CyberForce Competition™ Scoring Outlines

sCOARboard

Your team will receive an invitation email the week of November 26th asking you to register using your school's .edu email address. Please use the sCOARboard to enter your services and other requested information. These values should be entered by Friday, November 30, 2018 to ensure that your scoring is accurate during the competition. A follow-up email will be sent with the registration link and how to enter your services the week prior to the competition.

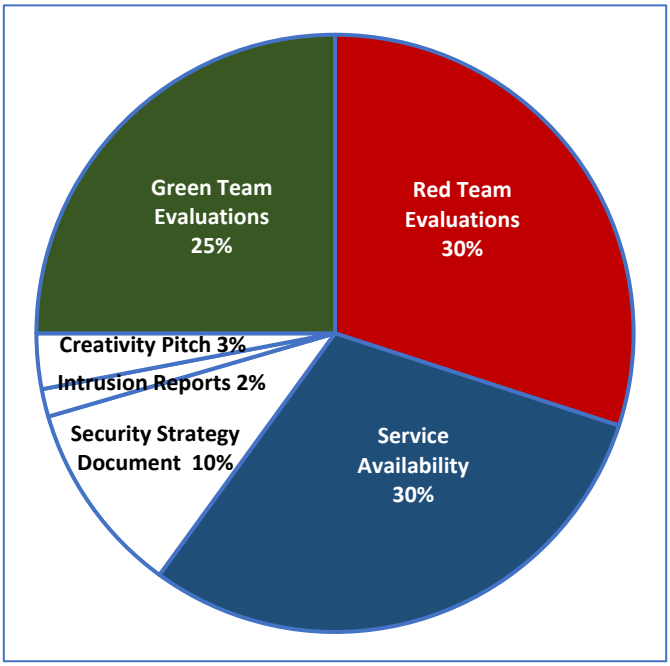
Additional Blue Team Responsibilities

Each Blue team is assigned a subnet of IPs for devices and services. If a Blue team damages non-physical components (e.g., virtual machines) beyond the point of recovery, the White team (National Laboratory) can provide a fresh, default image of the system, but your Blue team will incur a scoring penalty of 100 points per re-install per box. To prevent this, it is suggested that your team create backups or snapshots of the system along the way, especially before and after any major infrastructure changes. Blue teams may not perform any offensive actions aimed at other participants' networks, the Azure network, or the Laboratory network - doing so will result in disqualification and immediate removal from the competition site.

Scoring Breakdown

Overall Scoring Breakdown

- Red Team 1500 points 30%
- Blue Team Service Uptime 1500 points 30%
- White Team 750 points 15%
  - Documentation 525 points
  - Intrusion Reports 75 points
  - Creativity (Phish Tank) 150 points
- Green Team 1250 points 25%
- **Total 5000 points 100%**
- Anomalies – Up to 500 bonus points available



Red Team Scoring

TOTAL POINTS: 1500

Red team members will perform attacks on Blue team networks, topography and software. Red team points will be based on the how teams identify, protect, and respond to attacks as well as for sportsmanship demonstrated by the team during the competition. Red team score will be updated throughout the day. For additional scoring details please see the rubric provided at the competition.

Uptime Scoring

Service Uptime is based on the required services and their uptime. Total number of points for uptime scoring is 1500. For services that fail to be up during the required competition hours, teams will lose points. Blue teams are responsible for entering their required services into the sCOARboard.

White Team Scoring

White team members will evaluate two Blue team tasks:

TASK:	**TOTAL POINTS: 1000**
Documentation	525
Intrusion Reports	75
Phish Tank	150

Documentation must be submitted on or before November 27, 2018 at 11:59pm PT. Documentation submitted after the deadline will result in the loss of 15 percent of the scored document PER DAY. Additional information regarding the required documentation to be submitted to the White team is provided below. An example of one Blue Team's (White Team) Security Strategy Documentation that earned high scores from the White team will be provided in the "Security Strategy Document Guidance".

Also, at the end of this document is a rubric for the White Team Security Strategy Documentation. Please note that Blue teams are playing out a scenario and, like the real world, presentation and professionalism will play a factor in final scores.

Intrusion Reports

Intrusion reports are required of every team every other hour beginning at 1pm ET / 12pm CT / 10am PT. These reports should be entered via the template provided in sCOARboard. Analysis should be provided with each intrusion report. Intrusion Reports are worth a total of 75 points. A reporting template will be provided via the sCOARboard.

Creativity - Phish Tank/CISO Panel

150 points are at stake as you pitch your team's defensive strategy to the Phish Tank (aka CISO Panel). The Phish, volunteers with security leadership experience, will be looking to see how your team stands out from the pack. What is your team doing that is innovative, risky, and cutting edge? Are you just following checklists, or are you pushing the envelope? Your pitch will be limited to only a couple of minutes, and the time slot will be randomly assigned. Additional guidance on the scoring criteria is provided below.

Green Team Scoring

The Green team will review and evaluate each Blue team system's usability and experience and submit points based on documentation, overall performance, and helpfulness. The Green team will assess their ability to conduct routine business tasks by attempting to access and use the User Guide on the Blue Team Network.

Blue teams should develop a How-to/User Guide for their Green team members. This manual must be uploaded to the sCOARboard and may also be included on the Blue Team's website. The guide should be

written for new users who have no experience with your environment. Please note that each Green team member will only have 20-25 minutes to assess your system using the manual you provide. Your manual should include how to:

1. Select appropriate team number within sCOARboard.
2. Access and use the "User's Guide" from sCOARboard.
3. Log in to your team's website
4. View their ICS status
5. View the HPC status
6. Access the ICS Human Machine Interface
7. Add an engineering note
8. Check and add to engineering inventory
9. Access the file share and download sample file located there
10. Request support from the Help Desk (if needed)

While some of these steps may not be available to or needed by all Users (Green team), you should recognize that all Green team members will be using the same manual, so it is imperative that you clearly outline the anticipated result for each User. The criteria used by Green Team members to assess the Blue Team in this category is provided later in this document.

Additional Scoring Elements

Anomalies

In the real world of information assurance, there is never a dull moment. Anomalies simulate the stream of requests that IT employees and cybersecurity analysts must be prepared to handle. During the competition, anomalies will be delivered to you via the sCOARboard. They will be worth varying point values based on level of difficulty. Blue teams must submit responses to anomalies before they expire in order to earn points.

Responding to anomalies is **optional**. Blue teams that do not submit a response will not be awarded any points for that anomaly and no points will be deducted. Anomalies are worth up to 500 additional points and teams are strongly encouraged to respond to them. Blue team members are responsible for ensuring that responses to anomalies are submitted on time with complete documentation in order to earn points.

Penalties

Penalties will be assessed if a Blue team does not abide by the competition rules and guidelines. Teams should be aware of the following penalty deductions:

- Reimaging = 100 points per reinstall
- Receiving help from anyone outside Blue team members and White team during competition = 250 points each instance. This includes mentor help.
- Offensive action towards other teams' networks or hardware and/or network = Disqualification

Security Strategy Document (assessed by White Team) Scoring Rubric

	Network Diagram	Security Write Up	Professionalism and Formatting
90%-100%	• Diagrams include all assets located on competition network • Appropriate and accepted symbols and terminology (see appendix A)	• Hardening steps are comprehensive and technically sound • Steps from initial download to current version are incorporated, including patching, upgrades, etc.	• Document has aesthetic appeal • Complete sentences and correct terminology utilized throughout • No major spelling or grammatical errors
70-90%	• Diagrams omit minor components of competition environment (Each minor component omission will reduce overall score by 3%) • Diagrams make logical sense and are technically sound	• Hardening steps are comprehensive and technically sound • Includes most steps from initial download to current version are included but may omit some minor necessary steps	• Document looks presentable, but some areas may contain incorrect formatting or lack aesthetic appeal • Most of the document contains correct terminology • Some spelling or grammatical errors
50-70%	• Diagrams omit several major components of competition environment (Each major component omission will reduce score by 5%) • Diagrams have one or more gaps in technical or logical sense	• Hardening steps are taken but lack comprehensiveness or technical competence • Some major steps from initial download to current version are omitted	• Document has sections that are formatted differently • Presentation of materials detracts from overall effectiveness • Misuse or lack of technical language throughout the document • Many Spelling or grammar errors
Below 50%	• Core areas of networking are omitted • Major gaps in asset inventory • Major errors in logic or technical demonstration	• Hardening steps are taken but lack comprehensiveness or technical competence • Some major steps from initial download to current version are omitted	• Document is hastily or unformatted • Material is presented in an ad-hoc fashion • Little or no technical language is used • Spelling and grammar greatly detract from overall meaning

Intrusion Report Scoring Rubric

Points awarded	Intrusions	Defenses Implemented	Professionalism	Spelling, Grammar, and Formatting
100%	• All intrusions are documented in some fashion • Attempts by Red Team are identified and labeled	• Identify gaps in current security measures and implement appropriate mitigations, if applicable • Overall strengthening of security posture based on intrusions AND attempts	• Correct technical terminology is used • Layout and structure of document is well thought out	• No errors or mistakes
80%-99%	• Most intrusions are detected (>50%) • Some malicious actions are identified and labeled	• Implement mitigations to resolve intrusion attempts • Acknowledge security gaps in intrusion attempts with intent to fix later	• Most of document uses correct terminology • Some misplaced elements throughout document	• Small mistakes that do not detract from overall impact of report • Minimal amount of errors
50%-79%	• Some intrusions are detected (<50%) • Many malicious actions are misidentified, not identified, or mislabeled	• Acknowledge intrusions but cannot readily fix/mitigate • Acknowledge security gaps in intrusion attempts with intent to fix/mitigate later	• Some of document uses correct terminology • Frequent misplaced elements throughout document	• Small or medium size mistakes that inhibit ability to understand report
0-50%	• Severe deficiency in identifying intrusions • No/Sparse labeling of malicious intrusion attempts	• No intention to fix or mitigate vulnerabilities within the system	• Document is not written in a technical manner • Structure and layout is informal/haphazard	• Numerous error • Error severely detract ability to understand report

Phish Tank/CISO Panel Creativity Scoring Rubric

Phish Tank/CISO Creativity RUBRIC	**Capstone**	**Milestones**		**Benchmark**
	4	**3**	**2**	**1**
Acquiring competencies - *Refers to acquiring strategies and skills in the areas of IT/OT security*	Uses appropriate criteria to evaluate creative process that led to entirely new IT/OT security solution or idea	Creates an entirely new IT/OT security solution or idea for CFC	Successfully adapts an IT/OT security exemplar to CFC	Successfully reproduces an IT/OT exemplar.
Taking risks - *May include personal risk or risk of failure, i.e. going beyond original parameters, introducing new approaches, implementing unpopular ideas or solutions.*	Actively seeks out and follows through on untested and potentially risky directions or approaches to securing/ protecting IT/OT for the CFC	Incorporates new directions or approaches to securing/ protecting IT/OT for the CFC	Considers new directions or approaches to securing/ protecting IT/OT without going beyond the guidelines of the CFC	Stays strictly within the guidelines of the CFC in regard to securing/ protecting IT/OT
Solving Problems	Develops a logical, consistent plan to address CFC requirements, AND recognizes consequences of solution while articulating reasons	Selects from among alternatives to develop a logical, consistent plan to address CFC requirements	Considers and rejects less acceptable approaches to address CFC requirements	Only a single approach is considered and used to address the CFC requirements
Embracing Contradictions	Integrates alternate, divergent or contradictory perspectives or ideas fully	Incorporates alternate, divergent or contradictory perspectives or ideas in an exploratory way	Includes alternate, divergent or contradictory perspectives or ideas in a small way.	Acknowledges alternate, divergent, or contradictory perspectives or ideas.
Innovative Thinking - *Novelty or Uniqueness of Idea, Claim, Question, Form, etc.*	Extends a novel or unique IT/OT security idea, question, format, or product to create new knowledge or knowledge that crosses boundaries.	Creates a novel or unique IT/OT security idea, question, format, or product.	Experiments with creating a novel or unique IT/OT security idea, question, format, or product.	Reformulates a collection of available IT/OT security ideas.
Connecting, Synthesizing, Transforming	Transforms IT/OT security ideas or solutions into entirely new forms.	Synthesizes IT/OT security ideas or solutions into a coherent whole.	Connects IT/OT security ideas or solutions in novel ways.	Recognizes existing connections among IT/OT security ideas or solutions.

Green Team Survey Rubric

	Detail of Instructions	Clarity	Professionalism	Completeness	Supporting Documentation
Strongly Agree	There is sufficient detail given to each task for volunteer to be successful	Instructions are clear and easy to follow	Instructions properly formatted; appropriate terminology used; correct grammar	Green Team members can follow instructions and complete tasks as intended	Document is well-written, conveys tasks in a logical and easy to follow way with no gaps in logic
Agree	Details may be omitted that cause volunteers to assume next course of action	Instructions may not be completely clear	Instructions contain some formatting issues; most terminology appropriate and most grammar correct	Green Team members can follow instructions and complete tasks adequately	Document is well-written with small gaps in logic
Disagree	Some details are omitted, and volunteers must act independently	Instructions are vague and may not contain clear start or end points	Instructions missing sections or poorly formatted; some appropriate terminology and grammar	Green Team members may not be able to complete tasks	Majority of document t is well-written but large gaps in logic
Strongly Disagree	A majority of details are omitted; volunteers must act independently	A majority of instructions are not clear	Instructions obviously incomplete; some appropriate terminology and grammar	Green Team members cannot complete tasks	Document is not well-written; large gaps in logic