BLUE TEAM PACKET

THANK YOU TO OUR SPONSORS!

Diamond

EATON

SecurityRisk ADVISORS

Platinum

BATTELLE

FM

ICR Ideas, Commitment, Results

Amplify.

Gold

AMERICAN EXPRESS

M&T Bank

RESEARCH INNOVATIONS

MAGNET FORENSICS®

Miscreants®

Sharad Khanna

Silver

WINGSOVER

MINDEX

LOCKHEED MARTIN

Educational

bugcrowd

MetaCTF

no starch press

FORTRA™

Historical Timeline Taskforce & Protection (HTTP) Employee Memo

Dear employees of the Historical Timeline Taskforce & Protection (HTTP),

I reach out to you today in the midst of complete and total chaos. Our intelligence analysts have picked up evidence that events all across the timeline are rapidly being changed. With this information, our analysts have also found proof that these despicable acts are being carried out by none other than the notorious timeline terrorists, the Hourglass Inversion. We knew the day would come where they would execute their grand plan, and that day is today.

As the best in the business, I am personally reaching out to you, the HTTP field agents, to inform you that for the duration of this incident, HTTP will be all hands on deck. We are monitoring the timeline for changes as they arise. You will be responsible for traveling to and restoring those events to return the timeline to its original state. This is the moment you have been working for, so jump in your time machine and save the world as we know it.

We hold the line so the line continues on,
HTTP CEO

Please read on for more important information

Teams

Blue Team:

This is you! You are a field agent at HTTP. Your job is to travel through time and repair events as they are altered, restoring the timeline. You can accomplish this by keeping your services up as long as possible throughout the comp. However, don't forget about post mission reports (injects) assigned to you throughout the competition. At the end of the competition, you will also complete an Incident Response Report on what you found out in the field (in your network).

Red Team:

With the motto, "Sands fall where we decide," the Hourglass Inversion is a group notorious for travelling through time and altering events in whatever way they see fit. To prevent Red Team from destroying the timeline, try your best to keep them out and reverse any damage done.

White Team:

White Team are the analysts at HTTP. They are there to help facilitate communication between you and the HTTP higher ups (Black Team), assist with mission critical support (store purchases), and analyze post mission reports (grade injects). They keep the HTTP running smoothly while you are away on missions.

Black Team:

Black Team are the higher-ups at HTTP. They put this whole thing together and they intend to keep the HTTP going strong. HTTP higher-ups are known to step in if there are critical issues, and may be contacted by analysts (White Team) when additional support is needed.

Rules

These are the rules of IRSeC. Any breaking of the rules or intentional/deliberate attempts to skirt around or bypass them in any way will result in either a point deduction or disqualification of the team responsible. These are subject to change and we will let you know if any do change or are added.

1. Be respectful to all involved with the competition.
2. This competition exists for fun and learning- DO NOT break the spirit of the competition.
3. The White and Black Teams exist to help you. DO NOT attempt to deceive, mislead, or lie (including by omission) to either.
4. You must follow any directive issued to your team by the White Team or Black Team, verbal or in writing.
5. NEVER impersonate a Sponsor, White Team, or Black Team member. This includes but is not limited to any White Team users or credentials, both found or created to mimic White Team.
6. NEVER perform any competition related actions outside of "Hands On" periods. Hands on periods will be clearly communicated by White and Black teams, including when they may differ from the schedule.
7. Only registered blue team members may contribute to your team's work during the competition.
    a. Chaperones/Coaches are NOT permitted to coach, instruct, or guide your team in any way.
8. DO NOT attack out of scope infrastructure.
    a. In Scope- where "X" is your team number (refer to topology)
        i. LAN-10.X.1.0/24 (All Team LANs)
        ii. CLOUD-192.168.X.0/24 (All Team CLOUDs)

Rules

b. Out of Scope
    i. 172.16.1.0/24- Management Network
    ii. 172.20.1.0/24
    iii. *.irsec.club
    iv. *.ritsec.cloud
    v. RITSEC or RIT Hardware (including desktops)
    vi. Any DataDog agent processes, DataDog users, (dd-agent) and any IP located here: https://ip-ranges.us5.datadoghq.com/
        1. Files located in the /etc/datadog-agent, C:\ProgramData\Datadog, and C:\Program Files\Datadog\ directories
        2. Users with datadog or dd-dog
    vii. ANYTHING NOT LISTED AS IN SCOPE IS OUT OF SCOPE

9. DO NOT block subnets through Firewall rules or ACLs. Individual IP blocking is permitted.
    a. Out of scope IP addresses may not be blocked.
10. Injects may be written and submitted on competition networks or on your physical host machine.
11. DO NOT change the scored topology without explicit permission from White Team. This includes changing any scored services or redirecting or changing how a check is scored in any way
12. DO NOT attack, destroy, or attempt to attack or destroy any RIT or RITSEC property. This includes physical infrastructure (computers, chairs, etc) and virtual infrastructure (attempting to access management networks, denial of service attacks, etc.)
13. NEVER exfiltrate artifacts from the competition network/virtual infrastructure. This explicitly includes any type of antivirus at all (Including windows defender).

Rules

   a. This includes but is not limited to VirusTotal, NoDistribute, AntiScan, competitors laptops, console access machines, etc.
   b. Screenshots of virtual infrastructure are allowed.
14. Prestaging or pre-baking is allowed. IRSeC 2025 is an incident response competition.
15. Black Team reserves the right to modify what is in scope, and the definition of "scope" at any time and for any reason. Proper notice will be given when and if this occurs.
16. Any tools used must be adequately tested in good faith first, outside of RITSEC infrastructure.
    a. DO notify White Team if any tools used behave in unexpected ways which may degrade the competition experience.
17. All tools deployed must be publicly accessible- you must be able to pass White Team or Black Team an unauthenticated link to any tools you deploy at any time.
18. Black Team reserves the right to add, remove, modify, or in any way change the rules listed in this document at any time, with timely notice

Scoring Breakdown

Component	Weight
Uptime	35%
Injects	35%
Incident Response Report	30%

Live scoring will be available to you throughout the competition. Uptime scores will be provided by Scorify (access to which is detailed below). Teams will have access to two dashboards within Scorify. The first dashboard shows all teams and which services are still scoring (green). The second dashboard will show your individual team's score checks and will provide debugging information regarding why the services are not currently scoring. More information and a demo will be presented before the competition begins.

Network Topology

Our analysts have determined that the Hourglass Inversion are tampering with the following events:

Scored Services

Hostname	IP Address	Operating System	Service	Scored
Time Machine	10.x.1.254	pfSense	Routing	No
Big Bang	192.168.x.1	Fedora 42	MySQL	Yes
Dino Asteroid	192.168.x.2	Ubuntu 24.04	Wazuh	No
Wright Brothers	192.168.x.3	Win. Serv. 2022	SMB	Yes
Moon Landing	192.168.x.4	Windows 10	IIS	Yes
Pyramids	10.x.1.1	Win. Serv. 2022	AD/DNS	Yes
First Olympics	10.x.1.2	Windows 10	WinRM	Yes
Silk Road	10.x.1.3	Windows 10	ICMP	Yes
Viking Raids	10.x.1.4	Debian 12	SSH	Yes
Enlightenment	10.x.1.5	Ubuntu 24.04	FTP	Yes
Chernobyl	10.x.1.6	Rocky 9	Docker(Apache)	Yes

Timeline

07:30 - 08:00	Check-in first floor of GCI
08:00 - 09:00	Keynote in Conference Rooms
09:00 - 09:30	Initial Access (Credentials Given)
09:30 - 12:00	First Half of the Competition
12:00 - 13:00	Lunch
13:00 - 17:00	Second Half of the Competition
17:00 - 18:00	Incident Response Report
18:00 - 18:30	Break
18:30 - 19:00	Red Team Debrief
19:00 - 19:15	Final Scores and Prize Ceremony

** You will be notified by the CA when you are able to access the competition infrastructure

USERS

Domain Users

Administrators:

fathertime
chronos
aion
kairos

Local:

merlin
terminator
mrpeabody
jamescole
docbrown
professorparadox

Local Users

Administrators:

drwho
martymcFly
arthurdent
sambeckett

Local:

loki
riphunter
theflash
tonystark
drstrange
bartallen

Competition Access

During the competition, you will have access to your team's LAN environment via our in-house tool, Compsole. Before the competition begins, you will be given credentials to access Compsole. Along with Compsole, you will also have access to Scorify and the store with the following links:

Compsole: compsole.ritsec.cloud
Scorify: scoring.irsec.club
Store: store.irsec.club

Credentials for the services listed above will be given before the beginning of the competition. Service uptime will be determined by Scorify automatically. At any time during the competition, White Team may perform a manual service check to ensure that services are functioning properly. If a team is found to have taken measures to fraudulently pass service checks, points will be deducted from the team's score during final calculations at the discretion of White Team. More information regarding the store is given below.

Injects and The Final Incident Response Report

Injects:

While your network is under attack, you will be given several tasks to complete. All injects will be released via sheets of paper handed out by our Injects Lead, who is on Black Team at various points in the competition. Each inject will have its submission deadline, task, and grading rubric/weight on it.

Incident Response Report:

At the end of the competition, you will be asked to compile a report of all the obstacles that you have encountered. Make sure to keep an eye out for anomalous activity within your network as this means that the Hourglass Inversion have successfully altered the timeline (intruded your infrastructure). Take note of anything that you believe is evidence of an intrusion.

Submissions:

In order to submit an inject or the Incident Response Report for grading by White Team, you must upload a pdf file to Scorify before the deadline.

Store:

The following actions will supply you with credits to spend at the store:

- -Injects
- -Challenges