ERAU & A-ISAC CTF: Raising Awareness about Aviation Cybersecurity

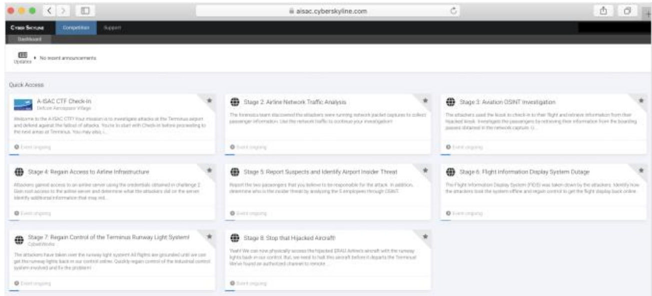
Prof. Jesse Chiu, Dr. Krishna Sampigethaya

Cyber Intelligence and Security Department

Embry-Riddle Aeronautical University–Prescott Campus (NCAE-CDE)

ERAU's Aviation Cyber CTF Facts

- ERAU is the NSF SFS institution for aviation and aerospace cyber security
- Aviation Information Sharing and Analysis Center (ISAC) sponsorship
- The first-ever virtual aviation cyber competition!
- Offered at AIAA, DEF CON, WiCyS, and other venues in 2020-2022
- Offered for free globally!



No recent announcements

Quick Access

A-ISAC CTF Check-In
Defcon Aerospace Village
Welcome to the A-ISAC CTF! Your mission is to investigate attacks at the Terminus airport and defend against the fallout of attacks. You're to start with Check-In before proceeding to the next areas at Terminus. You may also, i...
Event ongoing

Stage 2: Airline Network Traffic Analysis
[illegible]
Event ongoing

Stage 3: Aviation OSINT Investigation
[illegible]
Event ongoing

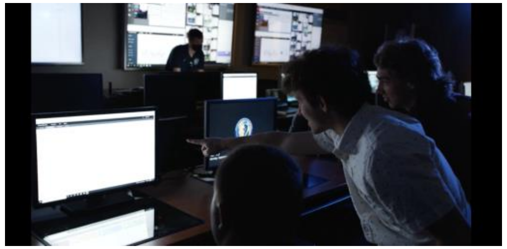
Stage 4: Regain Access to Airline Infrastructure
[illegible]
Event ongoing

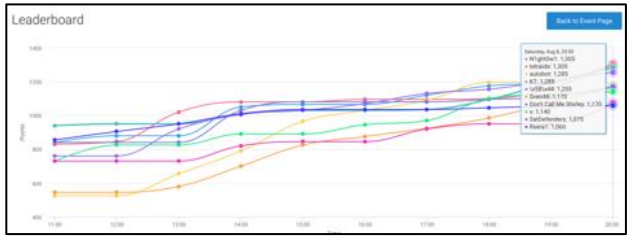
Stage 5: Report Suspects and Identify Airport Insider Threat
[illegible]
Event ongoing

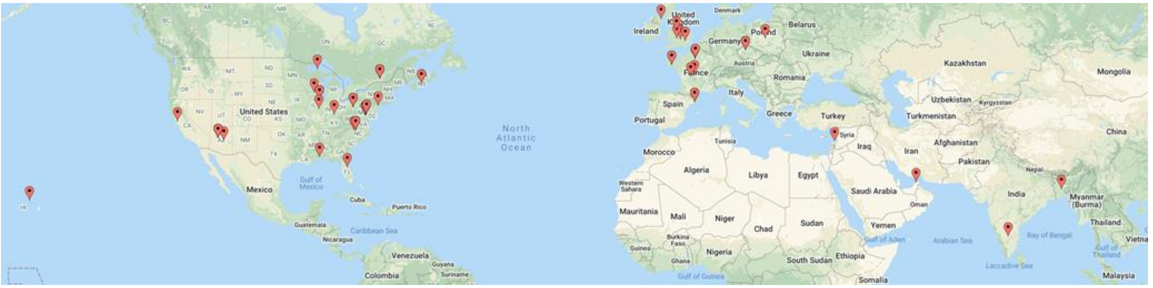
Stage 6: Flight Information Display System Outage
The Flight Information Display System (FIDS) was taken down by the attackers. [illegible]
Event ongoing

Stage 7: Regain Control of the Terminus Runway Light System!
[illegible]
Event ongoing

Stage 8: Stop that Hijacked Aircraft!
[illegible]
Event ongoing







ERAU’s Aviation Cyber CTF Objectives

- A competition that:
  - Builds educational awareness about aviation cybersecurity
  - Motivates talent in aviation cybersecurity
  - Shows cybersecurity assisting in aviation security incident response
  - Promotes the role of Aviation ISAC as an enabler in this subject area

ERAU’s Aviation Cyber CTF Overview

- Cyberattacks at a Tier-1 airport have caused business disruptions and a hijack!
- Can you be a cyber defender and restore normal operations at this airport?

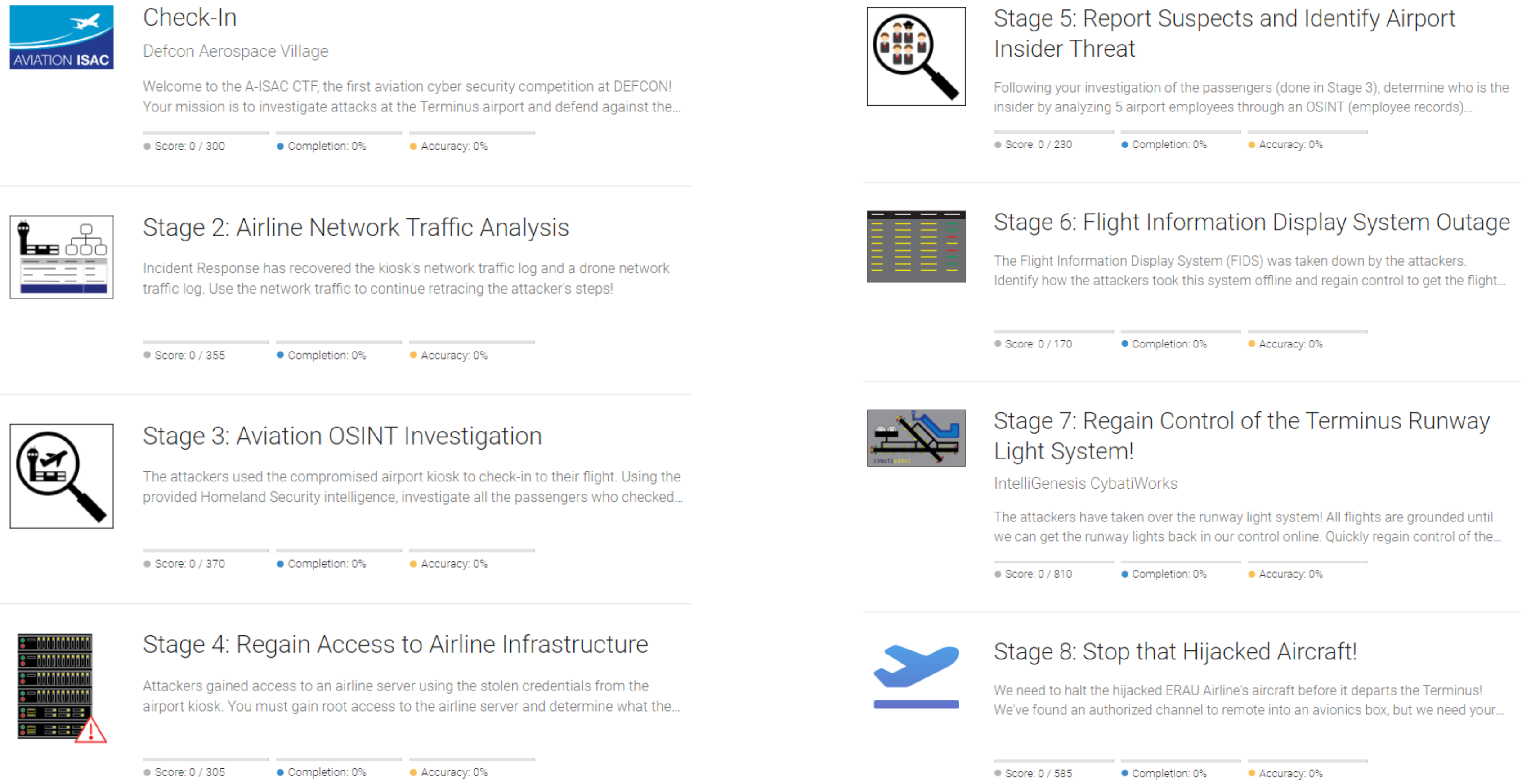
Hackers have hijacked an aircraft and compromised multiple systems at an airport! We need your help!

You must navigate the hackers trail through the airport. Help restore compromised systems.

Help regain control of the aircraft. Bring normalcy to airport operations. Hurry! You have 24 hours!

CTF Competition Challenges

EMBRY-RIDDLE
Aeronautical University
PRESCOTT, ARIZONA



Check-In

Defcon Aerospace Village

Welcome to the A-ISAC CTF, the first aviation cyber security competition at DEFCON! Your mission is to investigate attacks at the Terminus airport and defend against the...

Score: 0 / 300 Completion: 0% Accuracy: 0%

Stage 2: Airline Network Traffic Analysis

Incident Response has recovered the kiosk's network traffic log and a drone network traffic log. Use the network traffic to continue retracing the attacker's steps!

Score: 0 / 355 Completion: 0% Accuracy: 0%

Stage 3: Aviation OSINT Investigation

The attackers used the compromised airport kiosk to check-in to their flight. Using the provided Homeland Security intelligence, investigate all the passengers who checked...

Score: 0 / 370 Completion: 0% Accuracy: 0%

Stage 4: Regain Access to Airline Infrastructure

Attackers gained access to an airline server using the stolen credentials from the airport kiosk. You must gain root access to the airline server and determine what the...

Score: 0 / 305 Completion: 0% Accuracy: 0%

Stage 5: Report Suspects and Identify Airport Insider Threat

Following your investigation of the passengers (done in Stage 3), determine who is the insider by analyzing 5 airport employees through an OSINT (employee records)...

Score: 0 / 230 Completion: 0% Accuracy: 0%

Stage 6: Flight Information Display System Outage

The Flight Information Display System (FIDS) was taken down by the attackers. Identify how the attackers took this system offline and regain control to get the flight...

Score: 0 / 170 Completion: 0% Accuracy: 0%

Stage 7: Regain Control of the Terminus Runway Light System!

IntelliGenesis CybatiWorks

The attackers have taken over the runway light system! All flights are grounded until we can get the runway lights back in our control online. Quickly regain control of the...

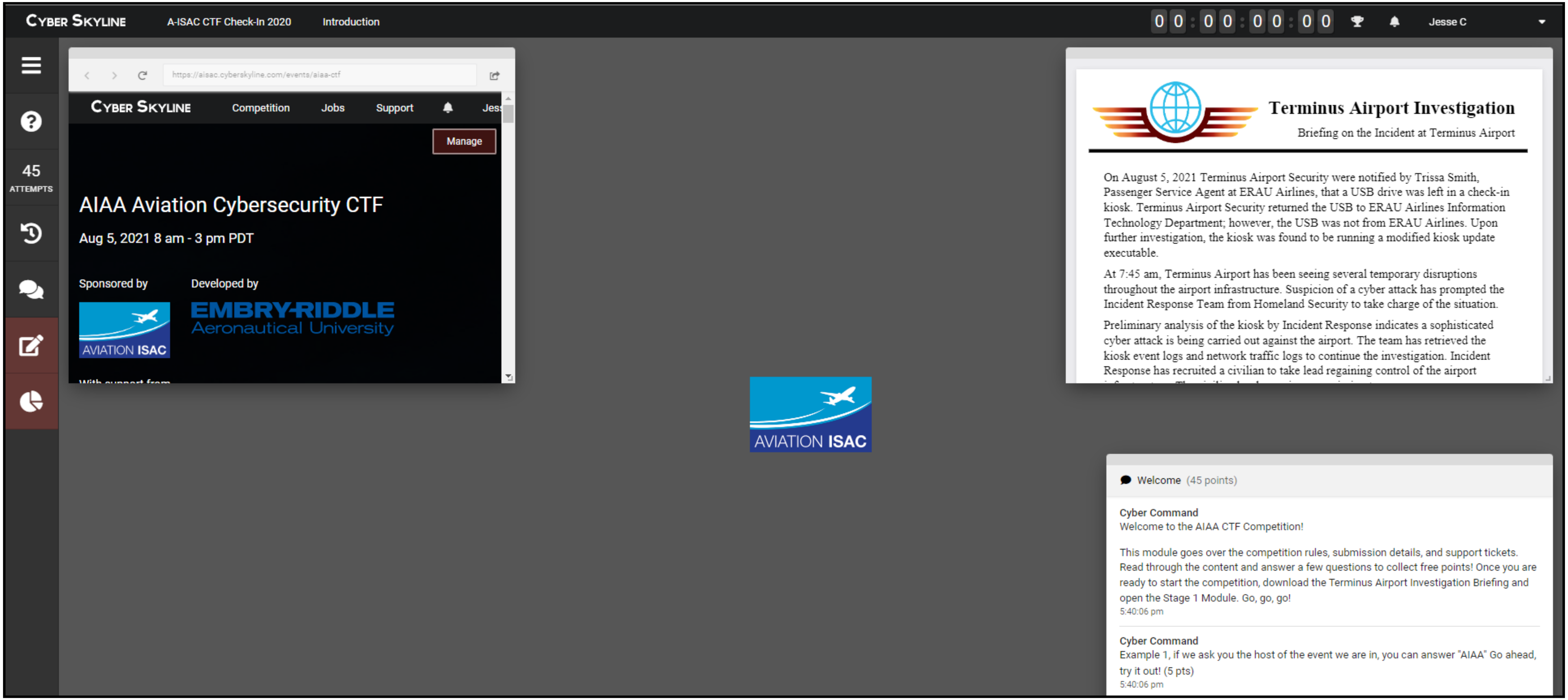
Score: 0 / 810 Completion: 0% Accuracy: 0%

Stage 8: Stop that Hijacked Aircraft!

We need to halt the hijacked ERAU Airline's aircraft before it departs the Terminus! We've found an authorized channel to remote into an avionics box, but we need your...

Score: 0 / 585 Completion: 0% Accuracy: 0%

- Participants are given authority for 24 hours and challenged to exercise their cybersecurity skills for: investigating hacking incidents at airport kiosks, airline networks/server, and airport database/displays; gather intelligence and identify attackers and insiders; regain control of a compromised runway light system and avionics of the hijacked aircraft.
- Participants also given opportunity to learn about aviation!



AIAA Aviation Cybersecurity CTF

Aug 5, 2021 8 am - 3 pm PDT

Terminus Airport Investigation

Briefing on the Incident at Terminus Airport

On August 5, 2021 Terminus Airport Security were notified by Trissa Smith, Passenger Service Agent at ERAU Airlines, that a USB drive was left in a check-in kiosk. Terminus Airport Security returned the USB to ERAU Airlines Information Technology Department; however, the USB was not from ERAU Airlines. Upon further investigation, the kiosk was found to be running a modified kiosk update executable.

At 7:45 am, Terminus Airport has been seeing several temporary disruptions throughout the airport infrastructure. Suspicion of a cyber attack has prompted the Incident Response Team from Homeland Security to take charge of the situation.

Preliminary analysis of the kiosk by Incident Response indicates a sophisticated cyber attack is being carried out against the airport. The team has retrieved the kiosk event logs and network traffic logs to continue the investigation. Incident Response has recruited a civilian to take lead regaining control of the airport

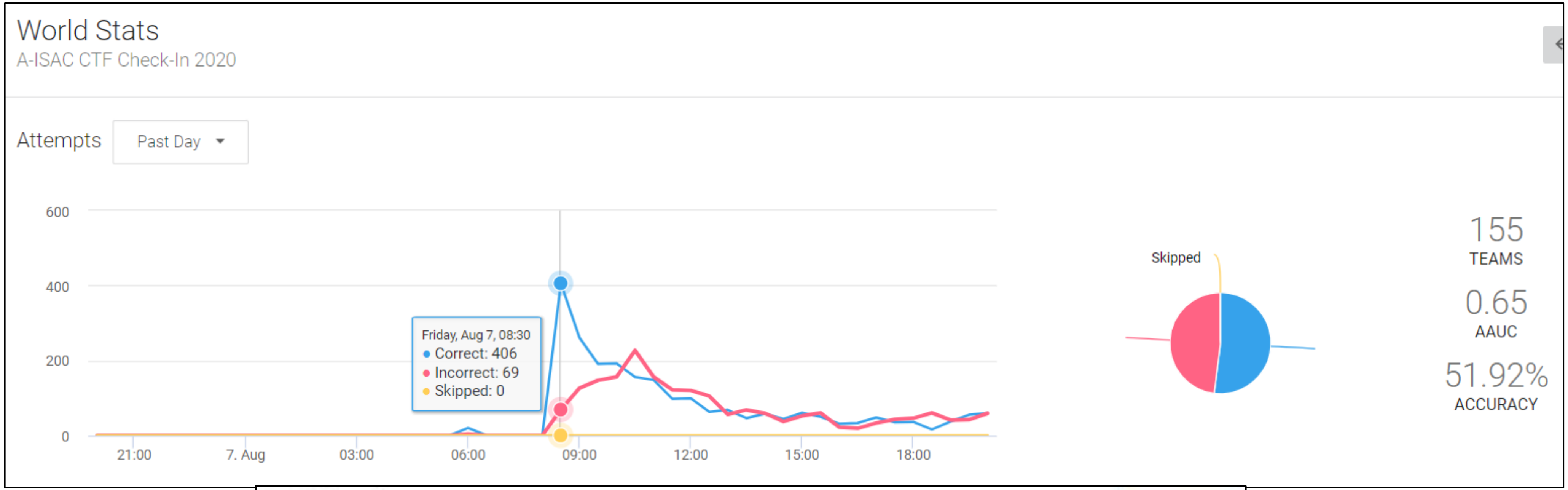
Welcome (45 points)

Cyber Command
Welcome to the AIAA CTF Competition!

This module goes over the competition rules, submission details, and support tickets. Read through the content and answer a few questions to collect free points! Once you are ready to start the competition, download the Terminus Airport Investigation Briefing and open the Stage 1 Module. Go, go, go!
5:40:06 pm

Cyber Command
Example 1, if we ask you the host of the event we are in, you can answer "AIAA" Go ahead, try it out! (5 pts)
5:40:06 pm

Cyber Skyline: Participant View



World Stats

A-ISAC CTF Check-In 2020

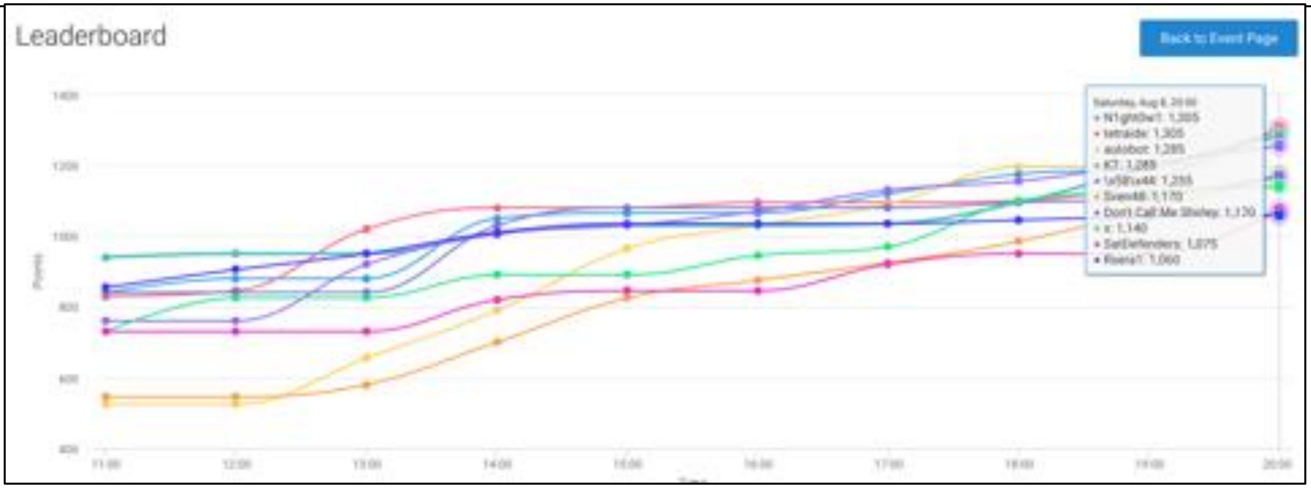
Attempts Past Day

Friday, Aug 7, 08:30
● Correct: 406
● Incorrect: 69
● Skipped: 0

155
TEAMS

0.65
AAUC

51.92%
ACCURACY

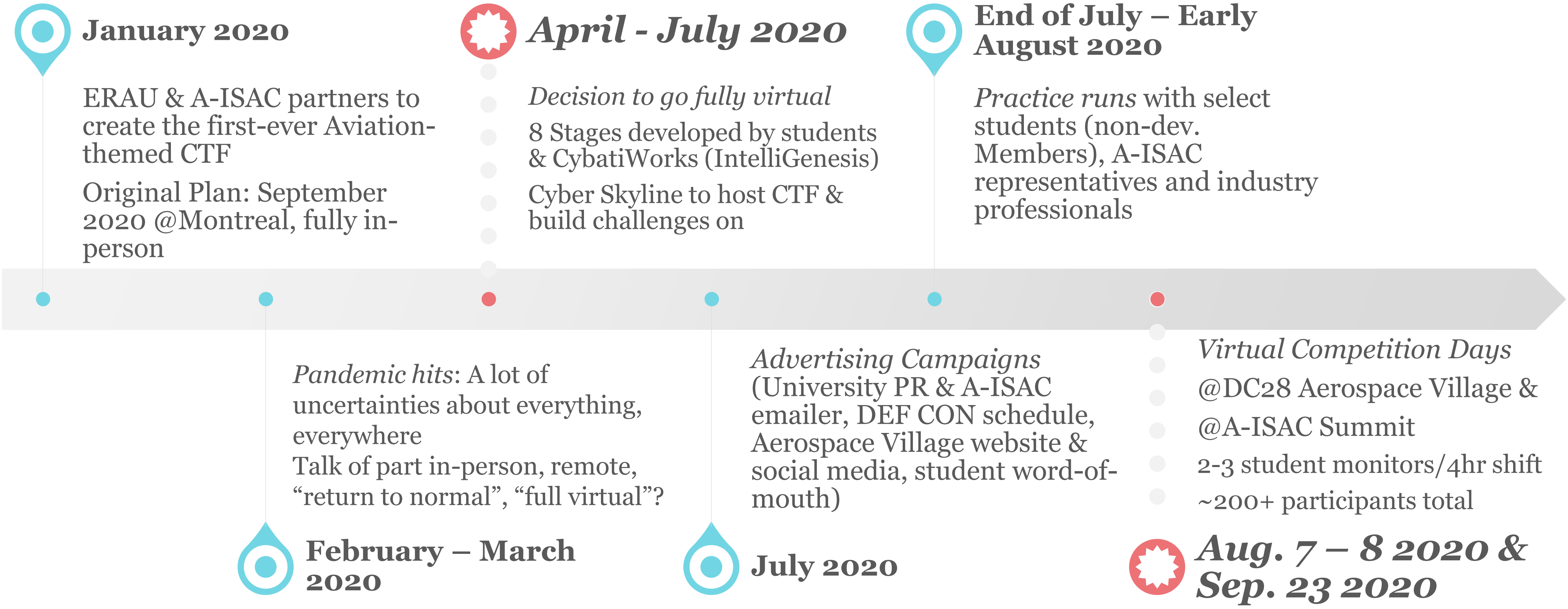


Leaderboard

Saturday, Aug 8, 20:00
• N1ghtOw1: 1,305
• tetraide: 1,305
• autobot: 1,285
• KT: 1,269
• \x58\x44: 1,255
• Sven88: 1,170
• Don't Call Me Shirley: 1,120
• x: 1,140
• SatDefenders: 1,075
• Rseria1: 1,060

Competition Day Stats

From Concept to Offering: 2020 Timeline



January 2020

ERAU & A-ISAC partners to create the first-ever Aviation-themed CTF

Original Plan: September 2020 @Montreal, fully in-person

February – March 2020

Pandemic hits: A lot of uncertainties about everything, everywhere
Talk of part in-person, remote, “return to normal”, “full virtual”?

April - July 2020

Decision to go fully virtual

8 Stages developed by students & CybatiWorks (IntelliGenesis)

Cyber Skyline to host CTF & build challenges on

July 2020

Advertising Campaigns (University PR & A-ISAC emailer, DEF CON schedule, Aerospace Village website & social media, student word-of-mouth)

End of July – Early August 2020

Practice runs with select students (non-dev. Members), A-ISAC representatives and industry professionals

Aug. 7 – 8 2020 & Sep. 23 2020

Virtual Competition Days

@DC28 Aerospace Village &

@A-ISAC Summit

2-3 student monitors/4hr shift

~200+ participants total

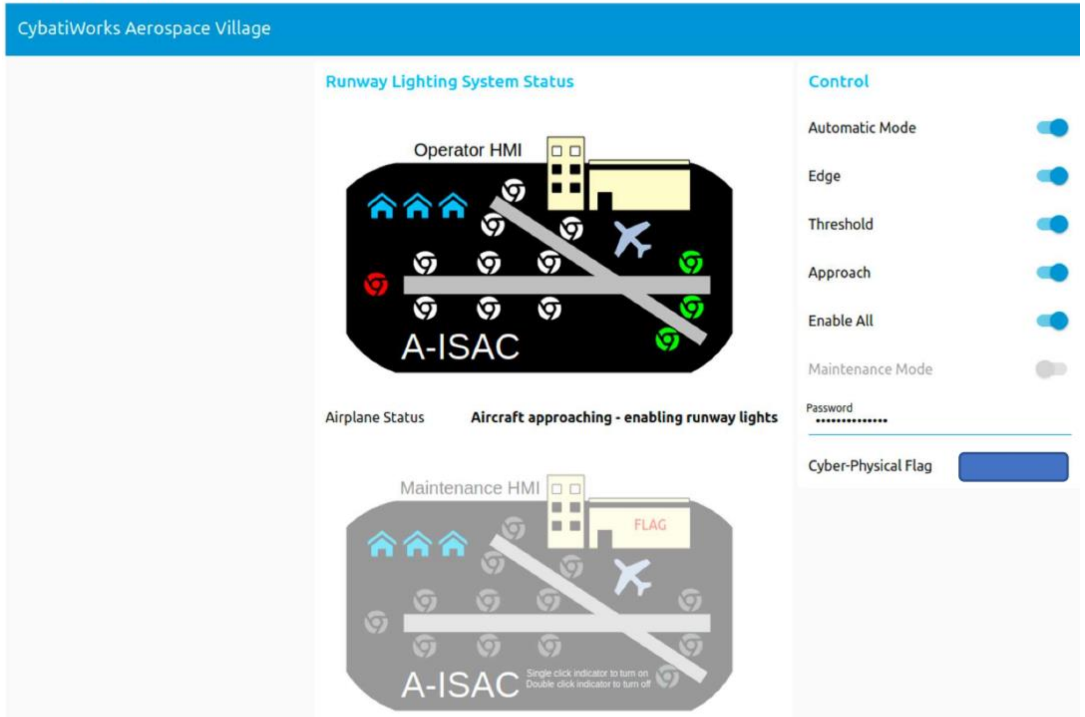
Lessons Learned: Flexibility & Creativity

Stay Flexible & Be Creative

In-person competition → "remote" & in-person → "fully virtual"

- Explored CTF hosting platforms that minimized overhead/workload
  - CTFd vs. Cyber Skyline
- All in-person challenges virtualized and/or made remotely accessible

Dashboard HMIs



CybatiWorks Aerospace Village

Runway Lighting System Status

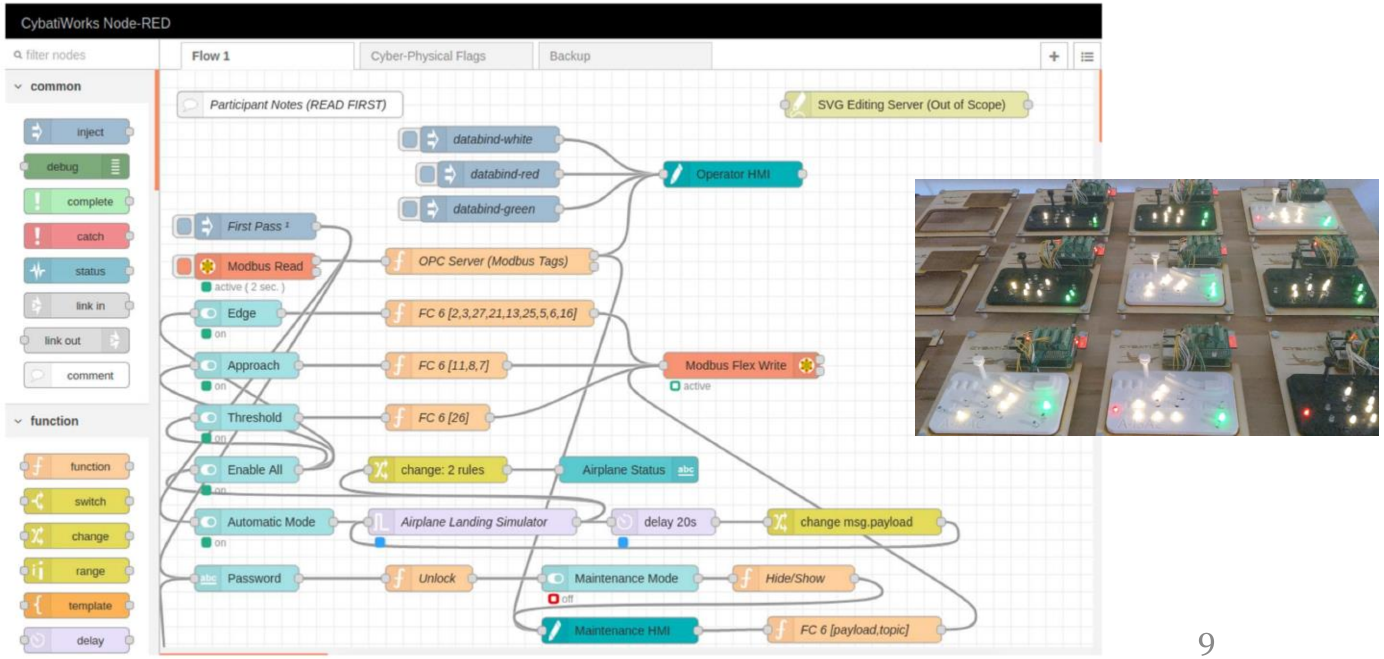
Operator HMI
A-ISAC
Maintenance HMI
FLAG
A-ISAC
Single click indicator to turn on
Double click indicator to turn off

Airplane Status: Aircraft approaching - enabling runway lights

Control

- Automatic Mode: on
- Edge: on
- Threshold: on
- Approach: on
- Enable All: on
- Maintenance Mode: off
- Password: ••••••••••••••
- Cyber-Physical Flag

Dashboard Logic



Lessons Learned: CTF Challenges

- Test, test, test….
  - Attention to detail was necessary
    - Question wording, minor configuration change in docker threw some contestants off
  - Unexpected issues came up (some due to contestants) even after multiple practice runs

- Improve flow of questions, stage locks, and scoring
  - Version 1.0 of the CTF had linear progression with stage locks (Stage 1 to Stage 2 to …)
  - Some participants lost focus after getting stuck, never to continue onto further challenges
  - Navigating between stages not intuitive, missed questions due to new UI & nested challenges
  - Stage 7 received very little attention due to its position despite its attractive challenges.

Lessons Learned: Partnerships

Formed Strong Partnerships that helped us greatly & react quickly

1. *Used a well-established CTF platform provider (Cyber Skyline)*

   We previously knew about the platform from NCL
   - Added advantage of students already familiar w/ platform from NCL

   No need to build, host and manage in-house large-scale CTF infrastructure
   - Received support on technical aspects & their experiences of hosting CTFs
   - question format, wording, layout, environment, etc…
     - a lot of headaches avoided upfront based on their lessons learned

2. *Advanced Level Qs by Industry Experts – Runway Lighting Challenges*
   - Simulated runway light challenges by IntelliGenesis (formerly CybatiWorks)
     - Challenge Part 1: Node-Red in docker hosted on Cyber Skyline
     - Challenge Part 2: Remotely access physical RPi controlling lights & bring the system back up

Lessons Learned: Partnerships

3. *Partnerships in Hosting & Promoting the CTF*

- University & A-ISAC
  - Departmental/college support
  - Promotions on official social media & newsletters
- Aerospace Village
  - Added the event on DEF CON schedule & CTF list
  - Promoted registration links on their website, twitter & LinkedIn
  - additional communication channel on Discord during competition day
- Students
  - A large majority of challenges developed by students
  - Word of mouth, provided feedback and beta tested challenges

Conclusions

- The first ever aviation-themed virtual Capture-the-Flag (CTF) competition
  - Created by ERAU w/ Aviation ISAC sponsorship
- 8 stages, 42 sections, 174 questions total
  - A wide range of topics covered
    - Digital Forensics, knowledge of aviation protocol (i.e. ARINC 429), password cracking, Linux admin, OSINT, aviation trivia, etc.
  - Hosted on a managed CTF platform (Cyber Skyline)
    - 230 participants at DEF CON 28 Safe Mode
    - 84 students, 28 teams at A-ISAC Collegiate CTF
- Developed by a dozen undergraduate students + 2 faculty & Cybatiworks (IntelliGenesis)
- Offered for free globally at multiple venues!

Thank you!
Questions/Comments?