Cyber Polygon 2021

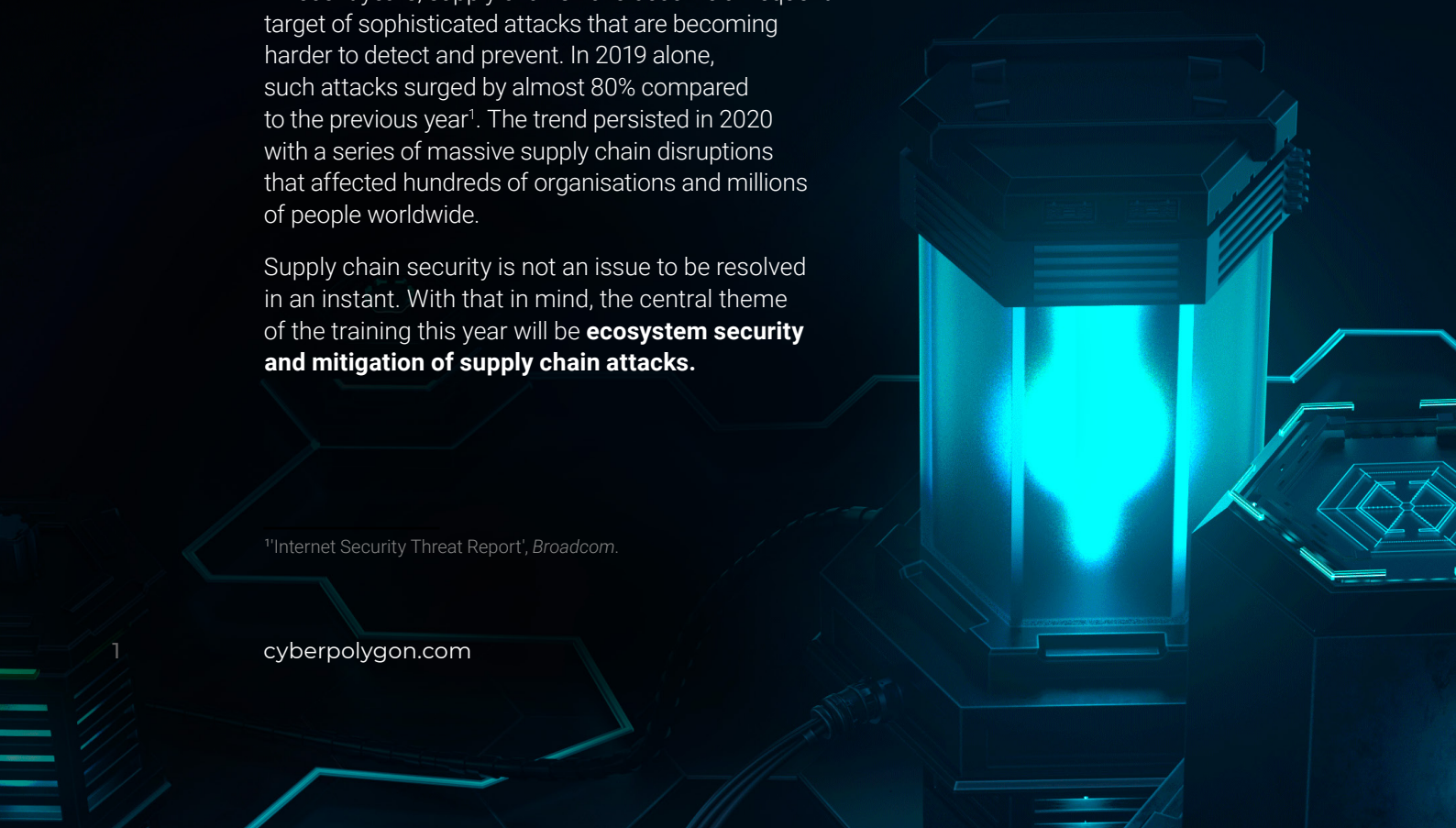
Training Description

Today, we see myriads of digital ecosystems emerge all around us. They are created by countries, large corporations and even small businesses for the purpose of streamlining their operations. These involve a large number of interactions, both external and internal, with all the parties being closely interconnected. In this context, the vulnerability of supply chains has become a growing concern: **an attack on a single company can jeopardise the entire ecosystem.**

In recent years, supply chains have become a frequent target of sophisticated attacks that are becoming harder to detect and prevent. In 2019 alone, such attacks surged by almost 80% compared to the previous year[1]. The trend persisted in 2020 with a series of massive supply chain disruptions that affected hundreds of organisations and millions of people worldwide.

Supply chain security is not an issue to be resolved in an instant. With that in mind, the central theme of the training this year will be **ecosystem security and mitigation of supply chain attacks.**

The participants will train their skills in repelling a targeted supply chain attack on a corporate ecosystem



[1] 'Internet Security Threat Report', *Broadcom*.

Format

Last year, the teams practised response actions at the moment of a targeted attack and investigated the incident. Such format proved effective, enabling the teams to improve their practical skills.

We decided to retain the same format, with just a few changes to accommodate the wishes of the teams.

The training will include two scenarios.

Defence

The participants will deflect an active attack on a corporate system responsible for assembling, testing and delivering applications. The system manages the entire lifecycle of the organisation's business-critical service.

Response

The teams will investigate the incident, which started with a subsidiary's host being compromised. The host communicates with the client's network via VPN. Same as last year, the participants will apply classic forensics and Threat Hunting techniques.

Roles

Red Team

Training organisers from BI.ZONE, simulate the attack.

Blue Team

Participating teams, protect their segments of the training infrastructure.

Terms of Participation

1. Only organisations may participate (please use your corporate email to apply).

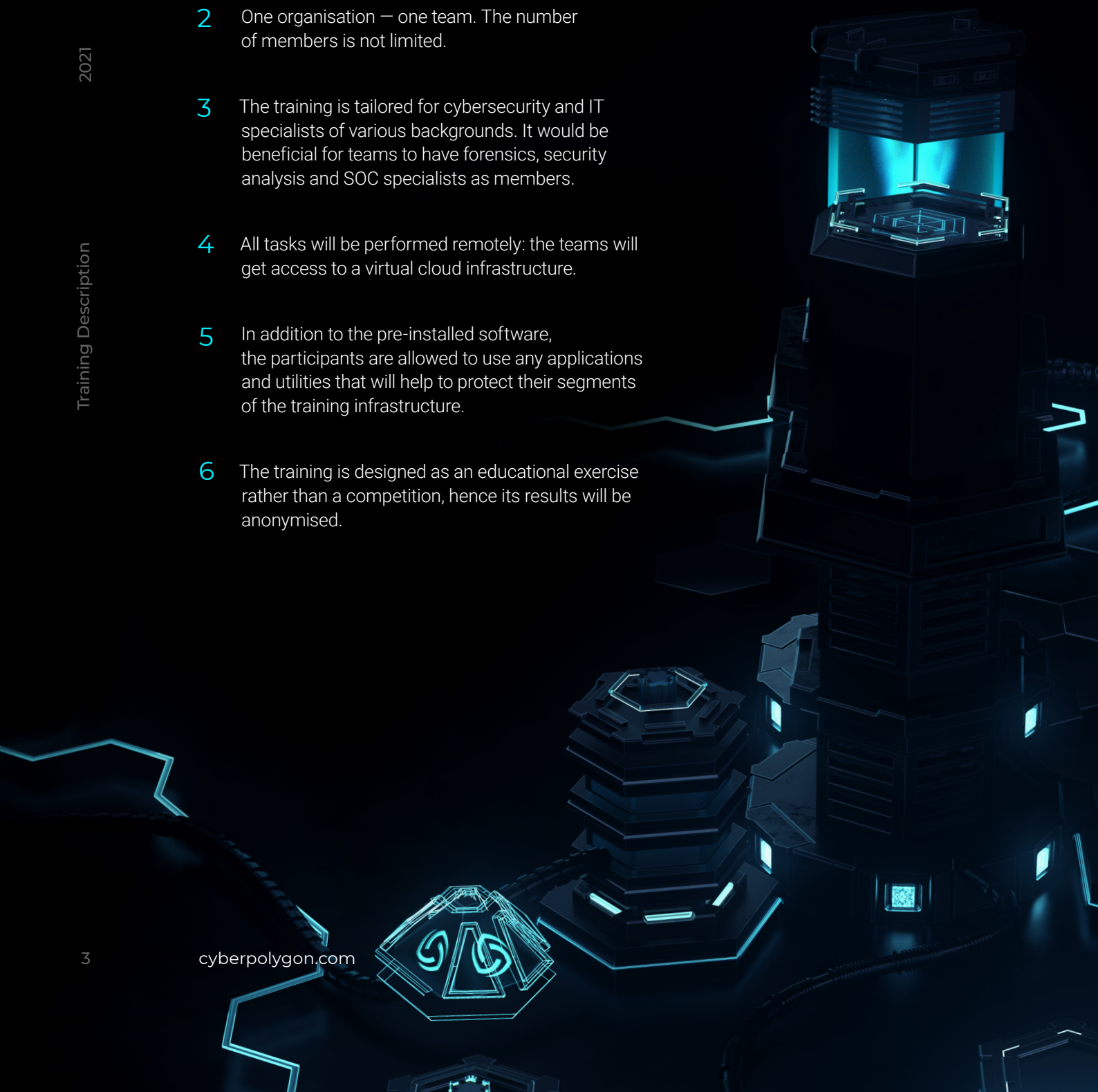
2. One organisation — one team. The number of members is not limited.

3. The training is tailored for cybersecurity and IT specialists of various backgrounds. It would be beneficial for teams to have forensics, security analysis and SOC specialists as members.

4. All tasks will be performed remotely: the teams will get access to a virtual cloud infrastructure.

5. In addition to the pre-installed software, the participants are allowed to use any applications and utilities that will help to protect their segments of the training infrastructure.

6. The training is designed as an educational exercise rather than a competition, hence its results will be anonymised.



Scenario 1. Defence

Legend

During an attack, an unknown hacker group could gain network access to a segment of the virtual corporate infrastructure. This segment contains services responsible for the continuous integration and deployment of the company's web application.

The threat actors could not gain access to the virtual servers but stole large amounts of information about the application being developed, including parts of the source code and development documentation.

The group's main target is the user data processed by the application. To this end, the attackers are planning to use the stolen information to tamper with the development process and embed backdoors into the application. The group would then be able to proceed to the final stage: attack the application in the production environment and take possession of the desired data.

Objective

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

Blue Team Actions

The participants will have to:

- contain the attack as fast as possible
- ensure the security of the application's supply chain
- minimise the amount of compromised information
- maintain the availability of the target web application and the entire supply chain

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

Scenario 2. Response

Legend

The Blue Team protects the ecosystem of a large group of companies. One of the workstation users at the parent company reports suspicious files in a directory. The investigation identifies the vector of compromise, specifically, the update installed on a business-critical application being developed by a subsidiary.

The Blue Team will be granted access to the parent company's Threat Hunting platform, which aggregates EDR and NTA events. The participants will be tasked to find as many artifacts of the incident as possible by applying the Threat Hunting approach.

Further, the team discovers that the infrastructure has been compromised through a modified update installed on a business-critical application. The update was provided by a subsidiary structure in charge of software development. Therefore, the focus of the investigation will switch to the subsidiary's infrastructure.

The subordinate organisation does not use any EDR solution. For this reason, the participants will have to resort to classic forensics and find as many artifacts of the breach as possible.

Objective

Develop skills in incident investigation based on a successful phishing attack.

Blue Team Actions

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

Parent company

The participants will investigate the incident by applying the Threat Hunting approach, gathering telemetry from the hosts and network server.

Subsidiary

The Blue Team will investigate the incident using the methods and tools of classic digital forensics.