

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

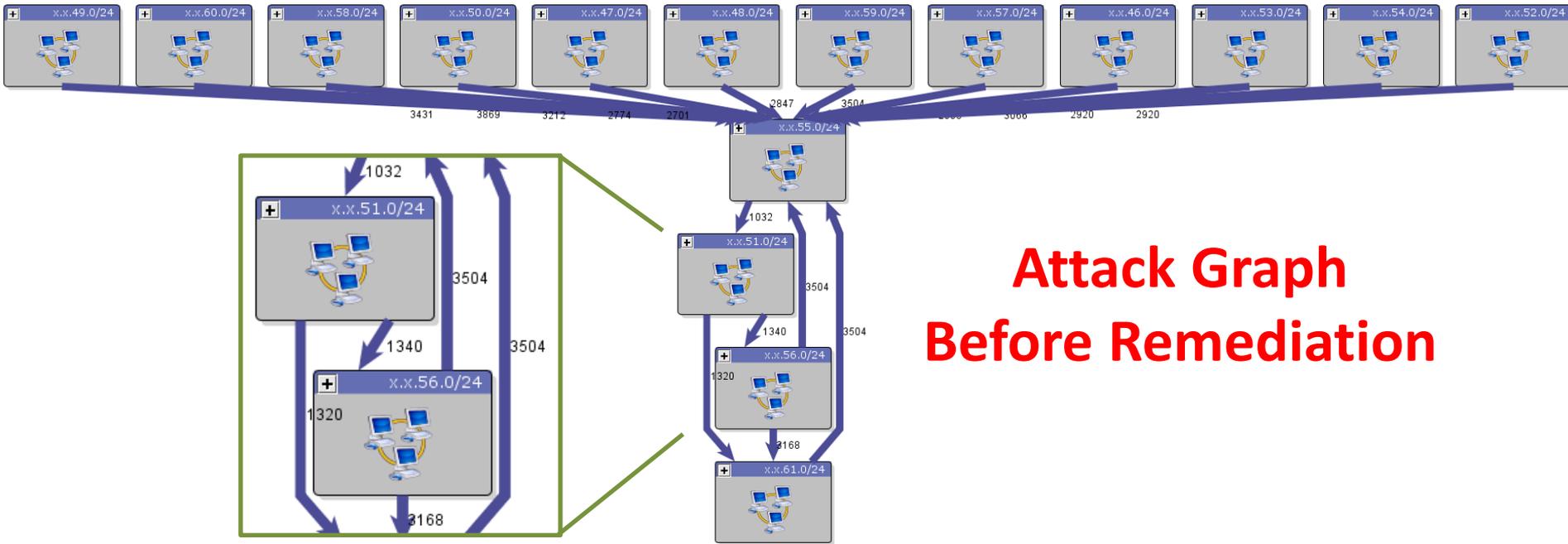




Motivation

- 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)

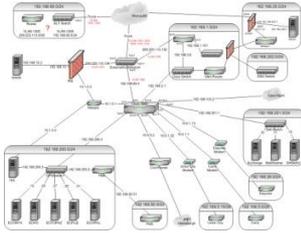
Motivating Example



**Attack Graph
Before Remediation**

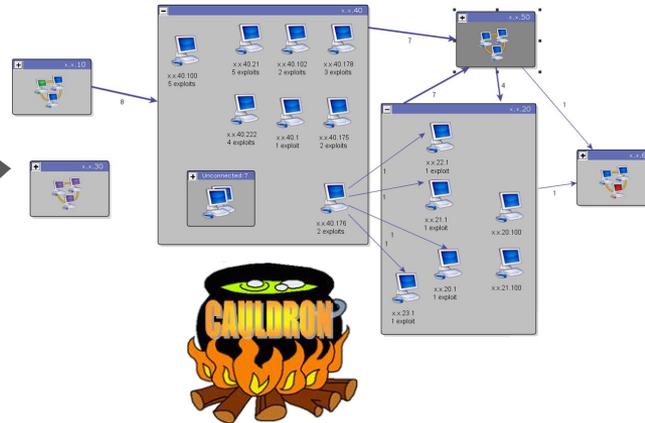
Attack Graph Metrics

Network Topology

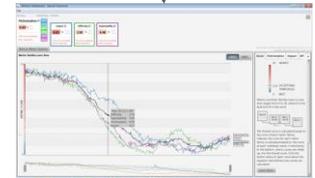


XML
CSV
Graphical

Attack Graph Analysis



Metrics Engine



Metrics Dashboard

Cisco ASA
Cisco IOS
Juniper JUNOS
Juniper ScreenOS
Fortinet
McAfee FE

Firewall Rules



Nessus
Retina
nCircle
Core Impact
Foundscan
Qualys
SAINT
nmap

Host Vulnerabilities

Severity	High	Medium	Low	Info
Critical	0	1	1	10
High	0	1	1	10
Medium	0	1	1	10
Low	0	1	1	10
Info	0	1	1	10

Cauldron Attack Graph

Attack Graph: network.xml

Root

- xx.10
 - xx.20
 - xx.20.1
 - xx.20.100
 - xx.21.1
 - xx.21.100
 - xx.22.1
 - xx.23.1
 - xx.30
 - Unconnected:7
 - xx.40.1
 - xx.40.100
 - xx.40.102
 - xx.40.175
 - xx.40.176
 - xx.40.178
 - xx.40.21
 - xx.40.222
 - xx.50
 - xx.60

Harden List

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

Node x.x.40 Details:

- xx.x.40.100: 5 exploits
- xx.x.40.21: 5 exploits
- xx.x.40.102: 2 exploits
- xx.x.40.178: 3 exploits
- xx.x.40.222: 4 exploits
- xx.x.40.1: 1 exploit
- xx.x.40.175: 2 exploits
- Unconnected:7
- xx.x.40.176: 2 exploits

Node x.x.50 Details:

- xx.x.22.1: 1 exploit
- xx.x.21.1: 1 exploit
- xx.x.20.100
- xx.x.20.100
- xx.x.20.1: 1 exploit
- xx.x.21.100
- xx.x.23.1: 1 exploit

Node x.x.60 Details:

- xx.x.20.100
- xx.x.20.1: 1 exploit
- xx.x.21.100
- xx.x.23.1: 1 exploit

Table:

From	To	Family	Name	CVE	Bugtraq	Summary	Ports	Description
xx.50.244	xx.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 3.7.1. Versions o
xx.50.244	xx.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 NTP
xx.50.244	xx.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 NTP
xx.50.244	xx.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 NTP
xx.50.244	xx.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 NTP
xx.40.176	xx.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
xx.40.176	xx.50.220	Useless s...	X Display Mana...			Checks if XDM has XDMCP protoc...		Synopsis: XDMCP is running on the remote host. Description: XDMCP allow
xx.40.176	xx.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 runni
xx.40.176	xx.50.1	Service det...	Telnet Server D...			Telnet Server Detection	Services/telnet, ...	Synopsis: A telnet server is listening on the remote port. Description: The re
xx.40.176	xx.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 NTP
xx.40.176	xx.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

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)

Common Vulnerability Scoring System (CVSS)

CVSS Base Metric

Exploitability

Impact

**Access
Vector**

**Access
Complexity**

Authentication

Confidentiality

Integrity

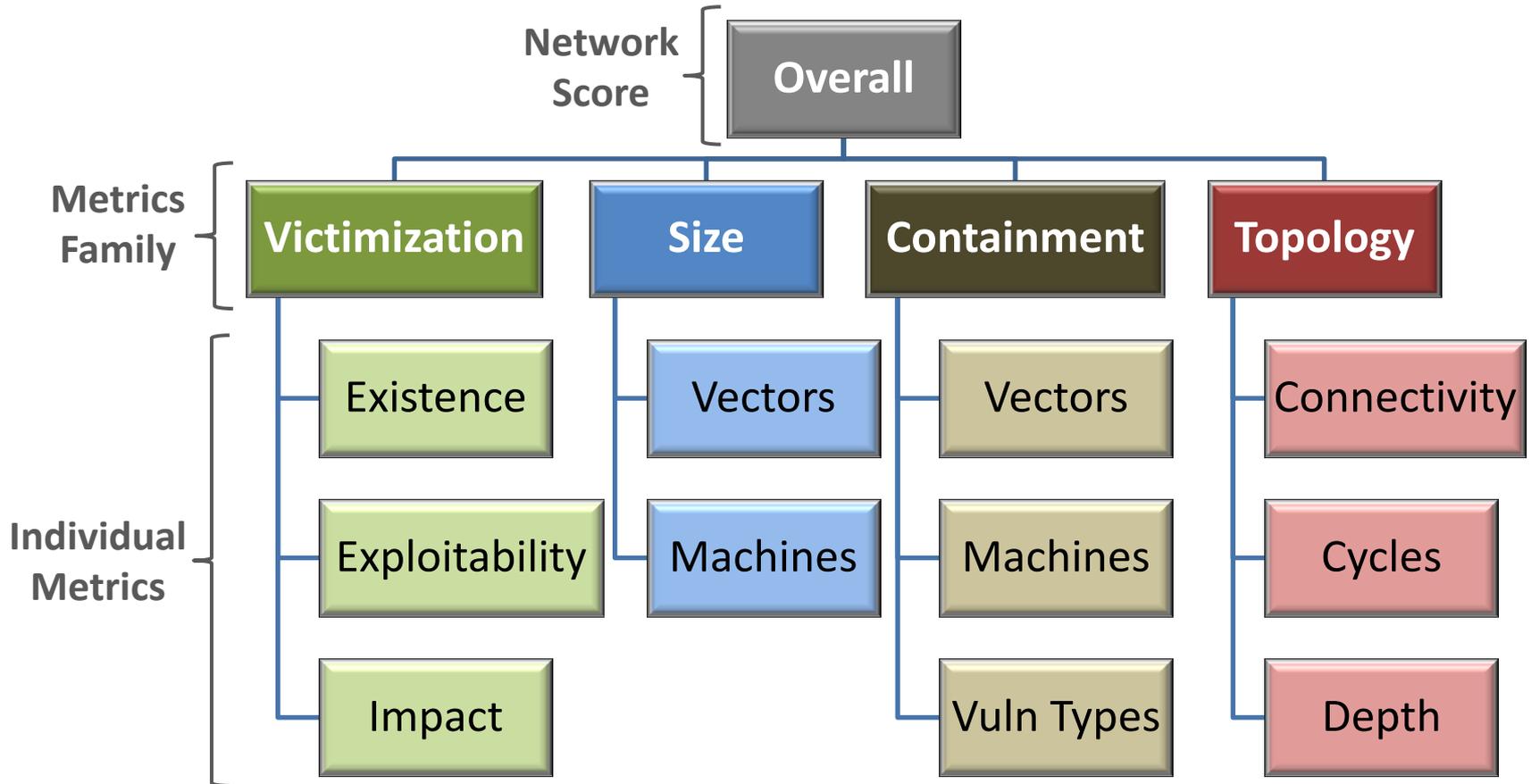
Availability



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)

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

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

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

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

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

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

Best

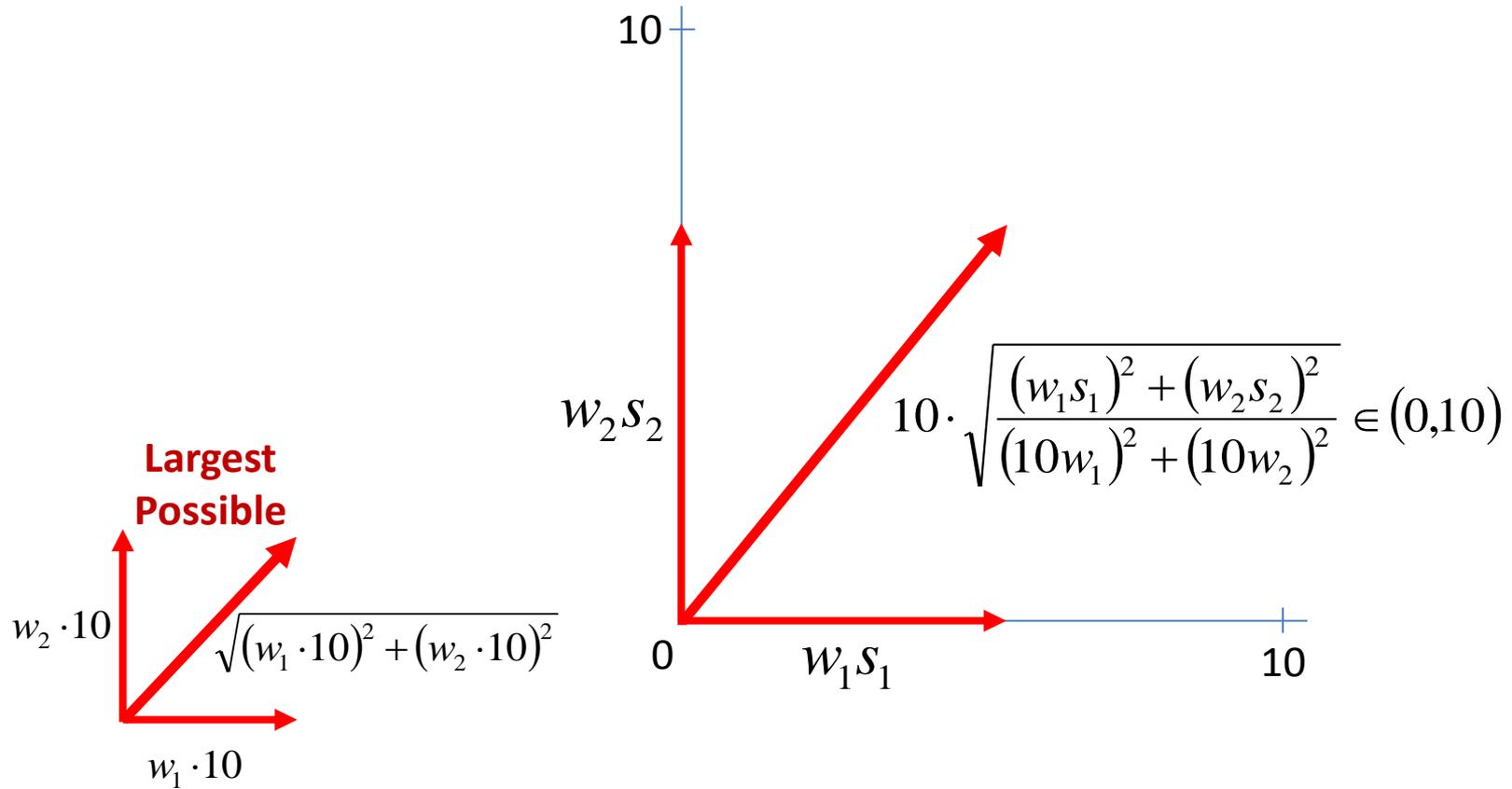
0

Worst

10

$f^{(5)}(x)$

Combining Metrics



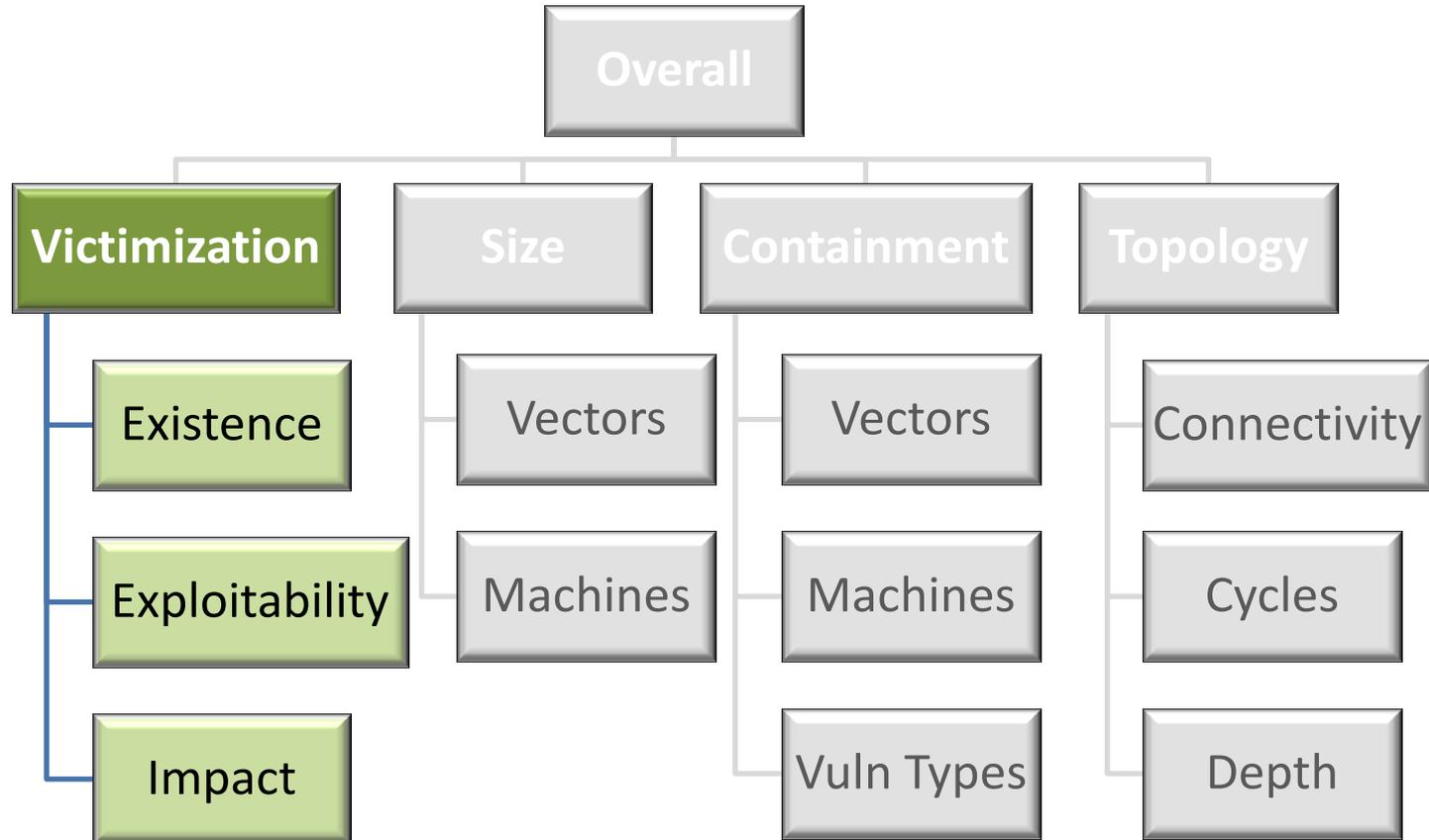
Combining Metrics

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

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

For individual score s_i with weight w_i .

Metrics Hierarchy



Metrics Family: Victimization

- Existence – relative number of ports that are vulnerable:

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

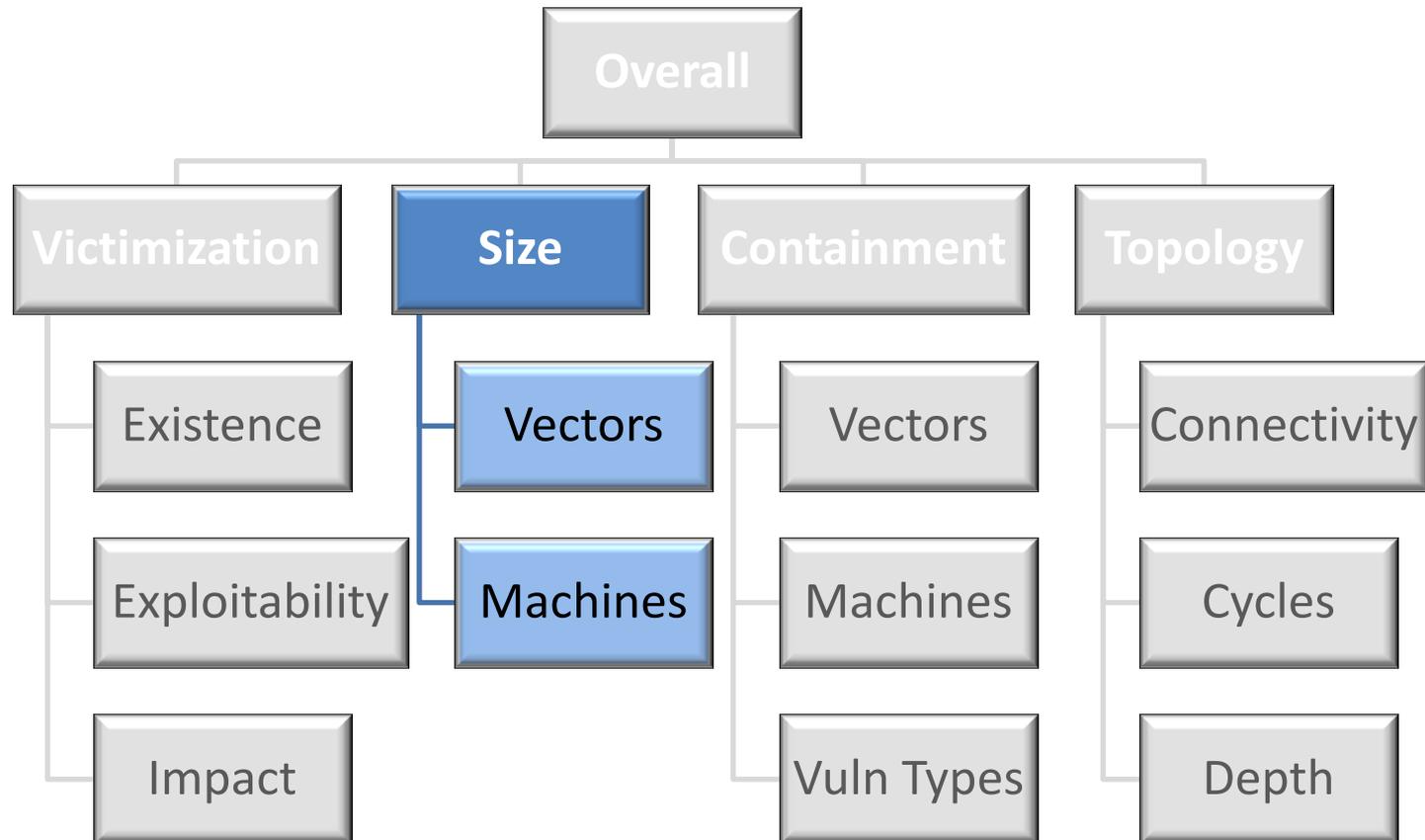
- Exploitability – average CVSS Exploitability:

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

- Impact – average CVSS Impact:

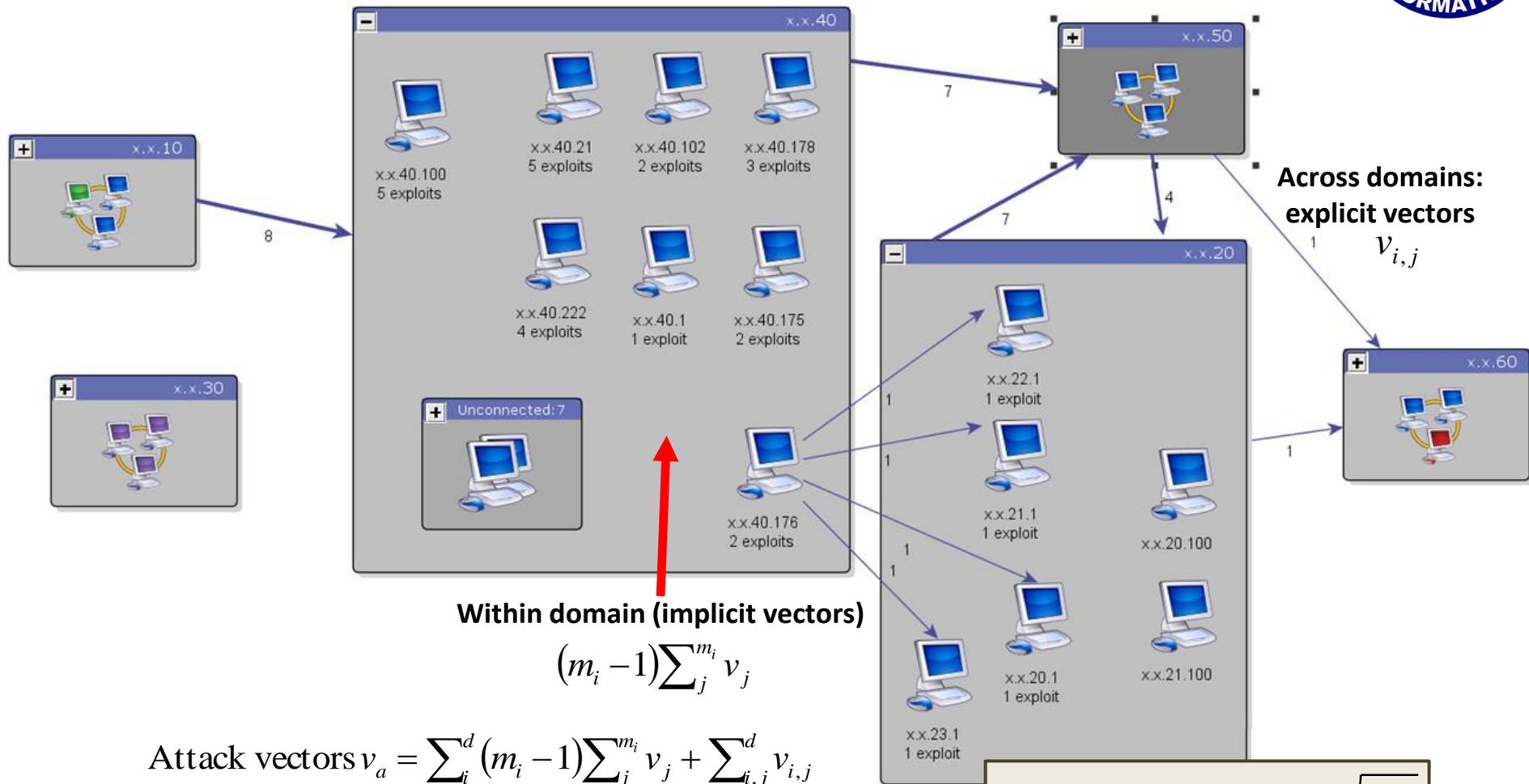
$$\text{Impact} = \sum_i^U m(u_i) / U,$$

Metrics Hierarchy



Size Family

Vectors Metric



$$(m_i - 1) \sum_j^{m_i} v_j$$

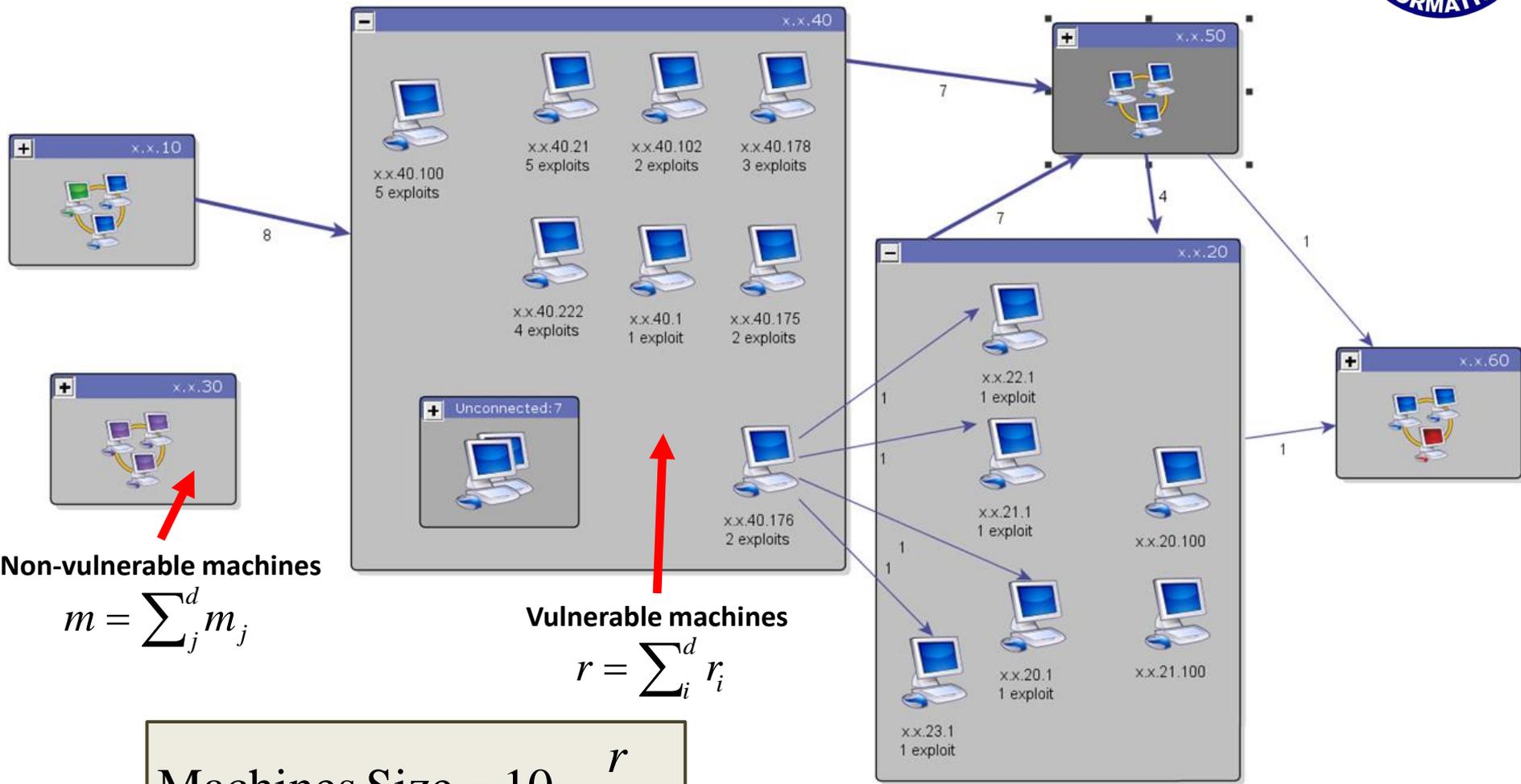
$$\text{Attack vectors } v_a = \sum_i^d (m_i - 1) \sum_j^{m_i} v_j + \sum_{i,j}^d v_{i,j}$$

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

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

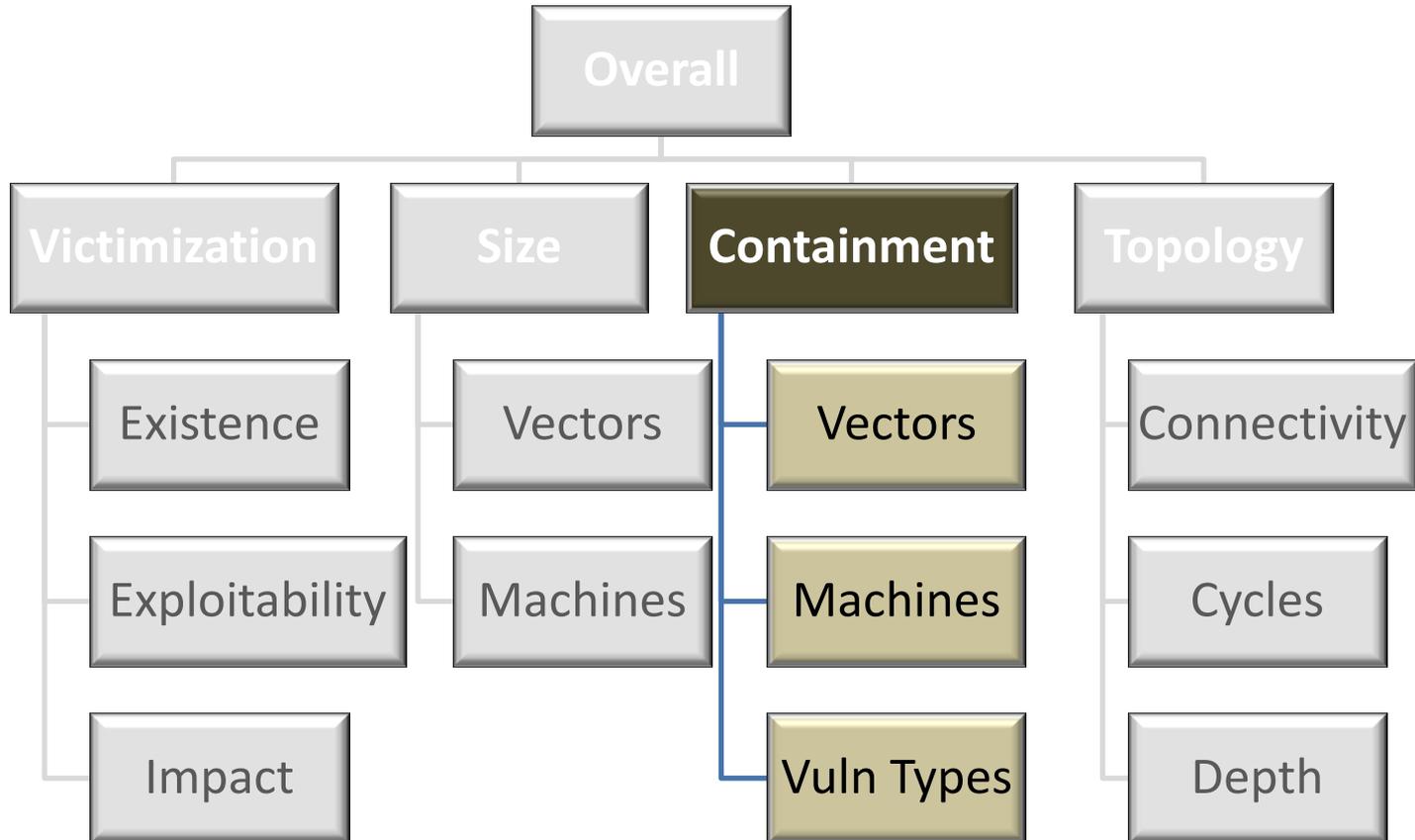
Size Family

Machines Metric



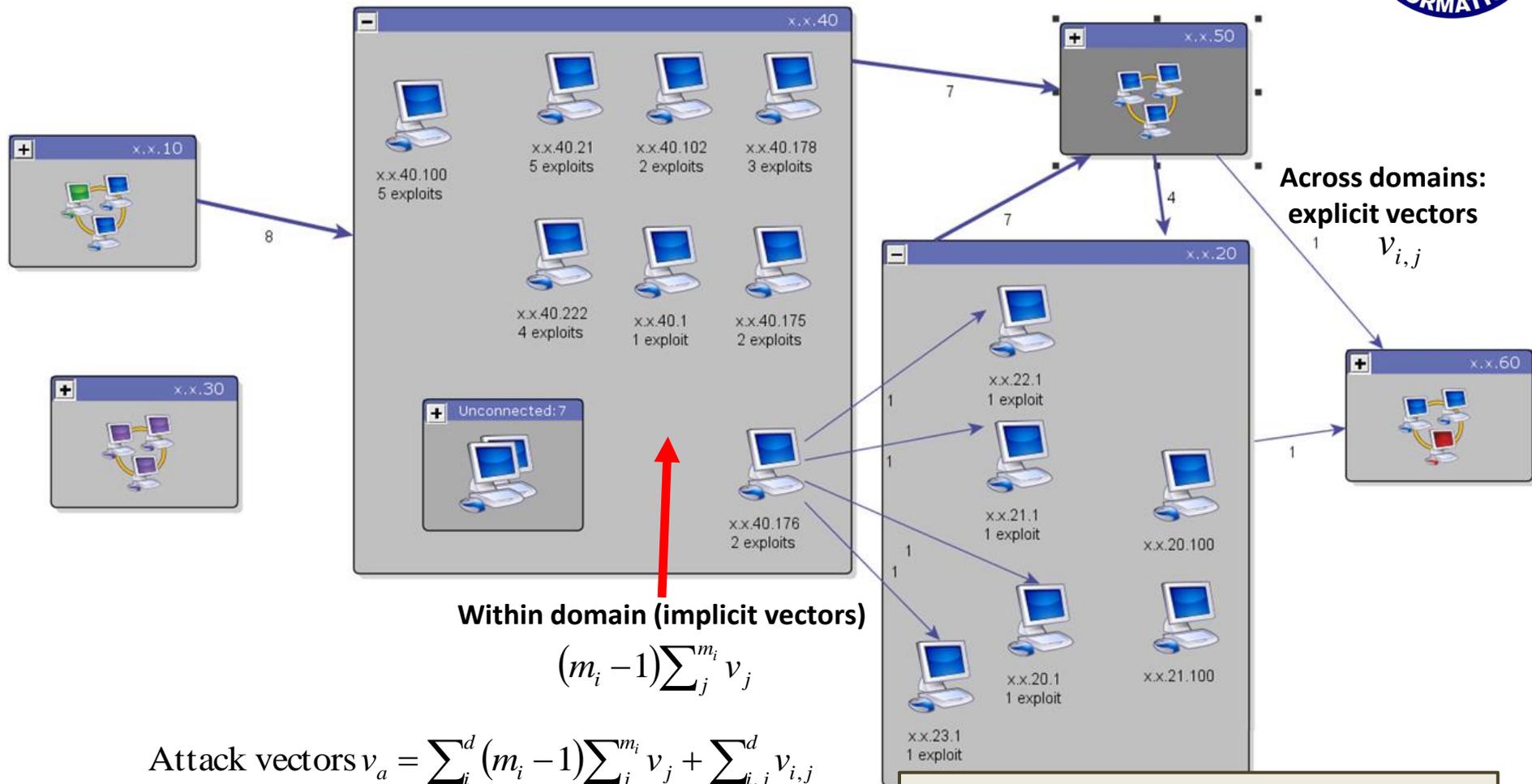
$$\text{Machines Size} = 10 \frac{r}{r + m}$$

Metrics Hierarchy



Containment Family

Vectors Metric



Across domains:
explicit vectors
 $v_{i,j}$

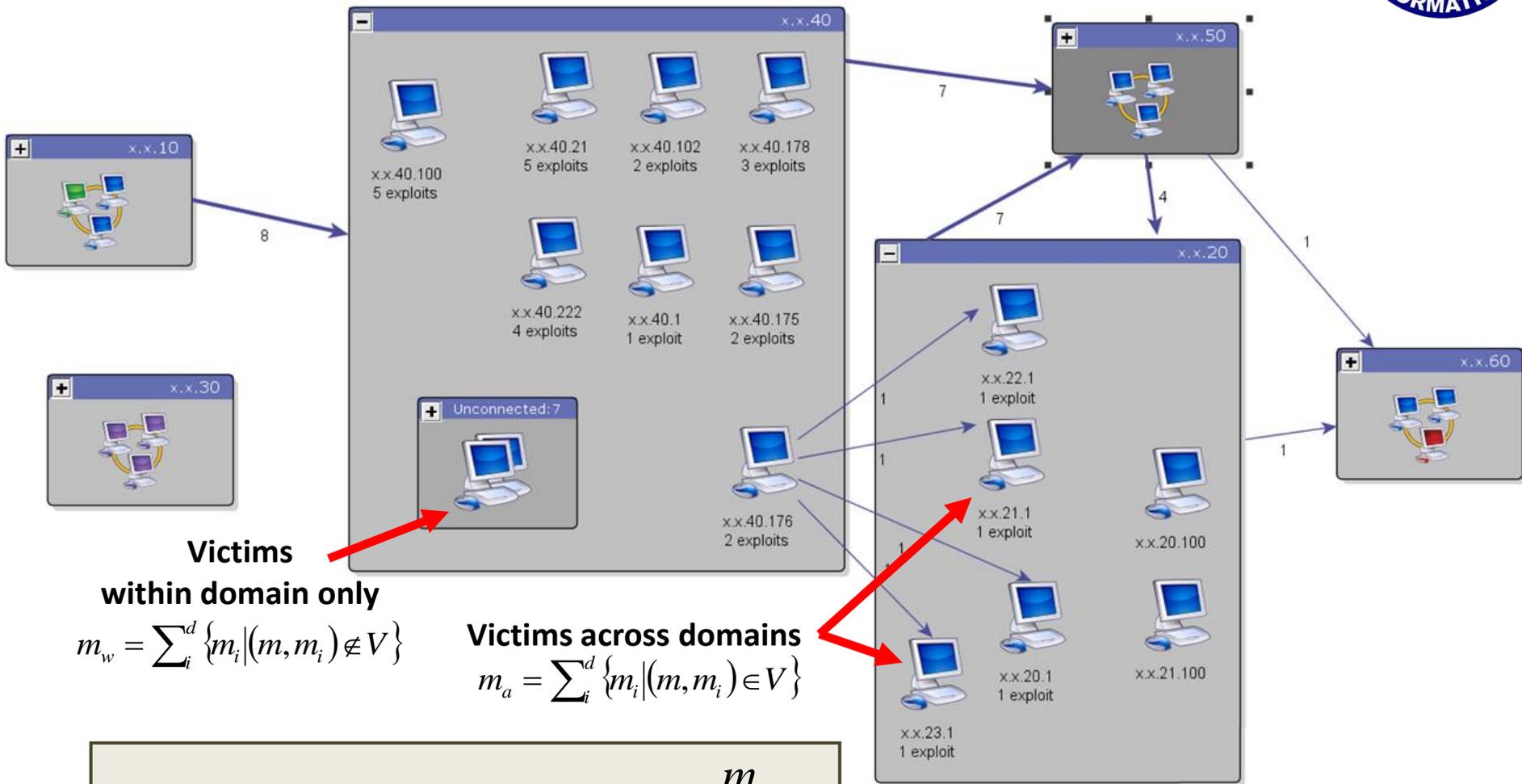
Within domain (implicit vectors)
 $(m_i - 1) \sum_j^{m_i} v_j$

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

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

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

Containment Family Machines Metric



Victims

within domain only

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

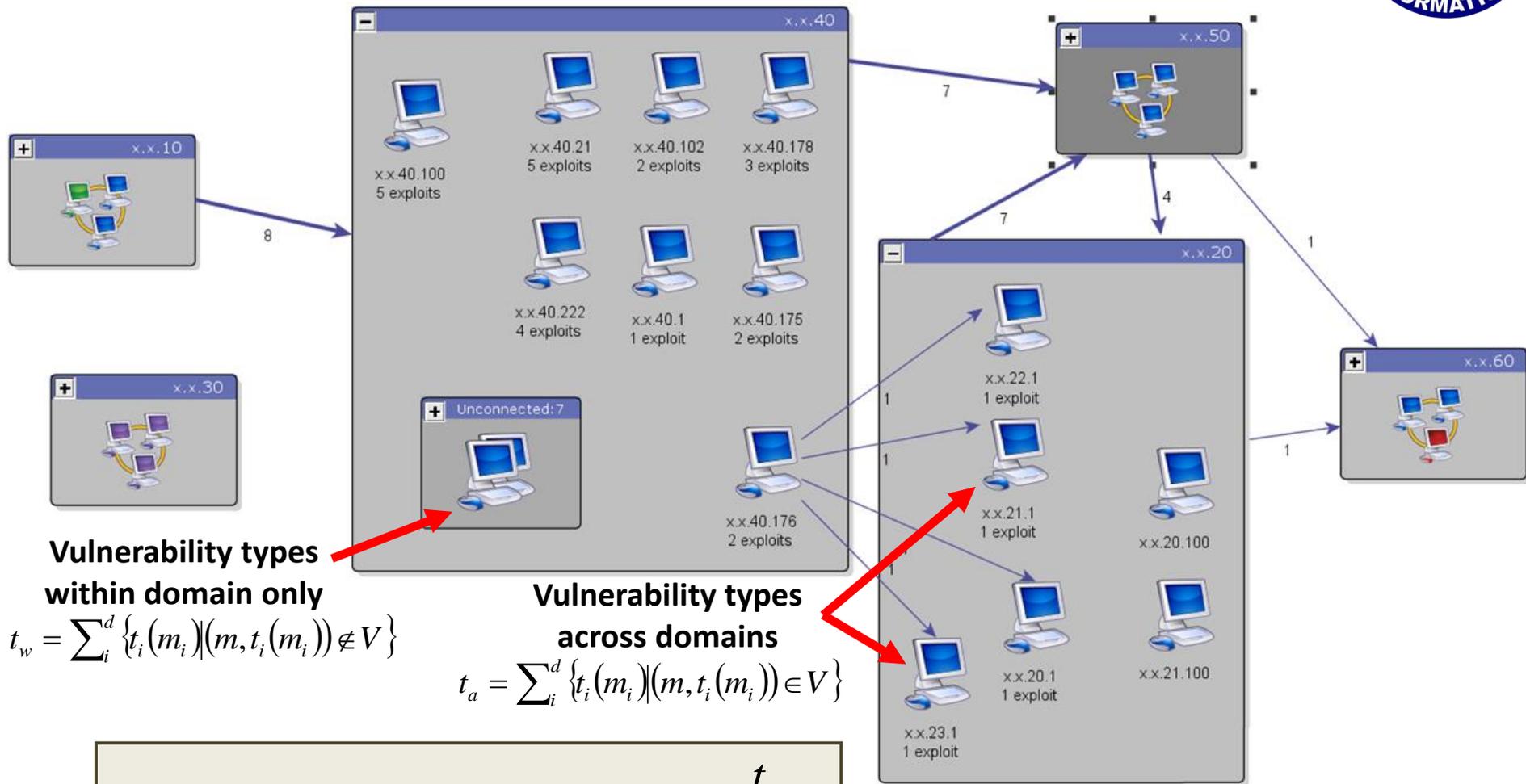
Victims across domains

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

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

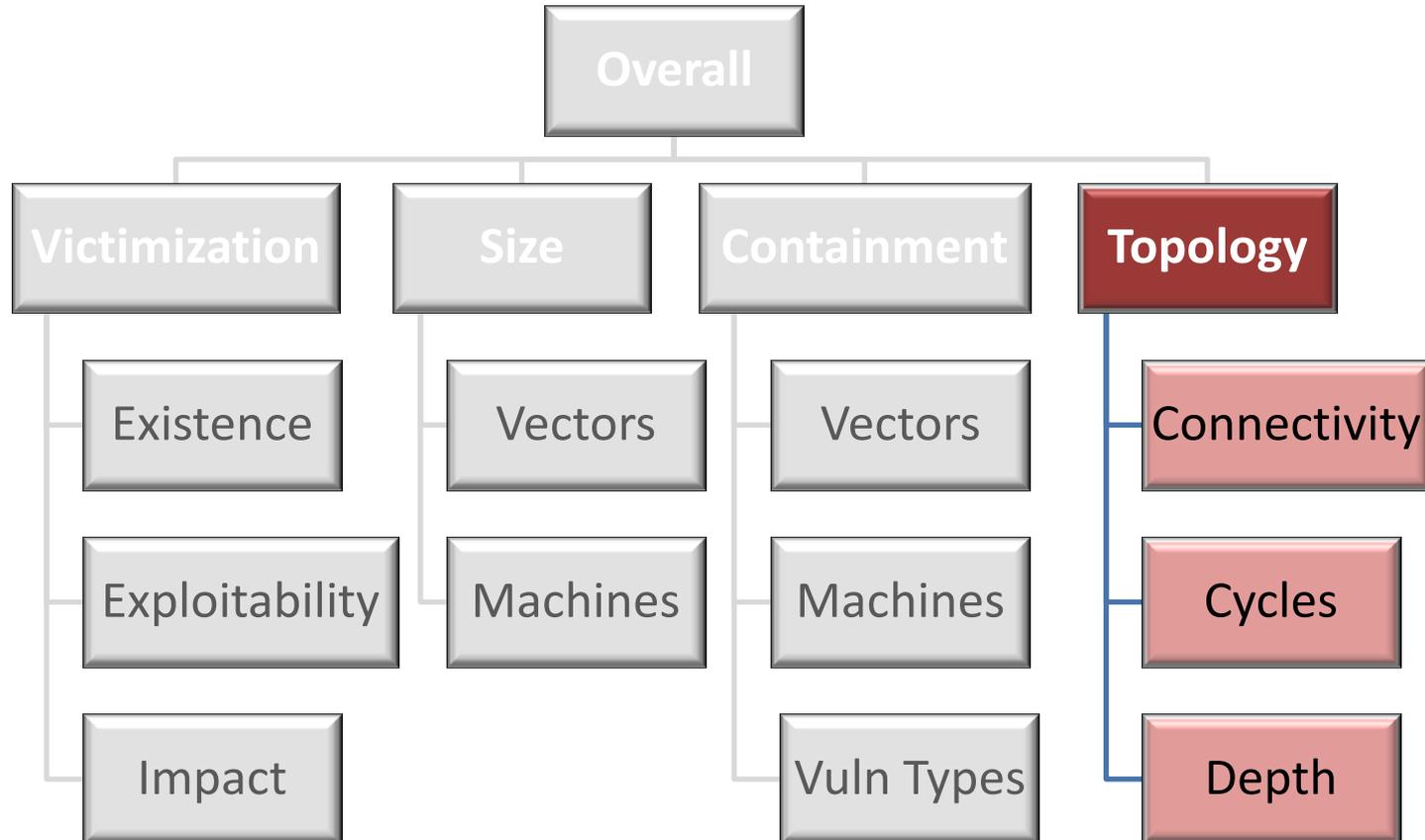
Containment Family

Vulnerability Types Metric



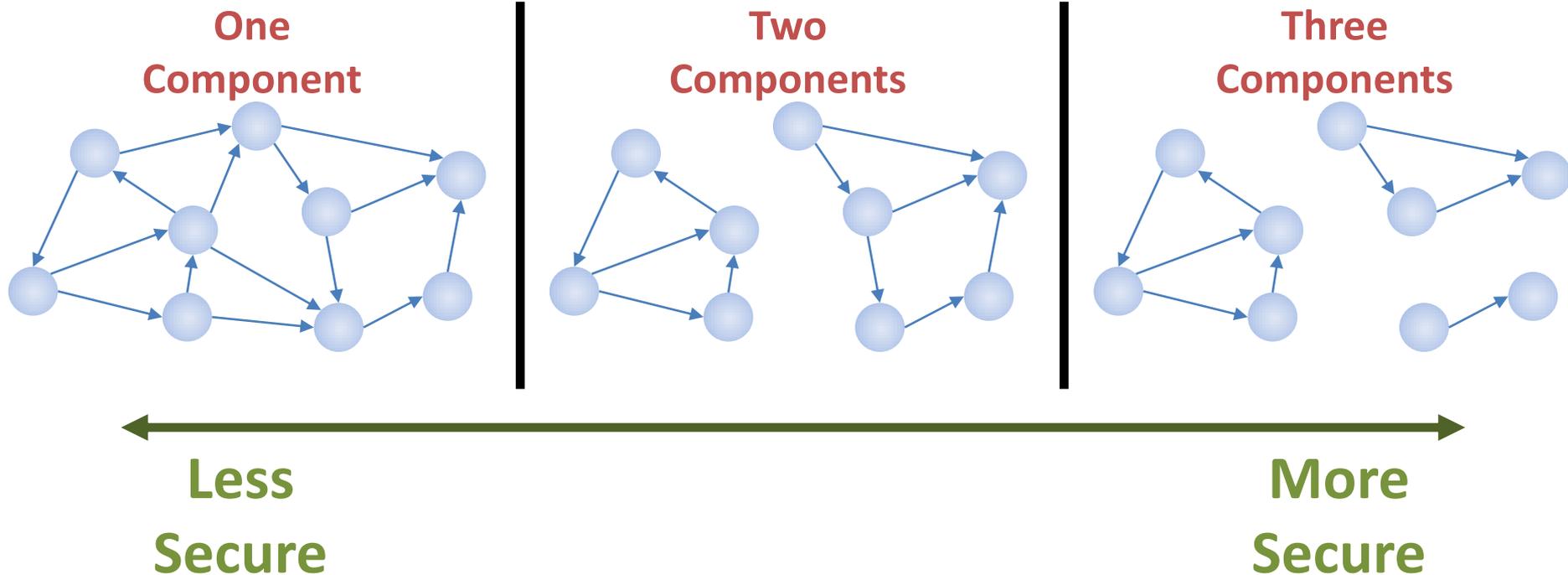
$$\text{Vuln Types Containment} = 10 \cdot \frac{t_a}{t_a + t_w}$$

Metrics Hierarchy



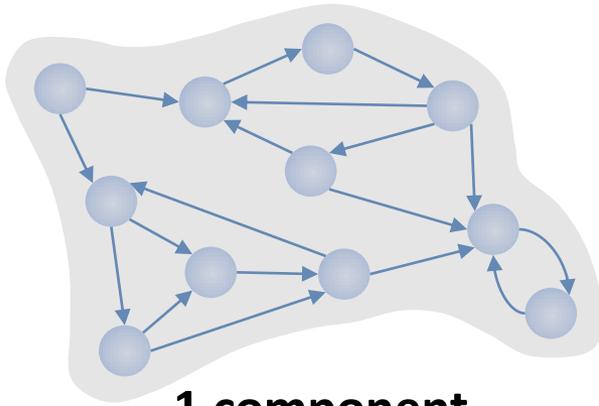
Attack Graph Connectivity

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



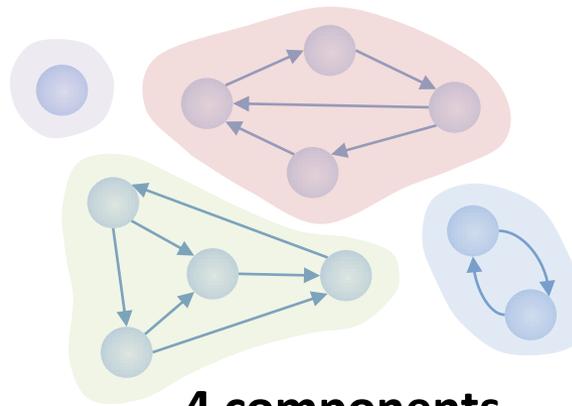
Topology Family

Connectivity Metric



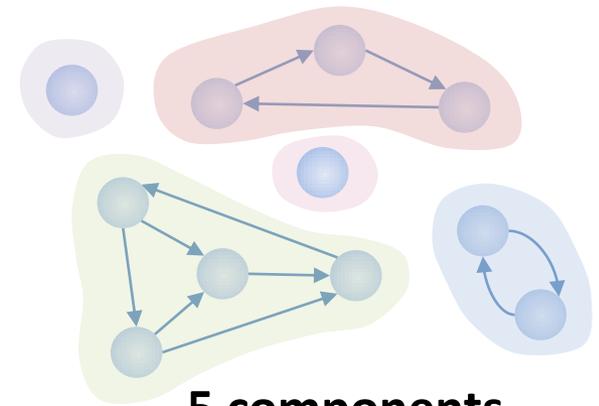
1 component

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



4 components

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

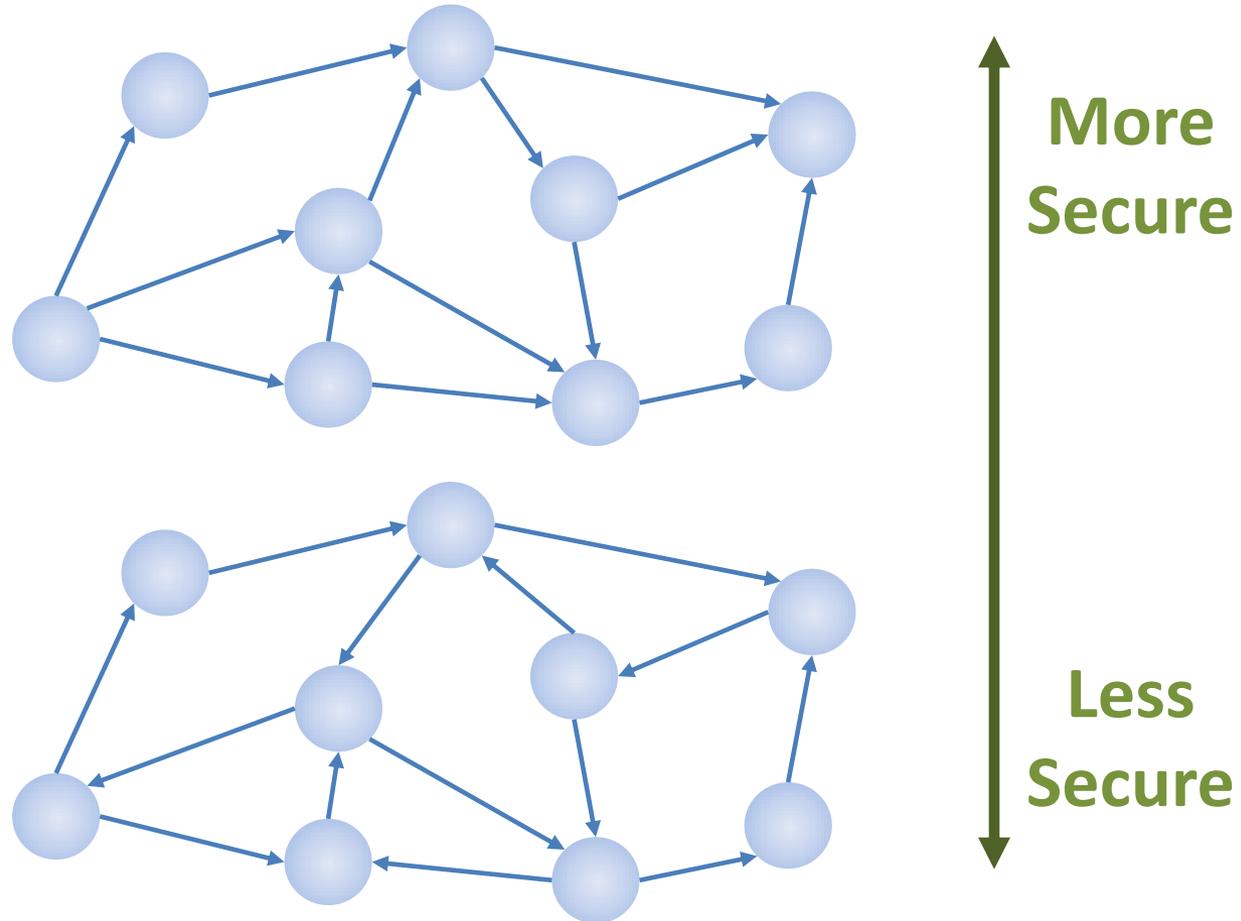


5 components

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

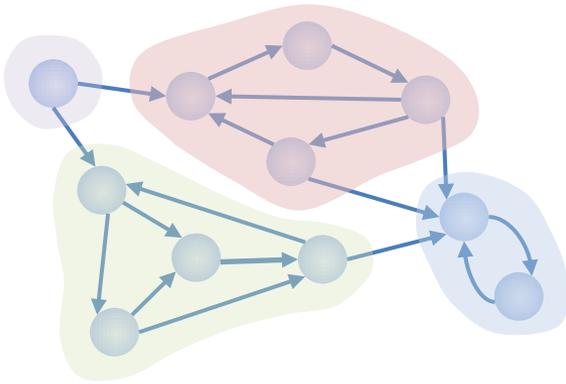
Attack Graph Cycles

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



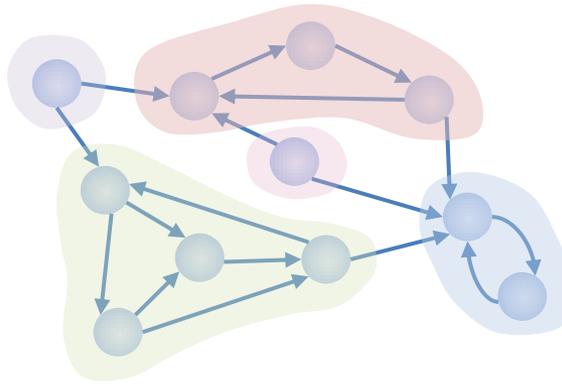
Topology Family

Cycles Metric



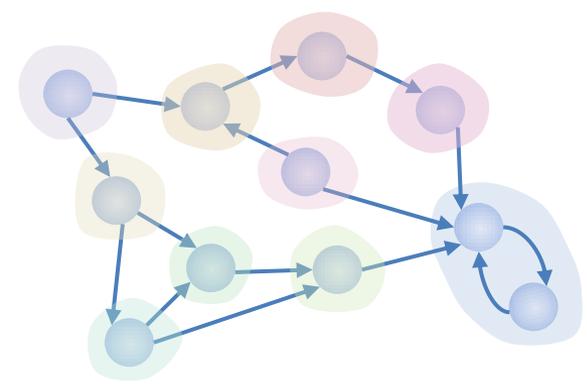
4 components

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



5 components

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

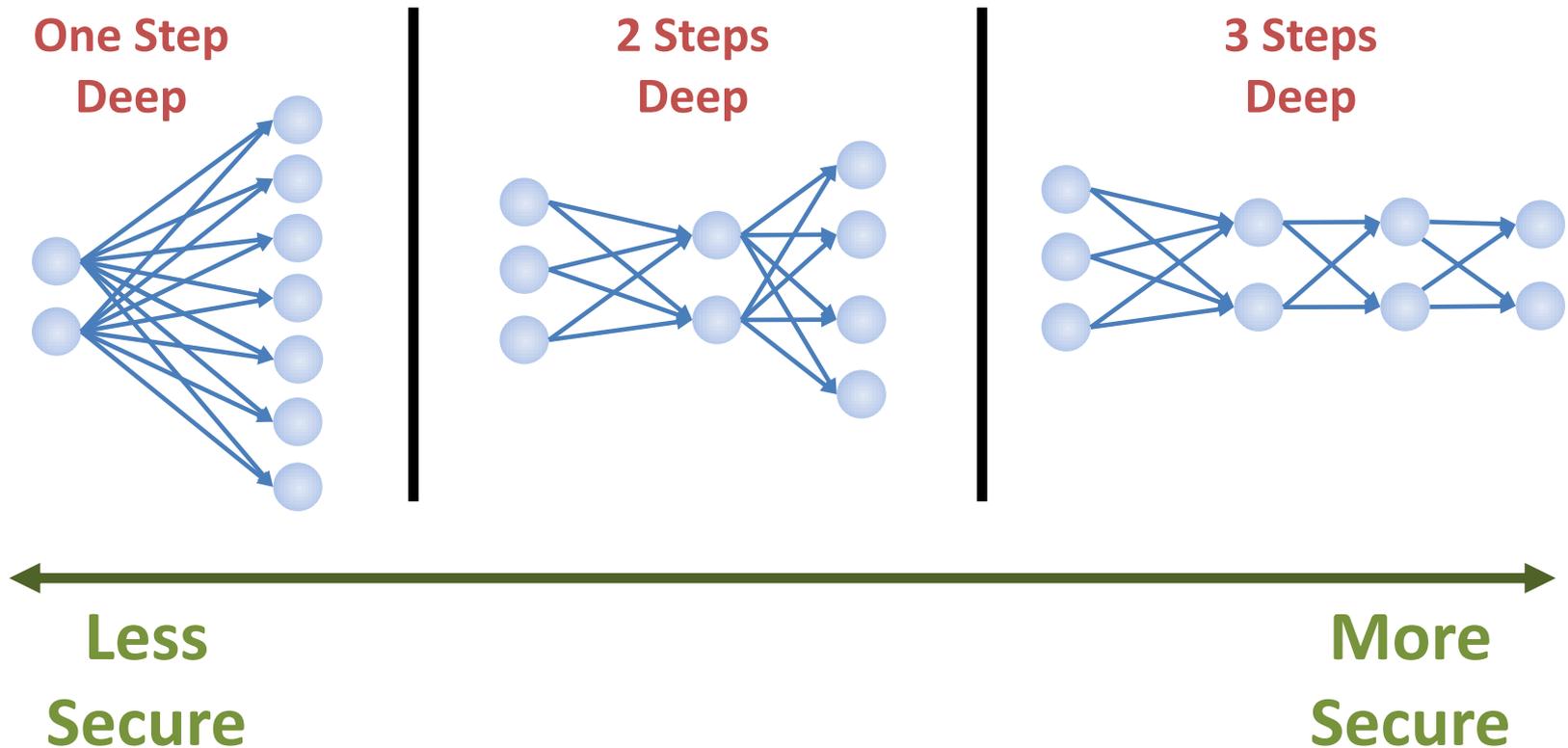


10 components

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

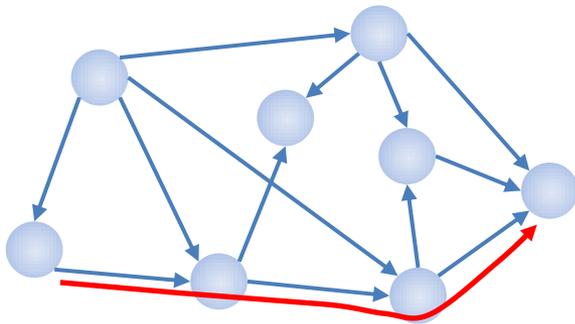
Attack Graph Depth

Motivation: Better to have attack graph deeper versus shallower



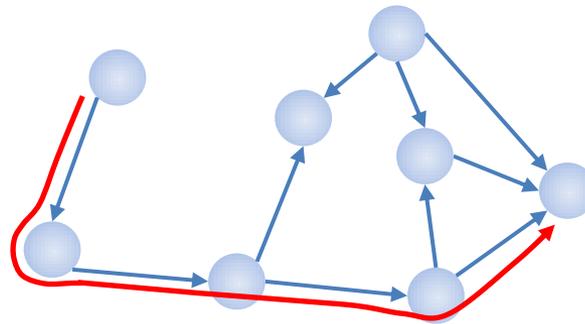
Topology Family

Depth Metric



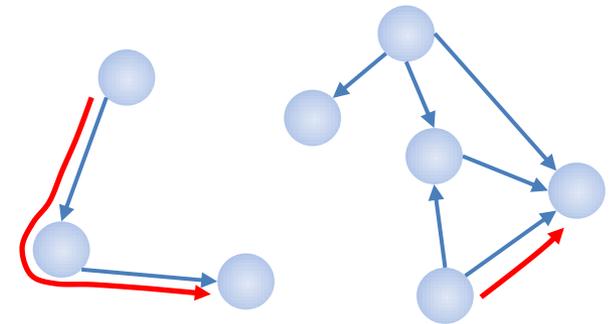
Shortest path 3/8

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



Shortest path 4/8

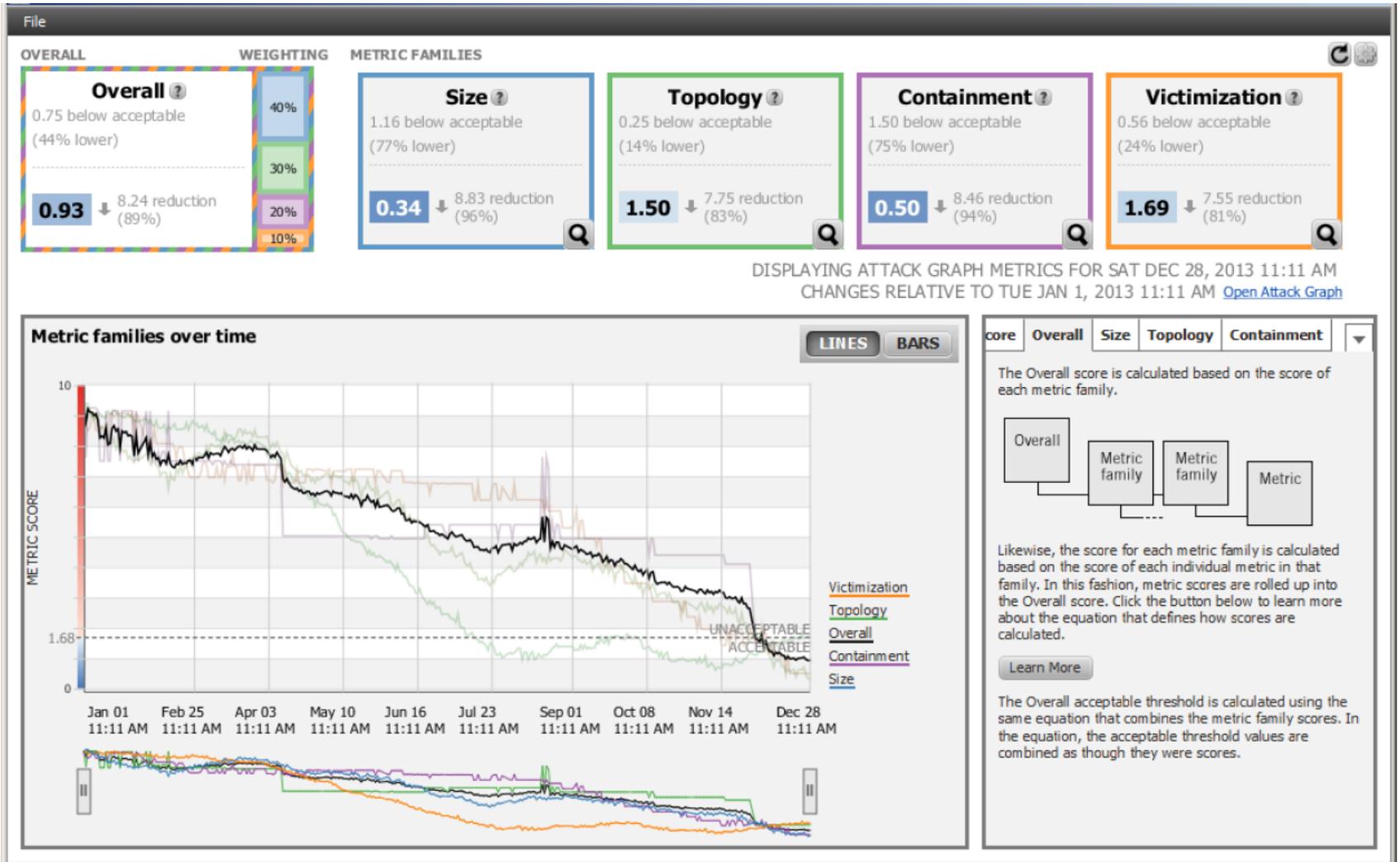
$$\text{Metric} = 10 \left(1 - \frac{4}{8-1} \right) = 4.3$$



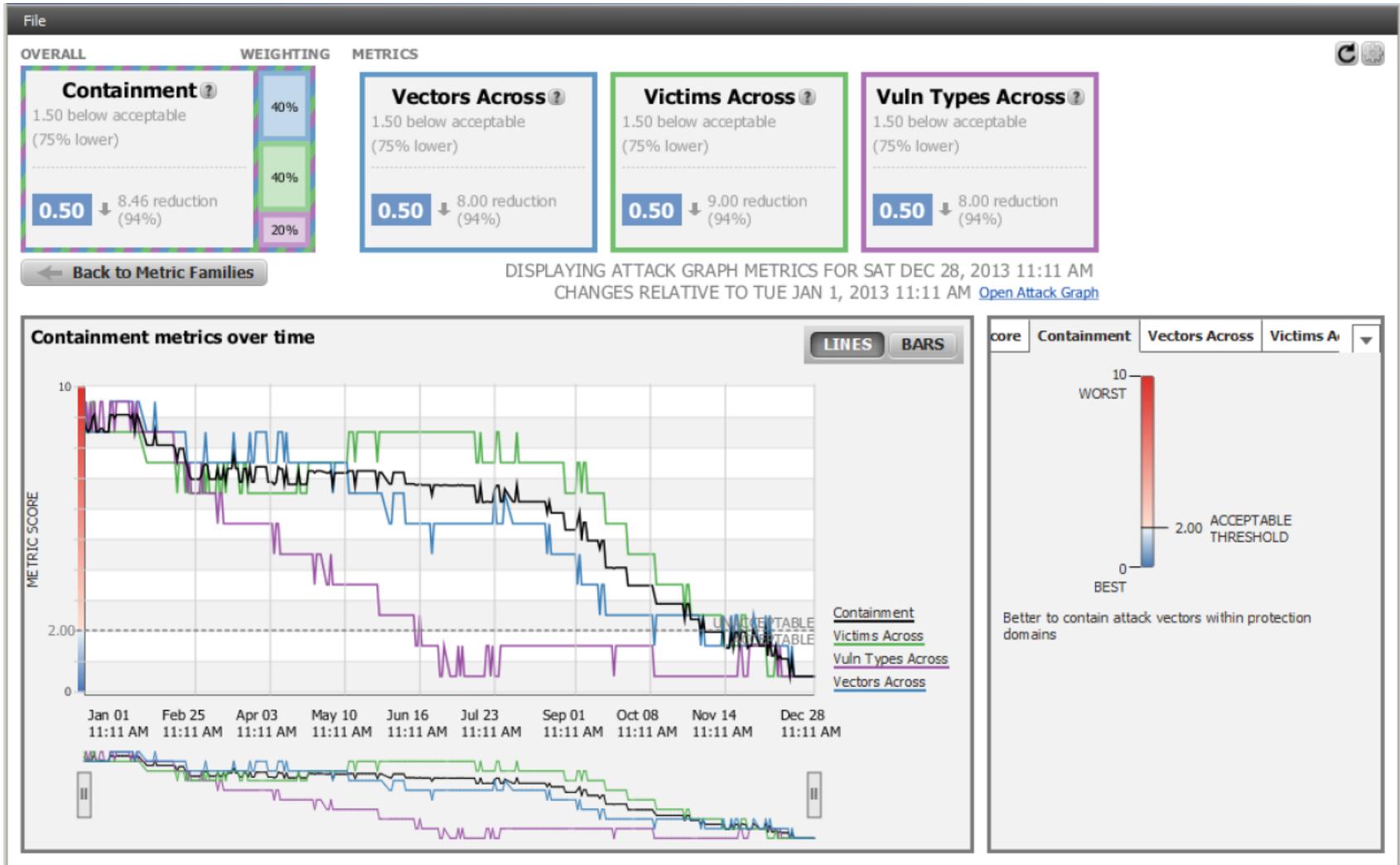
Shortests paths 2/3 and 1/5

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

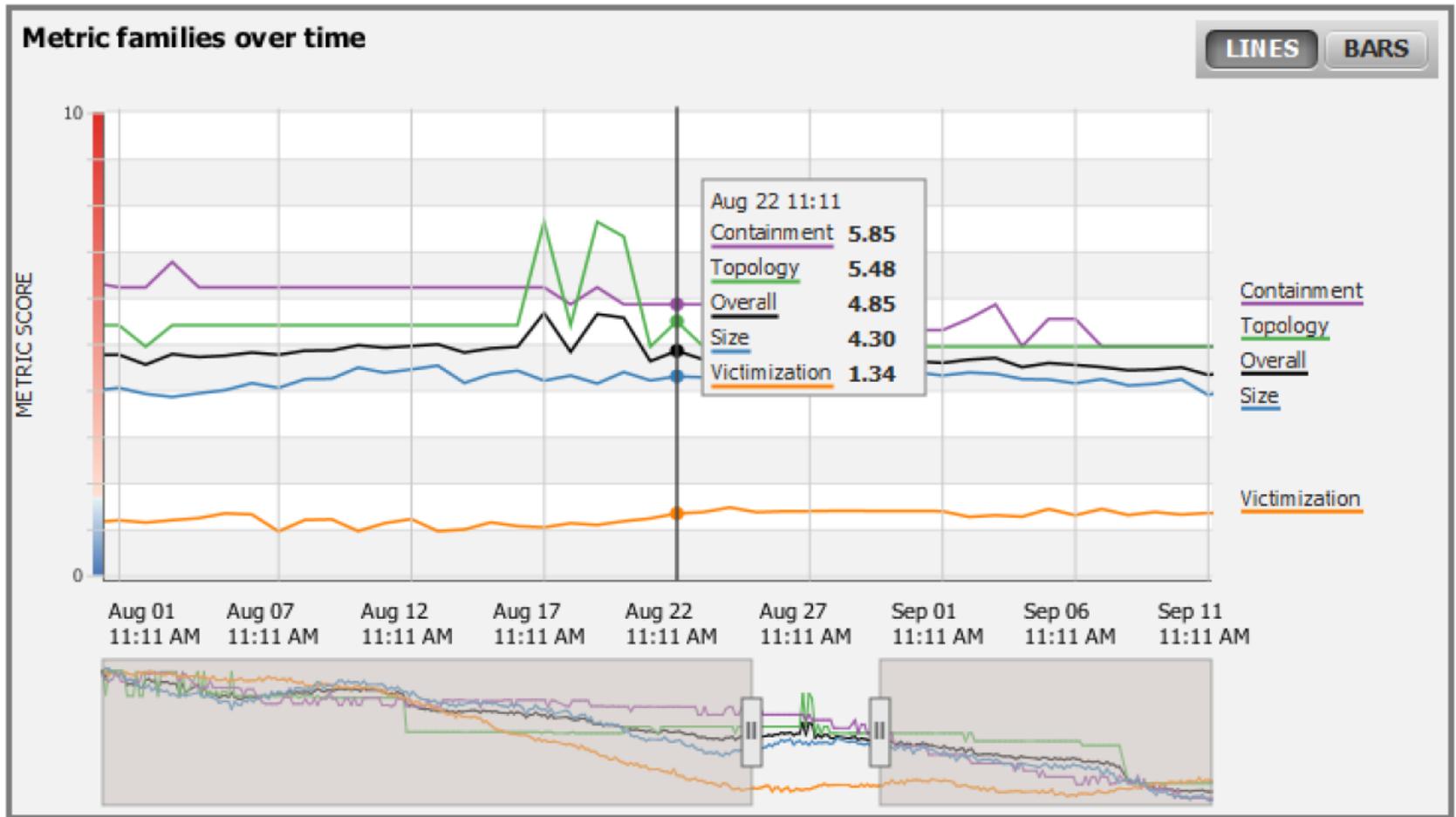
Metrics Dashboard



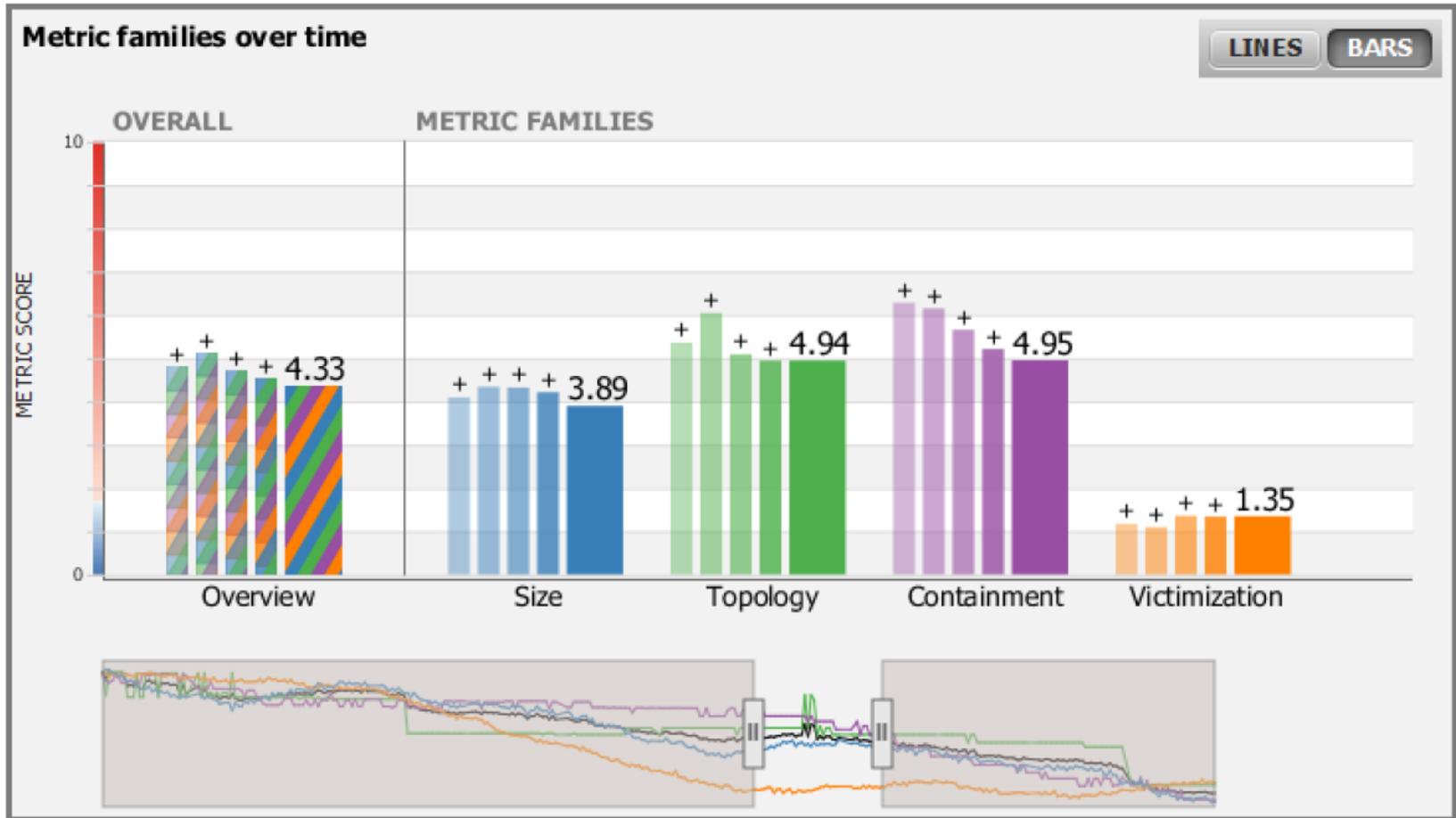
Family-Level Metrics



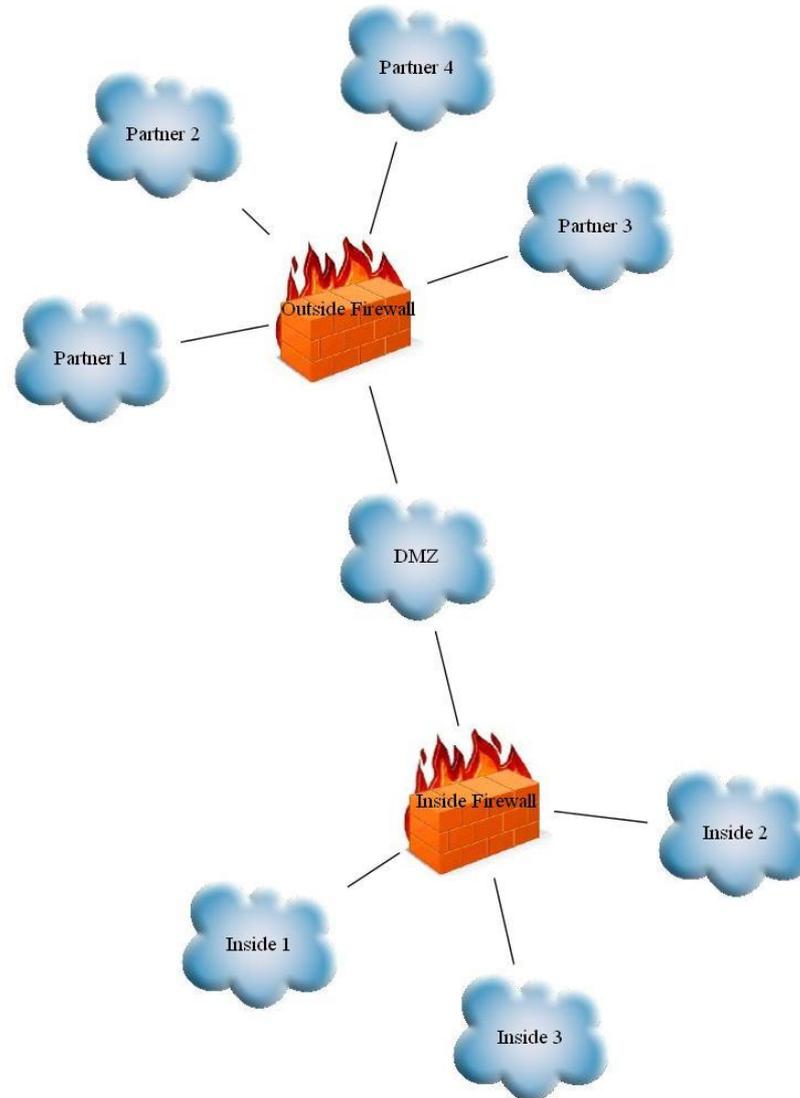
Temporal Zoom



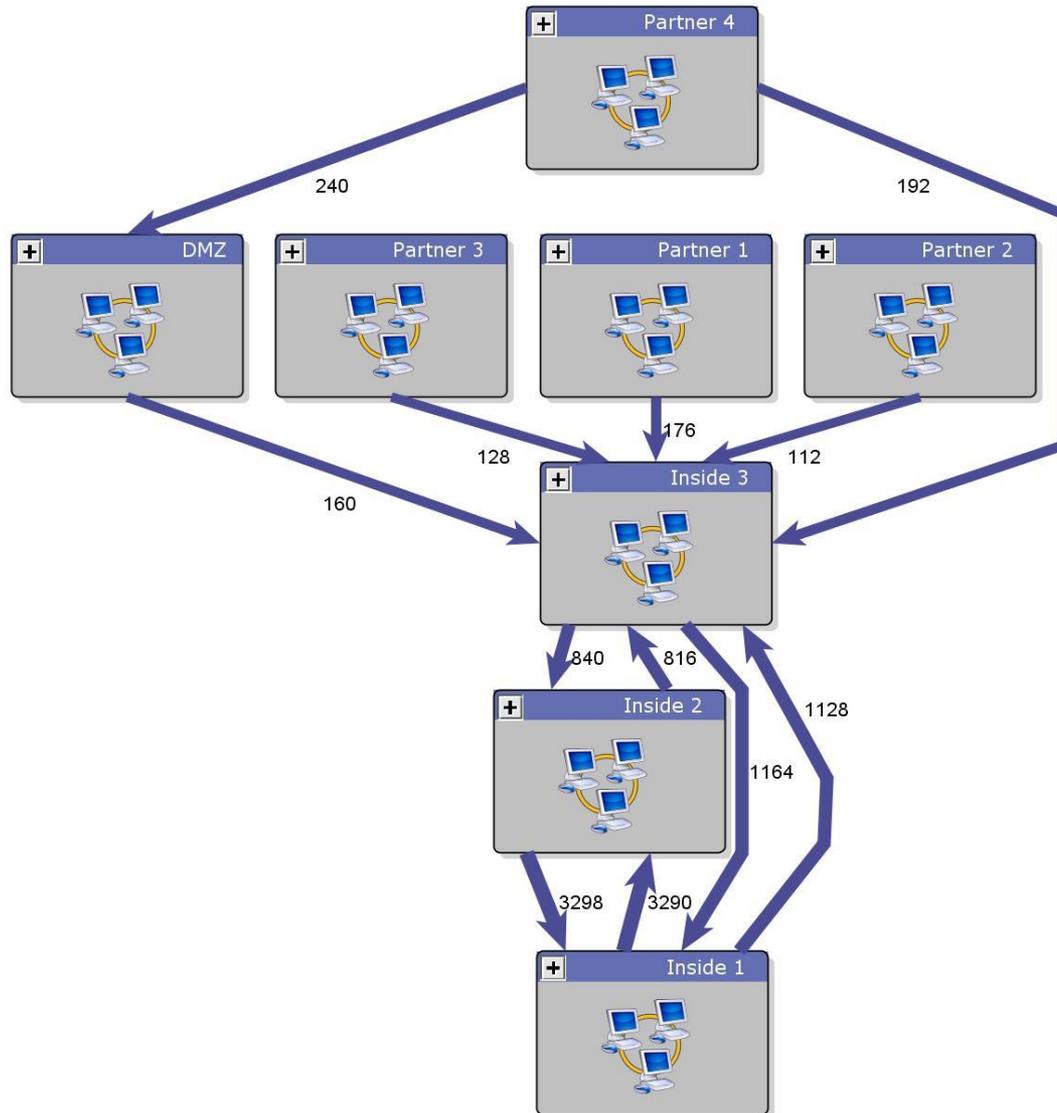
Trend Summary



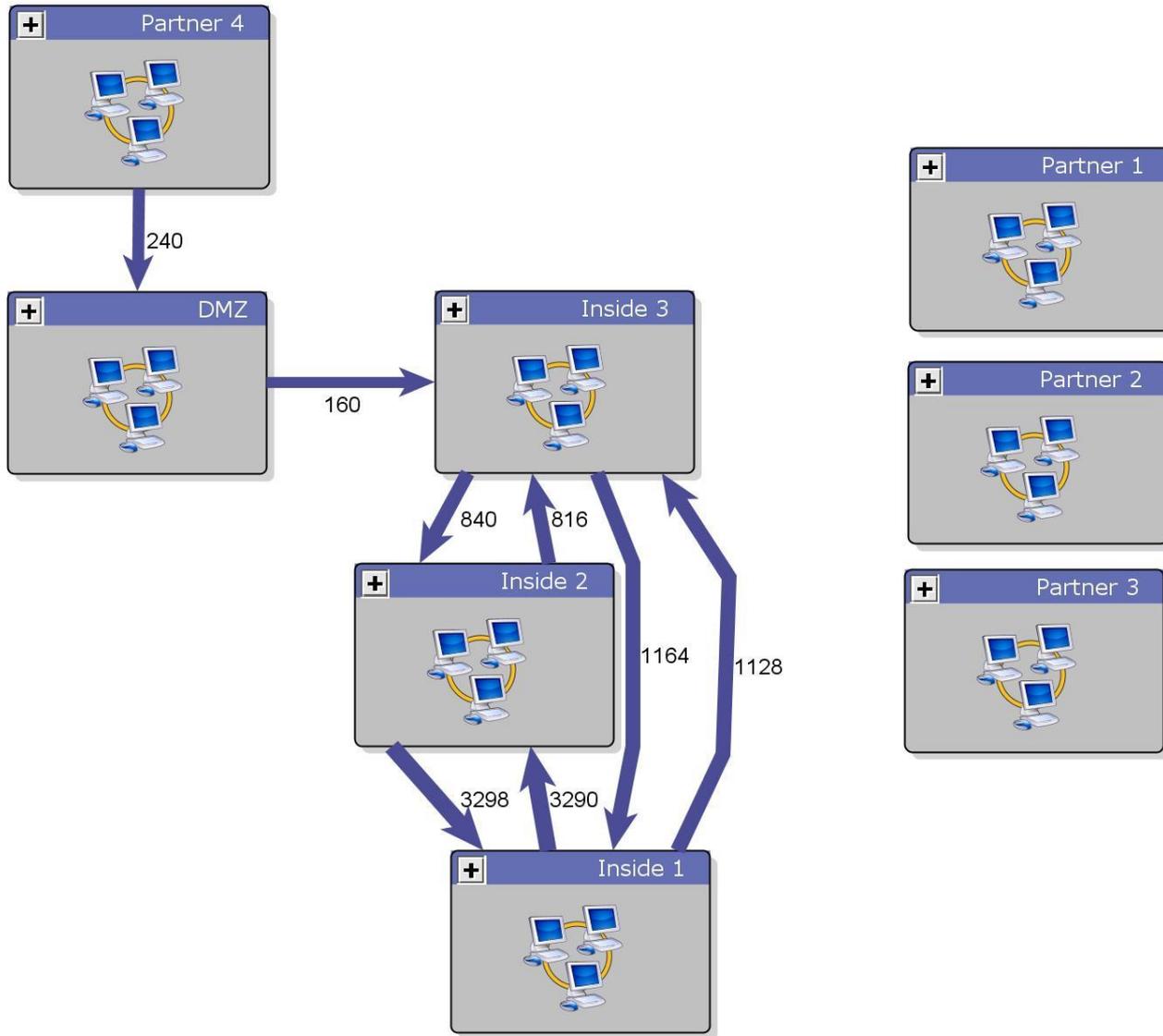
Example Network Topology



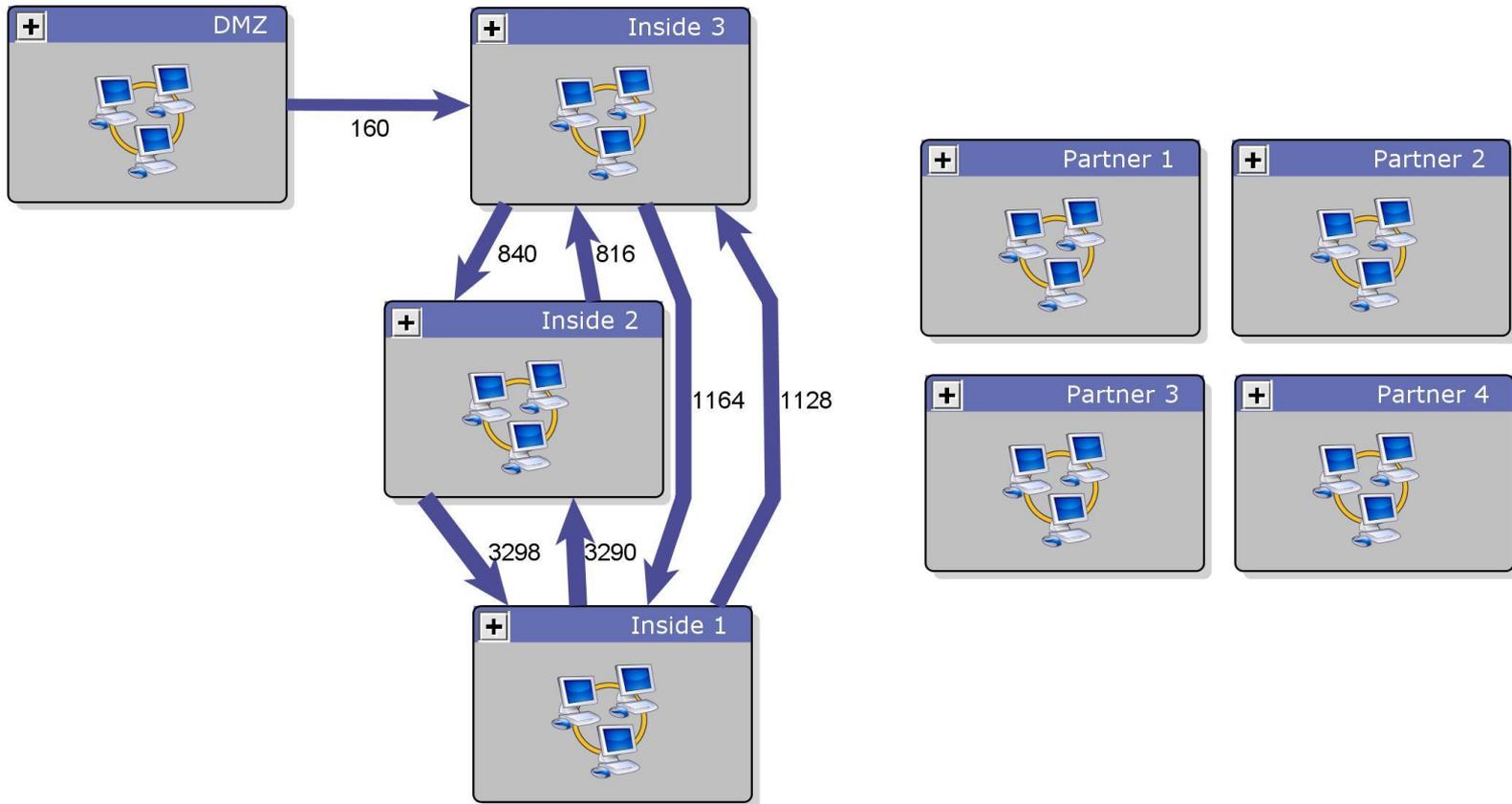
Attack Graph – No Hardening



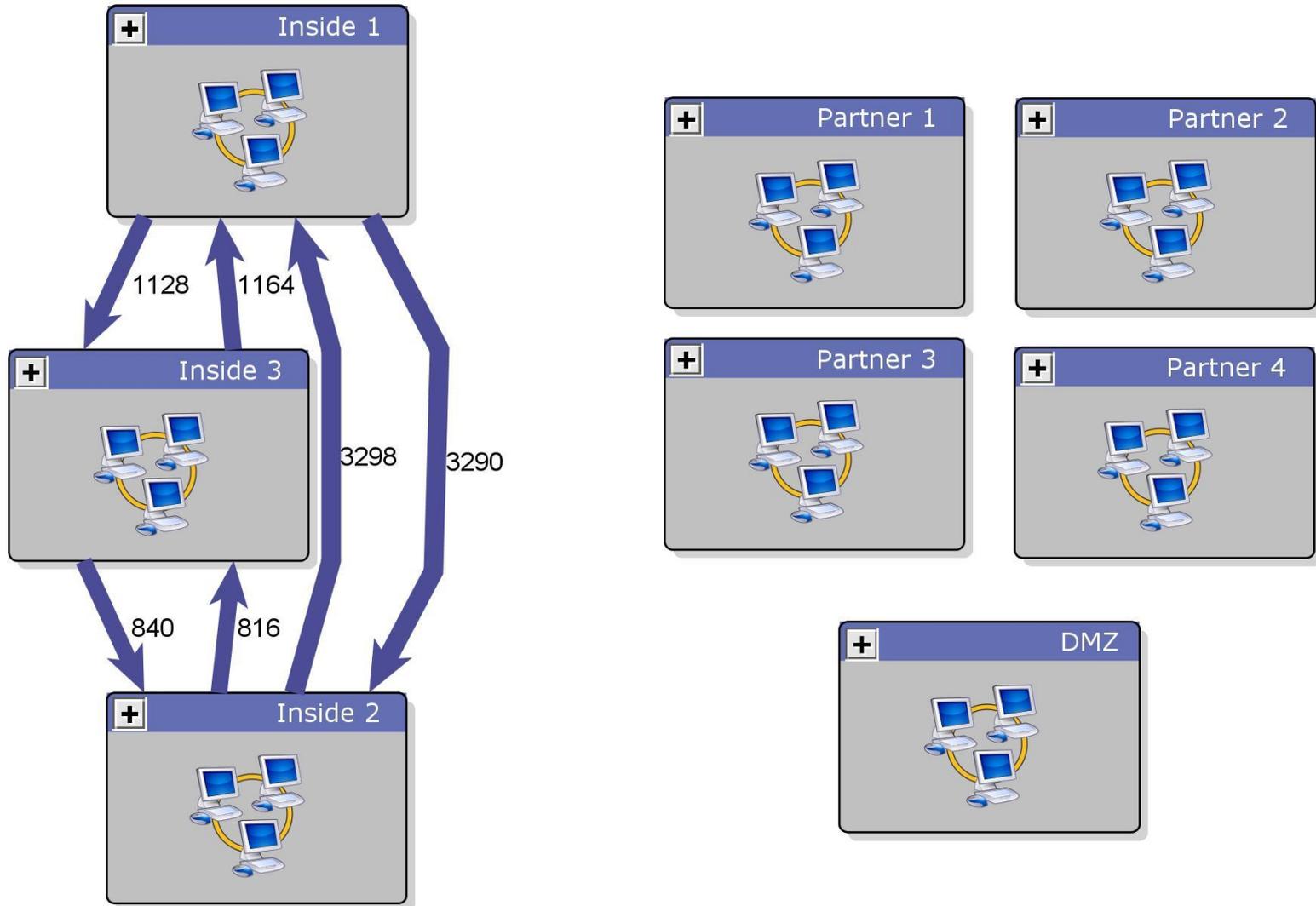
Block Partners to Inside



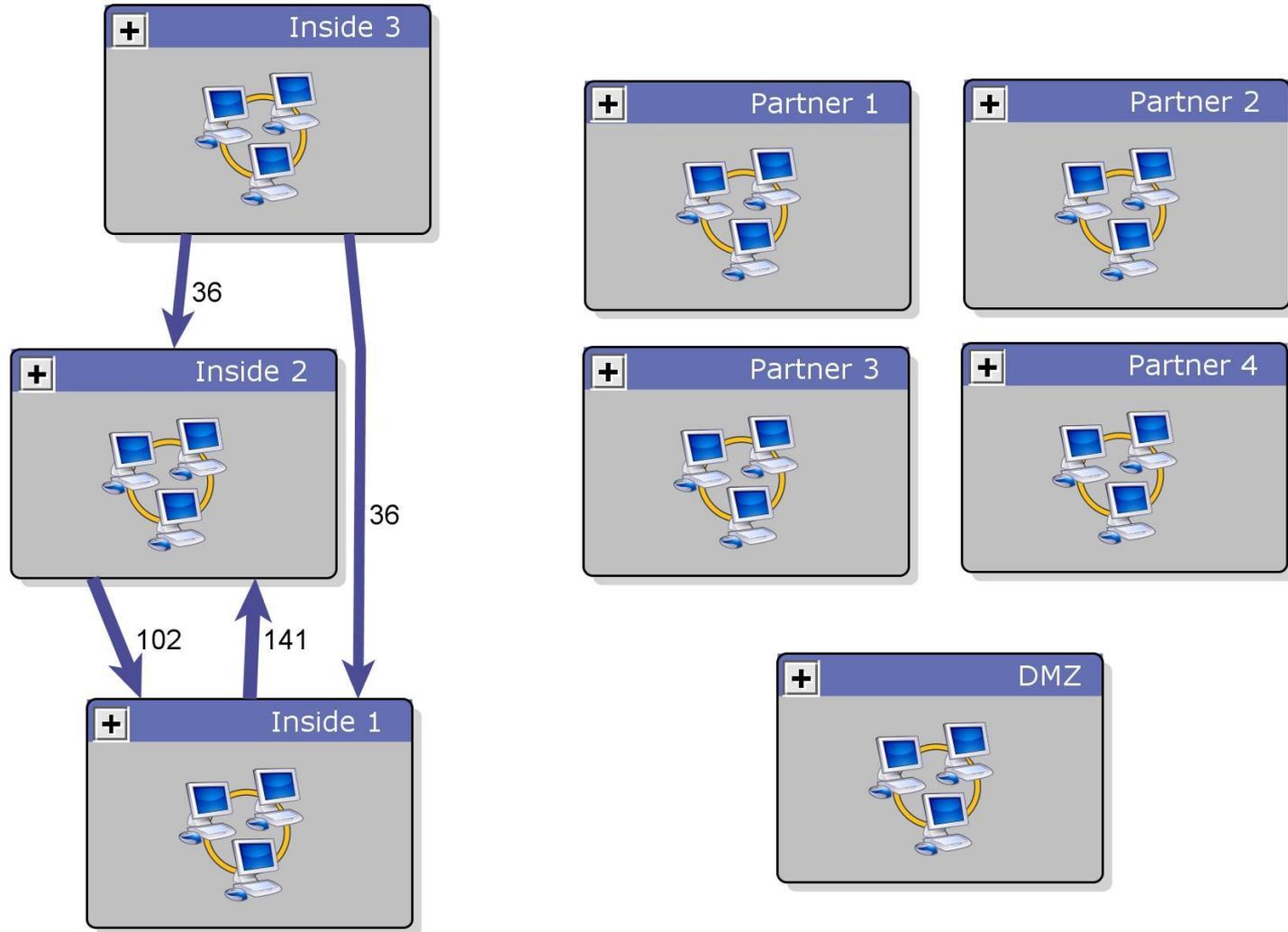
Block Partner 4 to DMZ

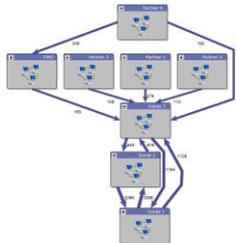


Block DMZ to Inside 3



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 ?

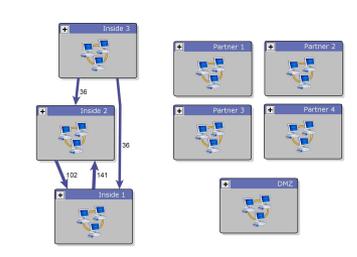
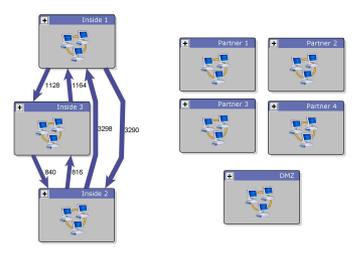
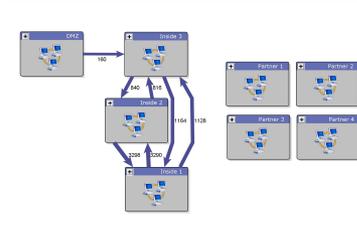
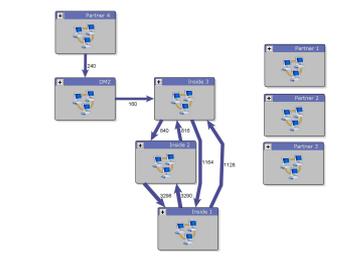
3.15 ↓ 5.59 (63%)

.65 until acceptable (26% reduction)

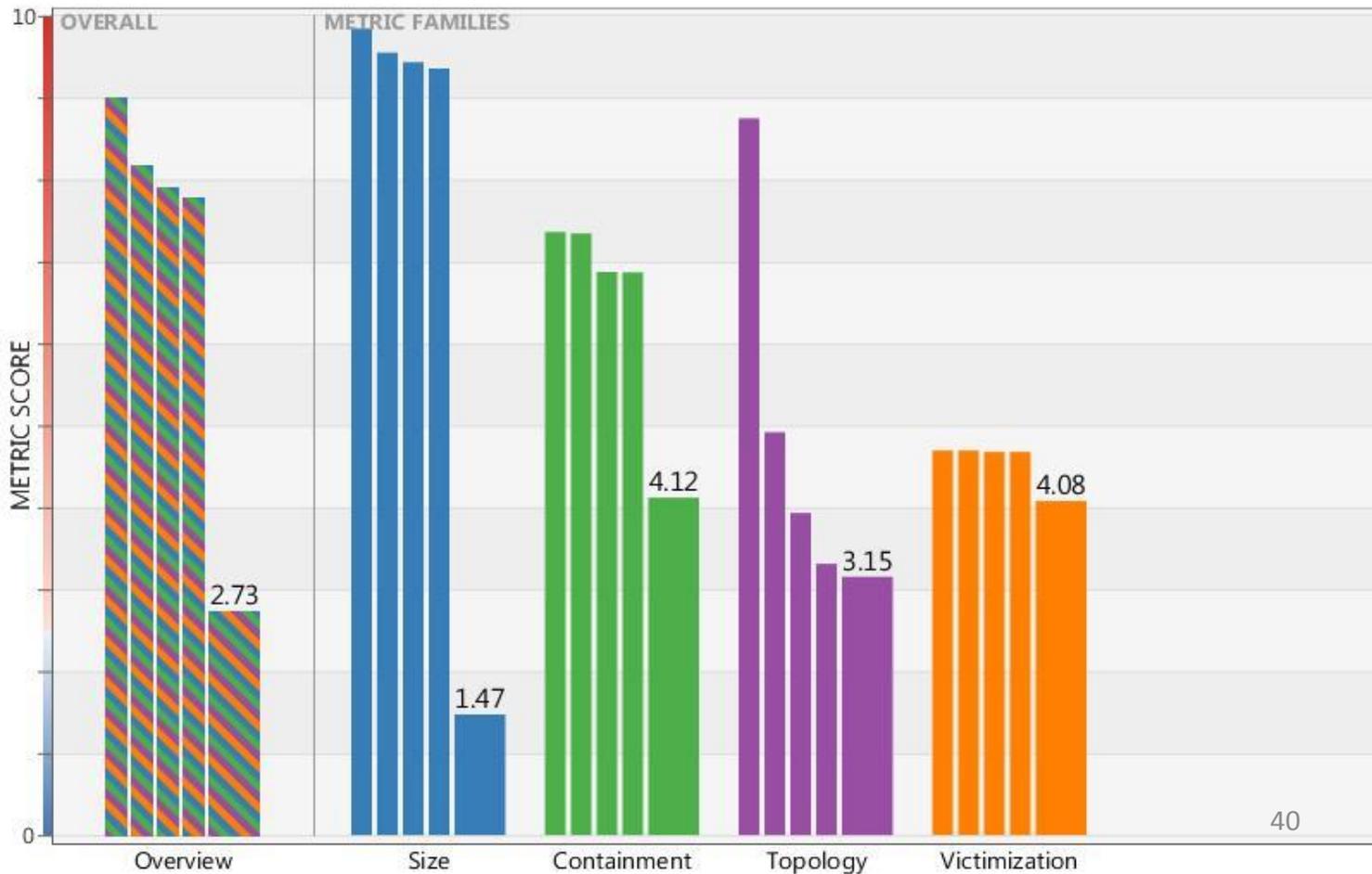
Victimization ?

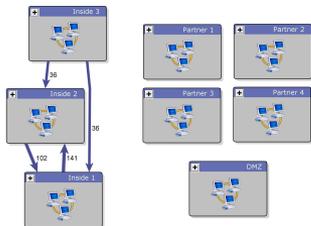
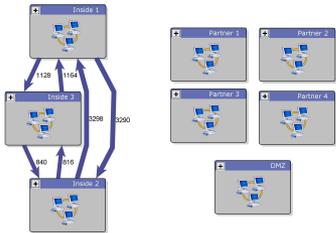
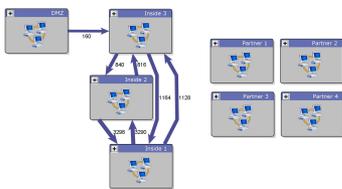
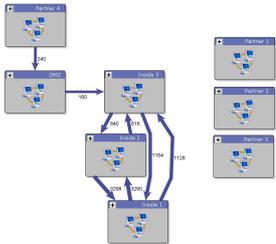
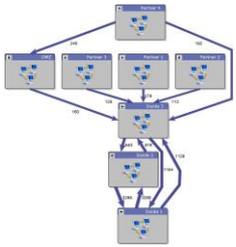
4.08 ↓ .62 (13%)

1.58 until acceptable (63% reduction)



Metric families over time





OVERALL WEIGHTING METRICS

Size ⓘ
 1.03 below acceptable
 (41% increase)

80.00%

1.47 ↓ 8.37 (85%)

20.00%

Attack Vectors ⓘ
 1.94 below acceptable
 (77% lower)

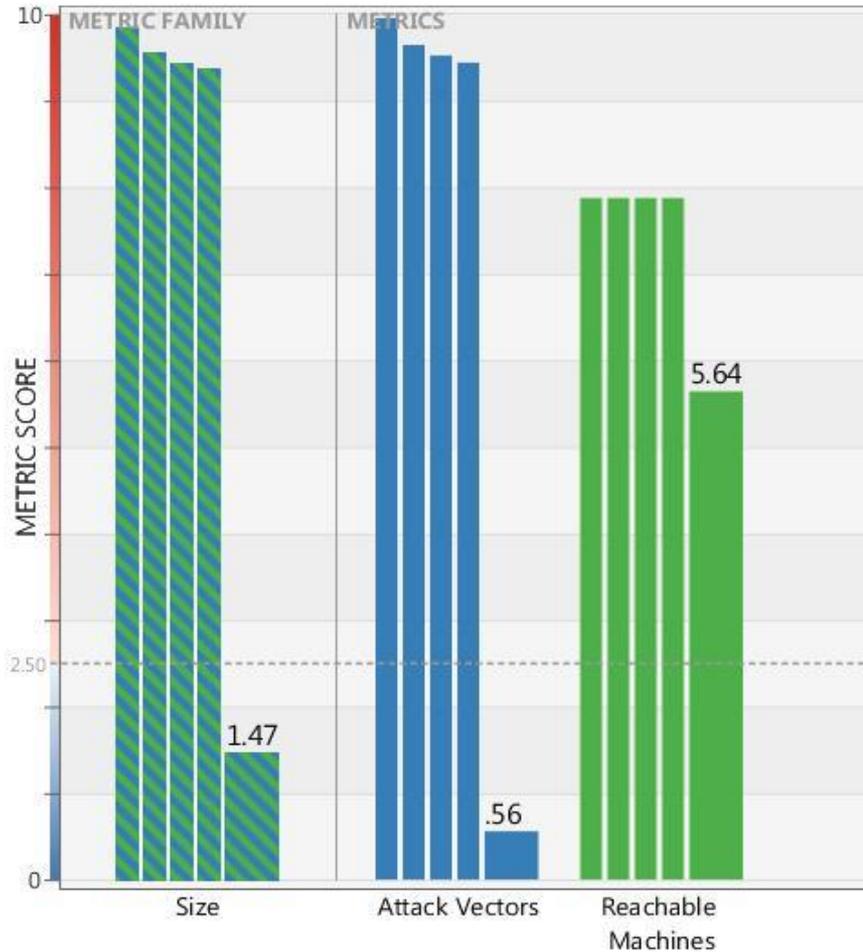
.56 ↓ 9.40 (94%)

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 ?

4.12 ↓ 3.24 (44%)

1.62 until acceptable (64% reduction)

50.00%

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)

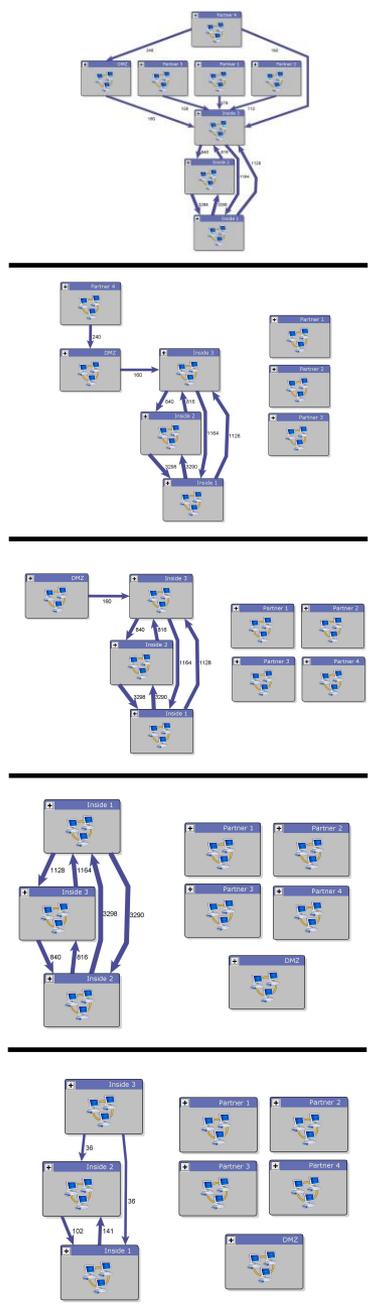
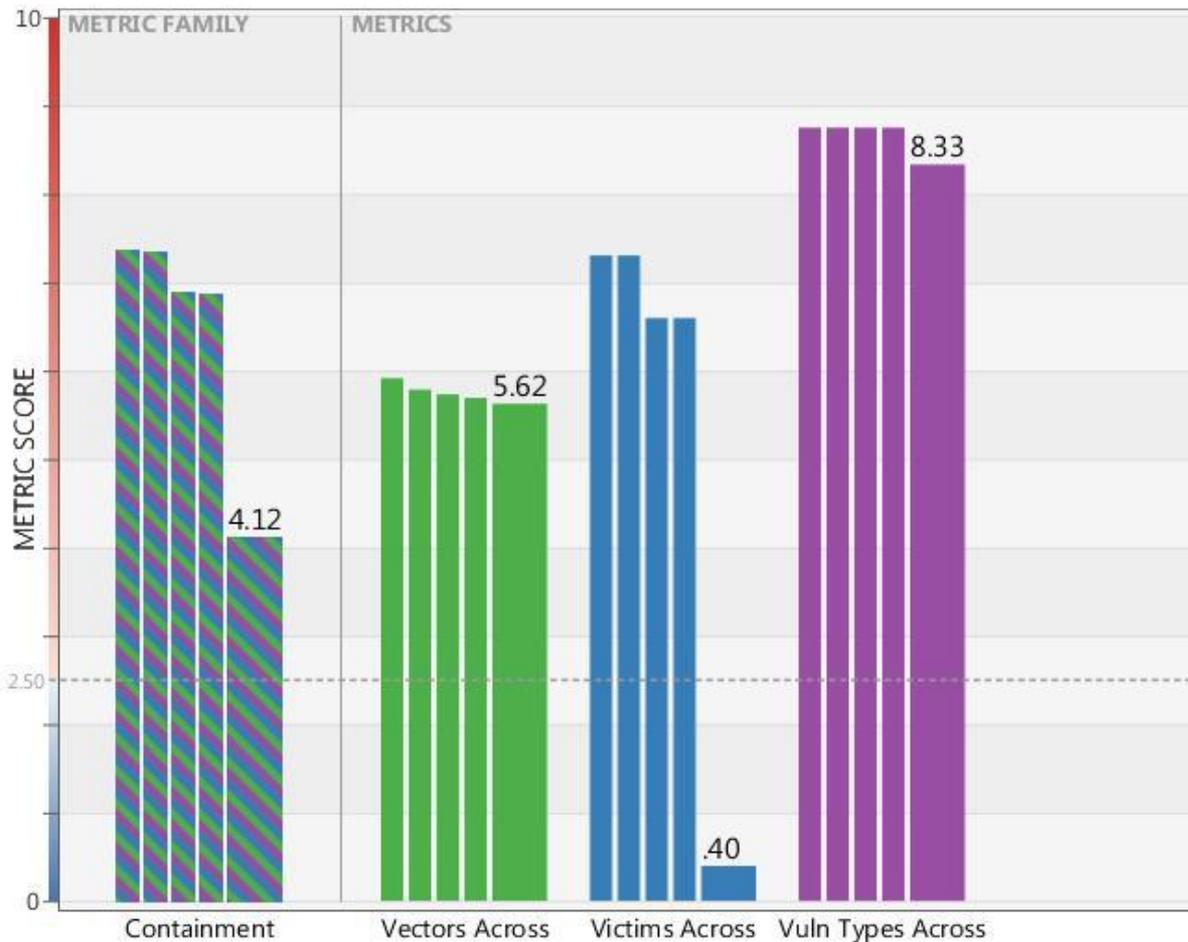
Vuln Types Across ?

8.33 ↓ .42 (4%)

5.83 until acceptable (233% reduction)

← Back to Metric Families

Containment metrics over time



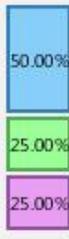


OVERALL WEIGHTING METRICS

Topology ?

3.15 ↓ 5.59
(63%)

.65 until acceptable
(26% reduction)



Connectivity ?

2.86 ↓ 7.14
(71%)

.36 until acceptable
(14% reduction)

Cycles ?

1.07 below acceptable
(42% lower)

1.43 ↓ 1.43
(50%)

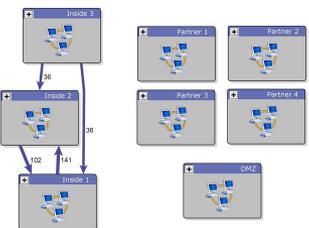
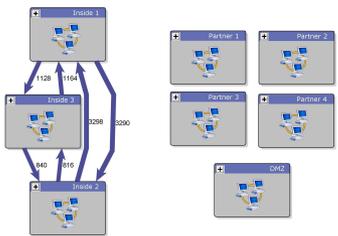
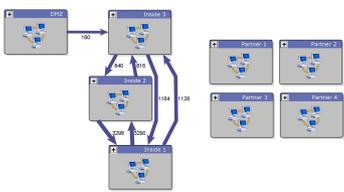
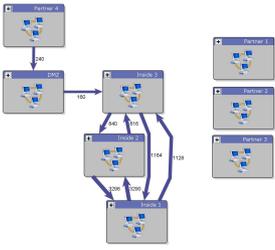
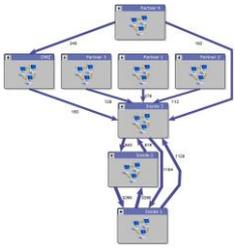
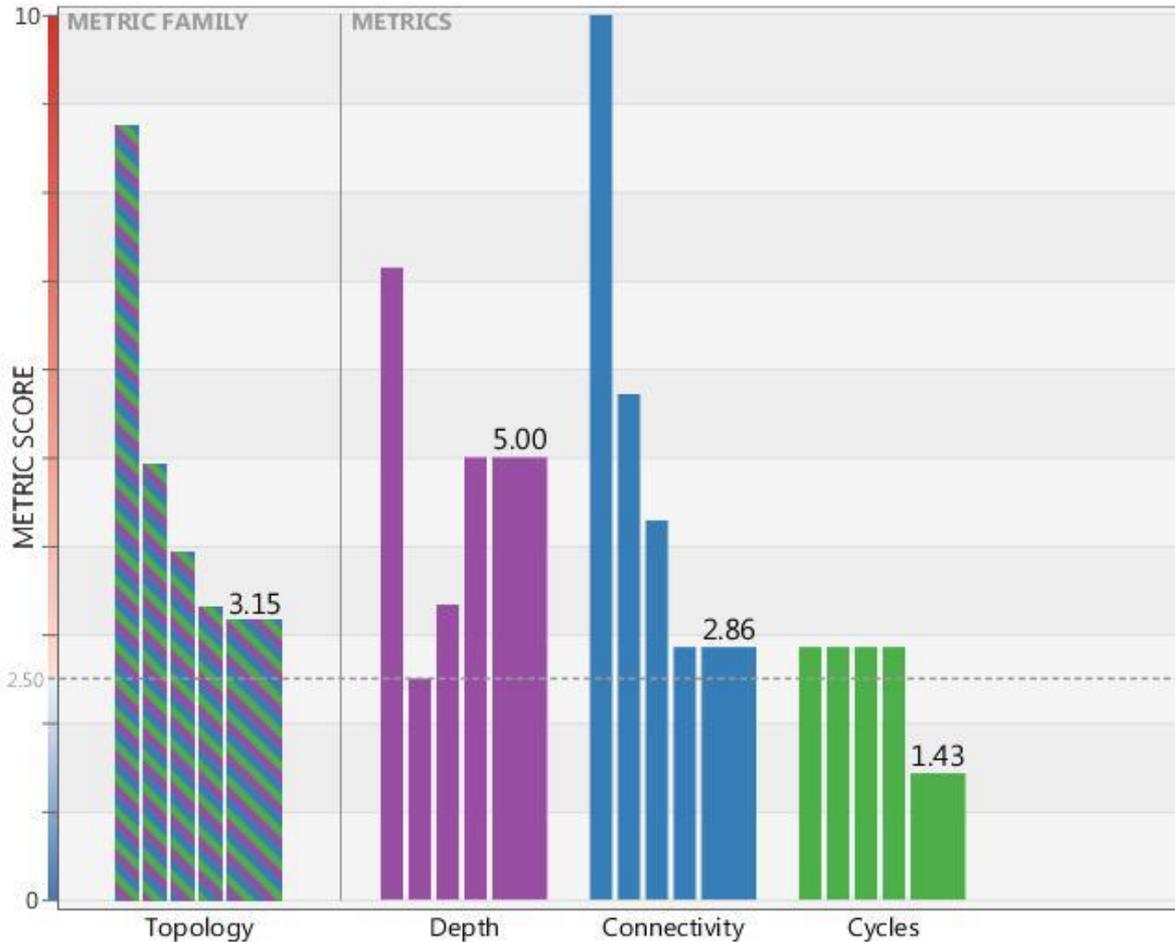
Depth ?

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)

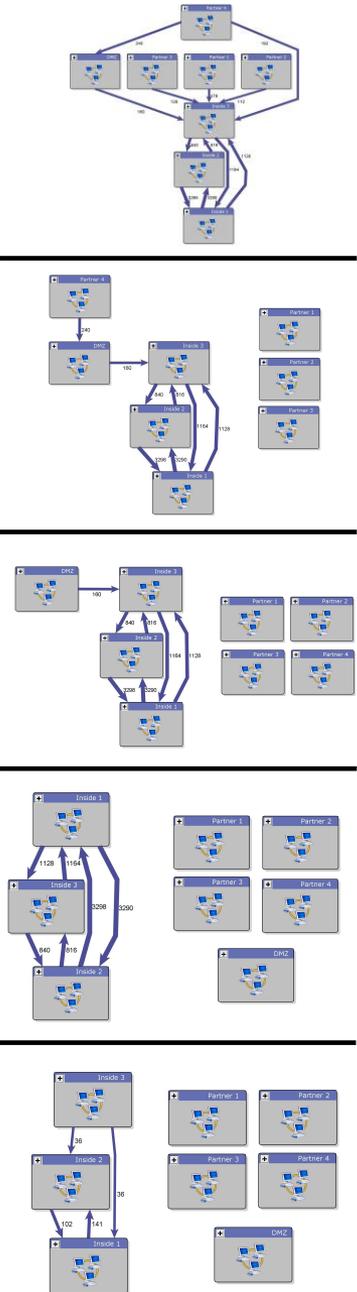
Impact ?

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

MITRE