

Splunk

Resumo básico para a ferramenta.

Fonte: [Curso](#)

O que é SIEM?

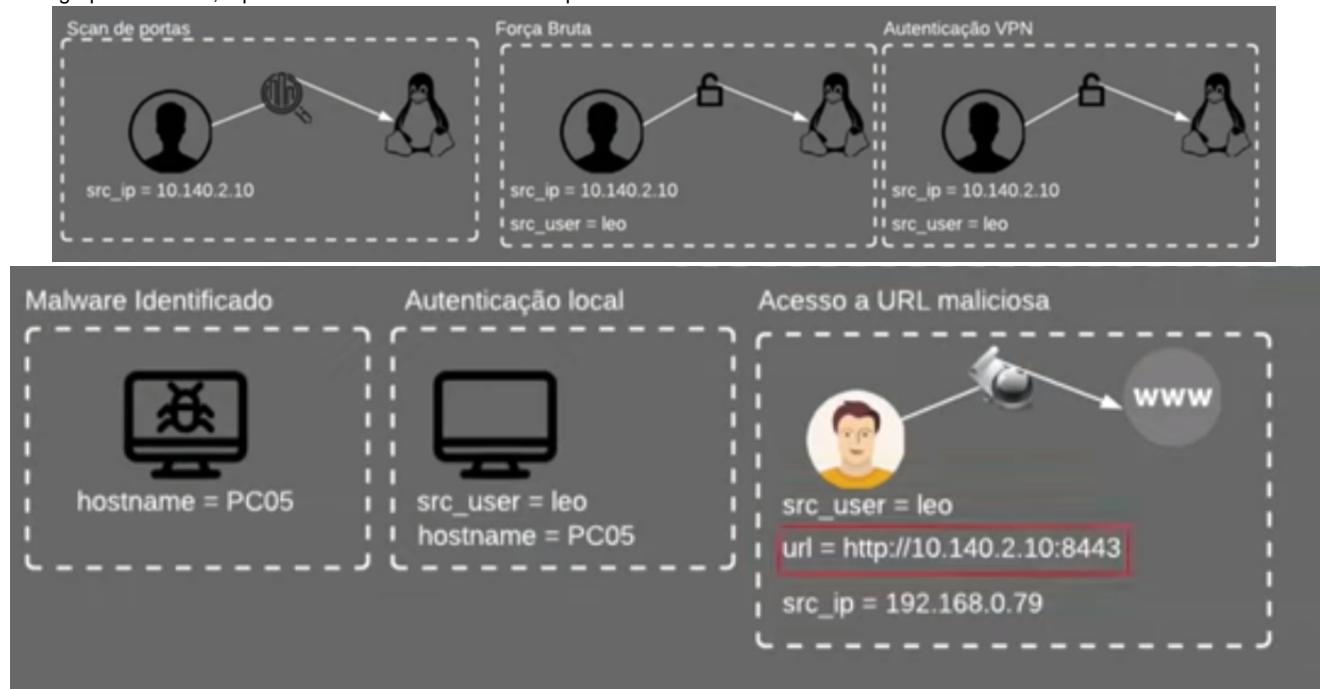
Security Information and event management

Principais recursos:

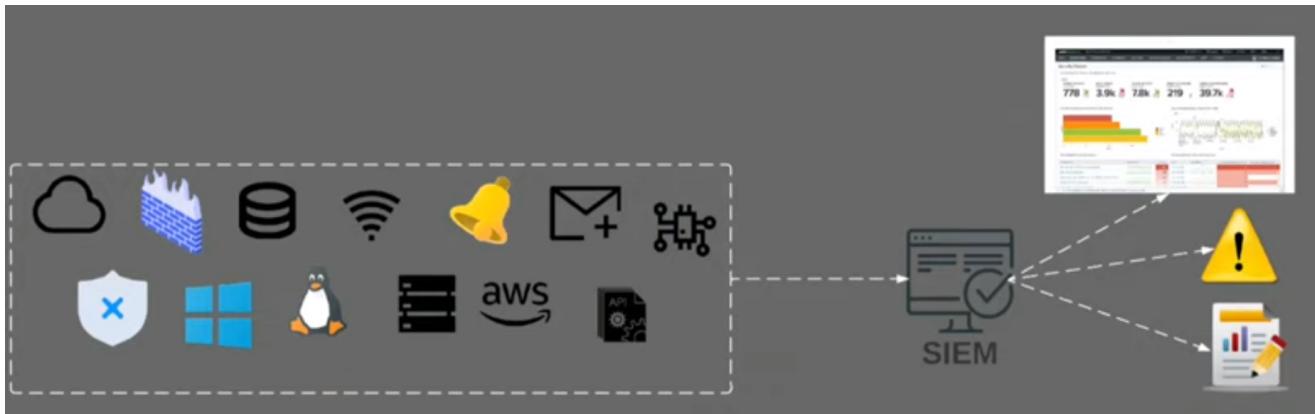
- Agregação de dados
 - Ponto central de busca de informação. Reune os dados relevantes;
 -



- Normalização de dados
 - Agrupar diferentes logs para serem buscados
- Análise e correlação
 - Por agrupar os dados, é possível relacionar as incidências para facilitar o entendimento:
 -



- O mesmo ip e hostname se repete, assim é possível relacionar os ocorridos para identificar a falha ou acontecimento.
- Monitoramento e alertas:



- É possível gerar alertas personalizados com os dados encontrados e suas necessidades.

Splunk



É uma plataforma para pesquisa de dados (SIEM). Atualmente (2022) uma das melhores do mercado.

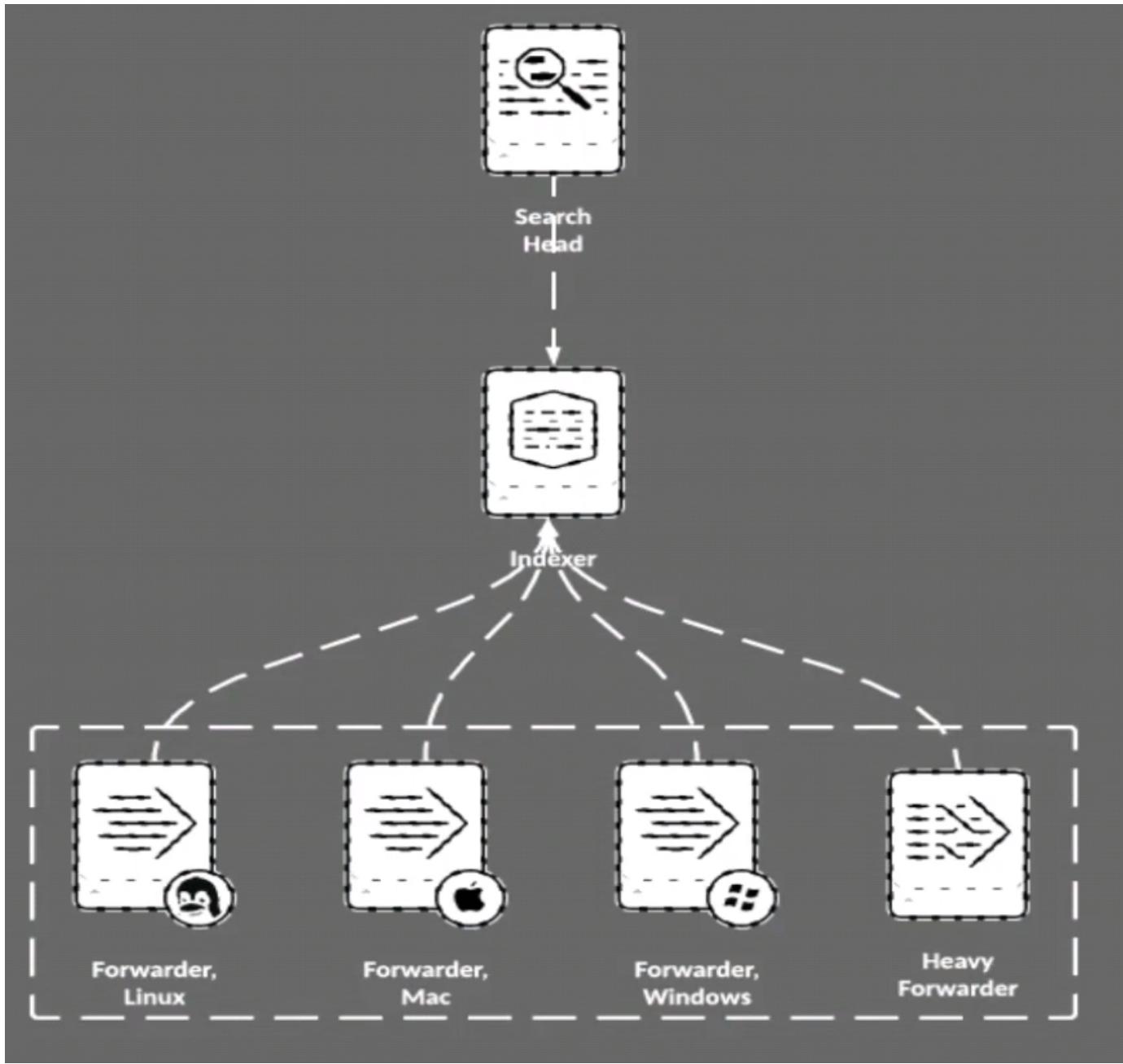
Funcionalidades:

- Análise de performance de sistemas
- Troubleshoot
- Monitorar métricas de negócio
- Pesquisa e investigação de incidentes
- Criação de painéis e relatórios
- Centralização de dados
- Alertas de anomalias

Quais dados o Splunk recebe?

- Computadores
- Máquinas virtuais
- Logs
- Sensores
- Bancos de dados
- Alertas
- Tickets
- etc

Como o Splunk Funciona



Indexer

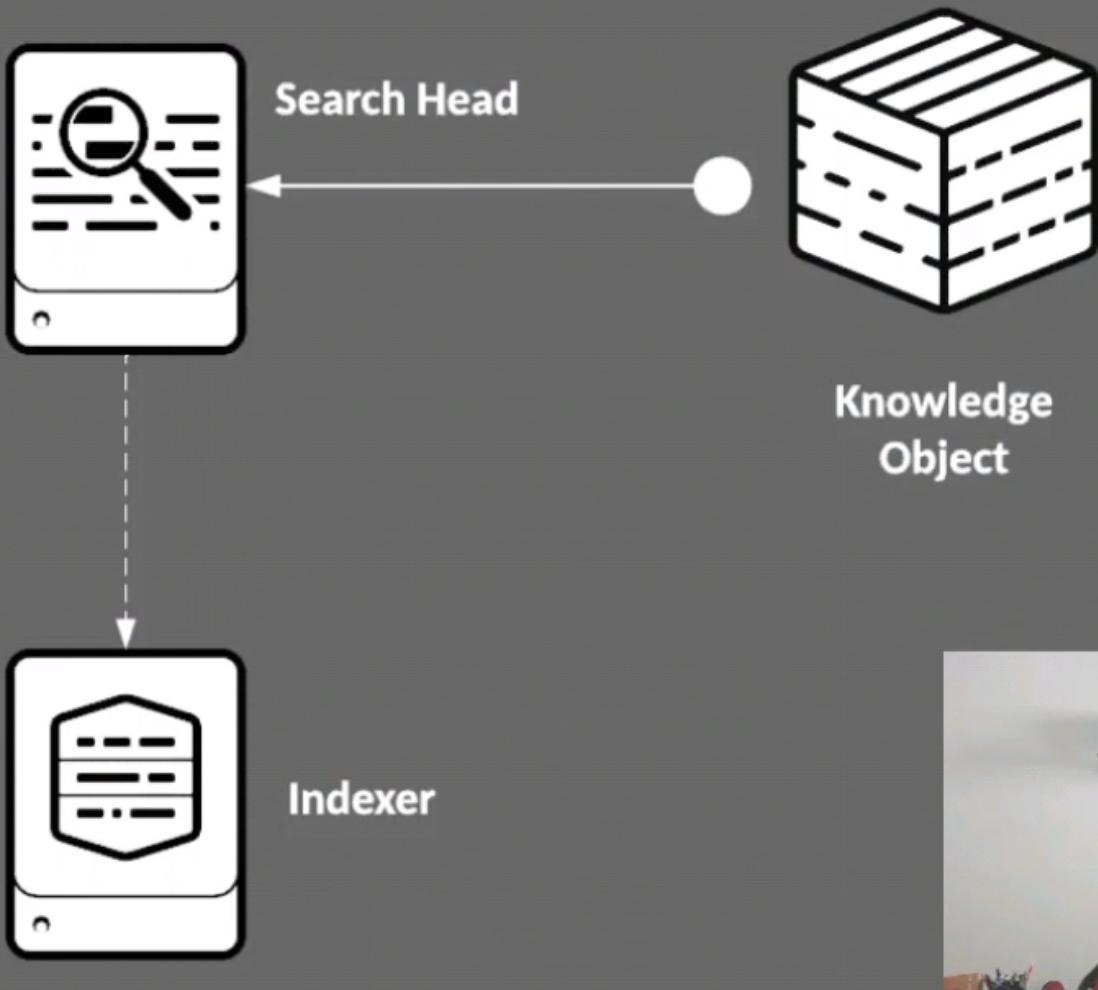
- Processa os dados, armazena os resultados em indexadores e permitem pesquisas e análises rápidas
- Conforme o indexador indexa os dados, ele cria uma série de arquivos organizados de diretórios por tempo

Pega os dados dos encaminhadores e começa a estruturá-los e separa em indexes.

Search Head

New Search

```
sourcetype=access_combined_wcookie action=addtocart status=200
```



- Permite que o usuário realize pesquisas nos dados indexados
- Consolida o resultado e retorna os campos solicitados pelo usuário
- Knowledge objects nas Search Heads podem ser criados para extrair campos, transformar e enriquecer dados sem alterar os dados no index
- Fornece ferramentas para aprimorar a experiência das pesquisas (reports, dashboards e visualizations)

Forwarder (Encaminhadores)

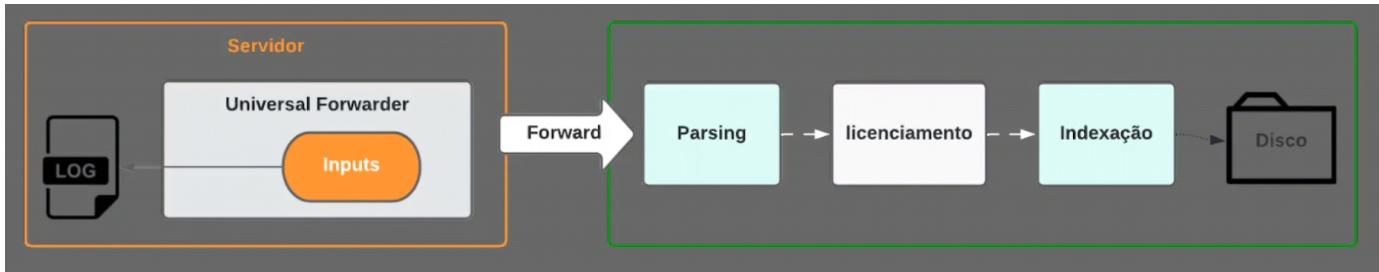
Universal Forwarder

- Baixo consumo de recurso
- Não realiza transformações
- Normalmente instalado direto na máquina onde os dados se originam

Heavy Forwarder

- Instâncias de Splunk Enterprise que consome e enviam dados para indexers
- Realiza descarte de logs e transformações

Processo de indexação



1. Fase de input: Manipulando os dados (Um forwarder)
 - a. Fontes de dados estão sendo abertas e lidas
2. Fase de Parsing: Manipulada por Indexers (ou Heavy Forwarders)
 - a. Os dados são divididos em eventos
3. Fase de Indexação
 - a. O medidor de licença é executado como dados e é inicialmente gravado em disco, antes da compactação

Metadados

- source: Caminho do arquivo de entrada, nome do host Ip:porta ou nome do script
- host: Nome do host de entrada
- sourcetype: Usa o nome do arquivo de origem se o Splunk não puder determinar automaticamente
- index: main

Modos de Pesquisa

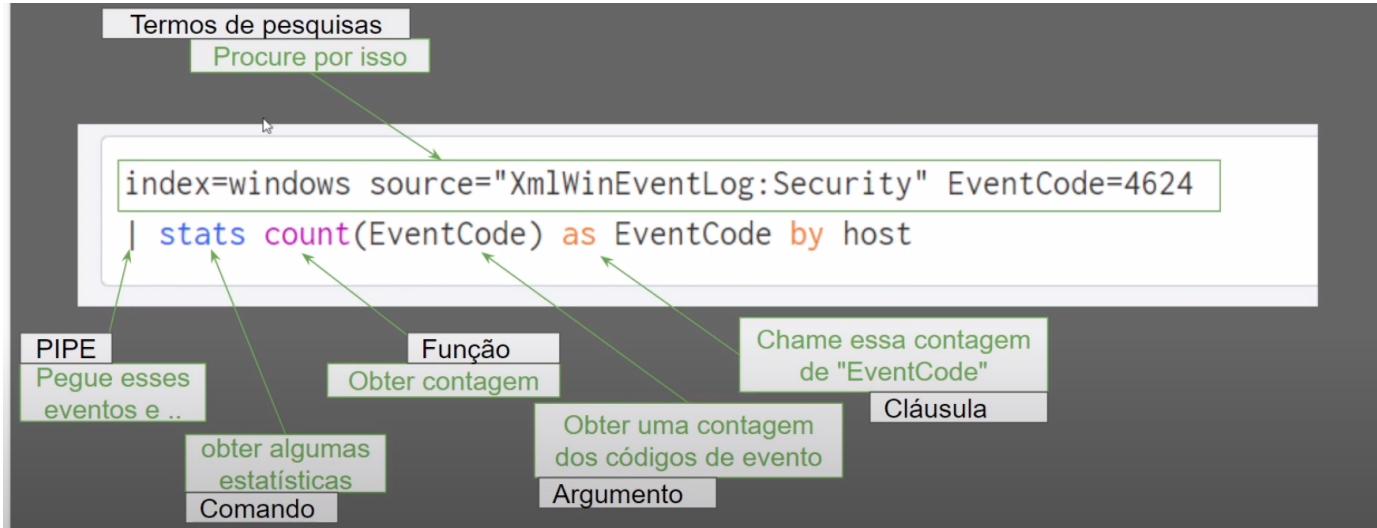
- Fast Mode: Foco na performance do que na riqueza de detalhes dos eventos
- Smart Mode: Tenta equilibrar performance com detalhes
- Verbose: Foco nos detalhes

Boas práticas em pesquisas

1. O tempo é o filtro mais eficiente
2. Especifique um ou mais valores de índices no início de sua string de pesquisa
 - a. index=windows source="lorem:lorem"
3. Inclua o maior número possível de termos de pesquisa
4. Torne seus termos de pesquisa mais específicos
5. A inclusão geralmente é melhor que a exclusão
6. Filre o quanto antes
7. Evite usar curingas (*) no início ou no meio de uma string
8. Quando possível, use or em vez de curingas

Guia de pesquisas: <https://docs.splunk.com/Documentation/Splunk/9.0.1/SearchReference/WhatsInThisManual>

Sintaxe da linguagem Splunk (SPL)



- Termos de pesquisas - O que está procurando?
- Comandos - O que você quer fazer com os resultados?
 - Criar gráficos, estatísticas, etc
- Funções - Como você deseja mapear os dados?
- Argumentos - Existem variáveis que você deseja aplicar a essas funções?
- Cláusulas - Como você deseja agrupar ou renomear o grupo

Comandos

Table

```
index=*main! sourcetype="access_combined.wookiee" action="addtocart" productId=
| table clientip action productId
```

New Search

1 index=*main! sourcetype="access_combined.wookiee" action="addtocart" productId= 2 | table clientip action productId

16.221 events (before 4/26/21 10:04:30,000 PM) No Event Sampling

Events (16.221) Patterns Statistics (16.221) Visualization

100 Per Page Format Preview

clientip	action	productId
182.236.164.11	addtocart	85-AG-089
182.236.164.11	addtocart	85-AG-089
182.236.164.11	addtocart	85-AG-089
182.236.164.11	addtocart	8C-SH-084
182.236.164.11	addtocart	8C-SH-084
182.236.164.11	addtocart	8B-AG-087
182.236.164.11	addtocart	8B-AG-087

Rename

```
index=*main! sourcetype="access_combined.wookiee" action="addtocart" productId=
| table clientip action productId
| rename cliente as "Cliente"
```

Fields (retorna somente os campos pedidos)

```
index=windows source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| fields + User EventCode
```

Stats (Estatísticas)

Calcula estatísticas agregadas, como média, soma etc

```
index=windows source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| fields + User EventCode
| stats count by User EventCode
| stats count
```

```

| stats count by clientip
| stats count by productId
| stats avg(bytes) as media_bytes
| stats avg(bytes) as media_bytes by clientip
| stats sum(bytes) as bytes by clientip
| stats max(bytes) as bytes by clientip
| stats min(bytes) as bytes by clientip
| stats first(clientip) as Client
| stats last(clientip) as Client
| stats list(clientip) as Client
| stats values(clientip) as Client

```

New Search

Save As ▾ Create Table View Close

Last 60 minutes ▾

index=windows source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| fields + User EventCode
| stats count by User EventCode|

✓ 962 events (5/29/22 10:52:00.000 PM to 5/29/22 11:52:23.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (962) Patterns Statistics (10) Visualization

20 Per Page ▾ Preview ▾

User	EventCode	count
NT AUTHORITY\LOCAL SERVICE	1	3
NT AUTHORITY\LOCAL SERVICE	5	4
NT AUTHORITY\NETWORK SERVICE	1	3
NT AUTHORITY\NETWORK SERVICE	5	3
NT AUTHORITY\SYSTEM	1	141
NT AUTHORITY\SYSTEM	5	139

Sort (Ordenar)

Crescente

```

index=windows source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| fields + User EventCode
| stats count by User EventCode
| sort count

```

Decrescente

```

index=windows source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| fields + User EventCode
| stats count by User EventCode
| sort -count

```

Top e Rare

Top - mostra os mais comuns

Rare - os menos comuns

```

| top productId
| top productId limit=0
| top action by productId limit=5
| rare productId

```

```
| rare productId limit=0
| rare action by productId limit=5
```

Where

O comando where usa (predicate-expressions) para filtrar os resultados da pesquisa. Uma expressão de predicado, quando avaliada, retorna VERDADEIRO ou FALSO.

```
index=main sourcetype=access_combined_wcookie | table _time method uri_path uri status action | where
status = 404
```

_time	method	uri_path	uri	status	action
2022-01-01 18:16:29	POST	/cart.do	/cart.do?action=purchase&itemId=EST-15&JSESSIONID=SD9SL7FF3ADFF53096	503	purchase
2022-01-01 18:16:27	POST	/cart.do	/cart.do?action=addtocart&itemId=EST-15&productId=DB-SG-G01&JSESSIONID=SD9SL7FF3ADFF53096	200	addtocart
2022-01-01 18:16:28	POST	/cart/success.do	/cart/success.do?JSESSIONID=SD9SL7FF3ADFF53096	200	purchase
2022-01-01 18:16:27	POST	/cart.do	/cart.do?action=purchase&itemId=EST-18&JSESSIONID=SD9SL7FF3ADFF53096	200	purchase
2022-01-01 18:16:26	POST	/cart.do	/cart.do?action=addtocart&itemId=EST-18&productId=MB-AG-T01&JSESSIONID=SD9SL7FF3ADFF53096	200	addtocart

Search

Pesquisa os índices do Splunk para eventos correspondentes.

```
index=main sourcetype=access_combined_wcookie | table _time method uri_path uri status action | search
status = 404
```

_time	method	uri_path	uri	status	action
2022-01-01 17:42:06	GET	/rush/signals.zip	/rush/signals.zip?JSESSIONID=SD10SL8FF3ADFF52952	404	purchase
2022-01-01 16:34:41	GET	/stuff/logo.ico	/stuff/logo.ico?JSESSIONID=SD9SL10FF5ADFF52576	404	
2022-01-01 16:28:24	GET	/hidden/anna_nicole.html	/hidden/anna_nicole.html?JSESSIONID=SD9SLFFF5ADFF52541	404	
2022-01-01 15:26:08	GET	show.do	show.do?productId=SF-BVS-01&JSESSIONID=SD9SL6FF1ADFF52200	404	
2022-01-01 14:52:37	GET	show.do	show.do?productId=SF-BVS-01&JSESSIONID=SD9SL10FF6ADFF51982	404	
2022-01-01 12:38:50	POST	/passwords.pdf	/passwords.pdf?JSESSIONID=SD9SL3FF3ADFF51356	404	
2022-01-01 12:17:15	POST	/hidden/anna_nicole.html	/hidden/anna_nicole.html?JSESSIONID=SD4SL1FF8ADFF51243	404	