*FloCon, Tucson Arizona*

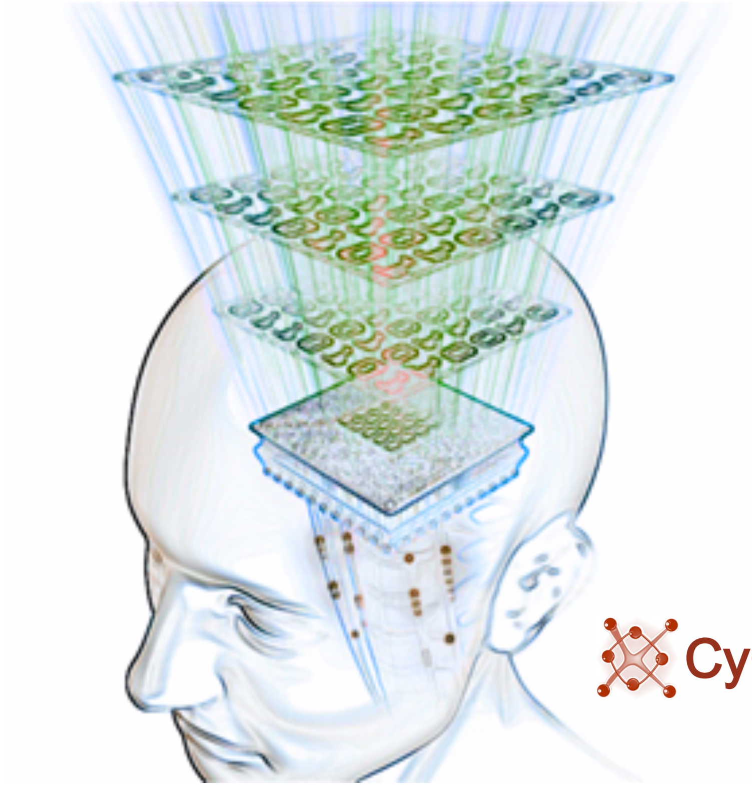
# CyGraph: Big-Data Graph Analysis For Cybersecurity and Mission Resilience

**Steven Noel, PhD**

**The MITRE Corporation**

**CyGraph Team:**
Eric Harley
Steve Purdy
Michael Limiero
Travis Lu
Will Mathews

January 11, 2018

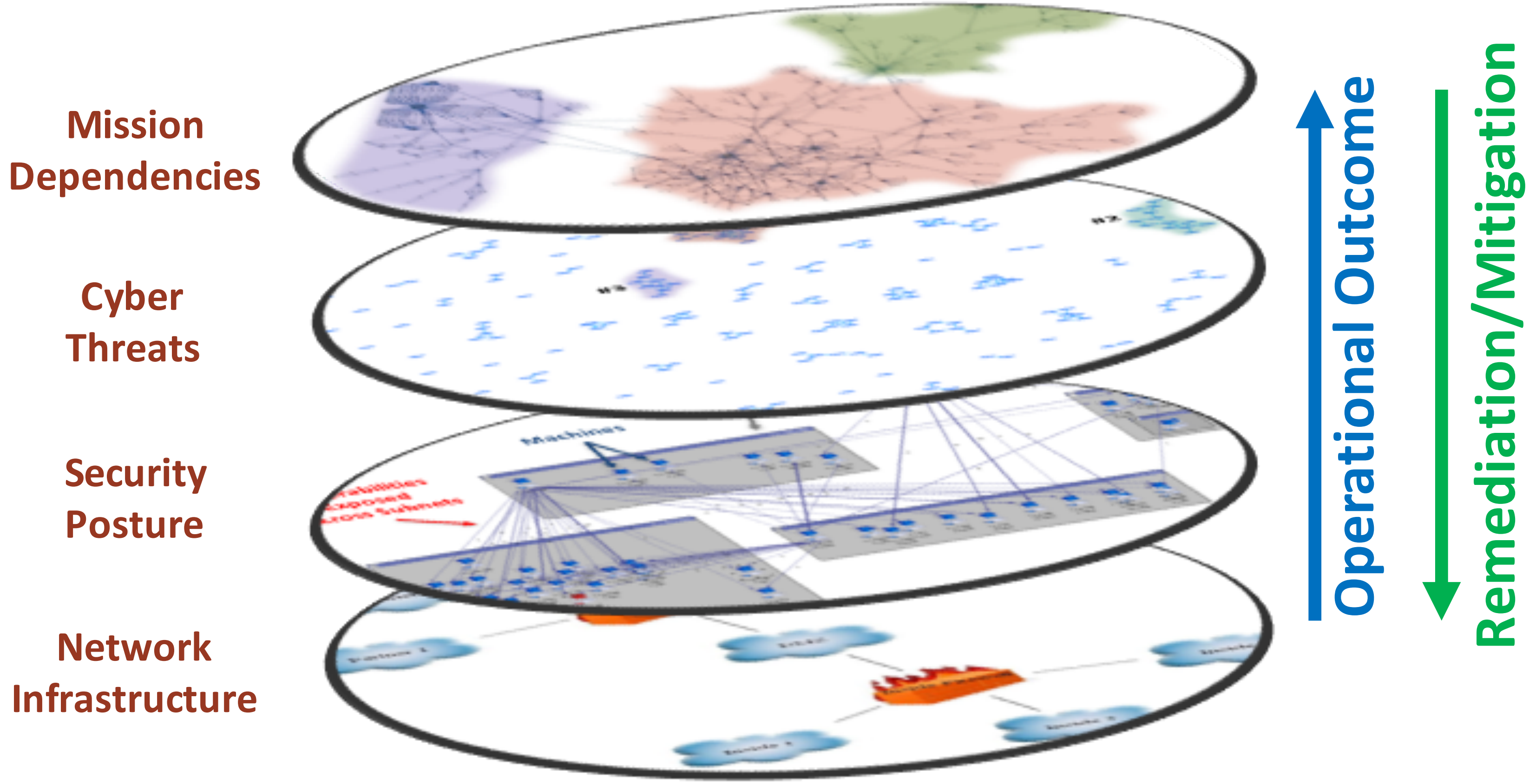


CyGraph

MITRE

Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

# Layered Graph Model for Cyber Resilience



Mission Dependencies

Cyber Threats

Security Posture

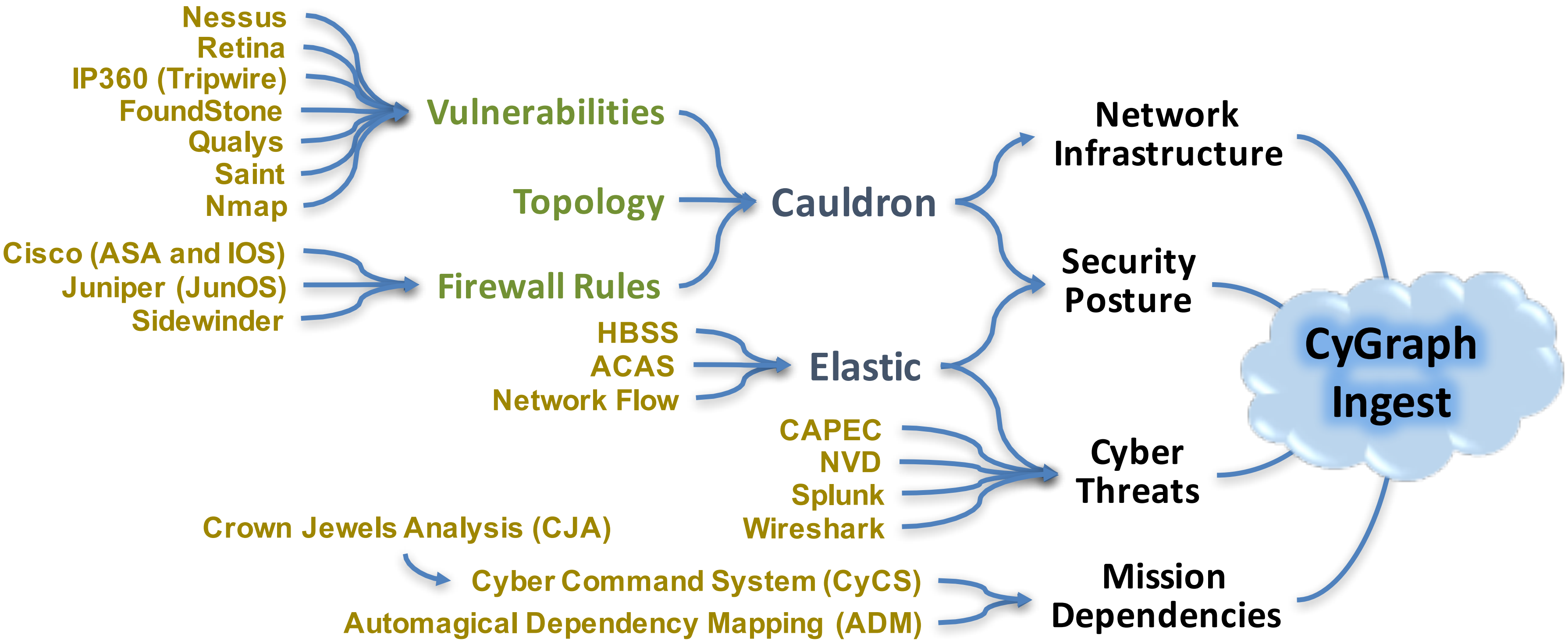
Network Infrastructure

Operational Outcome

Remediation/Mitigation

Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

# Example Data Sources



Nessus
Retina
IP360 (Tripwire)
FoundStone
Qualys
Saint
Nmap

Vulnerabilities

Topology

Cisco (ASA and IOS)
Juniper (JunOS)
Sidewinder

Firewall Rules

Cauldron

HBSS
ACAS
Network Flow

Elastic

CAPEC
NVD
Splunk
Wireshark

Crown Jewels Analysis (CJA)

Cyber Command System (CySC)
Automagical Dependency Mapping (ADM)

Network Infrastructure

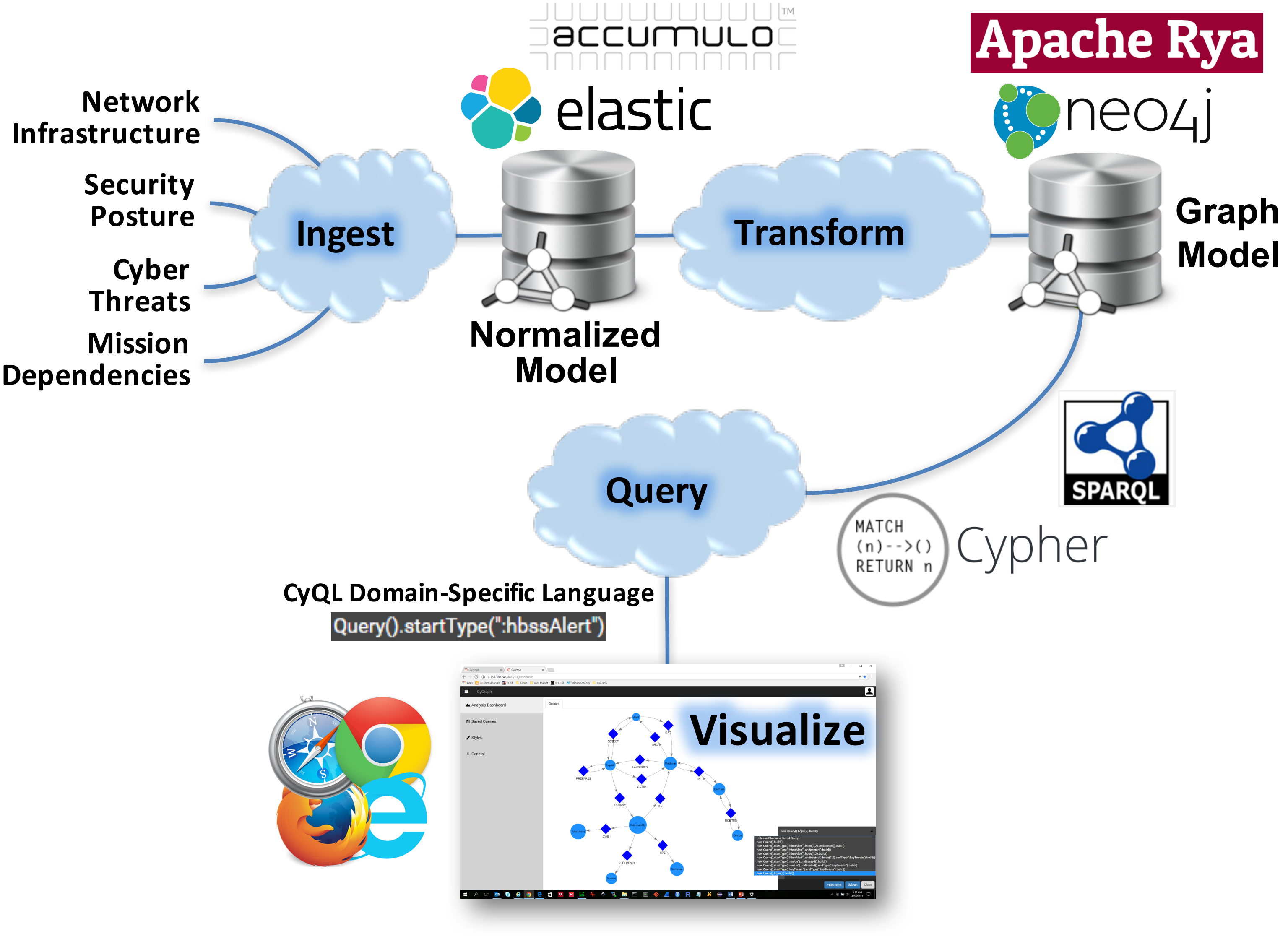
Security Posture

Cyber Threats

Mission Dependencies

CyGraph Ingest

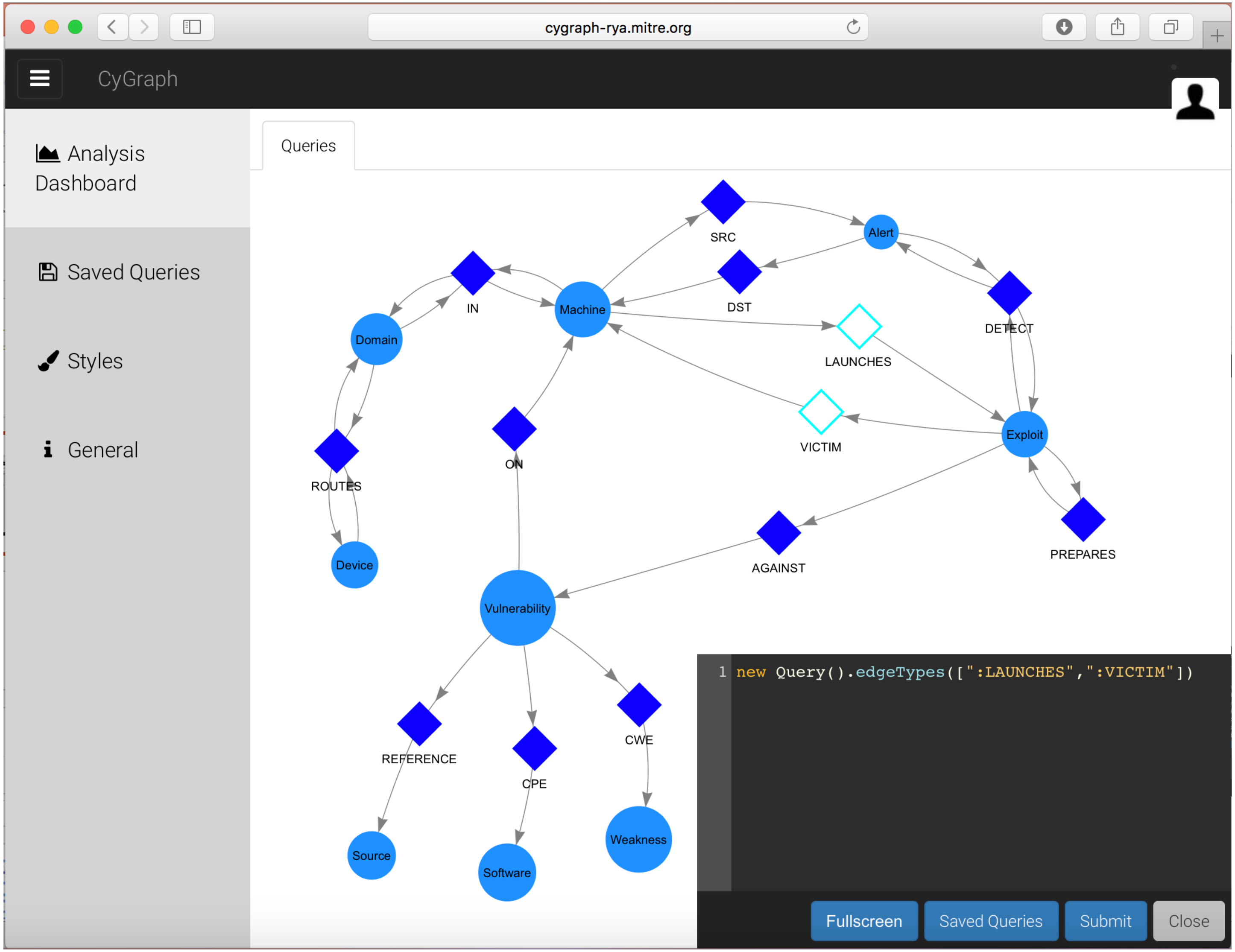
# CyGraph Architecture



```
Query().startType(":hbssAlert")
```

Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

# CyGraph Analysis Dashboard

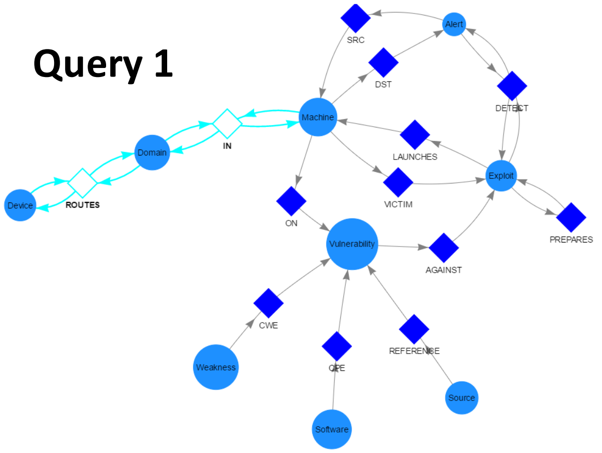


```
new Query().edgeTypes([":LAUNCHES",":VICTIM"])
```

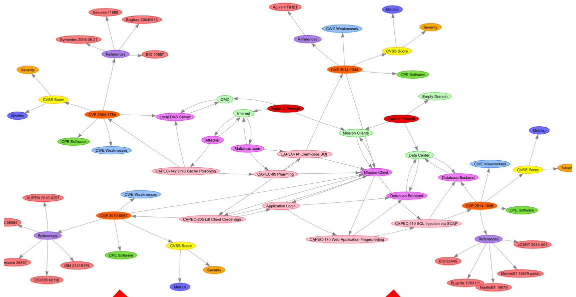
Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

# Queries via Dashboard Interaction

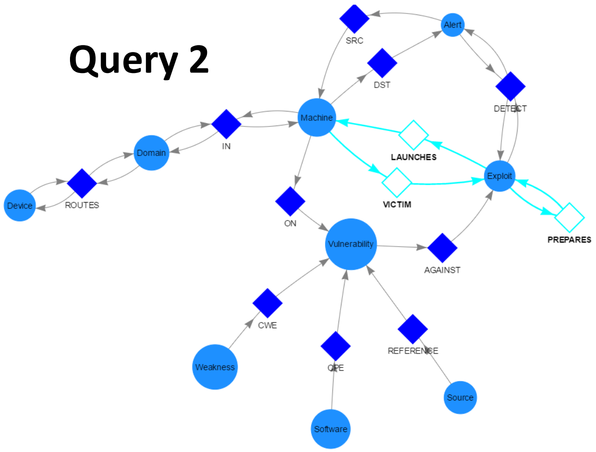
Query 1



Full Graph



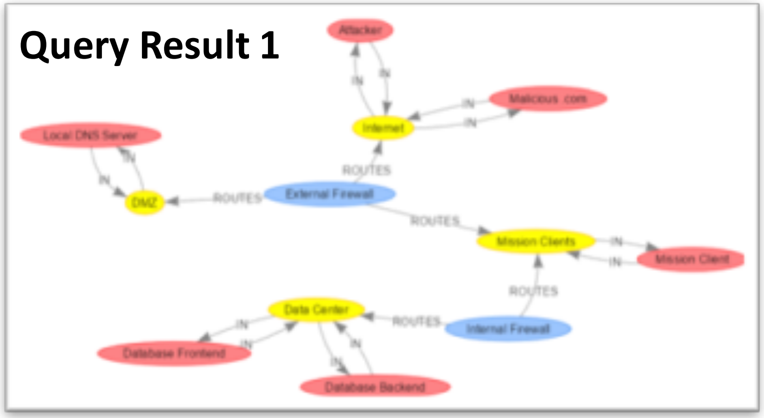
Query 2



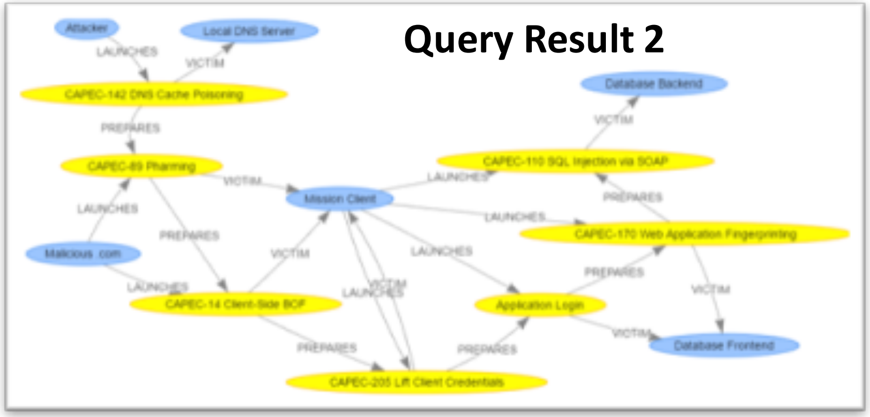
edgeTypes(:"IN",":ROUTES")

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

Query Result 1

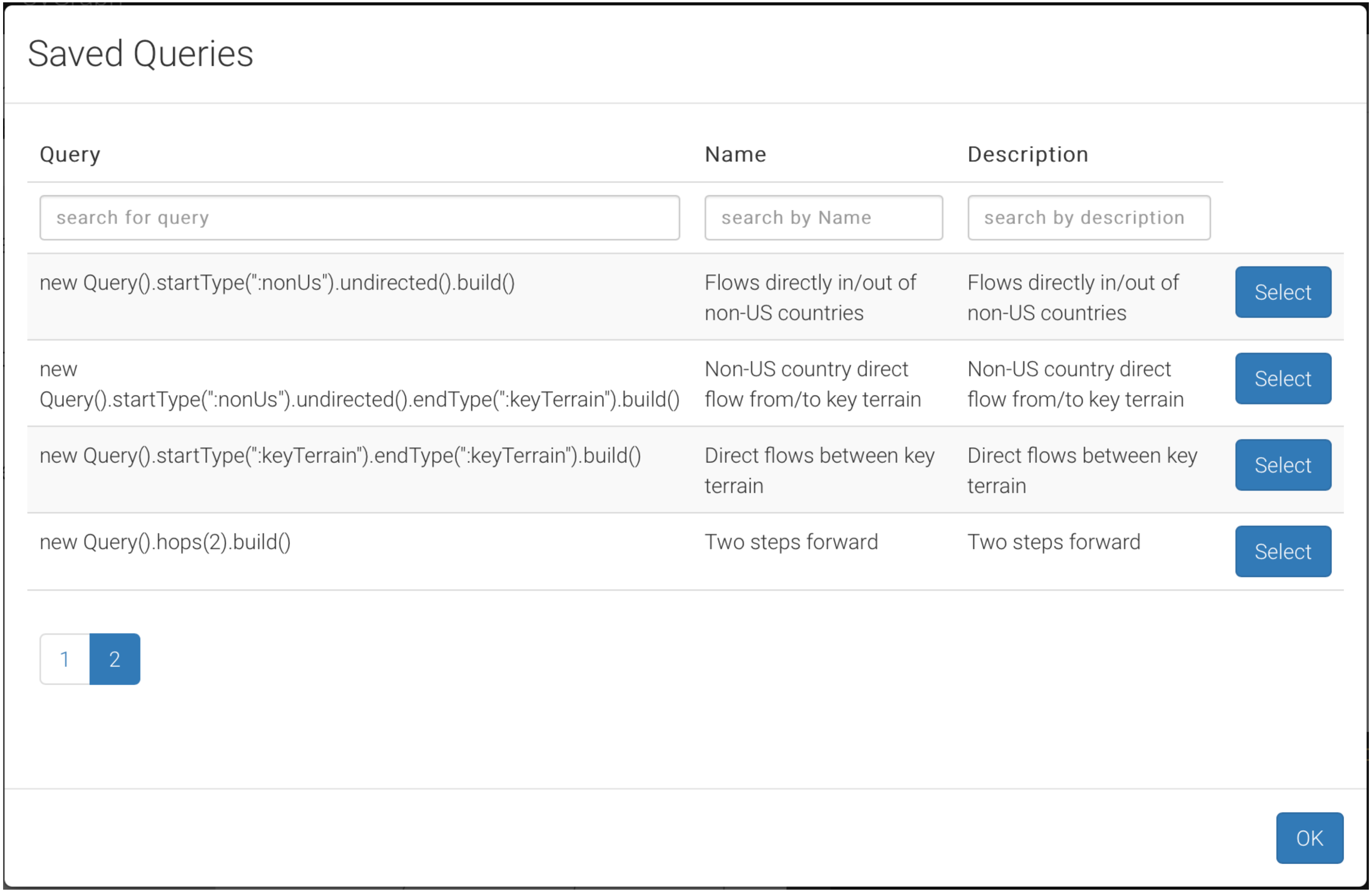


Query Result 2



Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

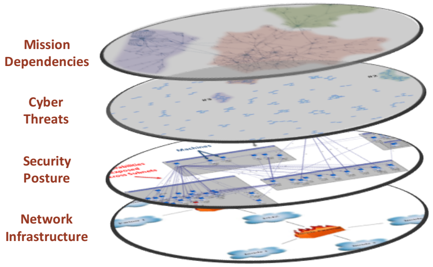
# Saved Queries

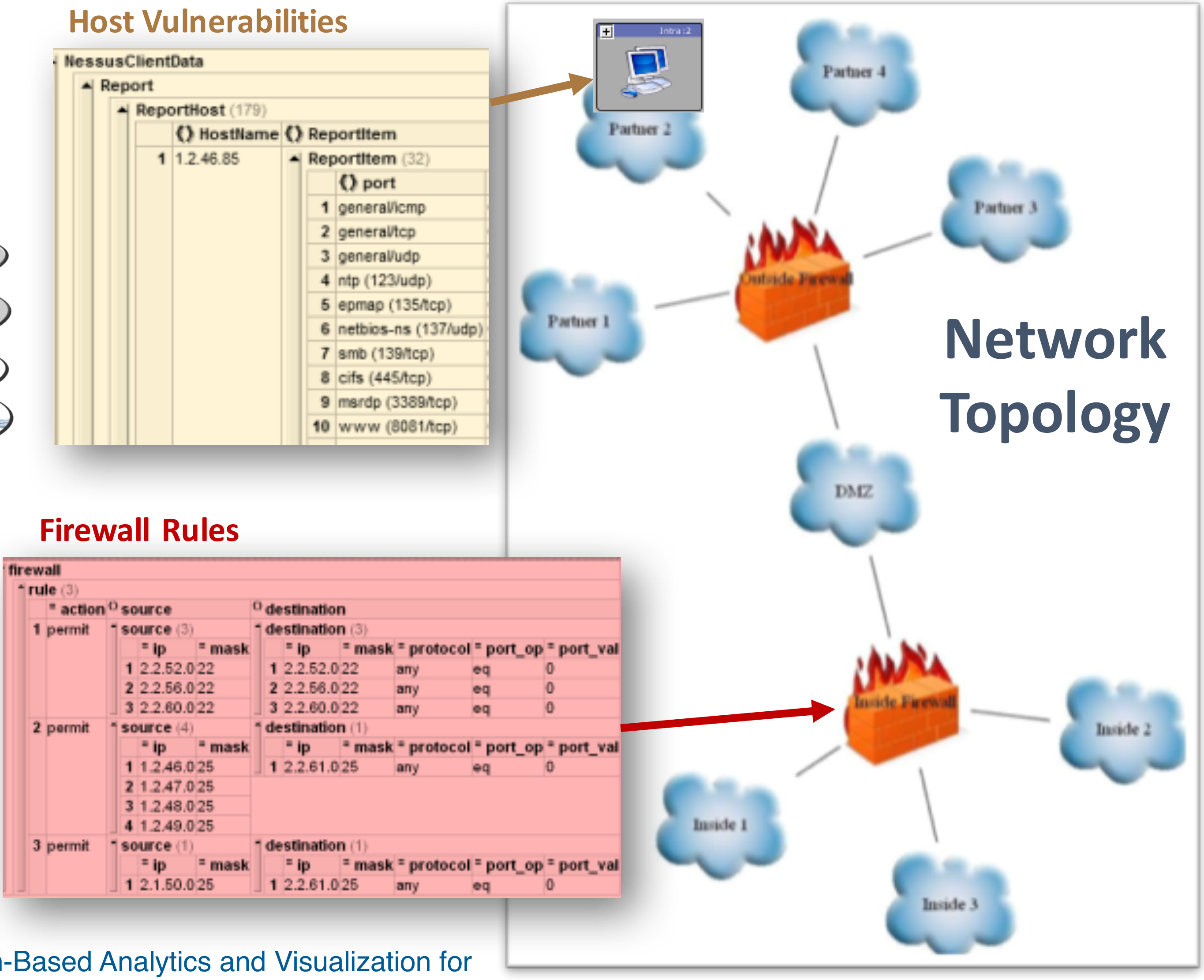


## Saved Queries

| Query | Name | Description | |
|---|---|---|---|
| search for query | search by Name | search by description | |
| new Query().startType(":nonUs").undirected().build() | Flows directly in/out of non-US countries | Flows directly in/out of non-US countries | Select |
| new Query().startType(":nonUs").undirected().endType(":keyTerrain").build() | Non-US country direct flow from/to key terrain | Non-US country direct flow from/to key terrain | Select |
| new Query().startType(":keyTerrain").endType(":keyTerrain").build() | Direct flows between key terrain | Direct flows between key terrain | Select |
| new Query().hops(2).build() | Two steps forward | Two steps forward | Select |

# 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)
```

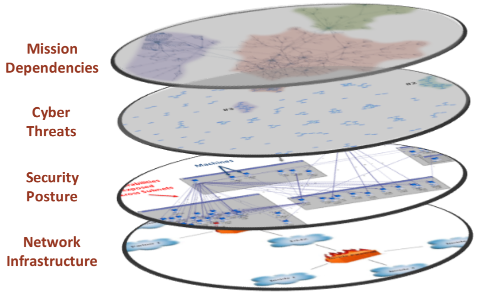
Firewall Rules

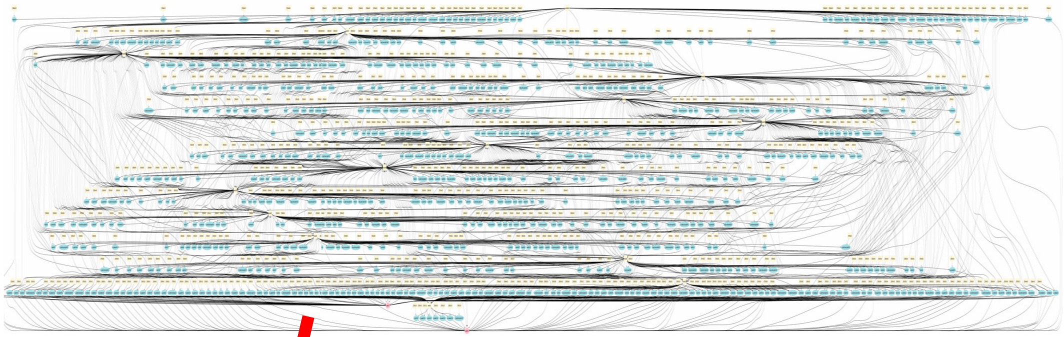
```
firewall
  rule (3)
       action  source             destination
     1 permit  source (3)         destination (3)
                  ip       mask      ip       mask  protocol  port_op  port_val
                1 2.2.52.0 22      1 2.2.52.0 22    any       eq       0
                2 2.2.56.0 22      2 2.2.56.0 22    any       eq       0
                3 2.2.60.0 22      3 2.2.60.0 22    any       eq       0
     2 permit  source (4)         destination (1)
                  ip       mask      ip       mask  protocol  port_op  port_val
                1 1.2.46.0 25      1 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
     3 permit  source (1)         destination (1)
                  ip       mask      ip       mask  protocol  port_op  port_val
                1 2.1.50.0 25      1 2.2.61.0 25    any       eq       0
```

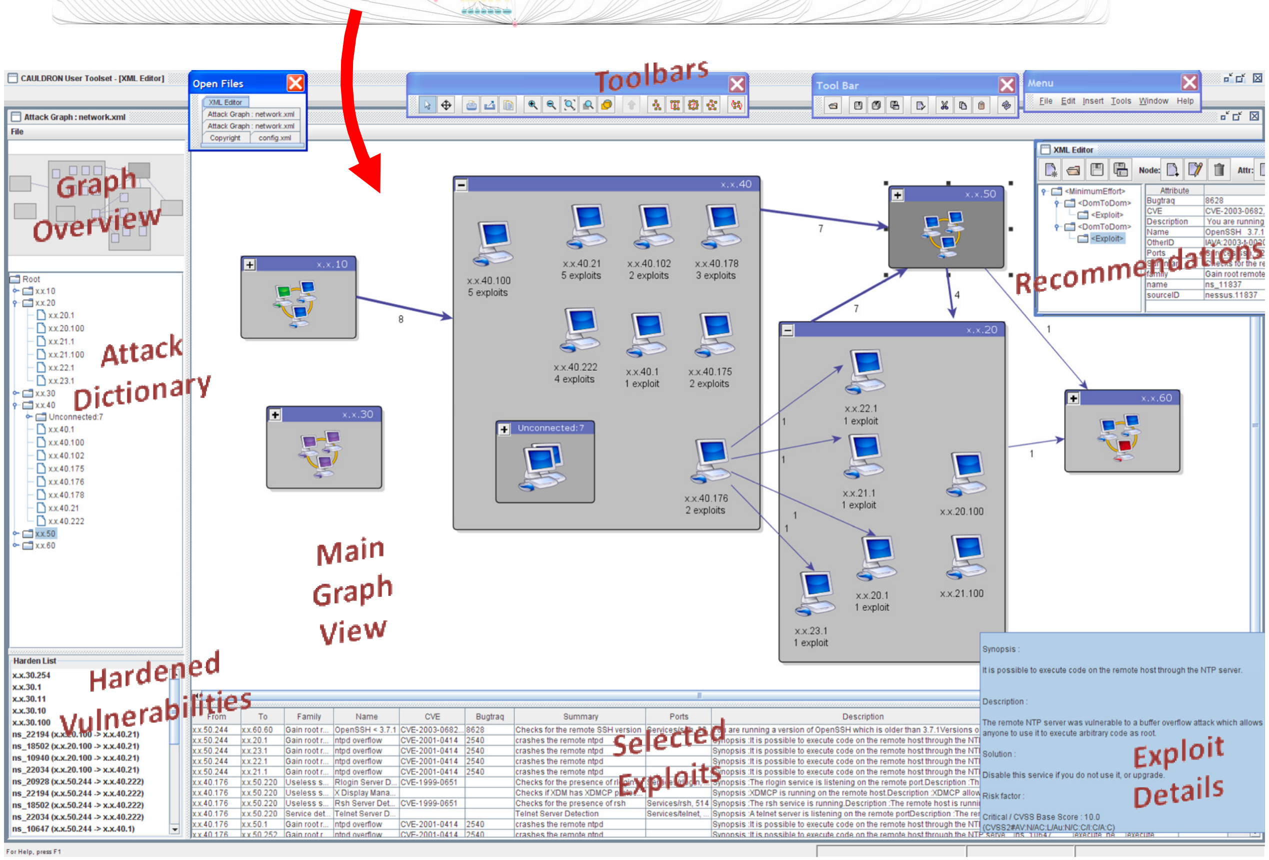
Network Topology

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

# Network Vulnerability Paths







| Attribute | |
|---|---|
| Bugtraq | 8628 |
| CVE | CVE-2003-0682, |
| Description | You are running |
| Name | OpenSSH 3.7.1 |
| OtherID | IAVA:2003-t-002 |
| Ports | [illegible] |
| [illegible] | [illegible] |
| family | Gain root remote |
| name | ns_11837 |
| sourceID | nessus.11837 |

Harden List

x.x.30.254
x.x.30.1
x.x.30.11
x.x.30.10
x.x.30.100
ns_22194 (x.x.20.100 -> x.x.40.21)
ns_18502 (x.x.20.100 -> x.x.40.21)
ns_10940 (x.x.20.100 -> x.x.40.21)
ns_22034 (x.x.20.100 -> x.x.40.21)
ns_20928 (x.x.50.244 -> x.x.40.222)
ns_22194 (x.x.50.244 -> x.x.40.222)
ns_18502 (x.x.50.244 -> x.x.40.222)
ns_22034 (x.x.50.244 -> x.x.40.222)
ns_10647 (x.x.50.244 -> x.x.40.1)

| From | To | Family | Name | CVE | Bugtraq | Summary | Ports | Description |
|---|---|---|---|---|---|---|---|---|
| x.x.50.244 | x.x.60.60 | Gain root r... | OpenSSH < 3.7.1 | CVE-2003-0682... | 8628 | Checks for the remote SSH version | Services/ssh, 22 | You are running a version of OpenSSH which is older than 3.7.1Versions o |
| x.x.50.244 | x.x.20.1 | Gain root r... | ntpd overflow | CVE-2001-0414 | 2540 | crashes the remote ntpd | | Synopsis :It is possible to execute code on the remote host through the NTI |
| x.x.50.244 | x.x.23.1 | Gain root r... | ntpd overflow | CVE-2001-0414 | 2540 | crashes the remote ntpd | | Synopsis :It is possible to execute code on the remote host through the NTI |
| x.x.50.244 | x.x.22.1 | Gain root r... | ntpd overflow | CVE-2001-0414 | 2540 | crashes the remote ntpd | | Synopsis :It is possible to execute code on the remote host through the NTI |
| x.x.50.244 | x.x.21.1 | Gain root r... | ntpd overflow | CVE-2001-0414 | 2540 | crashes the remote ntpd | | Synopsis :It is possible to execute code on the remote host through the NTI |
| x.x.40.176 | x.x.50.220 | Useless s... | Rlogin Server D... | CVE-1999-0651 | | Checks for the presence of rlogin | Services/rlogin, ... | Synopsis :The rlogin service is listening on the remote port.Description :Th |
| x.x.40.176 | x.x.50.220 | Useless s... | X Display Mana... | | | Checks if XDM has XDMCP p... | | Synopsis :XDMCP is running on the remote host.Description :XDMCP allow |
| x.x.40.176 | x.x.50.220 | Useless s... | Rsh Server Det... | CVE-1999-0651 | | Checks for the presence of rsh | Services/rsh, 514 | Synopsis :The rsh service is running.Description :The remote host is runnii |
| x.x.40.176 | x.x.50.220 | Service det... | Telnet Server D... | | | Telnet Server Detection | Services/telnet, ... | Synopsis :A telnet server is listening on the remote portDescription :The rer |
| x.x.40.176 | x.x.50.1 | Gain root r... | ntpd overflow | CVE-2001-0414 | 2540 | crashes the remote ntpd | | Synopsis :It is possible to execute code on the remote host through the NTI |
| x.x.40.176 | x.x.50.252 | Gain root r | ntpd overflow | CVE-2001-0414 | 2540 | crashes the remote ntpd | | Synopsis :It is possible to execute code on the remote host through the NTP serve |

Synopsis :

It is possible to execute code on the remote host through the NTP server.

Description :

The remote NTP server was vulnerable to a buffer overflow attack which allows anyone to use it to execute arbitrary code as root.

Solution :

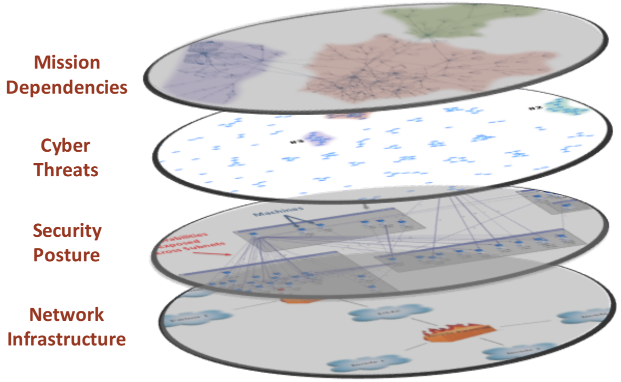
Disable this service if you do not use it, or upgrade.

Risk factor :

Critical / CVSS Base Score : 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

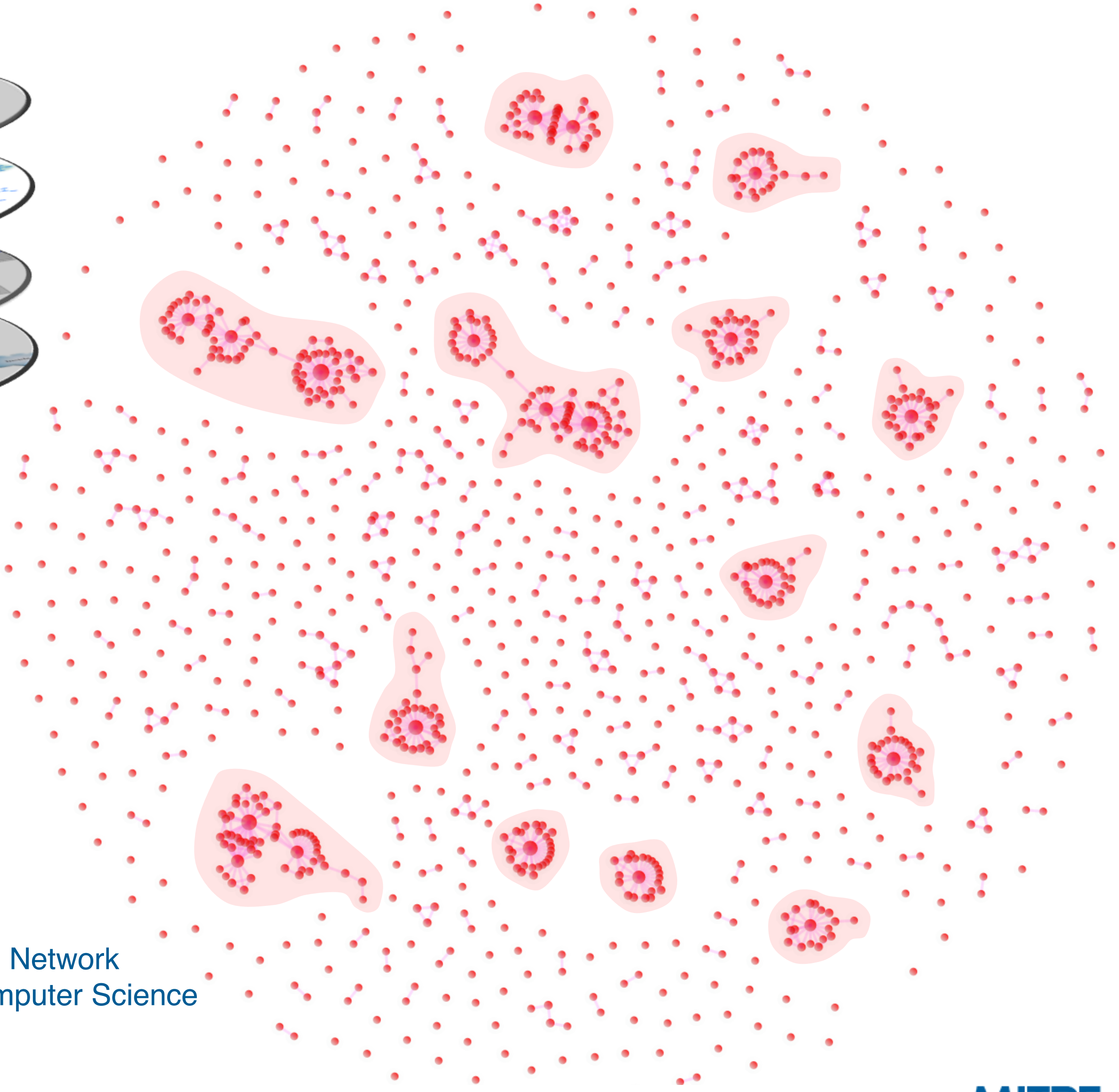
# Prioritizing Alert Clusters


Mission Dependencies

Cyber Threats

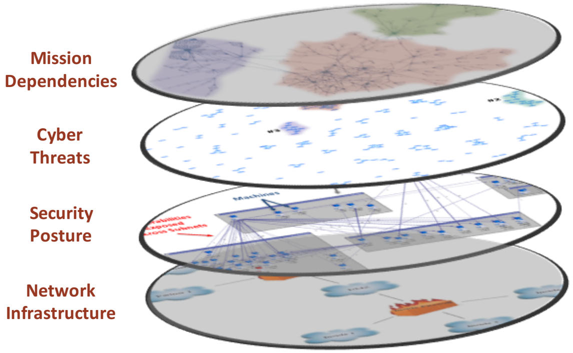
Security Posture

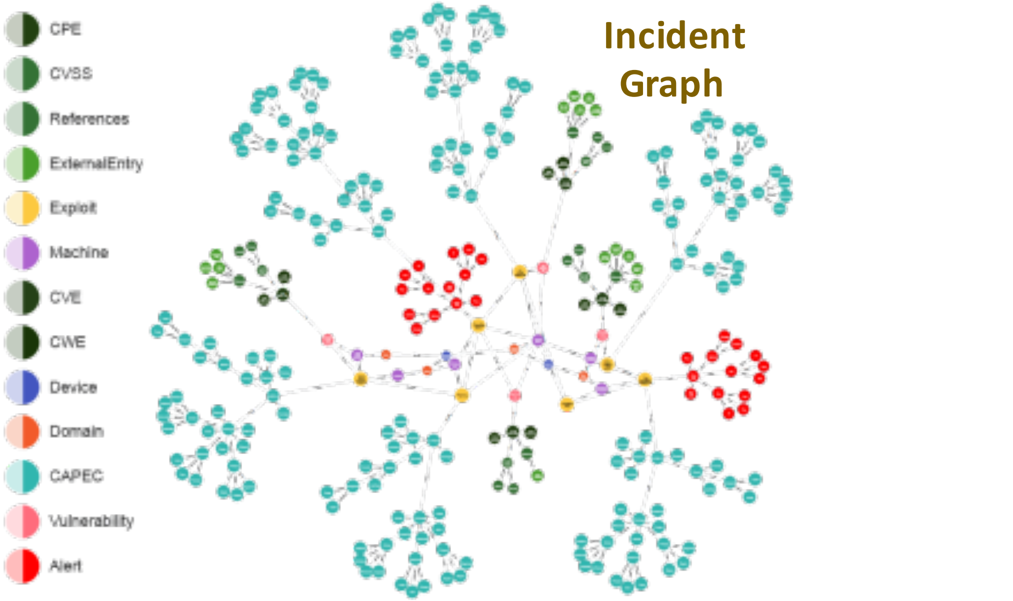
Network Infrastructure



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

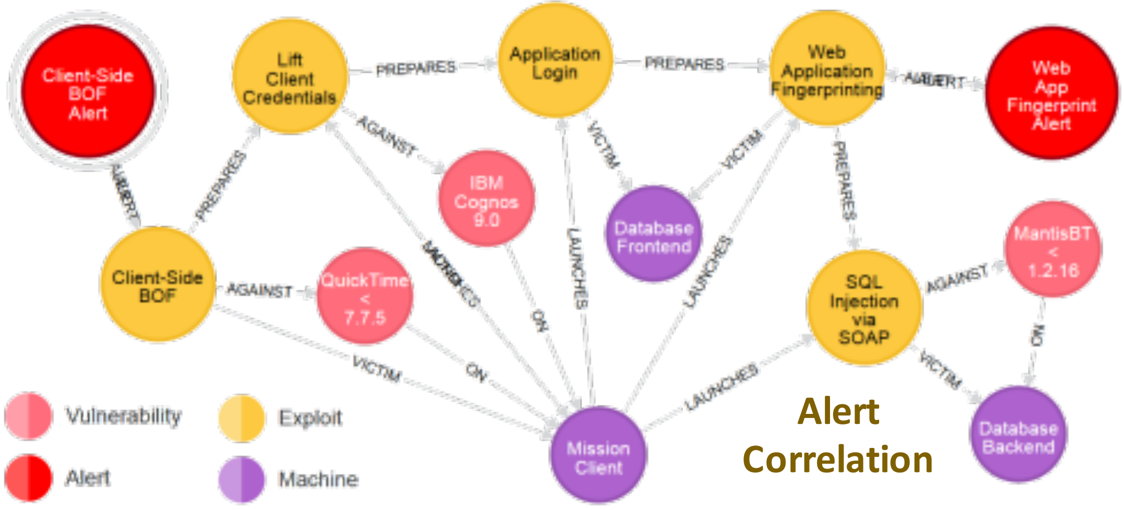
# Graph Query Analytics





Incident Graph

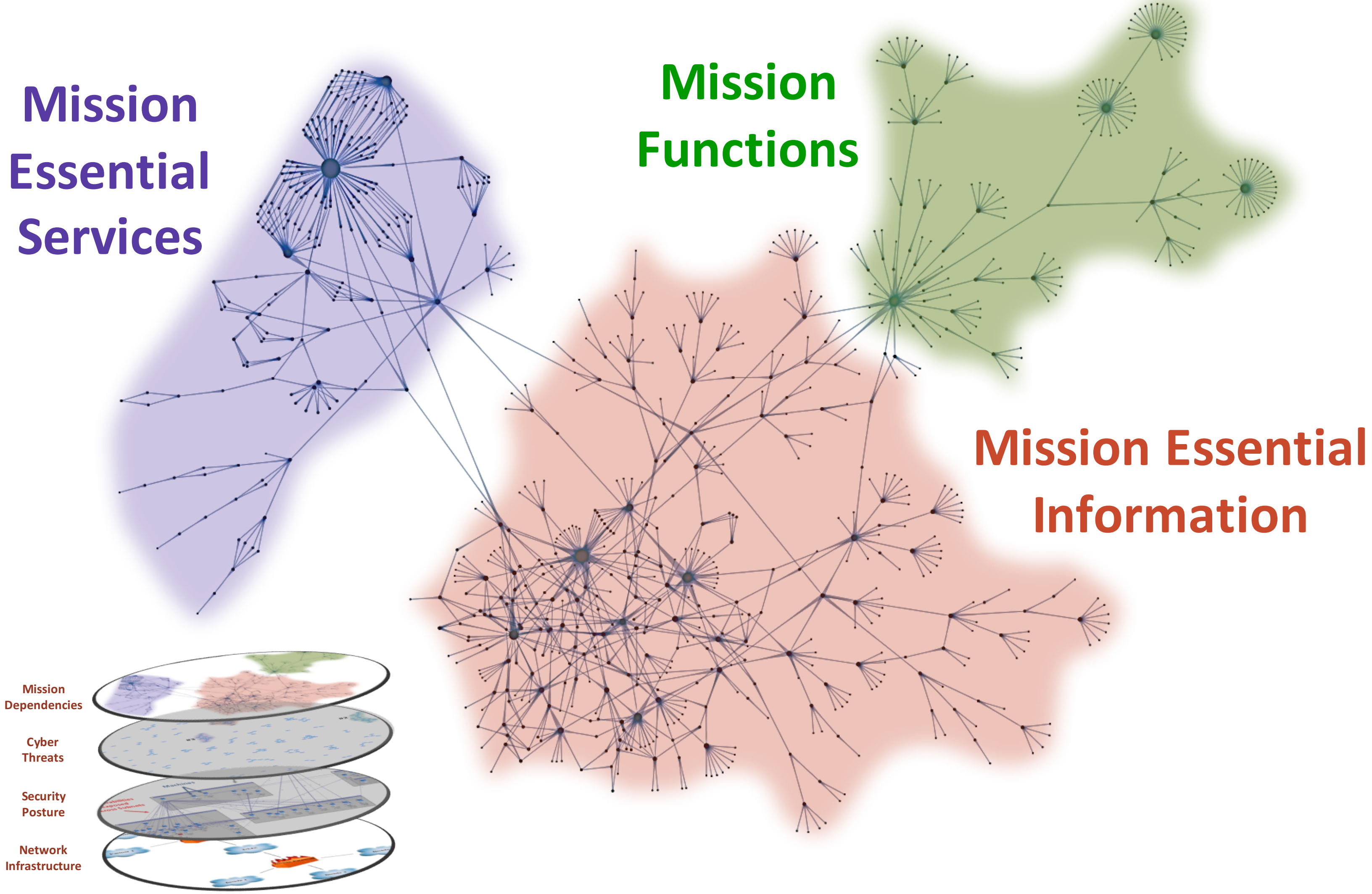
Noel et al, “Big-Data Architecture for Cyber Attack Graphs: Representing Security Relationships in NoSQL Graph Databases,” IEEE Symposium on Technologies for Homeland Security (HST), 2015.



Alert Correlation

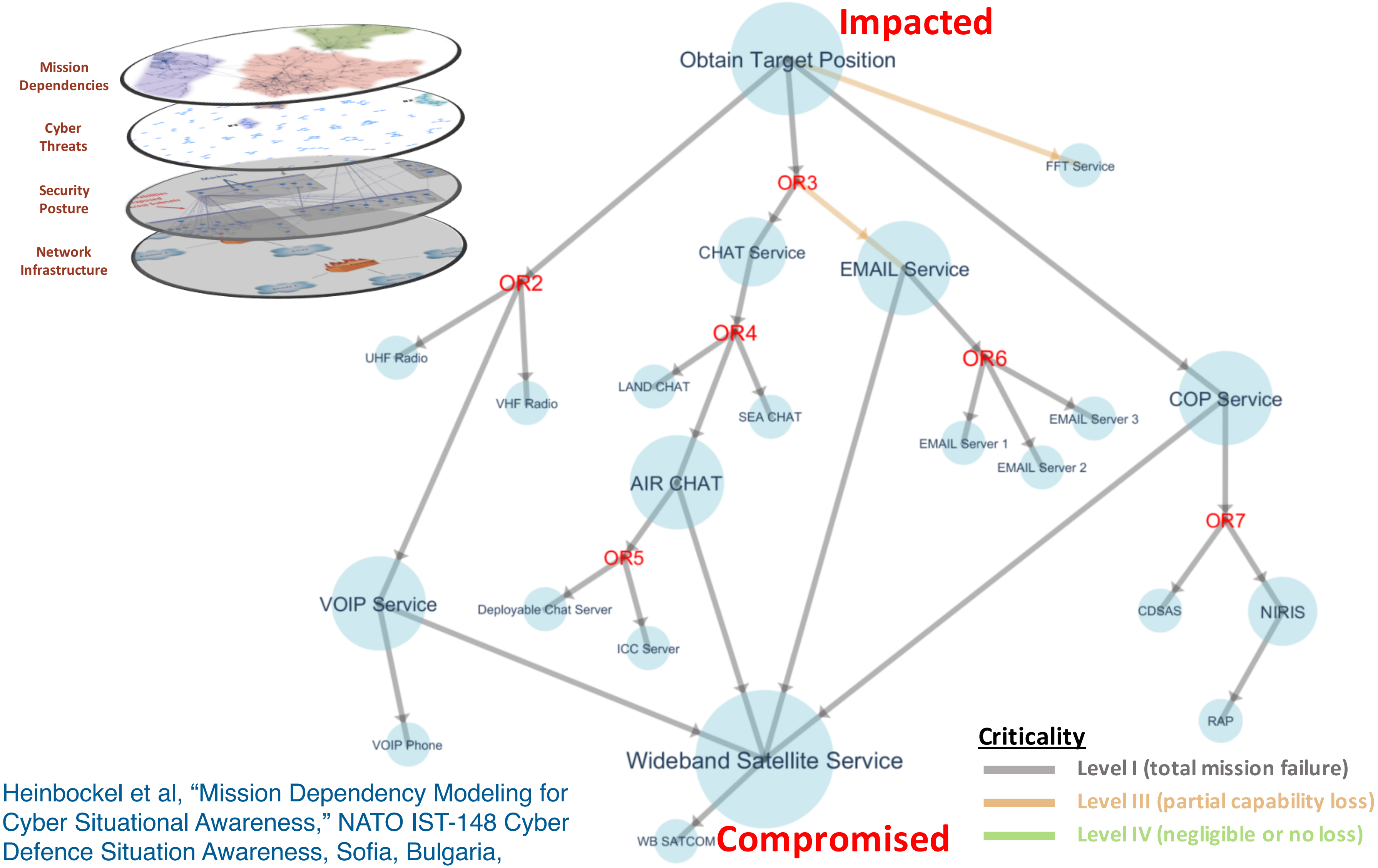
Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.

# Mission Dependencies



S. Musman, A. Turner, “A Game Theoretic Approach to Cyber Security Risk Management,” *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 2017.

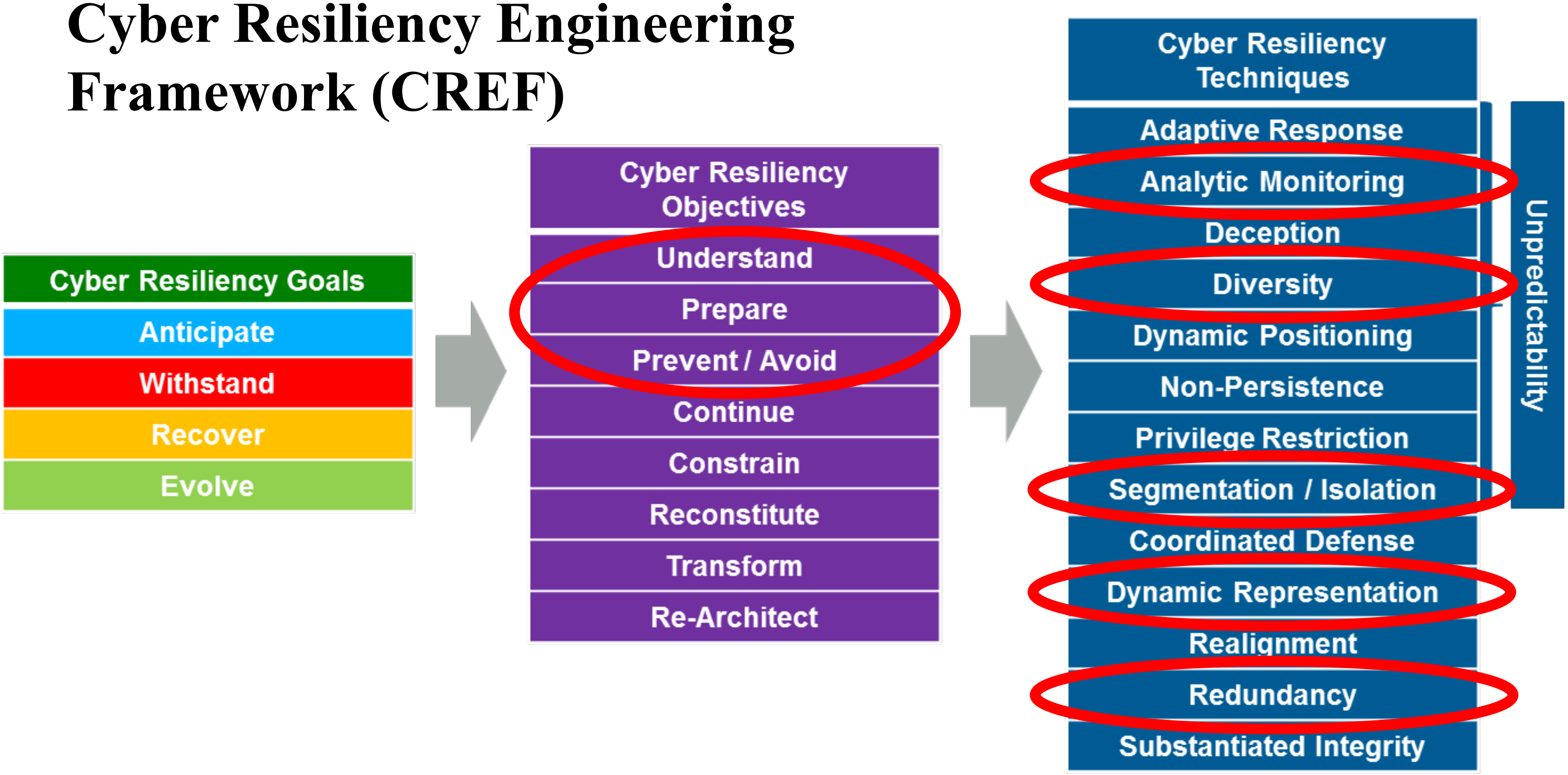
# Mission Impacts



Heinbockel et al, “Mission Dependency Modeling for Cyber Situational Awareness,” NATO IST-148 Cyber Defence Situation Awareness, Sofia, Bulgaria, October 2016.

# CyGraph Roles in Cyber Resilience

## Cyber Resiliency Engineering Framework (CREF)



Cyber Resiliency Goals

- Anticipate
- Withstand
- Recover
- Evolve

Cyber Resiliency Objectives

- Understand
- Prepare
- Prevent / Avoid
- Continue
- Constrain
- Reconstitute
- Transform
- Re-Architect

Cyber Resiliency Techniques

- Adaptive Response
- Analytic Monitoring
- Deception
- Diversity
- Dynamic Positioning
- Non-Persistence
- Privilege Restriction
- Segmentation / Isolation
- Coordinated Defense
- Dynamic Representation
- Realignment
- Redundancy
- Substantiated Integrity

- Bodeau and Graubart, *Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines*, MITRE Technical Report MTR17001, 2017.
- Bodeau, Graubart, Heinbockel, and Laderman, *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*, MITRE Technical Report MTR140499R1, 2015.

# Questions?

**Steven Noel**
**snoel@mitre.org**

Approved for Public Release; Distribution Unlimited. Case Numbers 17-2332, 16-2764, 16-0800.