



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

2

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)

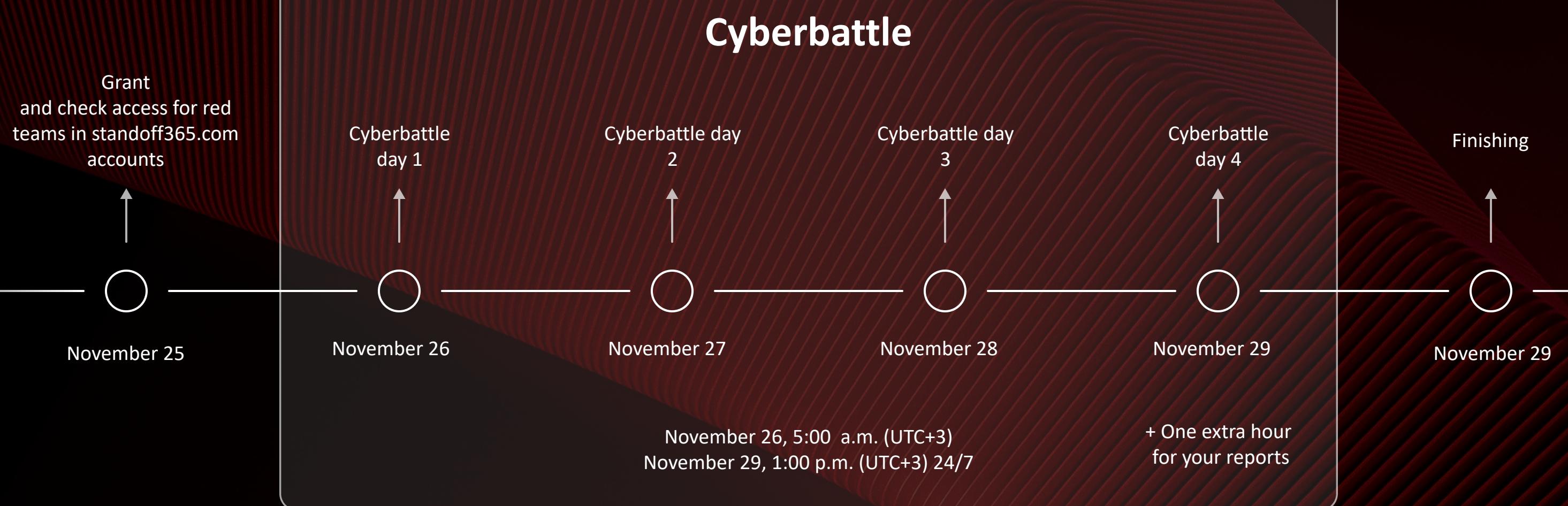
2nd USD 10 000 (money or licenses (Burp) or both)

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



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 activities

- 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.

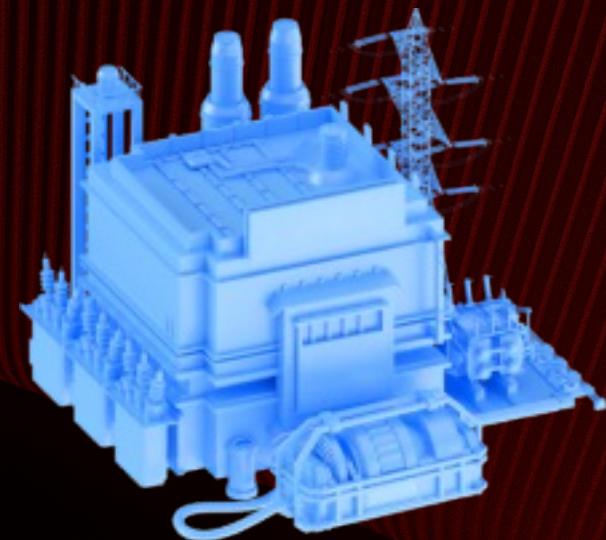
Only certain vulnerability classes are accepted: LPE, RCE, SQLi, XXE, SSRF, and Path Traversal.

Standoff Cyberrange: composition

The total number of critical events will exceed 80



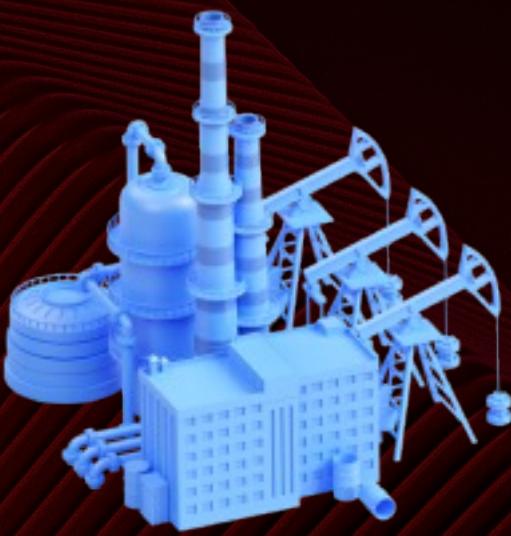
Tube oil and gas
company



Electric power
industry

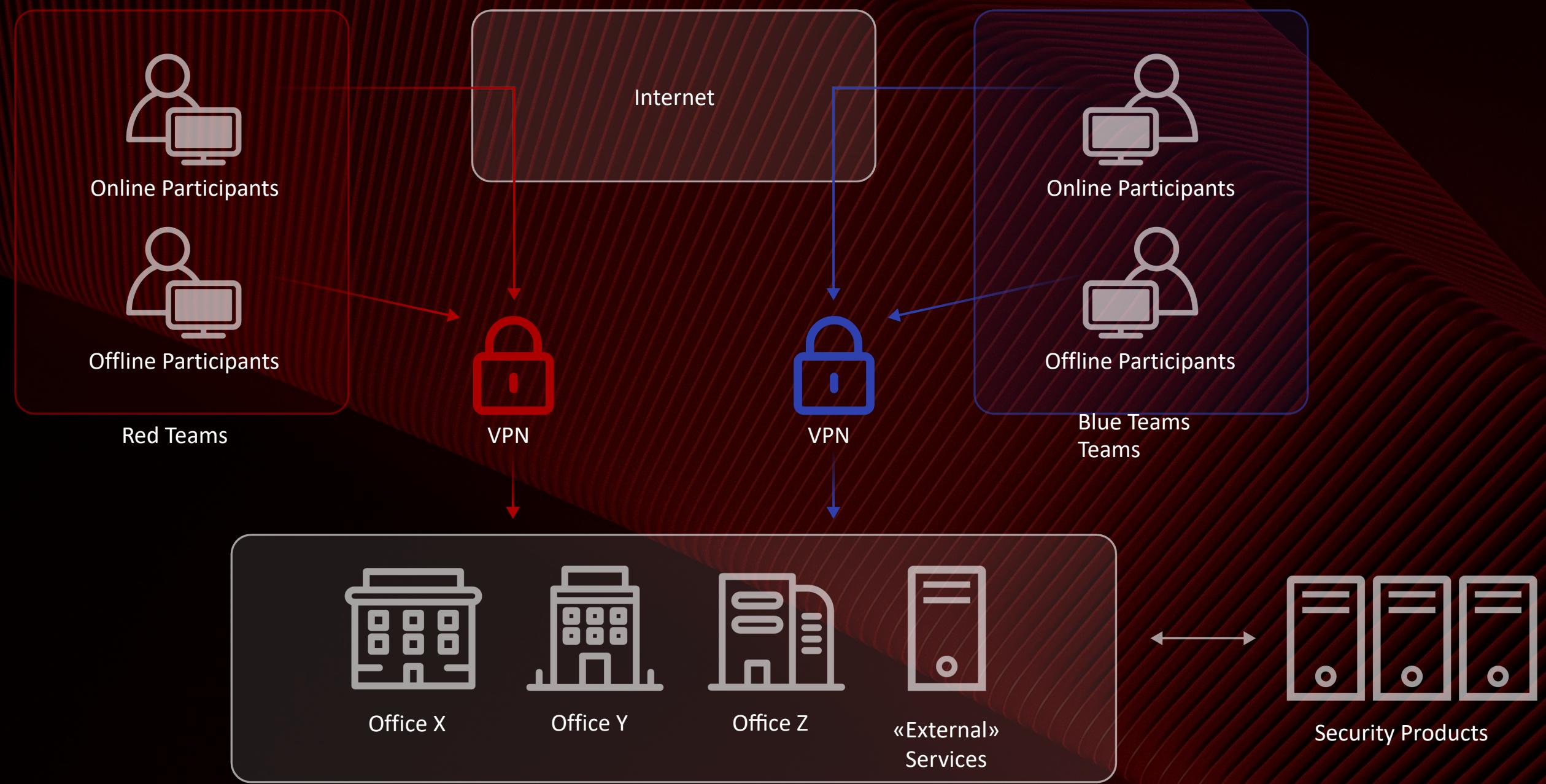


Banking sector



STFware IT company

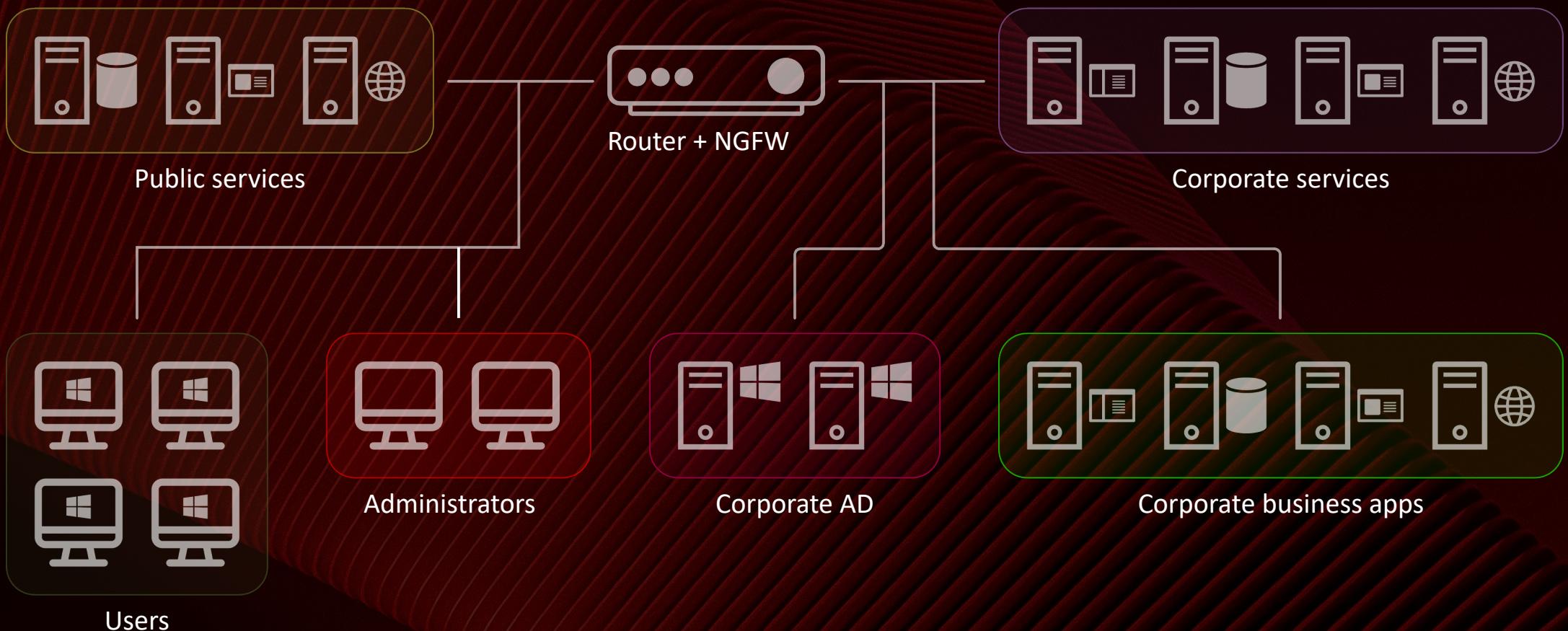
Cyberrange Infrastructure



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

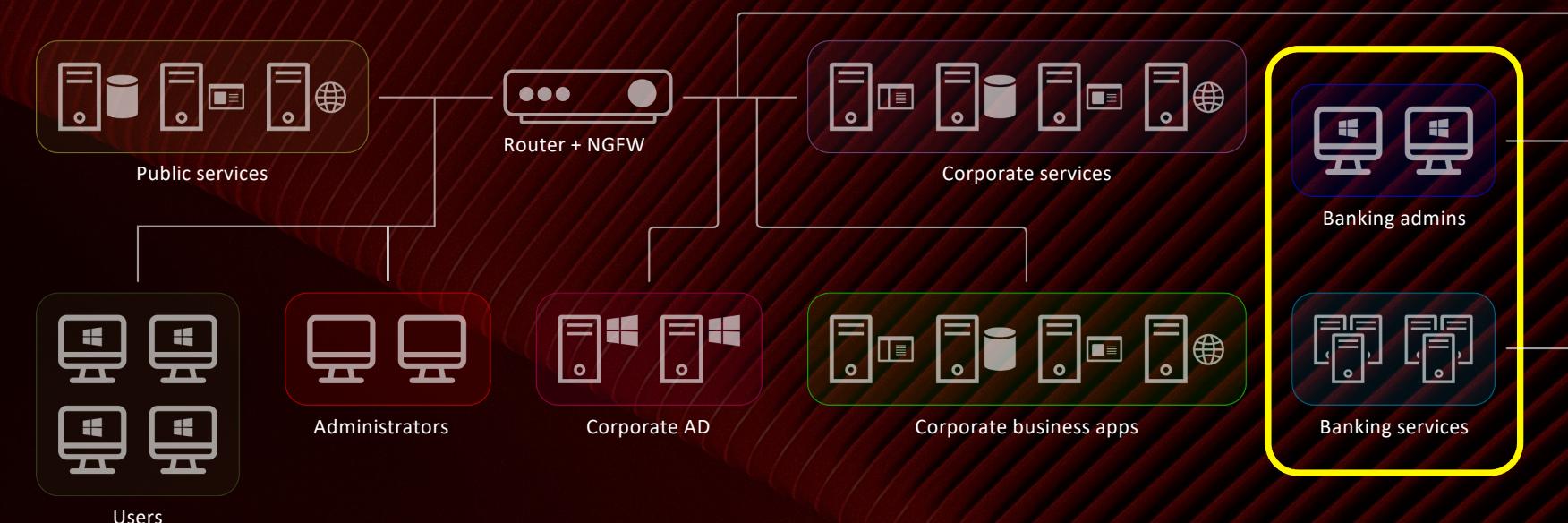
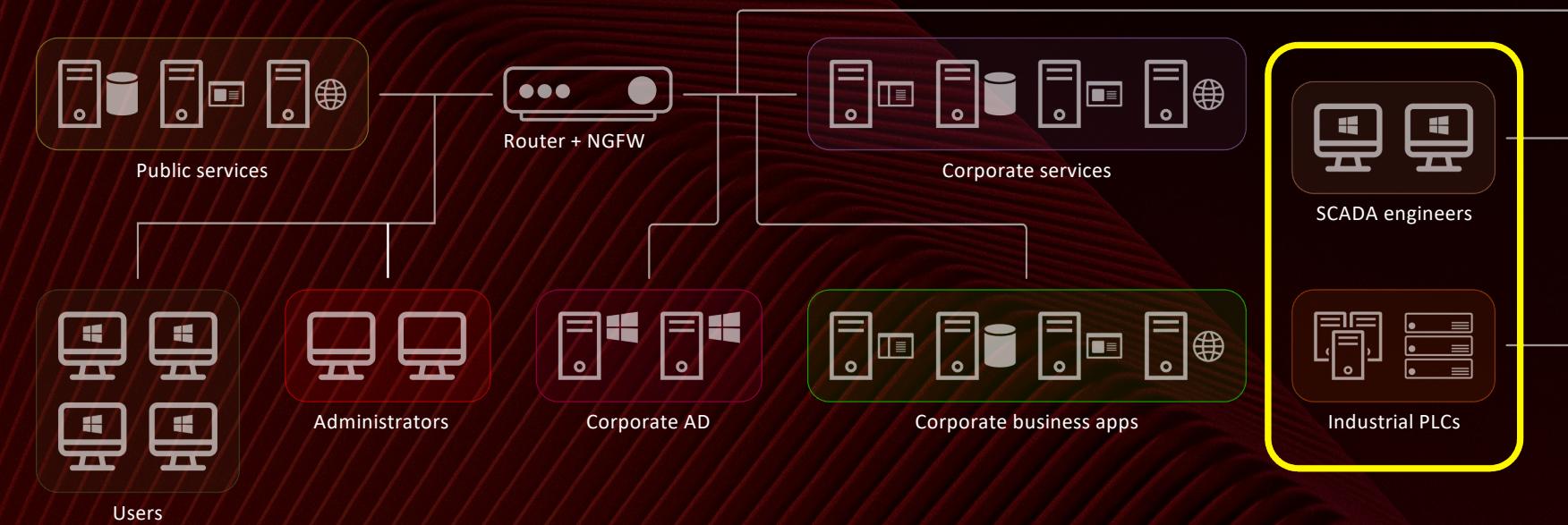
Engineers: operator workstations equipped with mission-critical software and hardware for ICS management

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

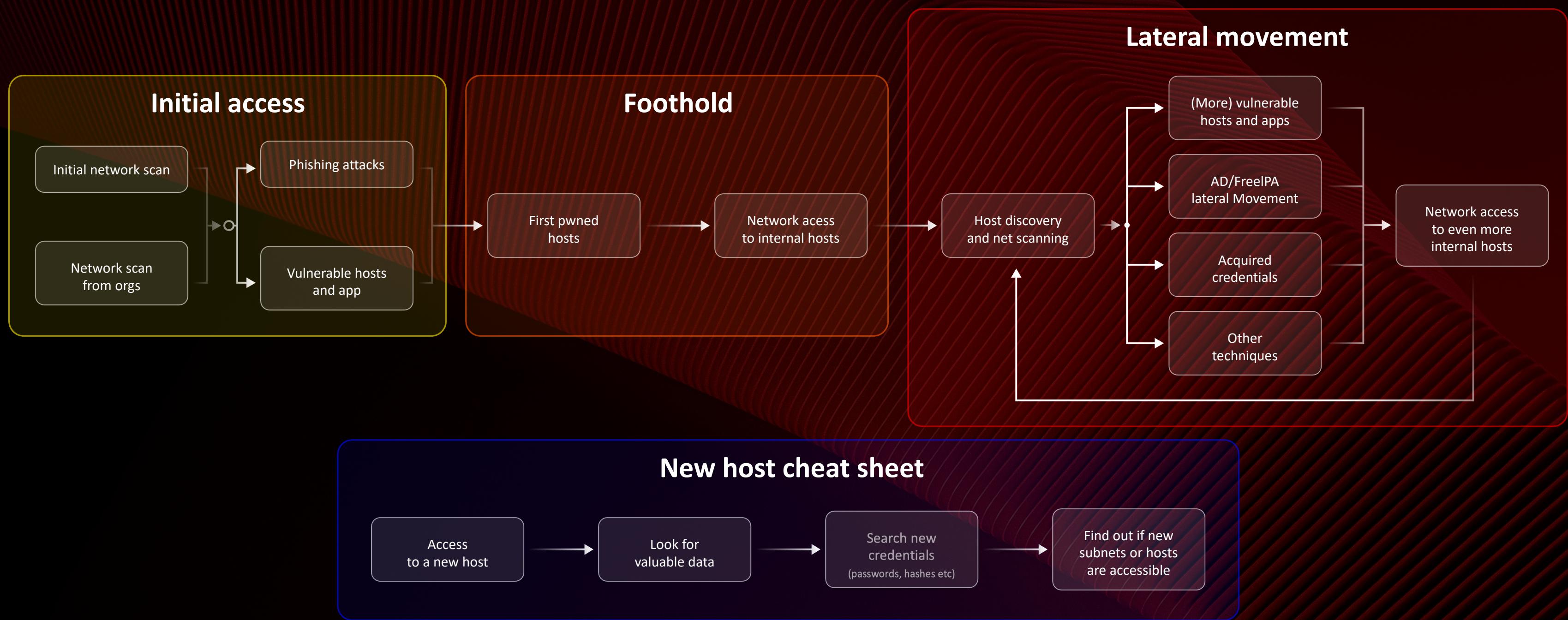
Banking systems

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?

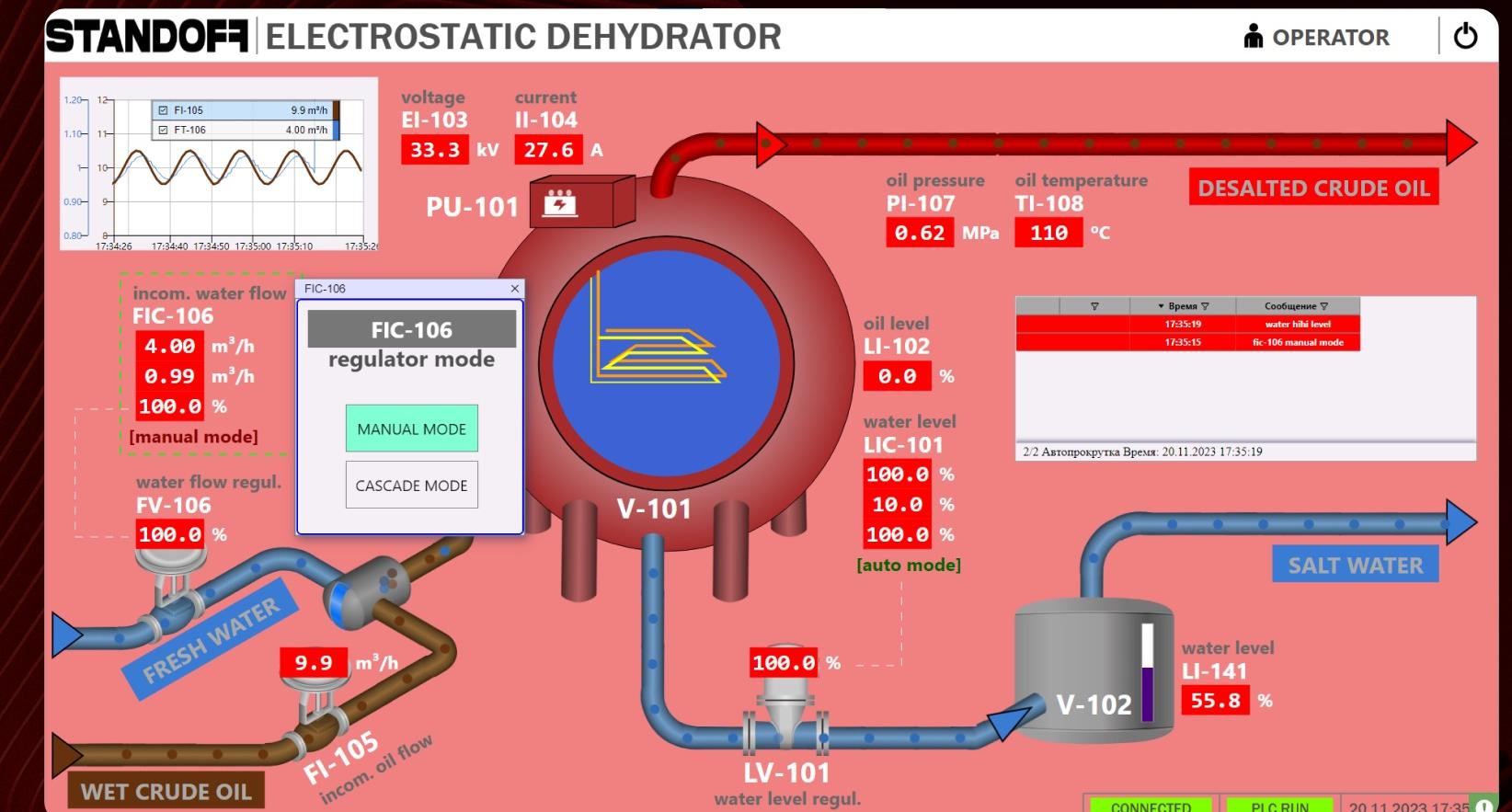
Tasks (your targets):

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

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

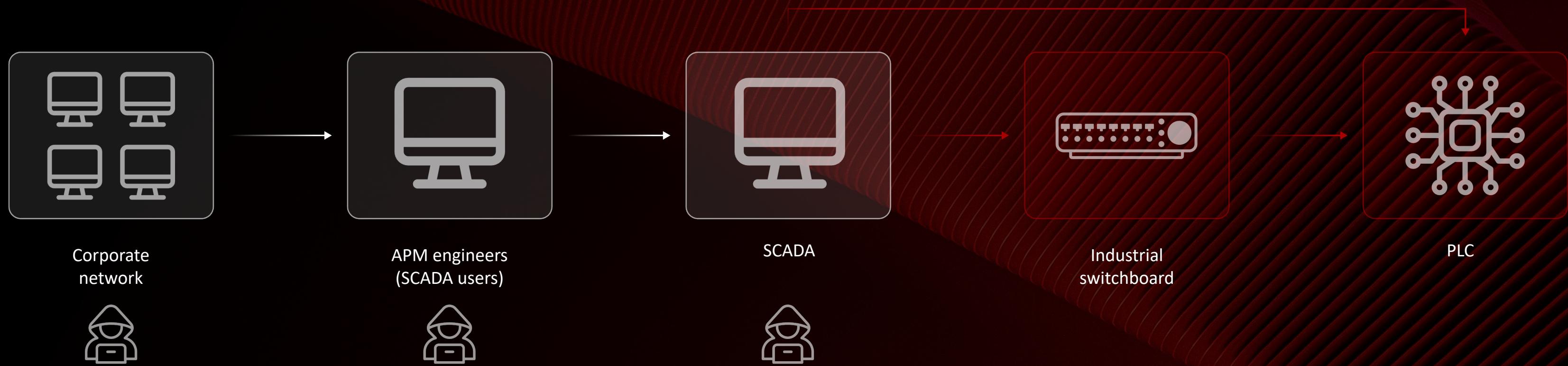
Spoof data on the operator's screen: parameters must differ from current actual values.

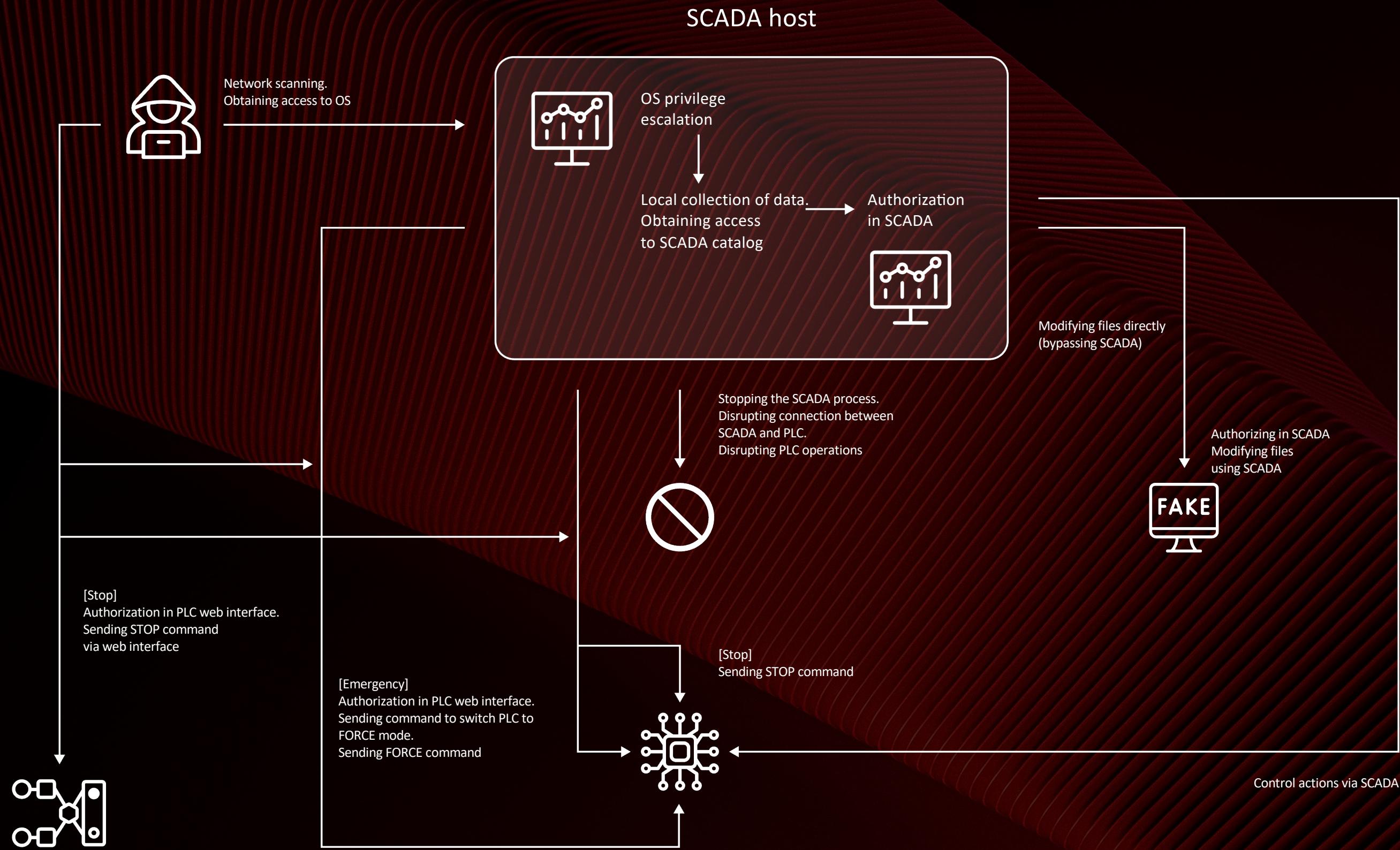
Attacks on industrial switches: disrupt communication between the PLC and SCADA.



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.





How to penetrate a SCADA operating system

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

The screenshot shows the F3 365 platform interface. At the top, there are navigation links: 'My reports' (blue icon), 'Results' (trophy icon), 'Электроэнергетика' (Electroenergetics icon with a factory silhouette), and 'Metal&Tech' (factory icon). Below these are tabs: 'Overview', 'Vulnerabilities', and 'Critical events' (which is highlighted in red). A large button labeled 'Submit report' is circled in red.

Critical events

Under the 'Critical events' section, there are three buttons: 'All' (selected), 'Triggered · 1', and 'Not triggered · 3'. Below this, a specific critical event is detailed:

Ransomware exploit

Difficulty: Low (blue circle icon). Points: up to 140 points can be earned. Status: Not triggered yet (you can be the first!).

A large 'Submit report' button is circled in red at the bottom right of this section.

At the very bottom, there are tabs for 'Description' (selected) and 'Task'.

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

The screenshot shows the CYBERRANGE platform's critical event report interface. At the top, there are navigation links for 'Reports' and 'Leaderboard'. Below that, the title 'Critical event report' is displayed, along with the event name 'Hello World Systems | Нарушение процесса выплавки стали' and a note to 'Select another event'. The main area is titled 'Step 1' and contains three sections: 'Action performed' (with a dropdown menu), 'Date and time' (showing '2024-05-16 4:46 PM'), and 'Description of attack and used vulnerability (or CVE)' (with a large text input field and a 'Preview' button). A note at the bottom states 'Markdown and embedded images are supported'.

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

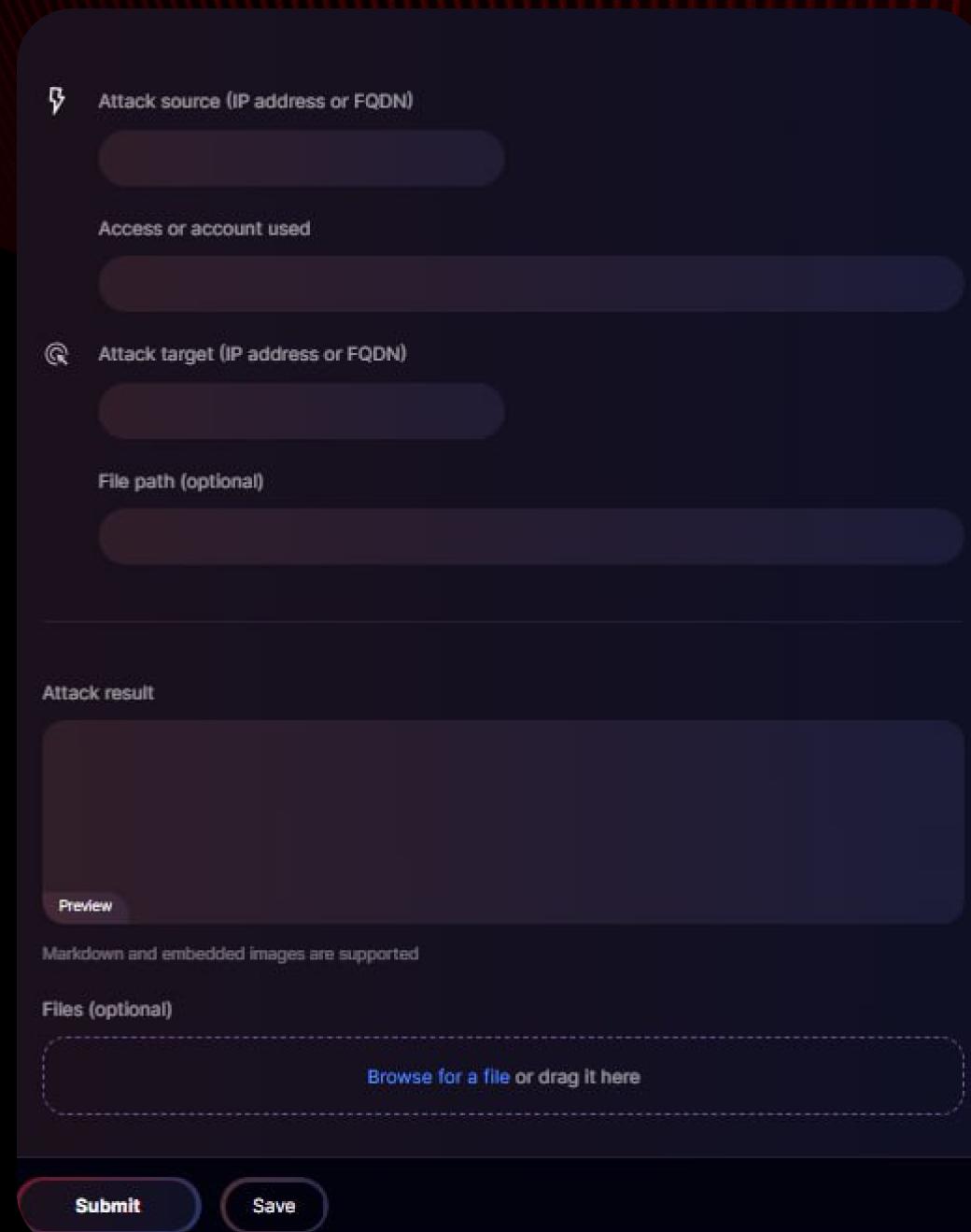
Use complete sentences to make each step a clear, reproducible sequence

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



The screenshot shows a dark-themed web form for reporting a critical event. The fields include:

- Attack source (IP address or FQDN)
- Access or account used
- Attack target (IP address or FQDN)
- File path (optional)
- Attack result
- Preview (with a note: Markdown and embedded images are supported)
- Files (optional) (with a browse/drag-and-drop input field)

At the bottom are "Submit" and "Save" buttons.

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

The diagram illustrates three user accounts connected by 'MemberOf' relationships:

- SRV_ADMIN@UF.CITY.STF
- M_DONOVAN_ADMIN@UF.CITY.STF
- L_WEBSTER_ADMIN@UF.CITY.STF

Relationships:

- SRV_ADMIN@UF.CITY.STF is connected to M_DONOVAN_ADMIN@UF.CITY.STF via a 'MemberOf' relationship.
- SRV_ADMIN@UF.CITY.STF is connected to L_WEBSTER_ADMIN@UF.CITY.STF via a 'MemberOf' relationship.
- M_DONOVAN_ADMIN@UF.CITY.STF is connected to L_WEBSTER_ADMIN@UF.CITY.STF via a 'MemberOf' relationship.

The screenshot shows a network graph with nodes representing users and edges representing 'MemberOf' relationships. The nodes are labeled with their respective email addresses. The edges are blue lines with the label 'MemberOf' written above them. The background is dark, and the nodes are white circles with black icons.

The screenshot displays a list of user credentials in a table format. The columns include Request, Payload, Status code, Error, Timeout, Length, and Comment. The 'Payload' column lists various passwords such as 'password', 'iloveyou', 'princess', etc. The 'Status code' column shows mostly 302. The 'Length' column shows values like 531. The 'Comment' column is empty. Below the table, a POST request is shown in raw JSON format. The 'destination' field contains a URL with redacted sensitive information.

Request	Payload	Status code	Error	Timeout	Length	Comment
0		302			531	
1	password	302			531	
2	iloveyou	302			531	
3	princess	302			531	
4	rockyou	302			531	
5	nicole	302			531	
6	abc123	302			531	1609
7	daniel	302			531	
8	babygirl	302			531	
9	12345	302			531	
10	pa\$\$word	302			531	
11	monkey	302			531	
12	lovely	302			531	
13	jessica	302			531	
14	michael	302			531	
15	ashley	302			531	
16	qwerty	302			531	
17	iloveu	302			531	
18	michelle	302			531	
19	tigger	302			531	
20	test	302			531	
21	sunshine	302			531	
22	chocolate	302			531	
23	soccer	302			531	

Request: POST /owa/auth_owa HTTP/1.1
Host: exchange.energy.stf
Cookie: PrivateComputer=true; PBack=0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 158
Origin: https://exchange.energy.stf
Referer: https://exchange.energy.stf/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fexchange.energy.stf%2fowa%2f
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive
destination=https%3A%2F%2Fexchange.energy.stf%2Fowa%2F&flags=4&forcedownlevel=0&username=energy.stf%5C0_Gregory&password=abc123&passwordText=&isUtf8=1

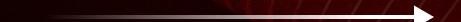
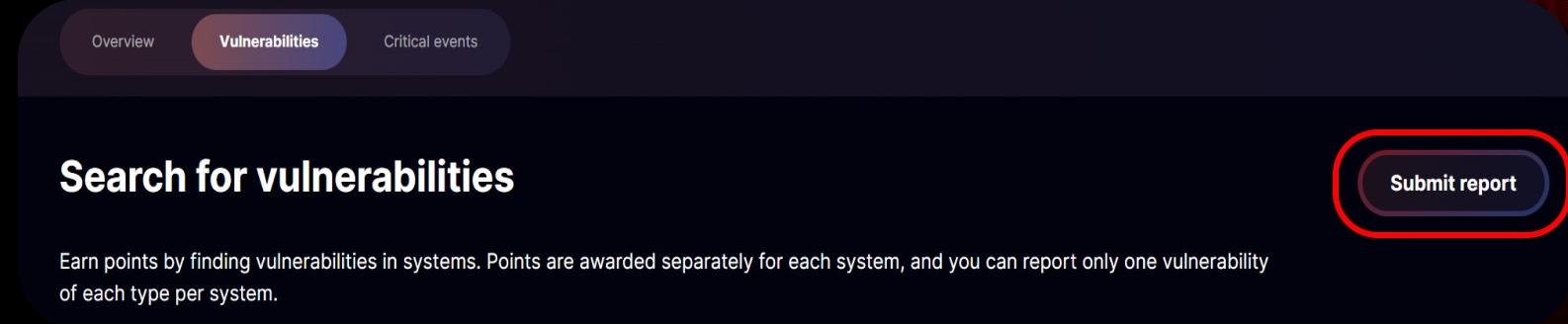
C:\Users\0_Personal\Downloads\Pictures\pseudoransomware_c7f9f656cd>ransomware.exe
The system is encrypted successfully!
Success!

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.



The screenshot shows a 'Vulnerability report' form. At the top, it says 'Reports' and 'Vulnerability report' with a 'Draft' status. The form has fields for 'Attack target (IP address or FQDN)' and 'Vulnerability type'. Below that is a large text area for 'Vulnerability description'. Underneath is a 'Preview' section with a note about Markdown support. At the bottom, there's a 'Files (optional)' section with a placeholder 'Browse for a file or drag it here'. At the very bottom are 'Submit' and 'Save' buttons.

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.

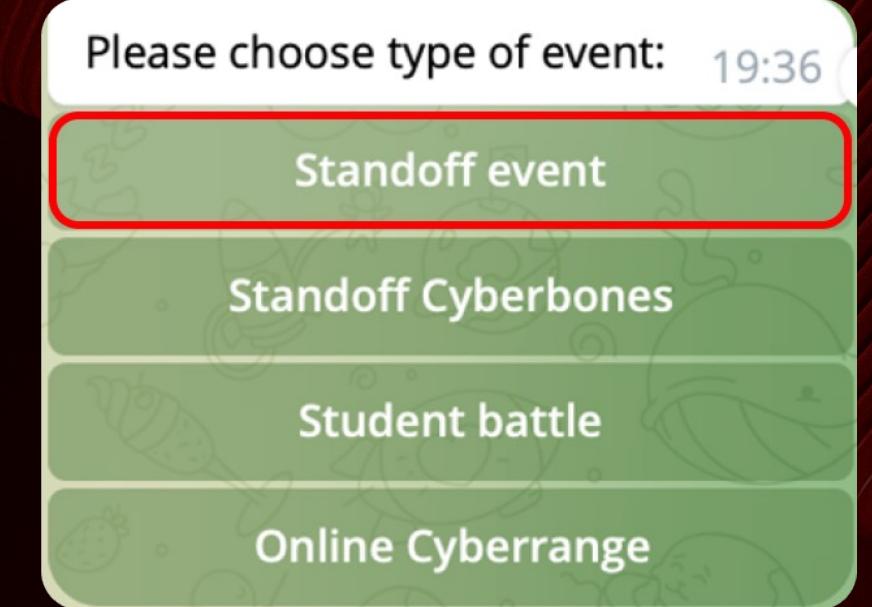
There you will also be able to see all your tickets, switch between them and provide information requested by the technical support team https://t.me/red_team_support_bot

What can this bot do?

Hey there!

As a Standoff support bot for attackers, we're here to assist you in every way possible.

Simply create a request and we'll be there for you!



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

