Purple Teaming simplified: Enhancing cyber Security collaboratively

What is Purple teaming?

Purple Teaming involves cooperative assessments of an organisation's security controls by both offensive "Red Team" attackers and defensive "Blue Team" defenders. This collaborative engagement simulates realistic attack scenarios to identify vulnerabilities and assess an organisation's ability to prevent, detect, and respond to real world cyber security threats.

Key aspects:

Red Team (attackers): The Red Team, which comprises of highly skilled security professionals, adopt the mindset and tactics of a malicious adversary. Using advanced techniques, such as social engineering and vulnerability exploitation, the team will identify and exploit vulnerabilities and gaps in the security controls of an organisation.

Blue Team (defenders): The Blue Team is responsible for detecting, responding to, and defending the organisation against the attacks deployed by the Red Team. Using advanced monitoring capabilities and incident response procedures, the Blue Team works to effectively identify, analyse, and mitigate any threats or vulnerabilities in real time.

Close collaboration: Unlike traditional Red Team engagements, Purple Teaming encourages open communication between the Red and Blue teams, fostering knowledge sharing to enhance defensive strategies. By spanning the entirety of the cyber kill chain, a Purple Teaming exercise transcends limited penetration tests and vulnerability assessments, delivering a holistic evaluation of an organisation's prevention, detection and response capabilities.

Purple Teaming Assessments:

Phase 1 – Preparation and scoping:

- Establish clear objectives and rules of engagement for the exercise.
- Identify the critical assets, systems, and processes to be evaluated.
- Define the scope and timeline for the purple teaming activities.

Phase 2 - Red Team assessment + Blue Team response:

- The Red Team conducts a thorough assessment of the organisation's security controls and defences.
- The Red Team uses advances techniques to uncover exploitable weaknesses, gaining unauthorised access into assets defined within the scope.
- The Blue Team, responsible for defending the organisation, monitors and responds to attacks from the Red Team.
- The Blue Team evaluates their ability to detect, analyse and respond to threats identified by the Red Team.
- Continuous feedback and collaboration between the Red and Blue Teams occur during this phase.

Phase 3 – Findings and recommendations

- The Red Team and Blue Team review the findings of the assessment and identify areas for improvement and discuss remediation steps.
- The Red Team produces a comprehensive report, outlining the vulnerabilities discovered, the effectiveness of security controls and the recommended remedial actions.

Levels of service offerings:

Bronze Level: Pre-defined list of commonly used Tactics, Techniques, and Procedures (TTPs).

Silver Level: TTPs defined using threat intelligence relevant to the organisation's industry.

Gold Level: TTPs defined using threat intelligence, aligned with the Mitre Att&ck Framework, and further customised to evade specific security controls.

Differences in service offerings:

All levels use the Mitre Att&ck Framework but with varying degrees of customisation.

Gold level includes further customisation to bypass security controls, akin to Advanced Persistent Threats (APTs).

Output:

Comprehensive report and optional presentation aligned with the Mitre Att&ck Framework.

Findings and recommendations communicated effectively to both technical and non-technical staff.

Team collaboration:

Red Team implements TTPs, creates the report, and manages the engagement.

Advanced Threat Intelligence (ATI) team assists in discovering relevant TTPs.

Collaboration between Red and Blue Teams ensures real-world, achievable remediations for undetected TTPs.

How can this service benefit your organisation?

This collaborative red team/blue team exercise yields several crucial benefits:

- Emulation of genuine threats: Rather than theoretical scenarios, your defences face the genuine tactics, techniques and procedures leveraged by sophisticated threat actors targeting organisations like yours.
- Learning and experience: Your analysts gain first-hand experience detecting and responding to live adversary actions, with immediate feedback to reinforce lessons learned.
- Validation of existing defences: Determine the true efficacy of your current security posture by witnessing how it holds up against a concerted, real-world campaign orchestrated by our red team.
- Identification of blind spots: Uncover vulnerabilities or gaps in your people, processes and technologies that could potentially be exploited by genuine adversaries before they are able to leverage them.

For further insights on the benefits tailored to your organisation, please reach out to our cyber security team.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit: cgi.com/uk/cyber-security

Email: cyber.enquiry.uk@cgi.com