65th Meeting of IFIP Working Group 10.4
On Dependable Computing and Fault Tolerance
Sorrento, Italy, January 23-27, 2014

Metrics Suite for Network Attack Graphs

Steven Noel

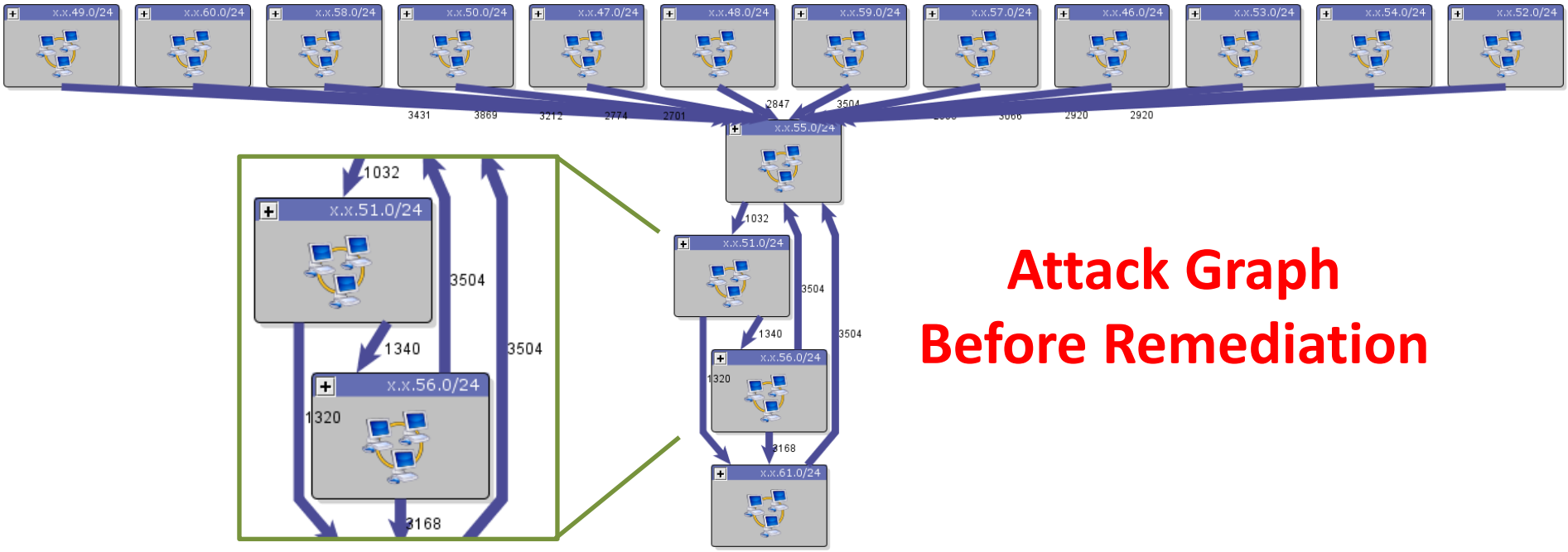
Center for Secure Information Systems
George Mason University

csis.gmu.edu

Motivation

- Impact of combined topology, policy, and vulnerabilities on security posture
  - Attack graphs show multi-step vulnerability paths through networks
  - But they lack quantitative scores that capture overall security state at a point in time
- Show metric trends over time
- Compare security across organizations
- Complementary dimensions of network security
- Funded by DHS BAA 11-02 (12 months)

Motivating Example

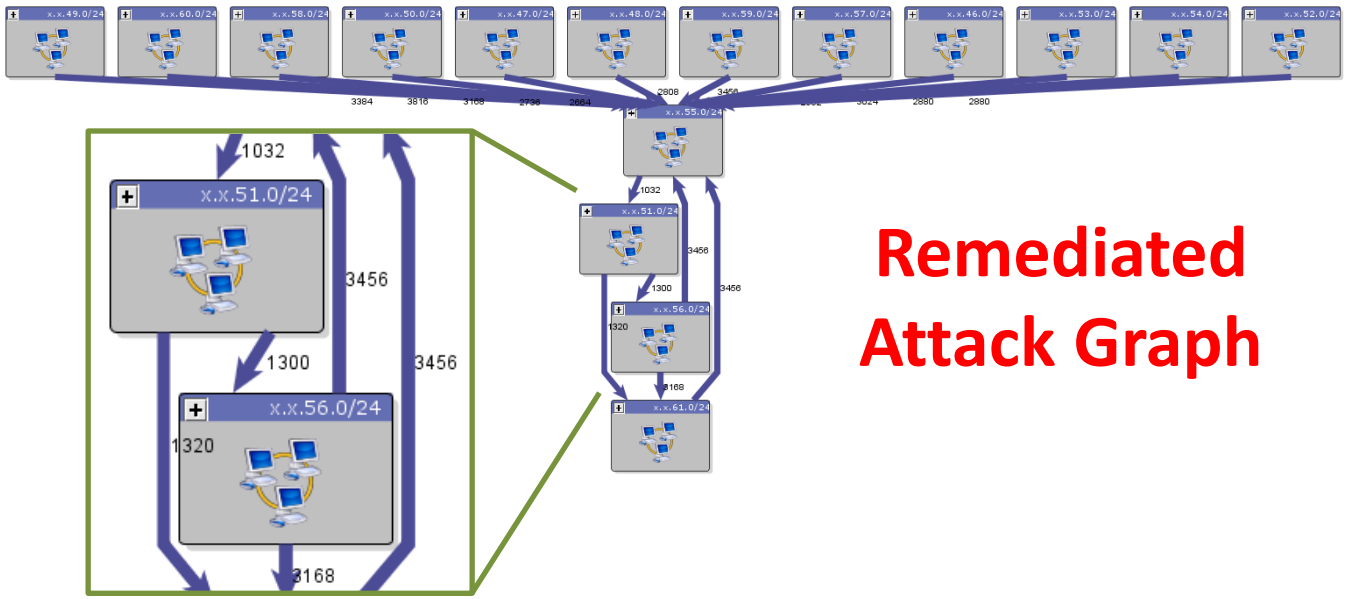


Attack Graph
Before Remediation

Top CVSS Vulnerabilities

CVSS > 7

CVSS Score	Include
10	☐
10	☐
10	☐
10	☐
10	☐
10	☐
10	☐
10	☐
7.6	☐
7.5	☐
7.5	☐
7.5	☐
7.5	☐
7.5	☐
7.5	☐
7.5	☐
6.9	☑
6.9	☑
6.5	☑
5.2	☑
5.2	☑
5	☑
5	☑
5	☑
5	☑
5	☑
5	☑
5	☑
4.3	☑
4.3	☑
4.3	☑
4.3	☑
4.3	☑
4.3	☑
4.3	☑
4.3	☑
-1	☑

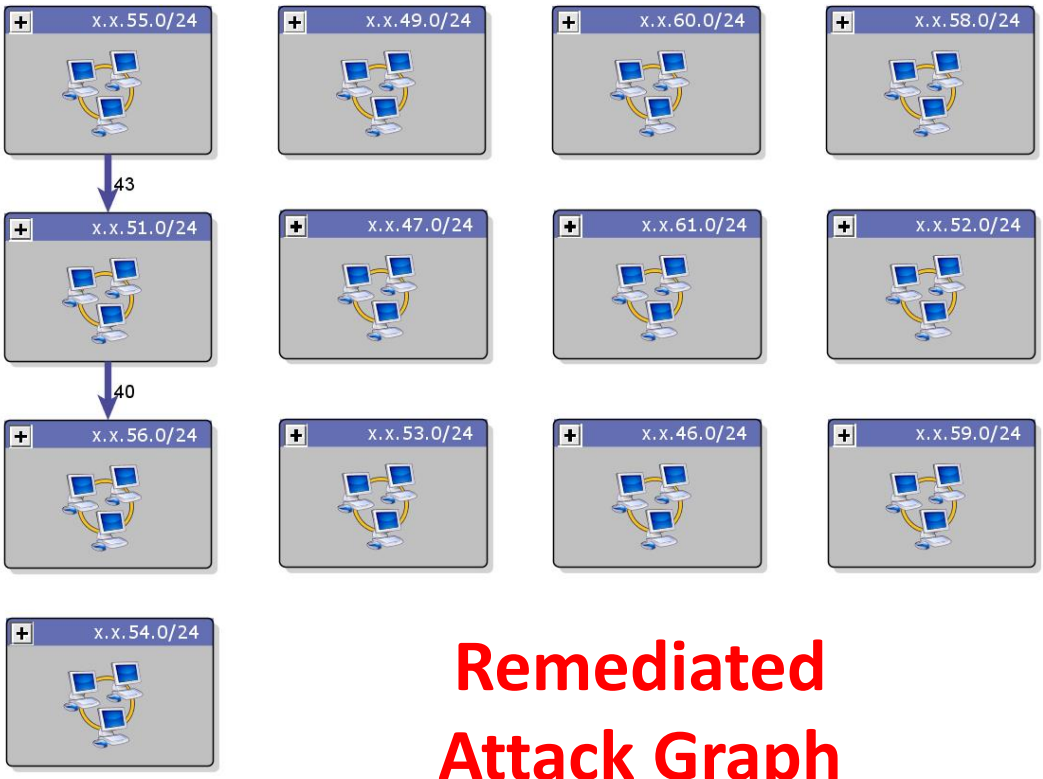


Remediated Attack Graph

Top Exposed Vulnerabilities

Top 3 Exposed

Connections	Include
25364	☐
25261	☐
609	☐
43	☑
20	☑
20	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑
0	☑

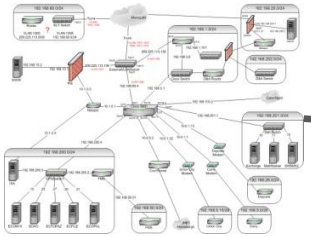


Remediated Attack Graph

Attack Graph Metrics

Network Topology

XML
CSV
Graphical

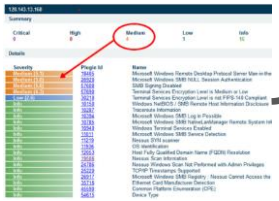


Firewall Rules

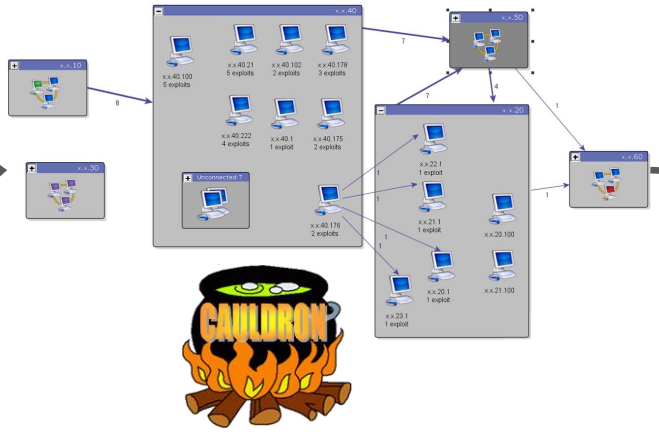
Cisco ASA
Cisco IOS
Juniper JUNOS
Juniper ScreenOS
Fortinet
McAfee FE

Host Vulnerabilities

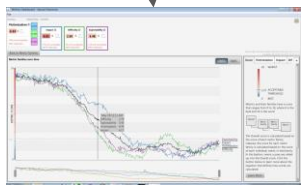
Nessus
Retina
nCircle
Core Impact
Foundscan
Qualys
SAINT
nmap



Attack Graph Analysis

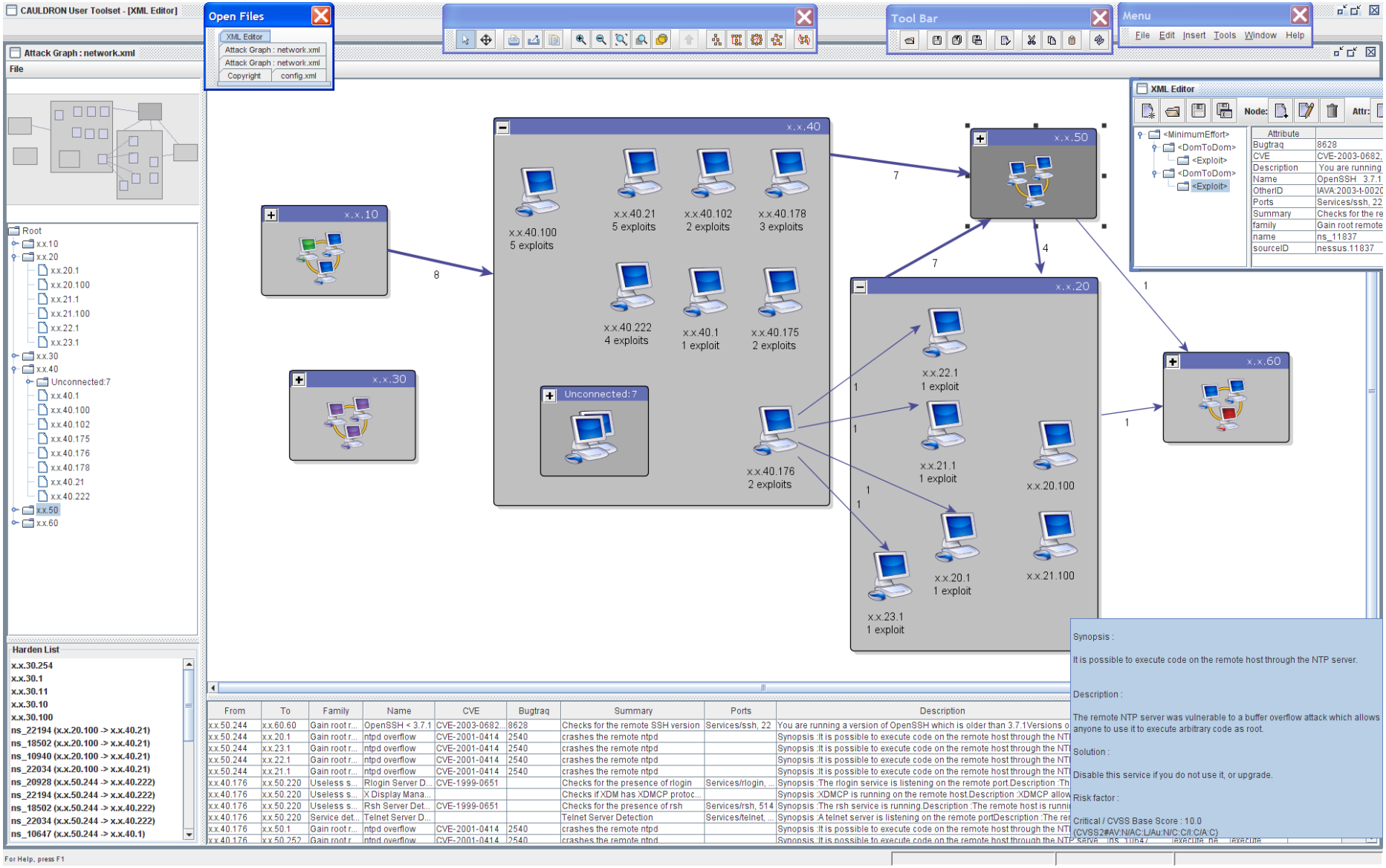


Metrics Engine

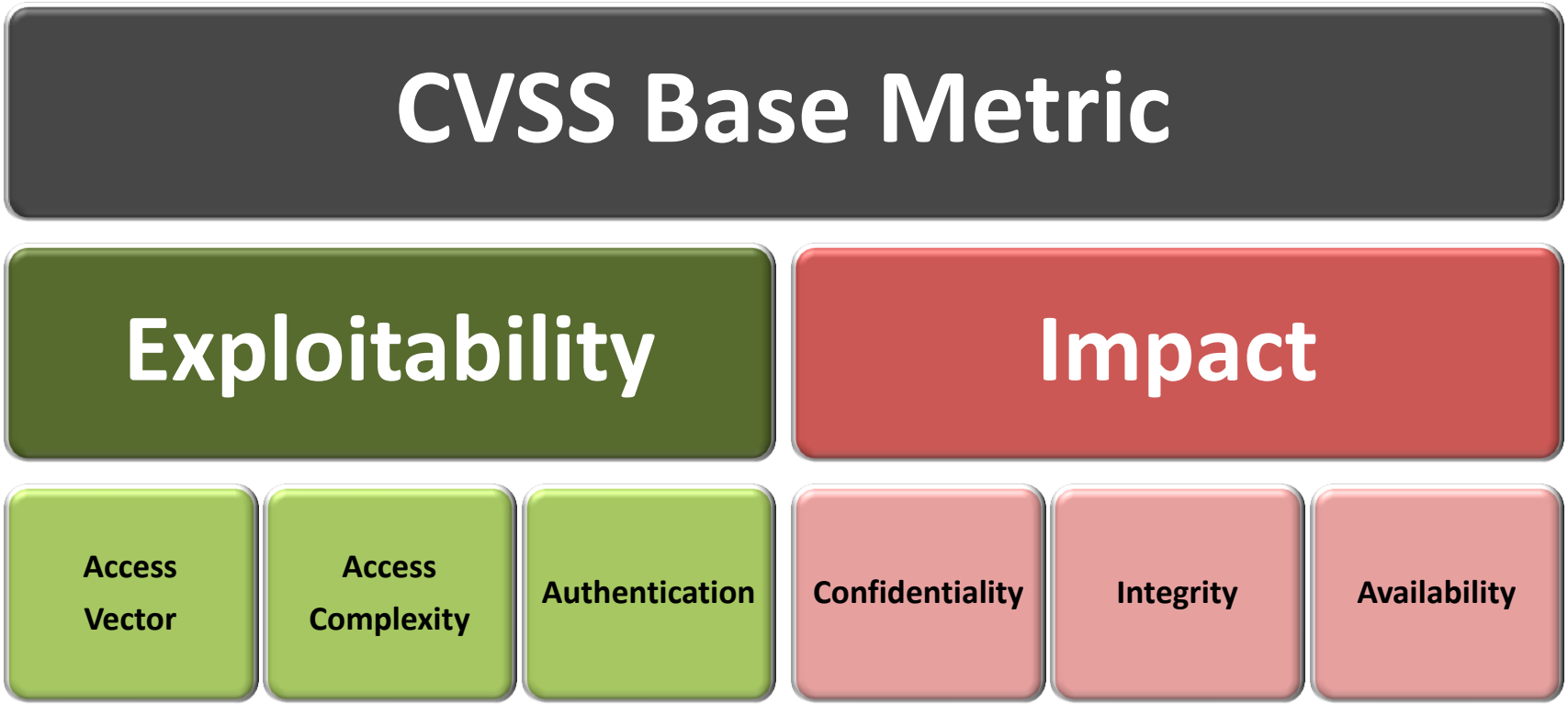


Metrics Dashboard

Cauldron Attack Graph



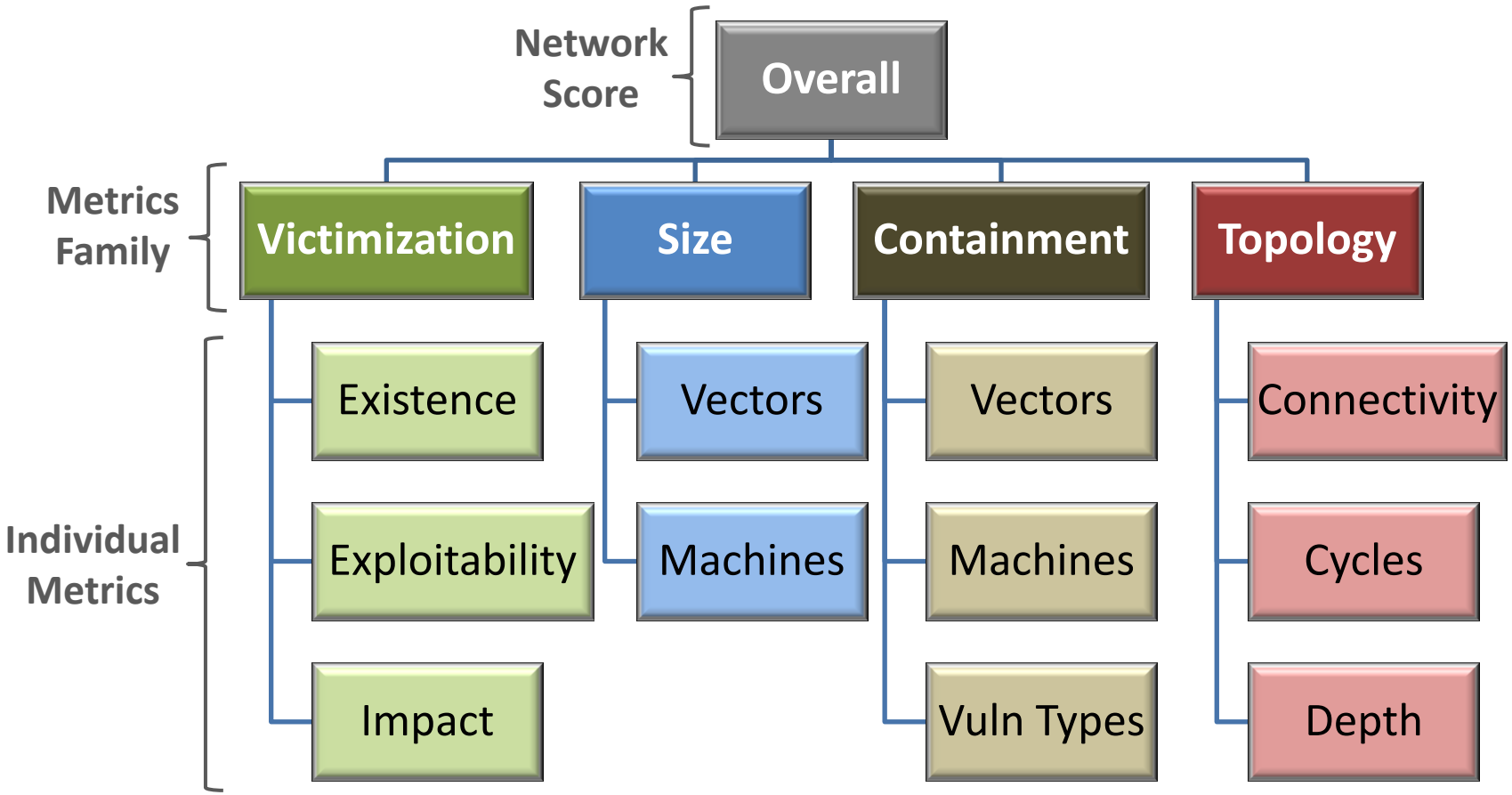
Common Vulnerability Scoring System (CVSS)



Attack Graph Metrics Families

- ***Victimization***: Individual vulnerabilities and exposed services each have elements of risk. We score the entire network across individual vulnerability victimization dimensions.
- ***Size***: The size of attack graph (vectors and exposed machines) is a prime indication of risk. The larger the graph, the more ways you can be compromised.
- ***Containment***: Networks are generally administered in pieces (subnets, domains, etc.). Risk mitigation should aim to reduce attacks across such boundaries, to contain attacks.
- ***Topology***: The connectivity, cycles, and depth of the attack graph indicate how graph relationships enable network penetration.

Metrics Hierarchy



Metrics Scaling

$$x \in (x_{\min}, x_{\max})$$

$$f^{(1)}(x) = x - x_{\min}$$

$$f^{(2)}(x) = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

$$f^{(3)}(x) = 10 \cdot \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

Metrics Scaling (Reversal)

$$x \in (x_{\min}, x_{\max})$$

$$f^{(1)}(x) = x - x_{\min}$$

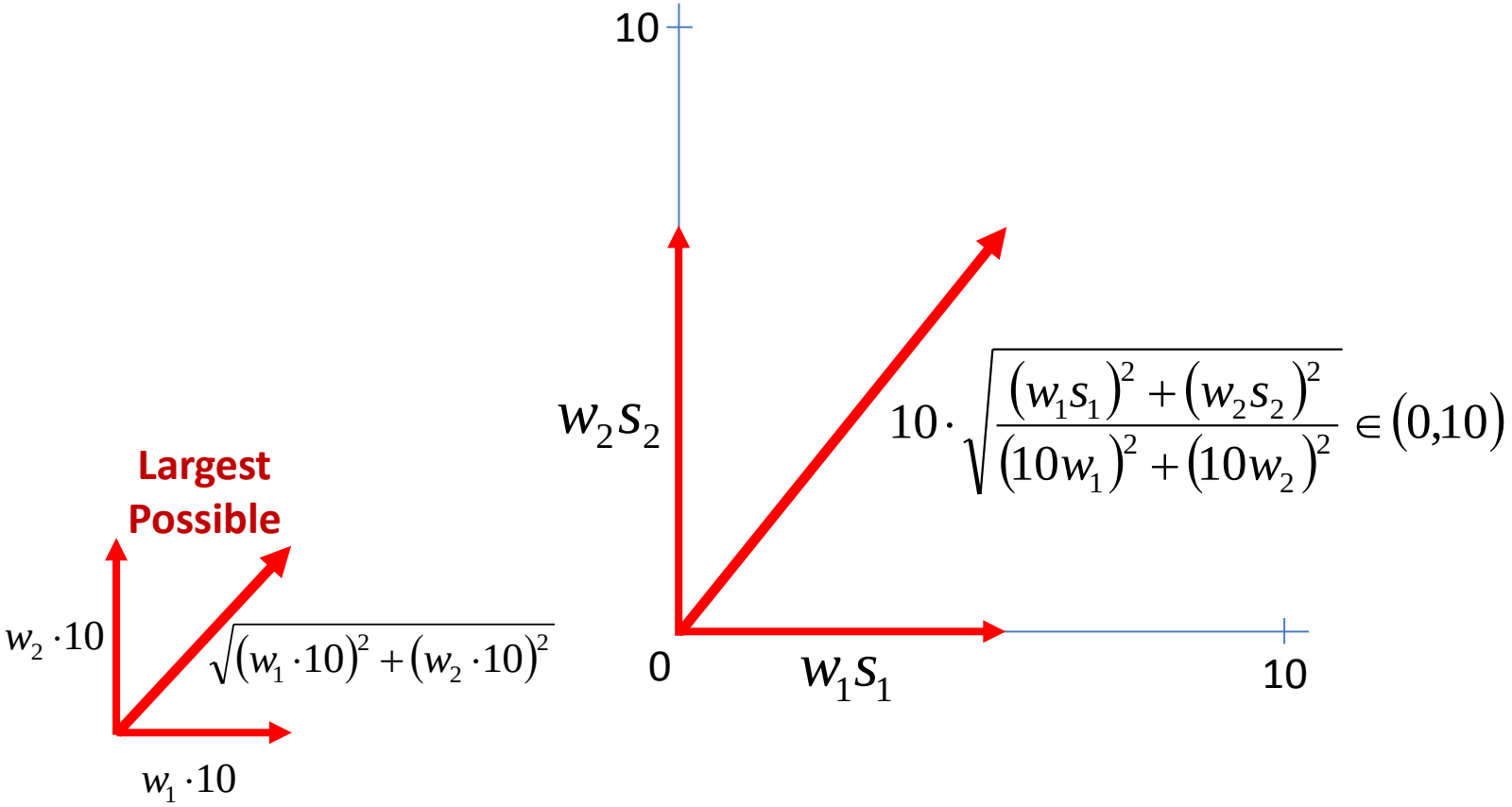
$$f^{(2)}(x) = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

$$f^{(3)}(x) = -1 \cdot \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

$$f^{(4)}(x) = 1 - \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

$$f^{(5)}(x) = 10 \cdot \left(1 - \frac{x - x_{\min}}{x_{\max} - x_{\min}}\right)$$

Combining Metrics



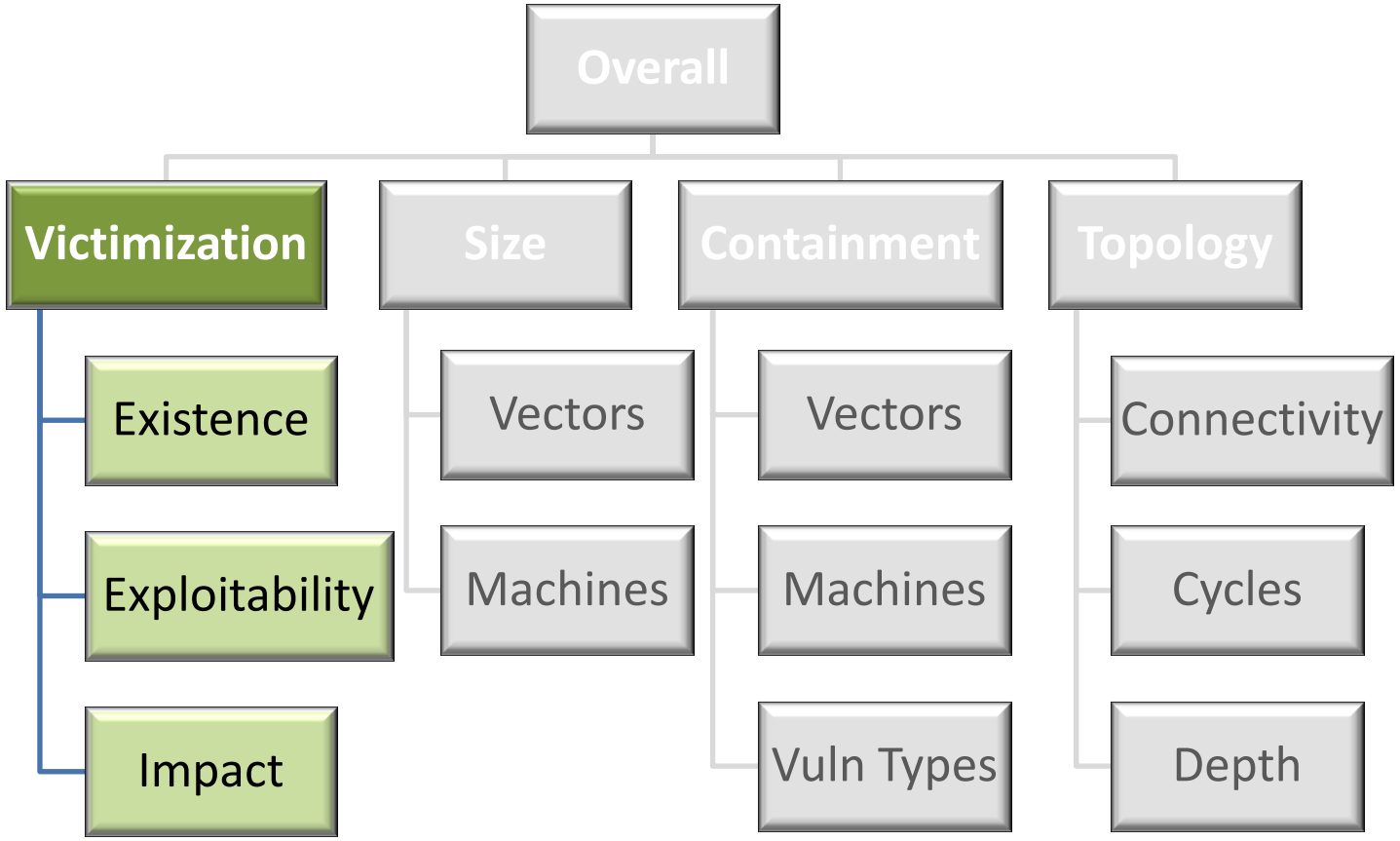
Combining Metrics

In general, for n scores, the combined score S is

$$S = 10 \cdot \sqrt{\frac{\sum_i^n (w_i s_i)^2}{\sum_i^n (10 w_i)^2}} \in (0,10)$$

For individual score s_i with weight w_i.

Metrics Hierarchy



Metrics Family: Victimization

- Existence – relative number of ports that are vulnerable:

$$\text{Existence} = 10 \cdot \frac{s_v}{s_v + s_n}$$

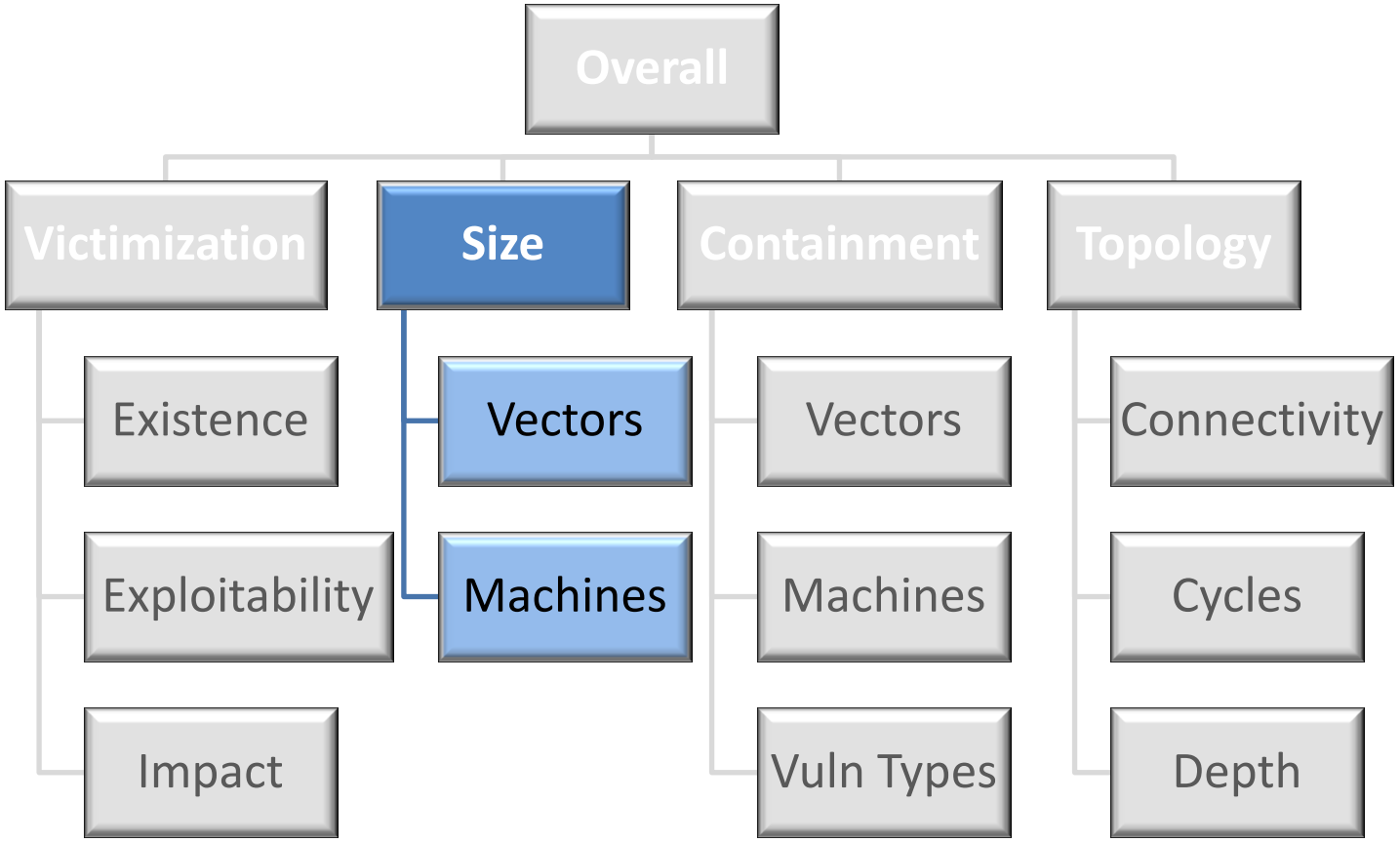
- Exploitability – average CVSS Exploitability:

$$\text{Exploitability} = \sum_i^U e(u_i) / U$$

- Impact – average CVSS Impact:

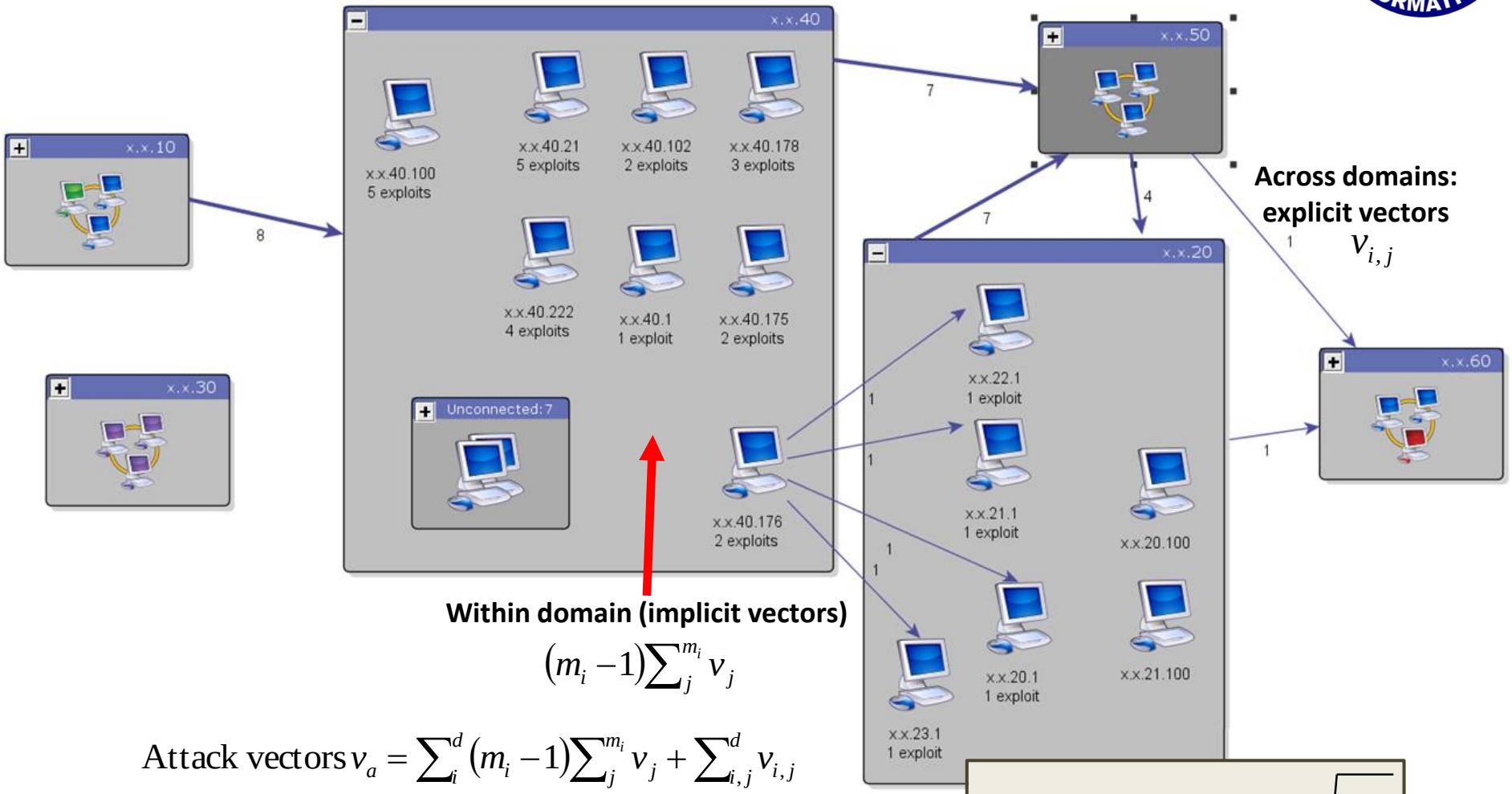
$$\text{Impact} = \sum_i^U m(u_i) / U,$$

Metrics Hierarchy



Size Family

Vectors Metric



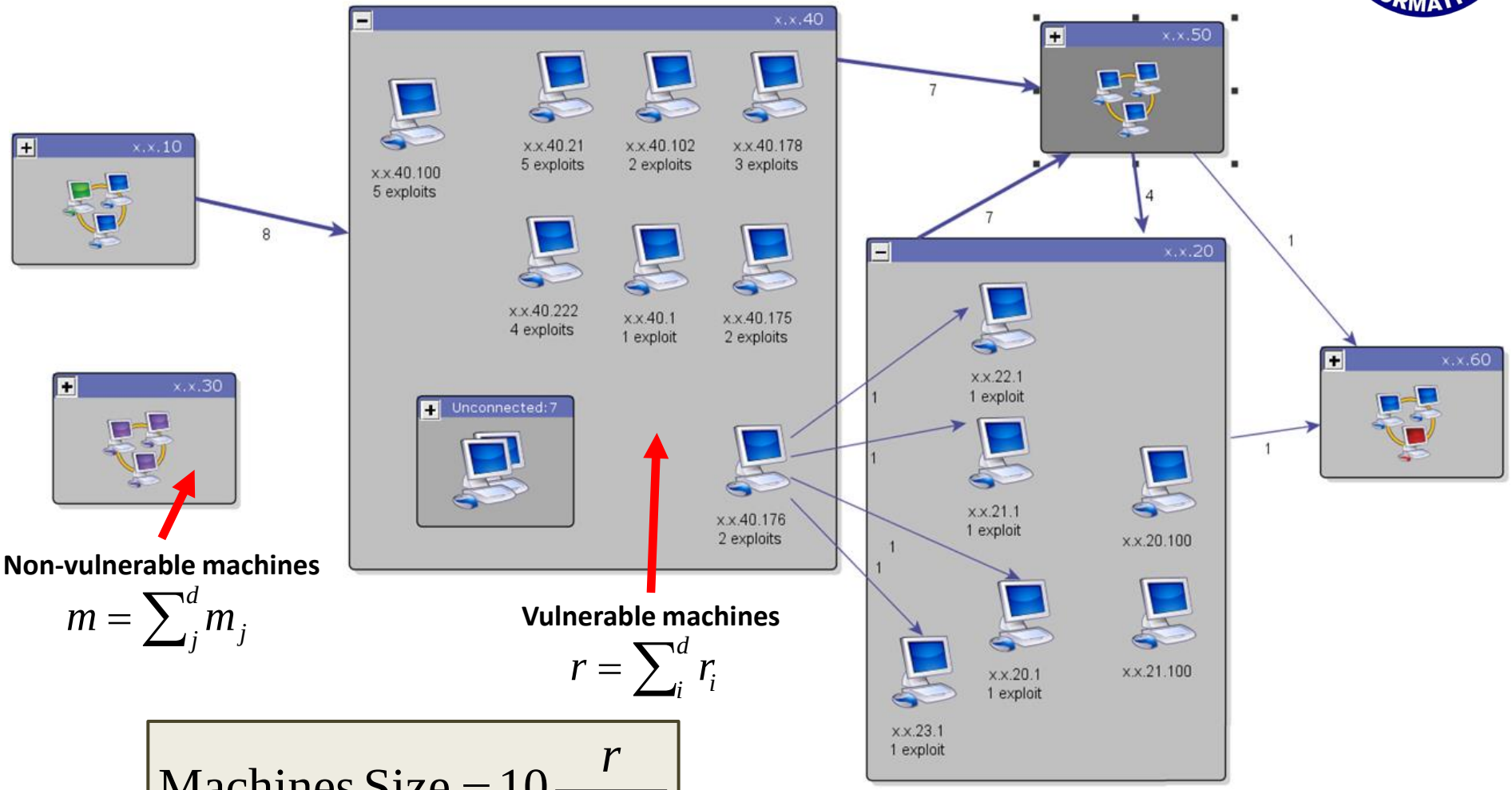
$$\text{Attack vectors } v_a = \sum_i^d (m_i - 1)\sum_j^{m_i} v_j + \sum_{i,j}^d v_{i,j}$$

$$\text{Total possible attack vectors } v_p = (m-1)\sum_i^m s_i$$

$$\text{Vectors Size} = 10\sqrt{\frac{v_a}{v_p}}$$

Size Family

Machines Metric



Non-vulnerable machines

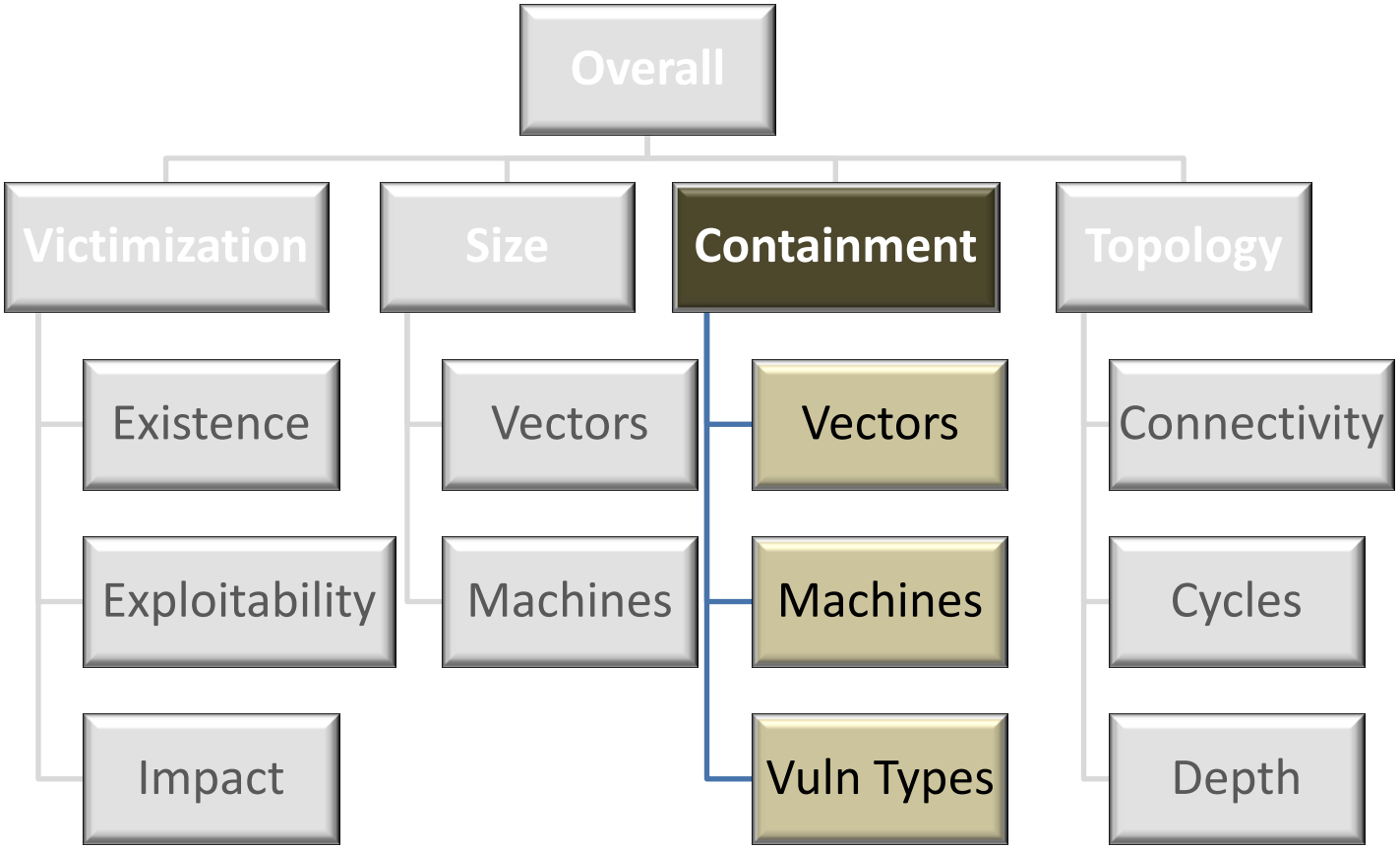
$$m = \sum_j^d m_j$$

Vulnerable machines

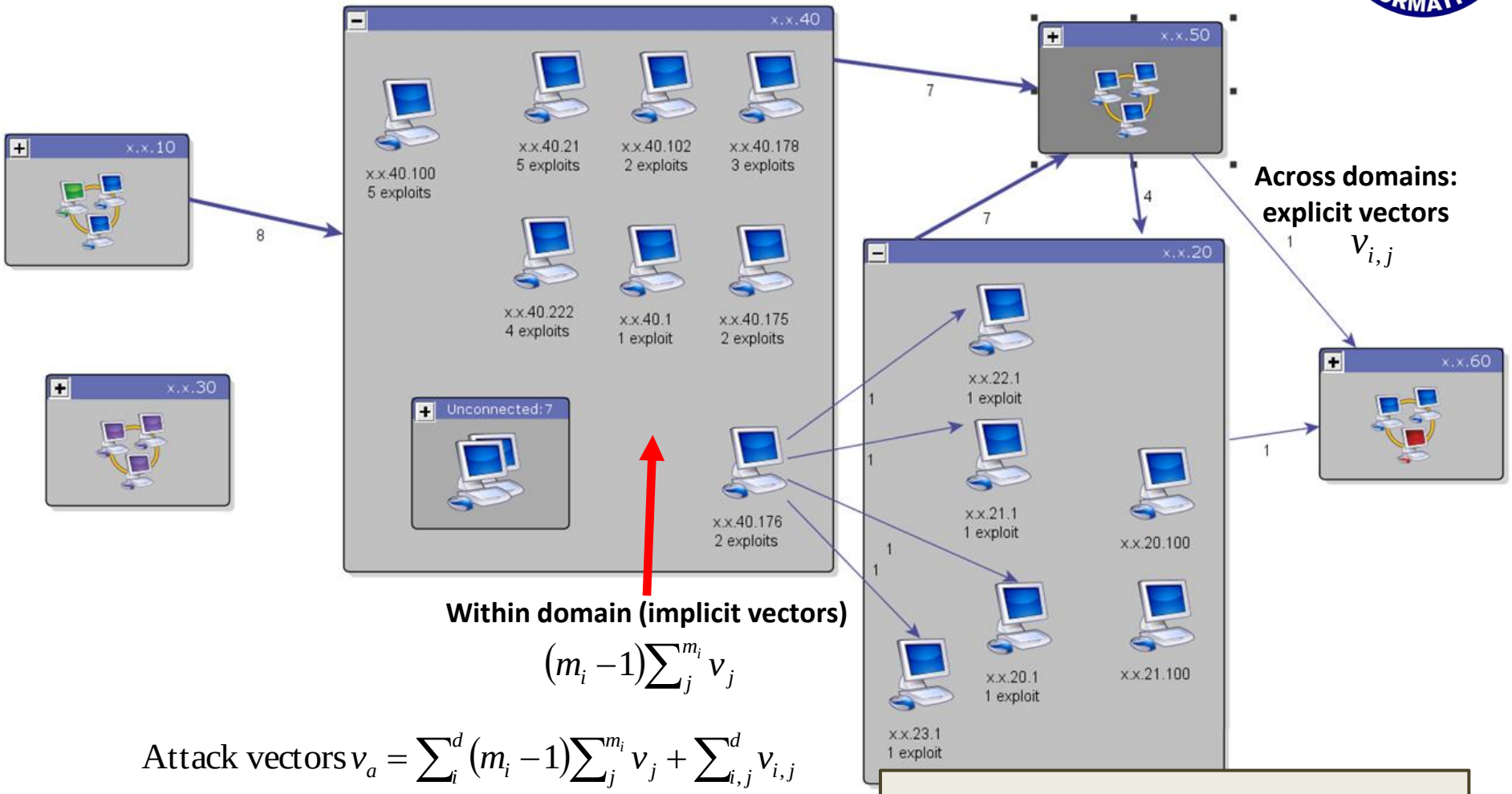
$$r = \sum_i^d r_i$$

$$\text{Machines Size} = 10\frac{r}{r+m}$$

Metrics Hierarchy



Vectors Metric



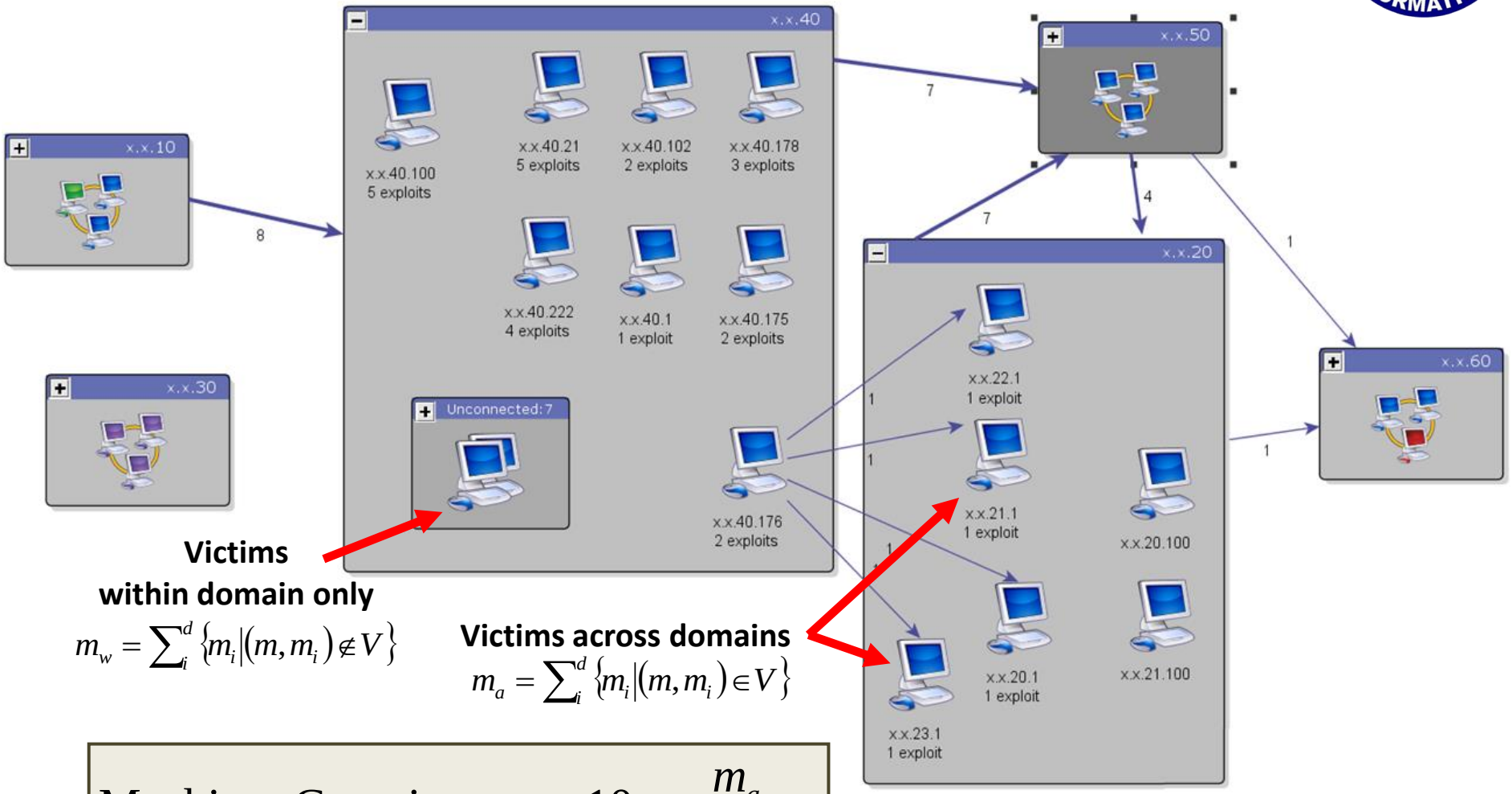
$$\text{Attack vectors } v_a = \sum_i^d (m_i - 1)\sum_j^{m_i} v_j + \sum_{i,j}^d v_{i,j}$$

$$\text{Attack vectors across domains } v_c = \sum_{i,j}^d v_{i,j}$$

$$\text{Vectors Containment} = 10 \cdot \frac{v_c}{v_a}$$

Containment Family

Machines Metric



Victims within domain only

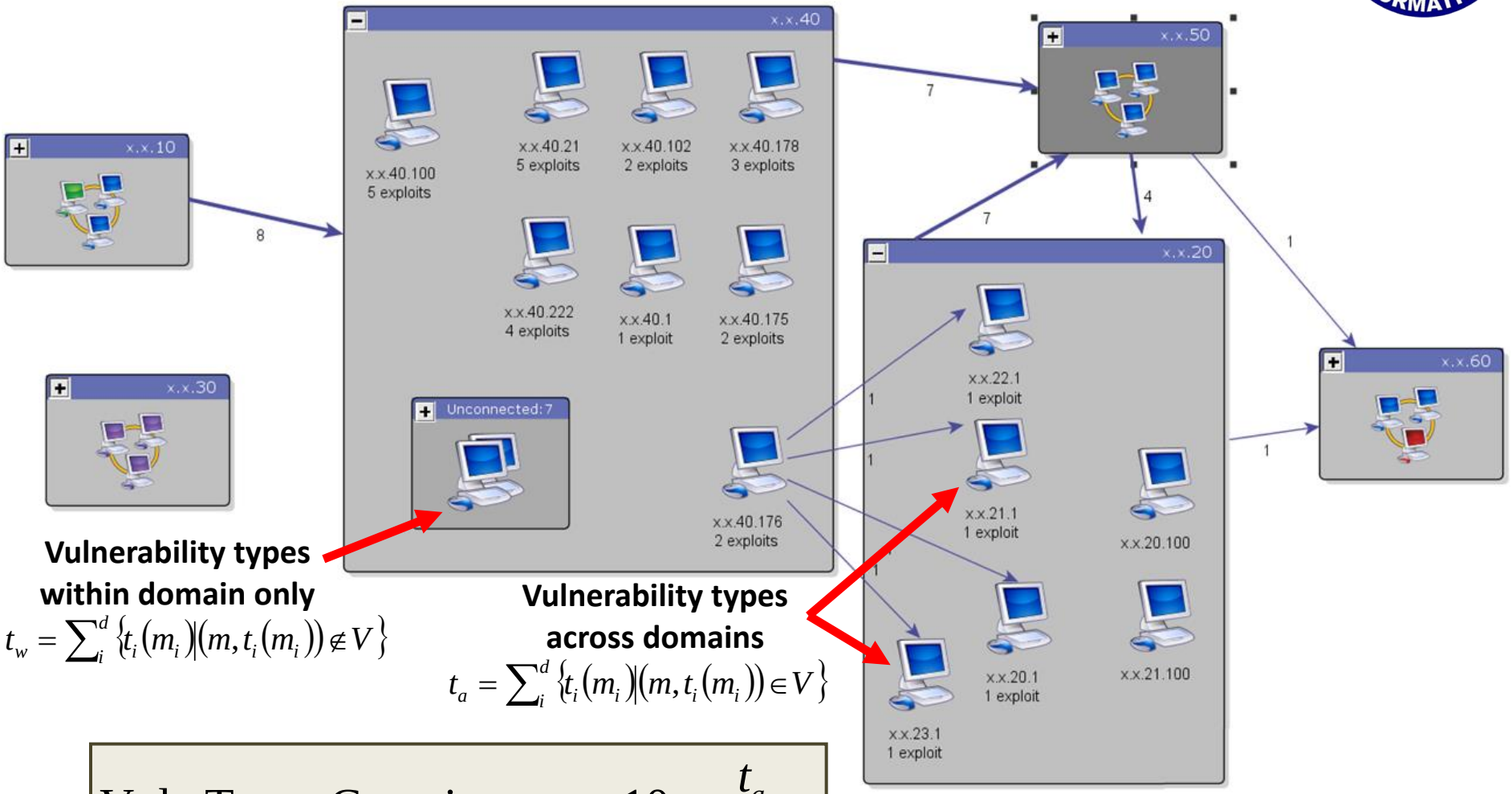
$$m_w = \sum_i^d \{m_i | (m, m_i) \notin V\}$$

Victims across domains

$$m_a = \sum_i^d \{m_i | (m, m_i) \in V\}$$

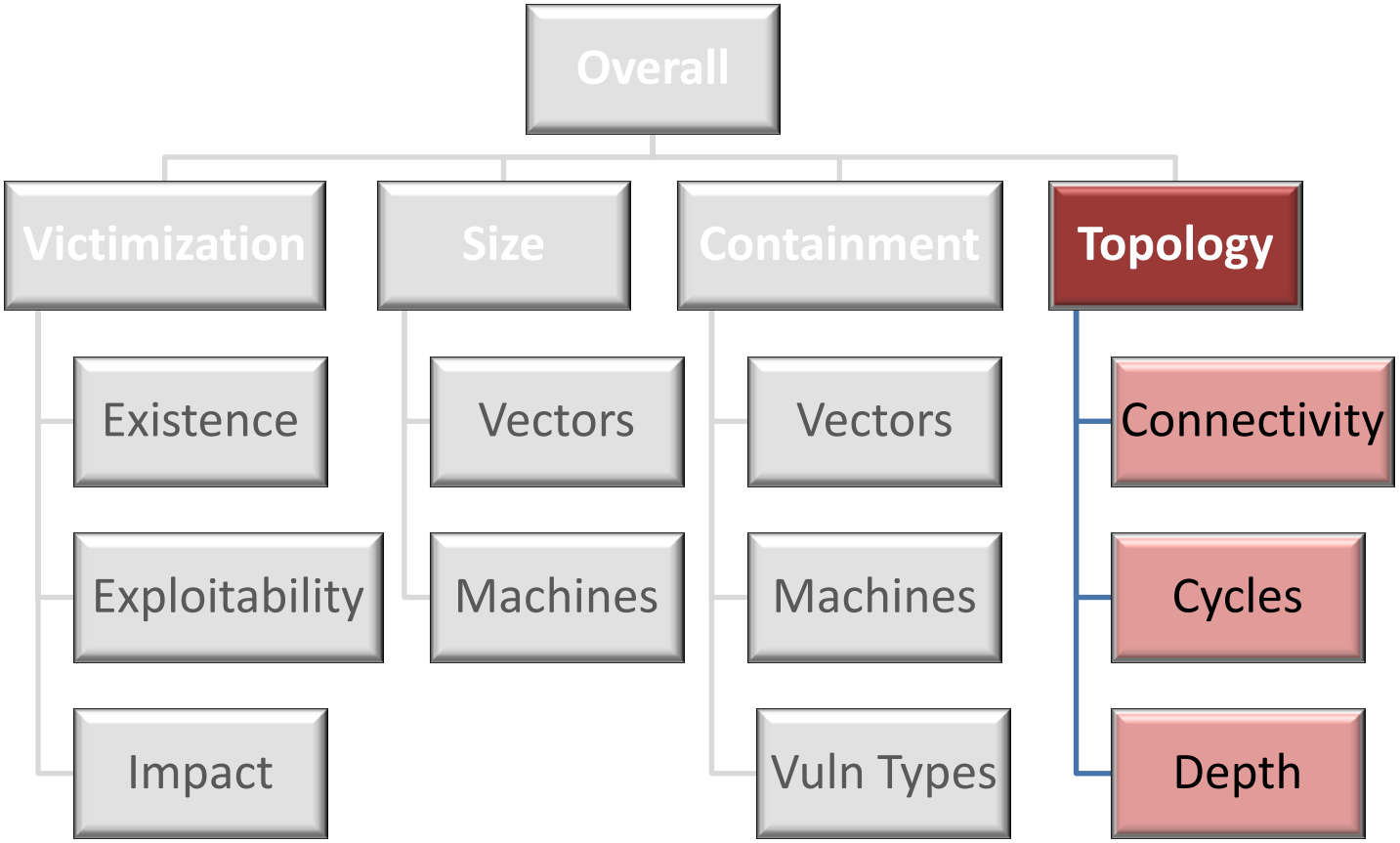
$$\text{Machines Containment} = 10 \cdot \frac{m_a}{m_a + m_w}$$

Vulnerability Types Metric



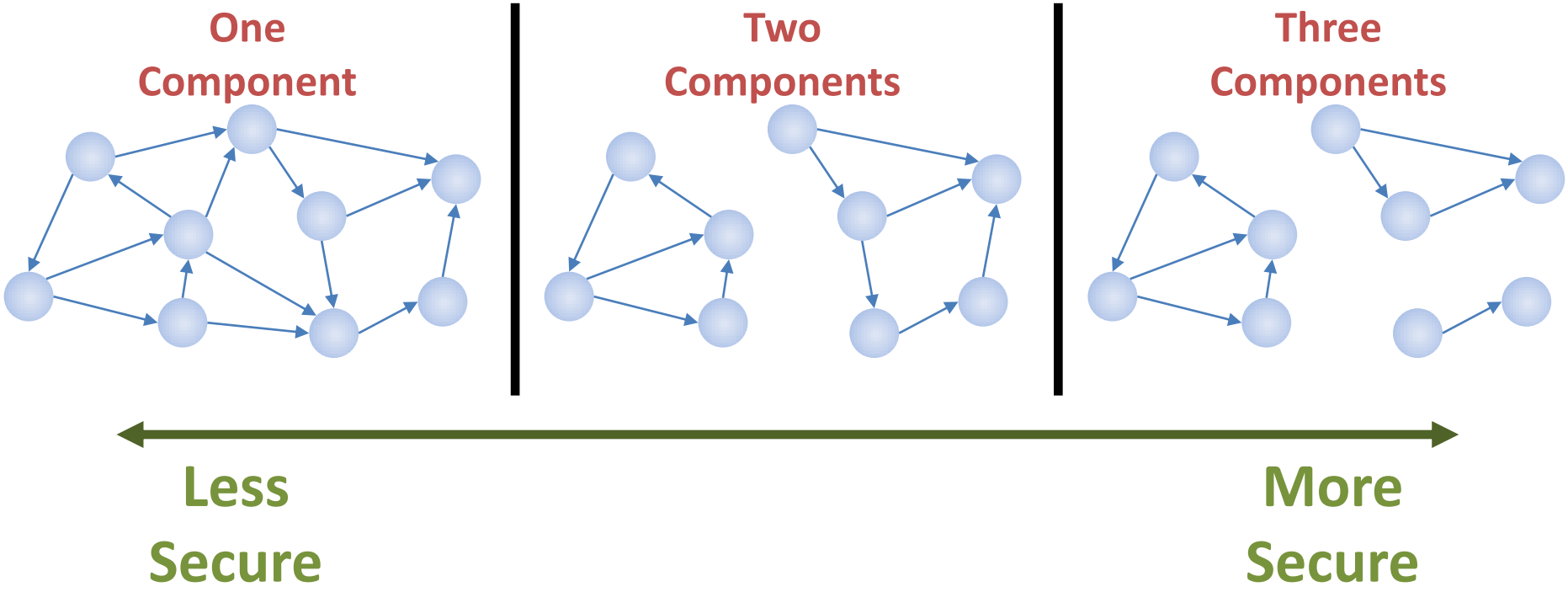
$$\text{Vuln Types Containment} = 10 \cdot \frac{t_a}{t_a + t_w}$$

Metrics Hierarchy



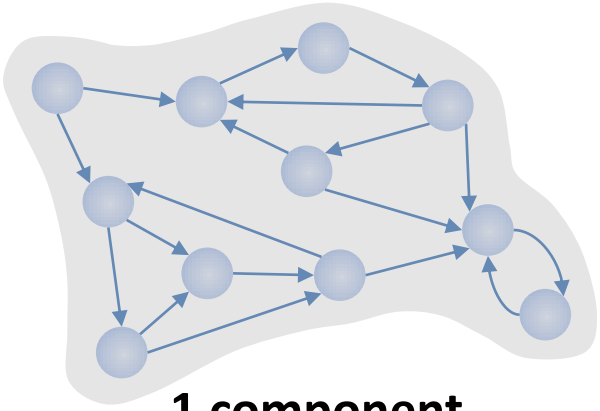
Attack Graph Connectivity

Motivation: Better to have attack graph as disconnected parts versus connected whole



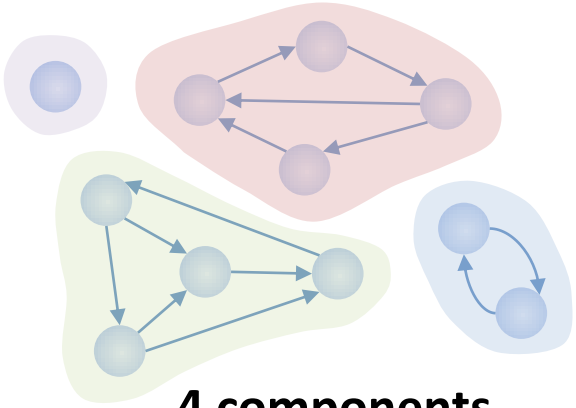
Topology Family

Connectivity Metric



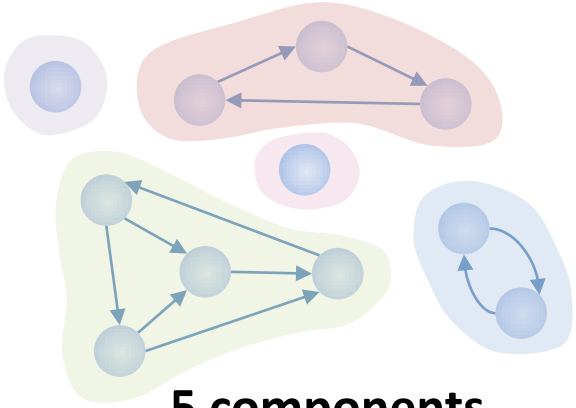
1 component

$$\text{Metric} = 10\left(1 - \frac{1-1}{11-1}\right) = 10$$



4 components

$$\text{Metric} = 10\left(1 - \frac{4-1}{11-1}\right) = 7$$

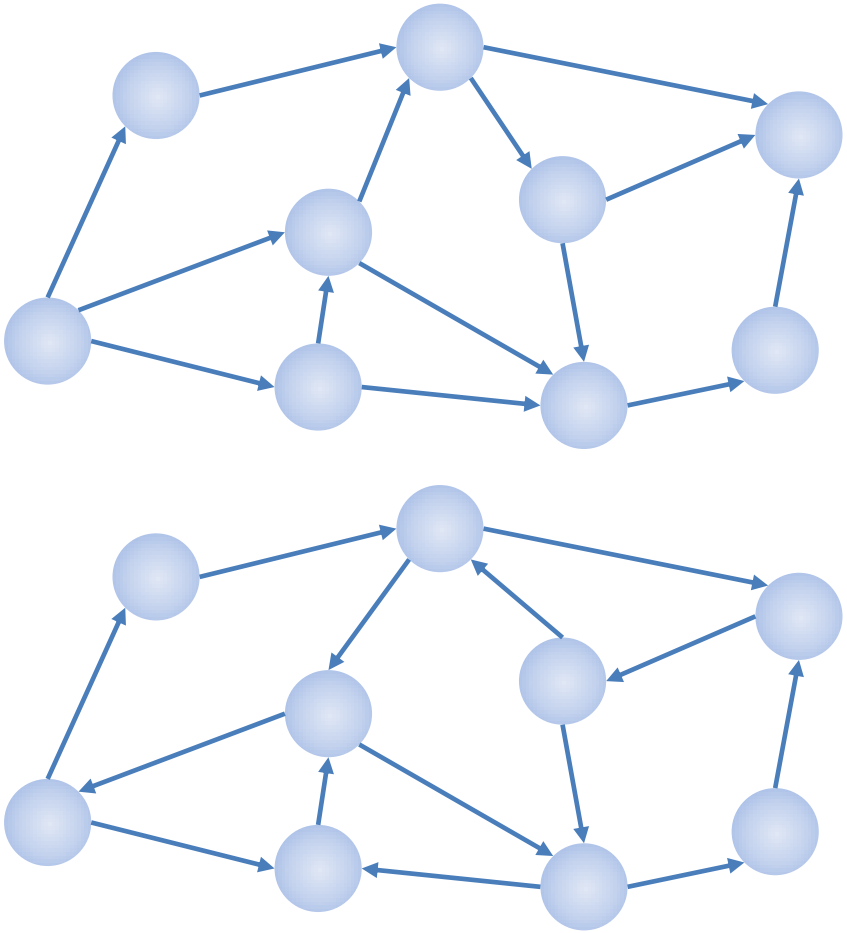


5 components

$$\text{Metric} = 10\left(1 - \frac{5-1}{11-1}\right) = 6$$

Attack Graph Cycles

Motivation: For a connected attack graph, better to avoid cycles among subgraphs

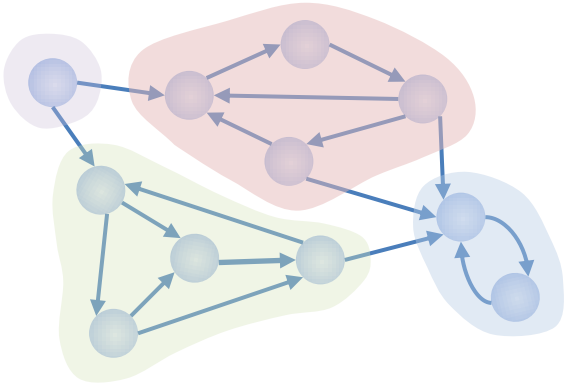


More Secure

Less Secure

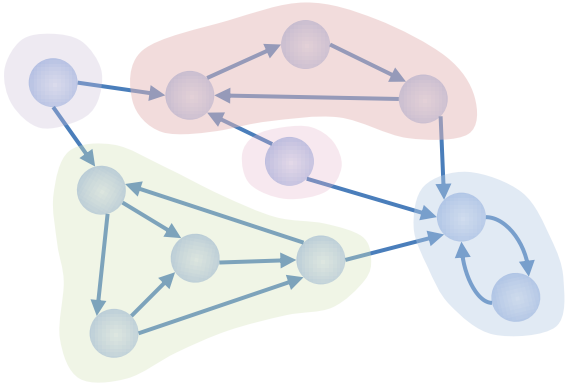
Topology Family

Cycles Metric



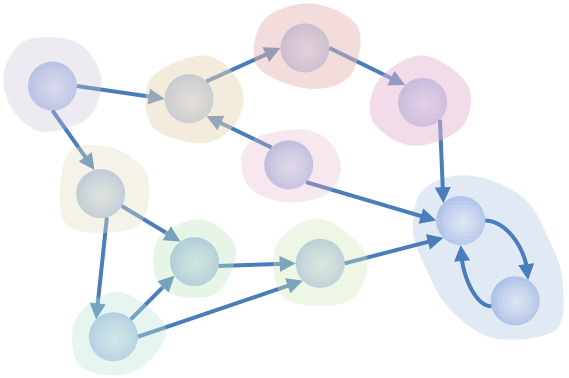
4 components

$$\text{Metric} = 10\left(1 - \frac{4-1}{11-1}\right) = 7$$



5 components

$$\text{Metric} = 10\left(1 - \frac{5-1}{11-1}\right) = 6$$

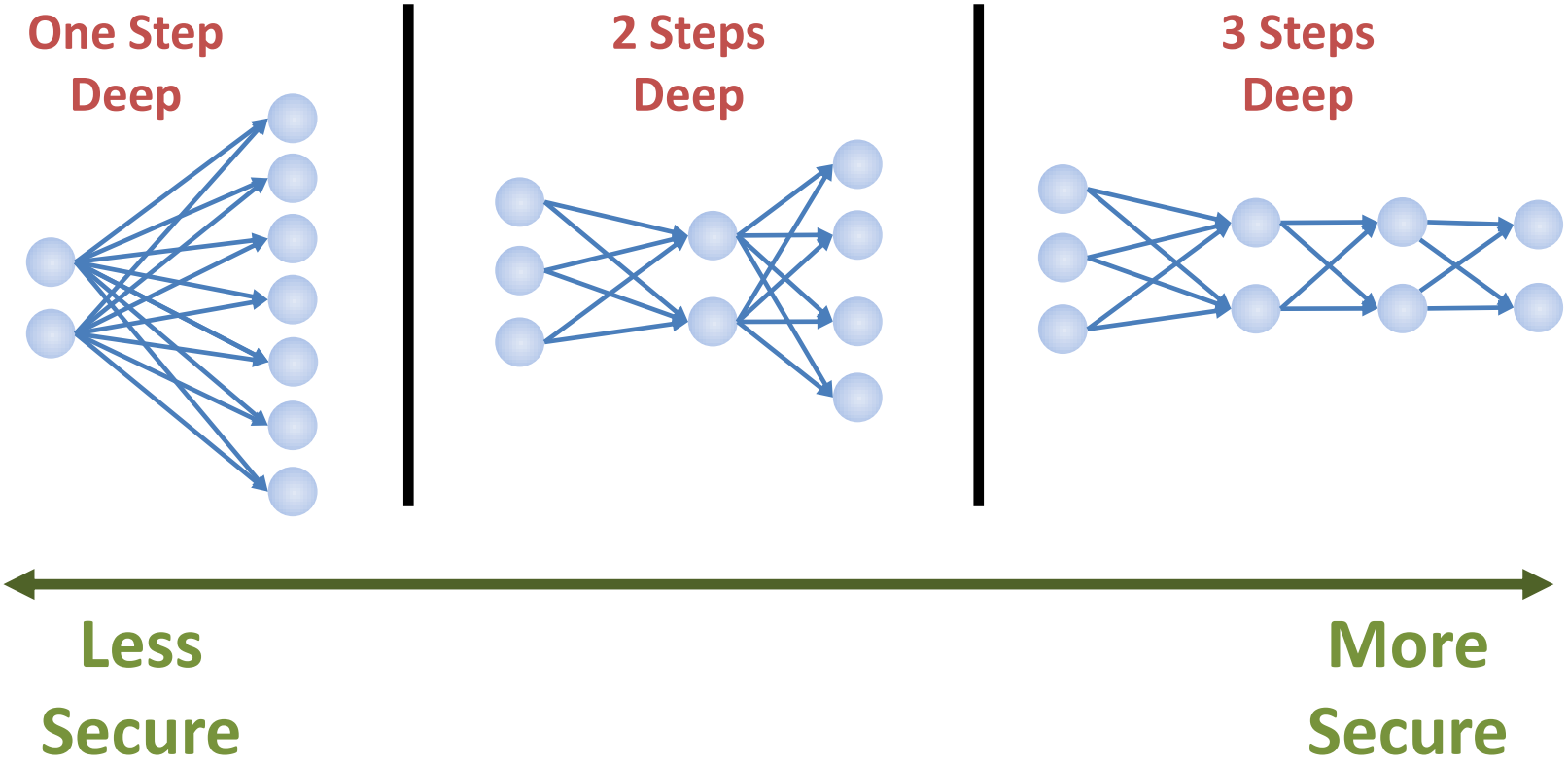


10 components

$$\text{Metric} = 10\left(1 - \frac{10-1}{11-1}\right) = 1$$

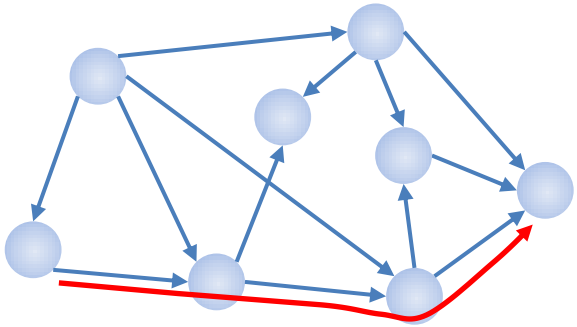
Attack Graph Depth

Motivation: Better to have attack graph deeper versus shallower



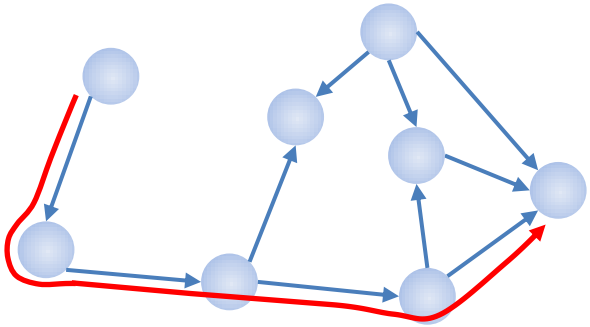
Topology Family

Depth Metric



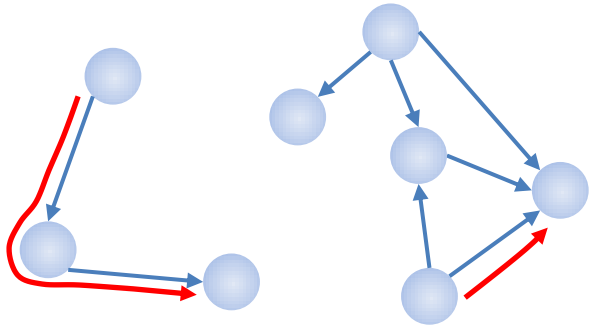
Shortest path 3/8

$$\text{Metric} = 10\left(1 - \frac{3}{8-1}\right) = 5.7$$



Shortest path 4/8

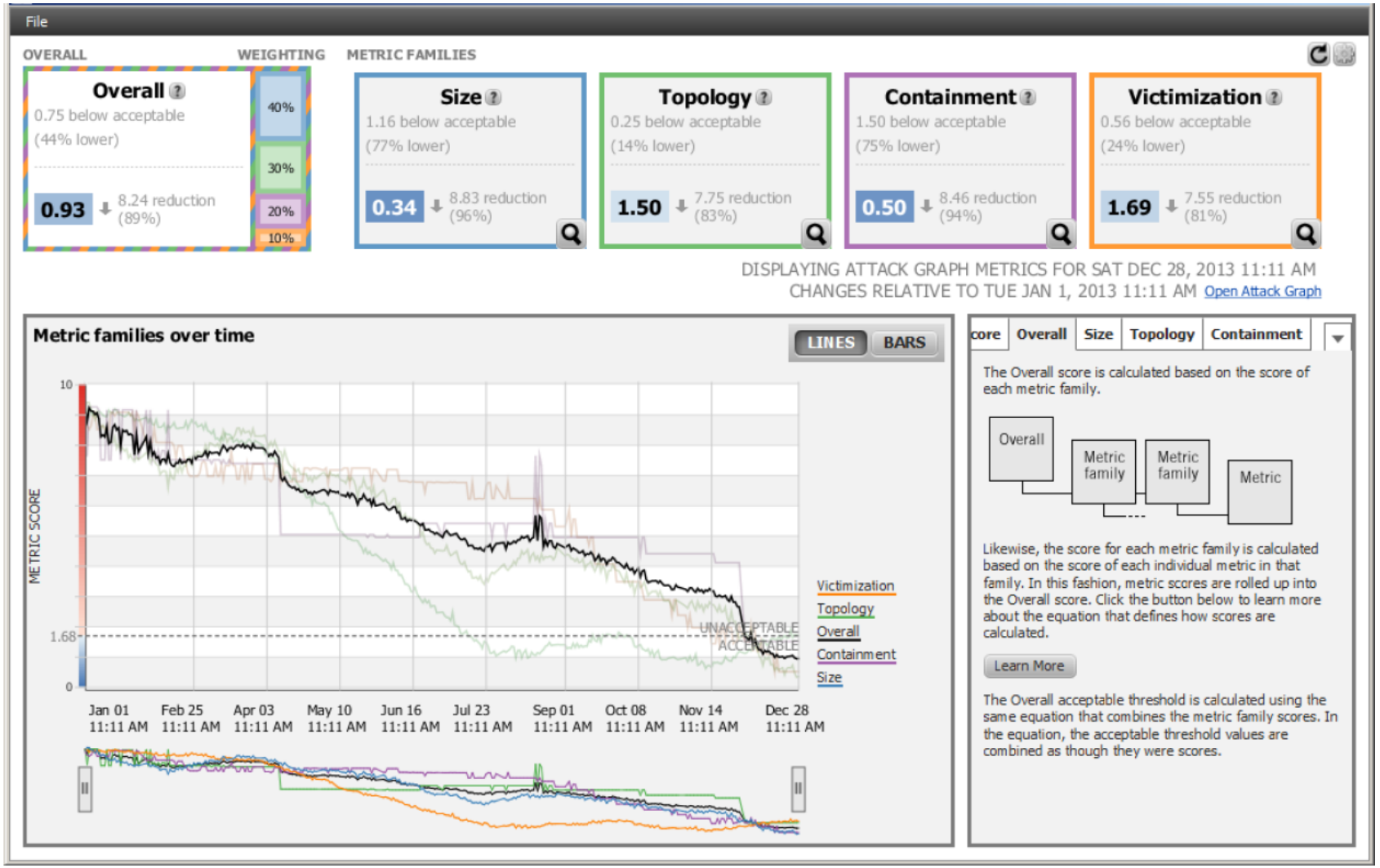
$$\text{Metric} = 10\left(1 - \frac{4}{8-1}\right) = 4.3$$



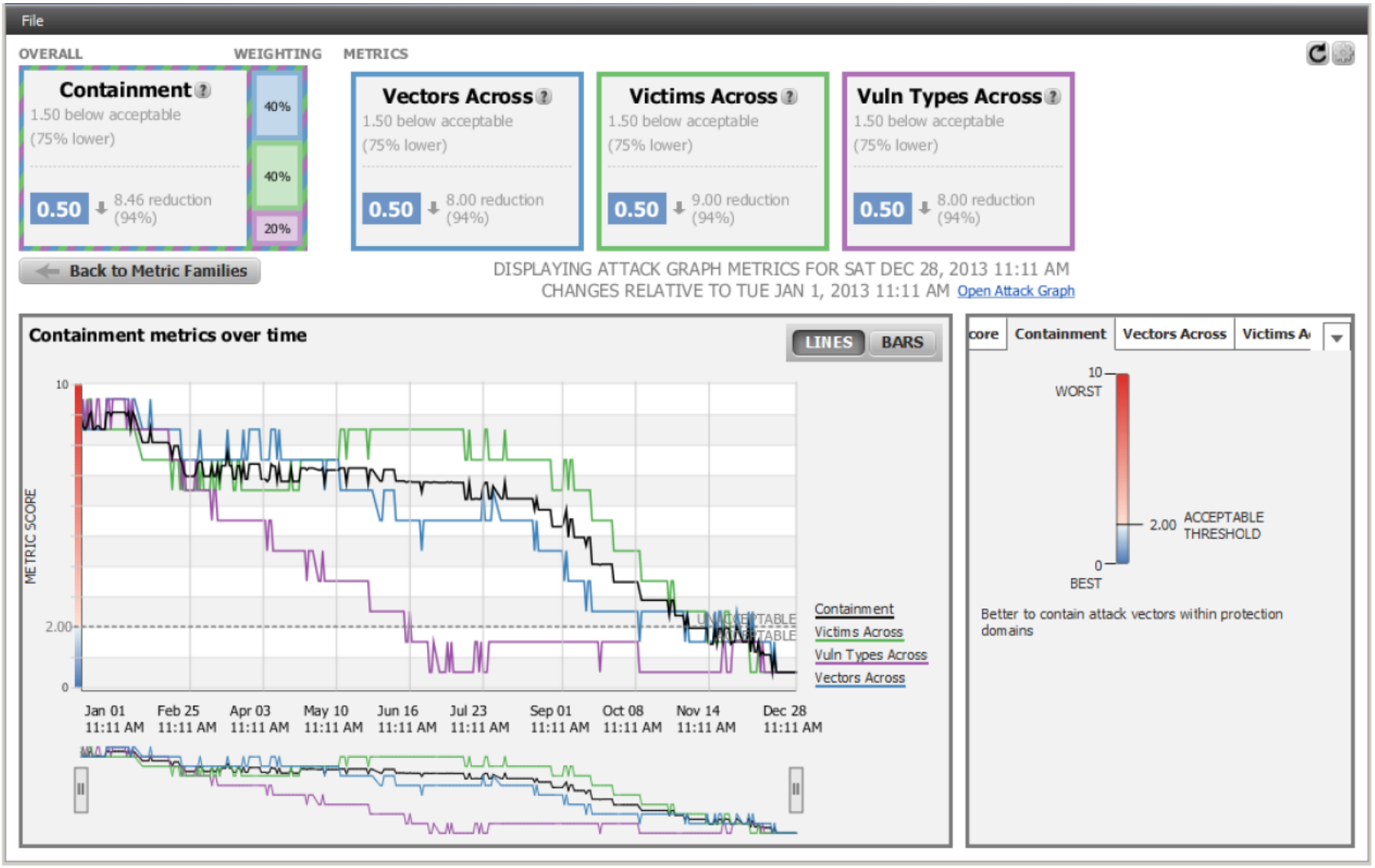
Shortests paths 2/3 and 1/5

$$\text{Metric} = \frac{10}{2 \cdot 8}\left[3 \cdot \left(1 - \frac{2}{3-1}\right) + 5 \cdot \left(1 - \frac{1}{5-1}\right)\right] = 2.3$$

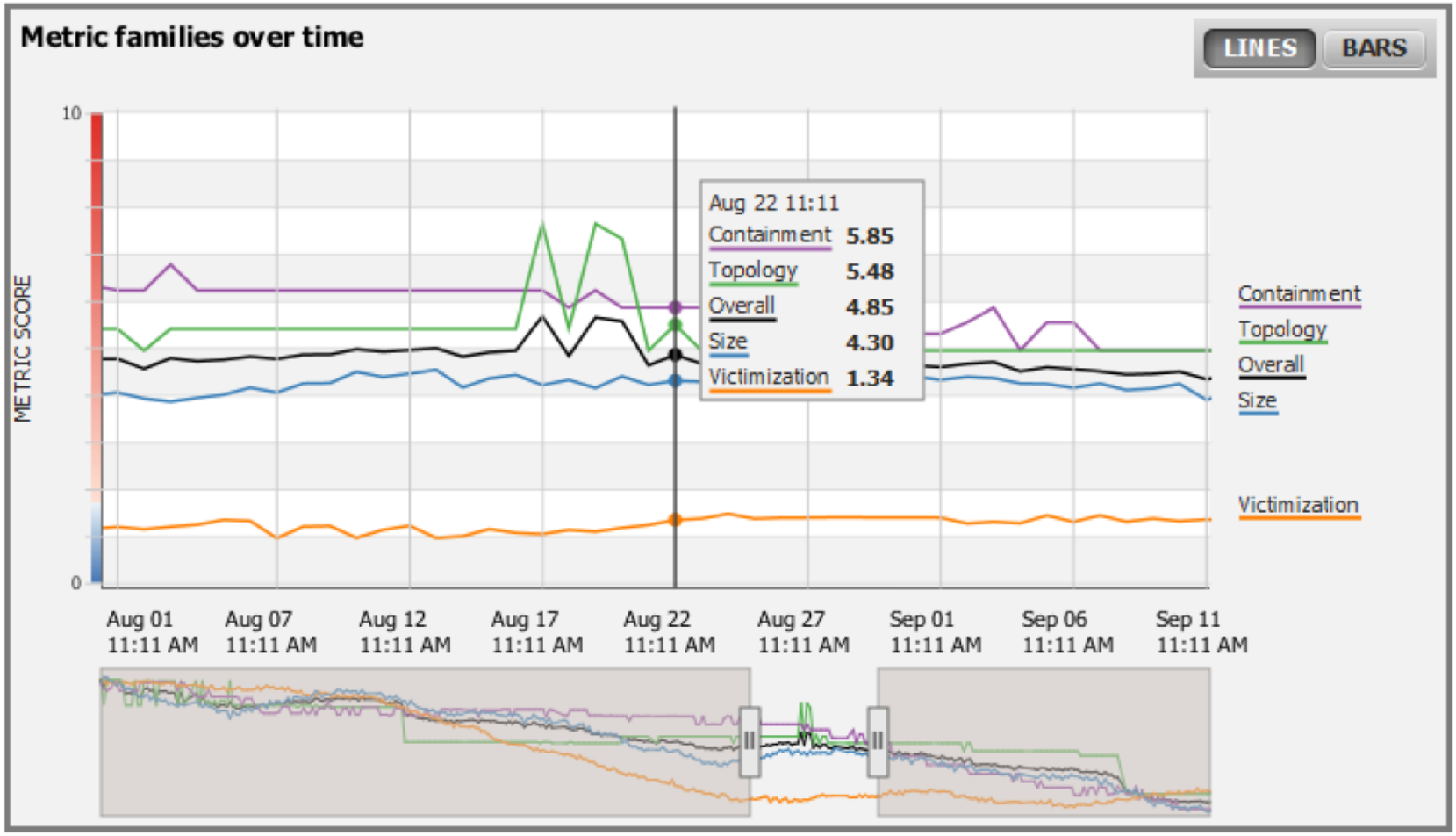
Metrics Dashboard



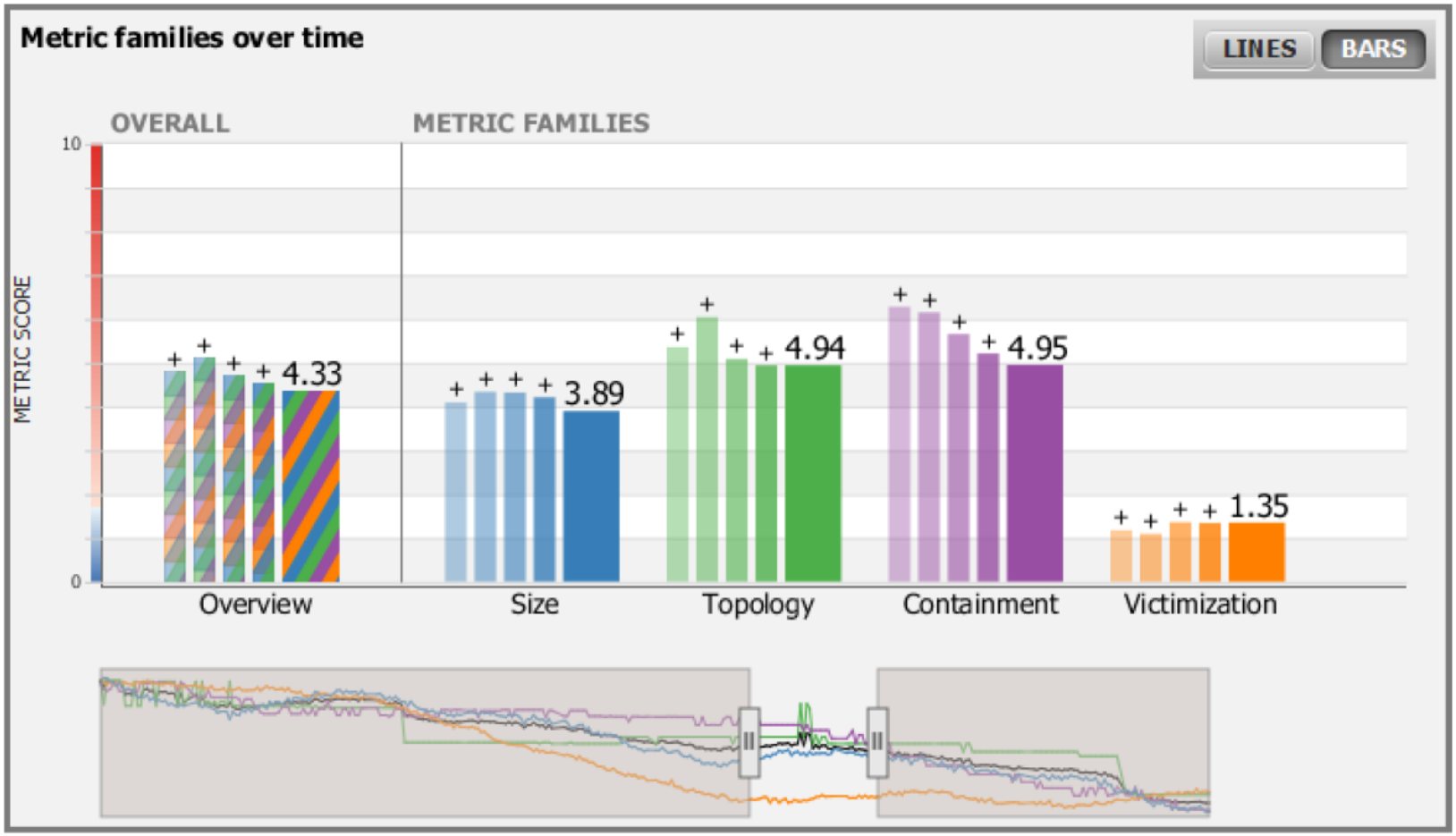
Family-Level Metrics



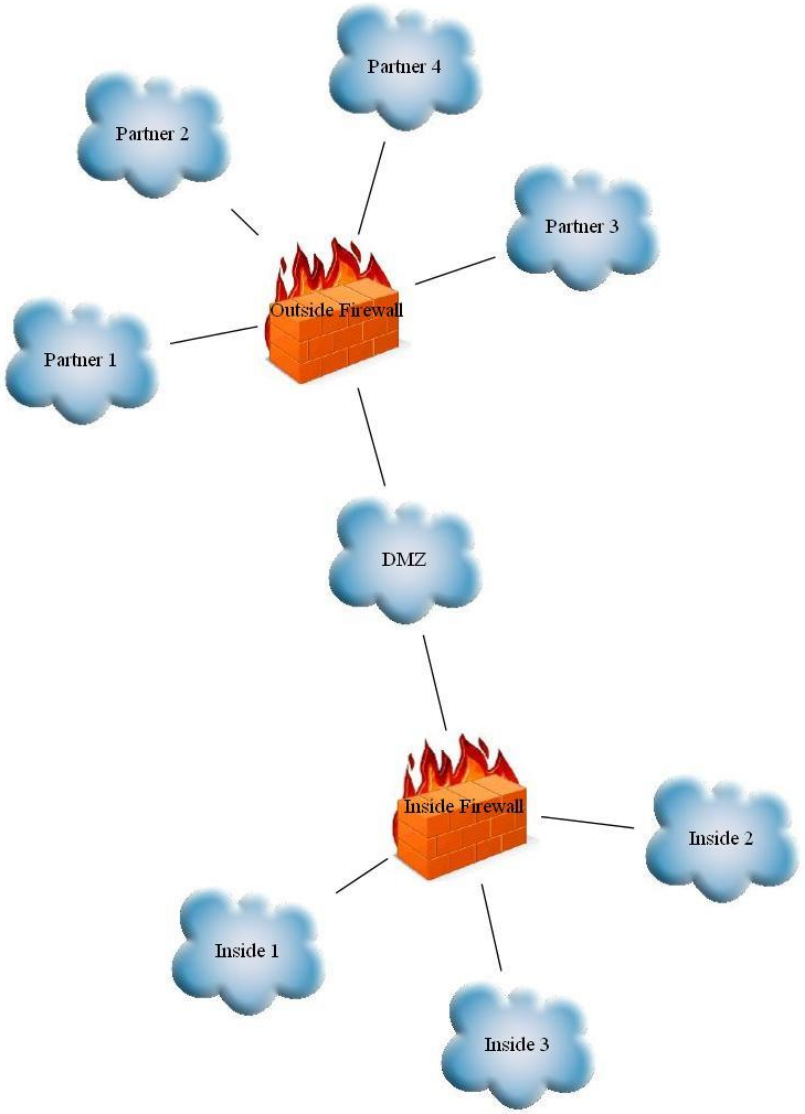
Temporal Zoom



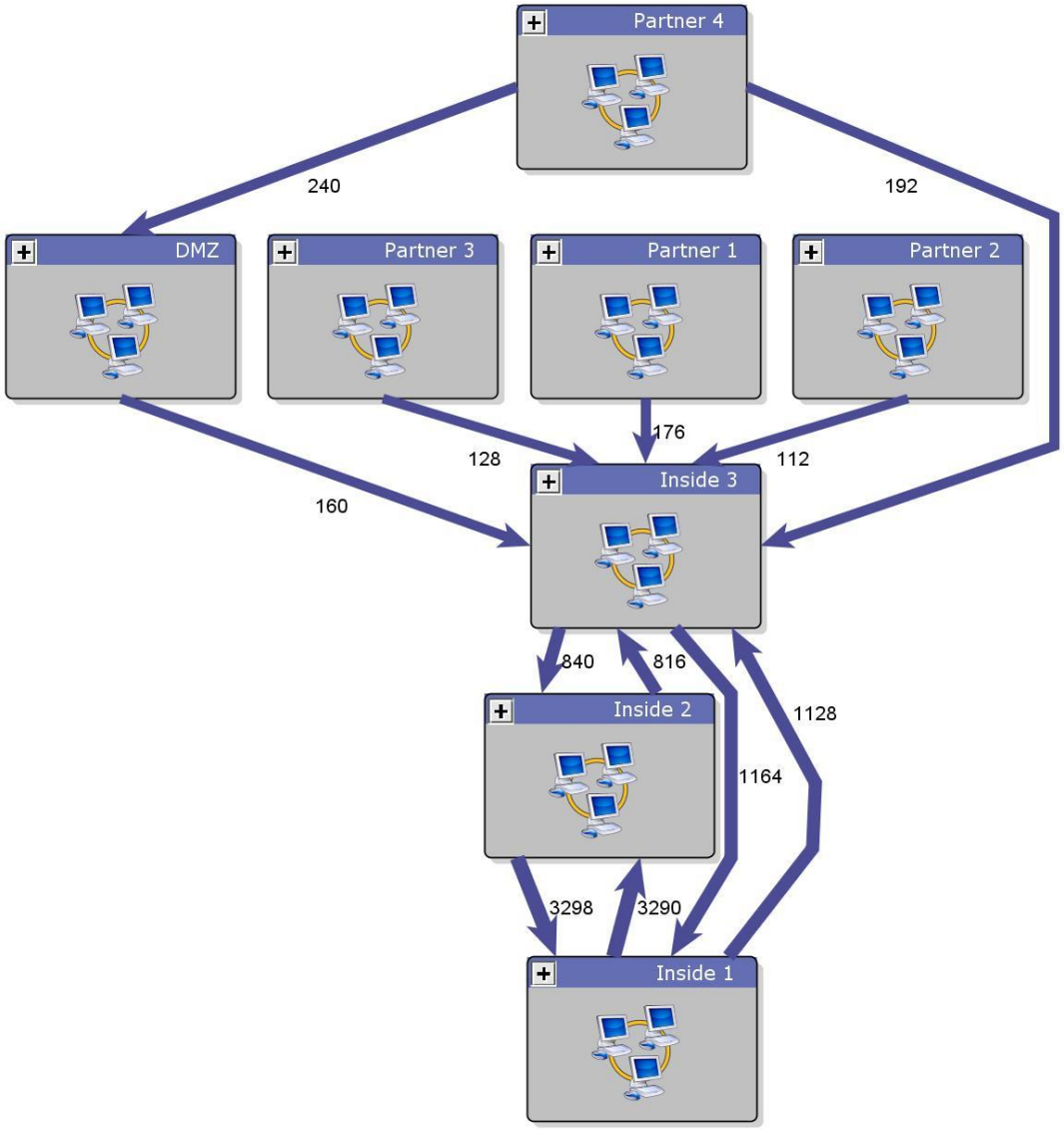
Trend Summary



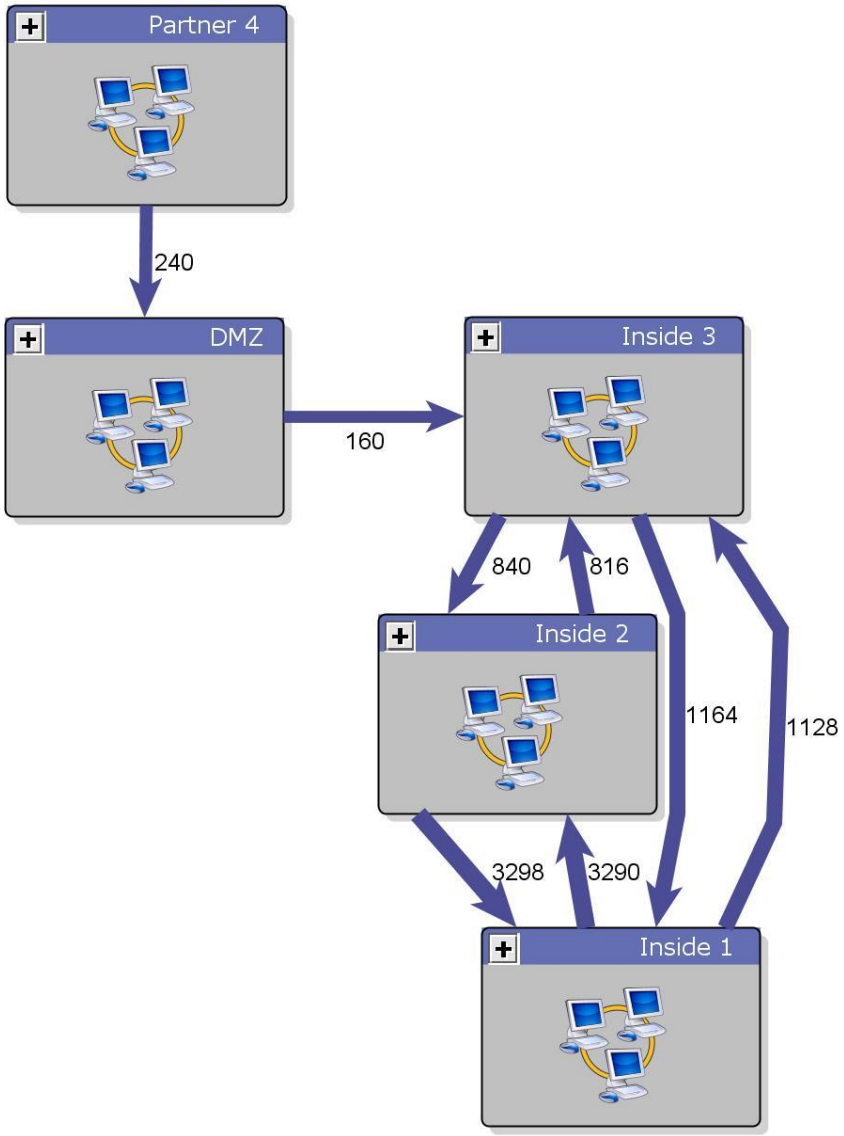
Example Network Topology



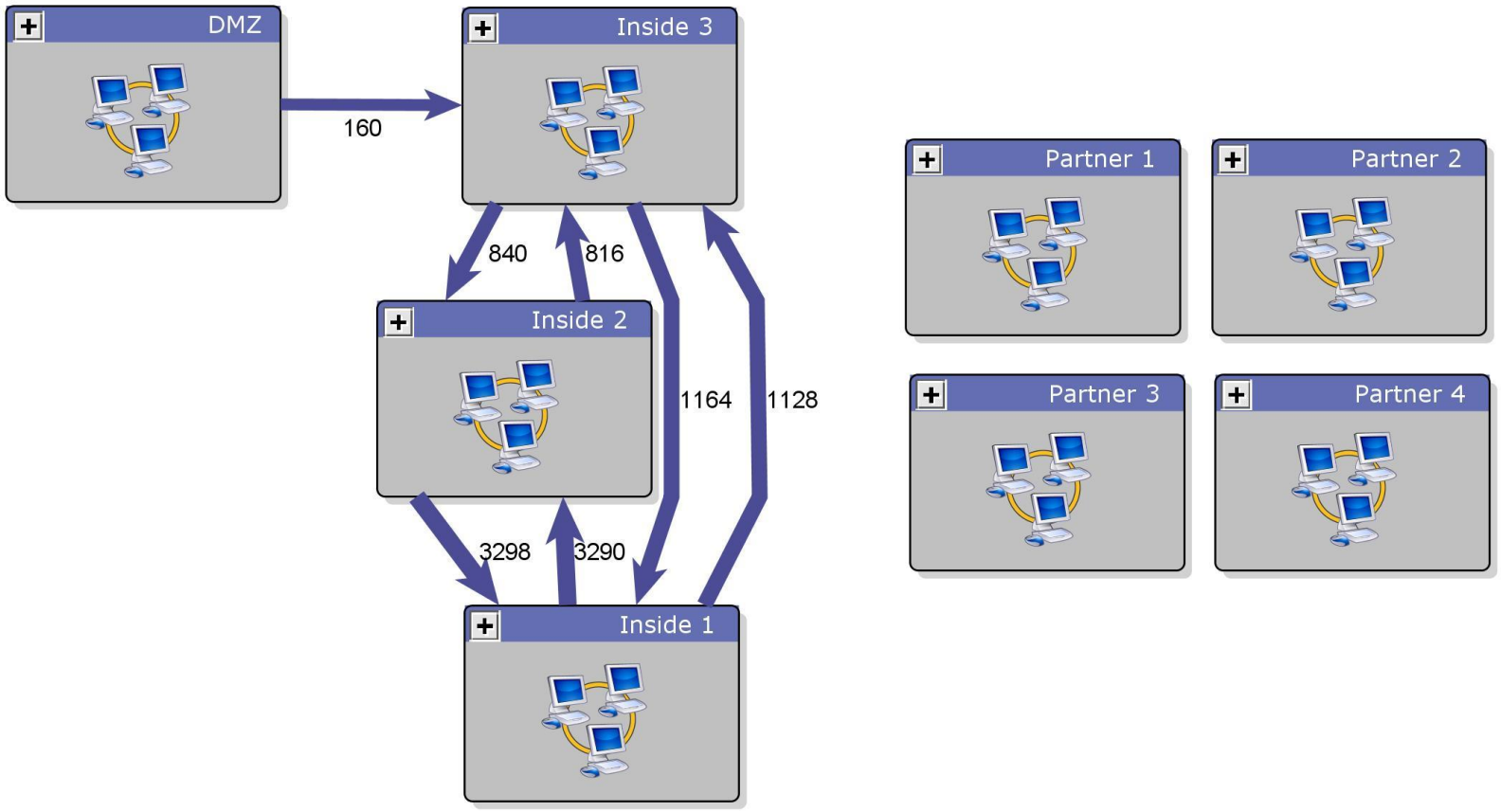
Attack Graph – No Hardening



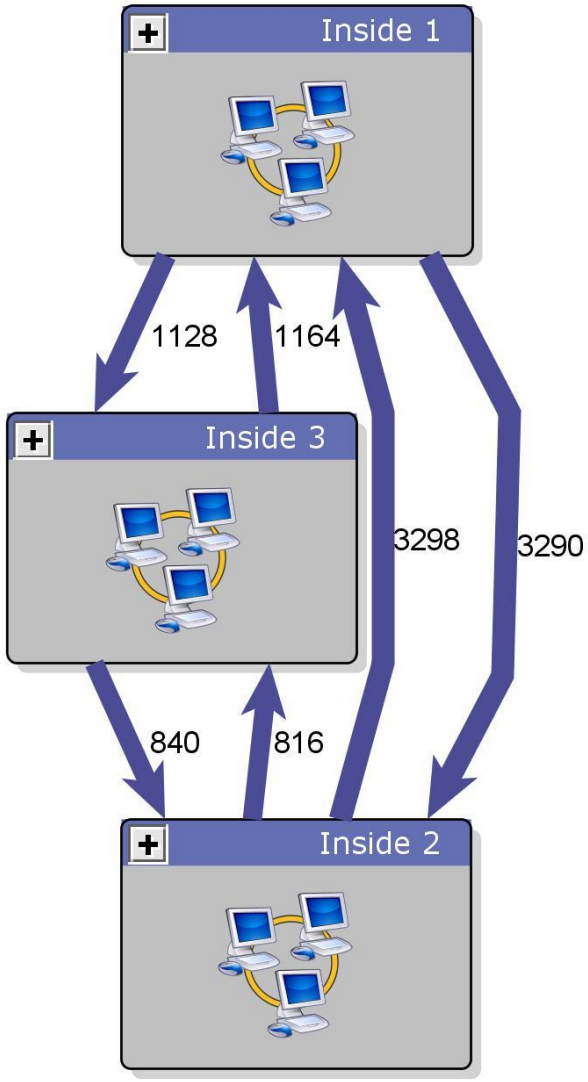
Block Partners to Inside

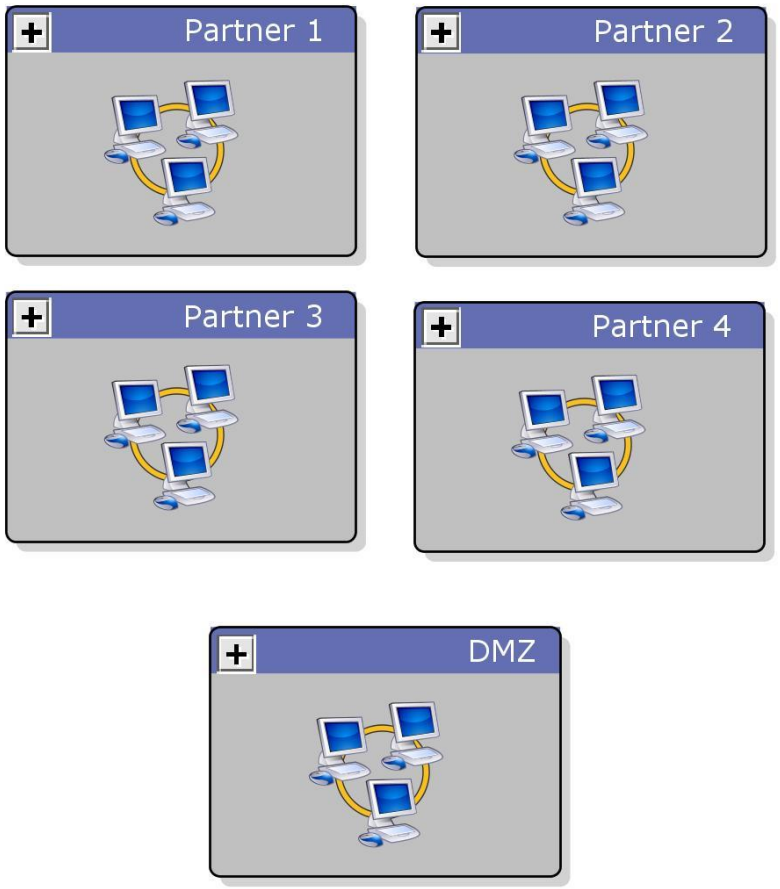


Block Partner 4 to DMZ

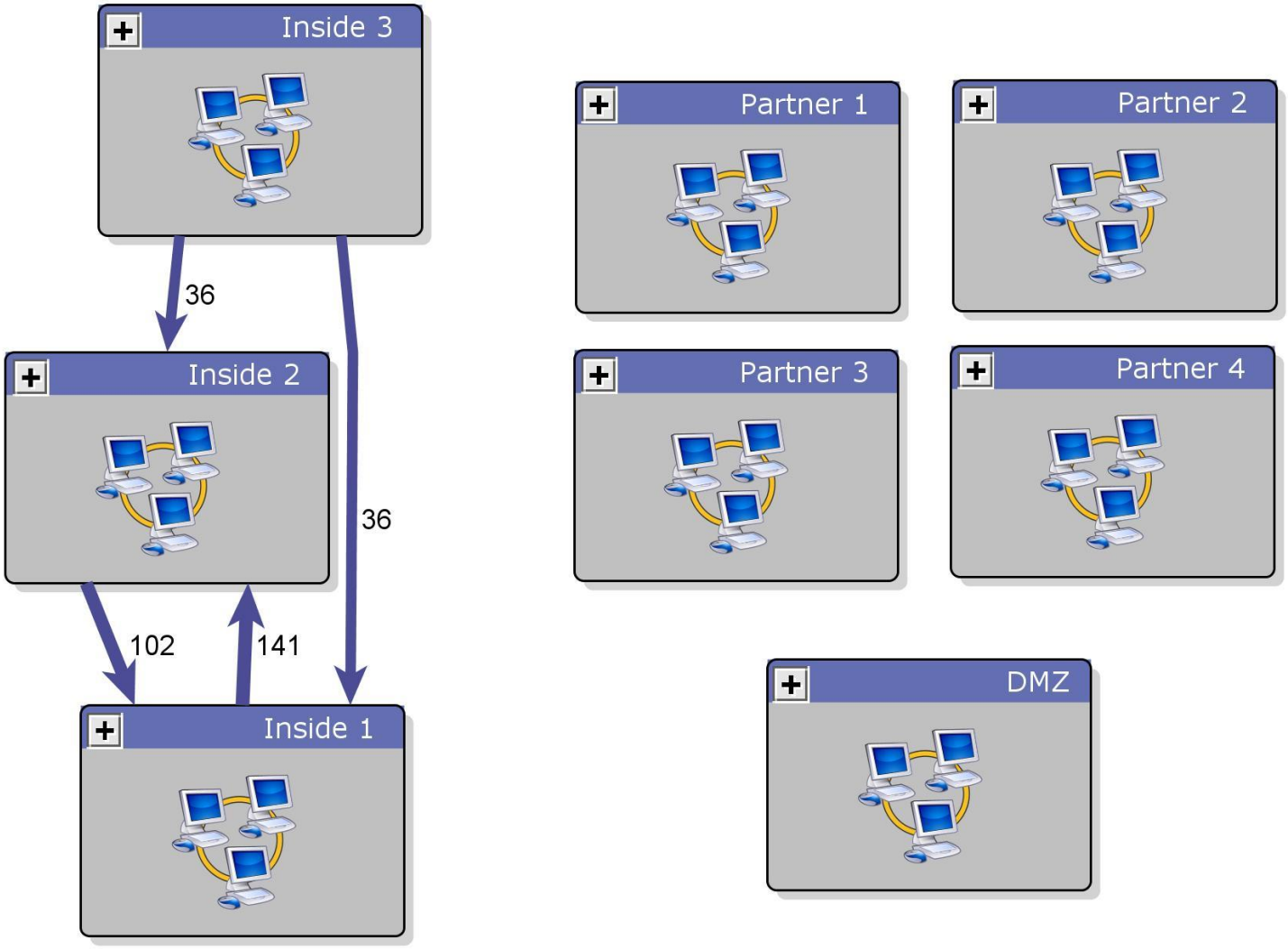


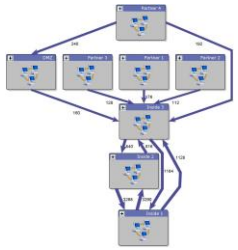
Block DMZ to Inside 3

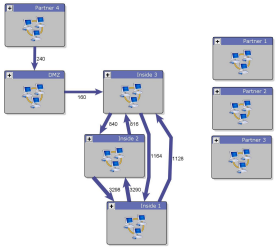


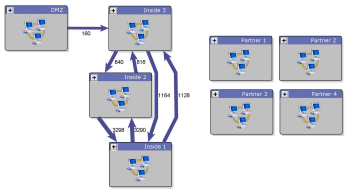


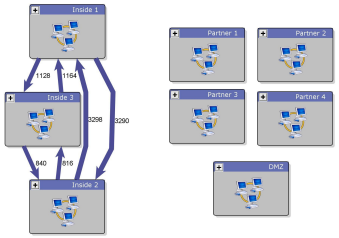
Patch Host Vulnerabilities

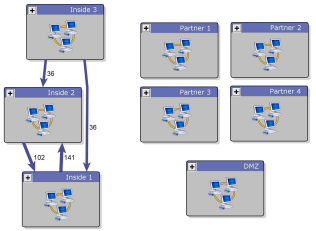












OVERALL WEIGHTING METRIC FAMILIES

Overall ?

2.73 6.27 (69%)

.23 until acceptable (9% reduction)

40.00% 25.00% 25.00% 10.00%

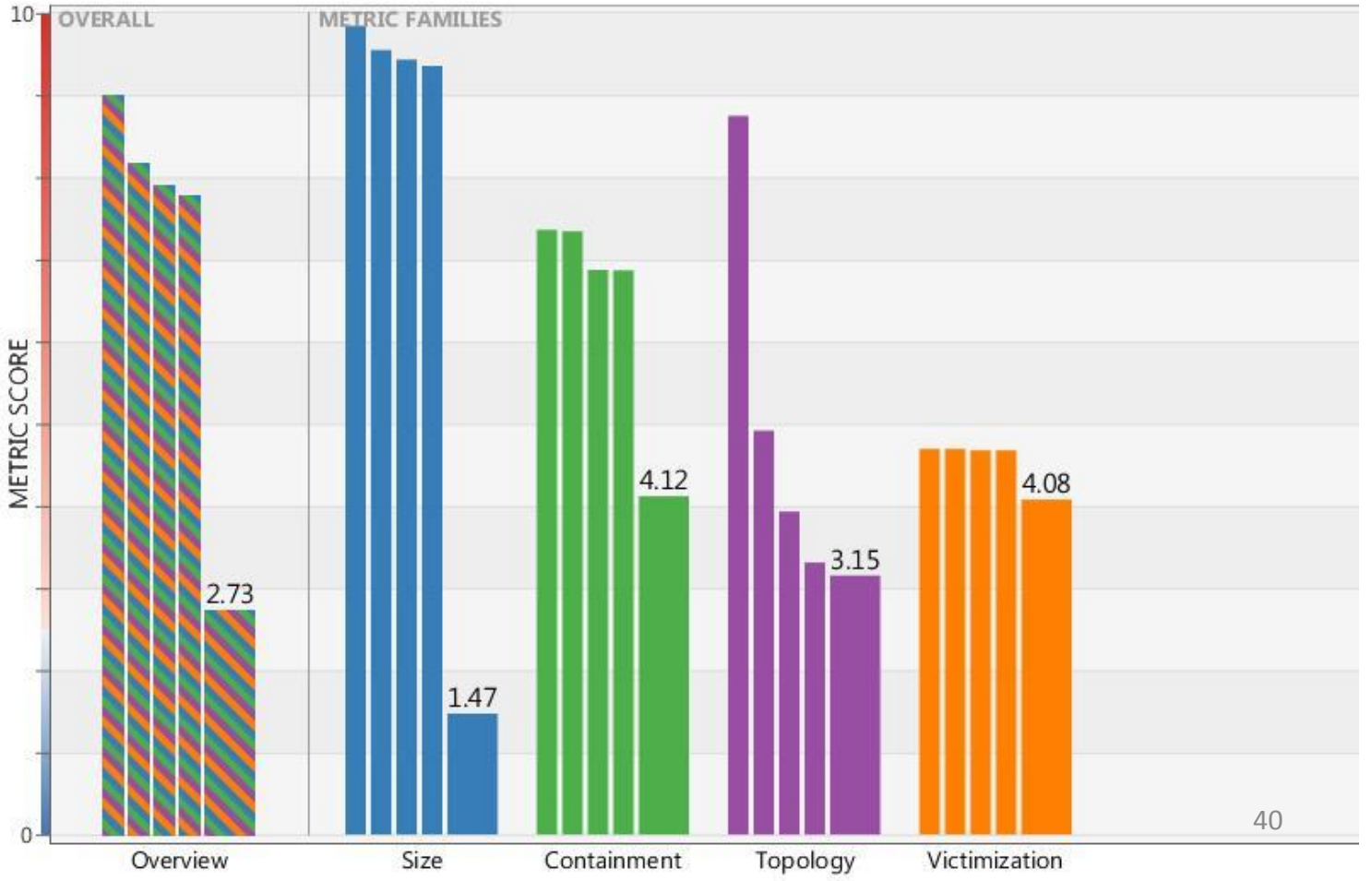
Size ?
1.03 below acceptable (41% lower)
1.47 8.37 (85%)

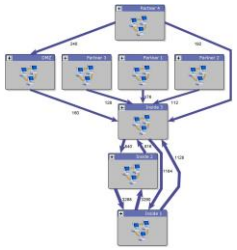
Containment ?
4.12 3.24 (44%)
1.62 until acceptable (64% reduction)

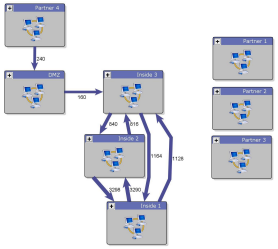
Topology ?
3.15 5.59 (63%)
.65 until acceptable (26% reduction)

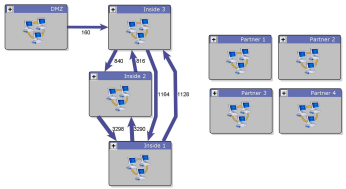
Victimization ?
4.08 .62 (13%)
1.58 until acceptable (63% reduction)

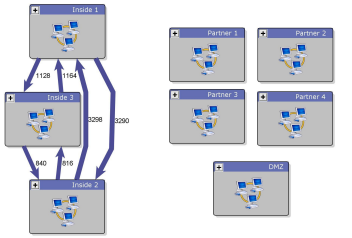
Metric families over time

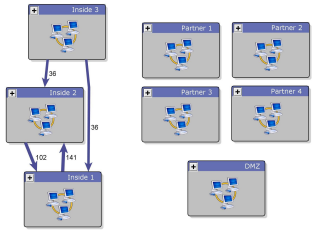












OVERALL WEIGHTING METRICS

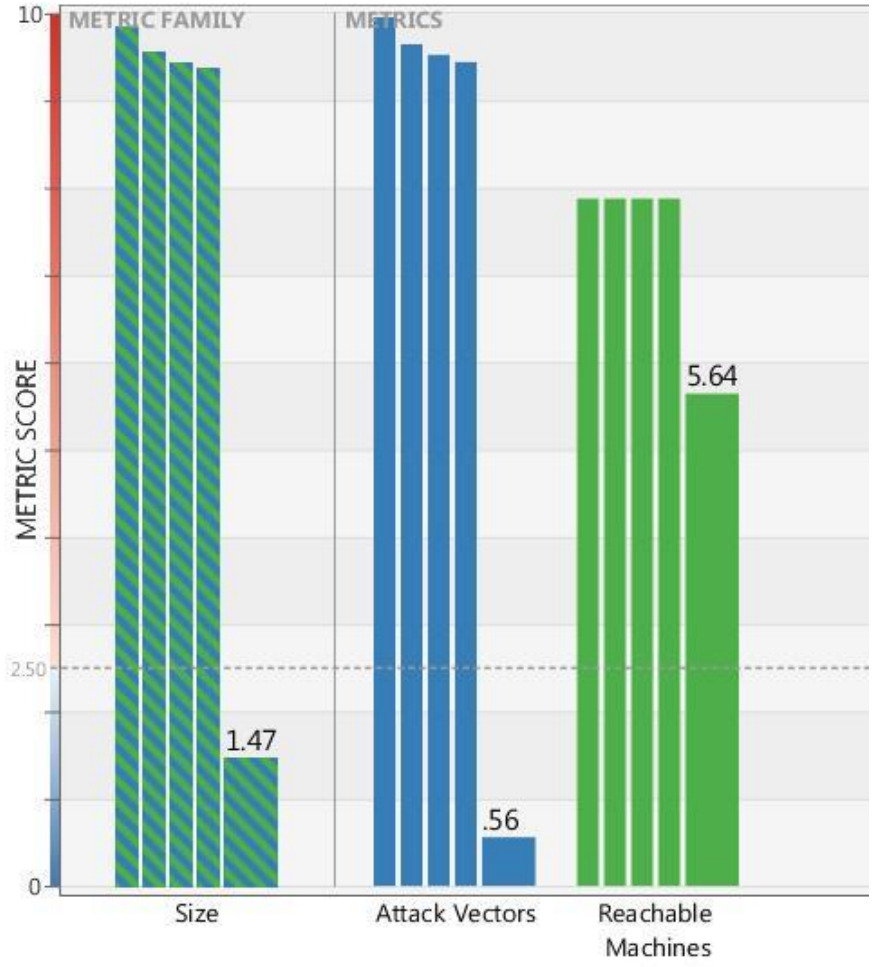
Size ?
1.03 below acceptable
(41% increase)
1.47 ↓ 8.37 (85%)
80.00%
20.00%

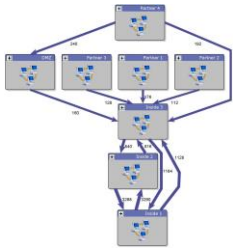
Attack Vectors ?
1.94 below acceptable
(77% lower)
.56 ↓ 9.40 (94%)

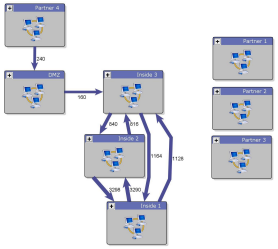
Reachable Machines ?
5.64 ↓ 2.23 (28%)
3.14 until acceptable
(125% reduction)

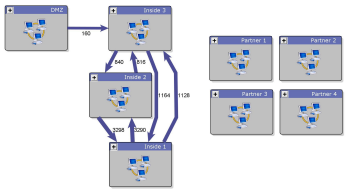
← Back to Metric Families

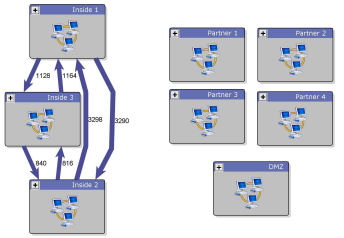
Size metrics over time

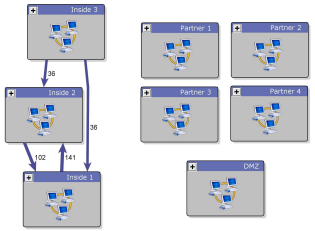












OVERALL WEIGHTING METRICS

Containment 50.00%

4.12 ↓ 3.24 (44%)

1.62 until acceptable (64% reduction)

25.00%

25.00%

Victims Across

2.10 below acceptable (84% lower)

.40 ↓ 6.91 (94%)

Vectors Across

5.62 ↓ .29 (4%)

3.12 until acceptable (125% reduction)

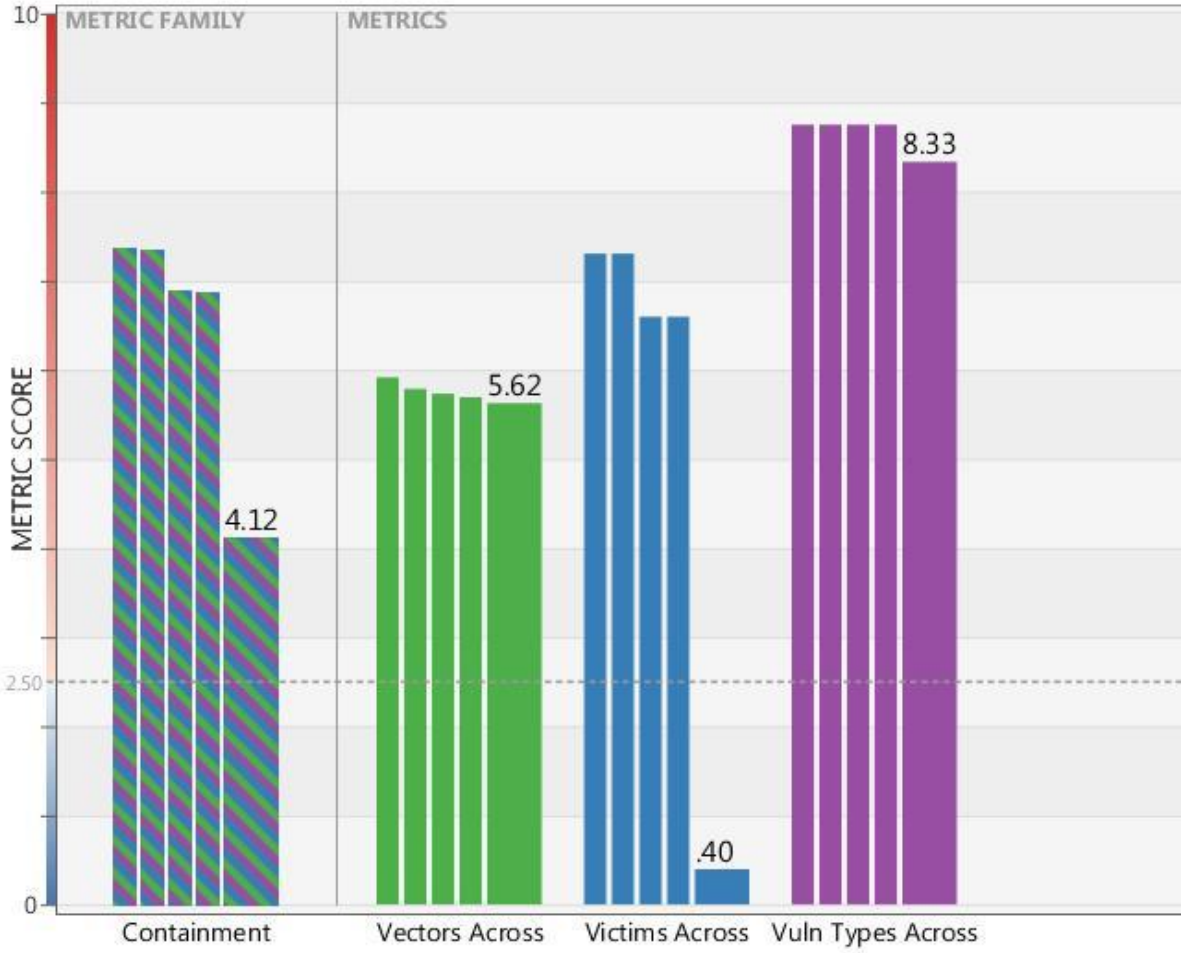
Vuln Types Across

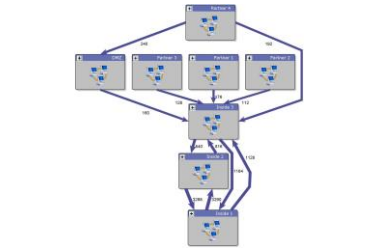
8.33 ↓ .42 (4%)

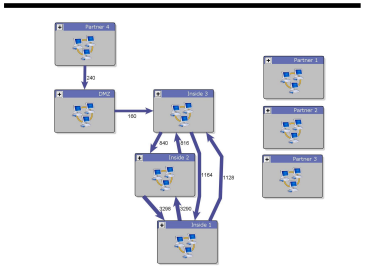
5.83 until acceptable (233% reduction)

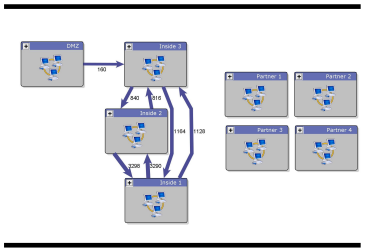
Back to Metric Families

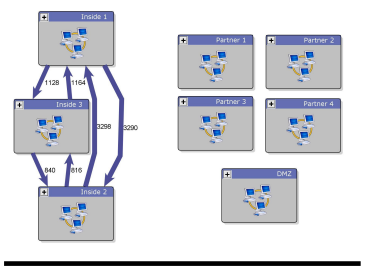
Containment metrics over time

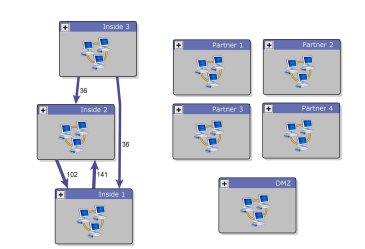












OVERALL WEIGHTING METRICS

Topology 50.00%

3.15 ↓ 5.59 (63%)

.65 until acceptable (26% reduction)

Connectivity 25.00%

2.86 ↓ 7.14 (71%)

.36 until acceptable (14% reduction)

Cycles 25.00%

1.07 below acceptable (42% lower)

1.43 ↓ 1.43 (50%)

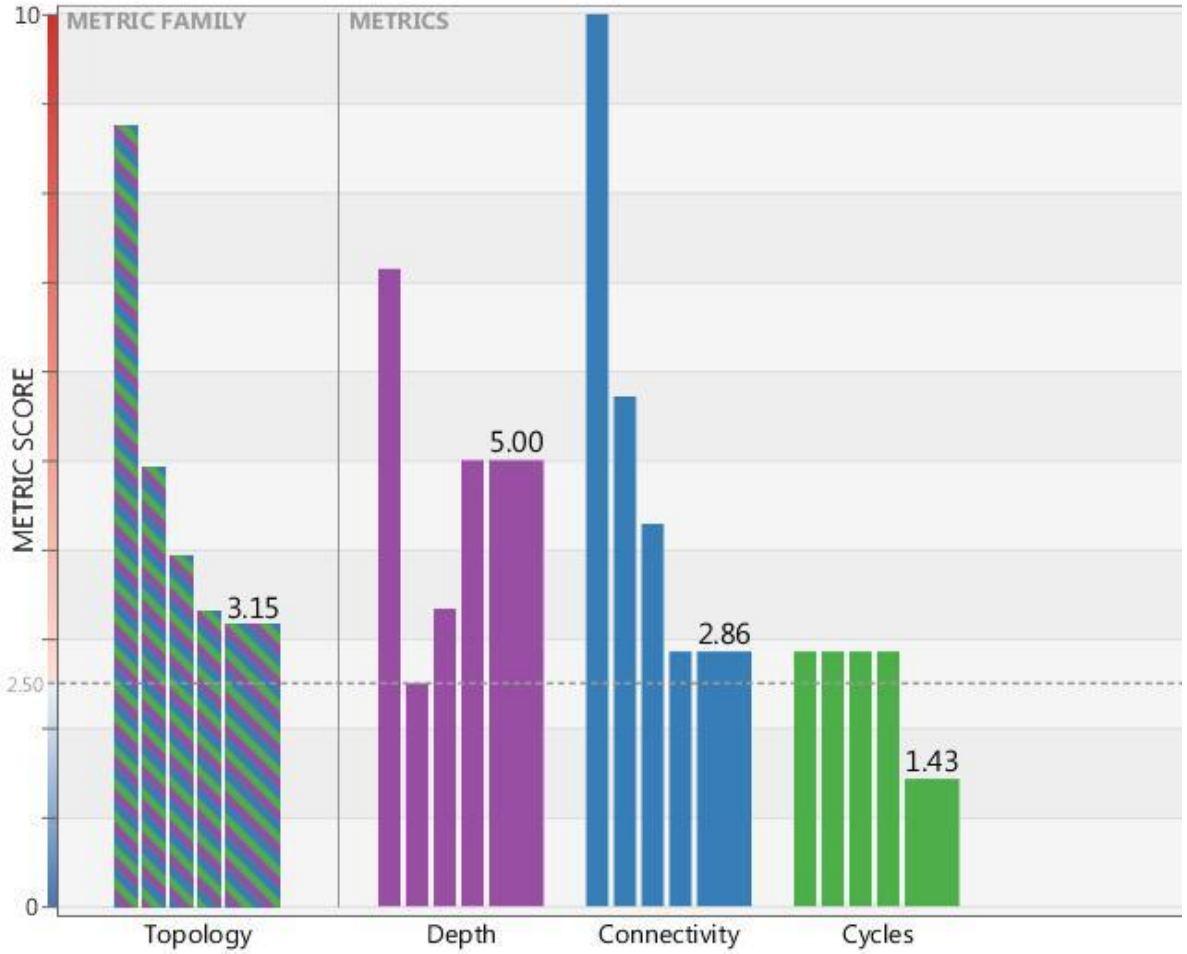
Depth

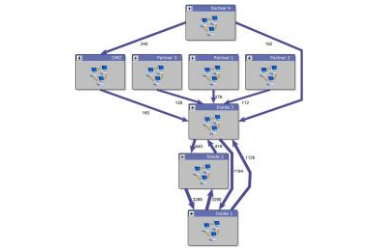
5.00 ↓ 2.14 (29%)

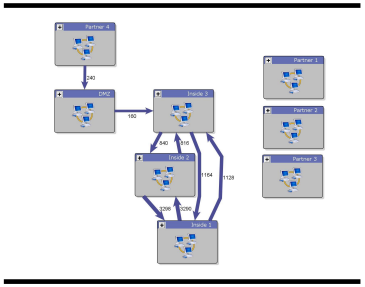
2.50 until acceptable (100% reduction)

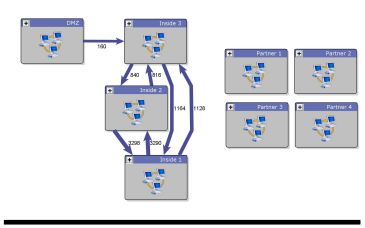
Back to Metric Families

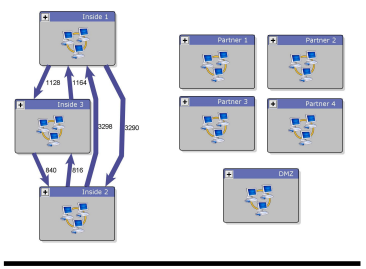
Topology metrics over time

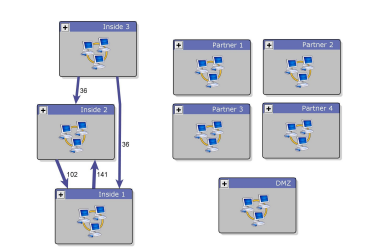












OVERALL WEIGHTING METRICS

Victimization ?

4.08 ↓ .62 (13%)

1.58 until acceptable (63% reduction)

50.00% | 25.00% | 25.00%

Existence ?

2.45 below acceptable (97% lower)

.05 ↓ 2.68 (98%)

Exploitability ?

6.07 ↓ 3.57 (36%)

3.57 until acceptable (142% reduction)

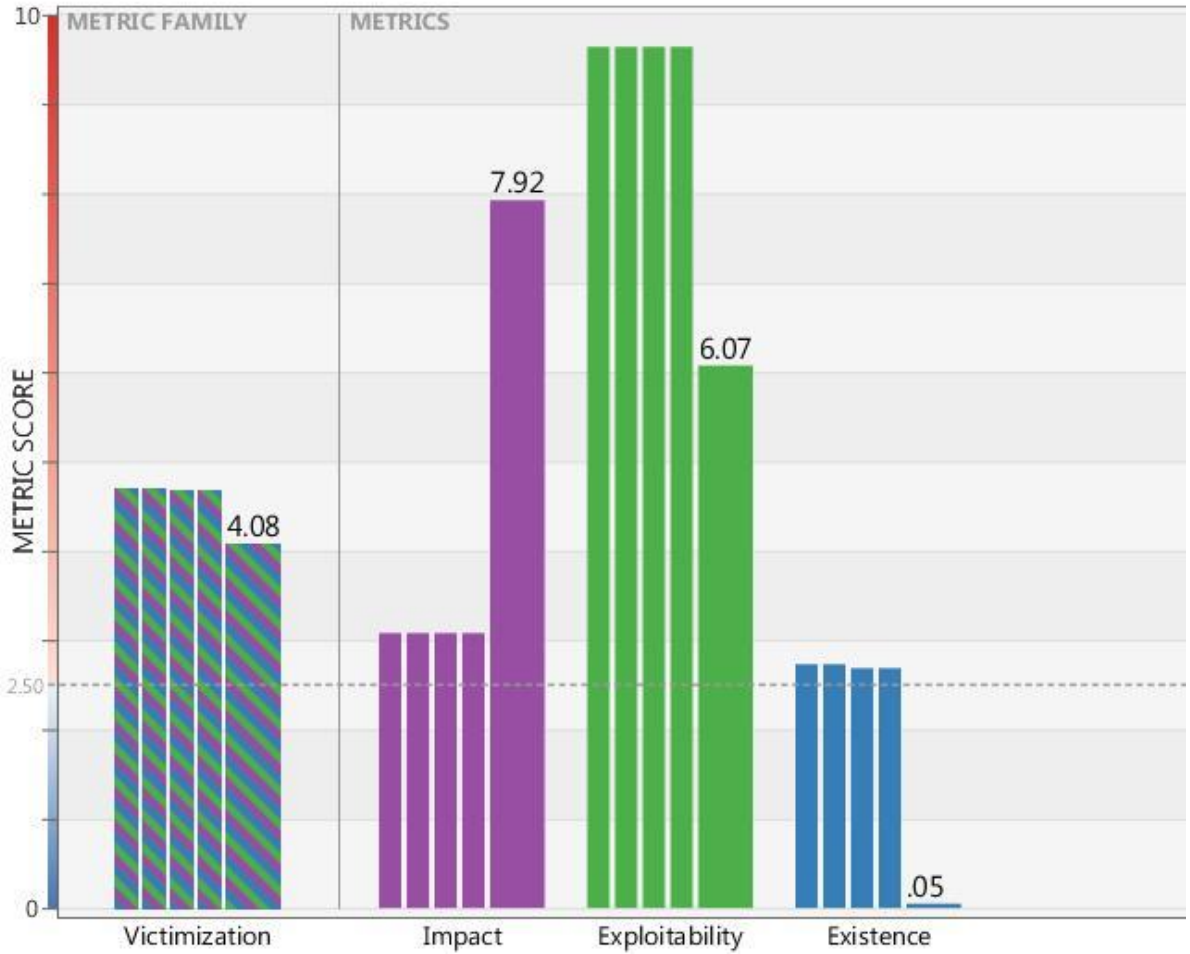
Impact ?

7.92 ↑ 4.84 (157%)

5.42 until acceptable (216% reduction)

← Back to Metric Families

Victimization metrics over time



Contact

Steven Noel

http://csis.gmu.edu/noel/

The MITRE Corporation
McLean, Virginia
snoel@mitre.org