



# Módulo 27: Trabalho com dados de segurança de rede



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@edu.sc.senai.br](mailto:clemilson.oliveira@edu.sc.senai.br)

# Objetivos do módulo

**Título do Módulo :** Trabalho com dados de segurança de rede

**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.

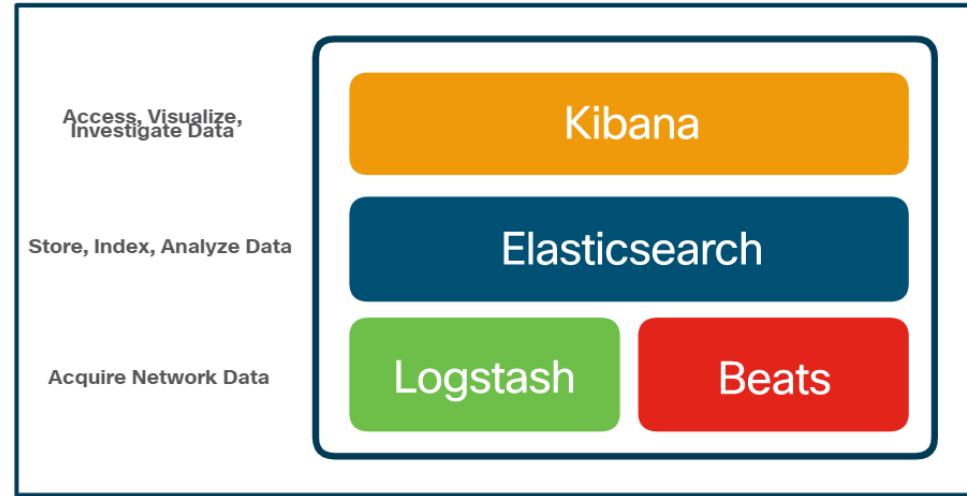
# 27.1 Uma plataforma de dados comum

# ELK

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

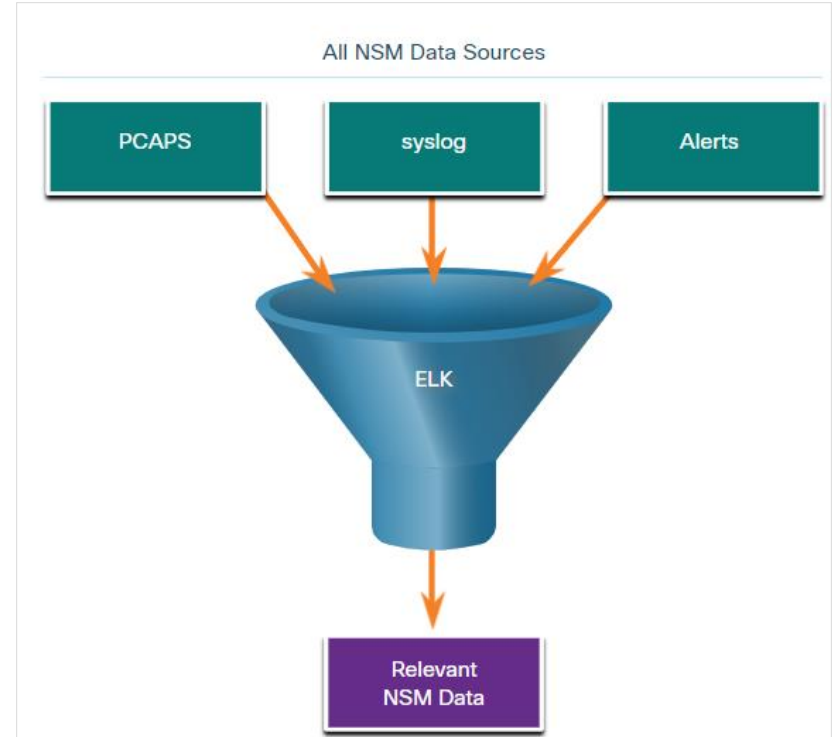
## Componentes Principais do ELK:

- **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.



## Redução de dados

- 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.



# Uma normalização de dados comum da plataforma dedados

- 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:

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

- 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.*

# Um laboratório de plataforma de dados comum - Converta dados em um formato universal

Neste laboratório, você completará os seguintes objetivos:

- **Parte 1:** Use ferramentas de linha de comando para normalizar manualmente as entradas de log.
- **Parte 2:** O campo de carimbo de data/hora deve ser normalizado.
- **Parte 3:** O campo IPv6 requer normalização.



## 27.2 Investigação dos dados de rede

# Investigando Dados de Rede Trabalhando em Sguil

- 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 entender o que está acontecendo na rede, pode ser útil classificar a coluna **CNT** para exibir os alertas com a frequência mais alta.

The screenshot shows the Sguil 0.9.0 interface. The top bar indicates 'Connected To localhost' and shows the user 'analyst' with ID 2. The main window displays a list of alerts with columns: ST, CNT, Sensor, Alert ID, DateTime, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The alerts are sorted by CNT (frequency). The first alert has CNT 881 and is a 'GPL ICMP\_INFO PING \*NIX' event. The second alert has CNT 296 and is a 'ET WEB\_SERVER Script tag in URI Possible Cross Site Scripting Atte...' event. The third alert has CNT 296 and is a 'ET WEB\_SERVER Script tag in URI Possible Cross Site Scripting Atte...' event. The fourth alert has CNT 252 and is a 'GPL ICMP\_INFO PING \*NIX' event. The fifth alert has CNT 123 and is a 'ET WEB\_SERVER Possible CVE-2014-6271 Attempt' event. The sixth alert has CNT 123 and is a 'ET WEB\_SERVER Possible CVE-2014-6271 Attempt in Headers' event. The seventh alert has CNT 123 and is a 'ET WEB\_SERVER Possible CVE-2014-6271 Attempt' event. The eighth alert has CNT 76 and is a 'ET INFO Executable Download from dotted-quad Host' event. The ninth alert has CNT 76 and is a 'ET INFO Executable Download from dotted-quad Host' event. The tenth alert has CNT 66 and is a 'ET WEB\_SERVER Possible CVE-2014-6271 Attempt' event.

ST	CNT	Sensor	Alert ID	DateTime	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1059	seconion...	1.3	2020-04-29 15:26:36	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in os...
RT	881	seconion...	1.2	2020-04-29 15:22:36	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports status (netstat) changed (new port opened or c...
RT	647	seconion...	7.1	2020-04-29 16:08:59	209.165.201.17		209.165.201.21		1	GPL ICMP_INFO PING *NIX
RT	296	seconion...	5.1	2020-04-29 16:55:12	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	296	seconion...	5.792	2020-05-10 21:20:28	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...
RT	296	seconion...	7.1105	2020-05-10 21:20:28	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...
RT	252	seconion...	3.1	2020-04-29 16:44:19	192.168.0.11		192.168.0.1		1	GPL ICMP_INFO PING *NIX
RT	123	seconion...	5.466	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
RT	123	seconion...	5.467	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
RT	123	seconion...	7.779	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
RT	123	seconion...	7.780	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
RT	76	seconion...	7.691	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	ET INFO Executable Download from dotted-quad Host
RT	76	seconion...	5.378	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	ET INFO Executable Download from dotted-quad Host
RT	66	seconion...	7.1672	2020-05-10 21:20:52	209.165.201.17	52204	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt

The bottom window shows a packet capture view for the alert with CNT 881. It displays the packet details, including the source IP (209.165.201.17), destination IP (209.165.201.21), and the ICMP type (8). The packet data is shown in hexadecimal and ASCII format.

## Alertas Sguil Ordenados na CNT

# Investigando dados de rede

## Sguil Queries

- As consultas podem ser construídas no Sguil usando o Construtor de Consultas. Ele simplifica a construção de consultas até um certo grau.
- O analista de segurança cibernética deve conhecer os nomes de campo e alguns problemas com valores de campo para efetivamente criar consultas no Sguil.
- Por exemplo, o Sguil armazena endereços IP em uma representação de inteiro.

The screenshot displays the Sguil 6.9.0 interface. The top section shows a query result table with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The bottom section shows a packet capture table with columns: IP, Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, and ChkSum. The packet data is shown in hexadecimal and ASCII format.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
ET	1	seconion-eth1-1	5.521	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
ET	1	seconion-eth1-1	5.522	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap SQL Spider Scan
ET	1	seconion-eth1-1	5.523	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed
ET	1	seconion-eth2-1	7.587	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
ET	1	seconion-eth2-1	7.588	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap SQL Spider Scan
ET	1	seconion-eth2-1	7.589	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	209.165.201.17	209.165.200.235	4	5	0	268	33065	2	0	63	33914

DATA	Source Port	Dest Port	R	O	G	K	H	T	N	N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
47 45 54 20 68 74 74 70 3A 2F 2F 54 57 69 68 69	40754	80	.	.	.	X	X	.	.	.	1692715185	667712887	8	0	229	0	50943

# Investigando dados de rede

## Pivotando do Sguil

- A Sguil oferece a capacidade de o analista de segurança cibernética pivotar para outras fontes de informação e ferramentas.
- Os arquivos de log estão disponíveis no Elasticsearch.
- Capturas de pacotes relevantes podem ser exibidas no Wireshark.
- O Sguil pode fornecer pivôs para informações sobre o Sistema de Detecção de Ativos em Tempo Real Passivo (PRADS) e o Security Analyst Network Connection Profiler (SANCP).

The screenshot displays the Sguil interface. The top section shows a list of events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. A red box highlights the 'Event History' section, which includes links for 'Transcript (force new)', 'Wireshark (force new)', 'NetworkMiner (force new)', and 'Bro (force new)'. Below this, the 'IP Resolution' table is visible, showing columns: SId, Net, Hostname, Type, and Last. The bottom section shows a packet capture view with columns: Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, ChkSum, and a detailed view of the packet structure (Source Port, Dest Port, R R R C S S Y I, Seq #, Ack #, Offset, Res, Window, Up, ChkSum).

**Nota:** A interface Sguil refere-se a PADS em vez de PRADS.

# Tratamento de eventos em Sguil

- O Sguil é um console que permite que um analista de segurança cibernética investigue, verifique e classifique alertas de segurança.
- Três tarefas podem ser concluídas no Sguil para gerenciar alertas:
- Alertas que foram encontrados como falsos positivos podem ser expirados.
- Um evento pode ser escalado pressionando a tecla F9.
- Um evento pode ser categorizado.
- O Sguil inclui sete categorias pré-construídas que podem ser atribuídas usando um menu ou pressionando a tecla de função correspondente.

The screenshot displays the Sguil console interface. At the top, a status bar shows 'File Query Reports Sound: Off ServerName: localhost Username: analyst UserID: 2' and a timestamp '2020-06-01 17:26:38 GMT'. Below this, there are tabs for 'RealTime Events' and 'Escalated Events'. The main window is divided into several sections:

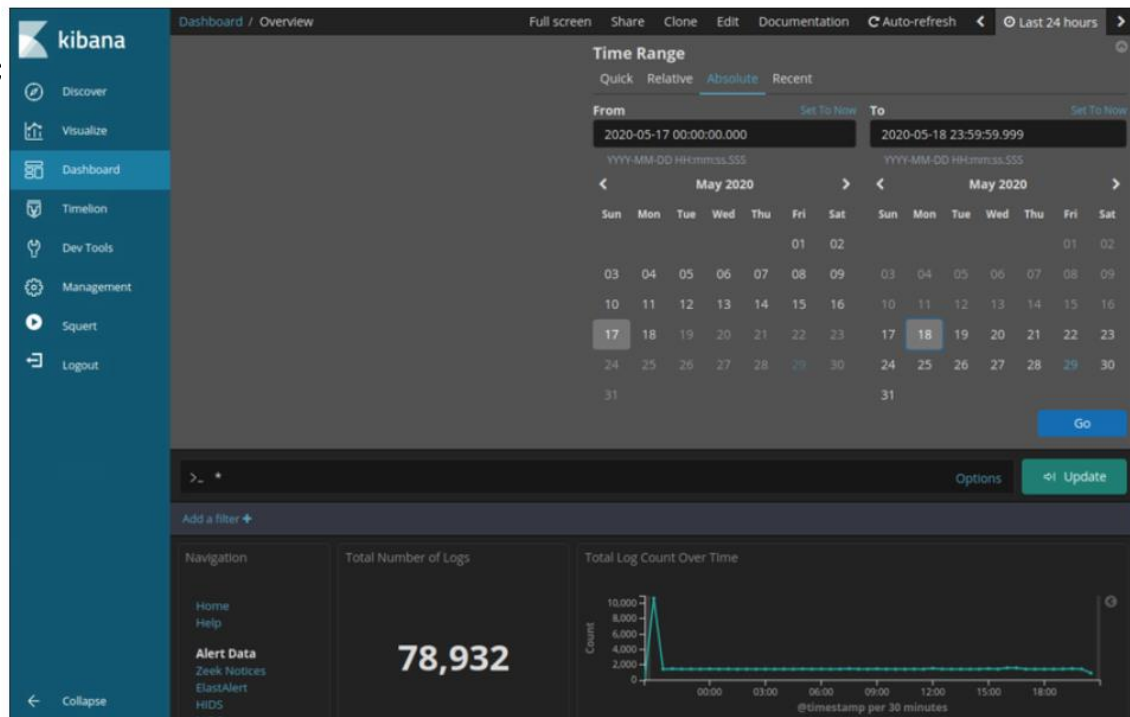
- Event List:** A table with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. It lists various events, including 'ET INFO Observed DNS Query to .bz2 TLD' and 'ET WEB\_SERVER WEB-PHP phpinfo access'.
- Update Event Status:** A section with a table for updating event status, including columns for ST, CNT, Sensor, Alert ID, and Date/Time.
- IP Resolution:** A table with columns: SId, Net, and Hostname, showing IP resolution results.
- Packet Data:** A section for packet analysis, including a table for packet data with columns: Source IP, Dest IP, Ver, HL, TOS, Len, ID, Flags, Offset, TTL, and ChkSum.

The interface also includes a search bar at the bottom right and a status bar at the bottom left.

# Investigando Dados de Rede

## Trabalhando no ELK

- Logstash e Beats são usados para ingestão de dados no Elastic Stack.
- Kibana, que é a interface visual nos logs, está configurado para mostrar as últimas 24 horas por padrão.
- 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 os dados no Elasticsearch é criar painéis visuais personalizados.





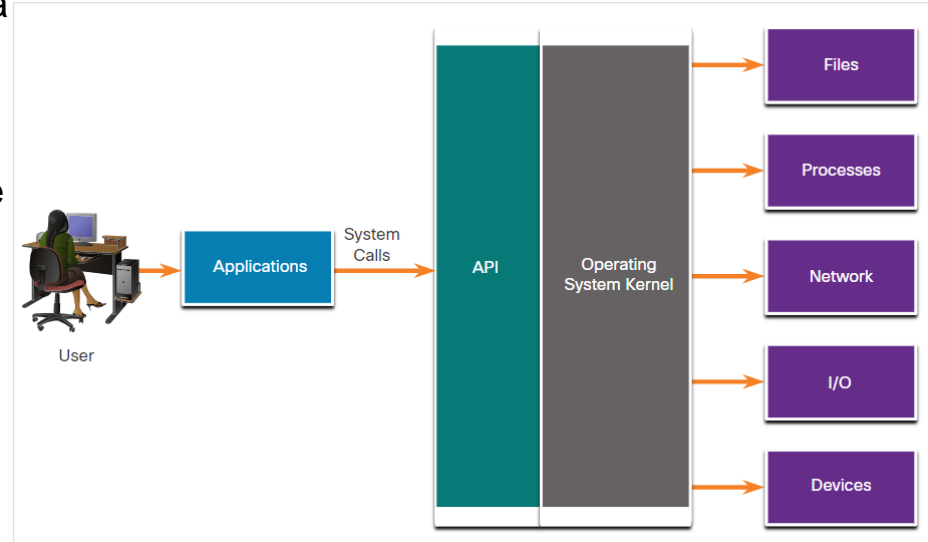
## Consultas em ELK

- O Elasticsearch é construído sobre o Apache Lucene, uma biblioteca de software de mecanismo de pesquisa de código aberto com recursos completos de indexação e pesquisa de texto.
- Usando bibliotecas de software Lucene, o Elasticsearch tem sua própria linguagem de consulta baseada em JSON chamado Query Domain Specific Language (DSL).
- Junto com JSON, consultas Elasticsearch fazem uso de elementos como operadores booleanos, Campos, Intervalos, Curingas, Regex, Pesquisa difusa e Pesquisa de texto.
- O Elasticsearch foi projetado para fazer interface com usuários usando clientes baseados na Web que seguem a estrutura HTTP REST.
- Os métodos utilizados para executar as consultas são URI, cURL, JSON e Ferramentas de Desenvolvimento.

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

# Investigando chamadas de processo ou API

- Os aplicativos interagem com um sistema operacional (SO) por meio de chamadas do sistema para a API (Interface de Programação de Aplicativos) do SO.
- Se o malware pode enganar um kernel do sistema operacional para permitir que ele faça chamadas de sistema, muitas explorações são possíveis.
- As regras OSSEC detectam alterações nos parâmetros baseados em host.
- As regras da OSSEC dispararão um alerta em Sguil.
- Ao pivotar 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





# Investigando dados de rede

## 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 para determinar se o arquivo é um malware conhecido.
- No Kibana, Zeek Hunting pode ser usado para exibir informações sobre os arquivos que entraram na rede.
- Note que no Kibana, o tipo de evento é mostrado como **bro\_files**, mesmo que o novo nome para Bro seja Zeek.

Dashboard / Zeek - Files

Full screen Share Clone Edit Documentation 15 minutes < Last 2M >

Search... (e.g. status:200 AND extension:PHP) Options Refresh

mimetype.keyword: "application/xml" Add a filter + Actions +

Files - Logs

event_type	bro_files
file_ip	209.165.201.17
fuid	FFRuizivIhrErrgBd
host	gateway
ips	209.165.200.235,
is_orig	true
local_orig	true
md5	56ceda5bb5c4c6be9ea6f16e86ab676f
message	{"ts":"2020-05-10T21:20:56.997512Z","fuid":"FFRuizivIhrErrgBd","tx_hosts":["209.165.201.17"],"rx_hosts":["209.165.200.235"],"conn_uids":["CMQAno37Z8pyV39ZVe"],"source":"HTTP","depth":0,"analyzers":["SHA1","MD5"],"mime_type":"application/xml","duration":0.0,"local_orig":true,"is_orig":true,"seen_bytes":714,"total_bytes":714,"missing_bytes":0,"overflow_bytes":0,"timeout":false,"md5":"56ceda5bb5c4c6be9ea6f16e86ab676f","sha1":"e4541e67581c859a6782c3492cb22da2ab2cf1c"}
mimetype	application/xml
missing_bytes	0B
overflow_bytes	0B
port	38524
seen_bytes	714B
sha1	e4541e67581c859a6782c3492cb22da2ab2cf1c
source	HTTP
source_ips	*
syslog-facility	user
syslog-file_name	/nsm/bro/logs/current/files.log

# Lab - Tutorial de expressão regular

Neste laboratório, você completará os seguintes objetivos:

- Use um tutorial on-line para explorar expressões regulares.
- Descreva as informações que correspondem a expressões regulares dadas.

# Laboratório de Dados de Rede - Extraia um Executável de um PCA

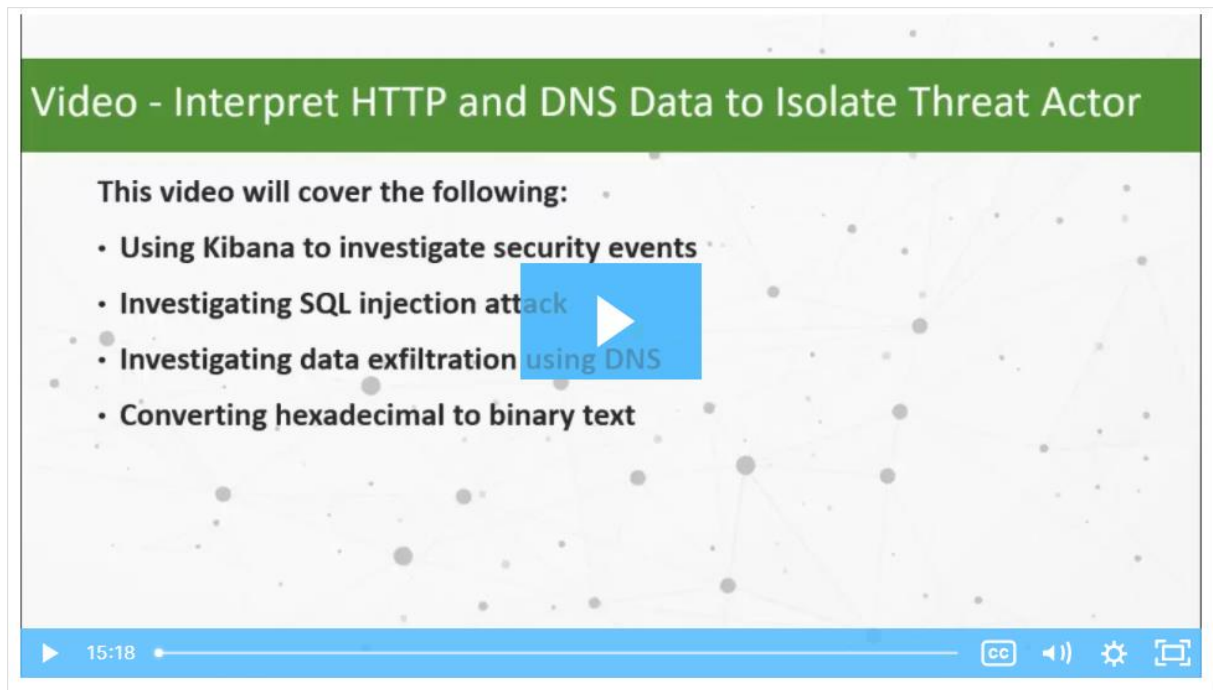
Olhar para registros é muito importante, mas também é importante entender como as transações de rede acontecem no nível do pacote.

Neste laboratório, você cumprirá o seguinte objetivo:

- Analise o tráfego em um arquivo pcap capturado anteriormente e extraia um arquivo executável do tráfego.

# Vídeo - interprete dados HTTP e DNS para isolar o ator da ameaça

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



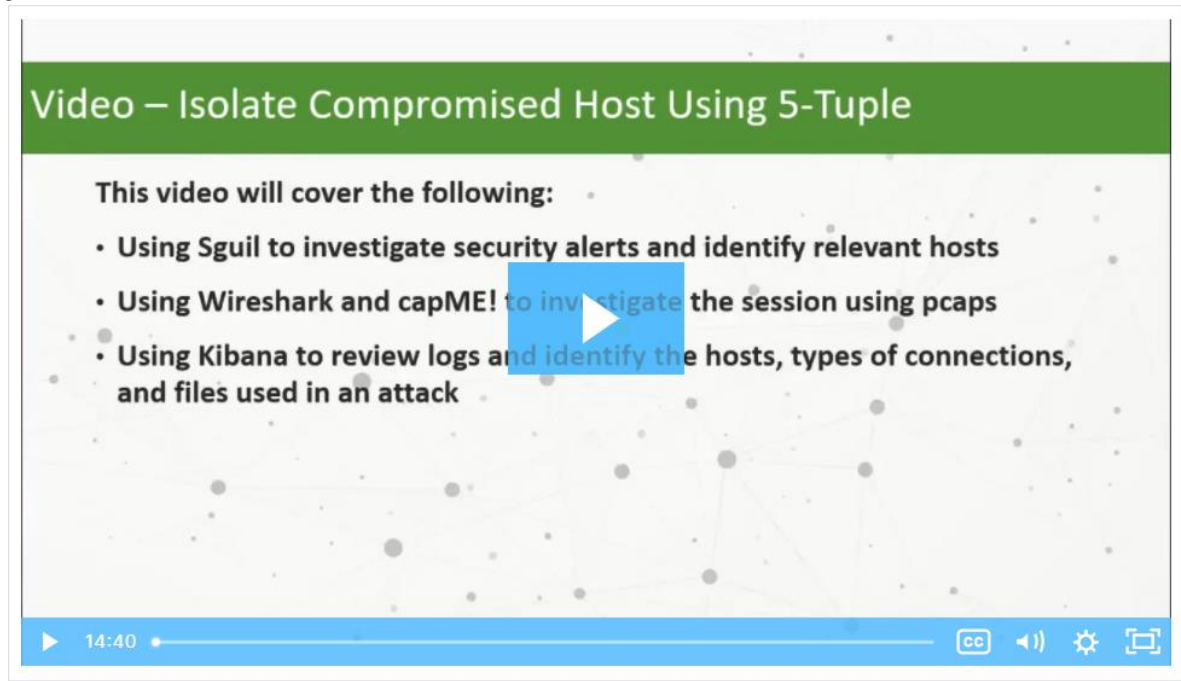
# Lab - Interprete dados HTTP e DNS para isolar o agente de ameaças

Neste laboratório, você cumprirá o seguinte objetivo:

- Investigue exploits de injeção de SQL e exfiltração de DNS usando as ferramentas Security Onion.

## 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.



## Lab - Isolar host comprometido usando 5 tuplas

Neste laboratório, você cumprirá o seguinte objetivo:

- Use as ferramentas Security Onion para investigar uma exploração.

# Lab - Investigar uma Exploit de Malware

Neste laboratório, você cumprirá o seguinte objetivo:

- Use Security Onion para investigar um malware mais complexo explorar o usa um kit de exploração para infectar hosts.



# Lab - Investigando um Ataque a um Host Windows

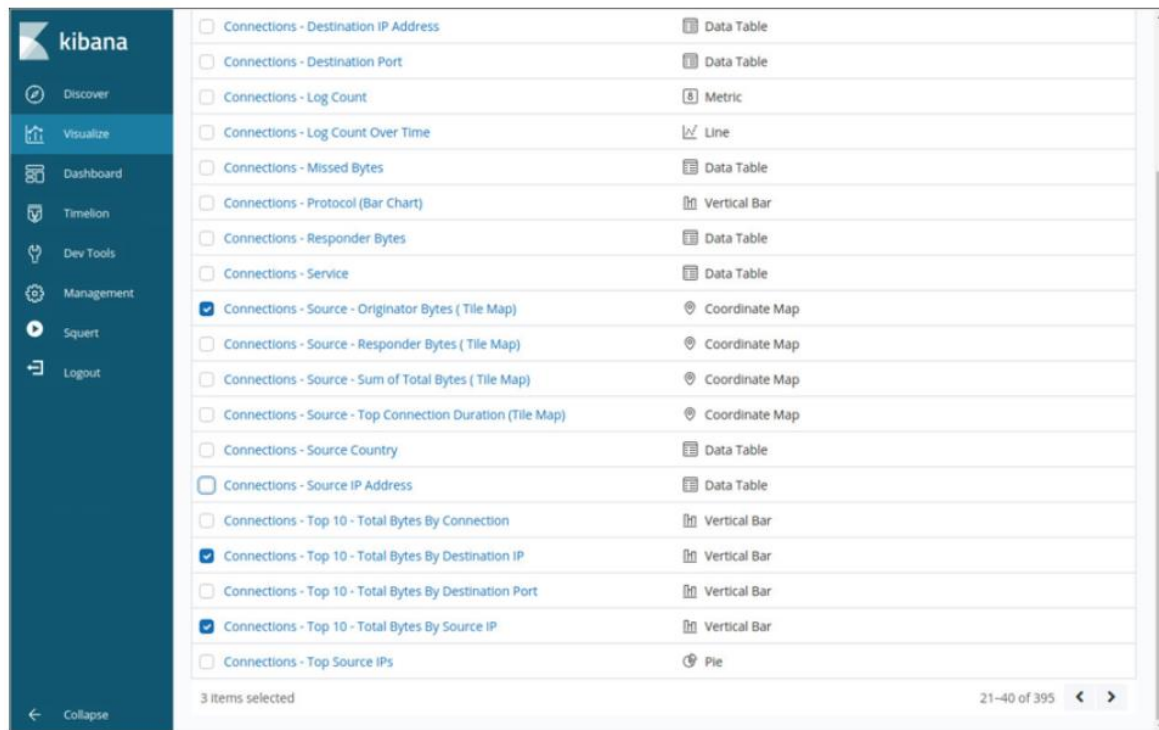
Neste laboratório, você completará os seguintes objetivos:

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

## 27.3 Como melhorar o trabalho do analista de segurança cibernética

# Melhorando o trabalho dos painéis e visualizações do analista de segurança cibernética

- Os painéis fornecem uma combinação de dados e visualizações que permite que os analistas de segurança cibernética se concentrem em detalhes e informações específicos.
- Painéis geralmente são interativos.
- Kibana inclui a capacidade de projetar painéis personalizados.
- Além disso, ferramentas como o Squert in Security Onion fornecem uma interface visual para os dados do NSM.



## Gestão de fluxo de trabalho

- Os fluxos de trabalho são a sequência de processos e procedimentos através dos quais as tarefas de trabalho são concluídas.
- Gerenciando os fluxos de trabalho SOC:
  - Aumenta a eficiência da equipe de operações cibernéticas
  - Aumenta a responsabilização do pessoal
  - Garante que todos os alertas potenciais sejam tratados adequadamente
- Sguil fornece um gerenciamento básico de fluxo de trabalho, mas não uma boa escolha para grandes operações. Existem sistemas de terceiros disponíveis que podem ser personalizados.
- Consultas automatizadas adicionam eficiência ao fluxo de trabalho de operações cibernéticasEssas consultas pesquisam automaticamente incidentes de segurança complexos que podem evitar outras ferramentas.

# 27.4 Resumo do trabalho com os dados de segurança de rede

# O que aprendi neste módulo?

- Uma plataforma de monitoramento de segurança de rede, como ELK ou Elastic Stack, deve unir os dados para análise.
- ELK consiste em Elasticsearch, Logstash e Kibana com componentes, Beats, ElastAlert e Curator.
- 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.
- O Sguil fornece um console que permite que um analista de segurança cibernética investigue, verifique e classifique alertas de segurança.
- As visualizações do Kibana fornecem insights sobre dados do NSM representando grandes quantidades de formatos de dados que são mais fáceis de interpretar.
- O gerenciamento de fluxo de trabalho adiciona eficiência ao trabalho da equipe SOC.

