Cyber Polygon
Training description

Targeted attacks are among the key cybersecurity threats. Their number is growing dramatically on a global scale. The goal of most these attacks is to steal confidential data. Therefore, in 2020 the World Economic Forum puts data theft in the top-10 of the most likely global risks.

Cyber Polygon 2020 will help IT and cybersecurity specialists to prepare for real digital challenges.

Training results will be analysed in a comprehensive report and presented at the World Economic Forum Annual Meeting on Cybersecurity in November.

During the online training participants will exercise the actions of the response team in a targeted attack aimed at stealing confidential data and thus resulting in damage to the company reputation.

Training structure

The training will include two scenarios.

Scenario 1. Defence

Participants will repel an active APT cyberattack.

Scenario 2. Response

Teams will investigate the incident using classic forensics and threat hunting techniques. Based on the information gathered, participants will compose a dossier that would help law enforcement agencies to locate the criminals.

Roles

Red Team

Training organisers from BI.ZONE will simulate cyberattacks.

Blue Team

Participating teams will protect their segments of the training infrastructure.

Conditions of participation

- Training participation is open strictly to organisations (therefore, use your corporate email to apply).
- One organisation — one team. Number of specialists in a team is not limited.
- All tasks can be performed remotely: teams will be provided with access to a virtual cloud infrastructure.
- Participants can use any applications and tools to protect their training infrastructure segment.
- The point of the exercise is education not competition, so the training results will be anonymous.

How to participate

1. Send your request to cyberpolygon@bi.zone.
2. Await confirmation.
3. Stay tuned and follow the updates on www.cyberpolygon.com.
4. July 8, 2020 at the appointed time, login to your account on the website and complete as many tasks as possible until the end of the training.

Scenario 1. Defence

Legend

The organisation's virtual infrastructure includes a service which processes confidential client information.

This service becomes the subject of interest to an APT group. Cybercriminals are going to steal confidential user data and then resell it on the Darknet in order to receive maximum financial benefit and cause damage to company reputation.

The APT group studied the target system in advance and discovered a number of critical vulnerabilities there. The gang plans to attack on the day of the exercise.

Objective

Develop skills of repelling targeted cyberattacks on a business-critical system.

Blue team actions

Participants will have to:

- cope with the attack as fast as possible;
- minimise the amount of information stolen;
- maintain service availability.

Blue Team can apply any applications and tools to protect the infrastructure. They can also fix system vulnerabilities by improving the service code.

Scenario 2. Response

Legend

This scenario involves the investigation of two identical incidents which differ in their indicators of compromise and the data available for analysis.

First round

One of the perimeter defence solutions detected a request to the command and control centre associated with the APT group. The information about the group was obtained through the threat data exchange platform.

Blue Team will receive data from a compromised host (memory dump, event logs, Windows registry hives export, etc.). Participants will have 2 ways of getting this information:

- download in advance using the link in participant's account (the password for the encrypted archive will be issued at the start of the event);
- use virtual machines in the training infrastructure with loaded data and pre-installed tools for analysis.

Second round

An identical incident (but with altered indicators of compromise) occurred in the organisation which has EDR solution agents pre-installed on the final hosts. These agents continuously collect telemetry from the hosts and send it to the Threat Hunting platform. Inside the platform, the collected telemetry is analysed with the use of detection rules, which reveal potentially anomalous activity. The platform also has a convenient interface for searching historical data.

Blue Team will have access to an individual installation of such a platform, filled with events from the compromised infrastructure hosts.

Objective

Develop skills in incident investigation taking the scenario, where cybercriminals gained access to a privileged account through a successful phishing attack, as an example.

Scenario 2. Response

Blue team actions

In both cases, Blue Team will have to solve a number of tasks, analysing the data provided, but the analysis methods will differ.

First round

Blue Team will investigate the incident using the methods and tools of classical computer forensics.

Second round

Blue Team will investigate the incident using the Threat Hunting approach: the initial step will be to analyse the functions of several detection rules.

At the end of each investigation, participants will practice to compile dossiers with information about the incident for law enforcement agencies.

Calculation of results

Final result of the team is the sum of points earned in two scenarios. Each scenario has its own method of scoring.

Scenario 1.

Points are awarded for two indicators: SLA and HP.

SLA (Service Level Agreement) indicates the integrity and accessibility of a service. It is measured as a percentage.

A checker will contact participants' services. SLA value is calculated as the percentage of successful checks (when the service is available and fully functional) to the total number of checks.

HP (Health Points) indicates the presence of vulnerabilities in the service and the ability to withstand attacks. It is scored as a simple numerical value.

Before the start of the scenario, each participant will receive the same amount of HP and the access to the training infrastructure with the same vulnerabilities.

Each time the Red Team successfully exploits a vulnerability in the team's service, the team will lose HP. The faster the team fixes the vulnerabilities in the service, the less HP it will lose by the end of the scenario.

Final result is calculated as SLA × HP.

Scenario 2.

The number of points awarded for the answer depends on the complexity of the task.

Each task has several hints available. Using these hints will reduce the number of points for the answer. The last hint gives the correct answer, but using it the team will receive zero points for the task.