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.

Gain insight into current state
Define desired state and plan
Implement required measures
Measure effectiveness
Update current state

Cyber Purple Teaming
Improving security through active cyber-defense workshops
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 respond 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.

- 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
1. 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.

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 organisation’s 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.

Purple Team Red Team Blue Team

Preparation Identify Scope Design attack scenarios Identify use cases in scope

Delivery Deliver scenario Improve attack scenarios Improve Use cases

Closing Debrief & lessons learned

Focused simulation
Tightly scoped exercise, covering a specific link of the kill chain, testing defenses relevant to this part.

Full simulation
Simulated realistic attack that is carried out in entirety, testing all defenses along the attack vector. Covers a wide range of topics and systems.
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.