Business from technology

”OPC UA Security Testing”

(Brief introduction)

OPC Day 18.10.2016 (Beckhoff, Hyvinkää)

Pasi Ahonen & Sami Noponen
VTT Technical Research Centre of Finland

Before starting, the penetration tester needs to know

Who is bad?

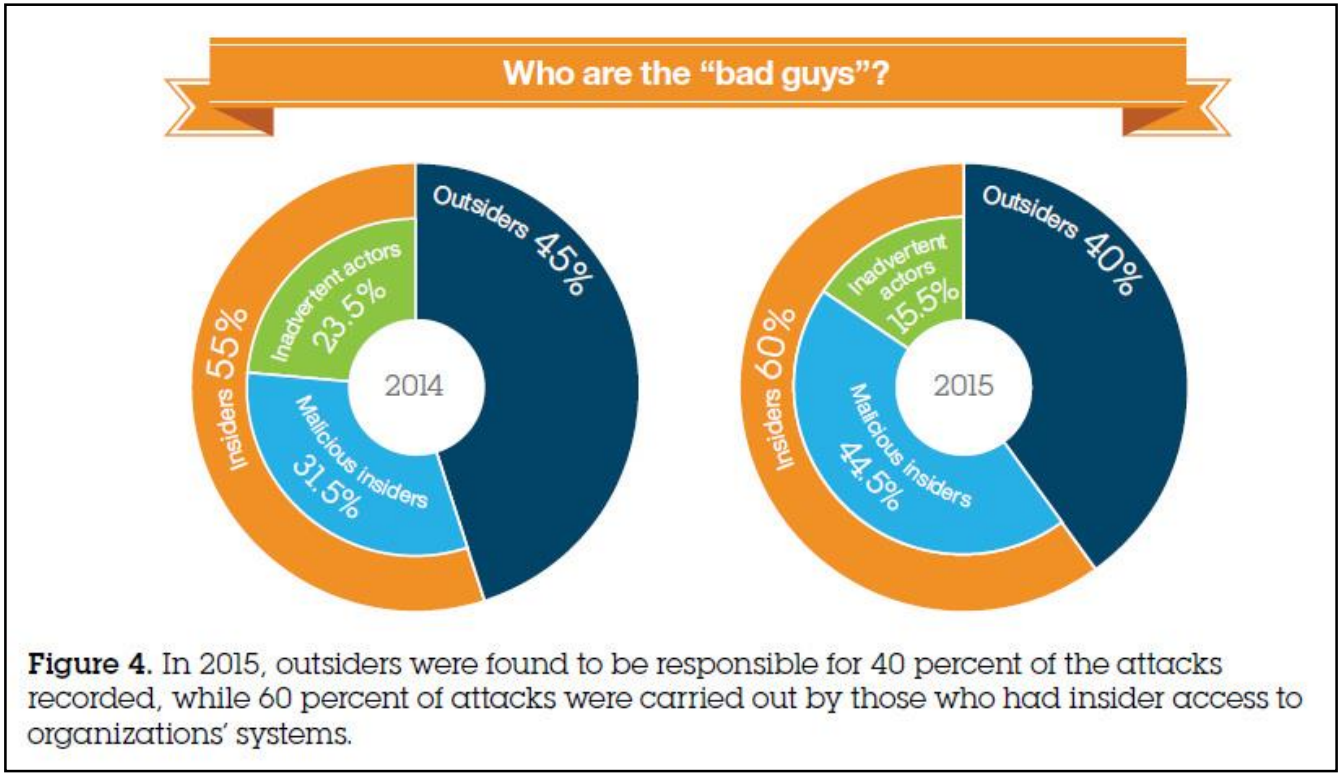


Figure 4. In 2015, outsiders were found to be responsible for 40 percent of the attacks recorded, while 60 percent of attacks were carried out by those who had insider access to organizations' systems.

Ref: "Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations", IBM X-Force® Research, 2016 Cyber Security Intelligence Index.

The cybercrime business is now PROFESSIONAL SERVICES!

List of activity categories

1. Crypting services
2. Dedicated servers
3. SOCKS proxy
4. VPN
5. PPI
6. Programming
7. DDoS services
8. Spam
9. C&C
10. Antivirus (AV) check
11. Laundering
12. File Transfer Protocol (FTP) accounts
13. Trojans
14. Rootkits
15. Carders
16. Social engineering
17. Account hacking
18. Document scan resale
19. Abuse services
20. SMS fraud
21. Ransomware
22. Obfuscation
23. Serials
24. Exploit
25. iMoney
26. Fake
27. Traffic
28. SEO
29. Money schemas
30. Web shell
31. Database
32. Remote access tool (RAT)
33. Online gaming accounts
34. Jabber
35. Android application package (APK) development
36. Fake APK software
37. Mobile traffic
38. Mobile fraud

Tester needs to understand what "services" attacker uses

Ref: TREND MICRO (2015), Russian Underground 2.0.

How to improve testing? – Together!

Industries

NESTE

TVO

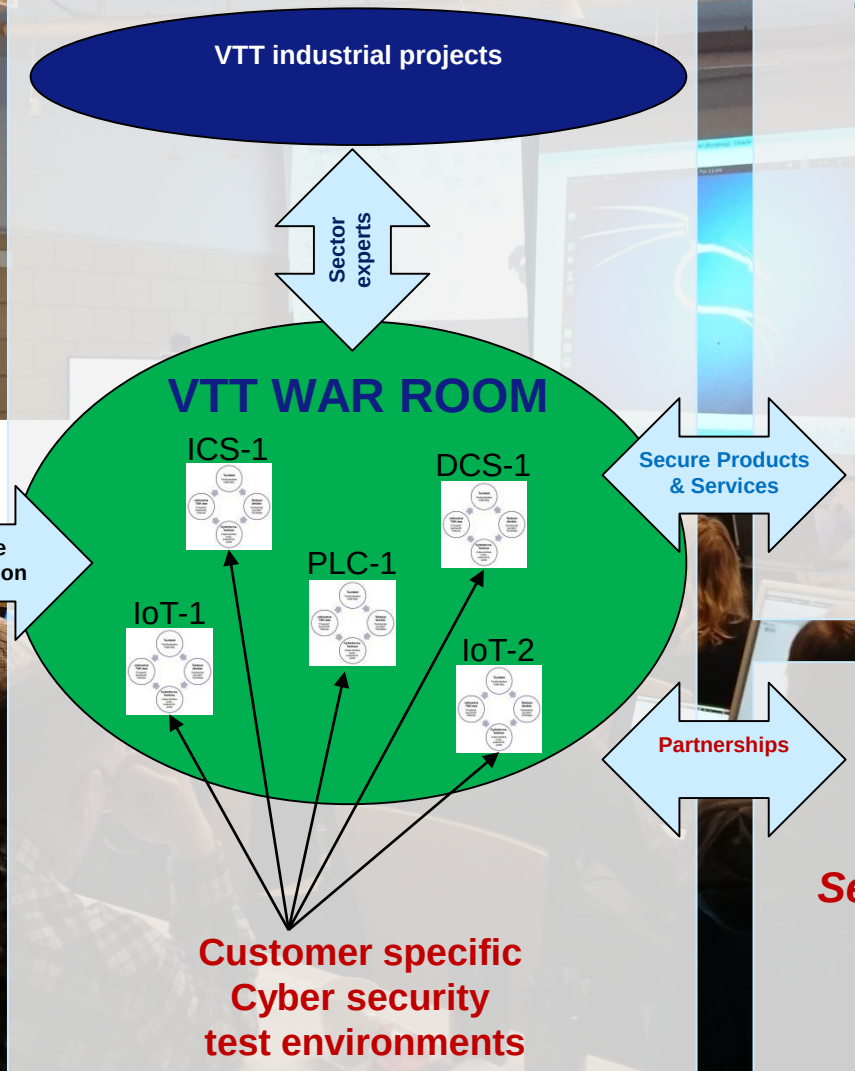
Turun seudun puhdistamo

HELEN

ORION

VALIO

VTT



Vendors & Service providers

ABB

VALMET/METSO

INSTA DEFSEC

SIEMENS

NETCONTROL

LAN&WAN

PROSYS

NIXU

Partners

NESA

The National Cyber Security Centre Finland

TUT

Synopsys

Rugged Tooling

Where to test without damages?

At VTT Cyber Security War Room!

What is the War Room?

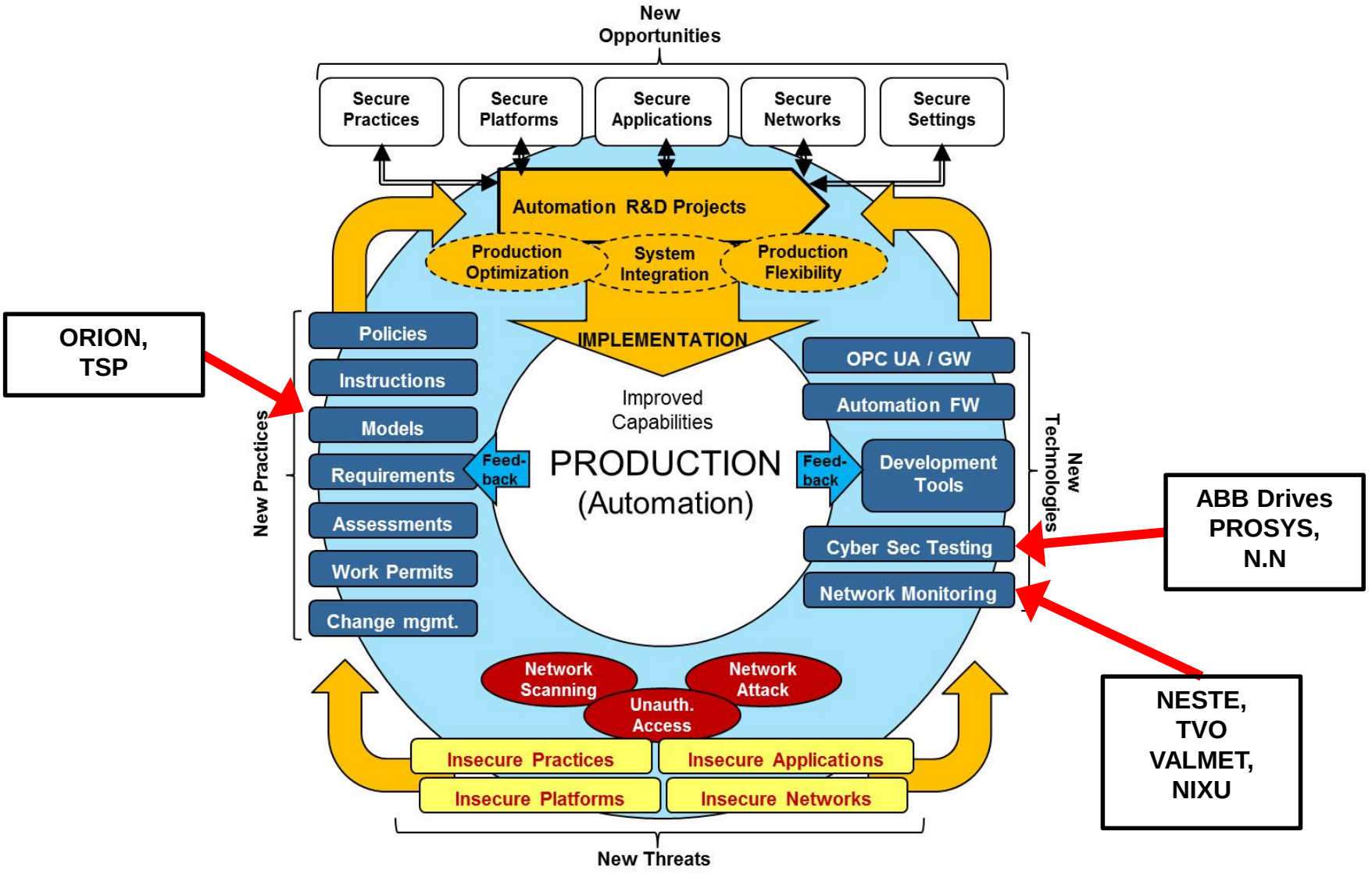
- Includes a mini-Internet environment that is completely isolated from all other telecommunications
- Devices or software can be subjected to highly realistic cyber-attacks in a controlled way
- Wide range of attacks can be tried to test the performance of various systems
- Personnel of over 30 researchers with extensive experience and knowhow on cyber security
- Equipped with cutting edge technologies and devices

War Room enables

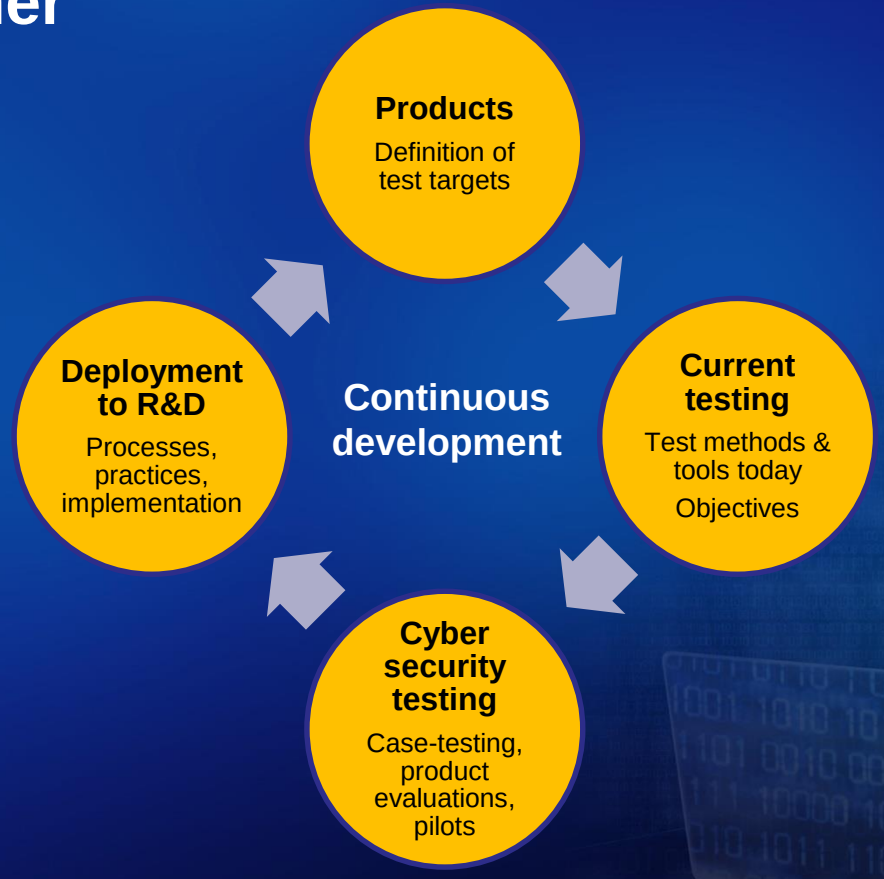
- Conducting of attacks aimed at seizing systems, implementation of typical hacker attack strategies and botnet attacks
- Identification of cyber attacks, threats and vulnerabilities
- Monitoring effective attacks and developing tools for cyber situational awareness
- In-depth cyber analyses from network traffic log information
- Security testing of products and services
- SW security auditing

Cyber security testing is one part of a bigger picture

KYBER-TEO (2015) Participant Cases



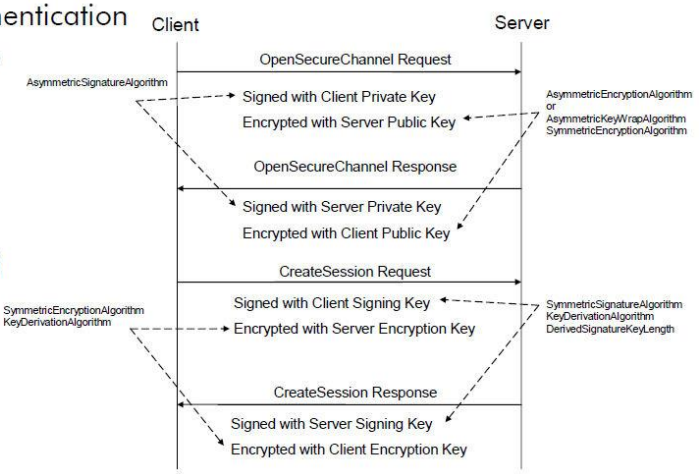
Cyber security test development with the customer



OPC UA Security

OPC UA Authentication & Security Modes

- OpenSecureChannel
  - Asymmetric encryption (RSA) with ApplicationInstance Certificates (X.509v3)
  - Application authentication
  - Exchange of the symmetric encryption key
- CreateSession
  - Symmetric encryption (AES)
- ActivateSession
  - User authentication



Authentication

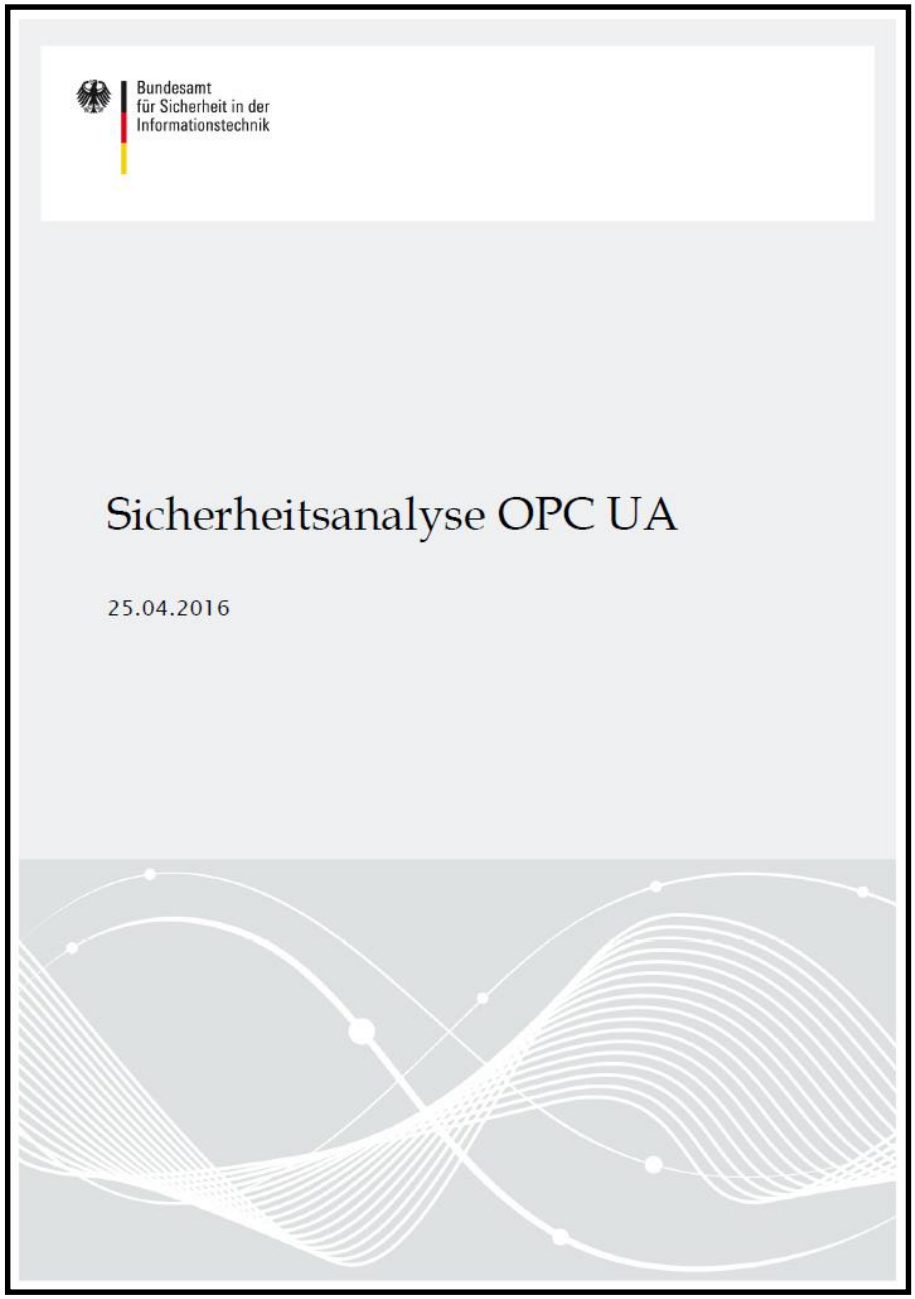
- User Authentication
  - –Anonymous
  - –User Name & Password
  - –User Certificate (X.509)
  - –External Tokens (e.g. Kerberos)
- Application Authentication
  - –Application Instance Certificate

SecurityModes

- **MessageSecurityMode**
  - **– None**
  - **– Sign**
  - **– Sign & Encrypt**
- SecurityPolicy
  - – Basic128Rsa15
  - – Basic256
  - – Basic256Sha256 (new, 1.02)
  - – New policies can be defined
- Client application defines the used security mode

Modes to record the OPC UA message sequences!

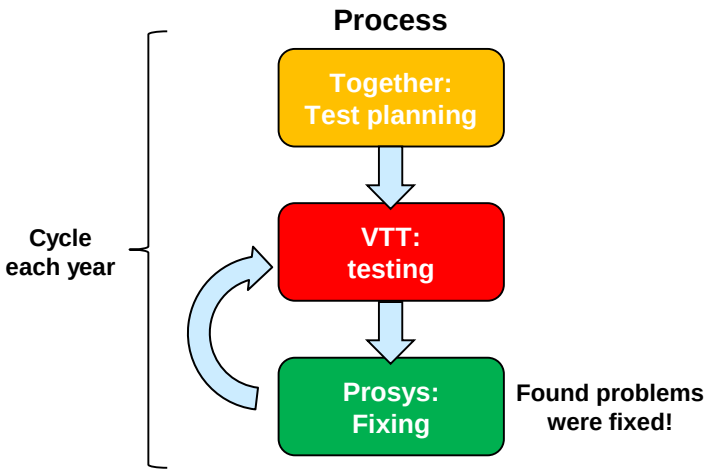
Reference: Prosys OPC



OPC UA security evaluation already done by BSI!

https://opcfoundation.org/security/

Case: VTT Cyber security testing of PROSYS OPC UA products



2014

System Under Test (SUT):

- Prosys OPC UA Simulation Server.

Test cases:

- Testing was conducted through fuzzing and manual vulnerability scanning. The SUT had default configurations. Anonymous client access to SUT was used with no encryption.

Findings under (something to fix):

- OPC UA TCP Binary encoding.
- OPC UA HTTP.

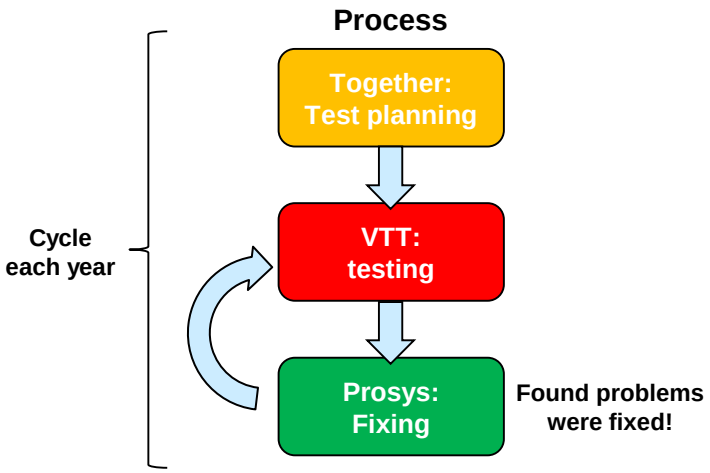
Notes:

- Session handling related issue prevented performing efficient fuzzing. Therefore fuzzing was done only with small sample sets with message types.

Further works:

- Testing potential fixes for the findings.
- More comprehensive fuzz test cases.
- Client testing.
- Testing OPC UA HTTP transport more through.

Case: VTT Cyber security testing of PROSYS OPC UA products



2015

Test target: Prosys OPC UA Simulation Server and OPC UA SDK Client Server (Evaluation)

Test tool: Codenomicon Defensics OPC UA Server Test Suite.

About testing:

- With the OPC-UA Test suite we tested Prosys OPC-UA Binary TCP protocol with model based methods (OPC UA modelled).
- Selected test cases were only run.
- Running of all tests cases typically takes several hours (overnight).

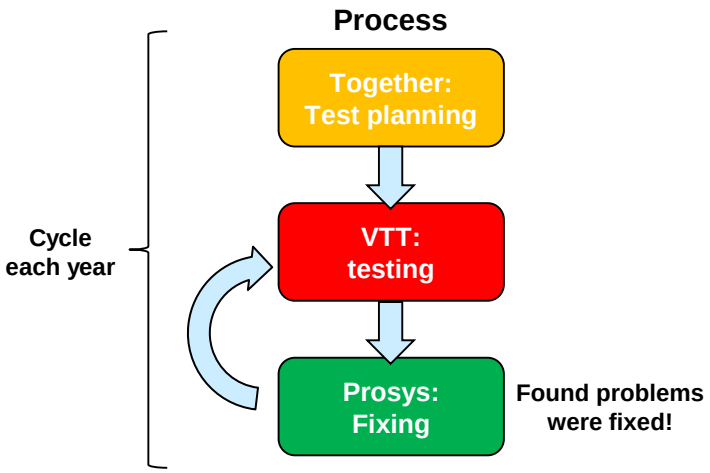
Test target behaviour under testing:

- Generally, the target survived well during the fuzzing and was able to continue correct operation.
- Testing of encryption and certificate handling was also touched a bit.
- Some slowdown of the services was typical reaction.

Other notes:

- Tenable Nessus -vulnerability scanner was useless here.
- hping3 DoS tool was also used to flood the test target with messages: Test target was able to automatically recover after the attacks.
- VTT developed threat modelling tool MVS was used to visualize the found threats.

Case: VTT Cyber security testing of PROSYS OPC UA products



2016

Test target: Prosys OPC UA Simulation server (Linux, Windows and SDK versions).

Test type: DoS-testing.

Test tools:

- nmap: port scanning.
- hping3: network flood testing.
- A tool for interactive packet manipulation with selected OPC UA messages.
- Codenomicon Defensics Traffic Capture Fuzzer: OPC UA protocol fuzzing based on recorded OPC UA packets.

Test target behaviour under testing:

- Generally, the target survived well and was able to continue correct operation.
- Log handling: Prosys had surely improved the log handling to correct level.
- High overload was found problematic to survive (Defensics).
- Only few test cases were found which repeatedly jammed the test target.

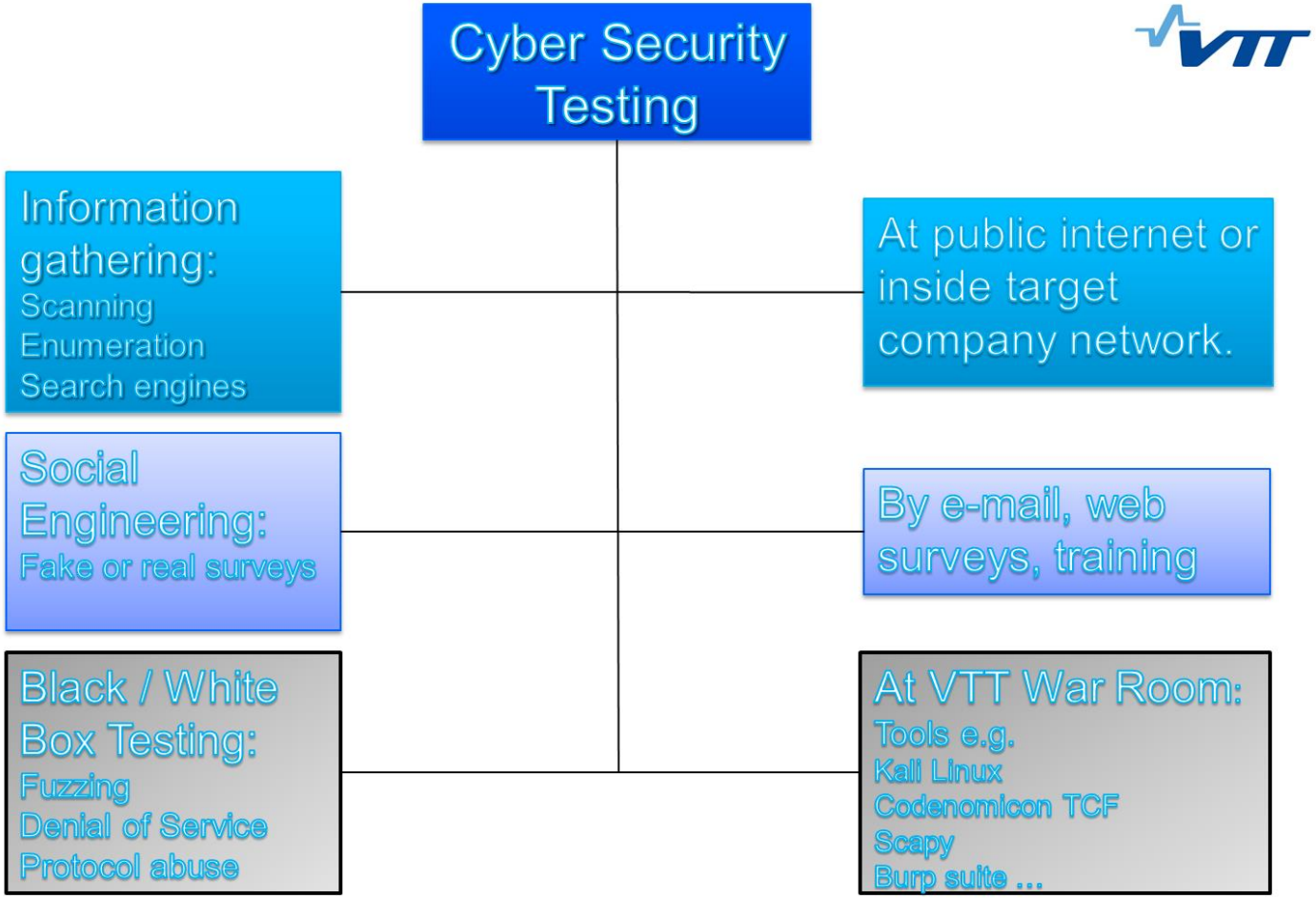
ULTIMATE GOAL:

To integrate Automated Cyber Security Testing to ICS application designer's daily tools!

OPC UA has an advantage because of its built-in security!

Examples of expanded

VTT cyber security testing



Example tools used in the War Room

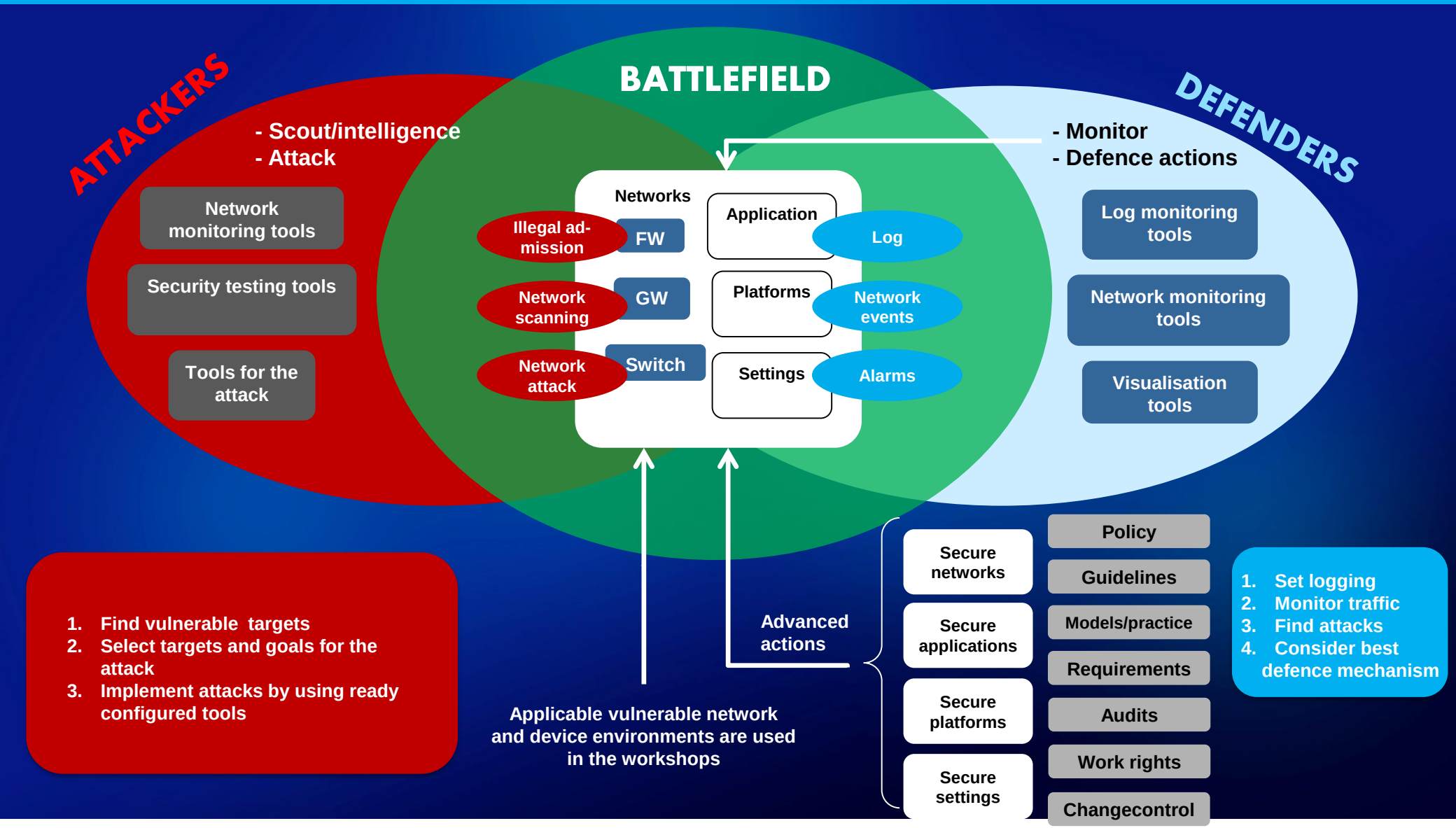
Used tools are selected for each case

Commercial:

- Codenomicon Defensics TCF
- Nessus
- Metasploit
- Burp Suite Professional

Free / Open source:

- CrypTools
- IDA Free
- Scapy
- OWASP ZAP
- Maltego
- Nikto
- Hydra
- sslyze
- Armitage
- Stompy
- Radamsa
- Nmap
- Wireshark
- Jack the Ripper
- Valgrind
- !Exploitable
- Xplico
- Bro NSM
- Snort



We also arrange ”Cyber defence” hands-on Workshops

THANK YOU!

This was part of KYBER-TEO ”Improving cyber security for industry”
(National program 2014 - 2016)

Developing and testing SERVICES in the participating companies to ensure the cyber security and continuity of Finnish industrial production

WP 1: Cyber security practices and mappings
WP 2: Deploying the cyber security to industrial production
WP 3: Cyber security monitoring services for automation networks

GOAL: To disseminate results and experiences between companies.

Focus on co-operation

- **Participating companies**
  - ✓ **Company specific cases**
  - ✓ **Project work (technology, services)**
- **Other industrial companies (e.g. through dedicated NESA HUOVI-portal project area)**
  - ✓ **Wide company reviews**
  - ✓ **Result dissemination seminars**
- **State authority & Research co-operation: (Advice, quality, development, dissemination, education)**
  - ✓ **National Emergency Supply Agency (Project owner)**
  - ✓ **VTT (Project lead & execution)**
  - ✓ **TUT - Tampere University of Technology (Project subcontractor)**
  - ✓ **Finnish Communications Regulatory Authority - The National Cyber Security Centre (NCSC)**

Contact point

Pasi Ahonen, Principal Scientist, VTT

Project Manager: TITAN, TEO-TT, COREQ-VE, COREQ-ACT, TEO-SUMMARY, KYBER-TEO…

pasi.ahonen@vtt.fi