

Rapid Security Framework (RSF)

Taxonomie, Bewertungsparameter und Marktanalyse zur Auswahl von Fuzzing-Tools

Motivation

Attacks

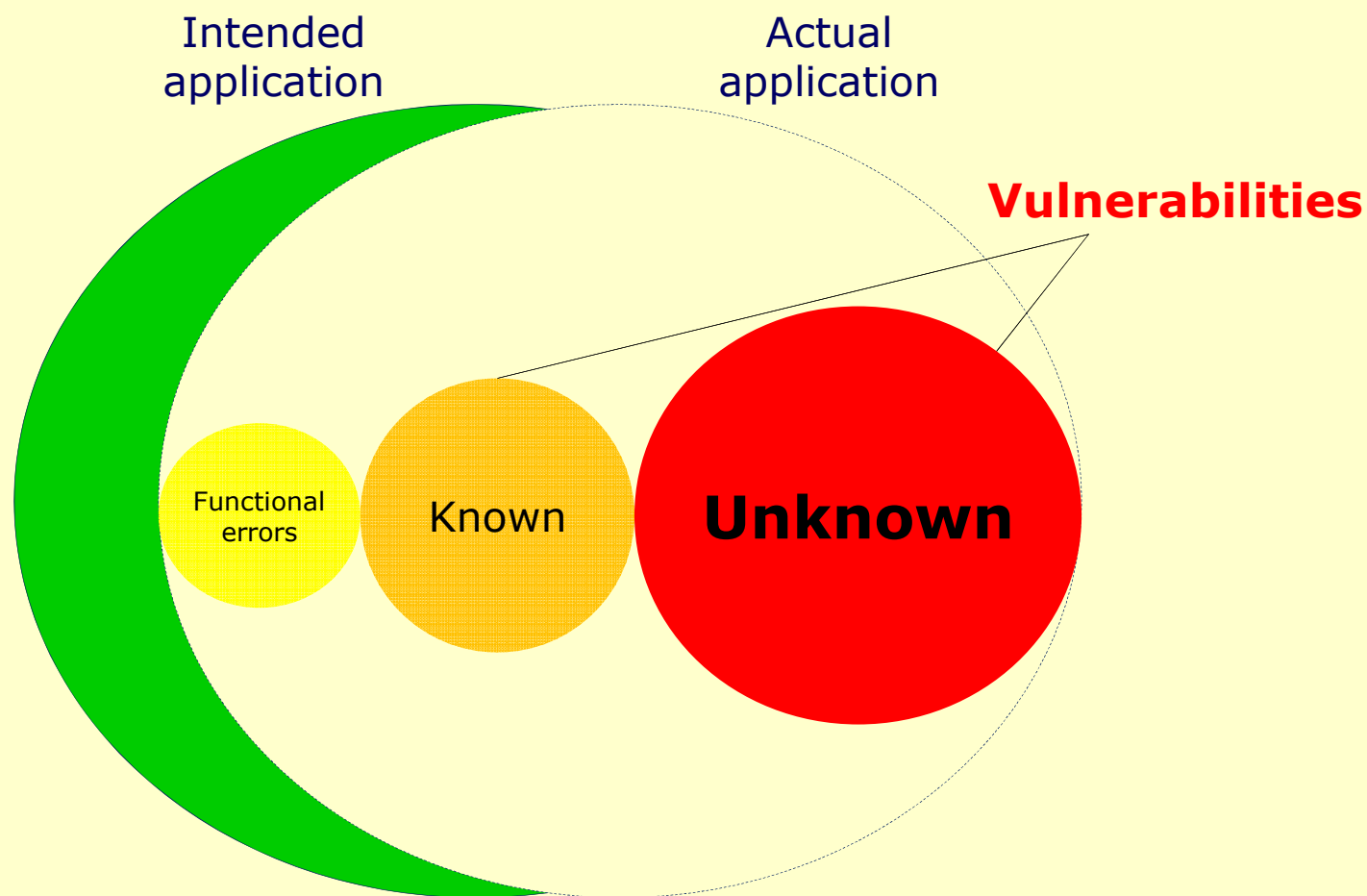
- Industrial espionage
- Sabotage
- Data privacy problems

Software is insecure

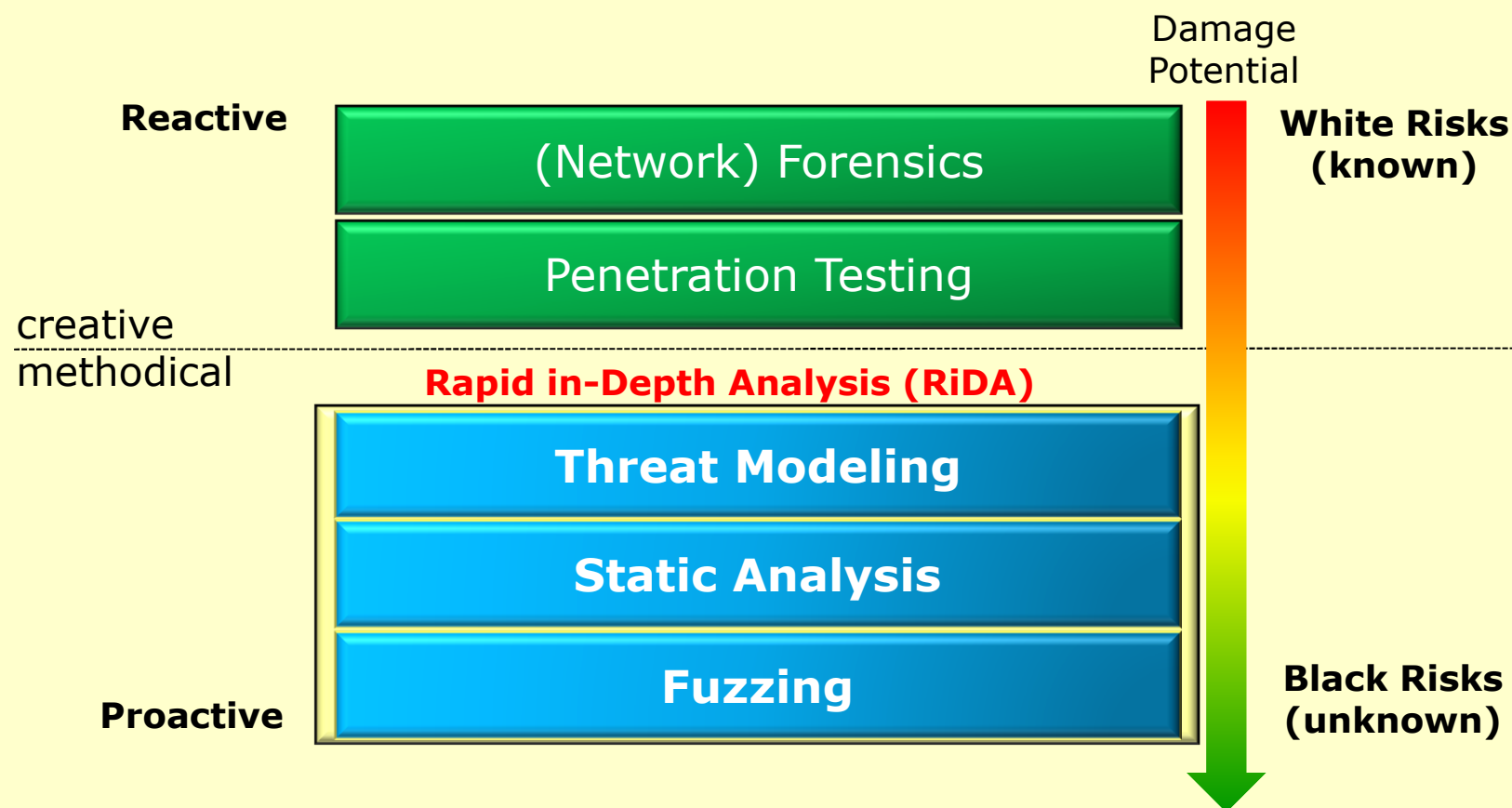
bugs: especially **security related bugs!**

- Detected and **undetected – (less-than-) Zero Day** – Vulnerabilities
- Vulnerability detection := **Secure Software + Costreduction**

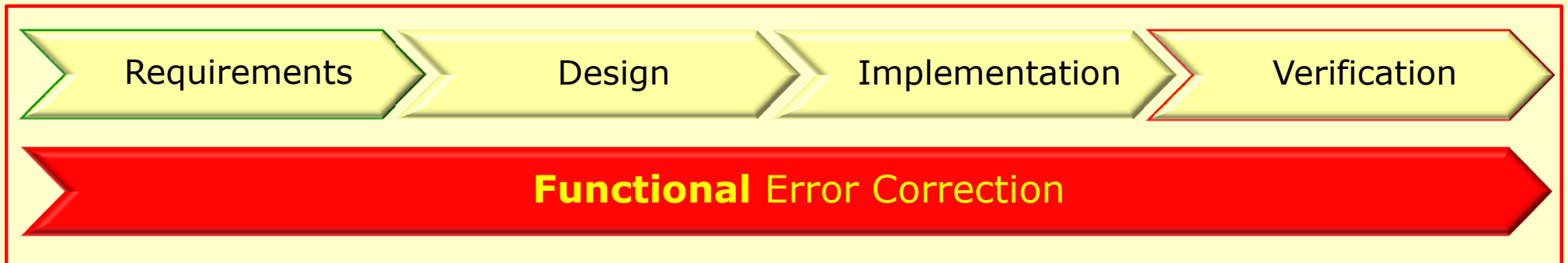
Known and unknown vulnerabilities



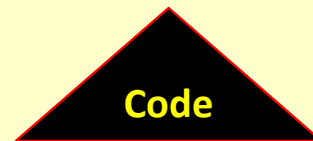
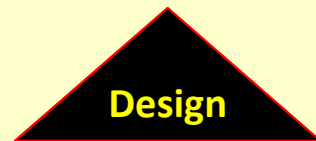
Methodical Penetration Testing: RiDA



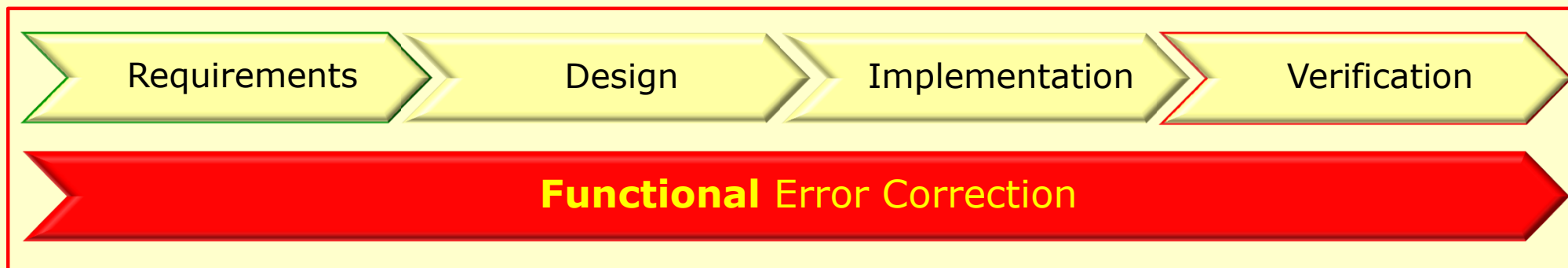
Standard software development



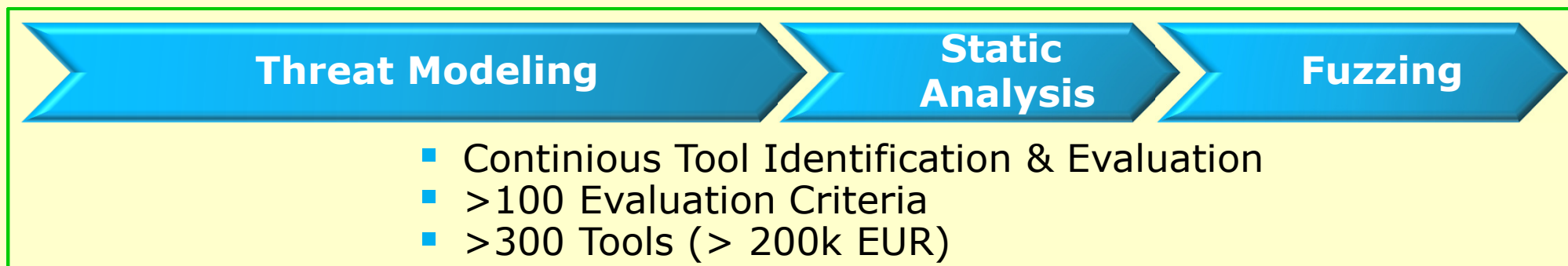
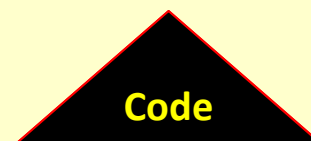
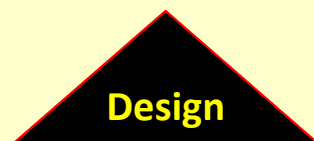
Zero-Day
Vulnerabilities



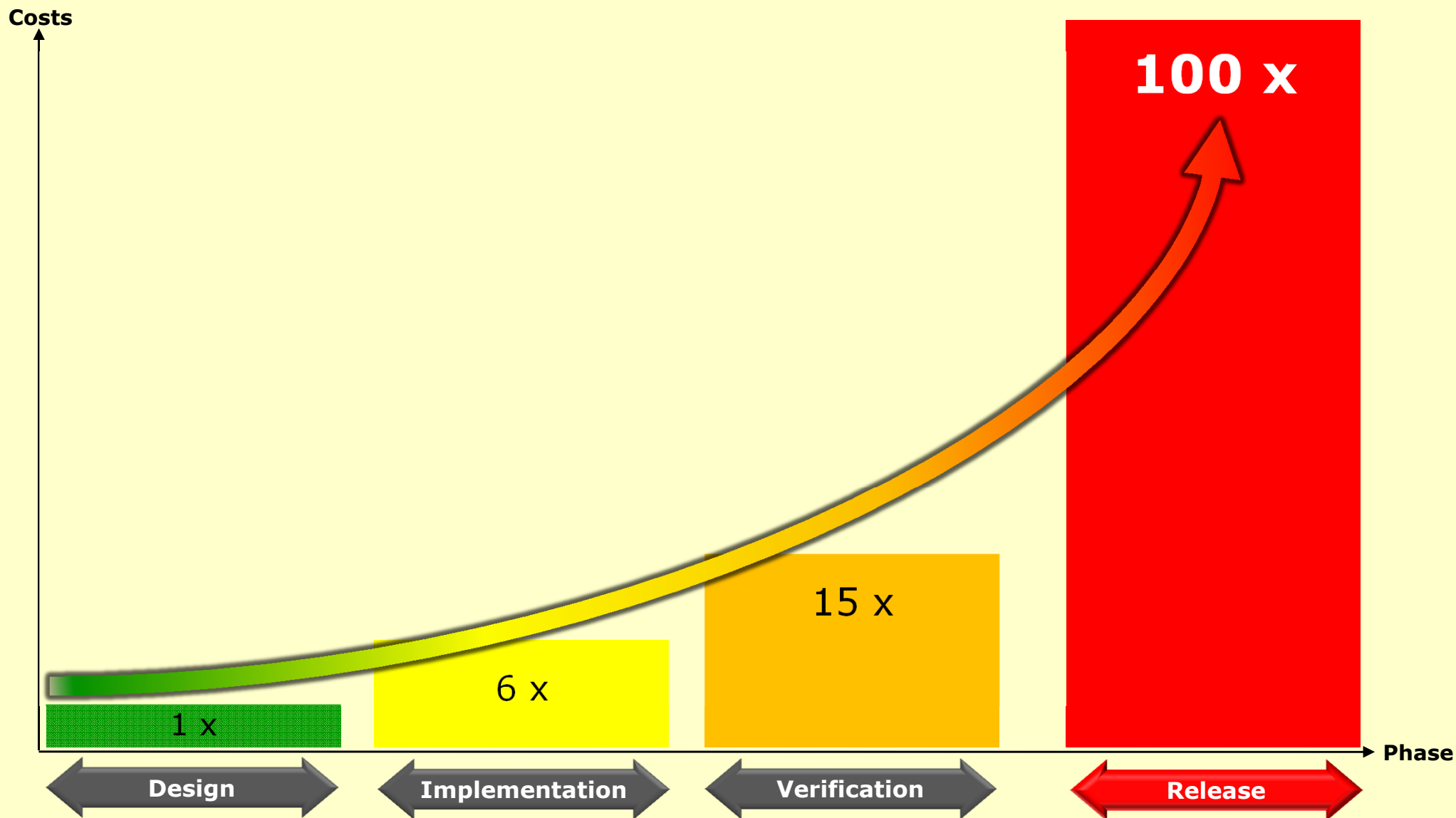
Secure software development



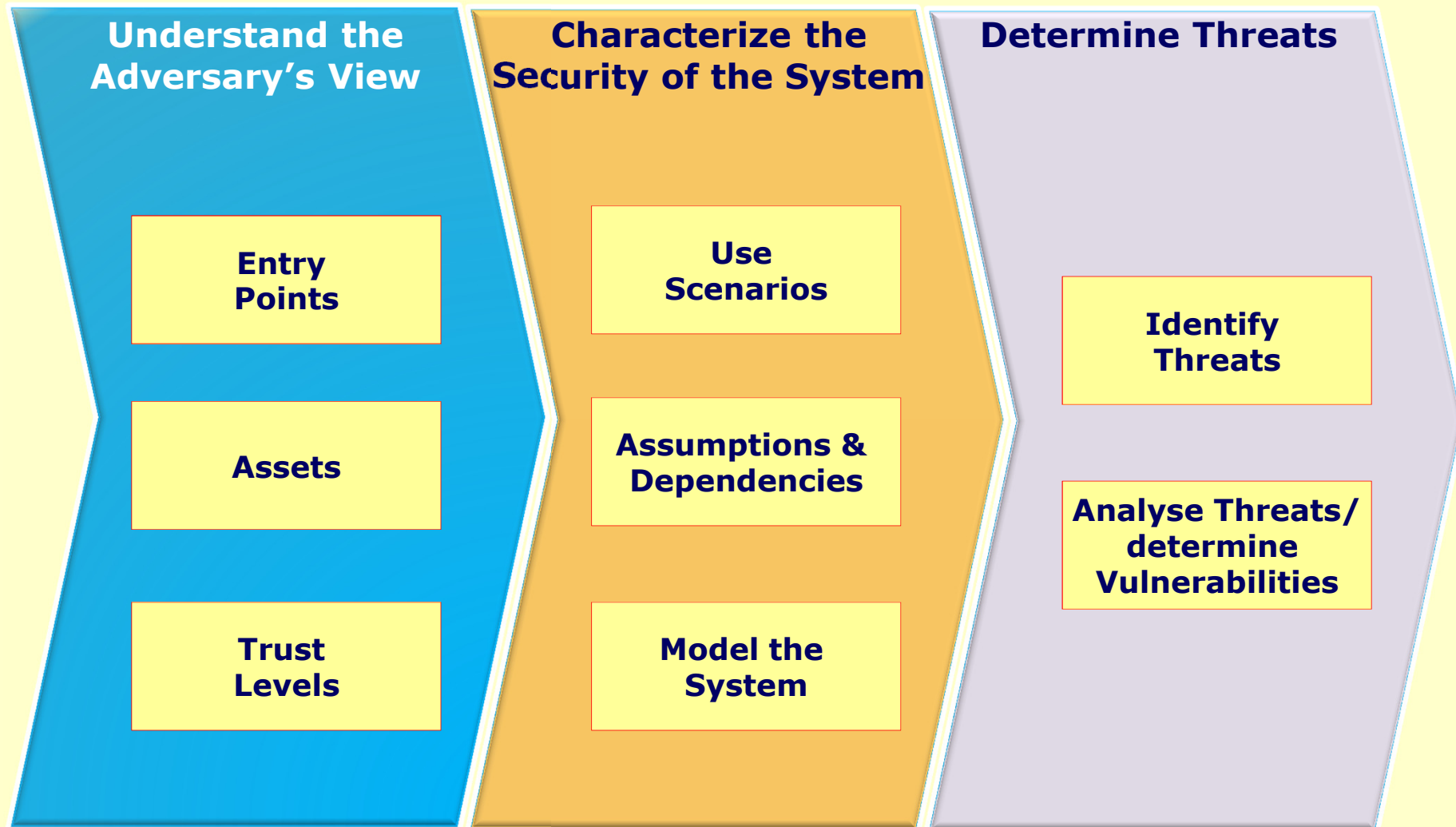
Zero-Day
Vulnerabilities



Benefit: cost of bug elimination



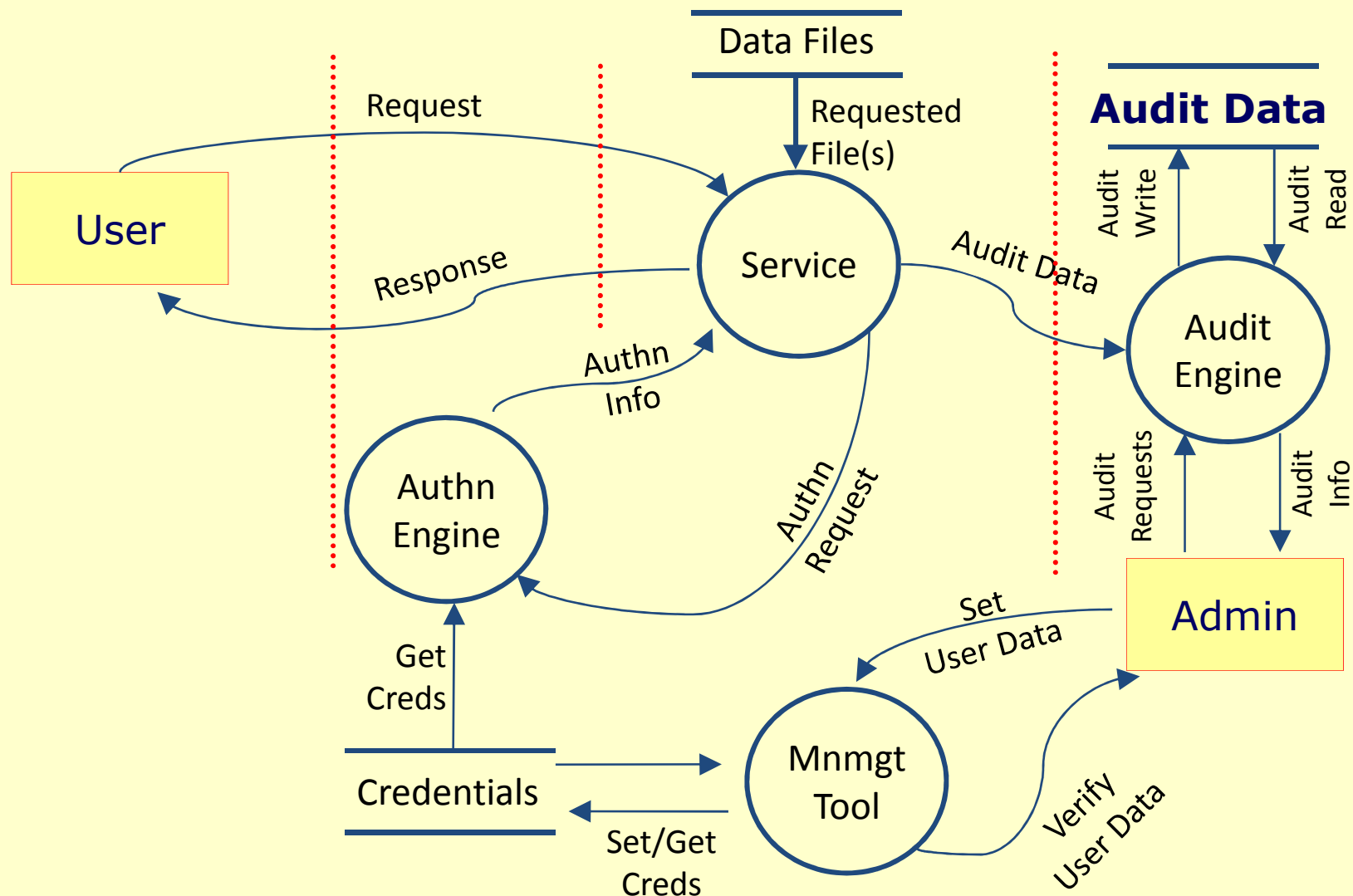
Threat Modeling process



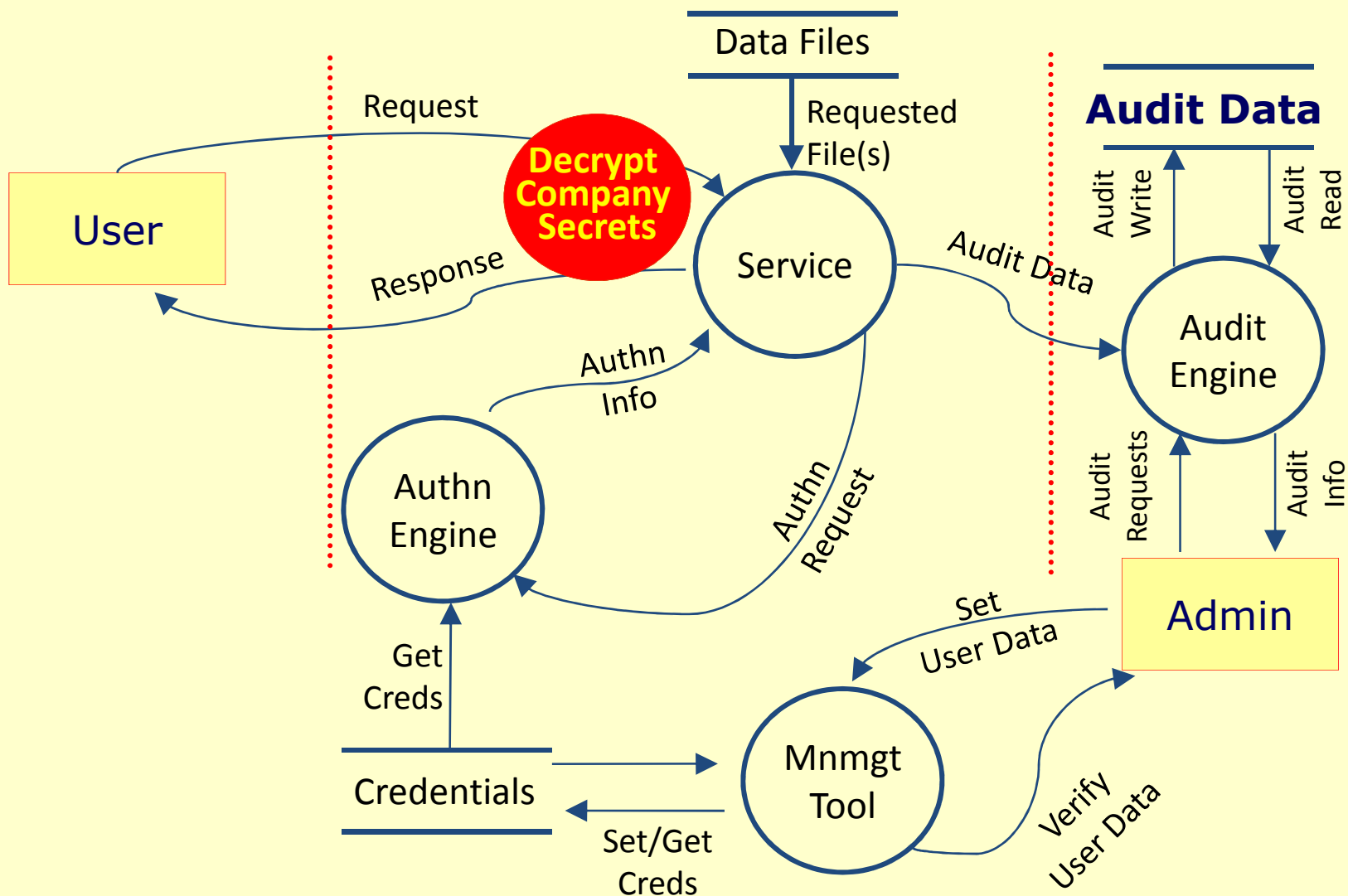
Threat Modeling techniques

- Data Flow Diagrams
- Attack Trees
- ...

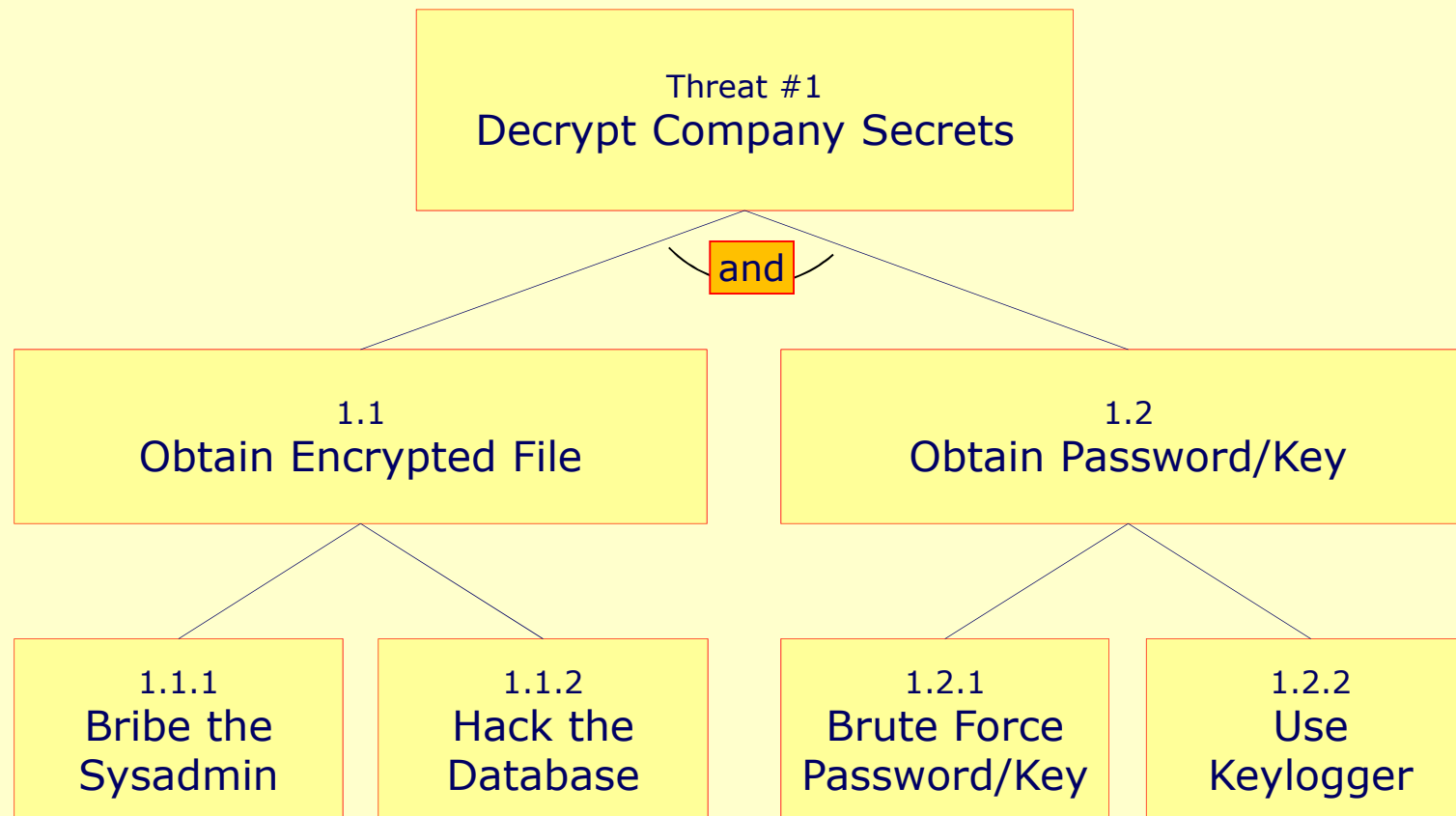
Data Flow Diagrams



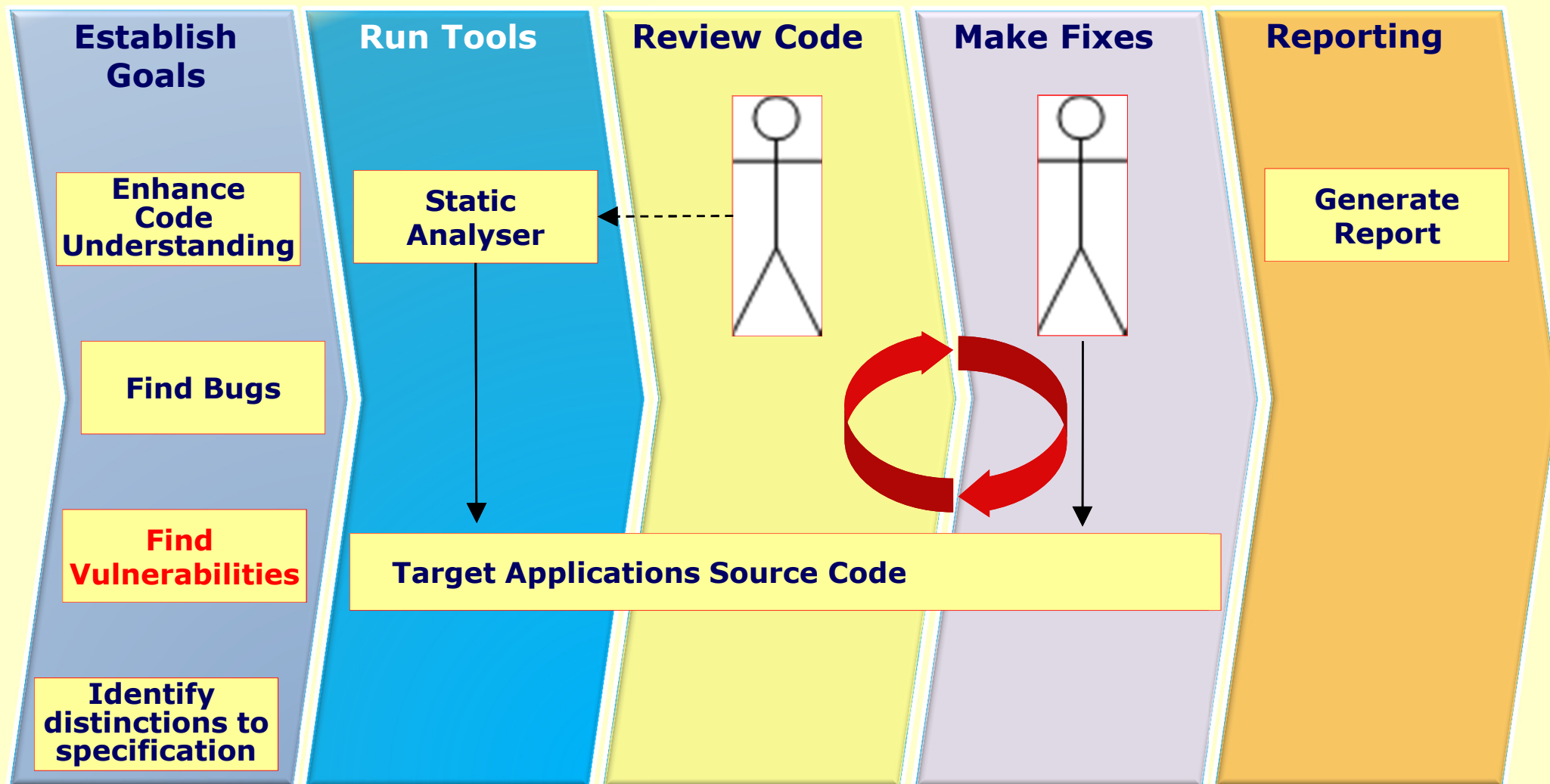
Data Flow Diagrams



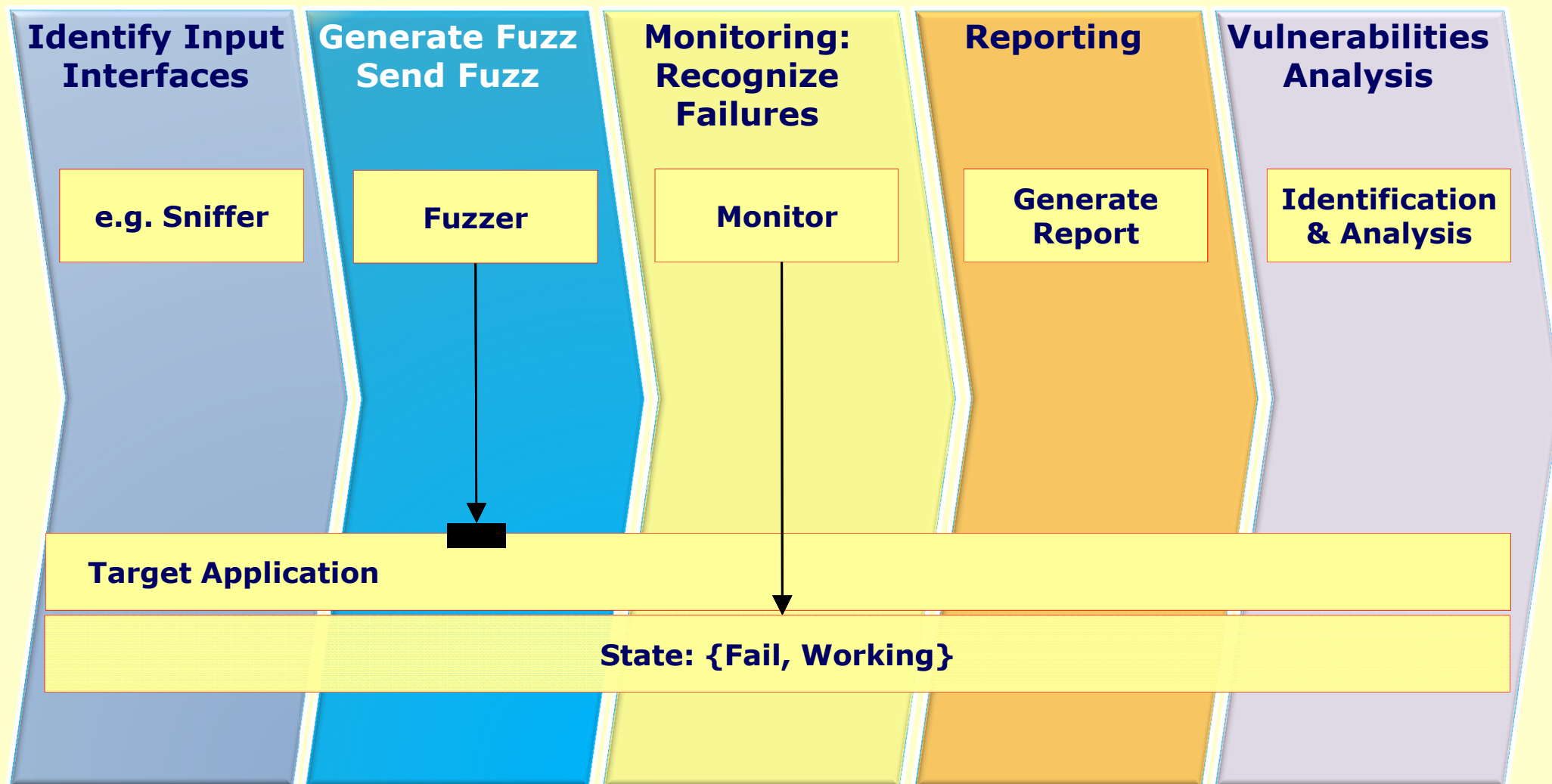
Attack Trees



Static Analysis Process



Fuzzing process



> 300 Fuzzer

Which are the right for your application(s)?

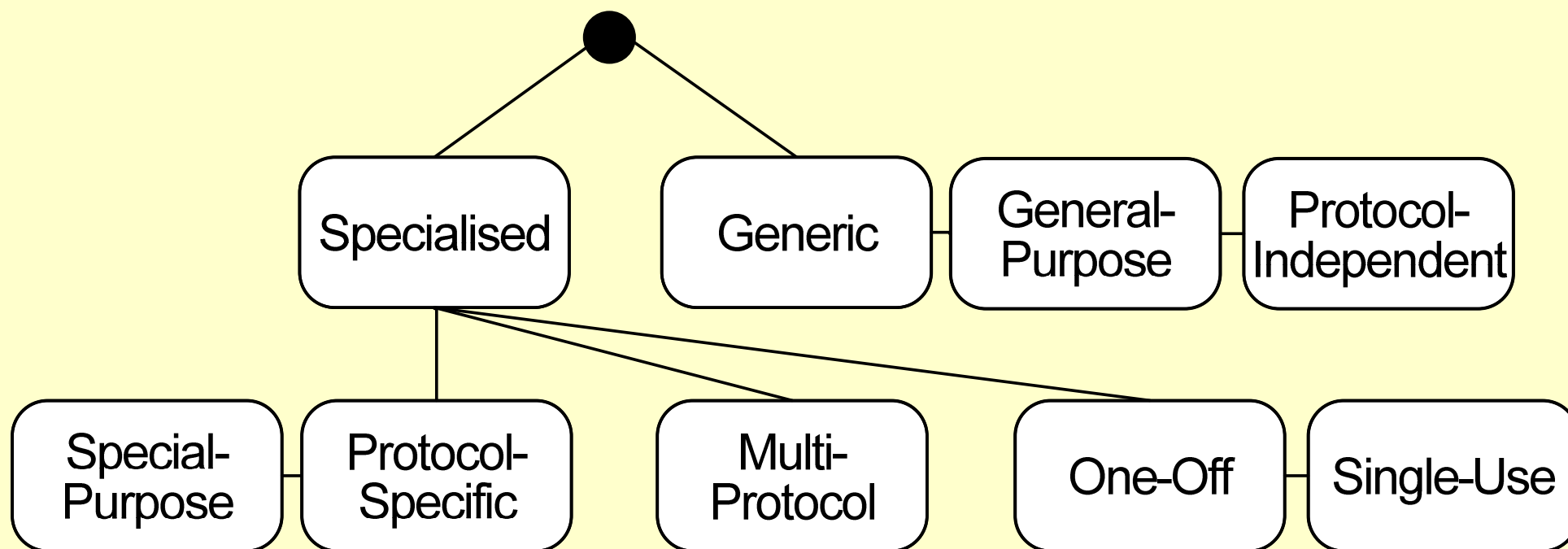
Rapid in-Depth Security Framework (RSF)

activities

1. Tool identification: search strategy- keywords
2. Screening: Taxonomies
3. Tool evaluation: objective, customisable evaluation criteria

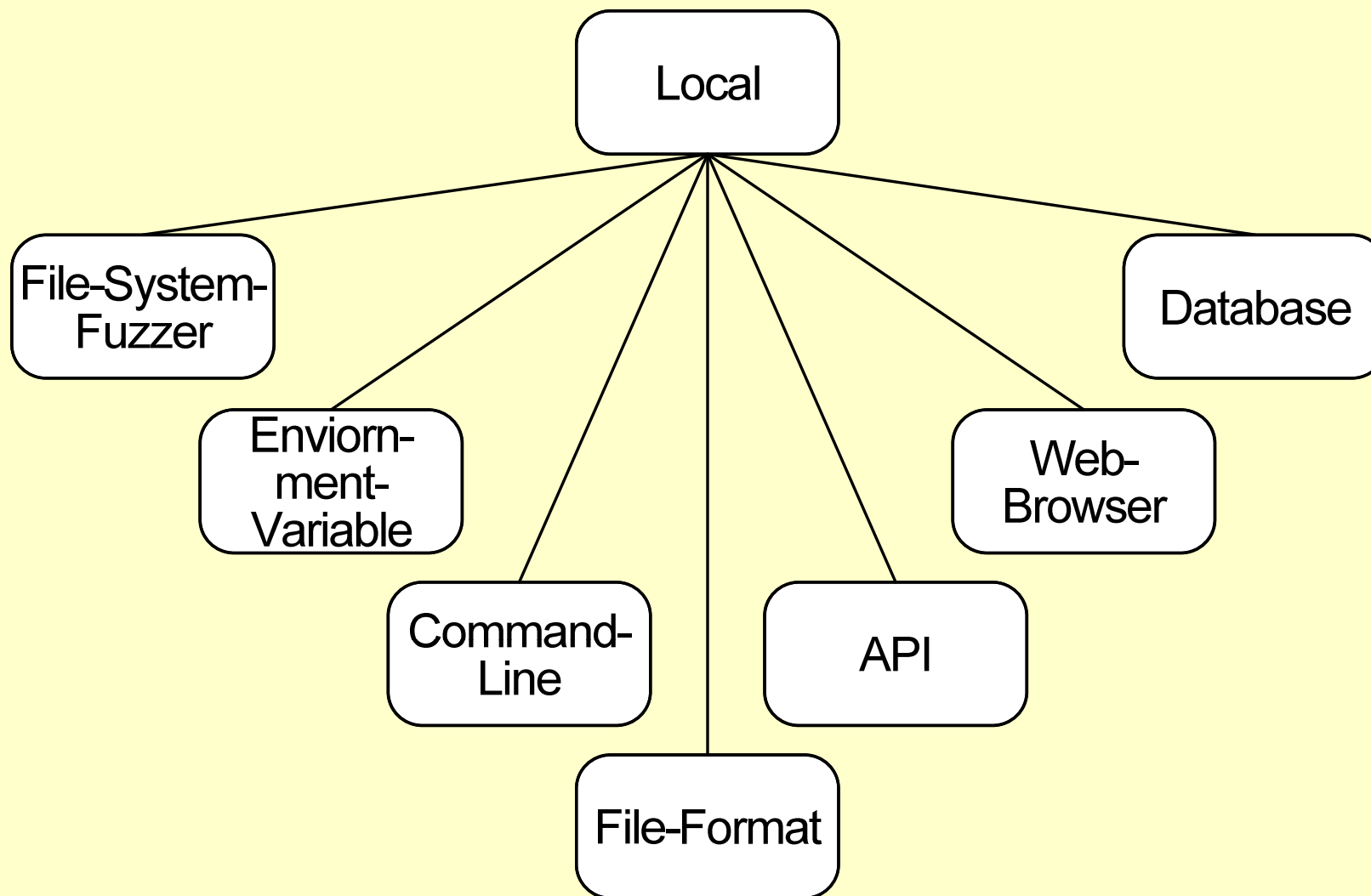
Fuzzer taxonomy

classified by **purpose**



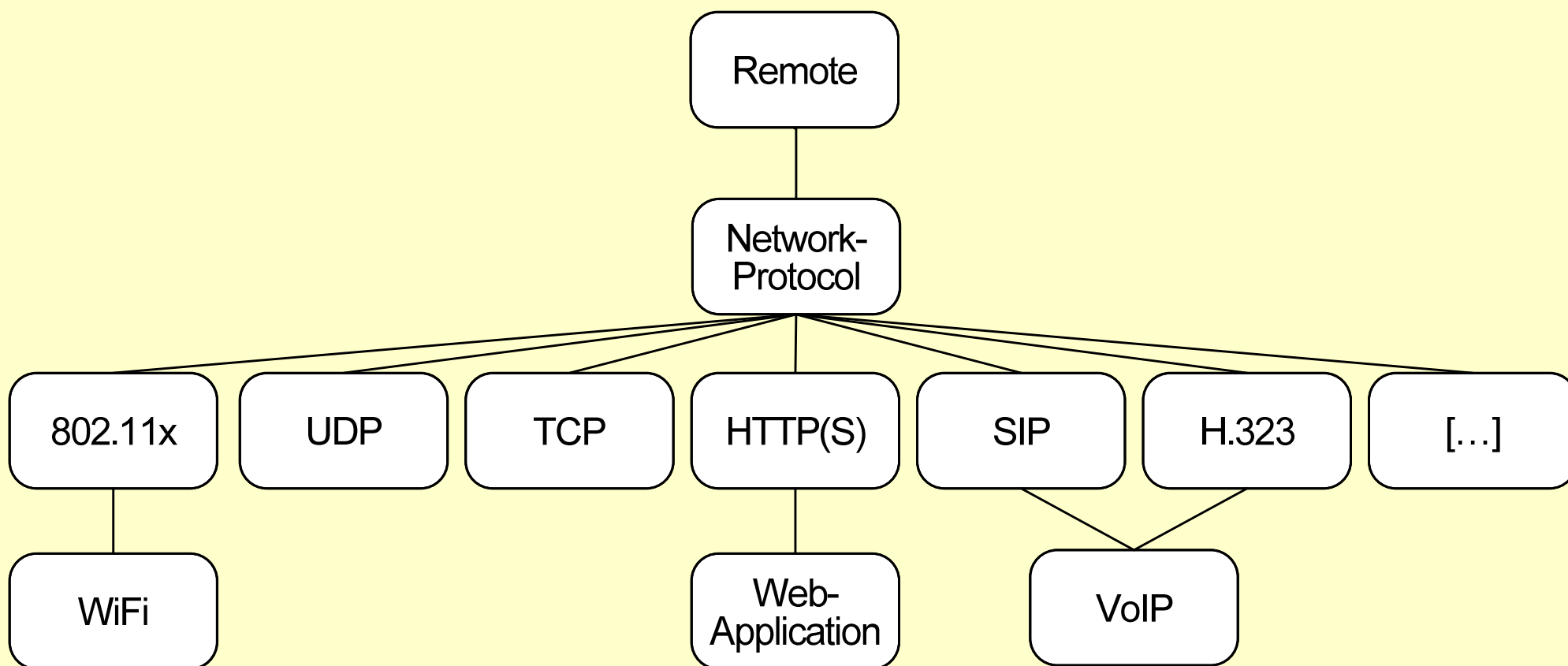
Fuzzer taxonomy

classified by **local interface**



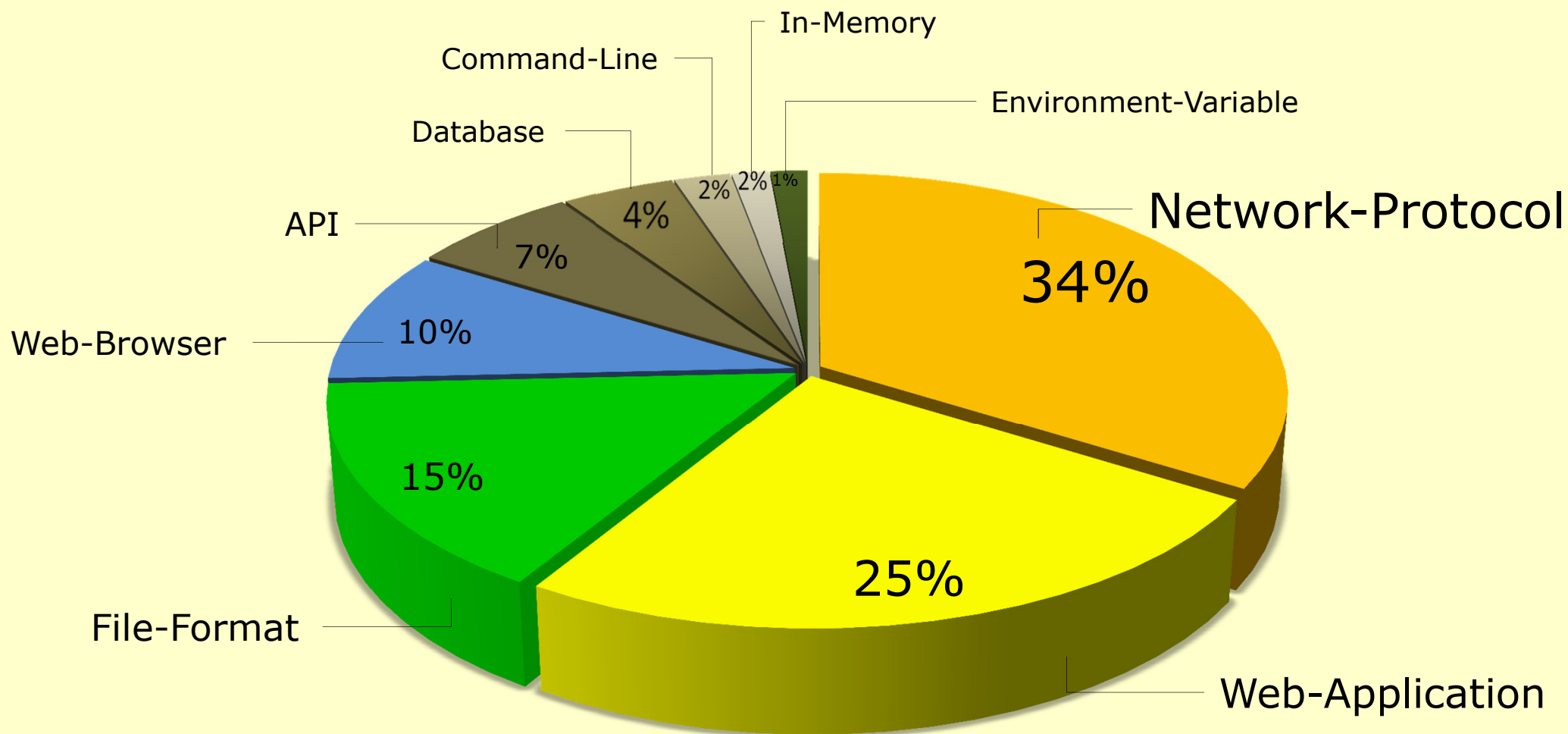
Fuzzer taxonomy

classified by remote interface

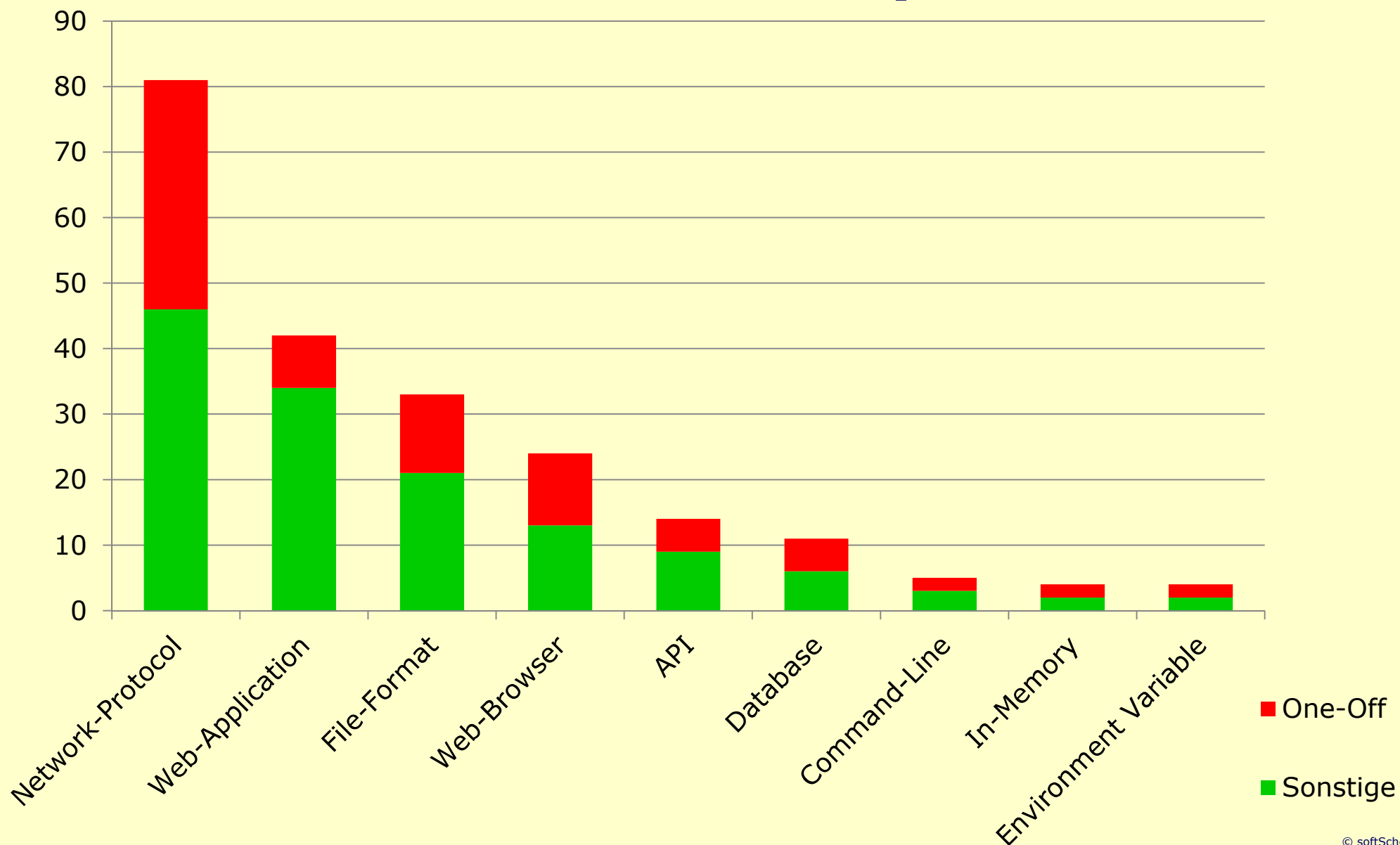


Market analysis Fuzzer: protocol specific

Supported interfaces



One-off Tools: Protocol Specific Fuzzer



Evaluation criteria & description parameter

Product description

Product name

Version

Release date

Developer

Distribution

Source

Available languages

Supported Operating Systems

Protocol modeling

Fuzz-data generation

Intended use

Interfaces

Target interpretation

Costs and license

License type and name

Costs for license

Costs for Updates

Costs for support

Additional paid features

Costs for purchase of additional components

Feature comprehensiveness

Target monitoring

Resetting of the target

Exception analysis

Reporting

Ability to parameterize

Error reproduction

Scheduled tasks

Support for parallel fuzzing

Ability to interrupt fuzzing

Software ergonomics

Effectively

Efficiency

Functional criteria

Dialog criteria

In- and output criteria

Documentation

User manual

Technical documentation

Quality of integrated help system

Quality of the FAQ

Quality of video documentation

Quality of Tutorials and How-to's

Quality of public support forum or similar system

Quality of customer support

Volume of 3rd party documentation

Case studies and Whitepapers

Webinars / Training

Development

Development status

Development activity

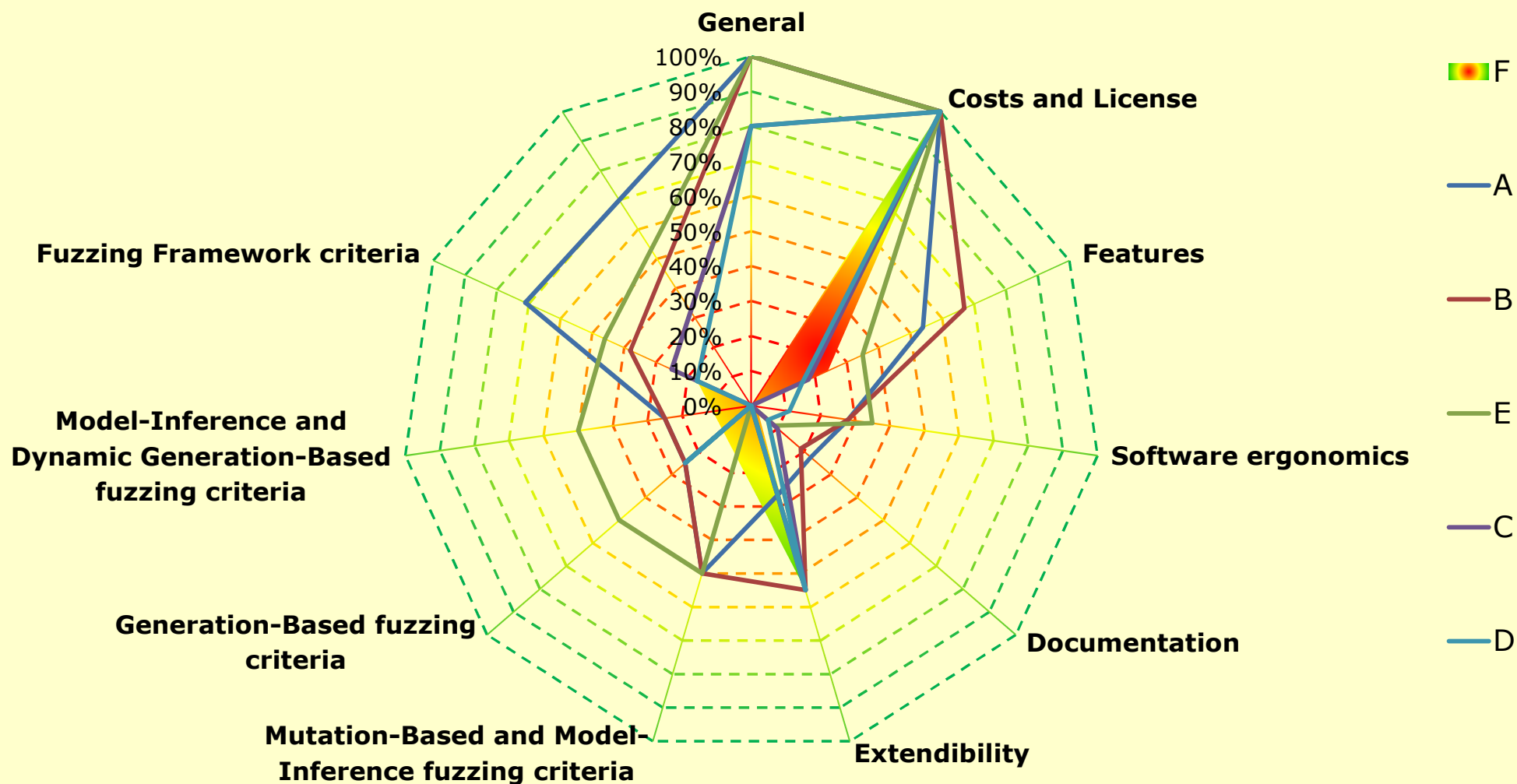
Interfaces for further development

Developer tools

Used programming language

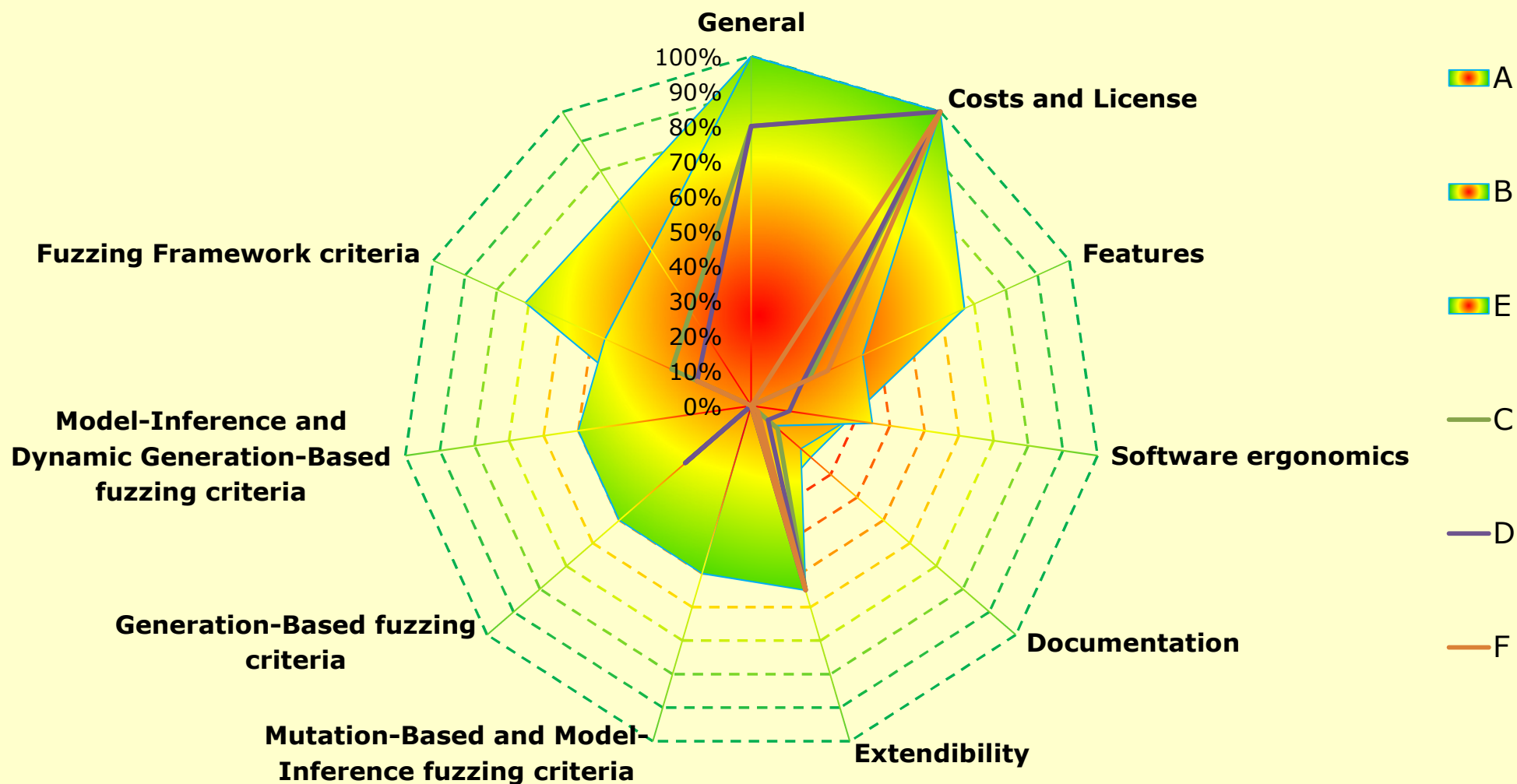
Tool-composition: 1 Tool

Casestudy: Fuzzing Frameworks



Tool-composition: **many Tools**

Casestudy: Fuzzing Frameworks



Test automation

SANS TOP 25 Vulnerabilities

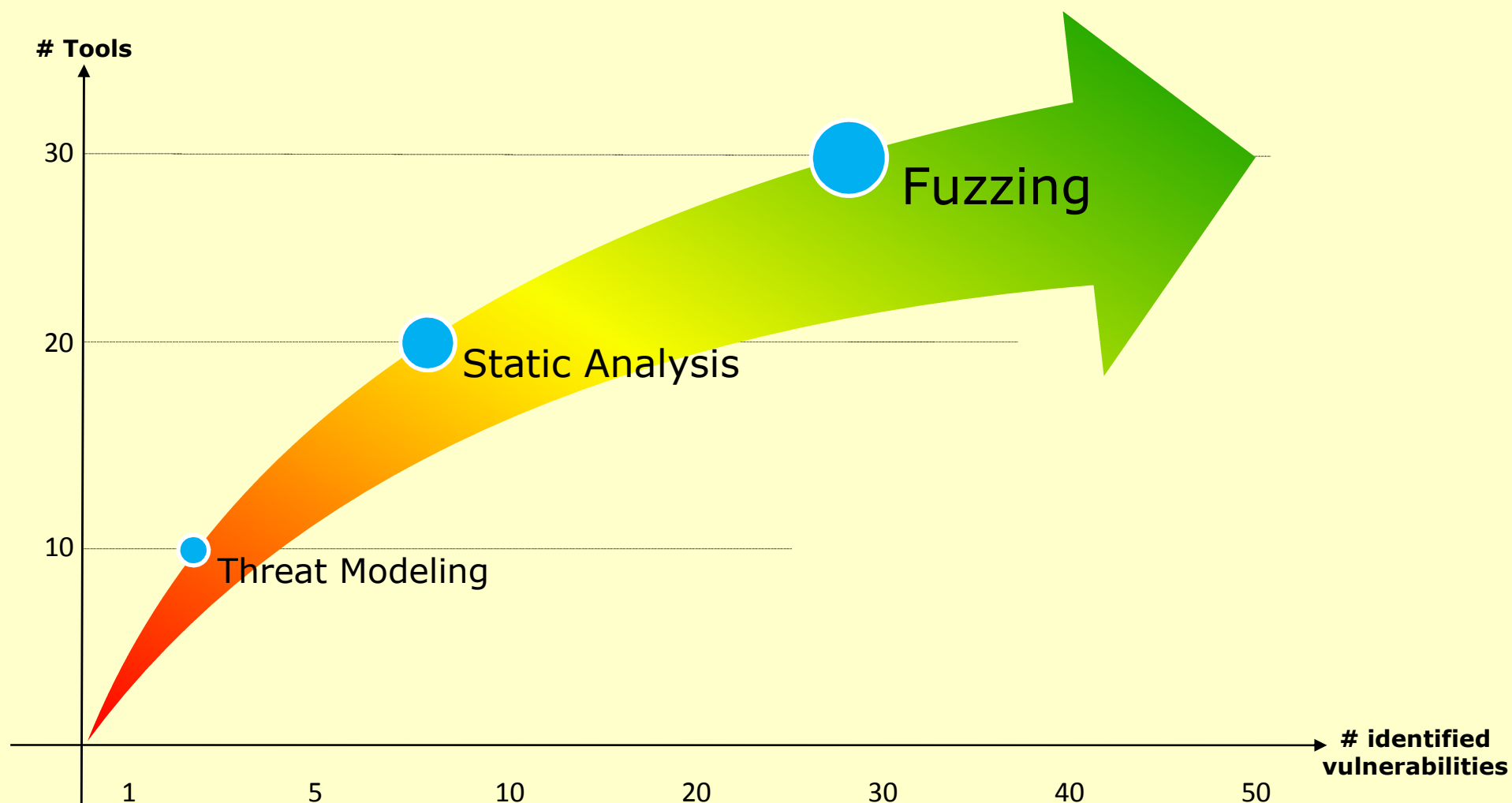
- | | |
|---|---|
| 1. Cross-Site Scripting (XSS) | 15. Improper Check for Unusual or Exceptional Conditions |
| 2. SQL Injection | 18. Incorrect Calculation of Buffer Size (AW) |
| 3. Buffer Overflow | 19. Missing Authentication for Critical Function |
| 7. Path Traversal | 21. Incorrect Permission Assignment for Critical Response |
| 8. Unrestricted Upload of Dangerous File Type | 22. Allocation of Resources Without Limits or Throttling |
| 9. OS Command Injection | 23. Open Redirect |
| 11. Hardcoded Credentials | 24. Use of a Broken or Risky Cryptographic Algorithm |
| 12. Buffer Access with Incorrect Length Value | 25. Race Conditions |
| 13. PHP File Inclusion | |
| 14. Improper Validation of Array Index | |

→ 80% **automated** identifiable: **Blackbox + Whitebox!**

→ 20% **manual** identifiable: e.g. '10. Missing Encryption of Sensitive Data'

Finding all the vulnerabilities: RiDA

Technology- and tool-composition



Future prospects

Rapid in-Depth Analysis Security Suite (RIASS)

- Technology integration: Threat Modeling, Static Analysis, Fuzzing
- Tool integration: up to 300 Tools
- People integration: whole development & product lifecycle

→ **Software development industry**

→ **Consulting industry:** QA, (security)testing industry, Compliance

Prof. Dr. Hartmut Pohl

Hartmut.Pohl@softScheck.com +49 (2241) 9558 - 881

Peter Sakal, B.Sc. M.Sc.

Peter.Sakal@softScheck.com +49 (2241) 9558 - 882

www.softScheck.com