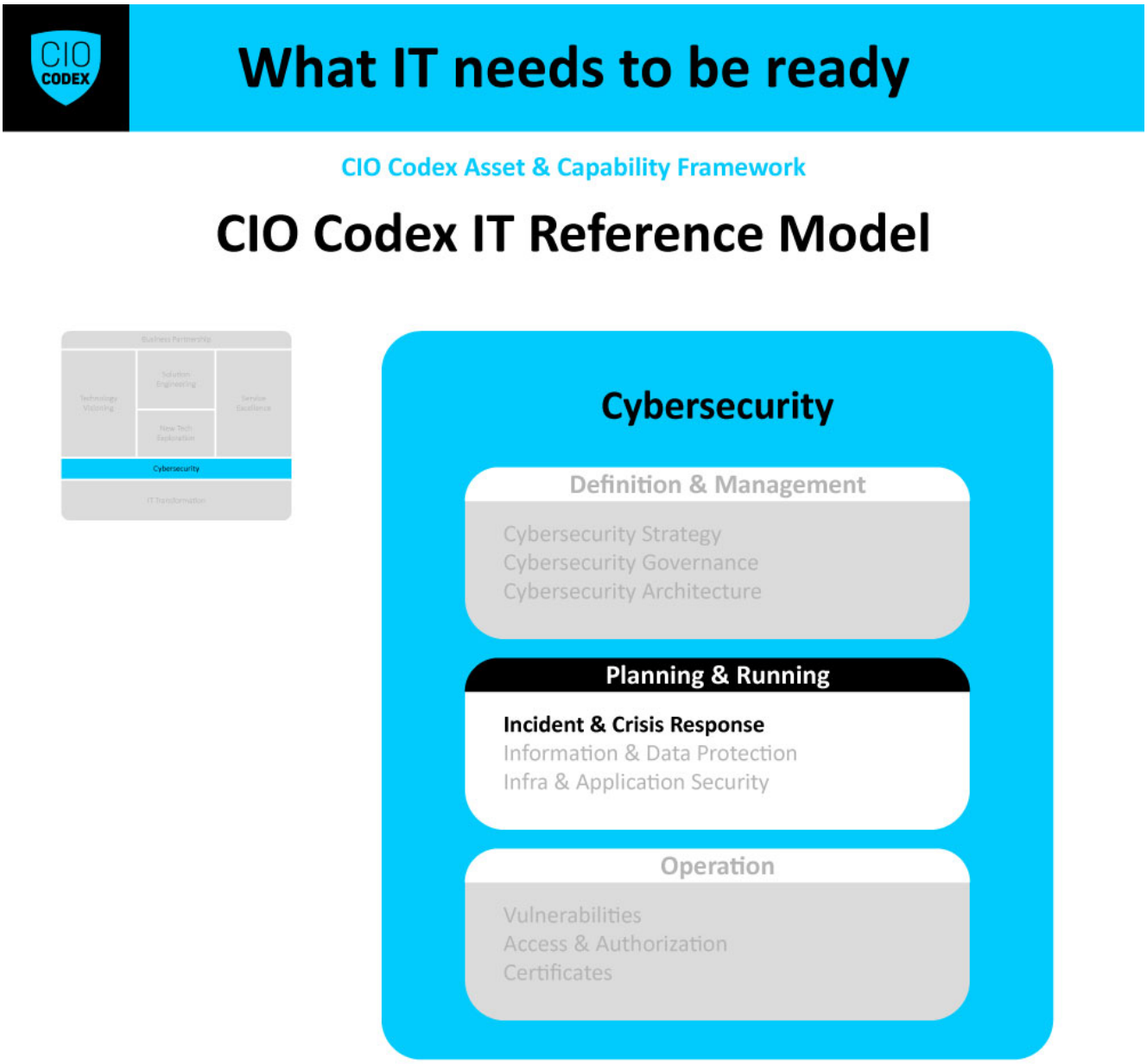

A capability de Incident & Crisis Response, situada na macro capability Planning & Running e enquadrada na camada Cybersecurity do CIO Codex Capability Framework, é essencial para assegurar a proteção da reputação, dos ativos e da continuidade das operações de uma organização diante de ameaças cibernéticas.

Esta capability se destaca por sua abordagem proativa e por processos bem definidos, preparando a organização para enfrentar eficientemente os desafios da segurança cibernética que estão em constante evolução.

No âmbito desta capability, os conceitos fundamentais incluem o Incidente de Segurança, que é qualquer evento que comprometa a integridade, confidencialidade ou disponibilidade dos ativos de informação da organização.

A Crise de Segurança Cibernética, por sua vez, é um incidente grave que representa uma ameaça significativa para a organização e exige uma resposta imediata e eficaz.

A Coordenação de Resposta é a habilidade de orquestrar esforços interdepartamentais para mitigar os incidentes de segurança de forma eficiente.

Entre as características desta capability, destacam-se a Detecção Rápida, a capacidade de identificar incidentes de segurança em tempo hábil para iniciar a resposta imediata.

O Plano de Resposta é crucial, delineando ações detalhadas em resposta a incidentes específicos.

A Comunicação Eficiente assegura a transmissão clara de informações às partes interessadas internas e externas durante os incidentes e crises.

A Mitigação de Danos envolve medidas para minimizar o impacto dos incidentes e reduzir os danos causados.

A Análise Pós-Incidente é vital para a avaliação detalhada de incidentes após sua resolução, identificando lições aprendidas e melhorias necessárias.

O Treinamento e Simulações são essenciais para garantir uma resposta eficaz quando ocorrer um incidente real.

O propósito central da Incident & Crisis Response é assegurar que a organização esteja preparada para identificar, responder e mitigar incidentes de segurança de forma rápida e eficaz.

Esta capability visa garantir a continuidade das operações e a proteção dos ativos digitais em momentos de crise cibernética.

Os objetivos da Incident & Crisis Response no contexto do CIO Codex Capability Framework incluem garantir a eficiência operacional, permitindo que a organização responda rapidamente a incidentes de segurança cibernética, minimizando o impacto nas operações normais.

A inovação em práticas e técnicas de resposta a incidentes é fundamental, incluindo a adoção de automação e inteligência artificial para detecção e resposta mais eficazes.

Além disso, a capacidade de lidar eficazmente com incidentes de segurança pode proporcionar uma vantagem competitiva significativa, inspirando confiança nos clientes e parceiros de negócios.

No aspecto tecnológico, a Incident & Crisis Response influencia diversas dimensões, incluindo a Infraestrutura, com a definição de protocolos e procedimentos para isolar áreas afetadas e garantir a continuidade das operações, a Arquitetura, integrando ferramentas e sistemas de detecção de ameaças e resposta a incidentes, os Sistemas,

desenvolvendo planos de ação para lidar com incidentes em sistemas específicos, a Cybersecurity, sendo crucial para mitigar danos e garantir a recuperação após ataques, e o Modelo Operacional, definindo papéis e responsabilidades durante incidentes e crises para assegurar uma coordenação eficaz.

Em resumo, a Incident & Crisis Response é uma capability de extrema importância que fornece às organizações as ferramentas e processos necessários para uma resposta eficiente e eficaz a incidentes e crises de segurança cibernética.

Sua implementação não só protege a organização contra interrupções significativas, mas também reforça a confiança dos stakeholders na capacidade da organização de manter suas operações seguras e contínuas, mesmo diante de ameaças cibernéticas.

Esta capability é, portanto, um componente crucial na estratégia de segurança cibernética de qualquer organização, garantindo uma abordagem proativa e preparada para enfrentar os desafios do cenário digital atual.

Conceitos e Características

A capability de Incident & Crisis Response é essencial para proteger a reputação, os ativos e a continuidade das operações de uma organização em face de ameaças cibernéticas.

Sua abordagem proativa e processos bem definidos garantem que a organização esteja pronta para enfrentar desafios de segurança cibernética em constante evolução.

Conceitos

- Incidente de Segurança: Qualquer evento que comprometa a integridade, confidencialidade ou disponibilidade dos ativos de informações da organização.
- Crise de Segurança Cibernética: Um incidente grave que representa uma ameaça significativa para a organização e requer uma resposta imediata.
- Coordenação de Resposta: A habilidade de orquestrar esforços interdepartamentais para mitigar os incidentes de segurança de forma eficiente.

Características

- Detecção Rápida: Capacidade de identificar incidentes de segurança em tempo hábil para iniciar a resposta imediata.
- Plano de Resposta: Desenvolvimento de planos detalhados que descrevem as ações a serem tomadas em resposta a incidentes específicos.
- Comunicação Eficiente: Estabelecimento de canais de comunicação claros e eficazes para informar as partes interessadas internas e externas durante incidentes e crises.
- Mitigação de Danos: Implementação de medidas para minimizar o impacto dos incidentes e reduzir os danos causados.
- Análise Pós-Incidente: Avaliação detalhada de incidentes após sua resolução para identificar lições aprendidas e melhorias necessárias.
- Treinamento e Simulações: Preparação constante por meio de treinamentos e simulações para garantir uma resposta eficaz quando ocorrer um incidente real.

Propósito e Objetivos

A Incident & Crisis Response é uma capability de extrema relevância para a gestão de incidentes e crises de segurança cibernética.

Seu propósito central é garantir que a organização esteja preparada para identificar, responder e mitigar incidentes de segurança de forma rápida e eficaz.

Além disso, visa assegurar a continuidade das operações e a proteção dos ativos digitais em momentos de crise cibernética.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da Incident & Crisis Response são claramente definidos:

- Eficiência Operacional: Esta capability tem como objetivo principal garantir a eficiência operacional, permitindo que a organização responda rapidamente a incidentes de segurança cibernética, minimizando o

impacto nas operações normais.
- Inovação: A busca por melhores práticas e técnicas inovadoras de resposta a incidentes é fundamental. Isso inclui a adoção de automação e inteligência artificial para a detecção e resposta mais eficazes.
- Vantagem Competitiva: A capacidade de lidar eficazmente com incidentes de segurança pode proporcionar uma vantagem competitiva significativa. Empresas que demonstram habilidades sólidas de resposta a incidentes podem inspirar confiança nos clientes e parceiros de negócios.

Impacto na Tecnologia

A Incident & Crisis Response afeta diversas dimensões da tecnologia:

- Infraestrutura: Define protocolos e procedimentos para isolar áreas afetadas e garantir a continuidade das operações.
- Arquitetura: Integra ferramentas e sistemas de detecção de ameaças e resposta a incidentes à arquitetura existente.
- Sistemas: Desenvolve planos de ação para lidar com incidentes em sistemas específicos, garantindo a proteção de dados e a recuperação rápida.
- Cybersecurity: Uma resposta eficaz a incidentes e crises é crucial para mitigar danos e garantir a recuperação após ataques.
- Modelo Operacional: Define papéis e responsabilidades durante incidentes e crises, garantindo uma coordenação eficaz.

Roadmap de Implementação

A capability de Incident & Crisis Response é um componente crítico no arsenal de segurança cibernética de uma organização.

Essa capability é essencial para proteger a reputação, os ativos e a continuidade das operações em um mundo digital permeado por ameaças cibernéticas constantes.

Neste contexto, o roadmap de implementação da Incident & Crisis Response, considerando os princípios do CIO Codex Capability Framework:

- Avaliação de Maturidade Atual: O ponto de partida para implementar a Incident & Crisis Response é uma avaliação cuidadosa da maturidade atual da organização nessa área. Isso inclui uma análise das práticas existentes, da estrutura organizacional e da capacidade de resposta a incidentes.
- Definição de Objetivos Claros: Estabeleça objetivos claros para a implementação dessa capability. Isso deve incluir metas relacionadas à eficiência operacional, inovação e como a organização deseja se destacar em relação à concorrência.
- Criação de Equipe e Papéis: Designe e forme uma equipe de Incident & Crisis Response com papéis claramente definidos. Isso inclui líderes de resposta, analistas de segurança, comunicadores de crises e outros especialistas necessários.
- Desenvolvimento de Planos de Resposta: Crie planos de resposta detalhados para incidentes específicos, cobrindo uma variedade de cenários. Esses planos devem incluir procedimentos claros, responsabilidades designadas e uma hierarquia de comunicação.
- Implementação de Ferramentas e Tecnologias: Avalie e implemente as ferramentas e tecnologias necessárias para apoiar a detecção, análise e resposta a incidentes. Isso pode incluir sistemas de detecção de ameaças, automação de resposta e plataformas de comunicação.
- Treinamento e Simulações: Treine regularmente a equipe de resposta por meio de simulações de incidentes. Isso ajuda a garantir que todos estejam familiarizados com os procedimentos e possam atuar eficazmente sob pressão.
- Detecção Rápida e Monitoramento Contínuo: Estabeleça sistemas de detecção de ameaças que permitam identificar incidentes rapidamente. Além disso, implemente monitoramento contínuo para acompanhar ameaças emergentes.
- Comunicação Eficiente: Desenvolva canais de comunicação eficazes para informar as partes interessadas internas e externas durante incidentes e crises. Isso inclui a definição de mensagens claras e processos de notificação.
- Mitigação de Danos e Recuperação: Implemente medidas para minimizar o impacto dos incidentes e acelerar a recuperação. Isso envolve isolamento de áreas afetadas, restauração de sistemas e análise pós-incidente.

- Análise Pós-Incidente e Melhoria Contínua: Após a resolução de incidentes, realize análises detalhadas para identificar lições aprendidas e áreas de melhoria. Use essas informações para aprimorar os planos de resposta e a capability geral de Incident & Crisis Response.
- Exercício de Coordenação: Realize exercícios regulares de coordenação de resposta que envolvam várias equipes e departamentos. Isso ajuda a garantir uma resposta eficaz em situações de crise.
- Auditoria e Revisão de Conformidade: Regularmente, realize auditorias de conformidade com as práticas de Incident & Crisis Response e ajuste os processos conforme necessário para atender a requisitos regulatórios e padrões de segurança.

A implementação bem-sucedida da Incident & Crisis Response não apenas fortalecerá a postura de segurança cibernética da organização, mas também contribuirá para sua eficiência operacional, inovação e vantagem competitiva.

Esta capability é um elemento crítico para enfrentar os desafios de segurança cibernética em constante evolução e garantir a proteção dos ativos digitais e da reputação da organização.

Melhores Práticas de Mercado

Dentro do contexto do CIO Codex Capability Framework, a capability de Incident & Crisis Response desempenha um papel crítico na proteção da reputação, ativos e continuidade das operações de uma organização em um cenário de ameaças cibernéticas em constante evolução.

Para garantir uma resposta eficaz a incidentes e crises de segurança cibernética, é fundamental adotar as melhores práticas de mercado.

A seguir, as principais melhores práticas amplamente reconhecidas neste campo:

- Detecção Rápida de Incidentes: A capacidade de identificar incidentes de segurança cibernética de forma rápida e precisa é crucial. A implementação de ferramentas avançadas de detecção, como SIEM (Security Information and Event Management), e a análise de registros de atividades podem acelerar a identificação de ameaças.

- Desenvolvimento de Planos de Resposta: A preparação é a chave para uma resposta eficaz. Desenvolver planos detalhados de resposta a incidentes que descrevam as ações a serem tomadas em cenários específicos é uma prática essencial. Isso inclui a definição de papéis e responsabilidades claros durante incidentes e crises.
- Comunicação Eficiente: Estabelecer canais de comunicação claros e eficazes é vital durante incidentes e crises. A organização deve ser capaz de informar rapidamente as partes interessadas internas e externas, incluindo autoridades regulatórias, clientes e parceiros de negócios, sobre a situação e as ações em andamento.
- Mitigação de Danos: Implementar medidas para minimizar o impacto dos incidentes é uma prática crucial. Isso pode envolver a isolamento de sistemas comprometidos, a interrupção de atividades suspeitas e a restauração de serviços essenciais o mais rápido possível.
- Análise Pós-Incidente: Após a resolução de um incidente, é fundamental conduzir uma análise detalhada para identificar lições aprendidas e áreas que necessitam de melhorias. Isso contribui para aprimorar os processos de resposta futuros e fortalecer a postura de segurança da organização.
- Treinamento e Simulações: Preparação constante é essencial. A organização deve realizar treinamentos regulares e simulações de incidentes para garantir que a equipe esteja bem-preparada e que os processos de resposta sejam testados e refinados.
- Automatização da Resposta: A automação desempenha um papel crescente na resposta a incidentes. A implementação de soluções de automação e inteligência artificial pode acelerar a detecção, análise e resposta a incidentes, permitindo uma ação mais rápida e eficaz.
- Colaboração Interdepartamental: A coordenação eficiente entre departamentos é essencial para lidar com incidentes complexos. A habilidade de orquestrar esforços interdepartamentais para mitigar os incidentes de segurança de forma eficiente é um diferencial importante.
- Monitoramento Contínuo: Além da detecção rápida, é essencial implementar monitoramento contínuo de ameaças. Isso permite a identificação precoce de atividades suspeitas e a resposta proativa a potenciais ameaças antes que se tornem crises.
- Políticas de Notificação de Incidentes: Ter políticas claras de notificação de incidentes em conformidade com as regulamentações aplicáveis é fundamental.

Isso garante que a organização esteja em conformidade com obrigações legais e regulatórias e evita penalidades.

Adotar essas melhores práticas de mercado na capability de Incident & Crisis Response ajuda as organizações a se prepararem para enfrentar os desafios de segurança cibernética em constante evolução, a protegerem seus ativos digitais e a manterem a continuidade das operações, mesmo em momentos de crise cibernética.

Desafios Atuais

A Capability de Incident & Crisis Response é fundamental para garantir que uma organização esteja pronta para enfrentar desafios de segurança cibernética em constante evolução.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam vários desafios atuais de mercado, alinhados com as melhores práticas do setor.

A seguir, os principais desafios enfrentados pelas organizações:

- Rapidez na Detecção: A detecção rápida de incidentes cibernéticos é um desafio crucial. As organizações precisam investir em tecnologias avançadas de detecção para identificar ameaças em tempo real.
- Complexidade das Ameaças: As ameaças cibernéticas estão se tornando cada vez mais complexas, incluindo ataques sofisticados de phishing, ransomware e APTs (Advanced Persistent Threats).
- Coordenação Interna: A coordenação eficaz entre departamentos é um desafio, pois diferentes equipes devem trabalhar juntas para mitigar um incidente de segurança.
- Resposta Rápida: A capacidade de responder rapidamente a incidentes é fundamental, mas muitas organizações ainda lutam para desenvolver processos de resposta ágeis.
- Comunicação Externa: Comunicar incidentes de segurança para partes interessadas externas, como clientes e reguladores, é complexo e exige transparência.
- Escassez de Talentos: A falta de profissionais qualificados em resposta a incidentes é um problema, pois a demanda por especialistas em

segurança cibernética supera a oferta.

- Maturidade da Cultura de Segurança: Estabelecer uma cultura de segurança cibernética em toda a organização é desafiador, pois requer educação e conscientização contínuas.
- Investimentos Adequados: Alocar recursos financeiros suficientes para a resposta a incidentes é um desafio, especialmente para organizações com orçamentos limitados.
- Integração de Ferramentas: Integrar e manter ferramentas de resposta a incidentes pode ser complexo, pois exige compatibilidade e atualização constante.
- Avaliação Pós-Incidente: Realizar análises pós-incidente eficazes é um desafio, pois requer a identificação de lições aprendidas e a implementação de melhorias.

Esses desafios destacam a importância crítica da Capability de Incident & Crisis Response em um cenário cibernético em constante evolução.

Superar esses obstáculos é essencial para proteger a reputação, os ativos e a continuidade das operações de uma organização diante das ameaças cibernéticas em constante

A capability de identificar rapidamente incidentes, coordenar esforços interdepartamentais, responder eficazmente e comunicar de forma transparente é fundamental para enfrentar esses desafios e manter a resiliência em um ambiente de ameaças em constante evolução.

Além disso, investir na capacitação da equipe e na integração de tecnologias avançadas é fundamental para garantir que a organização esteja preparada para enfrentar os desafios da segurança cibernética no mercado atual.

Tendências para o Futuro

A Capability de Incident & Crisis Response desempenha um papel vital na proteção das organizações contra ameaças cibernéticas e na garantia da continuidade das operações.

Sua abordagem proativa e processos bem definidos são essenciais para enfrentar os desafios em constante evolução no campo da segurança cibernética.

Considerando as expectativas do mercado e as grandes tendências, destacam-se as seguintes tendências futuras que moldarão o desenvolvimento dessa capability:

- Automatização da Resposta a Incidentes: A crescente complexidade das ameaças exigirá uma resposta mais rápida e eficiente. A automação desempenhará um papel crucial na detecção e resposta imediata a incidentes.
- Inteligência Artificial e Machine Learning: O uso de IA e ML será fundamental para a detecção precoce de ameaças, identificação de padrões de comportamento suspeito e tomada de decisões mais precisas durante incidentes.
- Resposta Orquestrada: A orquestração de resposta a incidentes se tornará uma prática comum, permitindo a coordenação eficaz de esforços em toda a organização durante crises cibernéticas.
- Detecção Avançada de Ameaças: A capacidade de detectar ameaças avançadas e persistentes se tornará fundamental, com o uso de tecnologias como detecção de anomalias e análise comportamental.
- Resposta Baseada em Dados: A análise de dados em tempo real desempenhará um papel crucial na identificação e resposta a incidentes, permitindo uma visão mais precisa das ameaças em evolução.
- Simulações de Crise: Organizações investirão em simulações regulares de crises cibernéticas para treinar equipes de resposta e avaliar a eficácia dos processos de resposta.
- Colaboração Externa: A colaboração com outras organizações, como órgãos reguladores e empresas de segurança cibernética, será essencial para combater ameaças compartilhadas.
- Proteção de Identidade Digital: A proteção das identidades digitais dos usuários se tornará uma prioridade, com a autenticação multifatorial e soluções de gerenciamento de identidade em destaque.
- Resposta à Internet das Coisas (IoT): Com a proliferação de dispositivos IoT, as organizações desenvolverão estratégias específicas para responder a incidentes relacionados à IoT.
- Testes de Resposta a Incidentes em Tempo Real: Organizações conduzirão testes de resposta a incidentes em tempo real para avaliar a eficácia de seus processos de maneira prática e dinâmica.

Essas tendências refletem a crescente sofisticação das ameaças cibernéticas e a

necessidade de adaptação contínua na Capability de Incident & Crisis Response.

À medida que o cenário de segurança cibernética evolui, essa capability desempenhará um papel fundamental na proteção da reputação, dos ativos e na garantia da continuidade das operações das organizações.

KPIs Usuais

A capacidade de Incident & Crisis Response desempenha um papel crucial na proteção das operações e ativos de uma organização contra ameaças cibernéticas.

A avaliação de seu desempenho por meio de KPIs é essencial para garantir uma resposta eficaz a incidentes e crises de segurança cibernética.

Abaixo, uma lista dos principais KPIs usuais no contexto do CIO Codex Capability Framework, que ajudam a medir o desempenho da Incident & Crisis Response:

- Tempo Médio de Detecção de Incidentes (Mean Time to Detect Incidents): Mede o tempo médio necessário para identificar um incidente de segurança desde o momento em que ocorre.
- Tempo Médio de Resposta a Incidentes (Mean Time to Respond to Incidents): Calcula o tempo médio que a equipe leva para iniciar a resposta a um incidente após sua detecção.
- Taxa de Resolução Bem-Sucedida de Incidentes (Successful Incident Resolution Rate): Avalia a eficácia da equipe de resposta em resolver incidentes de segurança de forma satisfatória.
- Taxa de Conclusão de Planos de Resposta (Response Plan Completion Rate): Indica quantos incidentes tiveram planos de resposta concluídos e seguidos adequadamente.
- Tempo Médio de Recuperação (Mean Time to Recovery): Calcula o tempo médio necessário para recuperar a funcionalidade total após a resolução de um incidente.
- Taxa de Reincidentes (Reincident Rate): Mede a frequência com que incidentes semelhantes ocorrem novamente após a resolução.
- Taxa de Adoção de Automação (Automation Adoption Rate): Avalia o uso de automação na detecção e resposta a incidentes, o que pode acelerar as ações de resposta.

- Avaliação de Comunicação de Crises (Crisis Communication Assessment): Mede a eficácia da comunicação durante crises, avaliando a clareza e a rapidez das informações compartilhadas com partes interessadas internas e externas.
- Taxa de Realização de Simulações (Simulation Execution Rate): Avalia a frequência com que a equipe realiza simulações de incidentes para garantir a prontidão.
- Tempo Médio de Análise Pós-Incidente (Mean Time for Post-Incident Analysis): Calcula o tempo médio gasto na análise pós-incidente para identificar lições aprendidas e melhorias necessárias.
- Taxa de Adoção de Novas Técnicas de Resposta (Adoption Rate of New Response Techniques): Indica a rapidez com que a equipe incorpora técnicas inovadoras de resposta a incidentes.
- Taxa de Coordenação de Resposta Eficiente (Efficient Response Coordination Rate): Avalia a habilidade da equipe de orquestrar esforços interdepartamentais de forma eficaz durante incidentes.
- Taxa de Avaliação de Impacto (Impact Assessment Rate): Mede a frequência com que a organização realiza avaliações de impacto após incidentes.
- Avaliação de Resposta a Crises de Segurança (Security Crisis Response Assessment): Mede a eficácia geral da resposta a crises de segurança cibernética, considerando a gestão de incidentes graves.
- Taxa de Melhoria Contínua (Continuous Improvement Rate): Avalia o compromisso da organização em implementar melhorias com base nas lições aprendidas após incidentes.

Esses KPIs ajudam a garantir que a capacidade de Incident & Crisis Response seja eficiente e eficaz na proteção da organização contra ameaças cibernéticas em constante evolução.

A medição regular desses indicadores é fundamental para aprimorar a capacidade de resposta e mitigação de incidentes e crises de segurança cibernética.

Exemplos de OKRs

A capability de Incident & Crisis Response na macro capability Planning & Running da camada Cybersecurity desempenha um papel crítico no gerenciamento e resposta a incidentes e crises de segurança cibernética.

Essa capability é vital para garantir a continuidade das operações de TI e minimizar os danos causados por incidentes de segurança.

Ela envolve a identificação rápida de incidentes de segurança, a implementação de medidas para mitigar o impacto e a coordenação de esforços para resolver o incidente.

Além disso, inclui a comunicação eficaz com as partes interessadas durante e após o incidente, bem como a análise pós-incidente para prevenir futuras ocorrências.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Identificação Rápida de Incidentes de Segurança

Objetivo: Garantir que os incidentes de segurança sejam identificados o mais rápido possível.

- KR1: Implementar sistemas de detecção de ameaças em tempo real.
- KR2: Estabelecer alertas automatizados para atividades suspeitas.
- KR3: Realizar treinamento contínuo da equipe para o reconhecimento de ameaças.

Mitigação de Impacto de Incidentes

Objetivo: Implementar medidas imediatas para minimizar o impacto de incidentes de segurança.

- KR1: Desenvolver planos de ação específicos para cada tipo de incidente.
- KR2: Estabelecer procedimentos de resposta a incidentes que incluam ações imediatas.
- KR3: Manter uma equipe de prontidão para responder a incidentes 24/7.

Coordenação de Esforços para Resolver Incidentes

Objetivo: Coordenar a equipe de resposta a incidentes para resolver incidentes de segurança de forma eficaz.

- KR1: Designar papéis e responsabilidades claros para os membros da equipe de resposta a incidentes.
- KR2: Realizar simulações regulares de resposta a incidentes para garantir prontidão.
- KR3: Estabelecer canais de comunicação eficazes entre os membros da equipe.

Comunicação Eficaz com Partes Interessadas

Objetivo: Manter as partes interessadas informadas durante e após um incidente de segurança.

- KR1: Desenvolver um plano de comunicação de incidentes que inclua os principais stakeholders.
- KR2: prover atualizações regulares sobre o status do incidente e as medidas de mitigação.
- KR3: Realizar revisões pós-incidente com as partes interessadas para identificar lições aprendidas.

Análise Pós-Incidente e Prevenção Futura

Objetivo: Realizar análises pós-incidente para identificar causas raízes e prevenir futuras ocorrências.

- KR1: Conduzir investigações detalhadas após cada incidente de segurança.
- KR2: Implementar medidas corretivas para eliminar as causas raízes identificadas.
- KR3: Atualizar políticas de segurança com base nas lições aprendidas.

Através desses OKRs, a capability de Incident & Crisis Response assegura uma resposta eficaz a incidentes de segurança cibernética, minimiza o impacto nas operações de TI e ajuda a prevenir futuras ocorrências.

Isso é fundamental para a proteção dos ativos da organização e a manutenção de uma postura de segurança cibernética eficaz.

Critérios para Avaliação de Maturidade

A capability Incident & Crisis Response, inserida na macro capability Planning & Running e na camada Cybersecurity, desempenha um papel vital no gerenciamento e resposta a incidentes e crises de segurança cibernética.

Avaliar sua maturidade é essencial para garantir a eficácia na identificação e resposta a incidentes.

Para essa avaliação, seguem critérios inspirados no modelo CMMI, considerando cinco níveis de maturidade: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

Nível de Maturidade Inexistente

- Não há processos ou procedimentos formais para identificar ou responder a incidentes de segurança.
- Ausência de conscientização sobre a importância da capacidade de resposta a incidentes.
- Não há equipe designada para gerenciar incidentes de segurança cibernética.
- Falta de ferramentas ou tecnologias para detectar incidentes de segurança.
- Ausência de um plano de comunicação em caso de incidentes.

Nível de Maturidade Inicial

- Processos iniciais para identificar incidentes, mas não são abrangentes.
- Conscientização limitada sobre a importância da capacidade de resposta a incidentes.
- Uma equipe designada para gerenciar incidentes, mas com recursos limitados.
- Algumas ferramentas de detecção de incidentes estão em uso.
- Um plano de comunicação em caso de incidentes está em

desenvolvimento.

Nível de Maturidade Definido

- Processos formalizados e documentados para identificar e responder a incidentes.
- Conscientização crescente sobre a importância da capacidade de resposta a incidentes.
- Uma equipe bem definida e treinada para gerenciar incidentes.
- Ferramentas de detecção de incidentes são utilizadas de forma consistente.
- Um plano de comunicação em caso de incidentes está em vigor.

Nível de Maturidade Gerenciado

- Processos de resposta a incidentes são eficazes e adaptáveis.
- Conscientização disseminada sobre a importância da capacidade de resposta a incidentes.
- Uma equipe experiente e bem equipada gerencia incidentes de segurança.
- Monitoramento contínuo e detecção proativa de incidentes.
- Comunicação eficaz com as partes interessadas durante e após os incidentes.

Nível de Maturidade Otimizado

- Processos de resposta a incidentes são altamente otimizados e inovadores.
- Conscientização e treinamento contínuos sobre segurança cibernética.
- Uma equipe de elite lidera a gestão de incidentes.
- Detecção avançada de incidentes com análise comportamental.
- Comunicação ágil e eficaz com as partes interessadas e análise pós-incidente aprimorada para prevenir futuros incidentes.

A avaliação de maturidade da capability Incident & Crisis Response é fundamental

para garantir a prontidão e eficácia da organização na gestão de incidentes e crises de segurança cibernética.

À medida que a maturidade aumenta, a capacidade de identificar, responder e mitigar incidentes melhora, fortalecendo a postura de segurança cibernética da organização.

Convergência com Frameworks de Mercado

A capability Incident & Crisis Response, inserida na macro capability Planning & Running e na camada Cybersecurity, desempenha um papel crucial no gerenciamento e resposta a incidentes e crises de segurança cibernética.

Esta capability inclui a rápida identificação de incidentes de segurança, implementação de medidas para mitigar o impacto, coordenação de esforços para resolver o incidente, comunicação eficaz com as partes interessadas e análise pós-incidente para prevenção de futuras ocorrências.

A seguir, é analisada a convergência desta capability em relação a um conjunto dez frameworks de mercado reconhecidos e bem estabelecidos em suas respectivas áreas de expertise:

COBIT

- Nível de Convergência: Alto
- Racional: O COBIT fornece um framework abrangente para governança de TI, incluindo gestão de riscos e segurança da informação. A Incident & Crisis Response se alinha estreitamente com este framework, oferecendo mecanismos para a gestão eficaz de incidentes e crises, um aspecto crucial da governança de TI.

ITIL

- Nível de Convergência: Alto
- Racional: O ITIL foca na gestão de serviços de TI, incluindo a gestão de incidentes. A Incident & Crisis Response complementa o ITIL ao prover

um método estruturado para responder a incidentes de segurança, garantindo a continuidade dos serviços de TI.

SAFe

- Nível de Convergência: Médio
- Racional: Embora o SAFe seja centrado em práticas ágeis e desenvolvimento de software, a integração da Incident & Crisis Response é benéfica para a identificação e resposta rápida a incidentes de segurança em ambientes de desenvolvimento ágil.

PMI

- Nível de Convergência: Médio
- Racional: Em projetos gerenciados com base nas práticas do PMI, a capacidade de responder eficazmente a incidentes e crises é vital. A Incident & Crisis Response apoia a gestão de riscos e a resiliência do projeto.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI foca na melhoria dos processos. A Incident & Crisis Response ajuda a criar processos mais robustos e seguros, contribuindo para a maturidade da gestão de segurança.

TOGAF

- Nível de Convergência: Médio
- Racional: O TOGAF aborda a arquitetura empresarial, onde a Incident & Crisis Response pode ser integrada para garantir que considerações de segurança sejam incorporadas no design arquitetônico e na gestão de incidentes.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em ambientes DevOps e SRE, a rápida identificação e resposta a incidentes são fundamentais. A Incident & Crisis Response fornece estruturas para gerenciar esses incidentes eficientemente.

NIST

- Nível de Convergência: Alto
- Racional: O NIST fornece diretrizes detalhadas para a segurança cibernética, incluindo a gestão de incidentes. A Incident & Crisis Response está alinhada com essas diretrizes, oferecendo um framework para responder a incidentes conforme as melhores práticas.

Six Sigma

- Nível de Convergência: Baixo
- Racional: Embora o Six Sigma se concentre na melhoria de processos e redução de defeitos, a Incident & Crisis Response pode contribuir para a melhoria da qualidade dos processos de segurança, minimizando riscos e incidentes.

Lean IT

- Nível de Convergência: Baixo
- Racional: O Lean IT visa a eficiência operacional, onde a Incident & Crisis Response pode ajudar indiretamente, reduzindo o tempo de inatividade e melhorando a eficiência na resposta a incidentes.

A capability Incident & Crisis Response é vital para garantir a resiliência e segurança organizacional.

KPIs relevantes incluem tempo de resposta a incidentes, tempo de recuperação após

incidentes e eficácia das comunicações durante crises.

Esta capability contribui significativamente para a capacidade de uma organização de operar de forma segura e eficaz em um ambiente de ameaças cibernéticas em constante evolução.

Processos e Atividades

Develop Incident Response Plans

O desenvolvimento de planos detalhados para resposta a incidentes de segurança é uma atividade crucial que visa preparar a organização para lidar eficientemente com incidentes de segurança cibernética.

Este processo envolve a criação de planos abrangentes que detalham as ações a serem tomadas em resposta a diferentes tipos de incidentes.

O plano deve incluir procedimentos específicos para detecção, análise, contenção, erradicação e recuperação de incidentes.

Além disso, deve abordar a comunicação interna e externa durante um incidente, assegurando que todas as partes interessadas sejam informadas de maneira oportuna e adequada.

O plano deve ser desenvolvido em colaboração com várias áreas da organização para garantir que todos os aspectos de segurança, operacionais e de negócios sejam considerados.

Documentar claramente os papéis e responsabilidades de cada membro da equipe de resposta é essencial para uma execução eficaz.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Conduct Risk Assessment	Realizar uma avaliação de riscos para identificar possíveis incidentes de segurança.	Dados de risco, análise de ameaças	Relatório de avaliação de riscos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Define Incident Scenarios	Definir cenários de incidentes que podem impactar a organização.	Relatório de avaliação de riscos	Lista de cenários de incidentes	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Develop Response Procedures	Desenvolver procedimentos de resposta para cada cenário de incidente identificado.	Lista de cenários de incidentes	Procedimentos de resposta	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
4	Assign Roles and Responsibilities	Atribuir papéis e responsabilidades para a equipe de resposta a incidentes.	Procedimentos de resposta	Documento de papéis e responsabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

5	Document Response Plan	Documentar o plano de resposta a incidentes de forma detalhada e acessível.	Documento de papéis e responsabilidades	Plano de resposta a incidentes	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Identify Incident Scenarios

A identificação de cenários de incidentes de segurança é um processo essencial para preparar a organização para possíveis eventos adversos.

Este processo envolve a análise de ameaças e vulnerabilidades conhecidas, além de considerar as especificidades do ambiente de TI da organização.

Os cenários devem abranger uma ampla gama de incidentes potenciais, desde ataques cibernéticos e violações de dados até falhas sistêmicas e desastres naturais.

A identificação precisa desses cenários permite à organização desenvolver planos de resposta direcionados e eficazes.

A colaboração entre diferentes áreas da TI e do negócio é fundamental para garantir que todos os possíveis incidentes sejam considerados e que as respostas planejadas sejam adequadas e eficazes.

- PDCA focus: Plan
- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Analyze Threat Landscape	Analisar o panorama de ameaças para identificar possíveis cenários de incidentes.	Dados de ameaças, inteligência de segurança	Relatório de análise de ameaças	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

2	Identify Vulnerabilities	Identificar vulnerabilidades no ambiente de TI que possam ser exploradas.	Relatório de análise de ameaças	Lista de vulnerabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Define Incident Types	Definir os tipos de incidentes que a organização pode enfrentar.	Lista de vulnerabilidades	Lista de tipos de incidentes	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
4	Develop Incident Scenarios	Desenvolver cenários detalhados para cada tipo de incidente identificado.	Lista de tipos de incidentes	Cenários de incidentes	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Document Incident Scenarios	Documentar todos os cenários de incidentes de forma clara e acessível.	Cenários de incidentes	Documentação de cenários	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

Execute Incident Response

A execução das respostas a incidentes conforme planejado é fundamental para mitigar os impactos negativos de incidentes de segurança cibernética.

Este processo envolve a implementação dos procedimentos de resposta detalhados nos planos de resposta a incidentes.

As ações incluem a detecção, análise, contenção, erradicação e recuperação de incidentes, além da comunicação contínua com as partes interessadas internas e externas.

A coordenação eficiente entre as diversas áreas da organização é crucial para uma resposta rápida e eficaz.

O treinamento contínuo e simulações ajudam a equipe de resposta a estar preparada para executar os planos de maneira eficiente.

A execução eficaz da resposta a incidentes minimiza os danos, restaura rapidamente as operações normais e fortalece a postura de segurança da organização.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Detect Incident	Detectar o incidente de segurança utilizando ferramentas e técnicas de monitoramento.	Ferramentas de monitoramento	Notificação de incidente	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

2	Analyze Incident	Analisar o incidente para determinar seu escopo e impacto.	Notificação de incidente	Relatório de análise de incidente	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Contain Incident	Conter o incidente para evitar sua propagação e minimizar o impacto.	Relatório de análise de incidente	Medidas de contenção implementadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
4	Eradicate Incident	Erradicar a causa raiz do incidente e restaurar os sistemas afetados.	Medidas de contenção implementadas	Sistemas restaurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

5	Recover Systems	Recuperar e restaurar as operações normais dos sistemas afetados pelo incidente.	Sistemas restaurados	Operações normalizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Monitor Incident Response Performance

O monitoramento contínuo do desempenho das respostas a incidentes é essencial para garantir a eficácia dos planos de resposta e identificar áreas de melhoria.

Este processo envolve a coleta e análise de dados sobre as respostas a incidentes, incluindo o tempo de resposta, a eficácia das ações tomadas e o impacto residual dos incidentes.

As métricas de desempenho são utilizadas para avaliar a capacidade de resposta da organização e para ajustar os planos de resposta conforme necessário.

O feedback contínuo é essencial para a melhoria contínua dos processos de resposta a incidentes.

Este processo também inclui a realização de auditorias e revisões pós-incidente para capturar lições aprendidas e implementar melhorias nos planos de resposta.

- PDCA focus: Check
- Periodicidade: Mensal

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Collect Incident Data	Coletar dados detalhados sobre cada incidente e a resposta realizada.	Relatórios de incidentes	Dados de incidentes coletados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Analyze Response Performance	Analisar o desempenho das respostas a incidentes utilizando métricas definidas.	Dados de incidentes coletados	Relatórios de desempenho	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Conduct Post-Incident Reviews	Realizar revisões pós-incidente para identificar lições aprendidas e áreas de melhoria.	Relatórios de desempenho	Relatórios de revisão pós-incidente	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Update Response Metrics	Atualizar as métricas de resposta com base nas revisões pós-incidente e novas informações.	Relatórios de revisão pós-incidente	Métricas atualizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

5	Report Findings	Relatar as descobertas e recomendações de melhoria para a alta gestão e partes interessadas.	Métricas atualizadas	Relatórios de descobertas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

Review and Improve Response Plans

A revisão e melhoria contínua dos planos de resposta a incidentes é um processo essencial para assegurar que a organização esteja sempre preparada para lidar com novos desafios de segurança cibernética.

Este processo envolve a análise detalhada dos resultados do monitoramento e das revisões pós-incidente para identificar áreas de melhoria nos planos de resposta.

As lições aprendidas são integradas aos planos existentes para fortalecer a capacidade de resposta.

Além disso, o processo inclui a atualização dos procedimentos, a realização de treinamentos regulares e a validação dos planos através de simulações e exercícios.

A melhoria contínua dos planos de resposta garante que a organização esteja sempre em uma postura de prontidão, capaz de responder eficazmente a qualquer incidente de segurança.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Analyze Review Findings	Analisar as descobertas das revisões pós-incidente e monitoramento de desempenho.	Relatórios de revisão pós-incidente	Análise de descobertas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Identify Improvement Areas	Identificar áreas de melhoria nos planos de resposta com base na análise das descobertas.	Análise de descobertas	Lista de áreas de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Update Response Procedures	Atualizar os procedimentos de resposta a incidentes para incorporar as melhorias identificadas.	Lista de áreas de melhoria	Procedimentos atualizados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity
4	Conduct Training Sessions	Realizar sessões de treinamento para assegurar que a equipe esteja familiarizada com os procedimentos atualizados.	Procedimentos atualizados	Sessões de treinamento realizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

5	Validate Response Plans	Validar os planos de resposta através de simulações e exercícios para assegurar sua eficácia.	Procedimentos atualizados	Planos validados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity