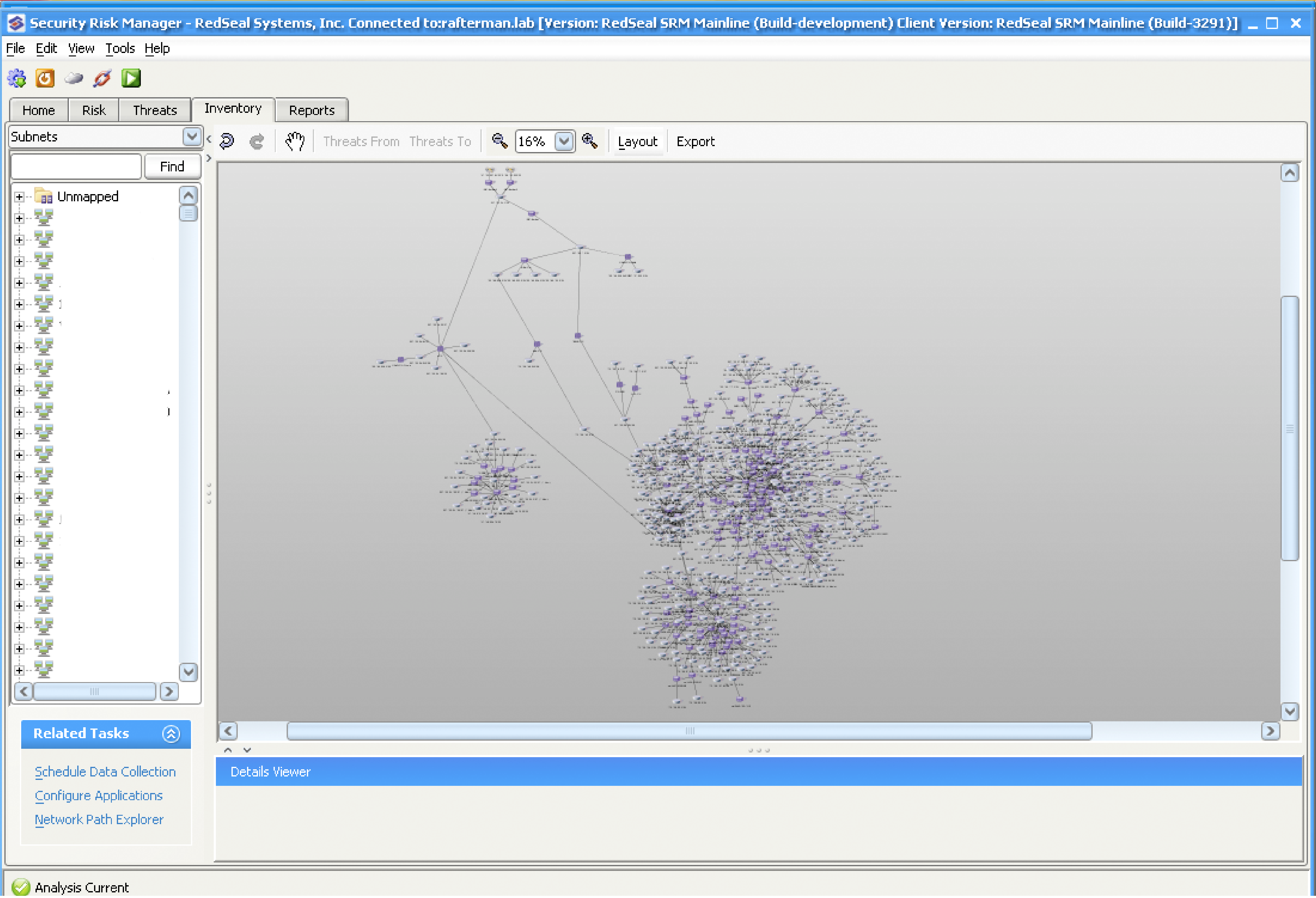
SECURITY RISK METRICS: THE VIEW FROM THE TRENCHES

Alain Mayer
CTO, RedSeal Systems
Alain@RedSeal.net

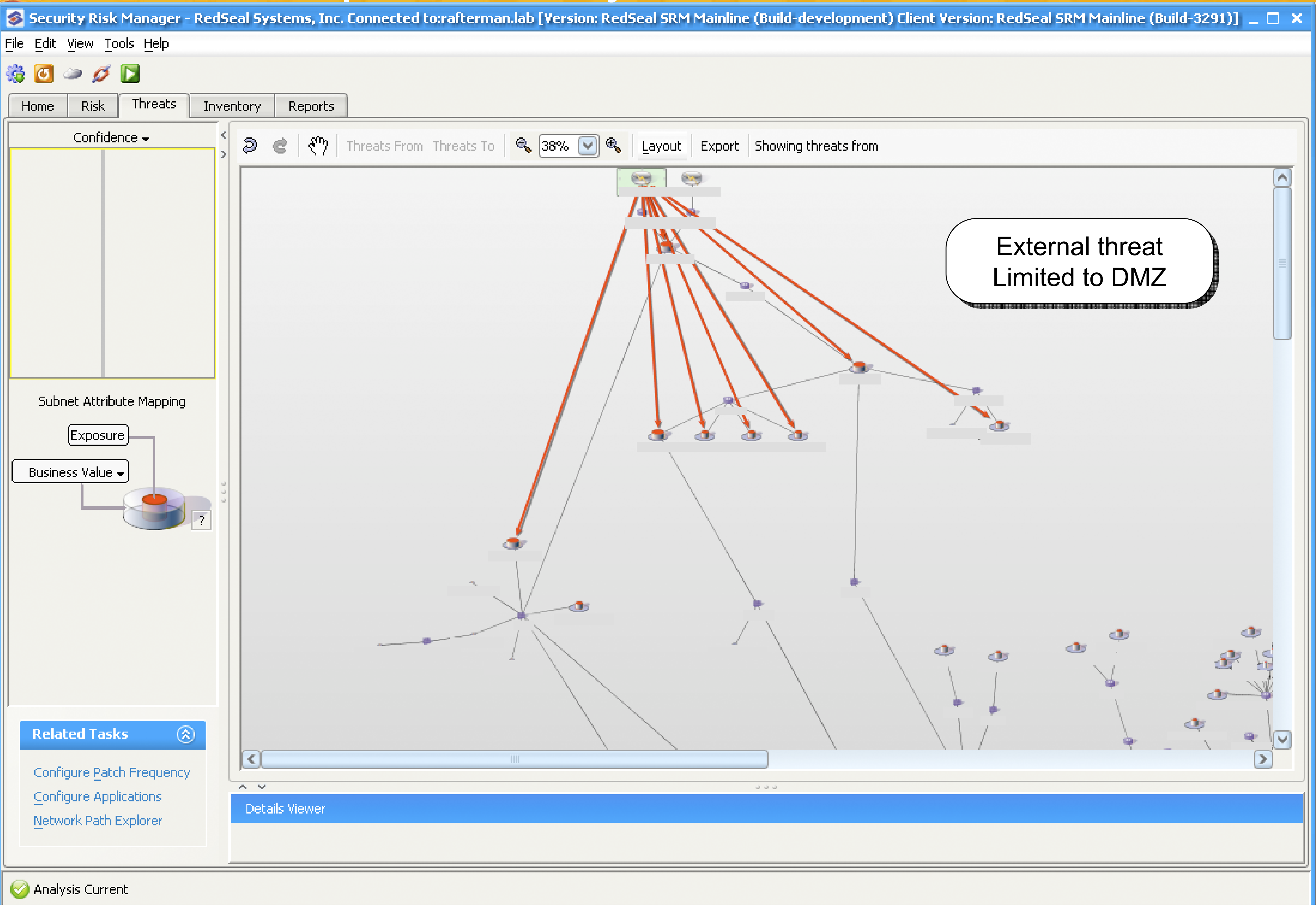
Security Defects

- Defects
  - Vulnerabilities on applications, OS, embedded systems
  - Un-approved applications
  - Outdated software
  - Mis-configuration of network devices, such as firewalls, routers, load balancers

- Defects cause
  - Business Risk
  - Policy Violations
  - Compliance Failures


Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]
File Edit View Tools Help
Home
Risk
Threats
Inventory
Reports
Subnets
Find
Unmapped
Threats From
Threats To
16%
Layout
Export
Related Tasks
Schedule Data Collection
Configure Applications
Network Path Explorer
Details Viewer
Analysis Current

Threat Graph: Security Defect Manifestation



Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]

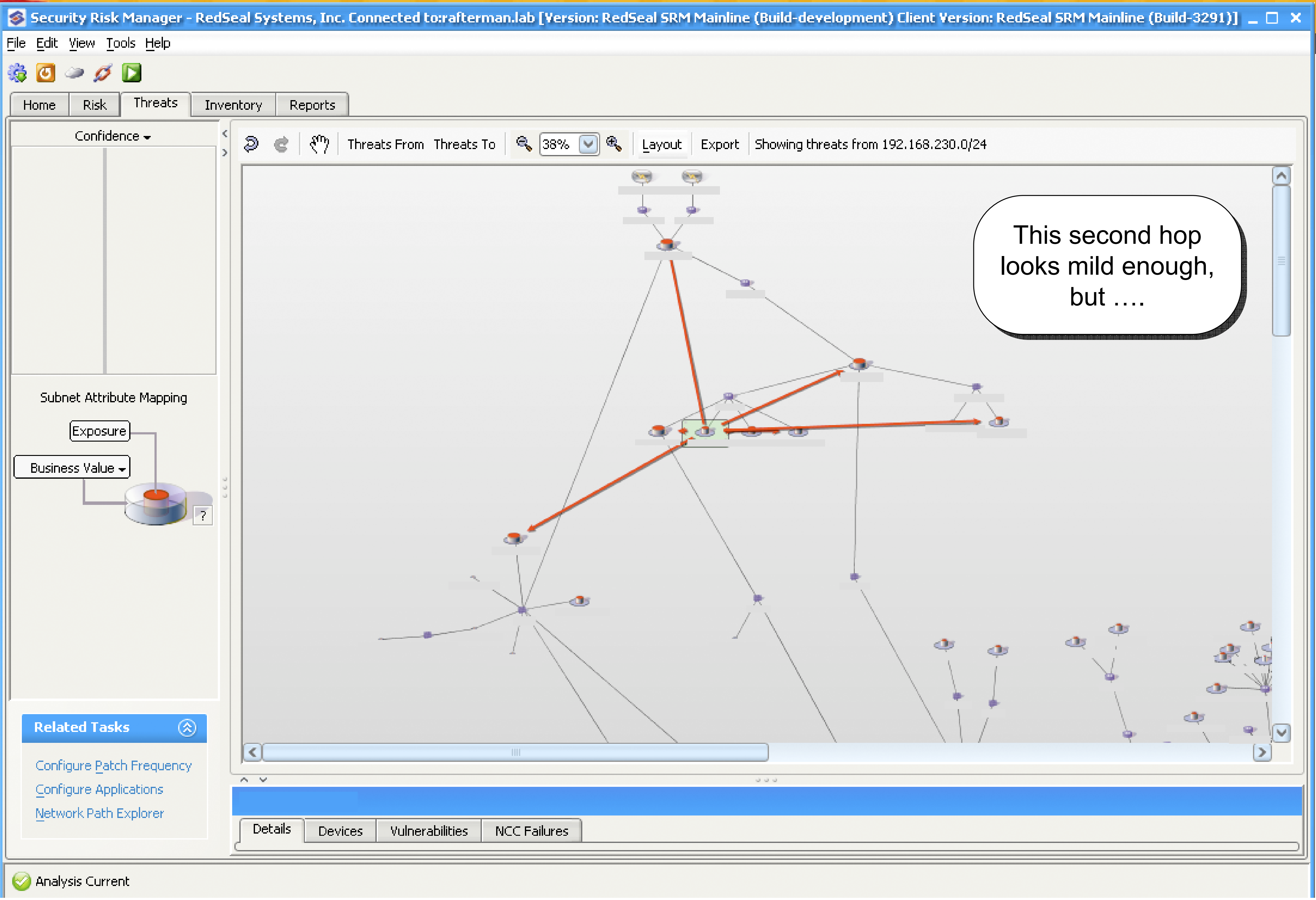
Zoom: 38%

Showing threats from

Analysis Current

External threat
Limited to DMZ

Threat Graph: Security Defect Manifestation

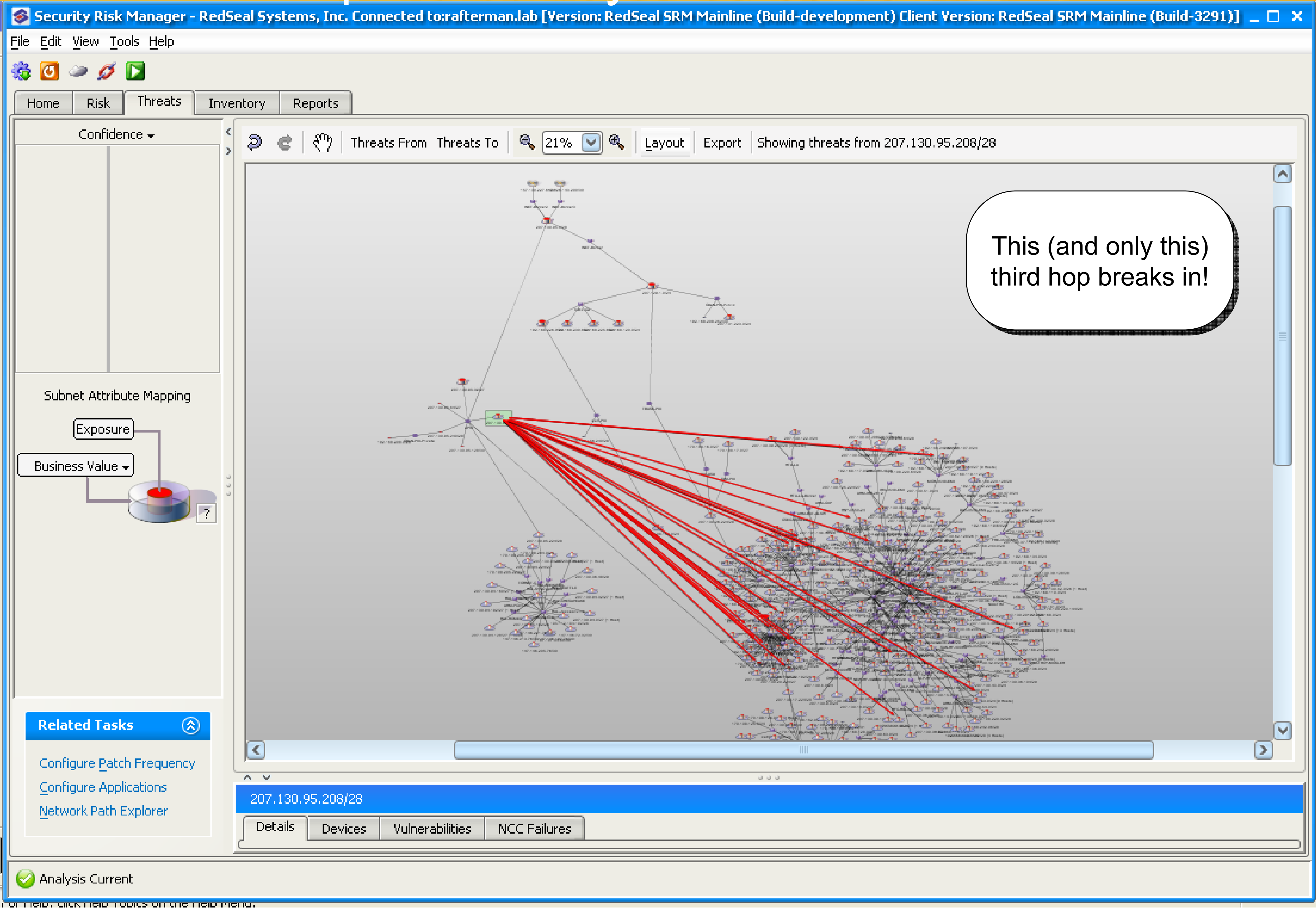


Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]
File Edit View Tools Help
Home Risk Threats Inventory Reports
Confidence
Threats From Threats To
38%
Layout Export
Subnet Attribute Mapping
Exposure
Business Value
?
Related Tasks
Configure Patch Frequency
Configure Applications
Network Path Explorer
Details Devices Vulnerabilities NCC Failures
Analysis Current

Showing threats from 192.168.230.0/24

This second hop looks mild enough, but ….

Threat Graph: Security Defect Manifestation



Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]

Showing threats from 207.130.95.208/28

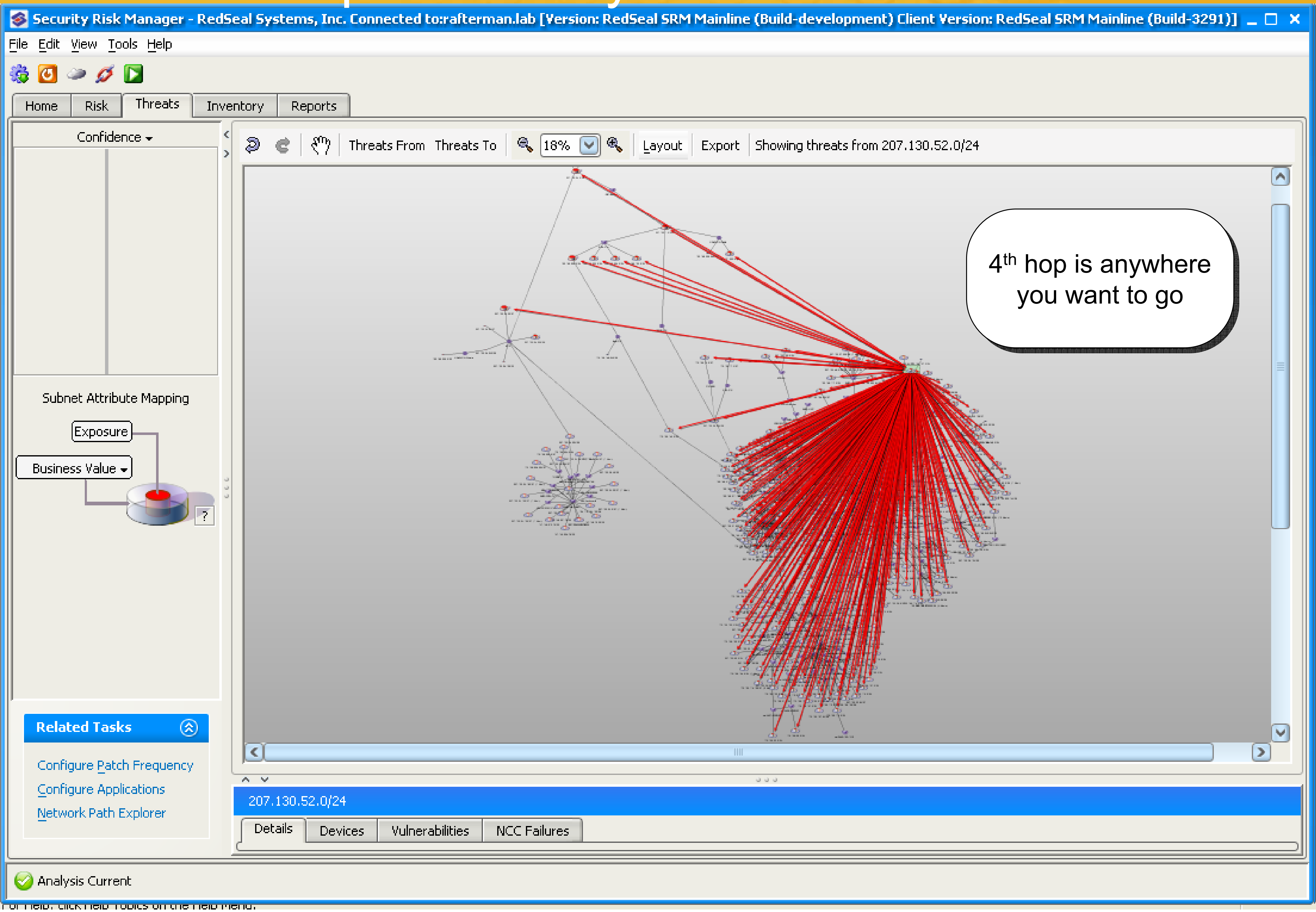
207.130.95.208/28

Analysis Current

For Help, click Help Topics on the Help menu.

This (and only this) third hop breaks in!

Threat Graph: Security Defect Manifestation



Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]

Showing threats from 207.130.52.0/24

207.130.52.0/24

Analysis Current

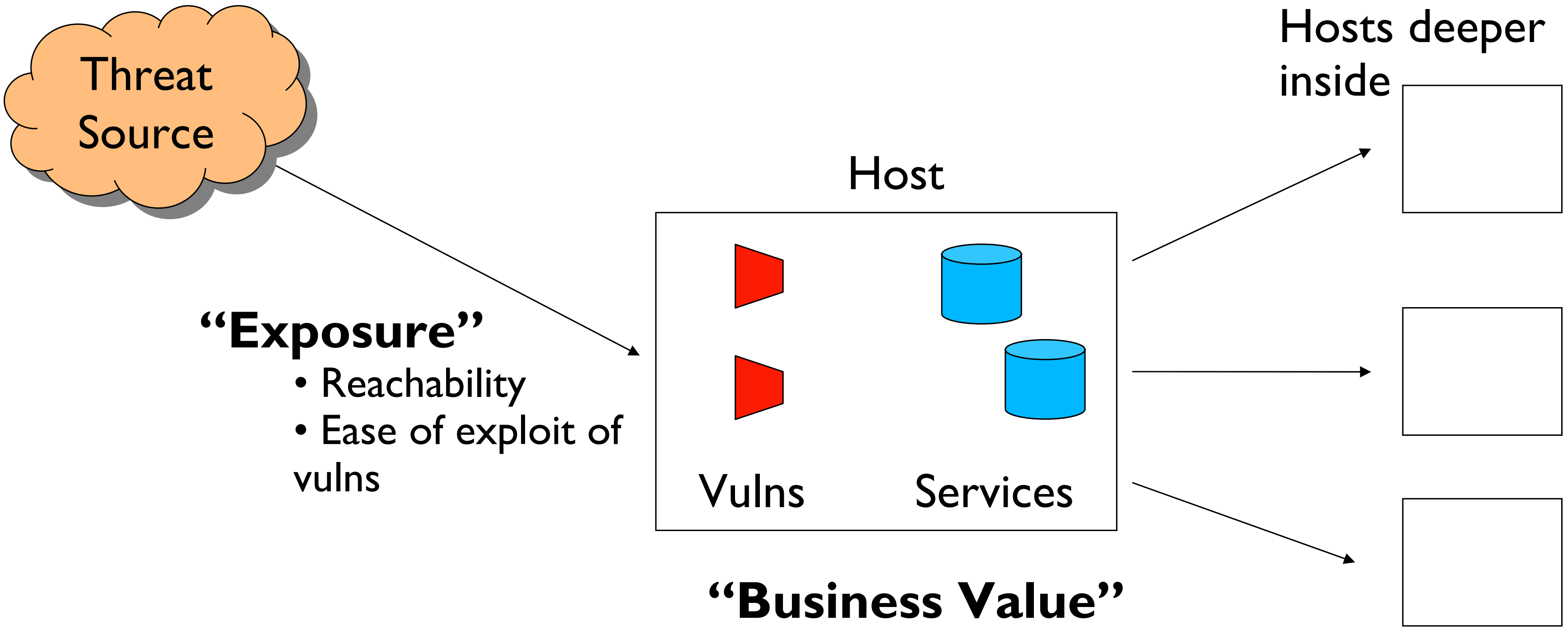
For Help, click Help Topics on the Help menu.

4th hop is anywhere you want to go

Metrics: Operational vs Infrastructural

- Operational: measure the business impact of defects
  - Results in a priority ranking.
  - Objective: Effectively deploy IT resources on highest ranked defects.
- Infrastructural: measures an aspect of the state of the IT infrastructure
  - Properties of the threat graph, network configurations, etc
  - Objective: Characterize IT security stance, Comparative(?)

Operational Metrics



"Exposure"

- Reachability
- Ease of exploit of vulns

"Business Value"

- Default is highest value service

"Risk"

- Exposure X Business Value

"Downstream Risk"

- Cumulative Risk over hosts attackable from here

Infrastructural Metrics

Threat Graph Metrics

1. Longest threat graph path (Max Path)
   - Proxy for the depth of defense
2. Threat graph coverage (Coverage)
   - Fraction of hosts in the threat graph viz all hosts
   - Indicator for the breadth of defense
3. Attack surface ratio (Surface)
   - Fraction of hosts that when patched (or any other o their defects fixed) will remove the whole threat map.
   - Indicator for the quality of the DMZ design
   - Indicator for the amount of mitigation work

Network Device Metric

1. Average device complexity (Complexity)
   - Average number of filtering elements per device

Collect Data for Infrastructural Metrics

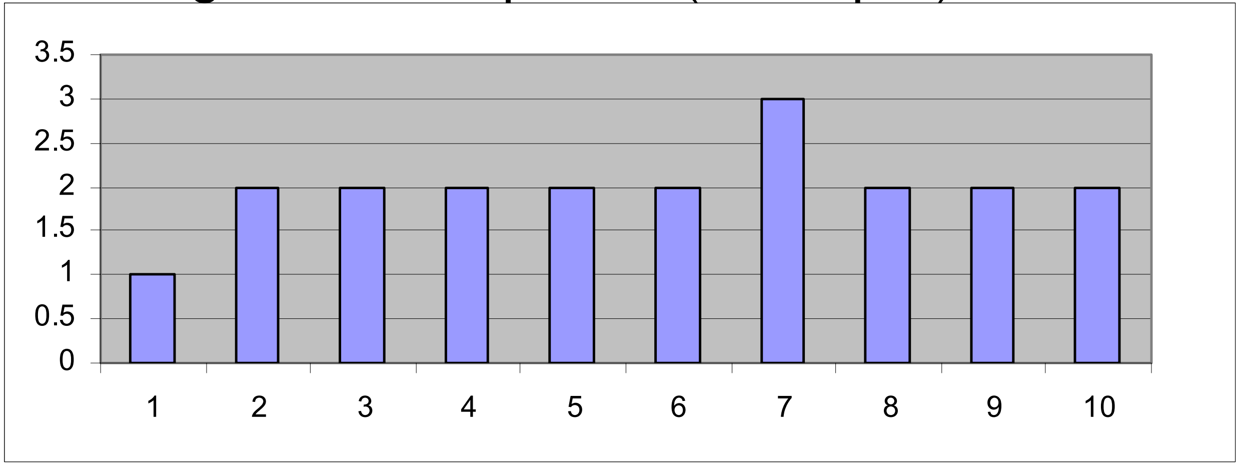
- Just ask!
- Obtained data during the evaluation (spot audit) of 14 prospects (now customers)
  - Representative sample
- Wide selection of verticals:
  - Health Care, Automotive, Financials, Online, etc.

- Threat Graph path lengths across our sample set
  - number of hops to take over all attackable hosts
  - depth of defense

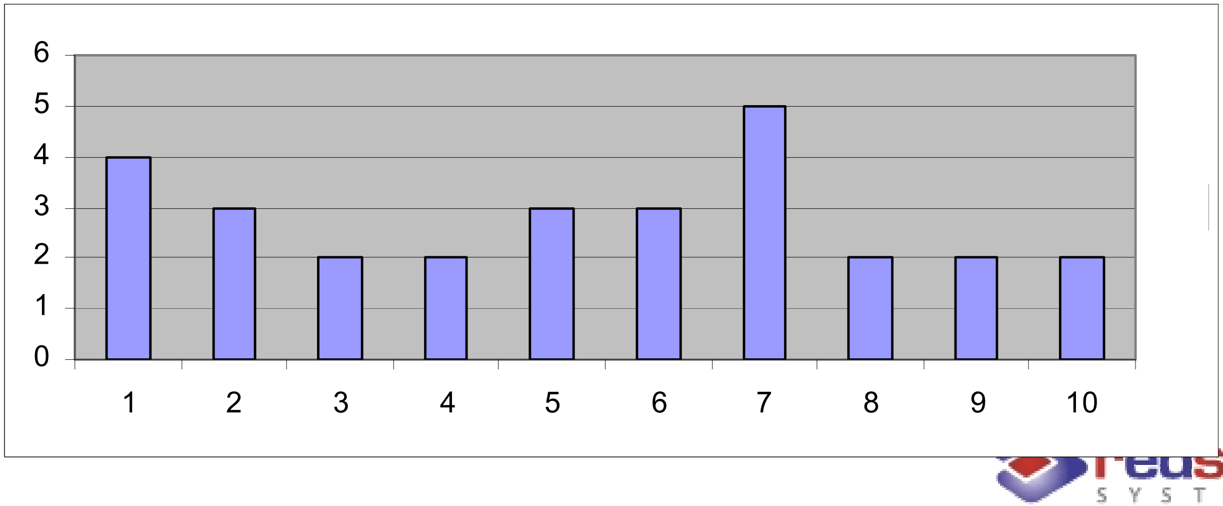
→ What is your guess relative to the earlier example??

Longest and Average Threat Graph Path

Average Threat Graph Path (10 samples)

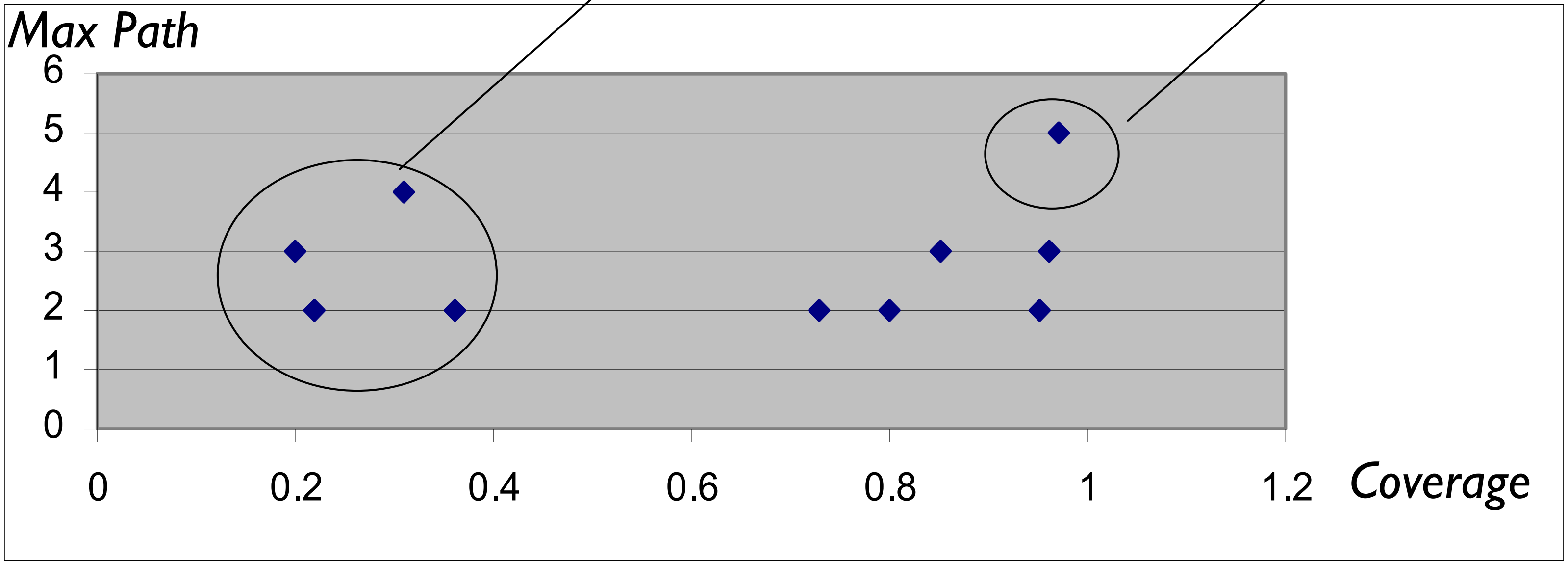


Longest Threat Graph Path (10 samples)



SURPRISED??

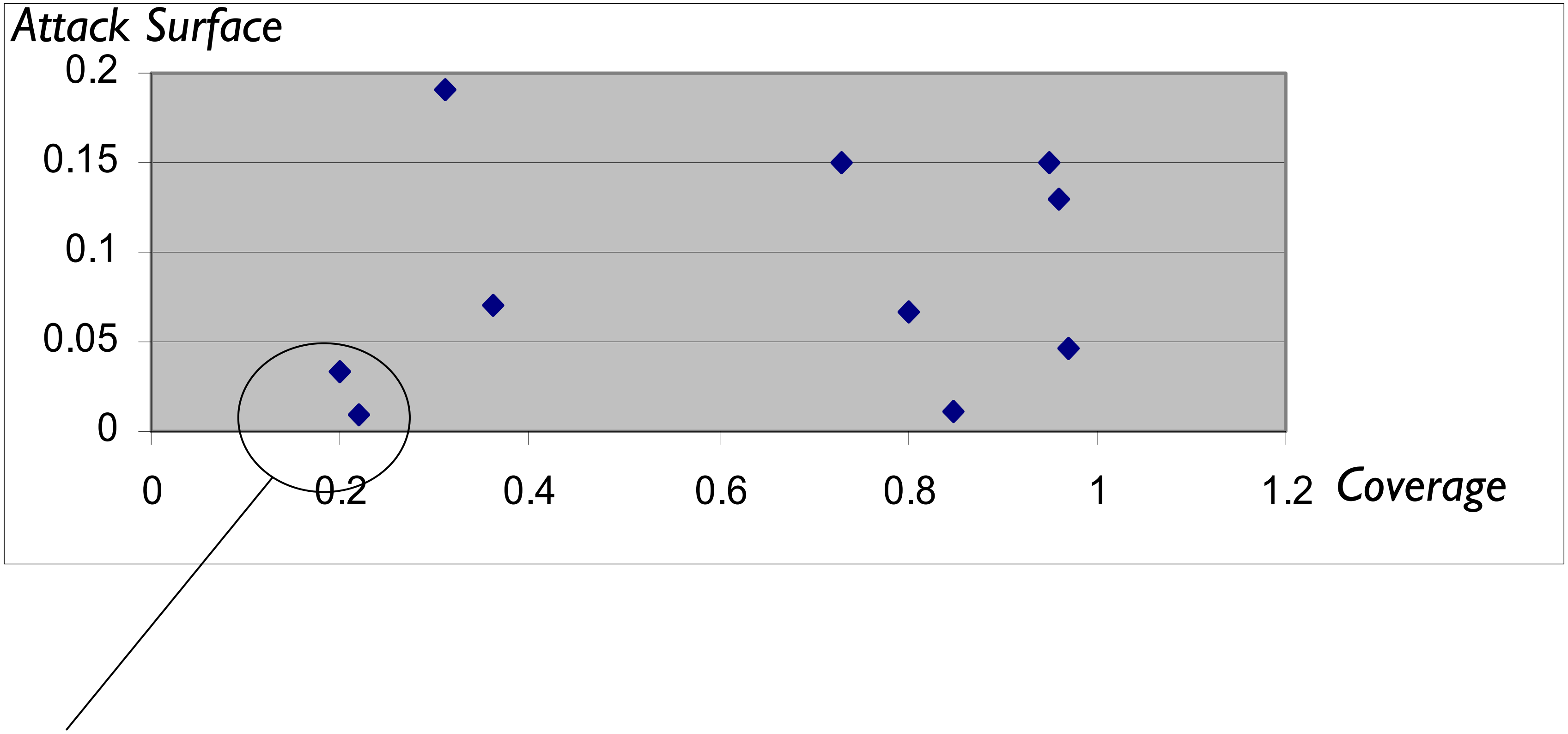
Max path vs coverage



>1/2 Hosts protected

Good Depth of Defense

Surface vs Coverage

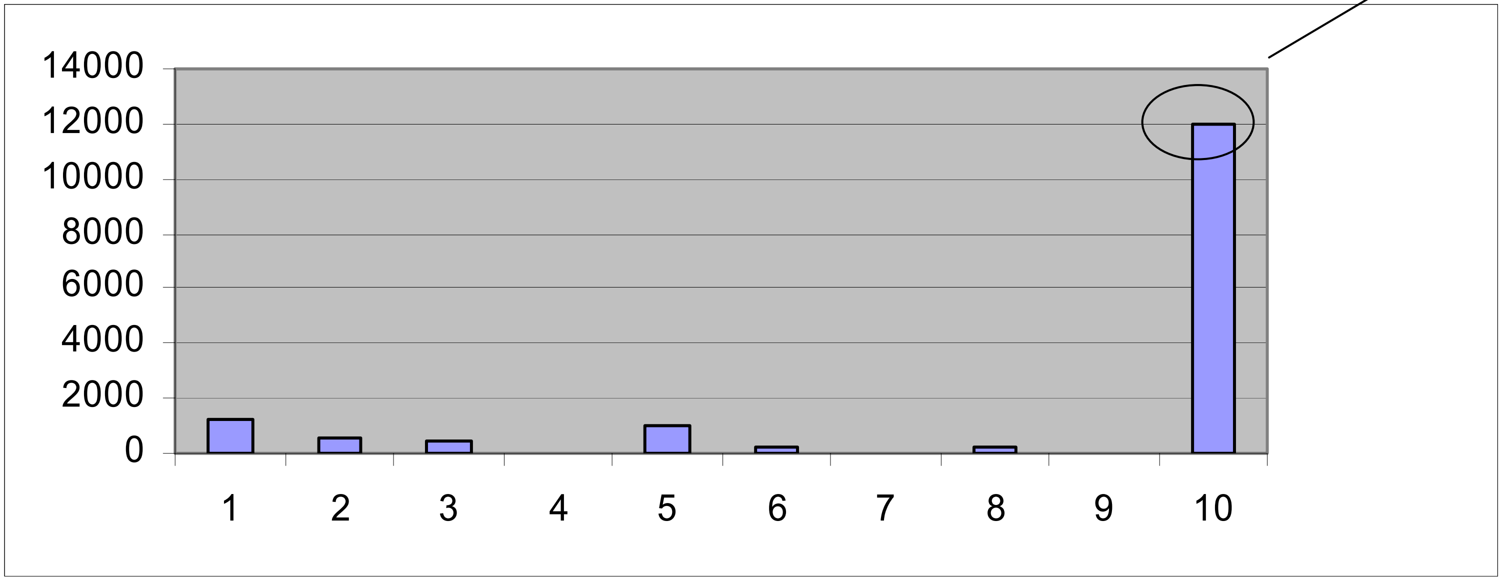


>75% of hosts are protected and easy to mitigate the rest

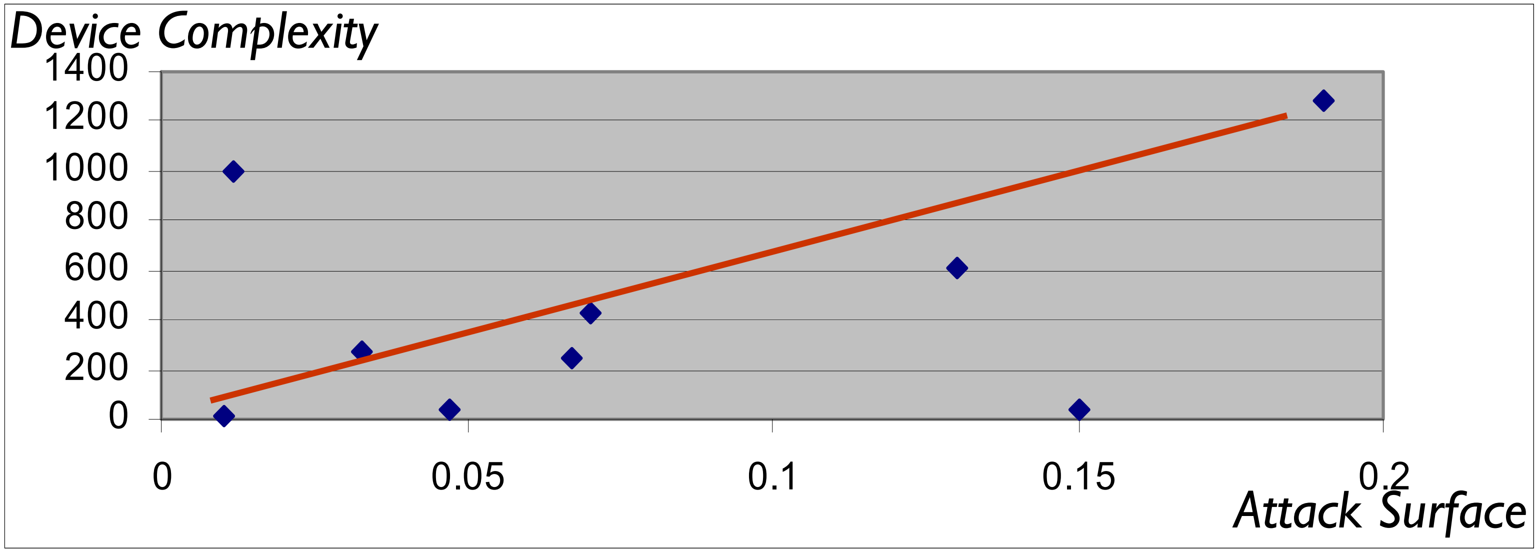
Average Device Complexity

Whoa

Average Device Complexity (10 samples)



Complexity vs attack surface



As the device complexity grows, the attack surface tends to grow too!

So…..

- Internal Segmentation … Like Bigfoot
  - Everybody has heard of it, but very few have seen it
  - Might change due to PCI Req 1?
    - Requires segments for card holder data, DMZ, wireless

So…

- Defects …..growing old in your infrastructure
  - Too many to fix them all…

[illegible]

So why?

- Security Silos
  - Rigidly patching only high-severity vulnerabilities might not remove defects with biggest risk impact
  - Firewall teams focused on enabling access for critical business systems
- Drift Happens!!
  - Even the best designed network does not stay that way (and not many are carefully designed to start with)
  - Frequent (sometimes daily) configuration changes eating away at the best intentions
- Complexity is not your Friend

So what?

- Understand risk by analyzing data across every aspect of your **entire infrastructure**.
- **Discover and rank** defects (i.e. vulnerabilities, misconfigurations, compliance failure, etc.) according to direct and indirect threat paths.
- **Coordinate the efforts** to patch, reconfigure, harden or re-architect based on fixing defects that pose the highest risk first.
- **Instantly assess** how changes will affect risk.