



Module 28: Análise e Resposta de Perícias Digitais e Incidentes



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br

Module Objectives

Module Title: Análise e Resposta de Perícias Digitais e Incidentes

Module Objective: Explique como o CyberOps Associate responde a incidentes de segurança cibernética.

Topic Title	Topic Objective
Atribuição de Manipulação de Evidências e Ataque	Explique o papel dos processos forenses digitais
A Cadeia de Mortes Cibernéticas	Identifique os passos da Cadeia de Mortes Cibernéticas
O Modelo diamante de análise de intrusão	Classifique um evento de intrusão usando o Modelo Diamante
Resposta a Incidentes	Aplique os procedimentos de tratamento de incidentes NIST 800-61r2 a um determinado cenário de incidente

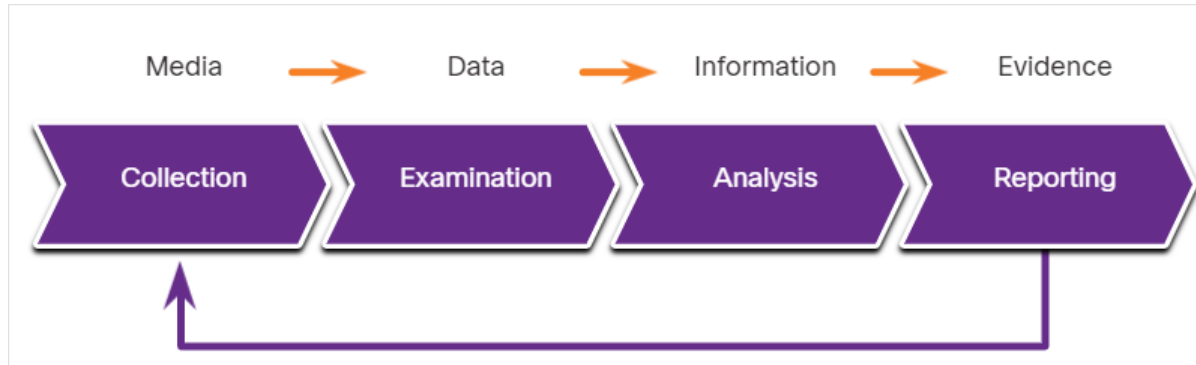
28.1 Evidence Handling and Attack Attribution

Perícia Digital

- A Perícia Digital é a recuperação e investigação de informações encontradas em dispositivos digitais no que se refere à atividade criminosa.
- Indicadores de compromisso são as evidências de que ocorreu um incidente de cibersegurança.
- Por exemplo, de acordo com as regulamentações hipaa dos EUA, se ocorreu violação de dados envolvendo informações do paciente, então a notificação da violação deve ser feita aos indivíduos afetados.
- A investigação forense digital deve ser usada para determinar os indivíduos afetados e também para certificar o número de indivíduos afetados para que a notificação apropriada possa ser feita em conformidade com as regulamentações da HIPAA.
- Às vezes, os analistas de cibersegurança podem estar em contato direto com evidências forenses digitais que detalham a conduta dos membros da organização.
- Os analistas devem conhecer os requisitos relativos à preservação e manuseio de tais evidências.

O Processo De Perícia Digital

- NIST descreve as quatro fases do processo forense de evidências digitais:
 - **Collection** - Identificação de fontes potenciais de dados forenses e aquisição, manuseio e armazenamento desses dados
 - **Examination** - Avaliar e extrair informações relevantes dos dados coletados
 - **Analysis** - Tirando conclusões dos dados e correlação de dados de múltiplas fontes
 - **Reporting** - Elaboração e apresentação de informações resultantes da fase de análise.



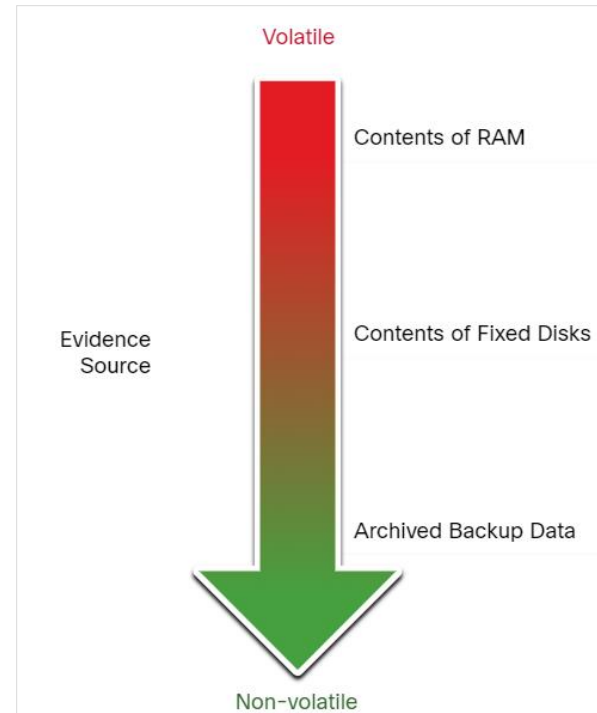
Tipos de Evidência

Em processos judiciais, as provas são amplamente classificadas como seguintes:

- **Direct Evidence** - A evidência que estava indiscutivelmente na posse do acusado, ou é testemunha ocular evidência de alguém que observou diretamente comportamento criminoso.
- **Indirect evidence** - Esta evidência estabelece uma hipótese em combinação com outros fatos. Também é conhecida como evidência circunstancial.
- **Best evidence** – Esta evidência pode ser dispositivos de armazenamento usados por um acusado, ou arquivos de arquivos que podem ser provados como sem marcas.
- **Corroborating evidence** - Esta evidência apoia uma afirmação que é desenvolvida a partir da melhor evidência.

Ordem de Coleta de Provas

- IETF RFC 3227 descreve uma ordem para a coleta de evidências digitais com base na volatilidade dos dados.
- Os dados armazenados na RAM são os mais voláteis e serão perdidos quando o dispositivo for desligado.
- A coleta de evidências digitais deve começar com as evidências mais voláteis e proceder ao menos volátil.
- Detalhes dos sistemas dos quais as evidências foram coletadas, incluindo quem tem acesso a esses sistemas e em que nível de permissões devem ser registradas.



Cadeia de Custódia

- A cadeia de custódia envolve a coleta, manuseio e armazenamento seguro de provas.
- Registros detalhados devem ser mantidos com o seguinte:
- Quem descobriu e coletou as provas?
- Todos os detalhes sobre o manuseio de provas, incluindo horários, locais e pessoal envolvido.
- Quem tem a responsabilidade primária pelas provas, quando a responsabilidade foi atribuída, e quando a custódia mudou?
- Quem tem acesso físico à evidência enquanto estava armazenada? O acesso deve ser restrito apenas ao pessoal mais essencial.

Integridade e Preservação de Dados

- O carimbo de tempo dos arquivos deve ser preservado. Assim, a evidência original deve ser copiada, e a análise só deve ser realizada em cópias do original.
- Os horários podem ser parte das evidências, a abertura de arquivos da mídia original deve ser evitada.
- Arquive e proteja o disco original para mantê-lo em sua condição original, sem problemas.
- Ferramentas especiais devem ser usadas para preservar evidências forenses antes que o dispositivo seja desligado e as evidências sejam perdidas.
- Os usuários não devem desconectar, desligar ou desligar máquinas infectadas, a menos que explicitamente dito para fazê-lo pelo pessoal de segurança.
- Seguir esses processos garantirá que qualquer evidência de negligência será preservada, e quaisquer indicadores de comprometimento podem ser identificados.

Atribuição de ataque

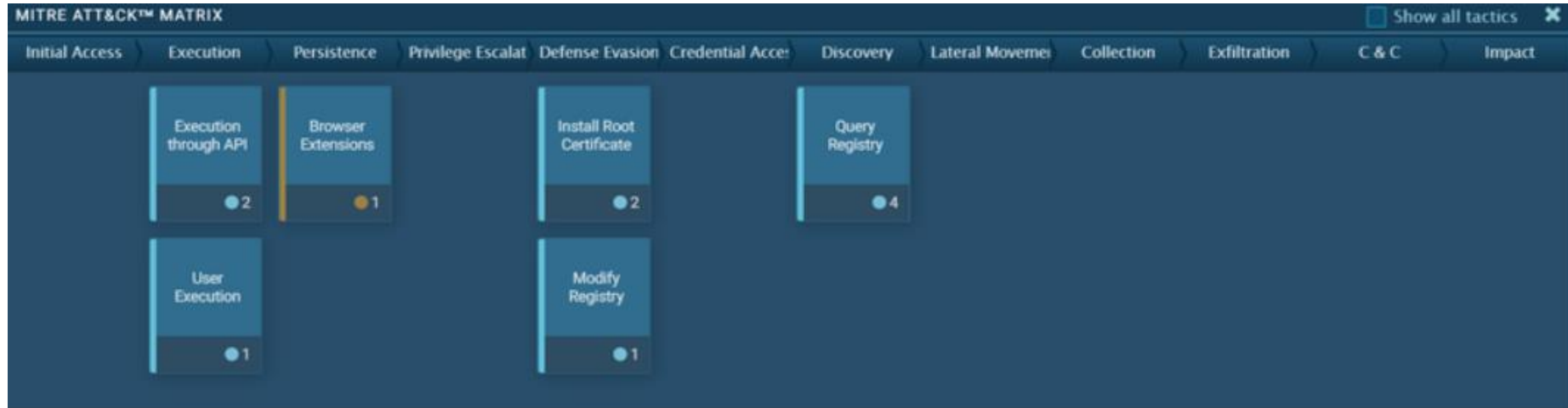
- A Atribuição de Ameaças refere-se ao ato de determinar o indivíduo, organização ou nação responsável por uma intrusão ou incidente de ataque bem sucedido.
- A identificação dos atores responsáveis de ameaça deve ocorrer através da investigação de princípios e sistemática das provas.
- Em uma investigação baseada em evidências, a equipe de resposta a incidentes correlaciona Táticas, Técnicas e Procedimentos (TTP) que foram usados no incidente com outras explorações conhecidas.
- Alguns aspectos de uma ameaça que pode ajudar na atribuição são a localização de hosts ou domínios originários, recursos do código usado em malware e ferramentas, e outras técnicas.
- Para ameaças internas, a gestão de ativos desempenha um papel importante. Descobrir os dispositivos dos quais um ataque foi lançado pode levar diretamente ao ator de ameaças.
- Endereços IP, endereços MAC e logs DHCP podem ajudar a rastrear os endereços usados no ataque de volta para um dispositivo específico.

O Quadro MITRE ATT&CK

- O Quadro DE Táticas Contraditórias, Técnicas & Conhecimento Comum (ATT&CK) da MITRE permite a capacidade de detectar táticas, técnicas e procedimentos do atacante (TTP) como parte da defesa de ameaças e atribuição de ataque.
- As táticas consistem nos objetivos técnicos que um atacante deve realizar para executar um ataque.
- Técnicas são os meios pelos quais as táticas são realizadas.
- Os procedimentos são as ações específicas tomadas pelos atores de ameaça nas técnicas que foram identificadas.
- O MITRE ATT&CK Framework é uma base global de conhecimento do comportamento de atores de ameaças.
- A estrutura foi projetada para permitir o compartilhamento automatizado de informações definindo estruturas de dados para a troca de informações entre sua comunidade de usuários e o MITRE.
- **Nota:** Faça uma pesquisa na internet na MITRE ATT&CK para saber mais sobre a ferramenta.

O Quadro MITRE ATT&CK (Contd.)

- A figura mostra uma análise de uma exploração de ransomware do ANY. EXECUTE caixa de areia on-line. As colunas mostram as táticas de matriz de ataque corporativo, com as técnicas que são usadas pelo malware.

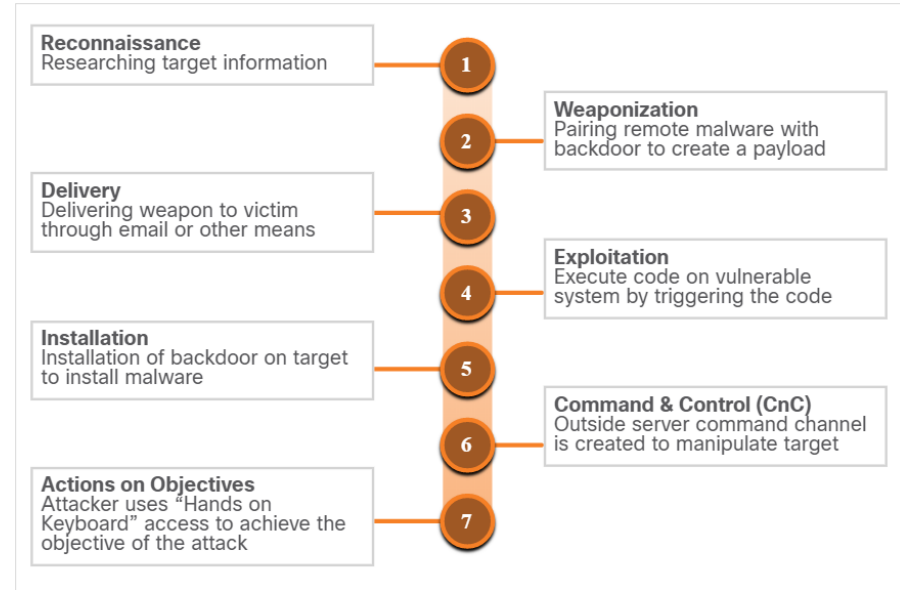


MITRE ATT&CK Matrix for a Ransomware Exploit

28.2 The Cyber Kill Chain

Etapas da Cadeia de Mortes Cibernéticas

- A Cyber Kill Chain foi desenvolvida pela Lockheed Martin para identificar e prevenir invasões cibernéticas.
- Ao responder a um incidente de segurança, o objetivo é detectar e parar o ataque o mais cedo possível na progressão da cadeia de mortes para evitar mais danos.
- Se o agressor for parado em qualquer fase, a corrente de morte é quebrada e o defensor conseguiu frustrar a intrusão do ator de ameaça..



Steps of Cyber Kill Chain

Nota: Ator de ameaça refere-se à festa que instiga o ataque. No entanto, a Lockheed Martin usa o termo "adversário" em Cyber Kill Chain. Portanto, os termos adversário e ator ameaça são usados intercambiavelmente neste tópico.

Reconhecimento

- Reconhecimento é quando o ator de ameaças realiza pesquisas, reúne inteligência e seleciona alvos.
- O ator de ameaças escolherá alvos que foram negligenciados ou desprotegidos porque terão maior probabilidade de serem penetrados e comprometidos.
- A tabela resume as táticas e defesas usadas durante a etapa de reconhecimento.

Táticas adversárias	Defesas SOC
<p>Planejar e realizar pesquisas:</p> <ul style="list-style-type: none">• Coletar endereços de e-mail• Identifique funcionários nas mídias sociais• Colete todas as informações de relações públicas (comunicados de imprensa, prêmios, participantes da conferência e assim por diante)• Descubra servidores voltados para a Internet• Realizar varreduras na rede para identificar endereços IP e portas abertas	<p>Descubra a intenção do adversário:</p> <ul style="list-style-type: none">• Alertas de log da Web e dados históricos de pesquisa• Análises do navegador de minas de dados• Construa cartilhas para detectar comportamentos que indiquem atividade de reconhecimento• Priorizar a defesa em torno de tecnologias e pessoas que a atividade de reconhecimento está mirando

Armamento

- A armamento usa as informações do reconhecimento para desenvolver uma arma contra sistemas específicos ou indivíduos na organização.
- Muitas vezes é mais eficaz usar um ataque de zero-day para evitar métodos de detecção.
- Um ataque de zero-day usa uma arma que é desconhecida para defensores e sistemas de segurança de rede.
- A tabela resume as táticas e defesas utilizadas durante a etapa de armamento.

Adversary Tactics	SOC Defence
<p>Prepare and stage the operation:</p> <ul style="list-style-type: none">• Obtain an automated tool to deliver the malware payload (weaponizer).• Select or create a document to present to the victim.• Select or create a backdoor and command and control infrastructure.	<p>Detect and collect weaponization artifacts:</p> <ul style="list-style-type: none">• Ensure that IDS rules and signatures are up to date.• Conduct full malware analysis.• Build detections for the behavior of known weaponizers.• Is malware old, “off the shelf” or new malware that might indicate a tailored attack?• Collect files and metadata for future analysis.• Determine which weaponizer artifacts are common to which campaigns.

Entrega

- Durante esta etapa, a arma é transmitida ao alvo usando um vetor de entrega. Se a arma não for entregue, o ataque não será bem sucedido.
- O ator de ameaças usará diferentes métodos para aumentar as chances de entregar a carga, como criptografar comunicações, fazer com que o código pareça legítimo ou ofuscar o código.
- Os sensores de segurança são tão avançados que podem detectar o código como malicioso, a menos que seja alterado para evitar a detecção.
- A tabela resume as táticas e defesas utilizadas durante a etapa de entrega.

Táticas adversárias

Lançar malware no alvo:

- Direto contra servidores web
- Entrega indireta através:
 - E-mail malicioso
 - Malware na vara USB
 - Interações nas redes sociais
 - Sites comprometidos

Defesa SOC

Bloquear a entrega de malware:

- Analise o caminho de infraestrutura utilizado para entrega.
- Entenda servidores, pessoas e dados direcionados disponíveis para atacar.
- Inferir intenção do adversário com base no alvo.
- Colete e-mails e registros web para reconstrução forense.

Exploração

- Depois que a arma é entregue, o ator de ameaça a usa para quebrar a vulnerabilidade e ganhar o controle do alvo.
- Os alvos de exploração mais comuns são aplicativos, vulnerabilidades do sistema operacional e usuários.
- A tabela resume as táticas e defesas usadas durante a etapa de exploração.

Táticas adversárias	Defesa SOC
<p>Explorar uma vulnerabilidade para obter acesso:</p> <ul style="list-style-type: none">• Use software, hardware ou vulnerabilidade humana• Adquirir ou desenvolva a exploração• Use uma exploração acionada por adversários para vulnerabilidades do servidor• Use uma exploração acionada pela vítima, como abrir um anexo de e-mail ou um link web malicioso	<p>Treinar funcionários, codificar e endurecer dispositivos:</p> <ul style="list-style-type: none">• Treinamento de conscientização sobre segurança dos funcionários e testes periódicos de e-mail• Treinamento de desenvolvedor web para garantir código• Testes regulares de varredura e penetração de vulnerabilidades• Medidas de endpoint de endpoint• Auditoria de ponto final para determinar forensemente a origem da exploração

Installation

- Na etapa de Instalação, o ator de ameaça estabelece uma porta traseira no sistema para permitir o acesso contínuo ao alvo.
- Para preservar esse backdoor, o acesso remoto não deve alertar analistas ou usuários de segurança cibernética. O método de acesso deve sobreviver através de varreduras antimalware e reinicialização do computador para ser eficaz.
- A tabela resume as táticas e defesas utilizadas durante a etapa de instalação.

Táticas adversárias	Defesa SOC
<p>Instale backdoor persistente:</p> <ul style="list-style-type: none">• Instale webshell no servidor web para acesso persistente.• Crie ponto de persistência adicionando serviços, chaves AutoRun, etc.• Alguns adversários modificam o fluxo de tempo do malware para fazê-lo aparecer como parte do sistema operacional.	<p>Detectar, registrar e analisar a atividade de instalação:</p> <ul style="list-style-type: none">• HIPS para alertar ou bloquear em caminhos comuns de instalação.• Determine se o malware requer privilégios elevados ou privilégios do usuário• Auditoria de ponto final para descobrir criações de arquivos anormais.• Determine se o malware é uma ameaça conhecida ou nova variante.

Command and Control

- O objetivo é estabelecer comando e controle (CnC ou C2) com o sistema de destino.
- Hosts comprometidos geralmente saem da rede para um controlador na internet.
- Os atores de ameaças usam canais CNC para emitir comandos para o software que eles instalaram no alvo.
- O analista de segurança cibernética deve ser capaz de detectar comunicações do CNC para descobrir o host comprometido.

Adversary Tactics	SOC Defence
<p>Canal aberto para manipulação de alvos:</p> <ul style="list-style-type: none">• Abra canal de comunicação bidires para infraestrutura CNC• Canais CNC mais comuns na Web, DNS e protocolos de e-mail• A infraestrutura do CNC pode ser de propriedade adversária ou da própria rede de vítimas	<p>Última chance de bloquear a operação:</p> <ul style="list-style-type: none">• Pesquise possíveis novas infraestruturas do CNC• Descubra a infraestrutura do CnC apesar da análise de malware• Isolar o tráfego de DNS para servidores DNS suspeitos, especialmente DNS Dinâmicos• Evitar impactos bloqueando ou desativando canal CNC• Consolidar o número de pontos de presença na internet• Personalizar regras de bloqueio de protocolos cnc em proxies da Web

Ações de Objetivos

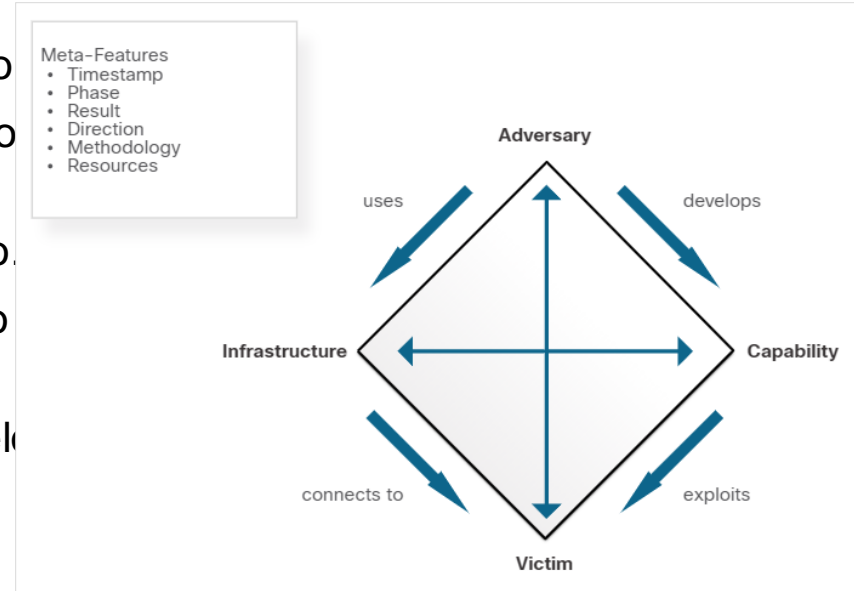
- Ações em Objetivos é a etapa final da Cadeia de Cyber Kill Chain que descreve o ator de ameaça alcançando seu objetivo original.
- Neste ponto, o ator de ameaças está profundamente enraizado nos sistemas da organização, escondendo seus movimentos e cobrindo seus rastros.
- É extremamente difícil remover o ator de ameaças da rede.
- A tabela resume as táticas e defesas utilizadas durante as ações na etapa objetiva.

Táticas adversárias	Defesa SOC
<p>Colher as recompensas do ataque bem sucedido:</p> <ul style="list-style-type: none">• Coletar credenciais de usuário• Escalada de privilégios• Reconhecimento interno• Movimento lateral através do meio ambiente• Coletar e exfiltrar dados• Destruir sistemas• Substituir, modificar ou corromper dados	<p>Detecte usando evidências forenses:</p> <ul style="list-style-type: none">• Estabeleça a cartilha de resposta a incidentes• Detectar exfiltração de dados, movimento lateral e uso de credenciais não autorizadas• Resposta imediata do analista para todos os alertas• Análise forense de pontos finais para triagem rápida• Capturas de pacotes de rede para recriar atividade• Avaliação de danos de conduta

28.3 O Modelo diamante de análise de intrusão

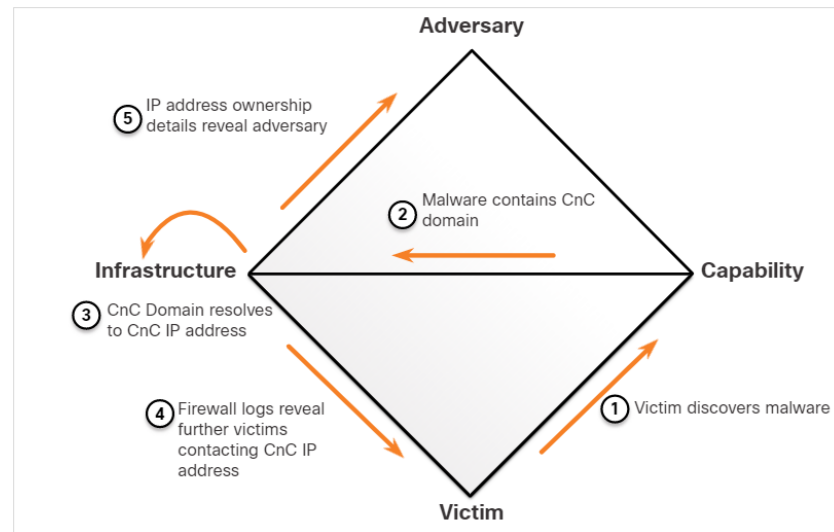
Visão geral do modelo diamante

- O Modelo diamante de análise de intrusão representa um incidente de segurança ou evento
- As quatro características principais de um evento de intrusão são:
 - **Adversary** - Partes responsáveis pela intrusão.
 - **Capability** - Ferramenta ou técnica usada pelo adversário para atacar a vítima.
 - **Infrastructure** – Caminhos de rede usados pelo adversário para estabelecer e manter o comando e controle sobre suas capacidades.
 - **Victim** – Alvo do ataque.
- Meta-características expandem o modelo ligeiramente para incluir os elementos importantes: **Timestamp, Fase, Resultado, Direção, Metodologia e Recursos**



Pivotando através do modelo diamante

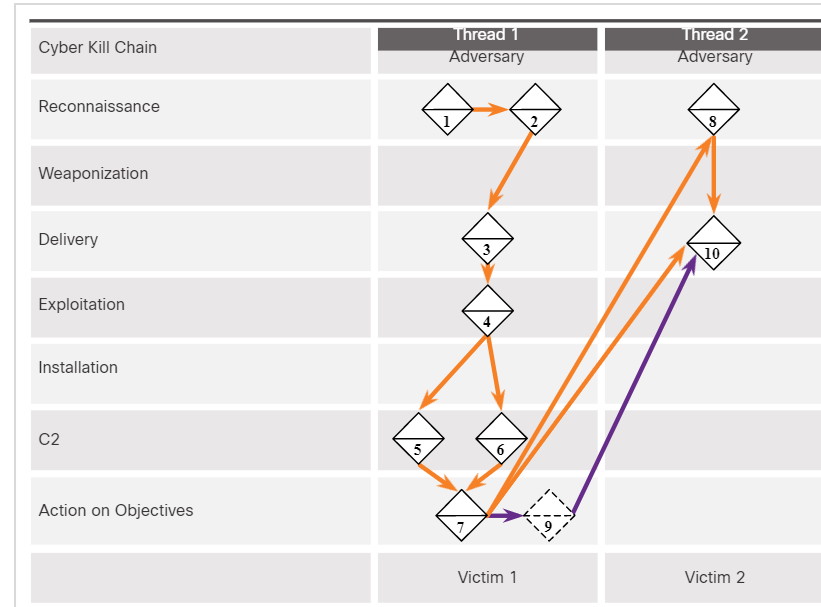
- O Modelo Diamante é ideal para ilustrar como o adversário gira de um evento para o outro. Por exemplo:
- Um empregado relata que seu computador está agindo de forma anormal. Uma varredura do host pelo técnico de segurança indica que o computador está infectado com malware.
- Uma análise do malware revela que o malware contém uma lista de nomes de domínio do CNC que resolvem uma lista de endereços IP.
- Esses endereços IP são usados para identificar o adversário e investigar registros para determinar se outras vítimas na organização estão usando o canal CNC.



Caracterização do modelo de diamante de uma exploração

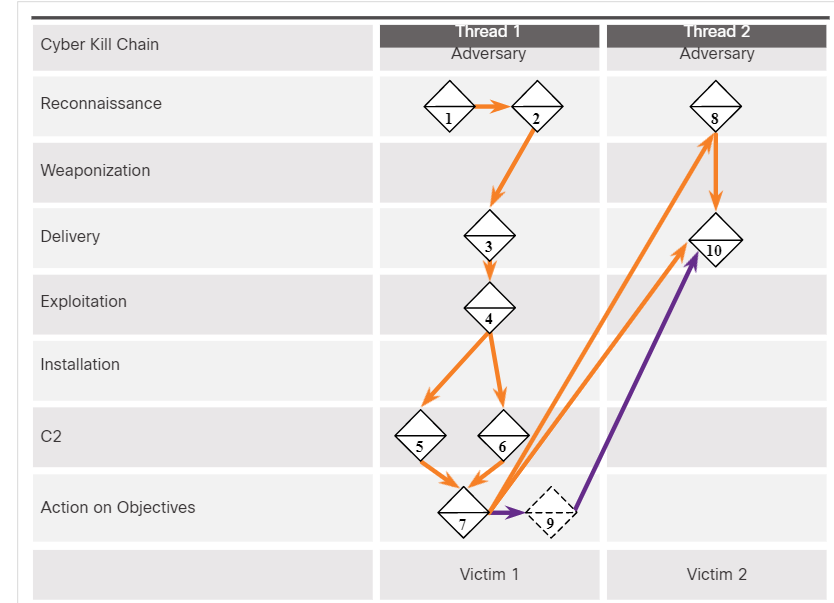
O Modelo Diamante e a Cadeia de Mortes Cibernéticas (Contd.)

- Os eventos são encadeados em uma cadeia na qual cada evento deve ser concluído antes do próximo evento. Este segmento de eventos pode ser mapeado para a Cadeia de Cyber Kill.
- O exemplo ilustra o processo de ponta a ponta de um adversário enquanto atravessam a Cadeia de Mortes Cibernéticas:
- O adversário realiza uma busca na web pela empresa de vítimas Gadgets, Inc. recebendo como parte dos resultados o nome de domínio gadgets.com.
- Pesquisa adversária "administrador de rede gadget.com" e descobre postagens em fóruns de usuários que afirmam ser administradores de rede de gadget.com e os perfis revelam seus endereços de e-mail.
- O adversário envia e-mails de phishing com um cavalo de Tróia anexado aos administradores da rede.



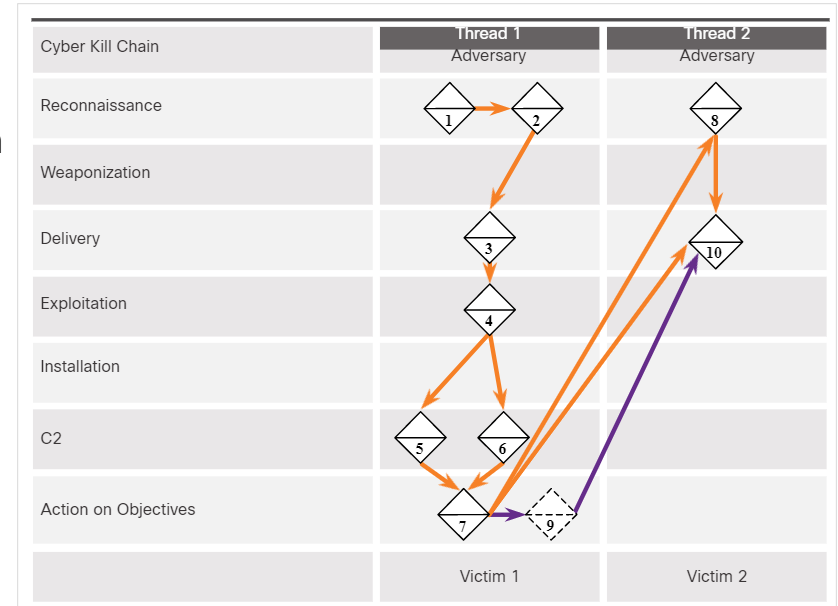
O Modelo Diamante e a Cadeia de Mortes Cibernéticas (Contd.)

- Um administrador de rede (NA1) abre o anexo malicioso que executa a exploração fechada.
- O host do NA1 registra-se com um controlador cnc enviando uma mensagem http post e recebendo uma resposta HTTP em troca.
- É revelado a partir da engenharia reversa que o malware tem endereços IP de backup adicionais.
- Através de uma mensagem de resposta HTTP do CnC enviada ao host do NA1, o malware começa a agir como um proxy para novas conexões TCP.



The Diamond Model and the Cyber Kill Chain (Contd.)

- Através de informações do proxy que está sendo executado no host do NA1, o Adversário pesquisa na web para "a pesquisa mais importante de todos os tempos" e encontra a Vítima 2, Interessante Research Inc.
- O adversário verifica a lista de contatos de e-mail do NA1 para obter quaisquer contatos da Interesting Research Inc. e descobre o contato para a Interessante Research Inc. Diretor de Pesquisa.
- Diretor de Pesquisa da Interesting Research Inc. recebe um e-mail spear-phish do endereço de e-mail na1 da Gadget Inc. enviado do host do NA1 com a mesma carga observada no Evento 3.
- O adversário agora tem duas vítimas comprometidas das quais ataques adicionais podem ser lançados.

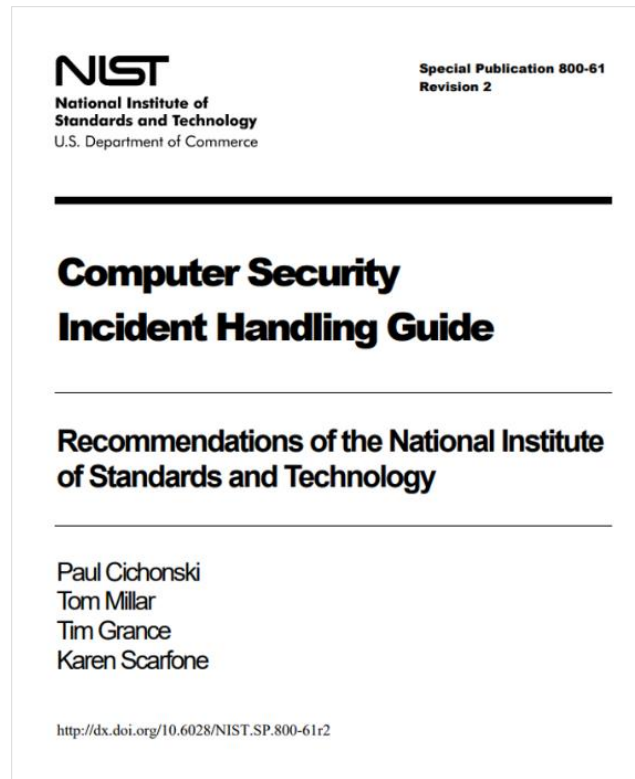


28.4 Resposta a Incidentes

Establishing an Incident Response Capability

- A resposta ao incidente visa limitar o impacto do ataque, avaliar os danos causados e implementar procedimentos de recuperação.
- A resposta a incidentes envolve os métodos, políticas e procedimentos que são usados por uma organização para responder a um ataque cibernético.

Note: Embora este capítulo ressiula o conteúdo no padrão NIST 800-61r2, você deve estar familiarizado com toda a publicação, pois abrange quatro tópicos principais do exame para o *Understanding Cisco Exame de Fundamentos de Operações de Cibersegurança*.



Establishing an Incident Response Capability (Contd.)

- A tabela abaixo resume os elementos de política, plano e procedimento em uma resposta a incidentes:

Elementos políticos	Elementos do Plano	Elementos do procedimento
<ul style="list-style-type: none">• Demonstração de compromisso de gestão• Propósito e objetivos da política• Escopo da política• Definição de incidentes de segurança de computador e termos relacionados• Estrutura organizacional e definição de papéis, responsabilidades e níveis de autoridade• Priorização das classificações de gravidade dos incidentes• Medidas de desempenho• Formulários de emissão de relatórios e contatos	<ul style="list-style-type: none">• Missão• Estratégias e metas• Aprovação da alta administração• Abordagem organizacional para resposta a incidentes• Como a equipe de resposta a incidentes se comunicará com o resto da organização e com outras organizações• Métricas para medir a capacidade de resposta a incidentes• Como o programa se encaixa na organização global	<ul style="list-style-type: none">• Processos técnicos• Usando técnicas• Preenchimento de formulários• Seguindo listas de verificação

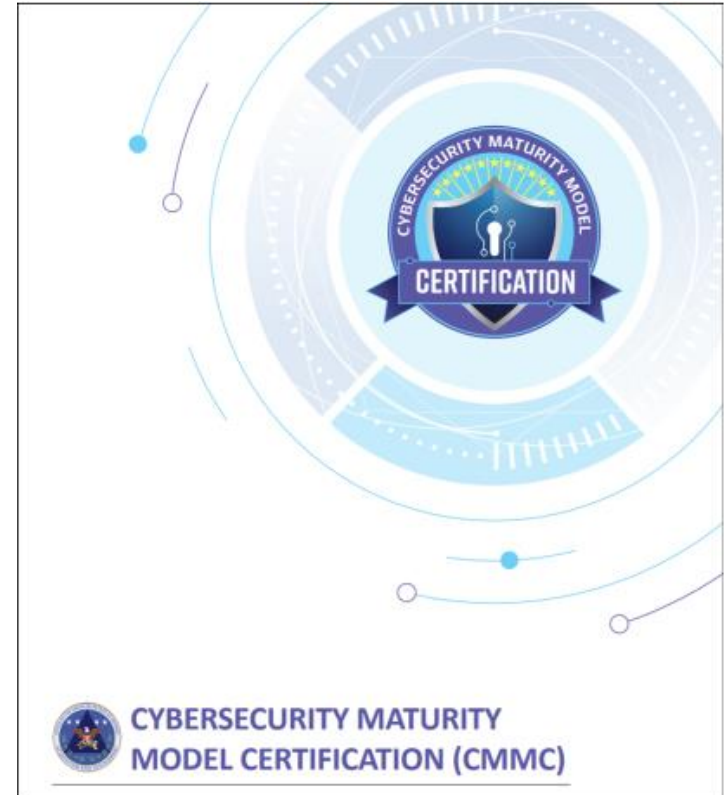
Incident Response Stakeholders

- As partes interessadas envolvidas na entrega de um incidente de segurança são as seguintes:
 - Gestão
 - Garantia de informações
 - Suporte de TI
 - Departamento Jurídico
 - Assuntos Públicos e Relações com a Mídia
 - Recursos humanos
 - Planejadores de Continuidade de Negócios
 - Gestão de Segurança Física e Instalações

Stakeholders de resposta a incidentes (Contd.)

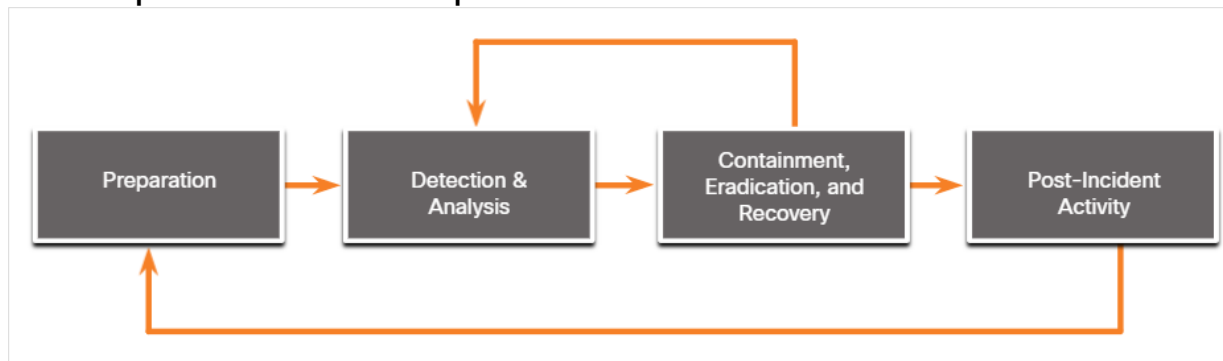
A Certificação do Modelo de Maturidade de Cibersegurança (CMMC)

- O CMMC certifica as organizações por nível. Para a maioria dos domínios, há cinco níveis, no entanto, para resposta a incidentes, há apenas quatro:
 - **Level 2** - Estabeleça um plano de resposta a incidentes que siga o processo NIST.
 - **Level 3** - Documentar e relatar incidentes às partes interessadas identificadas no plano de resposta a incidentes.
 - **Level 4** - Use o conhecimento do TTP do atacante para refinar o planejamento e a execução de resposta a incidentes.
 - **Level 5** - Utilizar técnicas aceitas e sistemáticas de coleta de dados forenses de computador.



Ciclo de vida de resposta a incidentes NIST

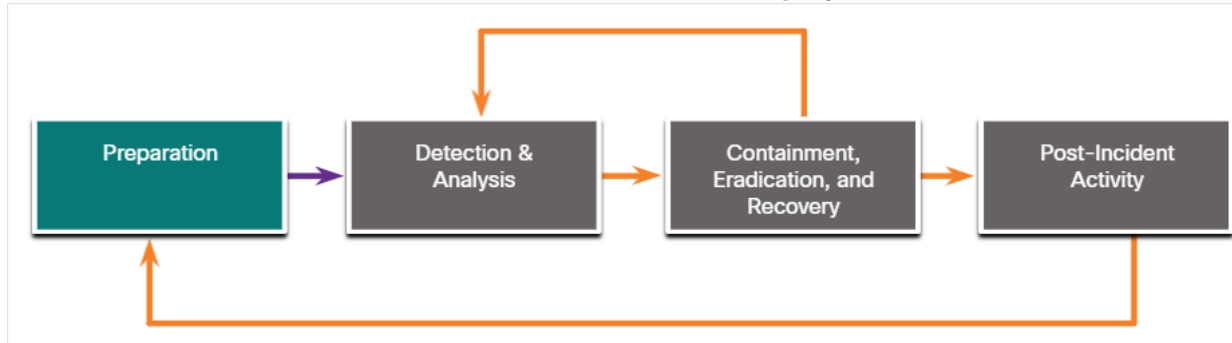
- NIST define quatro etapas no ciclo de vida do processo de resposta a incidentes:
 - **Preparation** - Os membros do CSIRT são treinados em como responder a um incidente.
 - **Detection and Analysis** – CSIRT identifica, analisa e valida rapidamente um incidente.
 - **Containment, Eradication, and Recovery** – O CSIRT implementa procedimentos para conter a ameaça, erradicar o impacto sobre os ativos organizacionais e usar backups para restaurar dados e software.
 - **Post-Incident Activities** – CSIRT documenta como o incidente foi tratado, recomenda alterações para resposta futura e especifica como evitar uma recorrência.



Incident Response

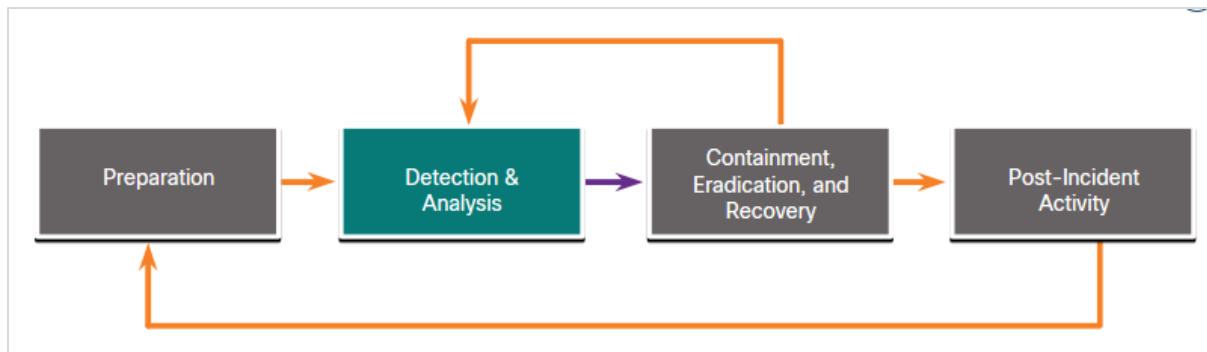
Preparation

- A fase de preparação é quando o CSIRT é criado e treinado. As ferramentas e ativos que serão necessários pela equipe para investigar incidentes são adquiridos e implantados.
- Os exemplos de ações na fase de preparação são os seguintes:
 - Instalações para hospedar a equipe de resposta e o SOC são criadas.
 - Avaliações de risco são usadas para implementar controles que limitarão o número de incidentes.
 - Materiais de treinamento de conscientização sobre segurança do usuário são desenvolvidos.
 - Necessário hardware e software para análise e mitigação de incidentes é adquirido.



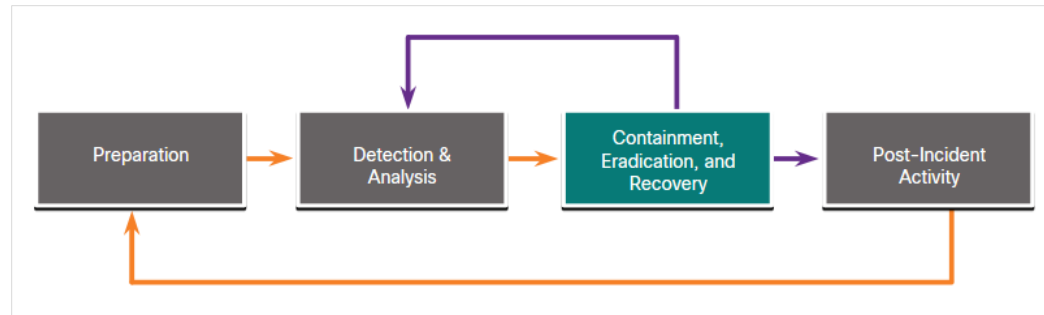
Detection and Analysis

- Diferentes tipos de incidentes exigirão respostas diferentes.
- **Attack Vectors:** Web, E-mail, perda ou roubo, personificação, atrito e mídia.
- **Detection:** Detecção automatizada - Software antivírus, IDS, detecção manual - relatórios do usuário.
- **Analysis:** Use o perfil de rede e sistema para determinar a validade de incidentes de segurança.
- **Scoping:** Fornecer informações sobre a contenção do incidente e análise mais profunda dos efeitos do incidente.
- **Incident Notification:** Notifique as partes interessadas e partes externas apropriadas, uma vez que o incidente é analisado e priorizado,



Containment, Eradication, and Recovery

- Após determinar a validade do incidente através da detecção e análise, ele deve ser contido.
- **Containment Strategy:** Para cada tipo de incidente, uma estratégia de contenção deve ser criada e aplicada dependendo de algumas condições.
- **Evidence:** Durante um incidente, evidências devem ser reunidas para resolvê-lo. É necessário para investigação subsequente pelas autoridades.
- **Attacker Identification:** Identificar invasores minimizará o impacto sobre ativos e serviços comerciais críticos.
- **Eradiation, recovery, and remediation:** erradicar, identificar todos os hospedeiros que precisam de remediação; para recuperar hosts, usar backups limpos e recentes ou reconstruí-los com mídia de instalação.

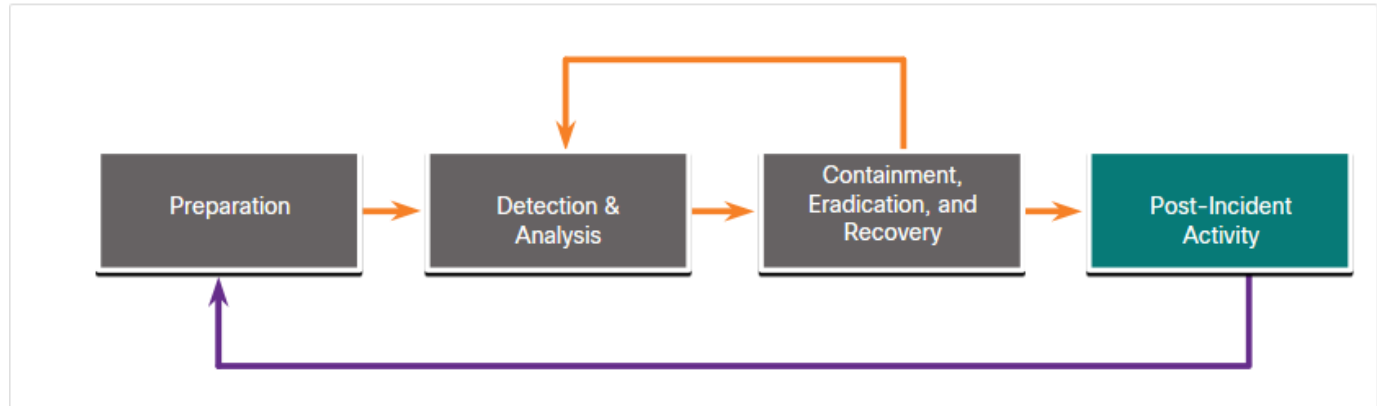


Post-Incident Activities

- É importante se reunir periodicamente com todas as partes envolvidas para discutir os eventos ocorridos e as ações de todos os indivíduos durante o tratamento do incidente.

Lessons-based hardening:

- A organização deve realizar uma reunião "lições aprendidas" para:
 - Revise a eficácia do processo de tratamento de incidentes.
 - Identificar o endurecimento necessário para os controles e práticas de segurança existentes.



Incident Data Collection and Retention

- A tabela abaixo resume a coleta e retenção de dados de incidentes:

Coleta de Dados de Incidentes	Retenção
<ul style="list-style-type: none">• Os dados coletados após a reunião aprendida com as lições podem ser usados para:• Determine o custo do incidente para o orçamento• Determine a eficácia do CSIRT• Identifique possíveis falhas de segurança em todo o sistema• O tempo de cada incidente fornece uma visão da quantidade total de trabalho utilizada e do tempo total de cada fase do processo de resposta a incidentes.• Apenas colete dados que possam ser usados para definir e refinar o processo de tratamento de incidentes.• Realize uma avaliação objetiva de cada Incidente.	<p>Alguns dos fatores determinantes para a retenção de evidências:</p> <ul style="list-style-type: none">• Acusação - Quando um agressor será processado por causa de um incidente de segurança, as provas devem ser mantidas até que todas as ações legais tenham sido concluídas.• Tipo de dado - Uma organização pode especificar que tipos específicos de dados devem ser mantidos por um período específico de tempo.• Custar - Se há um monte de hardware e mídia de armazenamento que precisa ser armazenado por um longo tempo, ele pode se tornar caro.

Requisitos de emissão de relatórios e compartilhamento de informações

- Os regulamentos governamentais devem ser consultados pela equipe jurídica para determinar a responsabilidade da organização em relatar o incidente.
- A administração precisa determinar qual comunicação adicional é necessária com outros stakeholders, como clientes, fornecedores, parceiros e assim por diante.
- A NIST recomenda que uma organização se coordene com as organizações para compartilhar detalhes sobre o incidente. As recomendações críticas do NIST para o compartilhamento de informações são as seguintes:
 - Planeje a coordenação de incidentes com partes externas antes que os incidentes ocorram.
 - Consulte o departamento jurídico antes de iniciar qualquer esforço de coordenação.
 - Realize o compartilhamento de informações sobre incidentes durante todo o ciclo de vida de resposta a incidentes.
 - Tente automatizar o máximo possível do processo de compartilhamento de informações.
 - Equilibre os benefícios do compartilhamento de informações com as desvantagens do compartilhamento de informações confidenciais.

Lab - Tratamento de Incidentes

Neste laboratório, você aplicará seu conhecimento sobre procedimentos de tratamento de incidentes de segurança para formular perguntas sobre determinados cenários de incidentes.

28.5 Resumo de Análise e Resposta de Perícias Digitais e Incidentes

O que aprendi neste módulo?

- A perícia digital é a recuperação e investigação de informações encontradas em dispositivos digitais no que se refere à atividade criminosa.
- Indicadores de compromisso são as evidências de que um incidente de segurança cibernética ocorreu.
- O processo forense inclui quatro etapas: coleta, exame, análise e relatório.
- Nos processos judiciais, as provas são amplamente classificadas como diretas, indiretas, melhores evidências e evidências corroboradoras.
- A atribuição de ameaça refere-se ao ato de determinar o indivíduo, organização ou nação responsável por uma intrusão ou incidente de ataque bem sucedido.
- Em uma investigação baseada em evidências, a equipe de resposta a incidentes correlaciona Táticas, Técnicas e Procedimentos (TTP) que foram usados no incidente com outras explorações conhecidas.

O que aprendi neste módulo?

- O Quadro DE Táticas Contraditórias, Técnicas & Conhecimento Comum (ATT&CK) da MITRE permite detectar táticas, técnicas e procedimentos de ataque (TTP) como parte da defesa de ameaças e atribuição de ataque.
- A Cyber Kill Chain foi desenvolvida para identificar e prevenir invasões cibernéticas.
- As etapas da Cadeia de Cyber Kill são reconhecimento, armamento, entrega, exploração, instalação, comando e controle e ações sobre objetivos.
- O Modelo diamante de análise de intrusão representa um incidente de segurança ou evento.
- As quatro principais características de um evento de intrusão são adversários, capacidade, infraestrutura e vítima.
- A Resposta a Incidentes envolve os métodos, políticas e procedimentos que são usados por uma organização para responder a um ataque cibernético.

