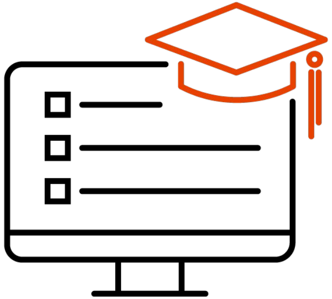
SIMSPACE

February 18, 2025

Cyber Cup 2025 Familiarization Session

Overview



- Purpose of Portal Familiarization Period
- Event Schedule
- Event Objectives
- Participating Teams
- Rules of Engagement
- Comms Channels
- Network Topology
- Portal Demo
- Range and Tool Tour

Portal Familiarization Session

What: Blue Team Familiarization Period

When: **Session 1 -** Tuesday (Feb 18th) at 4:00 PM Eastern Time
Session 2 - Thursday (Feb 20th) at 10:00 AM Eastern Time
Ends - Range access will end Monday (Feb 24th) at 5:00 pm Eastern Time

Where: SimSpace Portal → Live Action Event: **Cyber-Cup-Blue-Feb25-***

How: Complete the Pre-Event Checklist, verify portal & chat account logins, access and verify functionality of network security tools using a virtual hunt machine in the range, ask questions

Why: To prepare for the February 27th Competition

Execution Schedule

Time (ET)	Topic
9:30 - 10:00 AM	Login and Comms Checks
10:00 - 10:30 AM	Event Intro and Overview
10:30 AM	**Fight's ON**
10:30 AM - 1:30 PM	3 Hours of Interactive Challenges
1:30 PM	**Fight's OFF**
1:30 - 2:00 PM	Awards and Closing Remarks

Event Objectives

- Develop personal relationships between cyber security professionals
  - Friendly competition between participating teams
  - Virtual social interaction opportunities

- Potential learning opportunities
  - Learning moments during the exercise
  - Cross-team teaching moments

- Build upon best practices
  - Practice “a bad day” in a safe environment
  - Try new tactics, techniques, and procedures

Participants in Each Blue Team

1	2	3	4	5
Blue Team 1	**Xcaliber**	**Blue Team 3**	**#0000FF UwUers**	**Cyber Bucs**
Adam Hust	Jack Frambes	Jonathan Styles	Jonathan Beierle	John Liebenguth
Danny Pradia	Cooper Landen	Cooper Wiendl	Matthew Schramm	John Garcia
Scott Felch	Deep Ram	Andy Pompura	Jacob Acuna	Sandy Ruiz
Derick Morrow	Luke Stalbaum	Ardian Peach	Corey Burton	Elijah Fraley
Mason Prince	Julian Brito	Anthony Marrongelli	Fardeen Bjimani	Nathan Kloster
Dmitriy Massip	Ajay Jackson	Logen Autry	Vincent Dinh	
	Samuel Kadima	Martin Roberts	Dominic Baldassari	
	Cory Shaefer	Rodrigo Almeida Santos	Dylan Davis	

Participants in Each Blue Team

6

The Firewall Five

Ethan Weyer

Muhammad Essa

Tenzing Gurung

Ihor Makhynia

Darpan Basnet

7

Anbu Cyber

Timothy Kircher

Alessandro Lovadina

Jason Doan

Thiago Ries Pagliaroni

Isaac Ward

8

Cyber Runners

Joshua Gray

Vincent Knight

Aros Ontiveros

Julian Pena

Preston McKnight

Corrina Alcoser

John Yanez

9

null NEU

Pratik Mody

Samyukta Kurikala

Rahul Sharma

Tanmay Sharma

10

Blue Team 10

Dhanish Patil

Treson Mariotti

Mason Miller

Matthew Chan

Participants in Each Blue Team

11

Blue Team 11

Owen Dransfield

Asa Reynolds

Richard Joyce

Yash Parmar

Kekoa Merez

Tyler Clark

Ryan Zanoni

Winston White

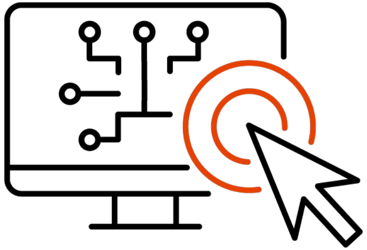
Rules of Engagement

Defenders

Your goal is to defend your network through detection and reporting

- Report what you see
  - Processes? Ports? Hosts? Files? Paths? DLL? ...use details
- Document change requests in Defender Logs
  - Think ITIL change process
- Don’t fight the range
  - The Control Cell will intervene if we determine that you are focusing on an artifact-of-simulation rather than the scenario
- Standard baselining and network analysis tactics will help you achieve this focus
  - Try to connect anomalous network traffic you detect to the hosts and processes generating that traffic; determine both network and host indicators of compromise

Rules of Engagement



Sim Users and Range

The range emulates users and their typical behaviors

- These users will:
  - Click links, open emails, browse the web, and work in various desktop office applications
  - Occasionally attempt to connect devices, install software, run nonstandard applications, and connect to various services
  - Complain if their services break
- Security Patching:
  - Updated security patches will not be applied during this event
  - The risk of zero-day vulnerabilities or other network hygiene related matters remain a potential risk

Rules of Engagement

Out of Bounds

- The following items related to range control and range support are out-of-bounds for both the Threat and Defender Teams:
    - **10.10.0.0/16** is the **Range Control network**. This network is used to administer the range and is only available to the Control Cell.
        - The threat will not use this network.
        - **Do not block** access to this network. Do not create any firewall rulesets other than allow any to any for this IP range.
    - Default SimSpace accounts are out-of-bounds and will not be used by the Threat Team.

Rules of Engagement

Out of Bounds

- The following processes are part of range support and should not be the focus of forensics efforts. The Threat Team will not use or inject into these processes:
  - Puppet
    - Software or files located in **C:\ProgramData\PuppetLabs**
    - Software or files located in **C:\Program Files\Puppet Labs**
    - Software or files located in **C:\ProgramData\staging**
    - Ruby
  - User Emulation
    - Software or files located in **C:\Program Files (x86)\Simspace**
    - **java.exe** listening/communicating on ports **49999, 49998, 5762, 15672, & 27017**
    - **amqp** listening on port **5672**
  - Other
    - **systeminit.exe** and all related files to this binary

Communications Channels

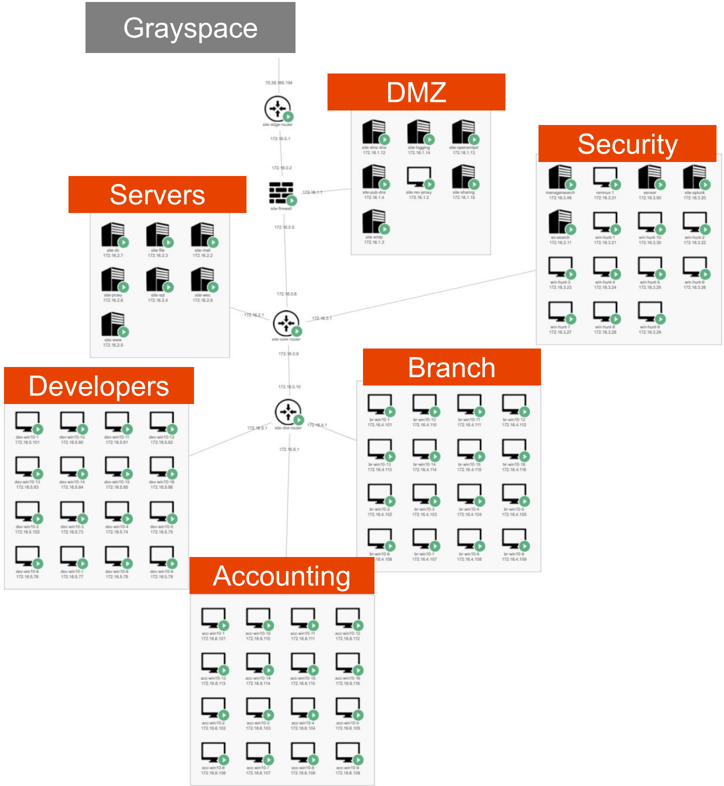
- Defender Logs – official channel of record in event **Cyber-Cup-Blue-Feb25-*** within the SimSpace portal
  - <u>Document and track</u> any adversary observations – the more the detail, the quicker the response, the better the event
    - **Main criteria for gaining points**
  - Request information from Control Cell for items not present within the exercise

- Mattermost Chat – **unofficial** communication channel
  - Items on interest to others on the team, exchange of data/ideas
  - Interesting observations but not yet determined as “bad”
  - **For login, Mattermost chat uses all lower case on the email address**

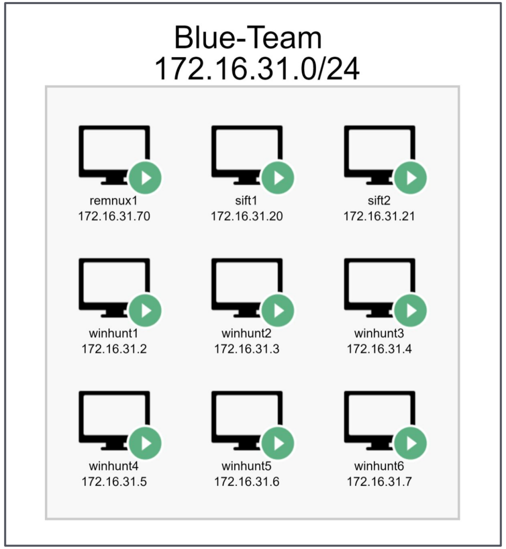
- Zoom – Event open communications channel
  - Used for welcome, checks, pre-brief, live engagement period, and closing remarks
  - Another unofficial communication channel
  - Each team will also have a Zoom breakout room for voice comms is needed

Topology

Shared Attack Segment



Team Access



Tools in Range

Splunk and Security Onion are the two SIEMs that will be available to query the following logs:

- Zeek
- Suricata (IDS)
- Windows Event Logs
- System
- Security
- Application
- PowerShell
- Sysmon
- Squid Proxy Logs

Demonstration

Portal

- Landing page
- Accessing the Event
- Event Documents
- Defender Logs
- Mattermost
- Other useful items

Network Topology & Security Tools

- Opening a console
- Tool access
- File Management

Contacts & Questions

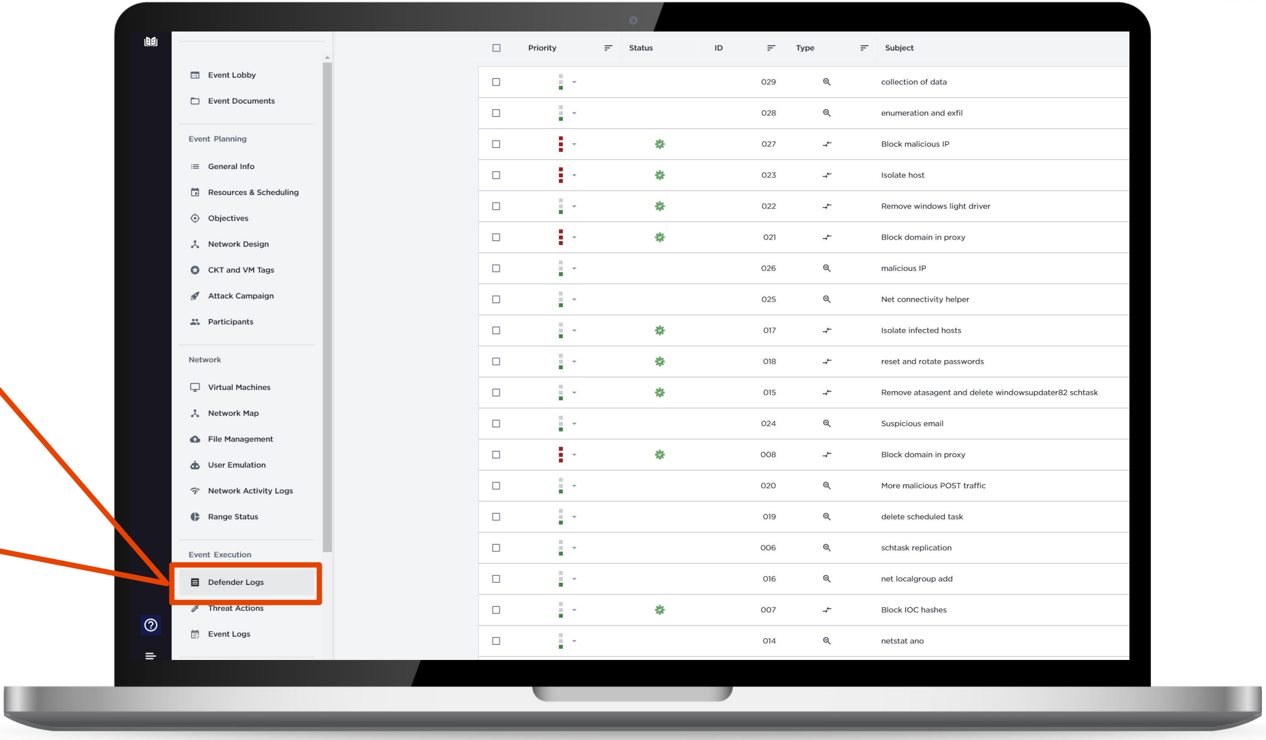
If you have any questions later during the Familiarization Period, please don’t hesitate to contact us!

SimSpace: support@simspace.com

Defender Logs – Simplified Ticketing System

- Defender Logs are records captured by blue team (defenders) during a live action event.

- The blue team records and organizes its actions, enabling these members to successfully combat the red team (attackers/adversaries) by coordinating information as it becomes available during a real-time live action event.



□	Priority	Status	ID	Type	Subject
□	🟩		029	🔍	collection of data
□	🟩		028	🔍	enumeration and exfil
□	🟥	✓	027	⇄	Block malicious IP
□	🟥	✓	023	⇄	Isolate host
□	🟩	✓	022	⇄	Remove windows light driver
□	🟥	✓	021	⇄	Block domain in proxy
□	🟩		026	🔍	malicious IP
□	🟩		025	🔍	Net connectivity helper
□	🟩	✓	017	⇄	Isolate infected hosts
□	🟩	✓	018	⇄	reset and rotate passwords
□	🟩	✓	015	⇄	Remove atasagent and delete windowsupdater82 schtask
□	🟩		024	🔍	Suspicious email
□	🟥	✓	008	⇄	Block domain in proxy
□	🟩		020	🔍	More malicious POST traffic
□	🟩		019	🔍	delete scheduled task
□	🟩		006	🔍	schtask replication
□	🟩		016	🔍	net localgroup add
□	🟩	✓	007	⇄	Block IOC hashes
□	🟩		014	🔍	netstat ano

Defender Logs – Three Types of Logs

Tracking Items

- A record used to monitor the progress of ongoing tasks, incidents, investigations, or anomalies detected within the security environment.
- It serves as a central point for tracking the resolution of a security event.
- If, during investigation, a need for a system or policy modification is identified, a change request can be generated directly from the tracking item to initiate the necessary updates.

Change Request

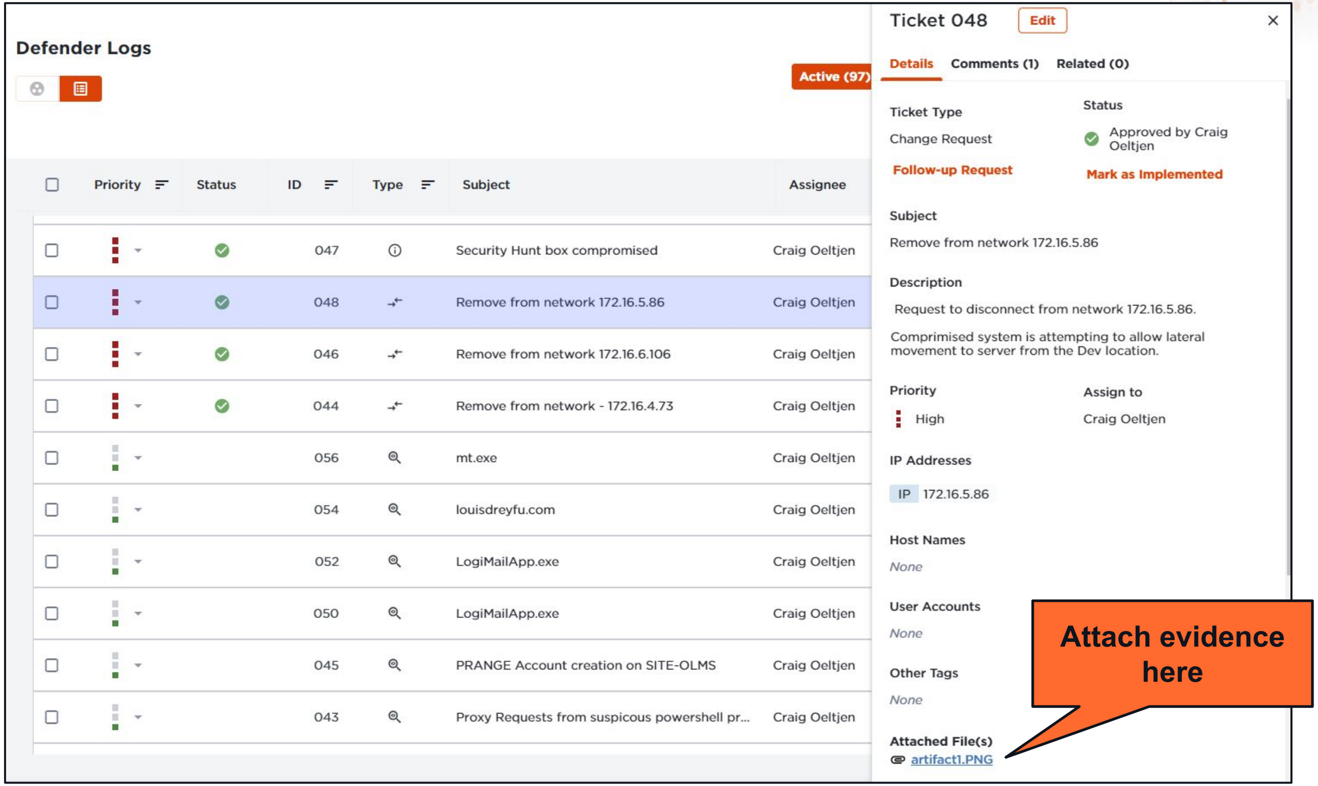
- A formal request to modify or update security systems, policies, or configurations to improve security posture or address identified vulnerabilities.
- This could involve firewall rule adjustments, software patching, or changes to security group policies.
- Change requests follow a defined approval process to ensure security and minimize risks before implementation

Request for Information

- A query submitted to obtain additional details, data, or clarification related to an ongoing investigation, security policy, or operational procedure.
- Information requests often seek logs, incident timelines, or threat intelligence to support decision-making or further investigation.
- Responses to these requests help ensure the team has the data needed to perform thorough analysis and remediation.

Defender Log Example - Change Request

- Ticket created to remove a compromised host from the network.
- Evidence, such as a screen shots, can be attached in support of tickets.



Defender Logs

Active (97)

□	Priority	Status	ID	Type	Subject	Assignee
□		✓	047	ⓘ	Security Hunt box compromised	Craig Oeltjen
□		✓	048	⇄	Remove from network 172.16.5.86	Craig Oeltjen
□		✓	046	⇄	Remove from network 172.16.6.106	Craig Oeltjen
□		✓	044	⇄	Remove from network - 172.16.4.73	Craig Oeltjen
□			056	🔍	mt.exe	Craig Oeltjen
□			054	🔍	louisdreyfu.com	Craig Oeltjen
□			052	🔍	LogiMailApp.exe	Craig Oeltjen
□			050	🔍	LogiMailApp.exe	Craig Oeltjen
□			045	🔍	PRANGE Account creation on SITE-OLMS	Craig Oeltjen
□			043	🔍	Proxy Requests from suspicous powershell pr...	Craig Oeltjen

Ticket 048 Edit ×

Details | Comments (1) | Related (0)

Ticket Type
Change Request

Status
✓ Approved by Craig Oeltjen

Follow-up Request

Mark as Implemented

Subject
Remove from network 172.16.5.86

Description
Request to disconnect from network 172.16.5.86.

Comprimised system is attempting to allow lateral movement to server from the Dev location.

Priority
High

Assign to
Craig Oeltjen

IP Addresses
IP 172.16.5.86

Host Names
None

User Accounts
None

Other Tags
None

Attached File(s)
artifact1.PNG

Attach evidence here

SIMSPACE