
STANDOFF
RULEBOOK

Contents

1. About Standoff 365

Standoff 365 is a social platform for communicating and sharing experience, a cyberrange for conducting cyberexercises, and a testing ground for assessing the security of systems and equipment. The underlying technology of the platform ensures quick deployment and access to the information infrastructure and allows external devices and equipment to be connected.

Standoff cyberexercises conducted on the platform enable the analysis of attacks against information infrastructure and applications and provide an opportunity to play out incident response scenarios. The cyberrange is deployed on the platform in segments. Each of the segments simulates information systems and processes that are typical of enterprises from a particular industry (commercial firms, banks, electricity suppliers, telecom operators, and industrial facilities). Each industry can include one or more services responsible for regulating activity or providing security at a given organization. Such services might include a mail server, FTP server, client database, document management system, firewall, traffic light management system, and wind generators.

Participants are grouped into teams with a common goal. At Standoff, there are two types of teams: attackers and defenders. Attackers seek to trigger non-tolerable events by doing things such as bringing SCADA systems to a halt or accessing confidential information. The objective of defenders is to quickly detect and investigate incidents.

Attacker teams receive points for their activities. The actions of defender teams are scored using metrics.

Information about the current state of the cyberexercise, participant results, and tasks are available on the Standoff 365 platform. The organizers provide participants with access to the platform.

2. Rules and instructions for attackers

This section describes how attackers prepare, connect, and compete.

In this section

2.1. Preparing

Attackers receive access to the cyberrange before the event starts. Each team is given configuration files, connection credentials, and other information needed to participate.

2.2. Connecting

Participants connect via a VPN server using the credentials received from the organizers during the preparation process.

2.3. During the exercise

During the cyberexercise, attackers attempt to score points by triggering non-tolerable events as specified in tasks proposed by the organizers.

The exercise is time-limited. The remaining time is shown on the Standoff 365 platform. Breaks for technical maintenance are provided during the cyberexercise.

Attackers may target only services located at addresses provided by the organizers. Points are not awarded for attacks on other addresses. 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 the team from the cyberexercise for using service accounts or attempting to gain access to them. The list of accounts will be published during the event.
>
> Warning. Attacker teams are forbidden to fix the detected vulnerabilities or block exploitation attempts. The organizers have the right to fine or disqualify the team for doing either of these things.
>
> Warning. Attacks on addresses not in the provided list may result in removal of the team from the exercise. Teams are also prohibited from conducting DoS and DDoS attacks on the services and applications of the cyberrange infrastructure. Teams performing such attacks may be removed from the exercise.

Points can be earned by doing the following:

- **Completing tasks offered by the organizers.** Tasks might involve, among other things, obtaining confidential information, disabling one or more services, or tampering with information on a company's official website.
- **Finding vulnerabilities.** An attacker team can report vulnerabilities in the infrastructure. Scanning subnets for vulnerabilities is subject to special restrictions (see the cyberexercise portal for details).
- **Performing other tasks provided in the personal account of the participant.**

2.4. Tasks

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

2.5. Scoring

Organizers determine how well a team has completed a task. The teams are ranked by points. The winner is the team with the most points.

> Warning. The organizers have the right to disqualify a team if it tries to pass off another team's report as its own.

In this section

Task scoring (see Section 2.5.1)

Points for vulnerabilities (see Section 2.5.2)

2.5.1. Task scoring

A task is deemed completed if an answer to it has been accepted as correct. For an answer to be checked, the participant must submit a report in a specific format (a report template is available on the page of the non-tolerable event).

Attackers earn points for each task they complete. The organizers may also decide to award extra points or deduct penalty points. The first team to complete a task receives the maximum points. If two teams complete a task at the same time, the organizers can award both teams the maximum points.

If an answer does not contain sufficient information about how the task was completed, the report is not accepted and no points are awarded. If this occurs, the organizers will post a comment in the personal account for the report in question. The report may be revised and re-submitted.

2.5.2. Points for vulnerabilities

For a vulnerability to be scored, it must be described in a report in any format. The report must include an example of how a vulnerability can be exploited. Depending on the type of a vulnerability detected, it may also be necessary to obtain a DBMS version, read a local file, send an arbitrary HTTP request, or display the output of the `ipconfig`/`ifconfig`, `whoami`, or `id` commands.

Only certain classes of vulnerabilities are accepted (RCE, SQLi, Path Traversal, XXE, SSRF).

Attackers receive points for each vulnerability they find that is accepted by the organizers.

3. Rules and instructions for defenders

This section describes how defenders prepare, connect, and compete.

In this section

3.1. Preparing

Defenders receive access to the cyberrange in advance (usually a month prior) so that they have a chance to get familiar with it. Each team is given configuration files, connection credentials, and other information needed to participate.

To become familiar with the infrastructure, the teams have access to a vulnerability scanner. Organizers provide infrastructure credentials for performing inventory and scanning. A team may use another vulnerability scanner of their choice, but they must install it themselves.

After familiarization, the team shall provide the organizers with a list of which security tools they plan to use and where. In general, teams are limited to three classes of security tools: next-generation firewalls, application firewalls, and security information and event management systems. Use of other tools may be possible subject to prior approval from the organizers.

3.2. Connecting

Participants connect via a VPN server using the credentials received from the organizers during the preparation process.

3.3. During the exercise

The primary objective of defenders is to detect and investigate incidents caused by attackers' actions. During the exercise, defenders gain experience in sustaining infrastructure under hyper-realistic conditions.

The exercise is time-limited. The remaining time is shown on the Standoff 365 platform.

The following criteria are calculated for each defender team: the number of detected incidents and the average attack investigation time.

In this section

3.3.1. Number of detected incidents

Defenders work to detect incidents at the companies to which they have been assigned. During the exercise, defenders may send reports on the incidents that they have detected (a template and sample report are available on the Standoff 365 platform).

Reports are reviewed by the organizers. If a report does not contain sufficient information, the organizers will not accept it and instead leave a comment on the cyberexercise portal. The report can be corrected and re-submitted.

The target history on the Standoff 365 platform will be periodically updated to reflect the number of incidents detected by defenders. If a defender team fails to detect incidents that have been detected by the organizers, the organizers' information will be displayed.

3.3.2. Average attack investigation time

After the organizers accept an event triggering report from an attacker team, the defenders are informed about the non-tolerable event that was triggered. The defender team must then investigate the non-tolerable event. A timer appears on the cyberexercise portal: it tracks the time spent on the investigation. The defender team should provide the organizers with an event investigation report (a template and sample report are available on the Standoff 365 platform).

Reports are reviewed by the organizers. If a report does not contain sufficient information about the attackers' actions, the organizers will not accept it and instead leave a comment on the cyberexercise portal. In response to the comment, the defenders may perform an additional investigation, revise the report, and re-submit it.

Once the organizers have accepted an event investigation report from the defenders, the time it took to complete the investigation is recorded. (Time taken by the organizers to verify the report is not included.)

Glossary

attack

Attackers' actions that cause a non-tolerable event to be triggered. After conducting a successful attack, the red team submits a report.

attackers

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

cyberexercise

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

cyberexercise portal

A web application for managing cyberexercises: adding tasks, reviewing reports submitted by attackers and defenders, and viewing statistics.

cyberrange segment

A virtual part of the cyberrange infrastructure simulating information systems and processes that are typical of enterprises from a particular industry.

defenders

A team or a participant whose objective is to protect information infrastructure and detect and investigate attacks.

event investigation report

A report by a defender team that describes supposed actions of attackers aimed at triggering a non-tolerable event. A template for this type of report is provided in the file investigation_report_BLUE.xlsx.

event triggering report

A report by an attacker team describing actions that allowed the team to trigger a non-tolerable event. A template for this type of report is provided in the file nontolerable_event_report_RED.xlsx. A sample report can be found in the file sample_nontolerable_event_report_RED.xlsx.

incident

A single action by attackers aimed at violating the accessibility, integrity, or confidentiality of data. After investigating an incident, the blue team submits a report on it.

incident report

A report by a defender team describing a detected action of attackers that affects the accessibility, integrity, and confidentiality of data. A template for this type of report is provided in the file incident_report_BLUE.xlsm.

non-tolerable 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. On Standoff 365, the objective of attackers is to trigger non-tolerable events, and the objective of defenders is to investigate these attacks.

service

A component of the cyberrange infrastructure that controls a certain process in the information system.

Standoff

Open cyberexercises that take place several times a year and may be held as part of an information security conference.

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.

task

A description of objectives for attackers to achieve.

vulnerability

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

vulnerability report

A report by an attacker team on a discovered vulnerability.

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 information infrastructure, while also allowing for connection of external devices and equipment to the infrastructure.

Standoff cyberrange is designed to re-create the infrastructure of real enterprises from various sectors of the global economy. Attackers and defenders will be able to try out their skills on facilities used in the transportation, mining, energy, and oil industries. Moreover, the cyberbattle will unfold across the smart city systems, financial structures, and a wide range of other contexts.

Companies and security professionals alike benefit from participating in Standoff by empirically testing the feasibility of cyberattacks in a safe environment, gaining knowledge and hands-on skills to detect and counter threats, gaming out response scenarios, and seeing first-hand the close relationship between cybersecurity and business.

org@standoff365.com standoff365.com