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

Objetivos

Neste laboratório, você analisará os logs de uma exploração de vulnerabilidades documentadas de HTTP e DNS.

Parte 1: Investigar um Ataque de Injeção SQL

Parte 2: Investigar a Exfiltração de Dados DNS

Histórico/Cenário

MySQL é um banco de dados popular usado por inúmeras aplicações web. Infelizmente, a injeção de SQL é uma técnica comum de hacking na web. É uma técnica de injeção de código em que um invasor executa instruções SQL maliciosas para controlar o servidor de banco de dados de uma aplicação web.

Os servidores de nomes de domínio (DNS) são directórios de nomes de domínio e traduzem os nomes de domínio em endereços IP. Este serviço pode ser usado para exfiltrar dados.

O pessoal de segurança cibernética determinou que ocorreu uma exploração, e dados contendo PII podem ter sido expostos a atores de ameaças. Neste laboratório, você usará o Kibana para investigar as explorações para determinar os dados que foram exfiltrados usando HTTP e DNS durante os ataques.

Recursos necessários

- Máquina virtual Security Onion

Instruções

Parte 1: Investigar um ataque de injeção SQL

Nesta parte, você investigará uma exploração em que o acesso não autorizado foi feito a informações confidenciais armazenadas em um servidor web. Você usará Kibana para determinar a origem do ataque e as informações acessadas pelo invasor.

Etapa 1: Altere o período de tempo.

Foi determinado que a exploração ocorreu em algum momento durante o mês de junho de 2020. O padrão do Kibana exibe os dados das últimas 24 horas. Você precisará alterar as configurações de hora para ver os dados do mês de junho de 2020.

a. Inicie a VM Security Onion e faça login com o **analyst** de nome de usuário e as **ciberops**de senha.

b. Digite o comando **sudo so-status** para verificar o status dos serviços. O status de todos os serviços deve ser **OK** antes de iniciar sua análise. Isso pode levar alguns minutos.

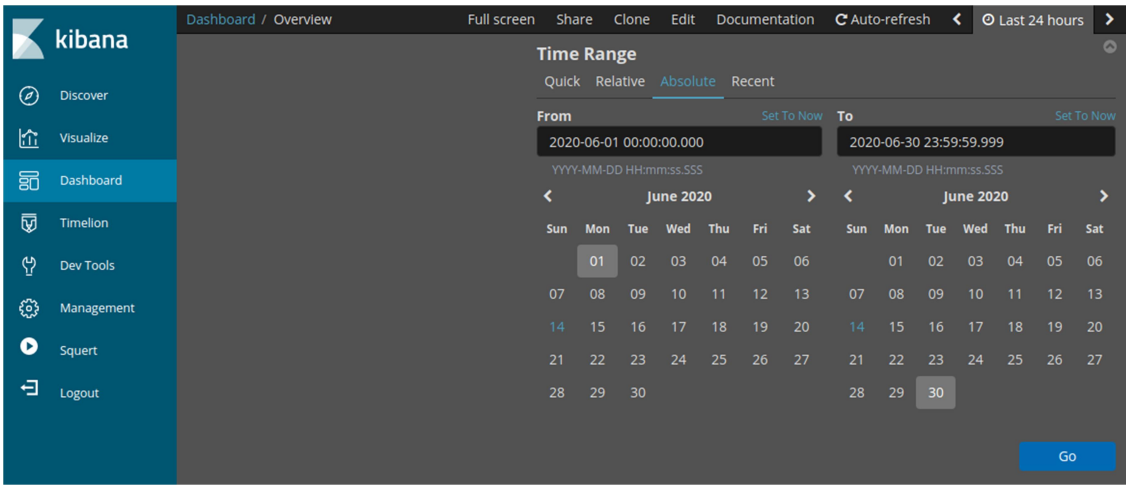
```
analyst @SecOnion: ~$ sudo so-status
Status: securityonion
  * sguil server [ OK ]
Status: seconion-import
  * pcap_agent (sguil) [OK]
  * snort_agent-1 (sguil) [OK]
  * barnyard2-1 (spooler, unified2 format) [ OK ]
```

```
Status: Elastic stack
  * so-elasticsearch [OK]
  * so-logstash [OK]
  * so-kibana [OK]
  * so-freqserver [OK]
```

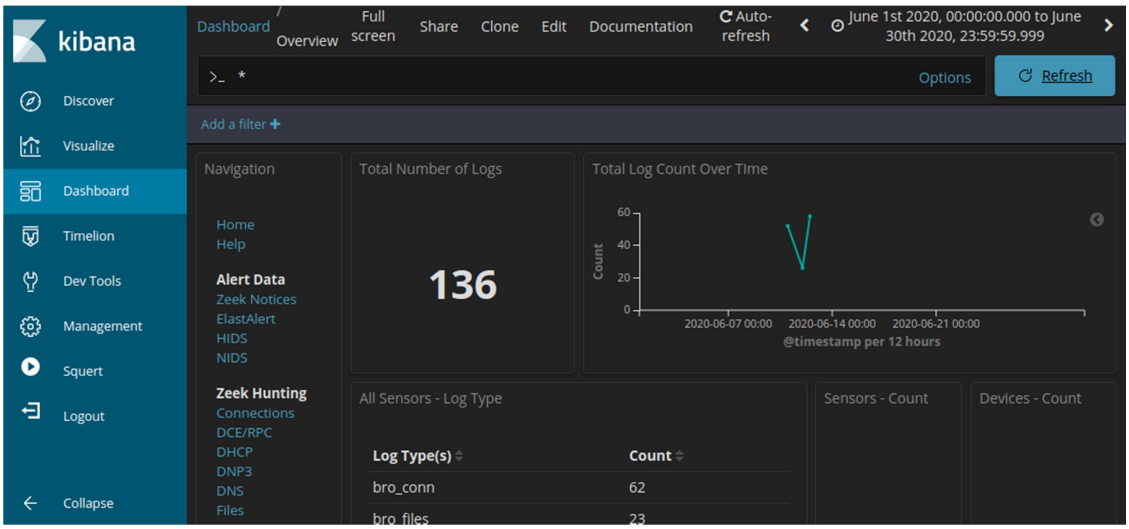
c. Depois de iniciar sessão, abra o Kibana usando o atalho na área de trabalho. Faça login com o **analyst** de nome de usuário e o **cyberops**de senha.

No Security Onion, o Kibana tem muitos painéis pré-construídos e visualizações para monitoramento e análise. Você também pode criar seus próprios painéis e visualizações personalizados para monitorar seu ambiente de rede específico. **Observação**: seu painel pode não ter resultados nas últimas 24 horas.

d. No canto superior direito da janela, clique em **Últimas 24 horas** para alterar o tamanho de intervalo de tempo de amostra. Expanda o intervalo de tempo para incluir os alertas interessantes. Um ataque de injeção SQL ocorreu em junho de 2020, então é isso que você precisa atingir. **Selecione Absolute em Intervalo de Tempo e edite os horários De e Até para incluir todo o mês de junho de 2020.** Clique em **Go** para continuar.



e. Observe o número total de logs para todo o mês de junho de 2020. Seu painel deve ser semelhante ao mostrado na figura. Reserve um momento para explorar as informações fornecidas pela interface Kibana.



Etapa 2: Filtro para tráfego HTTP.

a. Como o ator de ameaça avaliou os dados armazenados em um servidor Web, o filtro HTTP é usado para selecionar os logs associados ao tráfego HTTP. Selecione HTTP sob o cabeçalho Zeek Hunting, como mostrado na figura.

Percorra os resultados e responda às seguintes perguntas:

Qual é o endereço IP de origem?

Qual é o endereço IP de destino?

Qual é o número da porta de destino?

b. Role para baixo até os Logs HTTP. Os resultados listam os primeiros 10 resultados.

c. Expanda os detalhes do primeiro resultado clicando na seta que está ao lado do carimbo de data/hora da entrada de log. Observe as informações que estão disponíveis.

Qual é o carimbo de data/hora do primeiro resultado?

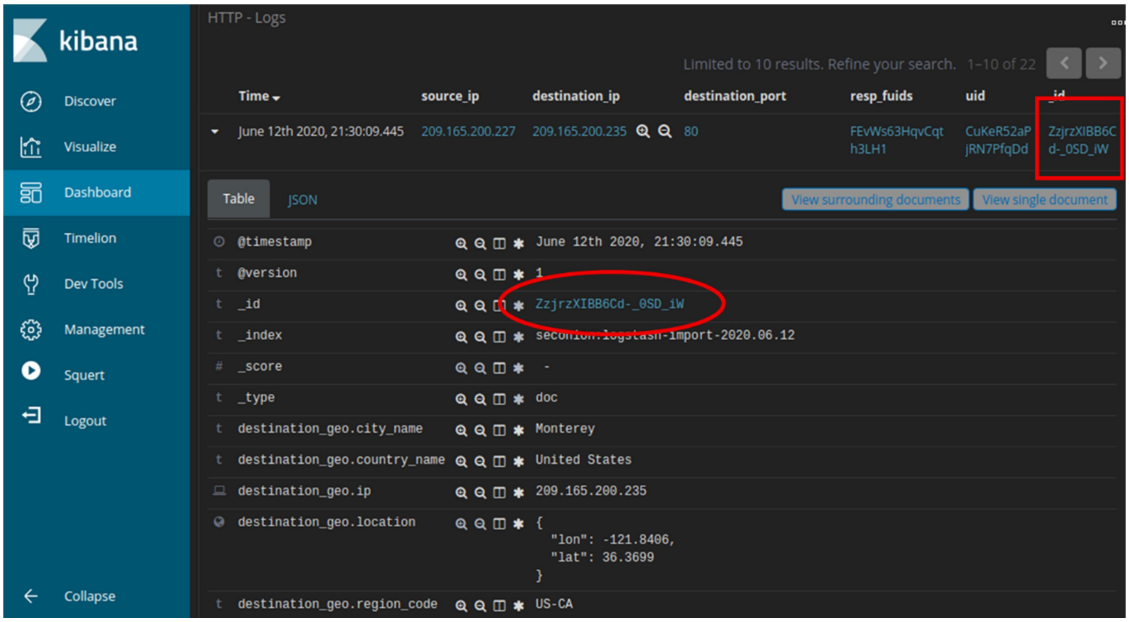
Qual é o tipo de evento?

O que está incluído no campo de mensagem? Estes são detalhes sobre a solicitação HTTP GET que foi feita pelo cliente para o servidor. Concentre-se especialmente no campo **uri** no texto da mensagem.

Qual é o significado desta informação?

Etapa 3: Reveja os resultados.

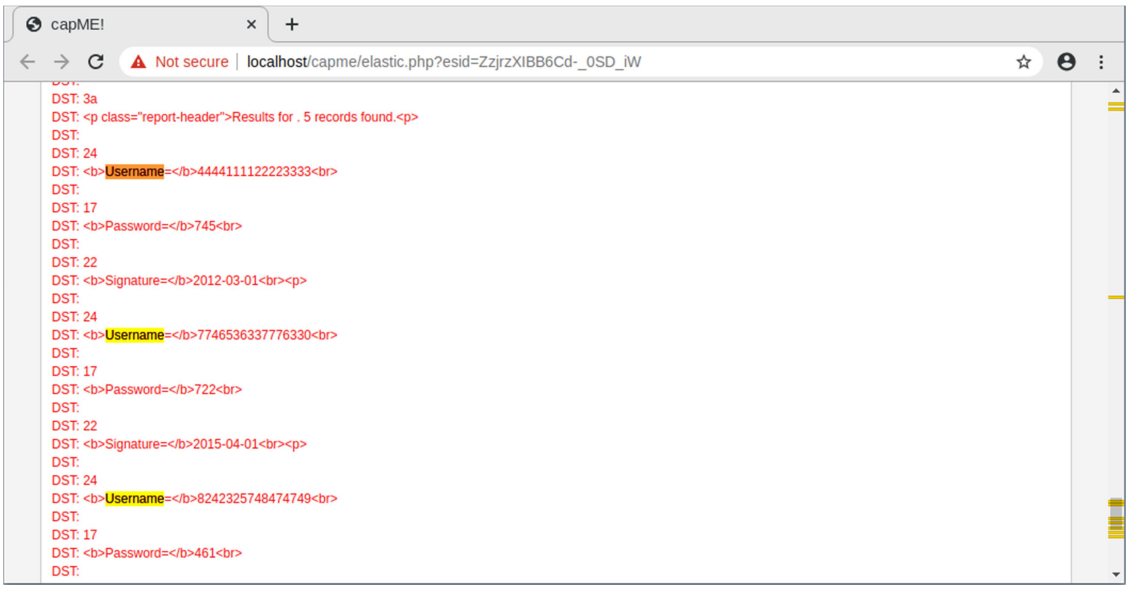
a. Algumas das informações para as entradas de log contêm hiperlinks para outras ferramentas. Clique no valor no campo **_id** de alerta da entrada de log para obter uma exibição diferente do evento.



b. O resultado é aberto em uma nova guia do navegador da Web com informações do CapMe!. CapMe! é uma interface web que permite visualizar uma transcrição pcap. O texto azul contém solicitações HTTP enviadas da origem (SRC). O texto vermelho é respostas do servidor Web de destino (DST).

c. Na seção Entrada de registro, que está no início da transcrição, observe a parte **username='+union+select+ccid, ccnumber, ccv, expiração, null+de+credit_cards+—+&password=** indica que alguém pode ter tentado atacar o navegador da Web usando injeção SQL para ignorar a autenticação. As palavras-chave, **union** e **select**, são comandos que são usados na pesquisa de informações em um banco de dados SQL. Se as caixas de entrada em uma página da Web não estiverem adequadamente protegidas contra entrada ilegal, os atores de ameaças podem injetar cadeias de caracteres de pesquisa SQL ou outro código que possa acessar dados contidos em bancos de dados vinculados à página da Web.

d. Encontre a palavra-chave **nome de usuário** na transcrição. Use **Ctrl-F** para abrir uma caixa de pesquisa. Use o botão de seta para baixo na caixa de pesquisa para percorrer as ocorrências encontradas.



Você pode ver onde o termo nome de usuário foi usado na interface da Web que é exibida para o usuário. No entanto, se você olhar mais para baixo, algo incomum pode ser encontrado.

O que você vê mais tarde na transcrição em relação aos nomes de usuário?

Dê alguns exemplos de um nome de usuário, senha e assinatura que foi exfiltrado.

e. Feche o CapMe! e volte ao Kibana.

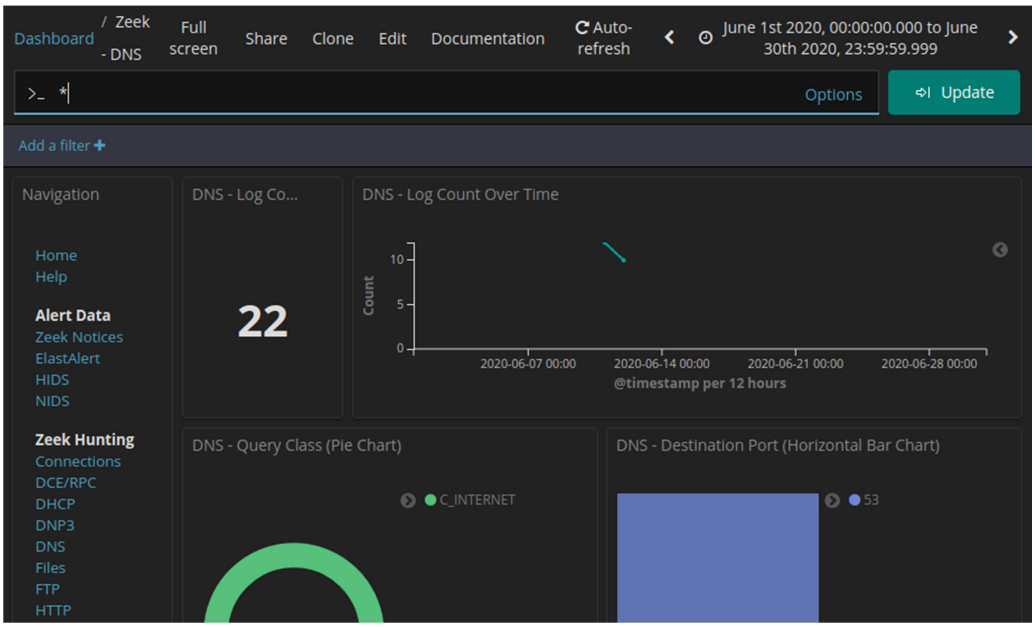
Parte 2: Analise a exfiltração de DNS.

Um administrador de rede notou consultas DNS anormalmente longas com subdomínios de aparência estranha. Seu trabalho é investigar a anomalia.

Etapa 1: Filtro para tráfego DNS.

a. Na parte superior do Painel Kibana, limpe todos os filtros e termos de pesquisa e clique em **Home** na seção Navegação do Painel. O período de tempo deve ainda incluir junho de 2020.

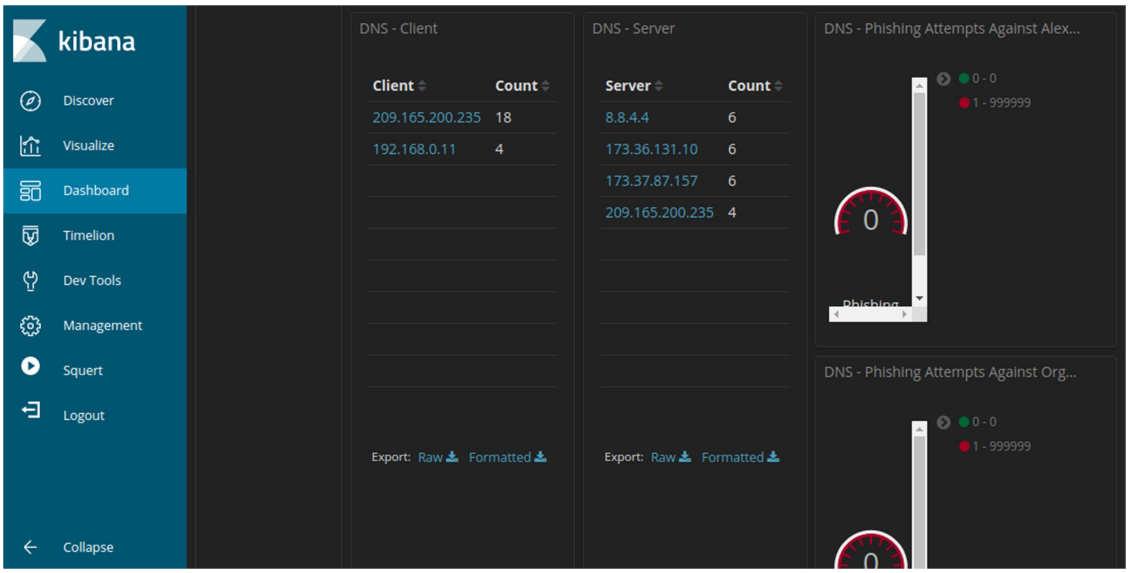
b. Na mesma área do Dashboard, clique em **DNS** na seção Zeek Hunting. Observe as métricas de Contagem de Log DNS e o gráfico de barras horizontais da Porta de



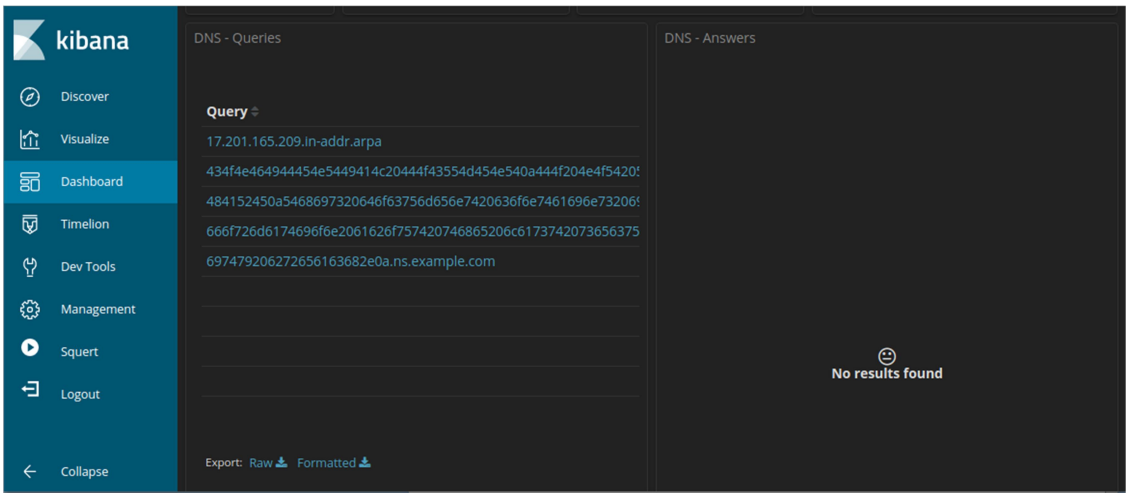
Etapa 2: Revise as entradas relacionadas ao DNS.

a. Role a janela para baixo. Você pode ver os principais tipos de consulta DNS. Você pode ver registros de endereço (registro A), registros de endereço IPv6 Quad A (AAAA), registros NetBIOS (NB) e registros de ponteiro para resolver os nomes de host (PTR). Você também pode ver os códigos de resposta DNS.

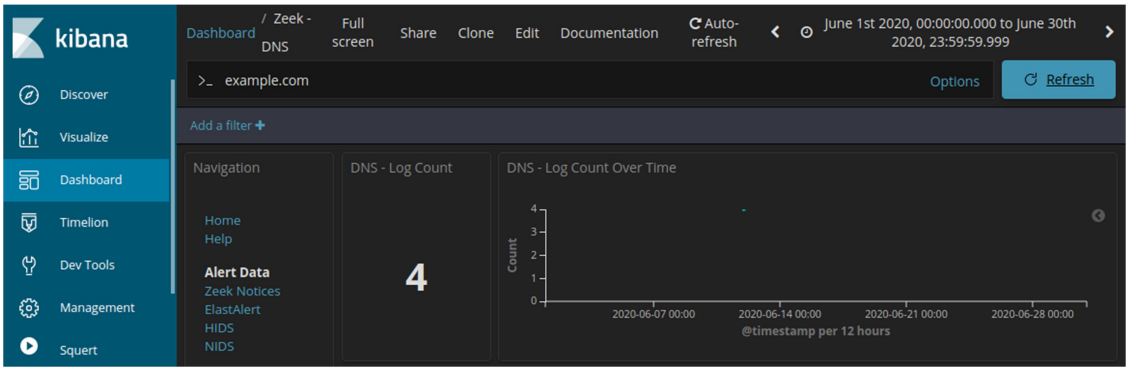
b. Ao rolar mais para baixo, você pode ver uma lista dos principais clientes DNS e servidores DNS com base em suas contagens de solicitações e respostas. Há também uma métrica para o número de tentativas de Phishing DNS, que também são conhecidas como phishing DNS, spoofing ou envenenamento.



c. Rolando mais para baixo na janela, você pode ver uma listagem das principais consultas DNS por nome de domínio. Observe como algumas das consultas têm subdomínios excepcionalmente longos anexados a ns.example.com. O domínio example.com deve ser investigado mais adiante.



d. Role de volta para a parte superior da janela e digite **example.com** na barra de pesquisa para filtrar por exemplo.com e clique em **Update**. Observe que o número de entradas na Contagem de Logs é menor porque a exibição agora está limitada a solicitações para o servidor example.com.

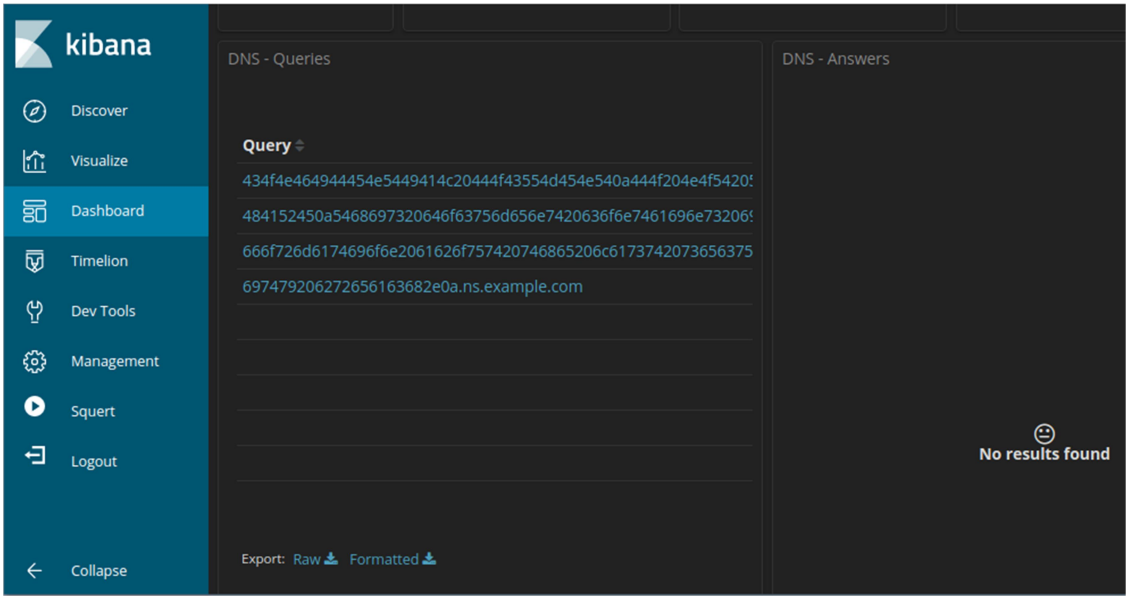


e. Localize informações sobre o DNS - Cliente e DNS - Servidor.

Registre os endereços IP do cliente e servidor DNS.

Etapa 3: Determine os dados exfiltrados.

a. Continue rolando para baixo para ver quatro entradas de log exclusivas para consultas DNS em example.com. Observe como as consultas são para subdomínios suspeitosamente longos anexados a ns.example.com. As cadeias longas de números e letras nos subdomínios parecem texto codificado em hexadecimal (0-9, a-f) em vez de nomes de subdomínio legítimos. Clique no link **Export: Raw** para baixar as consultas para um arquivo externo. Um arquivo CSV é baixado para a pasta /home/analyst/downloads.



b. Navegue até a pasta **/home/analyst/downloads**. Abra o arquivo usando um editor de texto, como gedit. Edite o arquivo excluindo o texto em torno da parte hexadecimal dos subdomínios, deixando apenas os caracteres hexadecimais. Certifique-se de remover as aspas também. O conteúdo do seu arquivo deve ser parecido com as informações abaixo. Salve o arquivo de texto editado com o nome original do arquivo.

```
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
6974792062726561636e0a
```

c. Em um terminal, use o comando **xxd** para decodificar o texto no arquivo CSV e salvá-lo em um arquivo chamado secret.txt. Use **cat** para enviar o conteúdo de secret.txt para o console.

```
analyst @SecOnion: ~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst @SecOnion: ~/$ cat secret.txt
```

Os subdomínios eram dos subdomínios de consultas DNS? Caso contrário, qual é o texto?

O que esse resultado implica sobre essas solicitações DNS específicas? Qual é o significado maior?

O que pode ter criado essas consultas DNS codificadas e por que o DNS foi selecionado como meio de exfiltrar dados?