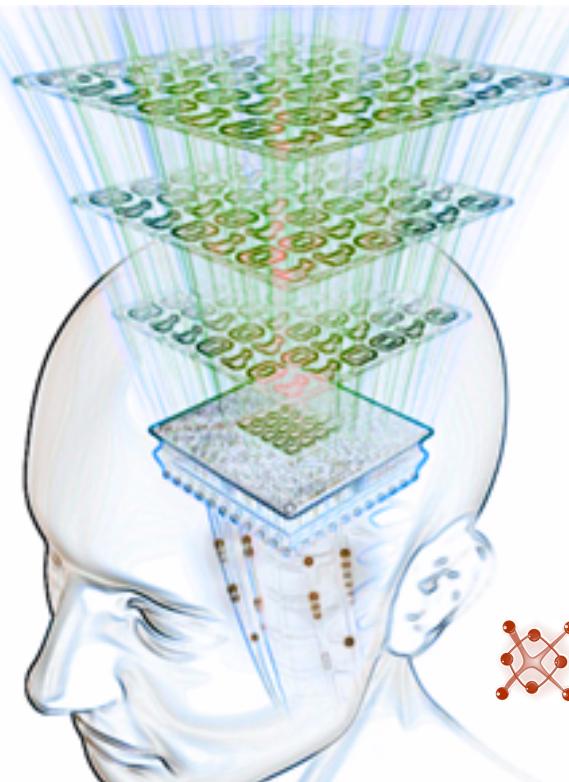


Microsoft BlueHat 2018

CyGraph: Big-Data Graph Analysis For Cybersecurity and Mission Resilience

Steven Noel, PhD
The MITRE Corporation

September 25, 2018



Security Tools Landscape – Too Much Data, Too Little Context

Intrusion Detection System

Short IDS Console Unfilter Refresh every 30 secs. View alerts since 9 AM or on

Alert Information			Sensors			Top Sources			Top Targets			Top Target Ports		
	%	Sensor	#	%	Sigs Alerts	IP Address	Sigs	Alerts	IP Address	Sigs	Alerts	TCP	Udp	ICMP
Signatures	82		19	19	182	6	188	6	513	513	155	128	128	128
TCR Alerts	1.12	42%	13	13	132	13	132	13	5	5	5	24	24	24
UDP Alerts	1.52	57%	11	11	240	3	21	3	24	443	443	133	24	24
ICMP Alerts	0	0%	11	11	131	2	108	2	352	352	143	122	111	111
Total Alerts	2,649	100%	9	9	298	2	92	2	92	3388	19	68		

Alert Overview by Signature

Earliest Alert: 2004-12-26 06:01:33
Latest Alert: 2004-12-29 05:15:12

Signatures					
	# Sensors	# Alerts	# Scts	# Dests	
1 WEB-MSC-2005 idle connection attempt [sig 1427]	2	355	2	2	2
1 WEB-MSC-2005 idle connection attempt [sig 1427]	1	1	1	1	1
1 MS-SQL-SMB raise error possible buffer overflow [sig 1380]	2	145	3	40	
1 WEB-MSC-NetDiscover authentication bypass attempt [sig 2441]	2	117	1	1	
1 MS-SQL-SMB cmshell program execution [sig 681]	1	110	1	1	
1 WEB-MSC-PCT Client -Hello overflow attempt [sig 2151]	2	33	1	1	
1 MS-SQL-up_cmshell program execution [sig 687]	2	25	1	8	
1 MS-SQL-up_cmshell up ready access [sig 689]	1	17	2	1	
1 MS-SQL-SMB raise error possible buffer overflow [sig 1427]	2	15	1	1	
1 MS-SQL-SMB raise error possible buffer overflow [sig 1427]	1	10	1	1	
1 MS-SQL-sp_start_job_program_execution [sig 673]	2	10	1	1	
1 MS-SQL-sp_start_job_program_execution [sig 673]	2	6	1	1	
1 MS-SQL_sa login failed [sig 688]	1	5	1	1	

Vulnerability Scanner

Firewall Manager

The screenshot shows the ACE Web Application Firewall Manager interface. The title bar reads "ACE Web Application Firewall Manager - Virtual Web Apps - Mozilla Firefox". The left sidebar contains a navigation tree with sections like Manager Dashboard, Policy Management, Resources, Reports & Tools, Administration, and Cisco. The main content area is titled "Virtual Web Applications" and shows a list of applications:

- Virtual Web Application [New]
- Dok Insurance App
- Security Resources [strict]
http://ve-example.com:8080/policy (prefix) => http://ve-example.com:8080
- External Developer App [pass-through profile]
http://ve-example0080/services (prefix) => http://ve-example:8080
- Customer Portal [PCI Compliance]
http://ve-target204.cisco.com:8080 (prefix) => http://ve-example.cisco.com:8080

Below the list, there's a note: "Set all virtual web apps to: - select mode - Set Use Monitor Mode by Default". At the bottom right, it says "ve-target204:8243".

Security Intelligence

The screenshot shows the CAPEC website's main page. At the top, there's a banner for the National Vulnerability Database (NVD) with links for Checklists, Product Dictionary, and Impact Metrics. The CAPEC logo is prominently displayed. Below the banner, the title "Common Attack Pattern Enumeration and Classification" is shown, followed by the subtitle "A Community Resource for Identifying and Understanding Attacks". On the left, a sidebar contains sections for "About CAPEC" (Documents, Glossary, FAQs), "CAPEC List" (Search, Review, Downloads, Documentation, Release Notes, Archive), "Submit Content", "Community" (Use & Citations, Related Activities, Discussion List), and "Attack". The main content area features a large "Security TechCenter" heading, a navigation bar with Home, Security Updates (highlighted in black), Tools, Learn, Library, and Support, and a sub-navigation bar with RESPONSE, BULLETINS, ADVISORIES, and MYBULLETINS. Below this is a large "Microsoft Security Bulletin" heading. Under "Upcoming Release", it says "Microsoft security bulletins are released on the second Tuesday of each month". Under "Latest Release", it says "Find the latest Microsoft security bulletins".

Security Information and Event Management (SIEM)

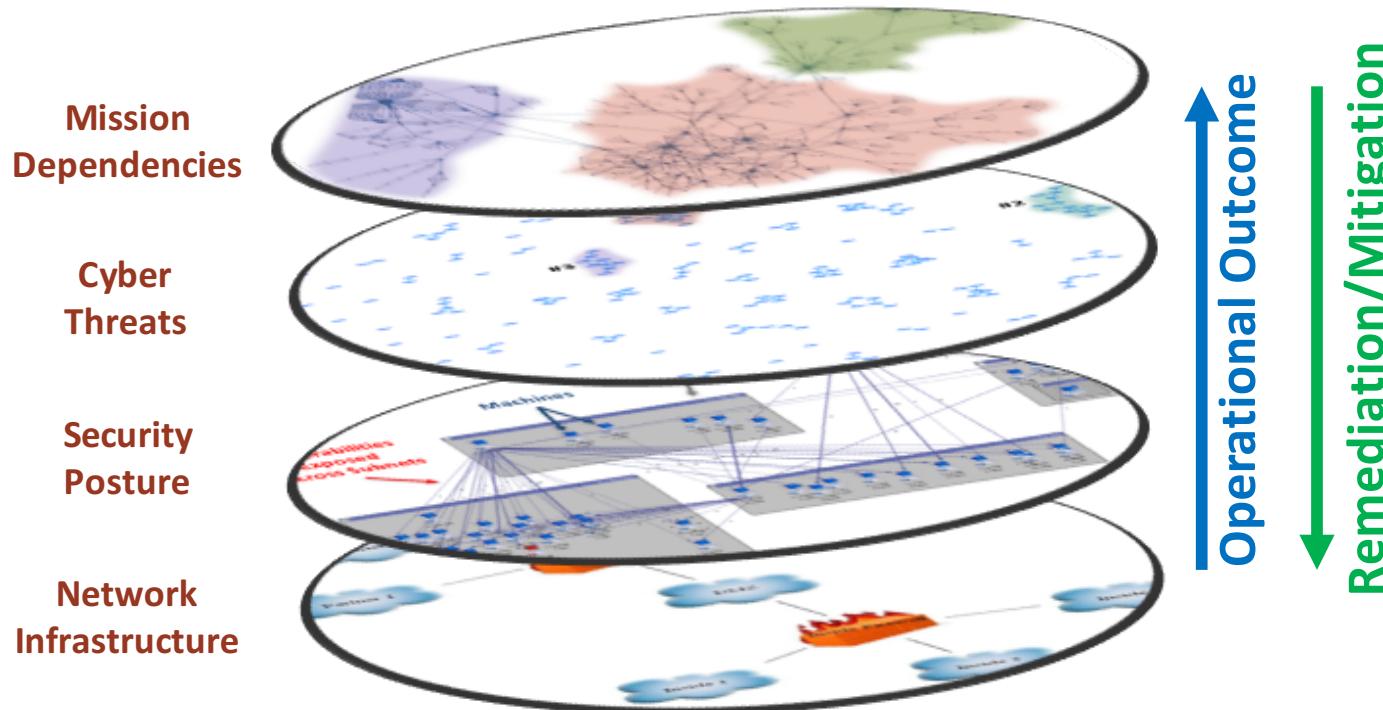
The screenshot displays the ArcSight Console interface with multiple windows open:

- Navigator:** Shows the navigation tree with sections like Resources, Packages, Use Cases, Dashboards, and Admin.
- Viewer:** The main workspace containing:
 - LogInsider EX Rule Firing:** A table of log entries with columns: End Time, Name, Device Event Class ID, User Acct EX, Config Change Type, and Rule ID.
 - LogInsider EX Rule Firing (Events):** A table of log entries with columns: End Time, Name, Device Event Class ID, User Acct EX, Config Change Type, and Rule ID.
 - Top Config Change Types:** A chart showing the total number of legends for different configuration change types.
 - Top Active Users:** A table of active users with their names, counts, and total log entries.
 - Event Inspector:** A detailed view of an event with tabs for Event, Details, Annotations, and Event Inspector.
- Inspect/Edit:** A sidebar for inspecting and editing objects, currently viewing the Exchange mailbox item properties.

At the bottom, there are status bars for the Navigator and Viewer, and a search bar.

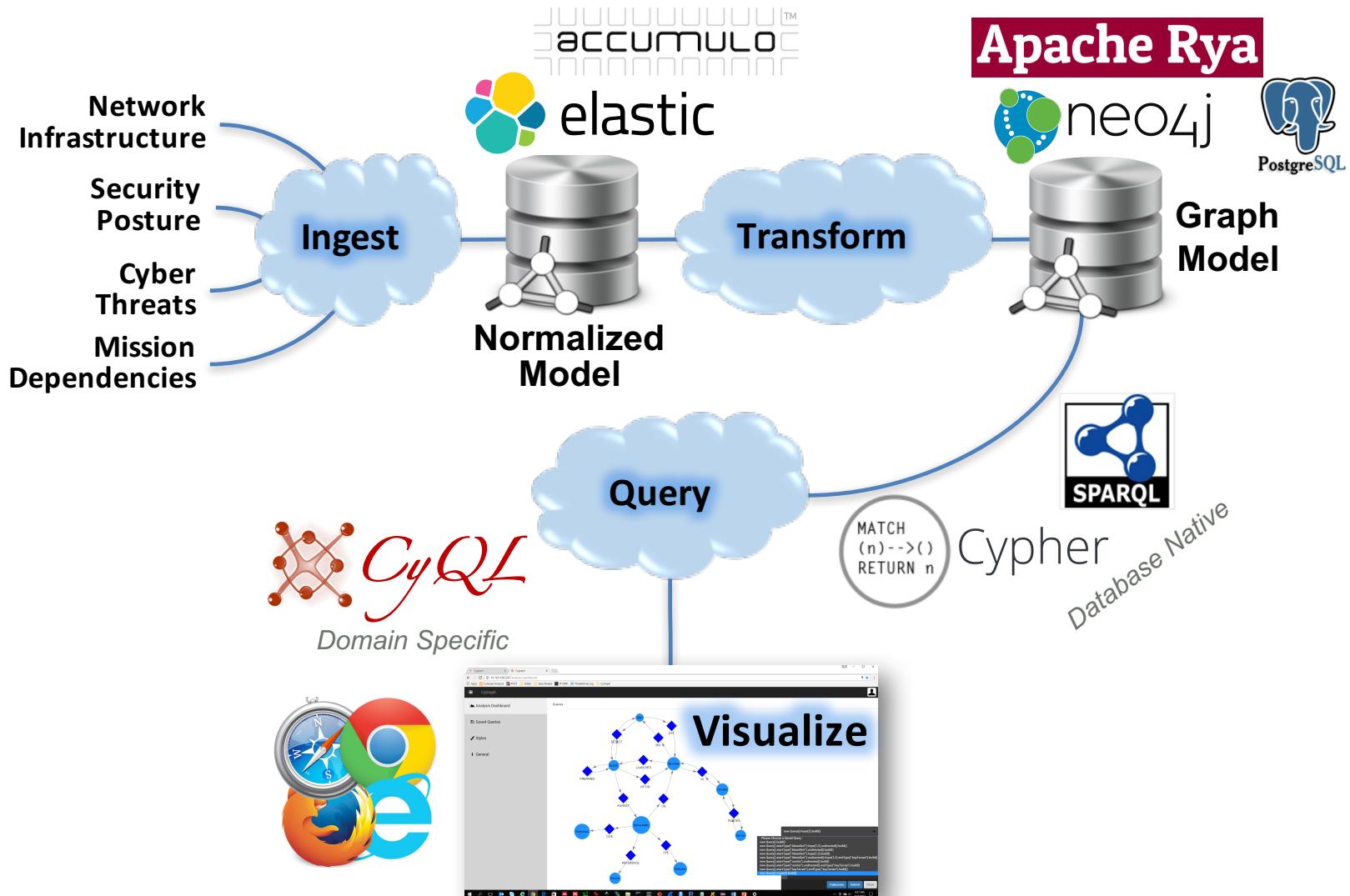
CyGraph Project Summary

- **CyGraph approach:**
 - Tool for capturing complex cybersecurity relationships in a graph knowledge base
 - Cyber-specific graph model, graph pattern matching queries, interactive visualization

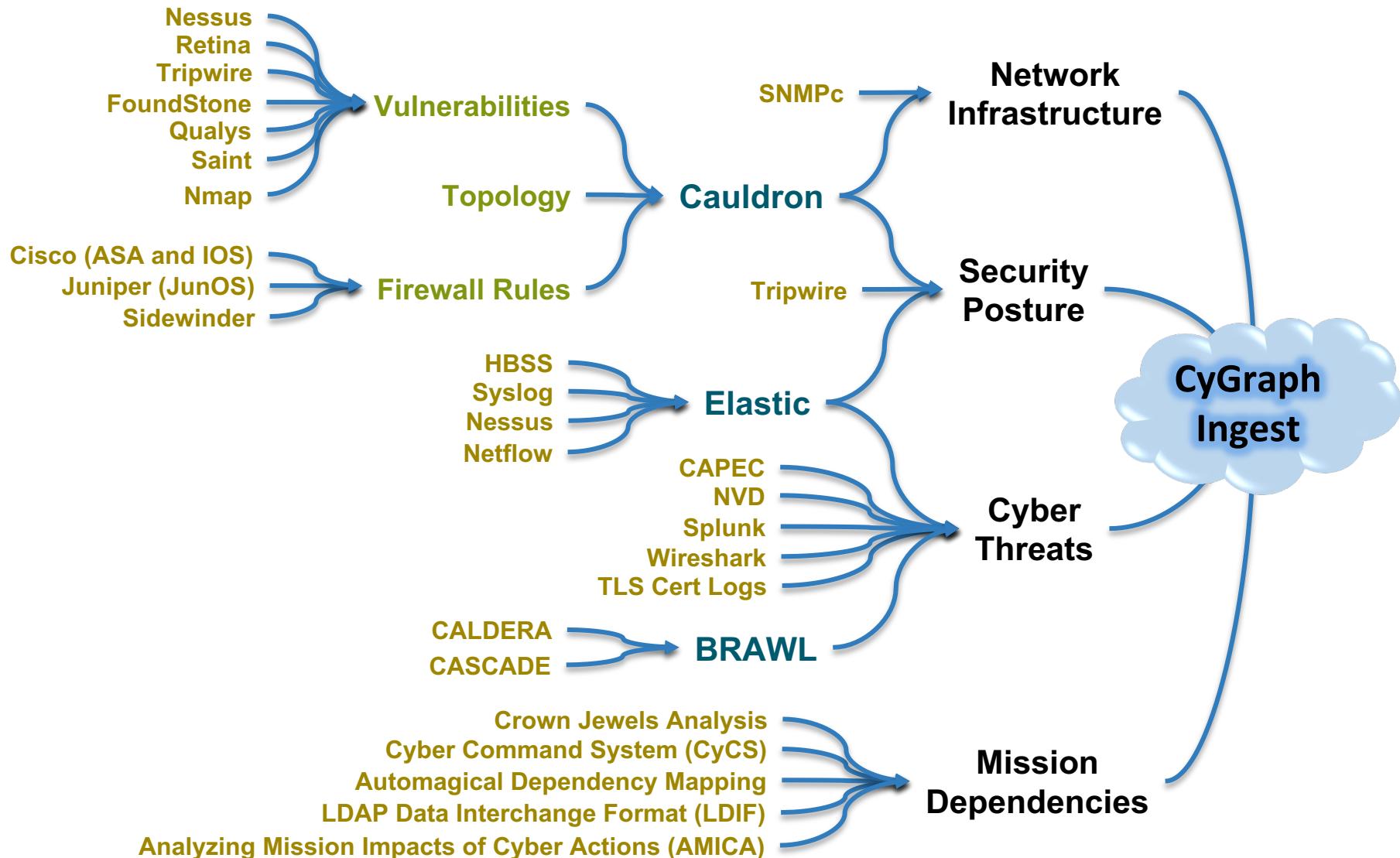


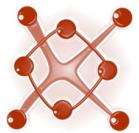
- **Example applications:** network hardening, alert correlation and prioritization, mission dependency/impact analysis
- **Outputs:** Application to 11 direct-funded projects, 18 publications, patent pending

CyGraph Architecture

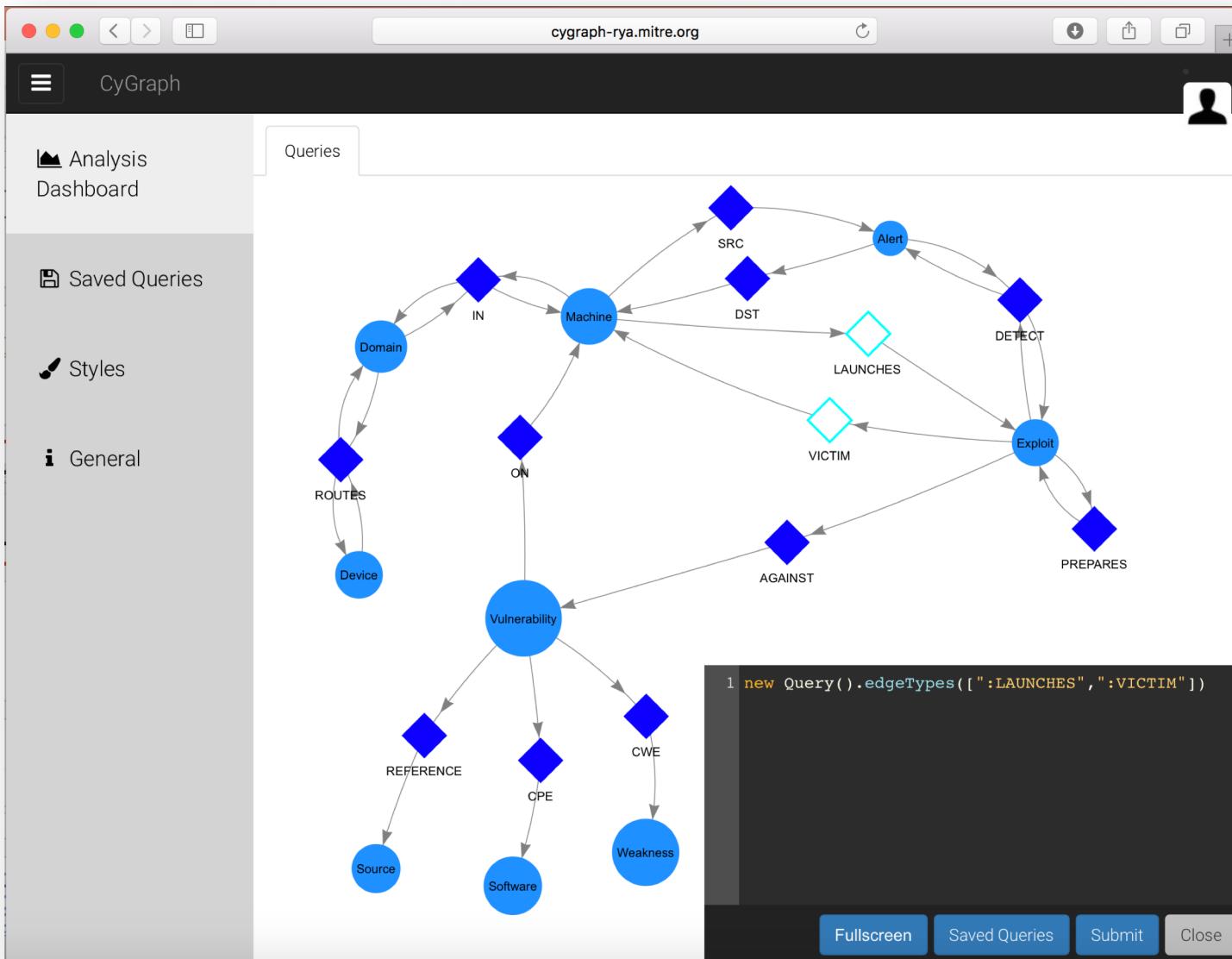


CyGraph Operational Data Sources





CyGraph Graph Model View



CyGraph Query Results

Analysis Dashboard

Saved Queries

Styles

Database Management

General

GUI Function Selection

Toolbar

Query Results Tabs

Query Results Visualization

Nodes Spreadsheet View

uid	Node	name
h	15689	h
h.1	15690	h.1
h.2	15691	h.2
h.3	15692	h.3
h.4	15693	h.4
h.5	15694	h.5

Options

- Lasso Mode
- Cursor Mode
- Clear Selection
- Nodes >
- Multiple Edges >
- Cluster... >
- Reset Zoom
- Show Toolbar
- Outgoing Nodes/Edges
- Incoming Nodes/Edges
- Incoming and Outgoing Nodes/Edges
- By All Properties
- By Node Properties
- Cluster Selected Nodes
- Expand Cluster

Node/Edge Properties

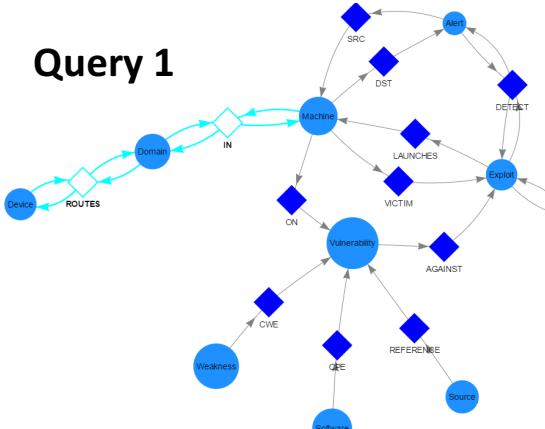
MATCH ()-[r*3]-(Compromised) 32 results (23 nodes, 24 edges)
RETURN r

Show Edges Tree View Physics Save Query Fullscreen Properties



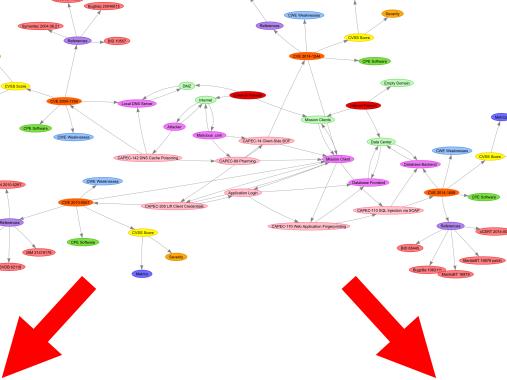
CyGraph Analytic Queries

Query 1

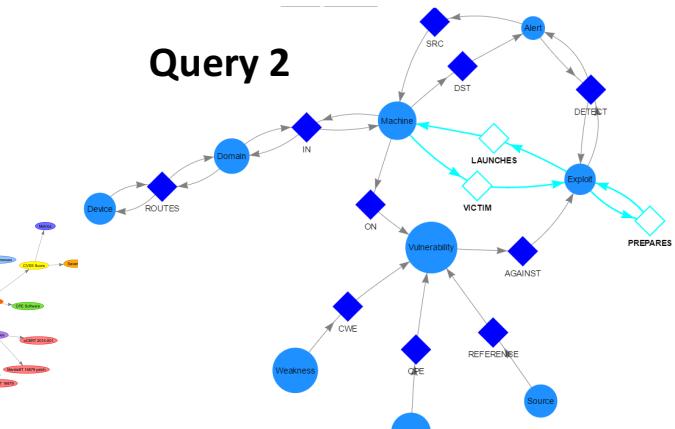


`edgeTypes(":IN", ":ROUTES")`

Full Graph

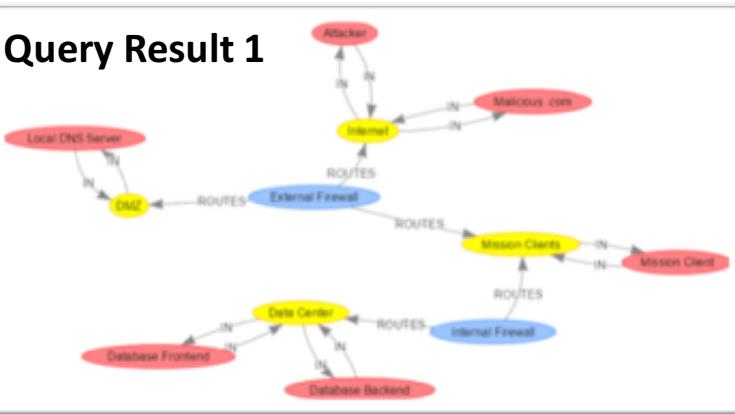


Query 2

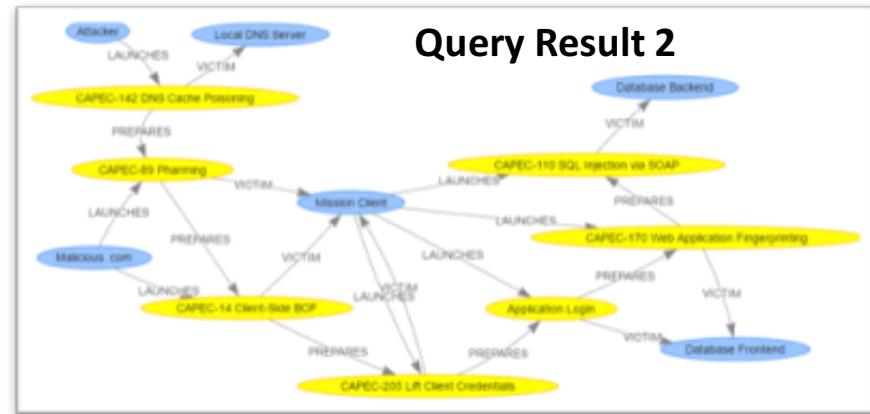


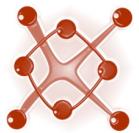
`edgeTypes(":PREPARE", ":LAUNCHES", ":VICTIM")`

Query Result 1

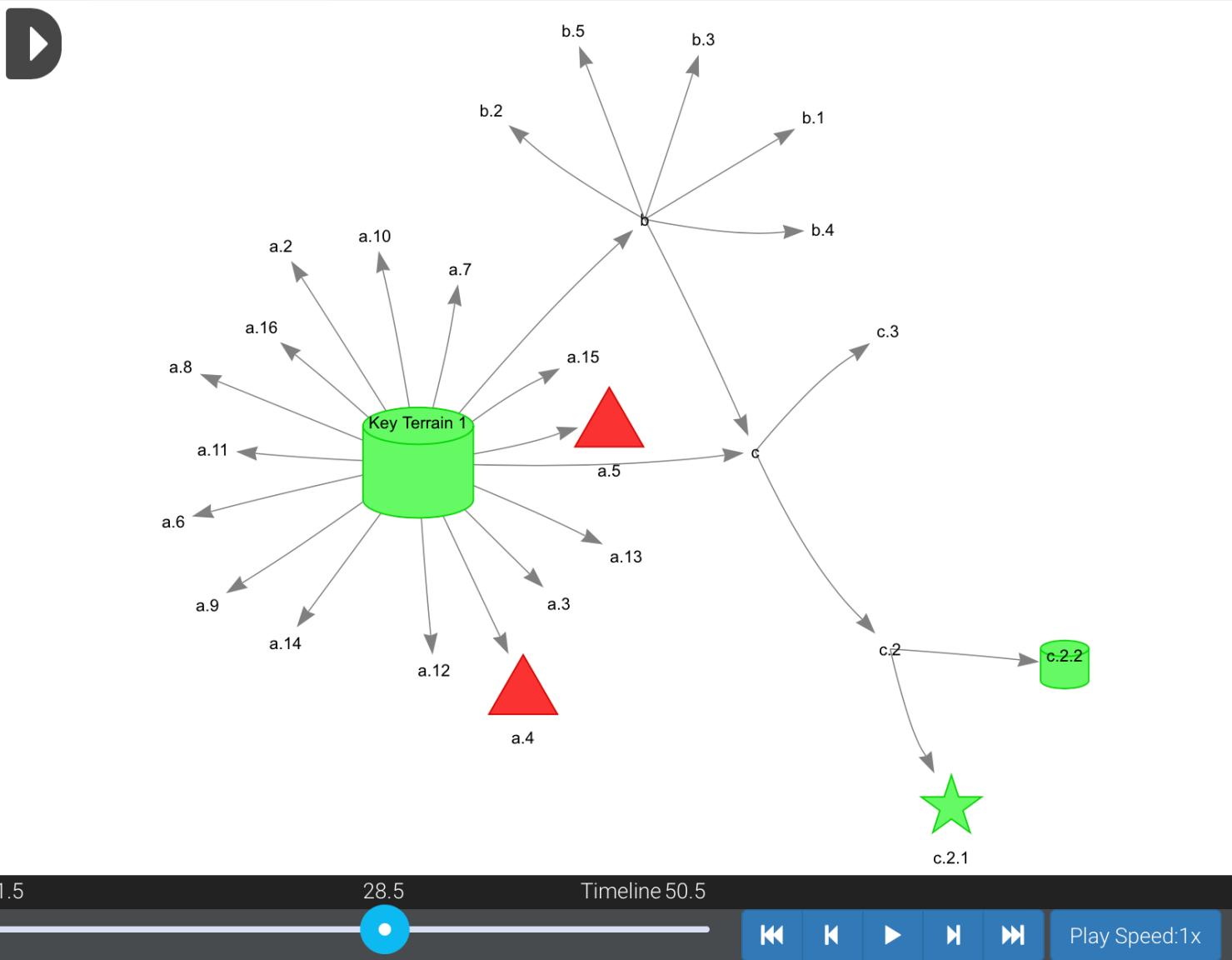


Query Result 2

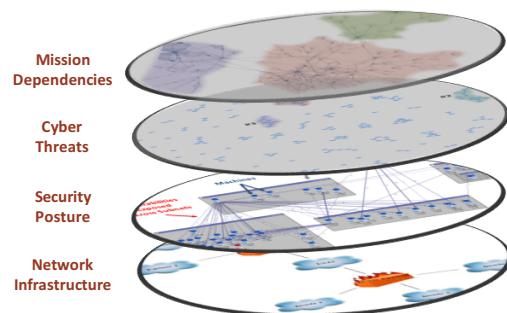




CyGraph Evolution over Time

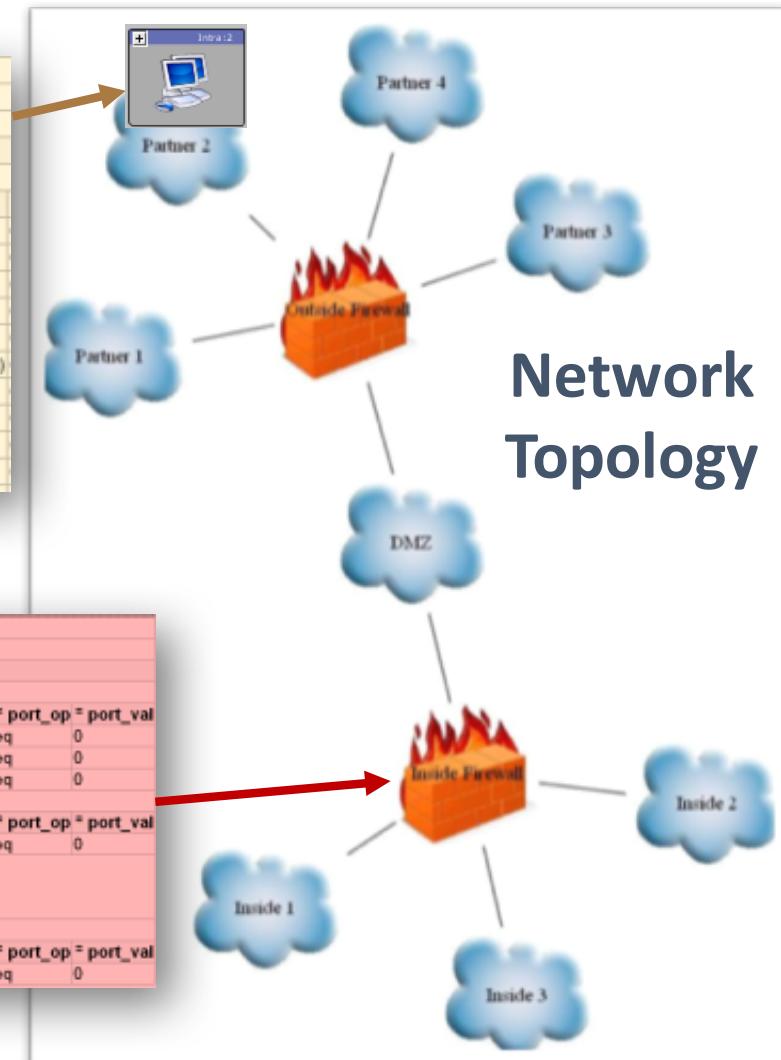


Inputs for Finding Vulnerable Paths



Host Vulnerabilities

Report	
ReportHost (179)	
	ReportItem
1	1.2.46.85
	ReportItem (32)
	port
1	general/icmp
2	general/tcp
3	general/udp
4	ntp (123/udp)
5	epmap (135/tcp)
6	netbios-ns (137/udp)
7	smb (139/tcp)
8	cifs (445/tcp)
9	mrdp (3389/tcp)
10	www (8081/tcp)

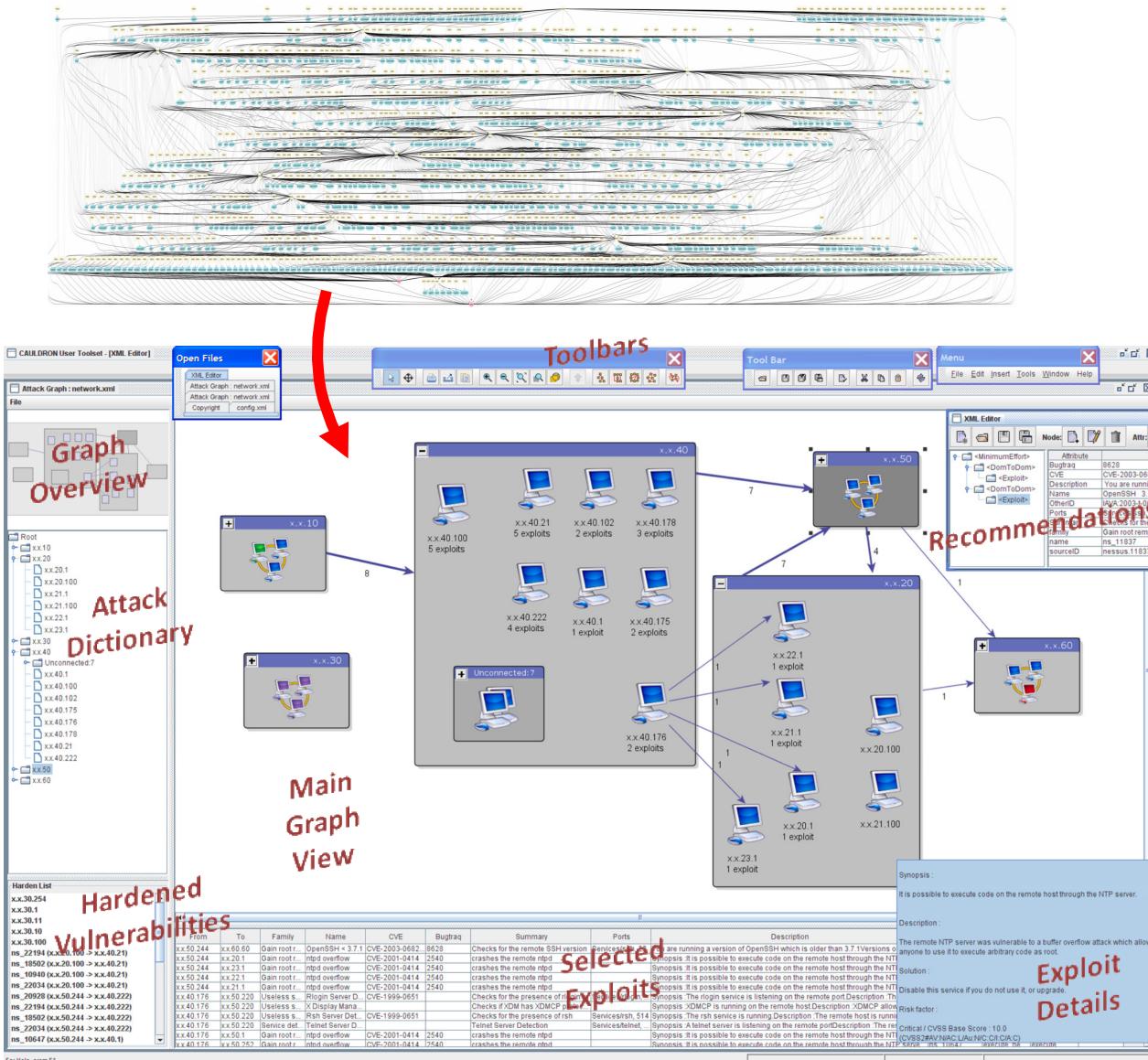


Firewall Rules

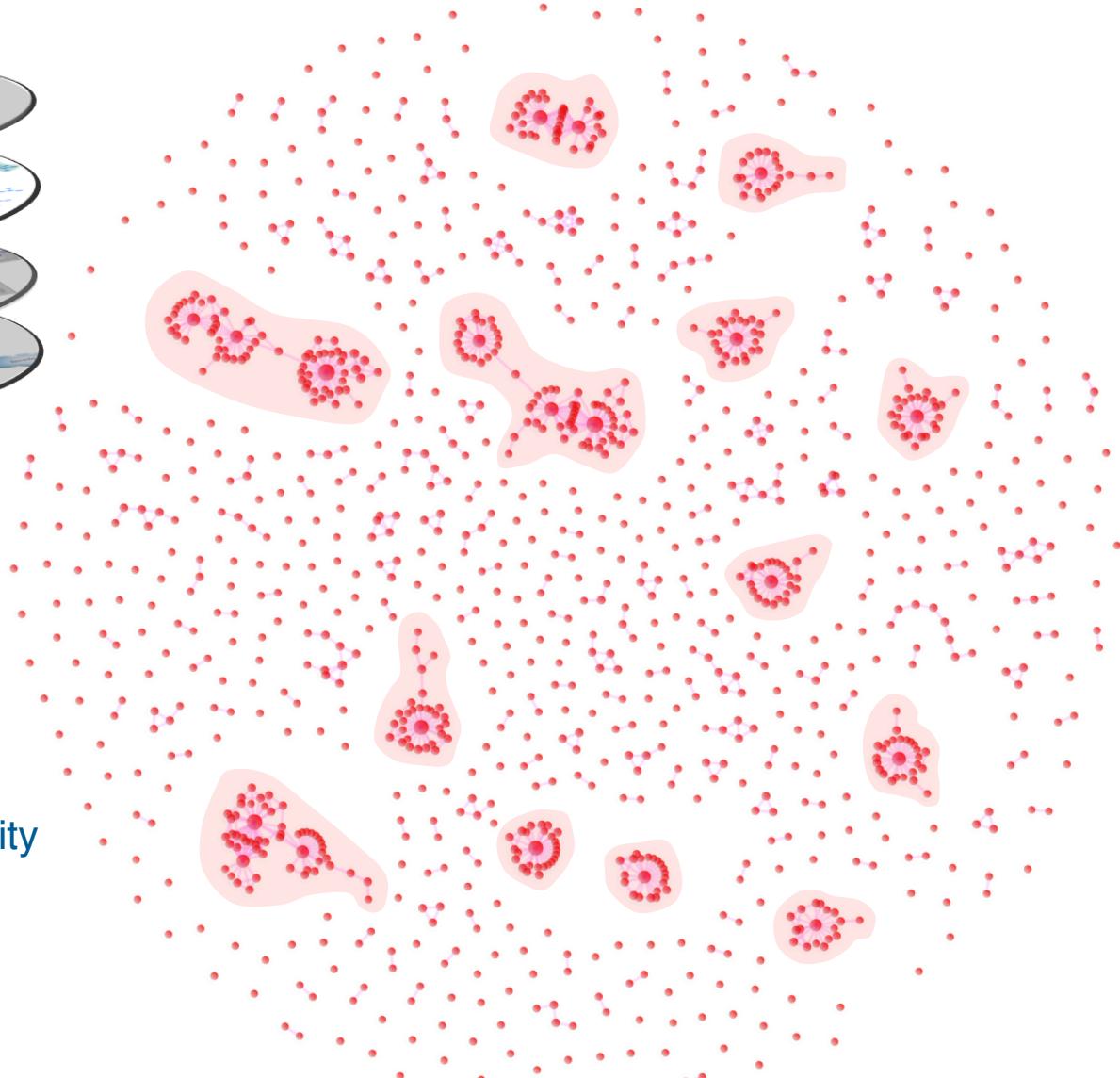
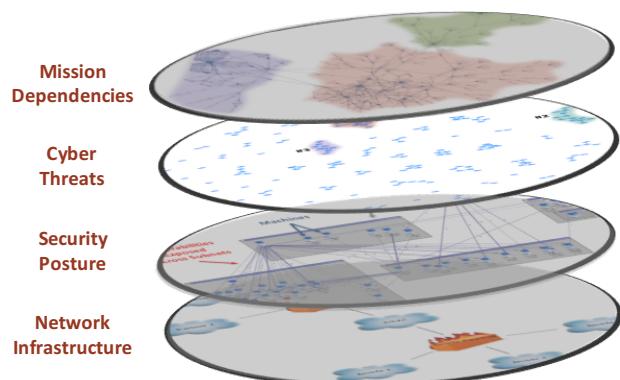
firewall	
rule (3)	
	action
1	permit
	source
1	= ip = mask
1	2.2.52.0.22
2	2.2.56.0.22
3	2.2.60.0.22
2	permit
	source
1	= ip = mask
1	1.2.46.0.25
2	1.2.47.0.25
3	1.2.48.0.25
4	1.2.49.0.25
3	permit
	source
1	= ip = mask
1	2.1.50.0.25
	destination
	= ip = mask = protocol = port_op = port_val
1	2.2.52.0.22 any eq 0
2	2.2.56.0.22 any eq 0
3	2.2.60.0.22 any eq 0
	destination (1)
	= ip = mask = protocol = port_op = port_val
1	2.2.61.0.25 any eq 0
	destination (1)
	= ip = mask = protocol = port_op = port_val
1	2.2.61.0.25 any eq 0

Noel et al,
“CyGraph: Graph-Based Analytics and Visualization for Cybersecurity,”
in *Cognitive Computing: Theory and Applications*
Elsevier, 2016.

Network Vulnerability Paths

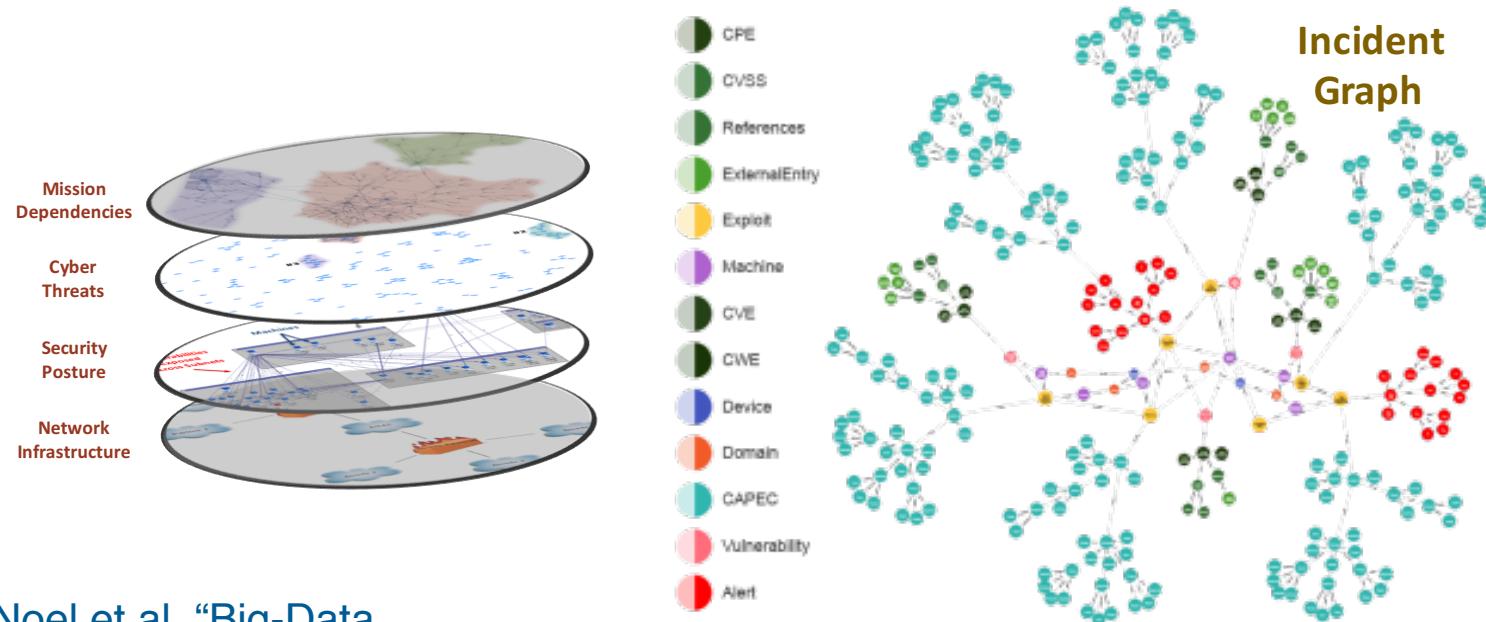


Prioritizing Alert Clusters

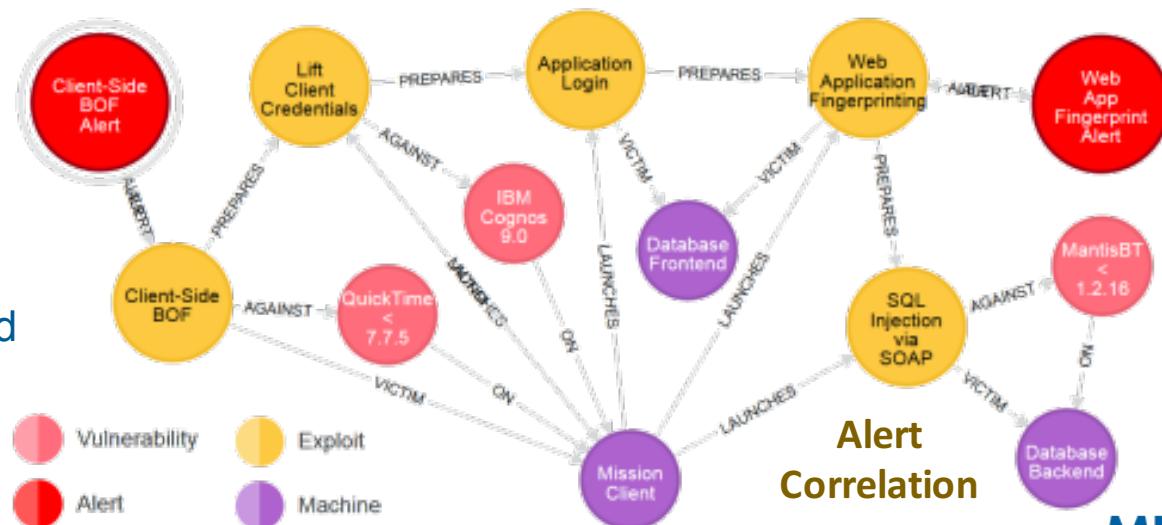


Noel, “A Review of Graph Approaches to Network Security Analytics,” Lecture Notes in Computer Science (Festschriften), Springer, 2018.

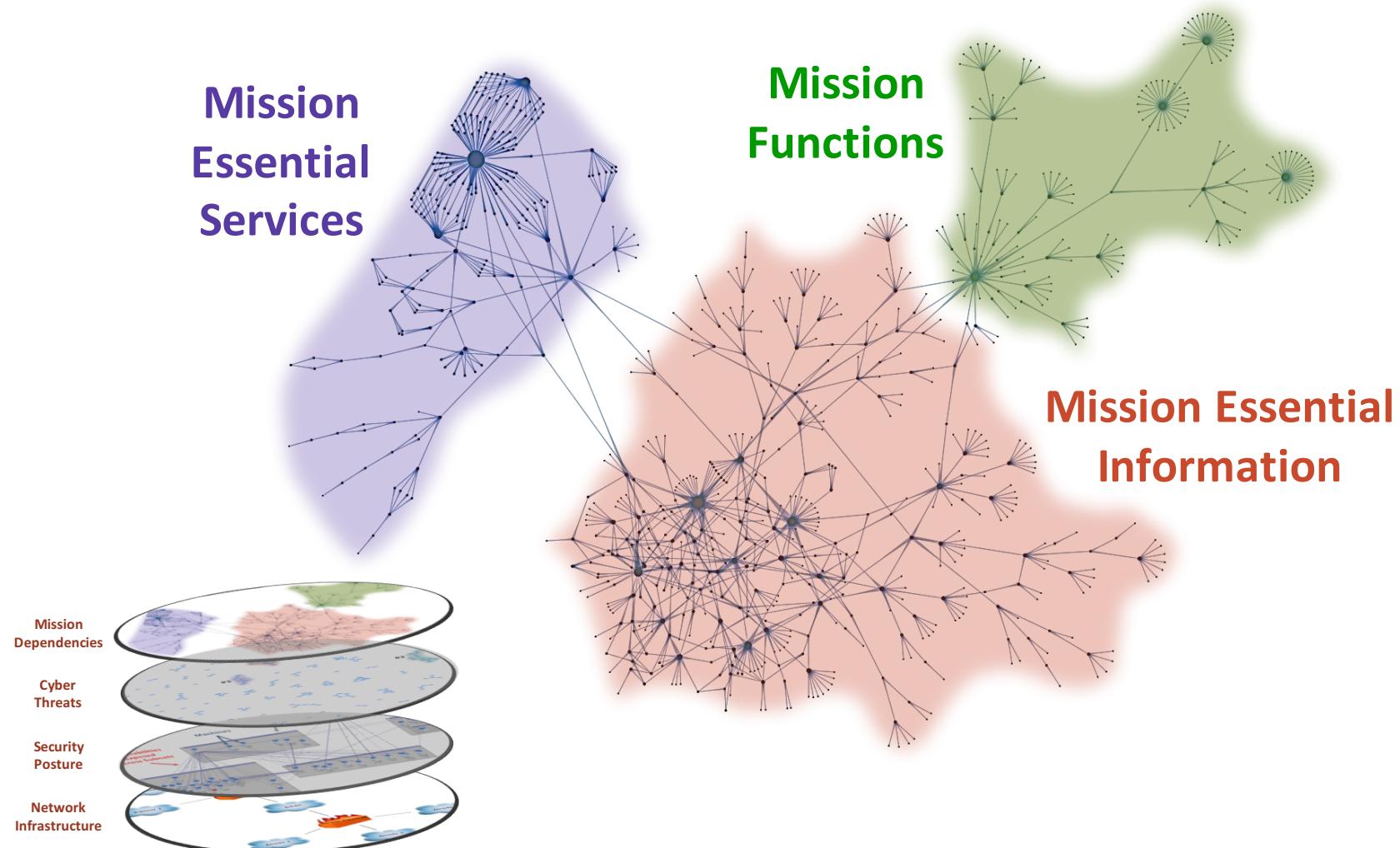
Graph Query Analytics



Noel et al, “Big-Data Architecture for Cyber Attack Graphs: Representing Security Relationships in NoSQL Graph Databases,” IEEE Symposium on Technologies for Homeland Security (HST), 2015.

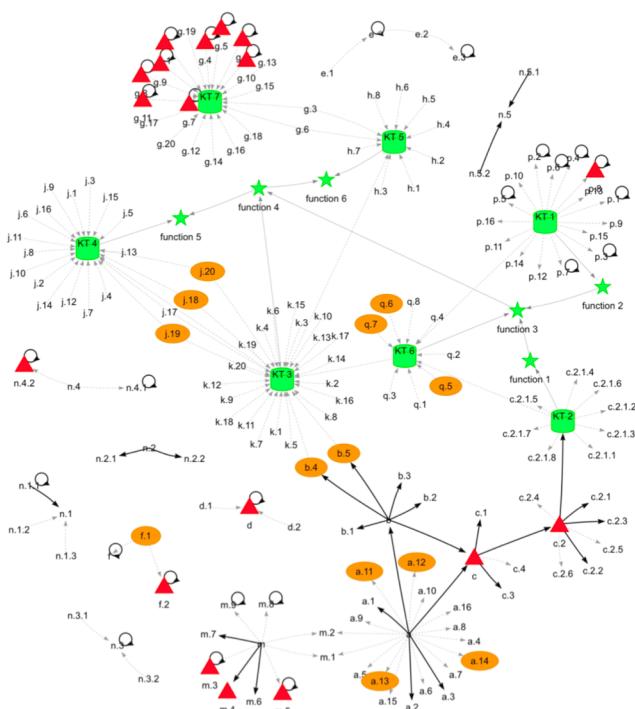


Mission Dependencies

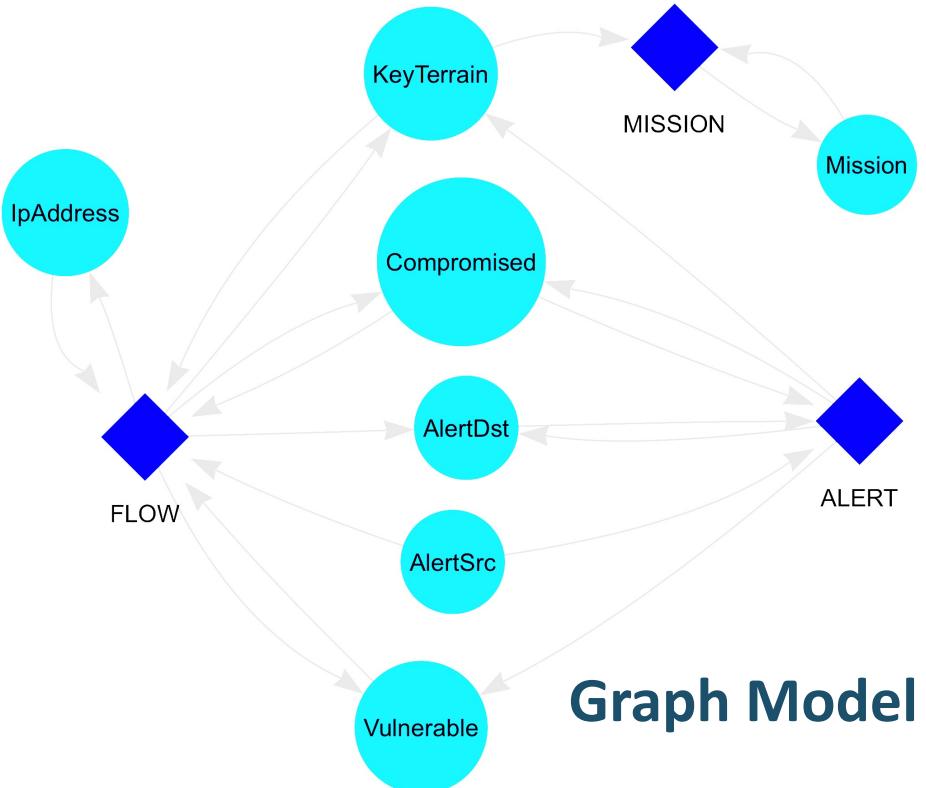


Noel et al, "Analyzing Mission Impacts of Cyber Actions (AMICA)," NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact, 2015.

Mission Functions, Intrusion Alerts, Network Flows, and Host Vulnerabilities

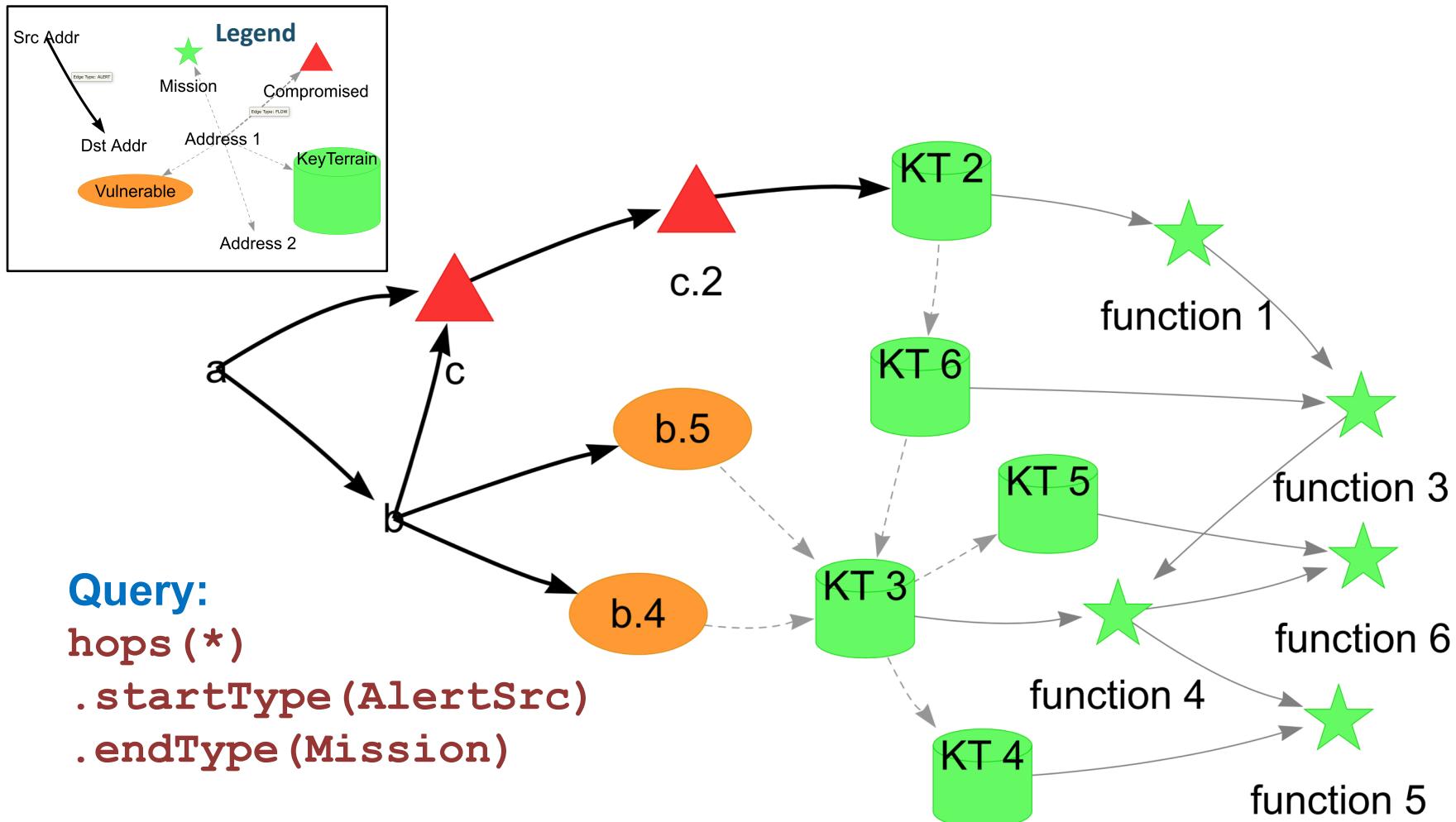


Populated Graph



Noel et al, "Mission-Focused Cyber Situational Understanding via Graph Analytics," 10th International Conference on Cyber Conflict (CyCon X), 2018.

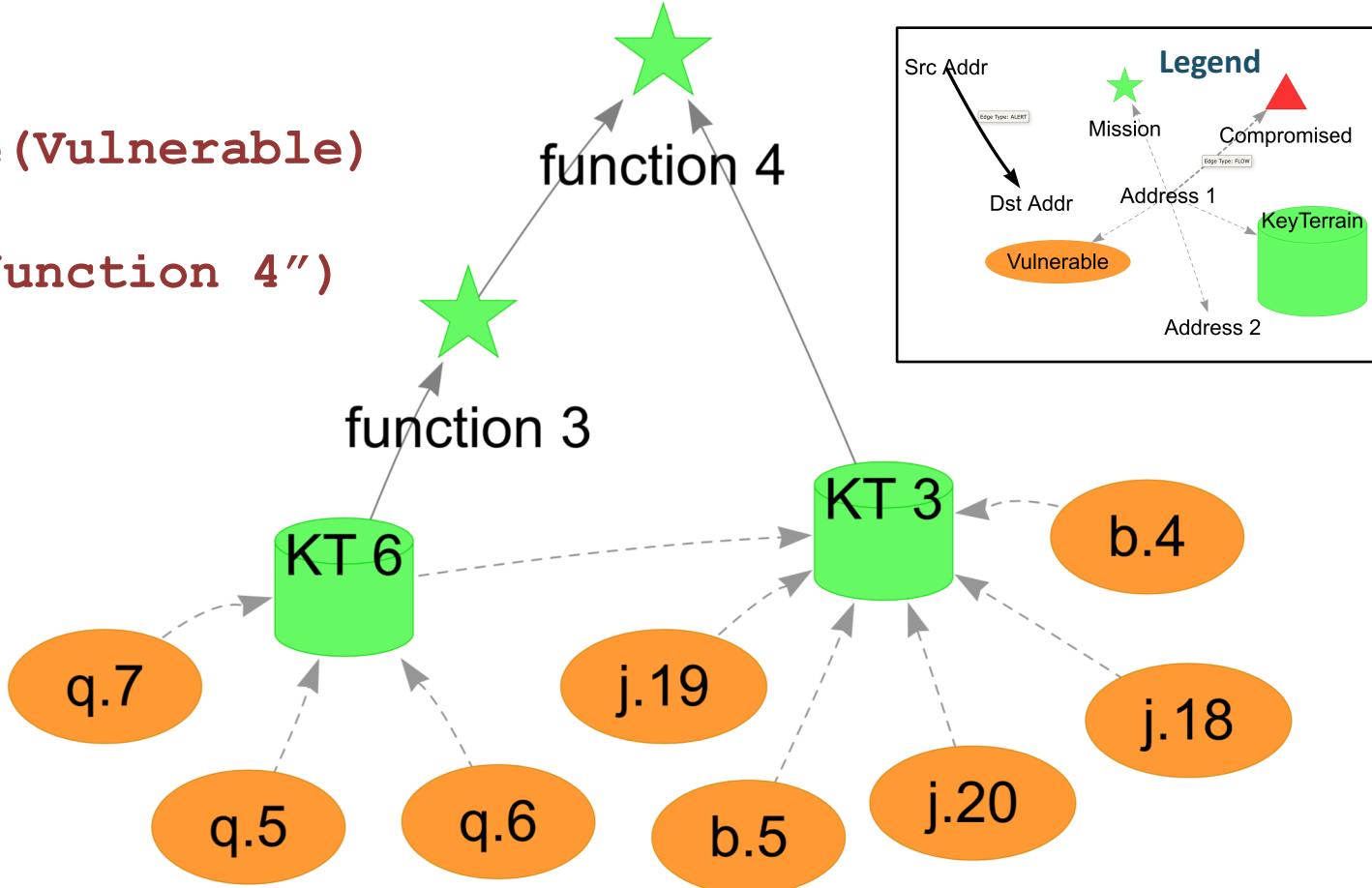
From Alert Source IP to Mission Function



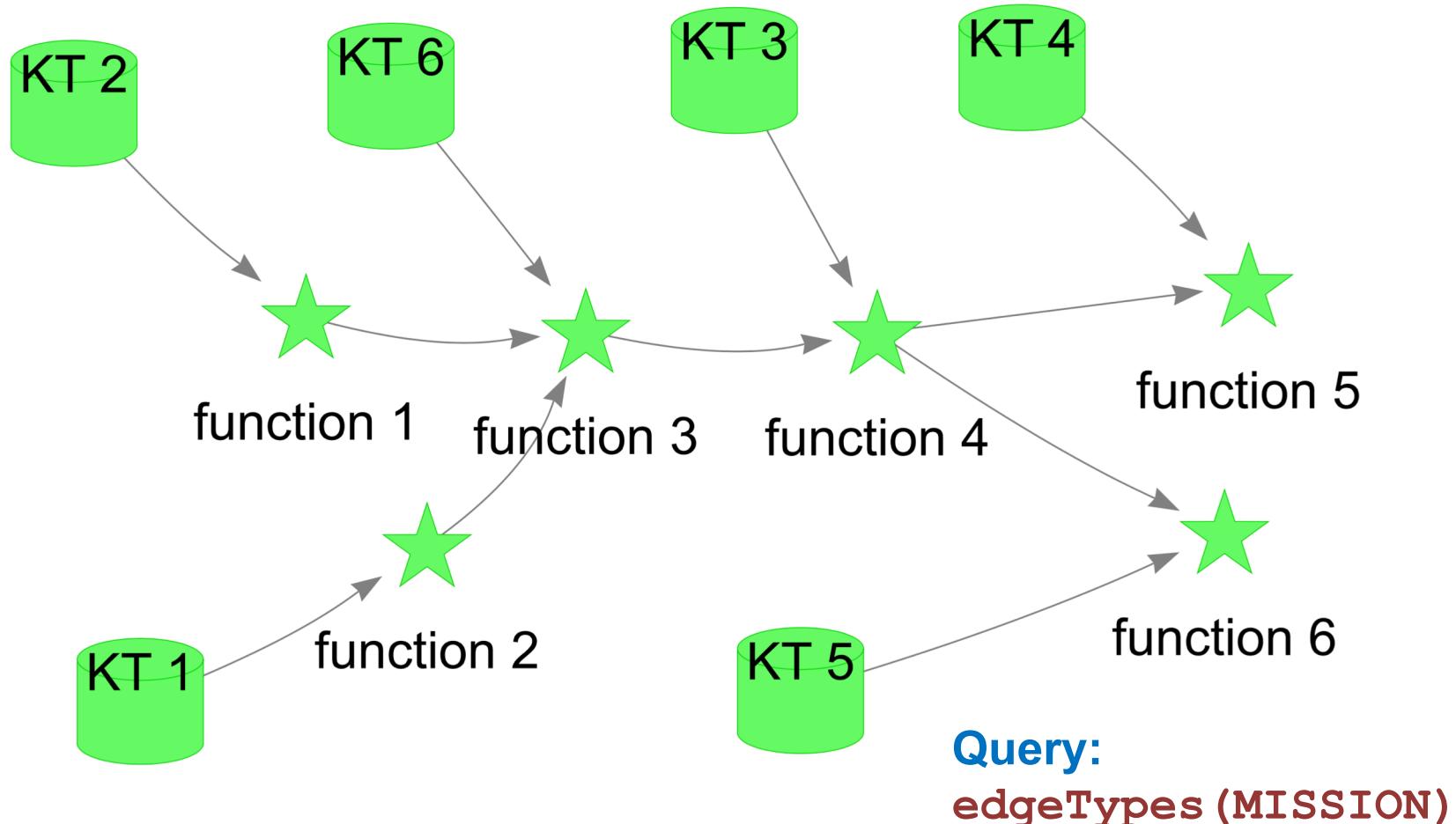
Vulnerable Hosts for a Mission Function

Query:

```
startType(Vulnerable)
.hops(*)
.endId("function 4")
```



Mission Dependency Edges





CyGraph Publications

- **Book Chapters**

1. Lecture Notes in Computer Science (Festschrifts), Springer, 2018
2. Computational Analysis and Understanding of Natural Languages, Elsevier, 2018
3. Network Security Metrics, Springer, 2017
4. Cognitive Computing: Theory and Applications, Elsevier, 2016

- **Conferences**

1. NATO International Conference on Cyber Conflict (CyCon X), 2018
2. CMU/SEI Large-Scale Data Analytics to Improve Security Operations (FloCon), 2018
3. NATO IST-153 Workshop on Cyber Resilience, 2017
4. NATO Cyber Defence Situational Awareness Solutions Demonstration, 2016
5. International Conference for Military Communications (MILCOM), 2016
6. NATO IST-148 Symposium on Cyber Defence Situation Awareness, 2016
7. IEEE International Conference on Technologies for Homeland Security, 2015
8. ACM Intelligent User Interfaces (IUI) Workshop on Visual Text Analytics, 2015
9. NATO Cyber Defence Situational Awareness Solutions Conference, 2015
10. Neo4j GraphConnect San Francisco, 2015
11. NATO IST-128 Workshop on Cyber Attack Assessment of Mission Impact, 2015
12. Oak Ridge Annual Cyber and Information Security Research Conference, 2014
13. IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance, 2014

- **White paper: “MITRE Solutions for Cyber Situational Awareness” (2015)**

Questions?



Steven Noel
snoel@mitre.org