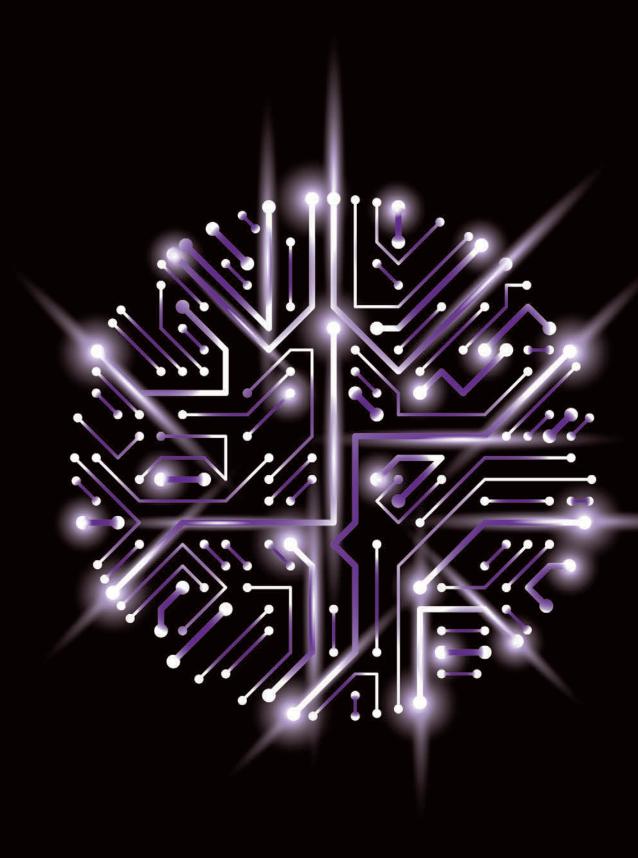
Deloitte.



Cyber Purple Teaming

Improving security through active cyber-defense workshops

Red+Blue=Purple

Combining the strengths of two core IT security defense teams

In a Purple Team assessment, the Red Team attempts to exploit vulnerabilities in a network, while the Blue Team works to detect and mitigate these activities. Purple Team assessments aim to mature the security of organizations while constantly developing the skills and processes of both teams.



Red Team

The aim of the Red Team is to help improve an organization's security, by highlighting the main weaknesses within their Infrastructure.



Purple Team

A Purple Team assessment combines the remedial efforts of a Blue Team with the weaknesses and vulnerabilities exposed by a Red Team.



Blue Team

The Blue Team's role is to detect and response to any Red Team activity. In the case of a Purple Team assessment the Blue Team would consist of your SOC team, supported by Deloitte personnel.

Purple Teaming – Two delivery models



Executive workshops

An executive level exercise that enhances traditional "table-top" and "paper-based" exercises using real threats and attacks created by a red team.

- Purple Team Executive Workshops are delivered at the executive level within your organization.
- Cyber Incident Response workshops have traditionally been delivered as "paper exercises", however Deloitte's Purple Team Executive Workshops involve a Red Team who will be conducting attacks and seeking to move across the organization's network in real-time.
- The workshop will be directed by a Deloitte facilitator, who will advise attendees that the network has been infiltrated using rogue devices.
- Workshop attendees will be tasked with directing the SOC (the Blue Team) to detect the rogue devices and respond to Red Team activity throughout the day.
- Prompts and updates will be provided by the facilitator and a representative from the Red Team. The Blue Team will be challenged to respond to a realistic attack scenario in real-time.



Hands-on workshops

A combined technical level exercise that takes advantage of the threats identified by a red team with the response activities of the blue team, in real-time.

Ö

- Purple Team Hands-on Workshops are delivered directly with the monitoring and defensive teams within your organization.
- Most organizations nowadays leverage teams of simulated attackers (red team) and defenders (blue team) to test assumptions about the state of their IT security.
- Purple team Hands-on Workshops effectively combine these two separate efforts into an integrated approach that allows for rapid and real-time identification of issues as well as remediation.
- During the workshop the defensive team will need to defend in real-time from attacks generated by the red team based on applicable use cases and targeted threat intelligence scenarios.
- Deloitte facilitators will be placed in the Blue Team and at the same time representatives from the Blue Team will be part of the Deloitte Red Team for learning and knowledge transfer.

Purple Teaming – Executive Workshops



Setup

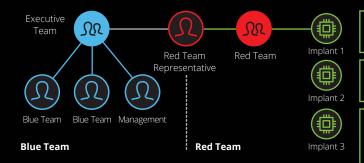
Prior to the workshop members of the Red Team will implant three malicious rogue devices onto the network, at locations in the client offices (these locations will be agreed with you in advance, and Deloitte will be supervised by an on-site contact).

Workshop

- Introduction of key concepts (e.g. Red Team and Blue Team), and an explanation of what the workshop involves.
- **2.** Identification of the three rogue devices, with an increasing level of difficulty.
- 3. Workshop close

Debrief

A full debrief will be conducted, covering what was detected by the Blue Team, what was not detected and areas in which the organisation could improve.



Connects back to Deloitte C2 server via DNS beaconing, allowing the Red Team to start browsing the network.

Connects to C2 server via 4G. Red Team browse the network and access files (targets agreed ahead of time).

Connects out using 4G. Performs completely passive enumerations activities. Device name mimics legitimate naming conventions on the network.

Purple Teaming – Hands-on Workshops



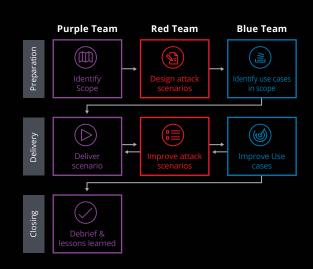
Tailored approach

Although the overall process for purple teaming will follow a formal pattern, overall delivery is fully customisable. Options range from a small-scale focused approach to a full scale actual attack simulation. Apart from various execution methods, we can also change the scope from broad to focused, to a single link in the cyber kill chain. By performing a threat assessment workshop before we start, we ensure that any and all simulated attacks are in line with your organizations' actual threat landscape.



Scoped sprints

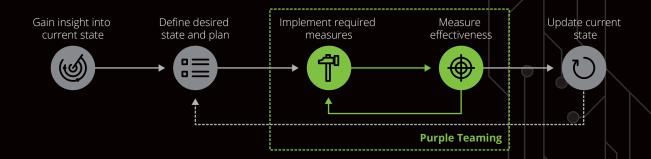
Our purple teaming approach is modeled in clearly defined sprints. In each sprint, scenarios are designed, corresponding SOC use cases identified, the simulation is executed and improvements identified in a loop.



Using Purple Teaming as part of security transformations

A measure of effectiveness

Purple teaming is a perfect tool to measure progress during multi-year security transformation projects. By leveraging regular purple teaming engagements, recently implemented measures can be tested for effectiveness in a very targeted way. A change in threat landscape will automatically be covered as well, since any purple team engagement will use up-to-date threat intelligence and knowledge about the current threats to the organization.



Deloitte.

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Japan member firm of Deloitte Touche Tohmatsu Limited (DTTL), a UK private company limited by guarantee, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Corporate Solutions LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With about 11,000 professionals in nearly 40 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/-jp/en.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Member of **Deloitte Touche Tohmatsu Limited**

