



A CYBERSECURITY GAME

Simeon Kakpovi

Greg Schloemer

Emily Hacker

Everton Berz

Thiago Marques

Azure Data Explorer

kc7latam1.eastus....

Adicionar conexão

Filtrar...

kc7latam1.eastus

BancoMares

- ArquivosCriados
- Autenticacao
- DnsPassivo
- Email
- Funcionarios
- NavegacaoExterna
- NavegacaoInterna
- Processos

Executar

Recall

1 Funcionarios

2 | take 100

3

4 Email

5 | take 100

Tabela 1 Estatísticas

timestamp	sender
> 2025-09-07 02:55:05.7390	robbie_lance@resor
> 2025-09-07 02:55:05.7390	robbie_lance@resor
> 2025-09-07 02:55:05.7390	robbie_lance@resor
> 2025-09-07 03:10:11.3910	atendimento ao clie

Introdução: Seja bem-vindo ao Banco Marés

Seja bem-vindo ao Banco Marés! Hoje é o seu primeiro dia como Analista Júnior de SOC (Security Operation Center) no nosso banco. Sua responsabilidade principal é proteger o Banco Marés e seus colaboradores de atividades maliciosas.



O Banco Marés é um banco com um nome que reflete a constante mudança e fluidez do mercado financeiro. Com uma abordagem inovadora e moderna, o Banco das Marés busca oferecer soluções financeiras personalizadas para cada cliente, priorizando a transparência e a segurança em todas as suas operações. Com o Banco das Marés, os clientes podem navegar com confiança em meio às marés do mercado financeiro.

O Banco Marés possui alguns clientes chaves que são importantes para se manter como um dos maiores bancos do país:

Cliente	Relacionamento
Oceanus Naval Ltda. (oceanusnaval.com.br)	A Oceanus é um parceiro importante para o Banco das Marés, pois ajuda a aumentar a sua presença no setor de transporte marítimo.
Aqua Farms SA (aquafarms.com.br)	O Banco das Marés fornece empréstimos para a Aqua Farms para expandir sua produção e construir novos tanques de criação. Em troca, a Aqua Farms mantém suas contas bancárias no Banco das Marés e utiliza seus serviços financeiros.
Resort Pé na Areia Ltda. (penaareia.com.br):	A Resort Pe na Areia Ltda é um cliente valioso para o Banco das Marés, pois gera um grande volume de negócios através do processamento de pagamentos de seus hóspedes e do gerenciamento de suas contas bancárias.

Nos últimos meses o Banco Marés implementou uma nova versão dos sistemas internos do banco, centralizando todos os processos utilizados pelas agências espalhadas pelo Brasil assim como também nos meios digitais. Com isso, o banco também viu a necessidade de investir mais na segurança. Por isso você foi contratado!

Como toda boa empresa, o Banco Marés coleta logs de dados de atividades que seus colaboradores realizam na rede corporativa. Estes logs de auditoria de segurança são armazenados no **Azure Data Explorer (ADX)** – um serviço de armazenamento de dados na Azure (nuvem da Microsoft). Você vai utilizar o Kusto Query Language (KQL) para analisar

diversos tipos de logs de segurança. Analisando estes logs você poderá nos ajudar a identificar se estamos sendo alvo de cibercriminosos.



Você pode encontrar a documentação completa do ADX aqui:

<https://learn.microsoft.com/pt-br/azure/data-explorer/kusto/query/tutorials/learn-common-operators?pivots=azuredataexplorer>

Objetivos

 No fim do seu primeiro dia de trabalho, você deve ser capaz de:


- ✓ Utilizar o Azure Data Explorer
- ✓ Utilizar vários conjuntos de dados para responder a perguntas específicas
- ✓ Encontrar atividade cibernética em logs incluindo: email, tráfego de navegação e logs de servidores
- ✓ Utilizar técnicas diversas para monitorar as atividades de ataques direcionados conhecidos como APTs (Advanced Persistent Threats)
- ✓ Utilizar dados de terceiros para descobrir informações adicionais sobre seus atacantes
- ✓ Desenvolver um relatório de inteligência de ameaças (Threat Intelligence Report)
- ✓ Recomendar ações que devem ser tomadas pelo banco para se proteger


Os atacantes já largaram na frente, então não vamos perder mais tempo ... hora de começar a trabalhar!


Alguns links interessantes:

- Placar KC7: <https://kc7cyber.com/scoreboard>
- Azure Data Explorer: <https://aka.ms/kc7bancomares>

Legenda

 **Ponto Chave** – Ocasionalmente, você irá encontrar um emoji de um dardo com um “ponto chave”. Eles sinalizam explicações de certos conceitos que podem ajudar no entendimento de ideias chaves de cibersegurança que são demonstradas no jogo.

 **Pergunta** – Os emojis “pensativo” representam perguntas que vão te permitir demonstrar domínio do conteúdo. Você poderá ganhar pontos ao responder as questões da sessão 3 no portal de pontuação disponível em kc7cyber.com/scoreboard.

 **Dica** – Os emojis “sussurrar” representam dicas do jogo. Estas dicas vão te mostrar o caminho certo ao responder algumas das perguntas.

Seção 1: Passo-a-passo

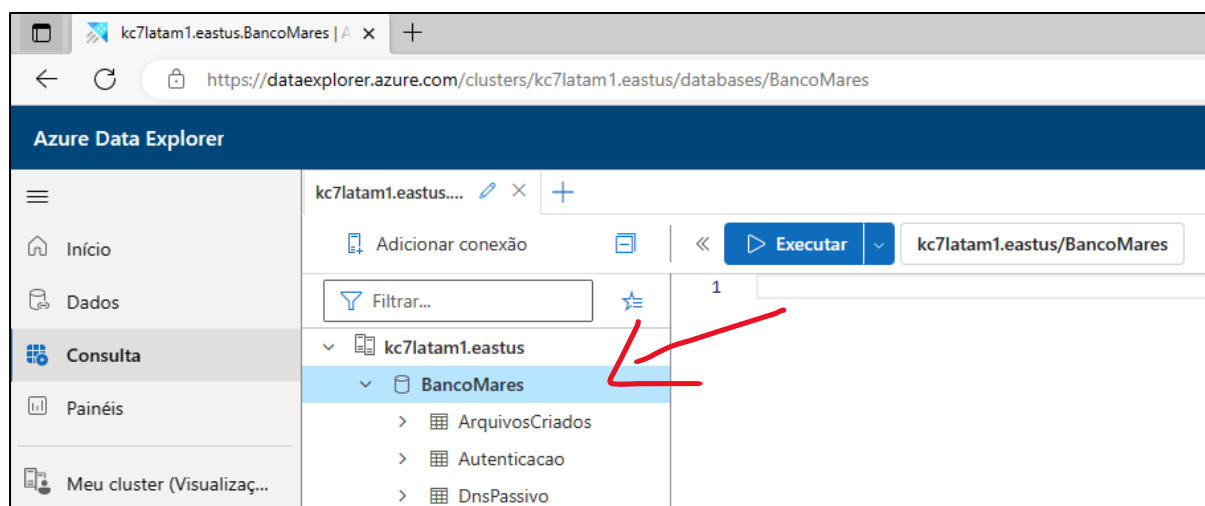
Como acessar o Azure Data Explorer (ADX)

ADX é a principal ferramenta utilizada no COS (Centro de Operações de Segurança – SOC em inglês) do Banco Marés para exploração e análise de dados. O grande diferencial do ADX é que ele é usado por analistas cibernéticos em muitas das menores e maiores organizações do mundo.

Vamos fazer com que você se conecte e comece a usar o ADX:

1. Acesse <https://aka.ms/kc7bancomares>
2. Faça o login com suas credenciais de conta no microsoft.com. Você pode usar suas credenciais de conta Hotmail.com, outlook.com, live.com, ou O365.

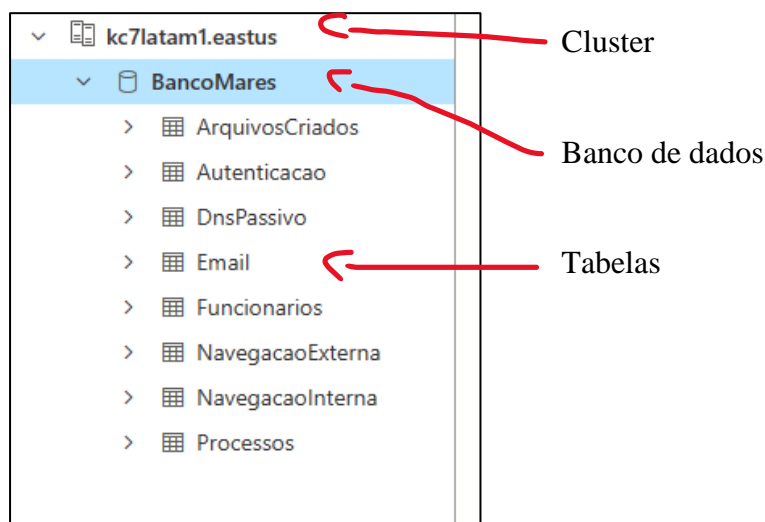
Uma vez conectado, você deve ver um cluster chamado "kc7latam1.eastus" que já foi adicionado à sua conta.



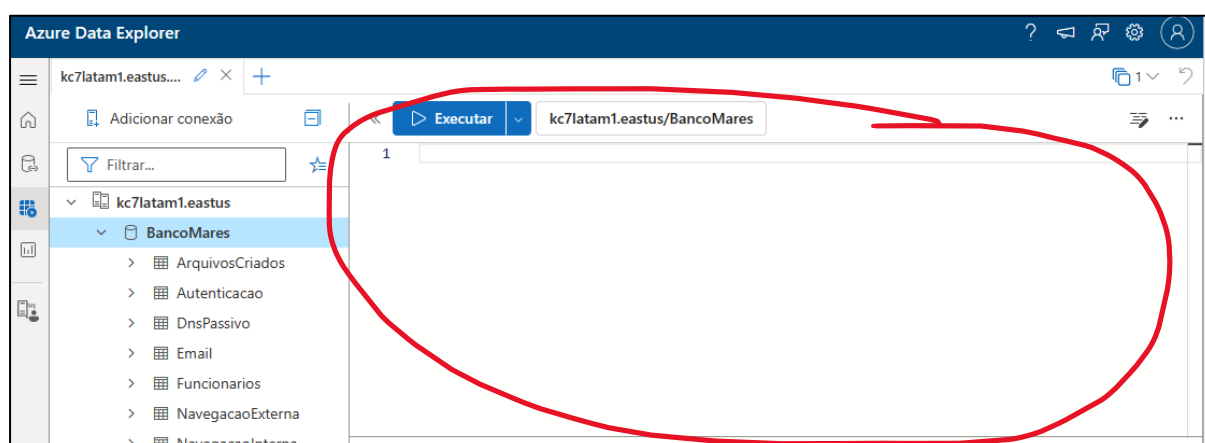
Os dados no ADX são organizados em uma estrutura hierárquica que consiste em **clusters**, **bancos de dados** e **tabelas**.

Todos os registros de segurança do Banco Marés são armazenados em um único banco de dados - o banco de dados BancoMares.

1. Selecione seu banco de dados
 - a. Expanda a seta ao lado do banco de dados **BancoMares**.
 - b. Clique no banco de dados **BancoMares**. Uma vez feito isto, você deve ver o banco de dados em destaque - isto significa que você selecionou o banco de dados e está pronto para consultar as tabelas dentro.



O grande espaço em branco à direita de sua lista de clusters é o espaço de trabalho de consulta. É lá que você realmente escreverá as consultas usadas para interagir com nossos dados de registro.




É isso então, chega de apresentações... mãos a obra!

Vamos dar uma olhada nos dados...

O banco de dados **BancoMares** contém oito tabelas. As tabelas contêm muitas linhas de dados semelhantes. Para fins de segurança, uma única linha normalmente representa uma única coisa feita por um funcionário ou um dispositivo na rede em um determinado momento.

Atualmente, temos oito tipos de dados de log. Como você verá no ADX, cada tipo de log corresponde a uma tabela que existe no banco de dados **BancoMares**:

Tabela	Descrição
Funcionarios	Contém informações sobre os funcionários da empresa
Email	Registra os e-mails enviados e recebidos pelos funcionários
NavegacaoInterna	Registra a atividade de navegação na Internet dentro da rede da empresa
NavegacaoExterna	Registra a atividade de navegação da empresa para fora da Internet
Autenticacao	Registra logins bem-sucedidos e fracassados em dispositivos da rede da empresa. Isto inclui logins para o servidor de correio da empresa.
ArquivosCriados	Registra os arquivos armazenados nos dispositivos dos funcionários
Processos	Registra processos criados nos dispositivos dos funcionários
DnsPassivo (Externo)	Registra as resoluções de domínio IP

 **Ponto Chave— Dados “Over the Horizon (OTH)”**: Uma das tabelas listadas acima não é como as outras - DnsPassivo. Ao invés de ser um log de segurança interna, DnsPassivo é uma fonte de dados que adquirimos de um fornecedor terceirizado. Nem toda atividade cibernética maliciosa acontece dentro da rede de nossa empresa, portanto, às vezes dependemos de dados de outras fontes para completar nossas investigações.

Você aprenderá mais sobre como usar cada um desses conjuntos de dados em apenas um minuto. Primeiro, vamos apenas fazer algumas consultas para que você possa praticar usando KQL e ADX.

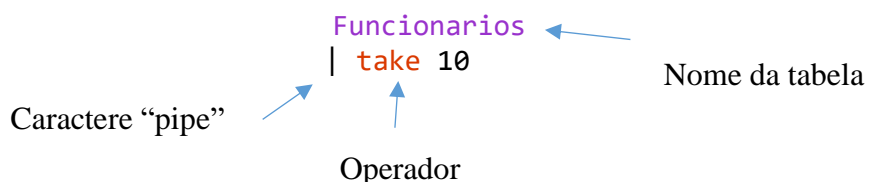
Introdução ao KQL

Digite a seguinte consulta no espaço de trabalho para visualizar as primeiras linhas na tabela de Funcionarios. Pressione "executar" ou "shift + enter" para executar a consulta.

Funcionarios


| take 10

Esta consulta tem algumas partes. Vamos dividi-la para entender melhor:



Componente da Consulta	Descrição
Nome da tabela	O nome da tabela especifica de qual tabela/origem de dados a consulta vai extrair os dados. Todas as consultas devem começar com uma tabela.
Caractere Pipe ()	O caractere pipe indica o início de uma nova parte da consulta. Um pipe será adicionado automaticamente após digitar o nome de uma tabela e pressionando enter. Você também pode adicionar um caractere pipe manualmente por segurando a tecla shift e pressionando a tecla backslash (\). Ela está logo abaixo da tecla backspace.
Operador	O operador diz à consulta o que exatamente você quer fazer. O primeiro operador que você aprendeu é take, que simplesmente pega um determinado número de linhas e mostra os dados lá. Você vai aprender e praticar mais operadores em breve!

O operador **take** é uma ferramenta poderosa que você pode usar para explorar linhas em uma tabela e, portanto, compreender melhor que tipos de dados são armazenados ali.

 **Ponto Chave – Como interagir quando você não sabe o que fazer:** Sempre que você estiver diante de uma tabela de banco de dados desconhecida, a primeira coisa que você deve fazer é consultar suas linhas usando o operador do take. Dessa forma, você sabe quais campos estão disponíveis para consulta e pode adivinhar que tipo de informação você pode extrair da fonte de dados.

A tabela de **Funcionarios** contém informações sobre todos os funcionários de nossa organização. Neste caso, podemos ver que a organização é denominada "Envolve Labs" e o domínio é "envovelabs.com".

1. 🤖 *Experimente você mesmo! Faça um **take 10** em todas as outras tabelas para ver que tipo de dados elas tem.*

Você pode facilmente escrever várias consultas na mesma aba de espaço de trabalho. Para fazer isso, certifique-se de separar cada consulta por uma linha vazia. Observe abaixo como separamos as consultas das tabelas **Funcionarios**, **Email** e **NavegacaoExterna** por linhas vazias nas linhas 3 e 6.

```

1  Funcionarios
2  | take 10
3
4  Email
5  | take 10
6
7  NavegacaoExterna
8  | take 10
-

```


Quando você tem várias consultas, é importante dizer ao ADX qual consulta você deseja executar. Para escolher uma consulta, basta clicar em qualquer linha que faça parte dessa consulta. Uma vez selecionada uma consulta, ela será destacada em azul, como visto nas linhas 4 e 5 acima.

Descobrimos quantidades: O operador *count*

Podemos usar o **count** para ver quantas linhas há em uma tabela. Isto nos diz quantos dados estão armazenados ali.

Funcionarios

| **count**

2. 🤖 Quantos empregados tem na empresa?

Filtrando dados com o operador *where*

Até agora, fizemos consultas que analisam todo o conteúdo da tabela. Muitas vezes, na análise cibernética de segurança, queremos olhar apenas os dados que atendem a um conjunto de condições ou critérios. Para isso, aplicamos filtros a colunas específicas.

Podemos usar o local onde o operador no KQL aplica filtros em um determinado campo. Por exemplo, podemos encontrar todos os funcionários com o nome "Linda", filtrando na coluna *name* na tabela de **Funcionarios**.

Instruções **where** são escritas utilizando uma estrutura específica. Use este gráfico útil abaixo para entender como estruturar uma instrução onde.

```
where campo operador "valor"
where name has "Linda"
```

Funcionarios

| **where name has "Linda"**


O operador **has** é útil aqui porque estamos procurando apenas uma correspondência parcial. Se quiséssemos procurar um funcionário com um nome e sobrenome específicos (uma correspondência exata), usaríamos o operador **==**:

Funcionarios

| **where name == "Linda Beck"**

3. 🤖 Cada funcionário no Banco Marés tem um IP associado. Qual funcionário tem o IP "192.168.0.191"?

Enquanto realizam suas tarefas diárias, os funcionários do Banco Marés enviam e recebem e-mails. Um registro de cada um desses e-mails é armazenado na tabela Email.

 **Ponto Chave – Privacidade dos Usuários e Metadados:** Como você pode imaginar, alguns e-mails são altamente sensíveis. Em vez de armazenar todo o conteúdo de cada e-mail enviado e recebido dentro da empresa em um banco de dados que pode ser facilmente acessado pelos analistas de segurança, nós só capturamos metadados de e-mail.

Os metadados de e-mail incluem informações como: a hora em que o e-mail foi enviado, o remetente, o destinatário, a linha de assunto, e quaisquer links que o e-mail possa conter. O armazenamento apenas de metadados de e-mail, ao invés de todo o conteúdo, ajuda a proteger a privacidade de nossos funcionários, ao mesmo tempo em que garante que nossos analistas de segurança possam nos manter seguros. Às vezes até mesmo os metadados podem revelar informações sensíveis, portanto é importante que você não fale sobre dados de registro com outros funcionários fora do SOC.

Podemos encontrar informações sobre os e-mails enviados ou recebidos por um usuário, procurando seu endereço de e-mail nos campos remetente e destinatário da tabela de **Email**. Por exemplo, podemos usar a seguinte consulta para ver todos os e-mails enviados por "Patricia Ware":

```
Email
| where sender == "patricia_ware@bancomares.com.br"
```

4. 🤖 *Quantos emails o funcionário Florentino Hernandez **recebeu**?*

Tão fácil quanto contar até 3... Consultas compostas e o operador *distinct*

Podemos usar o operador **distinct** para encontrar valores únicos em uma determinada coluna. Podemos usar a seguinte consulta para determinar quantos dos usuários da organização enviaram e-mails.

```
1 Email
2 | where sender has "bancomares"
3 | distinct sender
4 | count
-
```

Esta é nossa primeira vez usando uma consulta multi-linha com vários operadores, então vamos quebrar isso:

Na **linha 2**, pegamos a tabela de e-mail e filtramos os dados para encontrar apenas aquelas linhas com "envovelabs" na coluna do remetente.

Na **linha 3**, adicionamos outro caractere de tubo (|) e usamos o operador distinto para encontrar todos os remetentes exclusivos. Aqui, não estamos encontrando os remetentes únicos para todos os remetentes de e-mail, mas somente os remetentes únicos que são deixados após aplicarmos o filtro procurando linhas com "envovelabs" na coluna do remetente.

Finalmente, na **linha 4**, adicionamos outro caractere de tubo (|) e depois usamos o operador de contagem para contar os resultados das linhas 1-3 da consulta.

5. 🤖 *Quantos usuários receberam emails com o termo “ataques” no título (subject)?*

Rastreamento os cliques: NavegacaoExterna

Quando os funcionários do Banco Marés navegam em um site da Internet, essa atividade de navegação é registrada. Isto é armazenado na tabela **NavegacaoExterna**, que contém registros dos websites navegados por cada usuário da empresa. Sempre que alguém visita um website, um registro do mesmo é armazenado na tabela. Entretanto, o nome do usuário não é armazenado na tabela, apenas seu endereço IP é registrado. Existe uma relação 1:1 entre os usuários e seus endereços IP atribuídos, portanto, podemos consultar as tabelas de **Funcionarios** e **NavegacaoExterna** para descobrir quem navegou em um determinado website.

Se quisermos descobrir quais sites Maria Cameron visitou, podemos encontrar seu endereço IP a partir da tabela de Funcionarios.

```
Funcionarios  
| where name == "Maria Cameron"
```


A consulta acima nos diz que seu endereço IP é "192.168.0.144". Podemos pegar seu endereço IP e procurar na tabela **NavegacaoExterna** para determinar quais sites ela visitou.

```
NavegacaoExterna  
| where src_ip == "192.168.0.144"
```

6. 🤖 *Quantas visitas únicas a websites externos o funcionário “Fernando Lucas” fez?*

O que tem por trás dos nomes nas URLs? Detalhes sobre DNS passivo

Embora nomes de domínio como "google.com" sejam fáceis de lembrar para os humanos, os computadores não sabem como lidar com eles. Portanto, eles os convertem em endereços IP legíveis por máquina. Assim como o endereço de sua casa diz a seus amigos como encontrar sua casa ou apartamento, um endereço IP diz a seu computador onde encontrar uma página ou serviço hospedado na Internet.

 **Ponto Chave – Boas Práticas OPSEC:** Se quisermos descobrir qual endereço IP um determinado domínio resolve, podemos simplesmente navegar até ele. Mas, se o domínio for malicioso, você poderia baixar arquivos maliciosos para seu sistema de análise corporativo ou avisar os atacantes que você conhece sobre sua infra-estrutura. Como analistas de segurança cibernética, devemos seguir procedimentos e salvaguardas que protejam nossa capacidade de rastrear ameaças. Estas práticas são geralmente chamadas de segurança operacional, ou OPSEC.

Para eliminar a necessidade de *resolver ativamente* (ou seja, navegar diretamente ou interagir com um domínio para encontrar seu endereço IP relacionado) cada domínio que nos interessa, podemos confiar nos dados *DNS passivos*. Os dados DNS passivos nos permitem explorar com segurança as relações entre domínio e IP, para que possamos responder perguntas como:

- Para quais endereços IP este domínio resolve?
- Quais domínios estão hospedados neste endereço IP?
- Quantos outros IPs este domínio resolve?

Estes relacionamentos domínio-para-IP estão armazenados na tabela **DnsPassivo**.

7. 🤖 Quantos domínios nos registros de **DnsPassivo** contém a palavra “hack”? (dica: use o operador **contains** ao invés de **has**. Se você não avançar, faça um **take 10** na tabela para ver as colunas disponíveis.)

8. 🤖 Para quais IPs o domínio “sandbank.org” resolve?

🤖 Instruções “Let” – Tornando nossa vida mais fácil:

Às vezes precisamos usar a saída de uma consulta como entrada para uma segunda consulta. A primeira maneira de fazer isso é digitando manualmente os resultados na próxima consulta.

Por exemplo, e se quisermos ver toda a atividade de navegação na web dos funcionários chamados “Linda”?

Primeiro, você precisaria entrar na tabela **Funcionarios** e encontrar os endereços IP usados por estes empregados.

1Funcionarios

2| where name has "Linda"

Tabela 1

Estatísticas

Pesquisar

UTC

Concluído (0.806 s)

9 registros

timestamp	name	user_agent	ip_addr
> 2013-08-21 23:09:20.8900	Linda Barnes	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537...	192.168.3.112
> 2014-01-25 12:01:07.2200	Linda Smith	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/2010...	192.168.2.2
> 2014-12-11 16:27:25.5890	Linda Dixon	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; ...	192.168.2.144
> 2019-07-05 01:13:58.2100	Linda Beck	Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML...	192.168.0.125

Então, você poderia copiar e colar manualmente estes IPs em uma consulta contra a tabela de **NavegacaoExterna**. Note que podemos usar o operador “*in*” para escolher todas as

linhas que têm um valor correspondente a qualquer valor a partir de uma lista de valores possíveis. Em outras palavras, o operador `==` (comparação) procura por uma correspondência exata, enquanto o operador `"in"` procura por quaisquer valores da lista.

1 NavegacaoExterna
2 | where src_ip in ("192.168.3.112", "192.168.2.2", "192.168.2.144", "192.168.0.125", "192.168.2.144")
3
4
5

Tabela 1 Estatísticas Pesquisar UTC Concluído (0.325 s) 83 registros

timestamp	method	src_ip	user_agent	url
> 2023-02-19 06:14:16.8200	GET	192.168.2.2	Mozilla/5.0 (Windows ...	http://baggages-incisiveness.com/...
> 2023-02-19 07:11:19.4310	GET	192.168.1.21	Mozilla/5.0 (Windows ...	https://nakedthermals.us/online
> 2023-02-19 12:30:07.4510	GET	192.168.1.21	Mozilla/5.0 (Windows ...	psycholinguists.biz/share/modules?...
> 2023-02-19 12:43:59.9390	GET	192.168.1.71	Mozilla/5.0 (Windows ...	http://porthole-labvrinthine.net/se...

Embora esta seja uma forma válida de obter as informações necessárias, pode não ser tão elegante (ou oportuna) se você tivesse 100 ou mesmo 1000 funcionários chamados "Linda".

Podemos fazer isso de forma mais elegante usando uma instrução "let", que nos permite atribuir um nome a uma expressão ou a uma função. Podemos usar uma instrução *let* aqui para salvar e dar um nome aos resultados da primeira consulta, para que os valores possam ser reutilizados posteriormente. Isso significa que não precisamos digitar ou copiar e colar os resultados manualmente repetidamente.

```
1 let linda_ips = Funcionarios
2 | where name has "Linda"
3 | distinct ip_addr;
4 NavegacaoExterna
5 | where src_ip in (linda_ips)
```

À esquerda da declaração `let` está o nome da variável ("linda_ips" neste caso). O nome da variável pode ser qualquer coisa que desejarmos, mas é útil escolher um nome que tenha significado e nos ajude a lembrar quais valores estão sendo armazenados nela.

```
1 let linda_ips = Funcionarios
2 | where name has "Linda"
3 | distinct ip_addr;
4 NavegacaoExterna
5 | where src_ip in (linda_ips)
6
```

No lado direito da declaração `let` está a expressão que você está armazenando. Neste caso, usamos o operador `distinct` para selecionar valores de apenas uma coluna - então eles são armazenados em um array - ou lista de valores.

```


1  let linda_ips = Funcionarios
2  | where name has "Linda"
3  | distinct ip_addr;
4  NavegacaoExterna
5  | where src_ip in (linda_ips)
-

```

Note que a instrução `let` é concluída usando o sinal de ponto-e-vírgula.

Depois que armazenamos o valor de uma consulta em uma variável usando a declaração `let`, podemos nos referir a ela quantas vezes quisermos no restante da consulta. A consulta armazenada não mostra nenhum resultado. Lembre-se, no entanto, de que sua consulta KQL deve ter uma declaração tabular - o que significa que você deve ter outra consulta seguindo sua declaração `let`.

9. 🤔 *Quantas URLs únicas (distintas) foram acessadas pelos empregados com nome "Maria"?*

 **Ponto Chave – Pivotando:** Parte do trabalho de ser um grande analista de cibersegurança é aprender como usar múltiplas fontes de dados para contar uma história mais completa do que um atacante fez. Chamamos isso de "pivotagem". Fazemos isso ao pegar um dado conhecido em um conjunto de dados e procurar em outro conjunto de dados para aprender algo que ainda não sabíamos. Você praticou isso aqui quando começamos em um conjunto de dados - a tabela de funcionários - e usamos o conhecimento de lá para encontrar dados relacionados em outra fonte - NavegacaoExterna.

Seção 2: Apresentando os Hackers

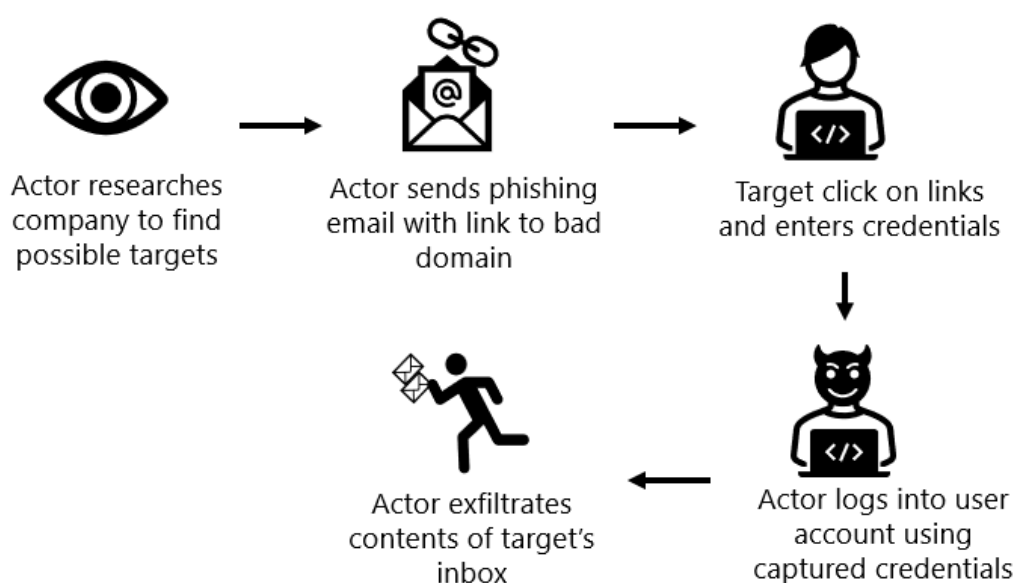
Agora que você completou a rodada inicial de treinamento, você está pronto para trabalhar no seu primeiro caso no SOC!


Um pesquisador de segurança tuitou que o domínio “immune.tech” estava sendo utilizado por hackers. Aparentemente os hackers estavam utilizando este domínio em emails de phishing.



⚠️ ATENÇÃO! Este domínio e outros utilizados neste jogo são fictícios e não representam atividade maliciosa real.


De acordo com a pesquisa de OSINT que seus colegas realizaram, este domínio pode ter sido utilizado como parte de uma campanha de phishing com as seguintes etapas:



 **Ponto chave – Open Source Intelligence (OSINT):** Pesquisadores de segurança e analistas normalmente utilizam dados gratuitos, disponíveis publicamente, como o Twitter por exemplo! Nós chamamos estes dados públicos de OSINT, e eles podem ser uma ótima forma de obter pistas para a investigação. Assim como todos os dados públicos na internet, você deve complementar qualquer dados coletado por OSINT com uma análise rigorosa, e não confiar totalmente na fonte.

 Responda as seguintes perguntas relacionadas a esta dica:

1. Quais usuários na nossa empresa que receberam emails contendo o domínio `imune.tech`?
2. Nós conseguimos bloquear alguns dos emails enviados contendo este domínio? Quem realmente recebeu este email na caixa de correio? (dica: o campo “accepted” na tabela **Email** indica se o email foi bloqueado ou não. Emails bloqueados vão aparecer como “false”).
3. Que outros domínios utilizam o mesmos IPs que o `imune.tech`? Você consegue encontrar a lista completa de domínios associados com esse ator baseado em dados de PassiveDns? (dica: você pode utilizar o operador **in** para verificar por múltiplos valores em um campo. E.x. `where campo in (“x”, “y”, “z”)`)
4. Quais endereços de email os hackers utilizaram para enviar estes emails?
5. Os usuários clicaram em algum dos links enviados nos emails de phishing?
6. Algum usuário teve a credencial roubada? Como você sabe?

 **Dica:** Para ter a credencial roubada, o usuário precisa acessar o site falso e digitar os dados de acesso, como usuário e senha. Após isso, o ator pode tentar logar na conta do usuário utilizando as credenciais roubadas. Você pode encontrar detalhes sobre as atividades de login na tabela **AuthenticationEvents**.

7. Algum usuário teve conteúdo exfiltrado (roubado) da caixa de correio? Como você sabe essa informação? Que riscos este conteúdo roubado pode trazer para a empresa?

Section 3: Hackers sending malware docs


After digging for a bit on the phishing activity, you come across another tweet from a threat intelligence vendor SolitaryStrike:




🧐 Use the tipper above to answer the following questions:
You can optionally submit your answers to the scoreboard at <https://kc7cyber.azurewebsites.net/> to get feedback and earn points.

1. How many emails contained the domain notice[.]io?
2. What email address sent the domain notice[.]io
3. What was the subject line of the emails containing the domain notice[.]io?
4. What is the name of the user who clicked on the notice[.]io link?
5. At what timestamp did the user above download the file: "Critical_Security_Path.docx"?
6. How many emails were sent to your organization on January 9th by users at wesellbeakers.com?
7. What other domains are hosted on the same IPs as notice[.]io?
8. What email address is seen sending emails containing one of the domains identified in question 7?
9. How many users downloaded the files observed in the emails from question 8?


10. One of the files observed in question 9 - IMPORTANT_INSTRUCTIONS.pptx - was seen in two separate emails. What are the subject lines of these emails?
11. Which compromised pharmasupplies.org email address was used to send a link to scanverify.com?
12. How many IPs has scanverify.com resolved to?
13. Consider the email address you found in question 11. What other domain did this email address send?
14. What is the name of the file hosted on scanverify.com?
15. Which .pptx file was used to target Gerald Kempinski and Kenny Salcido?
16. Which actor IP was used to search EnvolveLabs' website for the term "helpdesk ticket system"?
17. How many total emails were sent to your organization by this actor?
18. Which .dll file was dropped on a victim machine shortly after the user downloaded the malicious zip : EnvolveLabs_Research_Tool.7z

 **Hint:** Files that are created on employees' devices are captured in the **FileCreationEvents** log. Try looking there to see which employees downloaded this file.

19. Which six letter reconnaissance command was executed on the Machine of the user that loaded the implant above?

 **Hint:** Try narrowing down on one particular device that downloaded the EnvolveLabs_Research_Tool.7z file. Then, look in both the **FileCreationEvents** and **ProcessEvents** logs to find new files and processes created around the time when the file was downloaded.

20. A malicious file 'infector.exe' is observed performing suspicious actions on multiple devices. What process_commandline associated with this file is being used for persistence on the devices?

 **Hint:** Actors establish persistence so they can come back later and conduct manual tasks (called hands-on-keyboard activity) within your company's network. Try looking for systems creating connections to external domains and IPs, or unusual behaviors like creation of scheduled tasks.