Disclaimer
Confidentiality and publication

- This PDF has been created exclusively for visitors to the Swiss Cyber Storm event on 22 October 2024 in Bern and is available for download.
- Public use or distribution of this PDF and any information contained therein is not permitted.
- The content was checked for timeliness and accuracy at the time of the event. No statement can be made regarding its validity beyond this date.
- Copyright is held by Swiss Post Cybersecurity AG and the companies involved in this presentation.

Swiss Post Cybersecurity

Breach & Attack Simulation

Continuous Security Validation

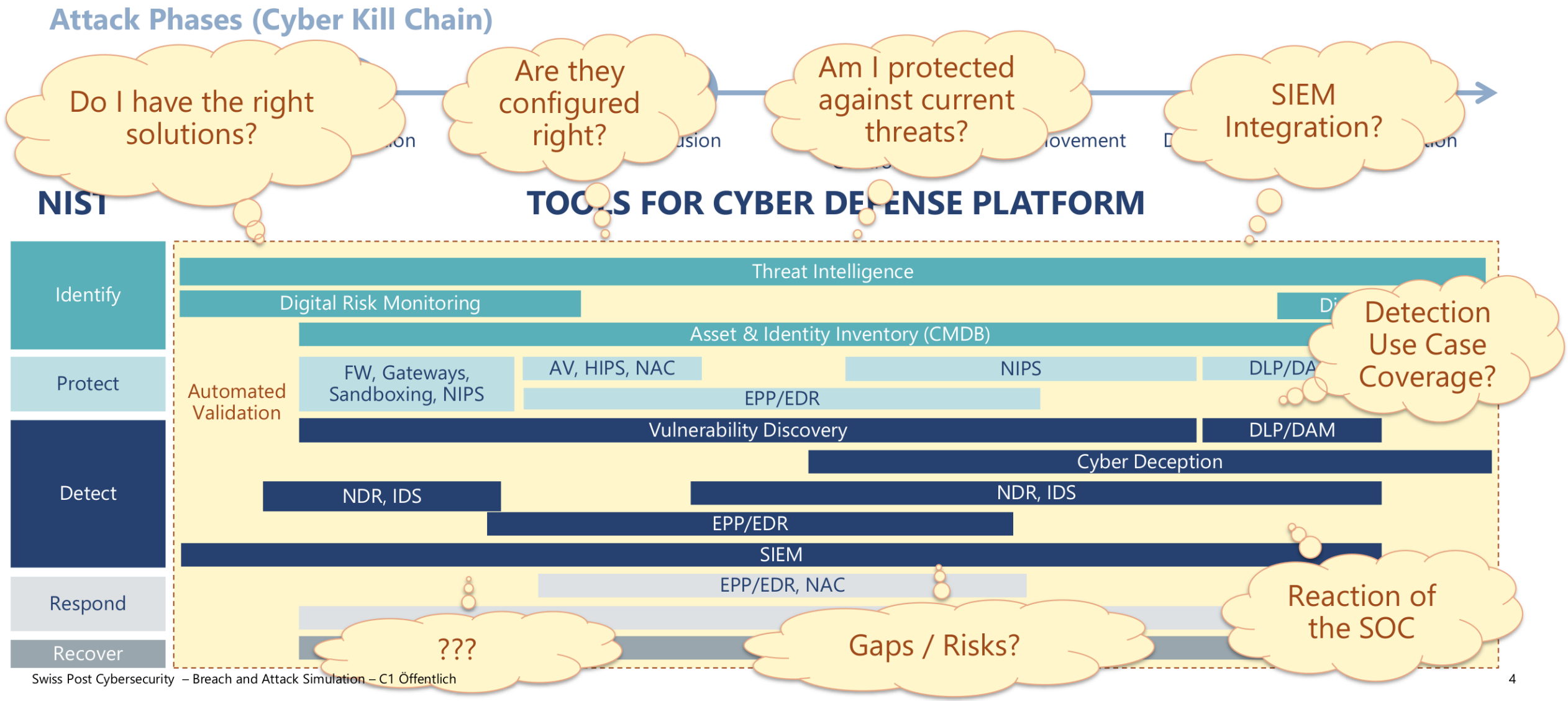
22. October 2024

whoami
Introduction

Raphael Ruf
Cyber Security Consultant at Swiss Post Cybersecurity

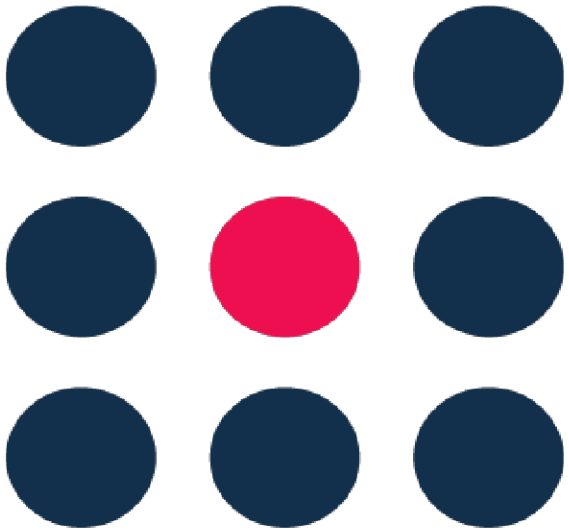
- 15 Years Experience in IT and OT
- Responsible for
  - IT & OT Penetration Tests
  - Vulnerability Management
  - Breach & Attack Simulation

Cyber Defense
Validate your security



Breach and Attack Simulation
What is BAS?

Continuous validation of your Security Controls



- **Continuous automated security validation**
  Security mechanisms are correctly configured and fulfil their function
- **Real Attack Simulation**
  Real attacks and threats – executed between simulators in your productive environment
- **Automated validation of the attacks**

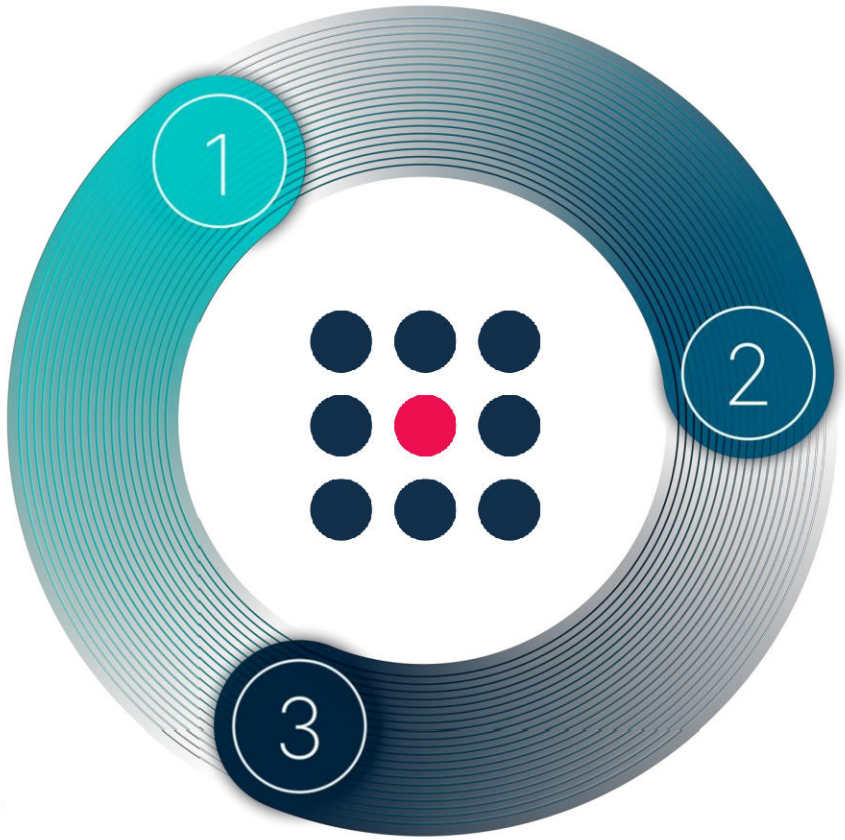
Our Partner

Pioneer in breach and attack simulation

BAS Process

Continuously attack

- Validate your security controls automatically and safely
- Most up to date and relevant playbook
- SLA - All US-CERT alert added within 24 hours



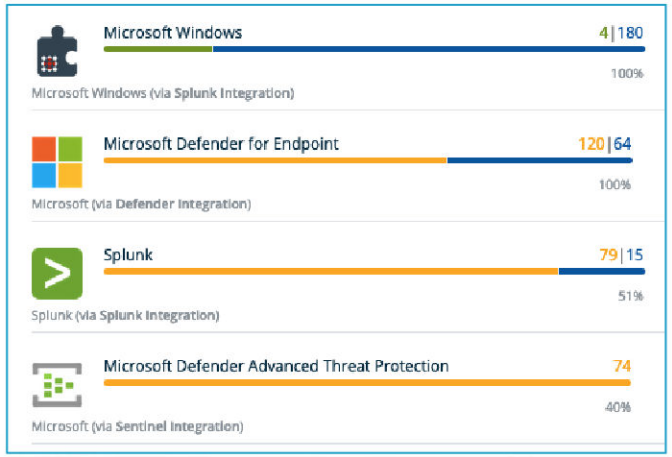
Prioritize results

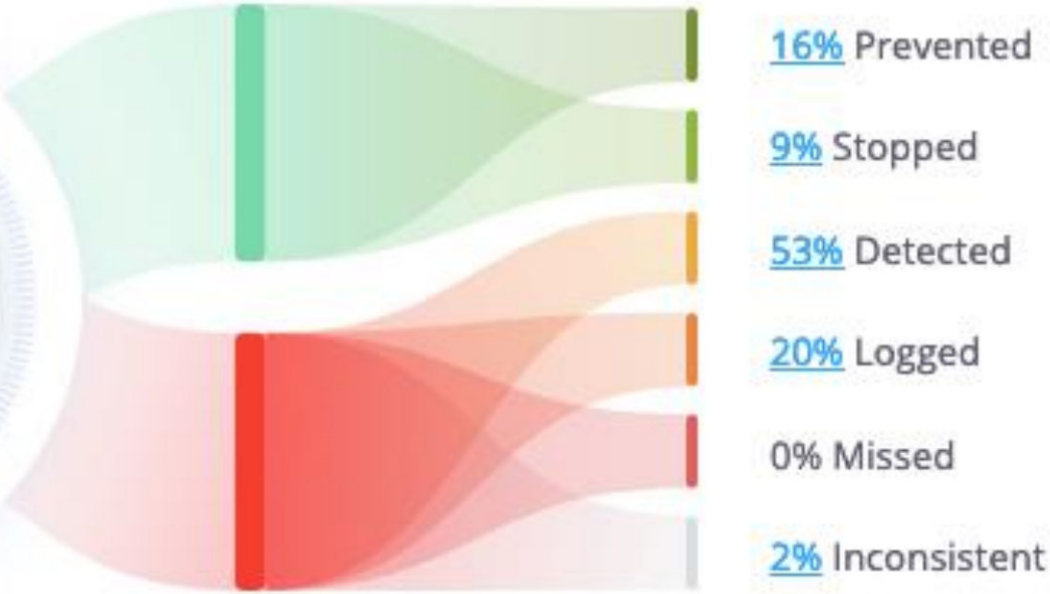
- Visualize the security posture
- Prioritize results and identify remediation

Drive down risk

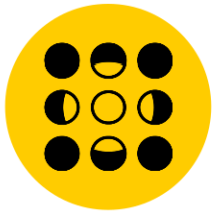
- Remediate findings
- Security posture optimizer to track progress and present board level KPIs

Validation
Security Control Integration



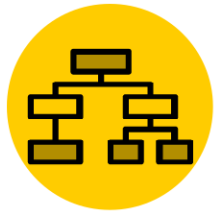


SafeBreach
Components



Simulators

- Lightweight SW agent, deployed on representative systems internal and external
- Assume attacker and target role in attacks to maintain safety
- External attacker in the cloud



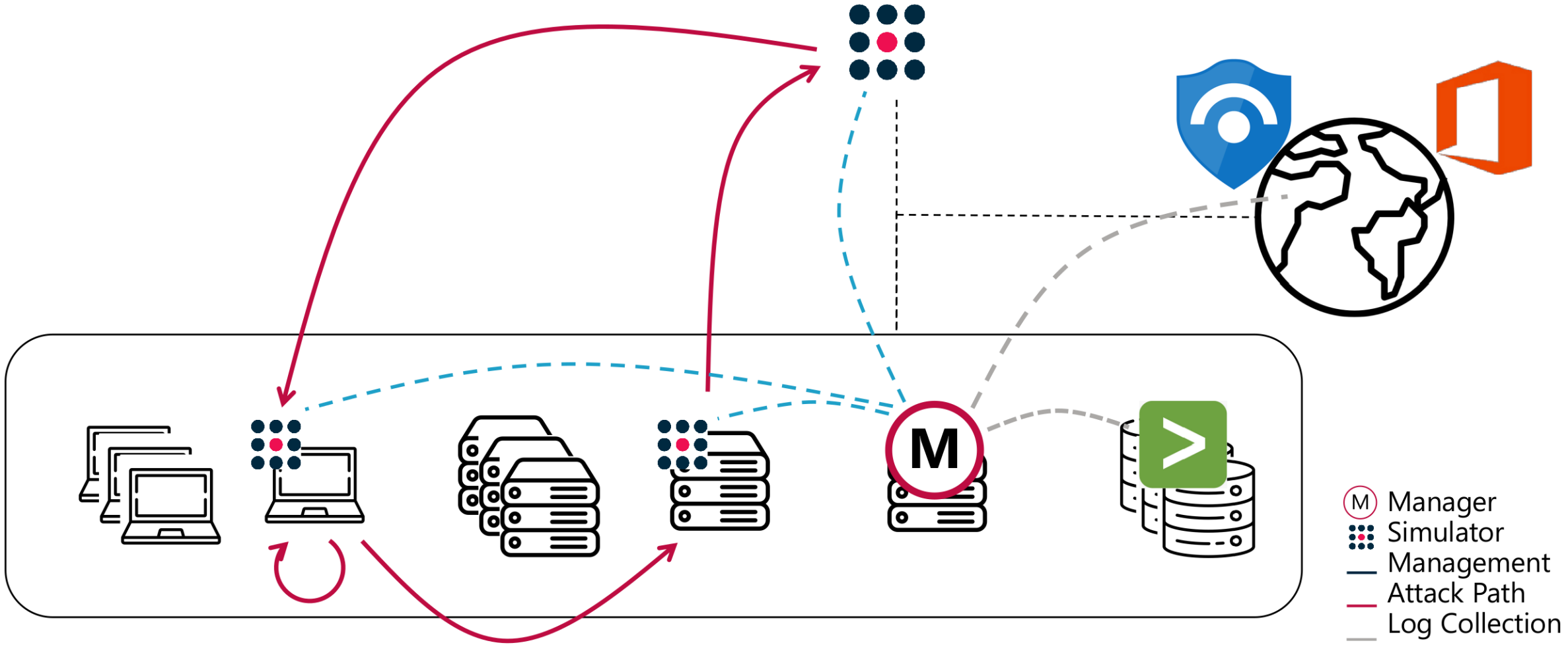
Management

- SaaS, On premises or air gapped
- Plans, orchestrates and aggregates results data into reports, visualizations and analytics
- Integration in Security Controls

Attack Playbook

- Cloud service which holds thousands of updated attack methods
- No software update required for new attacks, attacks updated automatically

Architecture
SafeBreach On-Prem

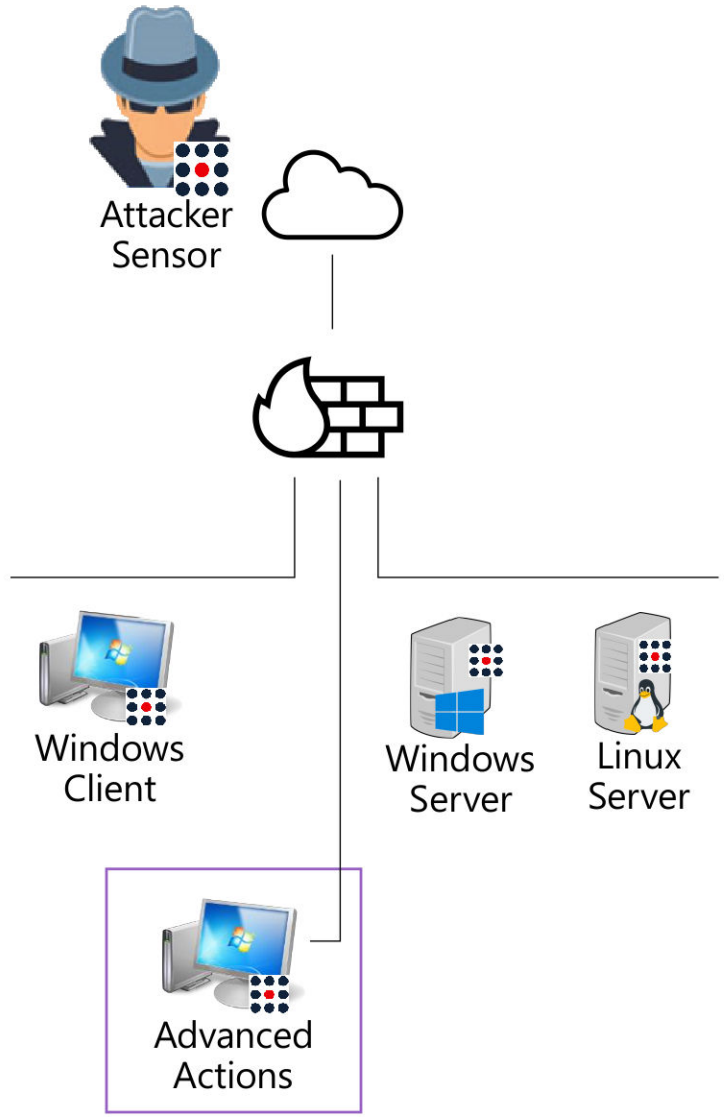


Architecture

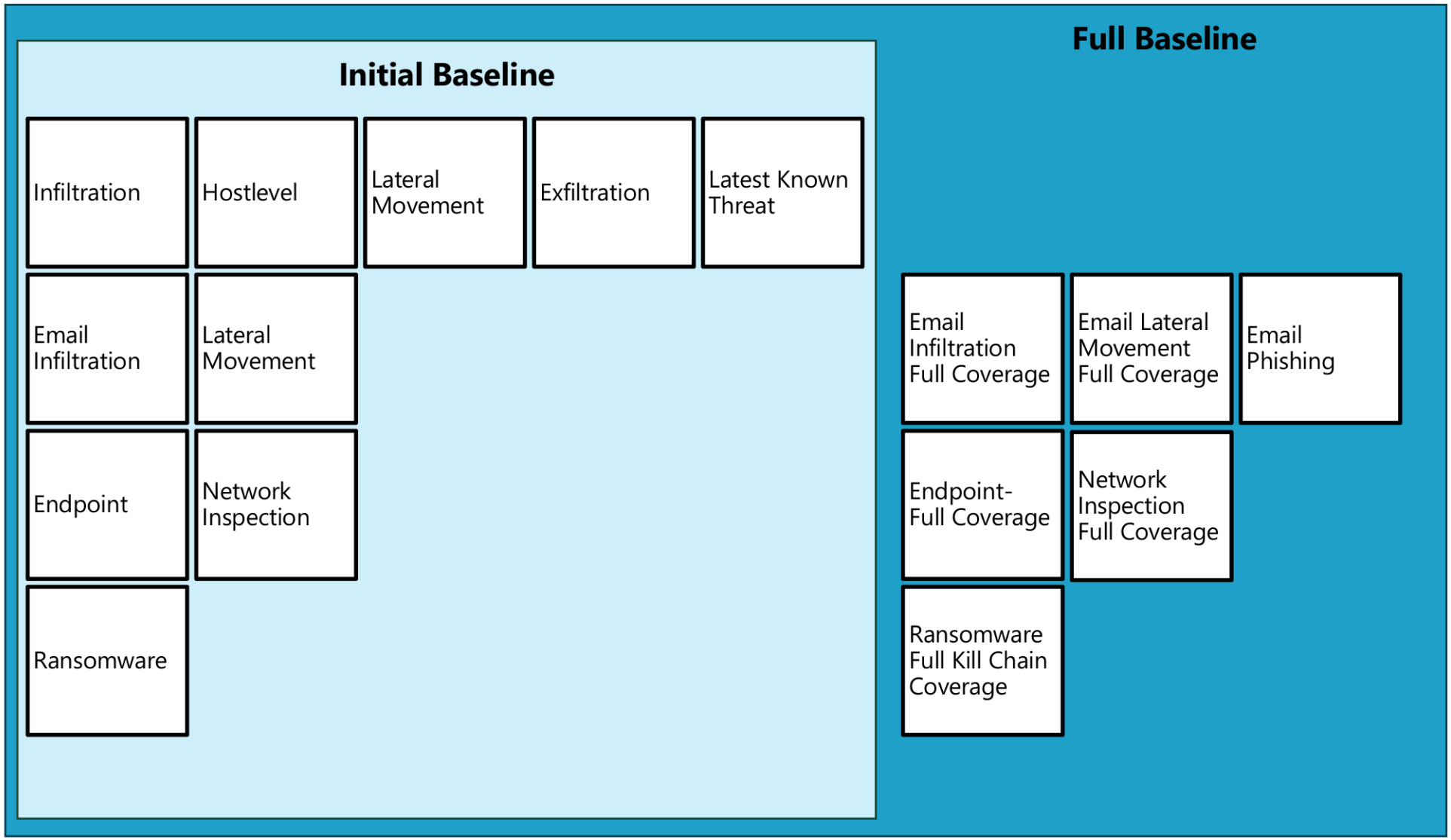
Where to place the simulators?

Minimal setup with 5 Simulators

- Cloud (external Attacker)
- Client
- 2x Server (Windows & Linux)
- Advanced Actions (for specific scenarios)
  - Isolated system
  - «real» Malware



Scenarios


Initial Baseline
Infiltration
Hostlevel
Lateral Movement
Exfiltration
Latest Known Threat
Email Infiltration
Lateral Movement
Endpoint
Network Inspection
Ransomware
Full Baseline
Email Infiltration Full Coverage
Email Lateral Movement Full Coverage
Email Phishing
Endpoint- Full Coverage
Network Inspection Full Coverage
Ransomware Full Kill Chain Coverage

BAS as a Service
Integration & Service

- SafeBreach running continuously
- Quarterly BAS-Status-Report with Enhancement Session
- Integration in SIEM with Use Case «SafeBreach Score Increased»
- Support through our SOC-Analysts
- Latest Known Threats
- AdHoc Simulations (Emergency Threads)

DEMO

Conclusion
Continuous Validation

1. Guarantee the effectiveness of your security controls
2. Fix issues before they become a problem
3. The perfect addition to manual Pentests / Purple Teaming
4. Real setup with real attacks, targeting your productive security controls

Questions

Thank you, Danke, Merci, Grazie