COHESITY

DOCUMENTO TÉCNICO

Mejore la resiliencia cibernética con un Digital Jump Bag™

Cómo restaurar rápidamente una capacidad mínima viable de respuesta y fortalecer la respuesta a incidentes

ÍNDICE

Adelante

James Blake
Vicepresidente de estrategia para la resiliencia cibernética

Durante más de 30 años, he estado en la primera línea de la respuesta cibernética a ataques cibernéticos destructivos y robo de datos. Mi experiencia abarca desde la ejecución de respuestas a incidentes hasta ataques wiper por parte de actores nacionales-estatales hasta liderar la gestión de riesgos cibernéticos en el banco más grande del mundo.

Durante este tiempo, he aprendido el valor de tener un "kit de emergencia (jump bag)". El término se usaba originalmente para describir un contenedor físico con el hardware y el software esenciales que debía recogerse al trasladarse a un sitio afectado por un ataque. Este kit de emergencia tenía los elementos esenciales para investigar rápidamente el incidente, recopilar evidencia y mitigar las amenazas. Además de hardware y software, contenía elementos como impresiones de la lista de contactos de partes interesadas clave dentro de la organización y terceros, el plan de gestión de crisis, flujos de trabajo para los tipos de incidentes a los que probablemente respondería y un teléfono móvil. La idea era estar preparado para responder de inmediato: apresurarse a encontrar todo lo que necesita mientras está bajo la presión de un incidente desperdicia tiempo valioso y lleva a olvidar algo esencial. El kit de emergencia contenía una mezcla de herramientas, detalles de procesos y un método para permitir la comunicación.

Hoy en día, vivimos en un mundo de adquisición remota, puntos finales y detección y respuesta extendidas (EDR/XDR), máquinas virtuales e instancias en la nube. Los kits de respuesta rápida aún pueden ser contenedores físicos que llevamos al sitio. Pero ahora, la mayor utilidad se puede encontrar en la preparación de un digital jump bag™. Este repositorio protegido y confiable proporciona un acceso rápido no solo a las herramientas requeridas para la adquisición y el análisis remotos, sino también a cualquier otro activo digital requerido para un resultado positivo durante una respuesta y recuperación ante incidentes.

Resumen ejecutivo

El digital jump bag™ es la base de una sala segura, un entorno seguro y aislado donde el equipo de operaciones de seguridad puede realizar los pasos de investigación necesarios para comprender cómo ocurrió un ataque. También utilizan una sala segura para realizar pasos correctivos antes de la recuperación para erradicar la amenaza y ayudar a evitar que vuelva a ocurrir. Lo que se incluye en el kit digital de emergencia depende de la madurez, estructura, procesos y herramientas de una organización.

En esencia, el kit digital de emergencia permite a una organización restaurar rápidamente una capacidad de respuesta viable mínima (Minimum Viable Response Capability, MVRC), un conjunto optimizado de herramientas, documentos y procesos esenciales necesarios para responder de manera efectiva a un ataque cibernético. La MVRC garantiza que las organizaciones puedan contener rápidamente las violaciones, restaurar las operaciones comerciales críticas y minimizar el tiempo de inactividad durante un incidente cibernético.

La **solución Cohesity Clean Room** respalda este enfoque moderno para ayudar a las organizaciones a combatir los ataques cibernéticos destructivos. Ofrece flexibilidad para adaptarse a diversas necesidades y respalda la mejora continua de la capacidad de resiliencia cibernética operativa con el tiempo.

En este documento técnico, recomendaremos lo que las organizaciones deben considerar incluir su kit digital de emergencia a medida que crean una estrategia de respuesta a incidentes más sólida y ágil.

Problemas comúnmente no abordados en la resiliencia cibernética

Los ataques cibernéticos destructivos a menudo implican la evasión de las herramientas de seguridad utilizadas dentro de la organización víctima, con capacidades de evasión EDR/XDR incorporadas en muchas de las plataformas comunes de ransomware como servicio (Ransomware-as-a-Service, RaaS) que son responsables de la gran mayoría de los ataques de ransomware que vemos hoy en día. Por su propia naturaleza, las soluciones EDR/XDR se encuentran en el punto final, que, cuando no se evaden, proporcionan una excelente visibilidad de los procesos, las conexiones de red y los sistemas de archivos.

Las mejores prácticas de respuesta a incidentes, como el ciclo de vida de respuesta a incidentes de seis pasos del Instituto SANS, la Guía de manejo de incidentes de seguridad informática SP800-61 del NIST, el Marco RE&CT y MITRE D3FEND, todas ellas protegen al contener la propagación de un incidente a través del aislamiento de redes y hosts infectados. En el mundo de los controles de punto final, en el mejor de los casos, esto deja a una organización solo con la información que ya ha recopilado para investigar el incidente.

Sin embargo, a medida que nos enfrentamos a un adversario que se adapta constantemente, es posible que no siempre sepamos qué información necesitamos recopilar para comprender un ataque con anticipación. Podemos encontrarnos cegados por el hecho de que nuestra capacidad de investigación y respuesta se ha convertido en una isla inalcanzable. Del mismo modo, la generación de imágenes forenses remotas de volúmenes en un host afectado se vuelve imposible si hemos cortado la conectividad.

Además de las herramientas de seguridad, muchos otros sistemas participan en las fases de investigación, mitigación y recuperación de la respuesta a incidentes. Estos pueden verse afectados por ataques cibernéticos destructivos como ransomware y wipers, pero con frecuencia se pasan por alto como críticos en muchos análisis de impacto comercial. He estado involucrado en incidentes en los que los responsables de respuesta a incidentes no pudieron entrar a sus edificios porque los controles de acceso físico se vieron afectados. Muchas organizaciones no pudieron comunicarse con la prensa, los reguladores, las fuerzas del orden, las aseguradoras cibernéticas o los interesados afectados debido a que sus servidores de voz sobre IP y correo electrónico fueron afectados. Muchos ejercicios de simulación de ransomware realizados por organizaciones no capturan suficientemente estos impactos creados por las técnicas dirigidas del adversario. Después de todo, los atacantes quieren asegurarse de que las organizaciones tengan dificultades para responder y recuperarse de los incidentes.

Con plataformas de RaaS que incorporan puntos vulnerables para vulnerabilidades recientemente parchadas en tan solo cinco días, necesitamos identificarlas en los sistemas y repararlas antes de volver a poner los sistemas en producción. De lo contrario, el mismo adversario u otro afiliado que utilice la misma plataforma RaaS volverá a ingresar.

También debemos identificar el vector de acceso inicial que nos da el primer sistema afectado, llamado “paciente cero”, y luego avanzar en el incidente. Es necesario comprender cómo el adversario mantiene la persistencia, escala los privilegios y encuentra otros artefactos del ataque para asegurarse de que cualquier recuperación esté en un estado seguro. Los equipos de respuesta también deben comprender la naturaleza de cualquier dato que se haya visto comprometido para cumplir con las obligaciones regulatorias de notificación.

El análisis de los sistemas cifrados no es suficiente. Por lo general, las pandillas de ransomware implementan cifradores justo al final de su ciclo de ataque, en los últimos minutos u horas de un ataque que podría haber estado dentro de nuestra infraestructura desde algunos hasta cientos de días. El cifrado es muy ruidoso y es probable que active controles de seguridad y detección de usuarios. En ese momento, es demasiado tarde. Esa necesidad de priorizar la velocidad es una de las razones por las que los programas de cifrado suelen no estar diseñados para garantizar la integridad, lo que provoca una gran pérdida de datos entre quienes pagan el rescate para obtener las claves de descifrado. Limitar el alcance a sistemas cifrados, sin identificar cómo el adversario ingresó y continúa habitando dentro de su red, es una receta para el desastre.

Las organizaciones que adoptan este enfoque a menudo se recuperan docenas de veces, solo para volver a infectarse una y otra vez. Este ciclo de "bucle de muerte" se resuelve investigando adecuadamente el incidente y utilizando las perspectivas obtenidas para remediar las amenazas.

Solo pregúntese, ¿en qué se diferenciaría su último resultado del ejercicio de simulación si no hubiera tenido teléfonos o correos electrónicos, hubiera sido bloqueado de sus edificios y no hubiera tenido acceso a sistemas de gestión de identidad y acceso al inicio del evento?

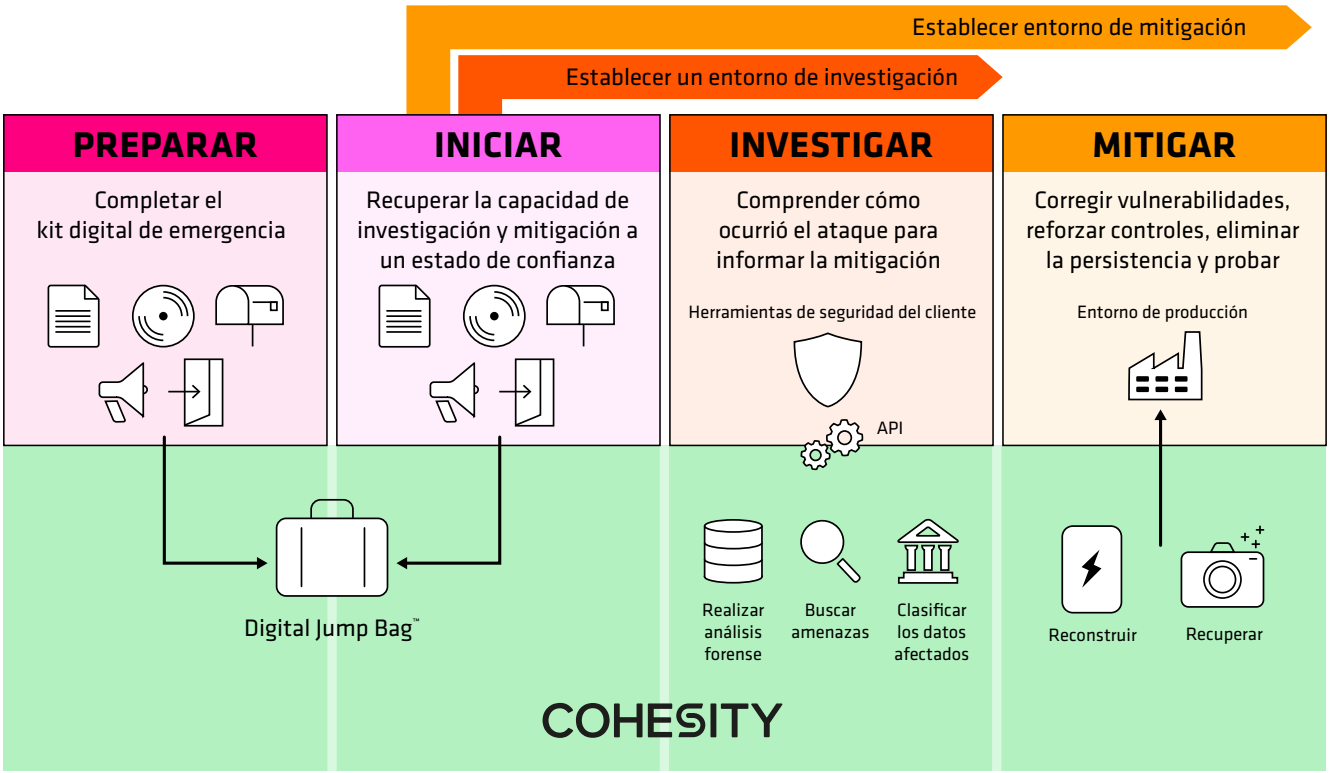
Cómo se integra el kit digital de emergencia en la solución Cohesity Clean Room

El kit digital de emergencia es la base de toda la solución Cohesity Clean Room, que respalda las etapas críticas de la respuesta a incidentes y la recuperación para permitir que las organizaciones restablezcan los datos limpios en la producción, como se muestra a continuación.

Revisemos lo que sucede en cada una de estas etapas.

Preparar

En esta etapa, elegimos lo que se incluye en el kit digital de emergencia, como configuraciones de red o hipervisor que admiten niveles de sistemas interdependientes que se restaurarían en el entorno de mitigación. Consulte la sección "¿Cuáles son los posibles componentes de su kit digital de emergencia?" para obtener sugerencias para habilitar las etapas posteriores.



Iniciar

En esta etapa, recuperamos la MVRC donde se recuperan las herramientas necesarias para la comunicación, colaboración e investigación de incidentes del kit digital de emergencia a un estado confiable dentro del entorno aislado de la sala segura. El kit digital de emergencia también establece los entornos de investigación y mitigación.

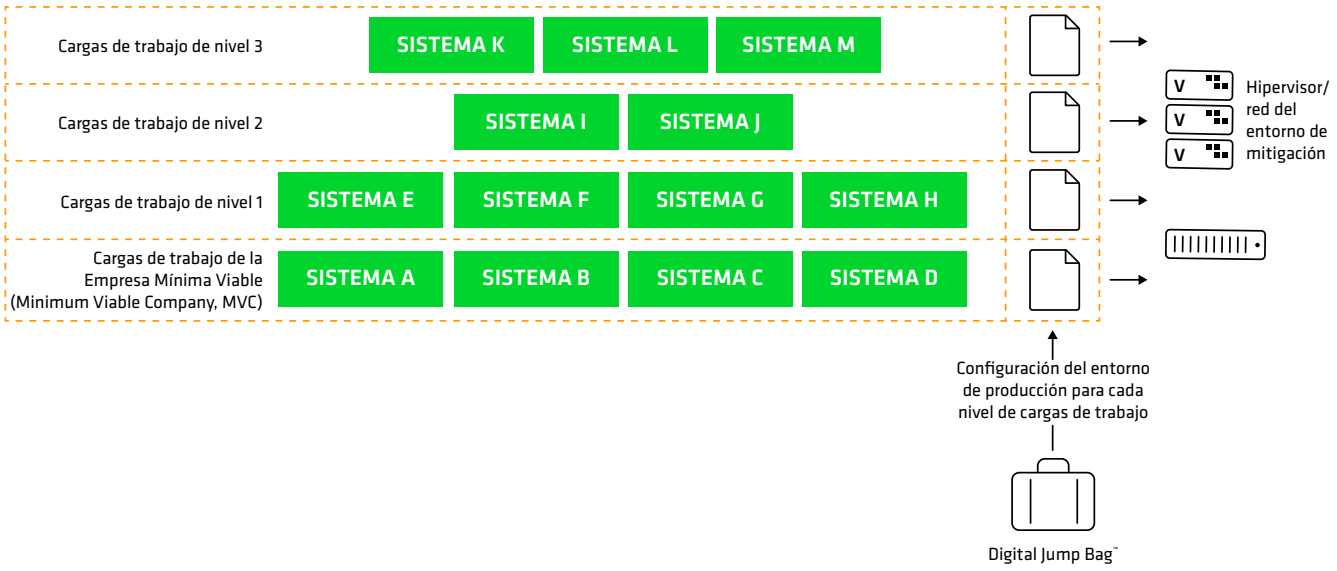
Investigar

Las operaciones de seguridad utilizan las herramientas de seguridad recuperadas en un estado confiable dentro de la sala segura aislada junto con las capacidades nativas de Cohesity para la clasificación de datos, la búsqueda de amenazas y la investigación forense del sistema de archivos para comprender todo el cronograma de incidentes de extremo a extremo. A medida que las herramientas de seguridad se recuperan a un estado confiable dentro de la sala segura y las capacidades de seguridad de Cohesity no están sujetas a las técnicas de evasión de defensa utilizadas contra los controles de punto final, se superan los desafíos de evasión y aislamiento debido a la contención. La Alianza de Seguridad de Datos de Cohesity proporciona un amplio conjunto de herramientas de proveedores de seguridad que pertenecen a mis Centros de Operaciones de Seguridad que están preconfigurados para trabajar junto con las soluciones de Cohesity.

Mitigar

Las operaciones de TI utilizan lo que el equipo de operaciones de seguridad ha descubierto sobre el incidente para recuperarse y luego limpiar, o elegir reconstruir los sistemas a un estado de confianza. Mientras que la etapa de investigación no implica una recuperación completa de los sistemas con interdependencias, la etapa de mitigación sí.

Los clientes a menudo reutilizan sus entornos de desarrollo como el entorno de mitigación durante la recuperación de incidentes. Los sistemas interdependientes se presentan en el entorno de mitigación con configuraciones de red que coinciden con los entornos de producción. Estas configuraciones de red o hipervisor se almacenan para cada nivel de sistemas interdependientes en el kit digital de emergencia. Esto se muestra a continuación.



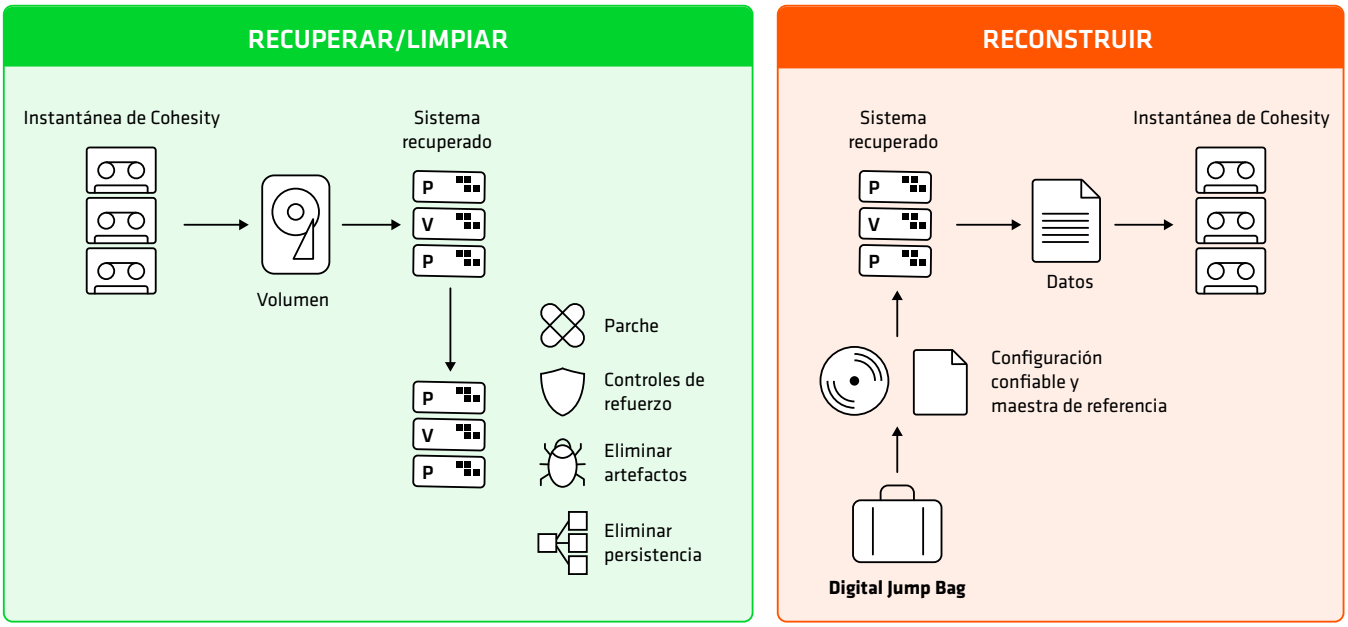
Alineación de Cohesity Clean Room con las mejores prácticas de respuesta a incidentes

Con la solución Cohesity Clean Room, la estrategia de "recuperar y limpiar" o "reconstruir a un estado confiable" puede aplicarse universalmente, o elegirse por sistema durante un incidente basado en el nivel de esfuerzo de corrección y el riesgo residual de amenazas. Revisemos una breve descripción de cada opción:

- **Recuperar y limpiar**: Los sistemas se recuperan de su instantánea y se llevan a cabo los pasos de mitigación descritos por el equipo de operaciones de seguridad en su etapa de investigación. Dado que los datos no se utilizan normalmente para transportar cargas maliciosas, la recuperación de datos a menudo puede ocurrir en paralelo con la reconstrucción del sistema, lo que reduce aún más los tiempos de recuperación finales.
- **Reconstruir los sistemas a un estado confiable**: El kit digital de emergencia contendrá configuraciones conocidas, scripts de instalación e imágenes de instalación maestra de referencia. Una vez reconstruidos, los datos se recuperarán de las instantáneas en los sistemas reconstruidos.

La sección "Uso del kit de emergencia para establecer la capacidad mínima viable de respuesta" detalla la comparación de cada enfoque.

Tener un entorno que satisfaga las necesidades de investigación del equipo de operaciones de seguridad y un entorno que permita al equipo de operaciones de TI garantizar que la recuperación esté en un estado seguro mediante la aplicación de mitigaciones ayuda a las organizaciones a lograr un modelo de responsabilidad compartida eficaz y adecuado para la resiliencia cibernética. Este enfoque optimiza la velocidad de la recuperación segura al garantizar que los activos de operaciones de TI y seguridad puedan utilizarse completamente.

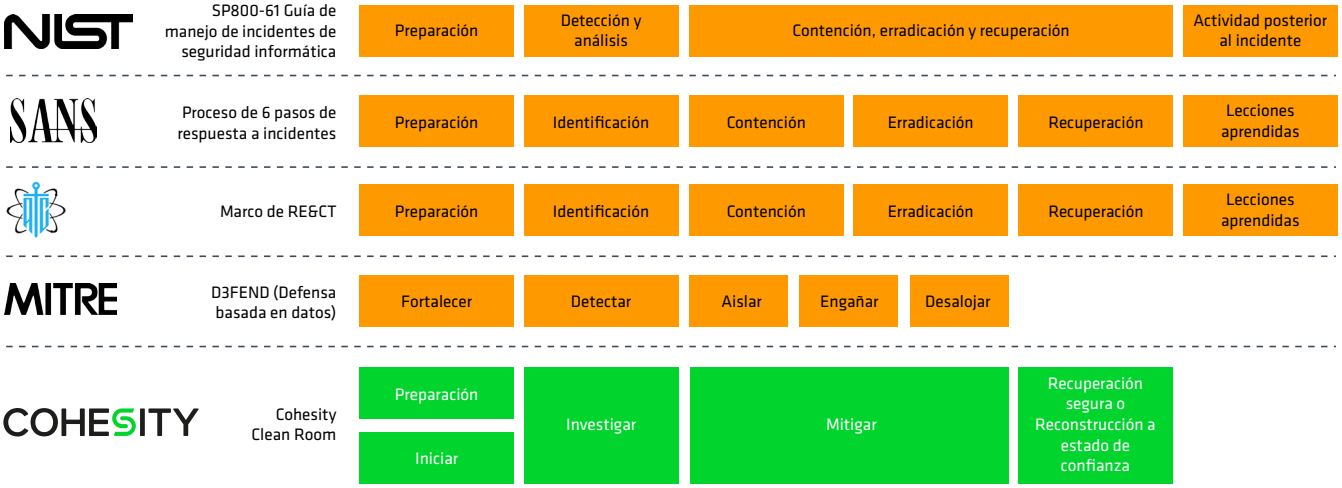


Cohesity Clean Room ofrece a los clientes la opción de recuperar y limpiar cargas de trabajo o reconstruir rápidamente a un estado confiable.

Una vez que los sistemas se han reconstruido o recuperado, se pueden realizar pruebas funcionales y de rendimiento en ese nivel de cargas de trabajo. Se toma una instantánea y luego se restaura toda la carga de trabajo interdependiente en el entorno de producción, con la seguridad de que se ha investigado todo el alcance del incidente, se han mitigado las amenazas y se han restaurado el rendimiento y la funcionalidad. Estos casos de prueba se pueden almacenar en el kit digital de emergencia para cada nivel de recuperación de cargas de trabajo interdependientes. En caso de que algo en investigación y mitigación se haya omitido, no es necesario volver al inicio, ya que la instantánea tomada al final de la fase de mitigación puede usarse como base para investigación y mitigación adicionales.

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

El kit digital de emergencia de Cohesity y la capacidad mínima viable de respuesta se alinean con las mejores prácticas de respuesta a incidentes cibernéticos descritas en el ciclo de vida de respuesta a incidentes de seis pasos del Instituto SANS, la Guía de manejo de incidentes de seguridad informática NIST SP800-61, el Marco RE&CT y MITRE D3FEND. Con este enfoque, las organizaciones que ya siguen estas metodologías pueden integrar fácilmente la solución Cohesity Clean Room en su flujo de trabajo existente. Los clientes que buscan mejorar su respuesta a incidentes y la madurez de la recuperación pueden adoptar la solución Cohesity Clean Room para poner en funcionamiento estas mejores prácticas.



Alineación de Cohesity Clean Room con las mejores prácticas de respuesta a incidentes

Reunión de las operaciones de seguridad y TI para ofrecer resiliencia

La resiliencia cibernética es un deporte de equipo: no puede ser entregada por las operaciones de TI en forma aislada ni por las operaciones de seguridad si actúan solas. Ambos equipos necesitan tener procesos integrados y herramientas complementarias. Del mismo modo, ningún proveedor puede ofrecer resiliencia cibernética. La solución Cohesity Clean Room está diseñada para permitir que el equipo de operaciones de seguridad aproveche y sea propietario del entorno de investigación, mientras que las operaciones de TI son propietarias y utilizan el entorno de mitigación. Esta propiedad y traspaso entre los equipos ayudan a garantizar un modelo de responsabilidad compartida claro, evitando que se pasen por alto ciertas actividades. La capacidad de revertir iterativamente instantáneas mitigadas previamente de vuelta a la etapa de investigación si algún aspecto del ataque se omite en la investigación inicial y mitigación, sin tener que comenzar al principio, reduce el tiempo de investigación y la recuperación final.

Tan pronto como las operaciones de seguridad hayan terminado de investigar una carga de trabajo en el entorno de investigación, se puede entregar a las operaciones de TI y al entorno de mitigación para su reconstrucción, recuperación y limpieza. Esto garantiza el uso más eficiente de los recursos de operaciones de TI y seguridad.

Responda más rápido, recupere de manera más inteligente: Cohesity CERT (Equipo de respuesta a eventos cibernéticos)

Muchas organizaciones carecen de la experiencia o los recursos para una respuesta efectiva a incidentes cibernéticos. Para minimizar el impacto, hemos mejorado nuestra solución de seguridad de datos de clase mundial con un servicio dedicado del Equipo de Respuesta a Eventos Cibernéticos (Cyber Event Response Team, CERT).

Cohesity CERT proporciona una recuperación rápida y dirigida por expertos de los ataques cibernéticos, lo que garantiza que sus datos se restablezcan y su negocio reanude las operaciones con un tiempo de inactividad mínimo.

Cohesity CERT está disponible para todos los clientes como parte de su suscripción a Cohesity.

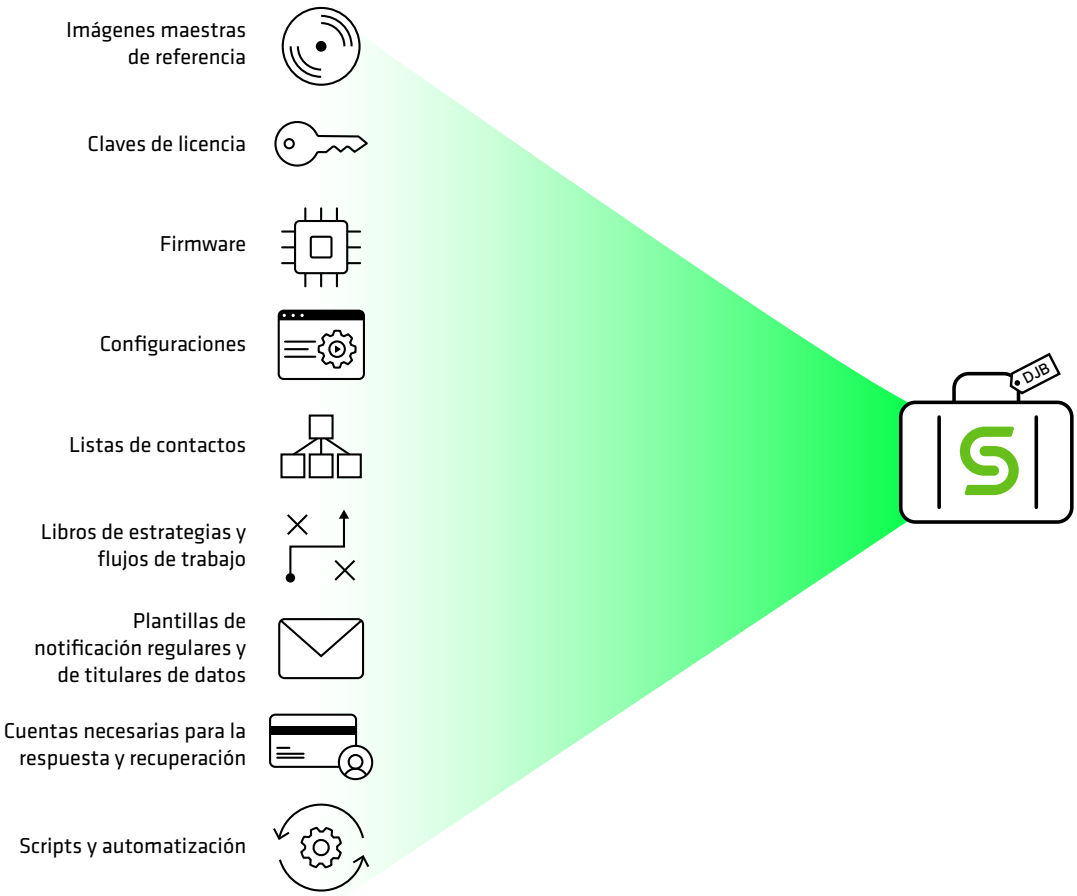
¿Cuáles son los posibles componentes de su kit digital de emergencia?

El contenido de su kit digital de emergencia depende de sus procesos individuales de triaje, investigación y mitigación, y de las herramientas que utiliza para lograrlos.

En general, vemos los siguientes artículos comúnmente incluidos en los kits digitales de emergencia de nuestros clientes:

Documentación

- Una lista de contactos que incluya a las partes interesadas internas y entidades externas, como las fuerzas del orden público, los centros de análisis e intercambio de información, las compañías de seguros, los servicios de respuesta a incidentes contratados y los reguladores.
- Diagramas de red.
- Posiblemente una copia de seguridad o volcado de la base de datos de gestión de configuración de la organización.
- Una copia del manual/flujo de trabajo de respuesta a incidentes.
- Contratos y documentos de políticas relacionados con servicios de respuesta a incidentes contratados y aseguradoras cibernéticas.
- Manuales de usuario para aplicaciones y herramientas.



Recursos para la etapa de inicio: Colaboración y comunicación.

- Es probable que sea necesaria la comunicación con partes interesadas internas y terceros externos, como las autoridades policiales, los centros de análisis y divulgación de información, las compañías de seguros, los responsables de respuesta a incidentes contratados, los reguladores, la prensa y los interesados afectados. Para establecer esta capacidad, un kit digital de emergencia podría contener lo siguiente:
  - Firmware y configuración de enrutador y conmutador conocidos para permitir una conectividad segura. Como alternativa, la organización puede mantener equipos de reserva confiables.
  - Software de firewall y configuración para restringir la entrada y salida solo a los recursos necesarios para la respuesta y recuperación (incluido el acceso a Cohesity Helios).
  - Los medios de instalación del sistema operativo base y las claves de licencia utilizadas como base para reconstruir otros sistemas, incluidos los de los entornos de investigación y mitigación.
  - Scripts de automatización y orquestación, que pueden ser cualquier cosa, desde archivos de respuesta de Windows para instalación sin supervisión, a través de libros de estrategias de Ansible, hasta infraestructura como código Terraform.
  - Software y configuración del servidor de gestión de voz sobre IP (VoIP). Es importante darse cuenta de que este no es todo el entorno VoIP de producción. Solo tiene líneas relacionadas con las actividades de respuesta y recuperación. La configuración de VoIP de producción se devolverá en línea después de la investigación y de que se haya mitigado cualquier amenaza encontrada.
  - Software y configuración del servidor de correo electrónico. Al igual que el servidor de VoIP, esta no es una capacidad de producción. Solo permite la comunicación por parte de los recursos involucrados en las actividades de respuesta y recuperación.
  - Otras herramientas de colaboración utilizadas por la organización, como la emisión de tickets, las conferencias o similares, pueden incluirse en el kit de emergencia.
  - Plantillas para la notificación del regulador y del interesado afectado.

Recursos para el entorno de la etapa de investigación

El equipo de operaciones de seguridad generalmente es propietario del entorno utilizado durante la etapa de investigación. Se centra en comprender el cronograma de ataque de extremo a extremo para que la organización pueda tomar decisiones informadas sobre la recuperación de la capacidad de producción mientras se protege de la reinfección y un nuevo ataque. Los sistemas se investigan dentro de la organización utilizando una mezcla de la capacidad de operaciones de seguridad nativa de Cohesity para realizar tareas como clasificación de datos, búsqueda de amenazas y análisis forense del sistema de archivos y por Cohesity que respalda otras herramientas de operaciones de seguridad. La caza de amenazas con Cohesity no se ve afectada por la contención de incidentes. Es pasiva, por lo que no es visible para el adversario y no está sujeta a técnicas de evasión comunes a las soluciones de seguridad de punto final. En el entorno de la etapa de investigación, los sistemas generalmente se investigan de forma aislada.

- Medios de instalación y configuraciones para software de seguridad. Esto permite la reinstalación de herramientas a un estado confiable dentro del entorno aislado de la sala segura, lo que garantiza la confianza de que las actividades de herramientas y respuesta no se evaden ni interrumpen.
- Las herramientas de seguridad se pueden volver a instalar en un estado confiable dentro de la sala segura. Esta herramienta depende en gran medida de las preferencias de su equipo de respuesta a incidentes de seguridad, pero generalmente contiene al menos algunos de los siguientes elementos:

- Las herramientas de Detección y respuesta de punto final (EDR) y Detección y respuesta extendidas (XDR) incluyen Palo Alto Networks, Cisco XDR y CrowdStrike.
- Herramientas de captura y análisis forenses como Dissect, Flare, Redline, Sleuth Kit, Autopsy, CyLR y Unix-like Artifacts Collector (UAC).
- Indicadores de compromiso y herramientas para compartir evidencia, como Cortex, Kuiper y MISP.
- Analizadores de registro de eventos como Event Log Explorer, Event Log Observer, Hayabusa, LogonTracer o Windows Event Log Analyzer (WELA).
- Escáneres de vulnerabilidad, como Qualys, Rapid7 neXpose, Tenable Nessus u OpenVAS.
- Software de análisis y captura de paquetes, como Wireshark.
- Analizadores de flujo de red/SFlow
- Captura de memoria y analizadores como Volatility, Memoryze, Orochi, Rekall y WindowsSCOPE.
- Sandboxes, ingeniería inversa de malware y herramientas de análisis, como Cuckoo, CAPA, CAPE, Ghidra, Joe Sandbox, Mastiff, Radare 2 y Valkyrie Comodo.
- Herramientas forenses del historial del navegador web como Internet History Forensics.
- Muchas de las herramientas anteriores están disponibles dentro de las distribuciones de software de seguridad, como Kali Linux y SANS Institute SIFT Workstation. Estos se pueden almacenar dentro del kit digital de emergencia en lugar de instalar cada herramienta.

Recursos para el entorno de la etapa de mitigación

El equipo de operaciones de TI generalmente es propietario del entorno de mitigación. En el entorno de mitigación, los sistemas operativos y las aplicaciones del sistema se reconstruyen a partir de medios de instalación y configuraciones confiables contenidos en el kit digital de emergencia o se recuperan de instantáneas de copia de seguridad y se limpian utilizando la información obtenida por las operaciones de seguridad durante la etapa de investigación. Se toman medidas correctivas para mitigar amenazas como parches de vulnerabilidades, la aplicación de controles o reglas faltantes para prevenir o detectar ataques futuros del mismo tipo, y se eliminan los mecanismos de persistencia, cuentas maliciosas u otros artefactos de ataque. En el entorno de mitigación, los sistemas interdependientes para entregar un producto o servicio se reúnen y reconstruyen o mitigan, hasta que finalmente se pueda probar el rendimiento y la funcionalidad restaurando los datos de una instantánea de copia de seguridad. En este momento se toma una instantánea y los sistemas se recuperan en el entorno de producción.

- Si la organización adopta un enfoque de "reconstrucción" en lugar de un enfoque de "recuperación y limpieza", el kit digital de emergencia contendrá los medios de instalación y configuraciones requeridos para la pila de aplicaciones.
- La configuración de red o hipervisor requerida para la carga de trabajo interdependiente actual. Esto permite que el entorno de mitigación replique el entorno de producción, en el que finalmente se recuperará la carga de trabajo.
- Casos de prueba para las cargas de trabajo.

Uso del kit de emergencia para establecer la capacidad mínima viable de respuesta

Cuando se utiliza el kit digital de emergencia para establecer los sistemas dentro del MVRC, un cliente tiene dos opciones: Recuperar un sistema preconstruido o reconstruir a partir de fuentes confiables.

- **Mantener la capacidad mínima viable de respuesta:** Cree los sistemas necesarios para la MVRC y realice una copia de seguridad a nivel de volumen en ellos, que se almacenan en el kit digital de emergencia. Si se sospecha de un incidente de ciberseguridad que afecta los sistemas necesarios para la respuesta y recuperación o evasión de herramientas de seguridad, se recuperan las instantáneas para establecer la capacidad mínima viable de respuesta.
- **Reconstruir a partir de los recursos en el kit digital de emergencia**: Aquí, las configuraciones confiables y las imágenes maestras de referencia para los sistemas requeridos para la MVRC se mantienen en el kit digital de emergencia. En caso de un incidente de ciberseguridad que afecte los sistemas necesarios para la respuesta y la recuperación o evasión de herramientas de seguridad, se monta el kit digital de emergencia. Estos sistemas se reconstruyen utilizando scripts o herramientas de orquestación.

Cada estrategia tiene ventajas y desventajas, descritas en la tabla a continuación:

Mantener una capacidad de respuesta viable mínima, respaldar y restaurar la instantánea después de un incidente.	
Ventajas:	**Desventajas:**
Acceso rápido a los sistemas funcionales durante la respuesta.	Los parches y las actualizaciones requieren más pasos (reconstruir, actualizar/parchar, hacer copias de seguridad), que requieren recursos continuos. Estos pasos pueden introducir errores que afectan la respuesta y la recuperación. Supongamos que una organización no ha podido mantener seguros los sistemas de TI y se ha visto afectada por el incidente. ¿Cuál es la garantía de que los sistemas de capacidad de respuesta mínima viable que se han construido y respaldado no tendrán los mismos problemas?
Capacidad de restaurar solo los componentes requeridos	Ocupa exponencialmente más espacio en el kit digital de emergencia, lo que incurre en costos de licencia.
	Es posible que deba actualizarse y parcharse durante una respuesta, lo que causa demoras.
	Puede introducir dependencias de infraestructura.
Requisitos:	
Realizar correctamente la prueba de creación de MVRC desde el kit digital de emergencia.	
Realizar una copia de seguridad de MVRC, permitir la retención legal para preservarla con fines legales, replicarla y archivarla fuera del sitio.	

Reconstruir la capacidad mínima viable de respuesta de fuentes confiables después de un incidente.	
Ventajas:	**Desventajas:**
Relativamente fácil de mantener fuentes, como cuando hay una nueva versión de un sistema operativo, aplicación o configuración, esto simplemente se exporta al kit de emergencia.	Requiere tiempo para reconstruir la infraestructura.
Muy portátil a través de replicación y archivo.	
Más adaptable a los cambios de hardware y plataforma.	
La huella de respaldo en el kit digital de emergencia es significativamente menor (es decir, una imagen de Windows Server 2025 es de alrededor de 3,6 GB y puede compartirse entre diferentes sistemas, mientras que cada servidor en la Capacidad de respuesta viable mínima que utilizó esa imagen requeriría alrededor de 35 GB).	
Requisitos:	
Establecer un proceso para completar y actualizar el kit digital de emergencia.	
Practicar diferentes escenarios de uso del contenido.	
Tener el hardware necesario a mano o definir un proceso para limpiar de forma segura el hardware existente.	

Conclusión

Ante los ataques cibernéticos cada vez más sofisticados y destructivos, las organizaciones deben pasar de la recuperación reactiva a la resiliencia estratégica. Esto implica integrar un kit digital de emergencia integral en su estrategia de respuesta a incidentes para estar mejor posicionada para responder rápidamente a los ciberataques. Un kit digital de emergencia bien preparado habilita la MVRC y sirve como base para una sala segura, equipando a los equipos de seguridad con las herramientas, los procesos y la documentación esenciales necesarios para investigar incidentes, contener amenazas y restaurar las operaciones con una interrupción mínima.

La solución Cohesity Clean Room proporciona un entorno confiable que acelera la respuesta a incidentes y respalda las investigaciones mientras minimiza el riesgo de ataques secundarios.

Gracias a un diseño modular, Cohesity crea rápidamente un entorno aislado, apoyando el proceso de respuesta y recuperación y permitiendo a los equipos colaborar en la mitigación de amenazas más rápidamente.

Acerca de Cohesity

Cohesity es el líder en seguridad de datos impulsada por IA. Más de 12 000 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 compañía 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 su sede central en San José, California, con oficinas en todo el mundo. Para obtener más información, siga Cohesity en **LinkedIn**, **X** y **Facebook**.

Descubra cómo Cohesity puede acelerar su camino hacia la seguridad de datos moderna en **www.cohesity.com**.

Lectura recomendada

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

- Desarrollar resiliencia cibernética en un mundo de ciberataques destructivos
- Topologías modernas de seguridad y gestión de datos: Una guía para líderes de TI
- Presentamos el diseño de sala segura 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

Más información en Cohesity

COHESITY

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

2000056-002-EN 4-2025