Hacerle frente a la complejidad

Cómo lidiar con incidentes cibernéticos complejos causados por amenazas modernas y sofisticadas

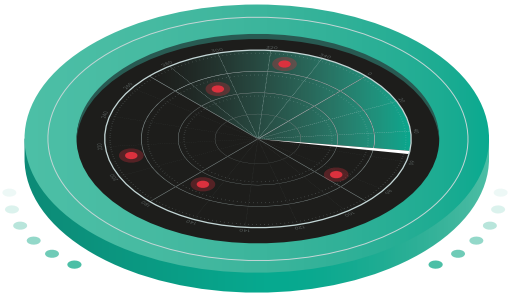
kaspersky BRING ON THE FUTURE

Puede que no siempre sea posible detener una amenaza antes de que penetre el perímetro de seguridad, pero está absolutamente en nuestro poder evitar que el ataque se propague y limitar o excluir el daño potencial resultante. Y, cuando se trata de ataques complejos o dirigidos, la velocidad de resolución de incidentes es crítica.

No obstante, los incidentes complejos presentan desafíos muy específicos porque suelen involucrar muchos aspectos de la infraestructura de la organización que atacan. En cierto sentido, esto presenta el dilema: ¿cómo sabemos por dónde empezar cuando aparentemente todo es lo más importante?

En este documento, veremos los cinco obstáculos clave para una resolución exitosa de incidentes complejos. Pero primero, comencemos por cuestionar la idea de complejidad en sí misma y lo que significa para los profesionales de la ciberseguridad.

¿Qué es exactamente un incidente complejo?



Un incidente complejo podría definirse más claramente en oposición a un incidente simple. Sería negligente no mencionar que la pandemia mundial de Covid-19 es el epítome de un incidente complejo: involucra a múltiples sistemas: países, organizaciones (gubernamentales y comerciales), comunidades, escuelas, sectores, familias y seres humanos individuales. Por no hablar del hecho de que el virus actúa como un incidente complejo dentro de los cuerpos de las personas que se enferman gravemente con él; sus efectos se extienden más allá del sistema respiratorio para incluir los sistemas cardiovascular, renal, dermatológico, neurológico, inmunológico e incluso psiquiátrico.

Ciberespacio complejo, panorama de amenazas complejo, incidentes cibernéticos complejos: ¿una cadena natural?

Vale la pena señalar que la creciente complejidad de los incidentes cibernéticos está directamente relacionada con la creciente complejidad de los sistemas de TI corporativos en crecimiento y, de hecho, con el propio ciberespacio. De hecho, según la ENISA (Agencia Europea de Seguridad de las Redes y de la Información), en el *informe de Tendencias emergentes de enero de 2019 a abril de 2020 sobre el panorama de amenazas,* "La interconexión de varios sistemas y redes permite que los incidentes cibernéticos se propaguen rápida y ampliamente, lo que hace que los riesgos cibernéticos sean más difíciles de evaluar y mitigar". En otras palabras, cuanto más compleja es la infraestructura de TI corporativa, mayor es el riesgo de ciberataques complejos, lo que hace que el desafío de los incidentes complejos sea aún más difícil para las grandes organizaciones empresariales intrínsecamente complejas.

Sin embargo, la correlación natural entre los entornos complejos y los incidentes complejos se extiende más allá del sistema empresarial complejo específico. El ciberespacio en sí está definido por la ISO/IEC 27032:2012 como un "entorno complejo resultante de la interacción de personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectadas a ella, que no existe en ninguna forma física". En otras palabras, lo que enfrentamos son, de hecho, tres capas de complejidad: el ciberespacio, el entorno de TI empresarial y los incidentes cibernéticos. Para complicar aún más este panorama, existe el hecho de que estas tres capas

están interconectadas y son interdependientes, cada una de las cuales se vuelve cada vez más compleja para lograr sus objetivos:

Ciberespacio: mayor dependencia de dispositivos, sistemas y procesos interconectados para respaldar la vida diaria de los negocios y el ocio, lo que lleva a una creciente complejidad del entorno

El entorno de TI empresarial: experimentar una superficie de ataque en expansión como resultado de una expansión en la cantidad de dispositivos, sistemas y procesos interconectados (incluida la cadena de suministro) y, simultáneamente, un fuerte crecimiento en la complejidad de los incidentes cibernéticos que enfrenta, así como las configuraciones de ciberseguridad necesarias para rechazarlos

El panorama de amenazas y sus actores: por un lado, responder a la creciente complejidad tanto en el ciberespacio como en el entorno empresarial, y por el otro, aprovechar específicamente esa complejidad para lanzar ataques avanzados altamente sofisticados (que implican el movimiento lateral de un orden que no es posible en los sistemas objetivos más simples).

La amarga verdad es que, de estos tres, son los actores de amenazas los que han encontrado más rápidamente formas de reducir los obstáculos de la complejidad, al recurrir al Malware-as-a-Service, entre otras cosas:

> "Hoy en día, los obstáculos de entrada para los posibles ciberdelincuentes están cayendo rápidamente porque los atacantes tienen una variedad de capacidades (técnicas) y recursos sustanciales a su disposición, ya que el malware y el malware-as-a-service se han vuelto más fácil y económicamente disponibles a través de varios medios y fuentes (como la Dark Web y la Deep Web). Como resultado, una variedad de técnicas y herramientas avanzadas (por ejemplo, técnicas de ingeniería social y programas de ataques de día cero) están disponibles y pueden ser utilizadas por los ciberdelincuentes para iniciar ataques dirigidos avanzados".
>
> Papastergiou, S., Mouratidis, H. y Kalogeraki, EM. **Manejo de amenazas persistentes avanzadas e incidentes complejos en infraestructuras TIC de salud, transporte y energía.** Sistemas en evolución (2020).

La buena noticia es que hay formas en que las empresas pueden reducir de manera significativa, eficaz y decisiva los obstáculos de la complejidad, y lo investigaremos más en el documento. Antes de hacerlo, veremos los cinco obstáculos clave para una resolución exitosa de incidentes complejos.

Los cinco obstáculos para resolver los incidentes complejos con éxito

Sabemos que está totalmente en nuestro poder detener el progreso y limitar el daño causado por amenazas complejas, incluso una vez que han penetrado el perímetro corporativo. Para empezar, vale la pena recordar que la mayoría de las Tácticas de acceso inicial dentro del marco empresarial MITRE ATT&CK siguen siendo relativamente tradicionales.

Ese spear phishing debería seguir siendo una táctica principal de acceso inicial, incluso para las APT (amenazas persistentes avanzadas), en el contexto del caos pandémico global, debería darnos una pausa para pensar. En primer lugar, debemos considerar cuántos ataques podrían evitarse automatizando las tareas rutinarias de ciberseguridad que bloquean el acceso inicial. Pero también, destaca el hecho de que la penetración de ataques (con excepciones como los ataques de día cero) no es lo que hace que un incidente sea *complejo*.

La complejidad comienza con tácticas como el movimiento lateral, el establecimiento de puertas traseras y con varios modos de entrega de carga útil y sigilo. Pero, ¿qué impide que los equipos de seguridad de TI puedan ejercer su poder y experiencia para evitar que un incidente se convierta en un incidente complejo? Y, una vez que el incidente se ha vuelto complejo, ¿por qué, con frecuencia, es tan difícil de mitigar y resolver con éxito?

Obstáculo n.° 1: la complejidad de los sistemas de ciberseguridad en sí mismos

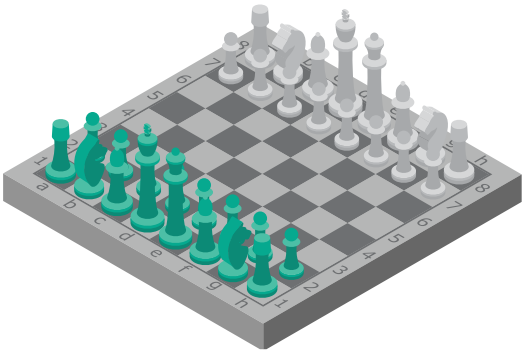
Para una persona externa, una configuración de ciberseguridad empresarial promedio es tan desconcertante como la cabina de un avión de combate furtivo. Por supuesto, no es que exista una empresa promedio o una configuración de ciberseguridad promedio. Múltiples herramientas, que se ocupan de tareas de seguridad específicas altamente especializadas, una gama de consolas de control, y montones y montones de alertas constantes. Ya hemos visto cómo surgió esta complejidad: es una evolución obvia en respuesta a la creciente complejidad de la infraestructura de seguridad de TI empresarial, por un lado, y el panorama de amenazas, por el otro.

Por lo tanto, es una tragedia terrible e irónica que la complejidad de la configuración de la ciberseguridad se convierta con demasiada frecuencia en un obstáculo real para la resolución exitosa de los incidentes muy complejos que deberían abordar. Esta complejidad frustra la mitigación y resolución exitosas de las siguientes maneras:

- Los equipos se están ahogando en herramientas, invierten tiempo valioso actuando como "intérpretes" entre soluciones dispares. Las pilas de tecnología de ciberseguridad (y las pilas de tecnología en general) con frecuencia se han convertido en Torres de Babel virtuales, con un funcionamiento fluido y sin problemas que se ve obstaculizado por el hecho de que diferentes herramientas hablan diferentes "idiomas".

- Cuando los datos de los incidentes cibernéticos se recopilan en pequeñas muestras de una variedad de sensores de datos no integrados en posibles puntos de penetración, los equipos, con frecuencia, pierden el panorama general y, por lo tanto, no pueden darse cuenta de que se está produciendo un incidente complejo antes de que aparezcan señales de entrada obvias. En otras palabras, el incidente no se comprende completamente y, en última instancia, esto puede provocar daños.

- La necesidad de un procesamiento manual constante que proviene de abordar las alertas de procesos de respuesta a incidentes no sistemáticos y no consistentes consume una energía valiosa, lo que hace que se pierdan alertas cruciales y se preste demasiada atención a los falsos positivos.



Obstáculo n.° 2: inteligencia de amenazas deficiente o irrelevante

Threat Intelligence debe pasar una prueba de fuego de tres partes si va a comenzar a cumplir su promesa de brindar una visibilidad profunda de las amenazas cibernéticas dirigidas a su organización:

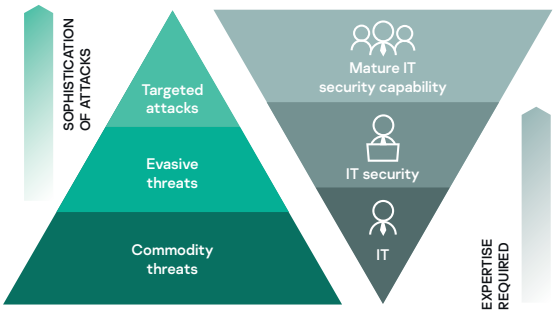
- ¿Es integral?
- ¿Es exacta?
- ¿Es actual?

Sin embargo, pasar esta prueba es solo el primer paso. El obstáculo que enfrentan muchas organizaciones empresariales hoy en día es que, si bien tienen acceso a la inteligencia de amenazas que es integral, exacta y actual, les falta una pieza crucial: la pertinencia. Cualquier profesional de seguridad de TI familiarizado con la variedad de fuentes de inteligencia de amenazas disponibles en la actualidad estará más que consciente de esto.

La pertinencia es quizás una forma de decir que la calidad es más importante que la cantidad, pero esto es solo parcialmente cierto. La inteligencia de amenazas debe provenir de una fuente que ofrezca ambas, y debe ser canalizada o procesada a través de un sistema holístico de ciberseguridad que en sí mismo dirige y crea pertinencia para esa organización específica, para ese momento específico y para ese entorno específico. La pertinencia no es un esfuerzo único, es un proceso continuo, que implica un ciclo de retroalimentación entre elementos integrados dentro de una configuración de ciberseguridad.

La inteligencia de amenazas contextualmente pertinente, integrada con otros mecanismos de detección y búsqueda de amenazas, encuentra significado y contexto automáticamente, lo que ahorra un tiempo valioso al brindar claridad desde el principio.

Obstáculo n.° 3: una tendencia histórica a centrarse demasiado en las amenazas básicas



Las amenazas básicas aún representan un porcentaje muy alto de todas las amenazas a las que se enfrentará cualquier organización. En ese sentido, no es de extrañar que la tendencia a centrarse demasiado en tales amenazas siga siendo endémica, incluso dentro de las grandes organizaciones desarrolladas en seguridad de TI.

Sin embargo, el costo de los incidentes asociados con estas amenazas es insignificante en comparación con el daño potencial causado por el porcentaje restante, que incluye ataques complejos devastadores como ataques dirigidos y APT.

La otra razón por la que algunos equipos de seguridad de TI todavía se centran demasiado en amenazas simples (a expensas de incidentes complejos) es más obvia. Es humano querer centrarse en un problema sencillo que sea fácil de resolver. Además, una de las razones por las que las amenazas simples son tan sencillas es que incluso la configuración de ciberseguridad más básica y mal estructurada podría hacer un trabajo bastante bueno al detectarlas automáticamente y, al mismo tiempo, no ofrecer suficiente automatización cuando se trata de resolverlas. Por lo tanto, las amenazas simples pueden ocupar demasiado espacio, exigiendo una atención que no deberían necesitar, a expensas de centrarse en incidentes complejos que son mucho más letales.

Obstáculo n.° 4: la crisis del talento en ciberseguridad

Un vistazo rápido al mapa de calor de Cyberseek, una iniciativa empezada por la Iniciativa Nacional para la Educación en Ciberseguridad de EE. UU. (NICE), revela el alcance de la crisis de talento en ciberseguridad. Si bien Cyberseek solo se ocupa de las brechas en el contexto estadounidense, sirve como un vistazo muy útil (y aleccionador) de una escasez global.

Al 30 de enero de 2021, hay 521 617 vacantes de trabajo para profesionales de ciberseguridad en los EE. UU., frente a una fuerza laboral total de ciberseguridad empleada de 941 904. Esa es una relación de oferta-demanda nacional promedio de 1,8.

Si bien esta es una buena noticia para los profesionales de la ciberseguridad en términos de seguridad laboral (y ahora sería un muy buen momento para alentar a sus hijos en edad de escuela secundaria a seguir una carrera similar), no es una buena noticia cuando se trata de la calidad y eficacia de la vida laboral.

La mayoría de los analistas concluyen que la crisis del talento en ciberseguridad es debido a fallas en la educación y la formación, pero esta información no ayudará a las organizaciones sobre el terreno. Hasta que estas fallas se aborden y corrijan (en parte, mediante iniciativas como Cyberseek), las organizaciones deben lidiar con este obstáculo maximizando el poder de sus equipos de seguridad de TI existentes, proporcionando las herramientas, el soporte, la orientación y el respaldo que necesitan para ser capaces de resolver con éxito incidentes complejos.

Obstáculo n.° 5: el problema de la velocidad

Este último obstáculo de la resolución exitosa de incidentes complejos vincula a los cuatro anteriores. Frente a desafíos complejos como los ataques de día cero, los ataques que no son de malware (non-malware attacks), los ataques sin archivos (fileless attacks) y los ataques living-off-the-land, la velocidad es todo.

Un incidente complejo no necesariamente comienza de una manera compleja, como hemos visto con la prevalencia continua del spear phishing como táctica para obtener acceso inicial. Las devastadoras (y costosas) consecuencias de demasiados incidentes complejos podrían haberse evitado si el equipo en cuestión hubiera podido responder con la suficiente rapidez.

Por supuesto, esto no sugiere que haya un punto en la evolución de un incidente complejo en el que se vuelva "demasiado tarde en el día", solo que, a medida que pasa el tiempo, también lo hace el grado de complejidad. Puede parecer demasiado simple afirmar que, cuando se trata de incidentes complejos, la velocidad es todo. Pero siempre que califiquemos lo que queremos decir con velocidad, es absolutamente cierto.

La velocidad no significa combatir incendios constantemente, o ser un pistolero y responder rápidamente a cualquier alerta que requiera nuestra atención. Significa velocidad para ejecutar con precisión todos los procesos esenciales de detección y respuesta, de manera decisiva y coherente. Esto incluye la búsqueda proactiva de amenazas, la causa raíz y el análisis retrospectivo, la remediación, la mitigación y la respuesta a incidentes, entre otros.

¿Qué les depara el futuro a las organizaciones que enfrentan incidentes complejos?

El comienzo del 2021 parece ser el peor momento en la memoria reciente para tratar de responder cualquier pregunta sobre el futuro. Después de todo, la pandemia es, en sí misma, un incidente complejo y uno para el que nuestras herramientas, sistemas y profesionales no estaban equipados. Pero todavía hay algunas cosas que sabemos con certeza. Por ejemplo, sabemos que las APT y otros ataques complejos seguirán evolucionando y sabemos que es probable que el teletrabajo siga creciendo, incluso después de que se haya resuelto la pandemia. Nuestro Equipo Global de Investigación y Análisis (GReAT) de investigadores de ciberseguridad líderes en el mundo ha hecho las siguientes predicciones para los APT en 2021:

- Los ataques de bandera falsa (como el Olympic Destroyer) alcanzarán un nuevo nivel
- El ransomware será cada vez más objetivo
- Surgirán nuevos vectores de pago y banca en línea
- Veremos más ataques a la infraestructura y ataques contra objetivos que no son PC
- Aumentarán los ataques en las regiones que se encuentran a lo largo de las rutas comerciales entre Asia y Europa
- Aumentará la sofisticación de los métodos de ataque
- Habrá un nuevo cambio de enfoque hacia los ataques móviles
- El abuso de la información personal: desde falsificaciones profundas hasta filtraciones de ADN

La perspectiva de incidentes tan complejos sobre las cabezas de los profesionales de seguridad de TI no tiene por qué ser una señal de fatalidad.

Volviendo al informe Temas de investigación de ENISA de enero de 2019 a abril de 2020, encontramos un núcleo de esperanza y un indicio de dónde enfocar nuestros esfuerzos mientras buscamos resolver con éxito incidentes complejos: la dimensión humana:

"La ciberseguridad todavía se considera la práctica de proteger redes, sistemas de información y datos (NIS). Esta definición debe ampliarse más allá de las cuestiones técnicas para incluir preocupaciones sociales, de comportamiento y económicas, y las diferentes funciones desempeñadas por las partes involucradas. Esto debería constituir una prioridad en los futuros debates sobre investigación e innovación en ciberseguridad. Una mejor comprensión de la dimensión humana es clave en la definición de cualquier estrategia de ciberseguridad para que las decisiones de seguridad se tomen para satisfacer sus necesidades, habilidades y expectativas".

Para nuestros propósitos, las "partes" mencionadas anteriormente se refieren a los profesionales de seguridad de TI, así como a los líderes empresariales ante los cuales son responsables. Es posible que no podamos reclutar todo el talento en ciberseguridad que necesitamos, por lo que la pregunta es: ¿cómo nutrimos lo que ya tenemos?

Expert tech in expert hands

El primer paso es comprender que no se espera que incluso las organizaciones con mayor grado de desarrollo en TI aborden amenazas complejas y ataques de APT. Es un problema global, que cambia constantemente entre regiones y sectores, y demasiados equipos se ven obstaculizados en sus esfuerzos por resolver con éxito incidentes complejos debido a los obstáculos que hemos analizado en este documento.

Es por eso que alentamos a todos nuestros clientes empresariales a que se aseguren de abordar con cuidado lo que consideramos los tres pilares de cualquier estrategia exitosa de incidentes complejos. Es decir, los equipos de seguridad deben ser los siguientes:

- **Equipados:**
  la ciberseguridad es un área de experiencia en la que hasta los trabajadores más hábiles pueden culpar válidamente a sus herramientas. La protección contra ataques multivectoriales y otros incidentes complejos requiere una plataforma unificada consolidada que brinde visibilidad total, al eliminar silos obstructivos y prevenir la "fatiga de alerta" y otras tareas rutinarias dentro del proceso de respuesta a incidentes.

- **Informados:**
  la experiencia avanzada existente de las organizaciones que han desarrollado TI nunca debe darse por sentada. Después de todo, el horizonte de la ciberdelincuencia cambia y se expande constantemente. La educación continua y la poderosa inteligencia de amenazas de un socio confiable de ciberseguridad son absolutamente cruciales.

- **Reforzados:**
  si se descubre un incidente complejo o APT, incluso los analistas de seguridad de TI más avanzados deben tener acceso a soporte externo para información de terceros, evaluación de seguridad, búsqueda de amenazas administrada y respuesta a incidentes. Si bien los incidentes complejos resultantes de las APT suelen ser muy específicos, rara vez se dirigen a una sola víctima. La experiencia externa puede arrojar una luz global multisectorial sobre los posibles caminos de una APT y brindar consejos prácticos sobre la forma más decisiva de eliminarla del sistema.

Revolucione la forma en que sus expertos en seguridad de TI asumen el control de los incidentes complejos

Una revolución en la forma en que sus expertos de seguridad de TI controlan los incidentes complejos con Kaspersky Expert Security: un concepto de defensa integral que le ofrece a su equipo herramientas, información y supervisión para combatir los ciberataques dirigidos más sofisticados. Es una plataforma de Extended Detection and Response (XDR), con una combinación perfecta de tecnología de punta, inteligencia de amenazas de élite, experiencia humana, capacitación y servicios, respaldada por las mentes más brillantes en ciberseguridad. Nuestro enfoque holístico fomenta el potencial en ciberseguridad de su equipo con detección de amenazas en varias dimensiones, investigaciones efectivas y búsqueda proactiva para dar una respuesta rápida y centralizada a toda la gama de amenazas modernas

Obtenga más información en https://go.kaspersky.com/expert-sp-mx.html

Noticias sobre ciberamenazas: www.securelist.com
Noticias sobre seguridad de TI: www.kaspersky.com/blog Threat Intelligence Portal: opentip.kaspersky.com
Introducción a las tecnologías: www.kaspersky.com/TechnoWiki
Premios y reconocimientos: media.kaspersky.com/en/awards
Herramienta de cartera interactiva: kaspersky.com/int_portfolio

latam.kaspersky.com

kaspersky BRING ON THE FUTURE