

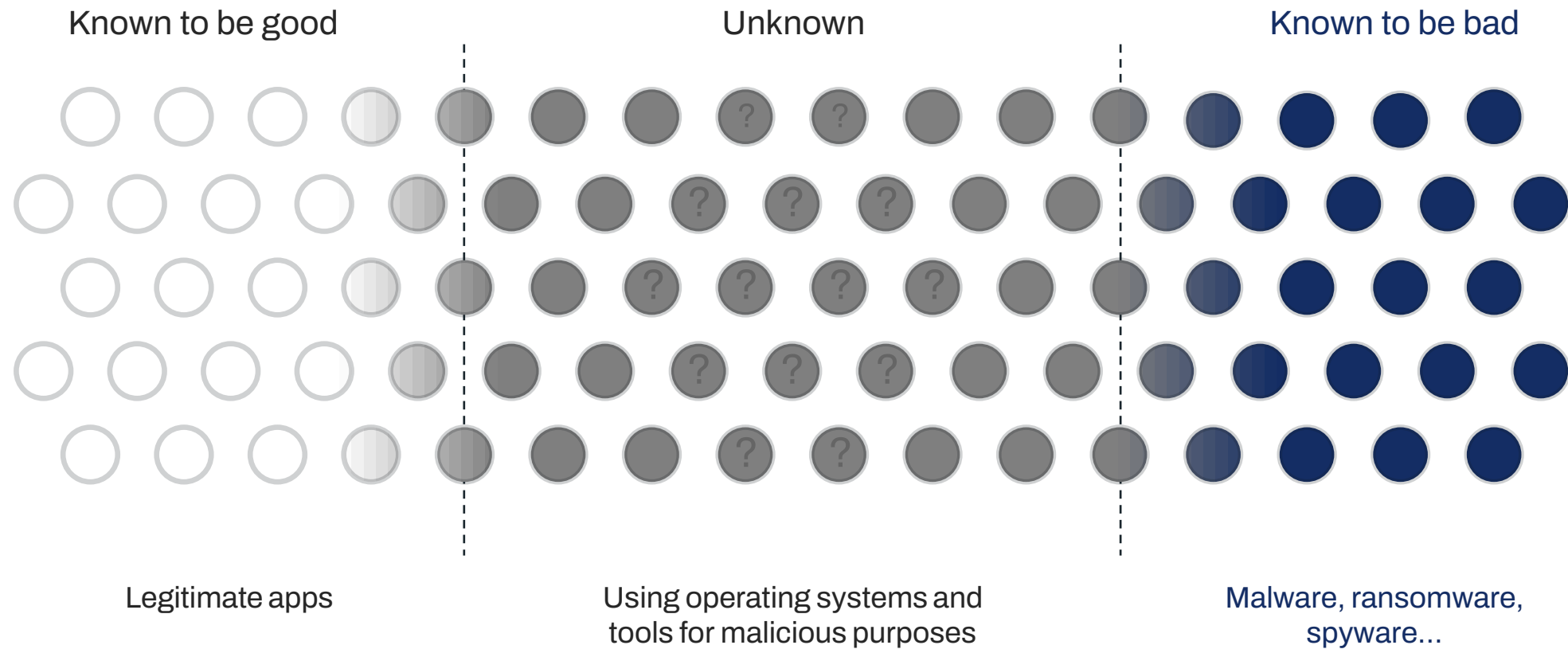
Managed SOC: Die Lösung aller Security Herausforderungen?

(ISC)² / ISACA Konferenz 2023 - 20.4.2023

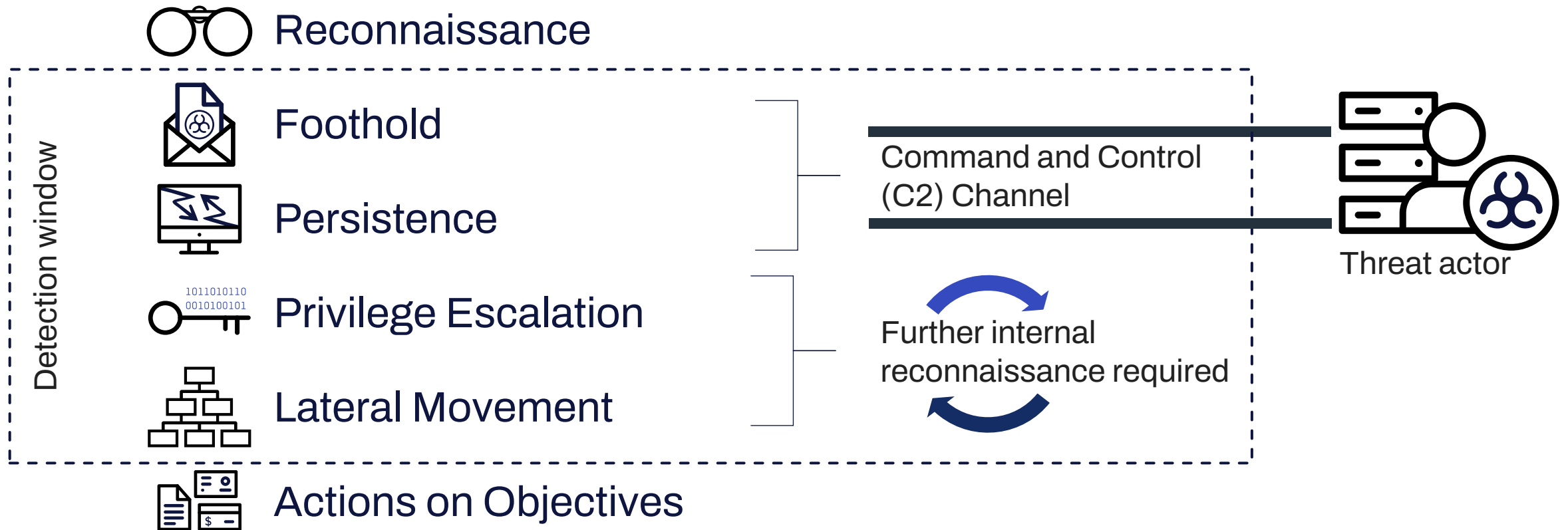
Jürgen Reinhart, CISSP, WithSecure GmbH



The Grey Area

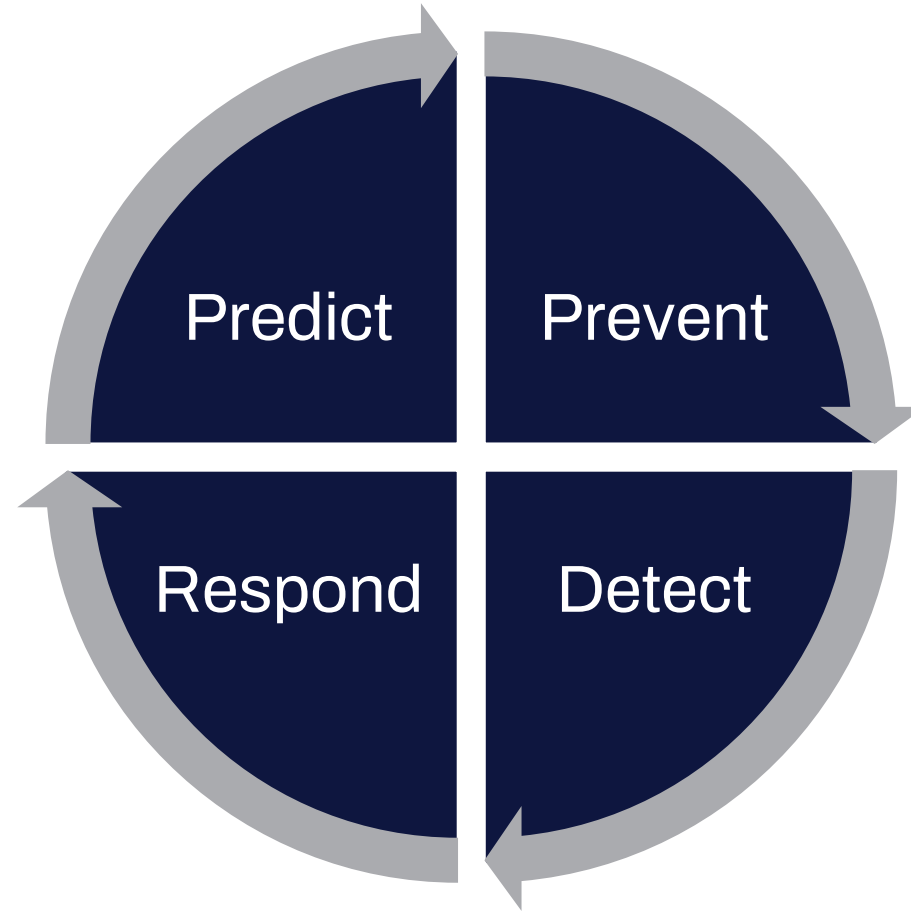


How attacks unfold



Ransomware | data theft | blackmail | business disruption | espionage

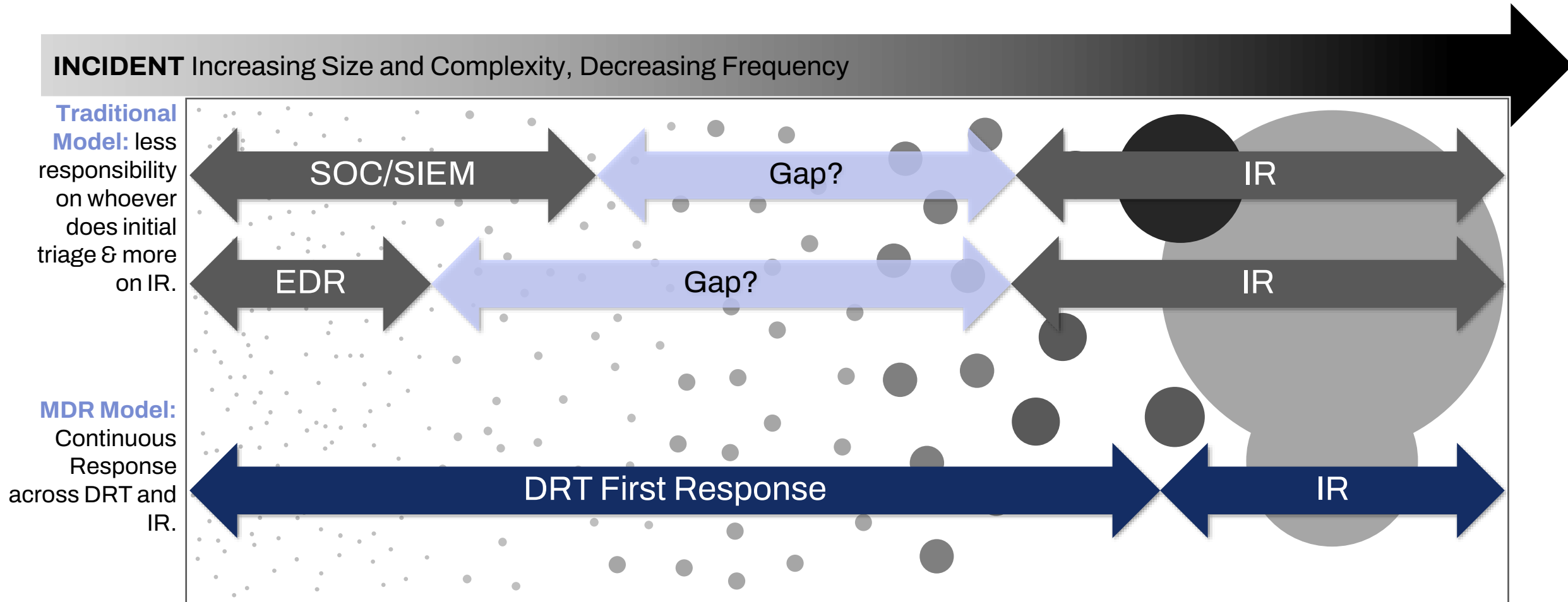
PPDR Model



Managed SOC, Incident Response, Managed Detection & Response



Managing the gap



24x7 Detection and Response service

Threat Hunting



- Gap Identification
- Use Cases
- Data Sources

Monitoring



- Data analysis
- Enrichment
- Alerting

Investigation



- Artefact retrieval
- Sample Analysis
- Reverse Engineering
- Event Correlation

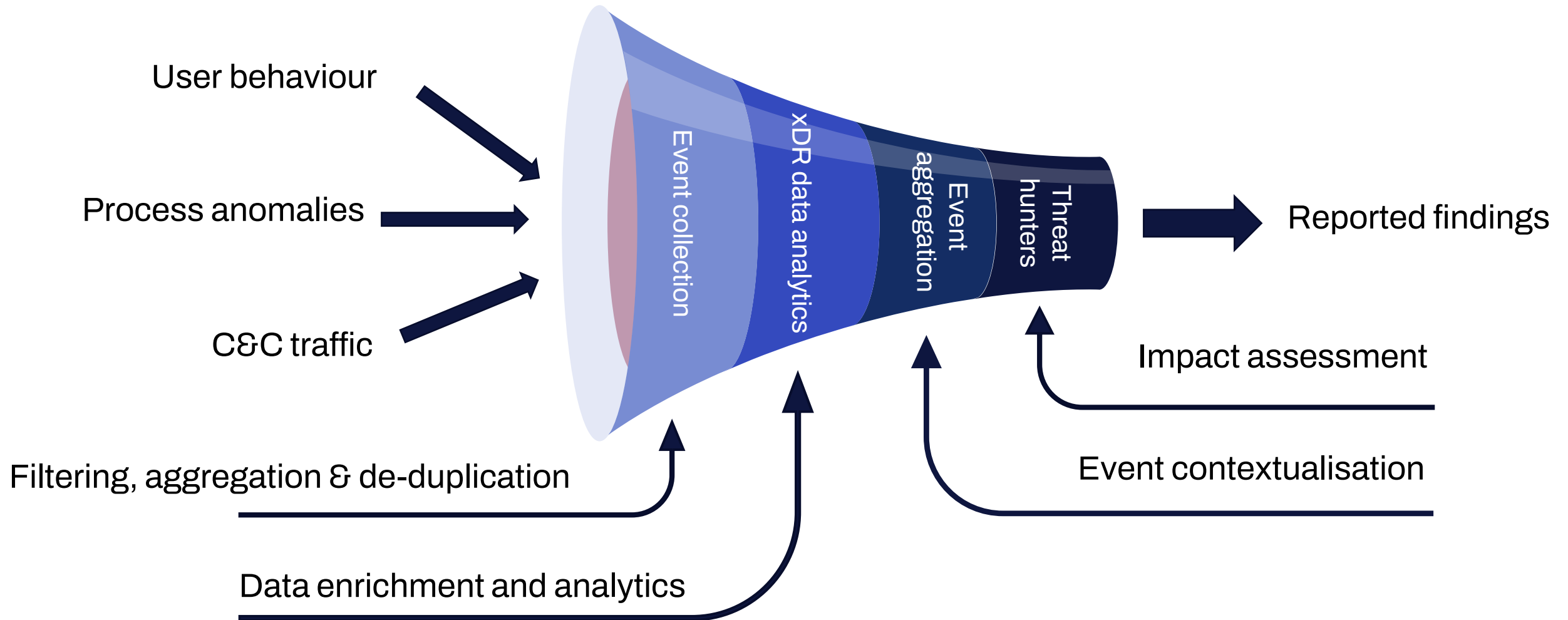
Response



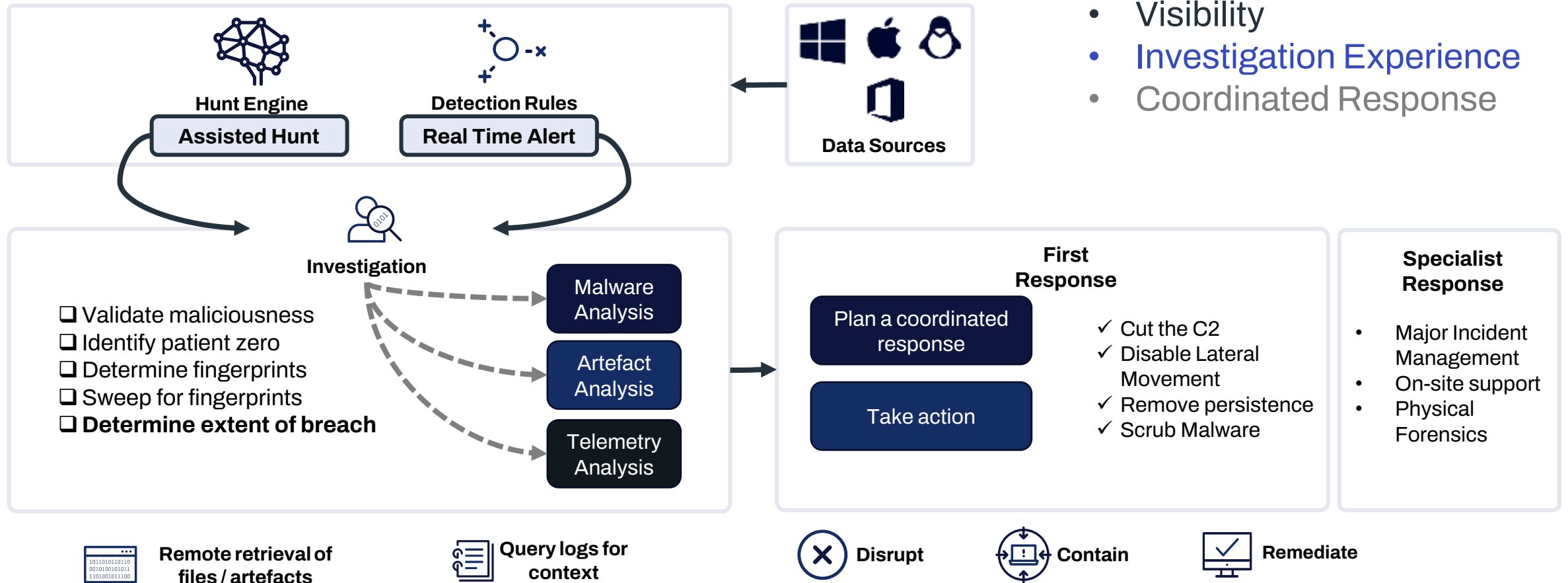
- Disrupt
- Contain
- Isolate
- Remediate

←—————→
A single team across all areas | Experienced Threat Hunters | Battle-Hardened

Context matters






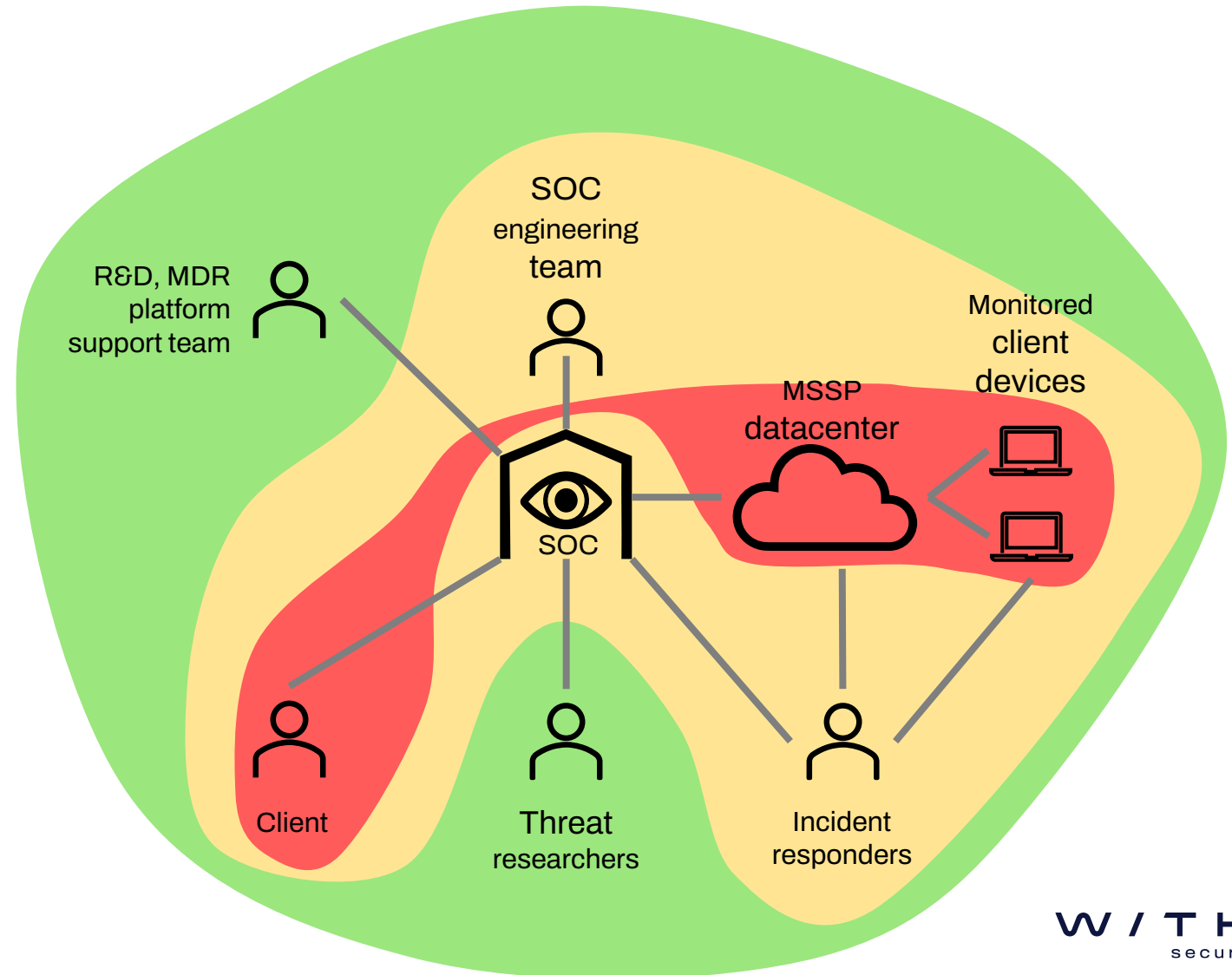
Effective Response



Each option offers a different degree of segregation

Types of Europe-only MDR service

-  1) Storage separation
-  2) Operational separation
-  3) Complete separation

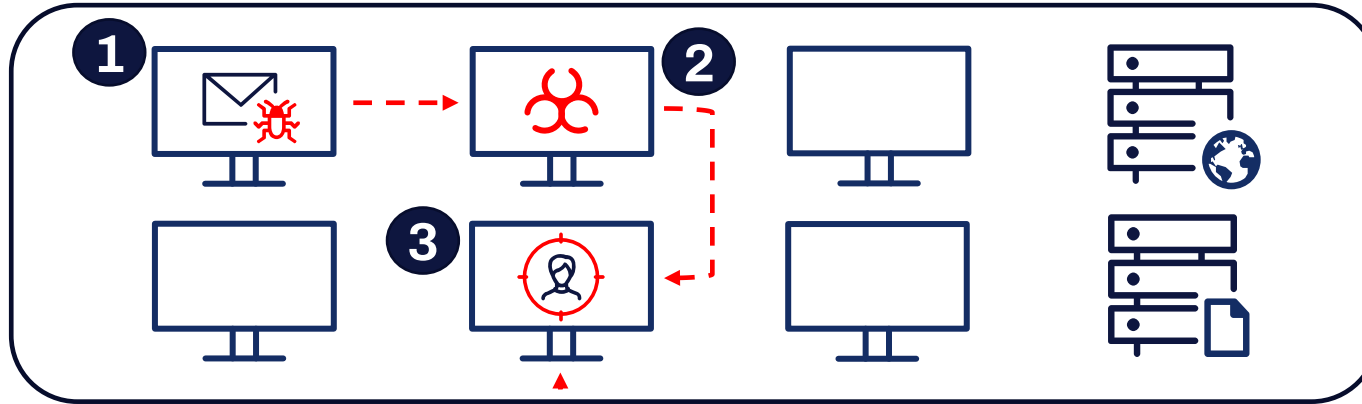


War Story



War Story

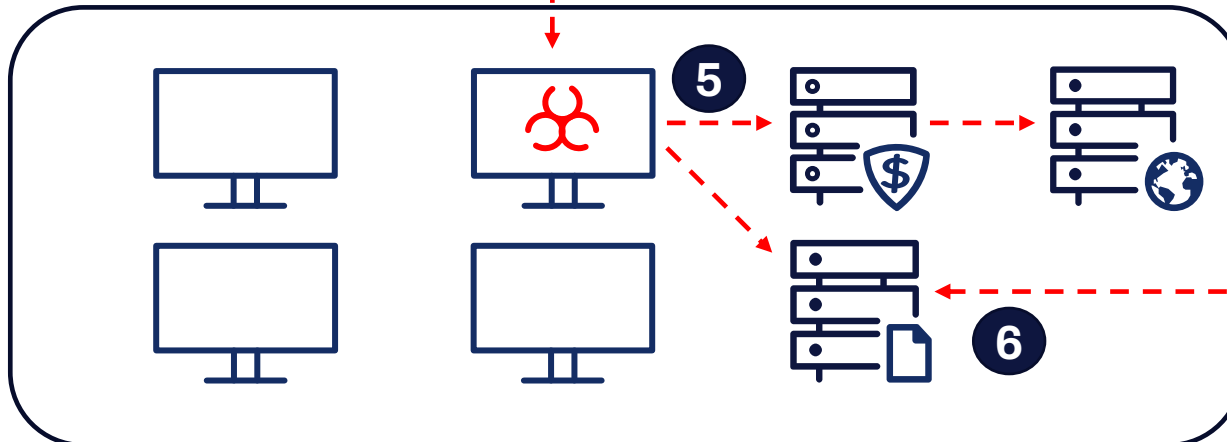
Parent Company



Domain trust with
parent company

Lateral
movement

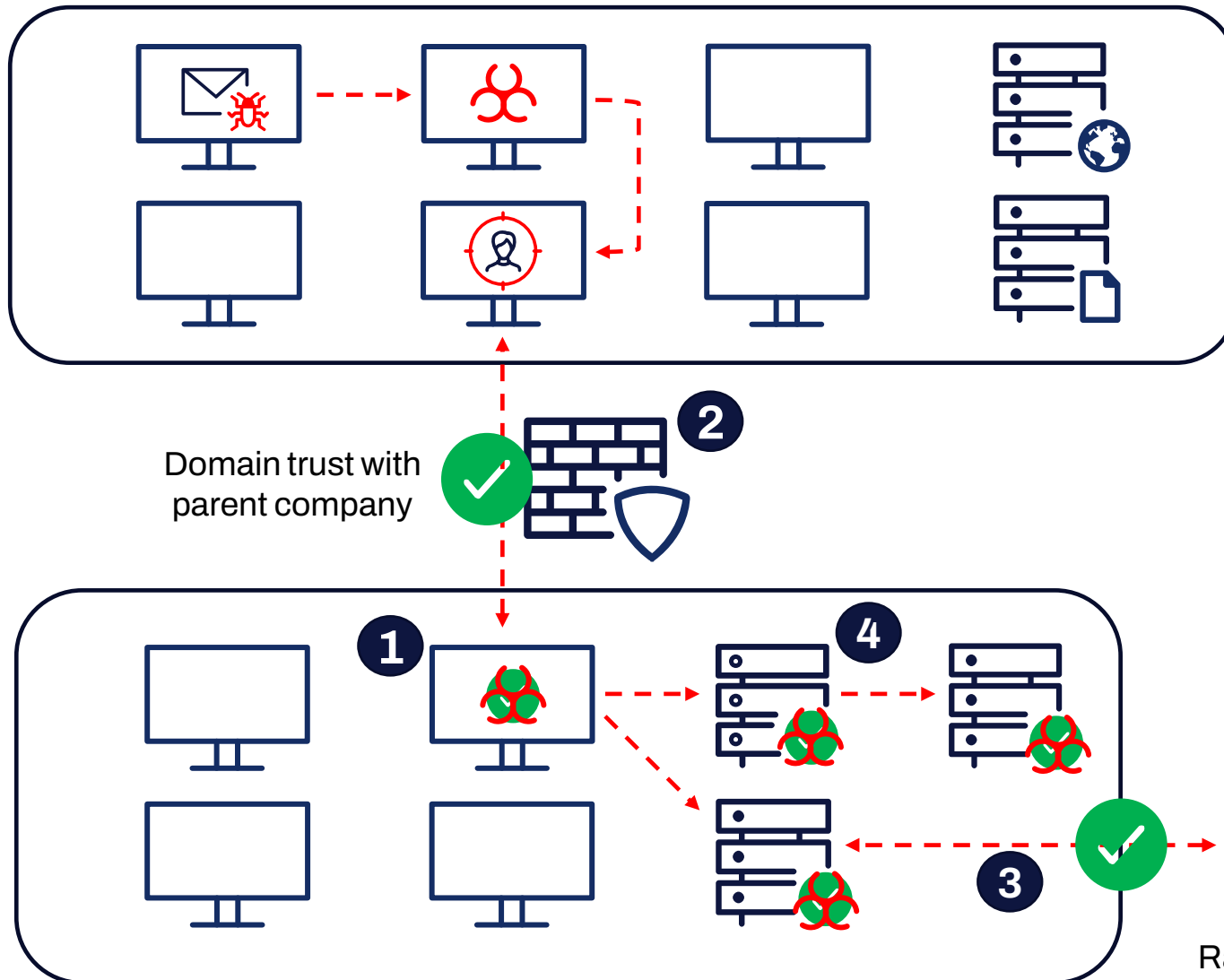
Customer Estate



- 1 Emotet payload delivered via email
- 2 Cobalt Strike used for lateral movement
- 3 Threat actor obtained domain admin credentials from the parent estate
- 4 Domain trust allowed the threat actor to gain access to our customers estate
- 5 Rapid access on to key domain assets
- 6 Command and Control to multiple domains

Ransomware
Operators

Detection and Response Timeline



① Movement onto the client estate fired an alert (Wednesday 20:27)

☎ The DRT triaged and confirmed the threat and then informed client via phone

② The DRT advised client to block connectivity from the parent network

③ The DRT passed the C2 domains to the customer to block on the firewall

④ The compromised endpoints were isolated and/or the beacons remotely terminated

✓ The attacker is completely removed from the client estate (Wednesday 21:47)



Incident investigated and contained in less than 90 mins

Ransomware Operators

Danke für ihre Aufmerksamkeit

Fragen?

Jürgen Reinhart - juergen.reinhart@withsecure.com



Weiterführende Information

- WithSecure Countercept (Managed SOC Service)
<https://www.withsecure.com/de/solutions/managed-services/countercept>
- WithSecure Labs
<https://labs.withsecure.com/home>
- WithSecure Incident Response
<https://www.withsecure.com/de/about-us/company-contacts/24-7-incident-hotline>
- WithSecure Webinare
<https://www.withsecure.com/de/whats-new/events/webinarreihe>



W / T H[®]
secure