

REPORTING THE KILL CHAIN

Types of Security Assessments

- Vulnerability Assessment
- Penetration Test
- Code Review
- Red Teaming
- Attack Simulation
- Audit
- White/Grey/Black-box Assessment
- Risk Assessment
- Threat Assessment
- Threat Modeling
- ...

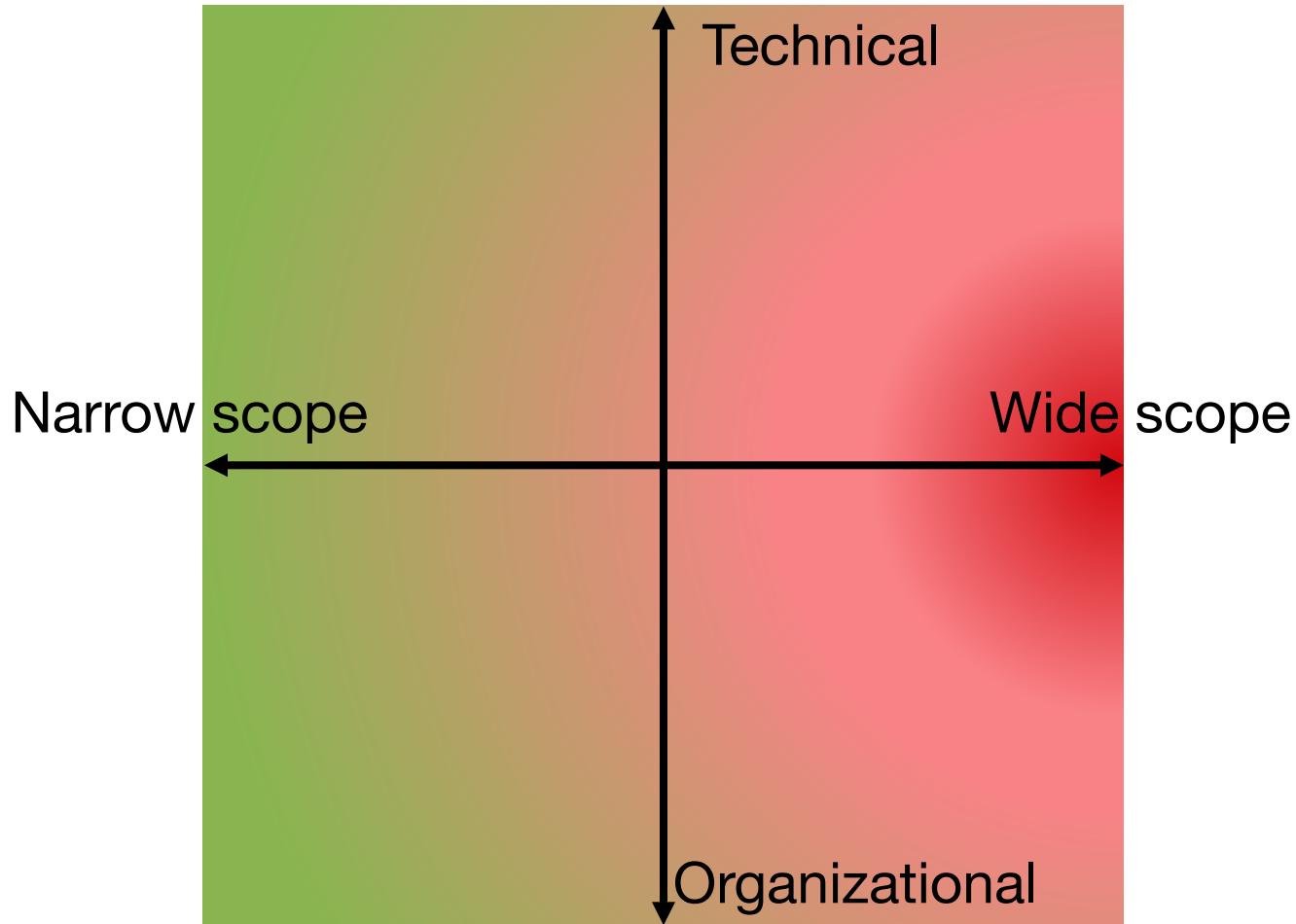
Easy reports

The screenshot shows the Nessus web interface with the following details:

- Header:** Nessus, Scans 88, Policies, Launch, Export, Filter Vulnerabilities.
- Breadcrumbs:** Hosts > 192.168.1.11 > Vulnerabilities 52.
- Table Headers:** Severity ▲, Plugin Name, Plugin Family, Count.
- Table Data:** A list of vulnerabilities including:
 - HIGH: NFS Share User Mountable (RPC, Count 1)
 - MEDIUM: SSL Certificate Cannot Be Trusted (General, Count 2)
 - MEDIUM: SSL Certificate with W (General, Count 2)
 - MEDIUM: SSL Self-Signed Certi (General, Count 2)
 - MEDIUM: AFP Server Directory (General, Count 2)
 - MEDIUM: Microsoft Windows SMB Guest Account Local User Access (Windows, Count 1)
 - MEDIUM: MySQL Protocol Remote User Enumeration (Databases, Count 1)
 - MEDIUM: NFS Exported Share Information Disclosure (RPC, Count 1)
 - MEDIUM: NFS Shares World Readable (RPC, Count 1)
 - MEDIUM: SMB Signing Disabled (Misc., Count 1)
 - INFO: Nessus SYN scanner (Port scanners, Count 16)
 - INFO: RPC Services Enumeration (Service detection, Count 12)
 - INFO: Service Detection (Service detection, Count 9)
- Host Details:** IP: [REDACTED], MAC: [REDACTED], OS: Linux Kernel 3.10, Linux Kernel 3.5, Linux Kernel 3.8, Linux Kernel 3.9, Start: Today at 7:19 PM, End: Today at 7:23 PM, Elapsed: 4 minutes, Status: Download.
- Vulnerabilities:** A donut chart showing the distribution of vulnerabilities by severity: High (orange), Medium (yellow), and Info (blue).

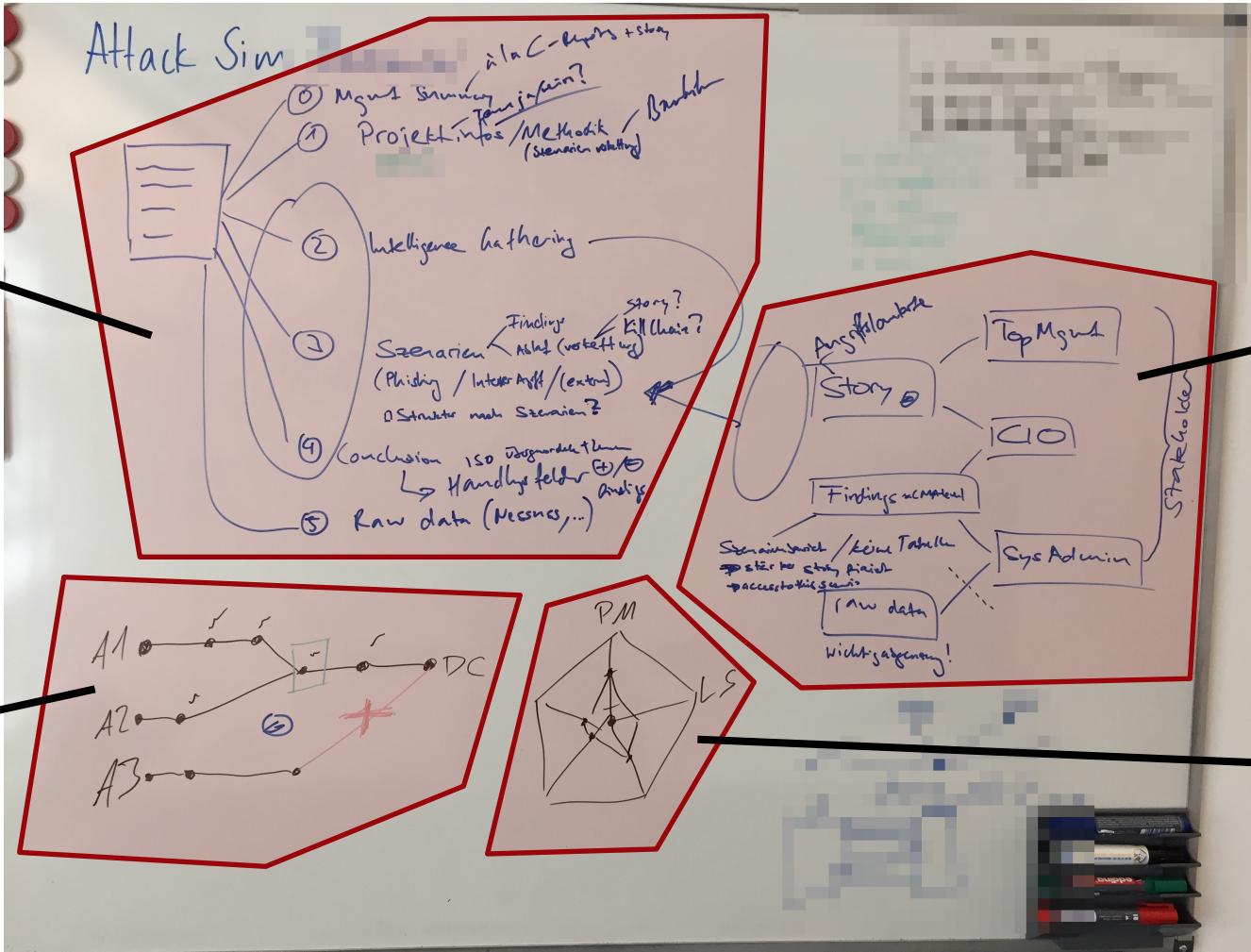
A large red box highlights the message: "Patch X is missing on target Y. Fix because vulnerability Z."

Complexity of Reporting



What makes a good report

Structure

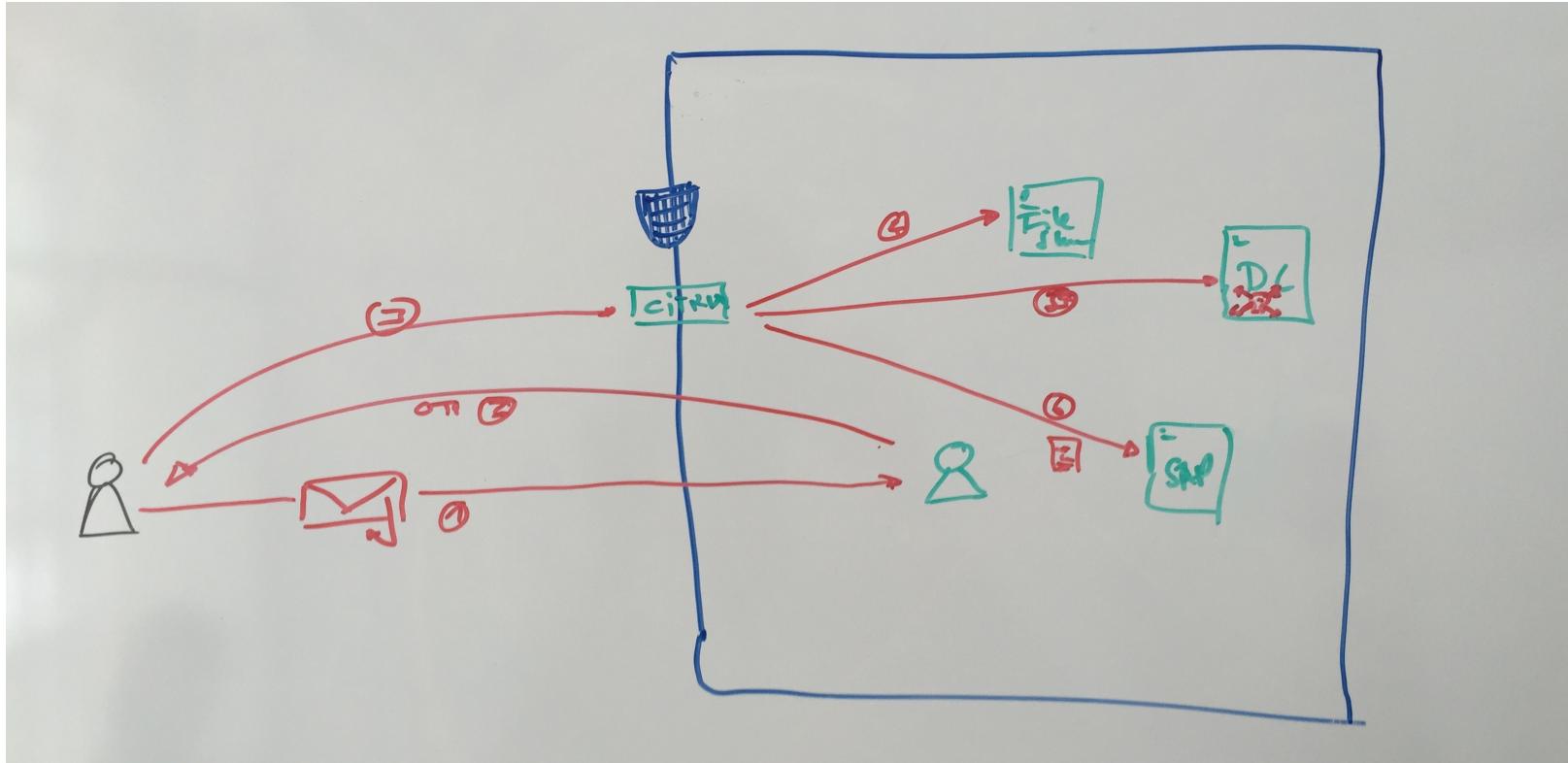


Shareholders

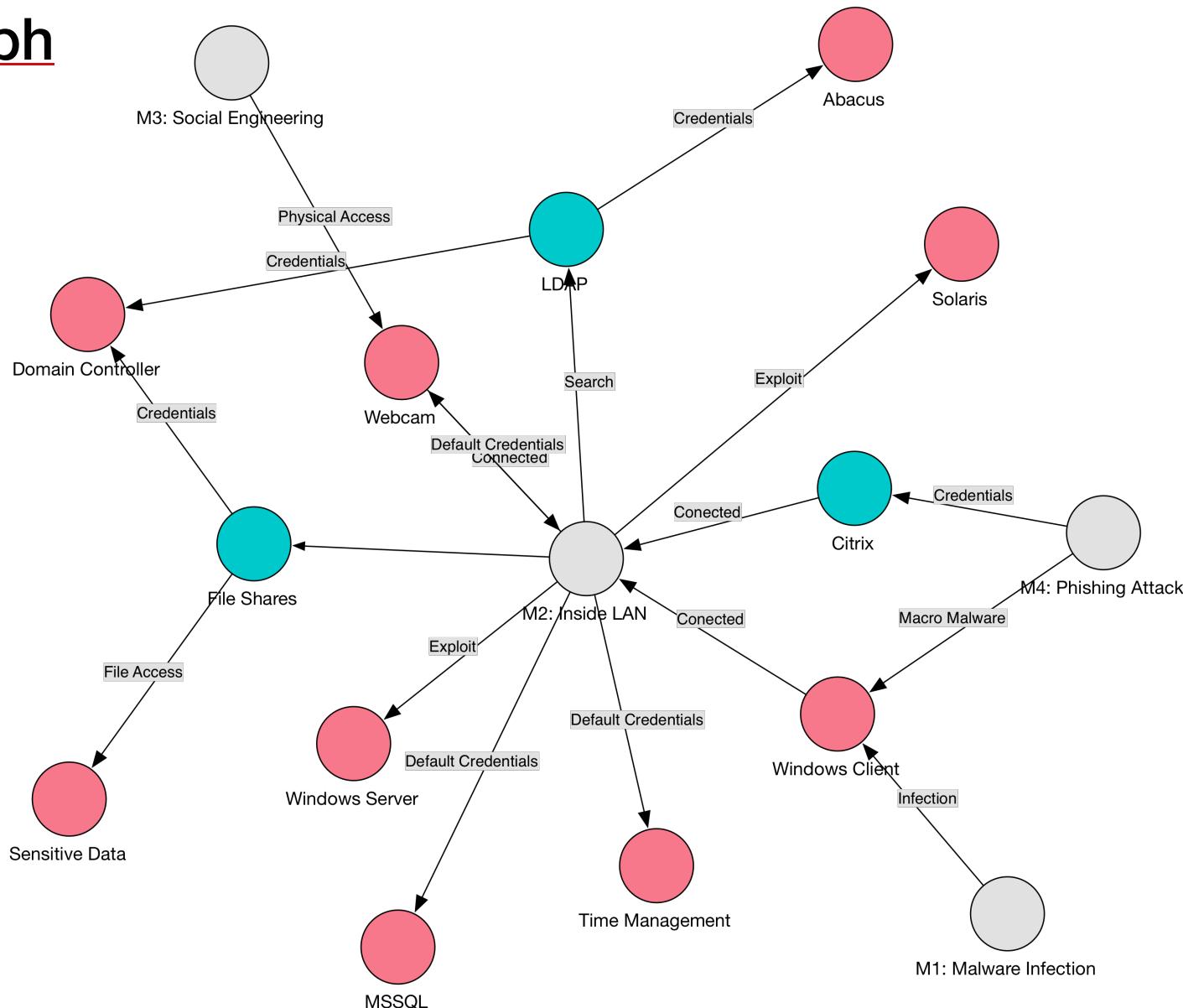
Visualization

Metrics

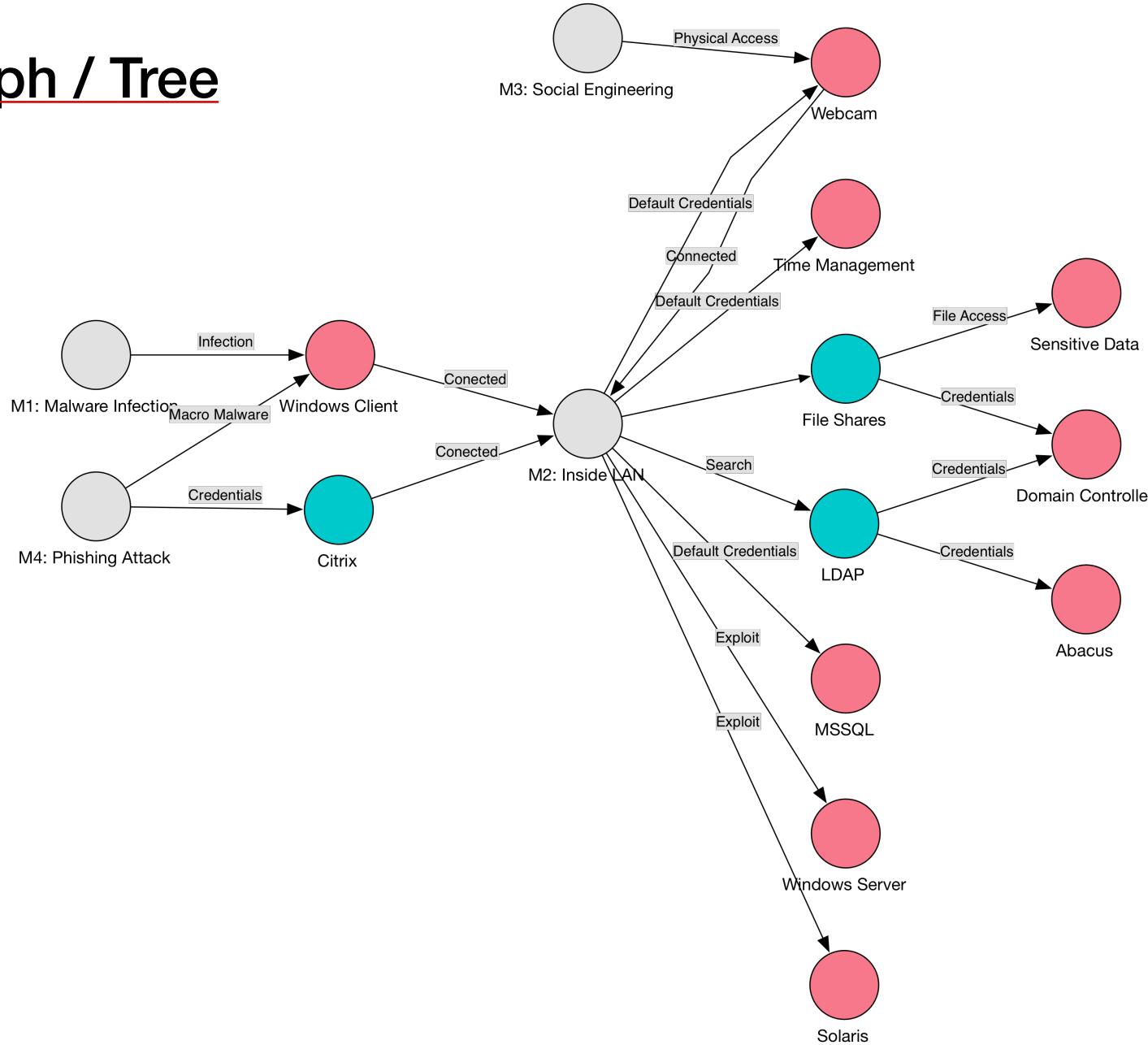
Scope vs. Scenario



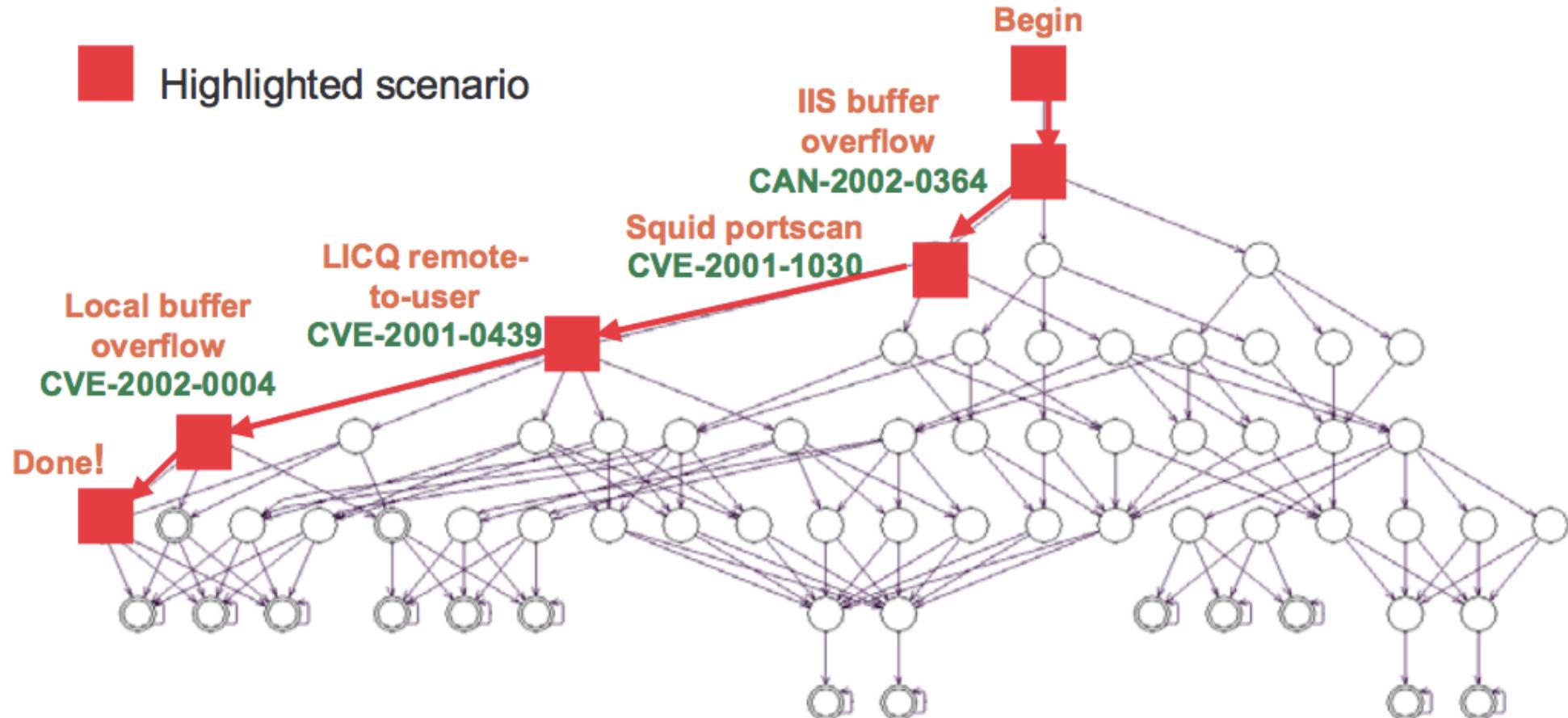
Attack Graph



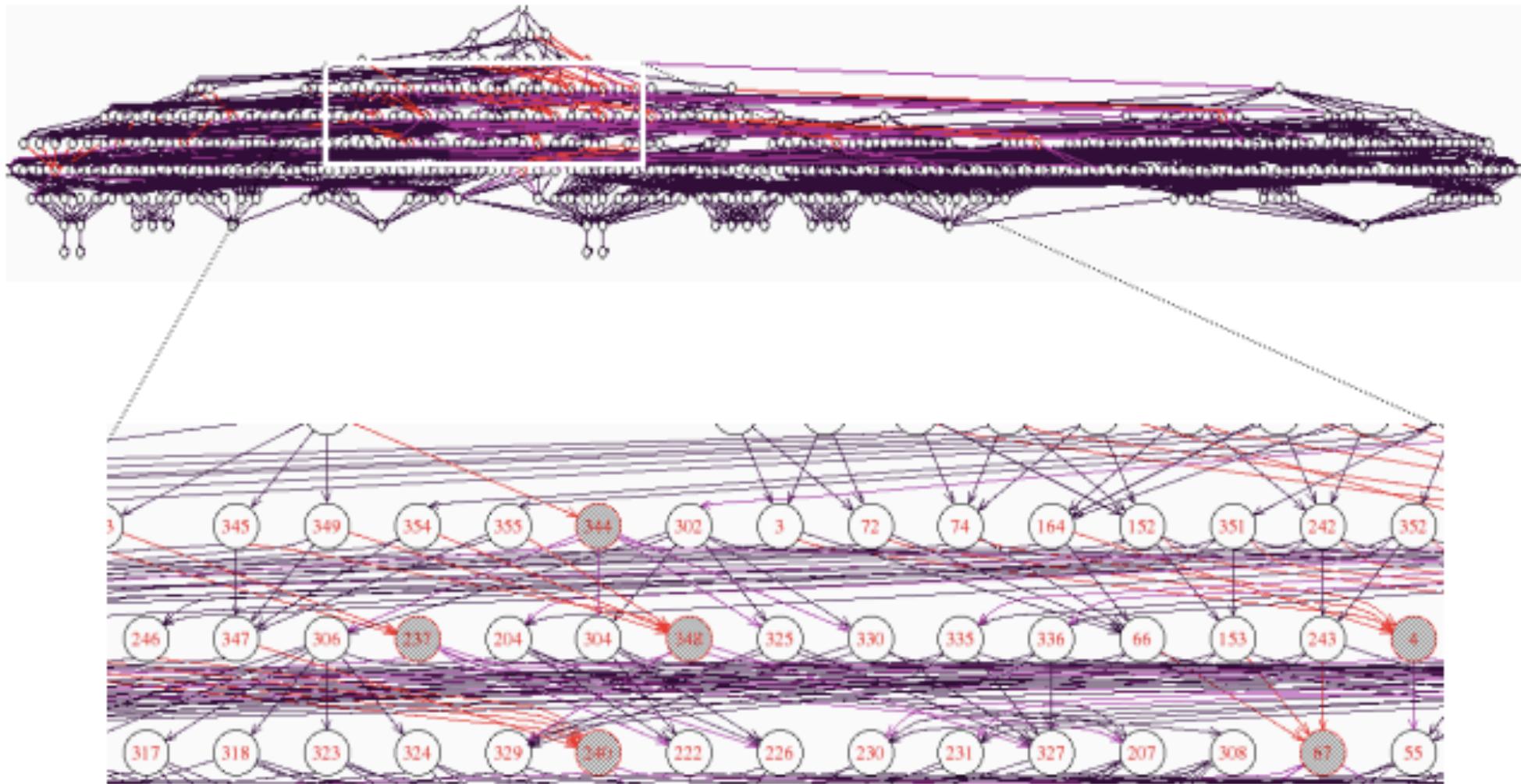
Attack Graph / Tree



Reality



Reality

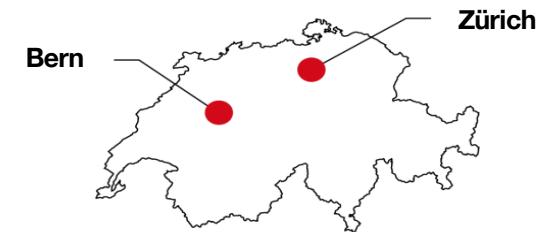


<https://www.cs.cmu.edu/~scenariograph/wing07.pdf>

Some Conclusions

- Vulnerability/Finding based reporting is easy
- We know what the customers want
- Reporting complex attack scenarios is hard
- The amount of data we gather during an assessment is huge
- Increasing complexity of our assessments allows less automation in the reporting phase
- Visualization helps but is also hard
- DIN A4 might not be the best to handle modern reports

Thanks for
your attention



REDGUARD
SECURING YOUR ASSETS

Redguard AG Eigerstrasse 60 CH-3007 Bern
T +41 (0)31 511 37 50 www.redguard.ch