COHESITY

ARTIGO TÉCNICO

Melhore a resiliência cibernética com uma digital jump bag™

Como restabelecer rapidamente um recurso de resposta mínimo viável e fortalecer a resposta a incidentes

ÍNDICE

Prefácio

James Blake
vice-presidente de resiliência cibernética estratégica

Há mais de 30 anos, estou na linha de frente da resposta cibernética a ataques destrutivos e roubo de dados. Minha experiência vai desde a condução de respostas a incidentes diante de ataques wiper a países até a liderança em gestão de riscos cibernéticos no maior banco do mundo.

Durante esse período, aprendi o valor de ter uma "jump bag". O termo originalmente se referia a um contêiner físico que armazenava hardware e software essenciais, pronto para ser levado até um local físico que havia sofrido um ataque. Essa jump bag continha o necessário para investigar rapidamente o incidente, coletar evidências e mitigar ameaças. Além de hardware e software, ela incluía itens como listas de contatos impressas de partes interessadas internas e externas, o plano para gestão de crises, fluxos de trabalho para os tipos de incidentes mais prováveis e, até mesmo, um telefone celular. A ideia era estar preparado para responder imediatamente, pois correr atrás de tudo o que é necessário em meio à pressão de um incidente consome um tempo valioso e pode fazer esquecer algo essencial. A jump bag reunia uma combinação de ferramentas, detalhes de processos e um método para permitir a comunicação.

Hoje vivemos em um mundo de aquisição remota, detecção e resposta avançada em endpoints (EDR/XDR), máquinas virtuais e instâncias em nuvem. As jump bags ainda podem ser contêineres físicos que levamos ao local. Mas agora, a maior utilidade está em preparar uma digital jump bag™. Esse repositório seguro e confiável garante acesso rápido não apenas às ferramentas necessárias para aquisição e análise remota, mas também a outros ativos digitais indispensáveis para um desfecho positivo durante a resposta e recuperação de incidentes.

Resumo executivo

A digital jump bag™ é a base da Sala limpa Cohesity: um ambiente seguro e isolado onde a equipe de operações de segurança pode realizar as etapas de investigação necessárias para entender como ocorreu um ataque. Esse mesmo espaço também é usado para executar medidas corretivas antes da recuperação, erradicar a ameaça e ajudar a evitar recorrências. O que compõe uma digital jump bag depende da maturidade, estrutura, processos e ferramentas de cada organização.

Em sua essência, a jump bag permite que uma organização restaure rapidamente o recurso de resposta mínimo viável (Minimum Viable Response Capability, MVRC), um conjunto simplificado de ferramentas, documentos e processos essenciais para responder de forma eficaz a um ataque cibernético. O MVRC garante que as organizações possam conter violações rapidamente, restaurar operações críticas e reduzir ao mínimo o tempo de inatividade durante um incidente cibernético.

A **Sala limpa Cohesity** apoia essa abordagem moderna para ajudar as organizações a combater ataques cibernéticos destrutivos. Ela oferece flexibilidade para se adaptar a diferentes necessidades e apoia a melhoria contínua do recurso operacional de resiliência cibernética ao longo do tempo.

Neste artigo técnico, recomendaremos o que as organizações devem considerar incluir na sua digital jump bag ao elaborarem uma estratégia de resposta a incidentes mais robusta e ágil.

Problemas frequentemente negligenciados na resiliência cibernética

Muitas vezes, os ataques cibernéticos destrutivos envolvem a evasão das ferramentas de segurança usadas dentro da organização atingida, com recursos de evasão EDR/XDR incorporados em muitas das plataformas mais comuns de ransomware como serviço (Ransomware-as-a-Service, RaaS), que são responsáveis pela grande maioria dos ataques de ransomware que vemos atualmente. Por sua própria natureza, as soluções EDR/XDR atuam no endpoint e, quando não são contornadas, oferecem excelente visibilidade de processos, conexões de rede e sistemas de arquivos.

As melhores práticas de resposta a incidentes, como o ciclo de resposta em seis etapas do SANS Institute, o Guia de Gestão de Incidentes de Segurança da Informação NIST SP800-61, a estrutura RE&CT e o MITRE D3FEND, recomendam conter a propagação de um incidente por meio do isolamento de redes e hosts infectados. No mundo do controle de endpoints, na melhor das hipóteses, isso deixa uma organização apenas com as informações já coletadas para investigar o incidente.

No entanto, ao enfrentar um criminoso que se adapta constantemente, nem sempre sabemos quais informações precisamos coletar para entender um ataque com antecedência. Podemos ficar sem o recurso real de investigação e resposta, deixando-nos sem clareza sobre a situação. Da mesma forma, a aquisição remota de imagens forenses de volumes em um host impactado torna-se impossível se a conectividade for interrompida.

Além das ferramentas de segurança, muitos outros sistemas estão envolvidos nas fases de investigação, mitigação e recuperação de um incidente. Esses sistemas podem ser impactados por ataques cibernéticos destrutivos, como ransomware e wipers, mas ainda assim são frequentemente negligenciados, apesar de serem críticos em muitas análises de impacto nos negócios. Já participei de incidentes em que as equipes de resposta não conseguiram entrar nos prédios porque os controles de acesso físico haviam sido comprometidos. Muitas organizações acabam não conseguindo se comunicar com a imprensa, órgãos reguladores, autoridades policiais, seguradoras cibernéticas ou, até mesmo, com as pessoas afetadas por incidentes, já que servidores de voz sobre IP e de e-mail podem ser atingidos. Muitos exercícios de simulação de ransomware realizados por empresas não conseguem capturar de forma adequada esses impactos criados pelas técnicas direcionadas dos invasores. No fim das contas, os invasores querem garantir que as organizações tenham dificuldade para responder e se recuperar de incidentes.

Com plataformas de RaaS explorando vulnerabilidades recém-corrigidas em apenas cinco dias, precisamos identificar essas falhas nos sistemas e aplicar patches antes de colocá-los novamente em produção. Caso contrário, o mesmo invasor ou outro afiliado que utilize a mesma plataforma de RaaS pode retomar o ataque.

Também precisamos identificar o vetor inicial de acesso, que mostra qual foi o primeiro sistema impactado, o chamado "ponto inicial da infecção", e a partir dele acompanhar a evolução do incidente. Entender como o criminoso mantém persistência, aumenta os privilégios e espalha outros elementos do ataque é essencial para garantir que qualquer recuperação devolva o ambiente a um estado seguro. As equipes de resposta também precisam compreender a natureza de todos os dados que possam ter sido comprometidos, a fim de cumprir as obrigações regulatórias de notificação.

Apenas analisar sistemas criptografados não é suficiente. Normalmente, grupos de ransomware acionam a criptografia no final do ciclo do ataque, nos últimos minutos ou horas, depois de permanecerem ocultos

na infraestrutura por dias ou até meses. A criptografia provoca grande volume de atividades detectáveis e tende a disparar controles de segurança e mecanismos de alerta dos usuários. Quando se chega a esse ponto, já é tarde demais. Essa necessidade de priorizar a velocidade é uma das razões pelas quais os programas de criptografia, muitas vezes, não são projetados para manter a integridade, resultando em grandes volumes de perda de dados mesmo entre aqueles que pagam o resgate para obter as chaves de descriptografia. Restringir o escopo apenas a sistemas criptografados, sem identificar como o invasor entrou e continua ativo dentro da rede, é uma receita para o desastre.

As organizações que adotam essa abordagem frequentemente se veem obrigadas a recuperar os sistemas dezenas de vezes, apenas para serem infectadas repetidamente. Esse ciclo vicioso só pode ser interrompido investigando adequadamente o incidente e utilizando os insights obtidos para corrigir as ameaças.

Basta se perguntar: como teria sido o resultado do seu último exercício de simulação se você tivesse ficado sem telefone ou e-mail, tivesse sido impedido de entrar nos prédios e não tivesse acesso aos sistemas de identidade e de gestão de acessos logo no início do incidente?

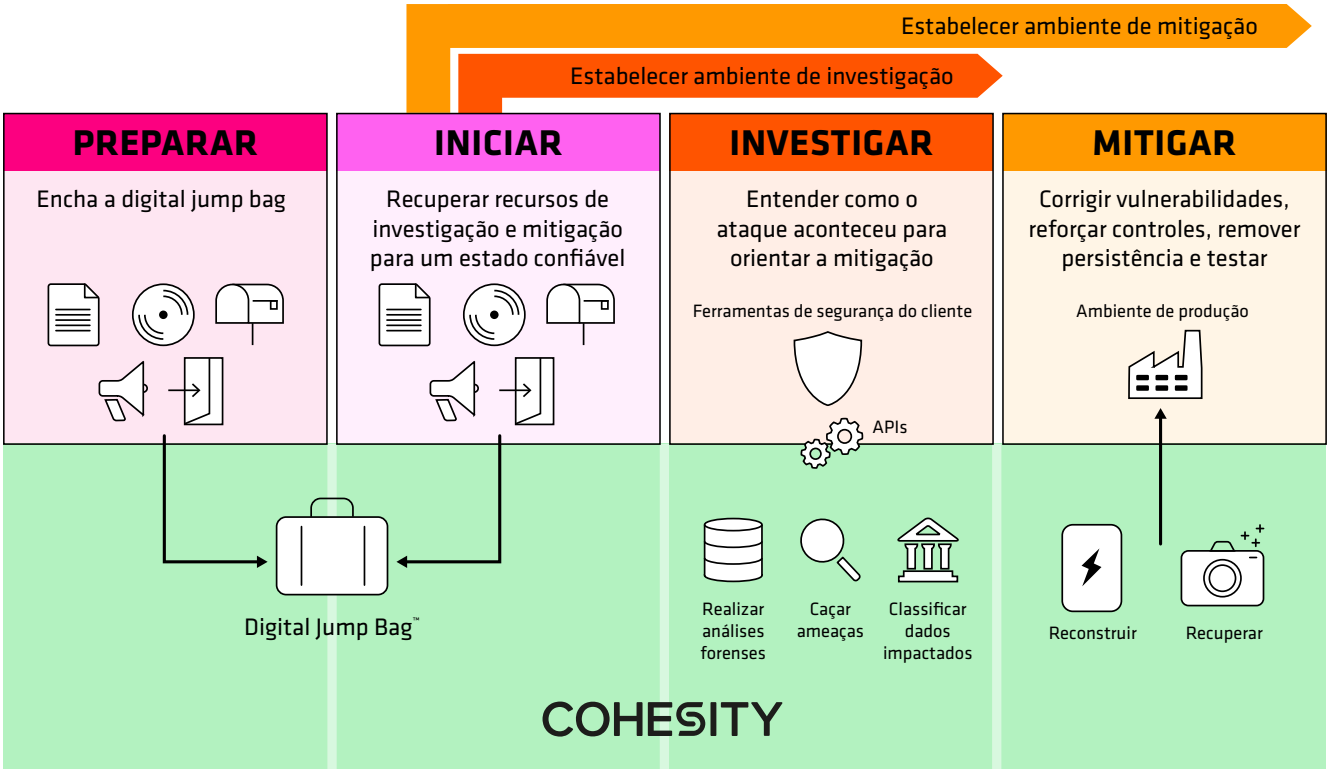
Como a digital jump bag se integra à solução Sala limpa Cohesity

A digital jump bag é a base de toda solução Sala limpa Cohesity, apoiando as etapas críticas de resposta e recuperação de incidentes para permitir que os dados íntegros sejam restaurados em produção.

Vamos analisar o que acontece em cada uma dessas etapas.

Preparar

Nesta fase, definimos o que deve compor a digital jump bag, como configurações de rede ou de hipervisores que sustentam camadas de sistemas interdependentes que seriam restaurados no ambiente de mitigação. Consulte a seção "Quais são os possíveis componentes da sua digital jump bag?" para sugestões que possibilitam as etapas seguintes.



Iniciar

Nesta etapa, recuperamos a MVRC, onde as ferramentas necessárias para comunicação, colaboração e investigação de incidentes são restauradas a partir da digital jump bag para um estado confiável dentro do ambiente isolado da sala limpa. A digital jump bag também estabelece os ambientes de investigação e mitigação.

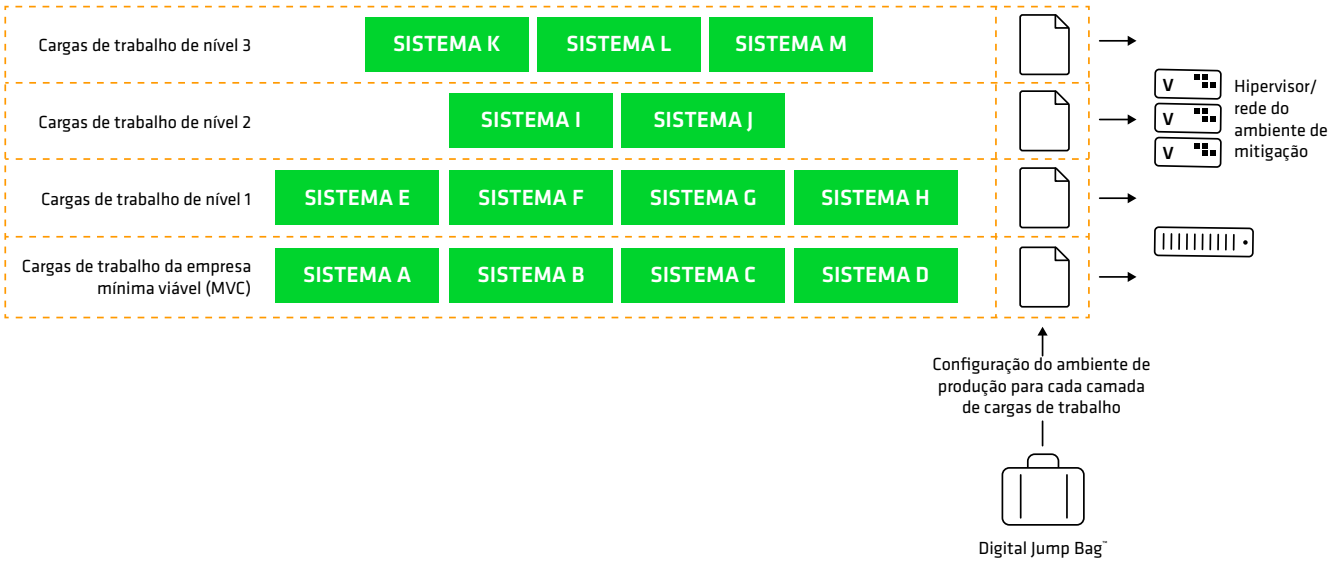
Investigar

As equipes de segurança utilizam as ferramentas recuperadas em um espaço confiável dentro do sala limpa isolada, junto com os recursos nativos da Cohesity para classificação de dados, caça a ameaças e análise forense de sistemas de arquivos, de forma a compreender todo o incidente de ponta a ponta. À medida que as ferramentas de segurança são restauradas para um estado confiável dentro da sala limpa, as capacidades de segurança da Cohesity não ficam sujeitas às técnicas de evasão usadas contra controles de endpoint. Assim, os desafios de evasão e isolamento, comuns durante a contenção, são superados. O Data Security Alliance da Cohesity oferece um conjunto abrangente de ferramentas de fornecedores de segurança, já integradas aos meus centros de operações de Segurança, que estão pré-configurados para trabalhar em conjunto com as soluções da Cohesity.

Mitigar

As equipes de TI utilizam as descobertas da equipe de operações de segurança sobre o incidente para decidir entre recuperar e depois limpar, ou reconstruir os sistemas diretamente para um estado confiável. Enquanto a fase de investigação não envolve a recuperação completa de sistemas interdependentes, a fase de mitigação abrange exatamente esse ponto.

Muitos clientes reutilizam seus ambientes de desenvolvimento como ambiente de mitigação durante a recuperação de incidentes. Os sistemas interdependentes são restaurados no ambiente de mitigação com configurações de rede que correspondem aos ambientes de produção. Essas configurações de rede ou de hipervisor são armazenadas para cada camada de sistemas interdependentes na digital jump bag. Isso é mostrado abaixo.



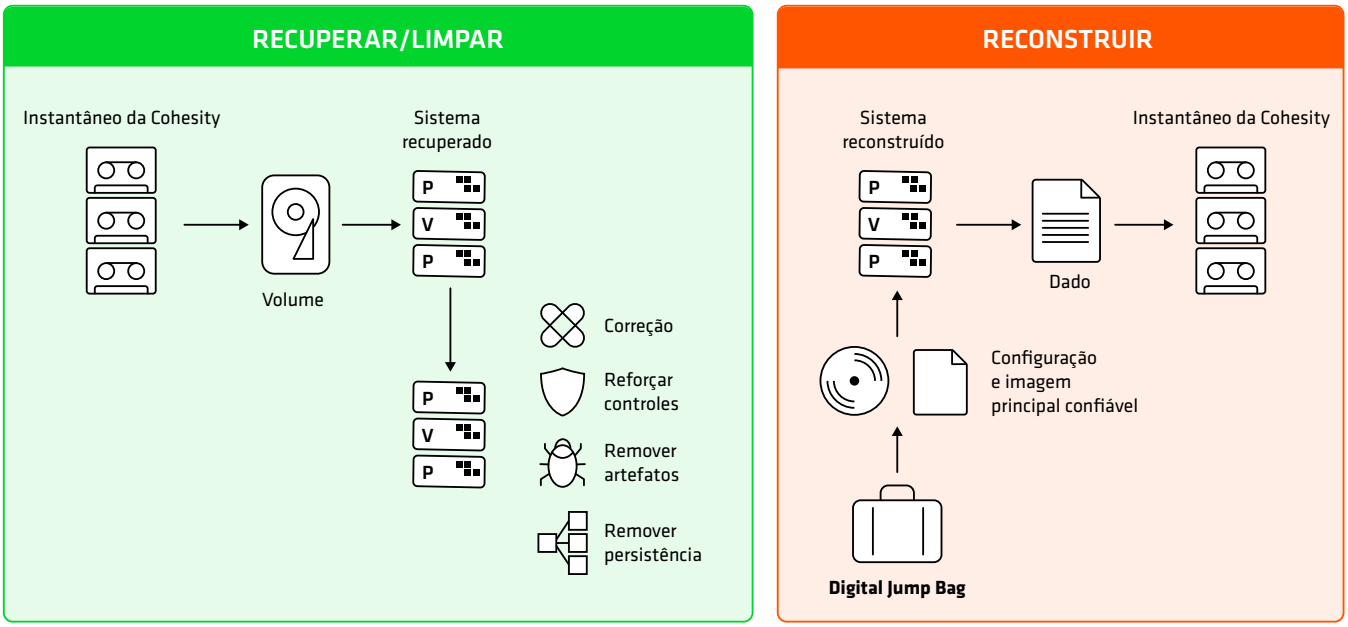
Alinhamento da Sala limpa Cohesity às melhores práticas de resposta a incidentes.

Com a Sala limpa Cohesity, a estratégia de "recuperar e limpar" ou "reconstruir para um estado confiável" pode ser aplicada de forma universal ou definida sistema a sistema durante um incidente, de acordo com o nível de esforço de remediação e o risco residual das ameaças. Vamos analisar uma breve descrição de cada opção:

- **Recuperar e limpar**: Os sistemas são recuperados a partir de seus instantâneos, e as etapas de mitigação definidas pela equipe de operações de segurança em sua fase de investigação são aplicadas. Como os dados normalmente não são usados para transportar cargas maliciosas, a recuperação pode ocorrer em paralelo à reconstrução do sistema, reduzindo ainda mais o tempo total de restauração.
- **Reconstruir sistemas para um estado confiável**: A digital jump bag conterá configurações reconhecidas como boas, scripts de instalação e imagens de referência de instalação. Uma vez reconstruídos, os dados serão recuperados a partir dos instantâneos nos sistemas restaurados.

A seção "Usando a jump bag para estabelecer o recurso de resposta mínimo viável" detalha a comparação entre cada abordagem.

Ter um ambiente que atenda às necessidades de investigação da equipe de operações de segurança e, ao mesmo tempo, permita que a equipe de TI garanta que a recuperação leve a um estado seguro por meio de mitigações, ajuda as organizações a alcançar um modelo de responsabilidade compartilhada adequado e eficaz para a resiliência cibernética. Essa abordagem otimiza a velocidade da recuperação segura, garantindo que os recursos de TI e de segurança possam ser totalmente aproveitados.



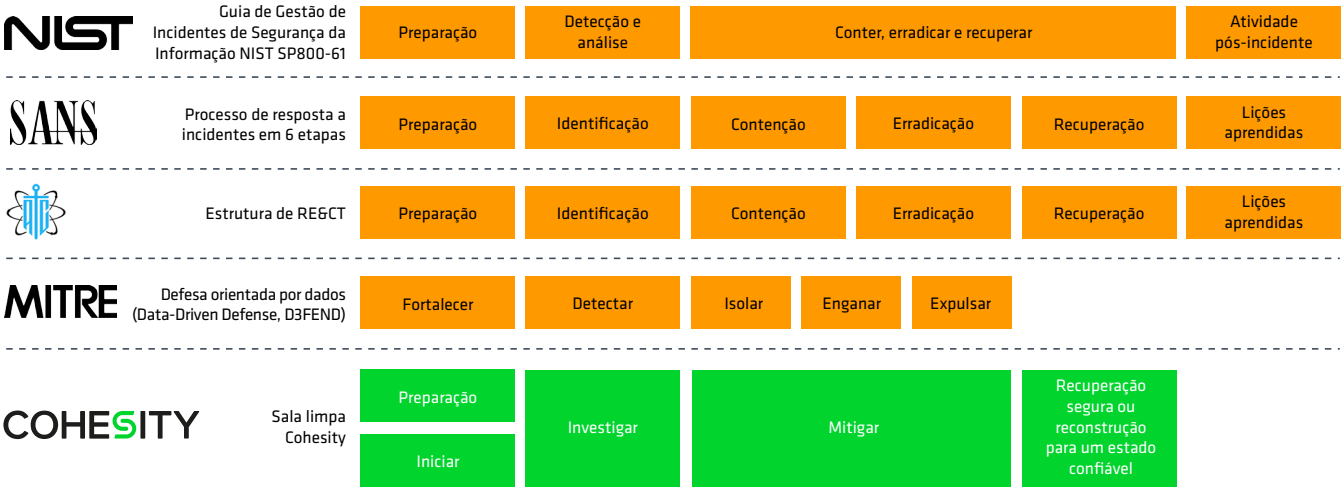
A Sala limpa Cohesity oferece aos clientes a opção de recuperar e limpar cargas de trabalho ou reconstruí-las rapidamente para um estado confiável.

Uma vez que os sistemas tenham sido reconstruídos ou recuperados, testes funcionais e de desempenho podem ser realizados nesse nível de carga de trabalho. Um instantâneo é criado e, em seguida, toda a carga de trabalho interdependente é restaurada em produção com segurança, na certeza de que o incidente foi completamente investigado, as ameaças mitigadas e o desempenho e a funcionalidade foram restabelecidos.

Esses casos de teste podem ser armazenados na digital jump bag para cada nível de cargas de trabalho interdependentes. Se algo tiver sido perdido durante a investigação e a mitigação, não é necessário voltar ao ponto inicial, pois o instantâneo feito no final da fase de mitigação pode ser usado como base para novas etapas de investigação e mitigação.

Como a Sala limpa Cohesity se alinha às melhores práticas de resposta a incidentes

A digital jump bag da Cohesity e o recurso de resposta mínimo viável estão em conformidade com as melhores práticas de resposta a incidentes definidas pelo SANS Institute, no Guia de Gestão de Incidentes de Segurança da Informação NIST SP800-61, pela estrutura RE&CT e pelo MITRE D3FEND. Com essa abordagem, organizações que já seguem essas metodologias podem facilmente integrar a solução Sala limpa Cohesity em seus fluxos de trabalho existentes. Os clientes que buscam aprimorar sua resposta a incidentes e a maturidade de recuperação podem adotar a Sala limpa Cohesity para operacionalizar essas melhores práticas.



Alinhamento da Sala limpa Cohesity às melhores práticas de resposta a incidentes

Unindo segurança e operações de TI para fortalecer a resiliência

A resiliência cibernética é um esforço coletivo: não pode ser alcançada apenas pelas operações de TI de forma isolada, nem pelas equipes de segurança agindo sozinhas. Ambas as equipes precisam ter processos integrados e ferramentas complementares. Da mesma forma, nenhum fornecedor isolado consegue entregar resiliência cibernética. A solução Sala limpa Cohesity foi projetada para permitir que a equipe de segurança lidere e assuma o controle do ambiente de investigação, enquanto a equipe de TI gerencia e utiliza o ambiente de mitigação. Essa divisão de responsabilidades entre as equipes ajuda a garantir um modelo claro de responsabilidade compartilhada e minimiza a chance de que atividades importantes sejam esquecidas. A capacidade de reverter iterativamente instantâneos já mitigados de volta à fase de investigação significa que, se algum aspecto do ataque não for identificado durante a investigação ou a mitigação iniciais, não é preciso recomeçar do zero. Isso reduz o tempo de investigação e acelera a recuperação final.

Assim que a equipe de segurança conclui a investigação de uma carga de trabalho no ambiente de investigação, ela pode repassá-la para a equipe de TI, que assume o controle do ambiente de mitigação para reconstrução, recuperação e limpeza. Isso garante o uso mais eficiente dos recursos de operações de TI e segurança.

Responder mais rápido, recuperar com mais inteligência: Cohesity CERT (Equipe de resposta a eventos cibernéticos)

Muitas organizações não dispõem de conhecimento técnico nem de recursos suficientes para uma resposta cibernética eficaz. Para reduzir o impacto, aprimoramos nossa solução de segurança de dados de classe mundial com um serviço dedicado da Equipe de Resposta a Eventos Cibernéticos (Cyber Event Response Team, CERT).

O Cohesity CERT oferece recuperação rápida liderada por especialistas contra invasores cibernéticos, garantindo que seus dados sejam restaurados e que sua empresa retome as operações com tempo de inatividade mínimo.

O Cohesity CERT está disponível para todos os clientes como parte de sua assinatura da Cohesity.

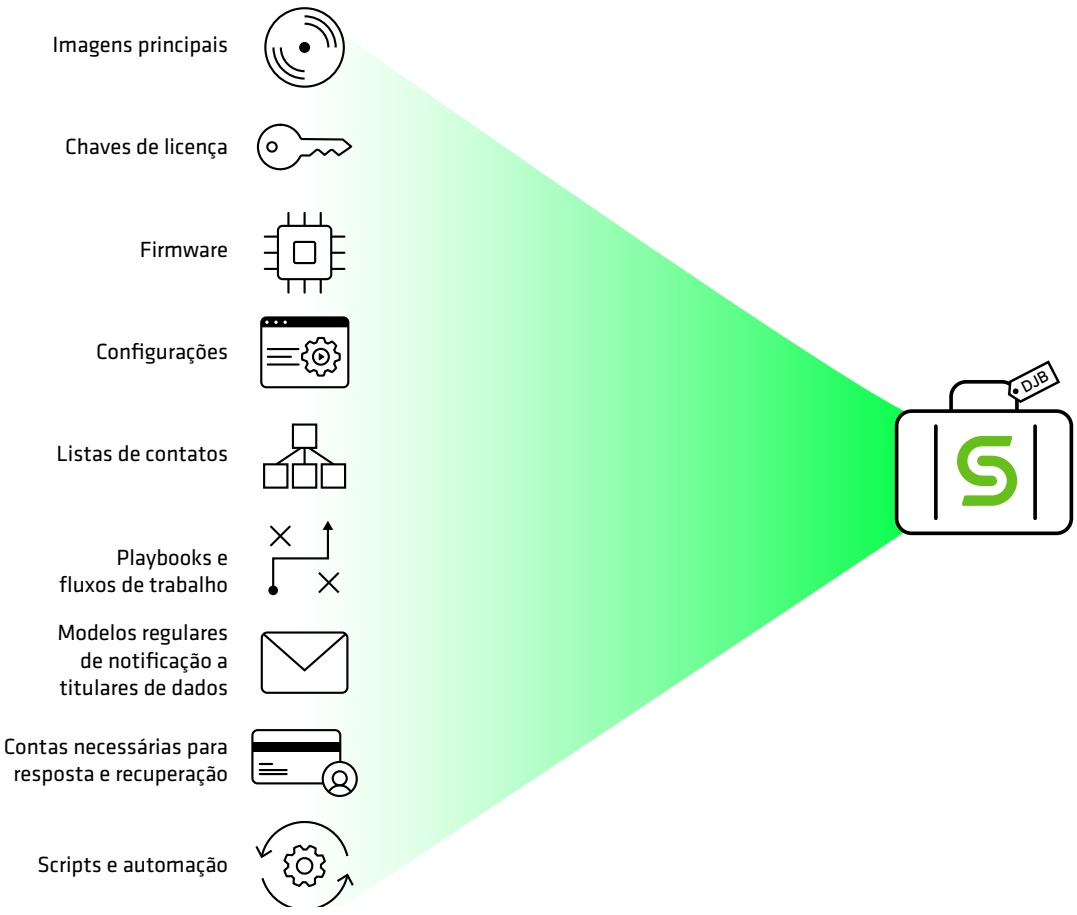
Quais são os possíveis componentes da sua digital jump bag?

O conteúdo da sua digital jump bag depende da sua estratégia individual de triagem, investigação e mitigação, além das ferramentas utilizadas para atingir esses objetivos.

Em geral, identificamos os seguintes itens como comumente incluídos nas jump bags digitais dos clientes:

Documentação

- Uma lista de contatos que inclua partes interessadas internas e entidades externas, como autoridades policiais, centros de compartilhamento e análise de informações, seguradoras cibernéticas, prestadores de serviços de resposta a incidentes e órgãos reguladores.
- Diagramas de rede.
- Opcionalmente, um backup ou exportação do banco de dados de gestão de configuração da organização.
- Uma cópia do guia de resposta a incidentes ou do fluxo de trabalho.
- Contratos e documentos de políticas relacionados a serviços de resposta a incidentes contratados e seguradoras cibernéticas.
- Manuais de usuário para aplicativos e ferramentas.



Recursos para a fase de Iniciação: Colaboração e comunicação

- É provável que seja necessário garantir a comunicação com partes interessadas internas e terceiros externos, como autoridades policiais, centros de compartilhamento e análise de informações, seguradoras cibernéticas, prestadores de serviços de resposta a incidentes, órgãos reguladores, a imprensa e pessoas afetadas por incidentes de dados. Para viabilizar esse recurso, uma digital jump bag pode conter os seguintes itens:
  - Firmware e configuração confiáveis de roteadores e switches, permitindo conectividade segura. Outra opção é que a organização mantenha equipamentos de reserva confiáveis.
  - Software e configuração de firewall para restringir entradas e saídas apenas aos recursos necessários para resposta e recuperação (incluindo acesso ao Helios da Cohesity).
  - Mídia de instalação do sistema operacional básico e chaves de licença utilizadas como base para reconstruir outros sistemas, inclusive nos ambientes de Investigação e Mitigação.
  - Scripts de automação e coordenação, que podem incluir desde arquivos de resposta do Windows para instalação automatizada, passando por playbooks do Ansible até o Terraform, como Infraestrutura como Código.
  - Software e configuração de servidor de gestão de voz sobre IP (VoIP). É importante entender que isso não representa todo o ambiente de VoIP em produção. Ele inclui apenas linhas relacionadas a atividades de resposta e recuperação. A configuração de VoIP em produção será restaurada após a investigação e depois que todas as ameaças identificadas tiverem sido mitigadas.
  - Software e configuração de servidor de e-mail. Assim como no caso do VoIP, não se trata de um recurso de produção. Ele apenas possibilita a comunicação entre os recursos envolvidos nas atividades de resposta e recuperação.
  - Outras ferramentas de colaboração utilizadas pela organização, como sistemas de chamados, conferência ou similares, podem ser incluídas na jump bag.
  - Modelos para notificações a órgãos reguladores e a titulares de dados impactados.

Recursos para o ambiente da fase de investigação

A equipe de operações de segurança geralmente é a responsável pelo ambiente usado na fase de investigação. O foco está em compreender toda a linha do tempo do ataque, permitindo que a organização tome decisões informadas sobre a restauração segura dos recursos de produção, ao mesmo tempo em que protege contra reinfecção e novos ataques. Os sistemas são investigados dentro da organização usando uma combinação da capacidade dos recursos nativos de segurança da Cohesity de executar tarefas como classificação de dados, caça a ameaças, análise forense de sistemas de arquivos, além de outras ferramentas de operações de segurança compatíveis com a Cohesity. A caça a ameaças com a Cohesity não é impactada pelo processo de contenção de incidentes. Ela é passiva, portanto não fica visível para o invasor e não está sujeita às técnicas de evasão comuns aplicadas a soluções de segurança de endpoint. No ambiente da fase de Investigação, os sistemas geralmente são analisados de forma isolada.

- Mídia de instalação e configurações para softwares de segurança. Isso permite a reinstalação das ferramentas em um estado confiável dentro do ambiente isolado da sala limpa, garantindo que os recursos e as atividades de resposta não sejam comprometidos nem interrompidos.
- As ferramentas de segurança podem ser reinstaladas em um estado confiável dentro da sala limpa. Esse conjunto de ferramentas depende bastante das preferências da equipe de resposta a incidentes de segurança, mas normalmente inclui pelo menos alguns dos seguintes itens:
  - Soluções de Detecção e Resposta em Endpoint (Endpoint Detection and Response, EDR) e de Detecção e Resposta Estendidas (Extended Detection and Response, XDR), como Palo Alto Networks, Cisco XDR e CrowdStrike.

- Ferramentas de captura e análise forense, como Dissect, Flare, Redline, Sleuth Kit, Autopsy, CyLR e Coletor de Artefatos Unix-like (Unix-like Artifacts Collector, UAC).
- Ferramentas de indicadores de comprometimento e de compartilhamento de evidências, como Cortex, Kuiper e MISP.
- Analisadores de registros de eventos, como Event Log Explorer, Event Log Observer, Hayabusa, LogonTracer ou Analisador de Logs de Eventos do Windows (Windows Event Log Analyzer, WELA).
- Verificadores de vulnerabilidade, como Qualys, Rapid7 Nexpose, Tenable Nessus ou OpenVAS.
- Softwares de captura e análise de pacotes, como Wireshark.
- Analisadores de Netflow/SFflow.
- Ferramentas de captura e análise de memória, como Volatility, Memoryze, Orochi, Rekall e WindowsSCOPE.
- Sandboxes e ferramentas de engenharia reversa de malware e análise, como Cuckoo, CAPA, CAPE, Ghidra, Joe Sandbox, Mastiff, Radare 2 e Valkyrie Comodo.
- Ferramentas de análise forense de histórico de navegadores, como Internet History Forensics.
- Muitas dessas ferramentas estão disponíveis em distribuições de software de segurança, como Kali Linux e SANS Institute SIFT Workstation. Elas podem ser armazenadas dentro da digital jump bag em vez de instaladas uma a uma.

Recursos para o ambiente da fase de mitigação

A equipe de operações de TI geralmente é a responsável pelo ambiente de mitigação. Nesse ambiente, sistemas operacionais e aplicativos são reconstruídos a partir de mídias de instalação confiáveis e configurações contidas na digital jump bag ou são recuperados de instantâneos de backup e limpos com base nas informações coletadas pela equipe de segurança durante a fase de Investigação. São aplicadas ações corretivas para mitigar ameaças, como a aplicação de patches em vulnerabilidades, a implementação de controles ou regras que previnam ou detectem ataques futuros semelhantes e a remoção de mecanismos de persistência, contas maliciosas ou outros artefatos de ataque. No ambiente de Mitigação, sistemas interdependentes necessários para entregar um produto ou serviço são reunidos e reconstruídos, ou mitigados, até que o desempenho e a funcionalidade sejam totalmente restaurados. Eles podem ser testados restaurando dados a partir de um instantâneo de backup. Um instantâneo é criado nesse ponto, e os sistemas são reintegrados ao ambiente de produção.

- Se a organização optar por uma "reconstrução" em vez de uma abordagem de "recuperar e limpar", a digital jump bag conterá a mídia de instalação e as configurações necessárias para a pilha de aplicativos.
- A configuração de rede ou hipervisor exigida para a carga de trabalho interdependente atual também deve estar disponível. Isso permite que o ambiente de mitigação replique o ambiente de produção, para o qual a carga de trabalho será finalmente recuperada.
- Casos de teste para as cargas de trabalho

Usando a jump bag para estabelecer o recurso de resposta mínimo viável

Ao usar a digital jump bag para configurar os sistemas dentro da MVRC, o cliente tem duas opções: Recuperar um sistema pré-construído ou reconstruí-lo a partir de fontes confiáveis.

- **Manter o recurso de resposta mínimo viável:** Construa os sistemas necessários para a MVRC e realize um backup por volume, que esteja armazenado na digital jump bag. Se houver suspeita de que um incidente de segurança cibernética impactou sistemas necessários para resposta e recuperação, ou que ocorreu evasão das ferramentas de segurança, os instantâneos são recuperados para estabelecer o recurso de resposta mínimo viável.
- **Reconstruir a partir dos recursos na digital jump bag**: Aqui, configurações confiáveis e imagens principais confiáveis para os sistemas necessários à MVRC são mantidas na digital jump bag. Em caso de incidente de segurança cibernética que afete sistemas críticos para resposta e recuperação, ou de suspeita de evasão das ferramentas de segurança, a digital jump bag é montada. Esses sistemas são reconstruídos usando scripts ou ferramentas de coordenação.

Cada estratégia possui vantagens e desvantagens, descritas na tabela a seguir:

Manter um recurso de resposta mínimo viável, fazer backup e restaurar o instantâneo após um incidente.	
Prós:	**Contras:**
Acesso rápido a sistemas funcionais durante a resposta.	Correções e atualizações exigem mais etapas (reconstrução, atualização/correção, backup), o que demanda recursos contínuos. Essas etapas podem introduzir erros que afetam a resposta e a recuperação. Suponha que uma organização não tenha conseguido manter seus sistemas de TI seguros e tenha sido impactada pelo incidente. Qual é a garantia de que os sistemas do recurso de resposta mínimo viável que foram construídos e armazenados em backup não apresentarão os mesmos problemas?
Capacidade de restaurar apenas os componentes necessários	Ocupa exponencialmente mais espaço na digital jump bag, gerando custos de licenciamento.
	Pode precisar ser atualizado e corrigido durante a resposta, causando atrasos
	Pode introduzir dependências de infraestrutura
Requisitos:	
Realizar com sucesso um teste de construção da MVRC a partir da digital jump bag	
Fazer backup da MVRC, habilitar retenção legal para preservá-la para fins jurídicos, replicá-la e arquivá-la fora do ambiente principal	

Reconstruir o recurso de resposta mínimo viável a partir de fontes confiáveis após um incidente.	
Prós:	**Contras:**
Relativamente fácil de manter as fontes, por exemplo, quando há uma nova versão de um sistema operacional, aplicativo ou configuração, basta exportá-la para a jump bag.	Exige tempo para reconstruir a infraestrutura
Muito portátil por meio de replicação e arquivamento	
Mais adaptável a mudanças de hardware e de plataforma	
A área de armazenamento do backup na digital jump bag é significativamente menor (por exemplo, uma imagem do Windows Server 2025 ocupa cerca de 3,6 GB e pode ser compartilhada entre diferentes sistemas, enquanto cada servidor com o recurso de resposta mínimo viável que utilizasse essa imagem precisaria de cerca de 35 GB).	
Requisitos:	
Estabelecer um processo para encher e atualizar a digital jump bag	
Praticar diferentes cenários de uso do conteúdo	
Manter o hardware necessário disponível ou definir um processo para limpar de forma segura o hardware existente	

Conclusão

Diante de ataques cibernéticos cada vez mais sofisticados e destrutivos, as organizações precisam avançar da recuperação reativa para a resiliência estratégica. Isso significa integrar uma digital jump bag abrangente em sua estratégia de resposta a incidentes, garantindo melhor preparação para reagir rapidamente a ataques cibernéticos. Uma digital jump bag bem estruturada viabiliza a MVRC e serve como a base de uma sala limpa, fornecendo às equipes de segurança as ferramentas, os processos e a documentação essenciais para investigar incidentes, conter ameaças e restaurar operações com mínima interrupção.

A solução Sala limpa Cohesity oferece um ambiente confiável que acelera a resposta a incidentes e dá suporte às investigações, ao mesmo tempo em que reduz o risco de ataques secundários.

Graças a um design modular, a Cohesity cria rapidamente um ambiente isolado, apoiando o processo de resposta e recuperação e permitindo que as equipes colaborem na mitigação de ameaças de forma mais ágil.

Sobre a Cohesity

A **Cohesity** é líder em segurança de dados com tecnologia de inteligência artificial. Mais de 12 mil clientes corporativos, incluindo mais de 85 das empresas da Fortune 100 e quase 70% das empresas da Global 500, confiam na Cohesity para fortalecer sua resiliência e, ao mesmo tempo, fornecer insights de IA generativa em suas vastas quantidades de dados. Formada a partir da combinação da Cohesity com o negócio de proteção de dados corporativos da Veritas, as soluções da empresa protegem os dados no local, na nuvem e na borda. Com o apoio da NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud e outros, a Cohesity tem sede em San Jose, Califórnia, EUA, e escritórios em todo o mundo. Para saber mais, siga a Cohesity no **LinkedIn**, no **X** e no **Facebook**.

Saiba como a Cohesity pode acelerar sua jornada para a segurança de dados moderna em **www.cohesity.com**.

Leitura recomendada

Acreditamos que você achará úteis os seguintes artigos técnicos, guias e blogs.

- Construindo resiliência contra ataques cibernéticos em um mundo de ameaças destrutivas
- Topologias modernas de segurança e gestão de dados: Um guia para líderes de TI
- Introdução ao design da Sala limpa Cohesity
- Um guia de campo para segurança de dados com IA: Como gerar resultados revolucionários para os negócios
- Um guia para executivos sobre segurança e gestão moderna de dados

Saiba mais sobre a Cohesity

COHESITY

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

2000056-002-EN 4-2025