Purple Teaming

Contents

3 LRQA’s purple teaming service

5 Why you need purple teaming

6 How do we make purple teaming, scalable, measurable and repeatable?

7 Why LRQA?

LRQA’s purple teaming service

What is purple teaming?

Purple teaming is a collaborative exercise between the Red (Offensive security) and Blue (Defensive security) teams to assess how the people, processes, and technology of an organisation would fair against real-world cyber-attacks.

Purple teaming is unique in that it allows both teams to collaboratively work together to identify gaps in the visibility, detection, and response capabilities of an organisation through various exercises, playbook reviews, and table-top workshops.

This allows an open forum between the teams for discussion, learning, and troubleshooting while working towards a common goal of improving the cybersecurity maturity of the organisation.

LRQA's purple teaming service

LRQA's services focus on strengthening the cybersecurity maturity of organisations by developing and honing protective and detective capabilities. We do this by emulating the tactics, techniques, and procedures (TTPs) associated with real-world threat actors – in alignment with the MITRE ATT&CK matrix.

LRQA's red team and Security Operations Centre (SOC) offerings continually work with and help clients to detect, respond, and deal with real-world attacks. This exposure provides our consultants with first-hand insight and experience of what offensive and defensive positions are needed, to not only prevent an attack but limit its impact allowing for a successful response and cost-effective quick recovery. All consultants are versed in industry-recognised standards and hold the highest level of certifications from both offensive and defensive practices.

Our purple teaming offering is enhanced not only through the use of experienced red team who are capable of simulating real-world threats, but can be further augmented by Breach and Attack Simulation (BAS) technology to improve consistency and to automate and repeat TTPs emulation at scale. This allows for additional time with security teams to understand the key elements of a cyber-attack.

If your organisation is ready to invest and empower security for the betterment and well-being of the company then it is likely you are ready to begin thinking about Purple Team exercises.

Ideally, your organisation will at least have some level of security tooling, team, and capability to build on. If you currently do not have an existing security framework or team, you can still get value, allowing you to determine where your gaps are, and the work required to put together a roadmap to strengthen your cybersecurity – this is why LRQA offers a tiered model for purple teaming:

TTP coverage assessment

- **Summary:** Standardised and scalable assessment covering a wide range of TTPs on a small number of hosts. This assessment aims to identify detection gaps within the current detection stack on endpoints and servers.
- **Target:** Organisations that require their detection capability reviewed to ensure that they have full coverage across the range of TTPs used by attackers.

Collaborative red team

- **Summary:** Simulated attack against the organisation with the red team aiding the blue team with threat hunting. This provides a great opportunity for the blue team to see a live attack against the organisation and to contextual their detection capability. The red team collaboration provides great value in threat hunting and understanding the indicators of compromise that the various attacks left behind.
- **Target:** Organisations with an in-house capability to conduct detection and response with an already existing baseline for TTP coverage that are looking to test their capability and increase threat-hunting knowledge in a guided fashion.

Attack chain discovery

- **Summary:** A variety of tabletop and simulated attack exercises to find as many attack chains within the environment to a given target. The aim of this engagement is to challenge preventative assumptions and to assess the risk to the organisation as a whole. Whilst this does provide an opportunity for the blue team to observe various attack chains within the environment, the focus of the simulated attacks would be validating attack paths rather than bypassing detection stacks.
- **Target:** Organisations that want to assess their risk to the organisation as a whole and test assumptions around preventative controls.

Why you need purple teaming

Purple teaming is distinct from other testing methods, instead of attacking an organisation and delivering post-test results, purple teaming executes known TTPs to test whether your defensive controls are effective and your policies and processes back up those controls.

LRQA's testing team then coordinates with the blue team to see whether their actions were prevented, detected, or visible but with no alerts.

Purple teaming facilitates active real-time simulation and enhancement, through this circular approach - testing assumptions and utilising the methods threat actors would use in an actual attack.

Purple teaming will benefit your organisation by:

1. Minimising your security teams from being blind to an attacker in your network by training your defensive teams to understand the latest threats being used in the wild.

2. Validating your defensive assumptions and assessing your existing capabilities using industry-recognised metrics to prove what is and is not detected.

3. Discovering the threshold of detection. This provides an indication as to the level of technical complexity that would be required by a threat actor in an attempt to avoid detection by defenders.

How do we make purple teaming, scalable, measurable and repeatable?

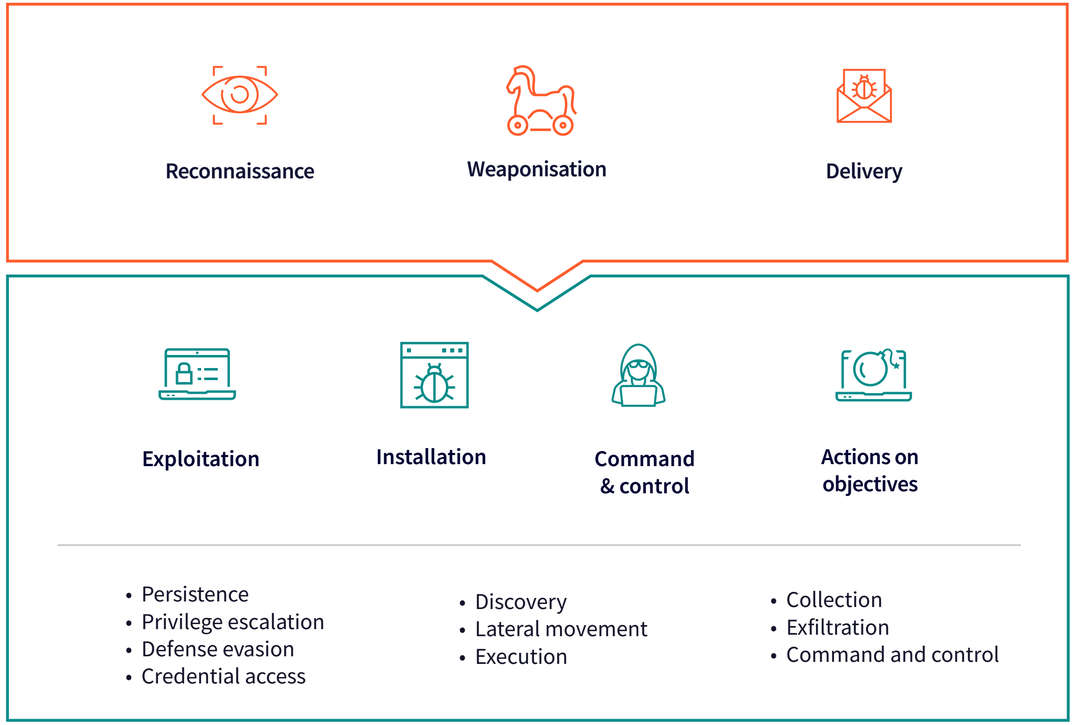
To deliver a tailored and unique purple team exercise that is, scalable, measurable and repeatable for your organisation, LRQA leverages the MITRE ATT&CK framework, knowledge of known threat actors, and breach and attack simulation technology. This allows both red and blue teams to track and correlate activity and effectiveness by developing a TTP map detailing your coverage and gaps.

This approach strengthens the blue team, as they become more informed about how to prioritise, measure, and improve their ability to detect threats and attacks.

LRQA also blends the cyber kill chain with the MITRE ATT&CK pillars, enabling our service to be focused on critical areas of visibility and detection for your organisation.

LRQA's purple team service lays the foundation by providing deep knowledge and reporting on each pillar, assisting your organisation in finding the gaps that are often overlooked.

Conducting purple teaming to identify vulnerabilities is essential to your organisation's security.



Why LRQA?

Regardless of the size of your organisation, purple teaming is one of the most effective ways to strengthen your cybersecurity maturity, driving an uplift in protect and detect capabilities.

LRQA's purple teaming service is available for all sizes of organisation, in a format most applicable to your needs.

Our approach and service are fully tailorable, enabling the emulation of all threat actor sophistication levels and known TTPs. Our red team add a diverse perspective on attacker techniques and mindset to drive security best practice and avoid thematic pitfalls that leave an organisation vulnerable.

Not only do we possess a rare mix of offensive and defensive technical knowledge but we also understand the business impact and risk, with a focus on people, process, and technology.

This enables you to strengthen your cybersecurity maturity and confidentially answer the question "How secure are we?"

About LRQA:

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **www.lrqa.com** for more information or email **cybersolutions@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom