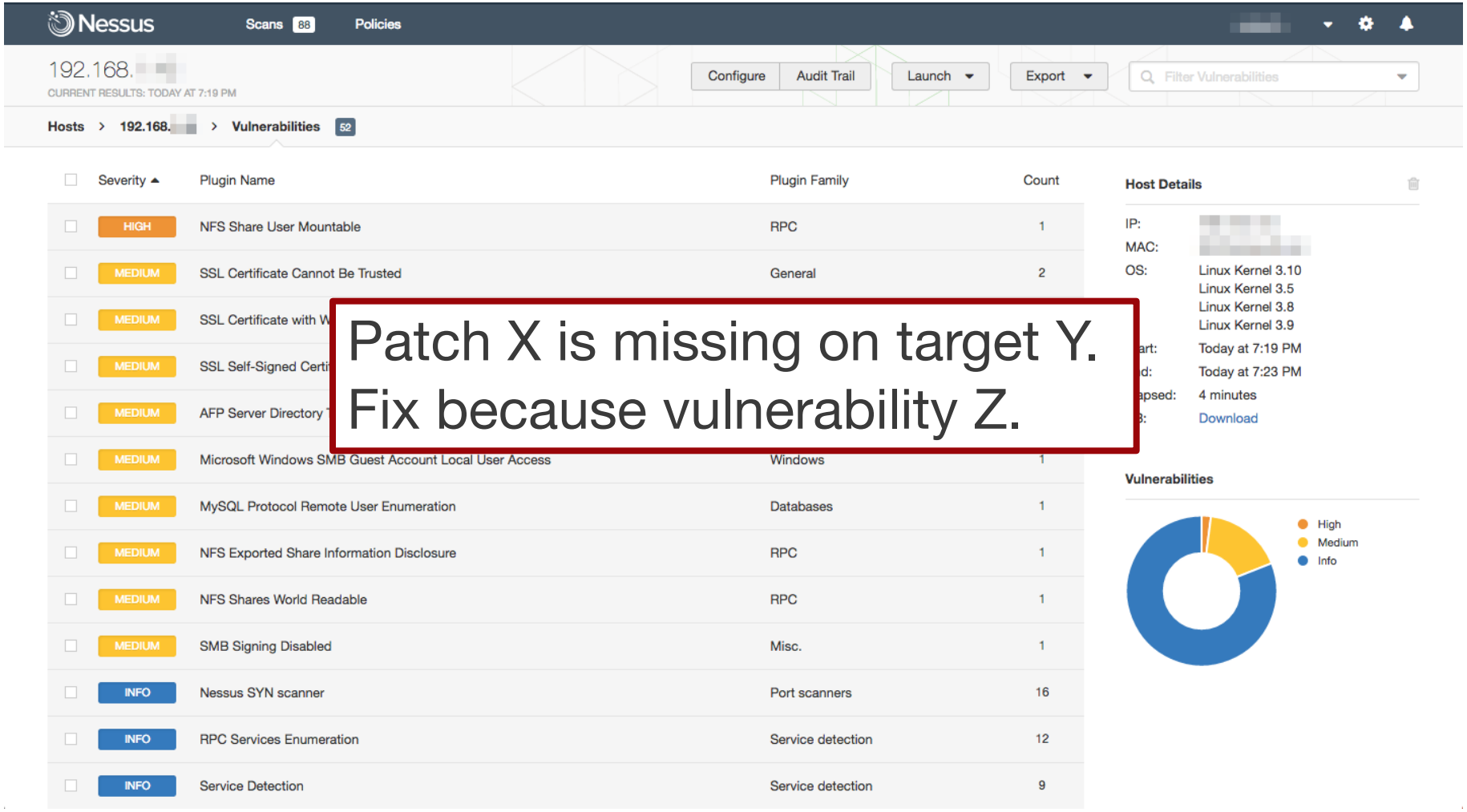
REPORTING THE KILL CHAIN

REDGUARD
SECURING YOUR ASSETS

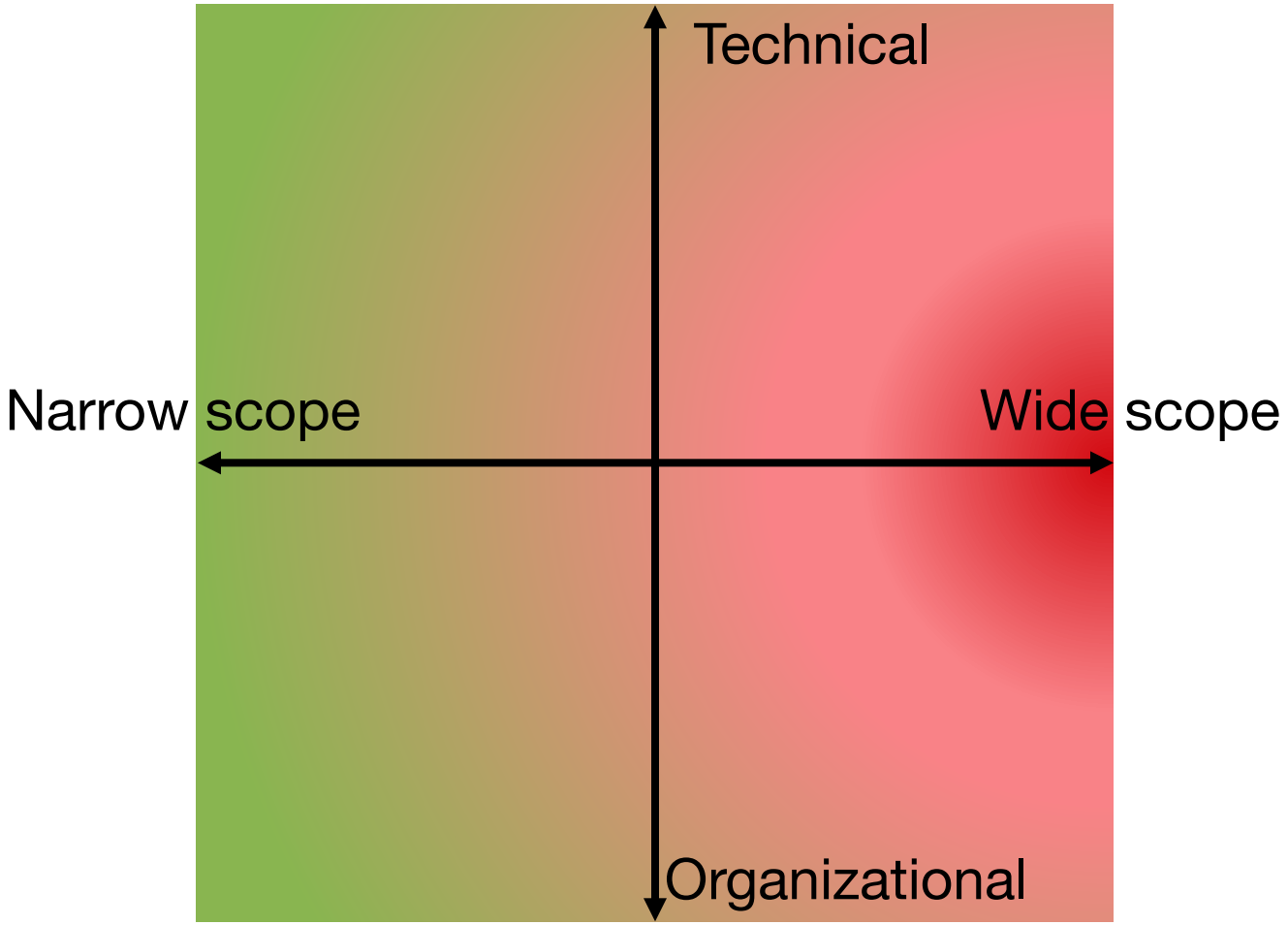
Types of Security Assessments

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

Easy reports



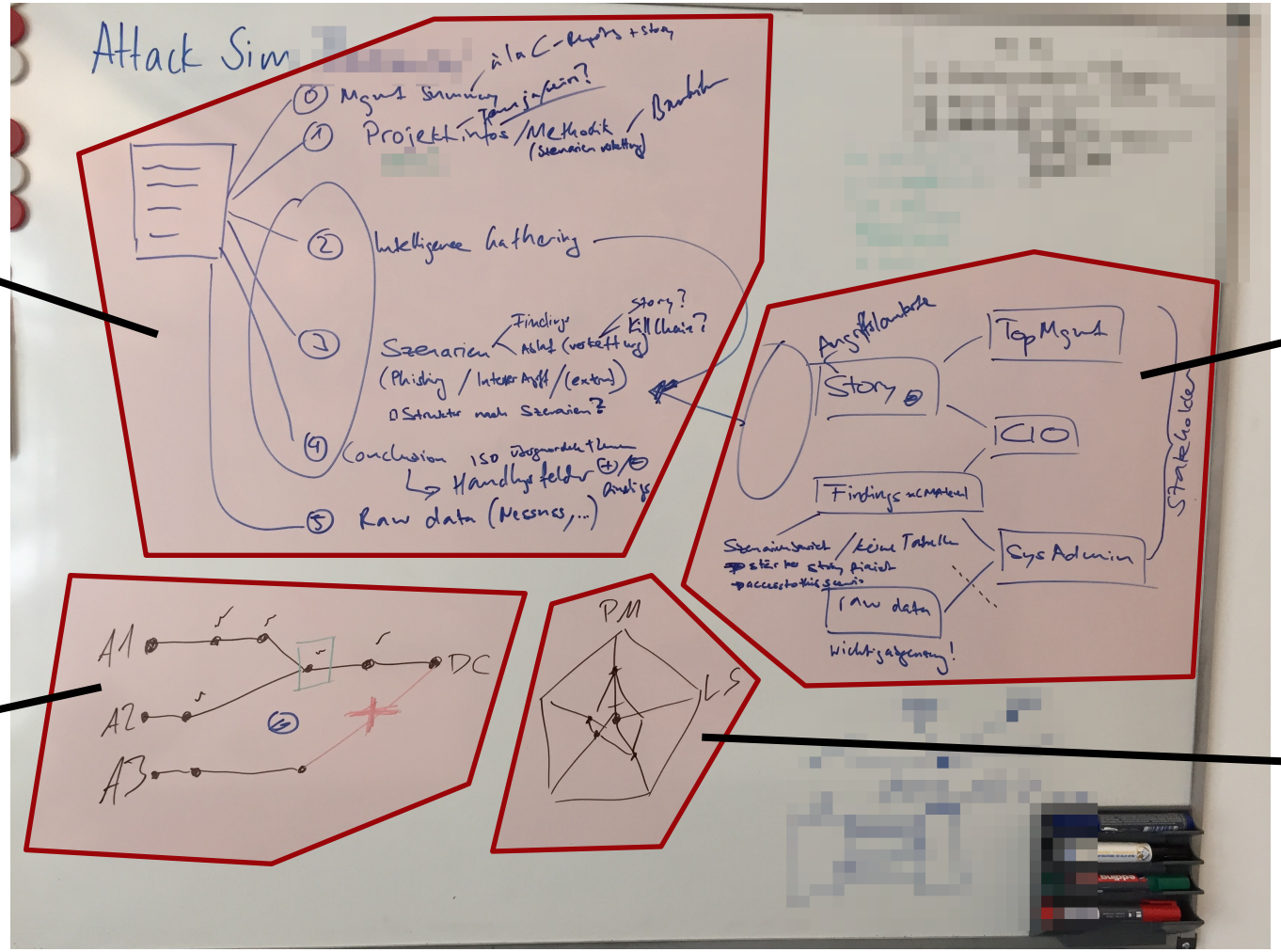
Complexity of Reporting



What makes a good report

Structure

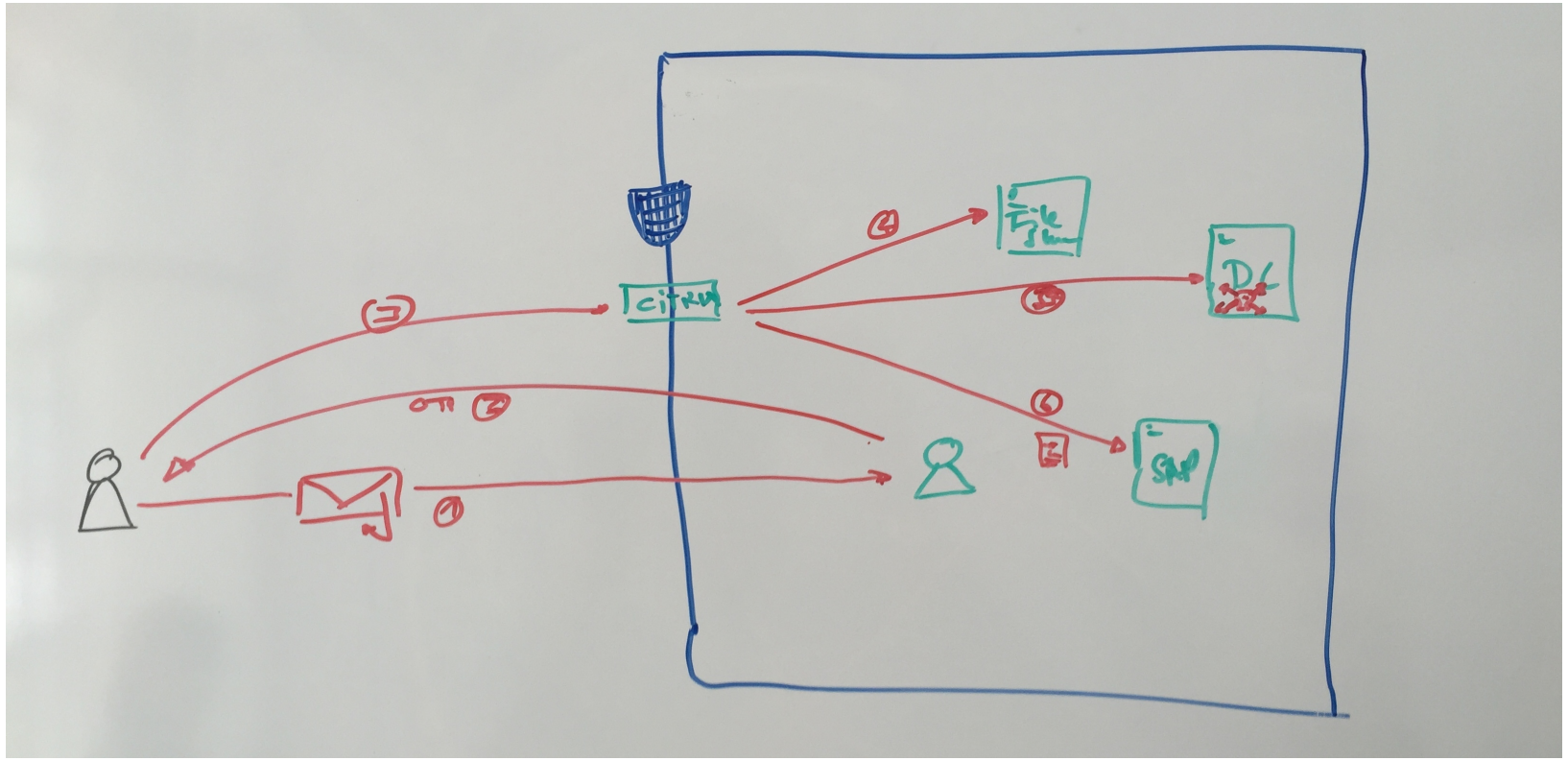
Visualization



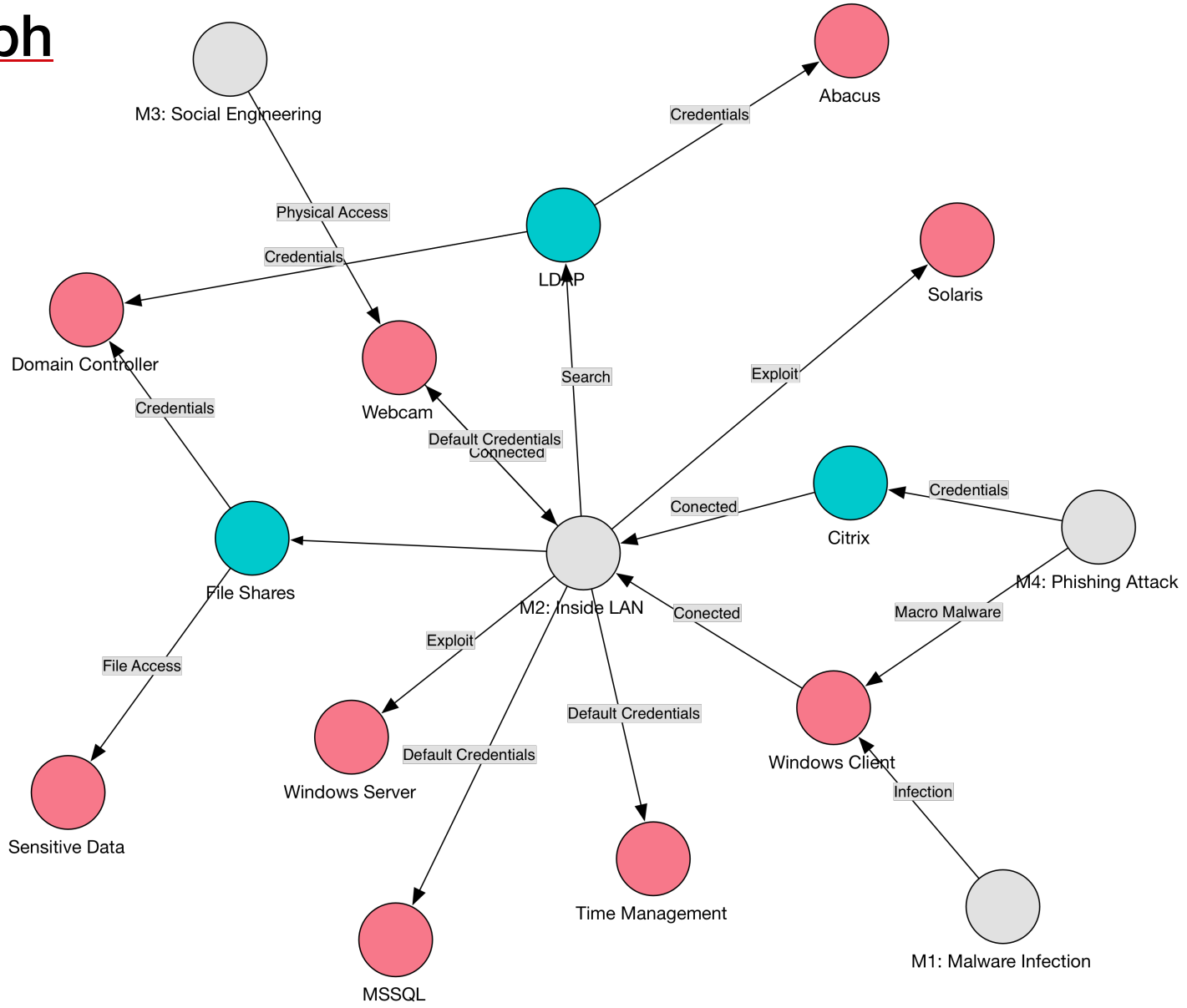
Shareholders

Metrics

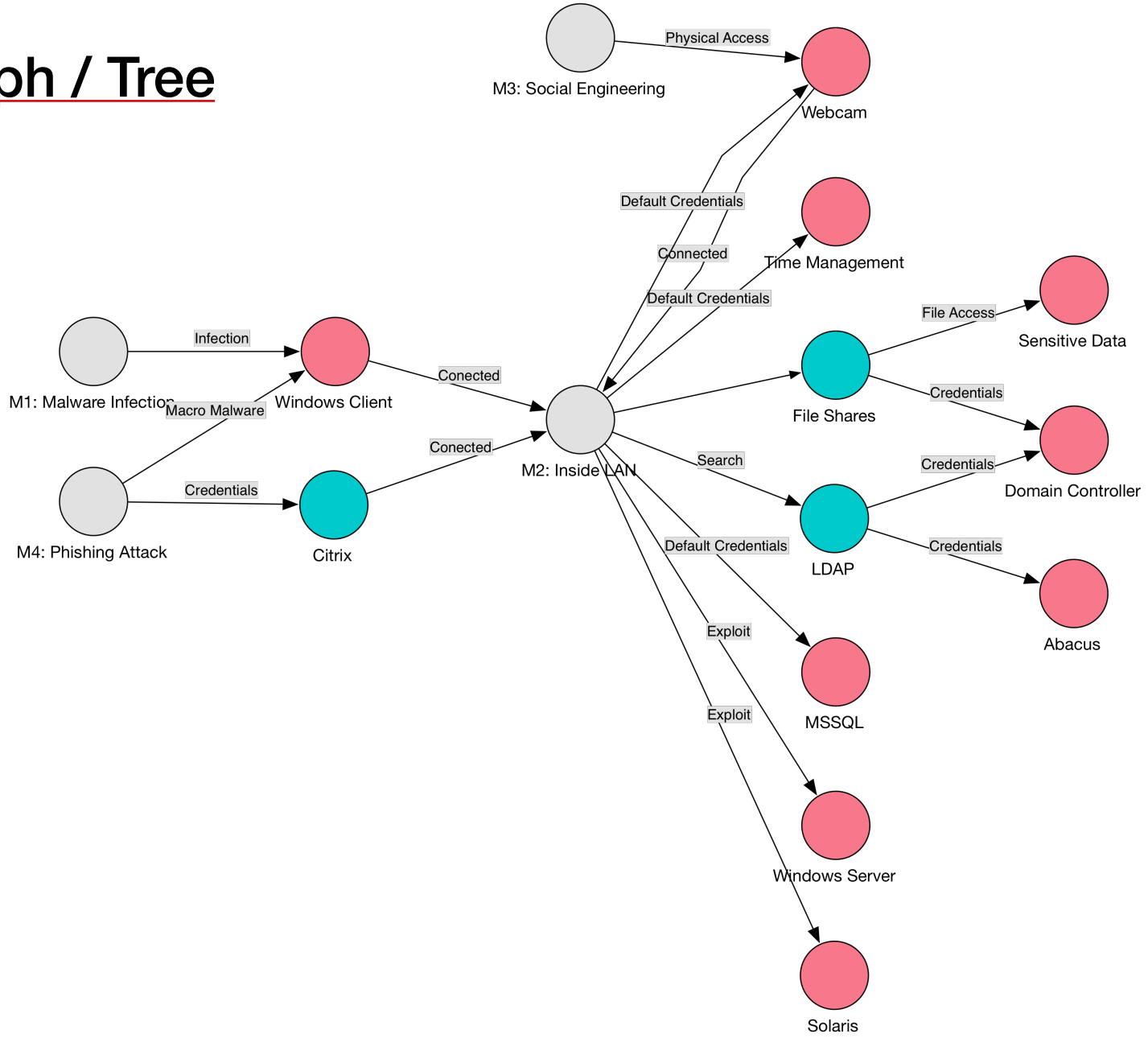
Scope vs. Scenario



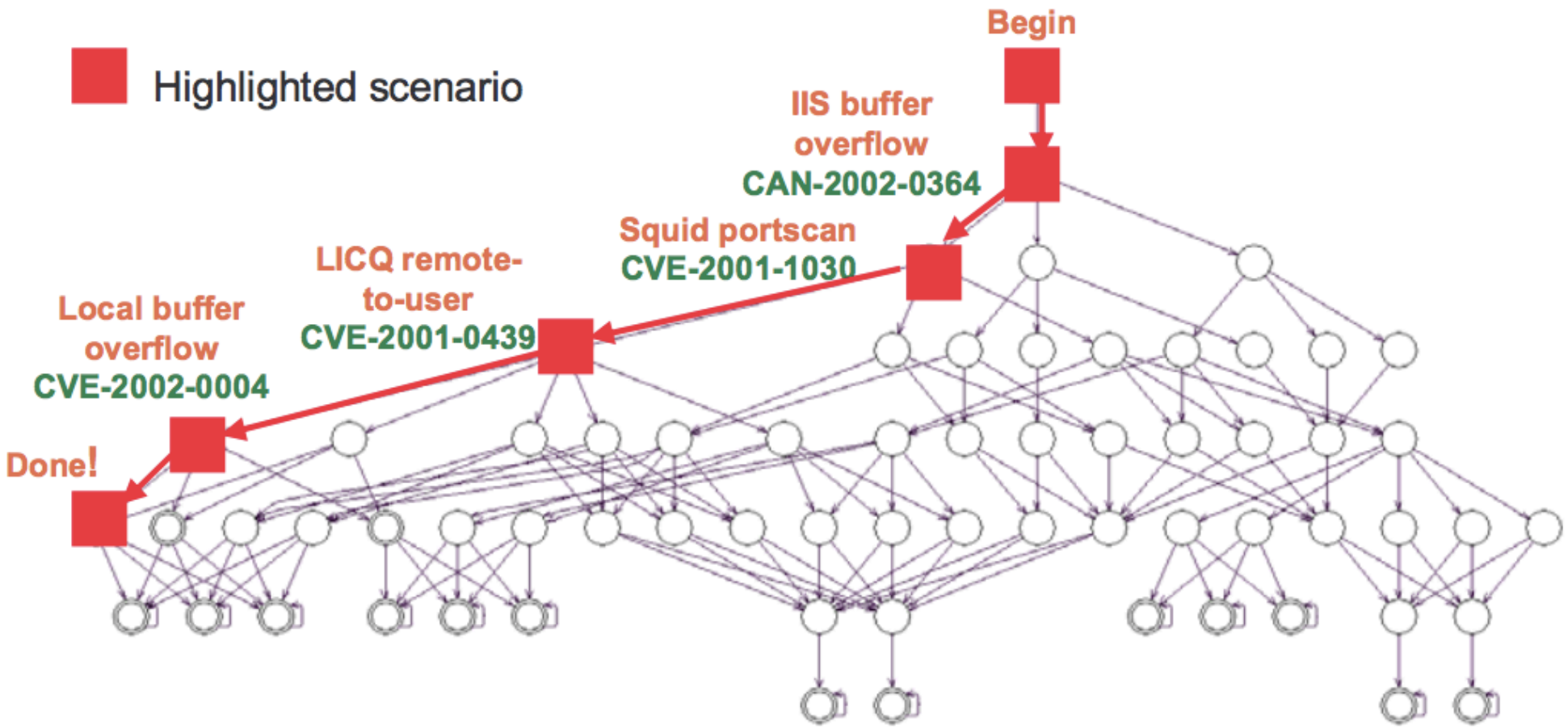
Attack Graph



Attack Graph / Tree

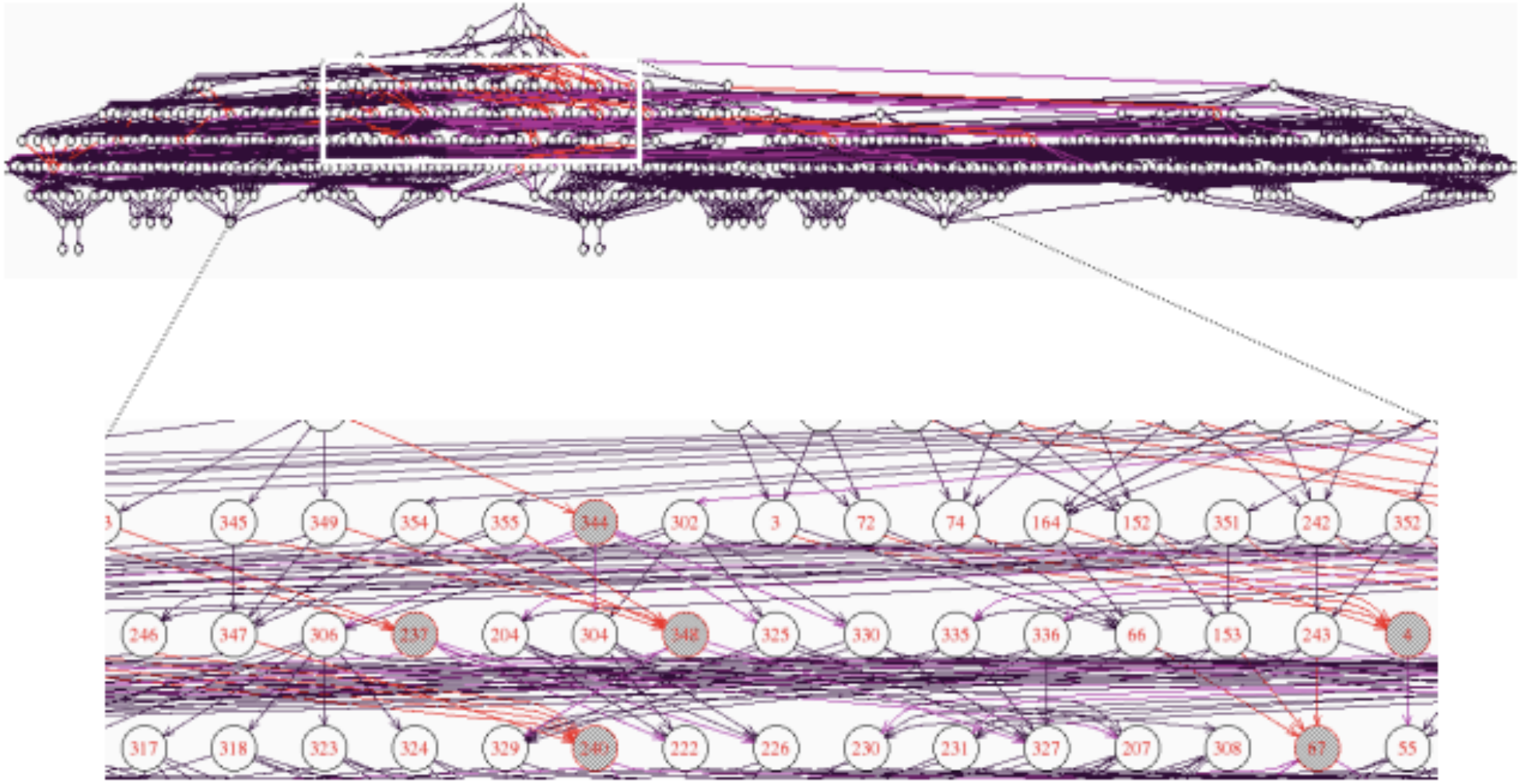


Reality



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

Reality

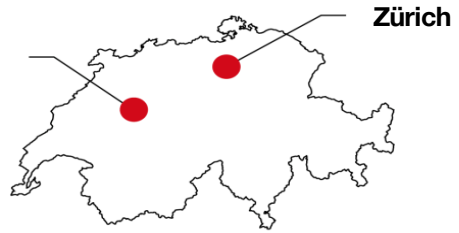


https://www.cs.cmu.edu/~scenariograph/wing07.pdf

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**