



E P O C H E & E S P R I

Vulnerability Analysis Taxonomy

Achieving completeness in a systematic way

Javier Tallón Guerri
10ICCC - Norway



1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

4. Lessons learned



1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

4. Lessons learned



1. Vulnerability Analysis according to CEM

- The evaluator vulnerability analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a Basic (for AVA_VAN.1 and AVA_VAN.2), Enhanced-Basic (for AVA_VAN.3), Moderate (for AVA_VAN.4) or High (for AVA_VAN.5) attack potential.

- Independent vulnerability analysis should consider generic potential vulnerabilities under each of the following headings
 - Bypassing
 - Tampering
 - Direct attacks
 - Monitoring
 - Misuse



1. Vulnerability Analysis according to CEM

- Due to the generic nature of the Common Criteria, this classification is too abstract and does not help to achieve the required completeness to the evaluator's work.
- CEM classification is useless by itself

1. Vulnerability Analysis according to CEM

- From AVA_VAN.4, vulnerability analysis should be **METHODICAL**:
"This method requires the evaluator to specify the structure and form the analysis will take"
- CEM ask for a methodical analysis but does not provide any method.
→ Every method would be acceptable

1. Vulnerability Analysis according to CEM





1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

4. Lessons learned

2. Pieces for a correct Vulnerability Analysis



- Here is the question...

How to achieve completeness in a systematic way?

- We will focus in software assessment



1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

4. Lessons learned

2.1 Attack Patterns

Very generic
vulnerability
classification

Vs

Attack Patterns

- Thinking like bad guys



2.1 Attack Patterns

- Attack Pattern: an attack pattern describes the approach used by attackers to generate an exploit against software.

- For example: MITRE provides CAPEC (Common Attack Pattern Enumeration and Classification)

2.1 Attack Patterns



Common Attack Pattern Enumeration and Classification

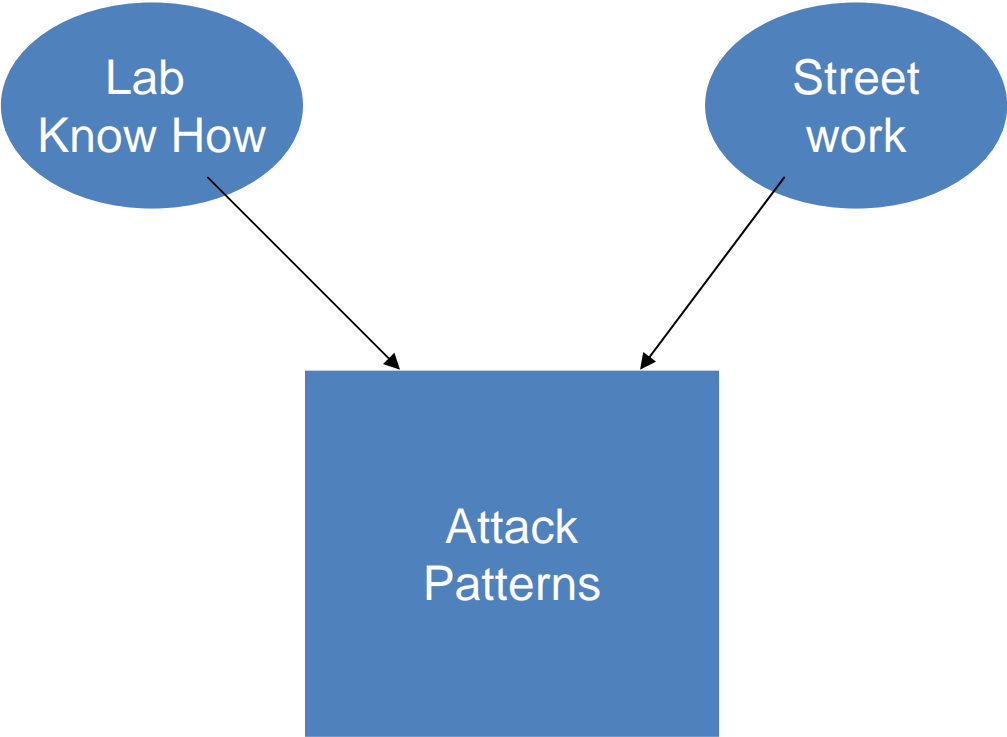
- ☐ Abuse of Functionality
- ☐ Spoofting - (156)
- ☐ Probabilistic Techniques
- ☐ Exploitation of Authentication
- ☐ Resource Depletion - (119)
- ☐ Exploitation of Privilege/Trust
- ☐ Injection (Injecting Control Plane content through the Data Plane) - (152)
- ☐ Data Structure Attacks
- ☐ Data Leakage Attacks - (118)
- ☐ Resource Manipulation
- ☐ Time and State Attacks - (172)



2.1 Attack Patterns

- CAPEC provides a free collection of attack patterns
- CAPEC is not the panacea
- **Each lab should manage its own attack pattern collection**

2.1 Attack Patterns





1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

4. Lessons learned

2.2 Systematic and Repeatable Methodology

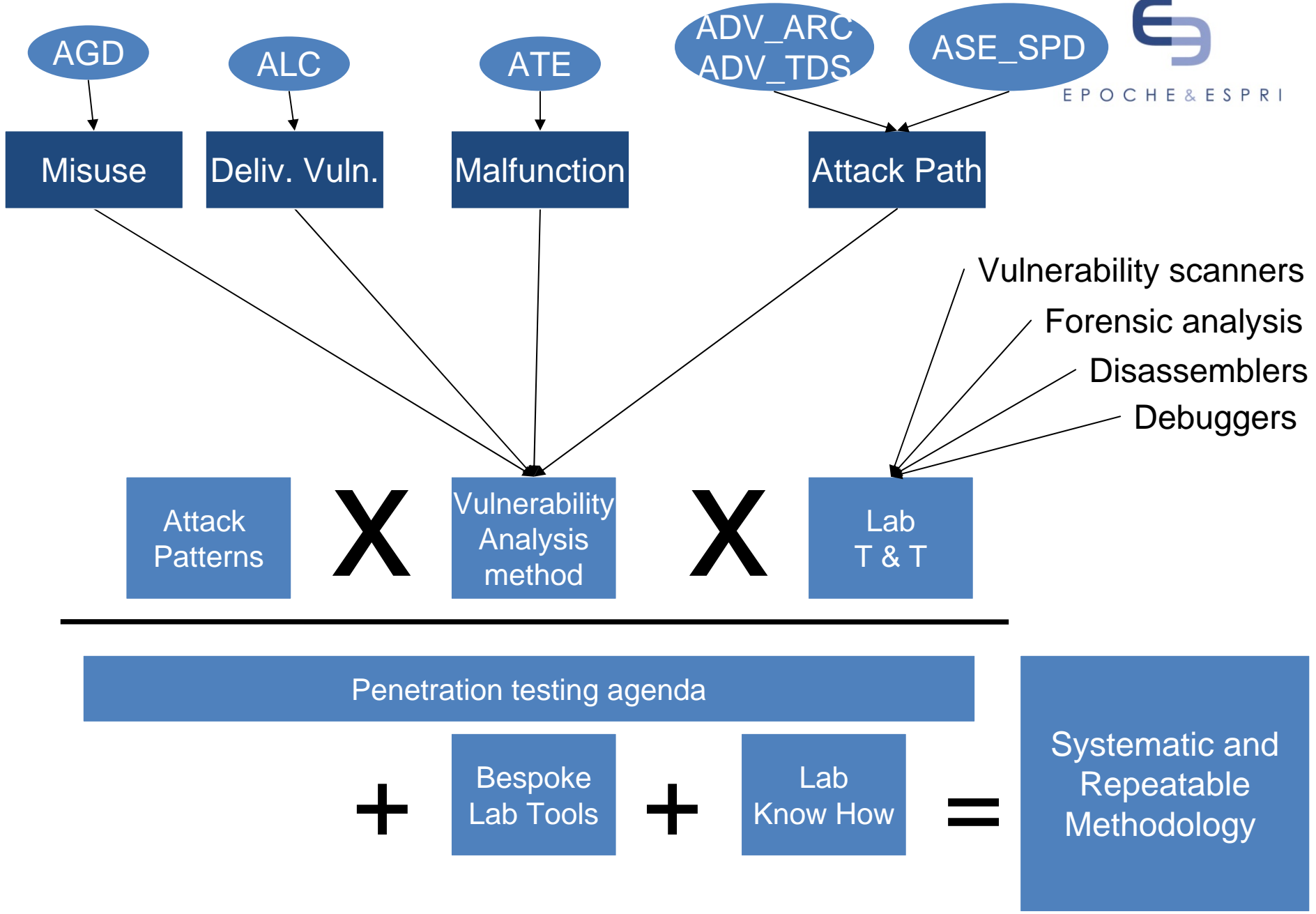
Undefined
Methodology

Vs

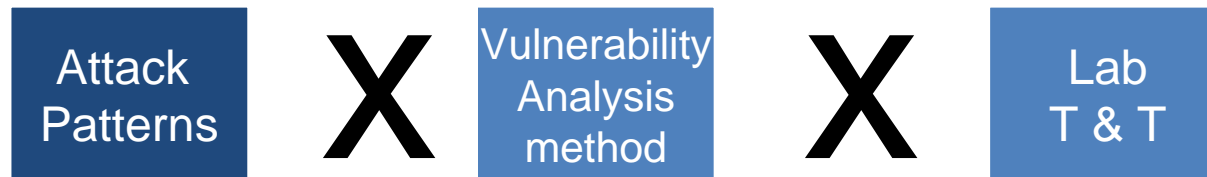
Systematic and
Repeatable
Methodology



EPOCHÉ & ESPRI



2.2 Systematic and Repeatable Methodology



Penetration testing agenda

2.2 Systematic and Repeatable Methodology



Attack
Patterns

X

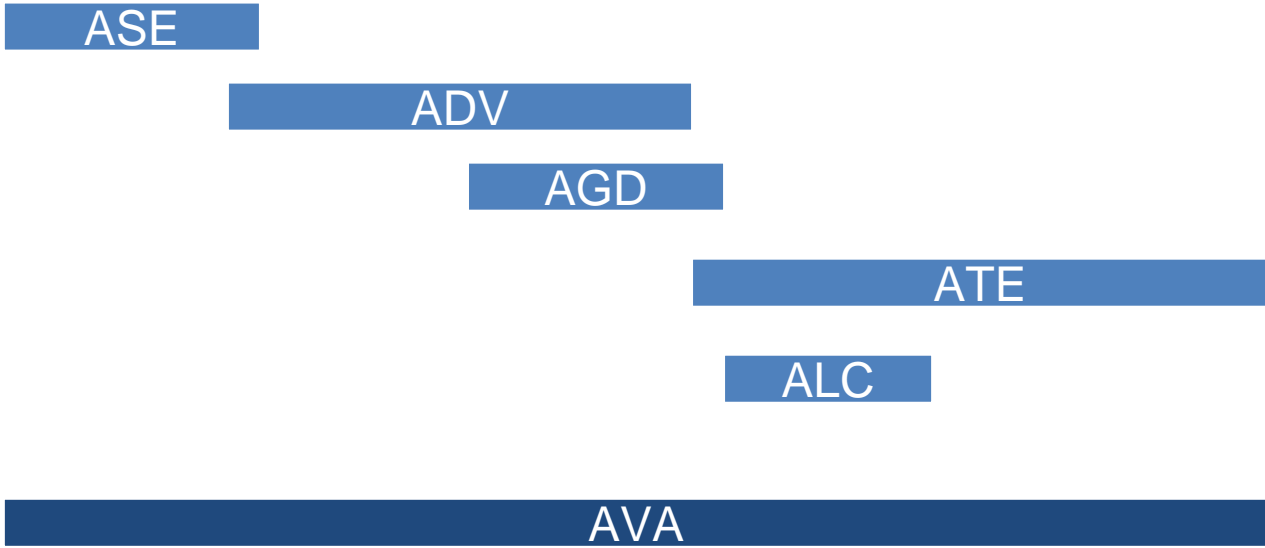
Vulnerability
Analysis
method

X

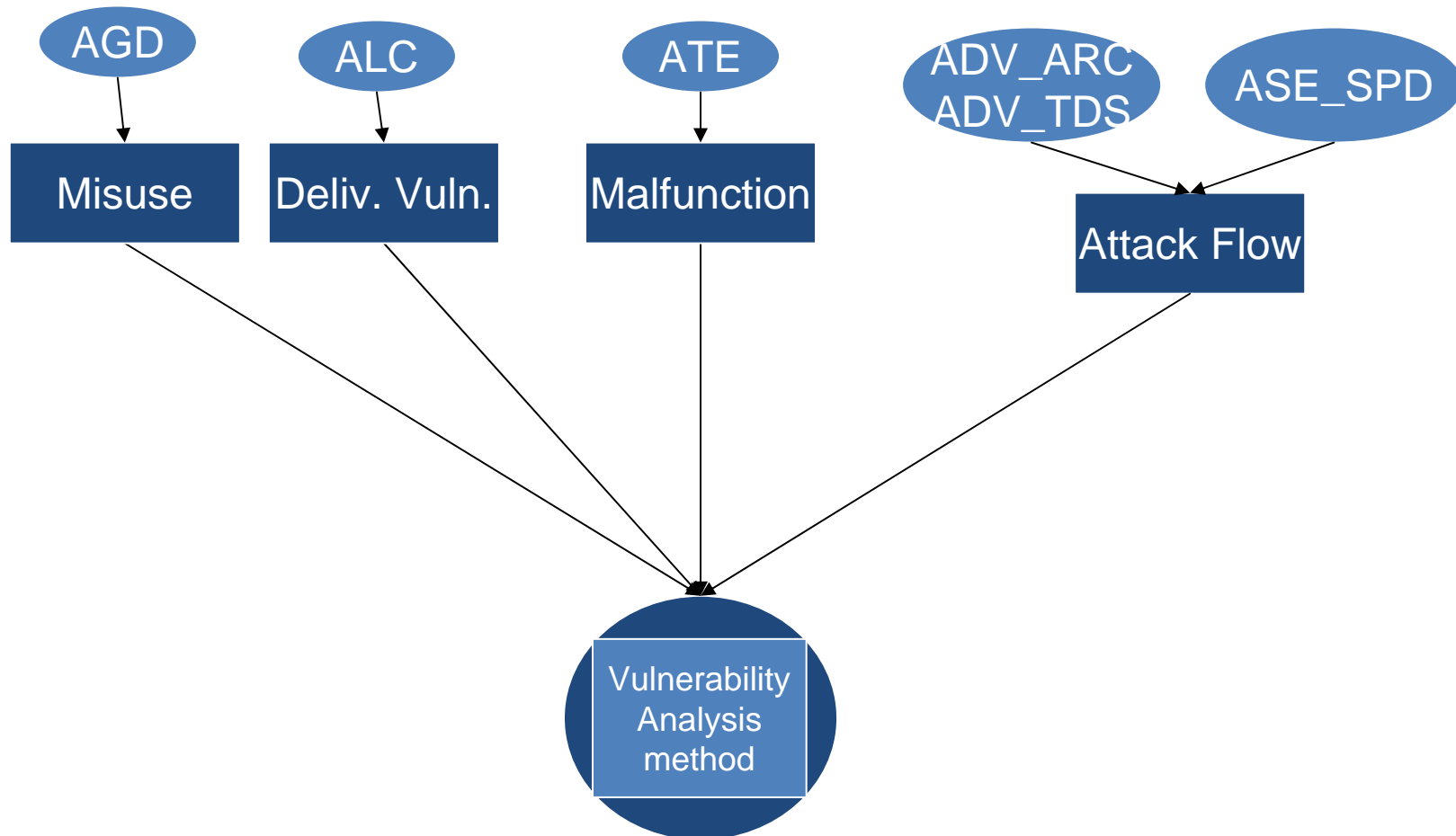
Lab
T & T

Penetration testing agenda

2.2 Systematic and Repeatable Methodology



2.2 Systematic and Repeatable Methodology



2.2 Systematic and Repeatable Methodology



Attack
Patterns

X

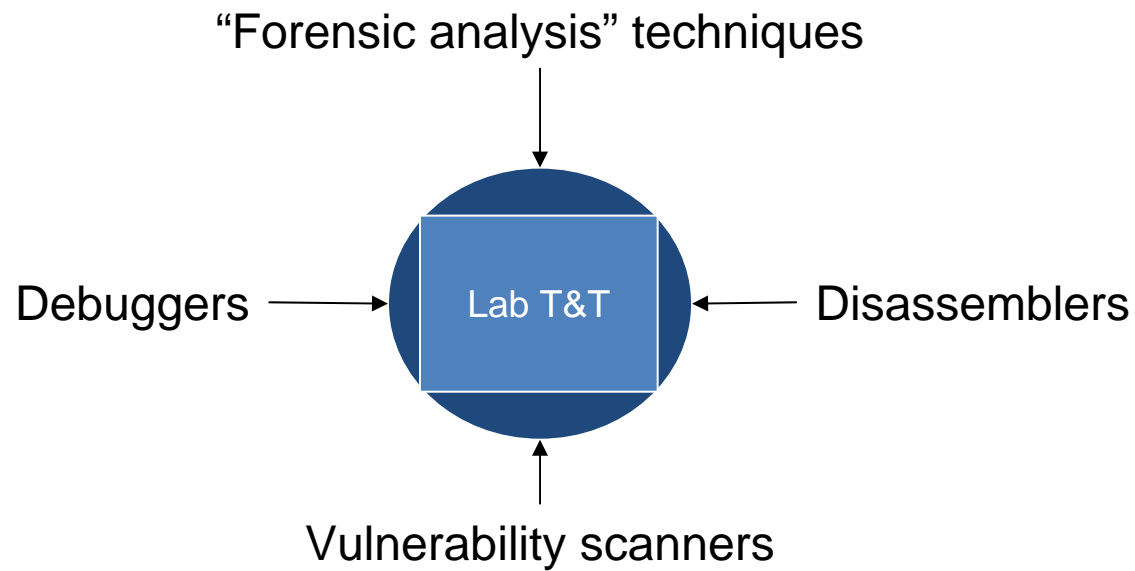
Vulnerability
Analysis
method

X

Lab
T & T

Penetration testing agenda

2.2 Systematic and Repeatable Methodology



2.2 Systematic and Repeatable Methodology



E P O C H E & E S P R I

Attack
Patterns

X

Vulnerability
Analysis
method

X

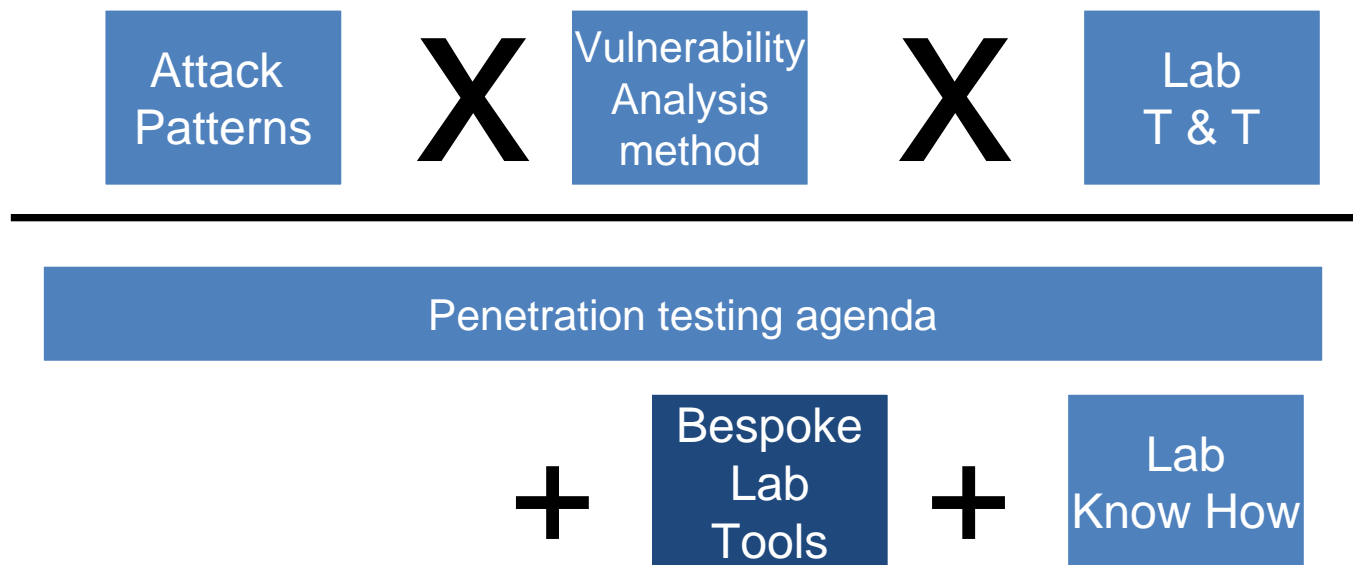
Lab
T & T

Penetration testing agenda

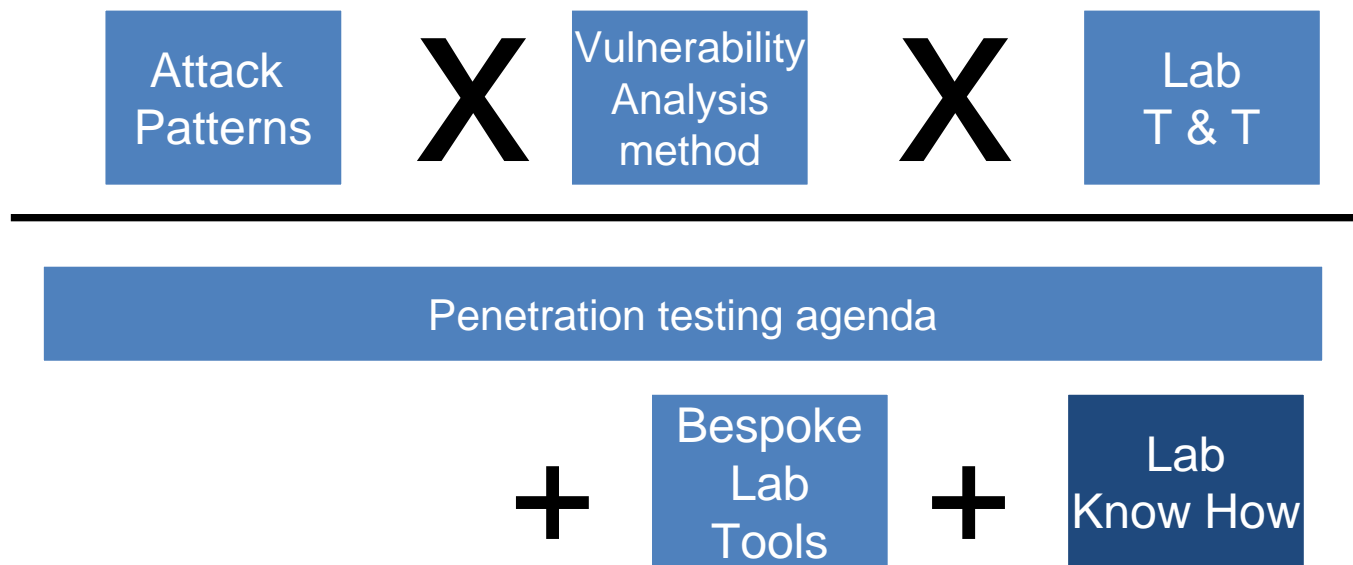
2.2 Systematic and Repeatable Methodology



E P O C H E & E S P R I

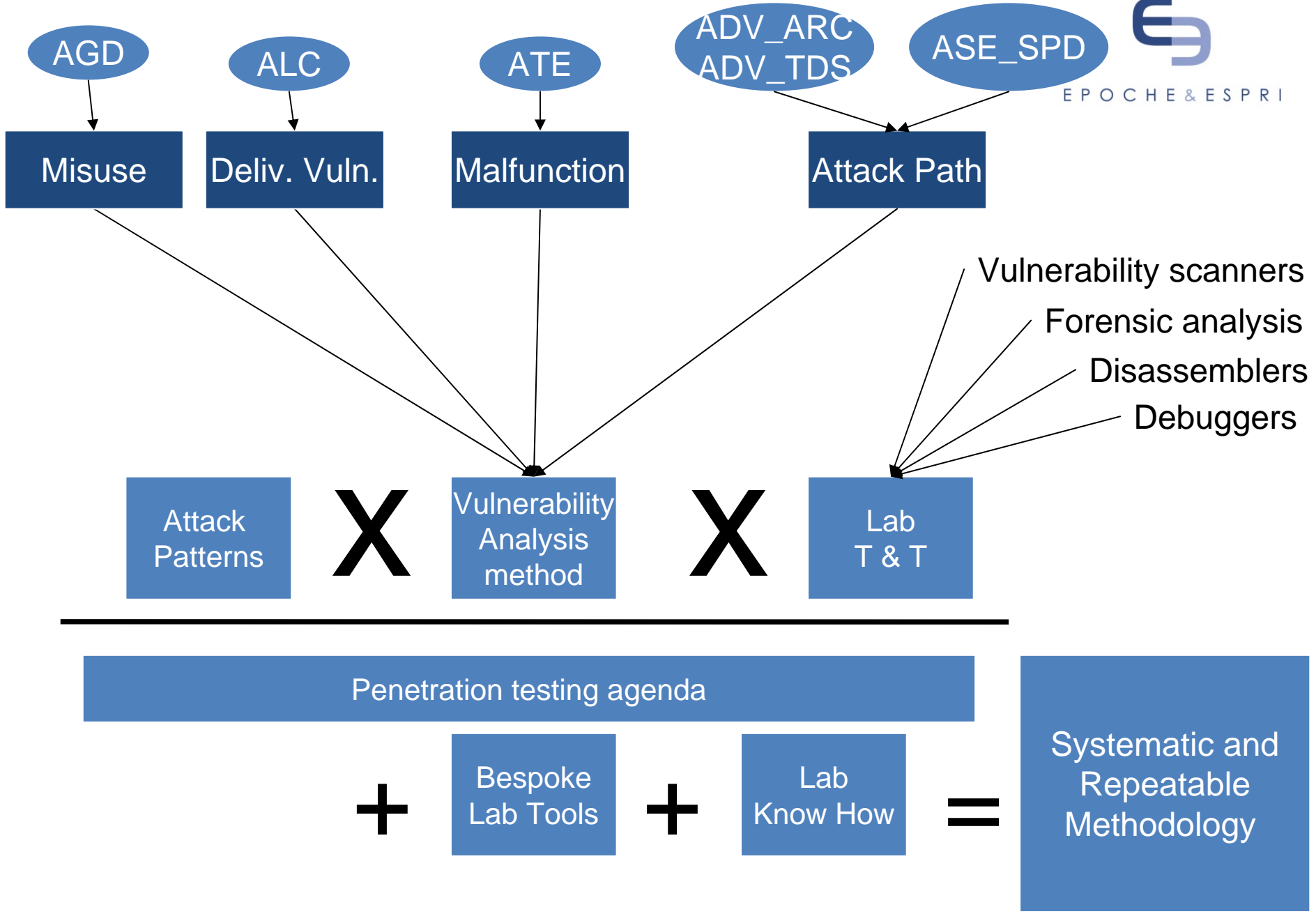


2.2 Systematic and Repeatable Methodology





EPOCHÉ & ESPRI





1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

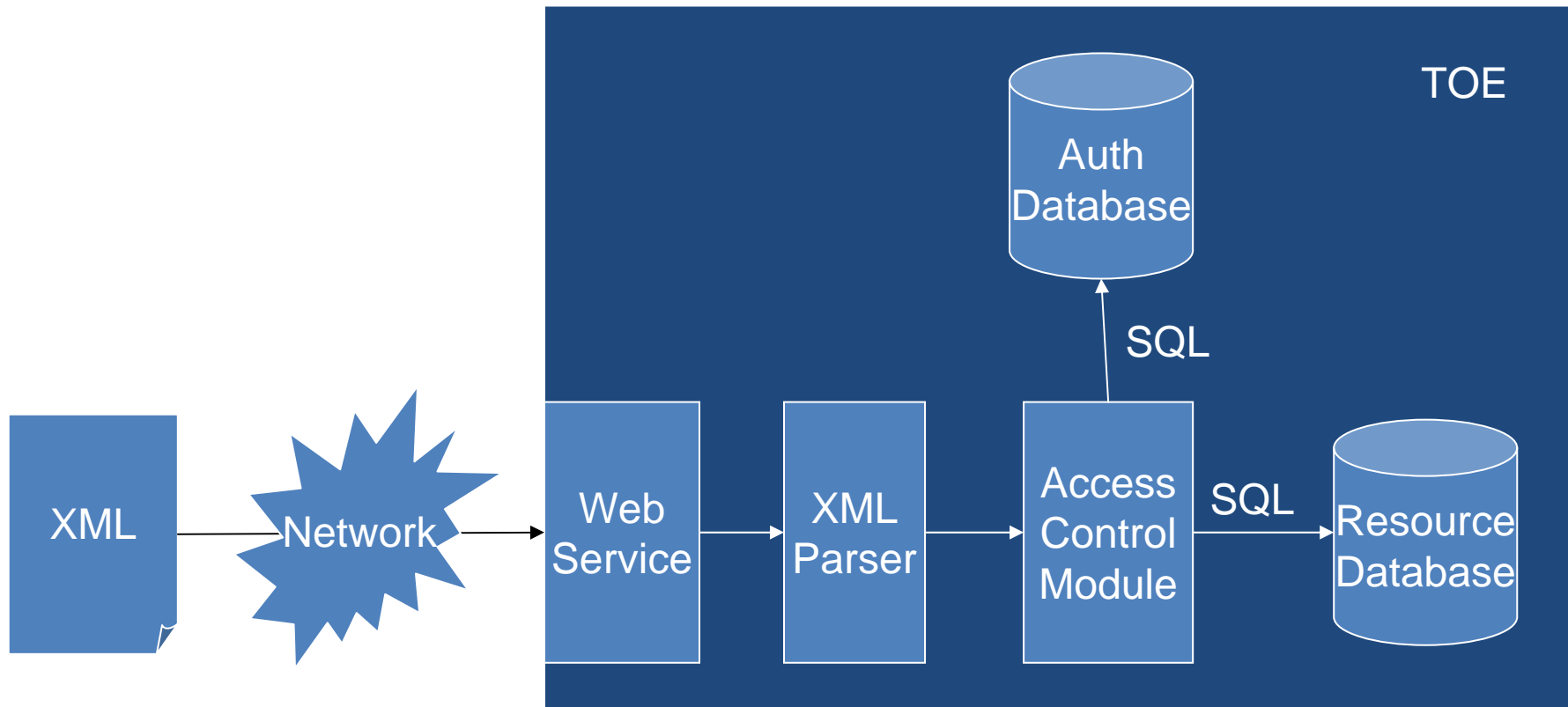
1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

4. Lessons learned

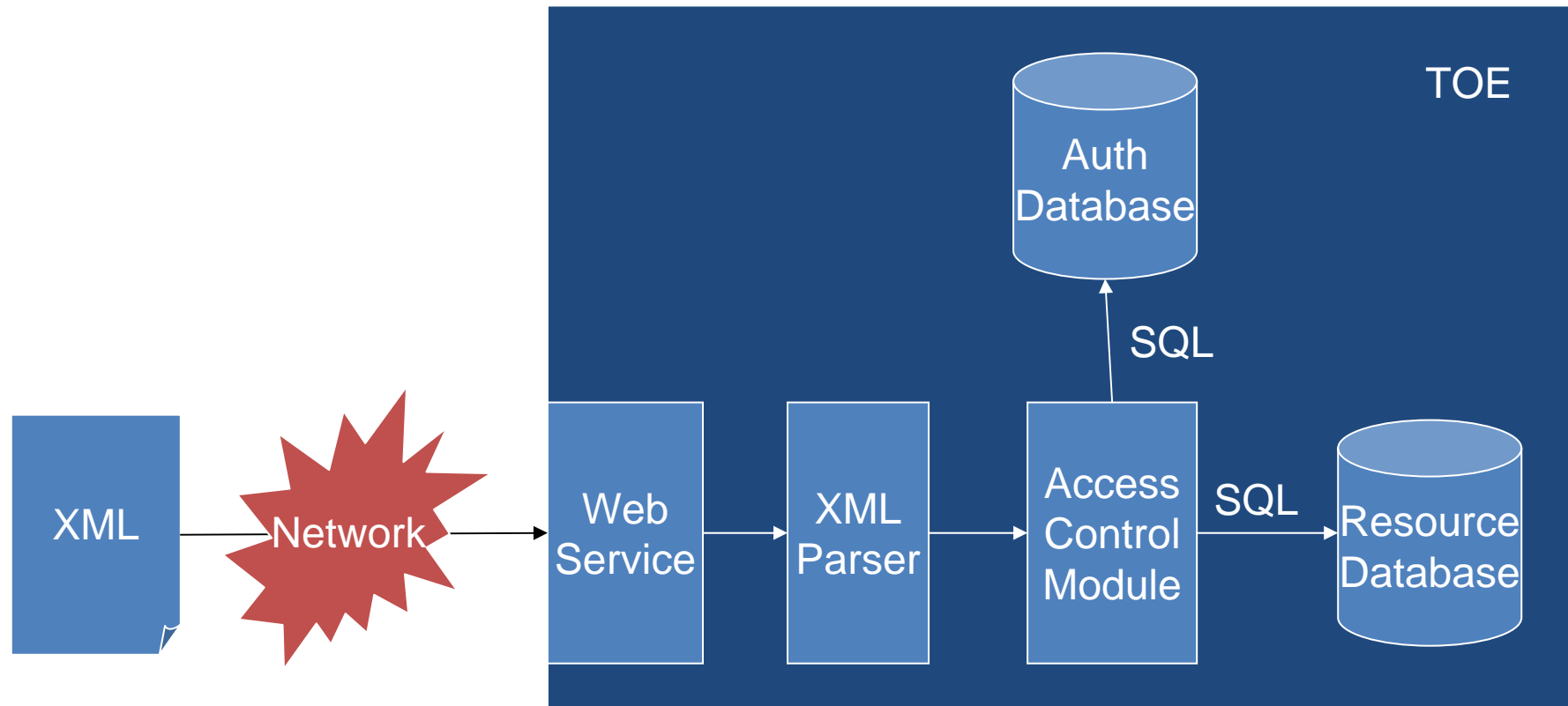
3. Example



3. Example



E P O C H E & E S P R I

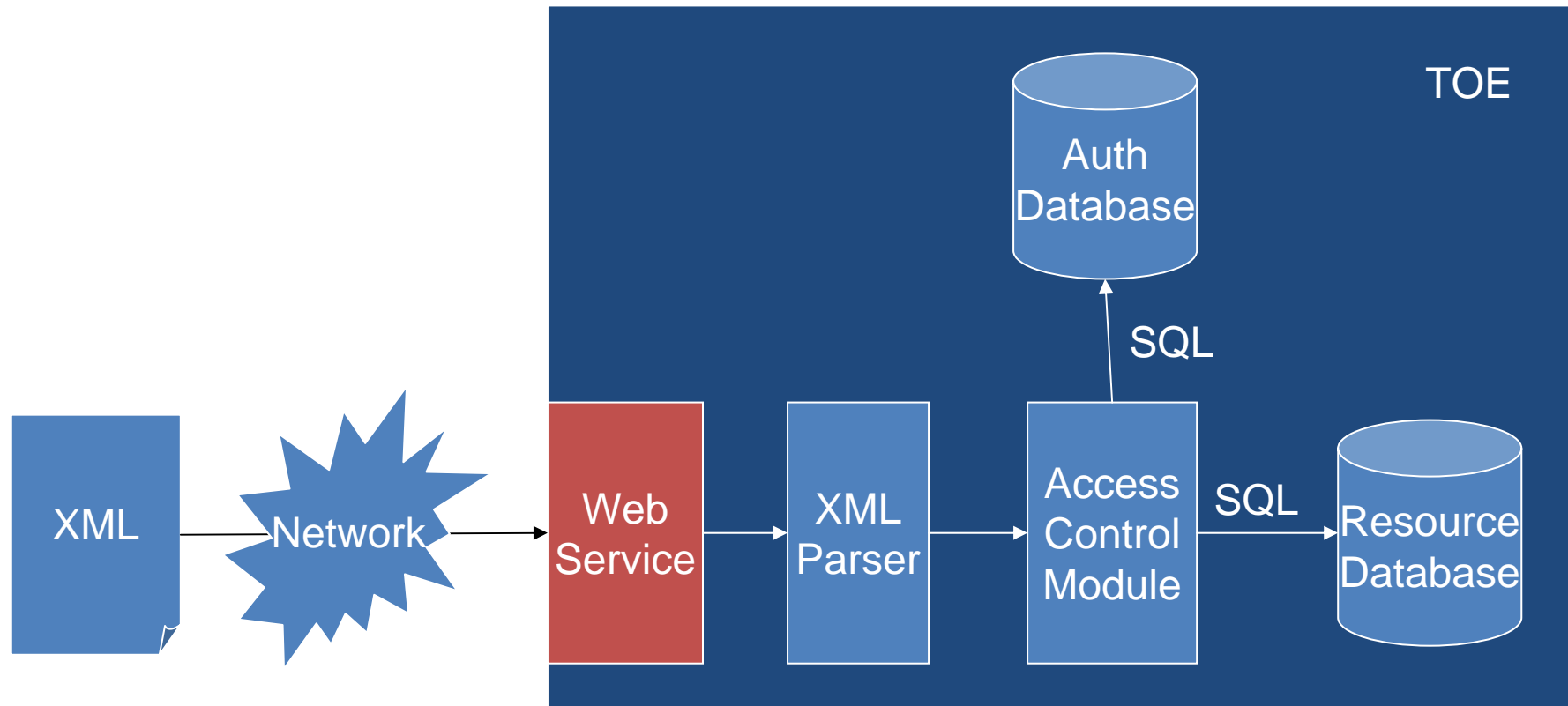


Sniffing Attacks
Man in the Middle
Denial of Service through Resource Depletion

3. Example



EPOCHESPRI

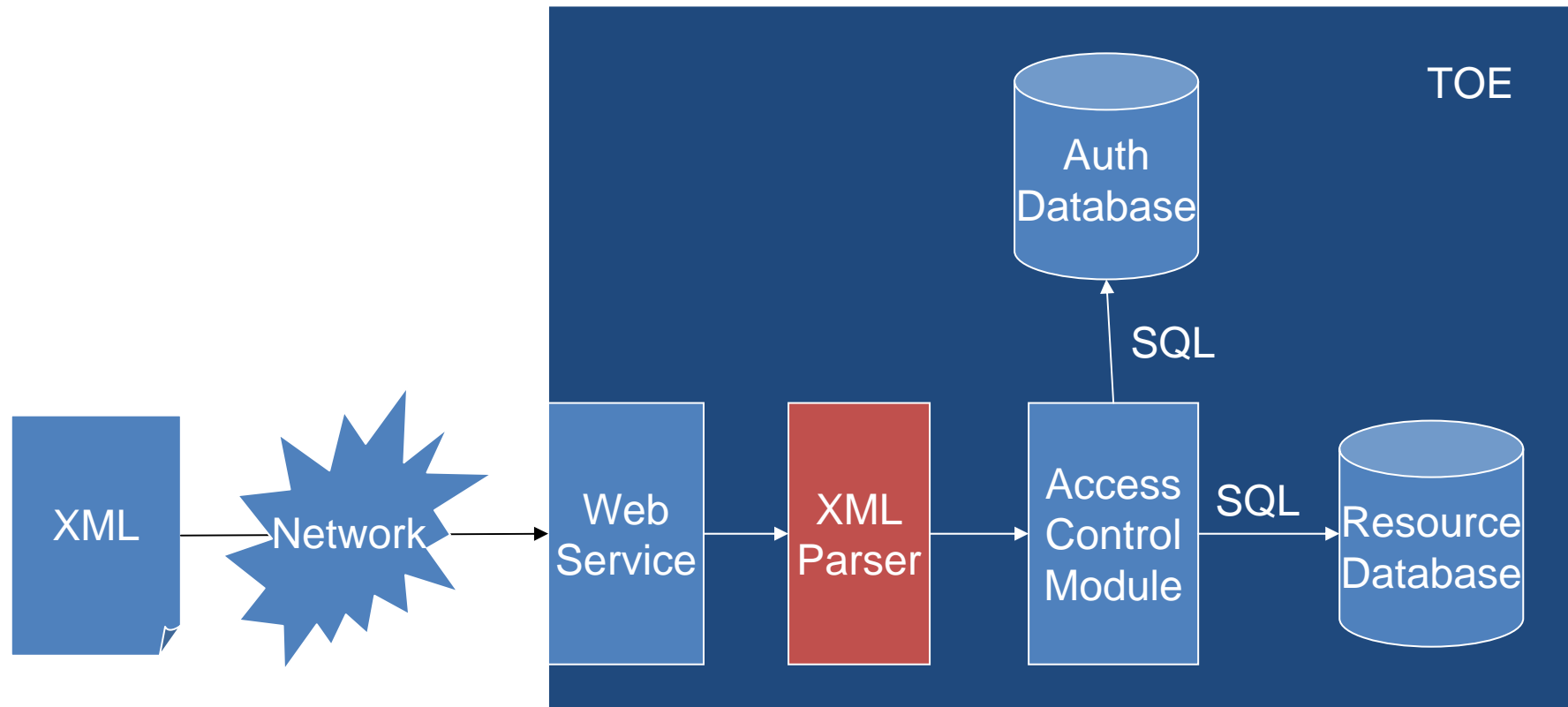


Detect Unpublicized Web Services
Web Services Protocol Manipulation

3. Example



E P O C H E & E S P R I



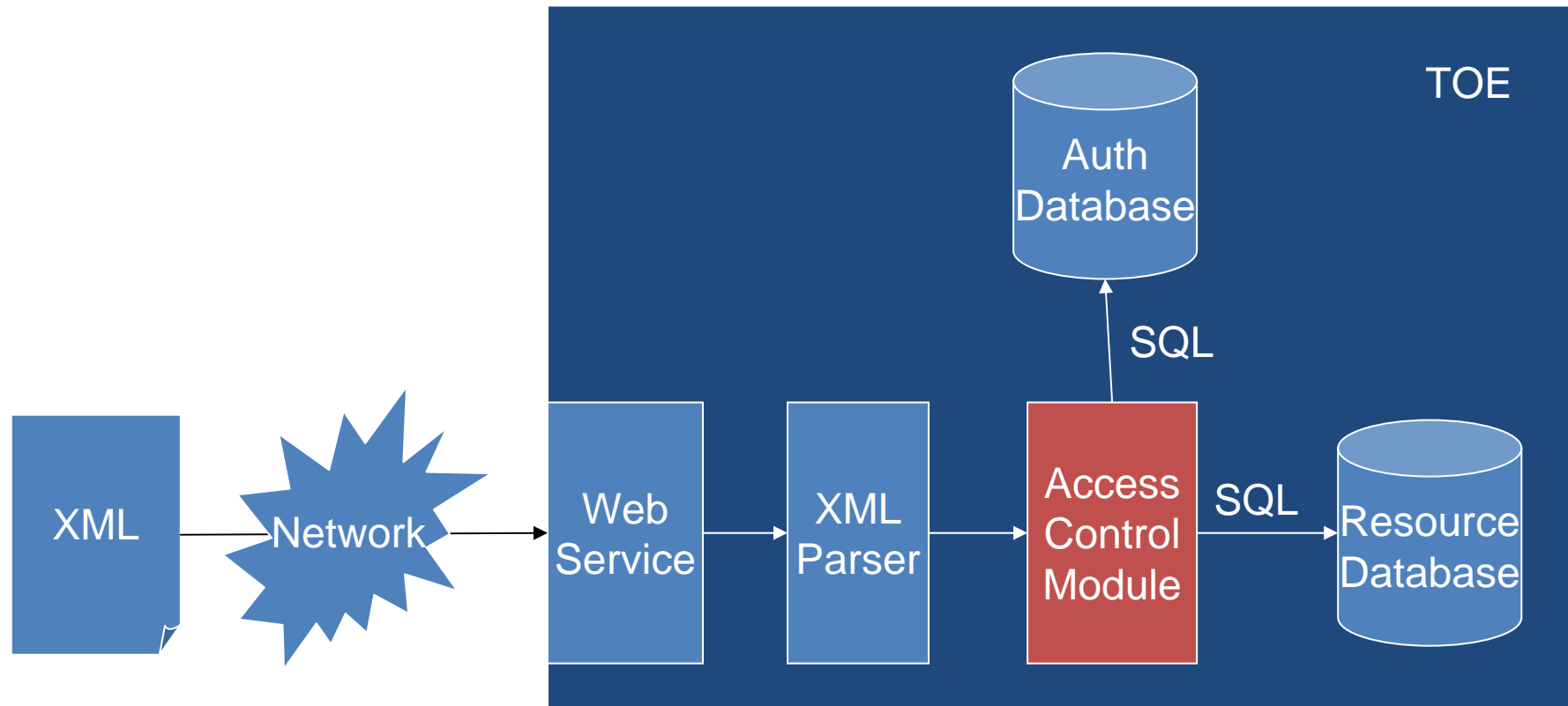
XML Routing Detour Attacks
XEE (XML Entity Expansion)
XML Attribute Blowup
Recursive Payloads Sent to XML Parsers

Oversized Payloads Sent to XML Parsers
XML Ping of Death
XML Schema Poisoning
XML Injection

3. Example



E P O C H E & E S P R I



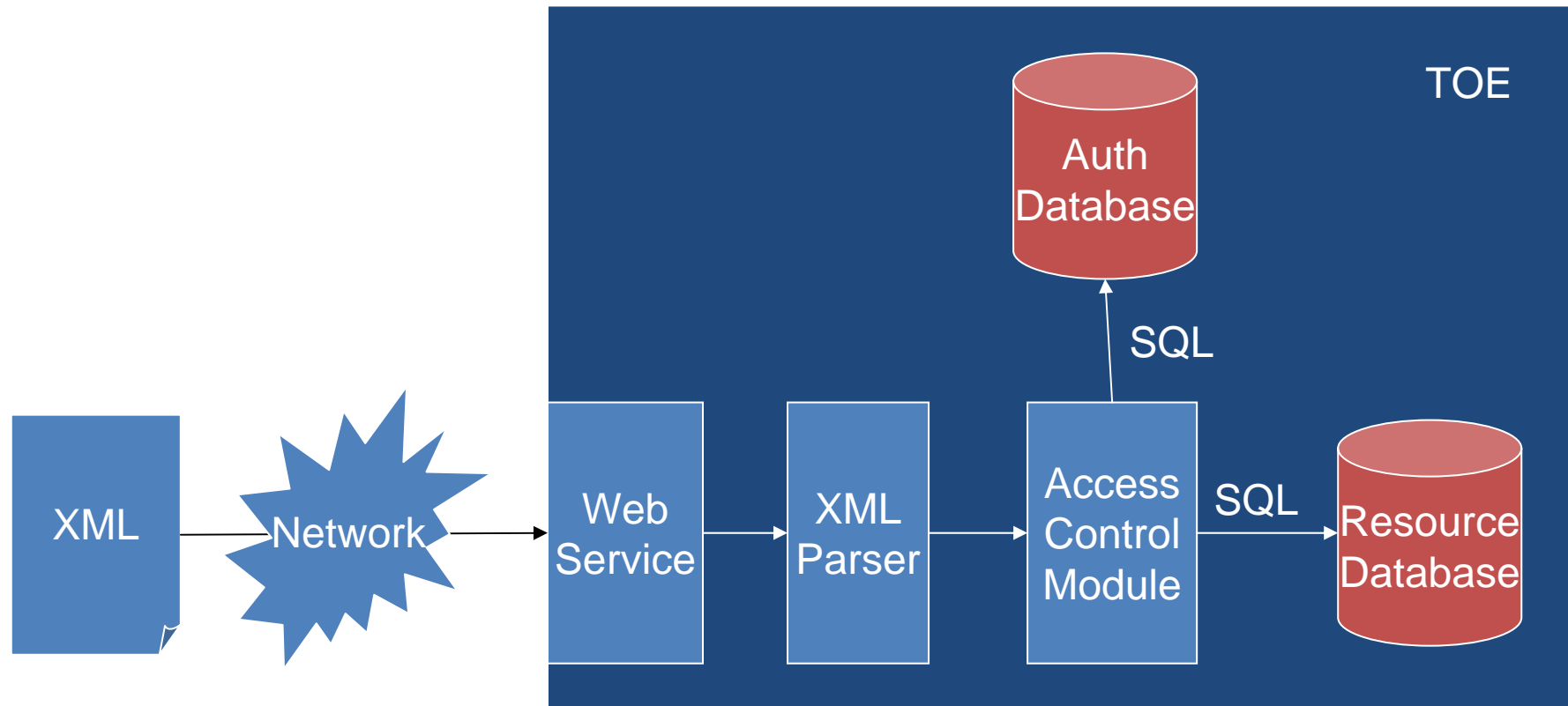
Authentication Bypass
Authentication Abuse
Reflection Attack in Authentication Protocol
Exploitation of Session Variables, Resource IDs and other
Trusted Credentials

Password Brute Forcing
Try Common (default) Usernames and Passwords
Dictionary-based Password Attack

3. Example



EPOCHÉ & ESPRI



SQL Injection
Blind SQL Injection



1. Vulnerability Analysis according to CEM

2. Pieces for a correct vulnerability analysis

1. Attack Patterns

2. Systematic and repeatable methodology

3. Example

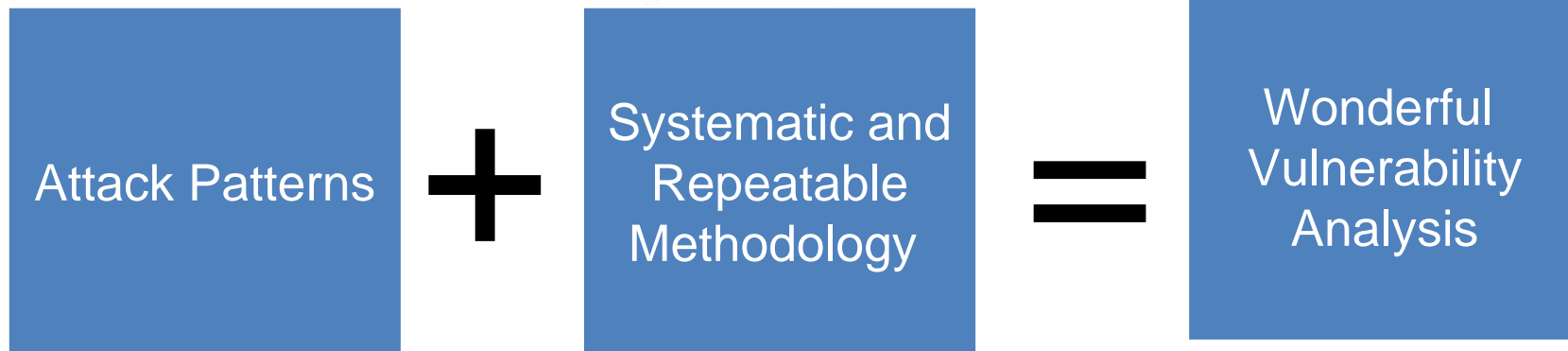
4. Lessons learned

4. Lessons learned

Motivation



Creativity





E P O C H E & E S P R I

Thanks for your attention!

Javier Tallón

Epoche & Espri, S.L.
Avda. de la Vega, 1
28108, Alcobendas,
Madrid, Spain.

eval@epoche.es