Purple Team Assessment

Evaluate risk, improve defensive capability

What is Purple Teaming?

RED TEAMING
are ethical hackers delivering attack simulations to establish the risks of likely attack methods.

BLUE TEAMING
are the organisation's defensive team whose objective is to detect and protect against attacks.

PURPLE TEAMING
brings both teams together in a joint exercise which simulates and analyses active attack scenarios based on pre-defined goals. Purple Team Assessments can be applied to the whole organisation, internal assets, the perimeter, and cloud environments..

How your organisation can benefit from Claranet's Purple Team Assessment

Effective Purple Team Assessments allow you to simultaneously evaluate the effectiveness of your defences whilst improving your team's capability to defend against real-world attack scenarios.

Throughout a Claranet Purple Team assessment, our experienced Red Team works closely with your defensive (Blue) teams to provide continuous feedback and knowledge transfer. Facing real-world attack scenarios, informed by threat intelligence, with the support and guidance of the ethical hacking team, we will help to develop the skills needed by your defensive team to detect attacks, proactively hunt for threats and monitor attack surfaces for suspicious behaviour.

Repeated cycle of activity which forms Purple Team assessment	
Threat Assessment	OSINT and threat analysis used to create attack plan to be deployed throughout the assessment, including custom tactics & techniques.
Tabletop Preview Session	Presentation of the Tactics, Techniques & Procedures (TTPs) to be simulated and discussion between Red and Blue Teams of expected outcomes based on existing capabilities.
Observed Attack Simulation	Blue Team members observe and participate in attack simulations.
Detect & Respond Activity	Blue Team follows existing processes to detect & respond to TTPs.
Tabletop Review Session	Guided discussion to review the exercise, understand effective remediation, improvement of existing capabilities and how to address any gaps in detection & response capability.

Key Features

- Bespoke service tailored to your organisation
- Guided discussions & knowledge transfer
- Close collaboration between Red and Blue Teams
- Comprehensive report with executive summary
- Attack scenario details & lessons learned
- Analysis of attacks undetected by Blue Team
- Clear recommendations
- Attack execution log with instructions to recreate exercises

Core Benefits

- Test, assess & improve your ability to detect & prevent successful cyber attacks
- Improve and refine the effectiveness of existing security solutions and processes
- Understand where security gaps exist and use the insight to inform buying decisions and security strategy
- Develop an attacker mindset within your defensive teams to better recognize and respond to suspicious activity

How we work with you

We provide a tailored approach based around your objectives, the size and capabilities of your defensive team and the type and sophistication of the attack simulations required. For example, some Purple Team Assessments require extensive knowledge transfer and collaboration throughout attack simulations, whilst others are based on a stealthy, realistic simulated attack delivery with subsequent review and debrief.

This bespoke approach ensures that our customers receive the right level of support to deliver insight and outcomes that improve the organisation's ability to defend against cyber attacks.

Our objective is to provide the threat visibility needed for you to make effective changes to security processes, deploy appropriately configured defensive technology and train key staff in a way that will make the job of an attacker more difficult and reduce the chances of a security breach.

Why Claranet Cyber Security

Claranet Cyber Security is the global cybersecurity services division within Claranet, bringing together 1,500 technical experts and 75 pentesters under a 25+ year legacy that includes work with FTSE250 Fortune 500 global customers.

We are a founding member of CREST and a leader in ISG's Provider Lens™ for both "Cybersecurity – Solutions & Services" and "Public Cloud – Solutions and Services" (2021). We are also a leading training provider at Black Hat across the world, as well as Check Point, Nano, Rapid7, and QA.

One of only a few MSPs to achieve the highest partner accreditation status with Microsoft, AWS, and Google, Claranet is recognised as a leader in Gartner's Magic Quadrant and a market leader in cybersecurity.

claranet cyber security