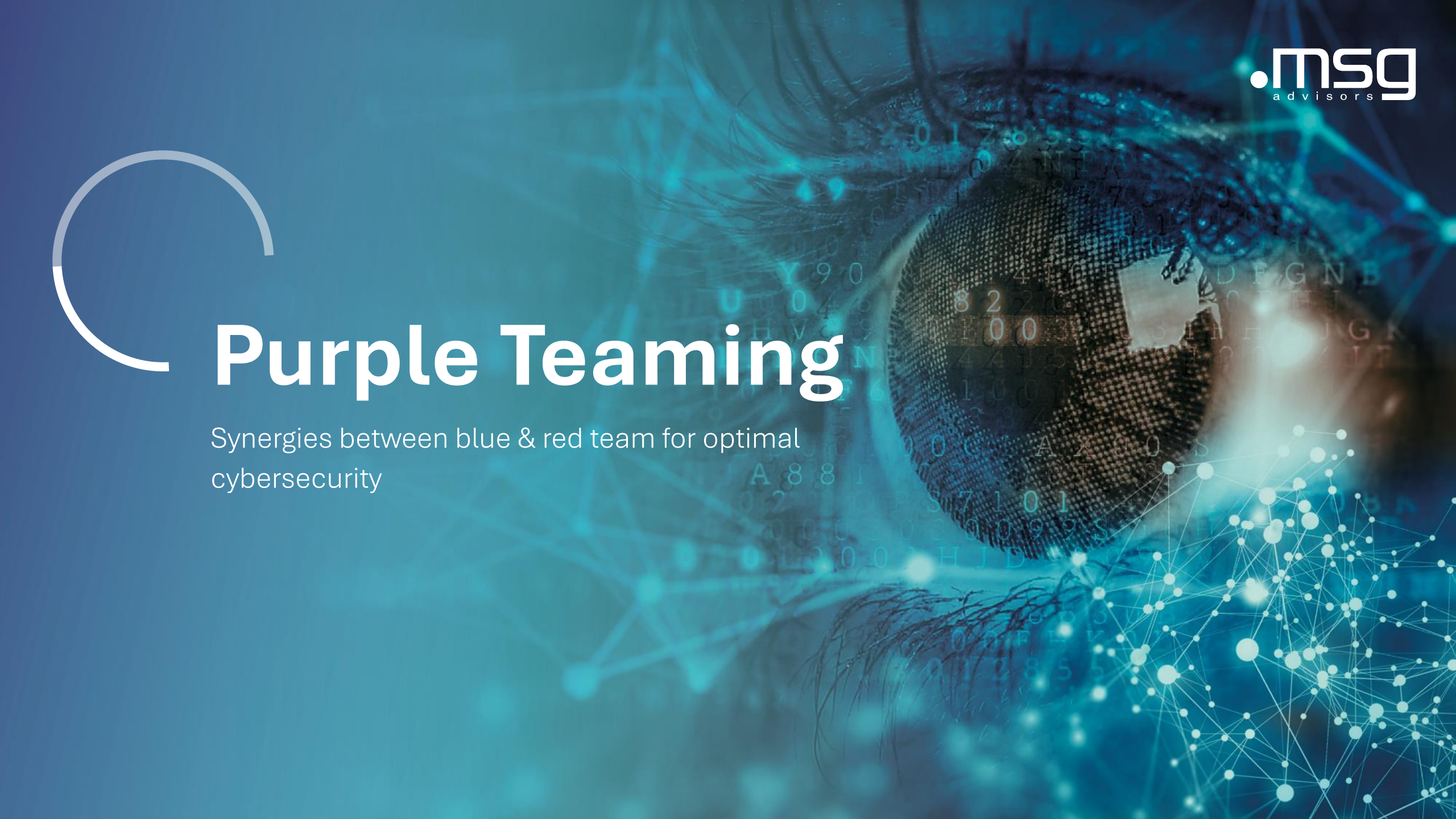


Purple Teaming

Synergies between blue & red team for optimal cybersecurity

Current state of security

We currently have 2 teams

The blue team

... sets up detections and alarms
... reacts to detections
... investigates attacks
... builds defenses

The red team

... conducts assessments
... prepares and builds attack infrastructure
... writes reports und publishes attack vectors

They rarely interact with each other, mostly just for pentests

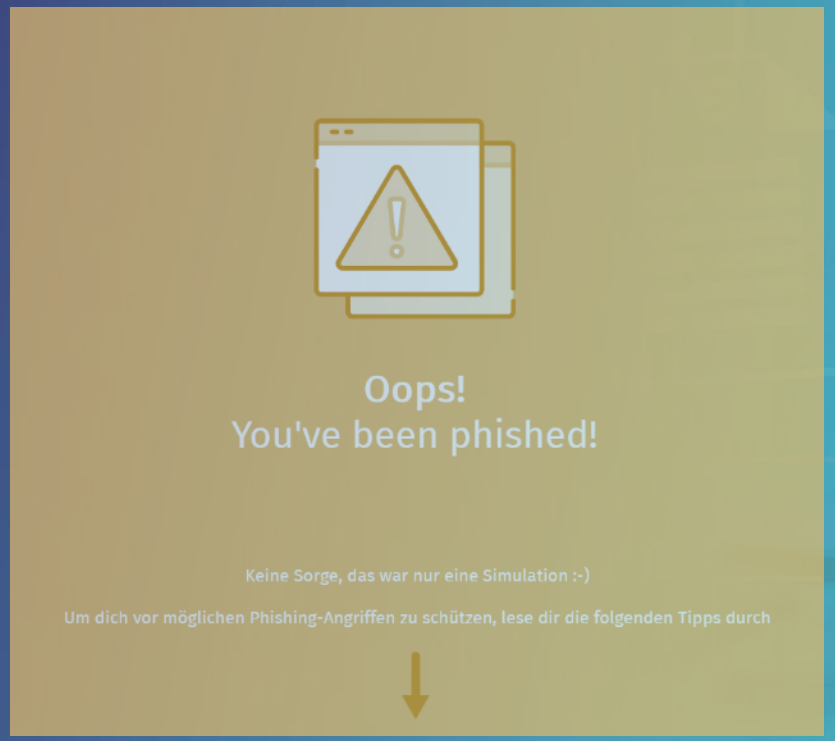
Examples for insufficient testing: Pentest

1. Define scope
2. Pentest team gets involved
3. Pentests for 1-2 weeks
4. Creates reports and leaves
5. Blue team then has to fix everything

Problems:

- Snapshot of a fast-moving ever-changing environment
- Can you be sure that your mitigations and detections work, even with a retest?
- Pre-defined scenarios in a constrained scope – How do you test something you don’t know?
- There are often multiple mitigations. Which is the right one?
- Who helps the blue team to pick the most cost-efficient choice?

Examples for insufficient testing 2: **Simulated phishing campaigns**



Is **red teaming** the cure?

- Red Teaming provides holistic, long-duration attacks
- Targets the entire organization, not just specific systems
- No or very broadly pre-defined scope
- Produces advanced, detailed reports covering complex vulnerabilities

But: Most organizations aren't ready for this level of complexity

- Reports are often too advanced for many organizations to take action
- Requires high-level security maturity - most organizations aren't there yet
- Weekly and detailed reports can be overwhelming, leading to partial or missed remediation
- Big one-time payment

How **purple teaming** aims at solving this

- **Collaborative approach**: Offense and defense work together.
- **Miniature assessments:** Continuous testing for each target and technique.
- **Cycle of improvement**: Test, detect, improve until detection and defense are effective.
- **Real-time feedback**: Immediate adjustments, no waiting for final reports
- **Cross-functional work**: Brings together diverse teams - security, operations, and developers.
- **Knowledge intersection**: Shared insights between offensive and defensive teams.

Let’s look at some use cases

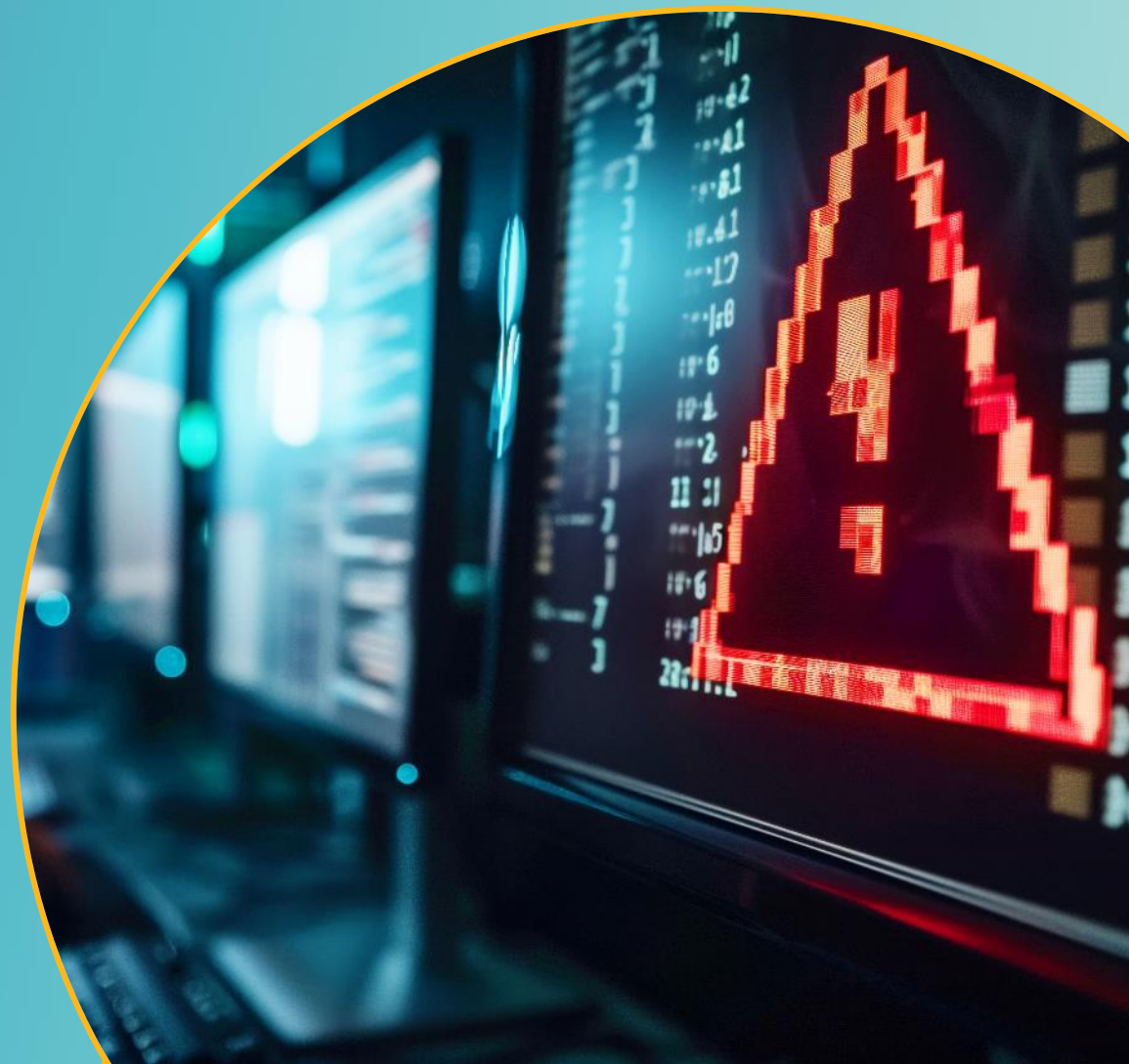
Use case 1: Malware development & analysis

- **Blue team:** Regularly conducts malware analysis.
- **Red team**: Develops implants for our C2 framework.

Collaborative practice:
Blue team dissects red team's malware.
- Test obfuscation quality.
- Provides real-world training material.

Mutual skill enhancement:
- Blue team improves analysis techniques.
- Red team improves obfuscation based on feedback.

Real-world application: Red team functions as "consultants" for malware analysts



Use case 2: Security validation / playbook reviews – what do we miss?

Blue team: Our SOC builds playbooks and detections.
Challenge: Does it detect every variant of the attack? Example: Rubeus Golden Ticket vs. Mimikatz.

Collaborative iteration:

- Test attack techniques with multiple tools.
- Review each detection outcome - what's missed and why.
- Work together to improve detection accuracy.

Repeat: Refine until all variations are covered.

Use case 3: Continuous knowledge sharing in practice

- **Weekly meetings:** Every Friday, offensive and DFIR teams collaborate.
- **Topic presentation:** One team member presents a topic (e.g., AD Pentests).
- **Collaborative discussion**: Both teams discuss prevention, detection, and improvements.

Example: AD pentests - attack strategies vs. detection and mitigation techniques.

- Daniel presents how a kerberoasting attack is performed
- Eike explains how he builds a detection for kerberoasting
- Jan adds then that in the past he changed the encryption of the ticket to make the cracking harder

Gained knowledge:

- Red team now knows about datapoints, which they must be more careful with to avoid detection
- Everybody in the dfir team now knows what is kerberoasting and how to mitigate and detect it

Use case 4: Improved incident response

- **Blue team:** Our SOC monitors customers for detections
- **Red team**: Has knowledge about how they would approach a target

Real-world application:

1. SOC detects attack
2. During investigation, they find out a lot of domains were contacted by an attacker
3. The attacker tried multiple mDNS requests
4. SOC asks red team why this happens
5. Red team explains that they used this technique in the past to do network discovery

Use case 5: Table top exercise

Dynamic & realistic scenarios: Exercises mirror real-world complexity.

Full team collaboration: Both red and blue teams participate, ensuring realistic challenges and responses.

No pre-defined solutions: Unlike traditional exercises, no static answers - forces adaptive thinking.

Reflect real reactions: Red team simulates evolving threats; blue team responds in real time.

Improved preparedness: Enables both teams to test their strategies under pressure, adjusting them based on real adversary behavior.

Challenges with purple teaming

For a useful purple teaming we need:

very good communication

willingness to share knowledge

time investment by both parties

If there is not a 100% commitment from both blue and red team it will fail

Key findings

Facts:

- We have a blue and red team
- Pentests are useful for product security
- Red teaming is good for orgs who have a mature security environment
- Purple teaming is good for orgs at any stage
- Purple teaming delivers continuous security improvement, in contrast to one-time tests

All three approaches have disadvantages

Contact

Daniel Riebel
Pentester & Red Teamer
daniel.riebel@msg.group
msg security advisors

Eike Steinweg
DFIR & SOC Analyst
eike.steinweg@msg.group
msg security advisors

msg security advisors
Robert-Bürkle-Straße 1
85737 Ismaning
Germany

Tel: +49 89 96101-0
Fax: +49 89 96101-1113

security-advisors@msg.group
https://security-advisors.msg.group