
# IT Risk – CVSS and Beyond

**Alain Mayer**

**CTO, RedSeal**

# IT Risk Management is Everywhere

- NIST
  - CVSS: Prioritized Risk
  - 800-30: Risk Management Guide for IT Systems
- Almost all security vendors have offering for IT Risk
  - McAfee Risk Advisor
  - Symantec Risk and Compliance
  - RSA Risk Management
  - Qualys IT Security Risk and Compliance

# CVSS


**Prioritized Risk**: When the environmental score is computed, the vulnerability now becomes contextual. That is, vulnerability scores are now representative of the actual risk to an organization. Users know how important a given vulnerability is in relation to other vulnerabilities.



RedSeal

# 800-30

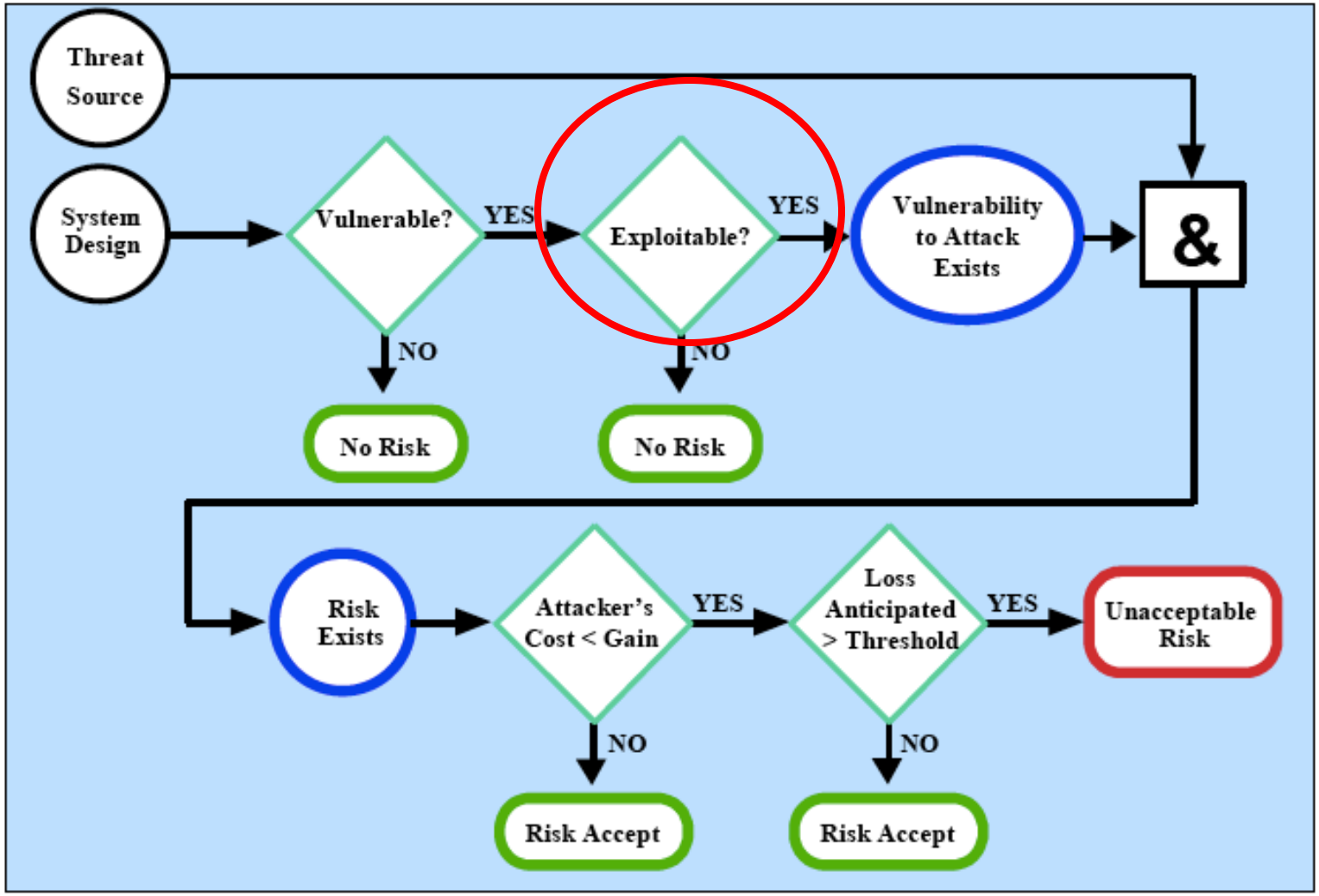
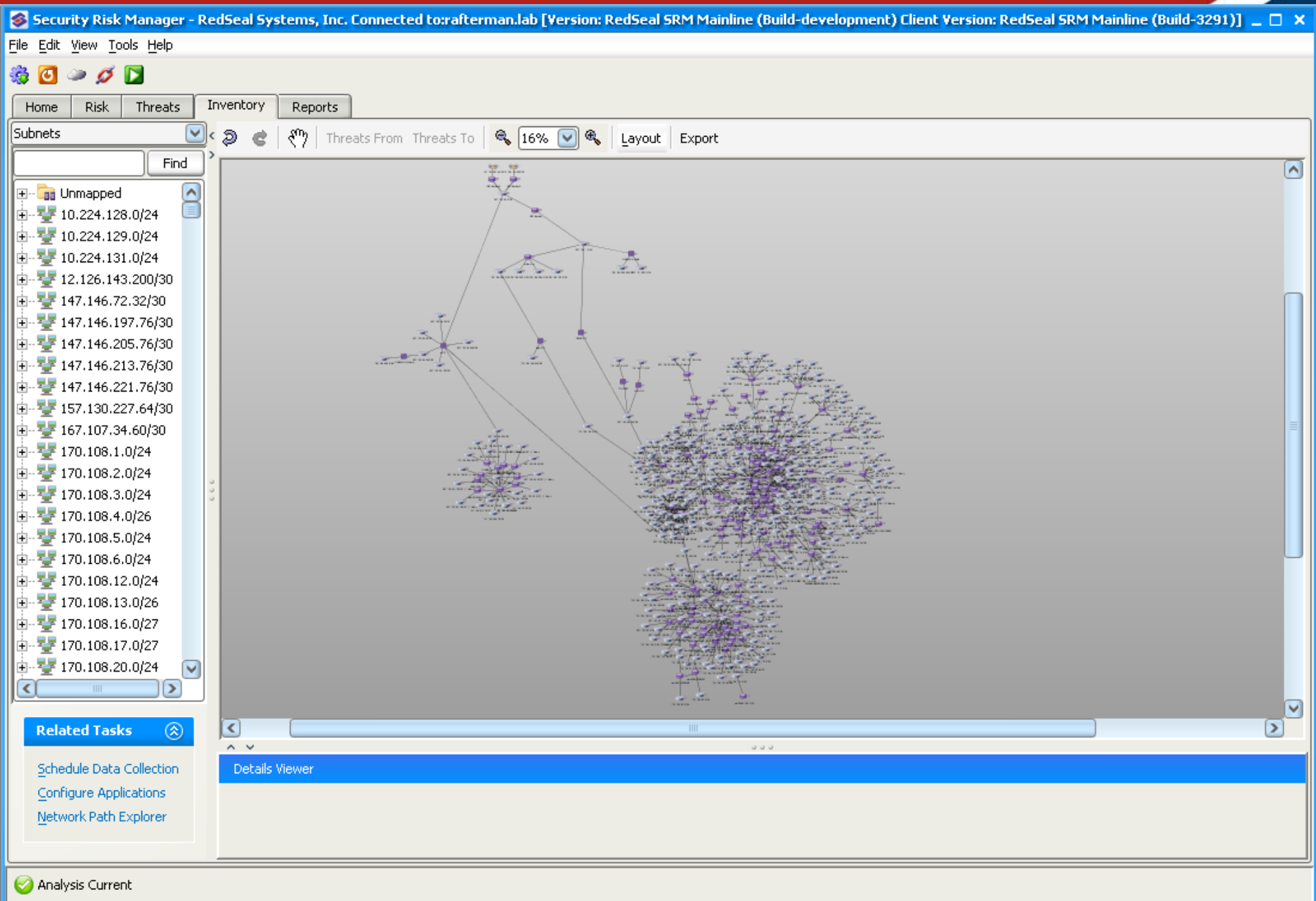
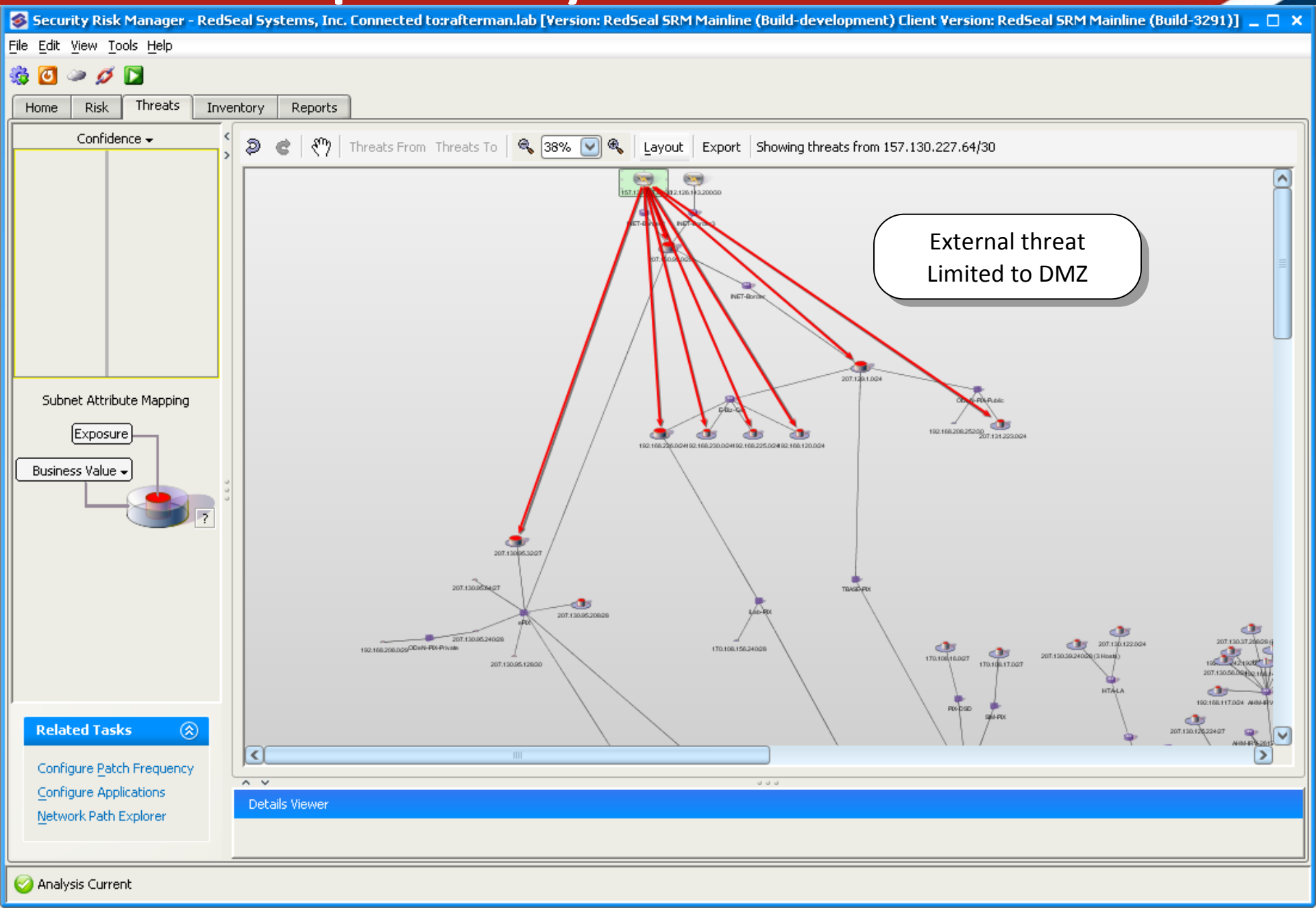



**Figure 4-1. Risk Mitigation Action Points**

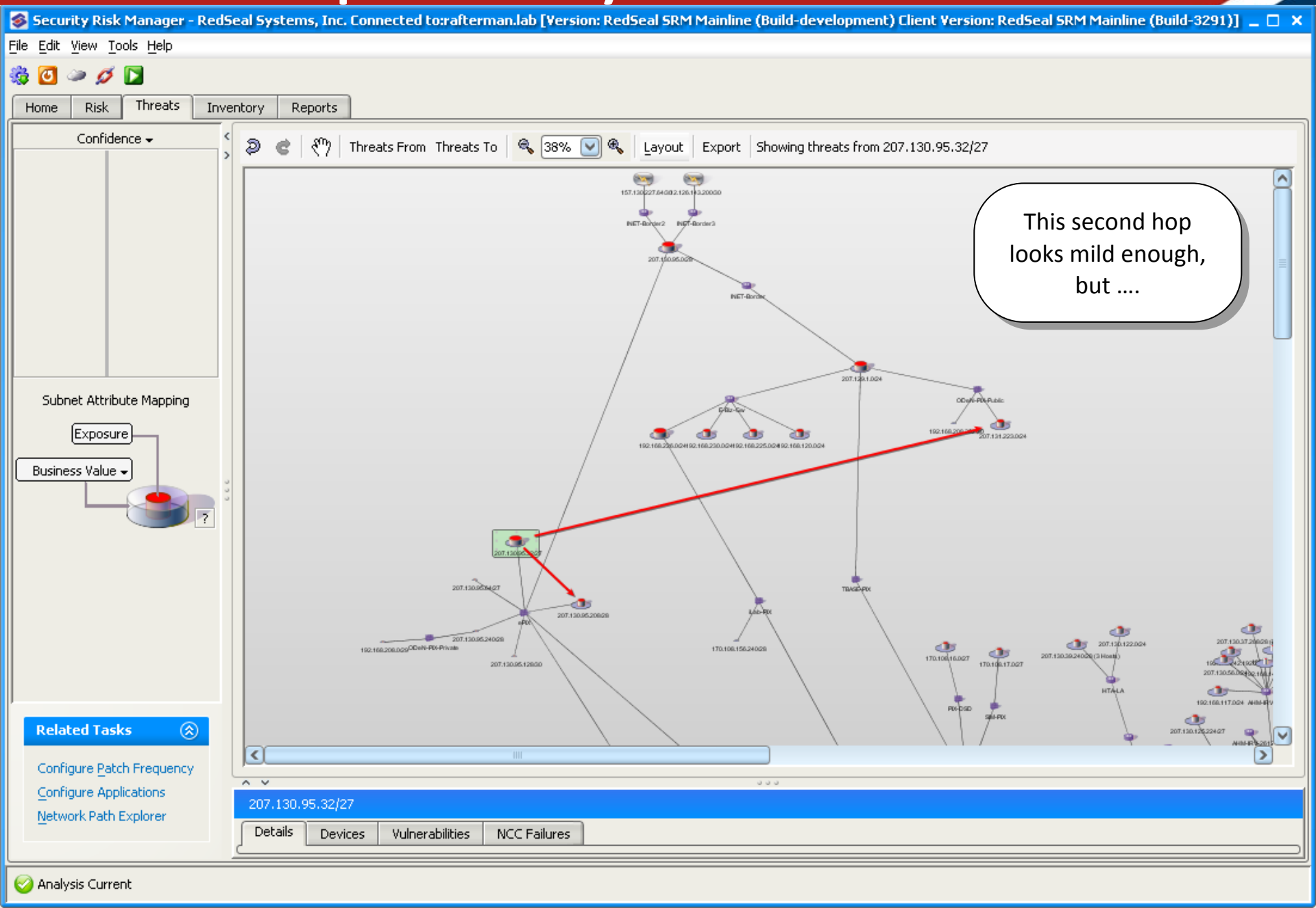
# Risk-based on Attack Graph



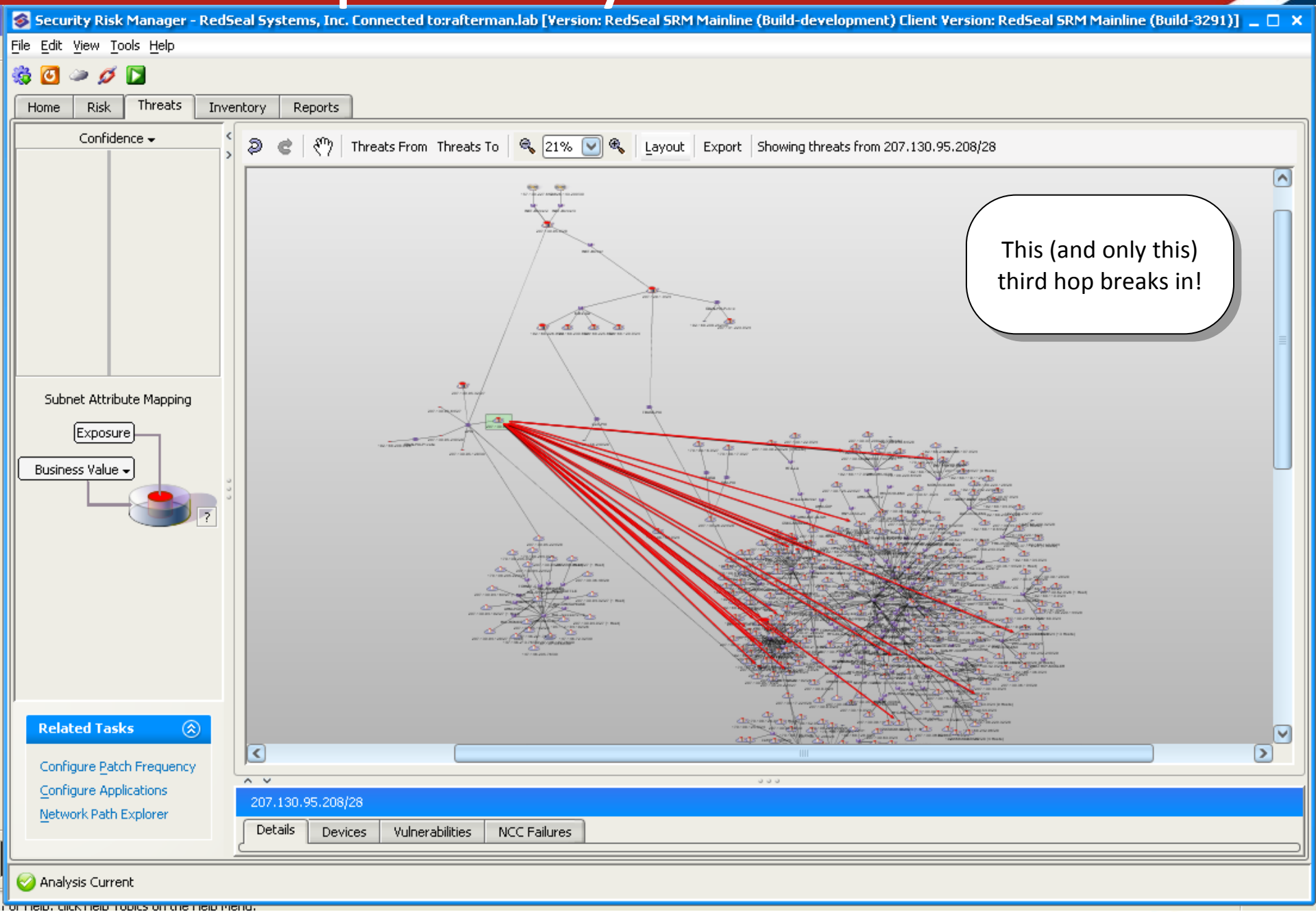
# Threat Map: Security Risk Manifestation



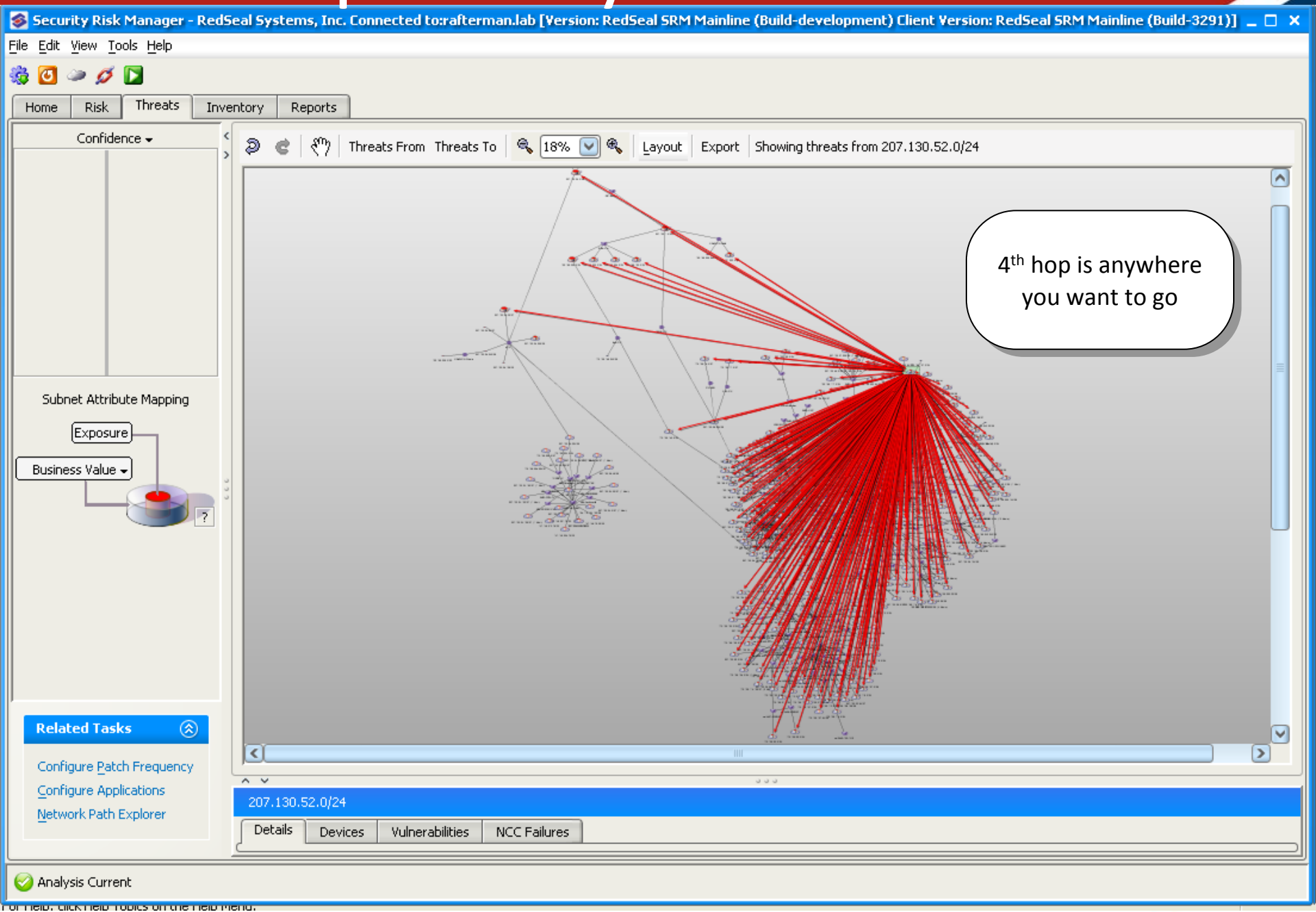
# Attack Graph: Security Risk Manifestation



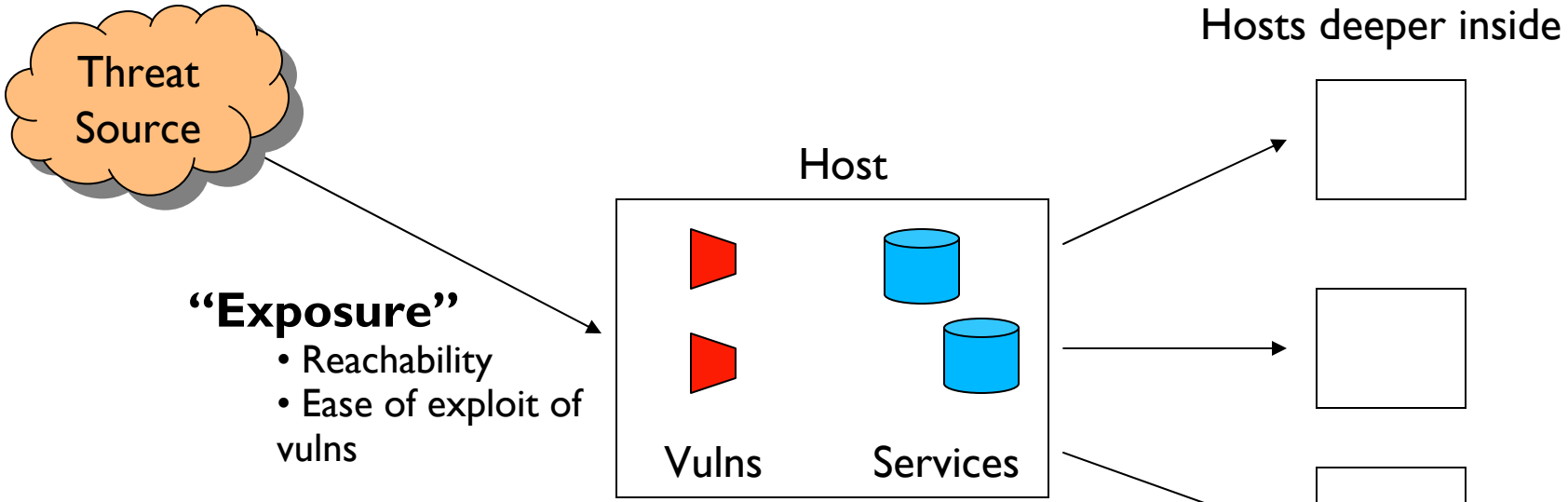
# Attack Graph: Security Risk Manifestation



# Attack Graph: Security Risk Manifestation



# Overview of the RedSeal Risk Metrics




**"Exposure"**

- Reachability
- Ease of exploit of vulns

**"Business Value"**

- Default is highest value service

**"Risk"**

- Exposure X Business Value



RedSeal

# Why is IT Risk Management Hard?

- **Security Silos**
  - Rigidly patching only high-severity vulnerabilities might not remove vulnerabilities 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**

# Steps toward effective IT Risk Management

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