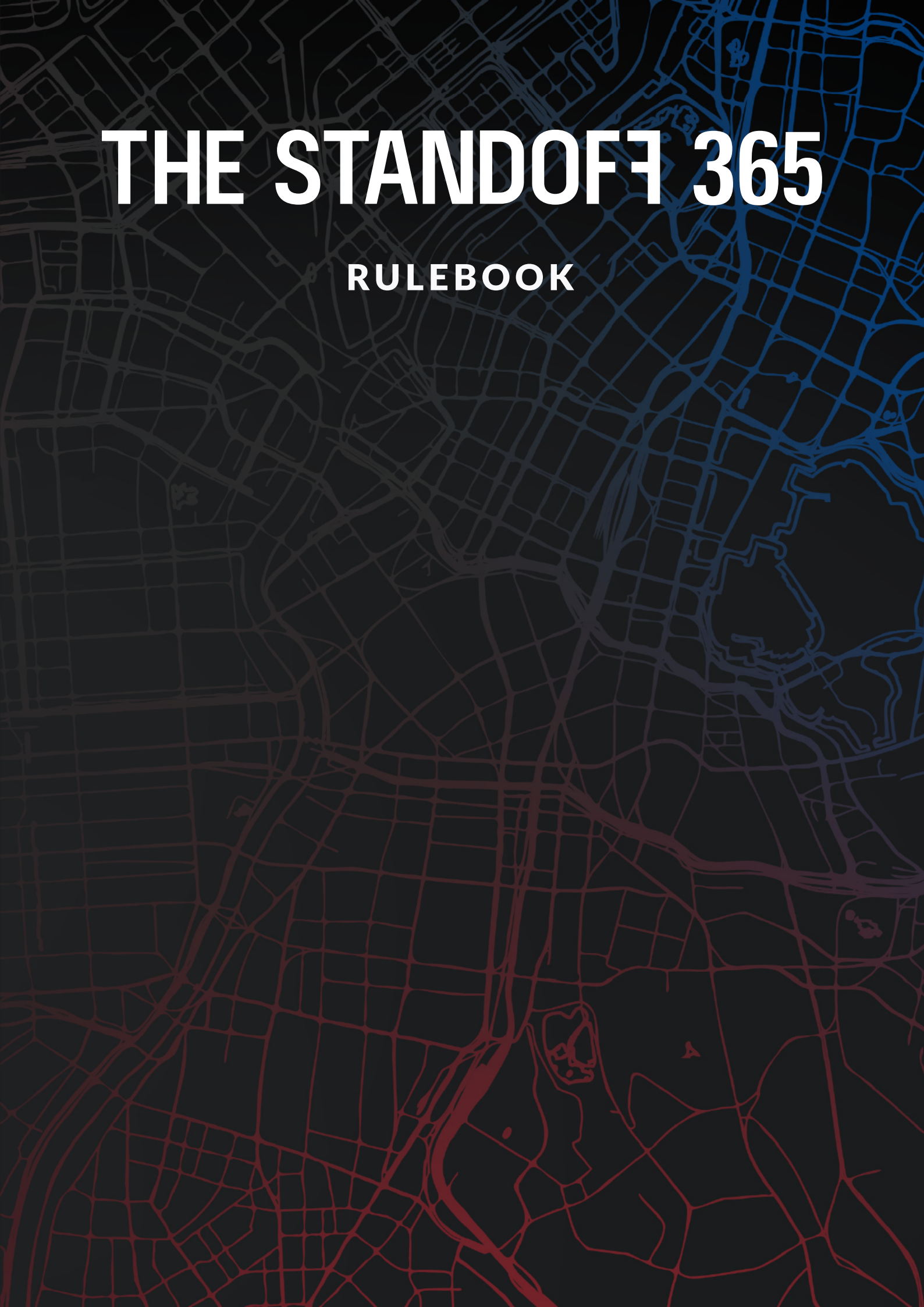
THE STANDOFF 365

RULEBOOK



Contents

1. About The Standoff 365

The Standoff 365 is a social platform for communicating and sharing experiences, a cyberrange for conducting cyberexercises, and a space for testing and assessing the security of systems and equipment. The underlying technology of the platform ensures quick deployment of and access to the IT communications infrastructure, while also allowing for connection of external devices and equipment to the infrastructure.

Cyberexercises that are held at the platform allow for the analysis of attacks against information infrastructure and applications. Cyberrange segments are deployed at the platform. Each of the segments is designed to re-create information systems and processes that are typical of enterprises from a particular industry (for example, banks and electricity and IT companies). Each industry can include one or more services responsible for activity or security at a given organization. Such services might include a mail server, FTP server, client database, document management system, firewall, traffic light management system, wind generators, electricity meters, and electrical substations.

Each participating attacker acts independently of all other participants. The goal of the attacker is to disrupt the functioning of the provided information systems by triggering unacceptable events and exploiting vulnerabilities. The participant receives points for completion of tasks.

Information about the current state of the cyberexercise, ranking of the participants, and tasks are available at The Standoff 365 platform.

2. Rules for attackers

This section describes how cyberexercise participants get started, connect to the cyberrange, and compete.

In this section

2.1. Preparing

To take part in cyberexercises, a user must register at standoff365.com and then go to online.standoff365.com where cyberrange segments are deployed.

2.2. Connecting

To access the cyberrange, the participant must go to the **Access and resources** tab at The Standoff 365 platform and follow the instructions under **VPN connection**.

2.3. During the exercise

During the cyberexercise, attackers attempt to find vulnerabilities and trigger unacceptable events by accomplishing tasks proposed by the organizers. Points are scored for successful attempts.

Attackers may target only services located at addresses provided by the organizers. Any attacks on addresses outside of that range will not be scored. Services located outside the infrastructure provided by the organizers are not included in the scope of the cyberrange and participants are prohibited from attacking them.

> Warning. The organizers can suspend a participant from cyberexercise for using service accounts or attempting to gain access to them.
>
> Warning. Attacks on addresses not in the provided list may result in removal of the participant from the exercise. Moreover, participants are prohibited from conducting DoS and DDoS attacks on the services and applications of the cyberrange infrastructure. Participants performing such attacks may be removed from the exercise.

Points can be earned in the following ways:

- **By triggering unacceptable events.** Tasks can involve obtaining confidential information, disabling one or more services, or changing information on a test website.
- **By finding vulnerabilities.** A participant can report vulnerabilities in the infrastructure.

2.4. Tasks

Tasks are intended to be realistic. The task description, along with the payoff (in points), is provided in the card of each vulnerability or unacceptable event.

2.5. Task scoring

Points are scored for completed tasks automatically. Participants are ranked by points.

> Warning. The organizers have the right to disqualify a participant if they try to pass off another participant's report as their own.

In this section

Points for triggered unacceptable events (see Section 2.5.1)

Points for vulnerabilities (see Section 2.5.2)

2.5.1. Points for triggered unacceptable events

To receive points for the triggering of an unacceptable event, the participant must submit a report with the correct answer to the task. The answer must contain a set of characters (flag) that the participant is supposed to find in a certain information system. The flag is used to confirm completion of the task.

The flag is checked automatically when the participant attempts to submit the report. If the report contains a wrong flag, the participant will be notified of that and will not be able to submit the report. After finding another flag, the participant can try to submit the report again.

2.5.2. Points for vulnerabilities

To receive points for a discovered vulnerability, the participant must submit a report that specifies the vulnerability type and vulnerable system and provides the correct answer to the task. The answer must contain a set of characters (flag) that the participant is supposed to find in a certain information system. The flag is used to confirm completion of the task.

The flag is checked automatically when the participant attempts to submit the report. If the report contains a wrong flag, the participant will be notified of that and will not be able to submit the report. After finding another flag, the participant can try to submit the report again.

Participants can report vulnerabilities of the following types: Remote Code Execution (RCE), SQL Injection (SQLi), Path Traversal, and Server-Side Request Forgery (SSRF).

Glossary

attack

Attackers' actions that cause an unacceptable event to be triggered. After conducting a successful attack, the red team submits an event triggering report.

attackers

A team or a participant whose objective is to find vulnerabilities and trigger unacceptable events at the cyberrange.

cyberexercise

A set of activities arranged to enhance the competence and skills of information security specialists.

cyberrange segment

A virtual part of the cyberrange infrastructure designed to re-create information systems and processes that are typical of enterprises from a particular industry.

service

An object of the cyberrange infrastructure that controls a certain process in the information system.

task

A description of objectives for attackers to achieve.

The Standoff

Open cyberexercises that take place several times a year and are sometimes timed to coincide with an information security conference.

The Standoff 365

A platform for information security specialists that includes a cyberrange, bug bounty programs, a social network, thematic blogs, and a platform for holding CTF competitions.

The Standoff 365 Cyberrange

A part of The Standoff 365 platform for conducting cyberexercises. It can consist of one or more cyberrange segments. The participants of cyberexercises are divided into two categories: attackers and defenders. The cyberrange provides an opportunity to watch how cyberattacks unfold and assess their impact in a safe environment.

unacceptable event

An event that leads to an organization's inability to achieve its operational and strategic goals or causes long-term disruption of its core activities. At The Standoff 365, the objective of attackers is to trigger unacceptable events, and the objective of defenders is to investigate such cases.

vulnerability

A weakness of a system that can be exploited to violate data accessibility, integrity, and confidentiality.

The Standoff 365 is a cyberrange that allows for the analysis of attacks against information infrastructure. The cyberrange contains full-fidelity replicas of the production chains, business scenarios, and technology landscape typical of different industries.

The Standoff 365 participants have the opportunity to test the feasibility of cyberattacks and assess the scale of their consequences in a safe environment.

org@standoff365.com online.standoff365.com