CAPÍTULO 01

RESPOSTA A INCIDENTE, FORENSE DIGITAL E SUAS ATUAÇÕES

	Resposta a Incidentes	Análise Forense
Metas	▪ Focado em determinar uma resposta rápida (gerenciar eventos em tempo real)	▪ Concluir a análise e coletar riscos e impactos (parte de uma confor midade programada, descoberta legal ou investigação policial) ▪ Focado em uma compreensão completa e resolução completa de uma violação
Requisitos de Dados	▪ Requer fontes de dados de curto prazo, muitas vezes não mais do que um mês	▪ Requer logs e arquivos muito mais duradouros. Um ataque bem-sucedido dura entre 150 e 300 dias
Habilidades da Equipe	▪ Fortes recursos de análise de log e análise de malware. Capaci-dade de isolar rapidamente um dispositivo infectado e desenvolver meios para mitigar ou colocar o dispositivo em quarentena ▪ Interação com outros membros da equipe de segurança e operações	▪ Fortes recursos de análise de log e análise de malware ▪ Requer interação com um conjunto muito mais amplo de departamentos, incluindo operações, jurídico, RH e conformidade
Benefícios	▪ Primeira linha de defesa em operações de segurança ▪ Elimine uma ameaça em uma máquina em tempo real ▪ Mantendo as violações isoladas e limitadas no impacto	▪ Análise pós-incidente ▪ Resolução de todas as ameaças com a análise cuidadosa de toda uma cadeia de ataque ▪ Capacidade de resposta judicial

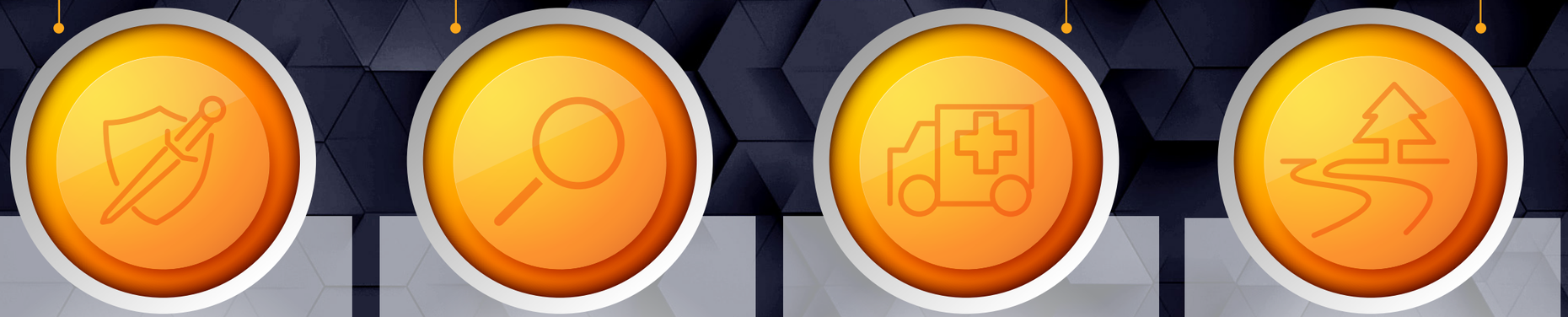
CAPÍTULO 02

PROCESSO DE RESPOSTA A INCIDENTE

Com um programa bem-sucedido de Resposta a Incidentes, os danos podem ser atenuados ou totalmente evitados.

CAPÍTULO 03

CICLO DE VIDA DE RESPOSTA A INCIDENTES PELO NIST



Preparação

- Preparação para tratar incidentes
- Prevenção de incidentes

Detecção e Análise

- Vetores de ataque
- Sinais de um incidente
- Fontes de precursores e indicadores
- Análise de incidente
- Documentação de incidente
- Priorização de incidente
- Notificação de incidente

Contenção, Erradicação e Recuperação

- Definindo uma estratégia de contenção
- Coleta e manuseio de evidências
- Identificação dos hosts atacantes
- Erradicação e recuperação

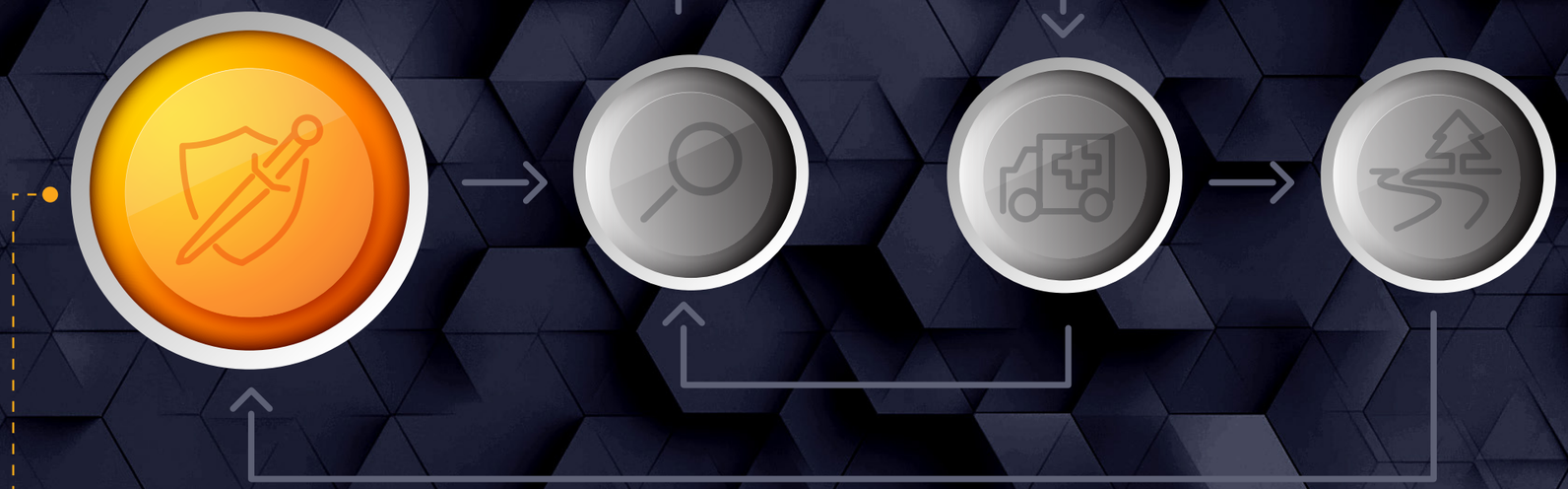
Atividades Pós-Incidente

- Lições aprendidas
- Utilização dos dados coletados no incidente
- Retenção de evidências
- Checklist de tratamento de incidentes
- Recomendações

CAPÍTULO 04

FASE 1 DO CICLO DE VIDA DE RESPOSTA A INCIDENTES:

PREPARAÇÃO

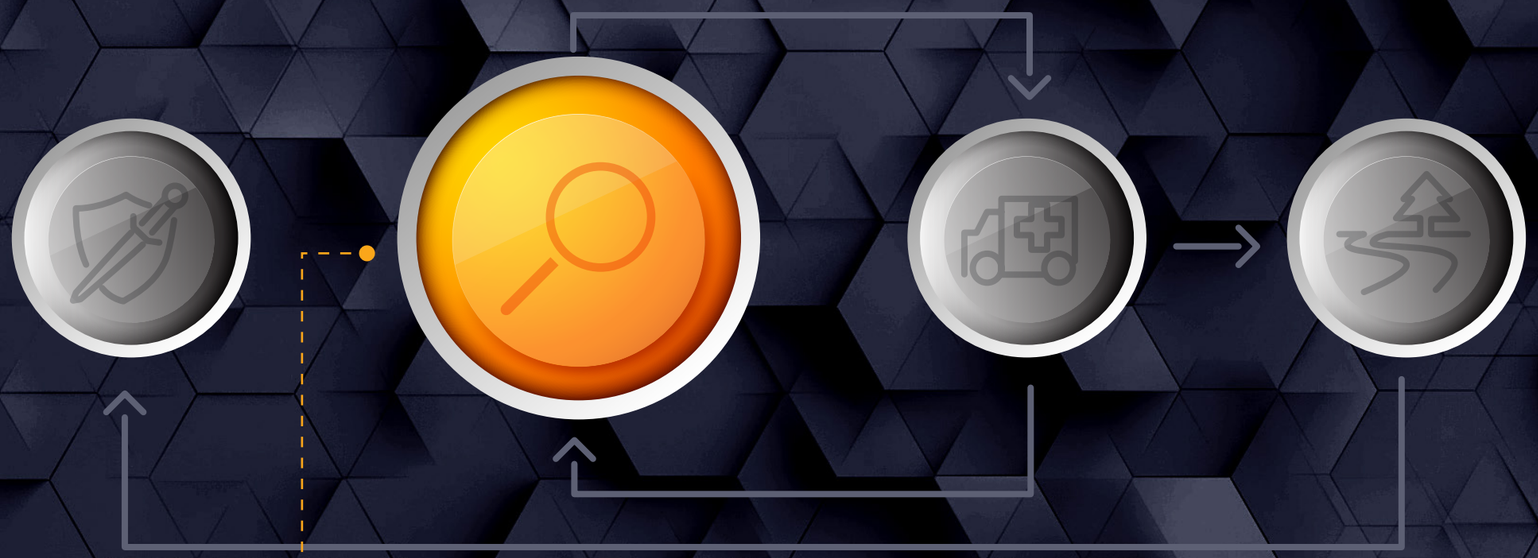


- Criação e/ou revisão da política de gestão de incidentes
- Avaliação de riscos
- Identificação de ativos críticos
- Definição de priorização
- Criticidade de incidentes
- Composição do CSIRT

CAPÍTULO 05

FASE 2 DO CICLO DE VIDA DE RESPOSTA A INCIDENTES:

DETECÇÃO E ANÁLISE

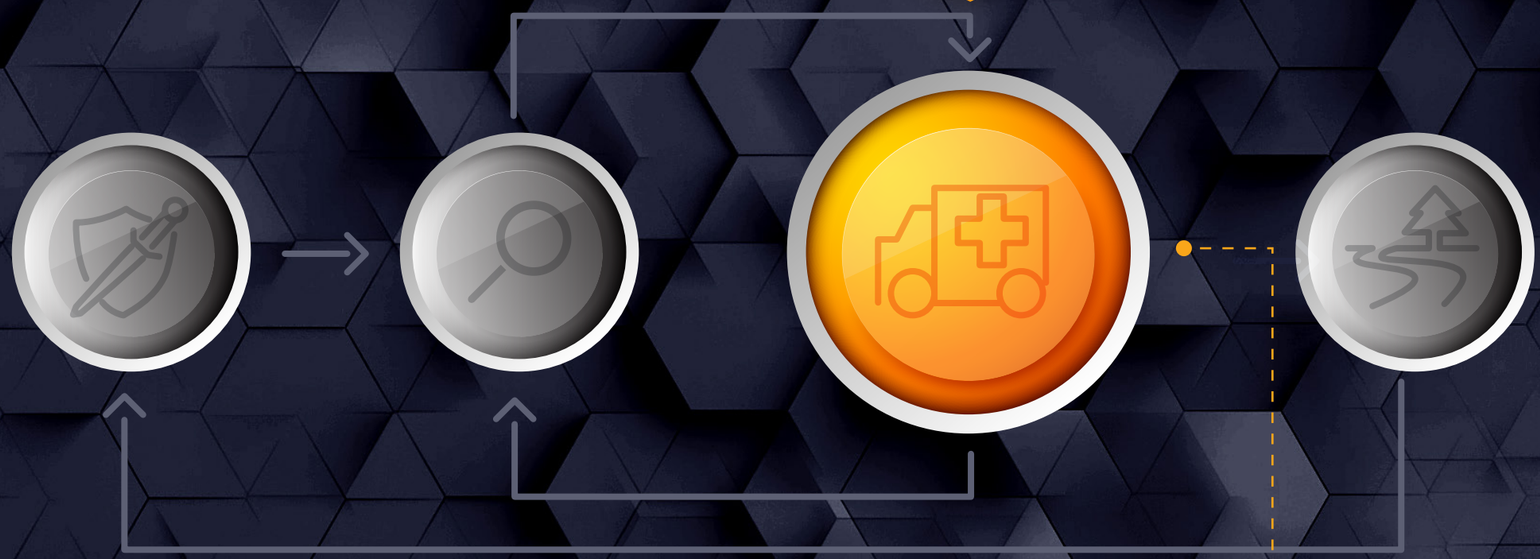


- Monitoramento de sistemas de tecnologia
- Detecção de desvios da operação normal
- Triagem e estabelecimento do tipo e severidade do incidente
- Notificação das partes interessadas
- Documentação de todos os fatos

CAPÍTULO 06

FASE 3 DO CICLO DE VIDA DE RESPOSTA A INCIDENTES:

CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

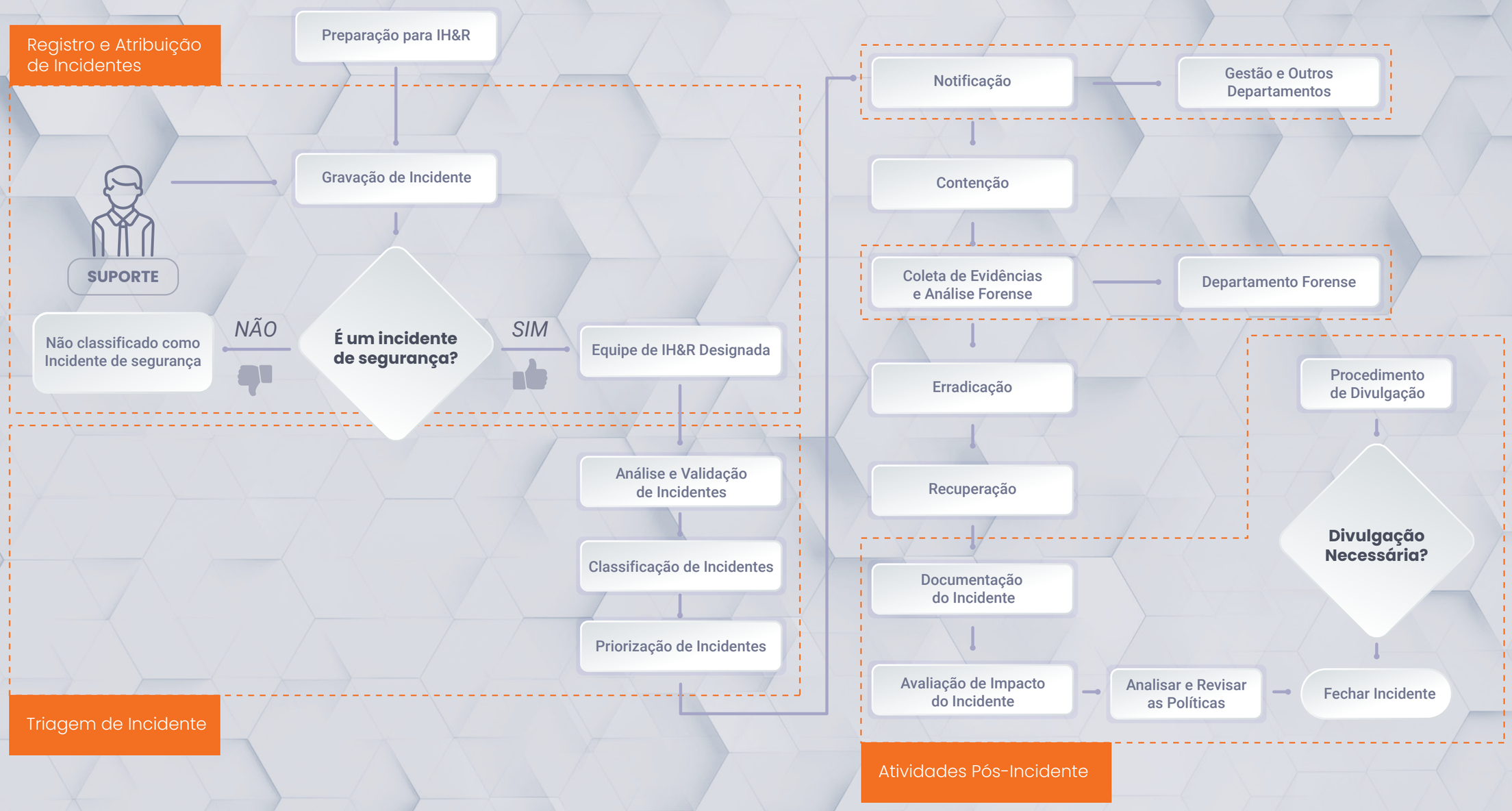


- Contenção de curto e longo prazo
- Remoção de infecção do sistema alvo
- Coleta de evidências
- Identificação de causa raiz
- Retorno de sistemas a operação normal

CAPÍTULO 07

FASE 4 DO CICLO DE VIDA DE RESPOSTA A INCIDENTES:

FLUXO DE UM PROCESSO DE RESPOSTA A INCIDENTE



CAPÍTULO 08

PREPARANDO UMA ORGANIZAÇÃO PARA UM INCIDENTE

das organizações em todo o mundo experimentaram pelo menos um incidente de segurança cibernética no ano passado

$3.62 MILLION

é o custo médio de uma violação

das organizações não tem um plano adequado de resposta a incidente de segurança cibernética

IDENTIFIQUE OS ATIVOS QUE VOCÊ PRECISA PROTEGER

- Qual é o tipo de dado ou informação que você está tentando proteger e onde ele está?
- Priorize os ativos mais importantes e valiosos para ajudar a desenvolver seu plano de resposta.

IDENTIFICAR RISCOS POTENCIAIS

- Sua organização é vulnerável?
- Como você lida com vulnerabilidades conhecidas
- Você realiza testes de penetração? Você entende seus riscos financeiramente?

CRIE UM PLANO DE RESPOSTA A INCIDENTES

- Criar um plano de resposta a incidentes
- Definir um incidente.
- Como você responderá e quem responderá?

CRIAR E APOIAR EQUIPES DE RESPOSTA

- Equipar a equipe de resposta com suporte e tecnologia para ter sucesso
- Esteja preparado com backups de dados e saiba como conter ameaças potenciais.

IMPLANTAR PLANO COM SUPORTE EXECUTIVO

- A resposta a incidentes é uma questão de nível de diretoria.
- Avalie seus piores e melhores cenários de uma perspectiva de negócios.

PESSOAS EXECUTAM PLANOS, NÃO TECNOLOGIA

- Combine força e talento com necessidades em todos os cenários.
- Use cenários e exercícios para identificar onde sua equipe precisa de mais treinamento.

MANTENHA SEU PESSOAL E PLANEJA EM FORMA

- Realize testes regulares de seu plano.
- Atualize o plano à medida que as ameaças e suas consequências evoluem.

REAVALIAR E INVESTIR

- O seu plano protege os problemas do seu alvo?
- Seu plano reduz o risco geral do negócio?
- Você pode fazer o seu plano mais rentável em termos de tempo, recursos e pessoal?

REFINAR E MELHORAR

- Nova tecnologia, incluindo lote, novas ameaças e mudança de pessoal. Mude seu plano de acordo.
- Apesar das organizações empregarem as melhores práticas de resposta a incidentes. dano está crescendo. Você continua investindo na melhoria de seus recursos de resposta a incidentes?

CAPÍTULO 09

ESTRATÉGIA E TÁTICA DE UM PLANO DE RESPOSTA A INCIDENTE

Chefe Executivo

Precisa estar no loop e ciente do que está acontecendo em Resposta a Incidentes

Auditoria

Podem ajudar a colocar um highlight em coisas que parecem estar esquecidas

Recursos Humanos

É bom ter parceria para garantir celeridade e transparência em promoção e demissão de colaboradores (revisão dos acessos), além de Programas de Ameaças Internas (Insider Threats)

Comunicações Relações Públicas

Tecnologia da Informação

Parceria sólida com todas as áreas de TI

Jurídico / Legal

Comitê Diretivo

Para garantir recursos e financiamento

Clientes

! APOIO DA ALTA ADMINISTRAÇÃO

Você precisará de suporte para que os logs de sistemas novos ou existentes sejam encaminhados para SIEM.

- Agentes devem ser instalados em sistemas novos para monitoração contínua.
- Firewall internos e outros mecanismos não podem bloquear a habilidade do time de security em detectar, monitorar, responder e recuperar um incidente.
- O Executivo precisa conhecer a missão de IR.
- Shadown IT não ficará feliz com o seu monitoramento.
- Estar ciente para não causar indisponibilidade no ambiente.

CAPÍTULO 10

LEIS E REGULAMENTAÇÕES

PCI DSS
Payment Card Industry Data Security Standard

Padrão de segurança para proteção de dados de cartões de pagamento. Requisitos para prevenção, detecção e resposta a incidentes de segurança.

California SB 1386

Lei estadual da Califórnia que exige notificação de violações de segurança que envolvam informações pessoais.

HIPAA
Health Insurance Portability and Accountability Act

Lei dos EUA para proteção de informações de saúde identificáveis. Exige medidas de segurança e diretrizes para resposta a incidentes.

NYS DFS 500
New York State Department of Financial Services Cybersecurity Regulation

Regulamento de segurança cibernética para instituições financeiras de Nova York. Inclui diretrizes para resposta a incidentes e notificação de violações de segurança.

FISMA
Federal Information Security Management Act

Lei federal dos EUA para segurança da informação em agências governamentais. Requer desenvolvimento de programas de segurança e resposta a incidentes.

SEC
Securities and Exchange Commission

Agência reguladora dos EUA para o mercado de valores mobiliários. Emite regulamentos relacionados à segurança cibernética, incluindo medidas de resposta a incidentes.

NERC-CIP
North American Electric Reliability Corporation Critical Infrastructure Protection

Padrões de segurança para o setor elétrico na América do Norte. Requisitos para proteção de infraestruturas críticas e resposta a ameaças cibernéticas.

GDPR
General Data Protection Regulation

Regulamento da UE para proteção de dados pessoais. Exige proteção de dados e notificação de violações às autoridades e indivíduos afetados.

CAPÍTULO 11

CONSTRUINDO O TIME DE RESPOSTA A INCIDENTES (CSIRT)

CAPÍTULO 12 IDENTIFICANDO OS ATIVOS ORGANIZACIONAIS E O RISCO

! GERENCIAMENTO DE ATIVOS

- Pode fazer parte e ser gerenciados os Softwares e o Hardwares
- Criticidade dos ativos precisa ser levada em conta
- Metas de DR/BCP e RTO/RPO precisam ser consideradas
- Um CMDB (Change Management Database) maduro que ilustra relacionamentos com outros ativos é necessário
- Informações e documentações atualizadas!

GERENCIAMENTO DE RISCO - FONTE DE DADOS

Dados de Avaliações de Riscos e Inteligência

COMO REALIZAR UMA AVALIAÇÃO DE RISCO CIBERNÉTICO

Faça um ***inventário*** de seus ativos e determine sua ***importância*** para sua organização

Identifique e priorize as vulnerabilidades que representam a maior ***ameaça*** aos seus ativos críticos

Calcule seu ***risco cibernético*** como uma combinação de probabilidade e impacto

CAPÍTULO 13

THREAT INTELLIGENCE E A VISIBILIDADE DE RISCO

OPEN SOURCE THREAT INTELLIGENCE

AlienVault OTX:
https://otx.alienvault.com/

Open CTI BR:
https://github.com/openctibr/threatFeeds

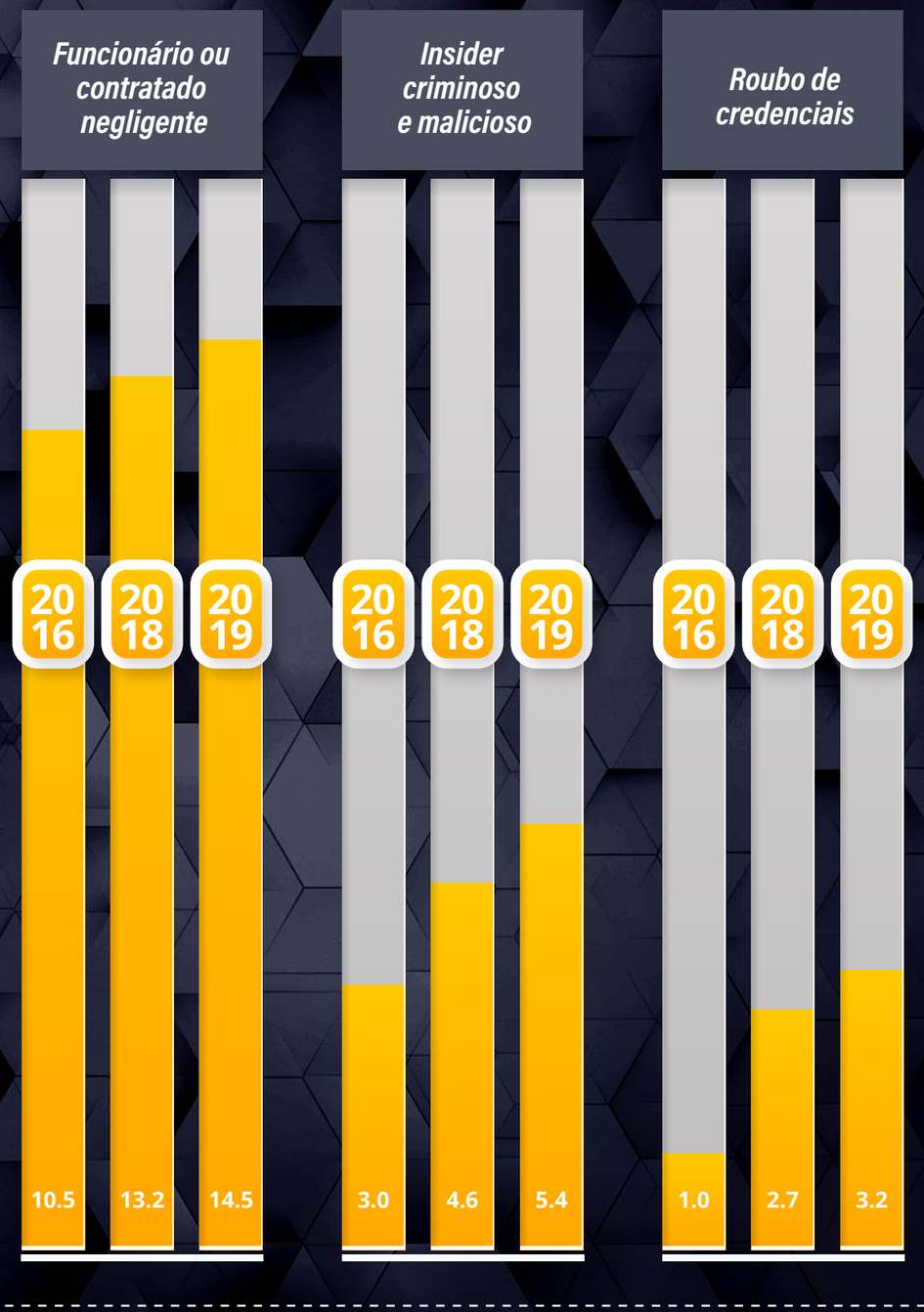
VirusTotal:
https://www.virustotal.com/gui/home/upload

THREAT INTELLIGENCE COMERCIAL

50 Plataformas de Threat Intelligence com Insights Valiosos:

https://digitalguardian.com/blog/50-threat-intelligence-tools-valuable-threat-insights

VISIBILIDADE DE RISCO:



CAPÍTULO 14

PROTEGENDO UMA ORGANIZAÇÃO DE UM INCIDENTE

UMA DEFESA EFETIVA REQUER ORGANIZAÇÃO

ANTES DO INCIDENTE:
BOA CIBERHIGIENE E GESTÃO DE VULNERABILIDADES

O CSIRT PRECISA DE ACESSO A DOCUMENTAÇÃO CRÍTICA E ATUALIZADA:

- Diagramas de Rede
- Documentação de Portas e Protocolos
- Baselines / Gold Images
- Arquivos de configuração

MANTENHA EM SEGURANÇA
AS CONFIGURAÇÕES, BACKUPS E BASELINES.

UMA *GESTÃO DE VULNERABILIDADES MADURA* PODE AJUDAR O CSIRT

- Provê visibilidade em vulnerabilidades que estão dentro da organização
- Gestão de patches e automação: Pentest em estações de trabalho!
- Métricas
- Aplicações de terceiros
- Sistema de placar (Score)
  Compreensível e escrito em política
  Common Vulnerability Scoring System:
  https://www.first.org/cvss/calculator/3.0

CONTROLES DE SEGURANÇA E PRIVACIDADE DO NIST 800-53

Security and Privacy Controls for Information and Organizations:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

- Tipicamente utilizado por ***Agências do Governo dos EUA***
- Inclui famílias de ***segurança e controles de privacidade***
- Utilizado em conjunto com ***Sistemas de Classificação e Avaliação de Riscos***
- Permite ***customização***

SLAS E MÉTRICAS PARA MONITORAR AS CAPACIDADES DE PROTEÇÃO

SLA (Service Level Agreement) define as responsabilidades de um provedor de serviços e a expectativa do cliente.

EXEMPLO:
TI vai remediar vulnerabilidades com CVSS de 9.0 ou superior com exploração ativa dentro de 48 horas.

Outros Exemplos:
Resultados do Pentest
Resultados do scan de vulnerabilidades por tipo e severidade
Porcentagem de incidentes detectados por controles internos
Porcentagem do budget de Segurança da Informação

CAPÍTULO 15

AS TECNOLOGIAS EMERGENTES NA RESPOSTA A INCIDENTES

BYOD

Bring **Y**our **O**wn **D**evice

TRAGA SEU PRÓPRIO APARELHO

- Tem a proposta de aumentar a produtividade do usuário por meio da sua familiaridade com seus dispositivos.
- Definição de políticas mínimas para ingressar no domínio corporativo.
- O seu Plano de Resposta a Incidentes precisa considerar as políticas de BYOD (Bring Your Own Device), caso elas sejam aceitas em sua organização.

ZTA

Zero **T**rust

CONFIANÇA ZERO

- É um modelo de segurança baseado na premissa de que ninguém é cegamente confiável e autorizado para acessar os recursos da organização até que este usuário seja validado como legítimo e autorizado.
- Fornece segurança em camadas por meio de constante reautenticação e desconfiança inerente a todos dispositivos, usuários e ações, mesmo que eles sejam parte do perímetro corporativo.

Princípios do Zero Trust:

→ Garanta a menor quantidade de privilégios.
→ Nunca confie! Sempre verifique!
→ Sempre monitore!

CASB

Cloud **A**ccess **S**ecurity **B**roker

AGENTE DE SEGURANÇA DE ACESSO À NUVEM

- CASB (Cloud Access Security Broker) é um software hospedado em nuvem ou on-premises ou ainda, hardware que age como um intermediário entre os usuários e os provedores do serviço em nuvem para aplicar políticas de segurança à medida que os recursos em nuvem são utilizados. Microsoft Cloud App Security: https://www.microsoft.com/en-us/security/business/cloud-app-security
- As políticas de segurança a serem aplicadas podem ser autenticação, logon único, autorização, mapeamento de credenciais, etc.

Pilares do CASB:

→ Visibilidade
→ Compliance
→ Segurança de dados
→ Proteção contra ameaças

SASE

Secure **A**ccess **S**ervice **E**dge

BORDA DO SERVIÇO DE ACESSO SEGURO

- SASE (Secure Access Service Edge) é uma arquitetura baseada em nuvem construída com uma combinação de serviços de segurança e rede para proteger usuários, aplicações e dados.
- O modelo SASE elimina a necessidade de soluções baseadas em perímetro e soluções legadas.
- Ao invés de entregar o tráfego para inspeção de segurança em um Appliance, por exemplo um Firewall, os usuários se conectam diretamente ao serviço de nuvem SASE, para utilizar com segurança os web services, aplicações e dados.

CAPÍTULO 16

DETECTANDO UM INCIDENTE DE SEGURANÇA

REGISTRO DE EVENTOS E INCIDENTES

Registro de eventos e incidentes hoje, amanhã e sempre!

- **Fonte dos alertas**
- **O que registrar?**

  Usuários e sistemas envolvidos

  Endereçamento IP e/ou hostnames

  Comentários e fluxo de trabalho para os respondentes

  Notificações e atribuição de ações

SOC e CSIRT são Diferentes

SOC E CSIRT NÃO SÃO A MESMA COISA

O SOC geralmente cobre múltiplos aspectos da operação de segurança, enquanto o CSIRT foca exclusivamente na resposta ao incidente.

Há ainda o termo CERT (Computer Emergency and Response Team).

SOAR

SOAR (Security Orchestration, Automation and Response) trata da integração entre diferentes soluções de segurança

- Customização de APIs entre diversos produtos de segurança.
- Permite a abstração de ferramentas e não requer que o CSIRT seja expert em tudo.
- Tomada de ações padronizadas de forma automática.
- Possibilidade de criar e executar Playbooks.

SIEM

SIEM (Security Information Event Management) trata do correlacionamento e agregação de logs a partir de uma vasta variedade de fontes

- Seja extremamente cuidadoso (a) com o fuso horário configurado. Sempre prefira UTC (Coordinated Universal Time) quando possível
- Utilize checklists para garantir que os feeds, alertas e dashboards estão funcionando corretamente
- Tenha um "dono (a)" do SIEM para mantê-lo atualizado e tunado
- Se eu tenho um SIEM, não preciso de um Syslog, certo? Veja bem...

FONTES DE DETECÇÃO

NUVEM

CASB (Cloud Access Security Broker), MFA (Autenticação Multifator), Logs SaaS (Software as a Service) Logs de Uso e Transferência de Dados (AWS, Azure, etc).

ATIVIDADE DE USUÁRIO

Tentativas de Acesso, Informação de Login, Utilização de MFA, UEBA (User Entity Behavior Analytics), Instalação de Software e Instalação de Hardware.

APLICAÇÕES

Acesso e Mudanças em Banco de Dados, Escalação de Privilégio em Aplicações, Acesso em Dados Sensíveis Modificação de Controles de Segurança, Mensagens de Notificação de Sistema e Eventos de Segurança.

DISPOSITIVOS MÓVEIS

MDM (Mobile Device Management) Logs, Instalação de Apps, Logs de Containerização, Informação de Localidade e Tentativas de Burlar os Controles de Segurança.

RECLAMAÇÕES DE USUÁRIOS

Reclamações do RH, Relatos de Usuários e Reclamações da Direção.

DESKTOPS / LAPTOPS

EDR (Endpoint Detection & Response), HIDS (Host Intrusion Detection System), Execução de Processo Mudanças em Registros, Evidência de Persistência.

SERVIDORES E INFRAESTRUTURA VIRTUALIZADA

HIDS (Host Intrusion Detection System), Gerenciamento de Virtualização, Alertas SCCM / SCOM e Alertas EDR (Endpoint Detection and Response).

SENSORES

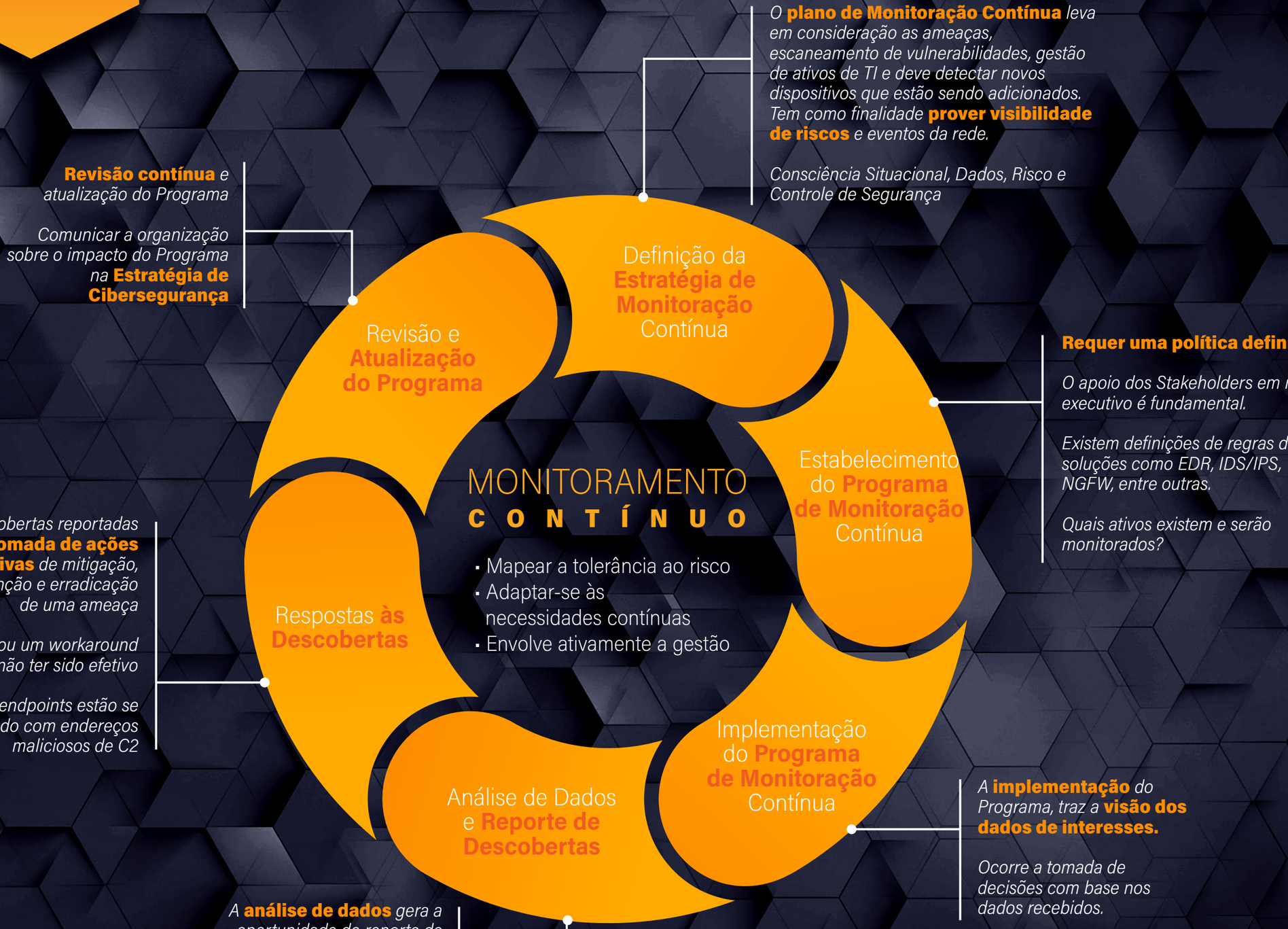
Taps de Rede.

TRÁFEGO DE REDE

IDPS (Intrusion Detection / Prevention System), Firewalls Sandbox, Proxies, DNS / DHCP, Decriptação TLS, Tabelas de Roteamento e Captura de Pacotes.

CAPÍTULO 17

DEFINIÇÃO DA ESTRATÉGIA DE MONITORAÇÃO CONTÍNUA



*O **plano de Monitoração Contínua** leva em consideração as ameaças, escaneamento de vulnerabilidades, gestão de ativos de TI e deve detectar novos dispositivos que estão sendo adicionados. Tem como finalidade **prover visibilidade de riscos** e eventos da rede.*

Consciência Situacional, Dados, Risco e Controle de Segurança

Requer uma política definida!

O apoio dos Stakeholders em nível executivo é fundamental.

Existem definições de regras de soluções como EDR, IDS/IPS, NGFW, entre outras.

Quais ativos existem e serão monitorados?

*A **implementação** do Programa, traz a **visão dos dados de interesses.***

Ocorre a tomada de decisões com base nos dados recebidos.

*A **análise de dados** gera a oportunidade do reporte de descobertas para os Stakeholders e inclusive, executivos que patrocinam o Programa.*

Os dados permitem por exemplo criar métricas e scorecards.

*As descobertas reportadas permitirão a **tomada de ações mais efetivas** de mitigação, contenção e erradicação de uma ameaça*

Um patch ou um workaround pode não ter sido efetivo

Alguns endpoints estão se comunicando com endereços maliciosos de C2

***Revisão contínua** e atualização do Programa*

*Comunicar a organização sobre o impacto do Programa na **Estratégia de Cibersegurança***

CAPÍTULO 18

RESPONDENDO UM INCIDENTE DE SEGURANÇA

OODA LooP

OBSERVAR

DESCRIÇÃO: O monitoramento de segurança contínuo ajuda a identificar comportamentos anormais de rede/sistema

FERRAMENTAS E TÁTICAS: Análise de log, alertas SIEM e IDS, monitoramento de rede, análise de vulnerabilidade, monitoramento de desempenho de serviço/aplicativo

CONCLUSÕES PRINCIPAIS: Observe o máximo que puder e documente todas as descobertas relacionadas ao sistema de segurança, rede e operações comerciais. Esta fase ajuda a responder e defender com sucesso o incidente.

ORIENTAR

DESCRIÇÃO: Avaliação do cenário de ameaças cibernéticas da organização. Conecte-se logicamente e apresente contexto em tempo real para priorizar incidentes de segurança.

FERRAMENTAS E TÁTICAS: Triagem de incidentes, inteligência de ameaças, conscientização sobre a situação atual, pesquisa de segurança

CONCLUSÕES PRINCIPAIS: Pense como o cibercriminoso para construir estratégias de defesa completas. Conte com a ajuda da inteligência de ameaças para capturar as informações corretas.

DECIDIR

DESCRIÇÃO: Com base nas observações e no contexto, decida um plano de ação que ofereça tempo mínimo de inatividade e recuperação mais rápida do sistema

FERRAMENTAS E TÁTICAS: Política de segurança corporativa da própria organização

CONCLUSÕES PRINCIPAIS: Documente diferentes aspectos do processo

AGIR

DESCRIÇÃO: Remediação, recuperação e documentação das lições aprendidas para uso futuro

FERRAMENTAS E TÁTICAS: Ferramentas de análise forense, backup do sistema, ferramentas de recuperação de dados, ferramentas e programas de treinamento de conscientização de segurança, gerenciamento de patches

CONCLUSÕES PRINCIPAIS: Melhorar os métodos de treinamento e comunicação para eliminar o incidente de forma eficaz

CAPÍTULO 19

DECLARANDO E NOTIFICANDO UM INCIDENTE

Quem tem permissão para declarar um Incidente?

Quem toma decisões sobre as notificações?

O fato é relevante para requerer notificação?
Antes de notificar pense criticidade:

A organização está impossibilitada de prover serviços críticos?
Houve violação de PII? Dados sensíveis foram violados?
Um Insider é suspeito?

TIPOS DE IOCS CONSIDERADOS EM UM INCIDENTE:

- Endereço IP
- Nomes de domínios
- Nomes de processos
- Caminhos de arquivos executáveis
- Mudança de registros
- Hashes
- Serviços
- Nome de arquivos

ESTRATÉGIA DE COMUNICAÇÃO

Comunicações alternativas:

- Você seguiria utilizando a sua rede mesmo se comprometida?
- Você tem a capacidade técnica de enviar e-mails criptografados?

Comunicação estratégica com os usuários:

- Intranet site
- Saudação do Service Desk
- E-mail
- Mensagens em áreas comuns
- Chamadas/mensagens em massa por meio de plataforma
- Mensagens de texto (SMS)

TRABALHANDO COM AGÊNCIA DE FORÇA DE LEI:

Tenha documentado **quem é o responsável** por acionar uma Agência de Força de Lei

Quais Agências de Força de Lei devem ser envolvidas?

Governo do Estado inaugura Divisão de Crimes Cibernéticos: https://www.saopaulo.sp.gov.br/spnoticias/governo-do-estado-inaugura-divisao-de-crimes-ciberneticos-2/

Não espere que a Agência de Força de Lei, responda ou investigue de forma ativa a não ser que existam circunstâncias únicas no caso relatado

Eles podem obter registros e **evidências adicionais** (Registros de ISPs (Internet Service Providers), Registros de Bilhetagem, etc).

Podem **acrescentar credibilidade** ao trabalho feito por um CSIRT.

Podem facilitar a **aquisição de evidências**.

Compartilhamento de **informações privilegiadas** e assistência com IOCs.

ISOLAMENTO DA REDE:

- Ás vezes pode ser uma ação tão simples quanto remover os hosts impactados da rede ou então desconectar toda organização
- Considere capacidades de arquitetura e VLANs (Virtual Local Area Networks) de remediação
- VLANs podem permitir certos tipos de comunicação e não alarmar os atacantes

AQUISIÇÃO DE EVIDÊNCIAS

- Considere assinalar a responsabilidade pela aquisição de evidências para poucas pessoas
- Tenha um checklist para potenciais fontes de aquisição
- Certifique que a evidência não foi alterada antes da aquisição
- Considere assinalar a responsabilidade pela aquisição de evidências para poucas pessoas
- Tenha um checklist para potenciais fontes de aquisição
- Certifique que a evidência não foi alterada antes da aquisição
- Proteja a evidência contra alterações após a aquisição
- Documente quem fez a aquisição, bem como quem manipula a evidência em todos os momentos
- Utilize os formulários de Cadeia de Custódia
- Tenha um espaço seguro, seja físico ou lógico, para o armazenamento de evidências

CAPÍTULO 20

RECUPERAÇÃO DE UM INCIDENTE DE SEGURANÇA

A recuperação pode envolver ações como **restaurar sistemas** *a partir de backups limpos,* **reconstruir sistemas do zero**, *substituir arquivos comprometidos com versões limpas, instalação de patches,* **alteração de senhas** *e restrição de rede segurança do perímetro (por exemplo, conjuntos de regras de firewall, listas de controle de acesso do roteador de limite). Níveis mais altos do* **Sistema de registro e monitoramento** *de rede geralmente fazem parte do processo de recuperação.*

ÁREA DE RECUPERAÇÃO

MÉTRICAS DE EXEMPLO

Avaliação de **danos e custos de incidentes**. Considere os **custos diretos e indiretos**; danos e custos de recuperação podem ser **evidências importantes** como parte de uma ação legal.

- Custos devido à perda de vantagem competitiva de divulgação de informações proprietárias ou confidenciais [dólar]
- Custos legais [dólares]
- Custos de hardware, software e mão de obra para executar o plano de recuperação [dólar]
- Custos relacionados à interrupção dos negócios, como sistema tempo de inatividade; por exemplo, perda de produtividade do funcionário, perda de vendas, etc. [tempo em horas, dias ou semanas]
- Outros danos consequentes, como perda de reputação da marca ou confiança do cliente pela divulgação de dados do cliente [número de parceiros de negócios atuais ou futuros, anunciantes e perdas de clientes em dólares]

Melhoria da Avaliação de **Risco Organizacional**.

- Dependências do sistema identificadas com precisão [número de ativos não identificados]
- Lacunas identificadas durante os exercícios ou testes de recuperação que ajudam a informar e impulsionar a melhoria nas outras funções do CSF [número de lacunas]

- Dependências do sistema identificadas com precisão [número de ativos não identificados]
- Lacunas identificadas durante os exercícios ou testes de recuperação que ajudam a informar e impulsionar a melhoria nas outras funções do CSF [número de lacunas]

Qualidade das **Atividades de Recuperação**.

- Número de interrupções de negócios devido a incidentes de serviço de TI [número de funções de negócios]
- Porcentagem das partes interessadas de negócios satisfeitas com a TI a entrega do serviço atende aos níveis de serviço acordados [satisfação do cliente]
- Porcentagem de serviços de TI atendendo aos requisitos de tempo de atividade [acordo de nível de serviço]
- Porcentagem de restauração bem-sucedida e oportuna de backup ou cópias de mídia alternativas [número de sistemas e tempos] Número de eventos de recuperação que alcançaram objetivos de recuperação [número de eventos de recuperação bem sucedidos]

Fonte: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

CAPÍTULO 21

RELATÓRIO DE INCIDENTE

RELATÓRIO DO INCIDENTE

- **Também conhecido como AAR** (After Action Report)
- **O foco do relatório não deve ser** encontrar culpados!
- **O foco do relatório deve ser** indicar o que foi bem e o que necessita de melhorias!

CONSTRUINDO O RELATÓRIO DO INCIDENTE

1. Sumário Executivo
2. Participantes e Membros do Time de Resposta a Incidentes
3. Linha do Tempo do Incidente e Detalhes
4. Avaliação de Impacto
5. Análise de Causa Raiz
6. Lições Aprendidas
7. Efetividade da Resposta
8. Oportunidades de Melhorias
9. Lacunas Identificadas
10. Próximos Passos e Roteiro

COMUNICAÇÃO COM OS EXECUTIVOS

- **Tenha cuidado e atenção** com o que for falado e escrito, pois pode ser algo "discoverable"
- Antecipe e **tenha resposta** para algumas questões: Quanto isso custará? Isso ocorreu por negligência? De quem? O que estamos fazendo para que isso não ocorra novamente?
- **Foco no futuro** e não no passado
- Se necessário, traga um **consultor externo**
- Atenção ao nível de detalhes técnicos! **Foco na missão, negócio e riscos!**

POA&Ms

Plan of Actions & Milestones, ou Plano de Ações e Marcos

- São usados para identificar, avaliar, priorizar e monitorar esforços corretivos para fraquezas de segurança, deficiências e/ou vulnerabilidades encontradas no ambiente. Eles tem foco nos níveis estratégicos e táticos da organização.
- Uma versão da planilha está disponível no Portal do Aluno

CAPÍTULO 22

RESPOSTA A INCIDENTES DE SEGURANÇA EM AMBIENTES WINDOWS/LINUX

EDR

Endpoint Detection and Response

- Trabalhe com soluções que irão apoiar a retomada segura do ambiente de tecnologia no caso de um incidente.
- O que custa mais? O produto de segurança ou 24, 48 ou 72 horas sem faturamento?

Um Dia Ruim no CSIRT...

Não entre em pânico! Eu disse...

NÃO ENTRE EM PÂNICO

- Os primeiros passos são duros...
- Erros e paralisia
- Necessidade de seguir em frente
- Necessidade de ter um plano

Captura de Memória RAM

Belkasoft Live RAM Capturer

É uma ferramenta que permite extrair de forma confiável todo o conteúdo da memória volátil do computador – mesmo se protegida por algum mecanismo Anti-dumping ou Anti-debugging.
Disponível em:
https://belkasoft.com/get?product=ram

FTK Imager

É uma ferramenta de visualização de dados e criação de imagem que permite o acesso a evidências digitais para análise forense sem a necessidade de alterações no material original.
Disponível em:
https://go.exterro.com/l/43312/2022-01-21/f6h1s3

Análise de Memória RAM

É um framework avançado de análise e extração de evidência da memória volátil (**RAM**) de um computador

Comandos de Referência:
https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

Nota: O comando volatility foi adicionado às variáveis de ambiente da VM Windows.

Identificação do Sistema Operacional.

Enumeração de processos, rede, DLL e command line.

Captura de Tráfego de Rede

Durante uma resposta a incidente, o tráfego de pacotes de rede poderá trazer visibilidade ímpar para o CSIRT

- Qual host está iniciando ou mantendo uma comunicação?
- Qual é a origem da comunicação entre os hosts?
- A infecção vem de um host interno ou externo?
- Quem são os atacantes?

Análise do dump de Rede:

- Detalhes de usuário
- Endereço de IP
- MAC address
- Horário/Data de Interações
- Protocolos/Portas
- Tipos de Conexões e Sistemas Acessados

Análise de Dump de Rede

Wireshark

- É um analisador de pacotes open source. É comumente utilizado para troubleshooting de rede, análise de software, comunicação e desenvolvimento de protocolos.
- Disponível em: https://www.wireshark.org/download.html

Filtros:

ip.addr == x.x.x.x
ip.addr == x.x.x.x && ip.addr == x.x.x.x
ip.src == x.x.x.x && ip.dst == x.x.x.x
http or dns
tcp.port == xxx
http.request

CAPÍTULO 23

RESPOSTA A INCIDENTES DE SEGURANÇA EM AMBIENTE WINDOWS

PRINCIPAIS COMANDOS

- Conexões de Rede
- Processos
- Contas de Usuários
- Serviços
- Agendador de Tarefas
- Entradas de Registro
- Configurações de Firewall
- Windows Event Ids

CAPÍTULO 24

RESPOSTA A INCIDENTES DE SEGURANÇA EM AMBIENTE LINUX

SISTEMA DE ARQUIVOS
PRINCIPAIS COMANDOS

Usuário e Privilégios

Contas de Usuários

Entrada de Logs

Recursos do Sistema

Processos

Serviços

Comunicação de Rede

Web Logs

CAPÍTULO 25

RESPOSTA A INCIDENTES DE SEGURANÇA E FORENSE EM NUVEM PÚBLICA

NIST SP 800-145

Definição de Computação em Nuvem

É a entrega sob demanda de capacidade em tecnologia que provê acesso a infraestrutura e aplicações por meio de subscrições de serviços por meio de comunicações via rede.

1. Sob demanda (self service)
2. Armazenamento distribuído
3. Rápida elasticidade
4. Gerenciamento automatizado
5. Amplo acesso a rede
6. Agrupamento de recursos
7. Serviço mensurável
8. Tecnologia de virtualização

Tipos de Serviços e Modelo de Responsabilidade Compartilhada

A segurança e a conformidade não são de responsabilidade exclusiva dos Provedores de Serviços em Nuvem (CSPs). Os clientes desempenham um papel importante na segurança da nuvem.

O PROCESSO DE RESPOSTA A INCIDENTE EM NUVEM

1 PREPARAÇÃO
Qual é o provedor de serviços em nuvem?
Qual é modelo de deployment em nuvem? (Pública, Híbrida ou Privada)?
Qual é o tipo de serviço em nuvem? (SaaS, PaaS, IaaS)

2 IDENTIFICAÇÃO
Há atividade não usual nos logs de auditoria?
Alguma coisa está ou foi desconfigurada?

3 CONTENÇÃO
Podemos desabilitar o acesso de um usuário?
Podemos isolar uma VM ou subrede?
Como adquirir uma imagem?

4 ERRADICAÇÃO
Podemos remover os sistemas afetados?
Podemos remover/substituir credenciais comprometidas?

5 RECUPERAÇÃO
Podemos retomar a operação normal do negócio?
Há um Plano de Continuidade de Negócio disponível?

6 LESSONS LEARNED
Quais brechas foram descobertas?
Como endereçar as lacunas e resolver as brechas?

CAPÍTULO 25

CONTINUAÇÃO

OPERAÇÃO DE SEGURANÇA PARA MICROSOFT DEFENDER 365

DIÁRIO

Gerenciar incidentes
Revise as ações automatizadas de investigação e resposta (AIR)
Revise as últimas análises de ameaças

1 Análise de ataque e alerta | 2 Contenção e erradicação | 3 Contenção e erradicação | 4 Resolução e aprendizado pós incidente

Responder a Incidentes

MENSAL

Revise as configurações do AIR
Revise a pontuação segura e o gerenciamento de ameaças e vulnerabilidades
Reporte à cadeia de gerenciamento de segurança de TI

TRIMESTRAL

Reporte ao CISO

ANUAL

Realizar incidente grave ou exercício de violação

Atualize ou refina processos, políticas e configurações de segurança

GOOGLE CLOUD SECURITY COMMAND CENTER

Detecção e Prevenção de Ameaças

Centro de Comando de Segurança

Ganhe Visibilidade	Descubra Vulnerabilidades	Detectar Ameaças	Manter a Conformidade
Inventário de Ativos	Erros de configuração	Atividade maliciosa na rede e na conta	Melhores práticas CIS 1.0, NIST 800-53
Acompanhamento de bens	Vulnerabilidades de aplicativos da Web	Atividade suspeita em contêineres	Padrões da indústria PCI, PCI DSS v3.2.1, ISO 27001

DETECTE AMEAÇAS CONTRA UM WORKLOAD

Amazon GuardDuty
O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente comportamentos mal-intencionados ou não autorizados para proteger suas contas, cargas de trabalho e dados da AWS armazenados no Amazon S3

Eventos de gerenciamento do CloudTrail
Eventos de gerenciamento do CloudTrail
Logs de fluxo de VPC
Logs de DNS

Habilitar GuardDuty
Com alguns cliques no console, monitore todas as suas contas da AWS sem software adicional para implantar ou gerenciar

Analisar continuamente
Analise automaticamente a atividade de rede, conta e acesso a dados em escala, fornecendo monitoramento contínuo de suas contas da AWS

Detecte ameaças de forma inteligente
GuardDuty usa aprendizado de máquina detecção de anomalias e inteligência de ameaças integrada para identificar e priorizar ameaças potenciais

Tome uma attitude
Revise descobertas detalhadas no console, integre-se ao gerenciamento de eventos ou sistemas de fluxo de trabalho ou acione o AWS Lambda para correção ou prevenção automatizada

CAPÍTULO 26

RESPOSTA A INCIDENTES DE SEGURANÇA EM ICS/SCADA

CAPÍTULO 27

CAÇA E DETECÇÃO DE AMEAÇAS E INTELIGÊNCIA DE AMEAÇAS

O THREAT HUNTING, LITERALMENTE PODE SER CHAMADO DE "PROCURAR PELO EM OVO"!

Resposta a Incidentes

- Ambas lidam com ameaças no ambiente, no entanto a resposta a incidentes é reativa.
- Não há evidências claras de ameaças, enquanto que na resposta a incidentes a ameaça está ativa.

Teste de Intrusão (Pentest)

- Ambas buscam pontos fracos no ambiente de tecnologia.
- O teste de intrusão busca falhas de configuração ou vulnerabilidades para obter acesso a informações confidenciais.
- O Threat Hunting não busca acesso a nada, apenas identificar as ameaças ocultas e erradicá-las.

Gerenciamento de Riscos

- Determinar os pontos fracos para corrigí-los, o que pode envolver a identificação de fontes de ameaças por meio do Threat Hunting.
- Tem escopo mais abrangente.

THREAT HUNTING FRAMEWORK

PLANEJE O SEU THREAT HUNTING:

- ***PROJETE** sua rede para caça*
- ***PREPARE** sua equipe*
- ***CONHEÇA** sua empresa*
- ***CONHEÇA** o seu adversário TTP*
- ***COLETE** dados de caça*
- ***CRIE** Hipóteses*
- ***COMECE** a Caçar*