

CYBER **SECURITY**

11

Dados de Segurança de Rede

Alex Sandro da Silva Feitosa

Resumo

Nessa aula iniciaremos com a memorização de quem são os atores de ameaças, amadores, hacktivistas, grupos do crime organizado, patrocinados pelo Estado e grupos terroristas, entre outros. Abordaremos sobre o Sistema Operacional Windows, Linux, e protocolos e conectividade das redes.

1.1. Tipos de dados de Segurança

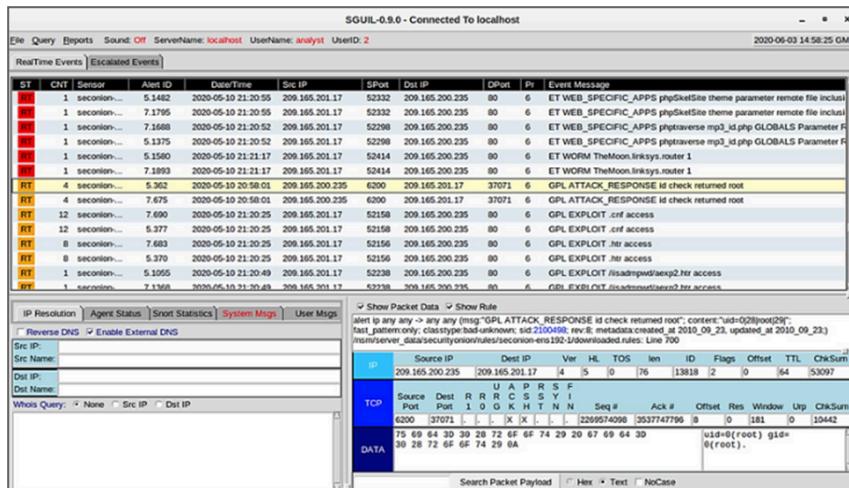
1.1.1 Dados de Alerta

Os dados de alerta consistem em mensagens geradas por sistemas de prevenção de intrusão (IPSs) ou sistemas de detecção de intrusão (IDSs) em resposta ao tráfego que viola uma regra ou corresponde à assinatura de um exploit conhecido.

Um IDS de rede (NIDS), como o Snort, vem configurado com regras para exploits conhecidos.

Os alertas são gerados pelo Snort e podem ser lidos e pesquisados pelos aplicativos Sguil e Squirt, que fazem parte do pacote Security Onion de ferramentas NSM.

Figura 1.1 Console Sguil mostrando alerta de teste do Snort IDS



Fonte: CCNA Cyber OPS Associate v1, 2020.

1.1.1.1 Dados de sessão e transação

Os dados da sessão são um registro de uma conversa entre dois pontos de extremidade da rede.

Inclui as cinco tuplas de endereços IP de origem e destino, números de porta de origem e destino e o código IP do protocolo em uso.

Os dados sobre a sessão incluem um ID de sessão, a quantidade de dados transferidos por origem e destino e informações relacionadas à duração da sessão.

A figura mostra uma saída parcial para três sessões HTTP de um log de conexão Zeek.

Figura 1.1 Saída parcial para três sessões HTTP de um log de conexão

1	2	3	4	5	6	7	8	9	10	11	12	13
ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	orig_pkts	resp_pkts
1320279567 CEv1Z54N5gT3PwJLog	192.168.2.76	52034	174.129.249.33		80	tcp	http	0.082899	389	1495	5	4
1320279567 Cl6Ueb3SkSJhWASNN4	192.168.2.76	52035	184.72.234.3		80	tcp	http	2.56194	905	731	9	8
1320279567 CaTMSv1Sb8HFunqj	192.168.2.76	52033	184.72.234.3		80	tcp	http	3.345539	1856	1445	15	13

1. ts: session start timestamp
 2. uid: unique session ID
 3. id.orig_h: IP address of host that originated the session (source address)
 4. id.orig_p: protocol port for the originating host (source port)
 5. id.resp_h: IP address of host responding to the originating host (destination address)
 6. id.resp_p: protocol of responding host (destination port)
 7. proto: transport layer protocol for session
 8. service: application layer protocol
 9. duration: duration of the session
 10. orig_bytes: bytes from originating host
 11. resp_bytes: bytes from responding host
 12. orig_pkts: packets from the originating host
 13. resp_pkts: packets from responding host

Fonte: CCNA Cyber OPS Associate v1, 2020.

Os dados de transação consistem nas mensagens que são trocadas durante as sessões de rede.

Essas transações podem ser visualizadas em transcrições de captura de pacotes.

As transações que representam as solicitações e respostas seriam registradas em um log de acesso em um servidor ou por um NIDS como Zeek.

Uma sessão pode incluir o download de conteúdo de um servidor da web,

1.1.2 Logs dos dispositivos finais

Logs de host: Os sistemas de detecção de intrusão baseados em host (HIDS) são executados em hosts individuais.

Muitas proteções baseadas em host enviam logs para servidores de gerenciamento de log centralizados que podem ser pesquisados de um local central usando ferramentas NSM.

Os logs de host do Microsoft Windows são visíveis localmente por meio do Visualizador de eventos. O Visualizador de eventos mantém quatro tipos de registros:

Logs de aplicativos: Contém eventos registrados por vários aplicativos.

Logs do sistema: Incluem eventos relacionados à operação de drivers, processos e hardware.

Logs de instalação: Registram informações sobre a instalação do software, incluindo atualizações do Windows.

Logs de segurança: Registram eventos relacionados à segurança, como tentativas de logon e operações relacionadas ao gerenciamento e acesso de arquivos ou objetos.

Logs de linha de comando: Os invasores que obtiveram acesso a um sistema e alguns tipos de malware executam comandos a partir da interface de linha de comando (CLI) em vez de uma GUI. A execução da linha de comando de registro fornecerá visibilidade sobre esse tipo de incidente.

Erro: É um evento que indica um problema significativo, como perda de dados ou funcionalidade. Por exemplo, se um serviço falhar ao carregar durante a inicialização, um evento de erro será registrado.

Aviso: É um evento que não é necessariamente significativo, mas pode indicar um possível problema futuro. Por exemplo, quando há pouco espaço em disco, um evento de aviso é registrado. Se um aplicativo se recuperar de um evento sem perda de funcionalidade ou dados, ele pode classificar o evento como um evento de aviso.

Informação: Ele descreve a operação bem-sucedida de um aplicativo, driver ou serviço. Por exemplo, quando um driver de rede é carregado com êxito, pode ser apropriado registrar um evento de informação. Observe que geralmente é impróprio para um aplicativo de desktop registrar um evento cada vez que é iniciado.

Auditoria de sucesso: É um evento que registra uma tentativa de acesso de segurança auditada com êxito. Por exemplo, a tentativa bem-sucedida de um usuário de fazer logon no sistema é um evento de auditoria bem-sucedido.

Auditoria de Falhas: É um evento que registra uma tentativa de acesso de segurança auditada que falhou. Por exemplo, se um usuário tentar acessar uma unidade de rede e falhar, a tentativa será registrada como um evento de auditoria de falha.

Syslog

O Syslog inclui especificações para formatos de mensagem, uma estrutura de aplicativo cliente-servidor e protocolo de rede. É um protocolo cliente / servidor.

Muitos tipos diferentes de dispositivos de rede podem ser configurados para usar o padrão syslog para registrar eventos em servidores syslog centralizados.

O formato completo de uma mensagem Syslog possui três partes distintas: PRI (prioridade), HEADER, MSG (texto da mensagem).

O PRI consiste em dois elementos, a facilidade e a gravidade da mensagem, que são valores inteiros.

O recurso consiste em fontes que geraram a mensagem, como o sistema, processo ou aplicativo.

A Gravidade é um valor de 0 a 7 que define a gravidade da mensagem.

Instalação

Códigos de instalações entre 15 e 23 (local0-local7) não são atribuídos a uma palavra-chave ou nome.

Eles podem ser atribuídos a diferentes significados, dependendo do contexto de uso. Além disso, vários sistemas operacionais foram encontrados para utilizar os recursos 9 e 15 para mensagens de relógio.

Gravidade

0 = Emergência : o sistema está inutilizável

1 = Alerta : a ação deve ser tomada imediatamente

2 = Crítico : condições críticas que devem ser corrigidas imediatamente e indicam falha em um sistema

3 = Erro : uma falha que não é urgente, deve ser resolvida em um determinado tempo

4 = Aviso : atualmente não existe um erro; mas, um erro ocorrerá no futuro se a condição não for tratada

5 = Aviso : um evento que não é um erro, mas que é considerado incomum. Não requer ação imediata.

6 = Informativo : mensagens emitidas sobre o funcionamento normal

7 = Depurar : mensagens de interesse para desenvolvedores

Prioridade

O valor de Prioridade (PRI) é calculado multiplicando o valor da Instalação por 8 e, em seguida, adicionando-o ao valor de Severidade, conforme mostrado abaixo.

$$\text{Prioridade} = (\text{Instalação} * 8) + \text{Gravidade}$$

O valor de Prioridade é o primeiro valor em um pacote e ocorre entre colchetes <>.

Logs do servidor

Os logs do servidor são uma fonte essencial de dados para o monitoramento da segurança da rede.

Os registros do servidor proxy DNS que documentam todas as consultas e respostas DNS que ocorrem na rede são especialmente importantes.

Dois arquivos de log importantes são os logs de acesso do servidor da web Apache e os logs de acesso do Microsoft Internet Information Server (IIS).

Figura 1.2 Log Apache

```
203.0.113.127 - dsmith [10/Oct/2016:10:26:57 - 0500] "GET /logo_sm.gif HTTP/1.0" 200 2254
""http://www.example.com/links.html"" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101
Firefox/47.0"
```

Fonte: CCNA Cyber OPS Associate v1, 2020.

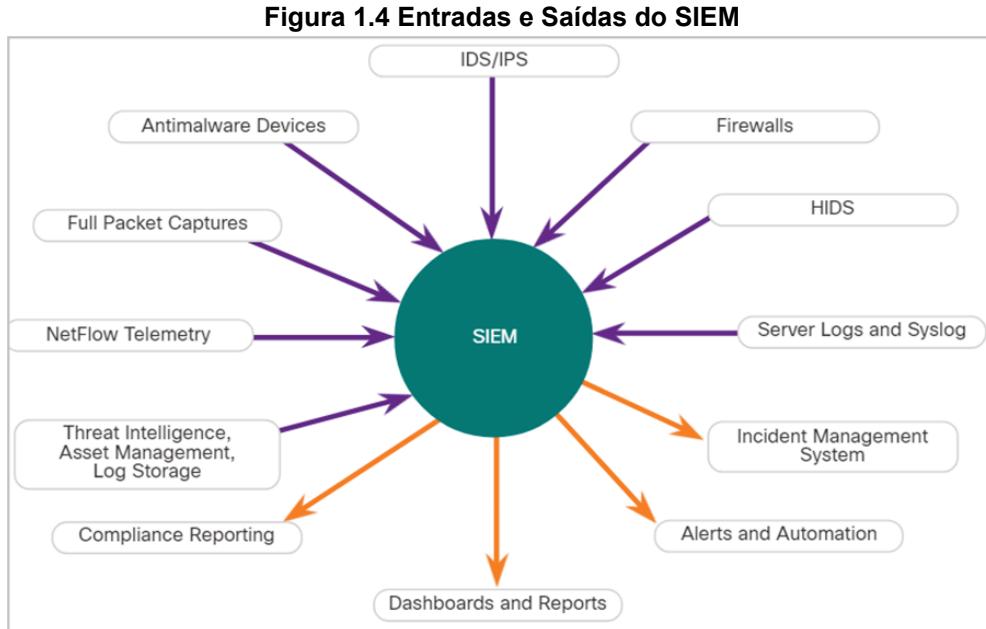
Figura 1.3 Log IIS

```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321,
159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0),
-, http://www.example.com
```

Fonte: CCNA Cyber OPS Associate v1, 2020.

SIEM e coleta de log

A tecnologia de gerenciamento de eventos e informações de segurança (SIEM) é usada em muitas organizações para fornecer relatórios em tempo real e análises de longo prazo de eventos de segurança, conforme mostrado na figura.



Fonte: CCNA Cyber OPS Associate v1, 2020.

O SIEM combina as funções essenciais das ferramentas SEM e SIM para fornecer uma visão da rede corporativa usando as seguintes funções:

Coleta de logs: registros de eventos de fontes em toda a organização fornecem informações forenses importantes e ajudam a atender aos requisitos de relatórios de conformidade.

Normalização: mapeia mensagens de log de diferentes sistemas em um modelo de dados comum, permitindo que a organização conecte e analise eventos relacionados, mesmo se eles forem inicialmente registrados em formatos de origem diferentes.

Correlação: conecta registros e eventos de sistemas ou aplicativos distintos, acelerando a detecção e a reação a ameaças à segurança.

Agregação: reduz o volume de dados de eventos consolidando registros de eventos duplicados.

Relatórios: Apresenta os dados de eventos agregados e correlacionados em monitoramento em tempo real e resumos de longo prazo, incluindo painéis gráficos interativos.

Conformidade: Este é um relatório para satisfazer os requisitos de vários regulamentos de conformidade.

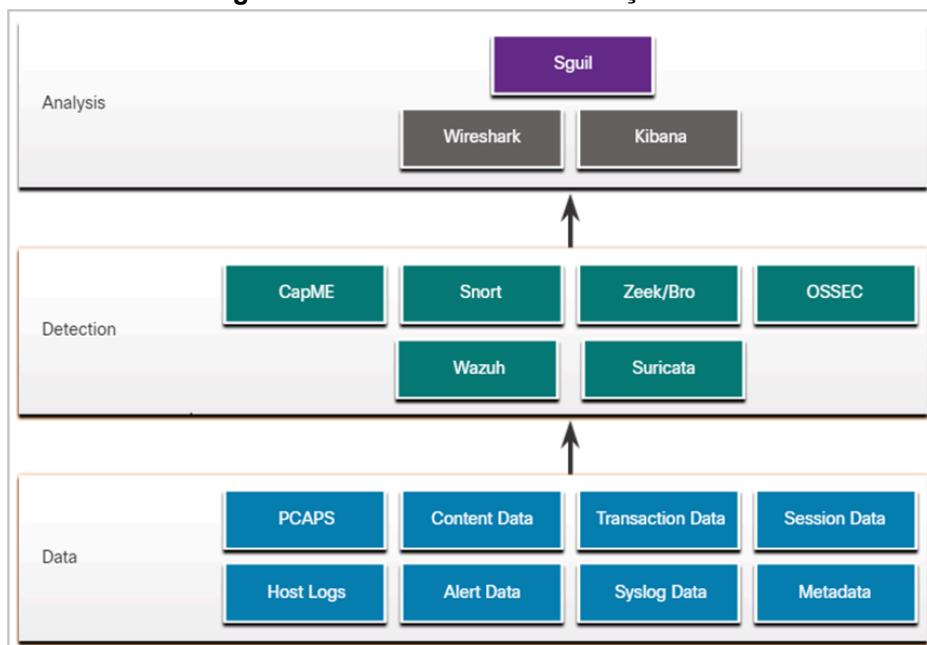
1.1.3 Visão geral da avaliação de alertas

Ferramentas de detecção para coletar dados de alerta

O Security Onion contém muitos componentes. É um ambiente integrado projetado para simplificar a implantação de uma solução NSM abrangente.

A figura ilustra a maneira como os componentes do Security Onion funcionam juntos.

Figura 1.5 Estrutura de uma solução NSM



Fonte: CCNA Cyber OPS Associate v1, 2020.

O cenário de ameaças muda constantemente à medida que novas vulnerabilidades e ameaças são descobertas. Conforme as necessidades do usuário e da organização mudam, também muda a superfície de ataque.

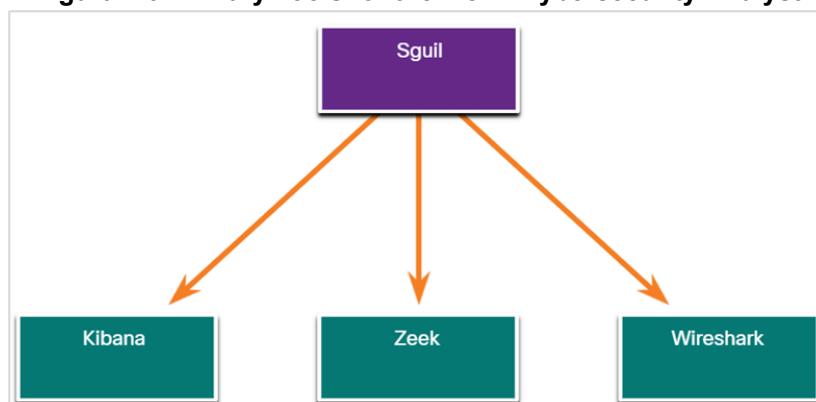
Os agentes de ameaças aprenderam como variar rapidamente os recursos de seus exploits para evitar a detecção.

É melhor ter alertas que às vezes são gerados por tráfego inocente do que regras que ignoram o tráfego malicioso.

É necessário que analistas de segurança cibernética qualificados investiguem alertas para determinar se uma exploração realmente ocorreu.

Os analistas de segurança cibernética de Nível 1 trabalharão por meio de filas de alertas em uma ferramenta como Sguil, alternando para ferramentas como Zeek, Wireshark e Kibana para verificar se um alerta representa uma exploração real.

Figura 1.6 Primary Tools for the Tier 1 Cybersecurity Analyst



Fonte: CCNA Cyber OPS Associate v1, 2020.

Os incidentes de segurança são classificados usando um esquema emprestado de diagnósticos médicos. Este esquema de classificação é usado para orientar as ações e avaliar os procedimentos de diagnóstico. A preocupação é que ambos os diagnósticos podem ser precisos, ou verdadeiros, ou imprecisos ou falsos.

Na análise de segurança de rede, o analista de segurança cibernética recebe um alerta. O analista de segurança cibernética precisa determinar se esse diagnóstico é verdadeiro.

Os alertas podem ser classificados da seguinte forma:

Verdadeiro positivo: o alerta foi verificado como 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 chamada de gatilho benigno.

Uma situação alternativa é que nenhum alerta 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:

Tabela 1.1 Classificações possíveis

	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

Fonte: do autor, 2022.

Os verdadeiros positivos são o tipo de alerta desejado. Eles significam que as regras que geram alertas funcionaram corretamente.

Falsos positivos não são desejáveis. Embora não indiquem que ocorreu uma exploração não detectada, eles são caros porque os analistas de segurança cibernética devem investigar alarmes falsos.

Negativos verdadeiros são desejáveis. Eles indicam que o tráfego normal benigno é ignorado corretamente e os alertas errados não estão sendo emitidos.

Falsos negativos são perigosos. Eles indicam que os exploits não estão sendo detectados pelos sistemas de segurança existentes..

Nota: Eventos “verdadeiros” são desejáveis. Eventos “falsos” são indesejáveis e potencialmente perigosos.

Eventos benignos são aqueles que não devem disparar alertas. O excesso de eventos benignos indica que algumas regras ou outros detectores precisam ser melhorados ou eliminados.

Quando há suspeita de verdadeiros positivos, um analista de segurança cibernética é necessário para escalar o alerta para um nível superior para investigação. O investigador irá prosseguir com a investigação a fim de confirmar o incidente e identificar qualquer dano potencial que possa ter sido causado.

Um analista de segurança cibernética também pode ser responsável por informar ao pessoal de segurança que falsos positivos estão ocorrendo a ponto de afetar seriamente o tempo do analista de segurança cibernética.

Falsos negativos podem ser descobertos bem após a ocorrência de uma exploração. Isso pode acontecer por meio de análise de segurança retrospectiva (RSA). RSA pode ocorrer quando regras recém-obtidas ou outra inteligência contra ameaças é aplicada aos dados de segurança de rede arquivados.

Por esse motivo, é importante monitorar a inteligência de ameaças para aprender sobre novas vulnerabilidades e explorações e para avaliar a probabilidade de que a rede estava vulnerável a eles em algum momento no passado.

Análise Determinística e Análise Probabilística

A análise determinística avalia o risco com base no que se sabe sobre uma vulnerabilidade. 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 em uma exploração tiver sido concluída com êxito, a próxima etapa também será bem-sucedida.

Em uma análise determinística, todas as informações para realizar uma exploração são consideradas conhecidas.

Na análise probabilística, assume-se que os números das portas que serão usados só podem ser previstos com algum grau de confiança.

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 ocorra com base na probabilidade de que cada etapa da exploração seja bem-sucedida.

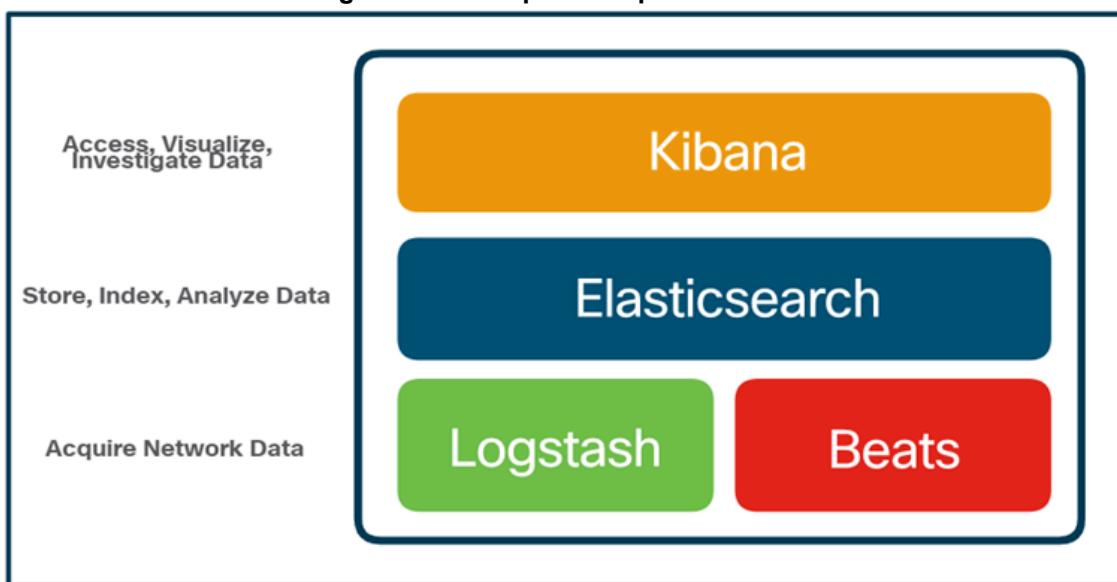
1.1.4 Uma plataforma de dados comum

O Security Onion inclui o Elastic Stack que consiste em Elasticsearch, Logstash e Kibana (ELK).

Componentes Principais do ELK:

- Elasticsearch: uma plataforma de núcleo aberto para pesquisar e analisar os dados de uma organização em tempo quase real.
- Logstash: permite a coleta e a normalização de dados de rede em índices de dados que podem ser pesquisados com eficiência pelo Elasticsearch.
- Kibana: Fornece uma interface gráfica para dados compilados pelo Elasticsearch.
- Beats: Série de plugins de software que enviam diferentes tipos de dados para os armazenamentos de dados do Elasticsearch.

Figura 1.7 Principais componentes ELK

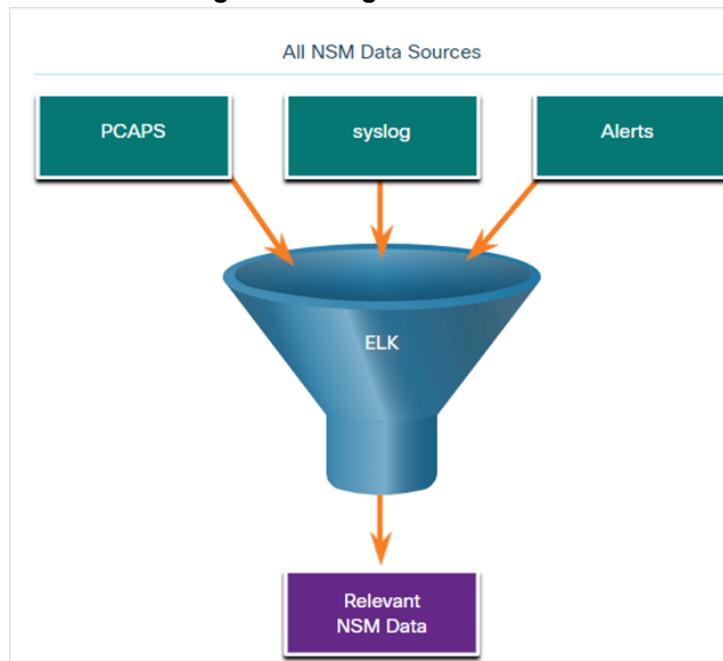


Fonte: CCNA Cyber OPS Associate v1, 2020.

Para reduzir os dados, é essencial identificar os dados de rede que devem ser coletados e armazenados para reduzir a carga sobre os sistemas.

Ao limitar o volume de dados, ferramentas como o Elasticsearch serão muito mais úteis.

Figura 1.8 Origem dos dados



Fonte: CCNA Cyber OPS Associate v1, 2020.

Normalização de dados é o processo de combinar dados de várias fontes em um formato comum.

Um esquema comum especificará os nomes e formatos para os campos de dados necessários.

Por exemplo, endereços IPv6, endereços MAC e data e hora podem ser representados em formatos variados:

Tabela 1.2 Representação de endereços IPv6, MAC e data e hora

Formatos de endereço IPv6	Formatos Mac	Formatos de Data
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Segunda-feira, 24 de Julho de 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Seg, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0: 33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

Fonte: do autor, 2022.

A normalização de dados também é necessária para simplificar a pesquisa de eventos correlacionados.

Arquivamento de Dados

A retenção de dados do Network Security Monitoring (NSM) indefinidamente não é viável devido a problemas de armazenamento e acesso.

O período de retenção para certos tipos de informações de segurança de rede pode ser especificado pelas estruturas de conformidade.

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

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.

Referências

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

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

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

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

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

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

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

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