# Purple Team

CrossCountry
CONSULTING

In a purple team assessment, the CrossCountry team works hand-in-hand with the client's blue team to improve their detection and response to popular adversary techniques, tactics, and procedures. The scope of the purple team can be adjusted to client needs and can include scenarios that involve perimeter breach and/ or social engineering, insider threats, and advanced persistence, as well as attacks on key and critical assets.

The goal of a purple team is to help a client improve their detection, response, and containment or eviction procedures by providing defenders with opportunities to practice incident response. Each scenario is developed to employ techniques that are mapped to the Mitre ATT&CK framework, with a focus on techniques frequently used by threat actors that operate against the client's organization. CrossCountry leverages its threat intelligence program to keep abreast of threat actors and emulates their techniques. Instead of focusing on specific vulnerabilities within your organization, purple teams focus on the indicators of compromise that defenders can use to better defeat adversaries.

## KEY DIFFERENTIATORS

Deliverables focus on the information defenders need to enhance their incident response capabilities

Scenarios can include single technique categories (e.g., persistence, lateral movement, etc.) for focused improvement, or cover an entire attack chain

Regular debriefings allow defenders the opportunity to ask questions and learn from the red team

To accommodate a variety of adversaries and skill levels, realistic scenarios are built to facilitate a wide array of experiences.

May include **common techniques**, such as:

- Open-source malware from Empire, Metasploit, or unmodified Cobalt Strike beacons
- "Noisy" reconnaissance, discovery, and credential collection (i.e., password spraying)
- Automated attacks

May include **advanced techniques**, such as:

- Spear phishing with fully functional payloads
- Sophisticated command and control (C2)
- EDR/ AV/ web filtering/ secure email evasion
- Living off the land
- Custom, scenario-specific malware

**Contact Us:** ERIC EAMES, *Advanced Cyber Risk Lead* • eeames@crosscountry-consulting.com