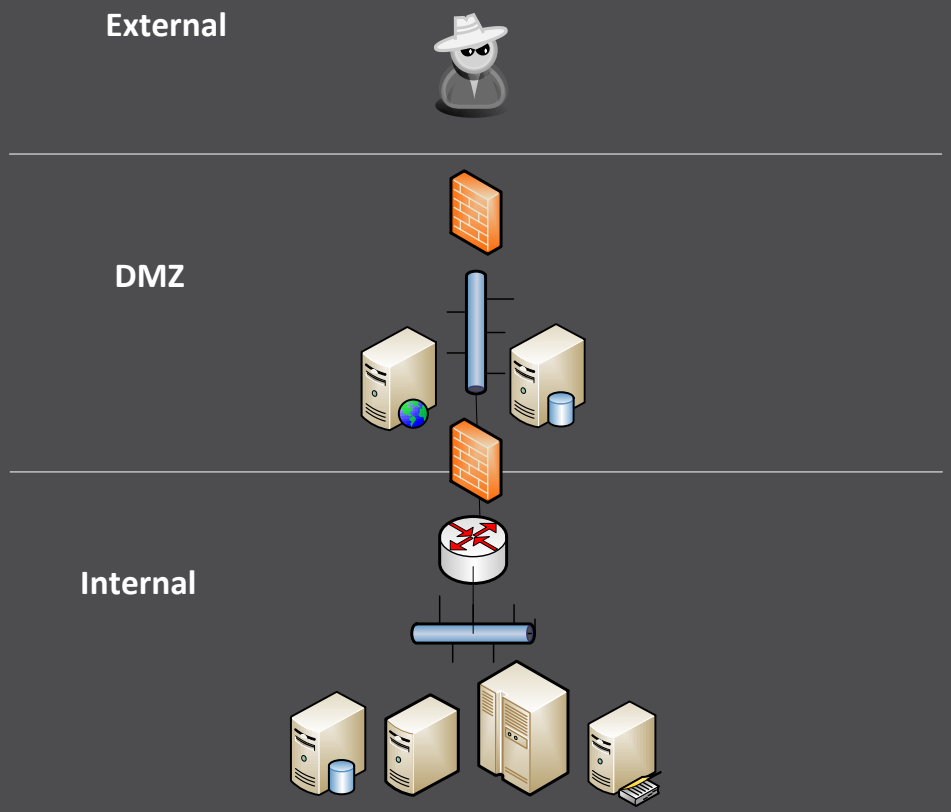
Developments in Red Team Penetration Testing

Mark Nicholls

11/07/2016

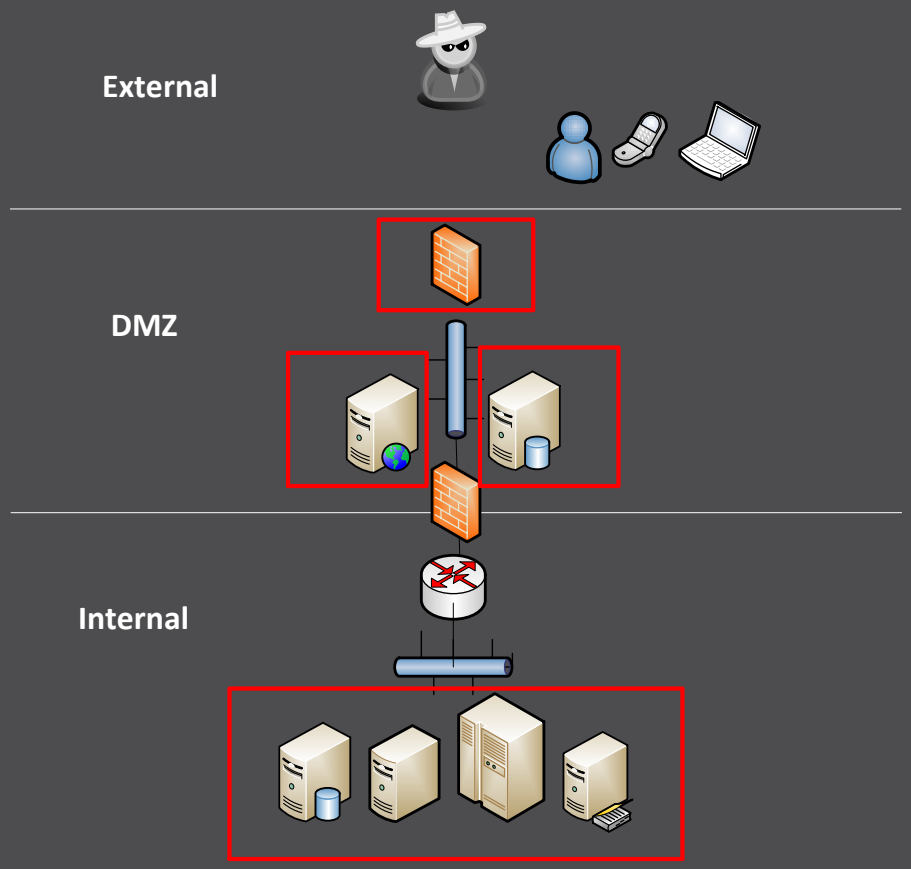
context

Security testing – original approach



context

Security testing – common approach today



context

Red team vs Pen Test

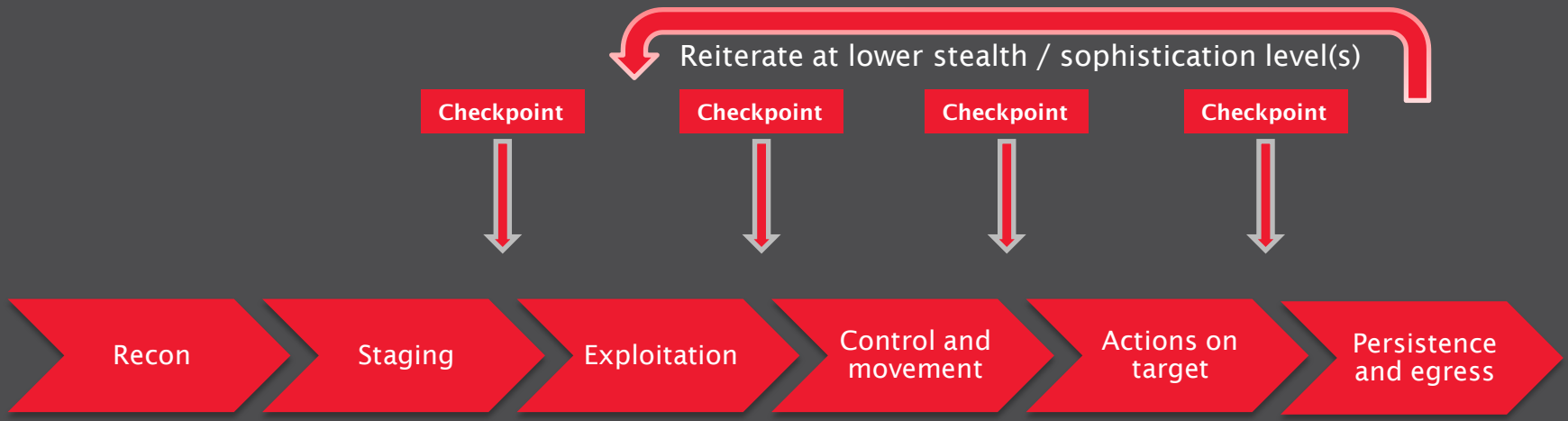
context

The red team approach

- Depth vs. breadth
- Target people and process as well as technology
- Assess capability of an organisation to identify, defend against, and respond to attacks
- End-to-end, real world assessment
  - Often with minimal non-public knowledge
  - Test with all security controls in place where possible
- Threat-led / attacker simulation
- Risk Mitigation – Make it safe and worthwhile
- Consider the whole picture

context

Our red team approach



context

Easy wins for attackers

- Profile vulnerable software from the internet
- Use Shellshock/Heartbleed vulnerability to compromise internet-facing server
- Send one email, get access to 300 workstations
- Fly under the radar using simple, undetectable tools
- Use the default SQL Server password to access financial data stores
- And then the password ‘Welcome1’ to access every server
- Exfiltrate data over HTTPS to avoid detection
- Find passwords on Internet and gain access remotely

context

Effective techniques for Context

Recon

- LinkedIn / Shodan

Attack Delivery

- Low email numbers
- Sophisticated email campaigns
- Repeated emails to small number of users
- Unsubscribe..
- Whitelisting our own sites

context

Effective techniques for Context

Internal Compromise, Movement

- PowerShell
- Plaintext credential dumping
- Network share enumeration
- Active Directory / Infrastructure Naming Conventions

context

Effective techniques for Context

Persistence / Maintaining Access

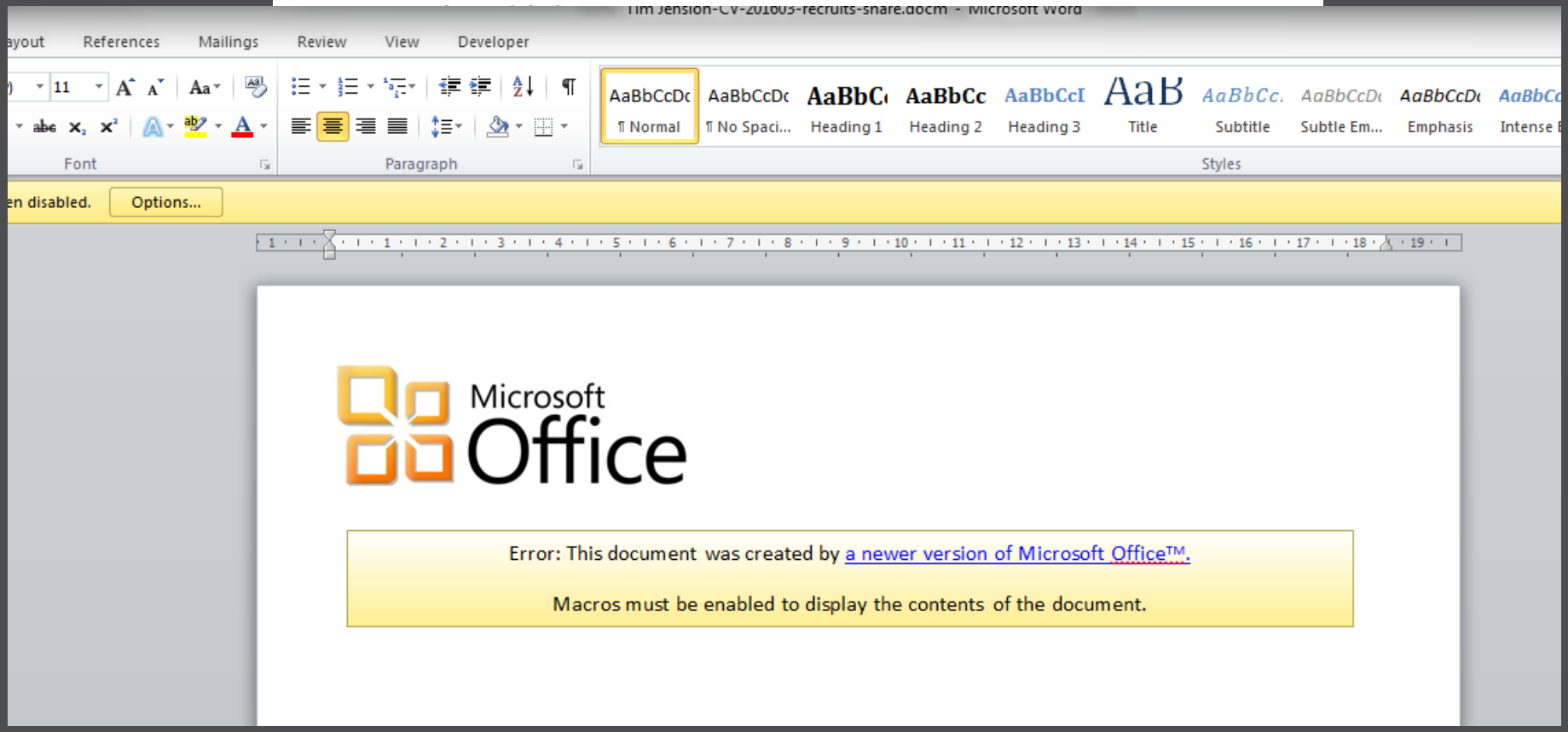
- Scheduled Tasks
- Single-Factor Authentication on Remote Access Systems

Exfiltration

- HTTPS

context

Effective techniques cont'd



context

How to defend well – Context's experiences

1. Deployment of border controls such as URL reputation filtering / whitelisting – SSL MiTM!
2. Patch everything – especially workstation software
3. Improve user awareness – particularly around reporting suspicions
4. Develop / Improve capability to respond to alerts – e.g. AV, traffic monitoring
5. Restrict and minimise use of DA / privileged accounts
6. Audit password quality, default passwords and lifetime
7. Segregate systems where possible
8. Network share lockdown

context

Successful red team?

context

50+ red teams in…

context

Improvements?

- Some orgs now have working SOCs.
- Companies have invested massively in security technologies and some of it works.
- Companies have been red teamed, had the wakeup call and made changes / fixes
- Still a long way to go
  - Tested companies were at the more difficult end of the scale
  - Recent assessments from different sectors have been a much easier target

context

Common Pitfalls

- ‘Just hack some stuff’
- ‘By any means available’
- ‘Provide a realistic and detailed simulation of 3x separate advanced threat actors… … in 2 weeks’
- ‘Get in, be undetected, get out’
- Deliver big scary report, get out

context

Looking forward and gaining value

- Collaborative and less about who 'wins'– it's time to improve the SOCs capability
- Subsequent red teams should be a training exercise
- Improve the scenarios for the red teams
- So what can we do?
  - Combine the red and blue teams – (1) Purple team engagements
  - Be more specific - (2) Targeted white-box red teams

context

(1) Red team as a SOC training exercise

- Treat as a dry run exercise against a real attack
- Identify what the SOC saw and didn't
- Move away from adversarial 'win / lose' approach
- Move away from adversarial 'get in and out without being seen'.
- Define metrics and apply them to defensive techniques

context

(1) Red team as a SOC training exercise

- Where were the attackers spotted?
- What level of coverage did the SOC have of the attack?
- Did the SOC get ‘lucky’?
- What defensive systems need refining?
- Which ones can be most relied on?
- Compare attacker logs and defender logs
- Refine processes based on the answers

context

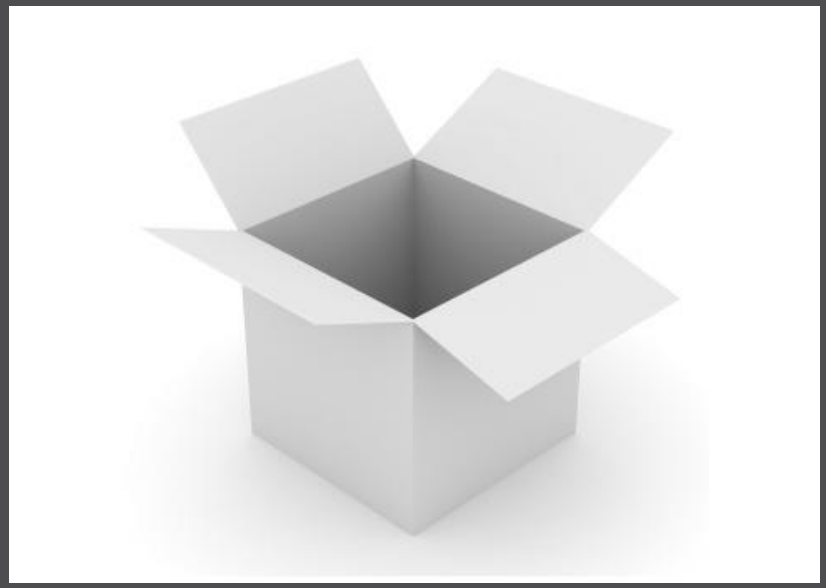
(1) Red team as a SOC training exercise

- Greater understanding of risk
  - Understand the attack and how to defend
- Better chance for us as testers to be part of the solution.
  - Not just delivering recommendations, but assisting on the solutions

context

(2) Targeted / white box red teaming

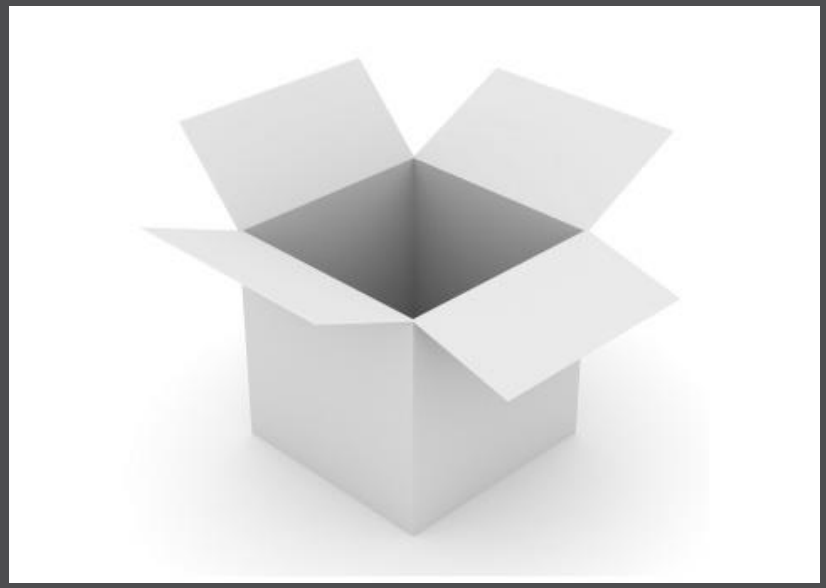
- Companies with advanced defences may well be able to repel a time limited red team.
- They can still have problems with attackers though.
- Looking forward - We can see it becoming more focused on detailed and specific scenarios



context

(2) Targeted / white box red teaming

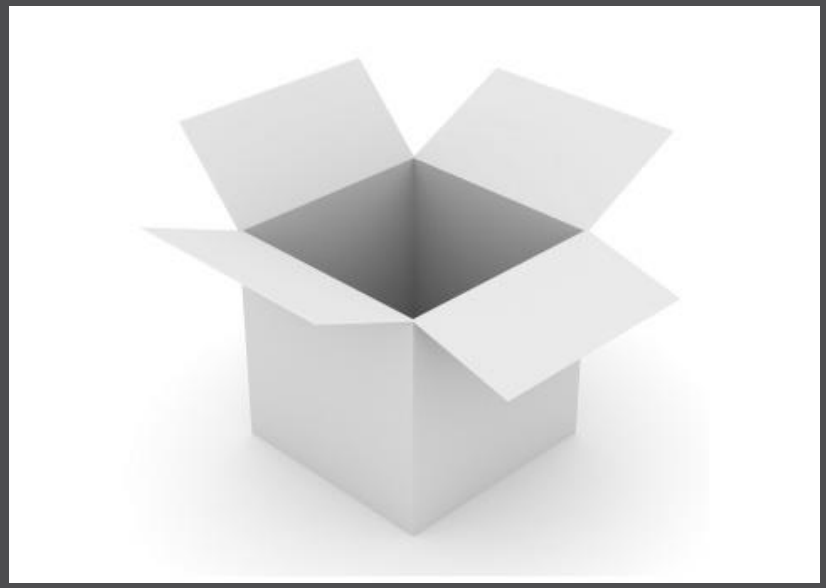
- ‘If you had compromised a border device, could you pivot from there to the internal network? How quickly would you be detected?
- You’re internal and privileged – can you get onto X system without triggering an alert?
- Can you get from [remote gateway] to [segregated network]?



context

(2) Targeted / white box red teaming

- Consider what controls you are testing
- Specific point red teams – e.g.. targeted against known elements of the environment.
- More defined TTPs taken from real attacks.
- More specific training goals.



context

And going further…

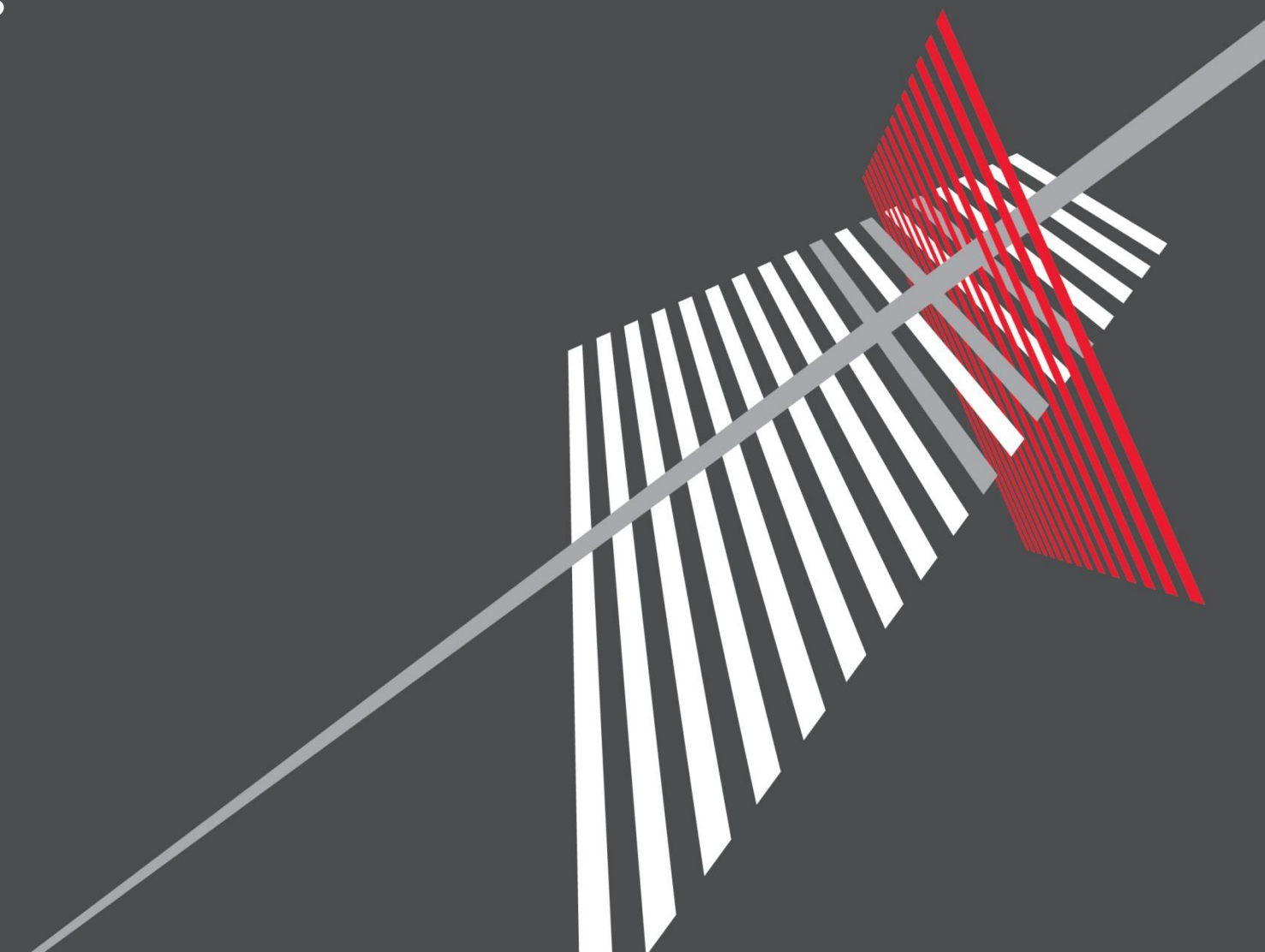
- Repeat the process and improve it
- Refine the SOC capability until it can deal with an array of attack types and actors
- Perform further target assessments on this, determine ways to creatively bypass these defences, whilst continuing to emulate attackers and their TTPs
- Remain vigilant and ensure we are emulating real threats

context

End results? Defensive advantages

- Can allow the SOC to maximise their training and experience with internal tools for specific types of attacks
- Allows them to maintain/develop skillsets and remain at the forefront of latest attacker TTPs
- Rather than buying in more capability, we are encouraging more effective and intelligent use of current defences according to the type and state of an attack
- Also beneficial to us as a red team testers – Improves ability

Questions?



End