CQURE
Security WorldWide
New York, Dubai, Warsaw

CSI: Windows - Techniques for Finding the Cause of the Unexpected System Takeovers

Paula Januszkiewicz

CQURE: CEO, Penetration Tester / Security Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
Contact: paula@cqure.us | http://cqure.us
@paulacqure @CQUREAcademy

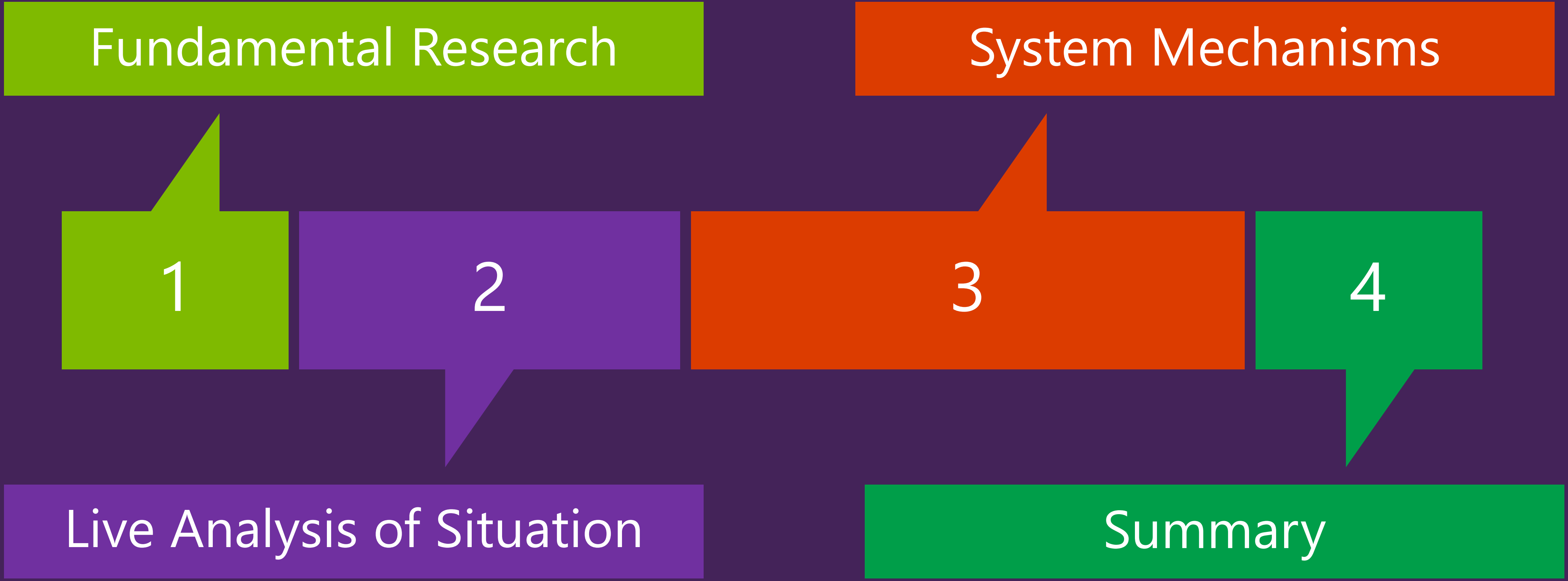
POLICE

Tools!

Check out the following link:

- Our tools: **http://cqure.pl → Tools**

Agenda



1 Fundamental Research

2 Live Analysis of Situation

3 System Mechanisms

4 Summary

Preserving Evidence

- Disk Data
  - Files from disk
  - Non-file data (e.g.. NTFS Journal, VSS)
- Memory ➔ Memory Dump
- Virtual Machine state
  - Disk and Memory
- Backup ➔ To revert back to the past events

Basic Terrain Orientation

Accounts

Groups

Processes

Network Activity

- ➔ Connections
- ➔ Resolver cache
- ➔ Arp cache

Basic Terrain Orientation

➔ CSI Fundamentals

Typical Traces

Logs

Security Log
RDP Operational Log
Application Logs

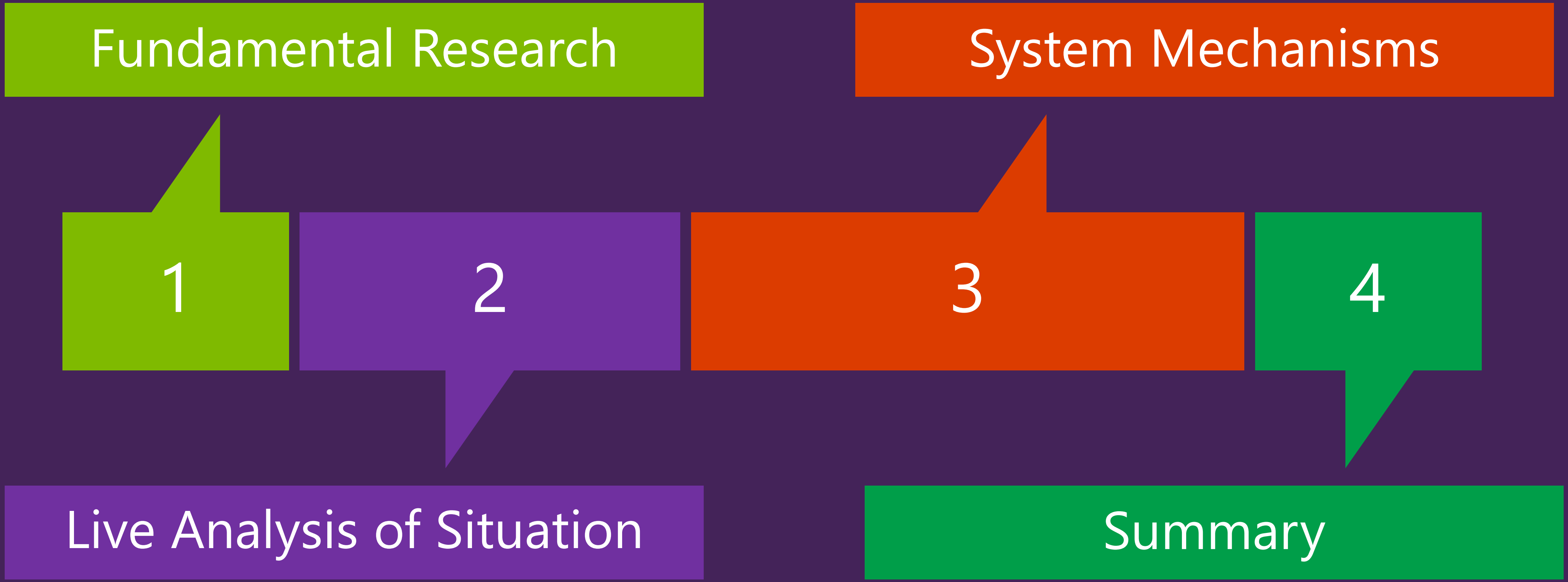
Windows Explorer

Profile, NTUSER
Run dialog
Most Recently Used (MRU)
Management Console (MMC)
Remote Desktop connections
Prefetch files
Recent documents

Typical Traces

CSI Fundamentals

Agenda



1 Fundamental Research

2 Live Analysis of Situation

3 System Mechanisms

4 Summary

Analyzing Malware

Static Analysis

Dissasembly, code review, memory dumps
IDA Pro, PeBrowse, PeBear, IlSpy, Volatility
VirusTotal, Upx

Dynamic Analysis

WinDBG, Xperf
Sniffers/Analyzers,
Event Log (Windows 8.1 only)
Sysinternals: Procexp, Procmon
Ollydb, Frst

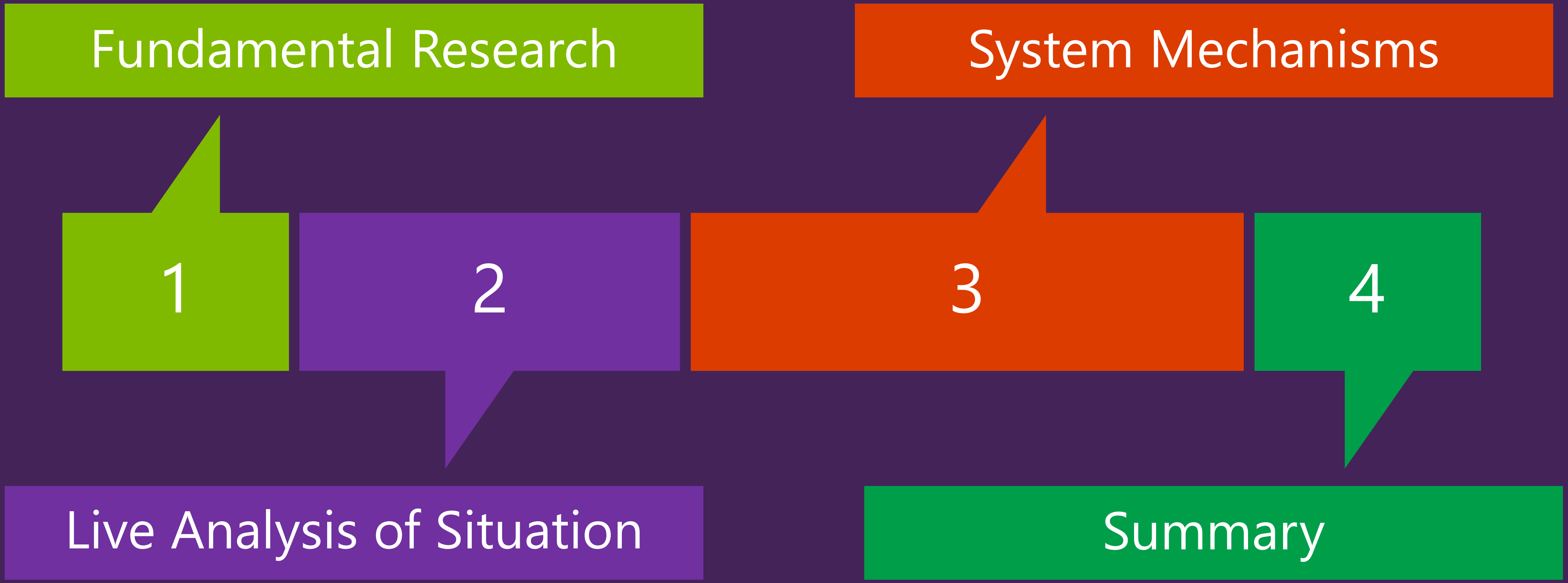
Sandbox

Virtualization PROs
Virtualization CONs

CSI Scenario

- *Something* is going on

Agenda



1 Fundamental Research

2 Live Analysis of Situation

3 System Mechanisms

4 Summary

How to Guard your Yard?

Fooling auditors

Log manipulations

Erasing logs

Playing with data

Dual booting

Absent data

Modification of the files

File metadata

NTFS journal

Deleting files

Dirty Games

Locking Handles

Handles

Keeping data secret

- File level games
  - Extension change
  - Joining files
  - Alternative data streams
  - Embedding
  - Playing with the content
  - Steganography
- Disk level games
  - Hiding data
  - Encryption

File Recovery

Preparing for unexpected

Logging

- Windows logs
- Application logs
- Audit logs

Keeping logs intact

- Subscriptions
- SIEM systems

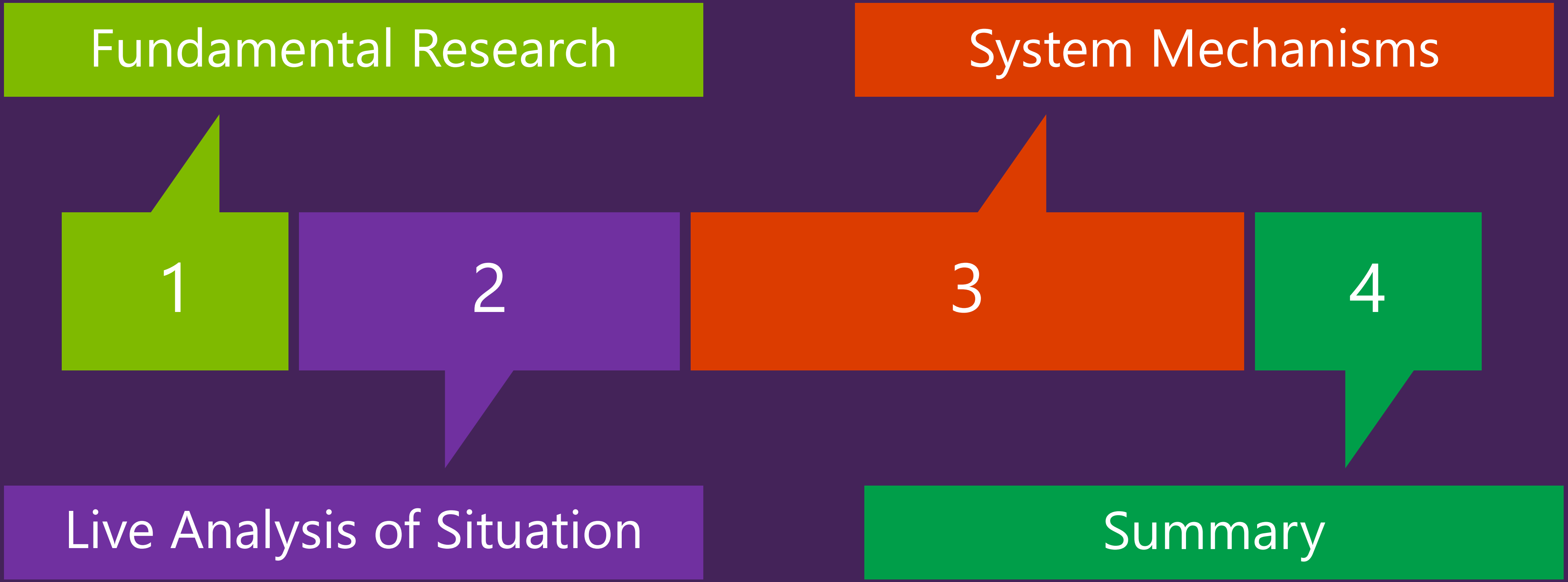
Backup and Recovery

- Service oriented NOT server oriented

https://www.flickr.com/photos/turkguy19/1019279760/

Nom, Nom, Nom ;>

Agenda



1 Fundamental Research

2 Live Analysis of Situation

3 System Mechanisms

4 Summary

Summary: CSI

Keep the data safe

Start the investigation

Analyze collected data

Search for correlations

Automate reactions