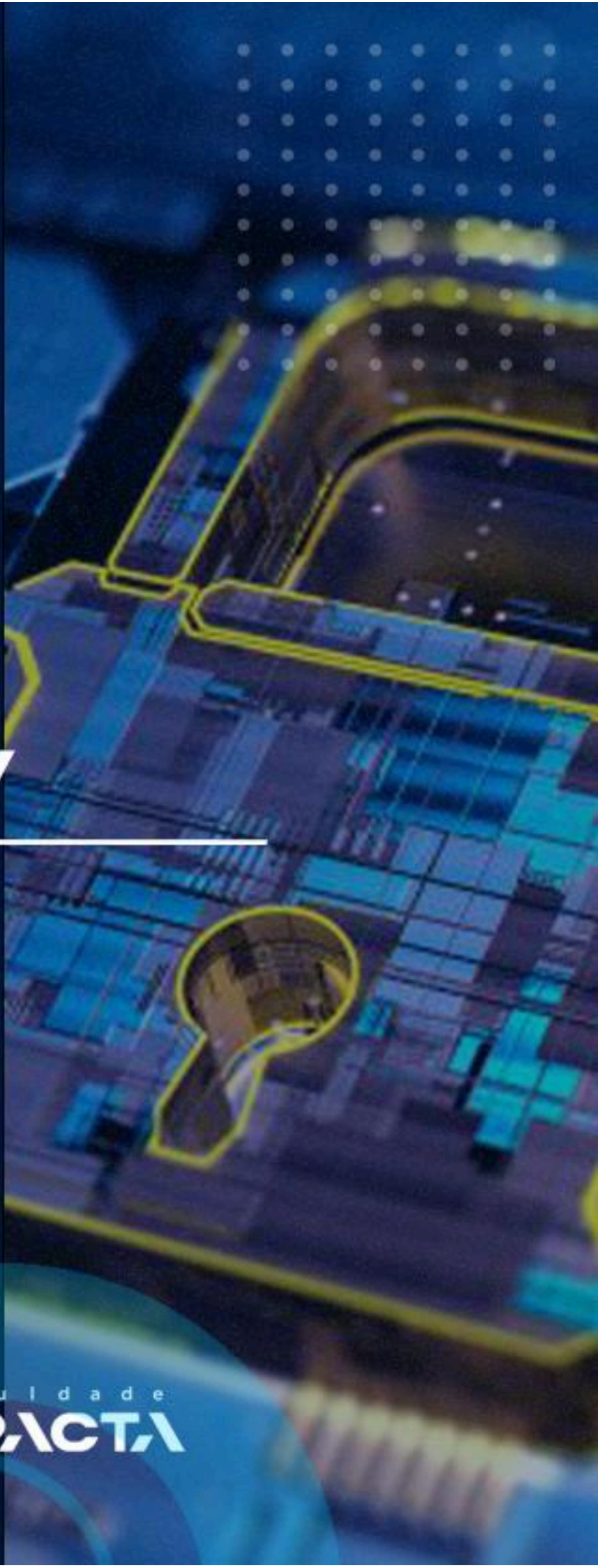
NEaD
Núcleo de Educação a Distância

CYBER SECURITY



Faculdade IMPACTA

12

Framework de Cibersegurança

Alex Sandro da Silva Feitosa

Resumo

Nessa aula iniciaremos com a função dos processos forenses digitais, Identificar as etapas na cadeia de destruição cibernética, classificar um evento de intrusão usando o modelo Diamond e Aplicar os procedimentos de tratamento de incidentes NIST 800-61r2 a um determinado cenário de incidente.

1.1. Forense Digital e Análise e Resposta a Incidentes

1.1.1 Manuseio de evidências e atribuição de ataque

A perícia digital é a recuperação e investigação de informações encontradas em dispositivos digitais no que se refere a atividades criminosas.

Os indicadores de comprometimento são a evidência de que ocorreu um incidente de segurança cibernética.

Por exemplo, de acordo com os regulamentos da HIPAA dos EUA, se a violação de dados tiver ocorrido envolvendo informações do paciente, 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 os regulamentos da HIPAA.

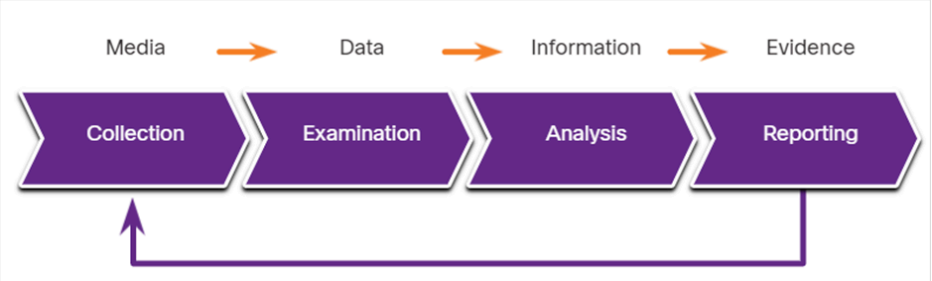
Às vezes, os analistas de segurança cibernética podem se encontrar em contato direto com evidências forenses digitais que detalham a conduta dos membros da organização.

Os analistas devem conhecer os requisitos relativos à preservação e manuseio de tais evidências.

O NIST descreve as quatro fases do processo forense de evidências digitais:

- **Coleta** - Identificação de fontes potenciais de dados forenses e aquisição, manuseio e armazenamento desses dados
- **Examinar** - Avaliação e extração de informações relevantes dos dados coletados
- **Análise** - Tirar conclusões dos dados e correlação de dados de fontes múltiplas
- **Relatórios** - Preparar e apresentar as informações resultantes da fase de análise.

Figura 1.1 fases do processo forense de evidências



Fonte: CCNA Cyber OPS Associate v1, 2020.

Em processos judiciais, as evidências são amplamente classificadas da seguinte forma:

- Provas diretas - As provas que estavam indiscutivelmente em posse do acusado ou são testemunhas oculares de alguém que observou diretamente o comportamento criminoso.
- Evidência indireta - Esta evidência estabelece uma hipótese em combinação com outros fatos. Também é conhecido como evidência circunstancial.
- Melhor evidência - essa evidência pode ser dispositivos de armazenamento usados por um acusado ou arquivos de arquivos que podem ser comprovados como inalterados.
- Evidência corroborante - Esta evidência apóia uma afirmação que é desenvolvida a partir das melhores evidências.

Ordem de coleta de evidências

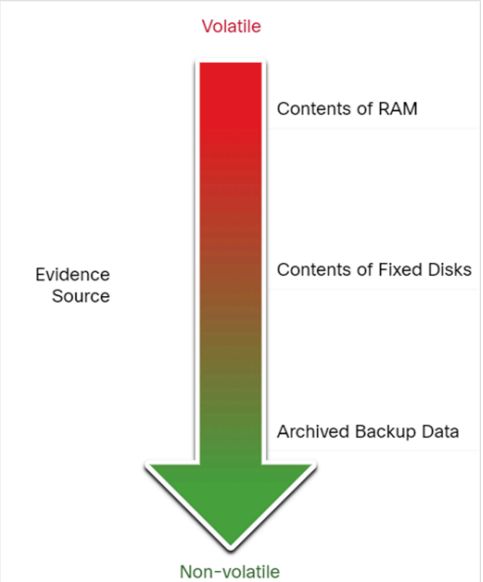
IETF RFC 3227 descreve uma ordem para a coleta de evidências digitais com base na volatilidade dos dados.

Os dados armazenados na RAM são os mais voláteis e serão perdidos quando o dispositivo for desligado.

A coleta de evidência digital deve começar com a evidência mais volátil e prosseguir para a 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 registrados.

Figura 1.2 IETF RFC 3227



Fonte: CCNA Cyber OPS Associate v1, 2020.

Cadeia de Custódia

A cadeia de custódia envolve a coleta, manuseio e armazenamento seguro de evidências.

Devem ser mantidos registros detalhados do seguinte:

- Quem descobriu e coletou as evidências?
- Todos os detalhes relativos ao manuseio de evidências, incluindo horários, locais e pessoal envolvido.
- Quem é o principal responsável pela evidência, quando a responsabilidade foi atribuída e quando a custódia mudou?
- Quem tem acesso físico às evidências enquanto elas foram armazenadas? O acesso deve ser restrito apenas ao pessoal mais importante.

Integridade e preservação de dados

O carimbo de data / hora dos arquivos deve ser preservado. Portanto, a evidência original deve ser copiada e a análise deve ser conduzida apenas em cópias do original.

Os carimbos de data / hora podem fazer parte das evidências, devendo-se evitar a abertura de arquivos da mídia original.

Arquive e proteja o disco original para mantê-lo em sua condição original, sem alterações.

Ferramentas especiais devem ser usadas para preservar as evidências forenses antes que o dispositivo seja desligado e as evidências sejam perdidas.

Os usuários não devem desconectar, desconectar ou desligar as máquinas infectadas, a menos que seja explicitamente instruído a fazê-lo pela equipe de segurança.

Seguir esses processos garantirá que qualquer evidência de negligência seja preservada e quaisquer indicadores de comprometimento possam ser identificados.

Atribuição de Ataque

Atribuição de ameaça refere-se ao ato de determinar o indivíduo, organização ou nação responsável por uma intrusão bem-sucedida ou incidente de ataque.

A identificação dos atores responsáveis pela ameaça deve ocorrer por meio de uma investigação sistemática e baseada em princípios das evidências.

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 podem ajudar na atribuição são a localização de hosts ou domínios de origem, recursos do código usado em malware e as ferramentas e outras técnicas.

Para ameaças internas, o gerenciamento de ativos desempenha um papel importante. Descobrir os dispositivos a partir dos quais um ataque foi lançado pode levar diretamente ao ator da ameaça.

Endereços IP, endereços MAC e logs de DHCP podem ajudar a rastrear os endereços usados no ataque a um dispositivo específico.

A Estrutura MITER ATT & CK

A estrutura MITER Adversarial Tactics, Techniques & Common Knowledge (ATT & CK) permite a capacidade de detectar táticas, técnicas e procedimentos (TTP) do invasor como parte da defesa contra ameaças e atribuição de ataques.

As táticas consistem nos objetivos técnicos que um atacante deve cumprir para executar um ataque.

As técnicas são os meios pelos quais as táticas são realizadas.

Os procedimentos são as ações específicas executadas pelos atores da ameaça nas técnicas que foram identificadas.

O MITER ATT & CK Framework é uma base de conhecimento global do comportamento do ator de ameaças.

A estrutura é projetada para permitir o compartilhamento automatizado de informações, definindo estruturas de dados para a troca de informações entre sua comunidade de usuários e o MITER.

Nota: Faça uma pesquisa na Internet sobre MITER ATT & CK para saber mais sobre a ferramenta.

1.1.2 A Cadeia de Eliminação Cibernética

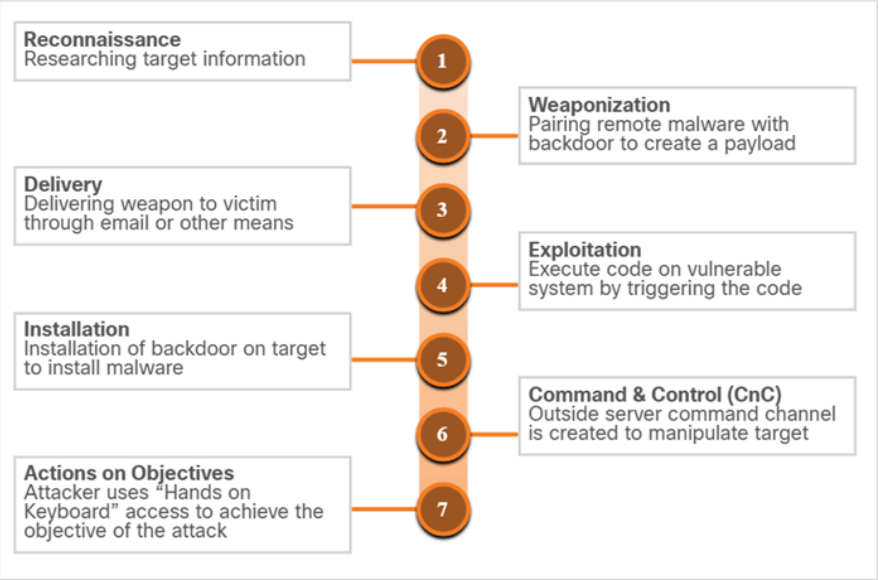
Etapas da cadeia de destruição cibernética:

O Cyber Kill Chain foi desenvolvido pela Lockheed Martin para identificar e prevenir intrusões cibernéticas.

Ao responder a um incidente de segurança, o objetivo é detectar e interromper o ataque o mais cedo possível na progressão da cadeia de destruição para evitar mais danos.

Se o atacante for interrompido em qualquer estágio, a cadeia de destruição será quebrada e o defensor impedirá com sucesso a intrusão do ator da ameaça.

Figura 1.3 Cyber Kill Chain



Fonte: CCNA Cyber OPS Associate v1, 2020.

Nota: O ator da ameaça refere-se à parte que está instigando o ataque. No entanto, a Lockheed Martin usa o termo "adversário" em Cyber Kill Chain. Portanto, os termos adversário e ator da ameaça são usados alternadamente neste tópico.

Reconhecimento

O reconhecimento é quando o agente da ameaça realiza pesquisas, reúne informações e seleciona os alvos.

O ator da ameaça escolherá os 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.

Tabela 1.1 Táticas e defesas durante a etapa de reconhecimento

Táticas Adversárias	**Defesas SOC**
Planejar e conduzir pesquisas: Colher endereços de e-mail Identifique os funcionários nas redes sociais Colete todas as informações de relações públicas (comunicados à imprensa, prêmios, participantes da conferência e assim por diante) Descubra servidores voltados para a Internet Realizar varreduras de rede para identificar endereços IP e portas abertas	Descubra a intenção do adversário: Alertas de log da web e dados históricos de pesquisa Análise do navegador da mina de dados Crie manuais para detectar comportamentos que indiquem atividade de reconhecimento Priorizar a defesa em torno de tecnologias e pessoas que a atividade de reconhecimento visa

Fonte: do autor, 2020.

Weaponization/Armamento

O armamento usa as informações do reconhecimento para desenvolver uma arma contra sistemas ou indivíduos específicos na organização.

Geralmente, é mais eficaz usar um ataque de dia zero para evitar métodos de detecção.

Um ataque de dia zero usa uma arma desconhecida para os defensores e sistemas de segurança de rede.

A tabela resume as táticas e defesas usadas durante a etapa de armamento.

Tabela 1.2 Táticas e defesas durante a etapa de armamento

Adversary Tactics	**SOC Defence**
Preparar e organizar a operação: Obtenha uma ferramenta automatizada para entregar a carga útil do malware (weaponizer). Selecione ou crie um documento para apresentar à vítima. Selecione ou crie uma backdoor e uma infraestrutura de comando e controle.	Detectar e coletar artefatos de armamento: Certifique-se de que as regras e assinaturas do IDS estejam atualizadas. Realize uma análise completa de malware. Crie detecções para o comportamento de armadores conhecidos. O malware é antigo, “disponível no mercado” ou é um malware novo que pode indicar um ataque personalizado? Colete arquivos e metadados para análises futuras. Determine quais artefatos de armador são comuns a quais campanhas.

Fonte: do autor, 2022.

Delivery/Entrega

Durante esta etapa, a arma é transmitida ao alvo usando um vetor de entrega. Se a arma não for entregue, o ataque não terá sucesso.

O ator da ameaça usará métodos diferentes para aumentar as chances de entregar a carga útil, como criptografar as 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 usadas durante a etapa de entrega.

Tabela 1.3 Táticas e defesas durante a etapa de entrega

Adversary Tactics	SOC Defence
Lançar malware no alvo: Direto contra servidores da web Entrega indireta por meio de: Email malicioso Malware em pen drive Interações de mídia social Sites comprometidos	Bloquear a entrega de malware: Analise o caminho da infraestrutura usado para entrega. Entenda os servidores, pessoas e dados direcionados disponíveis para o ataque. Inferir a intenção do adversário com base na seleção de alvos. Colete e-mails e logs da web para reconstrução forense.

Fonte: do autor, 2022.

Exploitation/Exploração

Depois que a arma foi entregue, o agente da ameaça a usa para quebrar a vulnerabilidade e obter 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.

Tabela 1.4 Táticas e defesas durante a etapa de exploração

Adversary Tactics	SOC Defence
Explorar uma vulnerabilidade para obter acesso: Use software, hardware ou vulnerabilidade humana Adquira ou desenvolva o exploit Use uma exploração acionada por adversário para vulnerabilidades de servidor Use uma exploração acionada pela vítima, como abrir um anexo de e-mail ou link da web malicioso	Treine funcionários, proteja o código e proteja os dispositivos: Treinamento de conscientização de segurança de funcionários e testes periódicos de e-mail Treinamento de desenvolvedor da Web para proteção de código Verificação regular de vulnerabilidade e teste de penetração Medidas de endurecimento de endpoint Auditoria de endpoint para determinar forense a origem da exploração

Fonte: do autor, 2022.

Installation/Instalação

Na etapa de instalação, o agente da ameaça estabelece uma porta dos fundos para o sistema para permitir o acesso contínuo ao alvo.

Para preservar esse backdoor, o acesso remoto não deve alertar analistas de segurança cibernética ou usuários. O método de acesso deve sobreviver por meio de verificações de antimalware e reinicialização do computador para ser eficaz.

A tabela resume as táticas e defesas usadas durante a etapa de instalação.

Tabela 1.5 Táticas e defesas durante a etapa de instalação

Adversary Tactics	SOC Defence
Instale backdoor persistente: Instale o webshell no servidor da web para acesso persistente. Crie um ponto de persistência adicionando serviços, chaves de AutoRun, etc. Alguns adversários modificam o carimbo de data / hora do malware para que ele apareça como parte do sistema operacional.	Detecte, registre e analise a atividade de instalação: HIPS para alertar ou bloquear em caminhos de instalação comuns. Determine se o malware requer privilégios elevados ou privilégios de usuário Auditoria de endpoint para descobrir criações de arquivos anormais. Determine se o malware é uma ameaça conhecida ou uma nova variante.

Fonte: do autor, 2022.

Command and Control/Comando e Controle

O objetivo é estabelecer Comando e Controle (CnC ou C2) com o sistema de destino.

Os hosts comprometidos geralmente emitem um beacon da rede para um controlador na Internet.

Os agentes de ameaças usam canais CnC para emitir comandos para o software que instalaram no destino.

O analista de segurança cibernética deve ser capaz de detectar comunicações CnC para descobrir o host comprometido.

A tabela resume as táticas e defesas usadas durante a etapa de comando e controle.

Tabela 1.6 Táticas e defesas durante a etapa de comando e controle

Adversary Tactics	**SOC Defence**
Open channel for target manipulation: Open two-way communications channel to CNC infrastructure Most common CNC channels over web, DNS, and email protocols CnC infrastructure may be adversary owned or another victim network itself	Last chance to block operation: Research possible new CnC infrastructures Discover CnC infrastructure though malware analysis Isolate DNS traffic to suspect DNS servers, especially Dynamic DNS Prevent impact by blocking or disabling CnC channel Consolidate the number of internet points of presence Customize rules blocking of CnC protocols on web proxies

Fonte: do autor, 2022.

Actions on Objectives/Ação e Objetivos

Ações com base nos objetivos é a etapa final da Cadeia de destruição cibernética que descreve o ator da ameaça alcançando seu objetivo original.

Nesse ponto, o ator da ameaça está profundamente enraizado nos sistemas da organização, escondendo seus movimentos e encobrindo seus rastros.

É extremamente difícil remover o ator da ameaça da rede.

A tabela resume as táticas e defesas usadas durante as ações sobre a etapa de objetivos.

Tabela 1.7 Táticas e defesas durante as ações sobre a etapa de objetivos

Adversary Tactics	SOC Defence
Obtenha as recompensas de um ataque bem-sucedido: Colete as credenciais do usuário Escalada de privilégios Reconhecimento interno Movimento lateral através do ambiente Colete e exfiltrar dados Destruir sistemas Substituir, modificar ou corromper dados	Detectar usando evidências forenses: Estabeleça o manual de resposta a incidentes Detecte exfiltração de dados, movimento lateral e uso não autorizado de credenciais Resposta imediata do analista para todos os alertas Análise forense de endpoints para triagem rápida Captura de pacotes de rede para recriar a atividade Realizar avaliação de danos

Fonte: do autor, 2022.

1.1.3 O modelo de diamante de análise de intrusão

O modelo Diamond de análise de intrusão representa um incidente ou evento de segurança.

Os quatro principais recursos de um evento de intrusão são:

Adversário - Partes responsáveis pela intrusão.

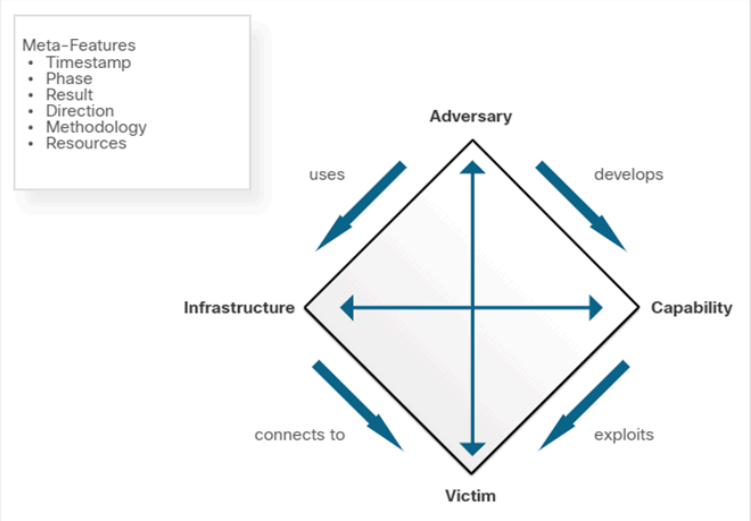
Capacidade - Ferramenta ou técnica usada pelo adversário para atacar a vítima.

Infraestrutura - Caminho (s) de rede usado (s) pelo adversário para estabelecer e manter o comando e controle sobre suas capacidades.

Vítima - alvo do ataque.

Os meta-recursos expandem o modelo ligeiramente para incluir os elementos importantes: Timestamp , Fase , Resultado , Direção , Metodologia e Recursos.

Figura 1.4 modelo Diamond



Fonte: CCNA Cyber OPS Associate v1, 2020.

Pivotando no Modelo Diamante

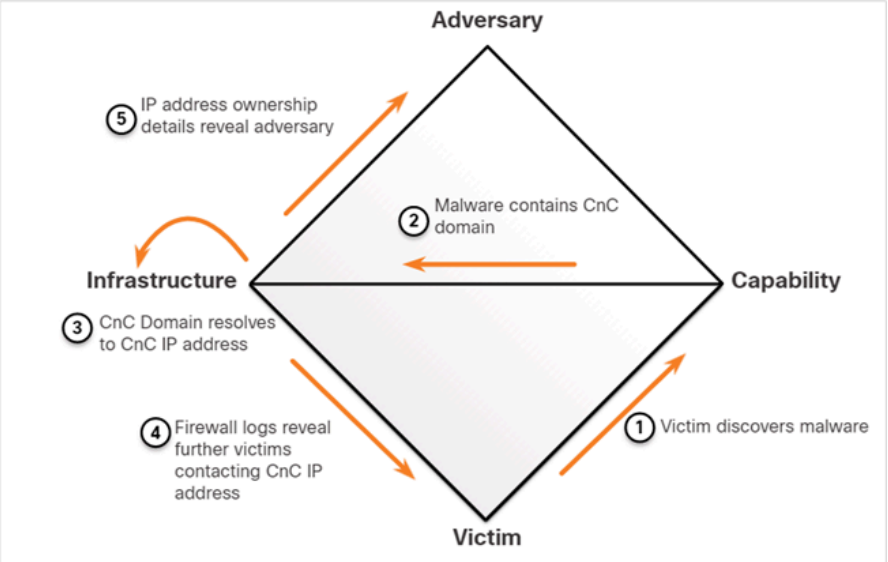
O modelo Diamond é ideal para ilustrar como o adversário gira de um evento para o outro. Por exemplo:

Um funcionário relata que seu computador está funcionando de maneira anormal. Uma varredura de 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 CnC que resultam em uma lista de endereços IP.

Esses endereços IP são usados para identificar o adversário e investigar os logs para determinar se outras vítimas na organização estão usando o canal CnC.

Figura 1.5 Diamond Model Characterization of an Exploit



Fonte: CCNA Cyber OPS Associate v1, 2020.

Os eventos são encadeados em uma cadeia na qual cada evento deve ser concluído antes do próximo evento. Este tópico de eventos pode ser mapeado para a Cadeia de Kill Cyber.

O exemplo ilustra o processo de ponta a ponta de um adversário à medida que atravessa a Cadeia de destruição cibernética:

O Adversary realiza uma pesquisa na web pela empresa vítima Gadgets, Inc., recebendo como parte dos resultados o nome de domínio gadgets.com.

Adversary pesquisa “administrador de rede gadget.com” e descobre postagens de fórum de usuários que afirmam ser administradores de rede de gadget.com e os perfis revelam seus endereços de e-mail.

O Adversary envia e-mails de phishing com um cavalo de Tróia anexado aos administradores de rede.

Um administrador de rede (NA1) abre o anexo malicioso que executa o exploit fechado.

O host do NA1 se registra com um controlador CnC enviando uma mensagem HTTP Post e recebendo uma resposta HTTP em retorno.

Foi revelado pela engenharia reversa que o malware possui endereços IP de backup adicionais.

Por meio de uma mensagem de resposta HTTP CnC enviada ao host do NA1, o malware começa a agir como um proxy para novas conexões TCP.

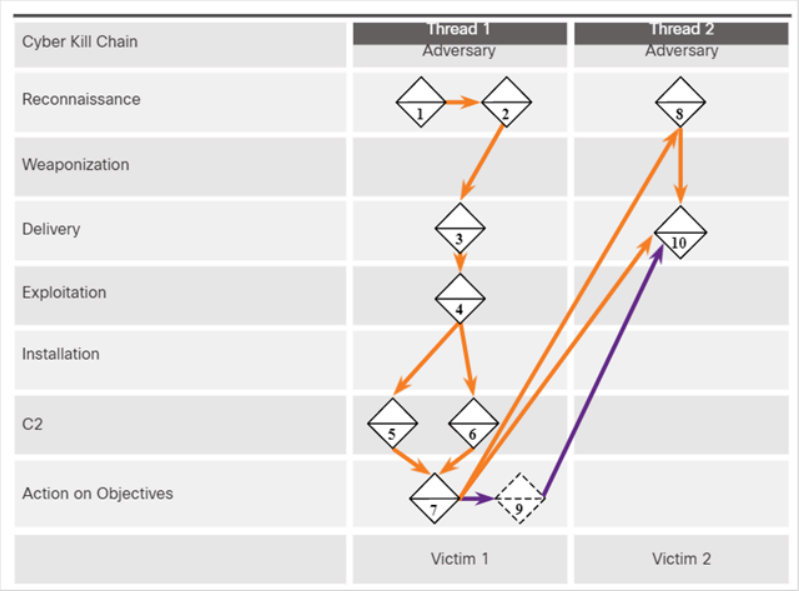
Por meio de informações do proxy que está sendo executado no host do NA1, o Adversary pesquisa na web por "a pesquisa mais importante de todos os tempos" e encontra Victim 2, Interesting Research Inc.

O Adversary verifica a lista de contatos de e-mail do NA1 em busca de qualquer contato da Interesting Research Inc. e descobre o contato do Diretor de Pesquisa da Interesting Research Inc.

O Diretor de Pesquisa da Interesting Research Inc. recebe um e-mail de spear-phish do endereço de e-mail do NA1 da Gadget Inc. enviado do host do NA1 com a mesma carga observada no Evento 3.

O adversário agora tem duas vítimas comprometidas a partir das quais ataques adicionais podem ser lançados.

Figura 1.5 Cyber Kill Chain



Fonte: CCNA Cyber OPS Associate v1, 2020.

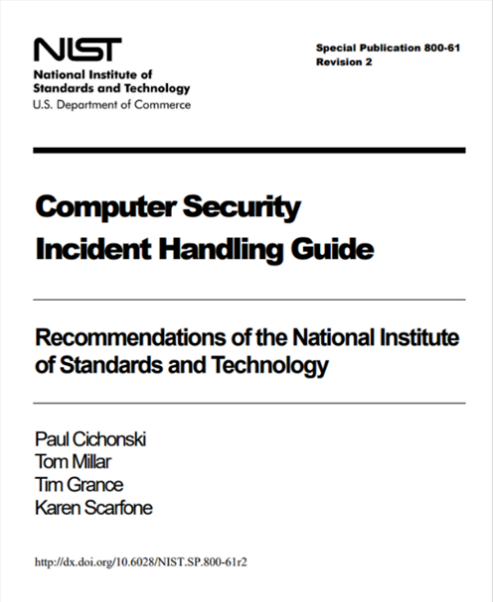
1.1.4 Resposta a Incidentes, Estabelecendo uma capacidade de resposta a incidentes

A resposta a incidentes 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 usados por uma organização para responder a um ataque cibernético.

Note: Embora este capítulo resuma o conteúdo do padrão NIST 800-61r2, você deve estar familiarizado com a publicação inteira, pois ela cobre quatro tópicos principais de exame para o exame Understanding Cisco Cybersecurity Operations Fundamentals.

Figura 1.6 NIST



Fonte: CCNA Cyber OPS Associate v1, 2020.

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

Tabela 1.8 Elementos de política, plano e procedimento em resposta a incidentes

Policy Elements	**Plan Elements**	**Procedure Elements**
Declaração de compromisso de gestão Finalidade e objetivos da política Escopo da política Definição de incidentes de segurança de computador e termos relacionados Estrutura organizacional e definição de funções, responsabilidades e níveis de autoridade Priorização de classificações de gravidade de incidentes Medidas de desempenho Relatórios e formulários de contato	Missão Estratégias e objetivos 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 geral	Processos técnicos Usando técnicas Preenchendo formulários Seguindo listas de verificação

Fonte: do autor, 2022.

As partes interessadas envolvidas em lidar com um incidente de segurança são as seguintes:

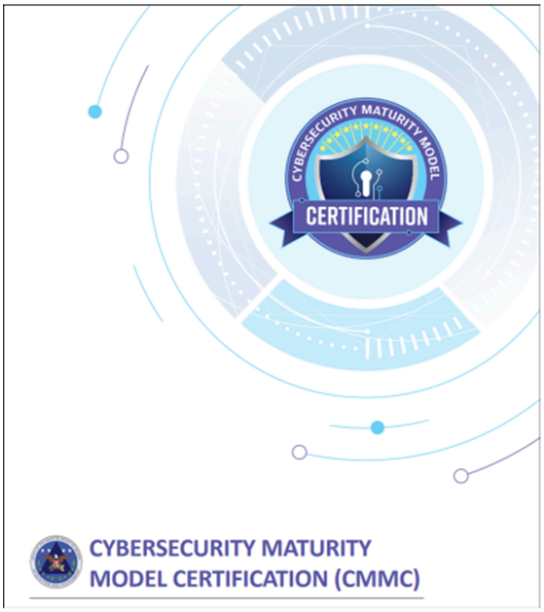
- Gestão
- Garantia de Informação
- Suporte de TI
- Departamento legal
- Relações Públicas e Relações com a Mídia
- Recursos Humanos
- Planejadores de Continuidade de Negócios
- Segurança Física e Gestão de Instalações

A Certificação do Modelo de Maturidade em Segurança Cibernética (CMMC)

O CMMC certifica organizações por nível. Para a maioria dos domínios, existem cinco níveis, no entanto, para a resposta a incidentes, existem apenas quatro:

- Nível 2 - Estabelece um plano de resposta a incidentes que segue o processo NIST.
- Nível 3 - Documentar e relatar incidentes às partes interessadas identificadas no plano de resposta a incidentes.
- Nível 4 - Use o conhecimento do invasor TTP para refinar o planejamento e a execução da resposta a incidentes.
- Nível 5 - Utilizar técnicas aceitas e sistemáticas de coleta de dados forenses por computador.

Figura 1.7 NIST



Fonte: CCNA Cyber OPS Associate v1, 2020.

Ciclo de vida de resposta a incidentes do NIST

O NIST define quatro etapas no ciclo de vida do processo de resposta a incidentes:

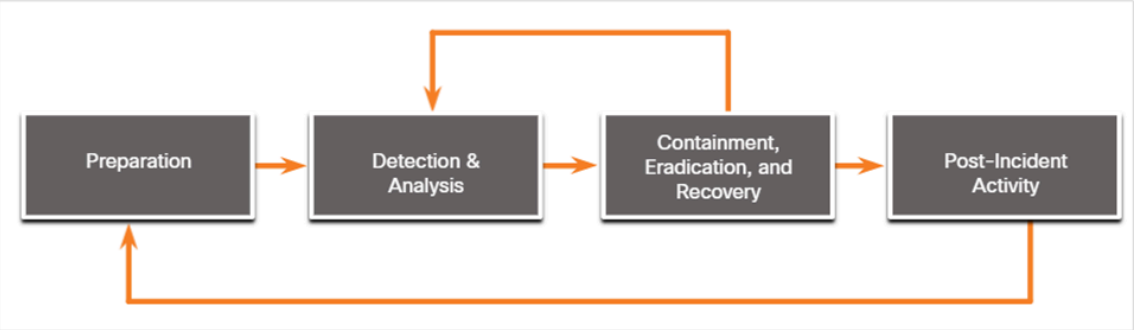
Preparação - Os membros do CSIRT são treinados em como responder a um incidente.

Detecção e análise - o CSIRT identifica, analisa e valida rapidamente um incidente.

Contenção, erradicação e recuperação - o CSIRT implementa procedimentos para conter a ameaça, erradicar o impacto nos ativos organizacionais e usar backups para restaurar dados e software.

Atividades pós-incidente - o CSIRT documenta como o incidente foi tratado, recomenda mudanças para resposta futura e específica como evitar uma recorrência.

Figura 1.8 Ciclo de vida de respostas a incidente do NIST



Fonte: CCNA Cyber OPS Associate v1, 2020.

Preparation

A fase de preparação é quando o CSIRT é criado e treinado. As ferramentas e ativos que serão necessários para a equipe 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.
- As avaliações de risco são usadas para implementar controles que limitarão o número de incidentes.
- Materiais de treinamento de conscientização de segurança do usuário são desenvolvidos.
- Hardware e software necessários para análise e mitigação de incidentes são adquiridos.

Detection and Analysis

Diferentes tipos de incidentes exigirão respostas diferentes:

Vetores de Ataque: Web, Email, Perda ou Roubo, Roubo de Identidade, Atrito e Mídia.

Detecção: Detecção automatizada - software antivírus, IDS, detecção manual - relatórios do usuário.

Análise: Use Network and System Profiling para determinar a validade dos incidentes de segurança.

Escopo: Fornece informações sobre a contenção do incidente e uma análise mais profunda dos efeitos do incidente.

Notificação de Incidente: Notifique as partes interessadas apropriadas e partes externas, uma vez que o incidente seja analisado e priorizado.

Containment, Eradication, and Recovery

Depois de determinar a validade do incidente por meio de detecção e análise, ele deve ser contido.

Estratégia de contenção: para cada tipo de incidente, uma estratégia de contenção deve ser criada e aplicada dependendo de algumas condições.

Provas: durante um incidente, as provas devem ser reunidas para resolvê-lo. É necessário para investigação subsequente por parte das autoridades.

Identificação de invasores: a identificação de invasores minimizará o impacto em ativos e serviços críticos de negócios.

Erradicação, recuperação e remediação: para erradicar, identifique todos os hosts que precisam de remediação; para recuperar hosts, use backups limpos e recentes ou reconstrua-os com a mídia de instalação.

Post-Incident Activities

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

Hardening baseado em lições

A organização deve realizar uma reunião de "lições aprendidas" para:

- Revise a eficácia do processo de tratamento de incidentes.
- Identifique o reforço necessário para os controles e práticas de segurança existentes.

A tabela abaixo resume a coleta e retenção de dados do incidente:

Tabela 1.9 Coleta e retenção de dados do incidente

Incident Data Collection	Retention
Os dados coletados após a reunião de lições aprendidas 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 mão de obra usada e o tempo total de cada fase do processo de resposta ao incidente. Colete apenas dados que podem ser usados para definir e refinar o processo de tratamento de incidentes. Faça uma avaliação objetiva de cada Incidente.	Alguns dos fatores determinantes para retenção de evidências: Acusação - Quando um invasor será processado por causa de um incidente de segurança, as evidências devem ser retidas até que todas as ações legais tenham sido concluídas. Tipo de dados - Uma organização pode especificar que tipos específicos de dados devem ser mantidos por um determinado período de tempo. Custo - se houver muitos hardwares e mídias de armazenamento que precisam ser armazenados por muito tempo, isso pode se tornar caro.

Fonte: do autor, 2021.

Requisitos de relatórios e compartilhamento de informações

As regulamentações governamentais devem ser consultadas pela equipe jurídica para determinar a responsabilidade da organização em relatar o incidente.

A gerência precisa determinar que comunicação adicional é necessária com outras partes interessadas, como clientes, fornecedores, parceiros e assim por diante.

O NIST recomenda que uma organização coordene com organizações para compartilhar detalhes do 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 o processo de compartilhamento de informações.
- Equilibre os benefícios do compartilhamento de informações com as desvantagens de compartilhar informações confidenciais.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível: <https://www.netacad.com>.

SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes**: primeiros passos. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security**: applications and standards. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002**: Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.