COHESITY

DOCUMENTO TÉCNICO

Cómo formular una estrategia de respuesta “en tiempos de guerra” ante ciberataques destructivos

Recupérese del ransomware y otras amenazas cibernéticas de manera segura y rápida con Cohesity

ÍNDICE

Resumen ejecutivo

Los ciberataques destructivos, como el ransomware y los ataques wiper, requieren un enfoque diferente de las operaciones de TI, en comparación con los escenarios tradicionales de continuidad del negocio y recuperación ante desastres. Los equipos de operaciones de ciberseguridad enfrentan varios desafíos para garantizar que se lleven a cabo las investigaciones y las remediaciones adecuadas de las amenazas. No es suficiente simplemente restaurar la entrega de sus productos y servicios lo más rápido posible. Las organizaciones también deben asegurarse de que la recuperación se lleve a cabo de manera segura para evitar un mayor tiempo de inactividad debido a una reinfección o un nuevo ataque.

Este documento técnico documenta las mejores prácticas para lidiar con los ciberataques destructivos y destaca cómo Cohesity puede ayudar a su organización a lograr esos resultados operativos.

Análisis de la situación: Por qué su organización opera de manera diferente en “tiempos de paz” y en “tiempos de guerra”

“Tiempos de paz” son las operaciones diarias normales de su organización. Las alertas de las herramientas de seguridad generalmente llegan a las consolas de su Centro de Operaciones de Seguridad (SOC) o proveedor de servicios de seguridad administrados (MSSP). La prioridad de estas alertas se clasifica y se descartan los falsos positivos, mientras se recopila evidencia adicional para identificar signos de intrusión dentro de la infraestructura de su organización. Cuando los analistas de SOC están seguros de que un adversario está atacando a la organización, declaran un incidente y siguen adelante con su investigación. En esta etapa, la organización está en modo de “tiempos de guerra”.

Durante la investigación, si los analistas descubren que la confidencialidad, la integridad o la disponibilidad de los sistemas y datos de la organización se han visto comprometidas, declaran una violación y continúan con su proceso de respuesta ante incidentes.

El tiempo que el adversario pasó dentro de la organización antes de su descubrimiento se define como su tiempo de permanencia. El adversario puede ser descubierto mediante las alertas de las herramientas de seguridad. Pero con demasiada frecuencia, las organizaciones solo se dan cuenta de un ataque cuando los sistemas dejan de estar disponibles. El tiempo de permanencia puede variar significativamente, desde tan solo cuatro a cinco días en ataques que utilizan ransomware como servicio (RaaS), hasta cientos de días en ataques de ransomware impulsados por humanos, o incluso años en el caso de actores estado nación.

Algunos ejemplos de cómo la confidencialidad, la integridad o la disponibilidad se ven comprometidas incluyen:

- **Confidencialidad**: los datos de la organización se han divulgado a partes no autorizadas. Esto incluye la exfiltración de datos con fines criminales por parte de bandas de ransomware o para espionaje por parte de actores estado nación antes de lanzar un ataque wiper.
- **Integridad**: durante las múltiples etapas de un ciberataque destructivo, los adversarios cambian los archivos de configuración, los registros, los sistemas de gestión de identidad y potencialmente incluso el firmware para mantener la persistencia dentro de las organizaciones víctimas. Todos estos cambios afectan la integridad de los sistemas.
- **Disponibilidad**: un ciberataque destructivo tiene como objetivo hacer que la infraestructura de TI de la organización, que es necesaria para entregar productos y servicios a los clientes, deje de estar disponible. Lo hacen cifrando datos o sistemas, como se ve en los ataques de ransomware, o eliminándolos, como en los ataques wiper.

Es importante comprender que no todos los incidentes se convierten en violaciones, y un SOC detecta y responde continuamente a los incidentes en sus primeras etapas para evitar que se conviertan en violaciones. Algunas violaciones están contenidas en ciertas áreas de la organización y se pueden gestionar utilizando manuales de estrategias de respuesta estándar ante incidentes.

Sin embargo, ciertos incidentes, especialmente los ataques de ransomware y wiper, pueden tener un amplio impacto. Son capaces de desactivar los sistemas necesarios para entregar productos y servicios a los clientes, así como los sistemas internos de TI esenciales para gestionar el incidente. Estos pueden incluir sistemas para el acceso físico a las instalaciones, la comunicación con los reguladores y las partes afectadas o los sujetos de datos, o la coordinación con las aseguradoras, las fuerzas del orden y la prensa. En tales casos, la organización puede declarar una **crisis cibernética** y llevar a cabo un flujo de trabajo diferente para garantizar que puedan gestionar el incidente.

Una vez que los equipos de seguridad y de TI hayan tratado el incidente, la violación o la crisis; hayan restaurado los sistemas a un estado de confianza; y hayan mitigado las amenazas de recurrencia, la organización puede volver a las operaciones de "tiempos de paz".

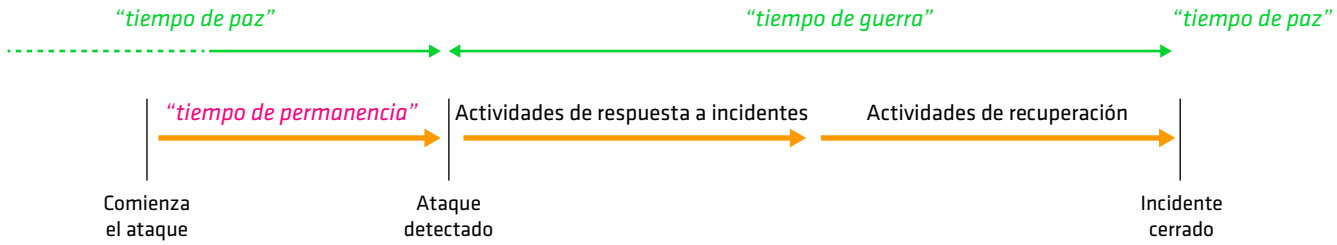

Figura 1. Etapas de "tiempos de guerra" y de "tiempos de paz" en un ciberataque destructivo.

Por qué los ciberataques destructivos difieren de la continuidad del negocio

Antes de la llegada de los ciberataques destructivos, se podían contar con una mano las causas fundamentales de las interrupciones del sistema de TI: inundaciones, incendios, fallas de equipos o software, configuraciones incorrectas o cortes de energía. Estos incidentes requerían una investigación mínima, y la respuesta estándar implicaba simplemente restaurar la última versión de la copia de seguridad.

Sin embargo, el ransomware es mucho más complejo. A diferencia de los virus o gusanos tradicionales, no es un único archivo binario que se pueda escanear. Los adversarios atacan mediante una cadena de 14 etapas, eligiendo entre cientos de técnicas para lograr sus objetivos en cada etapa. Están innovando constantemente, lo que hace que las configuraciones de control de seguridad de ayer sean ineficaces en la actualidad.

Agravando la amenaza, la situación geopolítica global actual ha aumentado el riesgo de ataques wiper por parte de actores estado nación. Con su capacidad operativa, financiamiento y motivación sin igual, estos actores maliciosos obligan a las organizaciones a desarrollar una ciberresiliencia superior a la que requieren las bandas criminales de ransomware.

Investigar y remediar el malware tradicional frente al ransomware

El malware tradicional, como virus y gusanos, se detecta escaneando los sistemas en busca de archivos binarios maliciosos. Una vez identificados, los equipos de seguridad pueden simplemente poner en cuarentena o eliminar el archivo binario malicioso. Por el contrario, los ataques de ransomware o wiper implican una cadena de eventos que permiten a los atacantes obtener acceso en pocos días luego del anuncio de una vulnerabilidad reciente. Estos ataques pueden aprovechar su infraestructura de TI para "vivir de los recursos" del propio sistema, utilizar cuentas autorizadas, alterar configuraciones para escalar privilegios o mantener la persistencia, preparar datos sensibles para su exfiltración y emplear secuencias de comandos y macros nativos de los sistemas operativos y aplicaciones, todo ello mientras evaden controles para dificultar su detección, respuesta y recuperación. A diferencia del malware tradicional, no hay un solo archivo binario que buscar y eliminar.

Recuperarse de manera segura de un ataque de ransomware o wiper requiere investigar cómo ocurrió el incidente. Las organizaciones deben remediar las amenazas y vulnerabilidades encontradas para evitar la reinfección y un mayor tiempo de inactividad. Esta es la esencia de todo marco de respuesta a incidentes de ciberseguridad basado en las mejores prácticas.

Las organizaciones deben remediar tres áreas críticas para garantizar que puedan resistir un ataque similar en el futuro y evitar la reinfección de los sistemas recuperados del ataque actual:

1. **Superficie de ataque**: los vectores de acceso inicial de ransomware más comunes, en orden de prevalencia, son: vulnerabilidades en la infraestructura orientada a internet, reutilización de credenciales de acceso legítimo y tácticas de ingeniería social, como phishing mediante correo electrónico. Debe comprender cómo se vio comprometido el "paciente cero", el punto de entrada inicial o la primera víctima identificada y, luego, remediar la amenaza en los sistemas recuperados. Esto puede implicar la implementación de parches en sistemas vulnerables, colocar los sistemas vulnerables detrás de alguna forma de protección como un firewall de aplicaciones web (WAF) y eliminar el correo electrónico de phishing que permitió el acceso inicial desde la bandeja de entrada de un usuario.
2. **Técnicas de evasión o brechas en los controles de seguridad**: la prevención o detección temprana de incidentes de seguridad, antes de que afecten la confidencialidad, la integridad o la disponibilidad, si bien incurre en un costo operativo, ayuda a evitar la pérdida de ingresos, daños a la reputación y potenciales, y costosas multas regulatorias y litigios de parte de los socios comerciales o los interesados afectados.

Las bandas de ransomware incorporan técnicas de evasión en sus plataformas de RaaS para los controles de seguridad más comunes, como la detección y respuesta de endpoints (EDR) y la detección y respuesta extendidas (XDR). También cuentan con la ventaja de ser los primeros en actuar antes de que se actualicen y difundan los informes de inteligencia sobre amenazas cibernéticas para incluir sus técnicas de ataque.

Antes de reanudar la producción, debe comprender por qué los controles de seguridad existentes no fueron capaces de detener o detectar el ataque antes de que este interrumpiera la prestación de los servicios de TI. Luego, puede asegurarse de que las herramientas de seguridad se hayan restablecido a un estado de confianza y que sus reglas se actualicen para prevenir o detectar ataques futuros de forma temprana.

3. **Mecanismos de persistencia**: en un ataque típico de ransomware o wiper, los atacantes a menudo dejan decenas de artefactos. Esto podría permitir a los atacantes establecer un punto de apoyo y seguir teniendo acceso al sistema si este se recupera sin comprender y eliminar completamente lo que se ha dejado atrás. Es común que las organizaciones pasen días recuperando sistemas solo para que se infecten en cuestión de minutos y que caigan de nuevo debido a un mecanismo de persistencia que se ha pasado por alto. Debido a la naturaleza multietapa de los ciberataques destructivos, generalmente se necesita una combinación de búsqueda de amenazas y análisis forense para crear un cronograma de ataque para identificar una lista completa de los artefactos que deben abordarse.

El concepto erróneo de los indicadores de compromiso (IOC)

El concepto de indicadores de compromiso (IOC) es clave para la inteligencia táctica de ciberamenazas. Es importante definir qué es un IOC antes de analizar las actividades en tiempos de guerra que las organizaciones deben llevar a cabo para lidiar con un ciberataque destructivo.

Los IOC proporcionan pistas que indican que un sistema ***puede*** haberse visto comprometido. Si bien sirven como punto de partida para buscar comportamientos adversarios, los IOC a menudo son solo señales, no el destino. Para recuperarse de manera segura, las organizaciones deben crear una imagen del ataque y analizarla para llevar a cabo las mitigaciones adecuadas descritas en la sección anterior. Por ejemplo, un archivo de configuración modificado que vuelve a ejecutar un código específico al reiniciarse es un IOC, al igual que un DLL malicioso que ha sido colocado en un directorio y que tiene el mismo nombre que uno legítimo. De manera similar, manipular la variable PATH para ejecutar este DLL malicioso antes que el legítimo también es un IOC. Si bien estos IOC nos dicen que algo está sucediendo, no pintan el panorama completo del ataque.

La búsqueda de IOC es fundamental para la respuesta a incidentes de ciberseguridad, pero las organizaciones deben aplicarlos en el contexto correcto. Depender únicamente de los IOC puede llevar a acciones inapropiadas. Además, la restauración prematura de las copias de seguridad sin una investigación más profunda permitirá la reinfección o causará otros problemas de disponibilidad.

Poner en cuarentena archivos a ciegas o restaurar versiones anteriores del archivo desde una instantánea de copia de seguridad que contenga el IOC no soluciona la causa fundamental. Todavía no sabe cómo entraron los atacantes para hacer esos cambios en primer lugar, dejándolos libres para atacar sus sistemas una y otra vez. Además, volver a configuraciones más antiguas e incompatibles podría crear problemas de disponibilidad, especialmente si, por ejemplo, se han implementado parches en los archivos binarios a versiones posteriores desde el inicio del ataque.

Del mismo modo, la ausencia de IOC en una instantánea de copia de seguridad no garantiza que esté "limpia". Dado que los IOC simplemente sirven como señales de actividades maliciosas, eliminar las señales aún deja intacto el "destino". En casos de reversión automatizada a instantáneas más antiguas, este enfoque puede dejar al equipo de respuesta ante incidentes sin conocimiento del ataque subyacente.

La detección de los IOC también depende de la recopilación, el análisis y la difusión de la inteligencia de amenazas cibernéticas, que a menudo queda rezagada respecto de las tácticas cambiantes de los adversarios. Esto significa que hay un retraso entre el adversario que cambia su comportamiento y el conocimiento de las nuevas técnicas de ataque de nuestras herramientas de seguridad. Esto explica por qué algunas de las organizaciones más grandes del mundo, a pesar de tener amplios presupuestos y equipos de ciberseguridad que ciertamente están utilizando las mejores y más recientes herramientas de ciberseguridad, aún se ven afectadas por el ransomware. El adversario cambia su comportamiento antes de que las herramientas de ciberseguridad actuales tomen conocimiento de ese cambio, lo que les permite entrar a la organización sin ser detectados. Una vez adentro, su capacidad de evasión de defensa deja ciegos a los controles de seguridad del endpoint. Cuando el proveedor de herramientas de seguridad toma conocimiento del nuevo comportamiento del adversario, y la inteligencia sobre amenazas relevantes se introduce en sus herramientas, ya es demasiado tarde. La herramienta ya ha sido evadida y no se activará.

Para mitigar estos desafíos, considere adoptar una actividad en tiempos de paz como la búsqueda periódica y proactiva de amenazas, utilizando una solución como **Cohesity DataHawk**. La solución funciona independientemente de los controles de seguridad tradicionales y no se puede evadir. DataHawk le permite encontrar ataques que pueden haberse inmiscuido en la red cuando las fuentes de inteligencia de amenazas cibernéticas no estaban al tanto de ellos.

Ganar la guerra: investigación, mitigación de amenazas y recuperación segura

El mejor enfoque consiste en desarrollar la resiliencia y la preparación mediante el uso de las soluciones tecnológicas adecuadas como multiplicadores de fuerza para los equipos de respuesta ante incidentes, la definición de procesos claros y un modelo operativo para que todos sepan exactamente lo que deben hacer. Utilice la automatización y la orquestación cuando sea posible. Además, el personal debe estar debidamente capacitado y participar en ejercicios realistas para responder, en lugar de reaccionar, cuando suceda lo peor.

La resiliencia cibernética no es un producto que pueda comprar. Es una propiedad emergente que aparece cuando su organización está preparada para actuar de manera correcta después de un incidente cibernético. Para lograr la resiliencia cibernética, debe trabajar con un proveedor que sea realista sobre los desafíos que enfrentan las organizaciones después de un ciberataque destructivo y que ofrezca la tecnología adecuada y el apoyo necesario para que usted construya una estrategia sólida de respuesta a incidentes.

Dar respuesta a los incidentes de ciberseguridad es una actividad compleja. El éxito proviene de reconocer esa complejidad, no de ignorarla. Pretender lo contrario solo afectará a la organización en el peor momento posible: durante un incidente.

Mejores prácticas del análisis forense digital y respuesta a incidentes de ciberseguridad

Existen cuatro marcos principales ampliamente adoptados para la investigación forense digital y la respuesta ante incidentes:

1. NIST SP800-61 Guía de manejo de incidentes de seguridad informática
2. Instituto SANS: Proceso de seis pasos de respuesta ante incidentes
3. Marco RE&CT (“React”)
4. MITRE D3FEND (“defensa basada en datos”)

En este documento técnico, nos centraremos en el uso del modelo del Instituto SANS. Dicho esto, todos los marcos están alineados en gran medida con los pasos necesarios para prepararse y responder a un ciberataque:

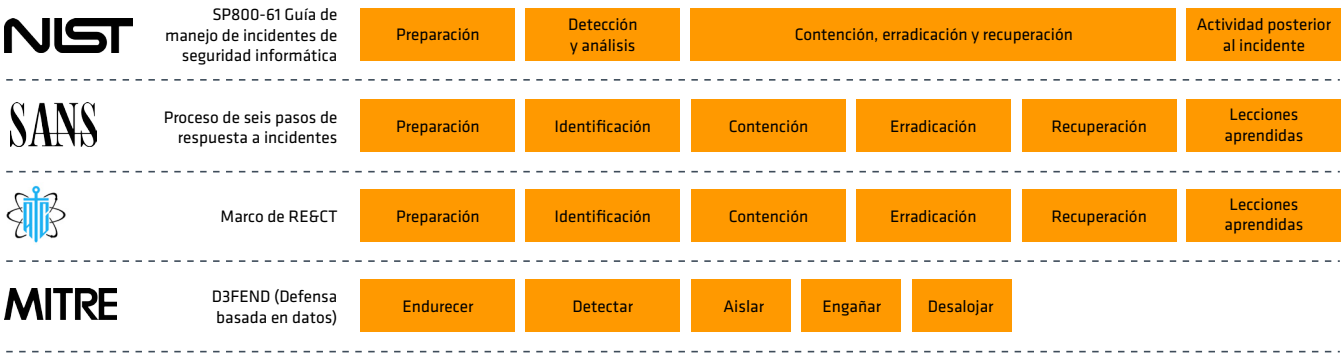

Figura 2. Mejores prácticas del análisis forense digital y respuesta a incidentes cibernéticos

Lograr las mejores prácticas operativas con Cohesity

Para las situaciones de guerra, todos los marcos de respuesta a los incidentes de ciberseguridad que adoptan las mejores prácticas incluyen las etapas de contención, investigación, mitigación de amenazas y, finalmente, recuperación. Las organizaciones que omiten las etapas de contención, investigación y mitigación y se apresuran a recuperarse dejan en el lugar a las vulnerabilidades que permitieron el ataque.

Las brechas en las defensas que no lograron detectar ni prevenir el ataque permanecen abiertas; a menudo, los mecanismos de persistencia y otros artefactos del ataque vuelven a actuar. Con frecuencia, esto provoca una reinfección o un reataque y posteriores tiempos prolongados de inactividad. No es inusual ver que las organizaciones que adoptan un enfoque centrado en la recuperación para responder a los ataques de ransomware tengan que recuperarse más de una docena de veces.

Identificación

Hay dos etapas involucradas en la identificación:

1. **Conocimiento inicial de que un posible incidente está en curso**: esto puede tomar la forma de un informe de un usuario o de un tercero, que debe clasificarse para confirmar su validez y alcance, o una alerta proveniente de alguna forma de control técnico.
2. **Comprender cómo ocurrió el ataque**: esto garantiza la erradicación adecuada de la amenaza, la eliminación de las vulnerabilidades explotadas y el refuerzo de los controles, lo que permite que los sistemas se recuperen a un estado seguro y resiliente.

Revisemos cada etapa con más detalle.

Conocimiento inicial

La concientización inicial es técnicamente una actividad en tiempos de paz, ya que no se puede declarar el tiempo de guerra hasta que la organización detecte un ataque en curso. Por lo tanto, es importante analizar los mecanismos para detectar ataques como el ransomware para comprender cómo esto puede afectar el flujo de trabajo de respuesta ante incidentes.

Las plataformas RaaS han mercantilizado la evasión de herramientas de seguridad populares como EDR y XDR, dejándolas ciegas ante los ataques. En el marco MITRE ATT&CK, la taxonomía más popular para describir cómo se llevan a cabo los ciberataques, la táctica de evasión de defensa tiene casi el doble de técnicas que la siguiente más cercana de las 13 tácticas. Estos mecanismos utilizados por los atacantes de ransomware no son capaces de evadir la detección de anomalías de **Cohesity DataProtect** y las capacidades de búsqueda de amenazas de DataHawk.

Las alertas, como las de **detección de anomalías basada en IA** de DataProtect, tienen un alto grado de **confianza**, lo que asegura que la alerta no sea un falso positivo, así como una alta **fidelidad**, que es la cantidad de información sobre lo que está sucediendo, que el analista del SOC recibe al observar la alerta. Esto acelera el proceso de triaje e investigación, lo que disminuye el tiempo necesario para recuperar los sistemas en producción de manera segura.

Si durante el triaje resulta evidente que los sistemas requeridos para responder a los incidentes se han visto afectados, o que el cifrado o la eliminación de sistemas en toda la organización están por encima de un cierto umbral predefinido, la organización puede declarar una **crisis cibernética**. Un flujo de trabajo de crisis cibernética predefinido permite a una organización establecer diferentes escalamientos y una autoridad prescrita para que la fuerza de respuesta ante incidentes lleve a cabo ciertas acciones más allá de las que normalmente realiza para una violación cibernética.

Es posible que se descubra que los sistemas necesarios durante la respuesta a incidentes se hayan visto afectados, no estén disponibles o sean poco confiables. Los problemas en esta situación pueden incluir:

- Es posible que no se disponga de listas de contactos de las partes interesadas en la respuesta a incidentes, como ejecutivos, reguladores, proveedores de seguros cibernéticos, empresas de respuesta a incidentes contratadas, socios de la cadena de suministro y la prensa.

- Los flujos de trabajo de respuesta ante incidentes pueden no estar disponibles.
- Es posible que los contratos para su póliza de seguro cibernético y los equipos de respuesta ante incidentes contratados no estén disponibles.
- Los servidores de gestión y las configuraciones para los sistemas de control de acceso físico o los controles ambientales para los edificios pueden estar inactivos.
- Los sistemas de comunicaciones necesarios para comunicarse con las partes interesadas, como el correo electrónico o la Voz sobre Protocolo de Internet, pueden estar inactivos o en un estado no confiable.
- Los enrutadores y configuraciones de conmutadores o firmware pueden no ser confiables, haciendo que cualquier conexión a internet para aplicaciones de software como servicio o comunicaciones esté sujeta a escuchas o interrupciones.
- Es posible que las herramientas de seguridad hayan sido evadidas o se hayan vuelto inutilizables.

Es comprensible que la mayoría de las organizaciones prioricen la restauración de las aplicaciones más críticas primero, aquellas esenciales para reanudar la entrega de productos y servicios, también conocidas como la viabilidad mínima de una empresa (MVC). Sin embargo, las organizaciones que sufren un ciberataque destructivo se dan cuenta de que también se necesita un subconjunto de cuentas, aplicaciones e infraestructura para gestionar el incidente de manera efectiva. Estos sistemas garantizan que los sistemas de producción críticos no solo se puedan recuperar, sino que también se puedan recuperar a un **estado seguro** mientras se cumple con las obligaciones regulatorias de la organización.

Cohesity define este subconjunto de infraestructura y recursos esenciales para gestionar los esfuerzos de respuesta y recuperación como la Capacidad de Respuesta Mínima Viable (MVRC). Supongamos que cualquier componente de la MVRC se ha vuelto poco confiable o no está disponible. En ese caso, las organizaciones necesitan una forma rápida de poner estos recursos a disposición y reconstruir un conjunto confiable de herramientas para gestionar las acciones de respuesta. La **solución Cohesity Clean Room** permite a las organizaciones reconstruir rápidamente su MVRC a un estado confiable y poner a disposición en minutos los recursos necesarios para gestionar el incidente.

Comprender cómo ocurrió el ataque

Una vez que se completa el triaje inicial y existe la confianza de que se está llevando a cabo un ciberataque destructivo, el analista declara un incidente y continúa con una investigación más profunda. Por lo general, desplegar cifradores en servidores y endpoints es la última tarea que efectúan las bandas de ransomware, ya que es la etapa más ruidosa del ataque, tanto en términos de activar controles de detección como de generar impactos visibles para los usuarios finales.

Es poco probable que enfocar las investigaciones y correcciones solo en sistemas cifrados descubra la causa fundamental del ataque. En cambio, la investigación debe extenderse más allá de estos sistemas. Los sistemas no cifrados suelen ser de mayor interés para el investigador, ya que pueden contener mecanismos de persistencia que los adversarios pueden usar para regresar después de cualquier intento de recuperación.

Antes de analizar en detalle este nivel más profundo de identificación, es importante comprender cómo otro aspecto de las mejores prácticas de todos los procesos de respuesta ante incidentes es capaz de impedir nuestra capacidad de efectuar esta tarea: la contención.

Contención

La contención es un requisito de todos los marcos de respuesta ante incidentes, ya que evita la propagación del ataque e interrumpe cualquier actividad de comando y control o exfiltración de datos. Sin embargo, la contención también presenta algunos desafíos para los equipos de operaciones de seguridad:

- **Las imágenes remotas no funcionan de forma aislada**. La mayoría de las organizaciones han pasado de adquirir físicamente contenido del disco duro a imágenes forenses remotas. Sin embargo, aislar un host infectado, o la red del host, puede eliminar repentinamente la capacidad de la organización para efectuar esta tarea. **DataProtect** proporciona una interfaz de usuario y una API que permite a la fuerza de respuesta ante incidentes efectuar análisis forenses a nivel de archivo no solo en la última instantánea, sino en una serie de instantáneas a lo largo del tiempo hasta el período de retención de la organización. Esto proporciona a los analistas forenses digitales el superpoder de viajar en el tiempo: les permite buscar binarios y otros artefactos que el adversario ya ha limpiado, e identificar rápidamente los actores maliciosos efectuados en las configuraciones y otros archivos. A diferencia de las soluciones de seguridad de endpoints

y los SIEM que normalmente solo retienen un corto plazo de registros, Cohesity permite a la fuerza de respuesta ante incidentes examinar eventos y el contenido de registros durante todo el período en el que se mantienen copias de seguridad para ese sistema; esto es efectuado por una plataforma inmutable que garantiza una cadena de custodia sólida. Lo mejor de todo es que estas capacidades se proporcionan sin conexión de red. Es inmune al espionaje y la interrupción, ya que DataProtect utiliza una copia sin conexión del sistema de archivos para esta tarea.

- **Las soluciones del endpoint se aíslan y la consulta/respuesta se vuelve imposible.** Si bien puede diferir la arquitectura de diferentes soluciones de endpoint, como EDR y XDR, casi todas tienen un servidor de gestión central que recibe telemetría de clientes de endpoint. Si la contención interrumpe la conexión entre el servidor de gestión y los endpoints, los analistas quedan solo con la información enviada previamente al servidor de gestión. Ya no pueden trabajar a modo de consulta y respuesta para profundizar en lo que está sucediendo en los endpoints en tiempo real.
- La contención también incluye el establecimiento de entornos aislados donde pueden ocurrir técnicas de respuesta a incidentes y recuperación. La solución Cohesity Clean Room proporciona un enfoque flexible para crear dichos entornos. Ayuda a las organizaciones a alinearse con las mejores prácticas de respuesta ante incidentes y a adoptar un modelo de responsabilidad compartida adecuado entre las operaciones de seguridad y de TI. Este enfoque ayuda a las organizaciones a evitar tiempos de inactividad prolongados y a prevenir la reinfección después de una recuperación.
- La solución Cohesity Clean Room:
- Permite la restauración rápida de la MVRC o de la infraestructura afectada o evadida, lo cual es esencial para investigar y remediar el incidente.
- Establece un entorno de investigación aislado que permite a los equipos de operaciones de seguridad utilizar las capacidades de seguridad nativas de la plataforma Cohesity Data Cloud junto con sus otras herramientas de seguridad para comprender el ataque integral y planificar las correcciones adecuadas para prevenir ataques futuros.
- Crea un entorno de mitigación aislado en el que los resultados de la investigación del equipo de operaciones de seguridad informan las correcciones, como la reconstrucción rápida de sistemas a partir de imágenes y configuraciones de instalación conocidas, la recuperación de sistemas y la implementación de parches en sus vulnerabilidades, el refuerzo de controles para que no sea posible evadirlos y la prevención o detección exitosa de futuros ataques similares. Por último, los sistemas pueden probarse en cuanto a funcionalidad y rendimiento, antes de restaurarlos a los sistemas de producción.

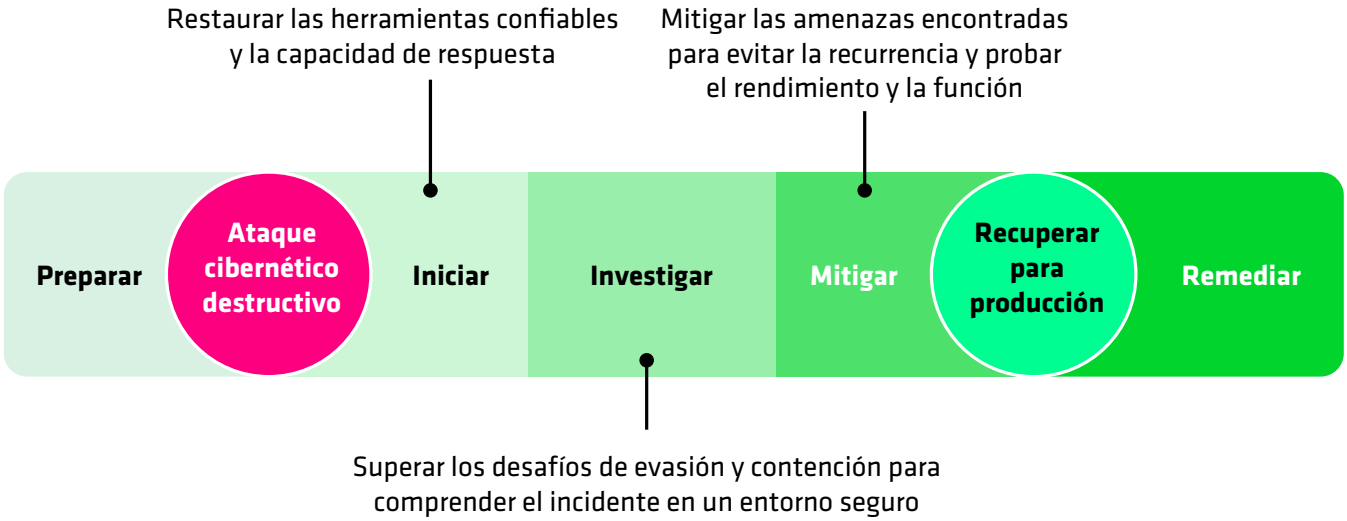

Figura 3. Las cuatro etapas de la solución Cohesity Clean Room que llevan a los clientes a la remediación de un ciberataque.

Repaso de la identificación: cómo ayuda la solución Cohesity Clean Room

Siguiendo las mejores prácticas forenses digitales y de respuesta ante incidentes, la organización ahora ha contenido las redes y los hosts infectados. En esta etapa, cualquier infraestructura afectada necesaria para investigar y remediar el incidente se restablecería a un estado de confianza: puede confiar en su conexión a internet y utilizar sus servicios de TI, empresariales y de seguridad basados en la nube. Además, se restablecería su capacidad de comunicación con las partes interesadas. Lo más importante, toda la documentación y los recursos necesarios para respaldar la respuesta y recuperación ante incidentes están al alcance de sus equipos de seguridad y operaciones de TI.

Ahora examinaremos cómo Cohesity ayuda con el nivel más profundo de la investigación, mientras que los activos que está investigando han sido aislados a modo de contención.

Descubrir las vulnerabilidades explotadas en el ataque

Las bandas de ransomware y los estados nación que se preparan para ataques wiper suelen obtener acceso inicial mediante vulnerabilidades en los activos orientados a internet. Incluso se sabe que los adversarios obtienen acceso inicial a través de vulnerabilidades e instalan mecanismos de persistencia, lo que les permite permanecer y luego implementar parches para evitar que otros atacantes obtengan acceso a esos sistemas.

¿Cómo pueden las organizaciones establecer qué vulnerabilidades existían al momento de un ataque? Esto se vuelve aún más difícil si el adversario ha borrado el sistema o si las medidas de contención impiden el acceso al sistema para efectuar un escaneo de vulnerabilidad.

Cohesity CyberScan proporciona una solución al permitir que las organizaciones escaneen instantáneas de copia de seguridad para detectar vulnerabilidades utilizando su licencia de administración de vulnerabilidades de Tenable. Esto permite que los equipos de seguridad identifiquen vulnerabilidades durante un ataque, incluso si un sistema es inaccesible debido a la contención, ha sido borrado o si un adversario implementó parches después de una intrusión.

Efectuar el análisis forense al sistema de archivos

La investigación forense del sistema de archivos es una disciplina central de la respuesta ante incidentes. Muchas organizaciones utilizan herramientas de adquisición remota para la obtención de imágenes forenses. Sin embargo, una vez implementadas las medidas de contención, los sistemas que requieren imágenes forenses a menudo ya no son accesibles.

DataProtect proporciona a los analistas acceso no solo a una instantánea de un solo volumen de los sistemas de archivos, sino también a una serie completa de instantáneas. Esto permite a los examinadores forenses

Figura 4. Cómo se alinea Cohesity Clean Room con las mejores prácticas de respuesta a incidentes

revisar la cronología de un incidente y todo el período de retención de copias de seguridad. Una serie temporal de volúmenes se puede montar y comparar rápidamente para identificar actores maliciosos. Los objetos de archivo se pueden extraer para efectuar ingeniería inversa, detonación en entornos aislados o análisis enviándolos a servicios basados en la nube.

En los análisis forenses digitales tradicionales, la fuerza de respuesta ante incidentes generalmente recopila una sola imagen del sistema después del ataque, forma una hipótesis sobre cómo el sistema llegó a ese estado final y luego vuelve a trabajar para recopilar evidencia que respalde o desacredite esa teoría. Por el contrario, mediante DataProtect, la fuerza de respuesta ante incidentes es ahora capaz de ver los cambios en el sistema de archivos dispuestos en una mayor extensión de la línea de tiempo del incidente, lo que continúa funcionando incluso si los esfuerzos de contención han aislado al host infectado.

Caza de amenazas

La búsqueda de IOC es otra tarea que la fuerza de respuesta ante incidentes generalmente debe hacer. Esta caza en tiempos de guerra se clasifica en dos categorías:

Búsqueda de IOC suministrados por un tercero. Estos terceros pueden incluir a un proveedor de inteligencia de amenazas cibernéticas, a una agencia gubernamental o a organizaciones afines. Los clientes de Cohesity que utilizan DataHawk pueden hacer uso de la alimentación actualizada con frecuencia de más de 117 000 IOC que están siendo usados por actores de ransomware y estados nación. La capacidad de escaneo de amenazas de DataHawk también admite fuentes comerciales de inteligencia de amenazas de CrowdStrike que la organización haya licenciado y puede consumir cualquier IOC que haya sido suministrado en formato YARA por parte de otros terceros.

Búsqueda de IOC descubiertos por su organización. A medida que los equipos de respuesta ante incidentes encuentren artefactos durante una investigación, querrán buscar si estos IOC existen en toda la infraestructura de la organización. A partir de allí, determinará si se deben incluir sistemas adicionales en el alcance de la respuesta al incidente.

Esto se hace comúnmente creando reglas YARA que describen el artefacto encontrado de una manera que permite la detección pero evita falsos positivos innecesarios. Con Cohesity, puede efectuar análisis forenses (como se discutió en la sección anterior), extraer artefactos del sistema de archivos y detonarlos en sandboxes como Cuckoo, que con un complemento puede generar automáticamente reglas YARA para cualquier IOC relacionado con ese archivo. La capacidad de búsqueda de DataHawk no depende de los agentes del endpoint. Sigue funcionando incluso si la organización ha aislado

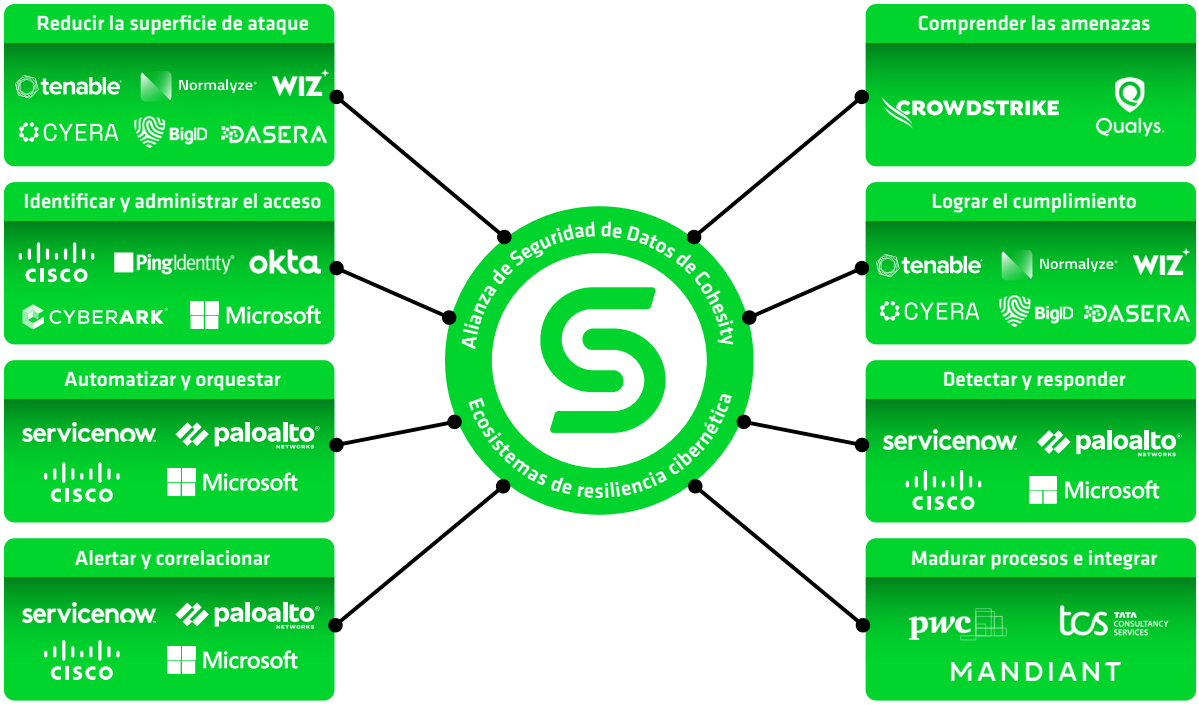

Figura 5. Alianza de Seguridad de Datos de Cohesity: un ecosistema para la resiliencia cibernética.

sistemas para su contención. No es vulnerable a las técnicas comunes de evasión de defensa que hacen que las soluciones de seguridad del endpoint no puedan buscar de manera efectiva.

Capacidades como **Cohesity Global Search** permiten a la fuerza de respuesta ante incidentes buscar rápidamente archivos en toda la infraestructura respaldada, lo que puede ayudar a dirigir los esfuerzos de investigación cuando se busca un artefacto o archivo en particular.

Lograr el cumplimiento normativo

Además de exigir procesos sólidos de respuesta ante incidentes, muchas regulaciones de cumplimiento recientemente actualizadas, como HIPAA, DORA y NIS 2, requieren que las organizaciones notifiquen a los reguladores y a los interesados afectados en caso de una violación de ciberseguridad. Comprender la naturaleza de la violación es parte de la etapa de identificación, al igual que comprender su impacto y garantizar una notificación oportuna.

Si el incidente ha afectado la comunicación, como parte del MVRC, Cohesity ayuda a restaurar esta capacidad. Las plantillas de comunicación se pueden guardar en la **Digital Jump Bag**™, la base de una sala limpia. Además, DataHawk puede **escanear copias de seguridad para identificar datos confidenciales y regulados**, lo que ayuda a las organizaciones a cumplir con los requisitos normativos. Esto es especialmente valioso después de un ciberataque destructivo cuando los almacenes de datos críticos son cifrados o borrados.

Integración de herramientas de operaciones de seguridad

La resiliencia cibernética es un deporte de equipo: ninguna solución de un solo proveedor puede investigar y remediar un incidente en su totalidad. Es por eso que Cohesity estableció la **Alianza de Seguridad de Datos**. Este ecosistema colaborativo permite que el poder de los datos y los datos a lo largo del tiempo se incorporen a herramientas y servicios de seguridad más amplios mediante integraciones para la gobernanza, la investigación y la recuperación comunes.

Automatización y orquestación

Cohesity admite la integración de API, que permite a una plataforma de orquestación de seguridad y respuesta automatizada (SOAR) impulsar estas tareas de investigación, aumentando aún más la eficiencia de los analistas.

Erradicación y recuperación

Hemos fusionado las etapas de erradicación y recuperación en la etapa de mitigación porque, para Cohesity, ninguna organización debería buscar recuperarse de un ciberataque destructivo sin tomar las medidas adecuadas para garantizar que el adversario que ataca a la organización no pueda reinfectar los sistemas o que un ataque futuro de la misma naturaleza no sea exitoso.

La solución Cohesity Clean Room admite una rápida recuperación de volúmenes, lo que permite recuperar todo un sistema de archivos antes de aplicar mitigaciones para

Enfoque de recuperación y limpieza	
Ventaja:	**Desventaja:**
Es más sencillo gestionar antes de un incidente.	Las investigaciones deben ir más en profundidad.
	El tiempo de corrección suele ser más largo que el necesario para los sistemas reconstruidos.
Enfoque de reconstrucción	
Ventaja:	**Desventaja:**
Oportunidad de recuperar datos, reconstruir sistemas e investigar incidentes en paralelo, proporcionando la recuperación más corta posible de los sistemas hacia un estado seguro.	La investigación generalmente no necesita ser tan profunda ya que los sistemas están en un estado confiable.
La corrección es más corta, por lo general solo valida la seguridad de las configuraciones, refuerza los controles e implementa parches en cualquier sistema vulnerable.	Requiere habilidades para crear secuencias de comandos de reinstalación.
	Los medios de instalación, las claves de licencia, los archivos de configuración y las secuencias de comandos deben mantenerse en el kit de emergencia digital.

erradicar amenazas. Esto garantiza una recuperación segura del sistema y, al mismo tiempo, facilita la rápida reconstrucción de los sistemas a partir de imágenes de software confiables y configuraciones conocidas y buenas. Cada enfoque tiene sus ventajas y desventajas:

Algunos clientes de Cohesity eligen admitir copias de seguridad y reconstrucciones a nivel de volumen. Esto les da la opción de elegir el método más adecuado de recuperación segura para cada host comprometido según el nivel de esfuerzo involucrado en la limpieza de ese sistema y el grado de confianza de que la limpieza no dejará artefactos de ataque.

Los clientes a menudo reutilizan su entorno de desarrollo para usarlo como el entorno de mitigación de Cohesity Clean Room. Este enfoque permite que los servidores de producción se aplanen en paralelo con las actividades de mitigación que ocurren dentro del entorno de mitigación aislado de Clean Room. El entorno de mitigación es configurado para imitar la estructura del entorno de producción, utilizando configuraciones almacenadas en el kit de emergencia digital.

Los sistemas pueden probarse una vez que las amenazas descubiertas en la etapa de investigación se mitigan mediante la recuperación y limpieza o reconstrucción a un estado confiable. Esto puede adoptar la forma de pruebas funcionales o pruebas de rendimiento para garantizar que la corrección, la implementación de parches y el refuerzo de los controles no hayan afectado la capacidad de entrega del sistema.

Finalmente, se toma una instantánea de estos sistemas para dos propósitos:

1. Si se pierde algún artefacto de ataque, no es necesario que regrese al punto de partida. La instantánea tomada después de la corrección servirá como la nueva línea de referencia para la investigación y corrección adicional y será transferida a la etapa de investigación.
2. Dado que el entorno de mitigación fue configurado para parecerse al de producción, esta instantánea simplemente puede "levantarse y trasladarse" a la red de producción.

Lecciones aprendidas

Cualquier organización que busque establecer resiliencia cibernética debe seguir un mantra de mejora continua. Comprender lo que funcionó, lo que no funcionó y lo que podría mejorarse es fundamental para garantizar que la organización no sufra un tiempo de inactividad continuo y pueda manejar incidentes futuros de manera más efectiva y eficiente. Como dice el adagio: "Ningún plan sobrevive al contacto con el enemigo". Simular ataques del mundo real es importante para probar la recuperación técnica, impulsar la mejora de los procesos, identificar oportunidades de automatización y construir memoria muscular en sus analistas y equipos de respuesta ante incidentes.

Una de las mayores ventajas de la solución Cohesity Clean Room es que permite a las organizaciones simular un incidente completo de extremo a extremo sin afectar los sistemas de producción. DataProtect permite la clonación de sistemas de producción, que luego pueden ser atacados por un equipo rojo interno o una empresa de pruebas de penetración externa para simular un ataque de ransomware o wiper de extremo a extremo. Todo el flujo de trabajo de respuesta y recuperación puede llevarse a cabo inmediatamente después de tomar la instantánea de referencia de los sistemas corregidos. Esto ofrece a las organizaciones un escenario del mundo real que garantiza que se implementen las personas, las habilidades, los procesos y la tecnología de apoyo adecuados para minimizar el impacto de un ciberataque destructivo cuando sucede lo inevitable y la organización se convierte en víctima.

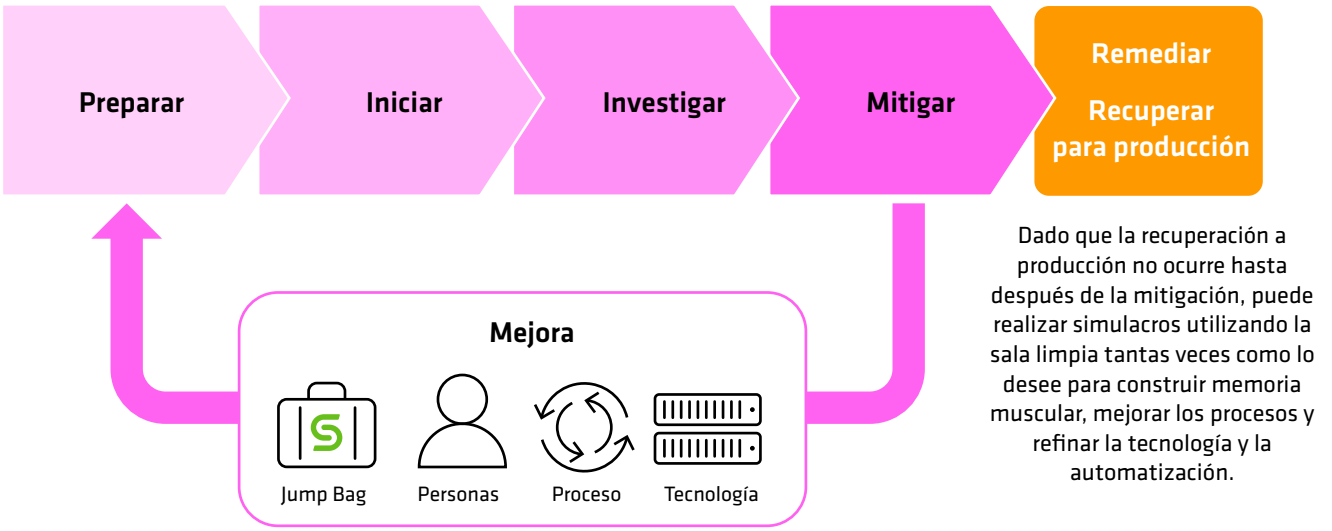

Figura 6. La solución Cohesity Clean Room permite una mejora continua a través de simulacros realistas.

Resumen

Cohesity puede agregar un valor tremendo en la recuperación y hacer que las etapas de respuesta a incidentes y análisis forense digital en tiempos de guerra sean efectivas y eficientes. Nuestro enfoque único para la resiliencia cibernética reduce el tiempo que lleva lograr una recuperación segura y ayuda a las organizaciones a garantizar que un ataque similar no causará más tiempo de inactividad.

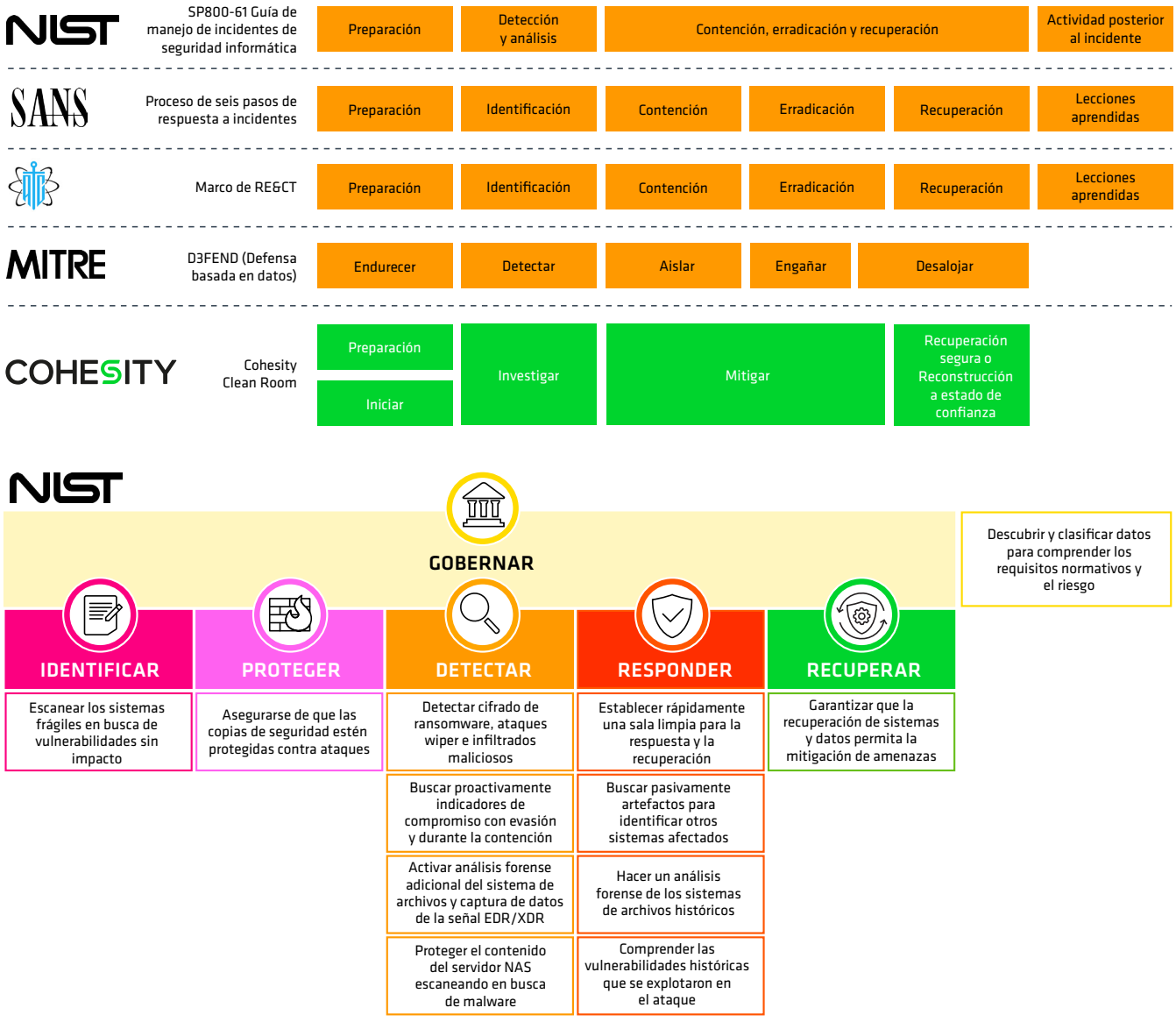

Figura 7. Lograr la respuesta a incidentes cibernéticos y las mejores prácticas del marco de ciberseguridad del NIST con Cohesity

Acerca de Cohesity

Cohesity es el líder en seguridad de datos impulsada por IA. Más de 13 600 clientes empresariales, incluidos más de 85 de las empresas Fortune 100 y casi el 70 % de las empresas Global 500, confían en Cohesity para fortalecer su resiliencia y, al mismo tiempo, proporcionar información sobre la inteligencia artificial generativa en sus vastas cantidades de datos. Formadas a partir de la combinación de Cohesity con el negocio de protección de datos empresariales de Veritas, las soluciones de la empresa aseguran y protegen los datos en las instalaciones, en la nube y en el borde. Con el respaldo de NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud y otros, Cohesity tiene sede en Santa Clara, CA, con oficinas en todo el mundo. Para obtener más información, siga a Cohesity en **LinkedIn**, **X** y **Facebook**.

Lecturas recomendadas

Creemos que los siguientes documentos técnicos, guías y blogs le resultarán útiles.

- Mejore la resiliencia cibernética con una Digital Jump Bag™
- Desarrollar resiliencia cibernética en un mundo de ciberataques destructivos
- Presentamos el diseño de sala limpia de Cohesity
- Una guía de campo para la seguridad de datos impulsada por IA: Cómo ofrecer resultados comerciales innovadores
- Una guía ejecutiva para la seguridad y gestión de datos modernos
- Topologías modernas de seguridad y gestión de datos: Una guía para líderes de TI

Más información en Cohesity

COHESITY

http://cohesity.com/es-es/
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000058-002-EN 4-2025