Bundesamt
für Sicherheit in der
Informationstechnik

Kickstart your SOC with [EU-][ATT&CK] Community Tooling

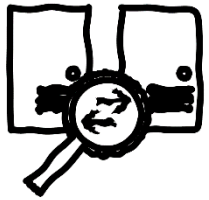
German Federal Office for Information Security
Division „Operational Cyber Security“,
Section „Integration/Planning“ […]

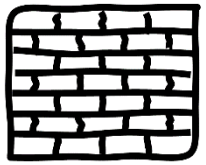
What makes a SOC...

a plan

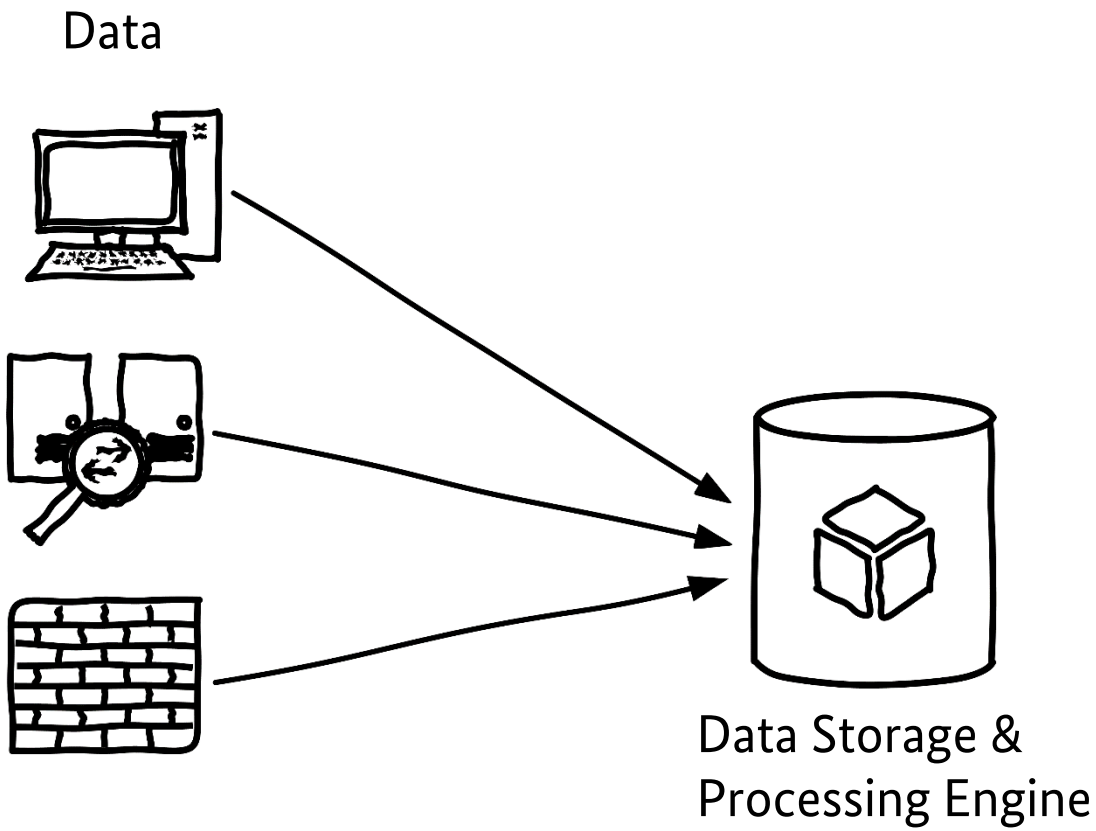
What makes a SOC...

Data

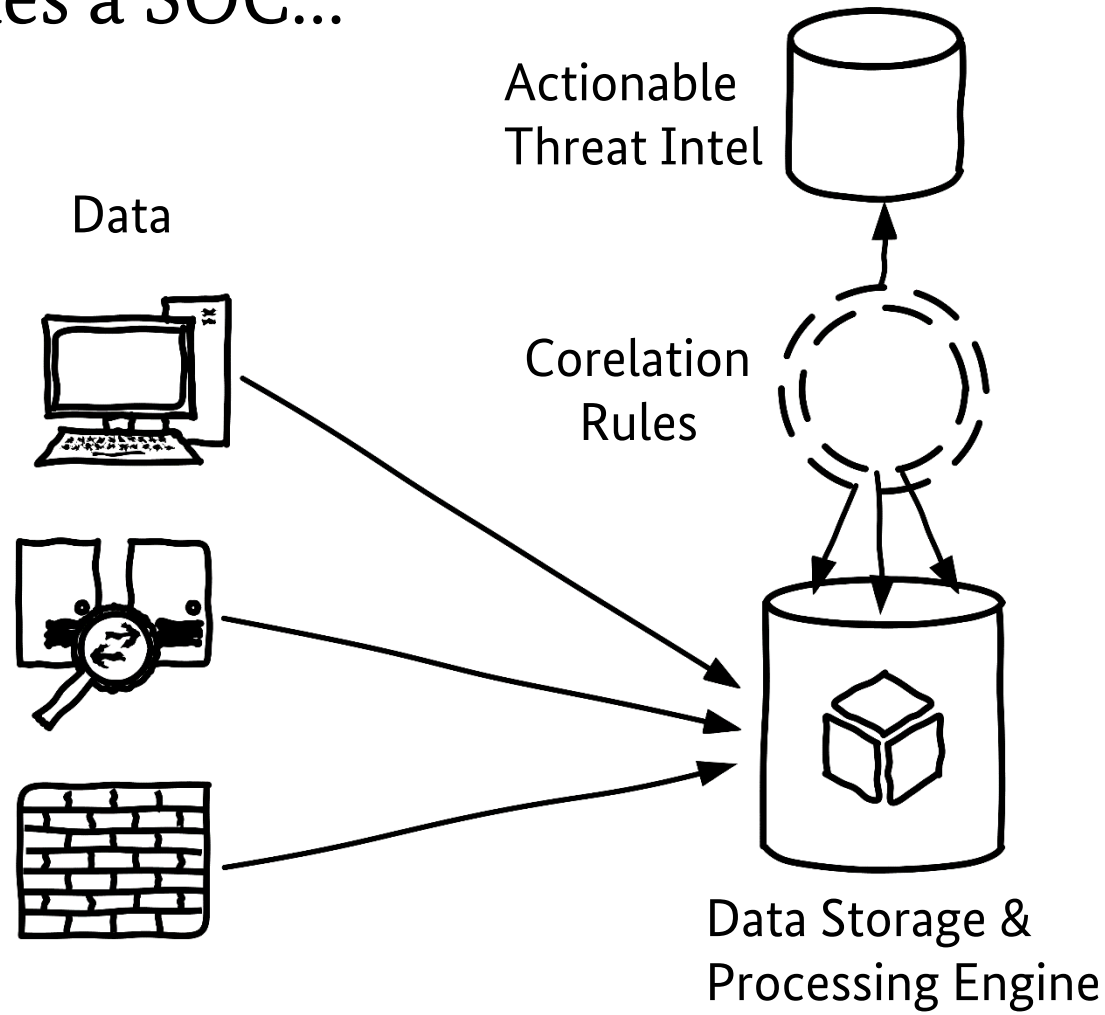




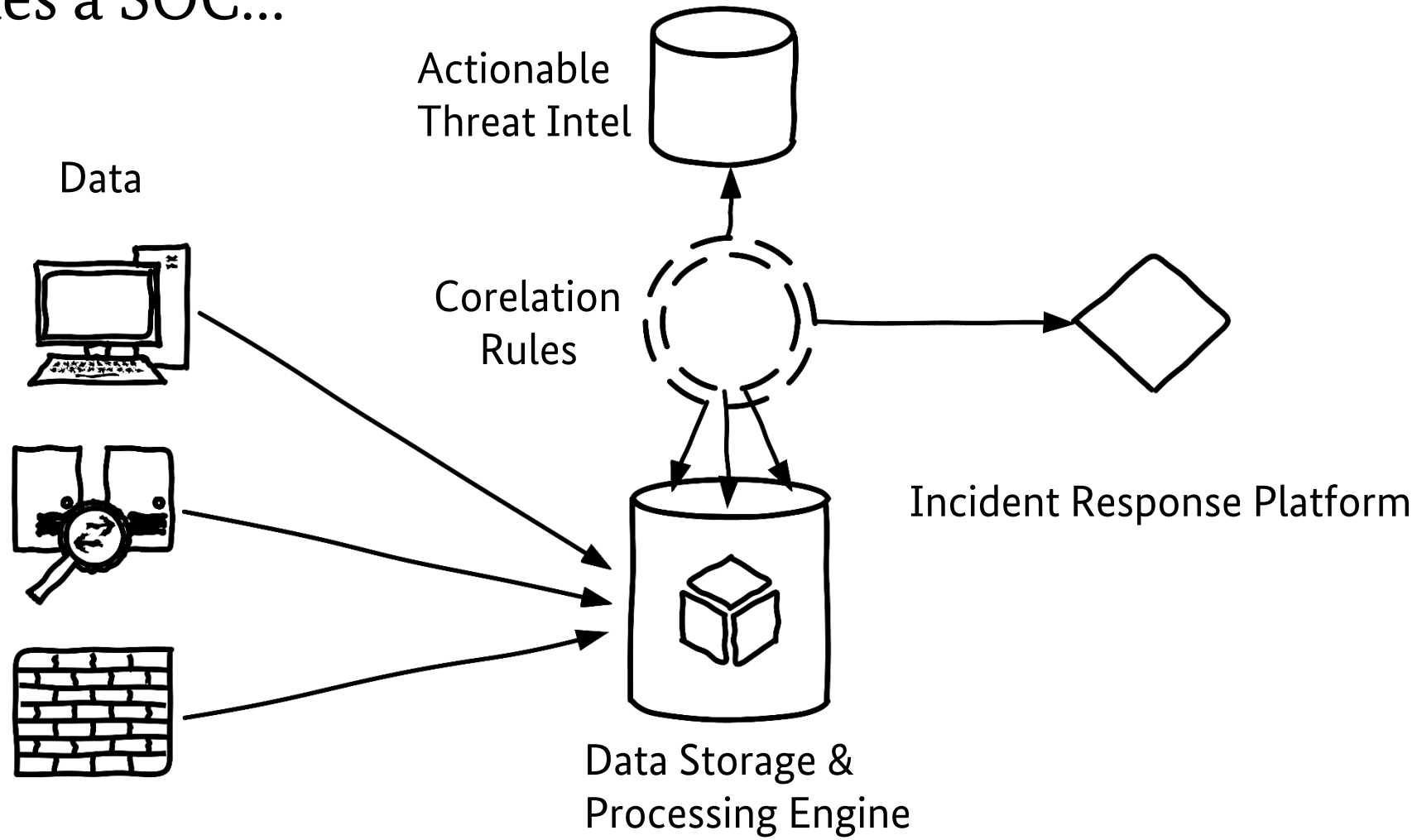
What makes a SOC…



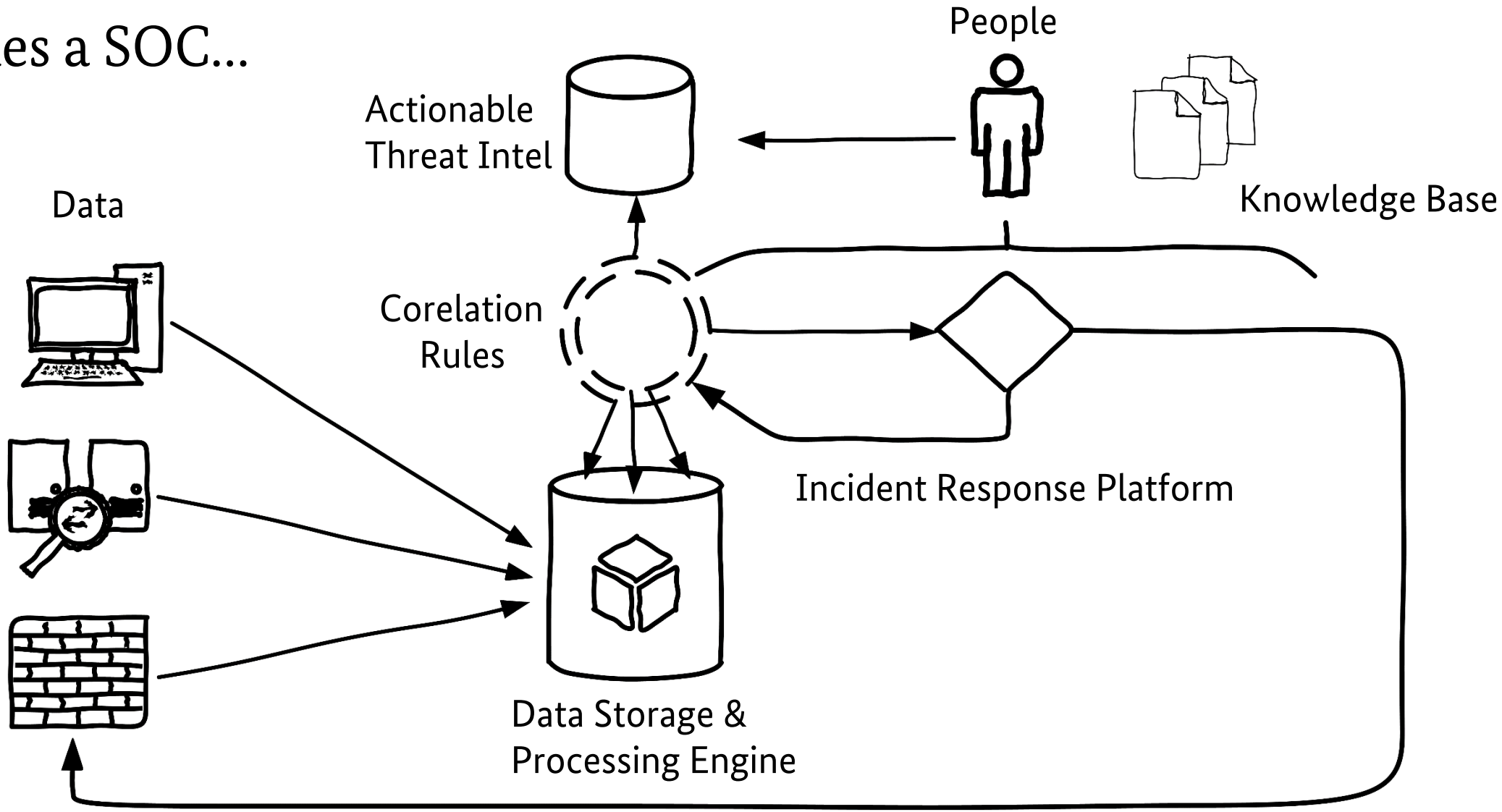
What makes a SOC...



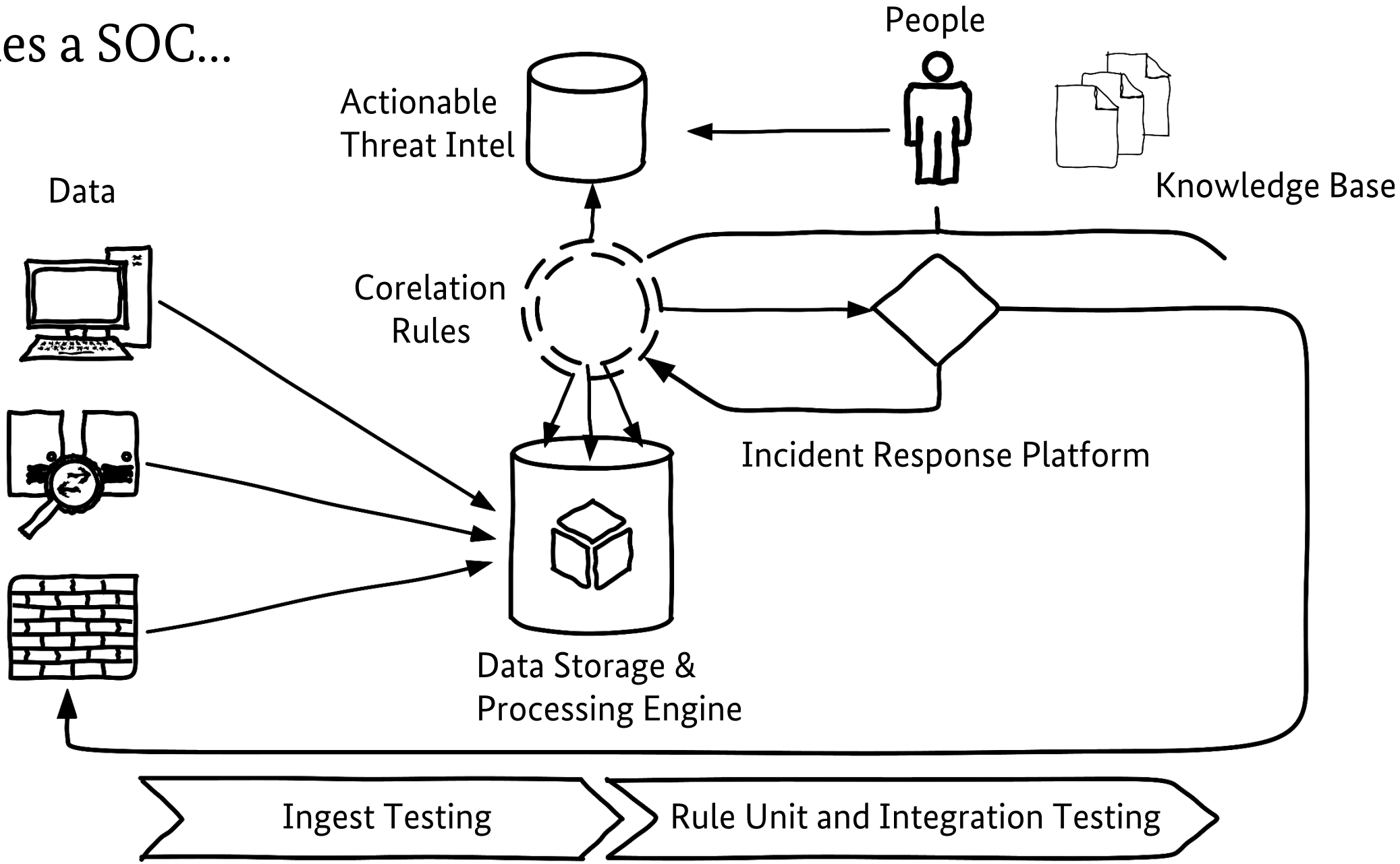
What makes a SOC...



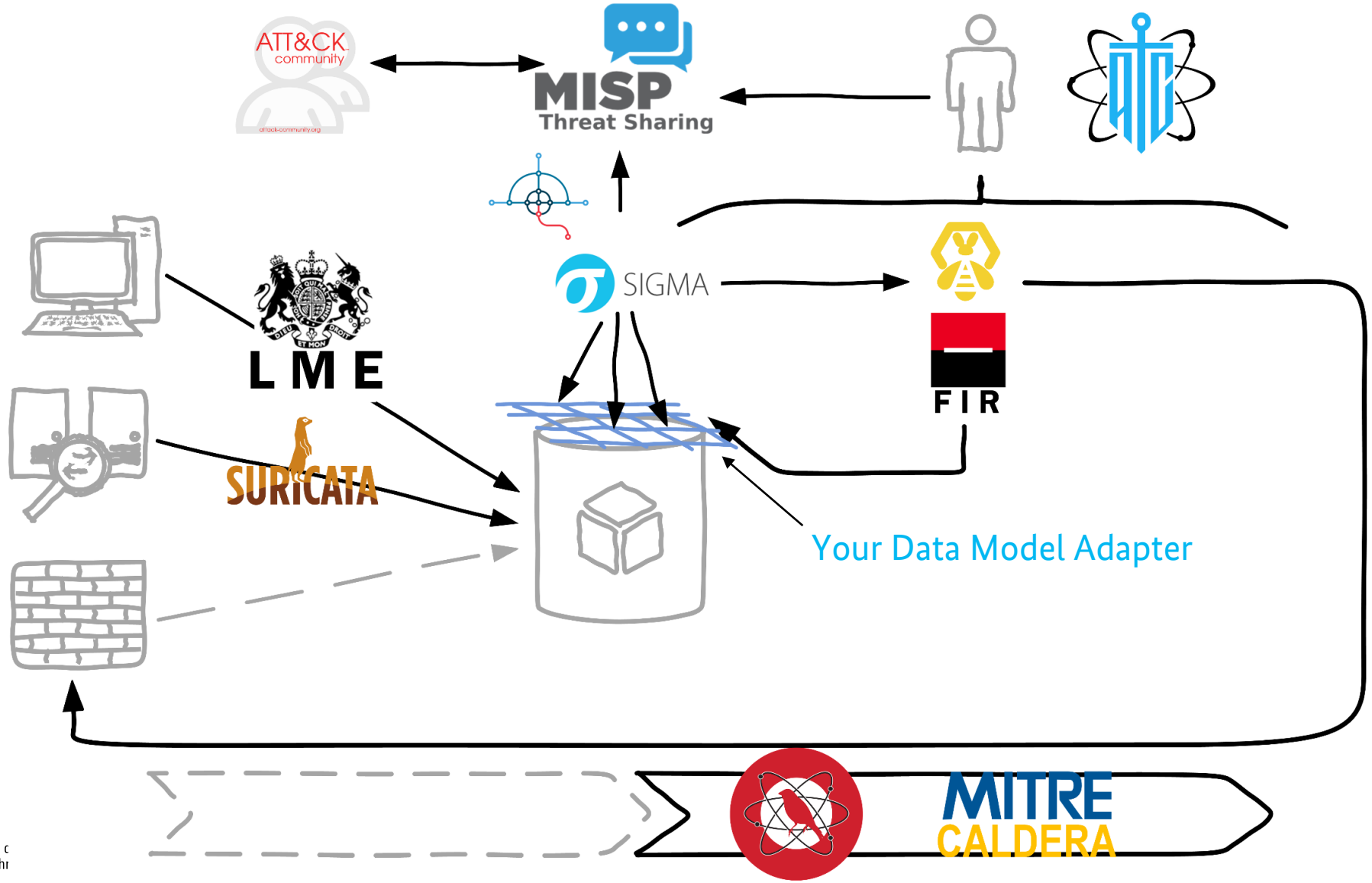
What makes a SOC...



What makes a SOC...



With [EU-][ATT&CK] Community Tooling you get...



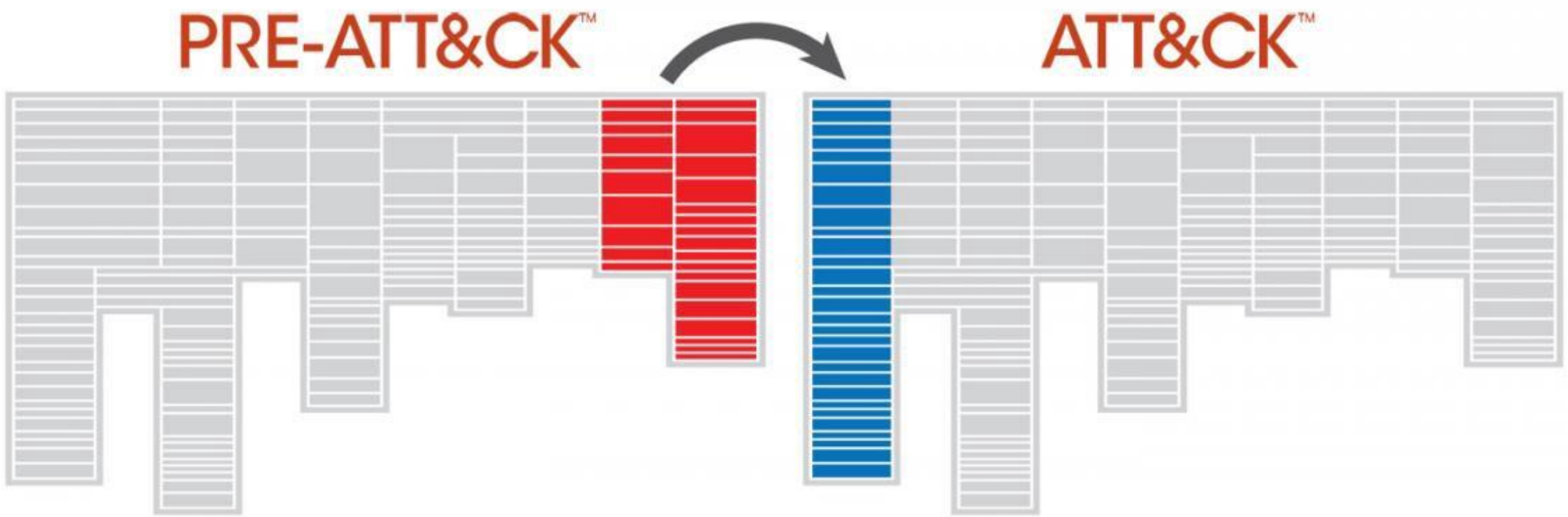
Just add:

- Your people
- Your assets
- Your Data Engine

A kickstarted SOC!

What about the plan?

The plan...



... is what you get out of ATT&CK Navigator.

How many attacks are you seeing?
Probable answers

0

A lot

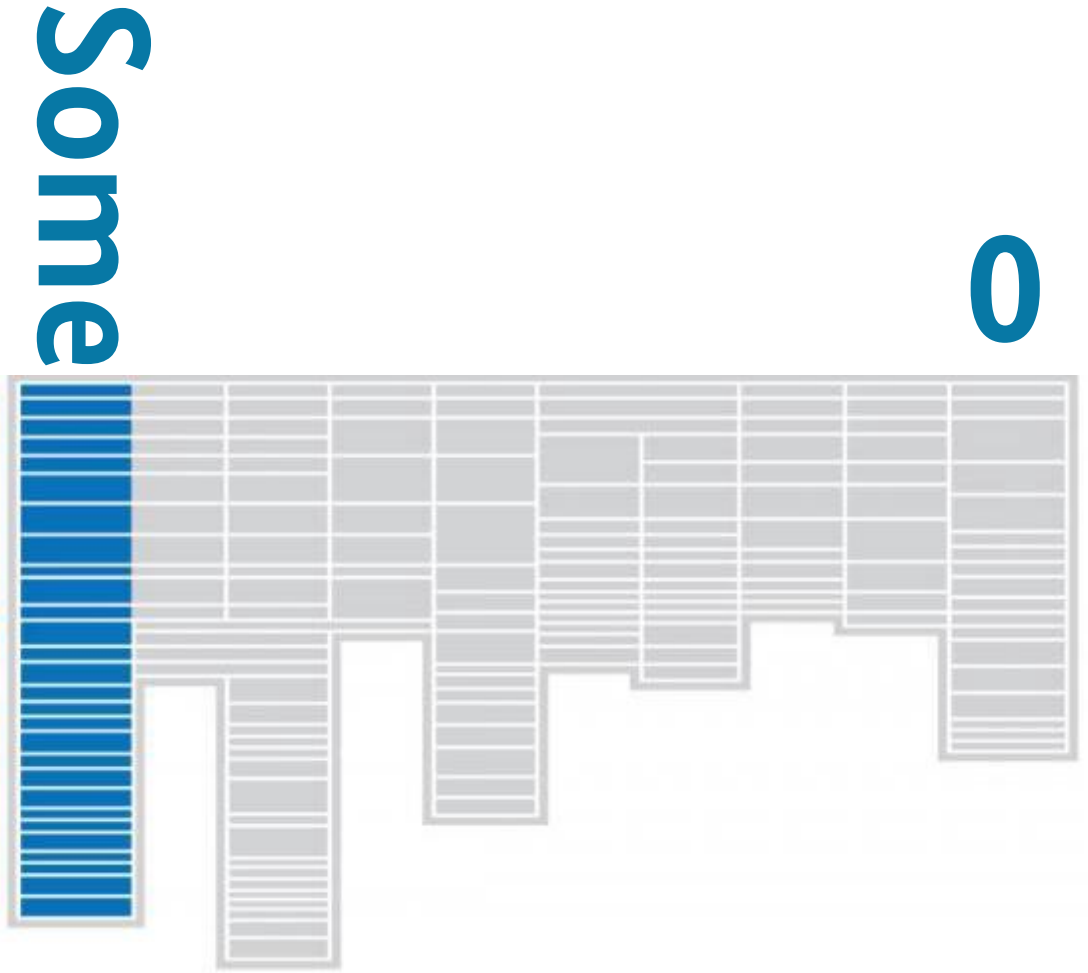
How many attacks are you seeing?
„Qualified“ answers

T1254 „Active Scanning“:

A lot

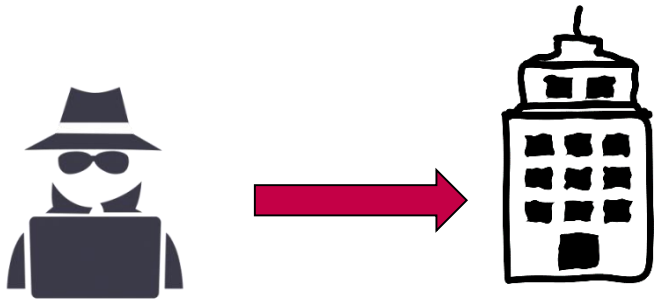
T1397 „Spear Phishing“:

Still a lot

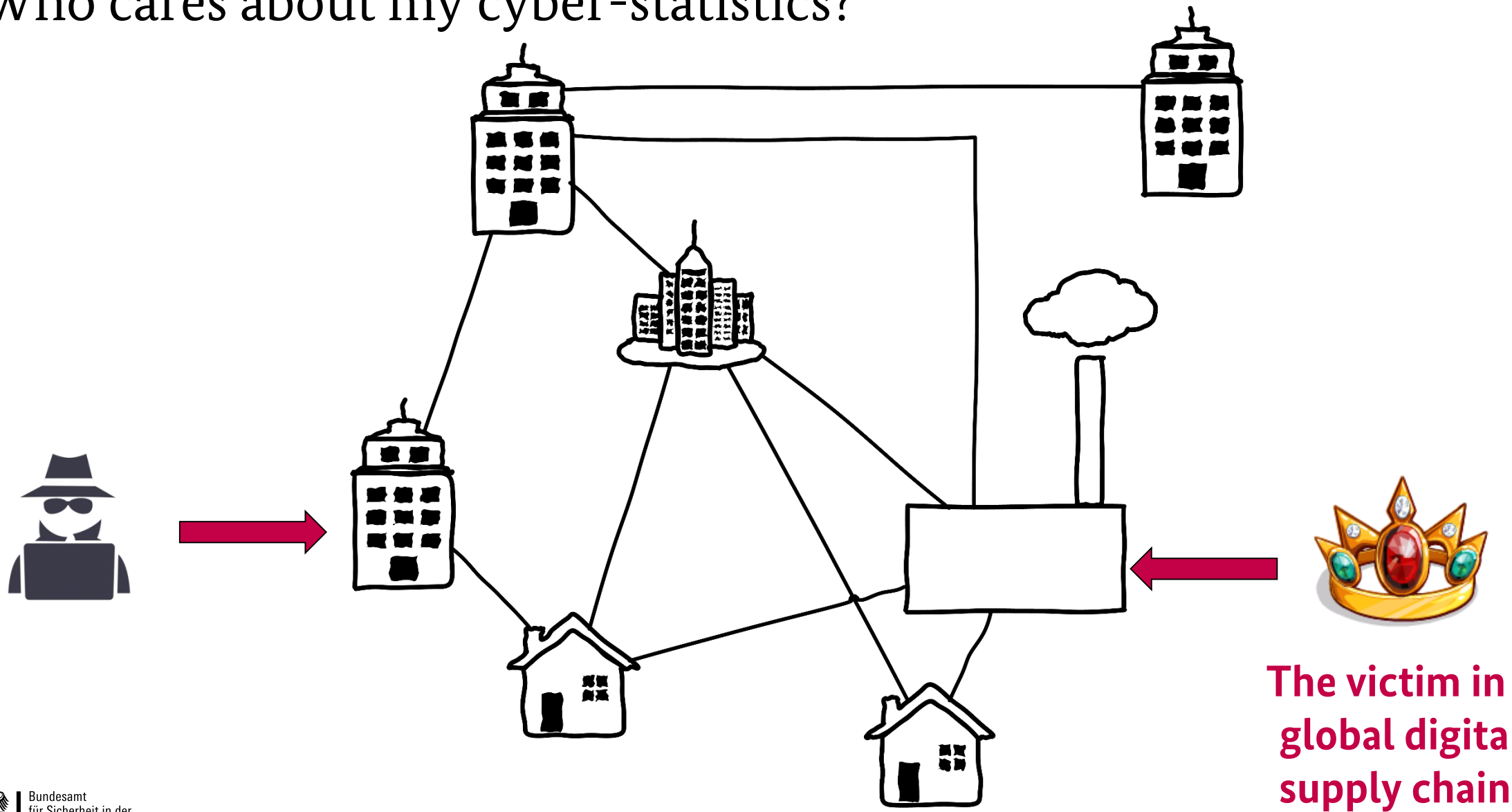


PRE-ATT&CK™ → ATT&CK™

Who cares about my cyber-statistics?



Who cares about my cyber-statistics?



The victim in a global digital supply chain!

Let‘s practice
Cyber-Security together
using
common vocabulary & tooling!

Ask me questions!

Contact

Hr. Jens Sieberg
Head of Section
protokollierungsrichtlinie@bsi.bund.de

Federal Office for Information Security
Section OC 11
Godesberger Allee 185-189
53175 Bonn

Personal Statement:

Stop using Domain-Trust!
Go beyond Trust!
Implement Dynamic Access Policies!

Break ATT&CK-Enterprise.
Save Money!

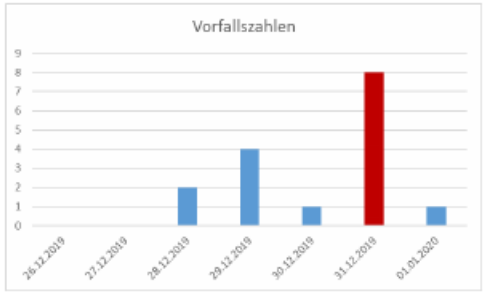
Backup

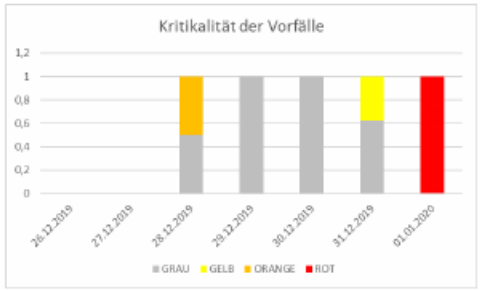
Characteristic numbers of IT-Security

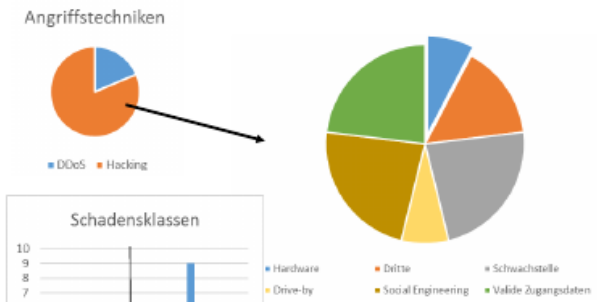
Describing the risk in a certain network using technical indicators

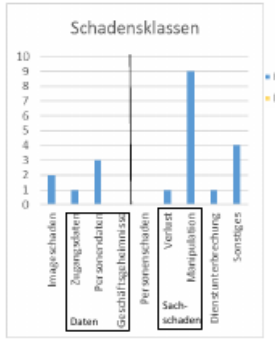
3.5
/10

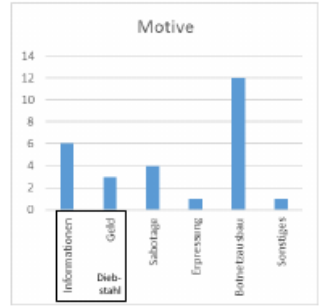
Overall
IT-Security-Index











Project Links

Planning & Reporting:
https://github.com/mitre-attack/attack-navigator

Data:
https://github.com/ukncsc/lme

Storage & Analytics & Data Model:
https://github.com/Cyb3rWard0g/HELK

Rules:
https://github.com/Neo23x0/sigma

TI:
https://www.misp-project.org/
https://github.com/certtools/intelmq

Incident Response:
https://thehive-project.org/
https://github.com/certsocietegenerale/FIR

Knowledge:
https://github.com/krakow2600/atomic-threat-coverage

Testing:
https://github.com/redcanaryco/atomic-red-team
https://github.com/mitre/caldera