

CYBER DEFENSE & CERT

DEUTSCHE TELEKOM CERT – TF CSIRT

Tallinn, September 24th/25th 2015 | Christian Gorecki



LIFE IS FOR SHARING.

CERT VS. CDC

AS WE UNDERSTAND IT

CERT

- Incident response handling/management
 - Communication / Exchange
 - Security projects (ignite/establish/foster)
 - Service offering
 - DDoS mitigation
 - Proxy blocking
 - Vulnerability management
 - Advisories
 - Scanning
-
- Digital forensics (imaging, file recovery, timeline analysis, ...)
 - Malware analysis
 - Cyber Situational Awareness

CDC

- Large scale log analysis/correlation
- Targeted defense (“hidden business value”, attack perspective driven)
- Large scale sniper forensics
 - Server scans
 - Office workstation scans
- Advanced forensics (router forensics, bypassing anti-forensics)
- Analysis of targeted attack malware
- Problem pull, service push
- Hunter Team mode of operation
- Knowledge building
 - Threat intelligence
 - Assets/Infrastructure
- Innovation

CYBER DEFENSE CENTER

MISSION STATEMENT

Defend Deutsche Telekom against cyber attacks

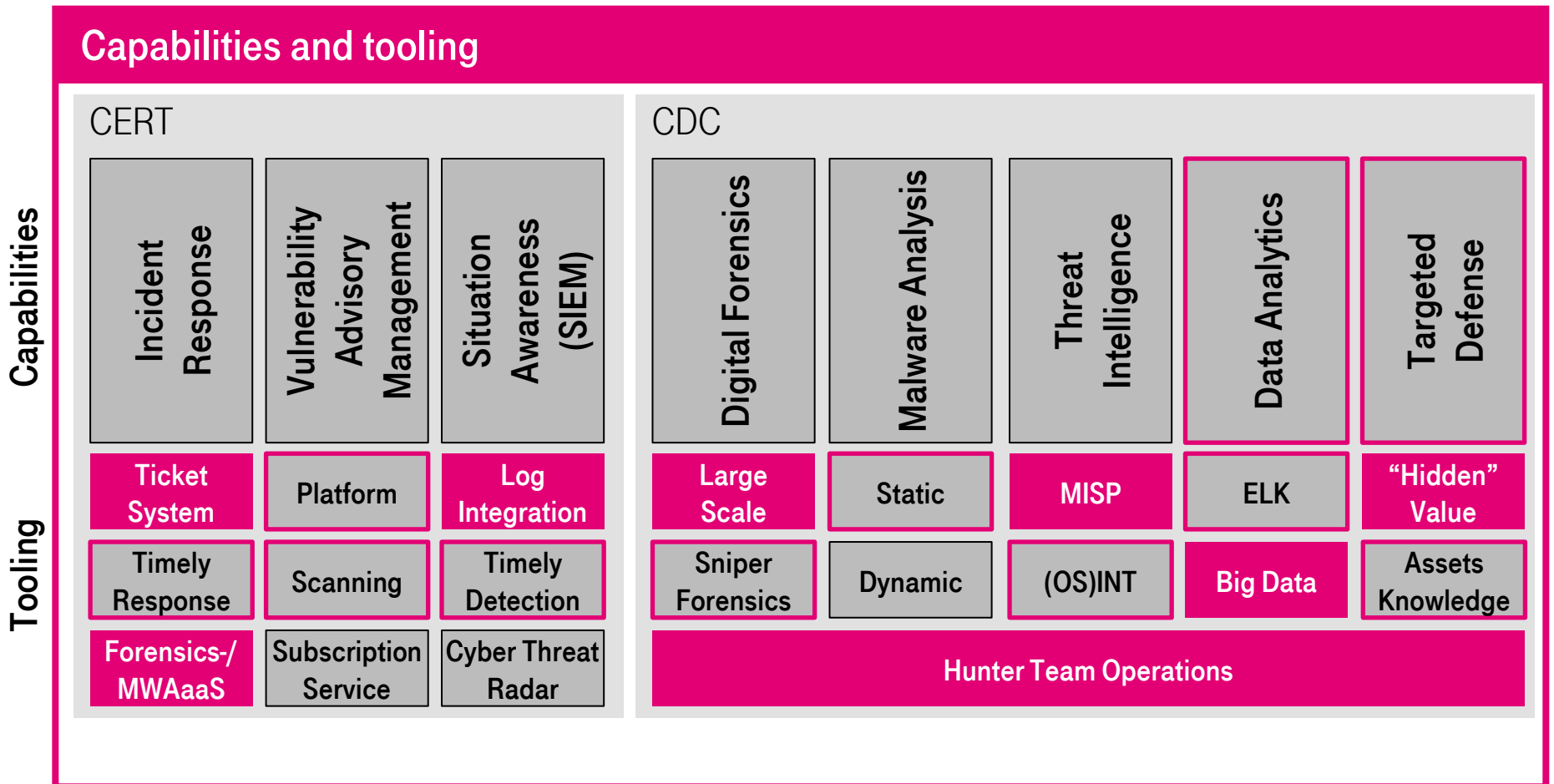
- Detect attacks that were unseen previously
- Focus on targeted attacks against Deutsche Telekom
- Minimize detection time (a.s.a.p.)
- Professionally manage cyber incidents
- Collaborate with international security community

Support enterprise customers of Deutsche Telekom

- Share CDC services, capabilities, tools and specific expert resources
- Share search profiles to be implemented in SIEM
- Share cyber intelligence and establish neighborhood watch

CYBER DEFENSE & CERT

CAPABILITIES AND TOOLING

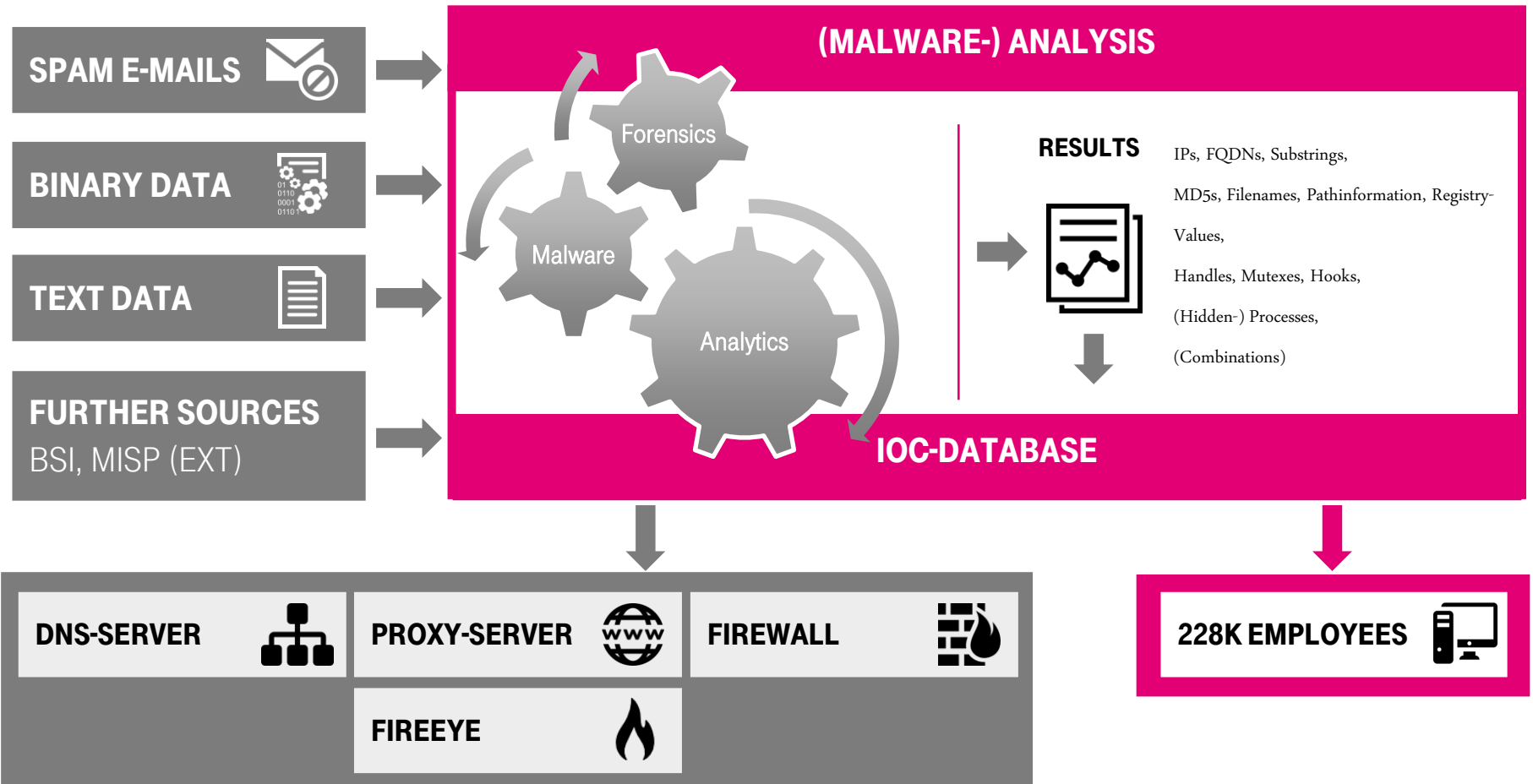


EXAMPLE

LARGE SCALE SNIPER FORENSICS

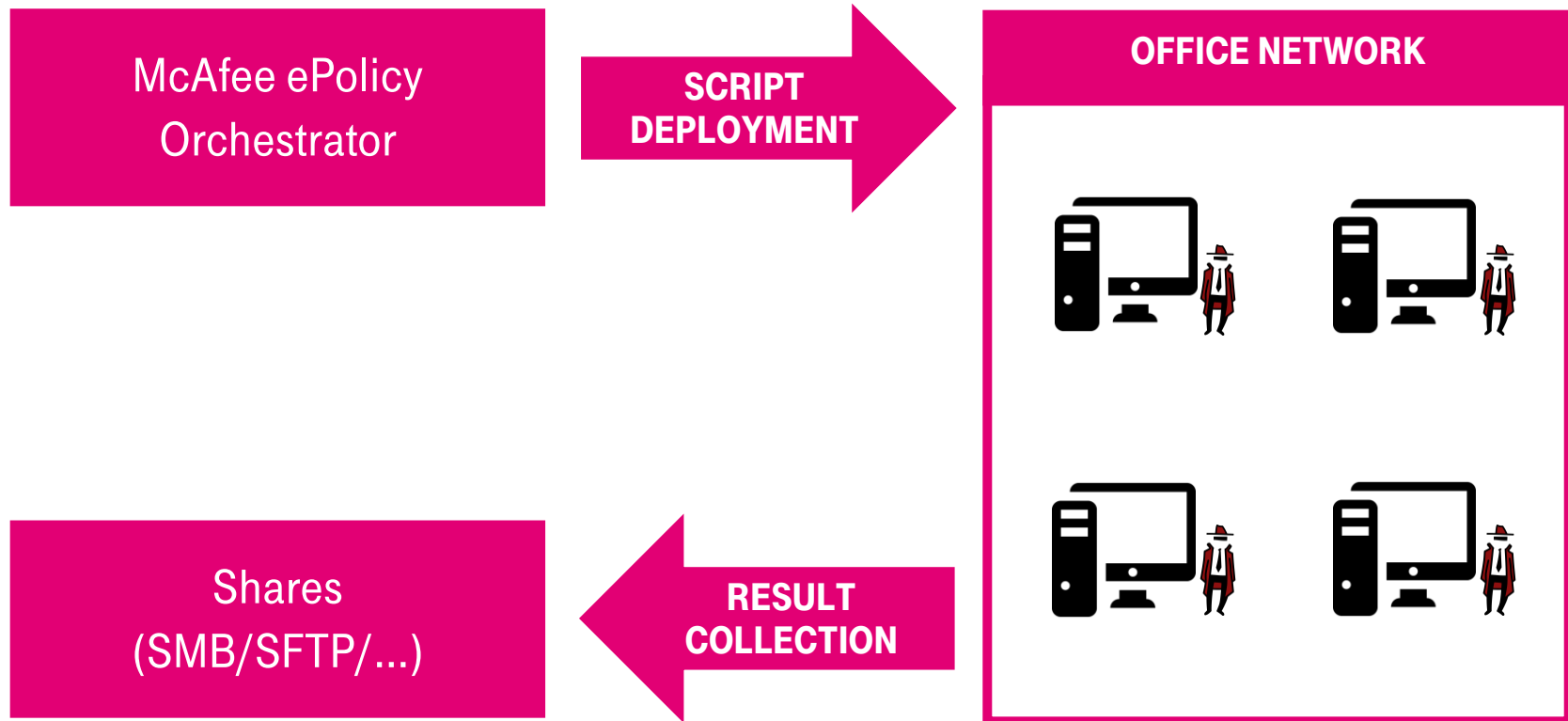
ONLINE-FORENSICS

SCOPE / CURRENT STATUS



EXAMPLE USING MCAFEE EPO

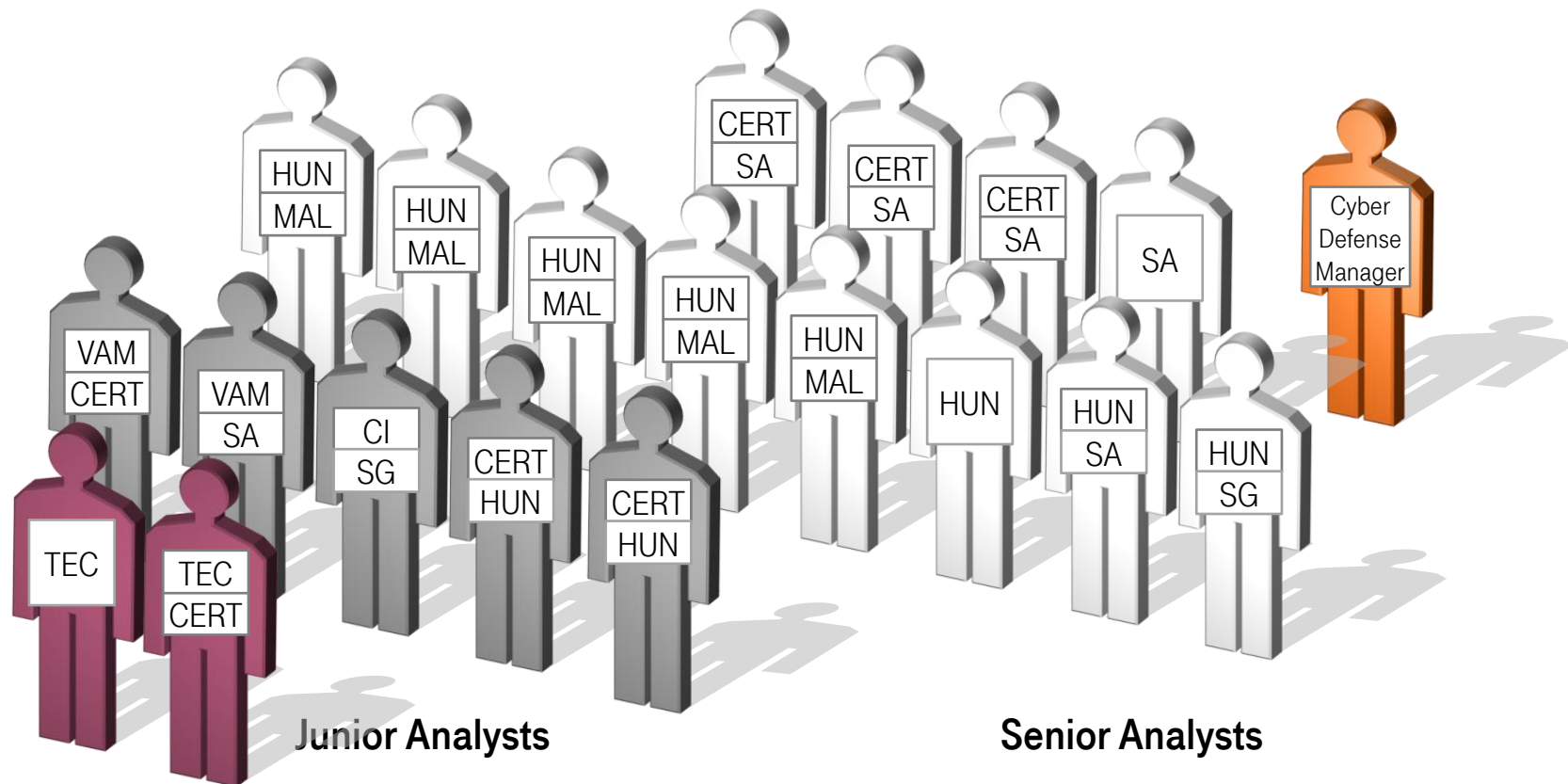
SCRIPT ROLLOUT / DATA COLLECTION



TELEKOM'S CYBER DEFENSE & CERT TEAM

CYBER DEFENSE CENTER

HUMAN RESOURCES



- **CERT:** Handling of cyber incidents, taskforces
- Strategic Advice (**SA**): projects etc.
- SIEM Governance (**SG**): mgmt. of SIEM operations
- Technician (**TEC**): Tool operations & maintenance

- Cyber Intel. (**CI**): Cyber sec. research, networking
- Hunter teams (**HUN**): security analysis & risk mgmt.
- **VAM:** Vulnerability Advisory Management
- **MAL:** Forensic & malware analysis experts

THANKS! QUESTIONS?

christian.gorecki@telekom.de



LIFE IS FOR SHARING.