SAMA spotlight | **Ethical red teaming**

Kingdom of Saudi Arabia | 15 December 2022

The protection of critical infrastructure is increasingly seen as a high national cyber security priority globally. Ethical red teaming - assessing the security capability of an organisation and its information system(s) by using threat intelligence to attack live production environments and trying to compromise organisational missions and/or business processes without exposing sensitive information – is seen by SAMA as a critical factor in ensuring its licensees are as resilient as possible in the face of increasing cyber risks. SAMA's red teaming framework applies to all its licensees, with D-SIBs required to undergo testing at least once every three years.

What happens in a 'red team' attack?

Certified, experienced ethical hackers with in-depth infosec knowledge use the latest attack tactics, techniques and procedures (TTPs) to try to reach an organisation's most important and valuable information assets while testing the organisation's detection and response capabilities.

Why has SAMA released an ethical red teaming framework?

- To govern red teaming activities and ensure red teaming is controlled
- To enhance the knowledge, awareness and capabilities of relevant stakeholders
- To support the sharing of threat intelligence, contributing to the cyber resilience of Saudi Arabia's financial sector

Who else is involved in a red team attack?

As well as the red team, other actors include:

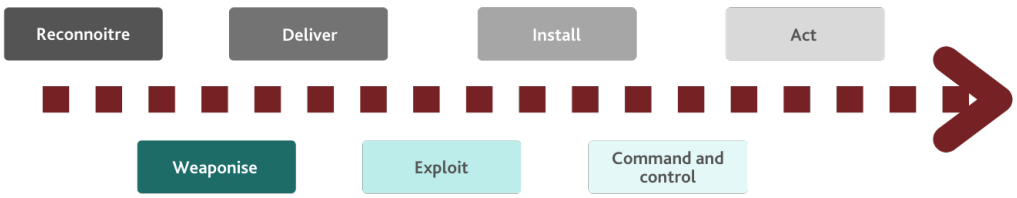
- **Green team** – provided by IT risk experts from SAMA - approves the selection of the red team and provides threat intelligence as appropriate
- **White team** – security and business experts from the FI being 'attacked' responsible for the controlled execution of the red teaming exercise – limited to a maximum of five to maintain confidentiality
- **Blue team** – the FI's cyber security monitoring team (often the SOC) charged with detecting the red team's malicious activities and following agreed incident response procedures

Is red teaming the same as penetration testing?

No. While penetration testing is often limited to testing the security of a specific application or system, red teams test an organisation's overall cyber resilience by testing cyber security controls as well as detection and response capabilities.

How do red teams operate?

While blue teams - interal cyber monitoring teams - try to prevent and detect attacks, red teams tend to follow the classic cyber kill chain methodology:



Contact us:

Srikant Ranganathan
Senior Director
srikant.ranganathan@keypoint.com
+966 50 063 8273

Tom Gilbert
Director
tom.gilbert@keypoint.com
+966 53 250 9866

Sagar Rao
Manager | IT Consulting
sagar.rao@keypoint.com
+966 55 739 6033

Muhammad Nauman Chisty
Assistant Manager | IT Consulting
nauman.chisty@keypoint.com
+966 55 904 8227