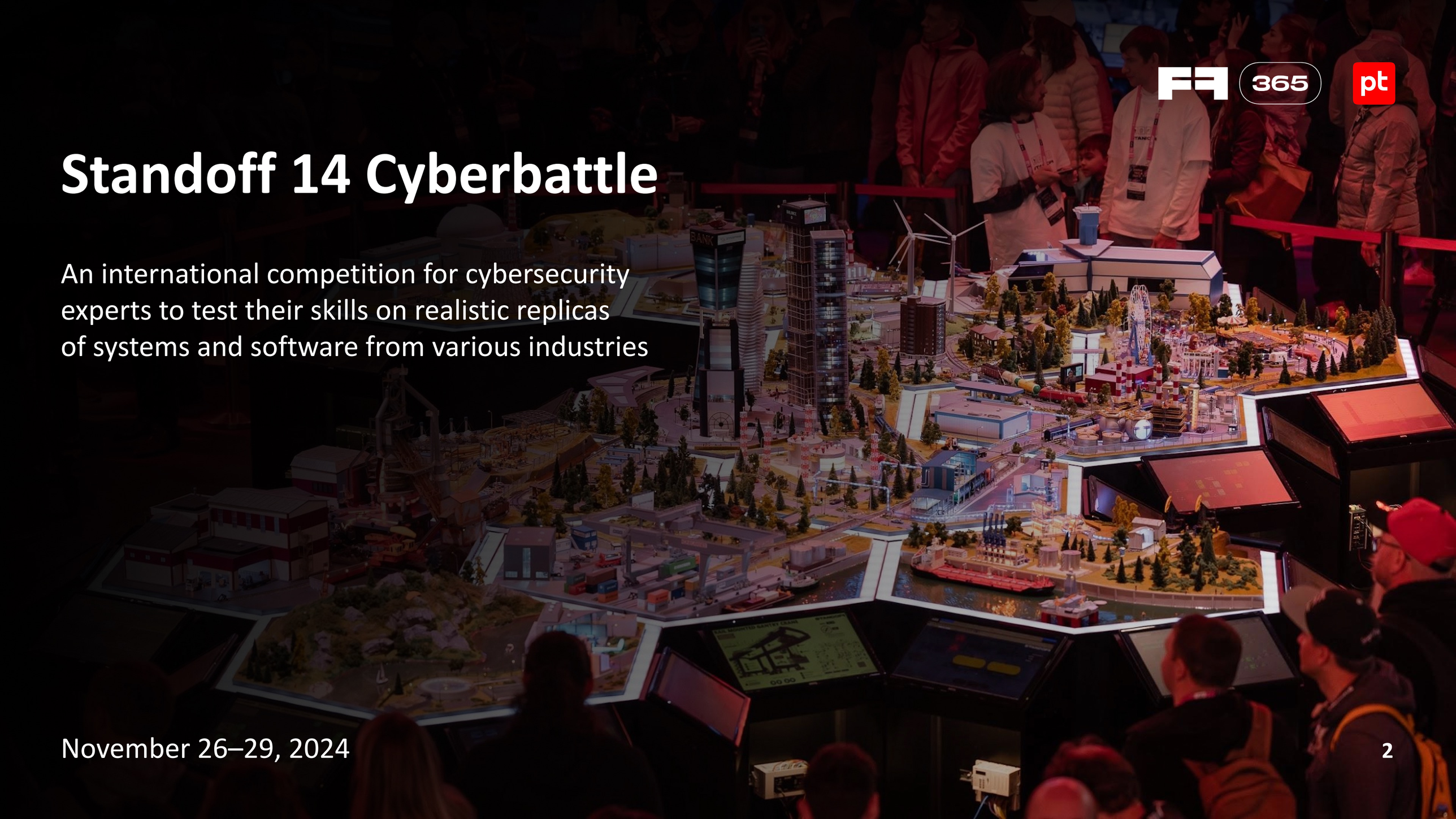
Standoff 14 Cyberbattle

Online. November 26–29, 2024

Standoff 14 Cyberbattle

An international competition for cybersecurity experts to test their skills on realistic replicas of systems and software from various industries



November 26–29, 2024

About Cyber battle Standoff 14

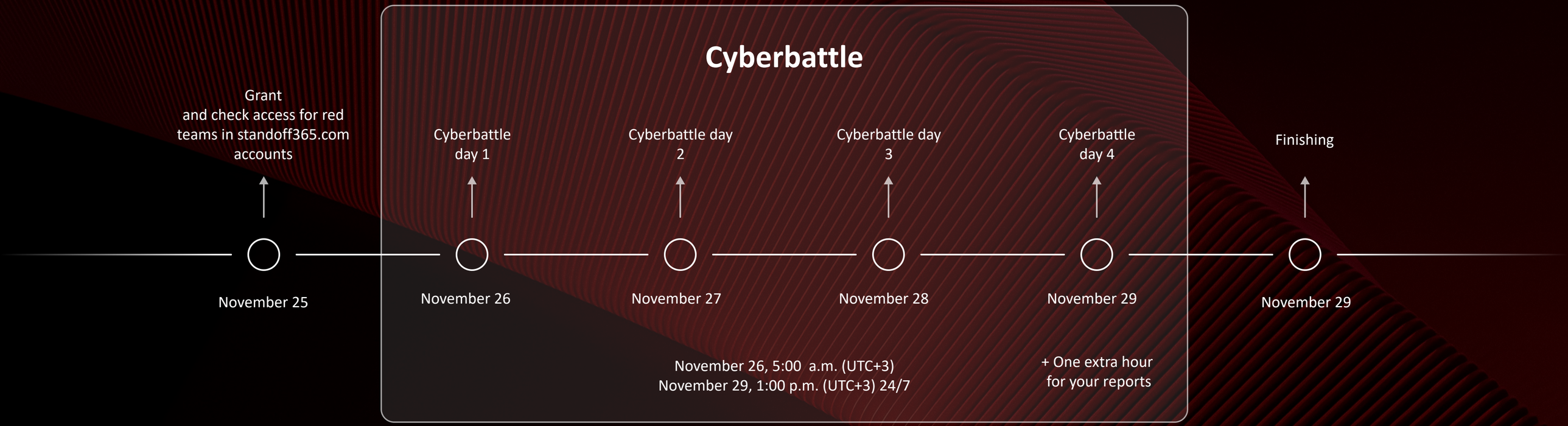
26th-29th Standoff 14 for professional red teams

26th of November 5:00 a.m. (UTC +3) - 29th of November 1:00 p.m. (UTC +3)

50 red teams

total prize pool USD 50000
1st USD 20 000 (money or licenses (Burp) or both)
2nd USD 10 000 (money or licenses (Burp) or both)
3rd USD 5 000 (money or licenses (Burp) or both)
4-8 places from USD 500 to 2500
+ special achievements (like "first blood" and etc.) USD 7500 total

Timeline


Cyberbattle
Grant
and check access for red teams in standoff365.com accounts
November 25
Cyberbattle day 1
November 26
Cyberbattle day 2
November 27
Cyberbattle day 3
November 28
Cyberbattle day 4
November 29
November 26, 5:00 a.m. (UTC+3)
November 29, 1:00 p.m. (UTC+3) 24/7
+ One extra hour for your reports
Finishing
November 29

Access

Check access to the cyberrange:
November 25 10:00 (UTC+3)

Access and the config to connect→
in your account at https://standoff365.com/

The VPN supports 10 simultaneous connections and has a speed restriction

Our Discord server for Standoff 14
https://discord.gg/TyWQ78dE8F

Red Team activivies

- Get points for vulnerability reports (bugbounty-style tasks).
- Get (way more) points for triggering critical events in the offices.

Critical events are events that would cause major damage to infrastructure and are non-tolerable for business. Some examples:
— Shutdown of the powerplant
— Critical data leak
— Oil spill from oil storage
— Financial damage

While vulnerability reports checked up automatically (flag-based system), scoring a critical event some times can require a full pentest-like report that is checked manually.

Red teams cannot commit destructive actions, aggressively scan the network, fix vulnerabilities embedded by the organizers, prevent other red teams from participating, or be rude to organizers or other participants.

Defender responsibilities

Analyze attacker behavior during the battle to identify weaknesses in information security systems

Detect as many attacks as possible

Investigate as many incidents as possible

Evaluation of actions

Attackers:

- Teams receive points for reports on triggering critical events.

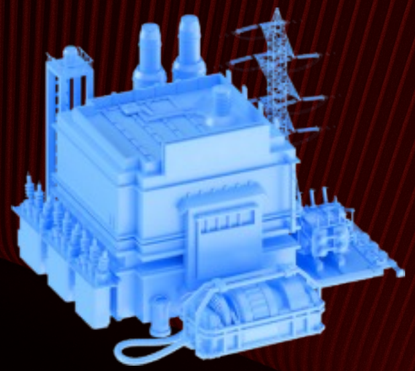
- Teams also receive points for bug bounty reports.

Only certain vulnerability classes are accepted: LPE, RCE, SQLi, XXE, SSRF, and Path Traversal.

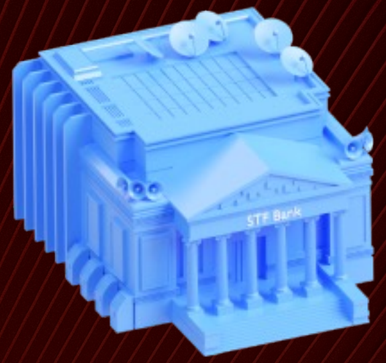
Standoff Cyberrange: composition

The total number of critical events will exceed 80

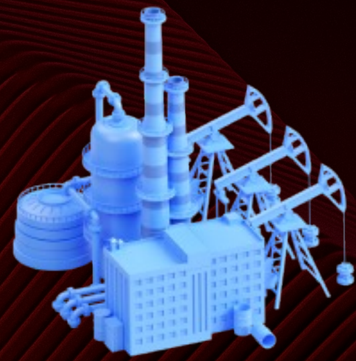
Tube oil and gas company



Electric power industry

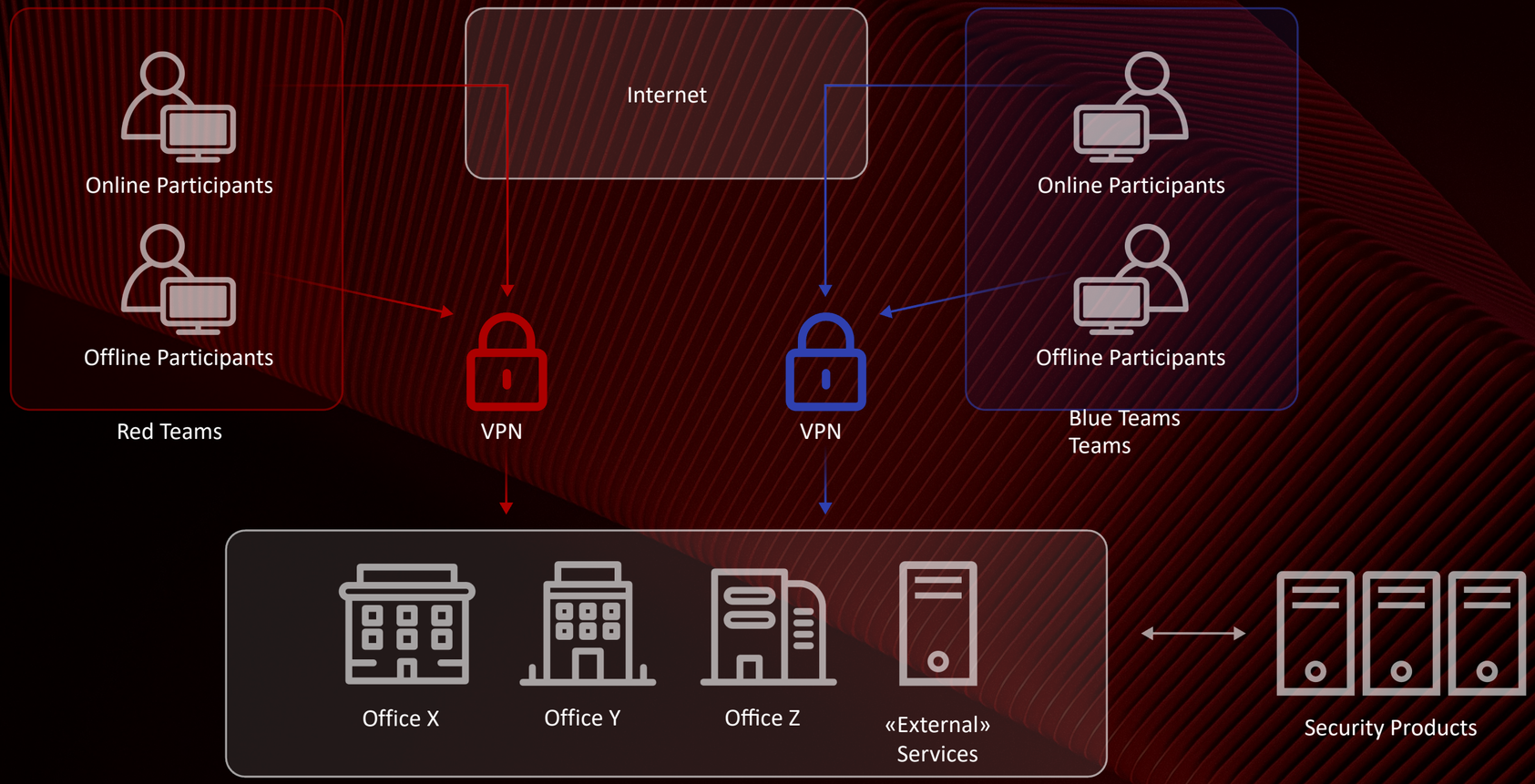


Banking sector



STFware IT company

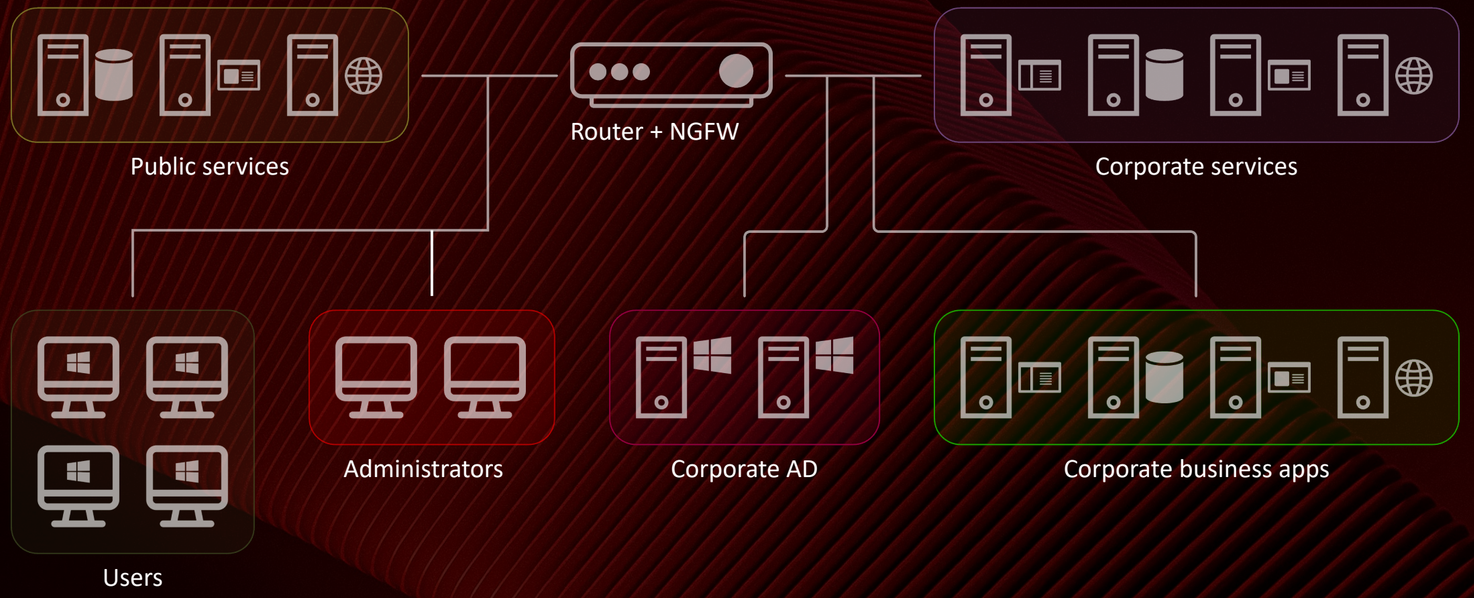
Cyberrange Infrastructure



Infrastructure

Vulnerable **web applications**

- **Windows AD** infrastructure
- **FreeIPA** infrastructure
- **MS Exchange** and other mail services
- User workstations **(Windows, Linux)**
- Corporate services
- Development infrastructure (**Gitlab, Teamcity**, etc)
- Specialized **banking software**
- **Industrial management systems**

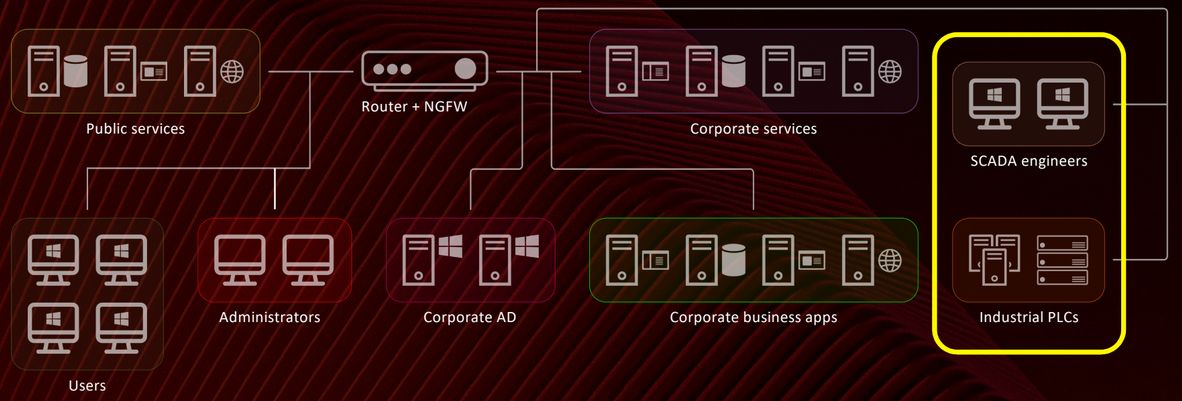


High value targets

Offices with ICS

Engineers: operator workstations equipped with mission-critical software and hardware for ICS management

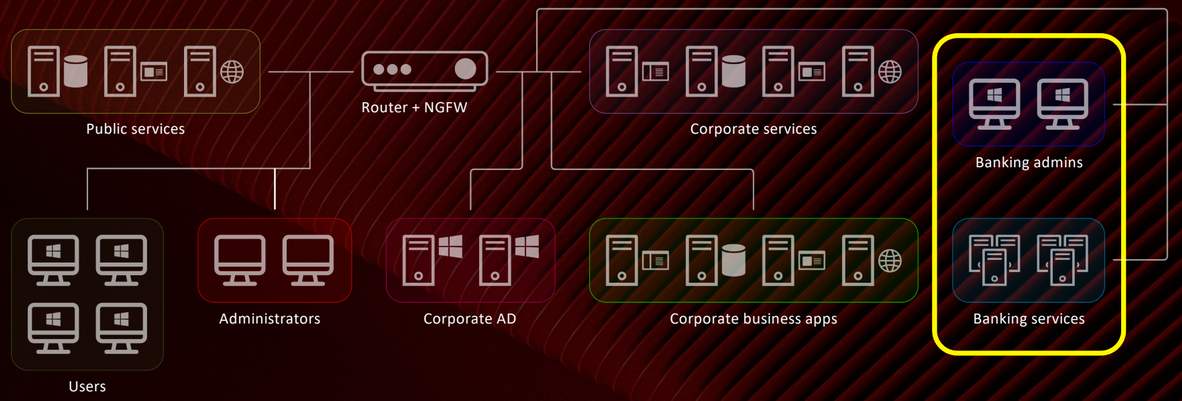
PLCs and SCADA: specialized industrial hardware units and software for monitoring and control



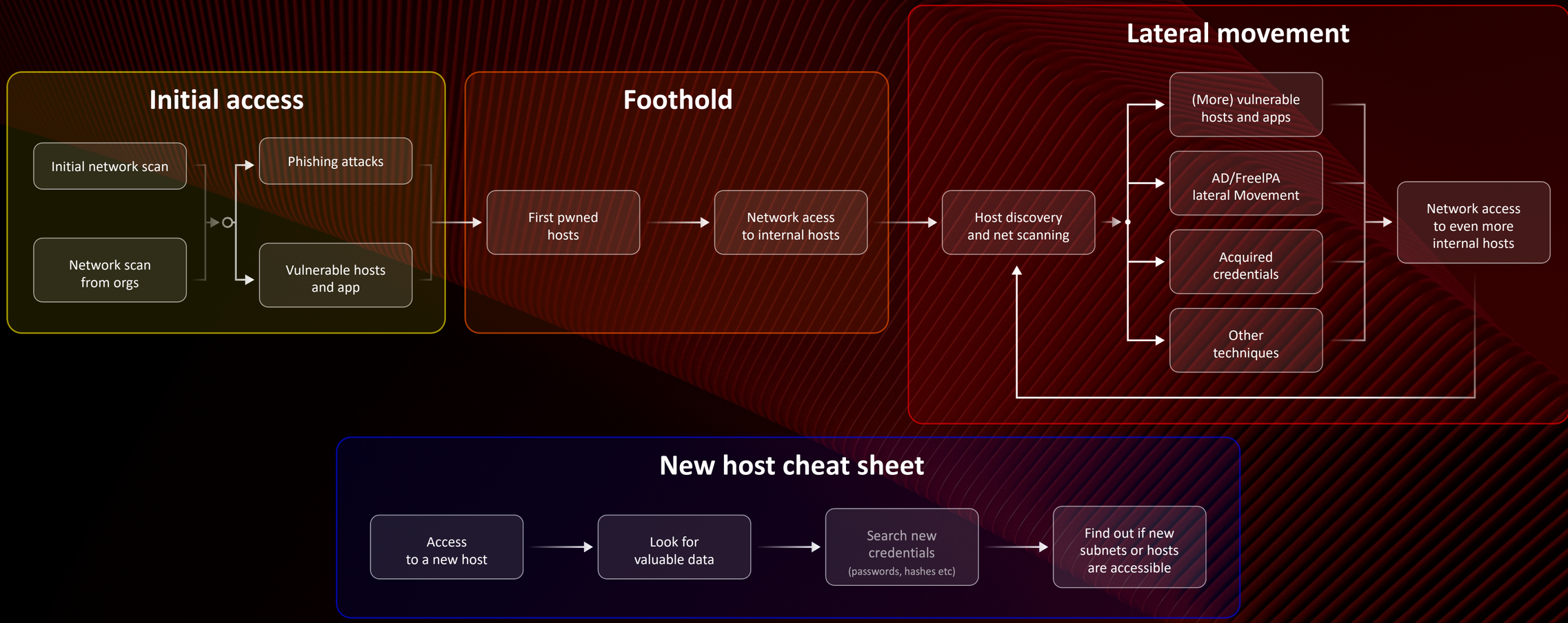
Banking systems

Administrators and operators: workstations for high-privileged bank employees and system administrators

Banking services: core financial software that supports essential banking operations and customer services

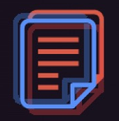


Methodology



Standoff365

Online cyberrange for beginners

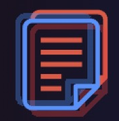


Workspace

Results

Bootcamp

Online cyberrange for professionals



Workspace

Results

Metal&Tech

HighTechEnergy

Banking system

NetFusionPro

Bank: tasks

19 critical events in the banking system

Commercial Bank of Standoff

- Transfer management panels
- Office in another country

First Partner Bank

- Mobile application
- Acquiring (QR code payment)

Global Digital Bank

- Automated bank without operators
- Mobile application and plastic cards

How are points earned in the ICS segment?

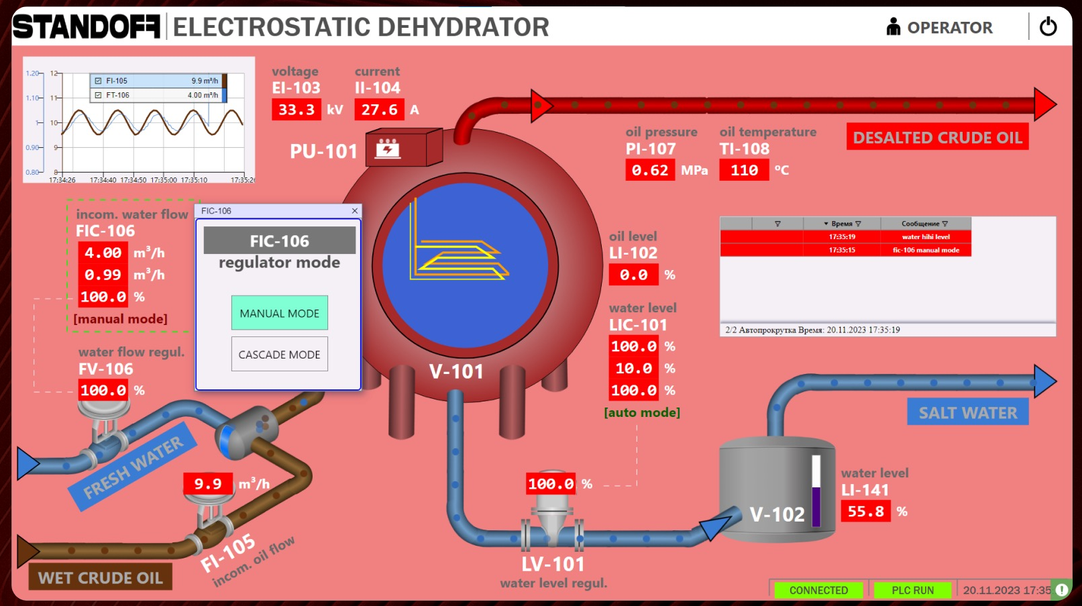
Tasks (your targets):

Cause an emergency: gain access (to PLC or SCADA) and disrupt normal operations.

Interrupt PLC operations: for example, DoS it or make it unavailable.

Spoof data on the operator's screen: parameters must differ from current actual values.

Attacks on industrial switches: disrupt communication between the PLC and SCADA.

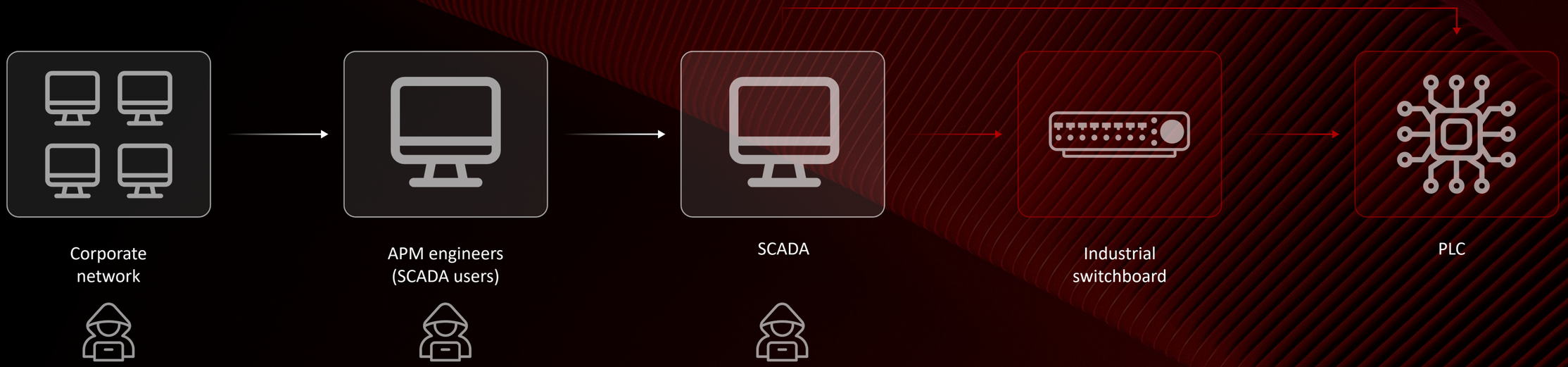


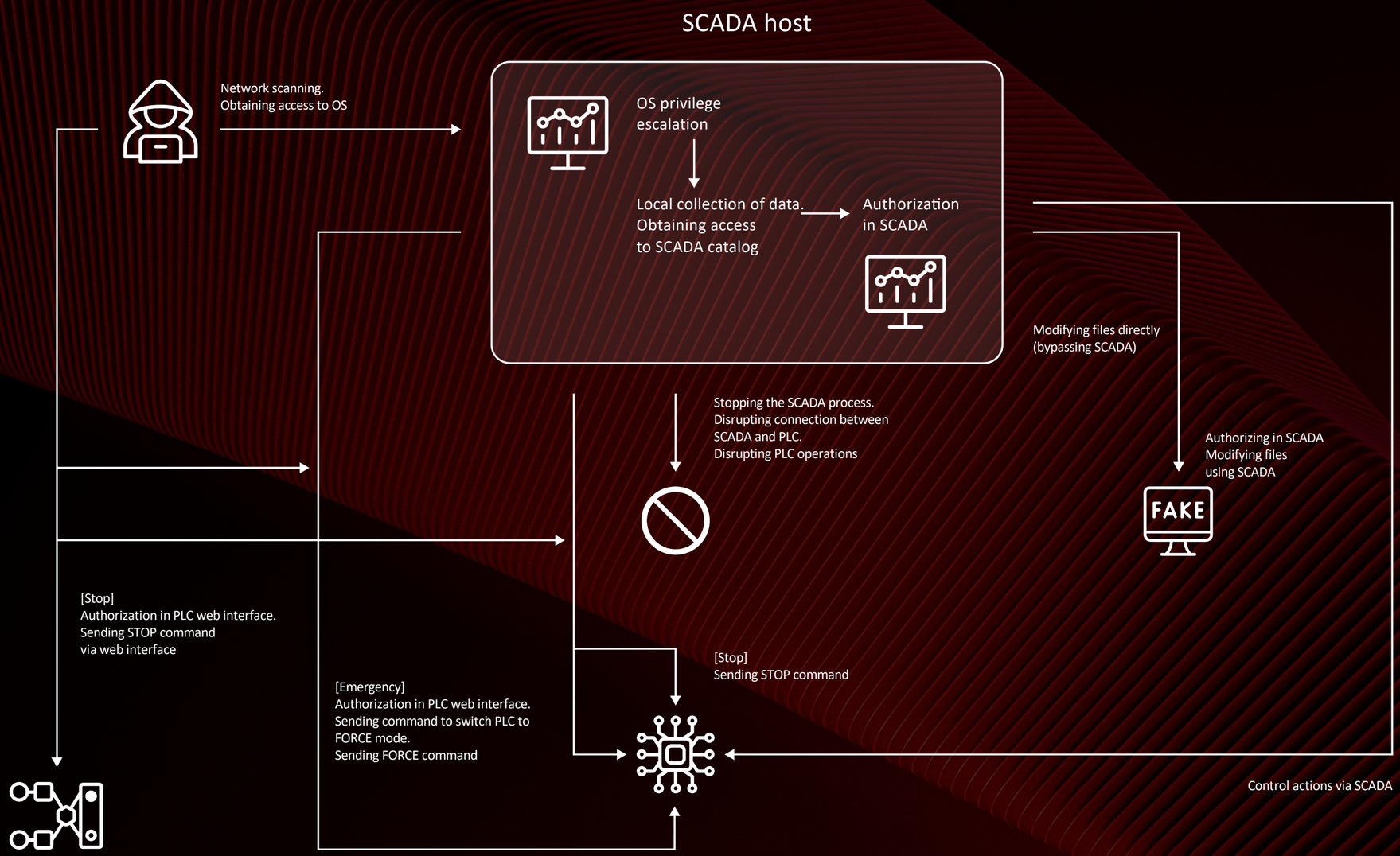
Attack paths

1. Access the SCADA system: you need to gain access to a SCADA device and project with the ability to elevate privileges or take full control to disrupt processes via the SCADA interface.

2. Access to an operator or engineering computer: gain access to operator or engineering workstations so you can interact directly with PLCs responsible for process control.

3. Or manipulate network equipment, meaning interfere with the operation of routers or switches that provide communication between the PLC and SCADA system. A malfunction in network equipment can interrupt communications or cause control failures.




SCADA host
Network scanning.
Obtaining access to OS
OS privilege
escalation
Local collection of data.
Obtaining access
to SCADA catalog
Authorization
in SCADA
Modifying files directly
(bypassing SCADA)
Stopping the SCADA process.
Disrupting connection between
SCADA and PLC.
Disrupting PLC operations
Authorizing in SCADA
Modifying files
using SCADA
FAKE
[Stop]
Authorization in PLC web interface.
Sending STOP command
via web interface
[Stop]
Sending STOP command
[Emergency]
Authorization in PLC web interface.
Sending command to switch PLC to
FORCE mode.
Sending FORCE command
Control actions via SCADA

How to penetrate a SCADA operating system

1. All credentials to access SCADA devices are arranged in vectors insegments

2. Exploit a known CVE or find your own RCE in the operating system or SCADA (ports of various SCADA services are open).

Successful attack = change PLC state

Organizers look at the state of the PLC and SCADA, and if they see changes in controller operations, then the attack is counted

Prohibited

Connect physically

Lie in reports

Brick devices

King of the hill and multiple access

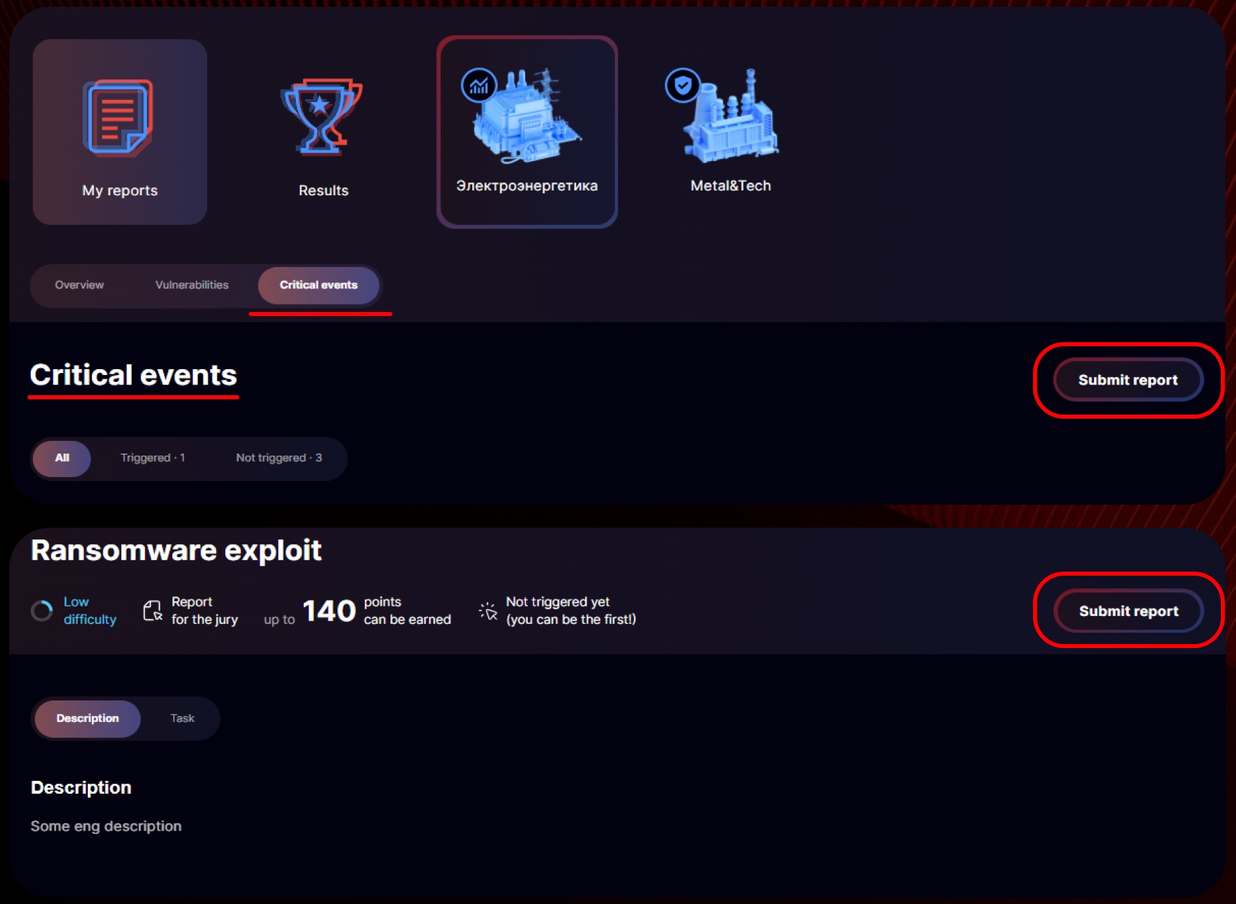
There's no multiple access to the SCADA.
Access is for one person only: participants have to take turns.
As soon as you get started, change the password on the device.
After 30 minutes, access is given to the next person.
The organizers will form a queue in a separate chat and table.

Rules

The **full list of rules** is available on the standoff365.com portal.
The rules cover:

1. How and what points are earned for
2. When reports are returned for correction and when they are rejected
3. Dynamic scoring description
4. What to do if you need help
5. Prohibited actions during the cyberbattle, including penalties

Critical event report



To submit a report, find the critical event you triggered on the portal and click the "Submit report" button

1. Industry page → CE → submit report

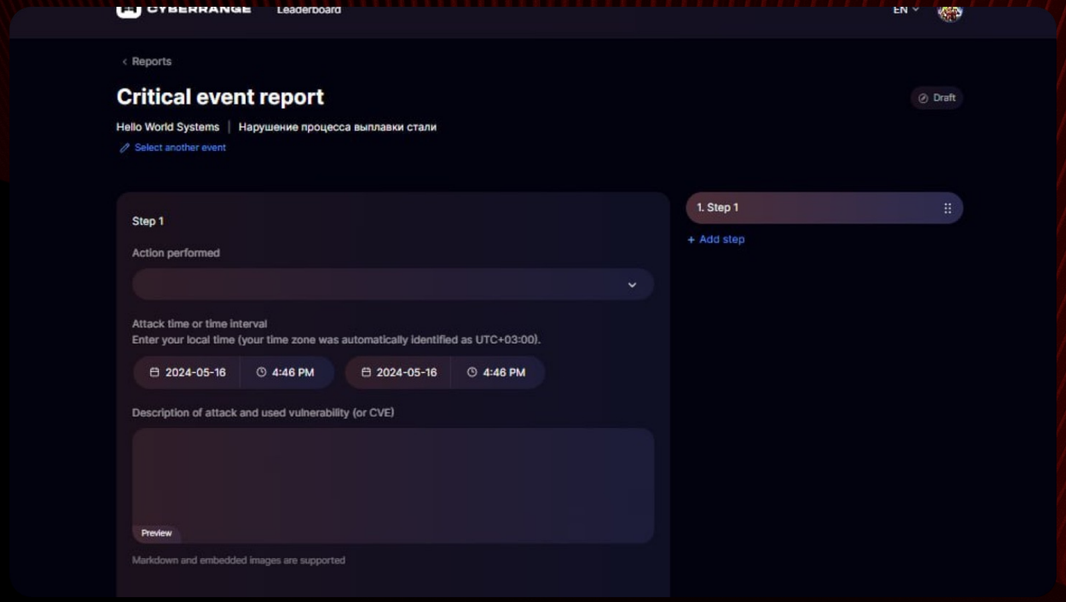
2. CE page → submit report

3. Team account → CE reports → submit report

4. Report group → submit new report

5. Report group → line with report → submit report based on this

Critical event report

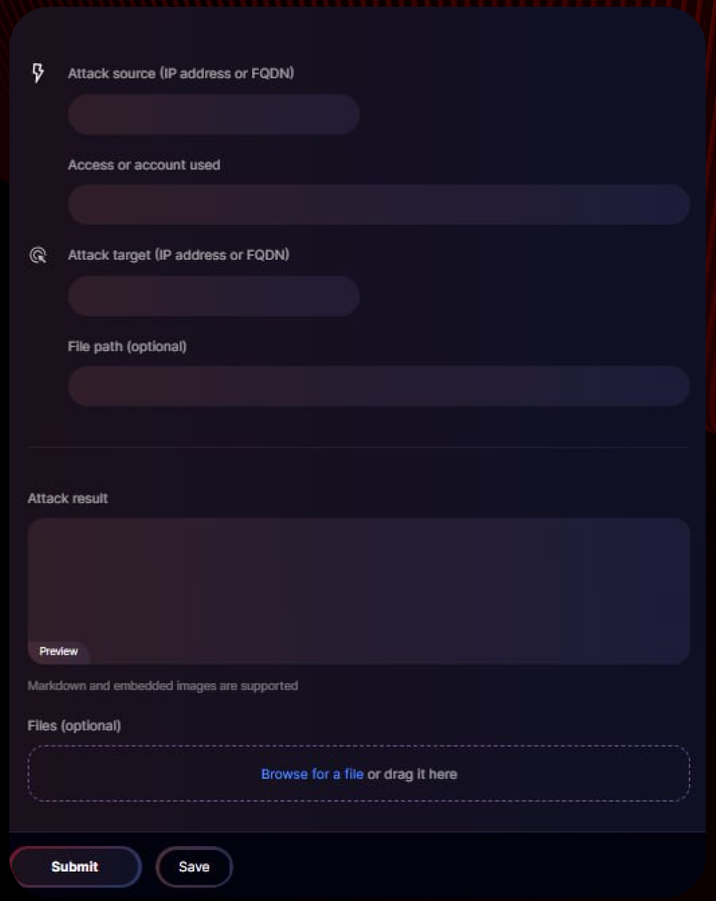


Action performed
Select from the drop-down list
Avoid repeating the same name excessively
Do not combine actions with different logic in a single step

Date and time
Write as precisely as possible
Use your local time zone (note that we will not convert it to GMT+3)

Description of attack
Use complete sentences to make each step a clear, reproducible sequence
Provide all details without assuming the reader has prior knowledge.
Clarity and completeness are essential.
Insert screenshots directly within the text to illustrate specific steps

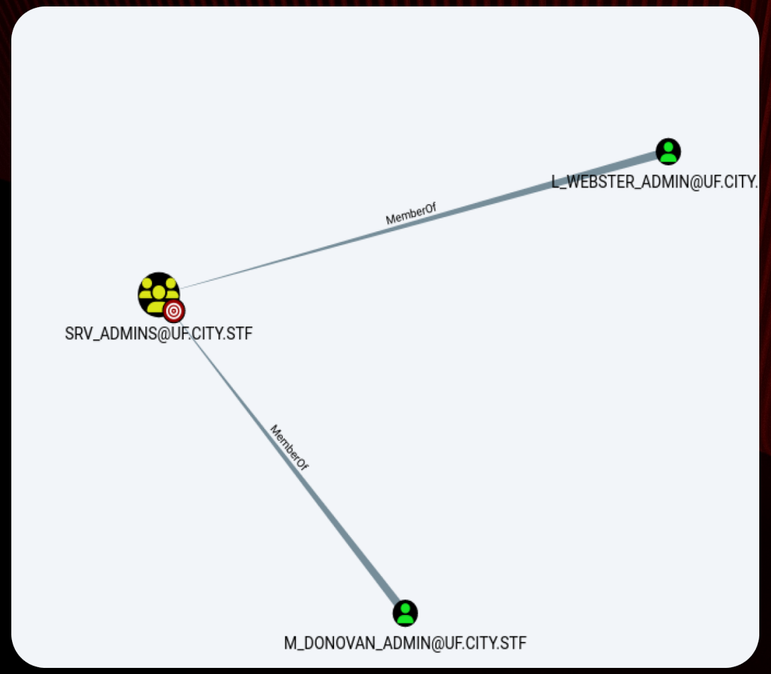
Critical event report

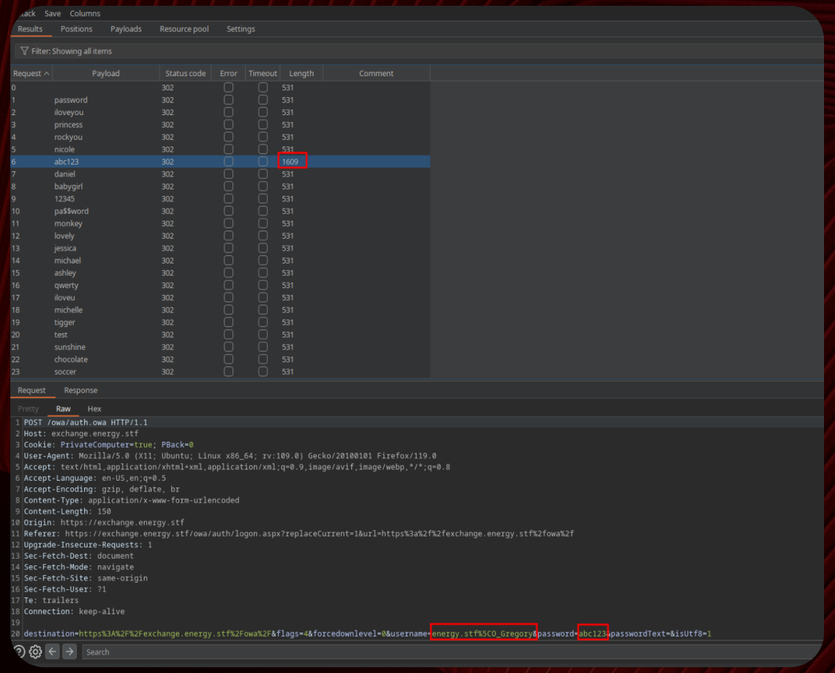


Source and attack goal
Ensure there are no typos and confirm that the scope of the attack is maintained.
Access or account used
Include the account details, access level (e.g., System), or username used to connect to the node. Each account must be traceable to previous steps and not appear without prior context.
File path
Specify any file paths for files uploaded to nodes.
Attack outcome
Describe the outcome of the attack. Screenshots can be included to support results.
Files
Final-step screenshots are required. Screenshots are also helpful for other steps, especially when timestamps are fully visible.

The more artifacts you provide — such as commands, screenshots, files, and exploit descriptions — the easier and faster the evaluation process becomes.

Report screenshot examples






```
C:\Users\[redacted]\Pictures\pseudoransomware_c7f9f656cd>ransomware.exe
The system is encrypted successfully!
Success!
```

Submitting a thorough and accurate report

✅ Carefully review all report fields. Check the header, confirm if the report applies to the CS, and ensure accuracy in the time zone and IP addresses.

✅ Confirm that the task is fully completed.

✅ Attach both intermediate and final screenshots.

✅ Specify details at each step of the attack. For example:

- If you gained an account, indicate the source.
- For privilege escalation, explain how it was achieved.
- For information discovered, specify the location.
- If a vulnerability was exploited, state the application and type of exploit.

✅ Ensure the attack chain is fully reproducible. Include every step and avoid assumptions about what the reader may know.

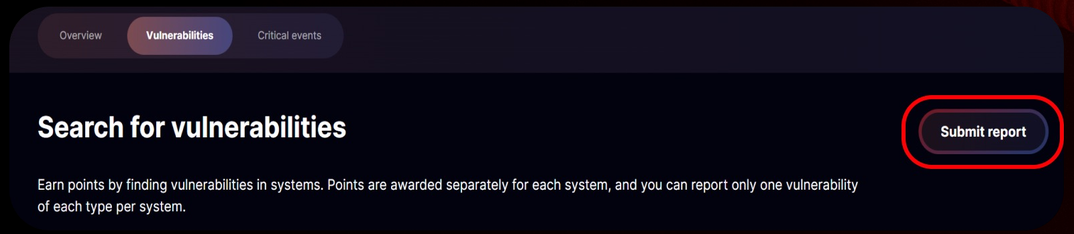
✅ Don't use slang in the report. Use clear, professional language.

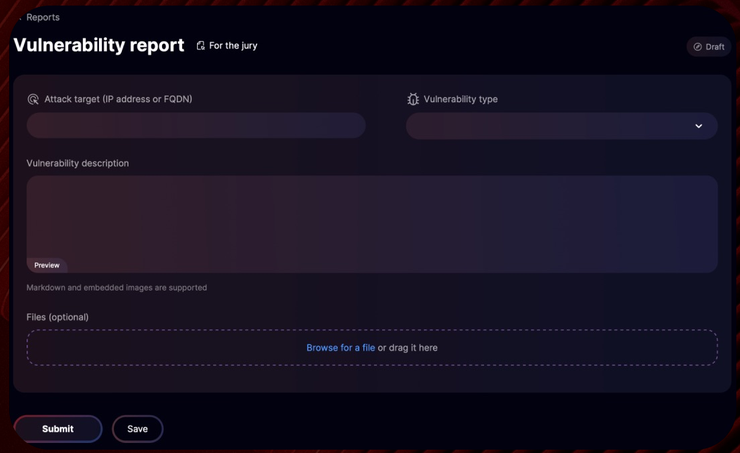
❌ Do not reference other reports related to CS or vulnerabilities. All vector steps must be included within the same report.

⚠️ Tip: take a few extra minutes to complete the report thoroughly now rather than risk needing more time for corrections later.

Refer to HackerOne sample reports for guidance

Each report must demonstrate how the vulnerability can be exploited. Depending on the vulnerability type, the report may also require DBMS version retrieval, reading of a local file, sending of an arbitrary HTTP request, or output display from commands like ipconfig/ifconfig, whoami, or id.





You can maximize points in vulnerability reports with the following:

1. Obtain root privileges on the main system, not within a container. The report must include output from /etc/shadow.

2. Submit each LPE method for Windows only once per segment of the cyberrange. Additional methods for the same segment may also be submitted if found.

3. Earn up to 1,500 points per node.

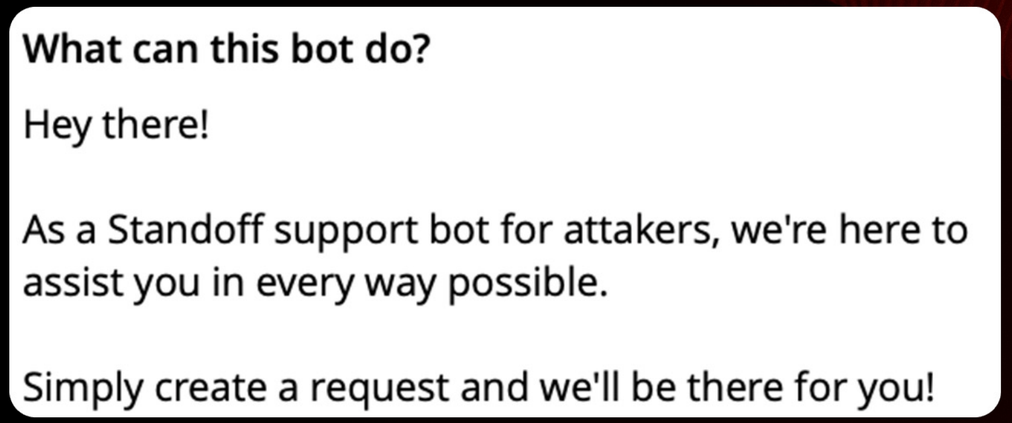
Criticality	Type	Cost
Low	Path Traversal	100
	SSRF	
Average	XXE	200
	SQLi	
High	RCE	300
Critical	LPE	400

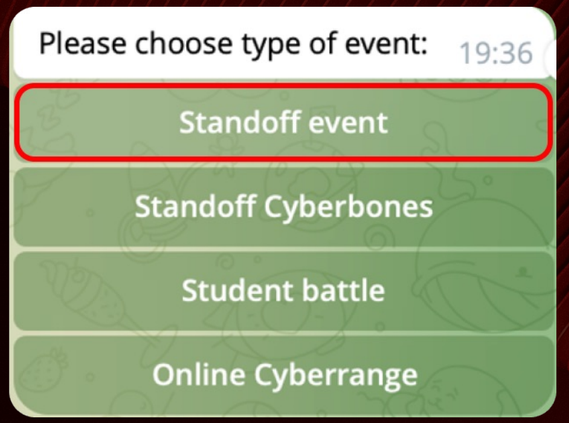
Technical support

All technical questions are to be sent via the bot

Those who use the bot will be in priority because it’s a single platform for processing tickets that allows to keep everything in one place and respond to you more quickly than in the group chat of the event.

There you will also be able to see all your tickets, switch between them and provide information requested by the technical support team https://t.me/red_team_support_bot





Mentor support

Our goal is to make your experience as successful and useful as possible.

That's why we provide a personal mentor (tutor) for each team.
The mentor will:

- Support you via a Discord chat (we create a designated chat for each team on our server).
- Assist with solving tasks.
- Communicate with the organizers on technical issues.
- Advise on tactics and tooling.

Discord

Visit our Discord channel

Invite your friends to participate in Standoff 14

Contact info

WhatsApp: +79119344809
WeChat ID: k4riN44
Telegram: t.me/k4riN44
hello@standoff365.com