**Introdução**

26.0.1

**Por que devo cursar este módulo?**

Uma habilidade crítica para um analista de segurança cibernética é a capacidade de avaliar alertas e decidir o que fazer com eles. Neste módulo, você aprenderá de onde vêm os alertas, fluxos de trabalho comuns associados a alertas e métodos padrão para avaliar e classificar alertas.

26.0.2

**O que vou aprender neste módulo?**

**Module Title**: Evaluating Alerts

**Module Objective**: Explain the process of evaluating alerts

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Fonte de Alertas | Identificar a estrutura dos alertas. |
| Visão geral da avaliação de alerta | Explique como os alertas são classificados |

# Fontes de alertas

26.1.1

## Security Onion

O Security Onion é um pacote de código aberto de ferramentas de Monitoramento de Segurança de Rede (NSM) que é executado em uma distribuição Ubuntu Linux. As ferramentas Security Onion fornecem três funções principais para o analista de segurança cibernética: captura completa de pacotes e tipos de dados, sistemas de detecção de intrusão baseados em rede e em host e ferramentas de analistas de alerta. Security Onion pode ser instalado como uma instalação autônoma ou como um sensor e plataforma de servidor. Alguns componentes do Security Onion são de propriedade e mantidos por corporações, como Cisco e Riverbend Technologies, mas são disponibilizados como código aberto.

Para obter mais informações e para obter o Security Onion, pesquise na internet o site Security Onion.

**Observação**: em alguns recursos, você pode ver Security Onion abreviado como SO. Neste curso, usaremos Security Onion.

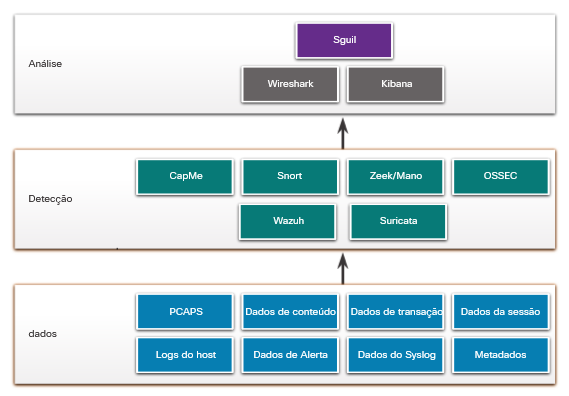
26.1.2

## Ferramentas de detecção para coleta de dados de alerta

Security Onion contém muitos componentes. É um ambiente integrado projetado para simplificar a implantação de uma solução NSM abrangente. A figura ilustra uma visão simplificada da maneira como alguns dos componentes do Security Onion trabalham juntos.

O gráfico exibe uma arquitetura de três níveis para Security Onion. O nível inferior é rotulado como dados. Ele inclui os seguintes elementos: pcaps, dados de transação de dados de conteúdo, dados de sessão, logs de host, dados de alerta, dados de syslog e metadados. A camada intermediária é rotulada como detecção. Inclui os seguintes elementos: CapMe, Snort, Bro, OSSEC e Suricata. O nível superior é rotulado como Análise. Inclui Sguil com Wireshark e ELSA suportando Sguil.

### Uma arquitetura do Security Onion



AnáliseDetecçãodadosSguilWiresharkKibanaCapMeSnortZeek/ManoOSSECPCAPSDados de conteúdoDados de transaçãoDados da sessãoLogs do hostDados de AlertaDados do SyslogMetadadosSuricataWazuh

CapMe

Esta é uma aplicação web que permite a visualização de transcrições pcap renderizadas com as ferramentas tcpflow ou Zeek. O CapMe pode ser acessado a partir da ferramenta ELSA (Enterprise Log Search and Archive). O CapMe oferece ao analista de segurança cibernética um meio fácil de ler para visualizar uma sessão inteira da Camada 4. O CapMe atua como um plugin para o ELSA e fornece acesso a arquivos pcap relevantes que podem ser abertos no Wireshark.

Snort

Este é um Sistema de Detecção de Intrusão de Rede (NIDS). É uma importante fonte de dados de alerta indexados na ferramenta de análise Sguil. O Snort usa regras e assinaturas para gerar alertas. O Snort pode baixar automaticamente novas regras usando o componente PulledPork do Security Onion. Snort e PulledPork são ferramentas de código aberto que são patrocinadas pela Cisco.

O Zeek

Anteriormente conhecido como Bro. Este é um NIDS que usa mais uma abordagem baseada em comportamento para detecção de intrusões. Em vez de usar assinaturas ou regras, o Zeek usa políticas, na forma de scripts que determinam quais dados registrar e quando emitir notificações de alerta. O Zeek também pode enviar anexos de arquivos para análise de malware, bloquear o acesso a locais mal-intencionados e desligar um computador que parece estar violando políticas de segurança.

**Observação:** Algumas interfaces dentro do Security Onion ainda não foram atualizadas com a alteração de nome de Bro para Zeek.

OSSEC

Este é um sistema de detecção de intrusão baseado em host (HIDS) integrado ao Security Onion. Ele monitora ativamente as operações do sistema host, incluindo a realização de monitoramento de integridade de arquivos, monitoramento de log local, monitoramento de processos do sistema e detecção de rootkit. Alertas OSSEC e dados de log estão disponíveis para Sguil e Kibana. O OSSEC requer que um agente seja executado nos computadores Windows da empresa.

Wazuh

Wazuh é um HIDS que substituirá OSSEC em Security Onion. É uma solução completa que fornece um amplo espectro de mecanismos de proteção de terminais, incluindo análise de arquivos de log do host, monitoramento de integridade de arquivos, detecção de vulnerabilidades, avaliação de configuração e resposta a incidentes. Assim como o OSSEC, ele exige que os agentes estejam sendo executados em hosts de rede.

Suricata

Este é um NIDS que usa uma abordagem baseada em assinaturas. Ele também pode ser usado para prevenção de intrusões em linha. É semelhante ao Zeek; no entanto, o Suricata usa multithreading nativo, que permite a distribuição do processamento de fluxo de pacotes em vários núcleos de processadores. Ele também inclui alguns recursos adicionais, como bloqueio baseado em reputação e suporte para multithreading de unidade de processamento gráfico (GPU) para melhorar o desempenho.

26.1.3

## Ferramentas de Análise

O Security Onion integra esses vários tipos de dados e logs do Sistema de Detecção de Intrusões (IDS) em uma única plataforma através das seguintes ferramentas:

* **Sguil** - Isso fornece um console de alto nível para investigar alertas de segurança de uma ampla variedade de fontes. Sguil serve como ponto de partida na investigação de alertas de segurança. Uma grande variedade de fontes de dados está disponível para o analista de segurança cibernética, girando diretamente do Sguil para outras ferramentas.
* **Kibana** - Kibana é uma interface de painel interativo para dados do Elasticsearch. Ele permite a consulta de dados do NSM e fornece visualizações flexíveis desses dados. Ele fornece recursos de análise de dados de exploração de dados e aprendizado de máquina. É possível girar do Sguil diretamente para o Kibana para ver exibições contextualizadas com base nos endereços IP de origem e destino associados a um alerta. Pesquise na internet e visite o site elastic.co para saber mais sobre os muitos recursos do Kibana.
* **Wireshark** - Este é um aplicativo de captura de pacotes integrado ao conjunto Security Onion. Ele pode ser aberto diretamente de outras ferramentas e exibirá capturas completas de pacotes relevantes para uma análise.
* **Zeek** - Este é um analisador de tráfego de rede que serve como um monitor de segurança. O Zeek inspeciona todo o tráfego em um segmento de rede e permite uma análise aprofundada desses dados. A rotação do Sguil para o Zeek fornece acesso a logs de transações muito precisos, conteúdo de arquivos e saída personalizada.

**Nota**: Outras ferramentas Security Onion que não são mostradas na figura estão além do escopo deste curso. Uma descrição completa do Security Onion e seus componentes pode ser encontrada no site Security Onion.

26.1.4

## Geração de alertas

Alertas de segurança são mensagens de notificação geradas por ferramentas, sistemas e dispositivos de segurança do NSM. Os alertas podem vir em várias formas, dependendo da fonte. Por exemplo, o syslog fornece suporte para classificações de gravidade que podem ser usadas para alertar analistas de segurança cibernética sobre eventos que exigem atenção.

No Security Onion, o Sguil fornece um console que integra alertas de várias fontes em uma fila com carimbo de data/hora. Um analista de segurança cibernética pode trabalhar na fila de segurança investigando, classificando, escalonando ou retirando alertas. Em vez de usar um sistema de gerenciamento de fluxo de trabalho dedicado, como o RTIR (Request Tracker for Incident Response), um analista de segurança cibernética usaria a saída de um aplicativo como o Sguil para orquestrar uma investigação do NSM.

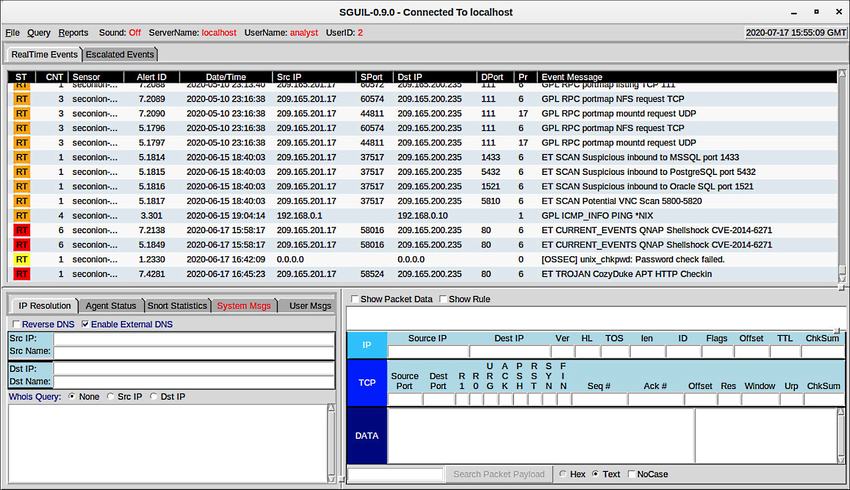
Os alertas geralmente incluem informações de cinco tuplas quando disponíveis, bem como carimbos de data/hora e informações que identificam qual dispositivo ou sistema gerou o alerta. Lembre-se de que as cinco tuplas incluem as seguintes informações para rastrear uma conversa entre um aplicativo de origem e destino:

* **SrcIP** - o endereço IP de origem para o evento.
* **SPort** - a porta de Camada 4 de origem (local) para o evento.
* **DstIP** - o IP de destino para o evento.
* **DPort** - a porta de Camada 4 de destino para o evento.
* **Pr** - o número do protocolo IP para o evento.

Informações adicionais podem ser se uma decisão de permissão ou negação foi aplicada ao tráfego, alguns dados capturados da carga útil do pacote ou um valor de hash para um arquivo baixado ou qualquer um dos vários dados.

A figura mostra a janela do aplicativo Sguil com a fila de alertas que estão aguardando para serem investigados na parte superior da interface.

### Janela Sguil



Os campos disponíveis para os eventos em tempo real são os seguintes:

* **ST** - This is the status of the event. RT means real time. The event is color-coded by priority. The priorities are based on the category of the alert. There are four priority levels: muito baixo, baixo, médio e alto. As cores variam de amarelo claro a vermelho à medida que a prioridade aumenta.
* **CNT** - Esta é a contagem do número de vezes que este evento foi detectado para o mesmo endereço IP de origem e destino. O sistema determinou que este conjunto de eventos está correlacionado. Em vez de relatar cada um em uma série potencialmente longa de eventos correlacionados nesta janela, o evento é listado uma vez com o número de vezes que foi detectado nesta coluna. Números altos aqui podem representar um problema de segurança ou a necessidade de ajuste das assinaturas de eventos para limitar o número de eventos potencialmente falsos que estão sendo relatados.
* **Sensor** - Este é o agente que relata o evento. Os sensores disponíveis e seus números de identificação podem ser encontrados na guia Status do agente do painel, que aparece abaixo da janela de eventos à esquerda. Esses números também são usados na coluna ID de alerta. No painel Status do Agente, podemos ver que os sensores OSSEC, pcap e Snort estão reportando ao Sguil. Além disso, podemos ver os nomes de host padrão para esses sensores, que inclui a interface de monitoramento. Observe que cada interface de monitoramento tem dados pcap e Snort associados a ele.
* **ID de alerta** - Este número de duas partes representa o sensor que relatou o problema e o número de evento desse sensor. Podemos ver a partir da figura que o maior número de eventos que são exibidos são do sensor OSSEC (1). O sensor OSSEC relatou oito conjuntos de eventos correlacionados. Destes eventos, 232 foram relatados com ID de evento 1.24.
* **Data/Hora** - Este é o carimbo de data/hora do evento. No caso de eventos correlacionados, é o carimbo de data/hora do primeiro evento.
* **Mensagem de Evento** - Este é o texto de identificação para o evento. Isso é configurado na regra que disparou o alerta. A regra associada pode ser visualizada no painel direito, logo acima dos dados do pacote. Para exibir a regra, a caixa de seleção **Mostrar regra** deve ser marcada.

Dependendo da tecnologia de segurança, os alertas podem ser gerados com base em regras, assinaturas, anomalias ou comportamentos. Não importa como eles são gerados, as condições que acionam um alerta devem ser predefinidas de alguma maneira.

26.1.5

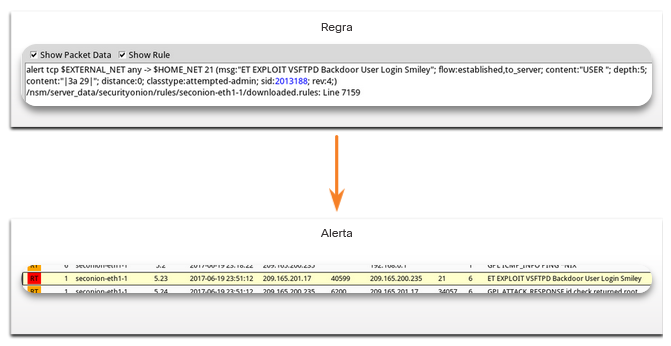
## Regras e Alertas

Os alertas podem vir de várias fontes:

* **NIDS** - Snort, Zeek e Suricata
* **HIDS** - OSSEC, Wazuh
* **Gerenciamento e monitoramento de ativos** - Sistema de detecção de ativos passivos (PADS)
* **Transações HTTP, DNS e TCP** - Registradas pelo Zeek e pcaps
* **Mensagens do Syslog**\* - Várias fontes

As informações encontradas nos alertas que são exibidos no Sguil serão diferentes no formato de mensagem porque elas vêm de fontes diferentes.

O alerta Sguil na figura foi acionado por uma regra que foi configurada no Snort. É importante que o analista de segurança cibernética seja capaz de interpretar o que acionou o alerta para que o alerta possa ser investigado. Por esse motivo, o analista de segurança cibernética deve entender os componentes das regras do Snort, que são uma das principais fontes de alertas em Security Onion.



A figura mostra duas seções principais: regra e alerta. Uma seta vai da seção de regra apontando para a seção de alerta. Informações na seção de regra: habilitada caixa de seleção Mostrar dados de pacote e caixa de seleção Mostrar regra. Text: alert t c p $EXTERNAL\_NET any -> $HOME\_NET 21 (msg:ET EXPLOIT VSFTPD backdoor user login smiley; flow:established,to\_server; content:USER; depth:5; content:|3a 29|; distance:0; classtype:attempted-admin; sid:2013188; rev:4;) /nsm/server\_data/securityonion/rules/seconion-eth1-1/downloaded.rules: Line 7159. Alert highlighted text: R T 1 seconion-eth1-1 5.23 2017-06-19 23:51:12 209 dot 165 dot 201 dot 17 40599 209 dot 165 dot 200 dot 235 21 6 ET EXPLOIT VSFTPD backdoor user login smiley.

### Alerta de Sguil e a Regra Associada

RegraAlerta

26.1.6

## Estrutura de Regra Snort

As regras de Snort consistem em duas seções, como mostrado na figura: o cabeçalho da regra e as opções da regra. O cabeçalho da regra contém a ação, o protocolo, os endereços IP de origem e destino e as máscaras de rede e as informações da porta de origem e destino. A seção Opções de regra contém mensagens de alerta e informações sobre quais partes do pacote devem ser inspecionadas para determinar se a ação da regra deve ser executada. A localização da regra às vezes é adicionada pelo Sguil. Local da Regra é o caminho para o arquivo que contém a regra e o número da linha em que a regra aparece para que ela possa ser encontrada e modificada, ou eliminada, se necessário.

A figura mostra o texto em azul : alert ip any any -> any any, in green: (msg: GPL ATTACK\_RESPONSE id check returned root; content: uid=0|28|root|29|; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;), and in purple: /nsm/server\_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692.

### Estrutura da regra Snort e informações fornecidas pelo SGUI



alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)/nsm/server\_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692

| **Componente** | **Exemplo (encurtado...)** | **Explicação** |
| --- | --- | --- |
| cabeçalho da regra | alert ip any any -> any any | Contém a ação a ser tomada, endereços e porta de origem e destino, e a direção do fluxo de tráfego |
| opções de regra | (msg:”GPL ATTACK\_RESPONSE ID CHECK RETURNED ROOT”;…) | Inclui a mensagem a ser exibida, detalhes do conteúdo do pacote, tipo de alerta, ID de origem e detalhes adicionais, como uma referência para a regra ou vulnerabilidade |
| local da regra | /nsm/server\_data/securityonion/rules/… | Adicionado pelo Sguil para indicar a localização da regra na estrutura do arquivo Security Onion e no arquivo de regra especificado |

**O cabeçalho da regra**

O cabeçalho da regra contém a ação, o protocolo, o endereçamento e as informações da porta, conforme mostrado na figura. Além disso, a direção do fluxo que acionou o alerta é indicada. A estrutura da parte do cabeçalho é consistente entre as regras de alerta Snort.

O Snort pode ser configurado para usar variáveis para representar endereços IP internos e externos. Essas variáveis, **$HOME\_NET** e **$EXTERNAL\_NET**, aparecem nas regras Snort. Eles simplificam a criação de regras, eliminando a necessidade de especificar endereços e máscaras específicos para cada regra. Os valores dessas variáveis são configurados no **snort.conf** arquivo. O Snort também permite que endereços IP individuais, blocos de endereços ou listas de ambos sejam especificados em regras. Os intervalos de portas podem ser especificados separando os valores superior e inferior do intervalo com dois pontos. Outros operadores também estão disponíveis.

A figura mostra o texto em azul: alerta ip any any -> any any any, em seguida, o texto na fonte normal: (msg: GPL ATTACK\_RESPONSE id check retornou root; content: uid=0|28|root|29|; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;) /NSM/server\_data/securityonion/rules/secon/ion-eth1-1/downloaded.regras:Linha 692.

### Estrutura do cabeçalho da regra Snort



alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)/nsm/server\_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692

| **Componente** | **Explicação** |
| --- | --- |
| alerta | a ação a ser tomada é emitir um alerta, outras ações são registradas e passadas |
| ip | o protocolo |
| qualquer | a fonte especificada é qualquer endereço IP e qualquer porta da Camada 4 |
| -> | a direção do fluxo é da origem para o destino |
| any any | o destino especificado é qualquer endereço IP e qualquer porta da Camada 4 |

**As Opções de Regra**

A estrutura da seção de opções da regra é variável. É a parte da regra que está entre parênteses, como mostrado na figura. Ele contém a mensagem de texto que identifica o alerta. Ele também contém metadados sobre o alerta, como um URL que fornece informações de referência para o alerta. Outras informações podem ser incluídas, como o tipo de regra e um identificador numérico exclusivo para a regra e a revisão da regra. Além disso, os recursos da carga do pacote podem ser especificados nas opções. O manual de usuários do Snort, que pode ser encontrado na internet, fornece detalhes sobre regras e como criá-las.

Mensagens de regra de snifar podem incluir a origem da regra. Três fontes comuns para as regras do Snort são:

* **GPL** - Regras mais antigas do Snort que foram criadas pelo Sourcefire e distribuídas sob uma GPLv2. O conjunto de regras GPL não é certificado pelo Cisco Talos. Inclui Snort SIDs 3464 e abaixo. O conjunto de regras GPL pode ser baixado do site do Snort e está incluído no Security Onion.
* **ET** - Regras Snort de ameaças emergentes. Emerging Threats é um ponto de coleta para regras Snort de várias fontes. As regras ET são de código aberto sob uma licença BSD. O conjunto de regras ET contém regras de várias categorias. Um conjunto de regras ET está incluído com Security Onion. Emerging Threats é uma divisão da Proofpoint, Inc.
* **VRT** - Essas regras estão imediatamente disponíveis para assinantes e são liberadas para usuários registrados 30 dias após sua criação, com algumas limitações. Eles agora são criados e mantidos pelo Cisco Talos.

As regras podem ser baixadas automaticamente do Snort.org usando o utilitário de gerenciamento de regras PulledPork que está incluído com o Security Onion.

Alertas que não são gerados pelas regras do Snort são identificados pelas tags OSSEC ou PADS, entre outras. Além disso, regras locais personalizadas podem ser criadas.

A figura mostra o texto em fonte normal: alert ip any any -> any any, then text in green: (msg: GPL ATTACK\_RESPONSE id check returned root; content: uid=0|28|root|29|; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;), então texto em fonte normal : /nsm/server\_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692.

### Estrutura de Opções de Regras Snort



alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)/nsm/server\_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692

| **Componente** | **Explicação** |
| --- | --- |
| msg: | Texto que descreve o alerta. |
| content: | Refere-se ao conteúdo do pacote. Nesse caso, um alerta será enviado se o texto literal “uid=0 (root)” aparecer em qualquer lugar nos dados do pacote. Valores que especificam a localização do texto na carga de dados podem ser fornecidos. |
| reference: | Isso não é mostrado na figura. Muitas vezes, é um link para uma URL que fornece mais informações sobre a regra. Nesse caso, o sid é hipervinculado à origem da regra na Internet. |
| classtype: | Uma categoria para o ataque. O Snort inclui um conjunto de categorias padrão que têm um dos quatro valores de prioridade. |
| sid: | Um identificador numérico exclusivo para a regra. |
| rev: | A revisão da regra que é representada pelo sid. |

26.1.7

## Laboratório - Regras de Snort e Firewall

Diferentes dispositivos de segurança e software executam funções diferentes e registram eventos diferentes. Como conseqüência, os alertas gerados por diferentes equipamentos e software também variam.

Neste laboratório, para se familiarizar com as regras de firewall e as assinaturas IDS, você:

* Realizar monitoramento ao vivo de IDS e eventos.
* Configure sua própria regra de firewall personalizada para impedir que hosts internos contatem um servidor de hospedagem de malware.
* Crie um pacote malicioso e inicie-o contra um alvo interno.
* Crie uma regra IDS personalizada para detectar o ataque personalizado e emitir um alerta com base nele.

[26.0](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[Introdução](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[26.2](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# Visão geral da avaliação de alerta

26.2.1

## A necessidade de avaliação de alerta

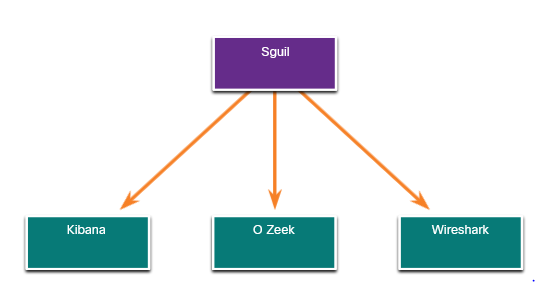
O cenário de ameaças está mudando constantemente à medida que novas vulnerabilidades são descobertas e novas ameaças evoluem. À medida que as necessidades do usuário e organizacional mudam, a superfície do ataque também. Os atores de ameaças aprenderam a variar rapidamente os recursos de suas explorações para evitar a detecção.

É impossível projetar medidas para evitar todas as façanhas. As explorações irão inevitavelmente fugir às medidas de protecção, por mais sofisticadas que sejam. Às vezes, o melhor que pode ser feito é detectar exploits durante ou depois de terem ocorrido. As regras de detecção devem ser excessivamente conservadoras. Em outras palavras, é melhor ter alertas que às vezes são gerados por tráfego inocente, do que ter regras que perdem tráfego malicioso. Por esse motivo, é necessário que analistas qualificados de segurança cibernética investiguem alertas para determinar se uma exploração realmente ocorreu.

Os analistas de segurança cibernética de nível 1 costumam trabalhar em filas de alertas em uma ferramenta como Sguil, girando para ferramentas como Zeek, Wireshark e Kibana para verificar se um alerta representa uma exploração real.

A figura mostra uma caixa de texto Squil no topo com uma linha apontando para cada uma das três caixas abaixo: Kibana, Zeek e WireShark.

### Ferramentas primárias para o analista de segurança cibernética de nível 1



SguilKibanaO ZeekWireshark

26.2.2

## Avaliação de alertas

Os incidentes de segurança são classificados usando um esquema emprestado de diagnósticos médicos. Este esquema de classificação é usado para orientar ações e avaliar procedimentos de diagnóstico. Por exemplo, quando um paciente visita um médico para um exame de rotina, uma das tarefas do médico é determinar se o paciente está doente. Um dos resultados pode ser uma determinação correta de que a doença está presente e o paciente está doente. Outro resultado pode ser que não há doença e o paciente é saudável.

A preocupação é que o diagnóstico pode ser preciso, ou verdadeiro, ou impreciso, ou falso. Por exemplo, o médico pode perder os sinais de doença e fazer a determinação incorreta de que o paciente está bem quando está de fato doente. Outro erro possível é decidir que um paciente está doente quando esse paciente é de fato saudável. Os falsos diagnósticos são caros ou perigosos.

Na análise de segurança de rede, o analista de segurança cibernética é apresentado com um alerta. Isso é semelhante a um paciente indo ao médico e dizendo: “Estou doente”. O analista de segurança cibernética, como o médico, precisa determinar se esse diagnóstico é verdadeiro. O analista de segurança cibernética pergunta: “O sistema diz que ocorreu uma exploração. Isso é verdade?”

Os alertas podem ser classificados da seguinte forma:

* **Verdadeiro Positivo**: O alerta foi verificado como sendo um incidente de segurança real.
* **Falso Positivo**: O alerta não indica um incidente de segurança real. A atividade benigna que resulta em um falso positivo é às vezes referida como um gatilho benigno.

Uma situação alternativa é que um alerta não foi gerado. A ausência de um alerta pode ser classificada como:

* **Verdadeiro Negativo**: Nenhum incidente de segurança ocorreu. A atividade é benigna.
* **Falso Negativo**: Ocorreu um incidente não detectado.

| **Quando um alerta é emitido, ele receberá uma das quatro classificações possíveis** | | |
| --- | --- | --- |
|  | **Verdadeiro** | **Falso** |
| **Positivo (Alerta existe)** | Ocorreu um incidente | Nenhum incidente ocorreu |
| **Negativo (Nenhum alerta existe)** | Nenhum incidente ocorreu | Ocorreu um incidente |
| **Nota**: Os eventos “Verdadeiros” são desejáveis. Os eventos “falsos” são indesejáveis e potencialmente perigosos. | | |

**Verdadeiros positivos** são o tipo de alerta desejado. Eles significam que as regras que geram alertas funcionaram corretamente. **Falsos positivos não** são desejáveis. Embora eles não indiquem que ocorreu uma exploração não detectada, eles são caros porque os analistas de segurança cibernética devem investigar alarmes falsos; portanto, o tempo é retirado da investigação de alertas que indicam verdadeiras explorações. **Verdadeiros negativos** são desejáveis. Eles indicam que o tráfego normal benigno é corretamente ignorado e alertas errôneos não estão sendo emitidos. **Falsos negativos** são perigosos. Eles indicam que as explorações não estão sendo detectadas pelos sistemas de segurança que estão em vigor. Esses incidentes podem passar despercebidos por um longo período de tempo, e a perda e danos contínuos de dados podem resultar.

Eventos benignos são aqueles que não devem acionar alertas. Os eventos benignos em excesso indicam que algumas regras ou outros detectores precisam ser melhorados ou eliminados.

Quando os verdadeiros positivos são suspeitos, um analista de segurança cibernética às vezes é obrigado a escalar o alerta para um nível mais alto para investigação. O investigador avançará com a investigação, a fim de confirmar o incidente e identificar qualquer dano potencial que possa ter sido causado. Essas informações serão usadas por mais funcionários de segurança sênior que trabalharão para isolar os danos, solucionar vulnerabilidades, mitigar a ameaça e lidar com os requisitos de relatórios.

Um analista de segurança cibernética também pode ser responsável por informar o pessoal de segurança de que falsos positivos estão ocorrendo na medida em que o tempo do analista de segurança cibernética é seriamente afetado. Esta situação indica que os sistemas de monitoramento de segurança precisam ser ajustados para se tornarem mais eficientes. Alterações legítimas na configuração da rede ou nas regras de detecção recém-baixadas podem resultar em um pico repentino de falsos positivos também.

Falsos negativos podem ser descobertos bem depois de uma exploração ter ocorrido. Isso pode acontecer por meio da análise de segurança retrospectiva (RSA). A RSA pode ocorrer quando regras recém-obtidas ou outras informações sobre ameaças são aplicadas a dados de segurança de rede arquivados. Por esse motivo, é importante monitorar as informações sobre ameaças para conhecer novas vulnerabilidades e explorações e avaliar a probabilidade de que a rede estava vulnerável a elas em algum momento no passado. Além disso, a exploração deve ser avaliada em relação aos danos potenciais que a empresa pode sofrer. Pode determinar-se que a adição de novas técnicas de atenuação é suficiente ou que deve ser realizada uma análise mais pormenorizada.

26.2.3

## Análise Determinística e Análise Probabilística

Técnicas estatísticas podem ser usadas para avaliar o risco de que as explorações serão bem-sucedidas em uma determinada rede. Esse tipo de análise pode ajudar os tomadores de decisão a avaliar melhor o custo de mitigar uma ameaça com os danos que uma exploração poderia causar.

Duas abordagens gerais utilizadas para isso são a análise determinística e probabilística. A análise determinística avalia o risco com base no que é conhecido sobre uma vulnerabilidade. Ele pressupõe que, para que uma exploração seja bem-sucedida, todas as etapas anteriores do processo de exploração também devem ser bem-sucedidas. Este tipo de análise de risco só pode descrever o pior caso. No entanto, muitos atores ameaçadores, embora conscientes do processo para realizar uma exploração, podem não ter conhecimento ou experiência para concluir com sucesso cada passo no caminho para uma exploração bem-sucedida. Isso pode dar ao analista de segurança cibernética a oportunidade de detectar a exploração e impedi-la antes que ela prossiga.

A análise probabilística estima o sucesso potencial de uma exploração, estimando a probabilidade de que, se uma etapa de uma exploração tiver sido concluída com sucesso, a próxima etapa também será bem-sucedida. A análise probabilística é especialmente útil na análise de segurança de rede em tempo real em que inúmeras variáveis estão em jogo e um determinado ator de ameaça pode tomar decisões desconhecidas à medida que uma exploração é perseguida.

A análise probabilística baseia-se em técnicas estatísticas que são projetadas para estimar a probabilidade de que um evento ocorrerá com base na probabilidade de ocorrerem eventos anteriores. Usando esse tipo de análise, os caminhos mais prováveis que uma exploração tomará podem ser estimados e a atenção do pessoal de segurança pode ser focada em prevenir ou detectar a exploração mais provável.

Em uma análise determinística, toda a informação para realizar uma exploração é assumida como sendo conhecida. As características da exploração, como o uso de números de porta específicos, são conhecidas de outras instâncias da exploração ou porque portas padronizadas estão em uso. Na análise probabilística, presume-se que os números de porta que serão utilizados só podem ser previstos com algum grau de confiança. Nessa situação, uma exploração que usa números de porta dinâmicos, por exemplo, não pode ser analisada deterministicamente. Tais explorações foram otimizadas para evitar a detecção por firewalls que usam regras estáticas.

As duas abordagens são resumidas a seguir.

* **Análise Determinística** - Para que uma exploração seja bem-sucedida, todas as etapas anteriores da exploração também devem ser bem-sucedidas. O analista de segurança cibernética conhece as etapas para uma exploração bem-sucedida.
* **Análise Probabilística** - Técnicas estatísticas são usadas para determinar a probabilidade de que uma exploração bem-sucedida ocorrerá com base na probabilidade de que cada etapa da exploração seja bem-sucedida.

26.2.4

## Verifique sua compreensão — Identifique cenários determinísticos e probabilísticos

Clique no campo apropriado abaixo de cada característica para indicar a abordagem de análise que ela descreve.

Presume que, para que uma exploração seja bem-sucedida, todas as etapas anteriores do processo de exploração também devem ser bem-sucedidas. - Determinístico

A análise é útil na análise de segurança de rede em tempo real em que inúmeras variáveis estão em jogo.- Probabilístico

A análise só pode descrever o pior caso – Determinístico

A análise estima a probabilidade de uma exploração ter sido bem sucedida.- Probabilístico

A análise pressupõe que os números de porta que serão usados por uma exploração só podem ser previstos com algum grau de confiança – Probabilístico

A análise pressupõe que todas as informações para realizar uma exploração são conhecidas. – Determinístico

26.2.5

## Verifique sua compreensão - Identifique a classificação de alerta

Parte superior do formulário

1. Que tipo de alerta não teria nenhum incidente relatado e nenhum incidente ocorreu? – verdadeiro negativo
2. Que tipo de alerta ocorreu quando um alerta é recebido, mas nenhum incidente ocorreu? Falso positivo
3. Que tipo de incidente ocorreu quando nada é relatado, mas ocorreu uma exploração? – Falso negativo
4. Que tipo de alerta é quando um alerta é recebido e uma exploração foi verificada? - Positivo real
5. Verdadeiro ou falso? Um evento benigno deve acionar um alerta. - Falso

Parte inferior do formulário

# Resumo de avaliação de alertas

26.3.1

## O que eu aprendi neste módulo?

**Fontes de alertas**

O Security Onion é um pacote de código aberto de ferramentas de Monitoramento de Segurança de Rede (NSM) que é executado em uma distribuição Ubuntu Linux. As ferramentas Security Onion fornecem três funções principais para o analista de segurança cibernética: captura completa de pacotes e tipos de dados, sistemas de detecção de intrusão baseados em rede e em host e ferramentas de analistas de alerta. Alguns componentes do Security Onion são de propriedade e mantidos por corporações, como Cisco e Riverbend Technologies, mas são disponibilizados como código aberto.

Security Onion contém muitos componentes. É um ambiente integrado projetado para simplificar a implantação de uma solução NSM abrangente. Security Onion integra esses vários tipos de dados e registros do Sistema de Detecção de Intrusão (IDS) em uma única plataforma através das seguintes ferramentas: Sguil - serve como ponto de partida na investigação de alertas de segurança. Kibana - Kibana é uma interface de painel interativo para dados do Elasticsearch. Ele permite a consulta de dados do NSM e fornece visualizações flexíveis desses dados. O aplicativo de captura de pacotes Wireshark é integrado ao pacote Security Onion. Zeek é um analisador de tráfego de rede que serve como um monitor de segurança. O Zeek inspeciona todo o tráfego em um segmento de rede e permite uma análise aprofundada desses dados.

Alertas de segurança são mensagens de notificação geradas por ferramentas, sistemas e dispositivos de segurança do NSM. No Security Onion, o Sguil fornece um console que integra alertas de várias fontes em uma fila com carimbo de data/hora. Um analista de segurança cibernética pode trabalhar na fila de segurança investigando, classificando, escalonando ou retirando alertas.

Os alertas geralmente incluem informações de cinco tuplas quando disponíveis, bem como carimbos de data/hora e informações que identificam qual dispositivo ou sistema gerou o alerta. Dependendo da tecnologia de segurança, os alertas podem ser gerados com base em regras, assinaturas, anomalias ou comportamentos. Os alertas podem vir de várias fontes, como NIDS, gerenciamento e monitoramento de ativos, transações HTTP, DNS e TCP e mensagens do Syslog.

O Snort é um Sistema de Detecção de Intrusões de Rede (NIDS). É uma fonte importante dos dados de alerta indexados na ferramenta de análise Sguil. Ele usa regras para identificar tráfego potencialmente malicioso. As regras de Snort consistem em duas seções: o cabeçalho da regra e as opções da regra. O cabeçalho da regra contém a ação, o protocolo, os endereços IP de origem e destino e as máscaras de rede e as informações da porta de origem e destino. A seção Opções de regra contém mensagens de alerta e informações sobre quais partes do pacote devem ser inspecionadas para determinar se a ação da regra deve ser executada. A estrutura da seção de opções da regra é variável.

Visão geral da avaliação de alerta

O cenário de ameaças está mudando constantemente à medida que novas vulnerabilidades são descobertas e novas ameaças evoluem. À medida que as necessidades do usuário e organizacional mudam, a superfície do ataque também. Os atores de ameaças aprenderam a variar rapidamente os recursos de suas explorações para evitar a detecção. As regras de detecção devem ser excessivamente conservadoras. É melhor ter alertas que às vezes são gerados por tráfego inocente, do que ter regras que perdem tráfego malicioso. Por esse motivo, é necessário que analistas qualificados de segurança cibernética investiguem alertas para determinar se uma exploração realmente ocorreu.

Os incidentes de segurança são classificados usando um esquema emprestado de diagnósticos médicos. Este esquema de classificação é usado para orientar ações e avaliar procedimentos de diagnóstico. A preocupação é que um diagnóstico pode ser preciso, ou verdadeiro, ou impreciso, ou falso. Os alertas podem ser classificados como Verdadeiro Positivo (O alerta foi verificado como um incidente de segurança real) ou Falso Positivo (O alerta não indica um incidente de segurança real). Uma situação alternativa é que um alerta não foi gerado. A ausência de um alerta pode ser classificada como: Verdadeiro Negativo (Nenhum incidente de segurança ocorreu. A atividade é benigna.) e False Negativo (Ocorreu um incidente não detectado). Verdadeiro Positivos e Verdadeiros Negativos são desejáveis. Falsos Positivos não são desejáveis, mas inevitáveis, e os Falsos Negativos são perigosos.

Técnicas estatísticas podem ser usadas para avaliar o risco de que as explorações serão bem-sucedidas em uma determinada rede. Esse tipo de análise pode ajudar os tomadores de decisão a avaliar melhor o custo de mitigar uma ameaça versus o dano que uma exploração pode causar. Duas abordagens gerais que são usadas para fazer isso são a análise determinística e probabilística. A análise determinística avalia o risco com base no que é conhecido sobre uma vulnerabilidade. Ele pressupõe que, para que uma exploração seja bem-sucedida, todas as etapas anteriores do processo de exploração também devem ser bem-sucedidas. Este tipo de análise de risco só pode descrever o pior caso. A análise probabilística estima o sucesso potencial de uma exploração, estimando a probabilidade de que, se uma etapa de uma exploração tiver sido concluída com sucesso, a próxima etapa também será bem-sucedida. A análise probabilística é especialmente útil na análise de segurança de rede em tempo real em que inúmeras variáveis estão em jogo e um determinado ator de ameaça pode tomar decisões desconhecidas à medida que uma exploração é perseguida.

26.3.2

Módulo 26: Avaliação de Alertas Questionário

Qual classificação é usada para um alerta que identifica corretamente a ocorrência de uma exploração? – Positivo real; Tópico 26.2.0 - Um verdadeiro positivo ocorre quando uma assinatura IDS e IPS é disparada corretamente e um alarme é gerado quando o tráfego ofensivo é detectado.

Que tipo de análise depende de condições predefinidas e pode analisar aplicativos que usam apenas portas fixas conhecidas? – Determinístico ; Tópico 26.2.0 - A análise determinística usa condições predefinidas para analisar aplicativos que estejam em conformidade com padrões de especificação, como a realização de uma análise baseada em porta.

Qual ferramenta está incluída no Security Onion que é usada pelo Snort para baixar automaticamente novas regras? – PulledPork; Tópico 26.1.0 - PulledPork é um utilitário de gerenciamento de regras incluído com Security Onion para baixar automaticamente regras para o Snort.

Qual ferramenta incluída no Security Onion é uma interface de painel interativa para os dados do Elasticsearch? – Kibana; Tópico 26.1.0 - Kibana é uma interface de painel interativo para dados do Elasticsearch. Ele permite a consulta de dados do NSM e fornece visualizações flexíveis desses dados. Ele fornece recursos de análise de dados de exploração de dados e aprendizado de máquina.

Que tipo de análise depende de diferentes métodos para estabelecer a probabilidade de um evento de segurança ter ocorrido ou acontecer? – Probabilístico; Tópico 26.2.0 - Métodos probabilísticos usam ferramentas poderosas para criar uma resposta probabilística como resultado da análise de aplicações.

Qual ferramenta NIDS usa uma abordagem baseada em assinaturas e multithreading nativo para detecção de alertas? – Suricata ; Tópico 26.1.0 - Suricata é uma ferramenta NIDS que usa uma abordagem baseada em assinaturas. Ele também usa multithreading nativo, que permite a distribuição do processamento de fluxo de pacotes em vários núcleos de processador.

Qual é a ferramenta de detecção de intrusões baseada em host integrada ao Security Onion? – OSSEC; Tópico 26.1.0 - Integrado ao Security Onion, o OSSEC é um sistema de detecção de intrusão baseado em host (HIDS) que pode realizar monitoramento de integridade de arquivos, monitoramento de log local, monitoramento de processos do sistema e detecção de rootkit.

Quais são as três ferramentas de análise integradas ao Security Onion? (Escolha três.) – Sguil, Wireshark, Kibana; Tópico 26.1.0 - De acordo com a arquitetura do Security Onion, as ferramentas de análise são Sguil, Kibana e Wireshark.

Qual função é fornecida pelo Snort como parte do Security Onion? – Para gerar alertas de intrusão de rede através de uso de regras e assinaturas; Tópico 26.1.0 - Snort é um NIDS integrado em Security Onion. É uma fonte importante dos dados de alerta indexados na ferramenta de análise Sguil. O Snort usa regras e assinaturas para gerar alertas.

Qual ferramenta é um sistema integrado de detecção de intrusões baseado em host Security Onion? – Wazuh; Tópico 26.1.0 - Wazuh é um HIDS que substituirá OSSEC em Security Onion. É uma solução completa que fornece um amplo espectro de mecanismos de proteção de terminais, incluindo análise de arquivos de log do host, monitoramento de integridade de arquivos, detecção de vulnerabilidades, avaliação de configuração e resposta a incidentes.

Qual ferramenta um analista usaria para iniciar uma investigação de fluxo de trabalho? – Sguil; Tópico 26.1.0 - O Sguil é um aplicativo baseado em GUI usado por analistas de segurança para analisar eventos de segurança de rede.

Qual classificação de alerta indica que as explorações não estão sendo detectadas pelos sistemas de segurança instalados? – Falso negativo; Tópico 26.2.0 - Uma classificação falsa negativa indica que um sistema de segurança não detectou uma exploração real.

# Introdução

27.0.1

## Por que devo cursar este módulo?

Existem muitos tipos diferentes de dados que são usados no monitoramento de segurança de rede. Ferramentas especializadas são necessárias para processar, pesquisar e investigar esses dados. Neste módulo, você aprenderá sobre os dados de segurança de rede e algumas das ferramentas que são usadas para investigá-los.

27.0.2

## O que vou aprender neste módulo?

**Título do Módulo:**z Segurança de rede de dados

**Objetivo do Módulo:** Interprete os dados para determinar a origem de um alerta.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Uma plataforma de dados comum | Explicar como os dados são preparados para uso no sistema de monitoramento de segurança de rede (NSM). |
| Investigando dados de rede | Usar as ferramentas de Security Onion para investigar eventos de segurança de rede. |
| Aprimorando o trabalho do analista de segurança cibernética | Descrever as ferramentas de monitoramento de rede que melhoram o gerenciamento do fluxo de trabalho. |

[26.3](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[Resumo de avaliação de alertas](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[27.1](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# Uma plataforma de dados comum

27.1.1

## ELK

Uma rede típica tem uma infinidade de logs diferentes para manter o controle e a maioria desses logs está em formatos diferentes. Com enormes quantidades de dados diferentes, como é possível obter uma visão geral das operações de rede e, ao mesmo tempo, ter uma sensação de anomalias sutis ou alterações na rede?

O Elastic Stack tenta resolver esse problema fornecendo uma única visualização de interface em uma rede heterogênea. O Elastic Stack consiste em Elasticsearch, Logstash e Kibana (ELK). É uma estrutura modular e altamente escalável para ingestão, análise, armazenamento e visualização de dados. O Elasticsearch é uma plataforma de núcleo aberto (código aberto nos componentes principais) para pesquisar e analisar os dados de uma organização em tempo quase real. Ele pode ser usado em muitos contextos diferentes, mas ganhou popularidade na segurança de rede como uma ferramenta SIEM. Security Onion inclui ELK e outros componentes do Elastic, incluindo:

* **Beats** — Esta é uma série de plugins de software que enviam diferentes tipos de dados para os armazenamentos de dados do Elasticsearch.
* **ElastAlert** — Isso fornece consultas e alertas de segurança com base em critérios definidos pelo usuário e outras informações de dados no Elasticsearch. Notificações de alerta podem ser enviadas para um console ou e-mail e outros sistemas de notificação, como a plataforma de resposta a incidentes de segurança do Hive.
* **Curador** — Isso fornece ações para gerenciar índices de dados do Elasticsearch.

O Elasticsearch, que é o componente do mecanismo de pesquisa, usa serviços Web RESTful e APIs, um cluster de computação distribuído com vários nós de servidor e um banco de dados NoSQL distribuído composto de documentos JSON. Funcionalidades adicionais podem ser adicionadas por meio de extensões personalizadas. A empresa Elasticsearch oferece uma extensão comercial chamada X-Pack que adiciona segurança, alerta, monitoramento, relatórios e gráficos. A empresa também oferece um complemento de aprendizado de máquina, bem como seu próprio produto Elastic SIEM.

O Logstash permite a coleta e a normalização de dados de rede em índices de dados que podem ser pesquisados com eficiência pelo Elasticsearch. Os módulos Logstash e Beats são usados para ingerir dados no cluster do Elasticsearch.

Kibana fornece uma interface gráfica para os dados que são compilados pelo Elasticsearch. Ele permite a visualização de dados de rede e fornece ferramentas e atalhos para consultar esses dados, a fim de isolar possíveis violações de segurança.

Os principais componentes de código aberto do Elastic Stack são Logstash, Beats, Elasticsearch e Kibana, conforme mostrado na figura.

A figura mostra os componentes principais do Elastic Stack: Kibana, que é usado para acessar, visualizar e investigar dados; Elasticsearch que é usado para armazenar, indexar e analisar dados, e Logstash e Beats que é usado para adquirir ou ingerir dados de rede.

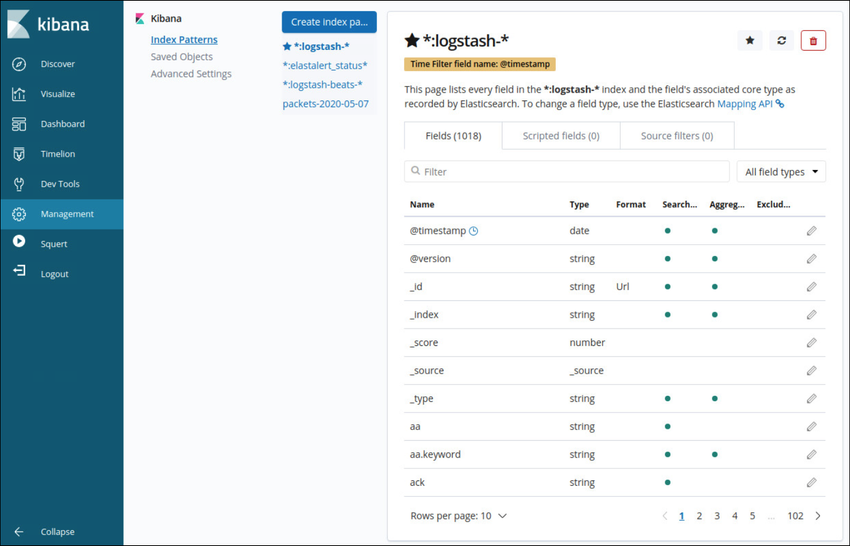
### Componentes do Elastic Stack Core

Acessar, visualizar, investigar dadosArmazenar, Índice, Analisar DadosAdquirir dados de

**Lostash**

Logstash é um sistema de extração, transformação e carga com a capacidade de receber várias fontes de dados de log e transformar ou analisar os dados através de tradução, classificação, agregação, divisão e validação. Depois de transformar os dados, os dados são carregados no banco de dados Elasticsearch no formato de arquivo apropriado. A figura mostra alguns dos campos que estão disponíveis no Logstash, como mostrado na interface Kibana Management.

### Quadro de gerenciamento Kibana mostrando detalhes do índice do Logstash



**Beats**

Os agentes Beats são clientes de software de código aberto usados para enviar dados operacionais diretamente para o Elasticsearch ou através do Logstash. Elastic, bem como a comunidade de código aberto, desenvolvem ativamente agentes Beats, portanto, há uma grande variedade de agentes Beats para enviar dados para o Elasticsearch em tempo quase real. Alguns dos agentes Beats fornecidos pelo Elastic são Auditbeat para dados de auditoria, Metricbeat para dados métricos, Heartbeat para disponibilidade, Packetbeat para tráfego de rede, Journalbeat para diários Systemd e Winlogbeat para logs de eventos do Windows. Algumas Beats de origem comunitária são Amazonbeat, Apachebeat, Dockbeat, Nginxbeat e Mqttbeat, para citar alguns.

**Elasticsearch**

Elasticsearch é um motor de busca empresarial de plataforma cruzada escrito em Java. Os componentes principais são de código aberto com addons comerciais chamados X-packs que dão funcionalidade adicional. O Elasticsearch suporta pesquisa quase em tempo real usando APIs REST simples para criar ou atualizar documentos JSON (JavaScript Object Notation) usando solicitações HTTP. Pesquisas podem ser feitas usando qualquer programa capaz de fazer solicitações HTTP, como um navegador web, Postman, cURL, etc Essas APIs também podem ser acessadas por Python ou outros scripts de linguagem de programação para operações automatizadas.

A estrutura de dados do Elasticsearch é chamada de índice **invertido**, que é projetado para permitir pesquisas de texto completo muito rápidas. Um índice é como um banco de dados, é um namespace para uma coleção de documentos que estão relacionados uns aos outros. Um índice pode ser particionado ou mapeado em diferentes tipos. Se você comparar um índice do Elasticsearch com um banco de dados relacional tradicional, o **índice** será como o banco de dados, os **tipos** serão como as tabelas e os **documentos** serão como as colunas e linhas, conforme mostrado na tabela.

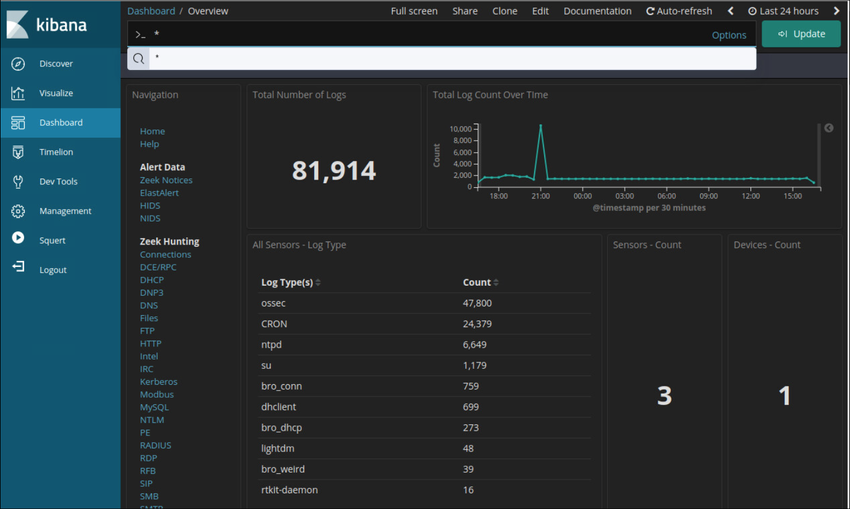
|  |  |  |  |
| --- | --- | --- | --- |
| Componente MySQL: | banco de dados | tabelas | colunas/linhas |
| Componente Elasticsearch: | **Indice** | **tipos** | **documentos** |

O Elasticsearch armazena dados em documentos formatados em JSON. Um documento JSON é organizado em hierarquias de pares chave/valor, com uma **chave** sendo um nome e o **valor** correspondente sendo uma string, número, booleano, data, matriz ou outro tipo de dados.

**Kibana**

Kibana fornece uma interface gráfica de usuário fácil de usar para gerenciar o Elasticsearch. Usando um navegador da Web, um analista pode usar a interface Kibana para pesquisar e visualizar índices. A guia de gerenciamento permite que você crie e gerencie índices e seus tipos e formatos. A guia descoberta é uma maneira rápida e poderosa de visualizar seus dados e pesquisá-los usando as ferramentas de pesquisa. A guia Visualize permite criar visualizações personalizadas, como gráficos de barras, gráficos de linhas, gráficos de pizza, mapas de calor e muito mais. As visualizações criadas podem ser organizadas em painéis personalizados para monitorar e analisar seus dados. Um painel Kibana é mostrado na figura.

### Um painel Kibana



27.1.2

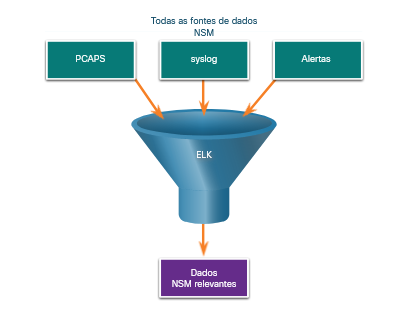
## Redução de dados

A quantidade de tráfego de rede que é coletada por capturas de pacotes e o número de entradas e alertas de arquivos de log gerados por dispositivos de rede e segurança podem ser enormes. Mesmo com os avanços recentes em Big Data, o processamento, armazenamento, acesso e arquivamento de dados relacionados ao NSM é uma tarefa assustadora. Por esse motivo, é importante identificar os dados de rede que devem ser coletados. Nem todas as entradas de arquivo de log, pacotes e alertas precisam ser coletadas. Ao limitar o volume de dados, ferramentas como Elasticsearch serão muito mais úteis, como mostrado na figura.

Algum tráfego de rede tem pouco valor para o NSM. Dados criptografados, como tráfego IPsec ou SSL, são praticamente ilegíveis. Algum tráfego, como o gerado por protocolos de roteamento ou protocolo de árvore de abrangência, é de rotina e pode ser excluído. Outros protocolos de broadcast e multicast geralmente podem ser eliminados das capturas de pacotes, assim como o tráfego de outros protocolos que geram muito tráfego de rotina.

Além disso, os alertas gerados por um HIDS, como auditoria de segurança do Windows ou OSSEC, devem ser avaliados quanto à relevância. Alguns são informativos ou de baixo impacto potencial na segurança. Essas mensagens podem ser filtradas a partir de dados do NSM. Da mesma forma, o syslog pode armazenar mensagens de severidade muito baixa que poderiam ser ignoradas para diminuir a quantidade de dados NSM a serem tratados.

A figura é uma representação simplificada de como dados como PCAPS, logs e alertas são alimentados no Logstash ou na pilha Elastic e analisados em dados relevantes de monitoramento de segurança de rede.



Todas as fontes de dados NSM PCAPSsyslogAlertasELKDados  
NSM relevantes

27.1.3

## Normalização de dados

Normalização de dados é o processo de combinar dados de uma série de fontes de dados em um formato comum. O Logstash fornece uma série de transformações que processam dados de segurança e os transformam antes de adicioná-los ao Elasticsearch. Plugins adicionais podem ser criados para atender às necessidades da organização.

Um esquema comum especificará os nomes e formatos para os campos de dados necessários. A formatação dos campos de dados pode variar muito entre as fontes. No entanto, para que a pesquisa seja eficaz, os campos de dados devem ser consistentes. Por exemplo, endereços IPv6, endereços MAC e informações de data e hora podem ser representados em formatos variados. Da mesma forma, máscaras de sub-rede, registros DNS e assim por diante podem variar em formato entre fontes de dados. As transformações Logstash aceitam os dados em seu formato nativo e tornam os elementos dos dados consistentes em todas as fontes. Por exemplo, um único formato será usado para endereços e carimbos de data/hora para dados de todas as fontes.

**Formatos de Endereço IPv6**

* 2001:db8:acad:1111:2222::33
* 2001:DB8:ACAD:1111:2222::33
* 2001:DB8:ACAD:1111:2222:0:0:33
* 2001:DB8:ACAD:1111:2222:0000:0000:0033

**Formatos MAC**

* A7:03:DB:7C:91:AA
* A7-03-DB-7C-91-AA
* A70.3DB.7C9.1AA

**Formatos de Data**

* Monday, July 24, 2017 7:39:35pm
* Mon, 24 Jul 2017 19:39:35 +0000
* 2017-07-24T19:39:35+00:00
* 1500925254

A normalização dos dados é necessária para simplificar a pesquisa de eventos correlacionados. Se existirem valores formatados de forma diferente nos dados do NSM para endereços IPv6, por exemplo, um termo de consulta separado precisaria ser criado para cada variação para que os eventos correlacionados sejam retornados pela consulta.

27.1.4

## Arquivamento de dados

Todos adorariam a segurança de coletar e salvar tudo, só por precaução. No entanto, reter dados do NSM indefinidamente não é viável devido a problemas de armazenamento e acesso. Note-se que o período de retenção para certos tipos de informações de segurança de rede pode ser especificado por estruturas de conformidade. Por exemplo, o Payment Card Industry Security Standards Council (PCI DSS) exige que uma trilha de auditoria das atividades do usuário relacionadas a informações protegidas seja mantida por um ano.

Security Onion tem diferentes períodos de retenção de dados para diferentes tipos de dados NSM. Para pcaps e logs brutos de Bro, um valor atribuído no **securityonion.conf** arquivo controla a porcentagem de espaço em disco que pode ser usada por arquivos de log. Por padrão, esse valor é definido como 90%. Para o Elasticsearch, a retenção de índices de dados é controlada pelo curador do Elasticsearch. O curador é executado em um contêiner do Docker e executa a cada minuto de acordo com os **cron** trabalhos. O curador registra sua atividade no curator.log. O curador usa como padrão os índices de fechamento com mais de 30 dias. Para modificar isso, altere CURATOR\ \_CLOSE\ \_DAYS em /etc/nsm/securityonion.conf. À medida que um disco atinge a capacidade, o Curator exclui índices antigos para impedir que o disco seja preenchido. Para alterar o limite, modifique LOG\ \_SIZE\ \_LIMIT em /etc/nsm/securityonion.conf.

Os dados de alerta Sguil são mantidos por 30 dias por padrão. Esse valor é definido no **securityonion.conf** arquivo.

Security Onion é conhecido por exigir muito armazenamento e RAM para executar corretamente. Dependendo do tamanho da rede, vários terabytes de armazenamento podem ser necessários. É claro que os dados Security Onion sempre podem ser arquivados em armazenamento externo por um sistema de arquivamento de dados, dependendo das necessidades e capacidades da organização.

**Observação**: Os locais de armazenamento para os diferentes tipos de dados Security Onion variam de acordo com a implementação do Security Onion.

27.1.5

## Laboratório - Converta dados em um formato universal

As entradas de log são geradas por dispositivos de rede, sistemas operacionais, aplicativos e vários tipos de dispositivos programáveis. Um arquivo contendo um fluxo sequenciado por tempo de entradas de log é chamado de arquivo de log. Por natureza, os arquivos de log registram eventos relevantes para a origem. A sintaxe e o formato dos dados dentro das mensagens de log geralmente são definidos pelo desenvolvedor do aplicativo. Portanto, a terminologia usada nas entradas de log geralmente varia de origem para origem. Por exemplo, dependendo da origem, os termos login, logon, evento de autenticação e conexão de usuário podem aparecer em entradas de log para descrever uma autenticação de usuário bem-sucedida em um servidor.

É desejável ter uma terminologia consistente e uniforme em logs gerados por diferentes fontes. Isto é especialmente verdadeiro quando todos os ficheiros de registo estão a ser recolhidos por um ponto centralizado. O termo normalização refere-se ao processo de conversão de partes de uma mensagem, neste caso, uma entrada de log, para um formato comum.

Neste laboratório, você usará ferramentas de linha de comando para normalizar manualmente as entradas de log. Na Parte 2, o campo de carimbo de data/hora deve ser normalizado. Na Parte 3, o campo IPv6 requer normalização.

[27.0](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[Introdução](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[27.2](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# Investigando dados de rede

27.2.1

## Trabalhando em Sguil

O principal dever de um analista de segurança cibernética é a verificação de alertas de segurança. Dependendo da organização, as ferramentas usadas para fazer isso variam. Por exemplo, um sistema de emissão de bilhetes pode ser usado para gerenciar a atribuição de tarefas e a documentação. Em Security Onion, o primeiro lugar que um analista de segurança cibernética irá verificar alertas é o Sguil.

O Sguil correlaciona automaticamente alertas semelhantes em uma única linha e fornece uma maneira de exibir eventos correlacionados representados por essa linha. Para ter uma noção do que está acontecendo na rede, pode ser útil classificar na coluna **CNT** para exibir os alertas com a maior frequência.

Clicar com o botão direito do mouse no valor **CNT** e selecionar **Exibir Eventos Correlacionados** abre uma guia que exibe todos os eventos relacionados pelo Sguil. Isso pode ajudar o analista de segurança cibernética a entender o período durante o qual os eventos correlacionados foram recebidos pelo Sguil. Observe que cada evento recebe um ID de evento exclusivo. Somente o primeiro ID de evento na série de eventos correlacionados é exibido na guia Eventos em Tempo Real. A figura mostra os alertas do Sguil classificados no **CNT** com o menu **Exibir eventos** correlacionados aberto.

### Alertas Sguil Ordenados na CNT



27.2.2

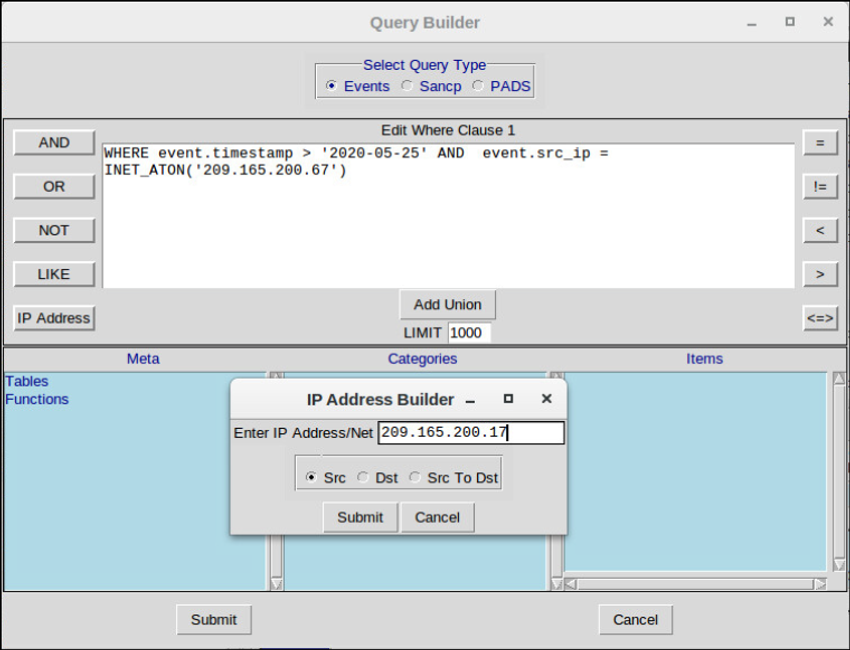
## Consultas Sguil

As consultas podem ser construídas no Sguil usando o Construtor de Consultas. Ele simplifica a construção de consultas até certo ponto, mas o analista de segurança cibernética deve conhecer os nomes de campo e alguns problemas com valores de campo. Por exemplo, o Sguil armazena endereços IP em uma representação de inteiro. Para consultar um endereço IP na notação decimal pontilhada, o valor do endereço IP deve ser colocado dentro da **INET\_ATON()** função. Construtor de consultas é aberto a partir do menu **Consulta** Sguil. Selecione **Tabela de Eventos de Consulta** para pesquisar eventos ativos.

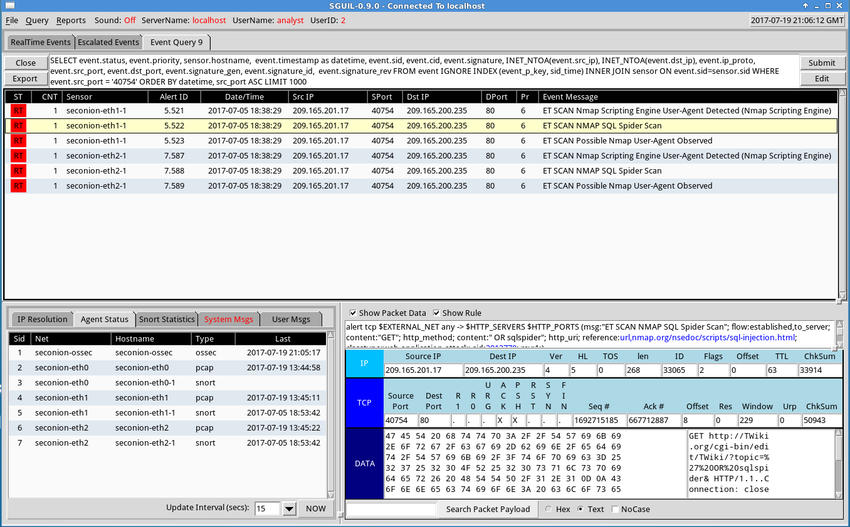
A tabela mostra os nomes de alguns dos campos da tabela de eventos que podem ser consultados diretamente. Selecionar **Mostrar Tabelas** de Banco de Dados **no menu** Consulta exibe uma referência aos nomes e tipos de campo para cada uma das tabelas que podem ser consultadas. Ao realizar pesquisas de tabela de eventos, use o padrão **event.fieldName = value**.

|  |  |  |
| --- | --- | --- |
| **Nome do Campo** | **Tipo** | **Descrição** |
| O Sid | int | o ID exclusivo do sensor |
| CID | int | o número de evento único do sensor |
| assinatura | varchar | o nome legível pelo homem do evento (por exemplo, “fonte de visualização WEB-IIS via cabeçalho de tradução”) |
| carimbo de hora | datetime | a data e a hora em que o evento ocorreu no sensor |
| status | int | a classificação Sguil atribuída a este evento. Eventos não classificados são prioridade 0. |
| src\_ip | int | o IP de origem para o evento. Use a função INET\_ATON () para encobrir o endereço para a representação inteira do banco de dados. |
| dst\_ip | int | o IP de destino para o evento |
| src\_port | int | a porta de origem do pacote que acionou o evento |
| dst\_port | int | a porta de destino do pacote que acionou o evento |
| ip\_proto | ando | Tipo de protocolo IP do pacote. (6 = TCP, 17 = UDP, 1 = ICMP, outros são possíveis) |

A figura mostra um carimbo de data/hora simples e uma consulta de endereço IP feita na janela Construtor de consultas. Observe o uso da **INET\_ATON()** função para simplificar a inserção de um endereço IP.



No exemplo abaixo, o analista de segurança cibernética está investigando uma porta de origem 40754 associada a um alerta de ameaças emergentes. No final da consulta, a **WHERE event.src\_port = ‘40754’** parte foi criada pelo usuário no Query Builder. O restante da consulta é fornecido automaticamente pelo Sguil e diz respeito a como os dados associados aos eventos devem ser recuperados, exibidos e apresentados.

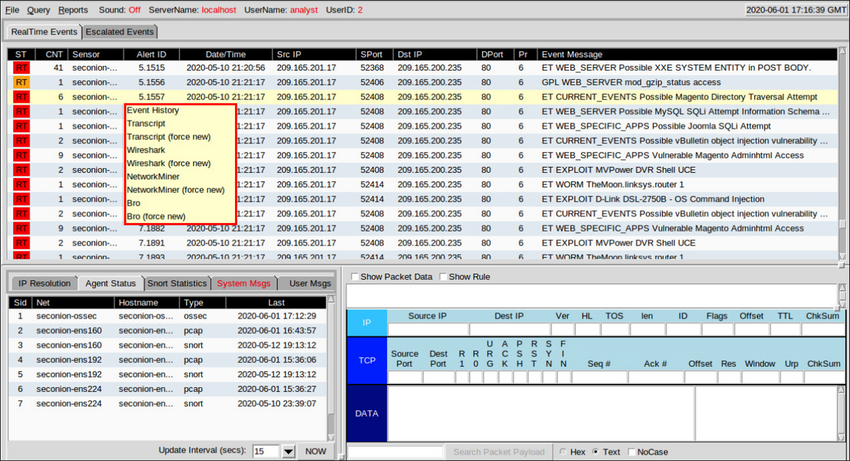


27.2.3

## Pivotante a partir de Sguil

A Sguil oferece a capacidade de o analista de segurança cibernética girar para outras fontes de informação e ferramentas. Os arquivos de log estão disponíveis no Elasticsearch. Capturas de pacotes relevantes podem ser exibidas no Wireshark. Transcrições de sessões TCP e informações de detecção Zeek (Bro) também estão disponíveis. O menu mostrado na figura foi aberto clicando com o botão direito do mouse em um ID de alerta. A seleção deste menu abrirá informações sobre o alerta em outras ferramentas, que fornecem informações ricas e contextualizadas ao analista de segurança cibernética.

### Pivotante a partir de Sguil



Além disso, o Sguil pode fornecer dinâmicas para informações sobre o Sistema de Detecção de Ativos em Tempo Real Passivo (PRADS) e o Security Analyst Network Connection Profiler (SANCP). Essas ferramentas são acessadas clicando com o botão direito do mouse em um endereço IP de um evento e selecionando os menus Consulta Rápida ou Consulta Avançada.

O PRADS reúne dados de criação de perfil de rede, incluindo informações sobre o comportamento dos ativos na rede. PRADS é uma fonte de eventos, como Snort e OSSEC. Ele também pode ser consultado através do Sguil quando um alerta indica que um host interno pode ter sido comprometido. A execução de uma consulta PRADS fora do Sguil pode fornecer informações sobre os serviços, aplicativos e cargas úteis que podem ser relevantes para o alerta. Além disso, o PRADS detecta quando novos ativos aparecem na rede.

**Nota**: A interface Sguil refere-se a PADS em vez de PRADS. PADS foi o antecessor do PRADS. PRADS é a ferramenta que é realmente usada em Security Onion. O PRADS também é usado para preencher tabelas SANCP. Em Security Onion, as funcionalidades do SANCP foram substituídas pelo PRADS, no entanto, o termo SANCP ainda é usado na interface Sguil. O PRADS coleta os dados e um agente SANCP registra os dados em uma tabela de dados SANCP.

As funcionalidades do SANCP dizem respeito à coleta e registro de informações estatísticas sobre tráfego e comportamento da rede. O SANCP fornece um meio de verificar se as conexões de rede são válidas. Isso é feito através da aplicação de regras que indicam qual tráfego deve ser registrado e as informações com as quais o tráfego deve ser marcado.

27.2.4

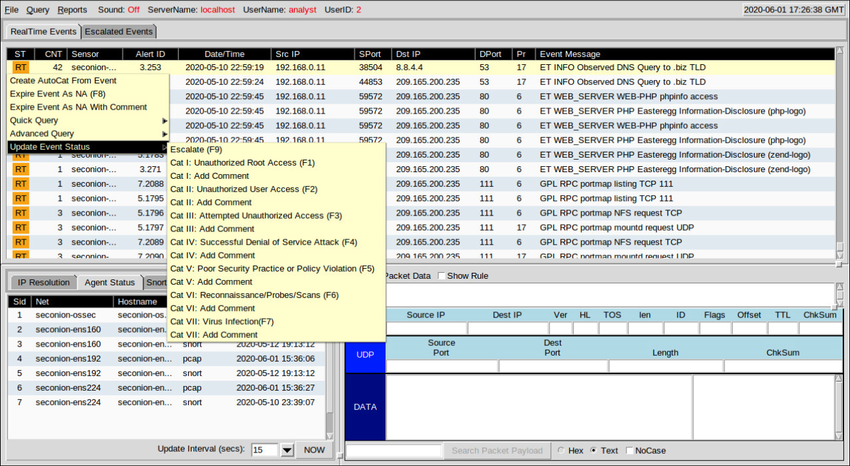
## Manipulação de eventos em Sguil

Finalmente, Sguil não é apenas um console que facilita a investigação de alertas. É também uma ferramenta para endereçar ou classificar alertas. Três tarefas podem ser concluídas no Sguil para gerenciar alertas. Primeiro, os alertas que foram encontrados como falsos positivos podem ser expirados. Isso pode ser feito usando o botão direito do mouse na coluna ST para o evento e usando o menu ou pressionando a tecla F8. Um evento expirado desaparece da fila. Em segundo lugar, se o analista de segurança cibernética não tiver certeza de como lidar com um evento, ele pode ser escalado pressionando a tecla F9. O alerta será movido para a guia Eventos Escalados do Sguil. Finalmente, um evento pode ser categorizado. A categorização é para eventos que foram identificados como verdadeiros positivos.

Sguil inclui sete categorias pré-construídas que podem ser atribuídas usando um menu, que é mostrado na figura, ou pressionando a tecla de função correspondente. Por exemplo, um evento seria categorizado como Cat I pressionando a tecla F1. Além disso, podem ser criados critérios que categorizam automaticamente um evento. Presume-se que eventos categorizados tenham sido tratados pelo analista de segurança cibernética. Quando um evento é categorizado, ele é removido da lista de Eventos em **Tempo Real**. O evento permanece no banco de dados no entanto, e ele pode ser acessado por consultas que são emitidas por categoria.

Este curso abrange Sguil em um nível básico. Existem inúmeros recursos na internet para aprender mais.

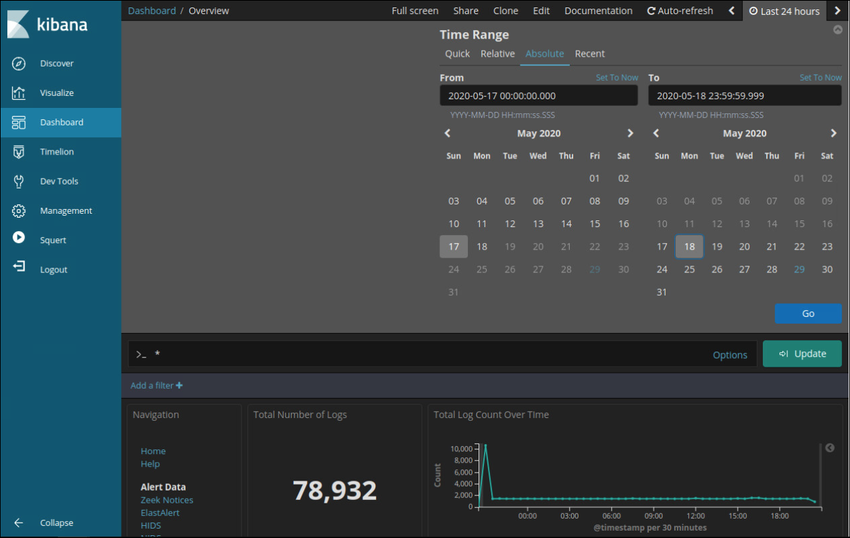
### Manipulação de eventos em Sguil



27.2.5

## Trabalhando no ELK

Logstash e Beats são usados para ingestão de dados no Elastic Stack. Eles fornecem acesso a um grande número de entradas de arquivo de log. Como o número de logs que podem ser exibidos é tão grande, Kibana, que é a interface visual nos logs, é configurado para mostrar as últimas 24 horas por padrão. Você pode ajustar o intervalo de tempo para exibir intervalos de dados mais amplos ou mais antigos.



Para ver registros de arquivos de log por um período diferente, clique na guia Últimas 24 horas no canto superior direito do Kibana. A partir daí, defina o Intervalo de Tempo selecionando a guia Rápido para intervalos de tempo predefinidos. Você também pode inserir as datas e horas manualmente usando a guia Absoluto. A figura mostra um intervalo de tempo absoluto de 17 de maio a 18 de maio de 2020. Os logs são ingeridos no Elasticsearch em índices ou bancos de dados separados com base em um intervalo de tempo configurado.

A melhor maneira de monitorar seus dados no Elasticsearch é criar painéis visuais personalizados que rastreiam os dados que você está interessado em usar. Uma variedade de gráficos visuais, incluindo gráficos de barras, gráficos de pizza, métricas de contagem, mapas de calor, mapas geográficos, listas de números superiores estão disponíveis. No Kibana, visualizações e gráficos podem ser pesquisados e filtrados com métricas específicas e buckets de dados.

27.2.6

## Consultas no ELK

O Elasticsearch é construído sobre o Apache Lucene, uma biblioteca de software de mecanismo de pesquisa de código aberto que possui recursos completos de indexação e pesquisa de texto. O Elasticsearch ingere dados em documentos chamados índices e esses documentos são mapeados para vários tipos de dados usando padrões de índice. Os padrões de índice criam uma estrutura de dados de campos e valores formatados em JSON. Os tipos de dados nos campos podem estar nos seguintes formatos:

* Core Datatypes: Texto (Strings), Numérico, Data, Booleano, Binário e Intervalo
* Complex Datatypes: Objeto (JSON), aninhado (matrizes de objetos JSON)
* Geo Datatypes: Geo-ponto (latitude/longitude), Geo-forma (polígonos)
* Specialized Datatypes: Endereços IP, contagem de tokens, histograma, etc.)

Usando bibliotecas de software Lucene, Elasticsearch tem sua própria linguagem de consulta baseada em JSON chamado Query DSL (Domain Specific Language). Consulta DSL apresenta consultas de folha, consultas compostas e consultas caras. Consultas de folha procuram um valor específico em um campo específico, como consultas de correspondência, termo ou intervalo. Consultas compostas incluem outras consultas de folha ou compostos e são usados para combinar várias consultas de uma forma lógica. Consultas caras são executadas lentamente e incluem correspondência difusa, correspondência regex e correspondência curinga.

**Idioma da consulta**

Junto com JSON, consultas Elasticsearch fazer uso dos seguintes elementos: operadores booleanos, Campos, Intervalos, Curingas, Regex, Pesquisa difusa, Pesquisa de texto.

* **Operadores booleanos** - operadores AND, OR e NOT:
  + “ php” OU “zip” OU “exe” OU “jar” OU “run”
  + “ RST” E “ACK”
* **Campos** - Em pares chave:valor separados por dois pontos, você especifica o campo de chave, dois pontos, um espaço e o valor:
  + dst.ip: “192.168.1.5”
  + dst.port: 80
* **Intervalos** - Você pode pesquisar campos dentro de um intervalo específico usando colchetes (inclusive) ou intervalo de chaves (exclusivo):
  + host: [1 TO 255] — Retorna eventos com idade entre 1 e 255
  + TTL: {100 TO 400} — Retorna eventos com preços entre 101 e 399
  + name: [Admin TO User] — Retorna nomes entre e incluindo Admin e Usuário
* **Curingas** - O\* caractere\ é para vários caracteres curingas e o? caractere para curingas de caractere único:
  + P?ssw?rd — Vai combinar Password, e P@ssw0rd
  + Pas\* — Vai combinar Pass, Passwd, e Password
* **Regex** — Estes são colocados entre barras (/):
  + /d\ [ao] n/ — Combina com dan e don
  + /<.+>/ — Corresponderá a um texto semelhante a uma marca HTML
* **Pesquisa difusa** - A pesquisa difusa usa a distância de Damerau-Levenshtein para corresponder aos termos que são semelhantes na ortografia. Isso é ótimo quando seu conjunto de dados tem palavras ortografadas incorretamente. Use o til (~) para encontrar termos semelhantes:
  + index.php~ - Isso pode retornar resultados como “index.html”, “home.php” e “info.php”.
  + Use o til (~) junto com um número para especificar o tamanho da distância entre as palavras:
  + term~2 - Isso vai combinar, entre outras coisas: "team", "terms", "trem" e "torn"
* **Pesquisa de texto** - Digite o termo ou valor que deseja localizar. Isso pode ser um campo, ou uma string dentro de um campo, etc.

**Execução da Consulta**

O Elasticsearch foi projetado para fazer interface com usuários usando clientes baseados na Web que seguem a estrutura HTTP REST. As consultas podem ser executadas usando os seguintes métodos:

* **URI** - Elasticsearch can execute queries using URI searches:
  + http://localhost:9200/\_search?q=query:ns.example.com
* **cURL** - Elasticsearch can execute queries using cURL from the command line:
  + curl “localhost: 9200/\ \_search?q=query:ns.example.com”
* **JSON** — O Elasticsearch pode executar consultas com uma pesquisa de corpo de solicitação usando um documento JSON que começa com um elemento de consulta e uma consulta formatada usando a linguagem específica de domínio de consulta.
* **Ferramentas de desenvolvimento** — O Elasticsearch pode executar consultas usando o console Dev Tools no Kibana e uma consulta formatada usando o Query Domain Specific Language.

**Observação**: As consultas avançadas do Elasticsearch estão além do escopo deste curso. Nos laboratórios, você receberá as instruções de consulta complexas, se necessário.

27.2.7

## Investigando chamadas de processo ou API

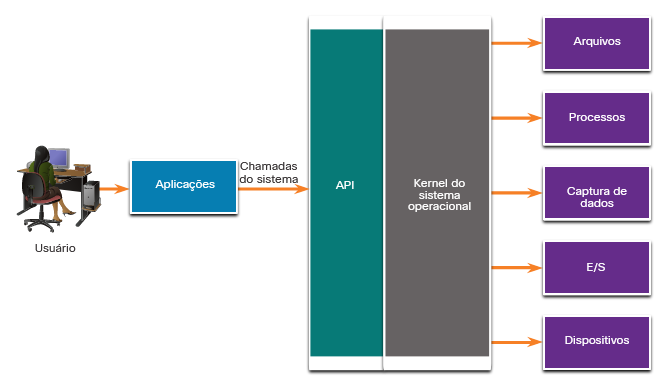
Os aplicativos interagem com um sistema operacional (SO) por meio de chamadas do sistema para a interface de programação de aplicativos (API) do sistema operacional, como mostrado na figura. Essas chamadas de sistema permitem o acesso a muitos aspectos da operação do sistema, tais como:

* Controle de processos de software
* Gerenciamento de Arquivos
* Gerenciamento de dispositivos
* Gerenciamento de informações
* Comunicação

O malware também pode fazer chamadas ao sistema. Se o malware pode enganar um kernel do sistema operacional para permitir que ele faça chamadas de sistema, muitas explorações são possíveis.

O software HIDS rastreia a operação de um sistema operacional host. As regras OSSEC detectam alterações nos parâmetros baseados em host, como a execução de processos de software, alterações nos privilégios do usuário e modificações no registro, entre muitos outros. As regras da OSSEC dispararão um alerta em Sguil. Ao girar para o Kibana no endereço IP do host, você pode escolher o tipo de alerta com base no programa que o criou. A filtragem de índices OSSEC resulta em uma exibição dos eventos OSSEC que ocorreram no host, incluindo indicadores de que o malware pode ter interagido com o kernel do sistema operacional.

A figura mostra como um usuário pode fazer uma chamada de sistema remoto, usando um aplicativo, para acessar a API de um sistema operacional remoto para acessar informações sobre os arquivos, processos, status e configuração da rede, E/S e dispositivos do computador.



APIAplicaçõesArquivosProcessosCaptura de dadosE/SDispositivosKernel do sistema operacionalUsuárioChamadas do sistema

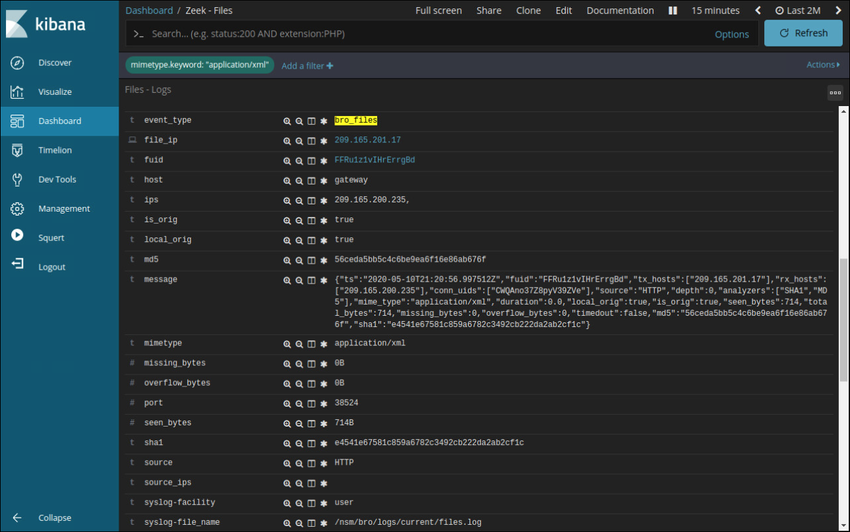
27.2.8

## Investigando Detalhes do Arquivo

No Sguil, se o analista de segurança cibernética suspeitar de um arquivo, o valor de hash pode ser enviado para um site online, como VirusTotal, para determinar se o arquivo é conhecido como malware. O valor de hash pode ser enviado a partir da guia Pesquisar na página VirusTotal.

No Kibana, Zeek Hunting pode ser usado para exibir informações sobre os arquivos que entraram na rede. A partir dos tipos MIME, ou mídia, que estão presentes, os filtros podem ser definidos para exibir informações sobre tipos específicos de arquivos, como **application/xml** ou **application/zip**. A partir daí, detalhes para os arquivos individuais podem ser exibidos, como mostrado na figura. Note que no Kibana, o tipo de evento é mostrado como **bro\_files**, mesmo que o novo nome para Bro seja Zeek.

### Detalhes do arquivo do Zeek como exibido no Kibana



Numerosos detalhes estão disponíveis para os arquivos. Neste exemplo, os hashes MD5 e SHA-1 são mostrados, assim como outros detalhes. As entradas azuis fornecem tabelas dinâmicas para visualizar detalhes das informações fornecidas na tabela no CapMe! ou outras ferramentas.

27.2.9

## Laboratório — Tutorial Expressão

Uma expressão regular (regex) é um padrão de símbolos que descreve dados a serem correspondidos em uma consulta ou outra operação. Expressões regulares são construídas de forma semelhante às expressões aritméticas, usando vários operadores para combinar expressões menores. Existem dois principais padrões de expressão regular, POSIX e Perl.

Neste laboratório, você usará um tutorial on-line para explorar expressões regulares. Você também descreverá as informações que correspondem a expressões regulares dadas.

27.2.10

## Laboratório - Extraia um executável de um PCAP

Olhar para registros é muito importante, mas também é importante entender como as transações de rede acontecem no nível do pacote.

Neste laboratório, você analisará o tráfego em um arquivo pcap capturado anteriormente e extrairá um arquivo executável do tráfego.

27.2.11

## Vídeo - Interpretar dados HTTP e DNS para isolar o agente de ameaças

Assista ao vídeo para ver um passo a passo do laboratório Security Onion Interpret HTTP e DNS Data to Isolate Threat Actor.

27.2.12

## Laboratório - Interprete dados HTTP e DNS para isolar o agente de ameaças

Neste laboratório, você investigará exploits de injeção de SQL e exfiltração de DNS usando as ferramentas Security Onion.

27.2.13

## Vídeo - Isolar host comprometido usando 5 tuplas

Assista ao vídeo para ver um passo a passo do Security Onion Isolate comprometido Host Using 5-Tuple lab.

27.2.14

## Laboratório - Isolar host comprometido usando 5 tuplas

Neste laboratório, você usará as ferramentas Security Onion para investigar uma exploração usando as ferramentas Security Onion.

27.2.15

## Laboratório - Investigar uma exploração de malware

Neste laboratório, você usará Security Onion para investigar um malware mais complexo explorar o usa um kit de exploração para infectar hosts.

27.2.16

## Laboratório - Investigando um Ataque a um Host Windows

Neste laboratório, você irá:

* Investigue um ataque em um host Windows.
* Use Sguil, Kibana e Wireshark na Cebola de Segurança para investigar o ataque.
* Examinar artefatos de exploração.

[27.1](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[Uma plataforma de dados comum](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[27.3](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# Aprimorando o trabalho do analista de segurança cibernética

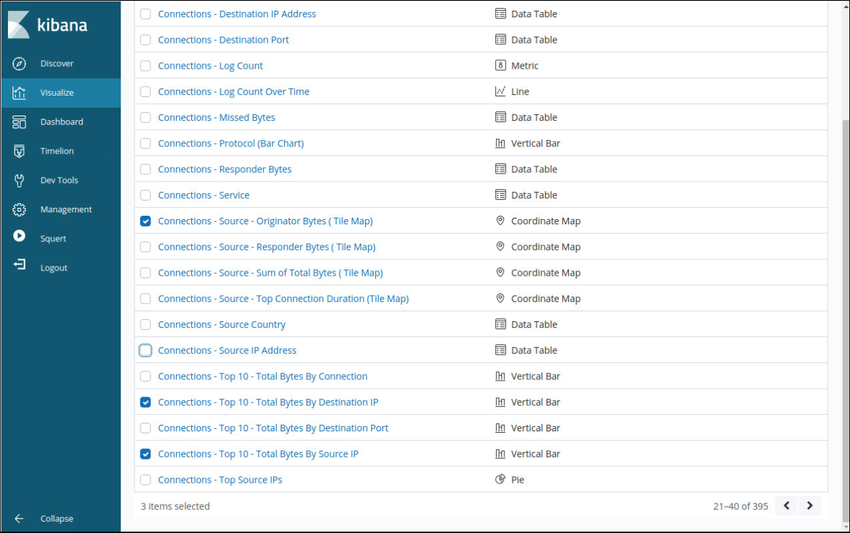
27.3.1

## Painéis e visualizações

Os painéis fornecem uma combinação de dados e visualizações que são projetados para melhorar o acesso e a interpretação de grandes quantidades de informações. Painéis geralmente são interativos. Eles permitem que os analistas de segurança cibernética se concentrem em detalhes e informações específicas clicando em elementos do painel. Por exemplo, clicar em uma barra em um gráfico de barras poderia fornecer um detalhamento das informações para os dados representados por essa barra. Kibana inclui a capacidade de projetar painéis personalizados. Além disso, outras ferramentas incluídas no Security Onion, como o Squert, fornecem uma interface visual para os dados do NSM.

A interface Kibana para selecionar as visualizações que irão compor um painel personalizado são mostradas na figura.

### Selecionando Visualizações para um Painel Kibana personalizado



27.3.2

## Gerenciamento do fluxo de trabalho

Devido à natureza crítica do monitoramento de segurança de rede, é essencial que os fluxos de trabalho sejam gerenciados. Os fluxos de trabalho são a sequência de processos e procedimentos através dos quais as tarefas de trabalho são concluídas. O gerenciamento de fluxos de trabalho SOC aumenta a eficiência da equipe de operações cibernéticas, aumenta a responsabilidade da equipe e garante que todos os alertas potenciais sejam tratados adequadamente. Em grandes organizações de segurança, é concebível que milhares de alertas sejam recebidos diariamente. Cada alerta deve ser sistematicamente atribuído, processado e documentado pela equipe de operações cibernéticas.

A automação de runbook, ou sistemas de gerenciamento de fluxo de trabalho, fornecem as ferramentas necessárias para agilizar e controlar processos em um centro de operações de segurança cibernética. O Sguil fornece gerenciamento básico de fluxo de trabalho. No entanto, não é uma boa escolha para grandes operações com muitos funcionários. Em vez disso, estão disponíveis sistemas de gerenciamento de fluxo de trabalho de terceiros que podem ser personalizados para atender às necessidades das operações de segurança cibernética.

Além disso, consultas automatizadas são úteis para adicionar eficiência ao fluxo de trabalho de operações cibernéticas. Essas consultas, às vezes conhecidas como playbooks ou playbooks, buscam automaticamente incidentes de segurança complexos que podem fugir a outras ferramentas. No Kibana, as pesquisas filtradas podem ser transformadas em visualizações, que podem ser atualizadas e monitoradas dinamicamente para rastrear eventos. A pilha ELK pode adicionar funcionalidade de alerta instalando a extensão X-Pack no Elastic. O X-Pack é uma extensão comercial do Elasticsearch e inclui recursos de segurança, alerta, monitoramento, emissão de relatórios e gráficos. O Elasticsearch fornece várias formas de notificação de alerta e pode notificar analistas de segurança cibernética por e-mail ou outros meios. Além do X-Pack, a Elastic.co também oferece seu próprio produto Elastic SIEM comercial com recursos avançados de monitoramento, alerta e orquestração.

[27.2](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[Investigando dados de rede](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[27.4](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# Trabalho com Resumo de Dados de Segurança de Rede

27.4.1

## O que aprendi neste módulo?

**Uma plataforma de dados comum**

Devido à diversidade de dados de monitoramento de rede, uma plataforma de monitoramento de segurança de rede deve unir os dados para análise. ELK, ou The Elastic Stack, é uma tal plataforma. ELK consiste em Elasticsearch, Logstash e Kibana com Beats, ElastAlert e Curator. Esses componentes permitem a coleta, normalização e análise de dados de monitoramento de rede. O Elasticsearch permite a busca rápida de grandes quantidades de dados. Os módulos Logstash e Beats compilam e normalizam dados de muitas fontes, e Kibana fornece uma interface gráfica de usuário e ferramentas para analisar os dados. Os dados de rede devem ser reduzidos para que apenas os dados relevantes sejam processados pelo sistema NSM. Os dados de rede também devem ser normalizados para converter os mesmos tipos de dados em formatos consistentes. Os dados devem ser arquivados por um período razoável de tempo e esse período pode ser especificado pelas estruturas de conformidade. O Security Onion é configurado para excluir dados automaticamente se o espaço disponível em disco se tornar muito baixo. O curador excluirá os índices Logstash com mais de 30 dias por padrão.

**Investigando dados de rede**

O Sguil fornece um console que permite que um analista de segurança cibernética investigue, verifique e classifique alertas de segurança. O Sguil correlaciona eventos com base em informações como endereços IP de origem e destino e portas de Camada 4, entre outros. Isso desenclutera o console do analista representando eventos relacionados em uma única linha. A coluna CNT indica o número de eventos que foram correlacionados para um alerta. O primeiro alerta da série é mostrado. A série inteira pode ser visualizada no Sguil clicando com o botão direito do mouse no valor CNT e escolhendo Exibir eventos correlacionados. Pivotantes envolvendo a mudança de informações em um aplicativo para diferentes ferramentas especializadas para visualizar detalhes dessas informações. O Sguil fornece maneiras de lidar com alertas escalonando, retirando e classificando.

O Kibana exibe apenas os dados das últimas 24 horas por padrão. Isto é para evitar que a exibição se torne desordenada. Ao investigar dados que ocorreram antes desse período, o intervalo de tempo deve ser definido pelo analista. Painéis personalizados com uma variedade de visualizações podem ser criados. Há várias maneiras de consultar ElasticSearch usando Query DSL (Domain Specific Language). Numerosos operadores, campos, curingas e outros termos podem ser especificados. As consultas podem ser executadas enviando-as diretamente para um URI RESTful ou através de cURL, JSON. ou usando Kibana Dev Tools. Chamadas de processo e API podem ser investigadas trabalhando com alertas OSSEC HIDS. Além disso, os detalhes do arquivo, como tipos de arquivo e hashes, podem ser acessados por meio do Kibana e podem ser enviados para uma fonte externa para ser identificada como benigna ou como malware. Uma dessas fontes é VirusTotal.

**Aprimorando o trabalho do analista de segurança cibernética**

As visualizações do Kibana fornecem insights sobre dados do NSM representando grandes quantidades de formatos de dados que são mais fáceis de interpretar. Alguns painéis fornecem a capacidade de clicar em elementos interativos que fornecerão informações focadas. O gerenciamento de fluxo de trabalho adiciona eficiência ao trabalho da equipe SOC. A automação de runbook, ou sistemas de gerenciamento de fluxo de trabalho, fornecem ferramentas para simplificar e controlar processos SOC. Consultas automatizadas também ajudam a aumentar a eficiência. Essas consultas, conhecidas como playbooks ou playbooks, buscam automaticamente incidentes de segurança complexos que podem evitar outras ferramentas.

27.4.2

## Módulo 27: Trabalho com teste de dados de segurança de rede

Parte superior do formulário

1. Quando o relatório em tempo real de eventos de segurança de várias fontes está sendo recebido, qual função no SIEM fornece captura e processamento de dados em um formato comum? – normalização; Tópico 27.1.0 - O SIEM combina ferramentas SEM e SIM para fornecer algumas funções úteis, uma das quais é a normalização dos dados. Normalização de dados é o processo de mapeamento de mensagens de log de diferentes sistemas em um modelo de dados comum, a fim de analisar eventos de segurança relacionados, mesmo que eles sejam inicialmente registrados em diferentes formatos de origem.
2. Qual é o valor dos hashes de arquivo para investigações de segurança de rede? – Eles podem servir como assinaturas de malware; Tópico 27.2.0 - Confidencialidade, integridade, disponibilidade e não repúdio de dados são componentes cruciais da segurança dos dados. O uso de algoritmos de criptografia garante a confidencialidade dos dados, salvaguardando que as informações sejam divulgadas a pessoas, processos ou dispositivos não autorizados. A Integridade de Dados usa hashes ou um resumo de mensagens para garantir a não alteração dos dados. A disponibilidade de dados garante acesso oportuno e confiável aos dados para usuários autorizados, enquanto que a não repúdio é a capacidade de provar que uma operação ou evento ocorreu e não pode ser repudiada posteriormente.
3. Qual tecnologia é um sistema SIEM de código aberto? – ELK; Tópico 27.1.0 - Há muitos sistemas SIEM disponíveis para administradores de rede. A suíte ELK é uma opção de código aberto.
4. Um administrador de rede está trabalhando com ELK. A quantidade de tráfego de rede a ser coletada por capturas de pacotes e o número de entradas e alertas de arquivos de log que serão gerados pela rede e dispositivos de segurança podem ser enormes. Qual é a hora padrão configurada no Kibana para mostrar as entradas de log? – 24horas; Tópico 27.2.0 - Logstash e Beats são usados para ingestão na pilha ELK. Eles fornecem acesso a um grande número de entradas de arquivo de log. Como o número de logs que podem ser exibidos é tão grande, Kibana, que é a interface visual nos logs, é configurado para mostrar as últimas 24 horas por padrão.
5. Em que linguagem de programação é escrito Elasticsearch? – Java; Tópico 27.1.0 - Elasticsearch é um mecanismo de pesquisa empresarial de plataforma cruzada escrito em Java.

1. Por quanto tempo o Payment Card Industry Security Standards Council (PCI DSS) exige que uma trilha de auditoria das atividades do usuário relacionadas a informações protegidas seja mantida? – 12 meses; Tópico 27.1.0 - Todos gostariam da segurança de coletar e salvar tudo, mas devido a problemas de armazenamento e acesso reter dados do NSM indefinidamente não é viável. O período de retenção para certos tipos de informações de segurança de rede pode ser especificado pelas estruturas de conformidade. O Payment Card Industry Security Standards Council (PCI DSS) exige que uma trilha de auditoria das atividades do usuário relacionadas a informações protegidas seja mantida por um ano.
2. Qual é a ferramenta de detecção de intrusões baseada em host integrada ao Security Onion? – OSSEC; Tópico 27.1.0 - Integrado ao Security Onion, o OSSEC é um sistema de detecção de intrusão baseado em host (HIDS) que pode realizar monitoramento de integridade de arquivos, monitoramento de log local, monitoramento de processos do sistema e detecção de rootkit.
3. Qual componente principal de código aberto do Elastic Stack é responsável por acessar, visualizar e investigar dados? – Kibana; Tópico 27.1.0 - Os principais componentes de código aberto da pilha Elastic são Logstash, Beats, Elasticsearch e Kibana. Kibana é responsável por acessar, visualizar e investigar dados. O Elasticsearch é responsável pelo armazenamento, indexação e análise de dados. A Logstash e a Beats são responsáveis pela aquisição de dados de rede.
4. Qual é a hora padrão definida no arquivo securityonion.conf para a retenção de dados
5. de alerta do Sguil? – 30 dias; Tópico 27.1.0 - Os dados de alerta Sguil são retidos por 30 dias por padrão. Esse valor é definido no arquivo securityonion.conf.
6. Qual ferramenta um analista usaria para iniciar uma investigação de fluxo de trabalho? – Sguill; Tópico 27.2.0 - O Sguil é um aplicativo baseado em GUI usado por analistas de segurança para analisar eventos de segurança de rede.
7. Qual componente principal de código aberto do Elastic Stack é responsável pelo armazenamento, indexação e análise de dados? – Elasticsearch; Tópico 27.1.0 - Os principais componentes de código aberto da pilha Elastic são Logstash, Beats, Elasticsearch e Kibana. Kibana é responsável por acessar, visualizar e investigar dados. O Elasticsearch é responsável pelo armazenamento, indexação e análise de dados. A Logstash e a Beats são responsáveis pela aquisição de dados de rede.
8. Qual ferramenta concentra eventos de segurança de várias fontes e pode interagir com outras ferramentas, como o Wireshark? – Sguill; Tópico 27.2.0 - O Sguil é um aplicativo baseado em GUI usado por analistas de segurança para analisar dados de sessão e capturas de pacotes.

Parte inferior do formulário

# Introdução

28.0.1

## Por que devo cursar este módulo?

Você aprendeu tudo sobre os diferentes vetores de ataque que você pode precisar para proteger, ferramentas e práticas para proteger seu sistema. Neste módulo final, você aprenderá o que fazer quando um ataque realmente acontecer.

28.0.2

## O que vou aprender neste módulo?

**Título do Módulo** - Modelos de resposta a incidentes

**Objetivo do Módulo** - Explique como o Associado CyberOps responde a incidentes de segurança cibernética.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Manuseio de evidências e atribuição de ataque | Explicar o papel dos processos forenses digital |
| A Cyber Kill Chain | Identifique as etapas no Cyber Kill Chain |
| The Diamond Model of Intrusion AnalysisIdentifique as etapas no | Classifique um evento de intrusão usando o modelo Diamond |
| Resposta a incidentes | Aplicar os procedimentos de tratamento de incidentes NIST 800-61r2 a um determinado cenário de incidente |

# Manuseio de evidências e atribuição de ataque

28.1.1

## Perícia Digital

Agora que investigou e identificou alertas válidos, o que faz com as provas? O analista de segurança cibernética irá inevitavelmente descobrir evidências de atividade criminosa. A fim de proteger a organização e prevenir o cibercrime, é necessário identificar os atores da ameaça, denunciá-los às autoridades competentes e fornecer provas para apoiar a acusação. Os analistas de segurança cibernética de nível 1 geralmente são os primeiros a descobrir delitos. Os analistas de segurança cibernética devem saber como lidar adequadamente com evidências e atribuí-la a atores ameaçadores.

A perícia digital é a recuperação e investigação de informações encontradas em dispositivos digitais no que diz respeito a atividades criminosas. Indicadores de comprometimento são a evidência de que ocorreu um incidente de segurança cibernética. Essas informações podem ser dados em dispositivos de armazenamento, na memória volátil do computador ou vestígios de cibercrime que são preservados em dados de rede, como pcaps e logs. É essencial que todos os indicadores de compromisso sejam preservados para análise futura e atribuição de ataques.

A atividade cibernética pode ser amplamente caracterizada como originária de dentro ou fora da organização. Investigações privadas estão preocupadas com indivíduos dentro da organização. Esses indivíduos poderiam simplesmente estar se comportando de maneiras que violam os acordos do usuário ou outras condutas não criminais. Quando indivíduos são suspeitos de envolvimento em atividades criminosas envolvendo roubo ou destruição de propriedade intelectual, uma organização pode optar por envolver autoridades policiais, caso em que a investigação se torna pública. Os usuários internos também poderiam ter usado a rede da organização para realizar outras atividades criminosas que não estão relacionadas à missão organizacional, mas estão em violação de vários estatutos legais. Neste caso, funcionários públicos realizarão a investigação.

Quando um invasor externo explora uma rede e rouba ou alterou dados, as evidências precisam ser coletadas para documentar o escopo da exploração. Vários órgãos reguladores especificam uma série de ações que uma organização deve tomar quando vários tipos de dados foram comprometidos. Os resultados da investigação forense podem ajudar a identificar as ações que precisam ser tomadas.

Por exemplo, de acordo com os regulamentos HIPAA dos EUA, se ocorrer uma violação de dados que envolva informações do paciente, a notificação da violação deve ser feita aos indivíduos afetados. Se a violação envolver mais de 500 pessoas em um estado ou jurisdição, a mídia, bem como os indivíduos afetados, devem ser notificados. A investigação forense digital deve ser usada para determinar quais indivíduos foram afetados e para certificar o número de indivíduos afetados para que a notificação apropriada possa ser feita em conformidade com os regulamentos HIPAA.

É possível que a própria organização possa ser objeto de uma investigação. Os analistas de segurança cibernética podem encontrar-se 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 tratamento de tais evidências. Se a intenção de destruir provas for estabelecida, poderá resultar em penalidades criminais para a organização e até mesmo para o analista de segurança cibernética.

28.1.2

## O Processo Forense Digital

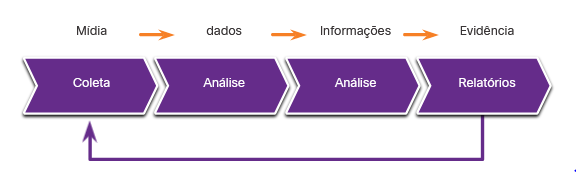
É importante que uma organização desenvolva processos e procedimentos bem documentados para análise forense digital. A conformidade regulamentar pode exigir esta documentação, e essa documentação pode ser inspecionada pelas autoridades em caso de investigação pública.

Publicação Especial NIST 800-86 Guia de integração de técnicas forenses para resposta a incidentes é um recurso valioso para organizações que exigem orientação no desenvolvimento de planos digitais forenses. Por exemplo, recomenda que a perícia seja realizada usando o processo de quatro fases.

A seguir, descreve as quatro fases básicas do processo forense de evidências digitais.

Esta imagem mostra o Processo Forense de Evidência Digital em uma barra de progresso movendo-se da direita para a esquerda. As quatro etapas são Coleta, Exame, Análise e Relatórios. Acima das etapas são listadas as entradas ou saídas para cada etapa. A mídia é coletada, e os resultados do exame em dados, Análise produz informações, e evidências são relatadas.

### O Processo Forense de Evidências Digitais



Coleta Análise Análise Relatórios Mídia dados Informações Evidência

1 - Coleta

Esta é a identificação de potenciais fontes de dados forenses e aquisição, manuseio e armazenamento desses dados. Este estágio é crítico porque deve-se ter especial cuidado para não danificar, perder ou omitir dados importantes.

2 – Análise

Isto implica avaliar e extrair informações relevantes dos dados recolhidos. Isso pode envolver descompactação ou descriptografia dos dados. As informações irrelevantes para a investigação podem ter de ser removidas. Identificar evidências reais em grandes coleções de dados pode ser muito difícil e demorado.

3 – Análise

Isto implica tirar conclusões dos dados. Recursos relevantes, como pessoas, lugares, horários, eventos, etc., devem ser documentados. Esta etapa também pode envolver a correlação de dados de várias fontes.

4 – Evidência

Isso implica preparar e apresentar informações resultantes da análise. Os relatórios devem ser imparciais e devem ser apresentadas explicações alternativas, se for caso disso. Limitações da análise e problemas encontrados devem ser incluídos. Devem também ser feitas sugestões para uma investigação mais aprofundada e para os próximos passos.

28.1.3

## Verifique sua compreensão - Identifique as etapas no processo de perícia digital

Parte superior do formulário

1. Qual técnica envolve a avaliação e extração de informações relevantes a partir dos dados coletados? Análise
2. Qual técnica envolve tirar conclusões dos dados? Análise
3. Qual é a técnica que inclui a identificação de potenciais fontes de dados forenses e a aquisição, manuseio e armazenamento desses dados? Coleta
4. Qual técnica inclui a preparação e apresentação das informações resultantes da análise? Relatórios

Parte inferior do formulário

28.1.4

## Tipos de Evidência

Em processos judiciais, as provas são geralmente classificadas como diretas ou indiretas. Provas diretas são provas que estavam indiscutivelmente na posse do acusado, ou são testemunhas oculares de alguém que observou diretamente o comportamento criminoso.

As provas são ainda classificadas como:

* **Melhor evidência** - Esta é evidência que está em seu estado original. Essas evidências podem ser dispositivos de armazenamento usados por um acusado, ou arquivos de arquivos que podem ser comprovados como inalterados.
* **Evidência corroborante** - Esta é uma evidência que suporta uma afirmação que é desenvolvida a partir da melhor evidência.
* **Evidência indireta** - Esta é evidência que, em combinação com outros fatos, estabelece uma hipótese. Isso também é conhecido como evidência circunstancial. Por exemplo, a evidência de que um indivíduo cometeu crimes semelhantes pode apoiar a afirmação de que a pessoa cometeu o crime de que é acusado.

28.1.5

## Verifique sua compreensão - Identifique o tipo de evidência

Parte superior do formulário

1. Que tipo de evidência estava indiscutivelmente na posse do acusado? – Evidência direta
2. Que tipo de evidência suporta uma afirmação que é desenvolvida a partir da melhor evidência? – Provas corroborantes
3. Que tipo de evidência é evidência circunstancial que, em combinação com outros fatos, estabelece uma hipótese? – Provas indiretas
4. Que tipo de evidência está em seu estado original? – Melhor evidência

Parte inferior do formulário

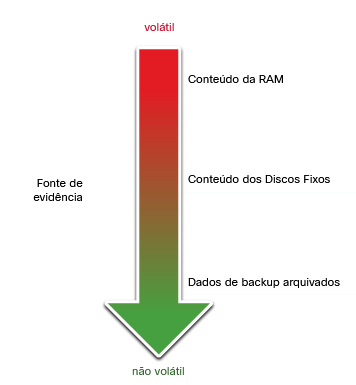
28.1.6

## Ordem de coleta de evidências

IETF RFC 3227 fornece diretrizes para a coleta de evidências digitais. Descreve uma ordem para a recolha de provas digitais com base na volatilidade dos dados. Os dados armazenados na RAM são os mais voláteis, e serão perdidos quando o dispositivo for desligado. Além disso, dados importantes na memória volátil podem ser substituídos por processos de rotina da máquina. Portanto, a coleta de evidências digitais deve começar com a evidência mais volátil e avançar para a menos volátil, como mostrado na figura.

Esta imagem usa uma seta apontada para baixo, classificada em cores de vermelho para verde, para atribuir um nível de volatilidade a certas fontes de evidência. A fonte mais volátil listada é o conteúdo da RAM, a fonte com volatilidade de nível médio é listada como o conteúdo de discos fixos e a fonte listada como não volátil são dados de backup arquivados.

### Prioridade de coleta



Fonte de  
evidênciaConteúdo dos Discos Fixosnão volátilvolátilConteúdo da RAMDados de backup arquivados

Um exemplo da ordem de coleta de evidências mais volátil a menos volátil é o seguinte:

1. Registros de memória, caches
2. Tabela de roteamento, cache ARP, tabela de processo, estatísticas de kernel, RAM
3. Sistemas de arquivos temporários
4. Meios não voláteis, fixos e removíveis
5. Dados de registro e monitoramento remotos
6. Interconexões físicas e topologias
7. Mídia de arquivamento, fita ou outros backups

Detalhes dos sistemas a partir dos quais as provas foram recolhidas, incluindo quem tem acesso a esses sistemas e a que nível de permissões devem ser registadas. Essas informações devem incluir configurações de hardware e software para os sistemas a partir dos quais os dados foram obtidos.

28.1.7

## Cadeia de Custódia

Embora possam ter sido recolhidas provas de fontes que apoiam a atribuição a um indivíduo acusado, pode-se argumentar que a evidência poderia ter sido alterada ou fabricada após a coleta. Para contrariar este argumento, deve ser definida e seguida uma rigorosa cadeia de custódia.

A cadeia de custódia envolve a coleta, manuseio e armazenamento seguro de evidências. Devem ser conservados registos pormenorizados dos seguintes elementos:

* Quem descobriu e recolheu as provas?
* Todos os detalhes sobre o tratamento de evidências, incluindo horas, locais e pessoal envolvido.
* Quem tem a principal responsabilidade pelas provas, quando a responsabilidade foi atribuída e quando a custódia mudou?
* Quem tem acesso físico à evidência enquanto foi armazenada? O acesso deve ser limitado apenas ao pessoal mais essencial.

28.1.8

## Integridade e preservação dos dados

Ao coletar dados, é importante que eles sejam preservados em sua condição original. O carimbo de data/hora (timestamp) dos arquivos deve ser preservado. Por esta razão, a prova original deve ser copiada e a análise deve ser realizada apenas em cópias do original. Isto é para evitar perda acidental ou alteração da evidência. Como os carimbos de data/hora podem fazer parte da evidência, abrir arquivos da mídia original deve ser evitado.

O processo utilizado para criar cópias dos elementos de prova utilizados no inquérito deve ser registado. Sempre que possível, as cópias devem ser cópias diretas em nível de bits dos volumes de armazenamento originais. Deve ser possível comparar a imagem do disco arquivado e a imagem do disco investigada para identificar se o conteúdo do disco investigado foi adulterado. Por esta razão, é importante arquivar e proteger o disco original para mantê-lo em sua condição original, sem adulteração.

Memória volátil pode conter evidências forenses, então ferramentas especiais devem ser usadas para preservar essa evidência antes que o dispositivo seja desligado e as evidências sejam perdidas. Os usuários não devem desconectar, desconectar da tomada ou desligar máquinas infectadas, a menos que explicitamente instruído pelo pessoal de segurança.

Seguir estes processos garantirá que qualquer evidência de delito será preservada, e quaisquer indicadores de comprometimento podem ser identificados.

28.1.9

## Atribuição de Ataque

Depois que a extensão do ataque cibernético foi avaliada e as evidências coletadas e preservadas, a resposta ao incidente pode passar para identificar a origem do ataque. Como sabemos, existe uma ampla gama de atores de ameaças, que vão desde indivíduos descontentes, hackers, cibercriminosos e gangues criminosas, ou estados-nação. Alguns criminosos agem de dentro da rede, enquanto outros podem estar do outro lado do mundo. A sofisticação do crime cibernético também varia. Os Estados-nação podem empregar grandes grupos de indivíduos altamente treinados para realizar um ataque e esconder seus rastros, enquanto outros atores ameaçadores podem abertamente se gabar de suas atividades criminosas.

Atribuição de ameaças refere-se ao ato de determinar o indivíduo, a organização ou a nação responsável por um incidente de invasão ou ataque bem-sucedido.

A identificação dos intervenientes responsáveis pela ameaça deve ocorrer através da investigação sistemática e baseada em princípios dos elementos de prova. Embora possa ser útil também especular quanto à identidade dos atores da ameaça, identificando potenciais motivações para um incidente, é importante não deixar que isso vise a investigação. Por exemplo, atribuir um ataque a um concorrente comercial pode levar a investigação longe da possibilidade de uma gangue criminosa ou um Estado-nação ter sido responsável.

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. Os cibercriminosos, assim como outros criminosos, têm traços específicos que são comuns à maioria dos seus crimes. Fontes de inteligência de ameaças podem ajudar a mapear o TTP identificado por uma investigação para fontes conhecidas de ataques semelhantes. No entanto, isso destaca um problema com a atribuição de ameaças. Evidência de cibercrime raramente é evidência direta. Identificar semelhanças entre TTP para atores conhecidos e desconhecidos da ameaça é evidência circunstancial.

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, as ferramentas usadas e outras técnicas. Por vezes, a nível da segurança nacional, as ameaças não podem ser atribuídas abertamente, porque isso exporia métodos e capacidades que precisam de ser protegidos.

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 DHCP podem ajudar a rastrear os endereços usados no ataque de volta para um dispositivo específico. Os logs AAA são muito úteis a esse respeito, pois rastreiam quem acessou quais recursos de rede a que horas.

28.1.10

## A estrutura MITRE ATT&CK

Uma maneira de atribuir um ataque é modelar o comportamento do ator de ameaça. O MITRE Táticas e técnicas adversas & Estrutura de Conhecimento Comum (ATT&CK) permite detectar táticas, técnicas e procedimentos do atacante (TTP) como parte da defesa contra ameaças e atribuição de ataques. Isso é feito mapeando os passos em um ataque para uma matriz de táticas generalizadas e descrevendo as técnicas que são usadas em cada tática. As táticas consistem nos objetivos técnicos que um atacante deve realizar para executar um ataque e as técnicas são o meio pelo qual as táticas são realizadas. Por último, os procedimentos são as acções específicas tomadas pelos intervenientes ameaçadores nas técnicas identificadas. Os procedimentos são o uso documentado de técnicas no mundo real por atores ameaçadores.

O MITRE ATT&CK Framework é uma base de conhecimento global do comportamento do ator de ameaças. Baseia-se na observação e análise de explorações do mundo real com o objetivo de descrever o comportamento do atacante, não o ataque em si. Ele foi projetado para permitir o compartilhamento automatizado de informações, definindo estruturas de dados para o intercâmbio de informações entre sua comunidade de usuários e MITRE.

A figura mostra uma análise de uma exploração de ransomware a partir da excelente sandbox online ANY.RUN. As colunas mostram as táticas de matriz de ataque corporativo, com as técnicas usadas pelo malware organizadas sob as colunas. Clicar na técnica, em seguida, lista detalhes dos procedimentos que são usados pela instância de malware específica com uma definição, explicação e exemplos da técnica.

**Nota**: Faça uma pesquisa na Internet no MITRE ATT&CK para saber mais sobre a ferramenta.

### Matriz MITRE ATT&CK para uma exploração de ransomware



# A Cyber Kill Chain

28.2.1

## Etapas da Cyber Kill Chain

A Cyber Kill Chain foi desenvolvida pela Lockheed Martin para identificar e prevenir intrusões cibernéticas. Existem sete etapas para o Cyber Kill Chain. O foco nessas etapas ajuda os analistas a entender as técnicas, as ferramentas e os procedimentos dos atores de ameaças. Ao responder a um incidente de segurança, o objetivo é detectar e parar o ataque o mais cedo possível na progressão da cadeia de eliminação. Quanto mais cedo o ataque for interrompido; menos dano é feito e menos o atacante aprende sobre a rede de destino.

A Cyber Kill Chain especifica o que um atacante deve completar para atingir seu objetivo. Os passos na Cyber Kill Chain são mostrados na figura.

Se o atacante for parado em qualquer fase, a cadeia de ataque é quebrada. Quebrar a corrente significa que o defensor frustrou com sucesso a intrusão do ator da ameaça. Os atores da ameaça só serão bem-sucedidos se concluírem a Etapa 7.

**Nota**: Ator ameaça é o termo usado ao longo deste curso para se referir à parte que instigou o ataque. No entanto, Lockheed Martin usa o termo “adversário” em sua descrição da Cyber Kill Chain. Portanto, os termos adversário e ator ameaça são usados de forma intercambiável neste tópico.

A figura mostra os passos da Cyber Kill Chain em uma lista vertical numerada. As etapas da Cadeia de Morte Cibernética são explicadas em detalhes nas próximas seções do texto.

1 2 3 4 5 6 7

**Reconhecimento**  
Pesquisando informações do alvo**Entrega**  
Entregar arma à vítima por e-mail ou outros meios**Instalação**  
Instalação de backdoor no destino para instalar malware**Ações em Objetivos**  
Atacante usa o acesso “Mãos no Teclado” para atingir o objetivo do ataque**Armaonização**  
Emparelhar malware remoto com backdoor para criar uma carga**Exploração**  
Execute código no sistema vulnerável acionando o código**Comando & Controle (CnC)**  
Canal de comando externo do servidor é criado para manipular o alvo

28.2.2

## Reconhecimento

Reconhecimento é quando o ator ameaça realiza pesquisas, coleta inteligência e seleciona alvos. Isso informará o ator da ameaça se o ataque vale a pena executar. Qualquer informação pública pode ajudar a determinar o que, onde e como o ataque a ser executado. Há muitas informações publicamente disponíveis, especialmente para organizações maiores, incluindo artigos de notícias, sites, procedimentos de conferência e dispositivos de rede voltados para o público. Quantidades crescentes de informações sobre os funcionários estão disponíveis por meio de redes sociais.

O agente da ameaça escolherá alvos que foram negligenciados ou desprotegidos porque terão uma maior probabilidade de serem penetrados e comprometidos. Todas as informações obtidas pelo agente da ameaça são revisadas para determinar sua importância e se revelam possíveis vias adicionais de ataque.

A tabela resume algumas das táticas e defesas usadas durante a etapa de reconhecimento.

| **Táticas do adversário** | **Defesas SOC** |
| --- | --- |
| Planejar e conduzir pesquisas:   * Coletar endereços de e-mail * Identificar funcionários nas redes sociais * Coletar todas as informações de relações públicas (comunicados de imprensa, prêmios, participantes de conferências, etc.) * Descubra servidores voltados para a Internet * Realize varreduras da rede para identificar endereços IP e portas abertas. | Descubra a intenção do adversário:   * Alertas de log da Web e dados de pesquisa * Coletar analiticamente os dados de navegação * Crie playbooks para detectar comportamentos que indicam atividade de reconhecimento * Priorizar a defesa em torno de tecnologias e pessoas que a atividade de reconhecimento está direcionada |

28.2.3

## Armamento

O objetivo desta etapa é usar as informações do reconhecimento para desenvolver uma arma contra sistemas específicos ou indivíduos na organização. Para desenvolver essa arma, o designer usará as vulnerabilidades dos ativos que foram descobertos e os construirá em uma ferramenta que pode ser implantada. Depois que a ferramenta foi usada, espera-se que o ator da ameaça tenha alcançado seu objetivo de obter acesso ao sistema ou rede de destino, degradando a integridade de um alvo ou toda a rede. O agente da ameaça examinará ainda mais a segurança da rede e dos ativos para expor fraquezas adicionais, obter controle sobre outros ativos ou implantar ataques adicionais.

Não é difícil escolher uma arma para o ataque. O agente da ameaça precisa analisar quais ataques estão disponíveis para as vulnerabilidades que eles descobriram. Existem muitos ataques que já foram criados e testados em geral. Um problema é que, como esses ataques são tão conhecidos, eles são provavelmente também conhecidos pelos defensores. Muitas vezes, é mais eficaz usar um ataque de dia zero para evitar métodos de detecção. Um ataque de dia zero usa uma arma que é desconhecida para os defensores e sistemas de segurança de rede. O ator ameaça pode querer desenvolver sua própria arma que é especificamente projetada para evitar a detecção, usando as informações sobre a rede e os sistemas que eles aprenderam. Os atacantes aprenderam a criar inúmeras variantes de seus ataques para evitar as defesas da rede.

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

| **Táticas do adversário** | **Defesa SOC** |
| --- | --- |
| Prepare e encene a operação:   * Obtenha uma ferramenta automatizada para entregar a carga de malware (armonizer). * Selecione ou crie um documento para apresentar à vítima. * Selecione ou crie uma backdoor e uma infraestrutura de comando e controle. | Detecte e colete artefatos de armamento:   * Certifique-se de que as regras e assinaturas do IDS estão atualizadas. * Realize uma análise completa de malware. * Construir detecções para o comportamento de armadores conhecidos. * O malware é antigo, “fora da prateleira” ou novo malware que pode indicar um ataque personalizado? * Colete arquivos e metadados para análise futura. * Determine quais artefatos de armamento são comuns a quais campanhas. |

28.2.4

## Entrega

Durante esta etapa, a arma é transmitida ao alvo usando um vetor de entrega. Isso pode ser através do uso de um site, mídia USB removível ou um anexo de e-mail. Se a arma não for entregue, o ataque não terá sucesso. O agente da ameaça usará muitos métodos diferentes para aumentar as chances de entregar a carga útil, 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 ele seja alterado para evitar a detecção. O código pode ser alterado para parecer inocente, mas ainda assim executar as ações necessárias, mesmo que possa demorar mais tempo para ser executado.

A tabela resume algumas das táticas e defesas usadas durante a etapa de entrega.

| **Táticas do adversário** | **Defesa SOC** |
| --- | --- |
| Inicie malware no destino:   * Direto contra servidores da Web * Entrega indireta através de:   + E-mail mal-intencionado   + Malware na pen USB   + Interações nas redes sociais   + Sites comprometidos | Bloquear a entrega de malware:   * Analise o caminho da infra-estrutura usado para a entrega. * Entenda servidores direcionados, pessoas e dados disponíveis para ataques. * Induzir a intenção do adversário com base no alvo. * Colete e-mails e logs da web para reconstrução forense. |

28.2.5

## Exploração

Depois que a arma foi entregue, o ator ameaça a usa para quebrar a vulnerabilidade e ganhar o controle do alvo. Os destinos de exploração mais comuns são aplicativos, vulnerabilidades do sistema operacional e usuários. O atacante deve usar uma exploração que ganhe o efeito que deseja. Isso é muito importante porque se a exploração errada for conduzida, obviamente o ataque não funcionará, mas efeitos colaterais não intencionais, como um DoS ou várias reinicializações de sistema, causarão atenção indevida que poderia facilmente informar os analistas de segurança cibernética sobre o ataque e as intenções do ator da ameaça.

A tabela resume algumas das táticas e defesas usadas durante a etapa de exploração.

| **Táticas do adversário** | **Defesa SOC** |
| --- | --- |
| Explore uma vulnerabilidade para obter acesso:   * Usar software, hardware ou vulnerabilidade humana * Adquirir ou desenvolver a exploração * Usar uma exploração acionada por adversários para vulnerabilidades de servidor * Usar uma exploração acionada por vítima, como abrir um anexo de e-mail ou um link de weblink malicioso | Treine funcionários, proteja códigos e dispositivos de proteção:   * Treinamento de conscientização de segurança dos funcionários e testes periódicos * Treinamento de desenvolvedores da Web para proteger código * Verificação regular de vulnerabilidades e testes de penetração * Medidas de endurecimento de endpoint * Auditoria de endpoint para determinar forense a origem da exploração |

28.2.6

## Instalação

Esta etapa é onde o ator ameaça estabelece um backdoor para o sistema para permitir o acesso contínuo ao alvo. Para preservar esse backdoor, é importante que o acesso remoto não alerte analistas ou usuários de segurança cibernética. O método de acesso deve sobreviver através de verificações antimalware e reinicialização do computador para ser eficaz. Esse acesso persistente também pode permitir comunicações automatizadas, especialmente eficazes quando vários canais de comunicação são necessários ao comandar uma botnet.

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

| **Táticas do adversário** | **Defesa SOC** |
| --- | --- |
| Instalar backdoor persistente:   * Instale o webshell no servidor web para acesso persistente. * Criar ponto de persistência adicionando serviços, chaves AutoRun, etc. * Alguns adversários modificam o carimbo de data/hora do malware para que ele apareça como parte do sistema operacional. | Detectar, registrar e analisar a atividade de instalação:   * HIPS para alertar ou bloquear 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. |

28.2.7

## Comando e controle

Nesta etapa, o objetivo é estabelecer comando e controle (CNC ou C2) com o sistema de destino. Os hosts comprometidos geralmente se sinalizam da rede para um controlador na Internet. Isso ocorre porque a maioria dos malwares requer interação manual para exfiltrar dados da rede. Os canais CNC são usados pelo ator de ameaças para emitir comandos para o software que eles instalaram no destino. O analista de segurança cibernética deve ser capaz de detectar comunicações CNC para descobrir o host comprometido. Isso pode ser na forma de tráfego não autorizado de Internet Relay Chat (IRC) ou tráfego excessivo para domínios suspeitos.

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

| **Táticas do adversário** | **Defesa SOC** |
| --- | --- |
| Canal aberto para manipulação de destino:   * Canal de comunicação bidirecional aberto para a infraestrutura CNC * Canais CNC mais comuns através de protocolos Web, DNS e e-mail * A infraestrutura do CNC pode ser de propriedade do adversário ou de outra rede vítima em si | Última chance de bloquear a operação:   * Investigar possíveis novas infraestruturas CNC * Descubra a infraestrutura CNC por meio da análise de malware * Isolar o tráfego DNS para servidores DNS suspeitos, especialmente DNS dinâmico * Evite o impacto bloqueando ou desativando o canal CNC * Consolidar o número de pontos de presença na Internet * Personalizar o bloqueio de regras de protocolos CNC em proxies da Web |

28.2.8

## Ações sobre os objetivos

O passo final da Cyber Kill Chain descreve o ator ameaçador alcançar seu objetivo original. Isso pode ser roubo de dados, realizar um ataque DDoS ou usar a rede comprometida para criar e enviar spam ou mina Bitcoin. Neste ponto, o ator ameaça está profundamente enraizado nos sistemas da organização, escondendo seus movimentos e cobrindo seus rastros. É extremamente difícil remover o agente de ameaça da rede.

A tabela resume algumas das táticas e defesas usadas durante as ações na etapa objetivos.

| **Táticas do adversário** | **Defesa SOC** |
| --- | --- |
| Colha as recompensas do ataque bem-sucedido:   * Coletar credenciais do usuário * Escalonamento de privilégios * Reconhecimento interno * Movimento lateral através do ambiente * Coletar e exfiltrar dados * Destruir sistemas * Substituir, modificar ou corromper dados | Detectar usando evidências forenses:   * Estabelecer livro de respostas a incidentes * Detectar exfiltração de dados, movimentação lateral e uso não autorizado de credenciais * Resposta imediata do analista para todos os alertas * Análise forense de endpoints para triagem rápida * Capturas de pacotes de rede para recriar a atividade * Realizar avaliação de danos |

28.2.9

## Verifique sua compreensão - identifique a etapa da Kill Chain

Parte superior do formulário

Identifique as etapas na cadeia de eliminação cibernética respondendo às perguntas.

1. Em que etapa o ator da ameaça explora a vulnerabilidade e obtém o controle do alvo? – Exploração
2. Em que etapa a arma é transmitida ao alvo através do uso de um site, mídia USB removível, um anexo de e-mail ou por outros meios? – Entrega

1. Em que etapa o ator da ameaça reúne inteligência e seleciona alvos? – Reconhecimento

1. Em que etapa o ator de ameaça usa um método de comunicação, como o IRC, para emitir comandos para o software instalado no destino? – Comando e controle
2. Em que etapa o ator da ameaça usa vulnerabilidades dos ativos que foram descobertos e os transforma em uma ferramenta? - Armamento

Parte inferior do formulário

[28.1](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[Manuseio de evidências e atribuição de ataque](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[28.3](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# O modelo Diamond de análise de intrusão

28.3.1

## Visão geral do modelo Diamond

O Modelo Diamond de Análise de Intrusão é composto por quatro partes, como mostrado na figura. O modelo representa um incidente ou evento de segurança. No Modelo Diamond, um evento é uma atividade limitada ao tempo que é restrita a uma etapa específica em que um adversário usa uma capacidade sobre a infraestrutura para atacar uma vítima para alcançar um resultado específico.

Os quatro principais recursos de um evento de intrusão são adversário, capacidade, infraestrutura e vítima:

* **Adversário** - Estas são as partes responsáveis pela intrusão.
* **Capacidade** - Esta é uma ferramenta ou técnica que o adversário usa para atacar a vítima.
* **Infraestrutura** - Este é o caminho ou caminhos de rede que os adversários usam para estabelecer e manter o comando e o controle sobre suas capacidades.
* **Vítima** - Este é o alvo do ataque. No entanto, uma vítima pode ser o alvo inicialmente e, em seguida, usada como parte da infra-estrutura para lançar outros ataques.

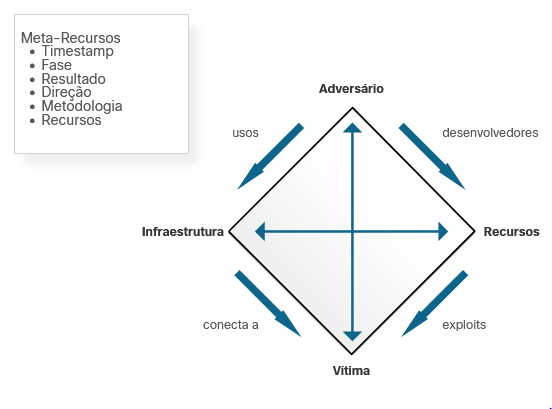
O adversário usa recursos sobre infraestrutura para atacar a vítima. O modelo pode ser interpretado como dizendo: “O adversário usa a infraestrutura para se conectar à vítima. O adversário desenvolve capacidade de explorar a vítima.” Por exemplo, um recurso como malware pode ser usado na infraestrutura de e-mail por um adversário para explorar uma vítima.

Os meta-recursos expandem o modelo ligeiramente para incluir os seguintes elementos importantes:

* **Timestamp** - Isso indica a hora de início e parada de um evento e é parte integrante do agrupamento de atividades mal-intencionadas.
* **Fase** - Isso é análogo às etapas da Cyber Kill Chain; atividade maliciosa inclui duas ou mais etapas executadas sucessivamente para alcançar o resultado desejado.
* **Resultado** - Isso delineia o que o adversário ganhou com o evento. Os resultados podem ser documentados como um ou mais dos seguintes: confidencialidade comprometida, integridade comprometida e disponibilidade comprometida.
* **Direção** - Indica a direção do evento em todo o Modelo Diamond. Elas incluem infraestrutura adversária, infraestrutura para vítima, vítima para infraestrutura e infraestrutura para adversário.
* **Metodologia** - Isso é usado para classificar o tipo geral de evento, como varredura de portas, phishing, ataque de entrega de conteúdo, syn flood, etc.
* \***Recursos** - Estes são um ou mais recursos externos usados pelo adversário para o evento de intrusão, como software, conhecimento do adversário, informações (por exemplo, nome de usuário/senhas) e ativos para realizar o ataque (hardware, fundos, instalações, acesso à rede).

28.3.2

## O Modelo Diamond



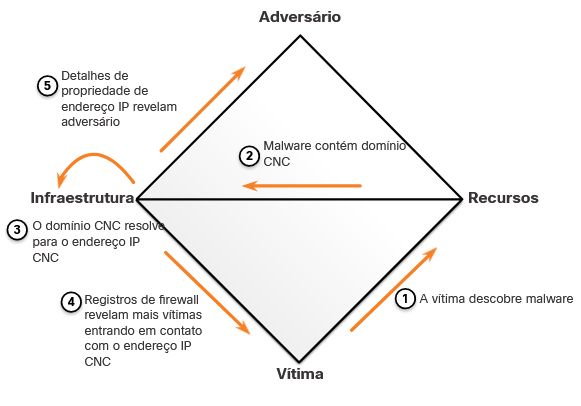
## Pivotando em todo o modelo Diamond

Como analista de segurança cibernética, você pode ser chamado a usar o Modelo Diamond de Análise de Intrusão para diagramar uma série de eventos de intrusão. O Modelo Diamond é ideal para ilustrar como o adversário giro de um evento para o outro.

Por exemplo, na figura um funcionário relata que seu computador está agindo de forma anormal. Uma verificação de host feita 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. Estes nomes de domínio resolvem para uma lista de endereços IP. Esses endereços IP são então usados para identificar o adversário, bem como investigar registros para determinar se outras vítimas na organização estão usando o canal CNC.

A figura retrata a caracterização do modelo de diamante de uma exploração. O diamante com as características do núcleo é mostrado, e há etapas numeradas com setas conectando as várias características do núcleo. O primeiro passo conecta a vítima à capacidade, e tem a nota Vítima descobre malware. A etapa 2 conecta o recurso e a infra-estrutura, e tem a nota Malware contém domínio CNC. A etapa 3 tem uma seta arqueada da infraestrutura para a nota que o domínio CnC resolve para o endereço IP CnC. A etapa 4 conecta a infraestrutura à vítima com a nota Os logs do Firewall revelam outras vítimas entrando em contato com o endereço IP do CNC. A etapa 5 conecta a infraestrutura ao adversário, com a nota Detalhes de propriedade do endereço IP revelam adversário

### Caracterização do modelo Diamond de uma exploração



AdversárioRecursosVítimaInfraestruturaMalware contém domínio CNCDetalhes de propriedade de endereço IP revelam adversárioO domínio CNC resolve para o endereço IP CNCRegistros de firewall revelam mais vítimas entrando em contato com o endereço IP CNCA vítima descobre malware

28.3.3

## O Modelo Diamond e a Cyber Kill Chain

Os adversários não operam em apenas um evento. Em vez disso, os eventos são encadeados em uma cadeia na qual cada evento deve ser concluído com êxito antes do próximo evento. Este segmento de eventos pode ser mapeado para a Cyber Kill Chain discutida anteriormente no capítulo.

O exemplo a seguir, mostrado na figura, ilustra o processo de ponta a ponta de um adversário à medida que eles atravessam verticalmente a Cyber Kill Chain, usam um host comprometido para girar horizontalmente para outra vítima e, em seguida, iniciar outro segmento de atividade:

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

2. O adversário usa o domínio recém-descoberto gadets.com para uma nova pesquisa “administrador de rede gadget.com” e descobre postagens de fóruns de usuários que afirmam ser administradores de rede do gadget.com. Os perfis de usuário revelam seus endereços de e-mail.

3. O adversário envia e-mails de phishing com um cavalo de Tróia anexado aos administradores de rede do gadget.com.

4. Um administrador de rede (NA1) do gadget.com abre o anexo malicioso. Isso executa a exploração fechada, permitindo a execução de código adicional.

5. O host comprometido do NA1 envia uma mensagem HTTP Post para um endereço IP, registrando-a com um controlador CNC. O host comprometido do NA1 recebe uma resposta HTTP em troca.

6. É revelado pela engenharia reversa que o malware tem endereços IP adicionais configurados que atuam como um backup se o primeiro controlador não responder.

7. Através de uma mensagem de resposta CNC HTTP enviada para o host do NA1, o malware começa a agir como um proxy da web para novas conexões TCP.

1. Através de informações do proxy que está sendo executado no host da NA1, Adversary faz uma pesquisa na web para “pesquisa mais importante de sempre” e encontra Victima 2, Interessante Research Inc.
2. Adversary verifica a lista de contatos de e-mail da NA1 para qualquer contato da Interessante Research Inc. e descobre o contato para o Diretor de Pesquisa Interessante da Inc.
3. O Diretor de Pesquisa da Interessante Research Inc. recebe um e-mail spear-phish do endereço de e-mail da Gadget Inc. enviado do host da NA1 com a mesma carga útil observada no Evento 3.

O adversário agora tem duas vítimas comprometidas, das quais ataques adicionais podem ser lançados. Por exemplo, o adversário poderia explorar os contatos de e-mail do Diretor de Pesquisa para as vítimas potenciais adicionais. O adversário também pode configurar outro proxy para exfiltrar todos os arquivos do Diretor de Pesquisa.

**Nota**: Este exemplo é uma modificação do exemplo do Departamento de Defesa dos EUA na publicação “The Diamond Model of Intrusion Analysis”.

## Exemplo de tópicos de atividades



28.3.4

## Verifique sua compreensão - Identifique os recursos do modelo Diamond

Parte superior do formulário

1. Que parte do modelo Diamond representa o ator ameaçador? – Adversário
2. Que parte do modelo Diamond representa o caminho de rede que é usado para uma exploração? – Infraestrutura em nuvem
3. Que parte do Modelo Diamante representa o alvo de uma exploração? – Vitima
4. Qual meta-característica representa o que o ator da ameaça ganhou de uma exploração? Ele pode ser caracterizado como confidencialmente comprometido, integridade comprometida e disponibilidade comprometida. – Resultado
5. Que parte do Modelo Diamond representa as ferramentas ou técnicas que o ator ameaça usa para atacar um alvo? – Capacidade
6. Qual meta-característica do Modelo Diamond indica o caminho entre as partes do Modelo Diamond que é usado por uma exploração? – Direção

# Resposta a incidentes

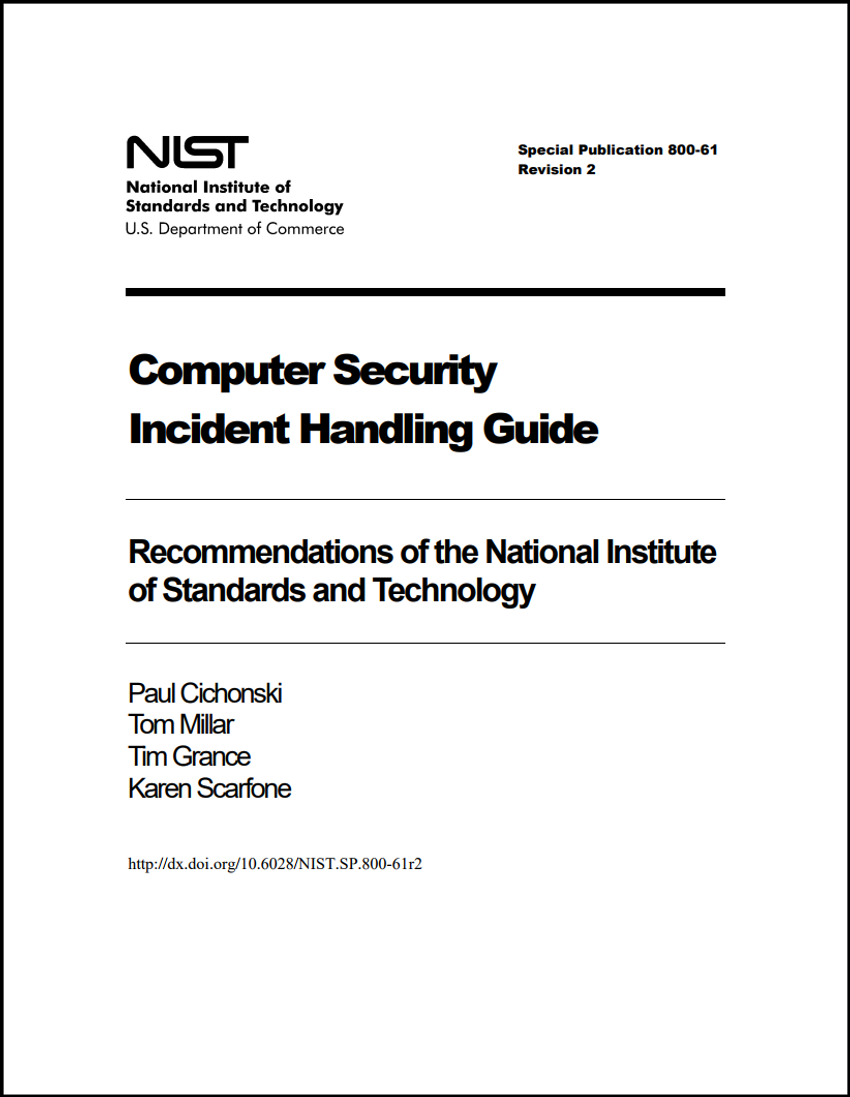
28.4.1

## Estabelecimento de um recurso de resposta

A resposta a incidentes envolve os métodos, políticas e procedimentos usados por uma organização para responder a um ataque cibernético. Os objetivos da resposta a incidentes são limitar o impacto do ataque, avaliar os danos causados e implementar procedimentos de recuperação. Devido à perda potencial de propriedade e receita em larga escala que pode ser causada por ataques cibernéticos, é essencial que as organizações criem e mantenham planos detalhados de resposta a incidentes e designem pessoal responsável pela execução de todos os aspectos desse plano.

As recomendações do NIST (National Institute of Standards and Technology, Instituto Nacional de Padrões e Tecnologia) dos EUA para resposta a incidentes estão detalhadas em sua Publicação Especial 800-61, revisão 2, intitulada “Computer Security Incident Handling Guide”, que mostra a figura.

**Observação**: Embora este capítulo resume grande parte do conteúdo do padrão NIST 800-61r2, você deve estar familiarizado com toda a publicação, pois ela aborda quatro tópicos principais de exame para o exame Noções Básicas de Operações de Segurança Cibernética da Cisco.



O padrão NIST 800-61r2 fornece diretrizes para o tratamento de incidentes, especialmente para analisar dados relacionados a incidentes e determinar a resposta apropriada a cada incidente. As diretrizes podem ser seguidas independentemente de plataformas de hardware, sistemas operacionais, protocolos ou aplicativos específicos.

O primeiro passo para uma organização é estabelecer uma capacidade de resposta a incidentes de segurança de computador (CSIRC). O NIST recomenda a criação de políticas, planos e procedimentos para estabelecer e manter um CSIRC.

**Elementos de Política**

Uma política de resposta a incidentes detalha como os incidentes devem ser tratados com base na missão, tamanho e função da organização. A política deve ser revista regularmente, de modo a ajustá-la de modo a atingir os objetivos do roteiro que foi elaborado. Os elementos de política incluem o seguinte:

* Declaração de compromisso de gestão
* Finalidade e objetivos da política
* Âmbito de aplicação da política
* Definição de incidentes de segurança informática e termos conexos
* Estrutura organizacional e definição de funções, responsabilidades e níveis de autoridade
* Priorização de classificações de gravidade de incidentes
* Medidas de desempenho
* Formulários de comunicação e contato

**Elementos do Plano**

Um bom plano de resposta a incidentes ajuda a minimizar os danos causados por um incidente. Ele também ajuda a melhorar o programa geral de resposta a incidentes, ajustando-o de acordo com as lições aprendidas. Ele garantirá que cada parte envolvida na resposta ao incidente tenha uma compreensão clara não só do que estará fazendo, mas também do que outros estarão fazendo. Os elementos do plano são os seguintes:

* Missão
* Estratégias e objetivos
* Aprovação da alta administração
* Abordagem organizacional para a resposta
* 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

**Elementos de procedimento**

Os procedimentos que são seguidos durante uma resposta a incidentes devem seguir o plano de resposta a incidentes. Os elementos de procedimentos são os seguintes:

* Processos técnicos
* Uso de técnicas
* Preenchimento de formulários,
* Seguindo listas de verificação

Estes são procedimentos operacionais padrão (SOPs) típicos. Esses POPs devem ser detalhados para que a missão e os objetivos da organização estejam em mente quando esses procedimentos forem seguidos. Os SOPs minimizam os erros que podem ser causados por funcionários que estão sob estresse durante a participação no tratamento de incidentes. É importante compartilhar e praticar esses procedimentos, certificando-se de que eles são úteis, precisos e apropriados.

28.4.2

## Verifique sua compreensão - Identifique os elementos do plano de resposta a incidentes

Parte superior do formulário

Identifique os elementos de um plano de resposta a incidentes respondendo às perguntas.

1. A definição de incidentes de segurança informática e elementos termos relacionados é em que parte do plano de resposta a incidentes? – Politica
2. O elemento estratégia e metas é em que parte do plano de resposta a incidentes? Plano
3. A estrutura organizacional e definição de funções, responsabilidades e níveis de elemento de autoridade está em qual parte do plano de resposta a incidentes? Politica
4. A priorização e as classificações de gravidade do elemento de incidentes está em qual parte do plano de resposta a incidentes? Política
5. Lista de verificação pode ser encontrada em que parte do plano de resposta a incidentes? Procedimento

Parte inferior do formulário

28.4.3

## Partes interessadas da Resposta

Outros grupos e indivíduos dentro da organização também podem estar envolvidos com o tratamento de incidentes. É importante assegurar que cooperarão antes de um incidente estar em curso. Sua experiência e habilidades podem ajudar a equipe de resposta a incidentes de segurança informática (CSIRT) a lidar com o incidente de forma rápida e correta. Estas são algumas das partes interessadas que podem estar envolvidas na entrega de um incidente de segurança:

* **Gestão** - Os gerentes criam as políticas que todos devem seguir. Eles também projetam o orçamento e são responsáveis pela equipe de todos os departamentos. A gerência deve coordenar a resposta ao incidente com outras partes interessadas e minimizar os danos de um incidente.
* **Garantia de informações** - Esse grupo pode precisar ser chamado para alterar coisas como regras de firewall durante alguns estágios de gerenciamento de incidentes, como contenção ou recuperação.
* **Suporte de TI** - Este é o grupo que trabalha com a tecnologia na organização e a entende mais. Como o suporte de TI tem uma compreensão mais profunda, é mais provável que eles executem a ação correta para minimizar a eficácia do ataque ou preservar as evidências adequadamente.
* **Departamento Jurídico** - É uma prática recomendada fazer com que o departamento jurídico revise as políticas, os planos e os procedimentos de incidentes para garantir que eles não violem quaisquer diretrizes locais ou federais. Além disso, se algum incidente tiver implicações legais, um perito jurídico terá de se envolver. Isso pode incluir acusação, coleta de evidências ou ações judiciais.
* **Assuntos Públicos e Relações com a Mídia** - Há momentos em que a mídia e o público podem precisar ser informados de um incidente, como quando suas informações pessoais foram comprometidas durante um incidente.
* **Recursos Humanos** - O departamento de recursos humanos pode precisar executar medidas disciplinares se ocorrer um incidente causado por um funcionário.
* **Planejadores de continuidade de negócios** - incidentes de segurança podem alterar a continuidade de negócios de uma organização. É importante que os responsáveis pelo planejamento de continuidade de negócios estejam cientes dos incidentes de segurança e do impacto que tiveram sobre a organização como um todo. Isto permitir-lhes-á fazer quaisquer alterações nos planos e nas avaliações de risco.
* **Segurança física e gerenciamento de instalações** - Quando um incidente de segurança ocorre devido a um ataque físico, como tailgating ou surf no ombro, essas equipes podem precisar ser informadas e envolvidas. É também da sua responsabilidade garantir instalações que contenham provas de uma investigação.

**A certificação do modelo de maturidade de segurança**

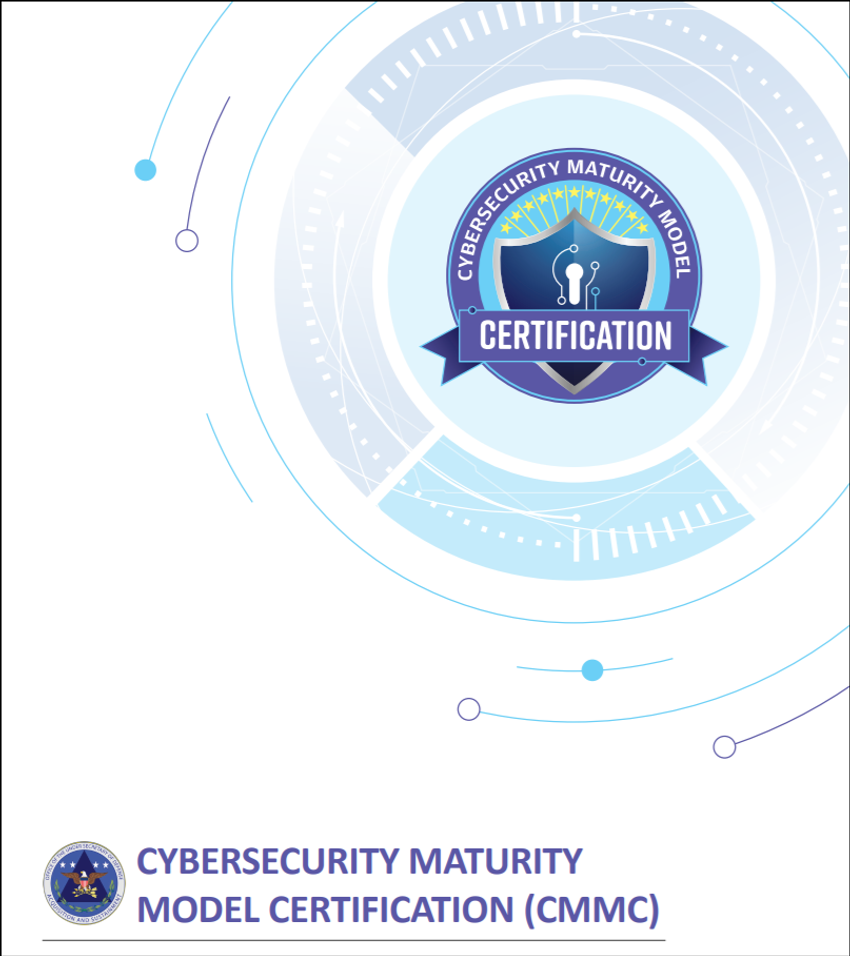
A estrutura de Certificação de Modelo de Maturidade de Segurança Cibernética (CMMC) foi criada para avaliar a capacidade das organizações que desempenham funções para o Departamento de Defesa dos EUA (DoD) para proteger a cadeia de suprimentos militar contra interrupções ou perdas devido a incidentes de segurança cibernética. Violações de segurança relacionadas às informações do DoD indicaram que os padrões do NIST não eram suficientes para atenuar o cenário de ameaças cada vez maior e em evolução, especialmente por parte dos atores do Estado-nação. Para que as empresas recebam contratos do DoD, essas empresas devem ser certificadas. A certificação consiste em cinco níveis, com diferentes níveis exigidos dependendo do grau de segurança exigido pelo projeto.

O CMMC especifica 17 domínios, cada um dos quais tem um número variável de recursos que estão associados a ele. A organização é classificada pelo nível de maturidade que foi alcançado para cada um dos domínios. Um dos domínios diz respeito à resposta a incidentes. Os recursos associados ao domínio de resposta a incidentes são os seguintes:

* Plano de resposta a incidentes
* Detectar e relatar eventos
* Desenvolver e implementar uma resposta a um incidente declarado
* Realizar revisões pós-incidentes
* Teste de resposta a incidentes

O CMMC certifica organizações por nível. Para a maioria dos domínios, há cinco níveis, no entanto, para resposta a incidentes, existem apenas quatro. Quanto maior o nível certificado, mais madura será a capacidade de segurança cibernética da organização. Um resumo dos níveis de maturidade do domínio de resposta à incidência é mostrado abaixo.

* **Nível 2 -** Estabeleça um plano de resposta a incidentes que siga o processo do NIST. Detectar, relatar e priorizar eventos. Responda a eventos seguindo procedimentos predefinidos. Analise a causa dos incidentes para mitigar problemas futuros.
* **Nível 3** - Documentar e relatar incidentes às partes interessadas que foram identificados no plano de resposta a incidentes. Teste a capacidade de resposta a incidentes da organização.
* **Nível 4 -** Use o conhecimento de táticas, técnicas e procedimentos do atacante (TPT) para refinar o planejamento e a execução da resposta a incidentes. Estabeleça um centro de operações de segurança (SOC) que facilite um recurso de resposta 24/7.
* **Nível 5 -** Utilize técnicas de coleta de dados forenses informáticas aceitas e sistemáticas, incluindo o manuseio e armazenamento seguros de dados forenses. Desenvolva e utilize respostas manuais e automatizadas em tempo real para possíveis incidentes que seguem padrões conhecidos.



28.4.4

## Ciclo de vida de resposta a incidentes do NIST

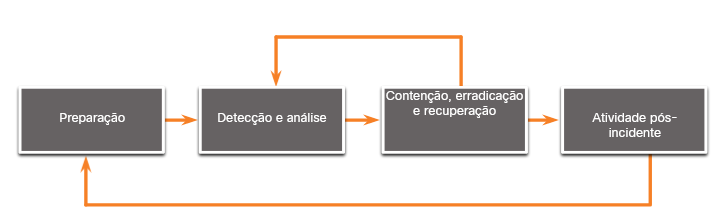
O NIST define quatro etapas no ciclo de vida do processo de resposta a incidentes, conforme mostrado na figura.

* **Preparação** - Os membros do CSIRT são treinados para responder a um incidente. Os membros do CSIRT devem desenvolver continuamente o conhecimento das ameaças emergentes.
* **Detecção e análise** - Através do monitoramento contínuo, 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. Esta fase pode voltar à detecção e análise para reunir mais informações, ou para expandir o escopo da investigação.
* **Atividades pós-incidente** - O CSIRT então documenta como o incidente foi tratado, recomenda alterações para resposta futura e especifica como evitar uma repetição.

O ciclo de vida de resposta a incidentes destina-se a ser um processo de aprendizagem auto-reforçado, pelo qual cada incidente informa o processo para lidar com incidentes futuros. Cada uma dessas fases é discutida com mais detalhes neste tópico.

A imagem mostra o ciclo de resposta a incidentes do NIST, com setas mostrando o fluxo de trabalho normal e o feedback em uma resposta a incidentes.

### Ciclo de vida de resposta a incidentes



PreparaçãoDetecção e análiseContenção, erradicação e recuperaçãoAtividade pós-incidente

28.4.5

## Preparação

A fase de preparação é quando o CSIRT é criado e treinado. Essa fase também é quando as ferramentas e ativos que serão necessários pela equipe para investigar incidentes são adquiridos e implantados. A lista a seguir contém exemplos de ações que também ocorrem durante a fase de preparação:

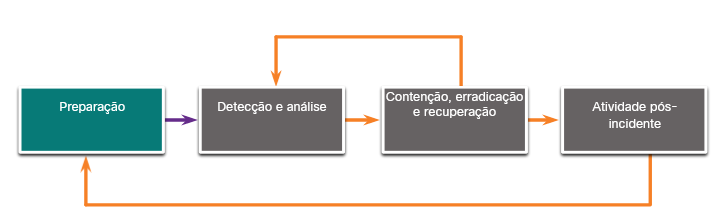
* Os processos organizacionais são criados para abordar a comunicação entre as pessoas na equipe de resposta. Isso inclui informações de contato para partes interessadas, outros CSIRTs e aplicação da lei, um sistema de rastreamento de problemas, smartphones, software de criptografia, etc.
* São criadas instalações para hospedar a equipe de resposta e o SOC.
* Hardware e software necessários para análise e mitigação de incidentes são adquiridos. Isso pode incluir software forense, computadores sobressalentes, servidores e dispositivos de rede, dispositivos de backup, sniffers de pacotes e analisadores de protocolo.
* As avaliações de risco são usadas para implementar controles que limitarão o número de incidentes.
* A validação da implantação de hardware e software de segurança é realizada em dispositivos de usuário final, servidores e dispositivos de rede.
* Materiais de treinamento de conscientização sobre segurança do usuário são desenvolvidos

Recursos adicionais de análise de incidentes podem ser necessários. Exemplos desses recursos são uma lista de ativos críticos, diagramas de rede, listas de portas, hashes de arquivos críticos e leituras de linha de base da atividade do sistema e da rede. O software de mitigação também é um item importante quando se prepara para lidar com um incidente de segurança. Uma imagem de um sistema operacional limpo e arquivos de instalação de aplicativos pode ser necessária para recuperar um computador de um incidente.

Muitas vezes, o CSIRT pode ter um kit de salto preparado. Esta é uma caixa portátil com muitos dos itens listados acima para ajudar a estabelecer uma resposta rápida. Alguns desses itens podem ser um laptop com software apropriado instalado, mídia de backup e qualquer outro hardware, software ou informações para ajudar na investigação. É importante inspecionar regularmente o kit de salto para instalar atualizações e certificar-se de que todos os elementos necessários estão disponíveis e prontos para uso. É útil praticar a implantação do jump kit com o CSIRT para garantir que os membros da equipe saibam usar seu conteúdo corretamente.

As mesmas caixas da seção anterior são mostradas com a caixa de preparação destacada.

### Fase de Preparação



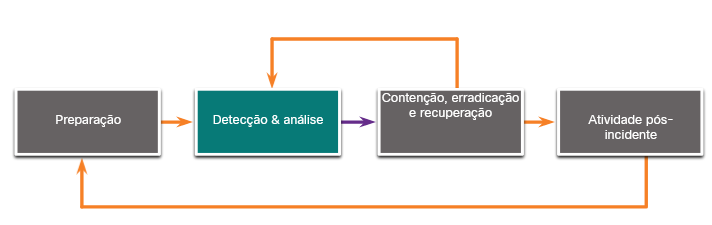
PreparaçãoDetecção e análiseContenção, erradicação e recuperaçãoAtividade pós-incidente

28.4.6

## Detecção e análise

As mesmas caixas da seção anterior são mostradas com a caixa de detecção e análise destacada.

### Detecção & Análise



Como há tantas maneiras diferentes em que um incidente de segurança pode ocorrer, é impossível criar instruções que cobrem completamente cada etapa a seguir para lidar com eles. Diferentes tipos de incidentes exigirão respostas diferentes.

Vetores de Ataque

Uma organização deve estar preparada para lidar com qualquer incidente, mas deve se concentrar nos tipos mais comuns de incidentes para que eles possam ser tratados rapidamente. Estes são alguns dos tipos mais comuns de vetores de ataque:

* **Web** - Qualquer ataque iniciado a partir de um site ou aplicativo hospedado por um site.
* **E-mail** - Qualquer ataque iniciado a partir de um email ou anexo de email.
* **Perda ou Roubo** - Qualquer equipamento usado pela organização, como um laptop, desktop ou smartphone, pode fornecer as informações necessárias para que alguém inicie um ataque.
* **Personificação** - Quando algo ou alguém é substituído com o propósito de intenção maliciosa.
* **Atrição** - Qualquer ataque que use força bruta para atacar dispositivos, redes ou serviços.
* **Mídia** - Qualquer ataque iniciado a partir de armazenamento externo ou mídia removível.

Detecção

Alguns incidentes são fáceis de detectar, enquanto outros podem passar despercebidos por meses. A detecção de incidentes de segurança pode ser a fase mais difícil no processo de resposta a incidentes. Os incidentes são detectados de muitas maneiras diferentes e nem todas essas formas são muito detalhadas ou fornecem clareza detalhada. Existem formas automatizadas de detecção, como software antivírus ou IDS. Há também detecções manuais por meio de relatórios de usuários.

É importante determinar com precisão o tipo de incidente e a extensão dos efeitos. Existem duas categorias para os sinais de um incidente:

* **Precursor** - Este é um sinal de que um incidente pode ocorrer no futuro. Quando precursores são detectados, um ataque pode ser evitado alterando medidas de segurança para abordar especificamente o tipo de ataque detectado. Exemplos de precursores são entradas de log que mostram uma resposta a uma varredura de porta ou uma vulnerabilidade recém-descoberta para o servidor Web de uma organização.
* **Indicador** - Este é um sinal de que um incidente já pode ter ocorrido ou está ocorrendo no momento. Alguns exemplos de indicadores são um host infectado com malware, vários logins com falha de uma fonte desconhecida ou um alerta IDS.

Análise

A análise de incidentes é difícil porque nem todos os indicadores são precisos. Em um mundo perfeito, cada indicador deve ser analisado para descobrir se é preciso. Isso é quase impossível devido ao número e variedade de incidentes registrados e relatados. O uso de algoritmos complexos e aprendizado de máquina muitas vezes ajudam a determinar a validade de incidentes de segurança. Isso é mais prevalente em grandes organizações que têm milhares ou mesmo milhões de incidentes diariamente. Um método que pode ser usado é a criação de perfis de rede e sistema. A criação de perfis é medir as características da atividade esperada em dispositivos e sistemas de rede para que as alterações nele possam ser mais facilmente identificadas.

Quando um indicador é considerado preciso, isso não significa necessariamente que ocorreu um incidente de segurança. Alguns indicadores acontecem por outras razões além da segurança. Um servidor que falha continuamente, por exemplo, pode ter RAM ruim em vez de um ataque de estouro de buffer ocorrer. Para ser seguro, até mesmo sintomas ambíguos ou contraditórios devem ser analisados para determinar se ocorreu um incidente de segurança legítimo. O CSIRT deve reagir rapidamente para validar e analisar incidentes. Isso é realizado seguindo um processo predefinido e documentando cada etapa.

Escopo

Quando o CSIRT acredita que um incidente ocorreu, ele deve executar imediatamente uma análise inicial para determinar o escopo do incidente, como quais redes, sistemas ou aplicativos são afetados, quem ou o que originou o incidente e como o incidente está ocorrendo. Essa atividade de escopo deve fornecer informações suficientes para que a equipe priorize atividades subsequentes, como contenção do incidente e análise mais profunda dos efeitos do incidente.

Notificação de incidentes

Quando um incidente é analisado e priorizado, a equipe de resposta a incidentes precisa notificar as partes interessadas e externas apropriadas para que todos os que precisam estar envolvidos desempenhem suas funções. Exemplos de partes que são normalmente notificadas incluem:

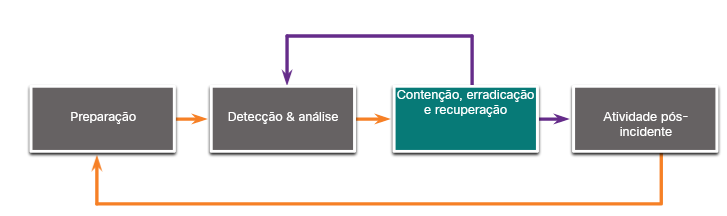
* Diretor executivo de informações (CIO)
* Chefe de segurança da informação
* Oficial de segurança da informação local
* Outras equipes de resposta a incidentes dentro da organização
* Equipas externas de resposta a incidentes (se apropriado)
* Proprietário do sistema
* Recursos humanos (para casos envolvendo funcionários, como assédio por e-mail)
* Assuntos públicos (para incidentes que possam gerar publicidade)
* Departamento jurídico (para incidentes com potenciais ramificações legais)
* US-CERT (necessário para agências federais e sistemas operados em nome do governo federal)
* Aplicação da lei (se for caso disso)

28.4.7

## Contenção, erradicação e recuperação

As mesmas caixas da seção anterior são mostradas com a caixa de contenção, erradicação e recuperação destacada.

### Fase de contenção, erradicação e recuperação



PreparaçãoDetecção & análiseContenção, erradicação e recuperaçãoAtividade pós-incidente

Depois que um incidente de segurança foi detectado e uma análise suficiente foi realizada para determinar se o incidente é válido, ele deve ser contido para determinar o que fazer sobre ele. Estratégias e procedimentos para contenção de incidentes precisam estar em vigor antes que um incidente ocorra e implementado antes que haja danos generalizados.

**Estratégia de contenção**

Para cada tipo de incidente, uma estratégia de contenção deve ser criada e aplicada. Estas são algumas condições para determinar o tipo de estratégia a ser criada para cada tipo de incidente:

* Quanto tempo levará para implementar e concluir uma solução?
* Quanto tempo e quantos recursos serão necessários para implementar a estratégia?
* Qual é o processo para preservar evidências?
* Um invasor pode ser redirecionado para uma área restrita para que o CSIRT possa documentar com segurança a metodologia do invasor?
* Qual será o impacto na disponibilidade de serviços?
* Qual é a extensão dos danos aos recursos ou ativos?
* Quão eficaz é a estratégia?

Durante a contenção, podem ocorrer danos adicionais. Por exemplo, nem sempre é aconselhável desconectar o host comprometido da rede. O processo malicioso pode notar essa desconexão para o controlador CNC e acionar um apagamento de dados ou criptografia no destino. É aqui que a experiência e a experiência podem ajudar a conter um incidente além do escopo da estratégia de contenção.

**Evidência**

Durante um incidente, as provas devem ser recolhidas para resolvê-lo. Os elementos de prova também são importantes para a investigação posterior por parte das autoridades. Documentação clara e concisa sobre a preservação de evidências é fundamental. Para que as provas sejam admissíveis em tribunal, a recolha de provas deve estar em conformidade com regulamentos específicos. Após a coleta de evidências, ela deve ser devidamente contabilizada. Isso é conhecido como cadeia de custódia. Estes são alguns dos itens mais importantes para registrar ao documentar evidências usadas na cadeia de custódia:

* Localização da recuperação e armazenamento de todos os elementos de prova
* Quaisquer critérios de identificação para todas as evidências, como número de série, endereço MAC, nome de host ou endereço IP
* Informações de identificação para todas as pessoas que participaram da coleta ou manuseamento das evidências
* Hora e data em que a evidência foi coletada e em cada instância foi tratada

É vital educar qualquer pessoa envolvida no tratamento de evidências sobre como preservar as evidências adequadamente.

**Identificação do atacante**

A identificação de invasores é secundária à contenção, erradicação e recuperação de hosts e serviços. No entanto, a identificação de invasores minimizará o impacto em ativos e serviços comerciais críticos. Estas são algumas das ações mais importantes a serem executadas para tentar identificar um host atacante durante um incidente de segurança:

* Use bancos de dados de incidentes para pesquisar atividades relacionadas. Esse banco de dados pode ser interno ou localizado em organizações que coletam dados de outras organizações e os consolidam em bancos de dados incidentes, como o banco de dados da comunidade VERIS.
* Valide o endereço IP do invasor para determinar se ele é viável. O host pode ou não responder a um pedido de conectividade. Isso pode ser porque ele foi configurado para ignorar as solicitações ou o endereço já foi reatribuído a outro host.
* Use um mecanismo de busca na internet para obter informações adicionais sobre o ataque. Pode ter havido outra organização ou indivíduo que tenha liberado informações sobre um ataque a partir do endereço IP de origem identificado.
* Monitore os canais de comunicação que alguns atacantes usam, como o IRC. Como os usuários podem ser disfarçados ou anonimizados em canais de IRC, eles podem falar sobre suas façanhas nesses canais. Freqüentemente, as informações coletadas a partir desse tipo de monitoramento são enganosas e devem ser tratadas como pistas e não como fatos.

Erradicação, recuperação e remediação

Após a contenção, o primeiro passo para a erradicação é identificar todos os hospedeiros que precisam de correção. Todos os efeitos do incidente de segurança devem ser eliminados. Isso inclui infecções de malware e contas de usuário que foram comprometidas. Todas as vulnerabilidades que foram exploradas pelo invasor também devem ser corrigidas ou corrigidas para que o incidente não ocorra novamente.

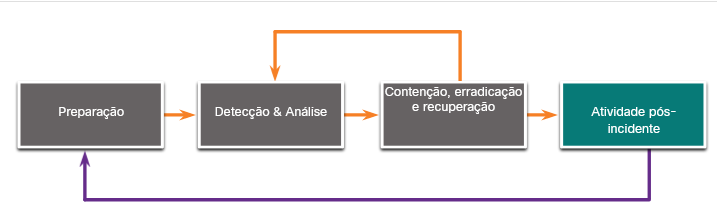
Para recuperar hosts, use backups limpos e recentes ou reconstrua-os com mídia de instalação se não houver backups disponíveis ou se eles tiverem sido comprometidos. Além disso, atualize e corrija totalmente os sistemas operacionais e o software instalado de todos os hosts. Altere todas as senhas de host e senhas para sistemas críticos de acordo com a política de segurança de senhas. Esse pode ser um bom momento para validar e atualizar a segurança da rede, as estratégias de backup e as políticas de segurança. Os atacantes freqüentemente atacam os sistemas novamente, ou usam um ataque semelhante para direcionar recursos adicionais, então não se esqueça de evitar isso da melhor forma possível. Concentre-se no que pode ser corrigido rapidamente enquanto prioriza sistemas e operações críticos.

28.4.8

## Atividades pós-incidente

As mesmas caixas da seção anterior são mostradas com a caixa de atividade pós-incidente destacada.

### Fase de atividade pós-incidente



PreparaçãoDetecção & AnáliseContenção, erradicação e recuperaçãoAtividade pós-incidente

Depois que as atividades de resposta a incidentes erradicaram as ameaças e a organização começou a se recuperar dos efeitos do ataque, é importante dar um passo atrás e periodicamente se reunir com todas as partes envolvidas para discutir os eventos que ocorreram e as ações de todos os indivíduos, enquanto Lidando com o incidente. Isso fornecerá uma plataforma para aprender o que foi feito corretamente, o que foi feito errado, o que poderia ser alterado e o que deve ser melhorado.

**Endurecimento baseado em lições**

Após um incidente importante ter sido tratado, a organização deve realizar uma reunião de “lições aprendidas” para analisar a eficácia do processo de manipulação de incidentes e identificar o fortalecimento necessário para controles e práticas de segurança existentes. Exemplos de boas perguntas a serem respondidas durante a reunião incluem o seguinte:

* Exatamente o que aconteceu, e quando?
* Quão bem a equipe e a gerência se comportaram ao lidar com o incidente?
* Os procedimentos documentados foram seguidos? Eram adequados?
* Quais informações foram necessárias antes?
* Foram tomadas quaisquer medidas ou medidas que possam ter inibido a recuperação?
* O que a equipe e a gerência fariam de forma diferente na próxima vez que ocorrer um incidente semelhante?
* Como o compartilhamento de informações com outras organizações pode ser aprimorado?
* Que medidas corretivas podem evitar incidentes semelhantes no futuro?
* Quais precursores ou indicadores devem ser observados no futuro para detectar incidentes semelhantes?
* Quais ferramentas ou recursos adicionais são necessários para detectar, analisar e mitigar incidentes futuros?

28.4.9

## Coleta e retenção de dados de incidentes

Ao realizar reuniões de “lições aprendidas”, os dados coletados podem ser usados para determinar o custo de um incidente por razões de orçamento, bem como para determinar a eficácia do CSIRT e identificar possíveis deficiências de segurança em todo o sistema. Os dados coletados precisam ser acionáveis. Colete apenas dados que possam ser usados para definir e refinar o processo de manipulação de incidentes.

Um maior número de incidentes tratados pode mostrar que algo na metodologia de resposta à incidência não está funcionando corretamente e precisa ser refinado. Poderia também mostrar incompetência no CSIRT. Um número menor de incidentes pode mostrar que a segurança da rede e do host foi melhorada. Também pode mostrar uma falta de detecção de incidentes. Contagens de incidentes separadas para cada tipo de incidente podem ser mais eficazes para mostrar pontos fortes e fracos do CSIRT e medidas de segurança implementadas. Essas subcategorias podem ajudar a direcionar onde reside uma fraqueza, em vez de se haver alguma fraqueza.

O tempo de cada incidente fornece informações sobre a quantidade total de mão-de-obra usada e o tempo total de cada fase do processo de resposta a incidentes. O tempo até a primeira resposta também é importante, bem como quanto tempo levou para relatar o incidente e encaminhá-lo para além da organização, se necessário.

É importante realizar uma avaliação objetiva de cada Incidente. A resposta a um incidente que foi resolvido pode ser analisada para determinar a sua eficácia. A Publicação Especial 800-61 do NIST fornece os seguintes exemplos de ativações realizadas durante uma avaliação objetiva de um incidente:

* Analisando logs, formulários, relatórios e outras documentações de incidentes para a adesão a políticas e procedimentos de resposta a incidentes estabelecidos.
* Identificando quais precursores e indicadores do incidente foram registrados para determinar com que eficácia o incidente foi registrado e identificado.
* Determinando se o incidente causou danos antes de ser detectado.
* Determinar se a causa real do incidente foi identificada e identificar o vetor de ataque, as vulnerabilidades exploradas e as características dos sistemas, redes e aplicativos alvo ou vitimizados.
* Determinando se o incidente é uma recorrência de um incidente anterior.
* Cálculo do dano monetário estimado do incidente (por exemplo, informações e processos comerciais críticos afetados negativamente pelo incidente).
* Medir a diferença entre a avaliação de impacto inicial e a avaliação de impacto final.
* Identificar quais medidas, se houver, poderiam ter evitado o incidente.
* A avaliação subjetiva de cada incidente exige que os membros da equipe de resposta a incidentes avaliem seu próprio desempenho, bem como o de outros membros da equipe e de toda a equipe. Outra fonte valiosa de entrada é o proprietário de um recurso que foi atacado, a fim de determinar se o proprietário acha que o incidente foi tratado de forma eficiente e se o resultado foi satisfatório.

Deve haver uma política em vigor em cada organização que descreva quanto tempo a evidência de um incidente é mantida. Muitas vezes, as provas são retidas durante muitos meses ou muitos anos após um incidente ter ocorrido. Em alguns casos, os regulamentos de conformidade podem exigir o período de retenção. Estes são alguns dos fatores determinantes para a retenção de evidências:

* **Promotoria** - Quando um atacante será processado por causa de um incidente de segurança, as provas devem ser mantidas até que todas as ações legais tenham sido concluídas. Isso pode ser vários meses ou muitos anos. Em ações judiciais, nenhuma evidência deve ser ignorada ou considerada insignificante. A política de uma organização pode declarar que qualquer evidência que envolva um incidente que tenha sido envolvido em ações legais nunca deve ser excluída ou destruída.
* **Tipo de Dados** - Uma organização pode especificar que tipos específicos de dados devem ser mantidos por um período de tempo específico. Itens como e-mail ou texto podem precisar ser mantidos apenas por 90 dias. Dados mais importantes, como os usados em uma resposta a incidentes (que não teve ação legal), podem precisar ser mantidos por três anos ou mais.
* **Custo** - Se houver muita mídia de hardware e armazenamento que precisa ser armazenada por um longo período de tempo, ela pode se tornar dispendiosa. Lembre-se também de que, à medida que a tecnologia muda, os dispositivos funcionais que podem usar hardware desatualizado e mídia de armazenamento também devem ser armazenados.

28.4.10

## Requisitos de relatórios e compartilhamento de informações

Os regulamentos governamentais devem ser consultados pela equipe jurídica para determinar com precisão a responsabilidade da organização em relatar o incidente. Além disso, o gerenciamento precisará determinar qual comunicação adicional é necessária com outras partes interessadas, como clientes, fornecedores, parceiros, etc.

Além dos requisitos legais e das considerações das partes interessadas, o NIST recomenda que uma organização coordene com as organizações para compartilhar detalhes sobre o incidente. Por exemplo, a organização poderia registrar o incidente no banco de dados da comunidade VERIS.

As recomendações críticas do NIST para o compartilhamento de informações são as seguintes:

* Planeje a coordenação de incidentes com partes externas antes que ocorram incidentes.
* Consulte o departamento jurídico antes de iniciar qualquer esforço de coordenação.
* Realizar 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.

Compartilhe o máximo possível de informações apropriadas sobre incidentes com outras organizações.

28.4.11

## Verifique sua compreensão - Identifique o termo de tratamento de incidentes

Parte superior do formulário

Responda às perguntas para identificar os termos de tratamento de incidentes.

1. Que termo é usado para um sinal de que um ator ameaça talvez esteja se preparando para atacar um ativo? Precursor
2. Qual termo é usado para o grupo de pessoas que fornecem serviços de resposta a incidentes a uma organização? CSIRT
3. Qual termo é usado para uma atividade limitada de tempo que é restrita a uma etapa específica em que um adversário ataca uma rede? Evento de segurança
4. O que é um sinal de que um evento de segurança de rede pode ter ocorrido ou está ocorrendo? Indicador
5. O que ocorreu quando há uma violação ou ameaça de violação de políticas de segurança? Incidente
6. Qual é o termo para um conjunto de políticas, planos e procedimentos projetados para lidar com violações de segurança cibernética? Capacidade de tratamento de incidentes

Um precursor é uma indicação de que um incidente de segurança de rede pode ocorrer.

Um CSIRT é uma equipe de pessoas que fornecem serviços de resposta a incidentes para uma organização.

Um evento de segurança é uma atividade vinculada ao tempo que faz parte de uma etapa específica de um ataque cibernético.

Um indicador é um sinal de que um evento de segurança de rede pode ter ocorrido ou está ocorrendo.

Ocorreu um incidente de segurança quando existe uma violação ou ameaça de violação de políticas de segurança.

Um conjunto de políticas, planos e procedimentos de resposta a incidentes definem o recurso de tratamento de incidentes de uma organização.

Parte inferior do formulário

28.4.12

## Laboratório - 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.

[28.3](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[O modelo Diamond de análise de intrusão](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

[28.5](https://contenthub.netacad.com/cyberops/26.0.1?lng=pt-br" \l "/cyberops/undefined.1)

# Análise forense digital e análise de incidentes e resumo de resposta

28.5.1

## O que aprendi neste módulo?

**Manuseio de evidências e atribuição de ataque**

A perícia digital é a recuperação e investigação de informações encontradas em dispositivos digitais no que diz respeito a atividades criminosas. Indicadores de comprometimento são a evidência de que ocorreu um incidente de segurança cibernética. É essencial que todos os indicadores de compromisso sejam preservados para análise futura e atribuição de ataques. Uma organização precisa desenvolver processos e procedimentos bem documentados para análise forense digital. NIST Special Publication 800-86 Guide to Integrating Forensic Techniques to Incident Response é um recurso valioso para organizações que precisam de orientação no desenvolvimento de planos forenses digitais. O processo forense inclui quatro etapas: coleta, exame, análise e relatórios. Em processos judiciais, as provas são geralmente classificadas como diretas ou indiretas. A evidência é ainda classificada como Melhor evidência (evidência que está em seu estado original), e evidência corroborante (evidência que sustenta uma afirmação que é desenvolvida a partir da melhor evidência). IETF RFC 3227 descreve uma ordem para a coleta de evidências digitais com base na volatilidade dos dados. A cadeia de custódia envolve a coleta, manuseio e armazenamento seguro de evidências.

Atribuição de ameaças refere-se ao ato de determinar o indivíduo, a organização ou a nação responsável por um incidente de invasão ou ataque bem-sucedido. A identificação dos intervenientes responsáveis pela ameaça deve ocorrer através da investigação sistemática e baseada em princípios dos elementos de prova. 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. Fontes de inteligência de ameaças podem ajudar a mapear o TTP identificado por uma investigação para fontes conhecidas de ataques semelhantes. 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. Uma maneira de atribuir um ataque é modelar o comportamento do ator de ameaça. O MITRE Táticas e técnicas adversas & Estrutura de Conhecimento Comum (ATT&CK) permite detectar táticas, técnicas e procedimentos do atacante (TTP) como parte da defesa contra ameaças e atribuição de ataques.

**A Cyber Kill Chain**

A Cyber Kill Chain foi desenvolvida para identificar e prevenir intrusões cibernéticas. Existem sete etapas para o Cyber Kill Chain. O foco nessas etapas ajuda os analistas a entender as técnicas, as ferramentas e os procedimentos dos atores de ameaças. Ao responder a um incidente de segurança, o objetivo é detectar e parar o ataque o mais cedo possível na progressão da cadeia de eliminação. Quanto mais cedo o ataque for interrompido; menos dano é feito e menos o atacante aprende sobre a rede de destino.

As etapas na Cyber Kill Chain são reconhecimento, armamento, entrega, exploração, instalação, comando e controle e ações sobre os objetivos. Reconhecimento é quando o ator ameaça realiza pesquisas, coleta inteligência e seleciona alvos. Isso informará o ator da ameaça se o ataque vale a pena executar. O objetivo do armamento é usar as informações do reconhecimento para desenvolver uma arma contra sistemas específicos ou indivíduos na organização. Durante a entrega, a arma é transmitida ao alvo usando um vetor de entrega. Depois que a arma foi entregue, o ator ameaça a usa para quebrar a vulnerabilidade e ganhar o controle do alvo. A instalação ocorre quando o agente da ameaça estabelece um backdoor no sistema para permitir o acesso contínuo ao destino. Para preservar esse backdoor, é importante que o acesso remoto não alerte analistas ou usuários de segurança cibernética. Command and Control, ou CNC, estabelece o controle do agente de ameaça sobre o sistema de destino. Os canais CNC são usados pelo ator de ameaças para emitir comandos para o software que eles instalaram no destino. Ações sobre Objetivos descreve o agente da ameaça que alcança seu objetivo original. Isso pode ser roubo de dados, realizar um ataque DDoS ou usar a rede comprometida para criar e enviar spam ou mina Bitcoin.

**O Modelo Diamond de Análise de Intrusão**

O Modelo Diamond de Análise de Intrusão representa um incidente ou evento de segurança. Um evento é uma atividade limitada ao tempo que é restrita a uma etapa específica em que um adversário usa uma capacidade sobre a infraestrutura para atacar uma vítima para alcançar um resultado específico. As quatro características principais de um evento de intrusão são adversário (as partes responsáveis pela intrusão), capacidade (a ferramenta ou técnica usada para atacar a vítima), infraestrutura (o caminho da rede ou caminhos usados para estabelecer e manter o CNC) e vítima (o alvo do ataque). Os meta-recursos, que expandem ligeiramente o modelo, incluem Timestamp, Fase, Resultado, Direção, Metodologia e Recursos (um ou mais recursos externos usados pelo adversário para o evento de intrusão).

Como analista de segurança cibernética, você pode ser chamado a usar o Modelo Diamond de Análise de Intrusão para diagramar uma série de eventos de intrusão. Os adversários não operam em apenas um evento. Em vez disso, os eventos são encadeados em uma cadeia na qual cada evento deve ser concluído com êxito antes do próximo evento. Esse segmento de eventos pode ser mapeado para a Cyber Kill Chain.

**Resposta a incidentes**

A resposta a incidentes envolve os métodos, políticas e procedimentos usados por uma organização para responder a um ataque cibernético. Os objetivos da resposta a incidentes são limitar o impacto do ataque, avaliar os danos causados e implementar procedimentos de recuperação. É essencial que as organizações criem e mantenham planos detalhados de resposta a incidentes e designem pessoal responsável pela execução de todos os aspectos desse plano. As recomendações do NIST (National Institute of Standards and Technology, Instituto Nacional de Padrões e Tecnologia) dos EUA para resposta a incidentes estão detalhadas em sua Publicação Especial 800-61, revisão 2, intitulada “Guia de Tratamento de Incidentes de Segurança

O primeiro passo para uma organização é estabelecer uma capacidade de resposta a incidentes de segurança de computador (CSIRC). O NIST recomenda a criação de políticas (detalhando como os incidentes são tratados), planos (definição clara de tarefas e responsabilidades) e procedimentos (ações específicas a serem tomadas) para estabelecer e manter um CSIRC. Outros grupos e indivíduos dentro da organização também podem estar envolvidos com o tratamento de incidentes. Sua experiência e habilidades podem ajudar a equipe de resposta a incidentes de segurança informática (CSIRT) a lidar com o incidente de forma rápida e correta. Algumas das partes interessadas incluem gerenciamento, garantia de informações, suporte de TI, departamento jurídico, relações públicas e mídia, recursos humanos, planejadores de continuidade de negócios, segurança física e gerenciamento de instalações. Os regulamentos governamentais devem ser consultados pela equipe jurídica para determinar a responsabilidade da organização por relatar o incidente. Além dos requisitos legais e das considerações das partes interessadas, o NIST recomenda que uma organização coordene com as organizações para compartilhar detalhes sobre o incidente. Deve haver uma política em vigor em cada organização que descreva quanto tempo a evidência de um incidente é mantida.

A estrutura de Certificação de Modelo de Maturidade de Segurança Cibernética (CMMC) foi criada para avaliar a capacidade das organizações que desempenham funções para o Departamento de Defesa dos EUA (DoD) para proteger a cadeia de suprimentos militar contra interrupções ou perdas devido a incidentes de segurança cibernética. O CMMC especifica 17 domínios, cada um dos quais tem um número variável de recursos que estão associados a ele. A organização é classificada pelo nível de maturidade que foi alcançado para cada um dos domínios. O CMMC certifica organizações por nível.

O NIST define quatro etapas no ciclo de vida do processo de resposta a incidentes: Preparação, Detecção e Análise, Contenção, Erradicação e Recuperação e Atividades Pós-Incidentes. O ciclo de vida de resposta a incidentes destina-se a ser um processo de aprendizagem auto-reforçado, pelo qual cada incidente informa o processo para lidar com incidentes futuros. A fase de preparação é quando o CSIRT é criado e treinado. Essa fase também é quando as ferramentas e ativos que serão necessários pela equipe para investigar incidentes são adquiridos e implantados. Os incidentes são detectados de muitas maneiras diferentes e nem todas essas formas são muito detalhadas ou fornecem clareza detalhada. Existem duas categorias para os sinais de um incidente: Precursor (um incidente pode acontecer no futuro) e Indicador (um incidente aconteceu ou está acontecendo). O uso de algoritmos complexos e aprendizado de máquina muitas vezes ajudam a determinar a validade de incidentes de segurança. Um método que pode ser usado é a criação de perfis de rede e sistema.

Quando o CSIRT acredita que um incidente ocorreu, ele deve executar imediatamente uma análise inicial para determinar o escopo do incidente, como quais redes, sistemas ou aplicativos são afetados, quem ou o que originou o incidente e como o incidente está ocorrendo. Quando um incidente é analisado e priorizado, a equipe de resposta a incidentes precisa notificar as partes interessadas e externas apropriadas para que todos os que precisam estar envolvidos desempenhem suas funções. Documentação clara e concisa sobre a preservação de evidências é fundamental. A identificação de invasores é secundária à contenção, erradicação e recuperação de hosts e serviços. Após a contenção, o primeiro passo para a erradicação é identificar todos os hospedeiros que precisam de correção. Todos os efeitos do incidente de segurança devem ser eliminados. Todas as vulnerabilidades que foram exploradas pelo invasor também devem ser corrigidas ou corrigidas para que o incidente não ocorra novamente. Após um incidente importante ter sido tratado, a organização deve realizar uma reunião de “lições aprendidas” para analisar a eficácia do processo de manipulação de incidentes e identificar o fortalecimento necessário para controles e práticas de segurança existentes.

28.5.2

## Módulo 26: Avaliação de Alertas Questionário

Parte superior do formulário

1. Para garantir que a cadeia de custódia seja mantida, quais três itens devem ser registrados sobre evidências coletadas e analisadas após um incidente de segurança ter ocorrido? (Escolha três.)

Hora e data em que a evidencia foi coletada

Números de serie e nome de hosts dos dispositivos usados como evidencia

Localização de todas as provas

1. Um ator de ameaça ganhou acesso administrativo a um sistema e alcançou o objetivo de controlar o sistema para um futuro ataque DDoS através do estabelecimento de um canal de comunicação com um CNC de propriedade do ator ameaça. Qual fase do modelo Cyber Kill Chain descreve a situação?

Ação nos objetivos

1. Qual elemento de meta-feição no Modelo Diamond descreve ferramentas e informações (como software, base de conhecimento black hat, nome de usuário e senha) que o adversário usa para o evento de intrusão?

Recursos

1. Qual ação deve ser incluída em um elemento de plano que faz parte de uma capacidade de resposta a incidentes de segurança do computador (CSIRC)?

Desenvolva métricas para medir a capacidade de resposta a incidentes e sua eficacia

1. Quais duas ações podem ajudar a identificar um host atacante durante um incidente de segurança? (Escolha duas.)

Valide o endereço ip do ator da ameaça para determinar se ele é viável

Use um mecanismo de pesquisa da internet para obter informações adicionais sobre o ataque

1. O que é uma estrutura MITRE ATT&CK?

Uma base de conhecimento do comportamento do ator de ameaça

1. De acordo com o NIST, qual etapa no processo de perícia digital envolve a identificação de potenciais fontes de dados forenses, sua aquisição, manuseio e armazenamento?

Coleta

1. Ao lidar com ameaças de segurança e usar o modelo Cyber Kill Chain, quais duas abordagens uma organização pode usar para ajudar a bloquear possíveis explorações de um sistema? (Escolha duas.)

Pontos finais de auditoria para determinar forensicamente a origem da exploração

Realizar treinamento de conscientização dos funcionários e testes de e-mail

1. Qual termo é usado no Modelo Diamond de intrusão para descrever uma ferramenta que um ator ameaça usa em direção a um sistema alvo?

Capacidade

1. Qual é o objetivo do elemento de política em um recurso de resposta a incidentes de segurança de computador de uma organização, conforme recomendado pelo NIST?

Ele detalha como os incidentes devem ser tratados com base na missão organizacional e funções

1. De acordo com o NIST, qual etapa no processo de perícia digital envolve a extração de informações relevantes dos dados?

Análise

1. Qual declaração descreve a Cyber Kill Chain ?

Identifica os passos que os adversários devem completar para alcançar seus objetivos

1. Depois de conter um incidente que infectou as estações de trabalho do usuário com malware, quais são os três procedimentos de correção eficazes que uma organização pode tomar para erradicação? (Escolha três.)

Reconstrua hosts com mídia de instalação se não houver backups disponíveis;

Use backups limpos e recentes para recuperar hosts

Atualize e corrija o sistema operacional e o software instalado de todos os hosts

1. Depois que um ator de ameaça concluir uma varredura de porta do servidor web público de uma organização e identificar uma vulnerabilidade potencial, qual é a próxima fase para o ator de ameaça para preparar e iniciar um ataque conforme definido na Cyber Kill Chain?

Armamento

1. Qual tarefa descreve a atribuição de ameaças?

Determinar quem é responsável pelo ataque

# Prepare-se para o exame e inicie sua carreira!

28.6.1

## Preparação para Certificação e Cupons de Desconto



**Parabéns!** Você concluiu seu curso Cisco Networking Academy! **Voucher de desconto**

Um voucher de desconto para o exame de certificação está disponível após você ter concluído o curso CyberOps Associate 1.0 (CA).

Se você obteve uma pontuação de 70% ou superior na **PRIMEIRA** tentativa do **Exame final CA**, e ter um "Aprovado" no cadeno de notas, então você está qualificado para um voucher de desconto para um exame de certificação Cisco.

Quando você se qualifica para um desconto de exame de certificação (voucher), um link será exibido na aula no NetAcad.com e no perfil do NetAcad.com.

* [Certification Advice and Overview](https://www.netacad.com/careers/career-advice/certification-advice)
* [Certification Exam Voucher FAQs](https://www.netacad.com/portal/faq-page)
* [Cisco Certifications Exams & Discount Vouchers](https://www.netacad.com/portal/resources/cisco-certifications-and-vouchers)

Materiais de estudo**adicionais para preparação**de certificação

Acesse materiais de estudo adicionais ou assista a webinars gratuitos do Learning @Cisco.

O registro é gratuito. Use seu login NetaCAD ou, se você já tiver feito um exame de certificação Cisco, use seu login cisco.com. Quando você estiver logado, use os links abaixo para obter informações para sua certificação.

* [Exam Topics](https://learningnetwork.cisco.com/s/cbrops-exam-topics)
* [Study Materials](https://learningnetwork.cisco.com/s/learning-plan-detail-standard?ltui__urlRecordId=a1c3i00000061LXAAY&ltui__urlRedirect=learning-plan-detail-standard)

28.6.2

## Recursos de carreira e oportunidades de emprego

**Prepare-se para uma carreira em tecnologia!**

Você está no caminho para uma carreira de tecnologia recompensal, mas você perguntou o que precisa fazer para estar pronto para o local de trabalho?

Fornecemos recursos valiosos de carreira para ajudá-lo a se preparar para fazer parte da força de trabalho e a procurar emprego com sucesso. Esses recursos foram criados para ajudá-lo, como aluno Networking Academy, bem-sucedido em uma carreira técnica. Se você está procurando orientação profissional, oportunidades de aprendizagem virtual e acesso a um mecanismo de correspondência exclusivo para procurar emprego, temos exatamente o que você precisa. Marque esses três links e comece a aumentar seu potencial hoje:

* [Employment Opportunities](https://www.netacad.com/careers/employment-opportunities)
* [Webinars](https://www.netacad.com/careers/webinars)
* [Career Advice](https://www.netacad.com/careers/career-advice)



**Encontre e candidate-se a vagas usando o Talent Bridge Matching Engine!**

Nosso [Matching Engine](http://bit.ly/nac2career) é a ferramenta de correspondência de empregos exclusiva da Networking Academy. O Matching Engine usa os dados do perfil do Networking Academy para exibir posições relevantes para as quais você se qualifica. Adicione certificações, experiência profissional e localização geográfica ao seu perfil para que os empregadores possam encontrá-lo. Em seguida, inscreva-se em trabalhos que lhe interessam, diretamente no painel do Matching Engine.

Mesmo que você não esteja procurando emprego, você pode começar a construir seu perfil e ver o que os empregadores estão procurando em candidatos a emprego.

[Cadastre-se e comece hoje mesmo] (<https://www.netacad.com/jobmatching>)

**Crie sua rede profissional!**

Independentemente de onde você está em sua jornada, você deve começar a construir sua rede profissional. Começe adicionando [Cisco Networking Academy](https://www.linkedin.com/school/cisco-networking-academy1/) na sua seção de educação em seu perfil do LinkedIn. Você terá acesso aos conselhos de carreira mais recentes, oportunidades de emprego, bem como ser mais facilmente encontrado por empregadores que buscam estudantes qualificados da Networking Academy para se juntarem à sua equipe.

Parte inferior do formulário