Integrating Incident Analysis and Digital Forensics Tooling for Automated Compromise Detection

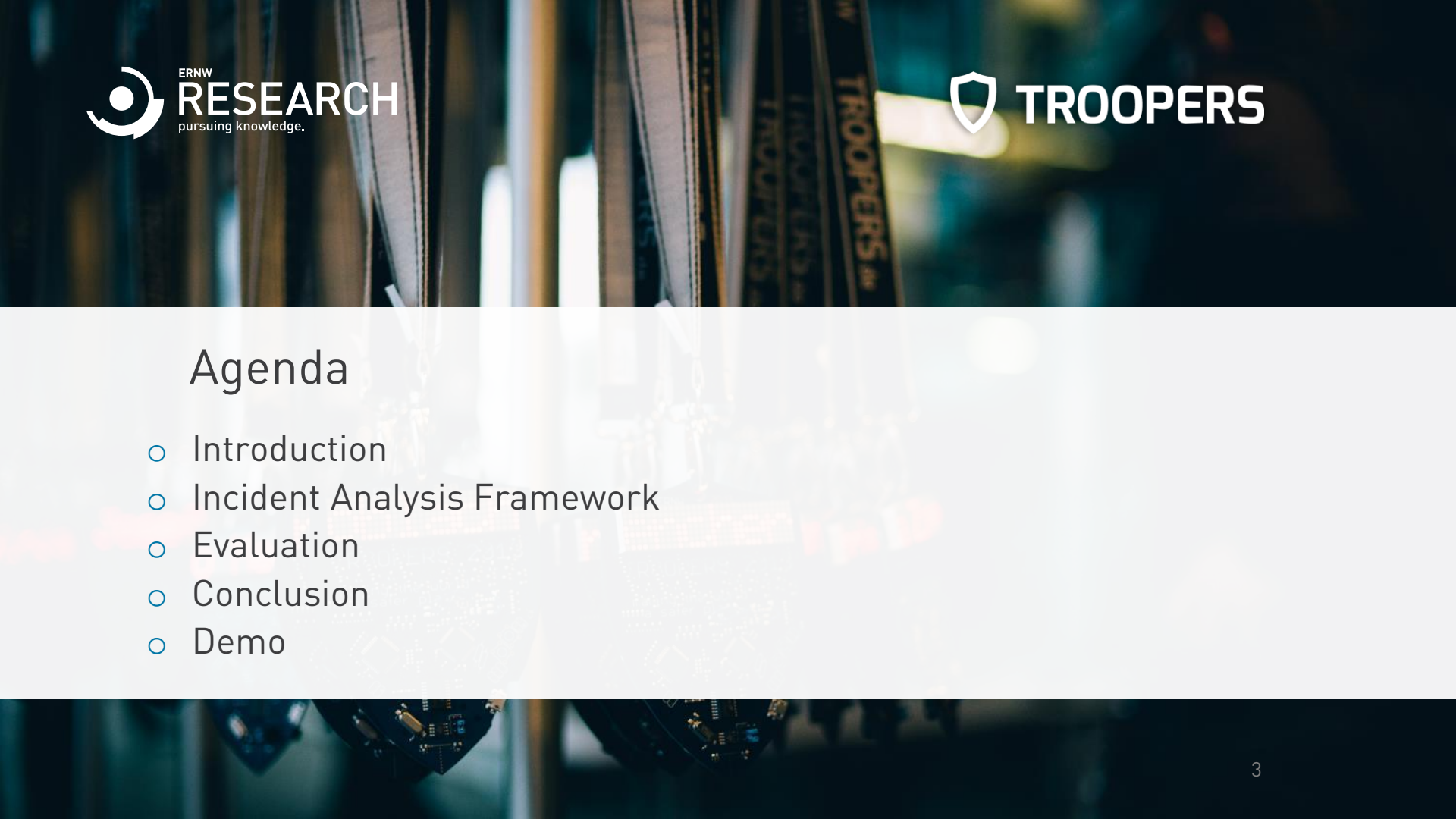
Ann-Marie Belz

Troopers 2026

ERNW RESEARCH
pursuing knowledge.

Who I Am

- B.Sc. and M.Sc. in Medical Informatics from Heidelberg University
- Security Analyst @ERNW Research
- Part of Penetration Testing & Incident Response Team



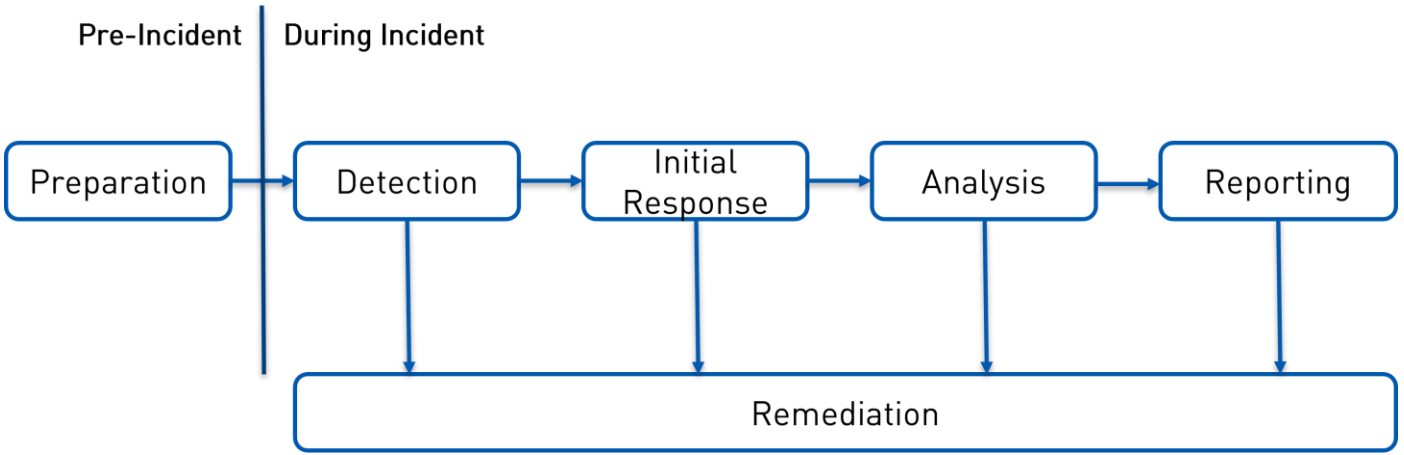
Agenda

- Introduction
- Incident Analysis Framework
- Evaluation
- Conclusion
- Demo

ERNW RESEARCH pursuing knowledge.

TROOPERS

Incident Response Process

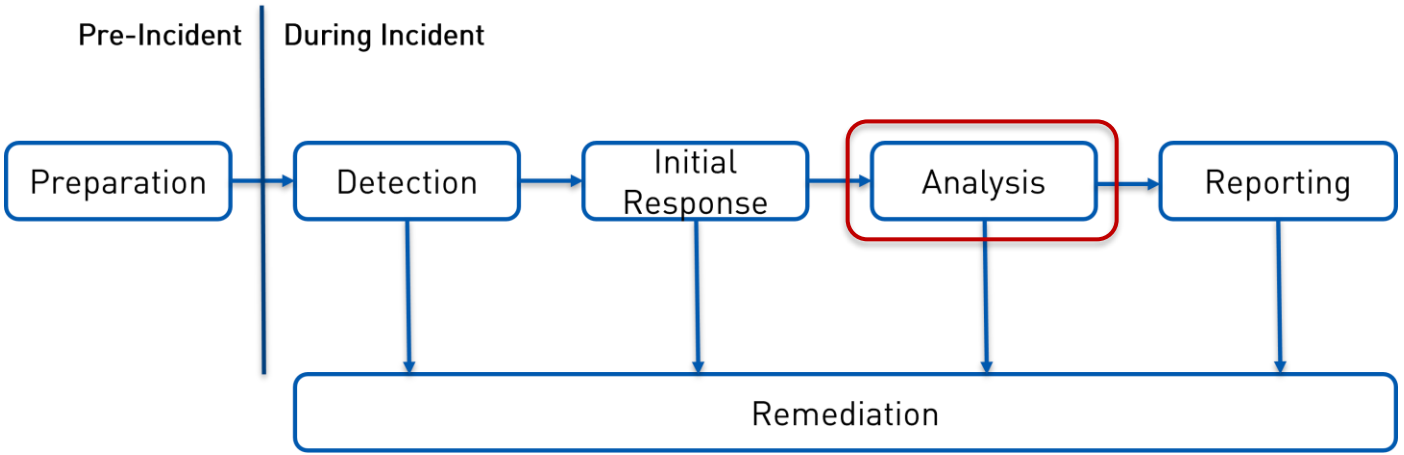


(Mandia et al., 2003)

ERNW RESEARCH pursuing knowledge.

TROOPERS

Incident Response Process



(Mandia et al., 2003)

ERNW RESEARCH pursuing knowledge.

TROOPERS

Challenges

- Time constraints
- Increasing storage capacities
- Expert knowledge required
- Lack of integration between tools

ERNW RESEARCH pursuing knowledge.

TROOPERS

Challenges

- Time constraints
- Increasing storage capacities
- Expert knowledge required
- Lack of integration between tools

⇨ Framework with flexible tool integration and automated decision making

ERNW RESEARCH pursuing knowledge.

TROOPERS

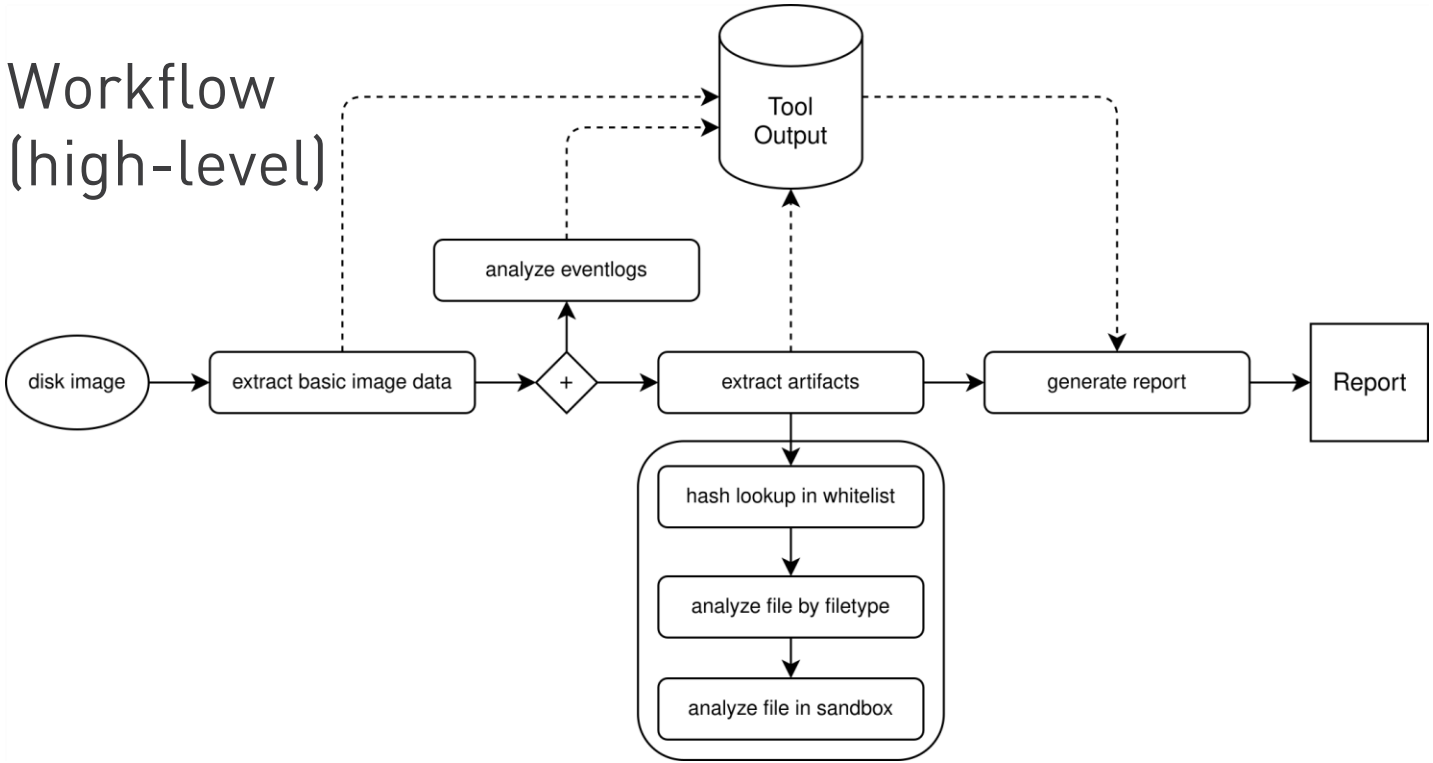
Incident Analysis

NTFS / Disk Artifacts	Windows Artifacts	Malware Analysis
Partition Table	Prefetch Files	Hash Comparison
Master File Table (MFT)	Registry	Static Analysis
Alternate Data Streams (ADS)	Event Logs	Dynamic Analysis

ERNW RESEARCH pursuing knowledge.

TROOPERS

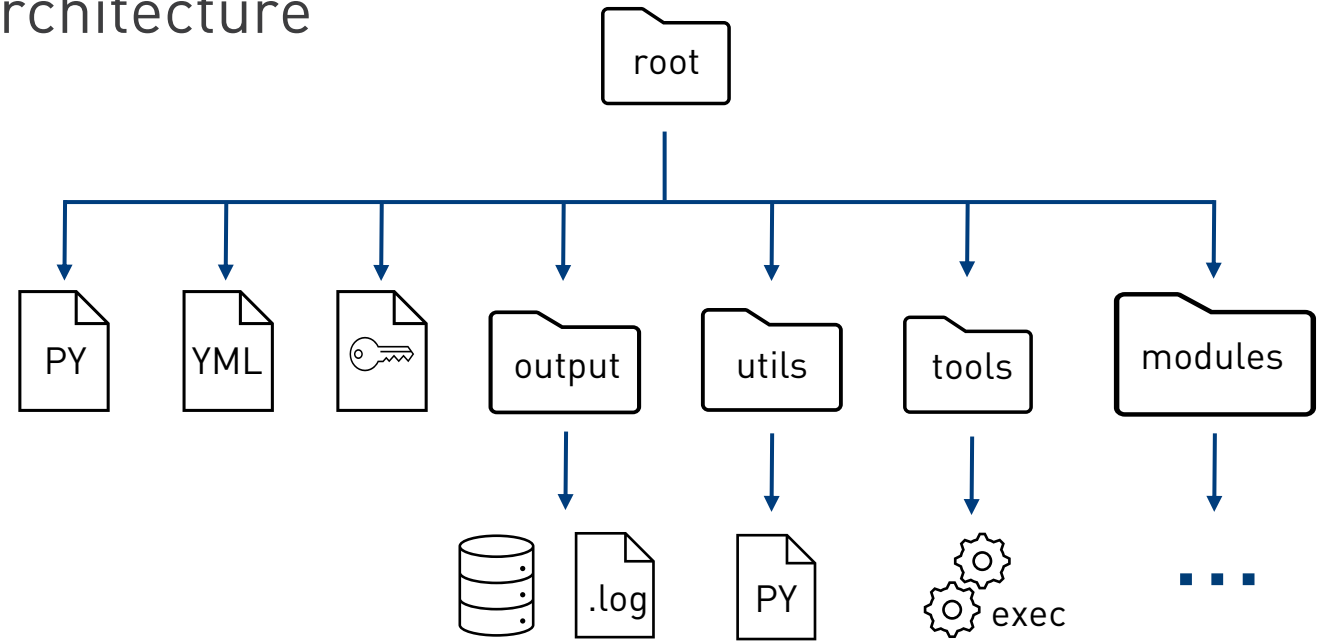
Workflow (high-level)



ERNW RESEARCH pursuing knowledge.

TROOPERS

Architecture

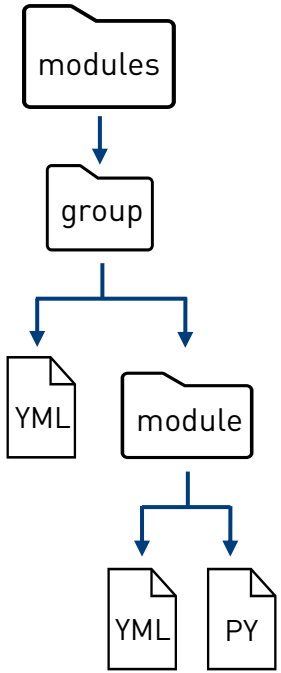


ERNW RESEARCH
pursuing knowledge.

TROOPERS

Modules

- Basic Information
- Event Log Analysis
- Artifact Extraction
- ADS Analysis
- Hash Lookup
- Static Filetype Analysis
- Dynamic Analysis
- Report Generation



ERNW RESEARCH
pursuing knowledge.

TROOPERS

Modules

- Basic Information
- Event Log Analysis
- Artifact Extraction
- ADS Analysis
- Hash Lookup
- Static Filetype Analysis
- Dynamic Analysis
- Report Generation

ERNW RESEARCH pursuing knowledge.

TROOPERS

Analysis Results

- All compromised images detected
- False positive analysis results from VMRay (23 %) and Sigma (96 %)
- ~69 % of IoCs found
- Only ~0.19 % of files per image needed to be analyzed
- Most malicious files found in Prefetch files and UserAssist
- Overall performance time: 22.5 hours, without VMRay: 43.5 min

ERNW RESEARCH pursuing knowledge.

TROOPERS

Conclusion

- Framework can detect compromises
- Framework operates in parallel with analysts
- Future extensions e.g., file carving and contextual indicators
- Integration of artificial intelligence for additional decision support


ERNW
RESEARCH
pursuing knowledge.
TROOPERS
TROOPERS
CONFIDENTIAL

DEMO

ERNW RESEARCH
pursuing knowledge.

TROOPERS

Thank you for your Attention!

Questions?

abelz@ernw.de

www.linkedin.com/company/ernw-research-gmbh

www.ernw-research.de

www.insinuator.net