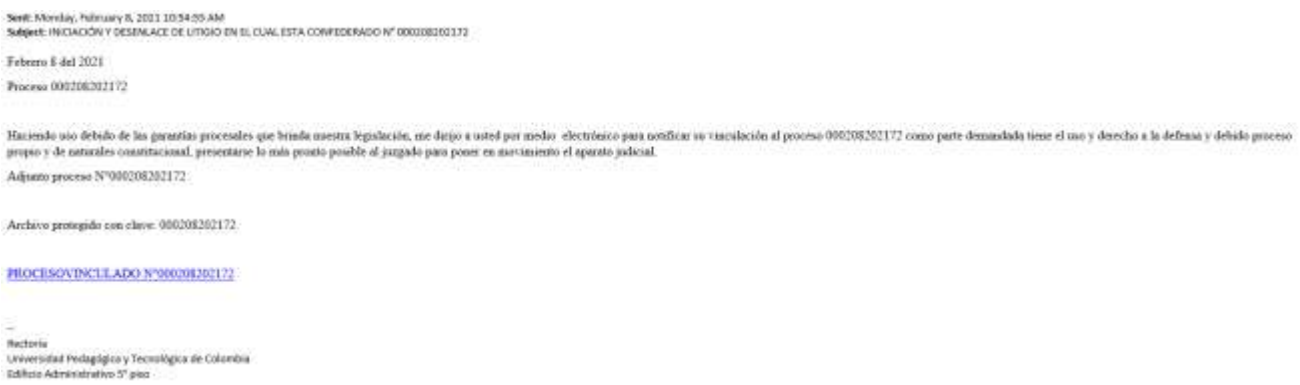
Pruebas de laboratorio en ambiente controlado

Adicional a las pruebas de seguimiento y conocimiento de la herramienta se preparó un equipo aislado de la red corporativa y en un ambiente controlado para poder hacer un análisis más exhaustivo de las amenazas que llegan por correo electrónico y otros medios, haciendo una emulación de la ejecución del archivo malicioso para ver su comportamiento.

Desde la Presidencia de Positiva se solicitó realizar un análisis de un correo con posible phishing, el cual se detalla a continuación:

- *Introducción:*

El día 08 de Febrero de 2021 a las 10:54 AM en uno de los buzones de la entidad se recibe un correo aparentemente proveniente de la universidad pedagógica y tecnología de Colombia, teniendo en cuenta que el registro MX del dominio uptc.edu.co no cuenta con registros SPF, el sistema de anti-spam de Positiva no pudo bloquear ya que no se pudo validar su legitimidad, este correo contiene un link que apunta a un ubicación en Google Drive, la cual contiene un archivo .RAR, el cual es un archivo cifrado con un password el cual es parte del mensaje del correo. Debido a lo sospechoso del correo el mismo es remitido a la OTI para su evaluación, para lo cual se prepara un ambiente controlado, con una máquina Windows 10 aislada totalmente de la red corporativa, la cual cuenta con la solución de Fortinet Endpoint Detection and Response o FortiEDR por sus siglas en Ingles, la cual es una plataforma de cacería y destrucción de amenazas conocidas y desconocidas basado en inteligencia artificial o AI, en el presente documento se detallan los resultados de la evaluación de este paquete de software sospechoso.



Sent: Monday, February 8, 2021 10:54:55 AM
Subject: INICIACIÓN Y DESENLACE DE LITIGIO EN EL CUAL ESTA CONFEDERADO N° 000208202172

Febrero 8 del 2021

Proceso 000208202172

Haciendo uso debido de las garantías procesales que brinda nuestra legislación, me dirijo a usted por medio electrónico para notificar su vinculación al proceso 000208202172 como parte demandada tiene el uso y derecho a la defensa y debido proceso propio y de naturales constitucional, presentarse lo más pronto posible al juzgado para poner en movimiento el aparato judicial.

Adjunto proceso N°000208202172

Archivo protegido con clave: 000208202172

PROCESOVINCULADO N°000208202172

--
Rectoría
Universidad Pedagógica y Tecnológica de Colombia
Edificio Administrativo 5° piso

- *Activos de Información Analizados*

Se realizó el análisis de comportamiento basado en inteligencia artificial sobre los siguientes activos:

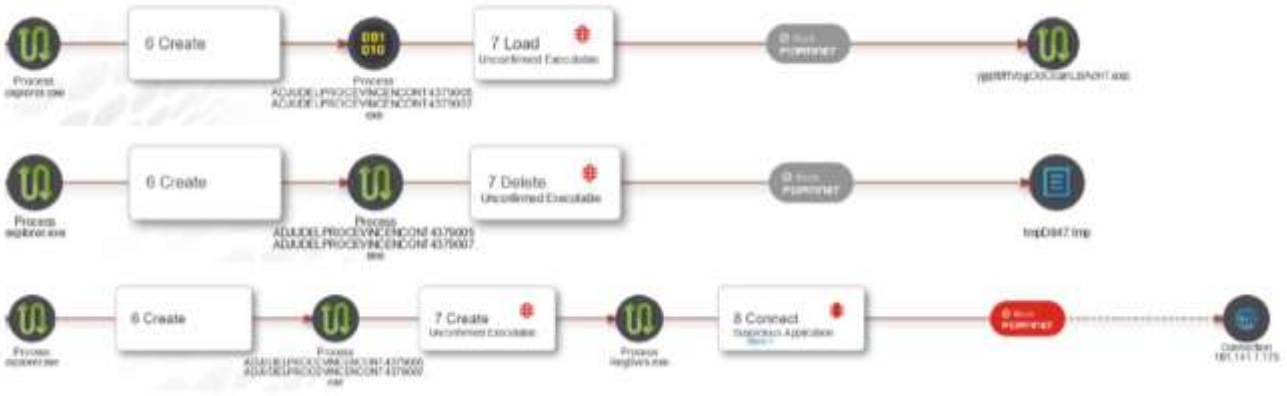
NOMBRE DEL ACTIVO
ADJUDELPROCEVINCENCONT4379007.exe

- *Resumen de Hallazgos*

Como resultado del análisis se logró identificar que el correo enviado es del tipo spear-phishing el cual es un tipo de ataque vía email el cual se centra en un grupo u organización y es un ataque dirigido, también se pudo determinar que el link contenía una pieza de software maliciosa la cual estaba compuesta por elementos con ransomware de Dia-0, lo cual hace imposible que soluciones tradicionales de detección de malware pudieran detenerlo en caso tal que el hash de la piza principal se vuelva polimórfica y sea mutada a una elemento desconocido, tales componentes se explican a continuación:

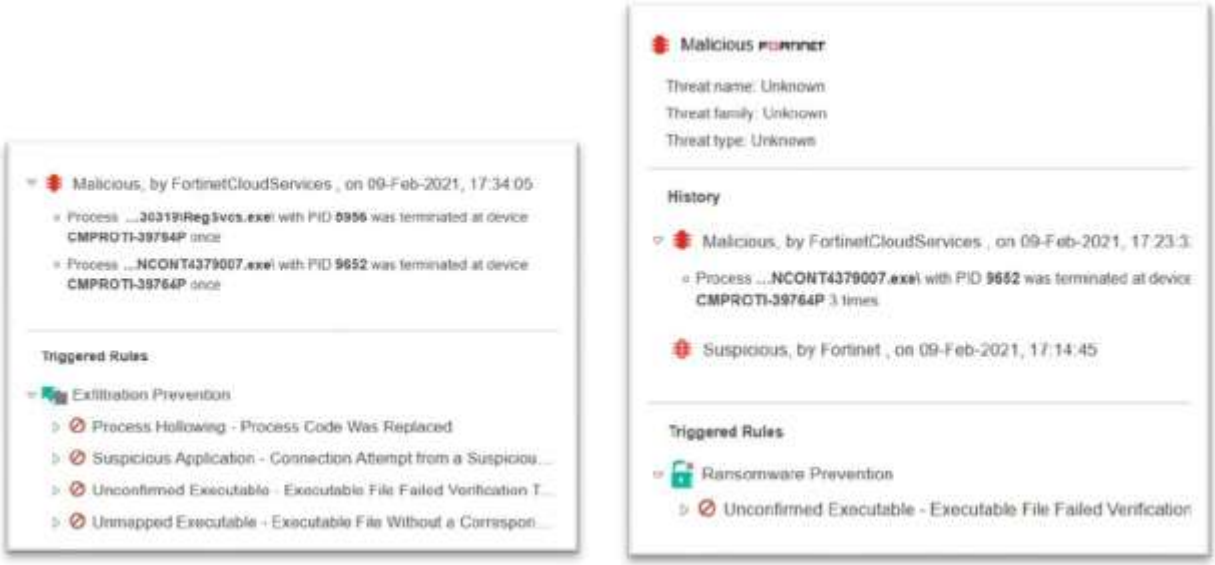
PROCESO	CLASIFICACION	DESTINO	FECHA	ACCION	USUARIO	RUTA
RegSvcs.exe	Malicious	181.141.1.175	2021-02-09 17:21:11	Block	POSITIVA \79887102	C:\Windows\Microsoft.NET\ Framework\w4.0.30319\RegS vcs.exe
RegSvcs.exe	Malicious	181.141.1.175	2021-02-09 17:14:39	Block	POSITIVA \79887102	C:\Windows\Microsoft.NET\ Framework\w4.0.30319\RegS vcs.exe
ADJUDELPROCEVI NCENCONT4379005 ADJUDELPROCEVI NCENCONT4379007. exe	Malicious	2 destinations File Delete Attempt File Write Access	2021-02-09 17:14:38	Block	POSITIVA \79887102	C:\Users\79887102\Downloa ds\ADJUDELPROCEVINCENCONT 4379005\ADJUDELPROCEVINCE NCONT4379005 ADJUDELPROCEVINCENCONT4379 007.exe
yjjqfBftVogOdCcanL BAcHT.exe	Suspicious	In memory Execution	2021-02-09 17:14:24	Block	POSITIVA \79887102	yjjqfBftVogOdCcanLBAcHT.e xe
ADJUDELPROCEVI NCENCONT4379005 ADJUDELPROCEVI NCENCONT4379007. exe	Malicious	3 destinations File Creation In memory Execution Service Access	2021-02-09 17:13:58	Block	POSITIVA \79887102	C:\Users\79887102\Downloa ds\ADJUDELPROCEVINCENCONT 4379005\ADJUDELPROCEVINCE NCONT4379005 ADJUDELPROCEVINCENCONT4379 007.exe

- *Grafo: resumen de hallazgos (cadena de eventos)*

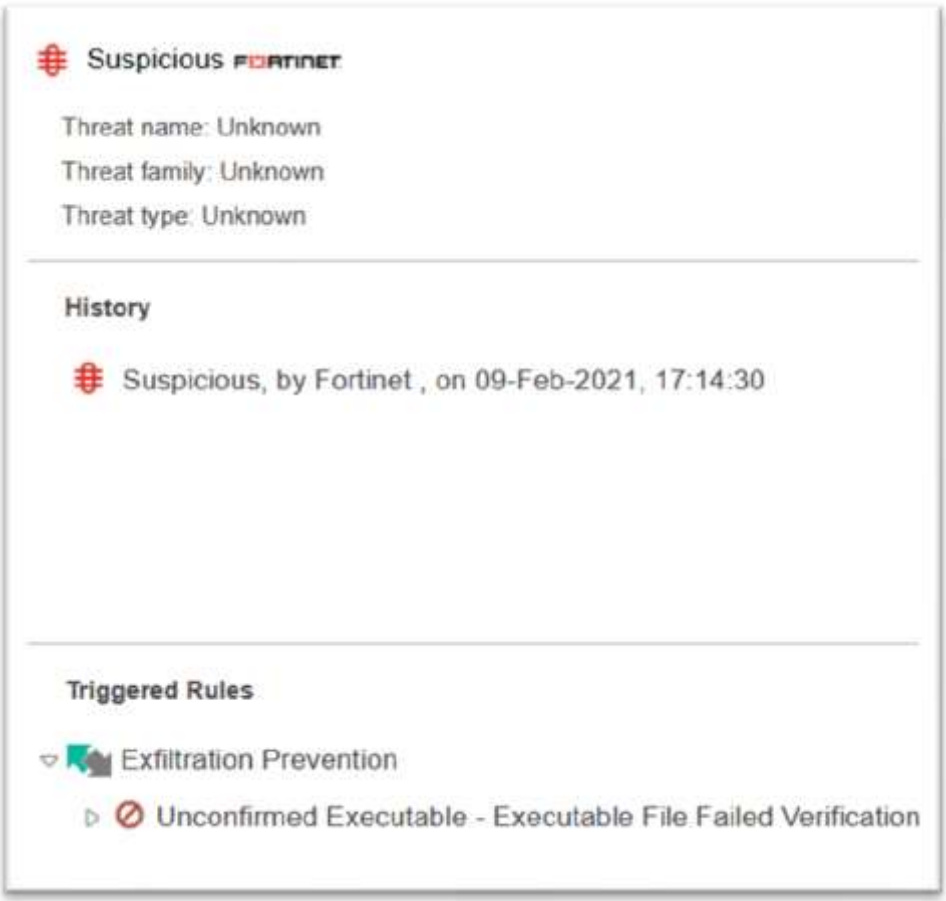


- *Resumen de eventos maliciosos*

Como se puede observar en las siguientes imágenes el paquete de software contenía ransomware y capacidades de robo de información, las cuales fueron bloqueadas por la solución.



- *Resumen de eventos sospechosos*



3. ESTUDIO DE LA DEMANDA		
¿Ha contratado la necesidad previamente?	Si ☒	No ☐
Contratará nuevamente con el mismo proveedor	Si ☒	No ☐
En caso de haber respondido afirmativamente, justifique su respuesta	El cambio del proveedor actual implica reprogramar la implementación, estabilización y afinamiento del servicio durante 5 meses aproximadamente, lo que generaría dejar de contar con el servicio y un sobrecosto del proceso y avances en la ciberseguridad de Positiva.	

Tras el incidente del 012 de mayo de 2017 (WannaCry) muchas empresas han decidido implantar un servicio de SOC (Security Operations Center) con el objetivo, entre otras cosas, de adelantarse a la materialización de una amenaza y la solución de EDR (Endpoint Detection and Response) que complementen a las medidas de EPP (Endpoint Protection Plataform - Antivirus) que ya tienen activas, llegando a donde estas no están consiguiendo llegar y robusteciendo la seguridad corporativa.

Una vez analizado los procesos contractuales a través del sistema electrónico de contratación Pública SECOP, portal Web *www.contratos.gov.co*, sobre entidades que hayan realizado contratos con condiciones similares en los últimos meses, se tiene lo siguiente:

Entidad Estatal	Referencia	Descripción	Fase actual	Fecha de publicación	Fecha de presentación de ofertas	Cuantía
INSTITUTO DE DESARROLLO URBANO	IDU-SASI-DTAF-001-2021 (Presentación de oferta)	CONTRATAR EL FORTALECIMIENTO, RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE DE LA PLATAFORMA SIEM (Presentación de oferta)	Presentación de oferta	19/02/2021 4:14 PM (UTC -5 horas)	8/03/2021 10:00 AM (UTC -5 horas)	451.000.000 COP

Entidad Estatal	Referencia	Descripción	Fase actual	Fecha de publicación	Fecha de presentación de ofertas	Cuantía
DIRECCION DE IMPUESTOS Y ADUANAS NACIONALES	IMC-00-036-2020	Compraventa de la suscripción del licenciamiento del producto Symantec End Point Protection (SEP) con la funcionalidad End Point Detection and Response (EDR).	Presentación de oferta	15/12/2020 6:18 PM (UTC -5 horas)	18/12/2020 10:00 AM (UTC -5 horas)	69.637.274 COP

El análisis de la demanda nos ofrece una mera referencia del estudio del sector, sin embargo, se puede concluir que de acuerdo con el estudio realizado los servicios solicitados se encuentran en el mercado nacional, el presupuesto asignado es razonable frente a las condiciones del mercado para dicha contratación y hay firmas que pueden proveer el servicio, de modo tal que se puede suplir la necesidad Institucional.

NOMBRE DE QUIEN ELABORÓ	*FIRMA*	*FECHA DE ELABORACIÓN*
Leonardo Estrada Castro		22 de febrero de 2021