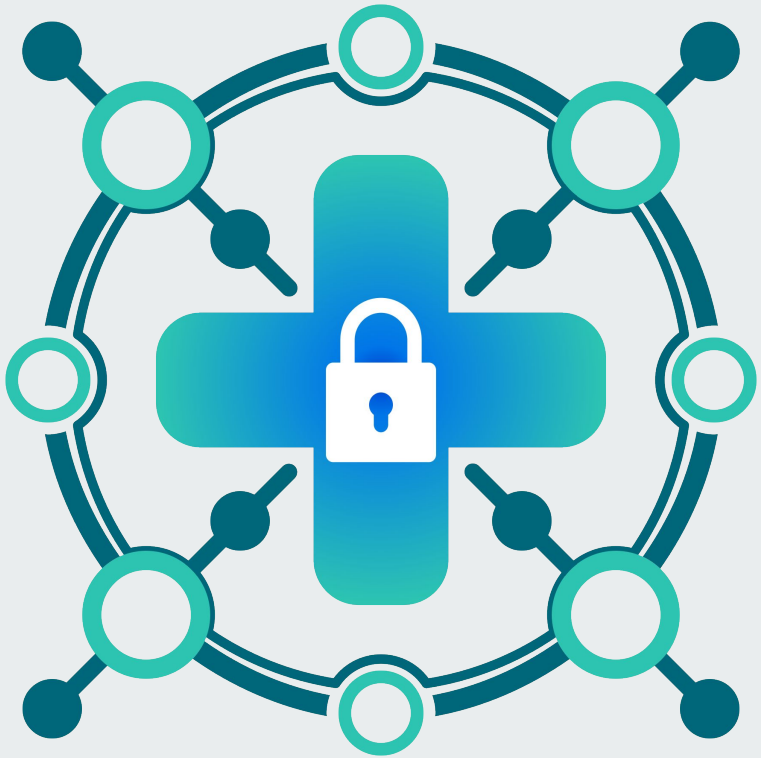
NECCDC 2025

Northeast Collegiate Cyber Defense Competition

RWU
Roger Williams
UNIVERSITY

Regional Info Session Agenda

- General Overview
- Black Team Overview
- White Team Overview
- Red Team Overview
- Logistics & Schedules
- Please Hold Questions Until Q&A



NECCDC 2025 General Overview

Competition Theme

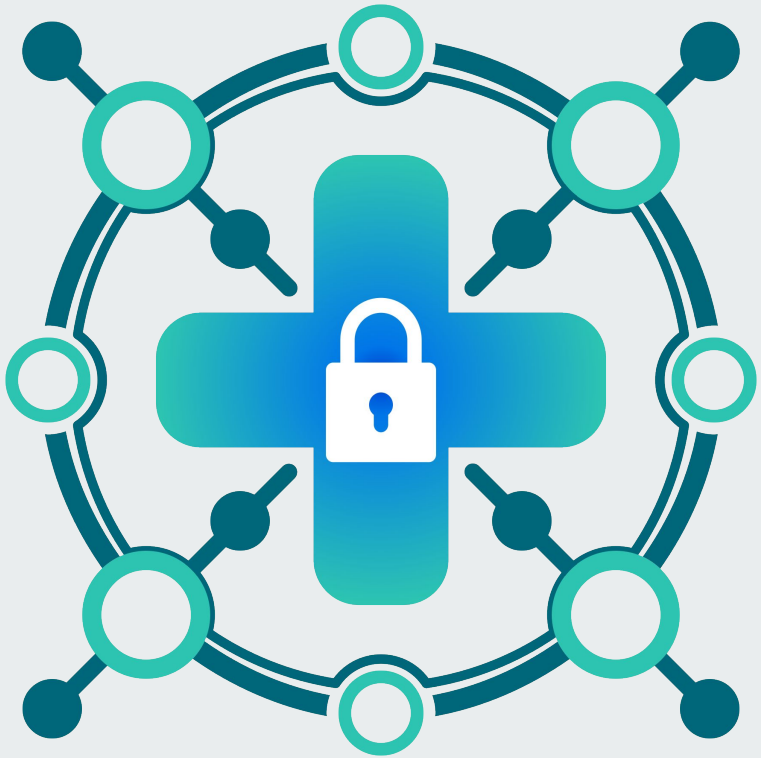
Third-party risk management is vital in healthcare to protect patient data and ensure compliance with regulations like HIPAA and HITECH. With increased reliance on external vendors for services like cloud storage and IT support, healthcare organizations face risks such as cyberattacks and data breaches. Effective management involves assessing vendors' security practices, robust contract management, and continuous monitoring to mitigate vulnerabilities, safeguard privacy, and maintain trust.

Competition Scenario - Recent Developments

In a significant move that marks a new chapter in its history, PlaceboPharma recently announced its acquisition of IllusioPharma, a company known for its focus on developing placebo-based digital therapeutics. This strategic merger combines PlaceboPharma's expertise in pharmaceutical innovation and clinical trials with IllusioPharma's cutting-edge technology in virtual placebo experiences. Together, the unified entity aims to explore new dimensions in placebo-driven therapies, from traditional pharmaceutical applications to emerging digital health solutions. The merger strengthens PlaceboPharma's position in the global market and provides opportunities to diversify its offerings and enhance its research capabilities. The combined resources and expertise promise to revolutionize how the industry approaches the integration of perception, technology, and healing.

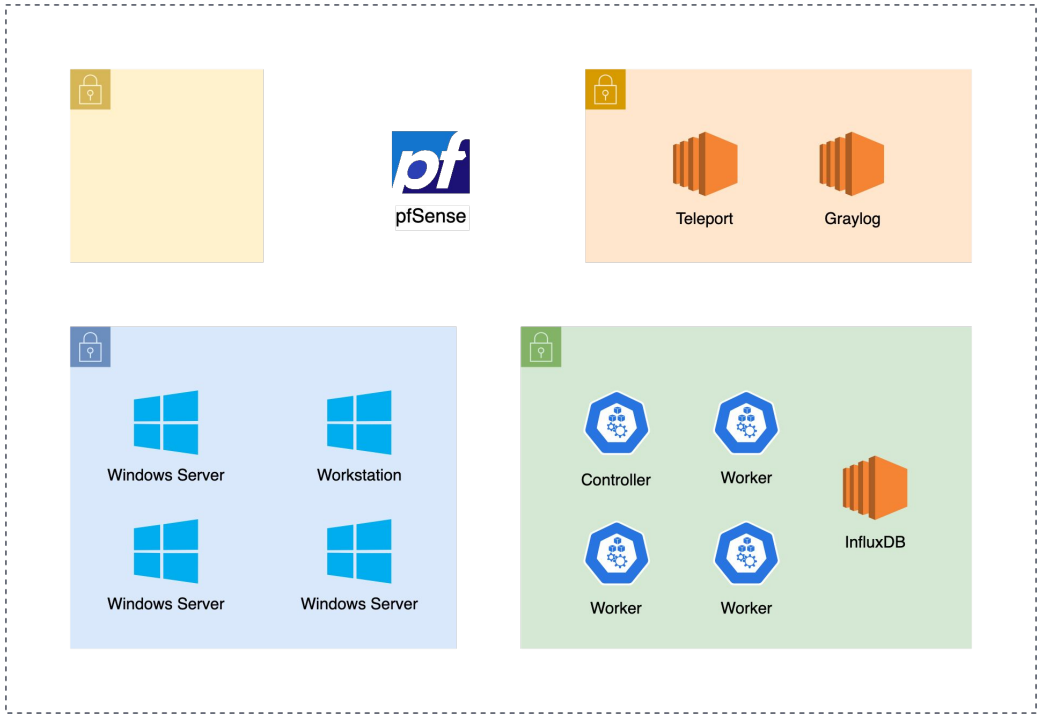
Competition Scenario - Summary of Changes

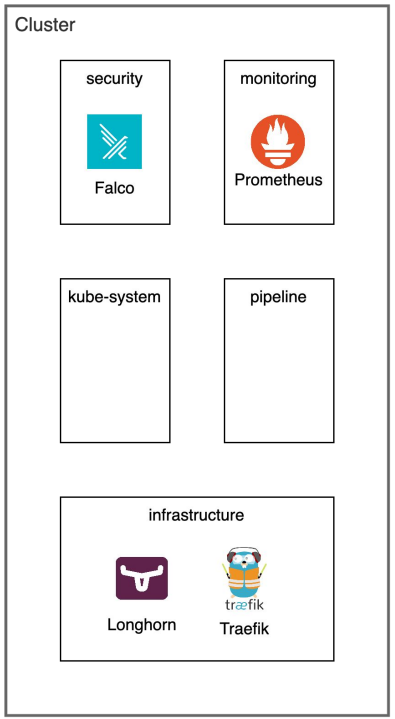
- PlaceboPharma was initially focused on consolidating its position & mitigating risks from third-party vendors
- Strategic acquisition of IllusioPharma is a game-changer
- While this allows the company to expand its reach & capabilities, it also faces new integration challenges



NECCDC 2025 Black Team Overview

Infrastructure Diagram





REMINDER: Supplies for Blue Teams

Similar setup for every team

- **Eight** Dell Inspiron laptops
  - **1 laptop connected to podium projector**
  - Lots of extra physical space
  - Spare table

Infrastructure

- Network switch for hardwired laptop connections **(Do not touch!)**

REMINDER: Blue Team Laptop Configuration

Ubuntu Desktop 22.04

Software Pre-installed

- Laptops will come pre-installed with common utilities
  - SSH, Nmap, web browsers, VSCode, RDP software
- Discord

Issues to be aware of

- Some laptops may experience battery issues, leading to sudden shutdowns, if unplugged (aim to identify & notify teams of any affected laptops beforehand)
- Please notify Black Team if other issues occur that impact your ability to participate

REMINDER: Blue Teams Accommodations

If you need accommodations to compete, contact blackteam@neccdl.org with your request.

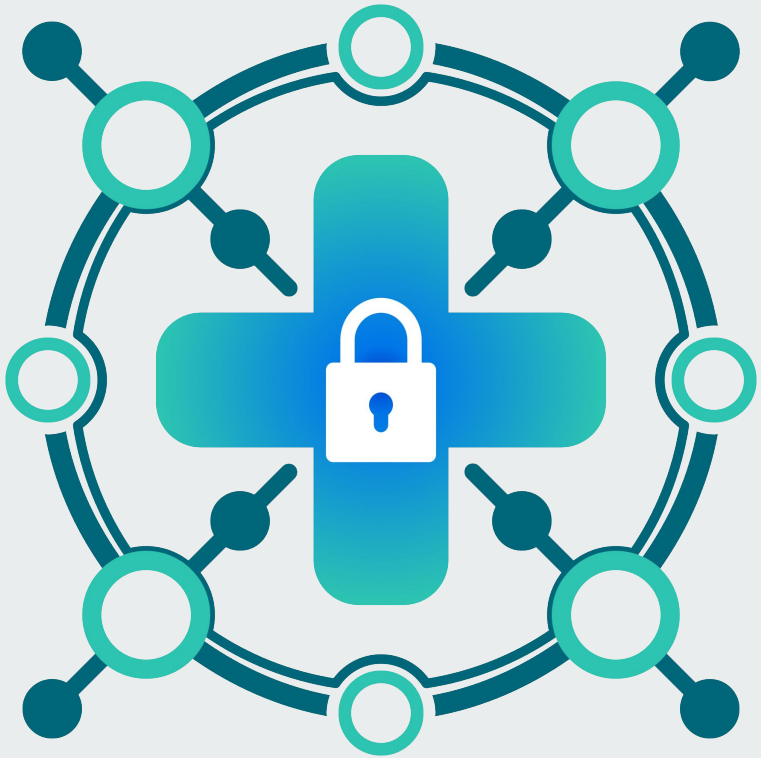
- Include your institution and full name in the email
- If requesting approval for peripheral devices, please include relevant pictures and relevant device information
- All requests must be submitted at least **one week before** the competition (e.g., BYOD pointer mouse)

REMINDER: Blue Team - Rules of Engagement

- Don’t modify the RWU network
  - Change settings, which ports are used, etc.
- Do not access other teams environments
- Each system has a “***black-team***” user/role. **Do not remove** or **restrict access** as they are used for scoring & remote assistance
- Complies with the National CCDC rules

REMINDER: Competition Access

- The infrastructure will be accessible directly from the RWU network
    - Wireguard will be used as a fallback in case of an issue during deployment
- Credentials will be released as soon as competition begins



NECCDC 2025 White Team Overview

Inject Advice

- Read / re-read directions & instructions → most answers are there!
- If inject requests executive summary → include one (remember audience)
- Ensure you submit correct & timely evidence of what was accomplished
- Not everything that anyone asks for is ok - think security & impact on mission
- Change your default passwords!
- Become familiar with game tech & infrastructure
- Pay attention to @**neccdl LinkedIn/Mastodon/BlueSky** & current events
- Any questions re: inject or need clarification or if you have a situation occur beyond your control that affects your inject submission:
    - Ask your moderator(s) to intercede on your behalf to @WhiteTeam - if you don't ask, they won't

Teamwork / Leadership Advice

- Know hierarchy for skills / knowledge & delegate tasks appropriately
- Encourage verbal communication with all team members
- Leaders should check-in regularly with team & leverage ideas while not micro-managing
- Use your tools, e.g. Discord team channel for organization
- Have contingency plans in place for loss of services
- Be calm, remain professional & have a good attitude under pressure
- Eat & hydrate - your brain needs energy to work. :)

3rd Party Risk Inject Tips & Hints

Validating Security Posture of 3rd Party Vendors

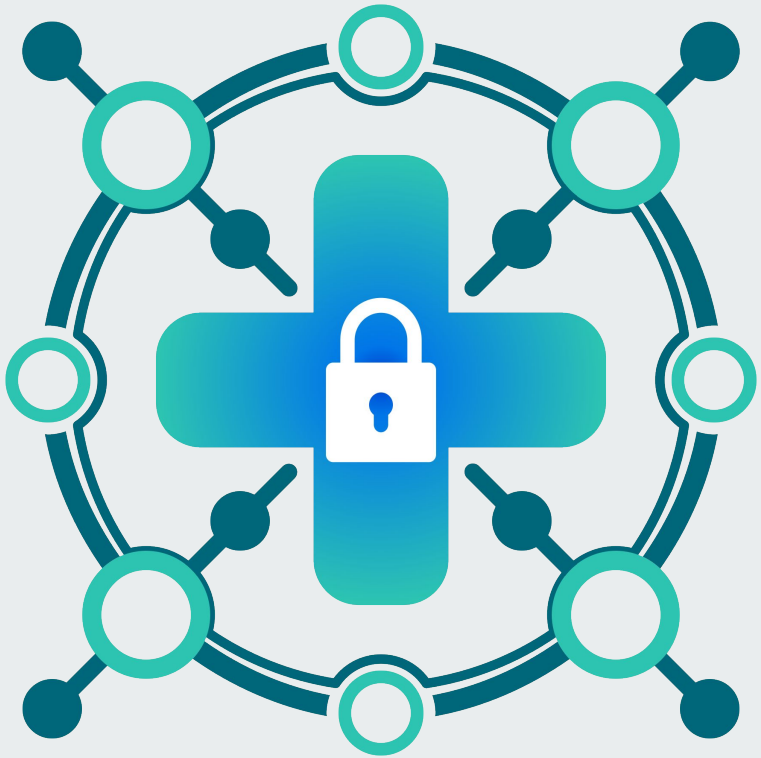
- Study Educause Community Vendor Assessment Toolkit: https://www.educause.edu/higher-education-community-vendor-assessment-toolkit
- Companies Public Disclosure: Privacy and Policy on Data Sharing

3rd Party Plug-ins | Add-ins

- OKTA: https://developer.okta.com/docs/guides/implement-oauth-for-okta/main/
- YouTube: https://www.youtube.com/watch?v=996OiexHze0

3rd Party Policy Creation:

- Purpose Section - highlighting the reason for the policy
- Scope Section – describing who, and what, the policy applies to
- Definition Section – define key terms or acronyms used in the document
- Policy Statement – a clear, concise declaration of the organization's commitment and approach toward the subject of the policy—in this case, third-party risk management.
- Risk Management: Vendor Due Diligence and Contractual Requirements, Risk Identification and Assessment, Ongoing Monitoring and Auditing, Incident Response and Breach Notification, Training and Awareness
- Compliance and Legal Requirements - outlines the key laws, regulations, and industry standards that PlaceboPharma must adhere to when engaging with third-party vendors and service providers



NECCDC 2025 Red Team Overview

Red Team - Rules of Engagement

Out-of-Scope

- Competition Network switches
- RWU Network (Wired & Wi-Fi)
- Competition Workstations (blue team laptops)
- Specific Team Accounts: Google Classroom & Discord

Red Team Advice

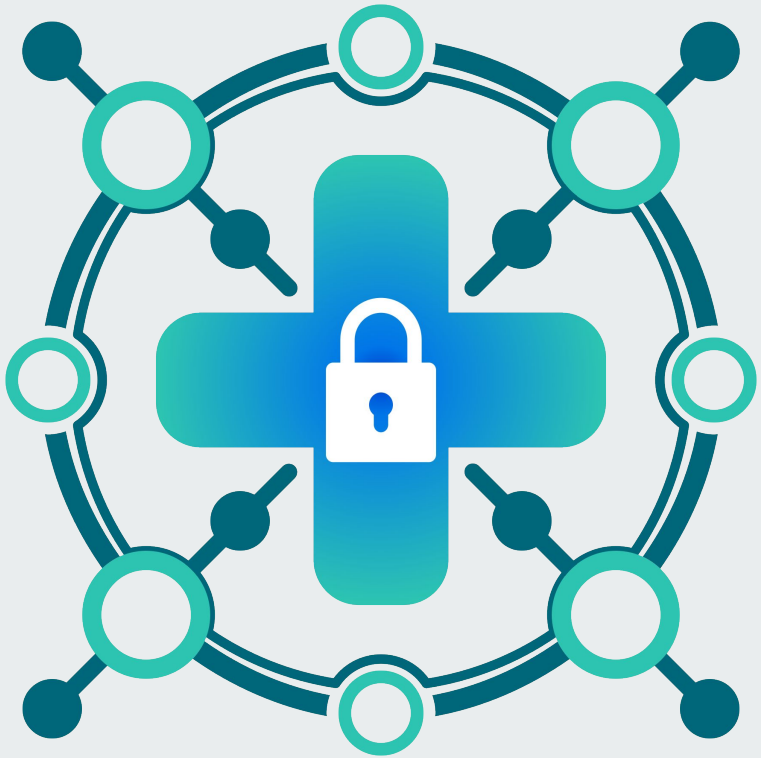
- Who ever has the most fun, wins - *Dan B.*
- Develop good teamwork & team support
- Find teammates that you enjoy working with under pressure
- Be a teammate that others enjoy working with under pressure
- Read the "2025 Red Team Advice" PDF
    - * Posted in Resources after presentation

IR Reports

- Submit good IR reports when incidents occur to reduce Red Team scoring impact
- Ensure professionalism when writing and enough necessary information & depth to describe the incident and business impact
- Ensure executive summaries and business impact analyses are written for the intended audience. **Minimize the technical jargon** in these sections of the report
- Ensure that you accurately identify the **business impact**

IR Reports

- Attempt to accurately determine the root cause
- Once an incident has been discovered, determine root cause & perform remediation. Any actions taken towards remediation/prevention should be detailed in the report
- Make sure you include relevant screenshots, visuals, and evidence
- Is what you are experiencing really due to Red Team activity, or is it misconfiguration, or actions by your own team?



NECCDC 2025 Event Schedule

Event Schedule - Fri 3/14 - Day 1

Friday, March 14	Event	Location
8:00 am - 9:00 am	Check In (Name tags & release forms)	GHH Main Level (Floor 1)
8:00 am - 9:00 am	Breakfast (informal breakout)	
9:00 am - 9:30 am	Competition Opening Ceremony	GHH Atrium (Lower level)
9:30 am - 10:00 am	Teams staging to rooms	
10:00 am - 4:00 pm	NECCDC Student Competition	Levels 0, 1, 2
12:00 pm - 12:45 pm	Team Lunch	GHH Main Atrium

Event Schedule - Sat 3/15 - Day 2

Saturday, March 15	Event	Location
8:00 am - 9:00 am	Breakfast	GHH Atrium (Lower level)
8:30 am - 9:00 am	Day 02 Debrief	GHH Atrium (Lower level)
9:30 am - 3:00 pm	NECCDC Student Competition	Levels 0, 1, 2
12:00 pm - 12:45 pm	Team Lunch	GHH Main Atrium
5:00 pm - 8:00 pm	Recruitment Event, Dinner	GHH Atrium (Lower level)

Event Schedule - Sun 3/16- Day 3

Sunday, March 16	Event	Location
8:30 am - 9:30 am	Breakfast	GHH Main Atrium
9:30 am - 11:30 am	Debriefs White/Red/Black	GHH Main Atrium
11:30 am - 12:30 pm	Awards Ceremonies + Lunch	GHH Main Atrium
12:30 pm - 2:00 pm	Networking & socializing	GHH Main Atrium

Recruitment Event

Networking Dinner: Saturday, March 15 between 5pm and 8pm

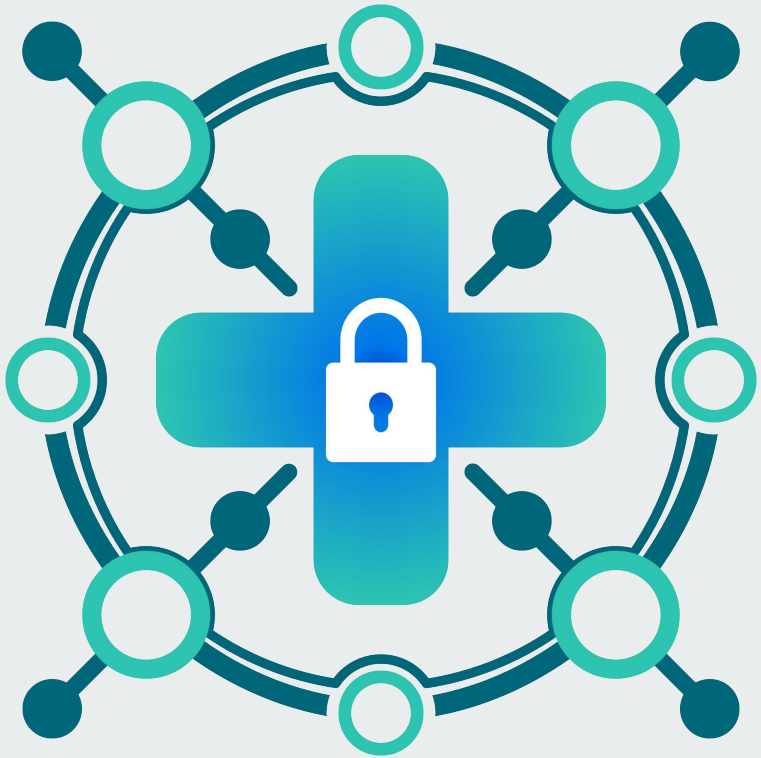
- Open to all **Blue Team members**, **coaches**, **sponsors**, **industry** & **student helpers**
- Lots of **good food** / **great networking opportunities**
- Open-mic night, companies can advertise **open internship** & **full-time positions**

Attending organizations (*tentative*)

- OSHEAN
- Roger Williams University
- Cisco
- Hurricane Labs
- Palo Alto Networks
- Splunk

Attending agencies (*tentative*)

- CISA
- NSA



NECCDC 2025 Sponsors

NECCDC Sponsors

Roger Williams University

Hurricane Labs

National Security Agency – United States of America

OSHEAN

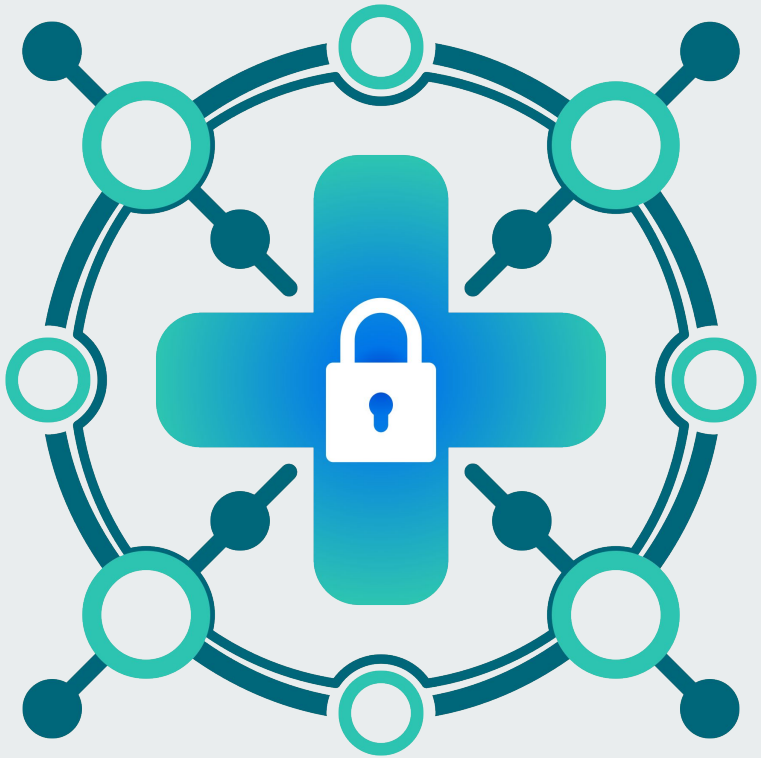
splunk> a CISCO company

paloalto NETWORKS | CYBERSECURITY ACADEMY

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY – CISA

Cisco Networking Academy

FORTRA Cobalt Strike



Q&A