SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

$25.00
DFPS_FOR578_v1.6_01-21
El póster fue creado por el instructor de SANS Robert M. Lee con el apoyo del profesorado de SANS DFIR

digital-forensics.sans.org

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

OPERATING SYSTEM & DEVICE IN-DEPTH

FOR308 Digital Forensics Essentials

FOR498 Battlefield Forensics & Data Acquisition GBFA

FOR500 Windows Forensics GCFE

FOR518 Mac and iOS Forensic Analysis and Incident Response

FOR585 Smartphone Forensic Analysis In-Depth GASF

INCIDENT RESPONSE & THREAT HUNTING

FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics GCFA

FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response GNFA

FOR578 Cyber Threat Intelligence GCTI

FOR610 REM: Malware Analysis GREM

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling GCIH

@sansforensics

sansforensics

dfir.to/MAIL-LIST

Threat Intelligence

CONSUMPTION

Existen tres niveles de inteligencia sobre amenazas: estratégico, operativo y táctico. Los niveles deben utilizarse como guía de referencia para recordar que diferentes públicos tienen diferentes requisitos de inteligencia sobre amenazas.

Nivel estratégico actores, como los ejecutivos y los responsables políticos, deben buscar la comprensión del panorama más amplio de las amenazas para identificar el riesgo para la organización y los cambios que se pueden hacer en las inversiones o en la cultura corporativa.

Nivel operativo el personal debe tratar de traducir los objetivos estratégicos en esfuerzos tácticos y viceversa, identificando los objetivos o tendencias generales de una operación o campaña. También deben tratar de estar al tanto de las campañas de los adversarios en lugar de las intrusiones individuales, identificar las lagunas de conocimiento de la organización y compartir información con organizaciones similares para aliviar esas lagunas de conocimiento.

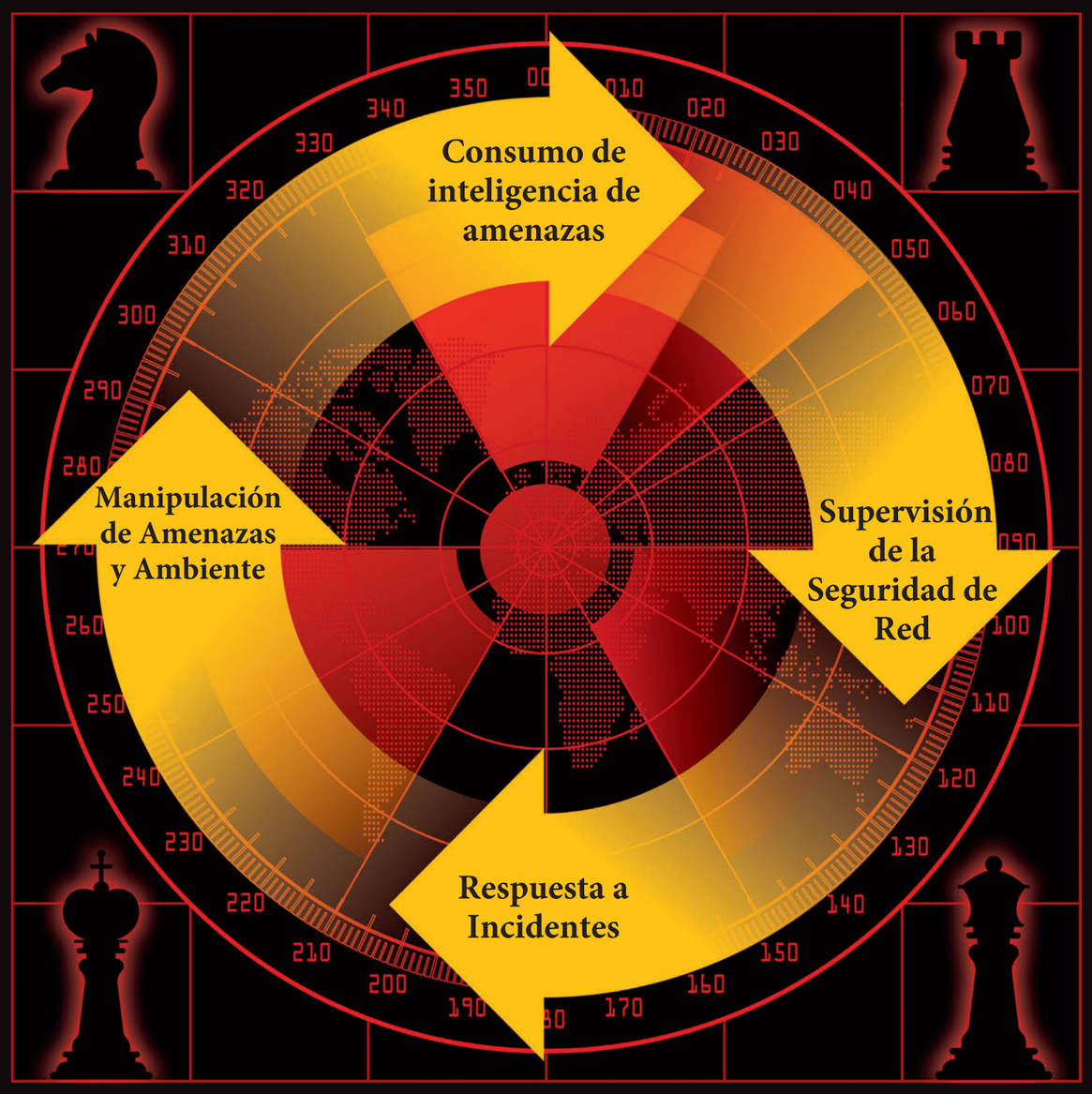
Nivel táctico la inteligencia se consume a menudo en forma de indicadores de compromiso (IOC) y tácticas, técnicas y procedimientos (TTP). Esto ayuda a impulsar la seguridad de una organización y le permite cazar las amenazas y responder mejor a ellas. Considere el uso de modelos como el Ciclo de Ciberdefensa Activa.

Ciclo de ciberdefensa activa

El ciclo de ciberdefensa activa es un modelo para consumir la inteligencia sobre amenazas. Se centra en la unión de varios equipos de seguridad para adoptar un enfoque de operaciones de seguridad para identificar y contrarrestar las amenazas. Puede comenzar en cualquier fase del ciclo, y las fases se alimentan continuamente entre sí para crear un proceso continuo.

Consumo de inteligencia de amenazas los analistas deben ser conscientes de los objetivos y necesidades de su organización, así como del espacio de ataque a la información. Deben ser capaces de buscar en la amplia gama de inteligencia de amenazas disponible y encontrar lo que es relevante para su organización. Se puede encontrar información como los IOC para ayudar a buscar amenazas en el entorno. .

Manipulación de amenazas y ambiente los analistas suelen realizar actividades como el análisis de malware; sin embargo, la amenaza no siempre utiliza malware. El análisis de la amenaza permite crear mejores COIs y comprender la amenaza y su impacto en el entorno y la organización. Recomendar cambios en el entorno cuando sea posible -como arreglar una vulnerabilidad o hacer un cambio lógico como el sinkholing de DNS- puede ayudar a reducir la efectividad de la amenaza.



La Supervisión de la seguridad de la red se centra en la búsqueda de amenazas en el entorno y consta de tres fases: recopilar, detectar y analizar. En la fase de recopilación, los analistas deben reunir datos del entorno, como el tráfico de red, los registros del sistema y los registros de los dispositivos de seguridad. En la fase de detección, los analistas deben buscar anormalidades y utilizar los IOCs y TTPs de los adversarios para buscarlos. La fase de análisis ayuda a confirmar que las amenazas son reales y no un falso positivo. Esto ayuda a reducir los falsos positivos de la respuesta a incidentes.

La Respuesta a incidentes debe centrarse en el alcance del impacto de la amenaza y de cualquier actividad maliciosa mientras se contiene y erradica la amenaza. Los COIs deben utilizarse para entender y fijar el verdadero alcance del problema para evitar reinfecciones.

FOR578:
Cyber Threat Intelligence
sans.org/FOR578

Threat Intelligence GENERATION

Las organizaciones que quieran generar inteligencia sobre amenazas deben tener prácticas de seguridad bien establecidas y ser capaces de recopilar datos de intrusiones exitosas e intentos de intrusión en sus organizaciones. La generación de inteligencia sobre amenazas debe comenzar con unos requisitos claros y proceder a aprovechar el conocimiento interno, como los datos sobre intrusiones, y el conocimiento externo, como los informes e información disponibles abiertamente. La clave está en capacitar a los analistas formados para que interpreten la información y produzcan conocimientos sobre las amenazas observadas, al tiempo que detallan la información técnica que puede utilizarse para ayudar a mejorar las operaciones de seguridad y la respuesta a los incidentes.

La cadena de muerte

La cadena de muerte destaca los pasos que los adversarios suelen realizar para completar su objetivo. Debe utilizarse como modelo de referencia para comprender la actividad del adversario y los indicadores de compromiso (IOC) observables. La categorización e identificación de indicadores y patrones a través de un gran número de intrusiones puede revelar conexiones en la actividad de intrusión, incluyendo la campaña de un adversario.

El reconocimiento es usualmente utilizado por los adversarios para investigar sus objetivos. Esto puede tener lugar en forma de escaneo o solicitudes a la infraestructura de cara al público. La investigación también puede realizarse contra su organización o personal sin interacción directa.

El armamento se produce cuando un adversario prepara una herramienta para utilizarla en la intrusión. Esto podría ser tan simple como un exploit y un malware combinados en un documento PDF. El analista debe centrarse en las opciones de exploits, malware o tácticas del adversario. Las elecciones del adversario pueden actuar como una huella en varias intrusiones.

La entrega es el paso en el que una amenaza entrega la capacidad armada en el entorno objetivo. Un ejemplo sería un correo electrónico de phishing con el PDF armado adjunto. También podría ser algo tan simple como una conexión VPN directamente en el entorno que está disponible para el abuso del adversario.

La explotación se manifiesta a menudo en el aprovechamiento técnico de las vulnerabilidades, pero no siempre se centra en ellas. Un adversario podría explotar la funcionalidad de PowerShell en un entorno para recopilar datos y evitar tener que usar malware.

La instalación suele observarse cuando se instala un malware en un sistema. Sin embargo, la instalación también puede observarse cuando un adversario ha modificado la funcionalidad nativa disponible en un entorno para mantener la persistencia.

Los servidores de mando y control (C2) ofrecen a las amenazas la oportunidad de interactuar con el entorno del objetivo y comunicarse con sus herramientas, como el malware, o interactuar directamente con los sistemas.

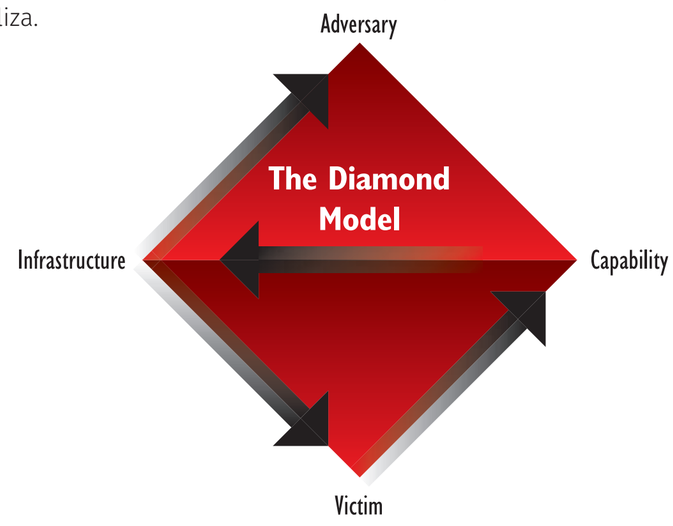
Las acciones sólo las dictan los adversarios y lo que tienen a su disposición. La intención del adversario es difícil de determinar porque el impacto observado puede no haber sido su intención. Cuando una amenaza llega al punto de completar las acciones del adversario y permitirle alcanzar su objetivo deseado, la intrusión es exitosa.

¿Qué es un TTP?

Una táctica, técnica o procedimiento (TTP) del adversario es el medio por el cual los adversarios logran sus objetivos. Las TTPs suelen consistir en de patrones de actividad de los adversarios que estos realizan de forma rutinaria. Por ejemplo, si un adversario obtiene constantemente acceso a VPNs no autenticadas en un entorno y luego aprovecha PowerShell dentro del entorno para robar documentos de propiedad intelectual, ese patrón podría observarse como una de sus TTPs. En el futuro, si identifica que el adversario está utilizando PowerShell en su entorno, puede querer salvaguardar rápidamente los documentos de propiedad intelectual mientras identifica y elimina las VPN no autenticadas. Como mínimo, los TTP deben incluir descripciones de la actividad observada del adversario (como el análisis de indicadores) con los objetivos percibidos del adversario.

El modelo del diamante

El Modelo Diamante de Análisis de Intrusiones identifica los cuatro componentes principales de cualquier evento malicioso: la víctima, la capacidad, la infraestructura y el adversario. Es un modelo independiente, pero también puede aplicarse a cada una de las fases de la cadena de muerte. La realización de este tipo de análisis permite a las organizaciones comenzar con un componente que pueden identificar (como la víctima) y trabajar para descubrir los otros tres componentes. Esto ayuda a comprender los motivos del adversario, así como la infraestructura y las capacidades que utiliza.



Referencias y lecturas recomendadas

Cadena de muerte:
http://dfir.to/KillChain

Modelo Diamante:
http://dfir.to/DiamondModel

La escala móvil de la ciberseguridad:
http://dfir.to/SlidingScale

Un ejemplo de proceso de SANS FOR578*.

Determinar las necesidades de inteligencia
¿Necesita la organización mejores conocimientos técnicos, como los COI y las tácticas, técnicas y procedimientos (TTP) del adversario, para aumentar la respuesta a los incidentes y la detección de las amenazas? O bien, ¿necesita la organización conocimientos sobre las campañas de los adversarios y orientación a los ejecutivos sobre el panorama de amenazas de la organización? Son estos objetivos específicos para ciertas amenazas o para salvaguardar datos específicos en la organización? Los requisitos guían lo que se recopila, qué y cómo se analiza, y el producto final que se difunde.

Analizar la información interna
¿Los responsables de la respuesta a incidentes, los equipos de seguridad de la empresa, los analistas de malware y otros miembros de su organización han proporcionado datos e información sobre intrusiones anteriores en la organización? Analice las intrusiones en función de modelos como el Diamond Model o el Kill Chain para extraer indicadores e identificar patrones de los adversarios. Las organizaciones deberían tener un mínimo de 60 días de registros para generar datos útiles. Por último, recuerde que los mejores datos son los internos de su organización.

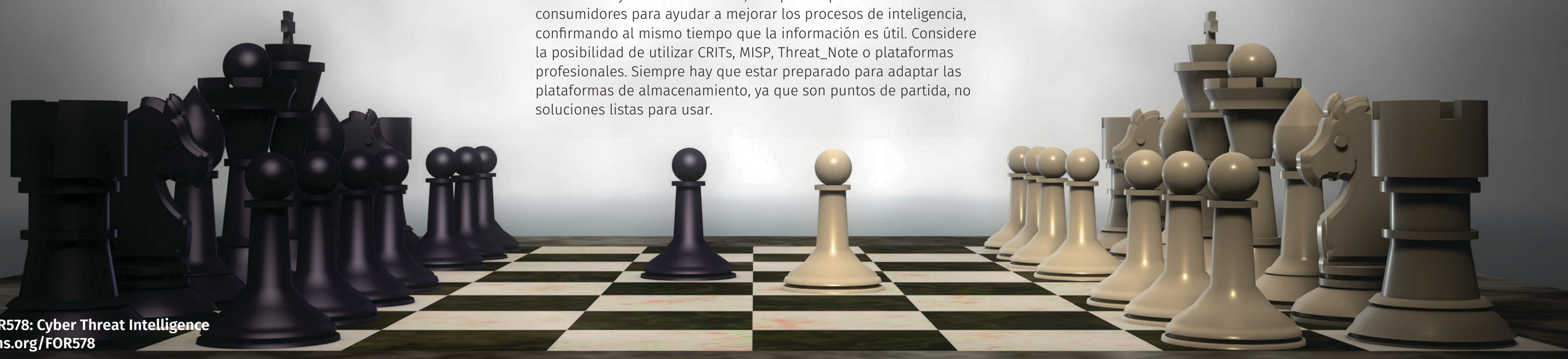
Enriquecer la información
Utilizar información de código abierto con herramientas como Google, ThreatMiner.org, o herramientas profesionales para determinar si otros han visto los indicadores técnicos o TTPs del adversario antes. Intentar evitar la duplicación de esfuerzos: utilizar la información existente.

Validar la información
La información de código abierto existe en abundancia y necesita ser validada. No toda la información es correcta o relevante para su organización. Tomar simplemente una fuente de datos o de amenazas y utilizarla a ciegas generará falsos positivos y sobrecargará a los analistas. Disponga de procesos para retirar los indicadores y la información que ya no sean útiles. El enfoque de los acumuladores de indicadores siempre fallará con el tiempo.

Almacenar la información
Almacene la información utilizando un formato común y asegúrese de que los analistas también puedan añadir notas e identificar las relaciones entre los indicadores técnicos. Asegúrese de que el personal de seguridad interno pueda acceder rápidamente a la información y utilizarla. Además, busque la opinión de los consumidores para ayudar a mejorar los procesos de inteligencia, confirmando al mismo tiempo que la información es útil. Considere la posibilidad de utilizar CRITs, MISP, Threat_Note o plataformas profesionales. Siempre hay que estar preparado para adaptar las plataformas de almacenamiento, ya que son puntos de partida, no soluciones listas para usar.

Compartir la información
Traduzca el formato común interno de su organización a formatos compartibles como STIX/TAXII para ponerlo a disposición de sus compañeros u organizaciones gubernamentales. Asegúrese de que en una relación de intercambio obtiene la información de vuelta para poder utilizarla para validar o mejorar sus conocimientos.

Producir la información
Cuando se requiera una evaluación de inteligencia, analice las fuentes de información que compiten entre sí para hacer evaluaciones sobre la amenaza y su impacto en su organización. Utilice modelos como el Análisis de Hipótesis Compitiendo para ayudar a vencer los sesgos de los analistas. Utilice un lenguaje como el de alta, media y baja confidencia para sus evaluaciones porque la inteligencia es siempre una evaluación y no una conclusión definitiva. La inteligencia producida suele entregarse en forma de informe o briefing.



*FOR578: Cyber Threat Intelligence
sans.org/FOR578