COHESITY

ARTIGO TÉCNICO

Como formular uma estratégia de resposta “em tempos de guerra” para ataques cibernéticos destrutivos

Recupere-se de ransomware e outras ameaças cibernéticas com segurança e rapidez com a Cohesity

CONTEÚDO

Resumo executivo

Os ataques cibernéticos destrutivos, como ransomware e ataques de wipers, exigem uma abordagem diferente das operações de TI, em comparação com os cenários tradicionais de continuidade de negócios e recuperação de desastres. As equipes de operações de segurança cibernética enfrentam vários desafios para garantir que investigações apropriadas e correções de ameaças sejam realizadas. Não basta apenas restaurar a entrega de seus produtos e serviços o mais rápido possível. As organizações também precisam garantir que a recuperação seja feita com segurança para evitar mais tempo de inatividade devido a uma reinfecção ou um novo ataque.

Este relatório técnico documenta as melhores práticas para lidar com ataques cibernéticos destrutivos e destaca como a Cohesity pode ajudar sua organização a alcançar esses resultados operacionais.

Análise da situação: Por que sua organização opera de forma diferente em "tempo de paz" e "tempo de guerra"

"Tempo de paz" corresponde à operação diária normal da sua organização. Alertas de ferramentas de segurança normalmente chegam aos consoles do seu Centro de Operações de Segurança (Security Operations Center, SOC) ou provedor de serviços de segurança gerenciados (managed security service provider, MSSP). Esses alertas são triados para priorização e para atenuar falsos positivos, enquanto evidências adicionais são coletadas para identificar sinais de intrusão na infraestrutura da sua organização. Quando os analistas do SOC estão confiantes de que um adversário está atacando a organização, eles declaram um incidente e continuam sua investigação. Neste estágio, a organização está no modo "tempo de guerra".

Durante a investigação, se os analistas descobrirem que a confidencialidade, integridade ou disponibilidade dos sistemas e dados da organização foi comprometida, eles declaram uma violação e continuam com o processo de resposta a incidentes.

O tempo que o criminoso permanece dentro da organização antes de ser descoberto é definido como tempo de permanência. O criminoso pode ser descoberto por meio de alertas de ferramentas de segurança. Mas muitas vezes, as organizações só tomam conhecimento de um ataque quando os sistemas ficam indisponíveis. O tempo de permanência pode variar significativamente, desde apenas quatro a cinco dias em ataques com Ransomware-as-a-Service (RaaS) a centenas de dias em ataques de ransomware realizados por humanos, ou mesmo, anos no caso de agentes de países.

Exemplos de como a confidencialidade, integridade ou disponibilidade são comprometidas incluem:

- **Confidencialidade**: os dados da organização foram divulgados a partes não autorizadas. Isso inclui a exfiltração de dados para fins criminosos por quadrilhas de ransomware ou para espionagem por parte de agentes de países estrangeiros antes de lançar um ataque de wiper.
- **Integridade**: durante os vários estágios de um ataque cibernético destrutivo, os adversários alterarão arquivos de configuração, registros, sistemas de gerenciamento de identidade e, potencialmente, até firmware para manter a persistência nas organizações vítimas. Todas essas alterações afetam a integridade dos sistemas.
- **Disponibilidade**: um ataque cibernético destrutivo tem como objetivo tornar a infraestrutura de TI da organização, que é necessária para entregar produtos e serviços aos clientes, indisponível. Eles fazem isso criptografando dados e/ou sistemas, como visto em ataques de ransomware, ou excluindo-os, como em ataques de wipers.

É importante entender que nem todos os incidentes se transformam em violações, e um SOC detecta e responde continuamente a incidentes em seus estágios iniciais para evitar que eles se tornem violações. Algumas violações ficam confinadas a áreas isoladas da organização e podem ser gerenciadas com manuais padrão de resposta a incidentes.

No entanto, certos incidentes, especialmente ransomware e ataques de wipers, podem ter um impacto amplo. Eles podem desativar sistemas necessários para entregar produtos e serviços aos clientes, além de sistemas internos de TI essenciais para gerenciar o incidente. Isso pode incluir sistemas de acesso físico às instalações, comunicação com reguladores e partes afetadas ou titulares de dados, ou coordenação com seguradoras, autoridades policiais e a imprensa. Nesses casos, a organização pode declarar uma **crise cibernética** e realizar um fluxo de trabalho diferente para garantir que possa gerenciar o incidente.

Assim que as equipes de segurança e TI tiverem lidado com o incidente, a violação ou a crise, restaurado os sistemas para um estado confiável e mitigado as ameaças de recorrência, a organização pode retornar às operações "tempo de paz".

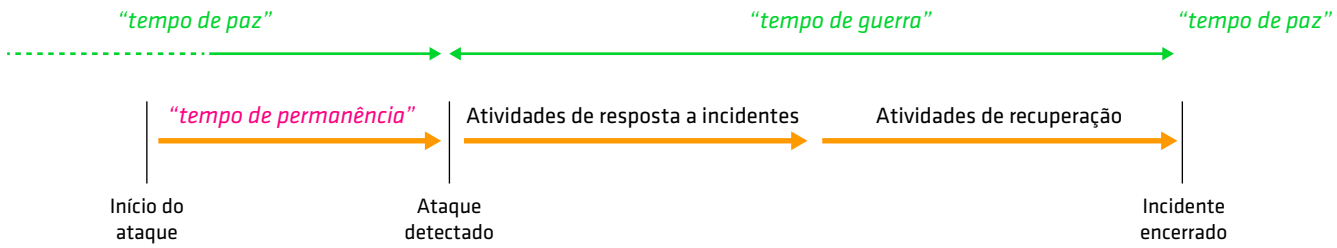

Figura 1. Estágios de "tempo de guerra" e "tempo de paz" em um ataque cibernético destrutivo.

Por que os ataques cibernéticos destrutivos diferem da continuidade dos negócios

Antes do advento de ataques cibernéticos destrutivos, você poderia contar em uma mão as causas-raiz das interrupções de TI: inundação, incêndio, falha de equipamentos ou software, configuração incorreta ou falta de energia. Esses incidentes exigiam investigação mínima, e a resposta padrão era simplesmente restaurar o último instantâneo de backup.

O ransomware, no entanto, é muito mais complexo. Diferentemente dos vírus ou worms tradicionais, ele não é um único arquivo binário que você possa procurar. Os criminosos atacam em uma cadeia de 14 estágios, escolhendo entre centenas de técnicas para atingir seus objetivos em cada estágio. Eles estão constantemente inovando, tornando as configurações de controle de segurança de ontem ineficazes hoje.

Agravando a ameaça, a atual situação geopolítica global aumentou o risco de ataques de wipers por parte de agentes de outros países. Com sua capacidade operacional, financiamento e motivação inigualáveis, esses agentes de ameaças exigem que as organizações desenvolvam resiliência cibernética além da necessária para quadrilhas de ransomware criminosas.

Investigando e corrigindo malware tradicional vs. ransomware

Malware tradicional, como vírus e worms, é detectado por sistemas de varredura em busca de binários maliciosos. Depois que ele é identificado, as equipes de segurança podem simplesmente colocar o binário malicioso ou excluí-lo. Por outro lado, ataques de ransomware ou de wipers envolvem uma cadeia de eventos que permite aos invasores obter acesso após dias de uma vulnerabilidade recém-anunciada. Esses ataques podem explorar sua infraestrutura de TI para "viver dos próprios recursos", aproveitar contas autorizadas, alterar configurações para ampliar privilégios ou manter persistência, preparar dados sensíveis para exfiltração e usar scripts nativos e macros incorporados em seus sistemas operacionais e aplicativos – tudo isso enquanto evitam controles para dificultar sua capacidade de detectar, responder e se recuperar. Ao contrário do malware tradicional, não há um único binário para procurar e remover.

Recuperar-se com segurança de um ataque de ransomware ou wiper requer investigar como o incidente ocorreu. As organizações precisam corrigir as ameaças e vulnerabilidades encontradas para evitar a reinfecção e mais tempo de inatividade. Esta é a essência de cada estrutura de melhores práticas para resposta a incidentes de segurança cibernética.

As organizações devem corrigir três áreas críticas para garantir que você possa resistir a um ataque semelhante no futuro e evitar a reinfecção dos sistemas recuperados do ataque atual:

1. **Superfície de ataque**: Os vetores de acesso inicial de ransomware mais comuns, em ordem de prevalência, são: vulnerabilidades na infraestrutura voltada para a Internet, credenciais de acesso legítimas reutilizadas e táticas de engenharia social, como e-mails de phishing. Você precisa entender como o "paciente zero", o ponto de entrada inicial ou a primeira vítima identificada, foi comprometido e, em seguida, corrigir a ameaça em sistemas recuperados. Isso pode envolver a aplicação de patches em sistemas vulneráveis, a colocação dos sistemas vulneráveis por trás de alguma forma de proteção, como um Web Application Firewall (WAF), e a remoção do e-mail de phishing que permitia o acesso inicial da caixa de entrada de um usuário.
2. **Técnicas de evasão ou lacunas nos controles de segurança**: Prevenir ou detectar incidentes de segurança precocemente, antes que eles afetem a confidencialidade, integridade ou disponibilidade, incorre em um custo operacional, mas ajuda a evitar perda de receita, danos à reputação e possíveis multas regulatórias dispendiosas e litígios de parceiros de negócios ou titulares de dados afetados.

As gangues de ransomware criam técnicas de evasão em suas plataformas de RaaS para controles de segurança comuns, incluindo detecção e resposta de endpoint (endpoint detection and response, EDR) e detecção e resposta estendidas (extended detection and response, XDR). Elas também têm a vantagem de agir antes que os feeds de inteligência de ameaças cibernéticas possam ser atualizados e disseminados para incluir suas técnicas de ataque.

Antes de retomar a produção, você deve entender por que os controles de segurança existentes falharam em parar ou detectar o ataque antes que ele interrompesse a entrega de serviços de TI. Em seguida, você pode garantir que as ferramentas de segurança sejam restauradas para um estado confiável e que suas regras sejam atualizadas para prevenir ou detectar ataques futuros antecipadamente.

3. **Mecanismos de persistência**: Em um ataque típico de ransomware ou wiper, os invasores muitas vezes deixam dezenas de artefatos para trás. Eles podem implantar uma base, permitindo que os invasores tenham acesso contínuo se os sistemas forem recuperados sem compreender totalmente e remover o que foi deixado para trás. É comum que as organizações passem dias recuperando sistemas, apenas para infectá-los em minutos, e caiam novamente devido a um mecanismo de persistência negligenciado. Devido à natureza de vários estágios de ataques cibernéticos destrutivos, uma combinação de caça a ameaças e análise forense é normalmente necessária para criar uma linha do tempo do ataque para identificar uma lista completa dos artefatos que precisam ser analisados.

O equívoco dos indicadores de comprometimento (IOCs)

O conceito de indicadores de comprometimento (IOCs) é fundamental para a inteligência tática de ameaças cibernéticas. Antes de discutir as atividades em tempos de guerra que as organizações devem executar ao enfrentar um ataque cibernético destrutivo, é importante definir um IOC.

Os IOCs fornecem pistas indicando que um sistema ***pode*** ter sido comprometido. Embora sirvam como ponto de partida para procurar comportamento criminoso, os IOCs são, muitas vezes, apenas sinais, não o destino. Para se recuperarem com segurança, as organizações devem criar um quadro do ataque e analisá-lo para realizar as mitigações apropriadas descritas na seção anterior. Por exemplo, um arquivo de configuração alterado que reexecuta um código específico na reinicialização é um IOC, assim como uma DLL maliciosa com o mesmo nome de uma legítima que foi inserida em um diretório. Da mesma forma, manipular a variável PATH para executar esta DLL maliciosa antes da legítima também é um IOC. Embora esses IOCs indiquem que há algo acontecendo, eles não mostram o quadro completo do ataque.

A busca por IOCs é fundamental para a resposta a incidentes de segurança cibernética, mas as organizações devem aplicá-los no contexto certo. Confiar exclusivamente em IOCs pode levar a ações inadequadas. Além disso, a restauração prematura de backups sem investigação mais profunda permitirá a reinfecção ou causará outros problemas de disponibilidade.

Colocar os arquivos em quarentena ou restaurar versões anteriores do arquivo de um instantâneo de backup contendo o IOC não resolve a causa raiz. Você ainda não descobriu como os invasores conseguiram entrar para fazer essas modificações, deixando-os livres para atacar seus sistemas várias vezes. Além disso, reverter para configurações mais antigas e incompatíveis pode criar problemas de disponibilidade, especialmente se, por exemplo, os binários tiverem sido corrigidos para versões posteriores desde o início do ataque.

Da mesma forma, a ausência de IOCs em um instantâneo de backup não garante que ele esteja "limpo". Como os IOCs simplesmente servem para fornecer sinais de atividades maliciosas, remover os sinais ainda deixa o "destino" intacto. Em casos de reversão automatizada para snapshots mais antigos, essa abordagem pode deixar a equipe de resposta a incidentes sem saber do ataque subjacente.

A detecção de IOCs também depende da coleta, análise e disseminação de inteligência sobre ameaças cibernéticas, que muitas vezes fica atrás da evolução das táticas criminosas. Isso significa que há um atraso entre o criminoso mudar seu comportamento e nossas ferramentas de segurança estarem cientes das novas técnicas de ataque. Isso explica por que algumas das maiores organizações do mundo, apesar de terem orçamentos e equipes de segurança cibernética abrangentes que certamente estão usando as melhores e mais recentes ferramentas de segurança cibernética, ainda são afetadas pelo ransomware. O adversário muda seu comportamento antes que as ferramentas atuais de segurança cibernética tomem conhecimento dessa mudança, permitindo que eles entrem na organização sem serem detectados. Uma vez dentro, seu recurso de evasão da defesa torna os controles de segurança do endpoint cegos. Quando o fornecedor da ferramenta de segurança toma conhecimento do novo comportamento criminoso e a inteligência de ameaças relevante é alimentada em suas ferramentas, já é tarde demais. A ferramenta já foi contornada e não disparará.

Para mitigar esses desafios, considere adotar uma atividade em tempos de paz, como a caça proativa periódica a ameaças, usando uma solução como o **Cohesity DataHawk**. A solução opera independentemente dos controles de segurança tradicionais e não pode ser contornada. O DataHawk permite que você encontre ataques que possam ter passado despercebidos quando as fontes de inteligência de ameaças cibernéticas ainda não estavam cientes deles.

Vencer a guerra: Investigação, mitigação de ameaças e recuperação segura

A melhor abordagem é construir resiliência e preparação, tendo as soluções tecnológicas certas como multiplicadores de força para seus responsáveis pela resposta a incidentes, definindo processos claros e um modelo operacional para que todos saibam exatamente o que precisam fazer. Use automação e orquestração sempre que possível. Além disso, a equipe deve ser devidamente treinada e participar de exercícios realistas para responder, em vez de reagir, quando o pior acontecer.

A resiliência cibernética não é um produto que você pode comprar. É uma propriedade emergente que chega quando a sua organização está preparada para fazer as coisas certas após um incidente cibernético. Para alcançar a resiliência cibernética, você deve trabalhar com um fornecedor realista sobre os desafios que as organizações enfrentam após um ataque cibernético destrutivo e que ofereça a tecnologia certa e o suporte necessário para que você crie uma estratégia robusta de resposta a incidentes.

A resposta a incidentes de segurança cibernética é uma atividade complexa. O sucesso vem de reconhecer essa complexidade, e não de ignorá-la. Fechar os olhos para isso só vai adiar o problema e prejudicar a organização no pior momento possível: durante um incidente.

Melhores práticas de análise forense digital e resposta a incidentes de segurança cibernética

Há quatro estruturas principais amplamente adotadas para análise forense digital e resposta a incidentes:

1. NIST SP800-61 Guia de tratamento de incidentes de segurança do computador
2. Processo de resposta a incidentes em seis etapas do SANS Institute
3. ESTRUTURA RE&CT (“Reagir”)
4. MITRE D3FEND (“Defesa orientada por dados”)

Neste artigo técnico, vamos nos concentrar no uso do modelo do SANS Institute. Dito isso, todas as estruturas estão amplamente alinhadas com as etapas necessárias para se preparar e responder a um ataque cibernético:

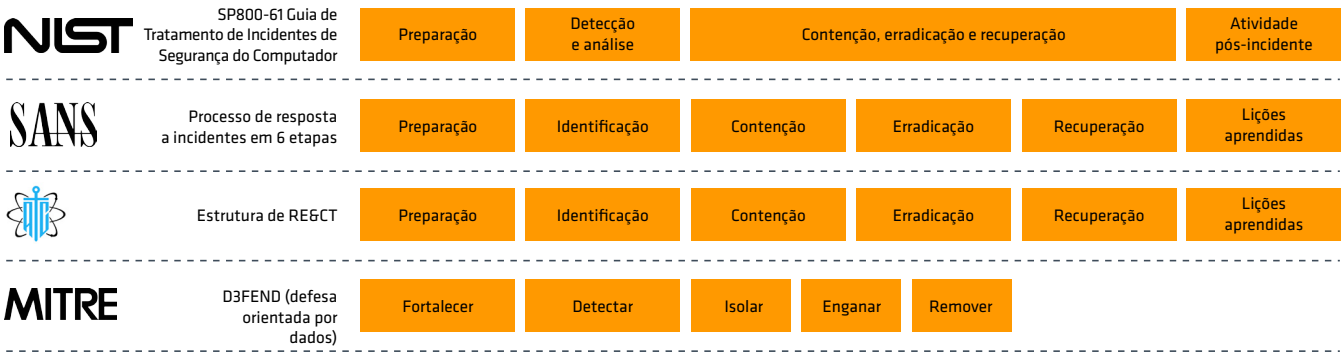

Figura 2. Melhores práticas de análise forense digital cibernética e resposta a incidentes.

Alcançando as melhores práticas operacionais com a Cohesity

Para situações de guerra, todas as melhores práticas de estruturas de resposta a incidentes de segurança cibernética incluem estágios de contenção, investigação, mitigação de ameaças e, finalmente, recuperação. As organizações que encurtam os estágios de contenção, investigação e mitigação e correm para a recuperação deixam as vulnerabilidades que permitiram o ataque in situ.

As lacunas nas defesas que não detectaram ou impediram o ataque permanecem abertas e, muitas vezes, os mecanismos de persistência e outros artefatos de ataque são trazidos de volta. Isso frequentemente resulta em reinfecção ou novo ataque e paradas prolongadas subsequentes. Não é incomum ver organizações que adotam uma abordagem de resposta a ataques de ransomware centrada na recuperação terem que se recuperar mais de uma dúzia de vezes.

Identificação

Há dois estágios envolvidos na identificação:

1. **Conscientização inicial de que um incidente potencial está em andamento**: Isso pode assumir a forma de relatório de um usuário ou terceiro, que precisa ser triado para confirmar sua validade e escopo, ou um alerta de alguma forma de controle técnico.
2. **Entendendo como o ataque aconteceu**: Isso garante a erradicação adequada da ameaça, a remoção das vulnerabilidades exploradas e o reforço dos controles, permitindo que os sistemas sejam recuperados em um estado seguro e resiliente.

Vamos analisar cada estágio com mais detalhes.

Conscientização inicial

A conscientização inicial é tecnicamente uma atividade em tempos de paz, pois o tempo de guerra não pode ser declarado até que a organização detecte que um ataque está em andamento. Portanto, é importante discutir os mecanismos para detectar ataques como ransomware para entender como isso pode afetar o fluxo de trabalho de resposta a incidentes.

As plataformas de RaaS comoditizaram a evasão de ferramentas de segurança populares, como EDR e XDR, tornando-as cegas para ataques. Na estrutura MITRE ATT&CK, a taxonomia mais popular para descrever como os ataques cibernéticos são realizados, a tática de Evasão da Defesa tem praticamente o dobro do número de técnicas em relação à tática seguinte das 13 táticas. Esses mecanismos usados por invasores de ransomware não podem evadir **a detecção de anomalias do DataProtect da Cohesity** e as capacidades de caça a ameaças do DataHawk.

Alertas, como os da **detecção de anomalia baseada em IA do DataProtect**, têm um alto grau de **confiança**, ou seja, você pode confiar que o alerta não é um falso positivo, assim como alta **fidelidade**, que se refere à quantidade de informações sobre o que está acontecendo que o analista do SOC recebe ao analisar o alerta. Isso acelera o processo de triagem e investigação, diminuindo o tempo necessário para recuperar os sistemas para a produção com segurança.

Se, durante a triagem, ficar evidente que os sistemas necessários para responder aos incidentes foram afetados, ou que a criptografia ou exclusão de sistemas em toda a organização estão acima de um determinado limite predefinido, a organização pode declarar uma **crise cibernética**. Um fluxo de trabalho predefinido de crise cibernética permite que uma organização estabeleça diferentes escalonamentos e autoridade previamente definidas para que os responsáveis pela resposta a incidentes realizem certas ações além daquelas normalmente realizadas para uma violação cibernética.

Pode-se descobrir que os sistemas necessários durante a resposta a incidentes são afetados, indisponíveis ou não confiáveis. Os problemas nessa situação podem incluir:

- Listas de contatos para stakeholders de resposta a incidentes podem estar indisponíveis, como executivos, reguladores, seguradoras da cobertura contra ataques cibernéticos, empresas de resposta a incidentes de prontidão, parceiros da cadeia de suprimentos e a imprensa.

- Os fluxos de trabalho de resposta a incidentes podem estar indisponíveis.
- Os contratos da sua apólice de seguro cibernético e da empresa de resposta a incidentes de prontidão podem estar indisponíveis.
- Servidores de gerenciamento e configurações para sistemas de controle de acesso físico ou controles ambientais para edifícios podem estar inativos.
- Os sistemas de comunicação, como e-mail ou Voice-over-IP, necessários para entrar em contato com as partes interessadas podem estar inativos ou em um estado não confiável.
- As configurações de roteadores e switches ou firmware podem não ser confiáveis, deixando qualquer conexão com a Internet para aplicativos de Software como Serviço ou comunicações sujeita a espionagem ou interrupção.
- Ferramentas de segurança podem ter sido contornadas ou inutilizadas.

Compreensivelmente, a maioria das organizações prioriza a restauração dos aplicativos mais críticos primeiro, aqueles essenciais para retomar a entrega de produtos e serviços, também conhecidos como Empresa Mínimo Viável (MVC). No entanto, as organizações que sofrem um ataque cibernético destrutivo percebem que um subconjunto de contas, aplicativos e infraestrutura também é necessário para gerenciar o incidente de forma eficaz. Esses sistemas garantem que os sistemas de produção críticos não possam ser apenas recuperados, mas recuperados em um **estado seguro**, satisfazendo as obrigações regulatórias da organização.

A Cohesity define esse subconjunto de infraestrutura e recursos essenciais para gerenciar os esforços de resposta e recuperação como a Capacidade mínima viável de resposta (Minimum Viable Response Capability, MVRC). Suponha que qualquer componente da MVRC tenha se tornado desconfiável ou indisponível. Nesse caso, as organizações precisam de uma maneira rápida de disponibilizar esses recursos e reconstruir um conjunto confiável de ferramentas para gerenciar as ações de resposta. A **solução Sala limpa Cohesity** permite que as organizações reconstruam rapidamente sua MVRC para um estado confiável e disponibilizem os recursos necessários para gerenciar o incidente em minutos.

Entendendo como o ataque aconteceu

Assim que a triagem inicial for concluída e houver confiança de que um ataque cibernético destrutivo está em andamento, o analista declara um incidente e continua uma investigação mais profunda. Normalmente, a implantação de aplicativos de criptografia em servidores e endpoints é a última tarefa que as quadrilhas de ransomware realizam, pois é o estágio do ataque que mais chama atenção, tanto em termos de acionar controles de detecção quanto de criar impactos visíveis para os usuários finais.

É improvável que focar as investigações e correções apenas em sistemas criptografados descubra a causa raiz do ataque. Em vez disso, a investigação precisa se estender além desses sistemas. Sistemas não criptografados são frequentemente de maior interesse para o investigador, pois podem conter mecanismos de persistência que os criminosos podem usar para retornar após qualquer tentativa de recuperação.

Antes de olharmos para esse nível mais profundo de identificação em detalhes, é importante entender como outro aspecto de todos os processos de resposta a incidentes de melhores práticas pode impedir nossa capacidade de realizar essa tarefa: contenção.

Contenção

Contenção é um requisito de todas as estruturas de resposta a incidentes, pois impede a disseminação do ataque e interrompe qualquer atividade de comando e controle ou de exfiltração de dados. No entanto, a contenção também apresenta alguns desafios para as equipes de operações de segurança:

- **A imagem remota não funciona isoladamente**. A maioria das organizações passou da aquisição física de conteúdo de disco rígido para a criação de imagens forenses remotas. No entanto, isolar um host infectado, ou a rede do host, pode remover repentinamente a capacidade da organização de realizar essa tarefa.O **DataProtect** fornece uma interface de usuário e API que permite que o responsável pela resposta a incidentes execute análises forenses em nível de arquivos, e não apenas no último instantâneo, mas em toda uma série de instantâneos até o período de retenção da organização. Isso fornece aos analistas forenses digitais o superpoder da viagem no tempo, permitindo que eles procurem binários e outros artefatos que o criminoso já limpou e identifiquem rapidamente deltas maliciosos feitos em configurações e outros arquivos. Diferentemente das soluções de segurança de endpoint e SIEMs que normalmente retêm apenas uma linha do tempo curta dos logs, o Cohesity permite que os responsáveis pela resposta a incidentes examinem eventos e o conteúdo dos logs durante todo o período para o qual há backups mantidos para esse

sistema, tudo entregue por uma plataforma imutável para garantir uma forte cadeia de custódia. O melhor de tudo é que essas capacidades são fornecidas sem uma conexão de rede. É imune a espionagem e interrupção, pois o DataProtect usa uma cópia offline do sistema de arquivos para essa tarefa.

- **As soluções de endpoint se tornam isoladas e a consulta/resposta fica impossível.** Embora a arquitetura de diferentes soluções de endpoint, como EDRs e XDRs, possa diferir, quase todas têm um servidor de gerenciamento central que recebe telemetria de clientes de endpoint. Se a contenção interromper a conexão entre o servidor de gerenciamento e os endpoints, os analistas ficarão apenas com as informações enviadas anteriormente para o servidor de gerenciamento. Eles não podem mais trabalhar em um formato de consulta e resposta para aprofundar o que está acontecendo nos endpoints em tempo real.
- A contenção também inclui o estabelecimento de ambientes isolados onde podem ser aplicadas técnicas de resposta e recuperação de incidentes. A solução Sala limpa Cohesity oferece uma abordagem flexível para criar tais ambientes. Ela ajuda as organizações a se alinharem às melhores práticas de resposta a incidentes e a adotarem um modelo de responsabilidade compartilhada apropriado entre as operações de segurança e TI. Essa abordagem ajuda as organizações a evitar o tempo de inatividade prolongado e prevenir a reinfecção após a recuperação.
- A solução Sala limpa Cohesity:
- Permite a restauração rápida da MVRC ou infraestrutura afetada ou contornada, o que é essencial para investigar e corrigir o incidente.
- Estabelece um ambiente de investigação isolado que permite que as equipes de operações de segurança usem as capacidades de segurança nativas da **plataforma Cohesity Data Cloud** juntamente com suas outras ferramentas de segurança para entender o ataque de ponta a ponta e planejar as correções apropriadas para evitar ataques futuros.
- Cria um ambiente de mitigação isolado onde os resultados da investigação da equipe de operações de segurança informam as correções, como a reconstrução rápida de sistemas a partir de imagens e configurações de instalação conhecidas e boas, recuperação de sistemas e correção das suas vulnerabilidades, reforço de controles para que não possam ser contornados e prevenção ou detecção bem-sucedida de futuros ataques semelhantes. Por fim, os sistemas podem ser testados quanto à funcionalidade e ao desempenho, antes de serem restaurados aos sistemas de produção.

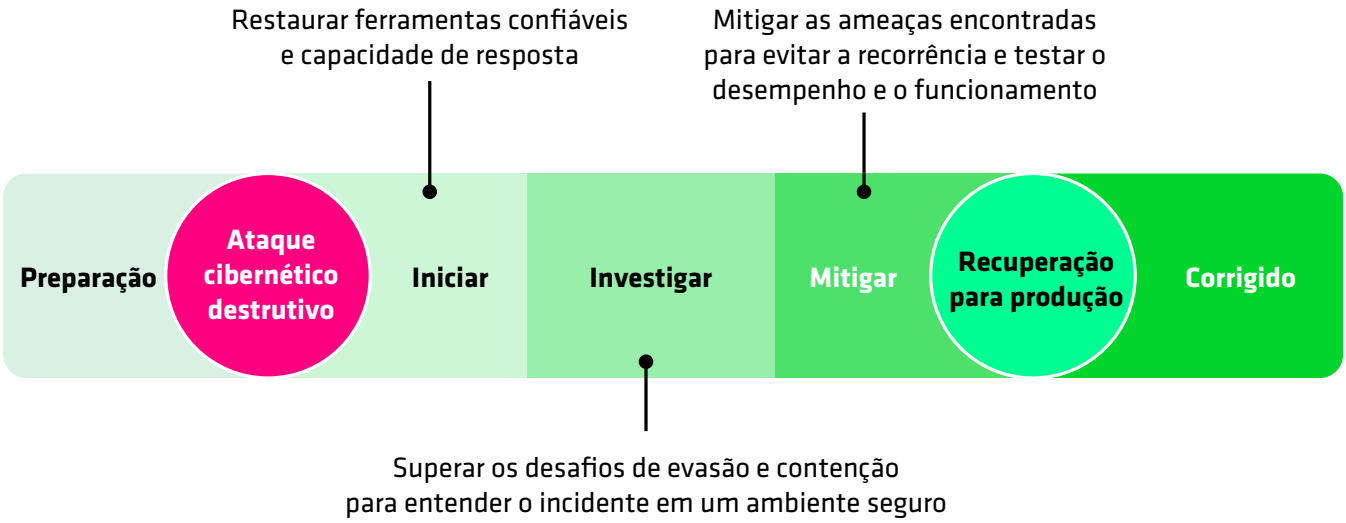

Figura 3. Os quatro estágios da solução Sala limpa Cohesity levam os clientes à correção de ataques cibernéticos.

Revisitando a identificação: Como a solução Sala limpa Cohesity ajuda

Seguindo as melhores práticas de análise forense digital e resposta a incidentes, a organização agora conteve as redes e os hosts infectados. Neste estágio, qualquer infraestrutura impactada necessária para investigar e corrigir o incidente seria restabelecida para um estado confiável: você pode confiar em sua conexão com a Internet e usar seus serviços de TI, negócios e segurança baseados em nuvem. Além disso, sua capacidade de comunicação com as partes interessadas seria restabelecida. Mais importante ainda, toda a documentação e os recursos necessários para apoiar a resposta e a recuperação de incidentes estão ao alcance das suas equipes de segurança e operações de TI.

Agora examinaremos como a Cohesity ajuda com o nível mais profundo de investigação, enquanto os ativos que você está investigando foram isolados por contenção.

Descobrindo vulnerabilidades exploradas no ataque

As quadrilhas de ransomware e os agentes de países que posicionam previamente ataques de wipers geralmente obtêm acesso inicial por meio de vulnerabilidades em ativos voltados para a Internet. Sabe-se que os criminosos obtêm acesso inicial por meio de vulnerabilidades e instalam mecanismos de persistência, permitindo que eles permaneçam e depois aplicam os patches para impedir que outros invasores obtenham acesso a esses sistemas.

Como as organizações podem estabelecer quais vulnerabilidades já existiam no momento de um ataque? Isso se torna ainda mais desafiador se o criminoso tiver apagado o sistema ou se medidas de contenção impedirem o acesso ao sistema para uma verificação de vulnerabilidade.

O **Cohesity CyberScan** fornece uma solução que permite às organizações verificar instantâneos de backup quanto a vulnerabilidades usando sua licença de gerenciamento de vulnerabilidades Tenable. Isso permite que as equipes de segurança identifiquem vulnerabilidades durante um ataque, mesmo que um sistema esteja inacessível devido à contenção, tenha sido apagado ou corrigido por um criminoso após uma intrusão.

Executando análise forense do sistema de arquivos

A análise forense do sistema de arquivos é uma disciplina central da resposta a incidentes. Muitas organizações usam ferramentas de aquisição remota para imagens forenses. No entanto, depois que as medidas de contenção são implantadas, os sistemas que exigem imagens forenses, muitas vezes, não estão mais acessíveis.

O DataProtect fornece aos analistas acesso não apenas a um único instantâneo de volume dos sistemas de arquivos, mas também a uma série inteira de instantâneos. Isso permite que os examinadores forenses analisem um cronograma de incidentes e todo o período de retenção de backup. Uma série temporal de volumes pode ser rapidamente montada e comparada para identificar deltas

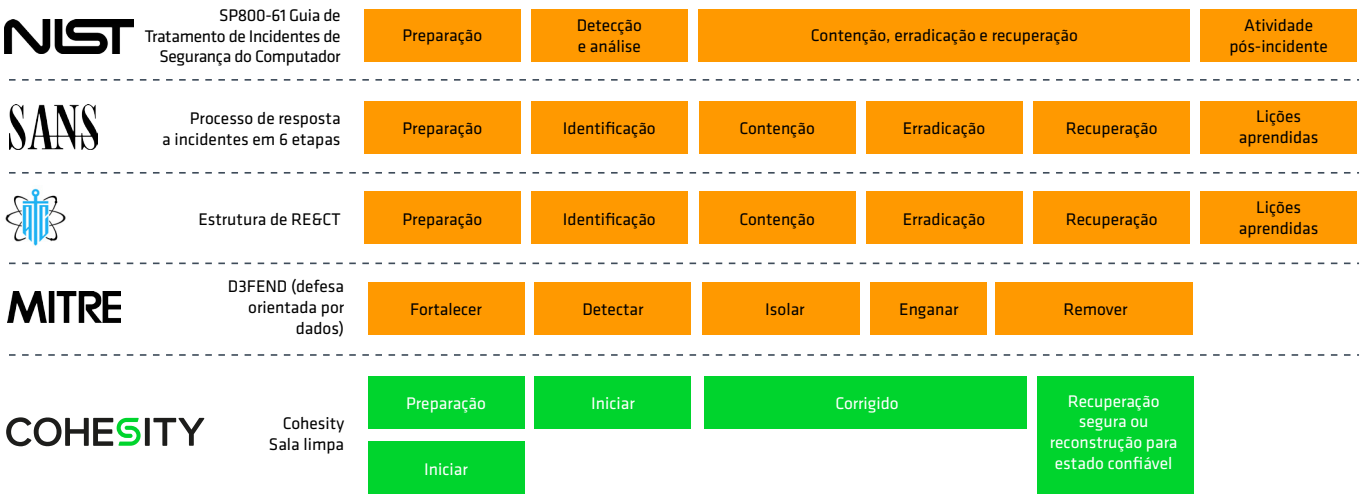

Figura 4. Alinhamento da Sala limpa Cohesity com as melhores práticas de resposta a incidentes

maliciosos. Os objetos de arquivo podem ser extraídos para engenharia reversa, detonação em sandboxes ou análise enviando-os para serviços baseados em nuvem.

Na análise forense digital tradicional, os responsáveis pela resposta a incidentes normalmente coletam uma única imagem do sistema após o ataque, formam uma hipótese sobre como o sistema chegou a esse estado final e, em seguida, simulam o caminho de volta para coletar evidências para confirmar ou eliminar essa teoria. Em contraste, usando o DataProtect, os responsáveis pela resposta a incidentes agora conseguem ver as modificações realizadas no sistema de arquivos ao longo de uma linha do tempo bem maior do incidente, o que continua a funcionar mesmo que os esforços de contenção tenham isolado o host infectado.

Caça às ameaças

Caça aos IOCs é outra tarefa que os responsáveis pela resposta a incidentes normalmente devem fazer. Esta caça em tempos de guerra se encaixa em duas categorias:

Varredura de IOCs fornecidos por terceiros. Esses terceiros podem incluir um fornecedor de inteligência de ameaças cibernéticas, órgão governamental ou organizações semelhantes. Os clientes da Cohesity que usam o DataHawk podem aproveitar o feed atualizado com frequência dos mais de 117.000 IOCs utilizados por criminosos de quadrilhas de ransomware e agentes de países estrangeiros. O recurso de varredura de ameaças do DataHawk também é compatível com feeds comerciais de inteligência de ameaças CrowdStrike que a organização licenciou e pode consumir qualquer IOC fornecido no formato YARA de outros terceiros.

Procurando por IOCs descobertos por sua organização. Quando os responsáveis pela resposta a incidentes encontram artefatos durante uma investigação, eles vão querer caçar para ver se esses IOCs existem na infraestrutura da organização. A partir daí, eles determinarão se sistemas adicionais devem ser incluídos no escopo da resposta ao incidente.

Isso é comumente feito criando regras YARA que descrevem o artefato encontrado de uma forma que permite a detecção, mas evita falsos positivos desnecessários. Com o Cohesity, você pode realizar análises forenses (conforme discutido na seção anterior), extrair artefatos do sistema de arquivos e detoná-los em sandboxes como o Cuckoo, que, por meio de um plugin, pode gerar automaticamente regras YARA para quaisquer IOCs relacionados a esse arquivo. O recurso de caça do DataHawk não depende de agentes de endpoint. Ele continua a funcionar mesmo que a organização tenha sistemas isolados para contenção. Ele não é vulnerável às técnicas comuns de evasão da defesa que tornam as soluções de segurança de endpoint incapazes de caçar com eficácia.

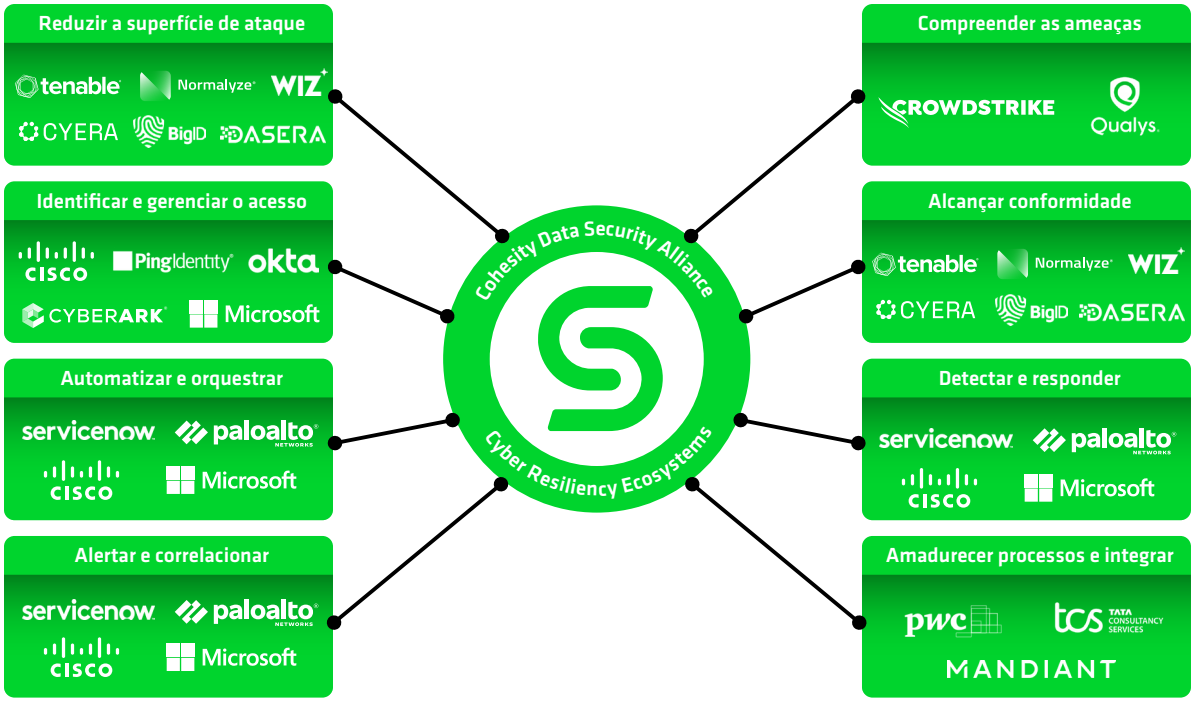

Figura 5. Data Security Alliance da Cohesity: Um ecossistema para resiliência cibernética.

Capacidades como o Cohesity Global Search permitem que os responsáveis pela resposta a incidentes busquem arquivos rapidamente em toda a infraestrutura de backup, o que pode ajudar a direcionar os esforços de investigação ao procurar um artefato ou arquivo específico.

Alcançar conformidade regulatória

Além de exigir processos sólidos de resposta a incidentes, muitos regulamentos de conformidade atualizados recentemente, como HIPAA, DORA e NIS 2, exigem que as organizações notifiquem os reguladores e os titulares de dados afetados em caso de violação de segurança cibernética. Compreender a natureza da violação faz parte do estágio de identificação, assim como entender seu impacto e garantir a notificação oportuna.

Se o incidente afetou a comunicação, a Cohesity, como parte da MVRC, ajuda a restaurar essa capacidade. Os modelos de comunicação podem ser mantidos na Digital Jump Bag™ – a base de uma sala limpa. Além disso, o DataHawk pode verificar backups para identificar dados confidenciais e regulamentados, ajudando as organizações a atender aos requisitos regulatórios. Isso é especialmente valioso após um ataque cibernético destrutivo em que os armazenamentos de dados críticos são criptografados ou apagados.

Integração de ferramentas de operações de segurança

A resiliência cibernética é um esporte de equipe – nenhuma solução de um único fornecedor pode investigar e corrigir um incidente em sua totalidade. É por isso que a Cohesity estabeleceu a Data Security Alliance. Esse ecossistema colaborativo permite que o poder dos dados e dos dados ao longo do tempo seja levado para ferramentas e serviços de segurança mais amplos por meio de integrações para governança, investigação e recuperação comuns.

Automatização e orquestração

O Cohesity é compatível com integração de API, que permite que uma plataforma de orquestração de segurança e resposta automatizada (security orchestration and automated response, SOAR) conduza essas tarefas de investigação, aumentando ainda mais a eficiência dos analistas.

Erradicação e recuperação

Mesclamos os estágios de erradicação e recuperação em mitigação porque, para a Cohesity, nenhuma organização deve tentar se recuperar de um ataque cibernético destrutivo sem tomar as medidas apropriadas para garantir que o criminoso que está atacando a organização não consiga reinfectar sistemas ou que um ataque futuro da mesma natureza não seja bem-sucedido.

A solução Sala limpa Cohesity oferece suporte à rápida recuperação de volume, permitindo que todo um sistema de arquivos seja recuperado antes de aplicar mitigações para erradicar ameaças. Isso garante a recuperação segura do sistema, além de facilitar a rápida reconstrução de sistemas a partir de imagens de software confiáveis e configurações conhecidas como boas. Cada abordagem tem seus prós e contras:

Abordagem de recuperação e limpeza	
Prós:	**Contras:**
É mais simples gerenciar antes de um incidente.	As investigações precisam se aprofundar mais.
	O tempo para corrigir normalmente é maior do que o necessário para sistemas reconstruídos.
Abordagem de reconstrução	
Prós:	**Contras:**
Oportunidade de recuperar dados, reconstruir sistemas e investigar incidentes em paralelo, fornecendo a recuperação mais curta possível dos sistemas em um estado seguro.	A investigação normalmente não precisa ser tão profunda quanto os sistemas em um estado confiável.
A correção é mais curta, normalmente validando apenas a segurança das configurações, reforçando os controles e corrigindo quaisquer sistemas vulneráveis.	Requer habilidades para criar scripts de reinstalação.
	A mídia de instalação, as chaves de licença, os arquivos de configuração e os scripts devem ser mantidos na digital jump bag.

Alguns clientes da Cohesity optam por oferecer suporte a backups e reconstruções por volume. Isso lhes dá a opção de escolher o método mais apropriado de recuperação segura para cada host comprometido, dependendo do nível de esforço envolvido na limpeza desse sistema e do grau de confiança de que a limpeza não deixará artefatos de ataque.

Os clientes frequentemente reutilizam o ambiente de desenvolvimento como ambiente de mitigação de Sala limpa Cohesity. Essa abordagem permite que os servidores de produção sejam reinstalados do zero em paralelo às atividades de mitigação que ocorrem no ambiente de mitigação isolado da Sala limpa. O ambiente de mitigação é configurado para imitar a estrutura do ambiente de produção usando configurações armazenadas na digital jump bag.

Os sistemas podem ser testados assim que as ameaças descobertas no estágio de investigação forem mitigadas por meio de recuperação e limpeza ou reconstrução a um estado confiável. Isso pode assumir a forma de testes funcionais e/ou testes de desempenho para garantir que a correção, aplicação de patches e reforço dos controles não tenham afetado a capacidade do sistema de entrega.

Por fim, um instantâneo desses sistemas é gerado com duas finalidades:

1. Se qualquer artefato de ataque passar despercebido, você não precisa voltar à estaca zero. O instantâneo obtido após a correção servirá como a nova linha de base para investigação e correção adicional e será passado para o estágio de investigação.
2. Como o ambiente de mitigação foi configurado para se parecer com a produção, esse instantâneo pode simplesmente ser "levantado e deslocado" para a rede de produção.

Lições aprendidas

Qualquer organização que busque estabelecer resiliência cibernética deve seguir um mantra de melhoria contínua. Entender o que funcionou, o que não funcionou e o que poderia ser melhorado é fundamental para garantir que a organização não sofra tempo de inatividade contínuo e possa lidar com incidentes futuros de forma mais eficaz e eficiente. Como diz o ditado: "Nenhum plano sobrevive ao contato com o inimigo". Simular ataques do mundo real é importante para testar a recuperação técnica, impulsionar a melhoria do processo, identificar oportunidades de automação e construir memória muscular em seus analistas e responsáveis pela resposta a incidentes.

Uma das maiores vantagens da solução Sala limpa Cohesity é que ela permite que as organizações simulem um incidente inteiro de ponta a ponta sem afetar os sistemas de produção. O DataProtect permite a clonagem de sistemas de produção, que podem então ser atacados por uma equipe vermelha interna ou empresa de testes de penetração externa para simular um ataque de ransomware ou wiper de ponta a ponta. Todo o fluxo de trabalho de resposta e recuperação pode ser realizado até imediatamente após a captura do instantâneo da linha de base dos sistemas corrigidos. Isso oferece às organizações um cenário do mundo real que garante que as pessoas, habilidades, processos e tecnologia de suporte certos estejam disponíveis para minimizar o impacto de um ataque cibernético destrutivo quando o inevitável acontece e a organização se torna vítima.

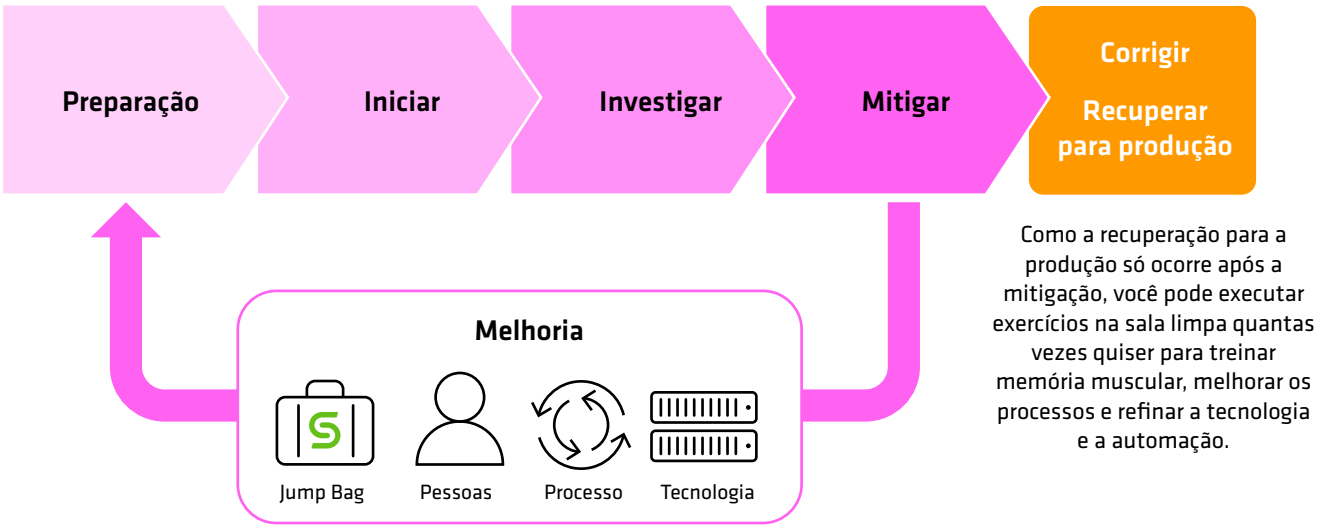

Figura 6. A solução Sala limpa Cohesity permite a melhoria contínua por meio de simulações realistas.

Resumo

A Cohesity pode agregar um enorme valor na recuperação e tornar as etapas de análise forense digital e resposta a incidentes em tempo de guerra eficazes e eficientes. Nossa abordagem exclusiva à resiliência cibernética reduz o tempo necessário para alcançar uma recuperação segura e ajuda as organizações a ter certeza de que um ataque semelhante não causará mais tempo de inatividade.

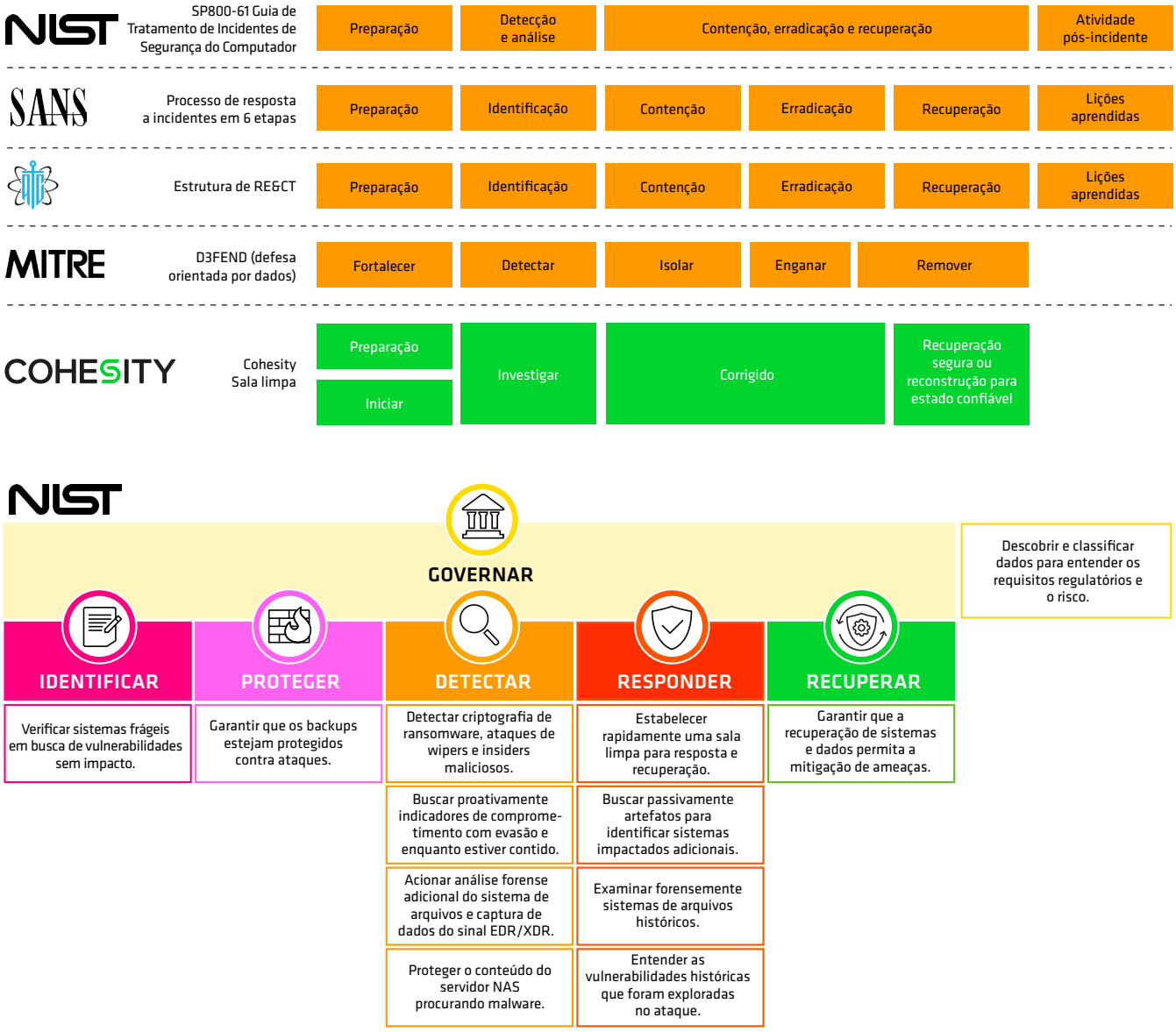

Figura 7. Alcançar a resposta a incidentes cibernéticos e as melhores práticas da estrutura de segurança cibernética do NIST com a Cohesity

Sobre a Cohesity

A Cohesity é líder em segurança de dados com tecnologia de inteligência artificial. Mais de 13.600 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 Santa Clara, Califórnia, e escritórios em todo o mundo. Para saber mais, siga a Cohesity no **LinkedIn**, no **X** e no **Facebook**.

Leitura recomendada

Achamos que os seguintes artigos técnicos, guias e blogs serão úteis.

- Melhore a resiliência cibernética com uma digital jump bag™
- Criando resiliência cibernética em um mundo de ataques cibernéticos destrutivos
- Apresentando o design de sala limpa Cohesity
- Um guia de campo para segurança de dados com tecnologia de IA: Como apresentar resultados de negócios inovadores
- Um guia executivo para segurança e gerenciamento de dados modernos
- Topologias modernas de segurança e gerenciamento de dados: Um guia para líderes de TI

Saiba mais em Cohesity

COHESITY

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

2000058-002-EN 4-2025