FORTINET

Las 5 capacidades más críticas de una plataforma de detección y respuesta

Índice

Resumen ejecutivo

La sofisticación de los ciberdelincuentes actuales y de sus campañas representa un reto crucial y una oportunidad para los equipos de operaciones de seguridad. Aunque una ciberdefensa eficaz requiere la capacidad de supervisar numerosas vías de ataque y diversos indicios de actividad maliciosa, lo que puede resultar complicado y llevar mucho tiempo, incluso para los profesionales de la seguridad más expertos, la implementación de las tecnologías adecuadas desempeña un papel fundamental a la hora de ayudar a su equipo a tener visibilidad del panorama general y responder con eficacia antes de que se produzca cualquier daño. Al evaluar las plataformas de detección y respuesta, debe tener en cuenta varias cuestiones críticas antes de adquirirlas.

Introducción

Al realizar inversiones en ciberseguridad, la mayoría de las organizaciones se han centrado históricamente en la prevención. Pero como se afirma en una reseña de investigación de Gartner: "Dada la complejidad de la detección de amenazas, la era de la adquisición del mejor producto de prevención de amenazas de su clase ha quedado prácticamente atrás. Lo que se requiere es una pila de detección capaz de recopilar suficiente telemetría mediante diversos métodos, incluidas las API, y analizarla correctamente para encontrar la aguja del ataque en el pajar de los datos".[1]

Dicho esto, los líderes empresariales reconocen cada vez más que la complejidad de la infraestructura de seguridad y la gestión de alertas suponen un reto constante. La buena noticia es que el 75 % de las organizaciones buscan la consolidación de proveedores de ciberseguridad, prefiriendo las plataformas a una serie de productos específicos puntuales.[2]

Sin embargo, no todas las plataformas proporcionan el nivel de cobertura adecuado. La superficie de ataque

y la cobertura de la fase de campaña, la tecnología de detección y el grado de integración pueden variar enormemente. Por último, aunque la mayor atención recae en la tecnología, las personas y los procesos siguen siendo esenciales para una defensa eficaz. Como reconoce acertadamente Gartner, "la pila que mejor se adapte a sus necesidades es la que cumpla sus objetivos de supervisión de la forma más eficaz y rentable".[3]

Cinco consideraciones para las inversiones en detección y respuesta a amenazas

Supongamos que está considerando adoptar una estrategia de plataforma para la detección y respuesta o que necesita ajustar su enfoque de la gestión de riesgos. En ese caso, hay cinco preguntas críticas que debe tener en cuenta antes de realizar nuevas inversiones.

1. ¿Qué puede inspeccionar?

Hay muchas formas por las que intentan acceder a su organización los actores de las amenazas (correo electrónico, descargas de Internet, aplicaciones y activos dirigidos al exterior de la empresa, servicios empresariales, etc.), muchos destinos dentro de ella (dispositivos de usuario final, servidores de aplicaciones, sistemas IoT y TO, etc.), por no mencionar objetivos adicionales fuera de la organización (software como servicio e infraestructura de nube pública, por ejemplo).

Como señalaba un informe reciente de Gartner, "Cuantos más POV [puntos de vista] tenga una pila, mayor será la cantidad y el tipo de amenaza que pueda detectar, o la calidad de la alerta que produzca.
Como mínimo, la pila debe tener un POV estratégico para el tipo de amenazas que más interesan".[4] No se puede detectar lo que no se inspecciona, así que asegúrese de tener todas las bases (o vectores de ataque e infraestructura objetivo, en este caso) cubiertas.

2. ¿Están cubiertas todas las etapas?

En la actualidad, muchos ataques progresan a través de múltiples etapas para eludir los controles orientados a la prevención, permaneciendo ocultos durante largos períodos y maximizando su impacto y el retorno de la inversión.
El marco MITRE ATT&CK y Cyber Kill Chain de Lockheed Martin refleja las etapas comunes y las tácticas utilizadas habitualmente, que abarcan desde la preparación previa al ataque, a la entrega del ataque y la actividad después de la infección y la intrusión. Afortunadamente, cuantas más etapas ejecute el ciberatacante antes de alcanzar su objetivo final, más posibilidades tendrá la organización de detectar e interrumpir el ataque antes de que tenga éxito.

Gartner menciona: "En general, lo mejor es encontrar una pila de detección que funcione en la fase de ataque y que produzca las alertas de mayor calidad para sus objetivos de supervisión".[5] Para ello, una plataforma de operaciones de seguridad debe cubrir todas las vías de ataque y expansión y todas las fases de Cyber Kill Chain – Cadena de Muerte. Estas incluyen el reconocimiento, el emplazamiento de armas, la entrega, la explotación, la instalación, la comunicación de mando y control, y las acciones posteriores sobre el objetivo.

3. ¿Qué tecnologías se utilizan para detectar?

Por supuesto, el hecho de inspeccionar la actividad a través de los vectores de ataque y a lo largo de Cyber Kill Chain no significa automáticamente que se puedan detectar los ataques, ya que cada vez se diseñan más para que parezcan o incluso utilicen servicios o acciones legítimas. De acuerdo con Gartner, "algunos métodos son muy sencillos hasta el punto de ser deterministas, otros dependen de un amplio conocimiento de las amenazas, mientras que otros pueden requerir un complejo análisis de datos. No existe el mejor método, pero algunos son más eficaces que otros para ciertas amenazas".[6]

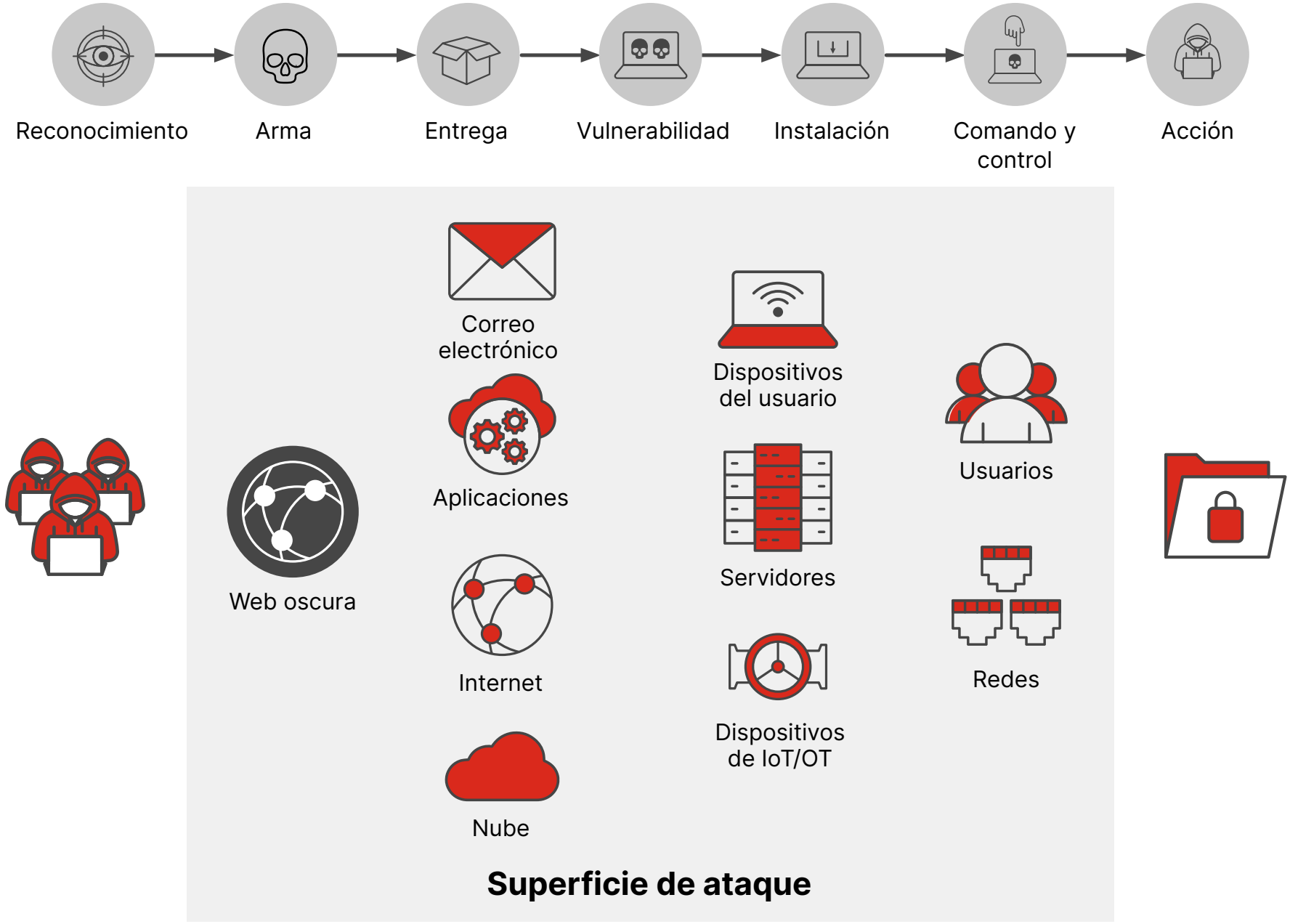

Figura 1: Superficie de ataque requerida y cobertura de Cyber Kill Chain

La inteligencia de amenazas y los Indicadores de Compromiso son muy precisos, pero poco predictivos. Las reglas y la heurística son más predictivas, pero también suelen producir falsos positivos. Los modelos estáticos de aprendizaje automático o profundo son mucho más predictivos, pero suelen ofrecer una probabilidad en la que inicialmente puede ser difícil confiar y difícil de mantener a lo largo del tiempo. El análisis del comportamiento ofrece algunos de los mejores indicadores, pero sólo si estos procesos pueden identificar con precisión tácticas, técnicas o procedimientos conocidos. Identificar actividades anómalas que pueden ser legítimas o no autorizadas lleva mucho tiempo a los equipos de seguridad. Considere la combinación correcta de tecnologías de detección adecuadas para su organización y equipo.

4. ¿Quién (o qué) se espera que responda?

La detección es solo el primer paso. La validación y contención de incidentes son necesarias para limitar el riesgo, y se requiere una investigación exhaustiva y un proceso de reparación para volver a las operaciones seguras.

Tradicionalmente, esta función la han manejado manualmente profesionales expertos en seguridad. Y, no nos equivoquemos, estos profesionales siguen siendo una parte esencial del proceso. Sin embargo, según Gartner, "los SOP [procedimientos operativos estándar] de respuesta son buenos para establecer los objetivos, procesos y actividades. Sin embargo, no podrán cubrir el nivel prescriptivo de lo que hay que hacer exactamente con cada objeto implicado en el ataque; basándose en el tipo específico de ataque que acaba de ocurrir".[7]

Las organizaciones deben decidir hasta qué punto confiar en el conocimiento institucional del equipo de seguridad frente a la construcción de ese conocimiento en procesos documentados que se puedan orquestar y automatizar mediante una plataforma. Una estrategia de operaciones de seguridad sólida se suele basar en ambos elementos, y las organizaciones deben determinar el equilibrio adecuado.

5. ¿Puede hacerlo funcionar su equipo?

Por supuesto, ni siquiera el sistema más sofisticado, orquestado y automatizado funcionará por sí solo. Como señala Gartner: "El último reto, y a menudo el más difícil, es el de las operaciones... Gran parte del trabajo no está relacionado con el daño y reparación, sino que adopta la forma de pensamiento crítico e investigación a nivel de expertos".[8]

Determine si la plataforma de detección y respuesta que selecciona puede ser ejecutada por su equipo o si necesita recurrir a expertos externos. En cuanto a la externalización, hay muchas opciones. La subcontratación se puede hacer ad hoc o de forma continuada, y puede decidir si necesita apoyo para todas las actividades o cobertura especializada para determinadas tareas. En cualquier caso, la externalización no exime a la organización del ciberriesgo. Simplemente utiliza las habilidades y el personal de otros proveedores, por lo que, si decide subcontratar, asegúrese de que está seleccionando una plataforma que puede recibir el soporte de un socio de confianza con la experiencia necesaria.

Resumen

La sofisticación de los actores de las amenazas actuales y la complejidad de sus ataques suponen tanto un reto como una oportunidad. Asegurarse de que dispone de un sistema de detección eficaz que cubra toda la superficie de ataque y Cyber Kill Chain con tecnología altamente fiable que permita una respuesta eficaz puede reducir en gran medida su riesgo cibernético.

[1] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, 19 de diciembre de 2022.

[2] Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022, Gartner, 13 de septiembre de 2022.

[3] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, 19 de diciembre de 2022.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

FORTINET

www.fortinet.com

marzo 25, 2024 12:38 p. m.

2504903-0-0-ES