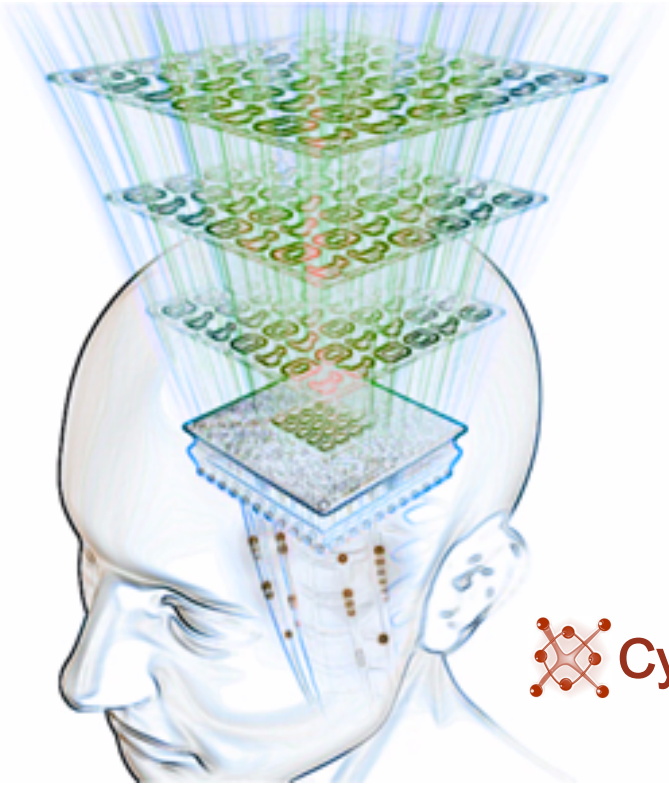
Microsoft BlueHat 2018

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

Steven Noel, PhD

The MITRE Corporation

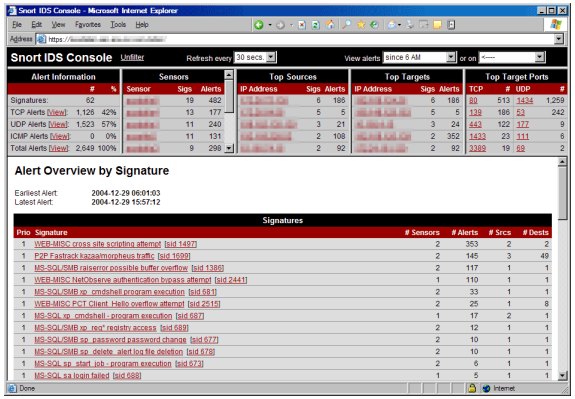
September 25, 2018



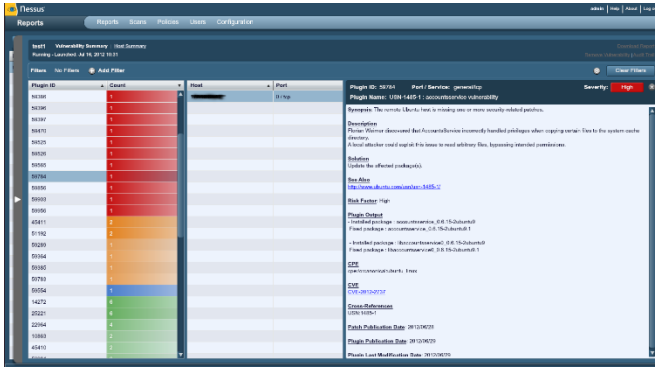
MITRE

Security Tools Landscape – Too Much Data, Too Little Context

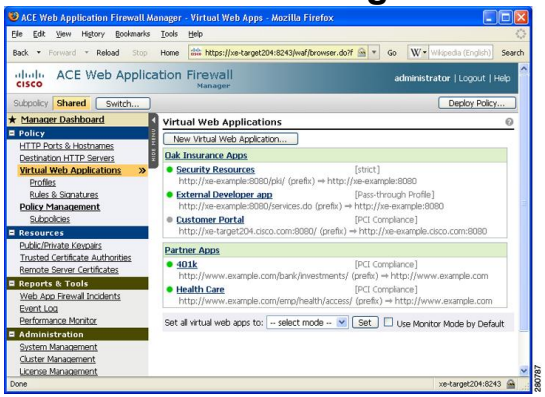
Intrusion Detection System



Vulnerability Scanner

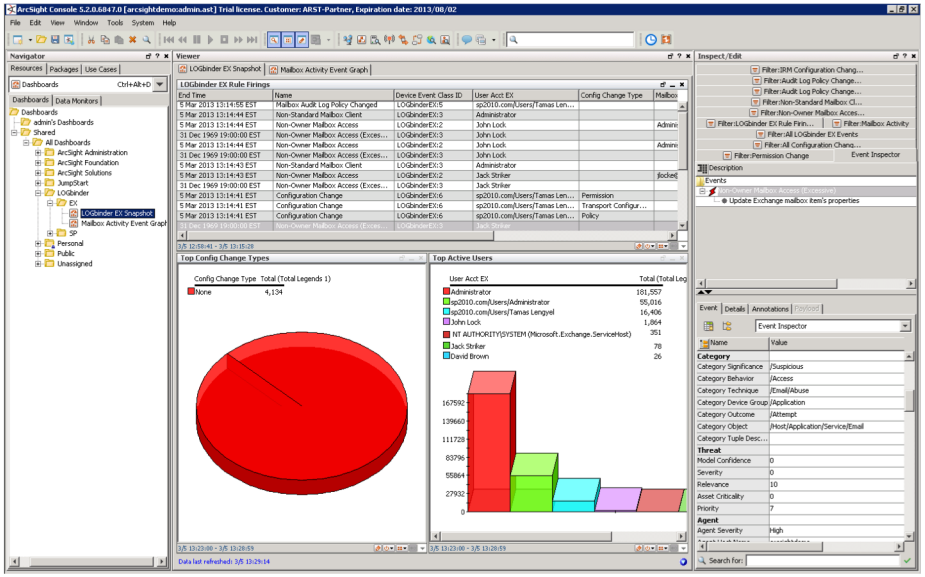


Firewall Manager



Security Intelligence

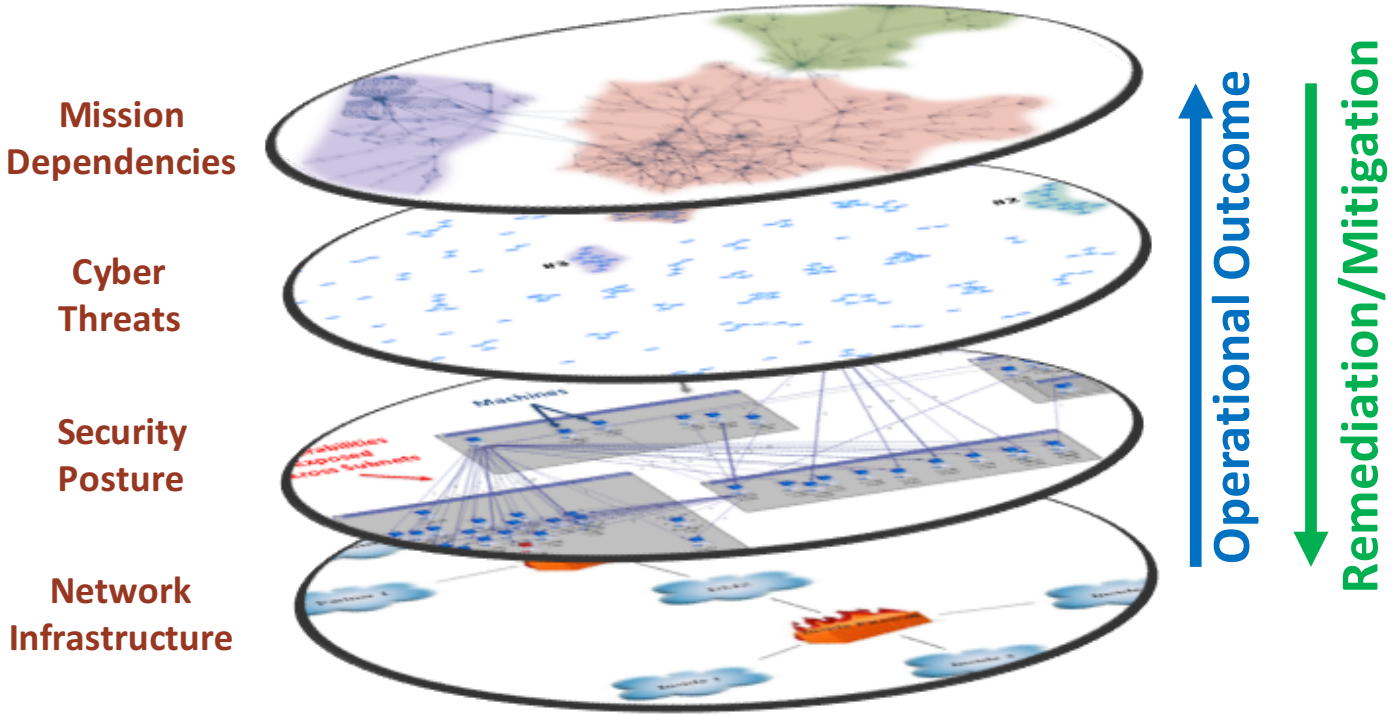
Security Information and Event Management (SIEM)



MITRE

CyGraph Project Summary

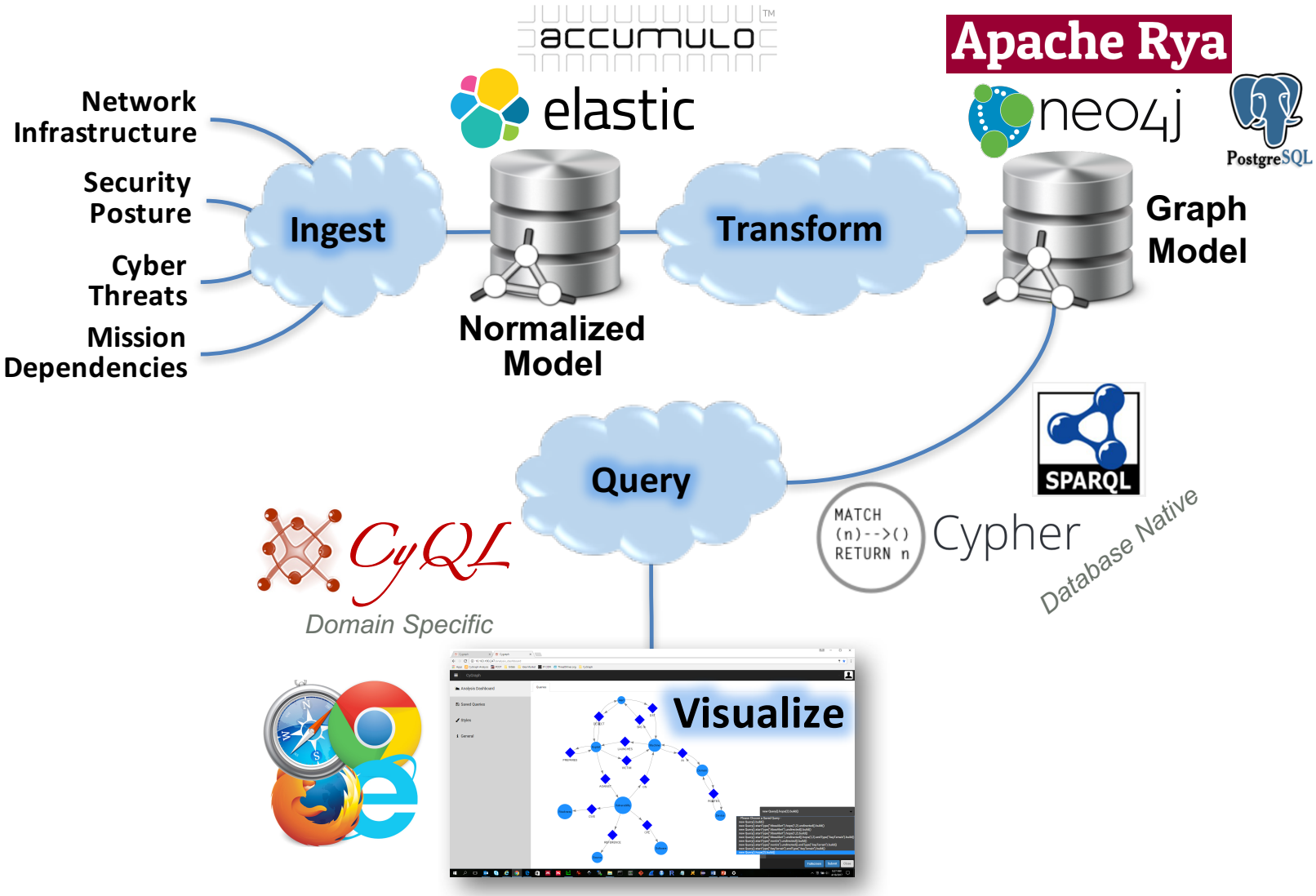
- **CyGraph approach:**
  - Tool for capturing complex cybersecurity relationships in a graph knowledge base
  - Cyber-specific graph model, graph pattern matching queries, interactive visualization



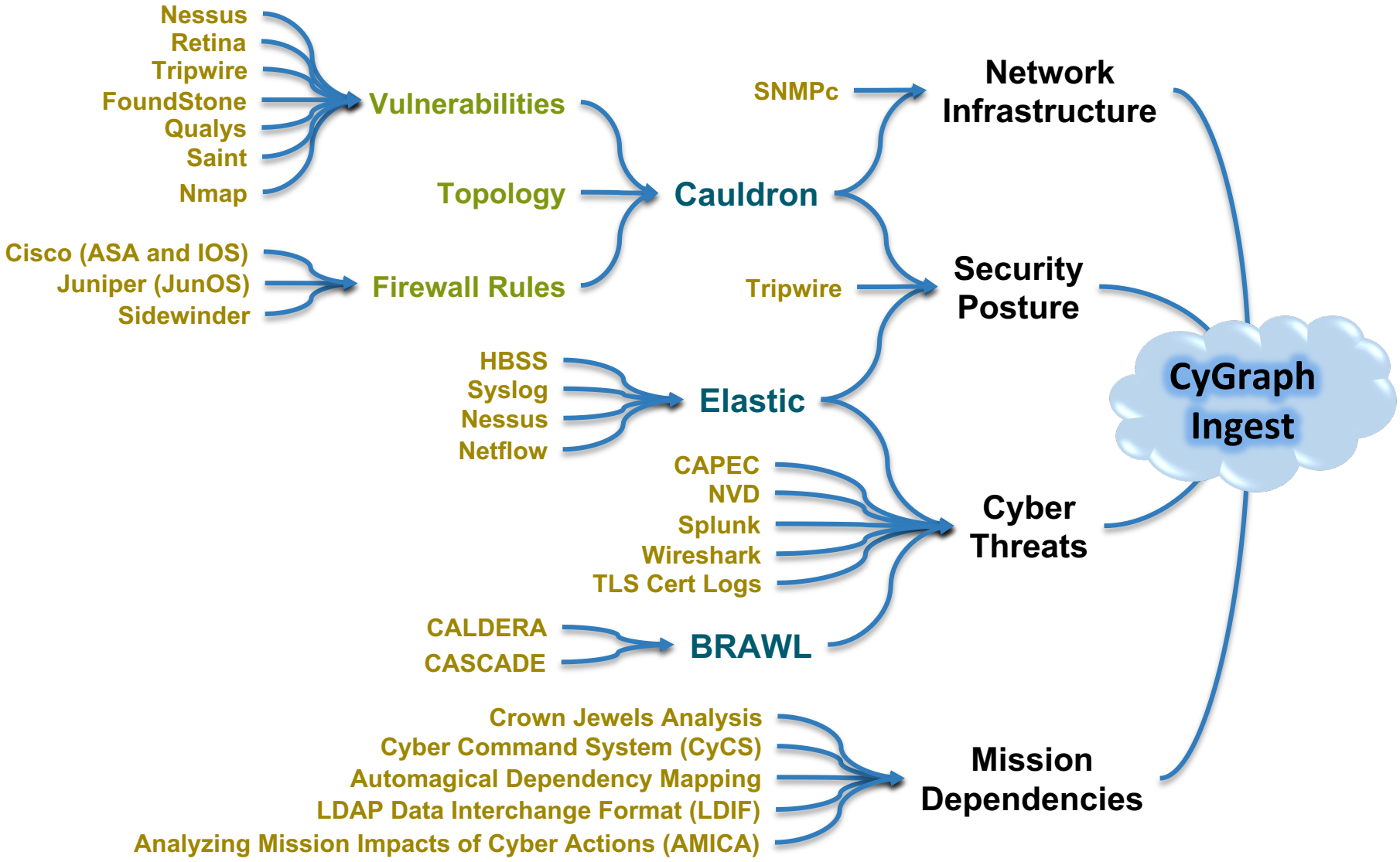
- **Example applications: network hardening, alert correlation and prioritization, mission dependency/impact analysis**
- **Outputs: Application to 11 direct-funded projects, 18 publications, patent pending**

MITRE

CyGraph Architecture

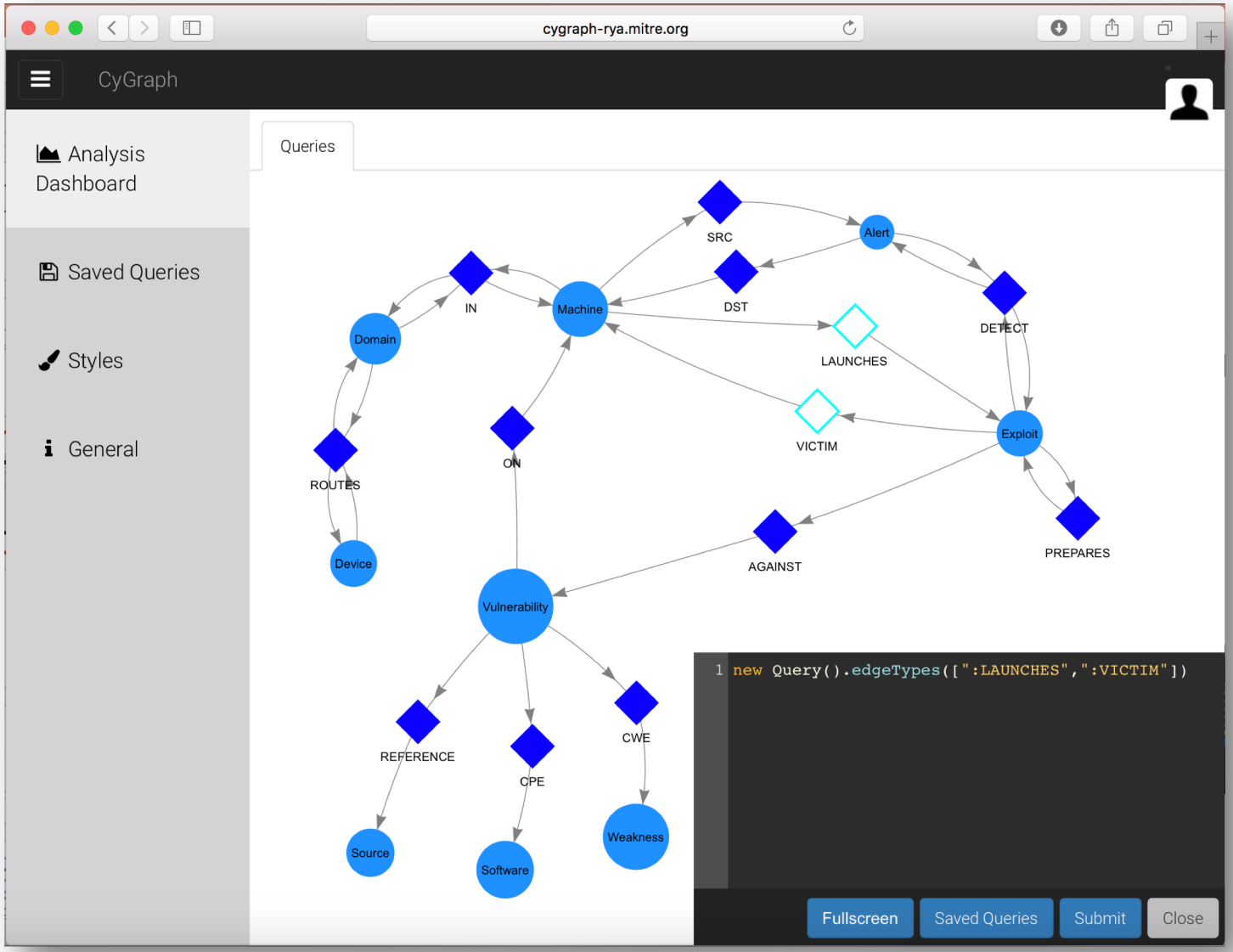


CyGraph Operational Data Sources



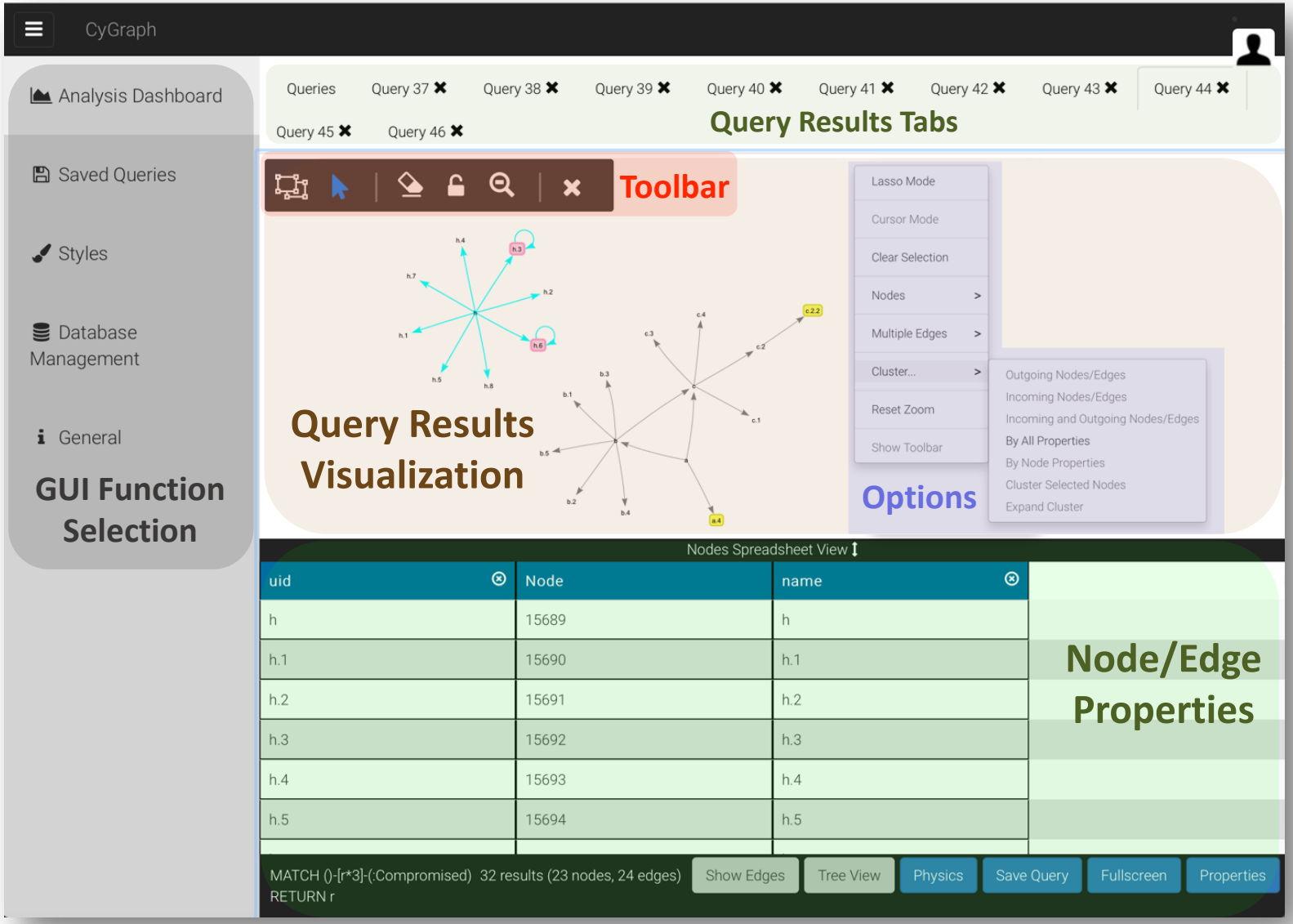
MITRE

CyGraph Graph Model View



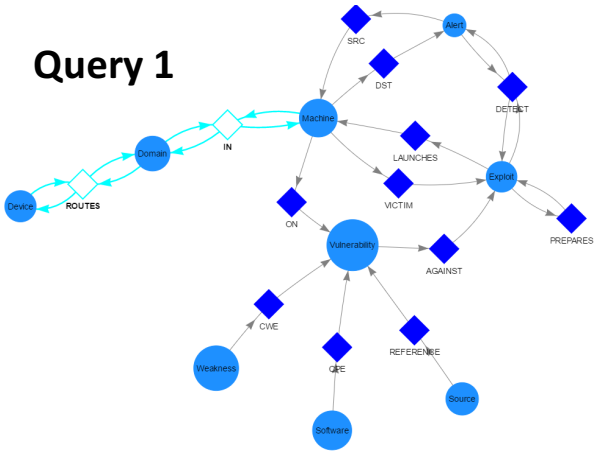
MITRE

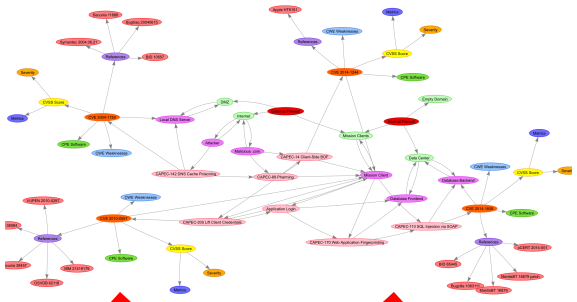
CyGraph Query Results

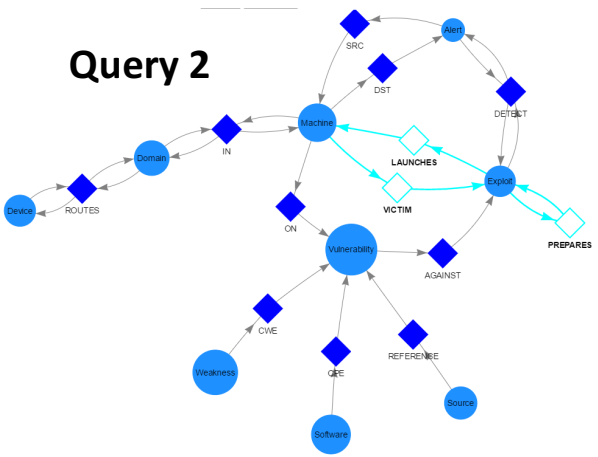


MITRE

CyGraph Analytic Queries

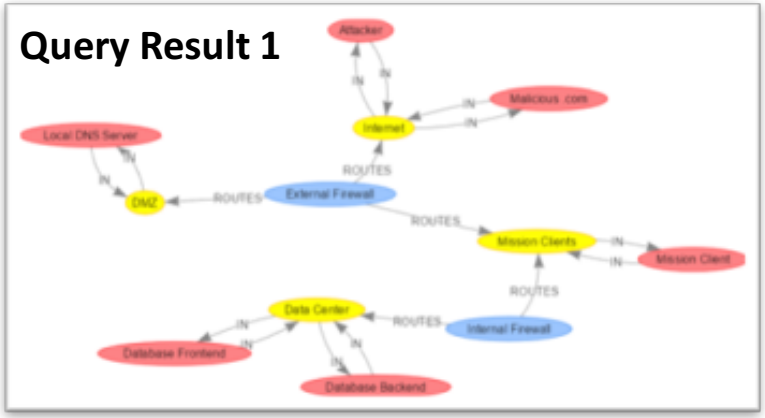


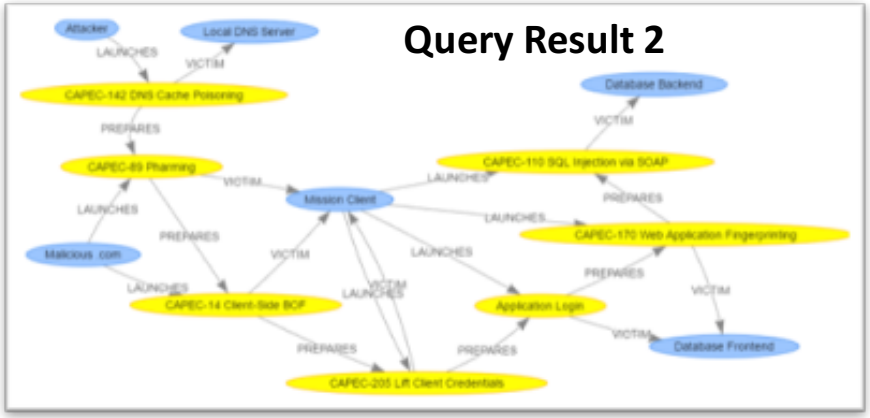




edgeTypes(:"IN",":ROUTES")

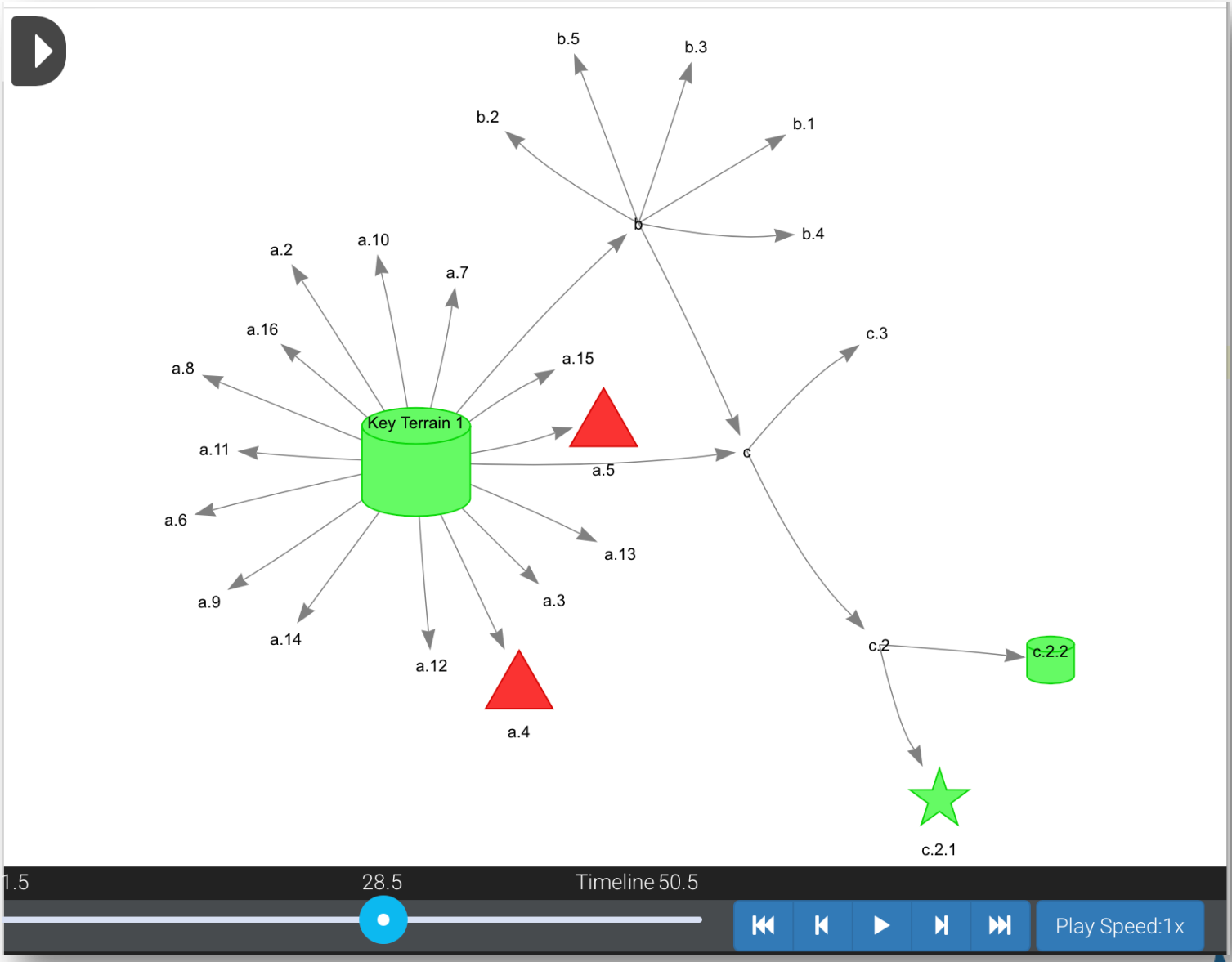
edgeTypes(":PREPARE",":LAUNCHES",":VICTIM")





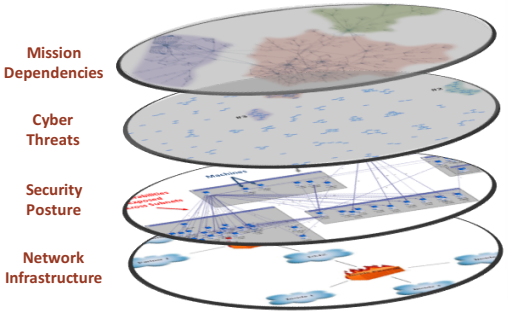
MITRE

CyGraph Evolution over Time



MITRE

Inputs for Finding Vulnerable Paths



Host Vulnerabilities

NessusClientData
Report
ReportHost (179)

	HostName	ReportItem
1	1.2.46.85	ReportItem (32)

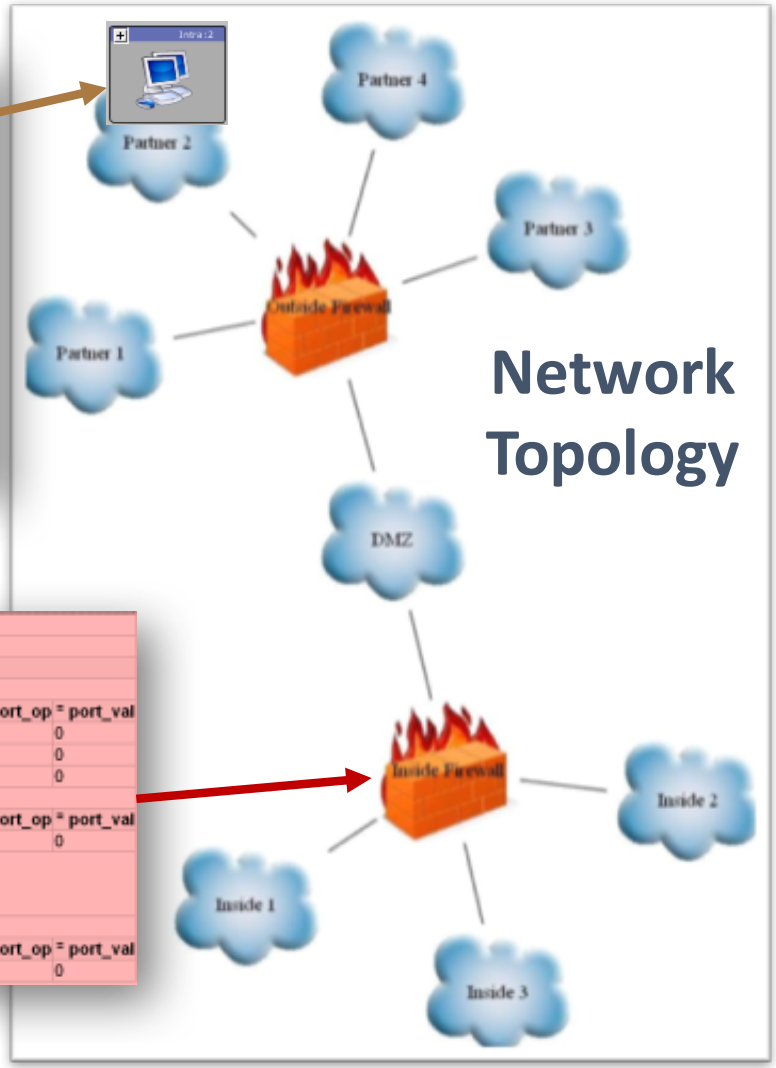
	port
1	general/icmp
2	general/tcp
3	general/udp
4	ntp (123/udp)
5	epmap (135/tcp)
6	netbios-ns (137/udp)
7	smb (139/tcp)
8	cifs (445/tcp)
9	msrdp (3389/tcp)
10	www (8081/tcp)

Firewall Rules

firewall
rule (3)

	action	source	destination
1	permit	source (3)	destination (3)
2	permit	source (4)	destination (1)
3	permit	source (1)	destination (1)

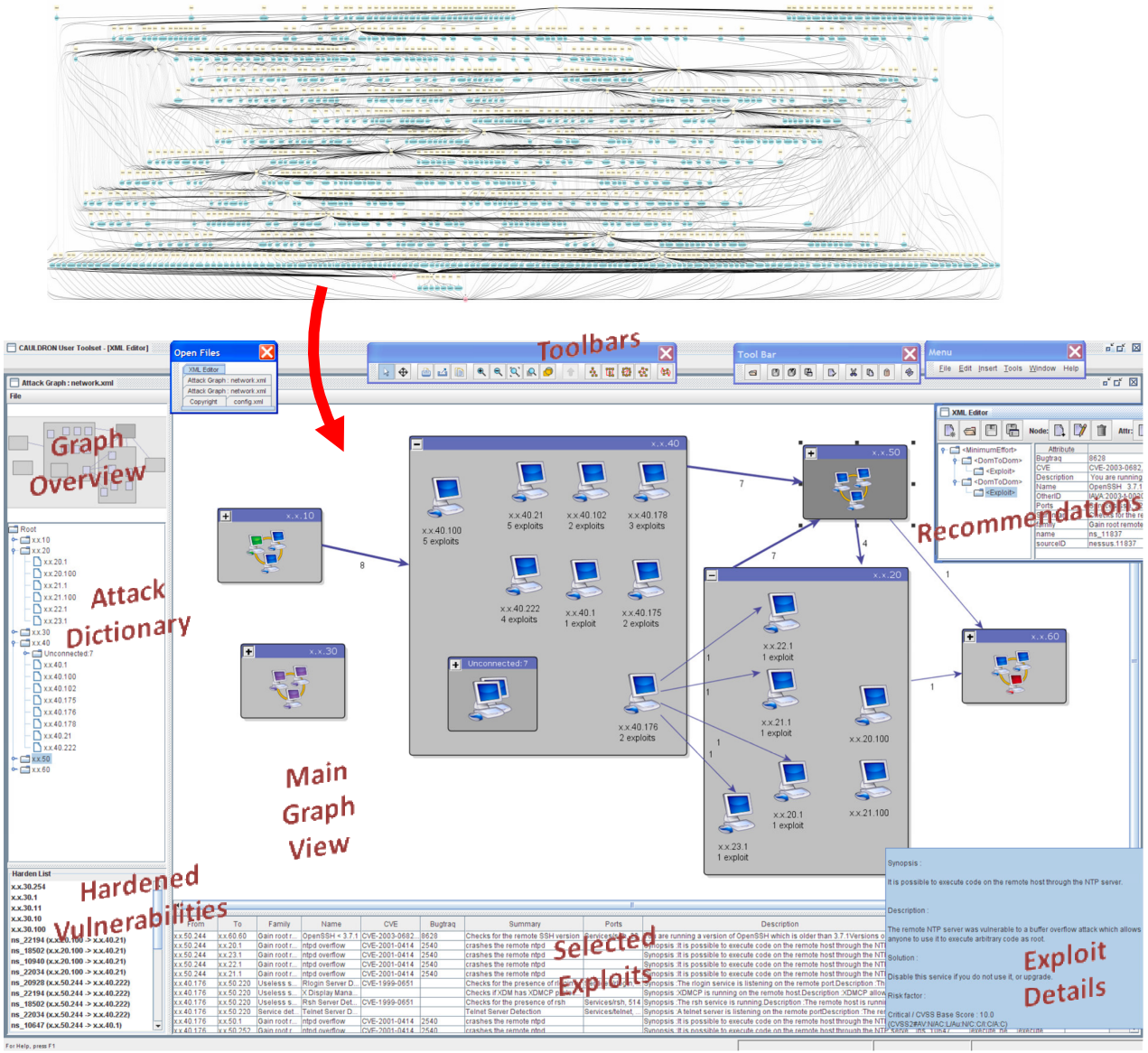
	source ip	source mask	destination ip	destination mask	protocol	port_op	port_val
1	2.2.52.0	22	2.2.52.0	22	any	eq	0
2	2.2.56.0	22	2.2.56.0	22	any	eq	0
3	2.2.60.0	22	2.2.60.0	22	any	eq	0
1	1.2.46.0	25	2.2.61.0	25	any	eq	0
2	1.2.47.0	25					
3	1.2.48.0	25					
4	1.2.49.0	25					
1	2.1.50.0	25	2.2.61.0	25	any	eq	0



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

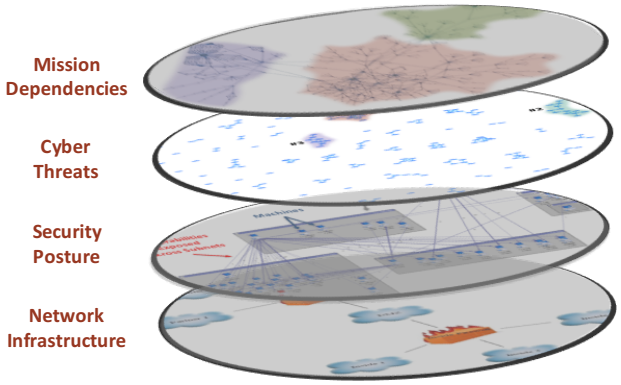
MITRE

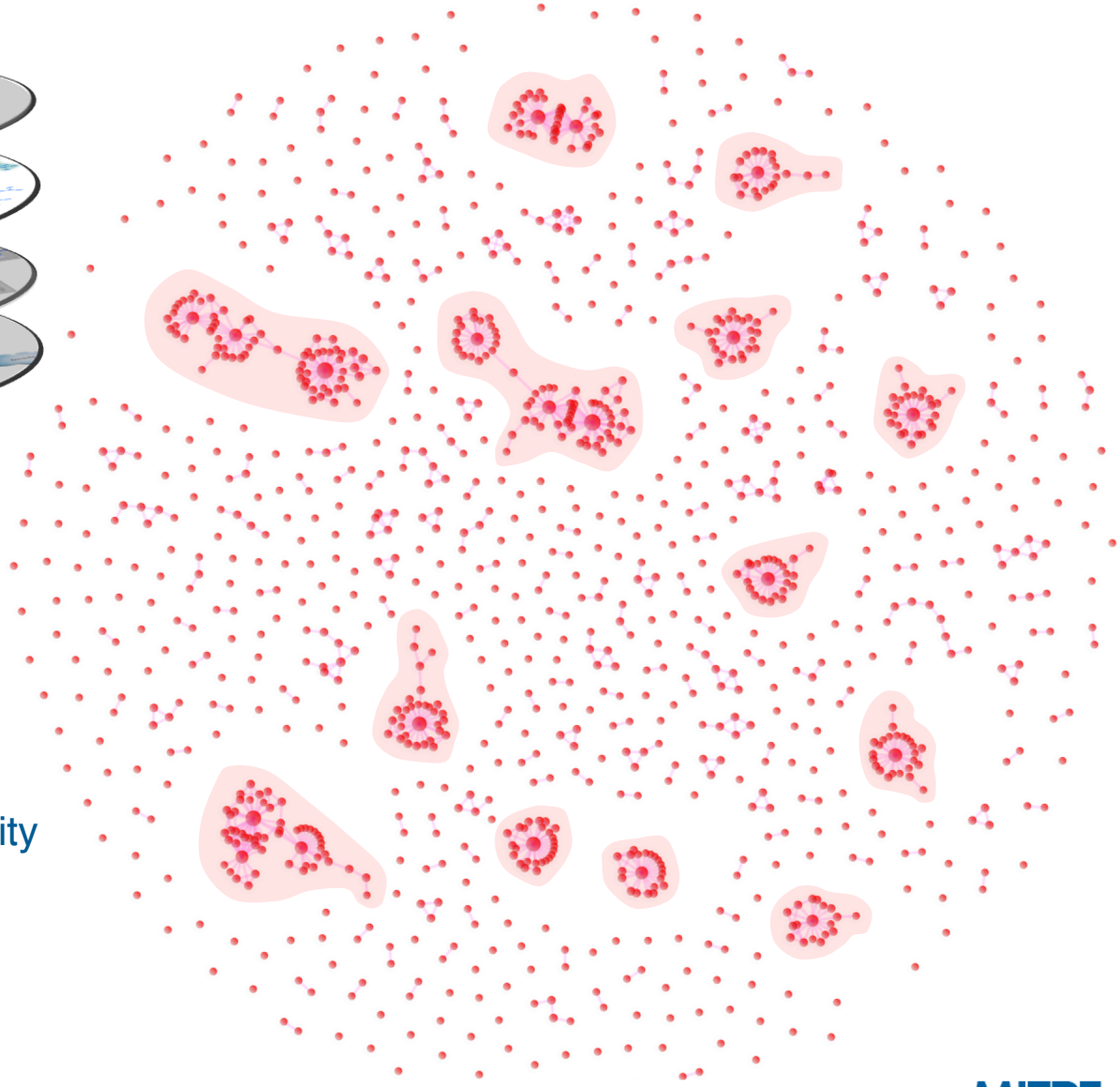
Network Vulnerability Paths



MITRE

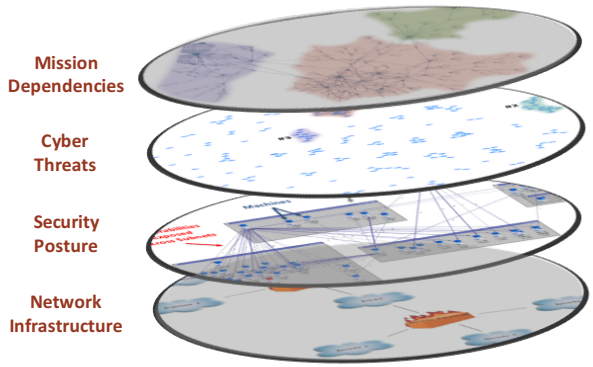
Prioritizing Alert Clusters

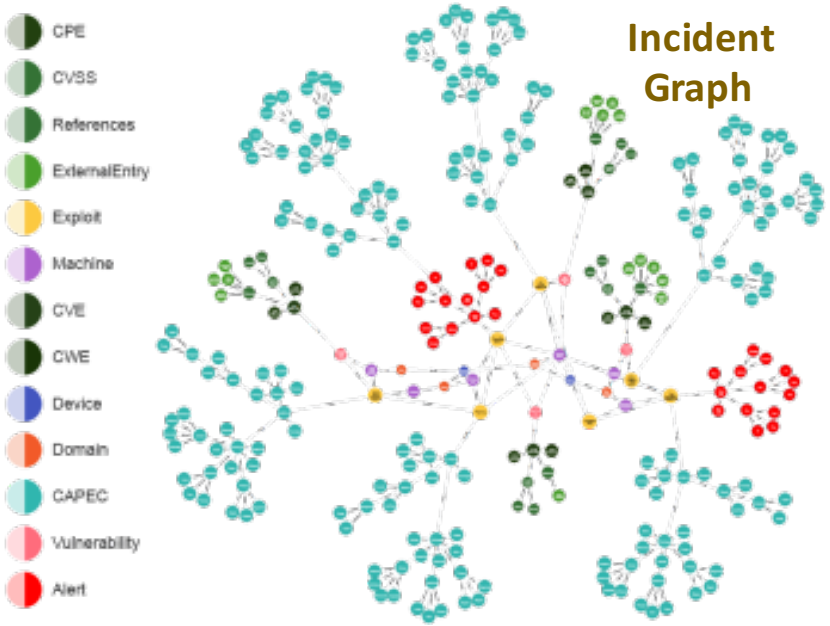




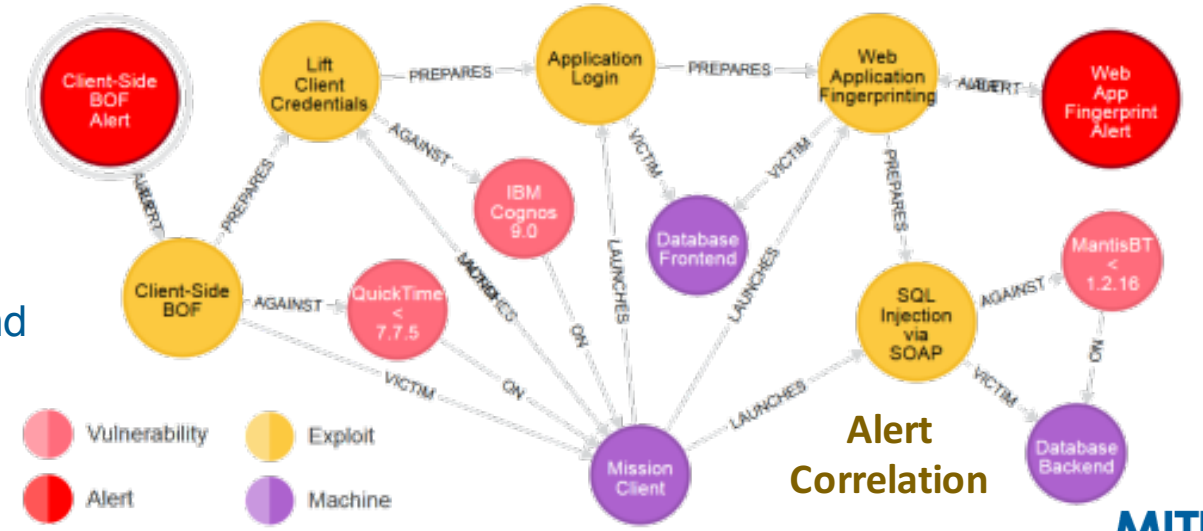
Noel, "A Review of Graph Approaches to Network Security Analytics," Lecture Notes in Computer Science (Festschrifts), Springer, 2018.

Graph Query Analytics



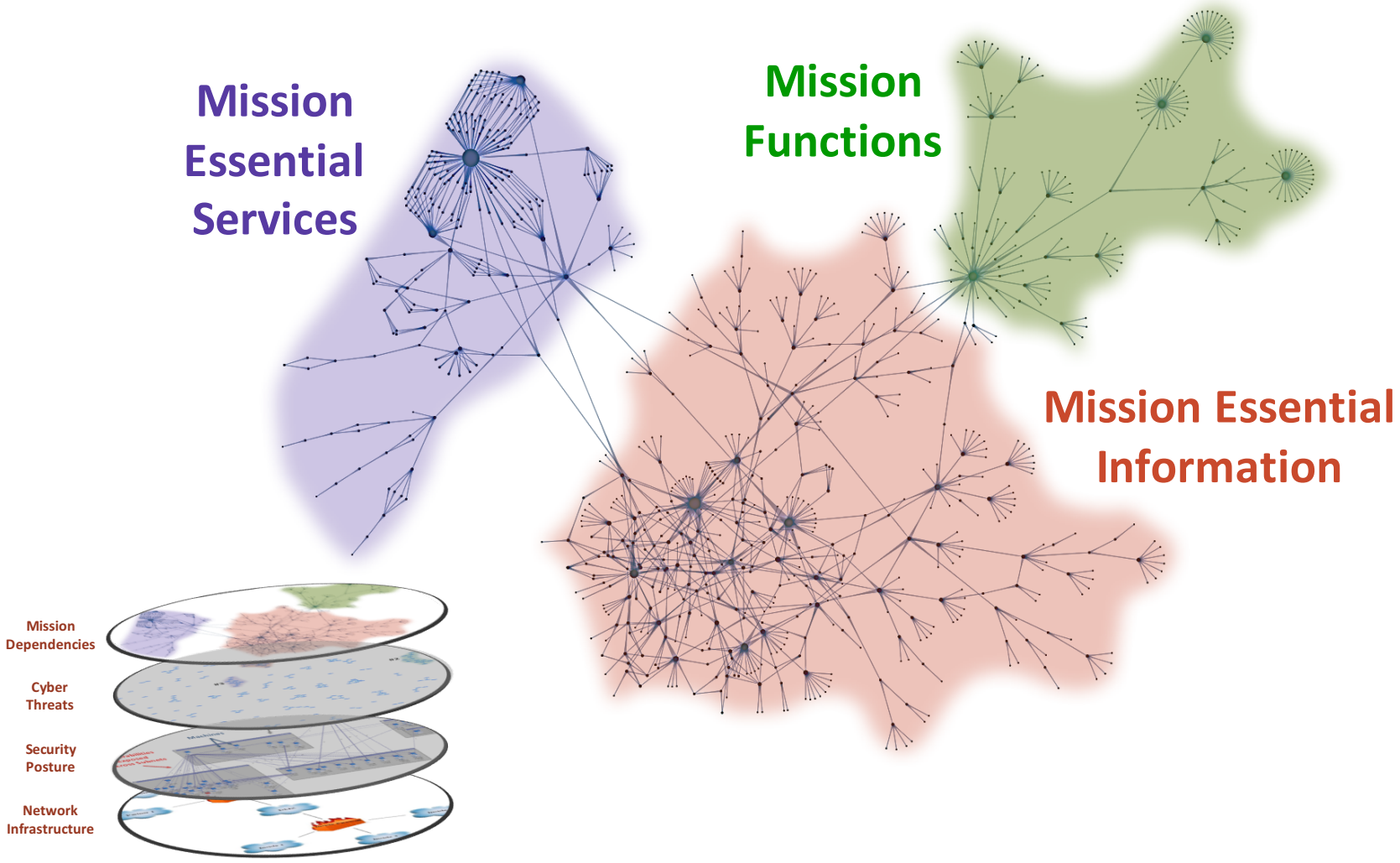


Noel et al, "Big-Data Architecture for Cyber Attack Graphs: Representing Security Relationships in NoSQL Graph Databases," IEEE Symposium on Technologies for Homeland Security (HST), 2015.



MITRE

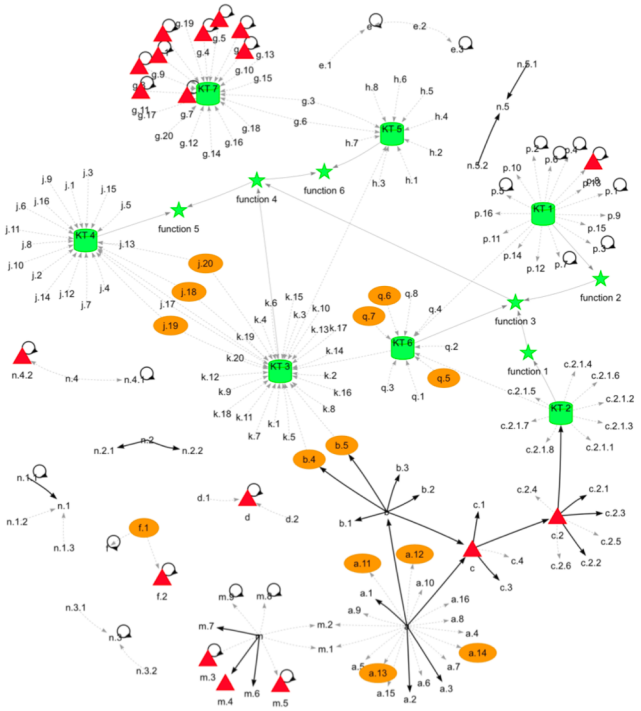
Mission Dependencies



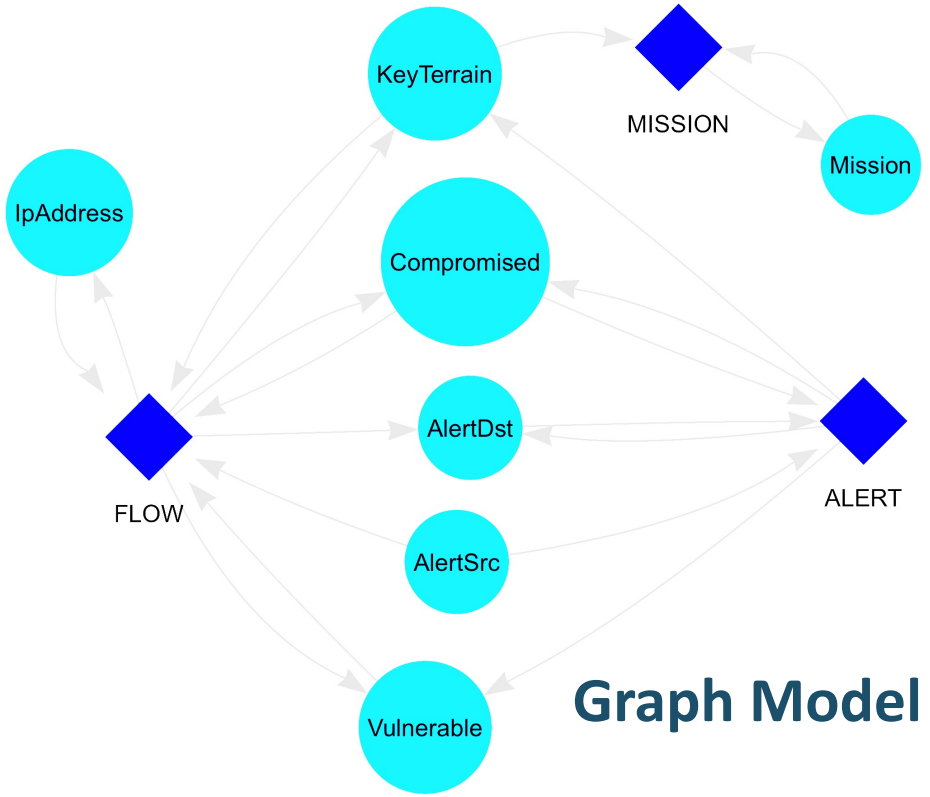
Noel et al, "Analyzing Mission Impacts of Cyber Actions (AMICA)," NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact, 2015.

MITRE

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



Populated Graph

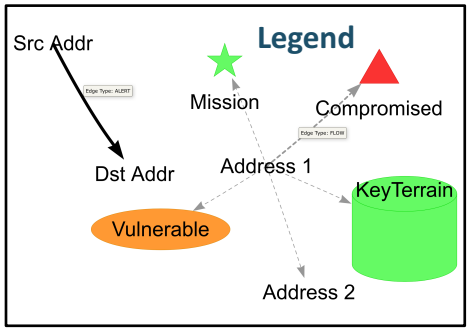


Graph Model

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

MITRE

From Alert Source IP to Mission Function



a
c
c.2
b
b.5
b.4
KT 2
KT 6
KT 5
KT 3
KT 4
function 1
function 3
function 6
function 4
function 5

Query:

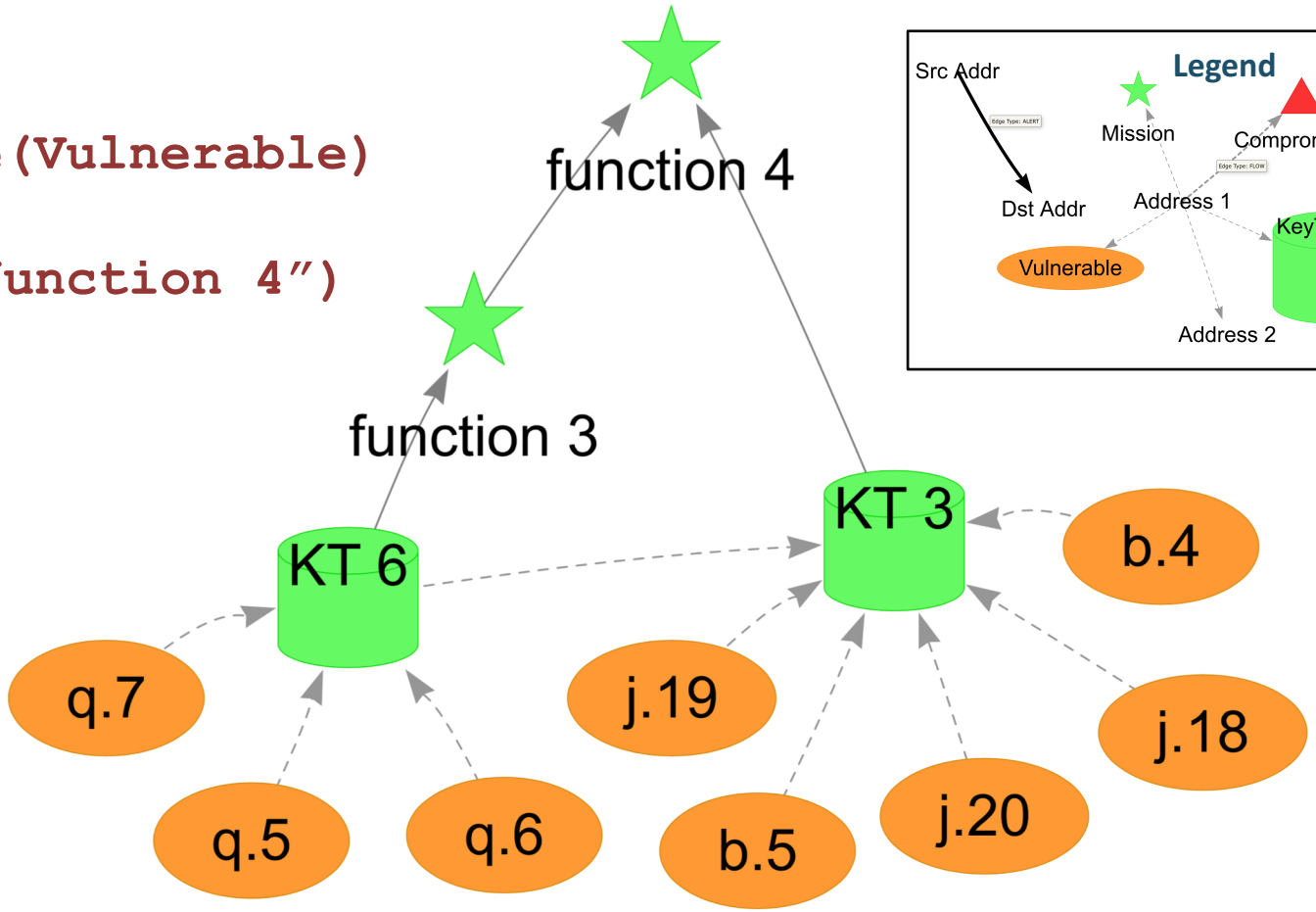
```
hops(*)
.startType(AlertSrc)
.endType(Mission)
```


MITRE

Vulnerable Hosts for a Mission Function

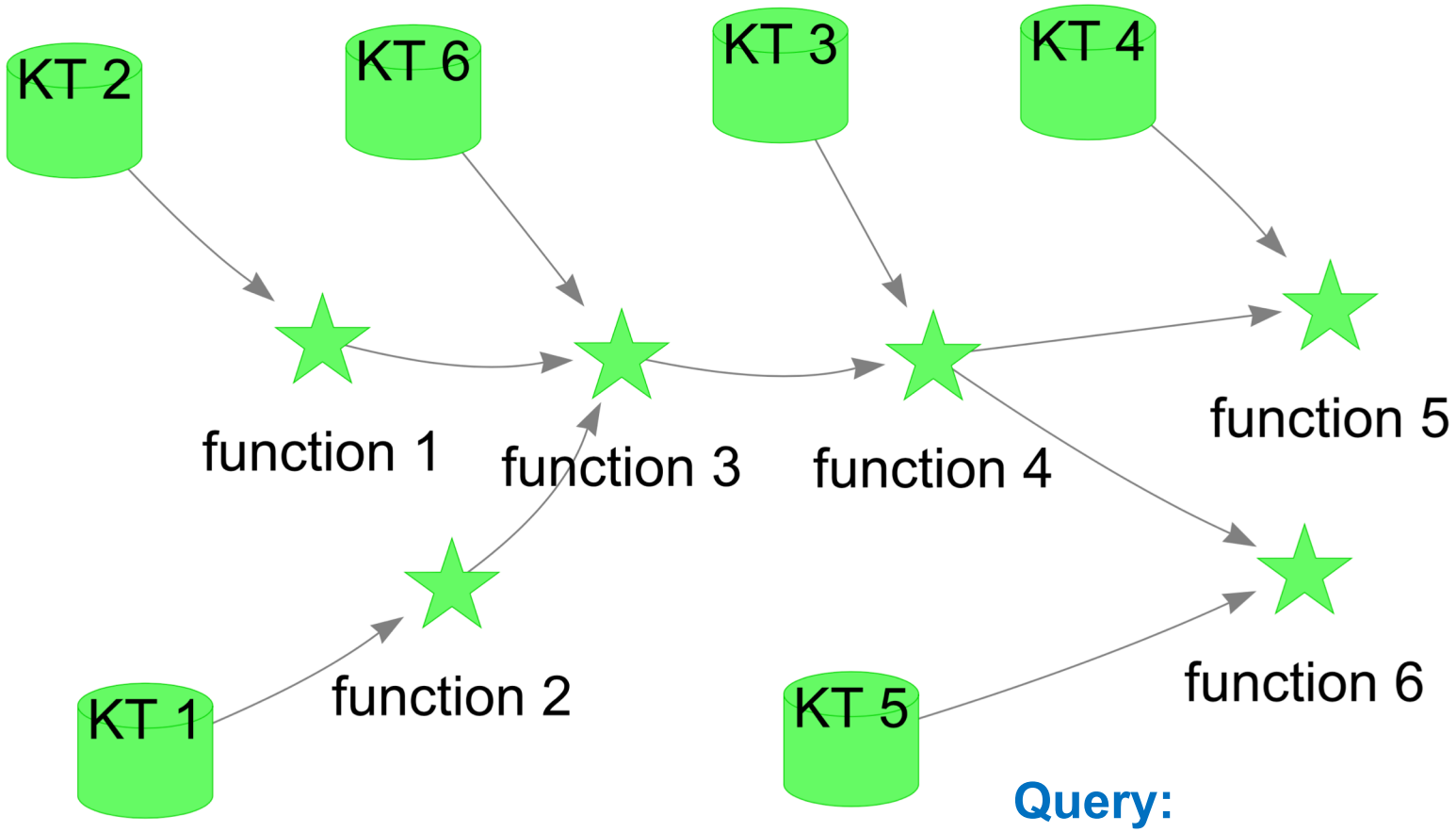
Query:

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



MITRE

Mission Dependency Edges



Query:

```
edgeTypes(MISSION)
```


MITRE

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

MITRE