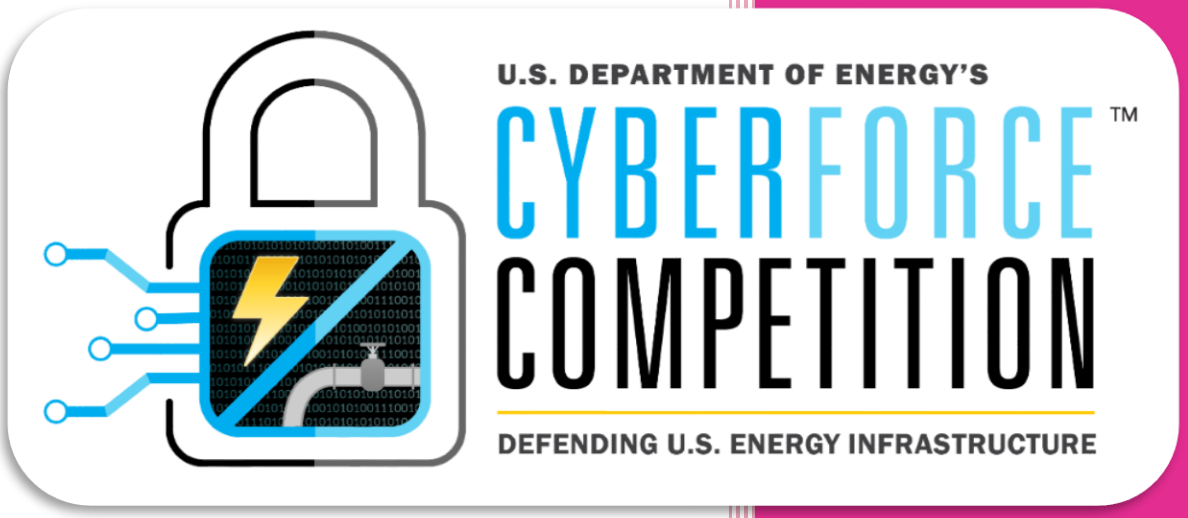


Overview, Rules, and Scoring

2019

10/28/2019

CYBERFORCE COMPETITION™

CONTENTS

COMPETITION OVERVIEW 2
KEY DATES 2
COMPETITION STRUCTURE 2
SETUP PHASE 2
INFORMATION GATHERING PHASE 2
ATTACK PHASE 2
GETTING STARTED: PRE-COMPETITION 3
COMMUNICATION CHANNELS 3
COMPETITION ENVIRONMENT 3
COME PREPARED: COMPETITION 4
HOST SITE QUESTIONS 4
LABORATORY PROVIDED HARDWARE AND EQUIPMENT 4
INDUSTRIAL CONTROL SYSTEM DEVICES 4

KEY RULES 5
UPDATES TO RULES 5
THE DO'S 5
THE DO NOT'S 6
COMPETITION REQUIREMENTS 7
REQUIRED SERVICES AND PORT NUMBERS 7
REQUIRED USERS 7
REQUIRED DOCUMENTATION 8

SCORING BREAKDOWN 9
RED TEAM SCORING 9
BLUE TEAM SCORING 9
GREEN TEAM SCORING 9
WHITE TEAM SCORING 10
SECURITY DOCUMENTATION 10
INFORMATION SHARING 10
CISO PANEL BRIEF 10
ANOMALY SCORING 11
PENALTIES 11

RUBRICS 12
RED TEAM CATEGORY 1 & 2 RUBRIC 12
RED TEAM CATEGORY 3 RUBRIC 12
SECURITY DOCUMENT SCORING RUBRIC 13
INFORMATION SHARING RUBRIC 14
CISO PANEL RUBRIC 15
GREEN TEAM SURVEY 16

COMPETITION OVERVIEW

KEY DATES

Key Dates	Activity
Monday, October 28, 2019	Students are provided full rule set, guidance, access to their Azure platform, and remote access to their ICS device.
Monday, November 4, 2019	Instructions to register on sCOARboard
Friday, November 8. 2019 11:59pm PST	Security Documentation due to sCOARboard
Thursday, November 14, 2019 12pm Local Time of Hosting Site	Students temporarily lose remote access to their industrial control
Friday, November 15, 2019 See hosting laboratory's agenda	Students are provided physical access to their hosting laboratory* and their industrial control systems Students are required to have all user information, including usernames and passwords, into the sCOARboard for Saturday morning.
Saturday, November 16, 2019	Competition Day

* Please note some laboratories require arrival by certain times on Friday and Saturday.

COMPETITION STRUCTURE

SETUP PHASE

Blue teams will be given access to their Azure environment on October 28, 2019. Blue teams should use this time to assess, build, secure, and test their system prior to the competition as well as familiarizing themselves with the competition scenario.

INFORMATION GATHERING PHASE

Red team members will scan networks and gather background information about Blue team systems beginning November 8, 2019. Red team scanning will be limited to passive reconnaissance which is both non-destructive and non-permanent. No logging into the machines is allowed. Nothing invasive or destructive may occur during this period. If Blue team members notice unauthorized access attempts or other invasive actions to their system, they should notify CyberForceCompetition@anl.gov immediately. Please be prepared to show proof that something was altered such as logs containing the offending action.

ATTACK PHASE

On the day of the competition (Saturday), the Red team (attackers) will attempt to gain access to Blue team services while the Green team (users) attempts to use them. The White team (competition technical team) will assess Blue team service uptime. Blue teams must monitor their systems, be active in information sharing, answer anomalies, and support their Green team users.

During this phase, the Blue team may not receive help from anyone not registered as a competitor on their team or the White team. Receiving help from others, including mentors, external parties, etc., will result in disqualification.

GETTING STARTED: PRE-COMPETITION

COMMUNICATION CHANNELS

SLACK

Students have been provided a registration link for the CyberForce Competition 2019 Slack channel. When registering in Slack, please be sure to include your Team # in your username (i.e., T23 – Janet; T45M – Bob). Teams are encouraged to assist one another via the Slack Channel.

EMAIL

Students may also email CyberForceCompetition@anl.gov. Please note, this email is only monitored during normal business hours in Central Time, Monday – Friday.

COMPETITION ENVIRONMENT

NETWORK TOPOLOGY

- You will inherit a /26 Azure subnet in a /24 Azure virtual network with a competition exposed ICS (which must stay accessible to red and green users).
- Any changes to your Blue team infrastructure must be clearly documented in Strategy Documentation.

LOGIN INSTRUCTIONS

VPN INSTALL INSTRUCTIONS

The competition uses OpenVPN for access to the Azure environment. You will be provided an OVPN configuration file to connect to your network. Clients for each operating system can be found below:

- Windows - https://openvpn.net/index.php/download/community-downloads.html
  - Place the OVPN file into "C:\Program Files\Openvpn\config".
- MacOS – https://www.tunnelblick.net
  - Double click the OVPN file to import it to Tunnelblick
- Linux – sudo apt (or yum) install openvpn
  - Run "openvpn --config YOUR_OVPN_FILE.ovpn"

AZURE CREDENTIALS

You will receive an email from CyberForceCompetition@anl.gov with your Azure credentials.

If you have not received this email yet, please patiently wait until 5pm CT on Monday, October 28, 2019 before contacting CyberForceCompetition@anl.gov. This allows ample time for the lab staff to ensure all accounts went out. This email will be sent to the email that is on file with your registration. The CyberForce email will be monitored until 7pm CT on Monday.

SCOARBOARD CREDENTIALS

Use the sCOARboard to enter your services and other information required by the White team.

- Your team will receive an invitation via email the week of November 4, 2019 to register each team member using your school's [.edu] email

- Scored services can be tested during the week before the competition. Services should be entered by Friday, November 15, 2019 to ensure that your scoring is accurate during the competition.

INDUSTRIAL CONTROL SYSTEM DEVICES

- If there is a suspected network outage or your ICS device is not working properly **CORRECTLY BEFORE** the competition, please contact CyberForceCompetition@anl.gov or a lab staff member on Slack.

RESTORING SYSTEMS TO INITIAL STATE

If a Blue team damages any virtual machines beyond the point of recovery, the White team can provide a fresh, default image of the system. However, your team will incur a scoring penalty of 250 points per VM restoration. To prevent a scoring penalty, your team is encouraged to create disk snapshots of each system as it is set up and configured, especially before and after any significant infrastructure changes.

COME PREPARED: COMPETITION

HOST SITE QUESTIONS

If you have specific questions about your hosting laboratory, please reach out via Slack in the laboratory channel, ask your team point of contact to reach out to the local host or email CyberForceCompetition@anl.gov.

LABORATORY PROVIDED HARDWARE AND EQUIPMENT

Teams will gain physical access to their competition space on Friday, November 15, 2019. The following items are provided by the hosting site:

- Industrial Control System
- Power Strip(s)* with a minimum of 10 outlets
- One 8-port switch
- Internet access to allow VPN access to competition space
- One monitor, keyboard, and mouse

* Some laboratories have strict guidelines about the use of power strips. Please be mindful that power strips outside those provided may not be allowed.

The National Laboratories will not provide any display, network, power, or other adapters for competition use.

INDUSTRIAL CONTROL SYSTEM DEVICES

If there is a suspected network outage or your industrial control system is not working correctly DURING the competition, contact your local White team.

Replacing physical components often requires long-lead times in the real world and for this competition—any physical damage to the ICS components may not be repairable during the competition.

KEY RULES

- Each team must have 4-6 students or 3-5 for professional teams.
- One faculty mentor should be present at the national laboratory on the day of the competition. In the case that a faculty member cannot attend, an appropriate substitute mentor will be identified and the hosting laboratory must be notified. The hosting lab must then acknowledge and approve the change for the substitute to be allowed on premise.
- Faculty mentors may not provide any assistance to their teams on the day of the competition. Any team receiving help from a coach or mentor will be warned and/or disqualified.
- Each national laboratory has their own rules and procedures concerning wireless and site access. You are responsible for understanding and following these rules during the competition. Please familiarize yourself with this information prior to the competition.
- As a Blue team member, you are not allowed to perform any offensive measures towards other Blue teams, Red teams, the Green teams, the competition network, or your host laboratory. Doing so will disqualify your team from the competition.
- Each Blue team will have access to their Azure environment beginning on October 28, 2019. The White team operates the administrative accounts on Azure. These White team administrative accounts will not be used maliciously and are only there to ensure proper scoring and enforcement of rules.
- Security documentation is due no later than 11:59pm PST on Friday, November 8, 2019. Teams will upload a PDF of their security document and a separate PDF of their network diagram to the sCOARboard. Early submission is encouraged. Any documentation submitted after this deadline will be reduced by 15% of its scored value per day. If no documentation is submitted by competition start, the team will receive zero points. Please refer to the Scoring Breakdown for more information. Please ensure your documentation follows the format: Team # – Security Documentation.
- WARNING: Changing an IP directly on the VM that is provided by Microsoft Azure infrastructure may lock you out of your workstations. IP changes must be done in the Azure network interface settings in the Azure Portal.
- Secure pre-existing required services on **PROVIDED** VMs as outlined in the Blue team Azure and VPN PDF.
- The required services **provided MUST** be the services used for scoring purposes in the sCOARboard.
- Keep the provided name of your inherited machines in Azure. If restoring from a snapshot or redeploying an image, ensure it is renamed to the original name.
- These rules ensure that each team participates under the same circumstances and thus has an equal opportunity to succeed. Depending on the offense, failure to comply with the rules of the competition may result in penalty points or disqualification. Egregious offenses may result in disqualification from the competition. If you see a breach of competition rules, please notify the competition staff immediately. Communications with White team members are confidential.

UPDATES TO RULES

Updates to rules will be found on the CyberForce Competition website under the Rules & Guidelines Tab as well as posted on the Slack Channel (cyberforce2019.slack.com). It is each team's responsibility to be aware of any updates to the rules.

THE DO'S

- Secure existing required services on provided VMs as outlined in the Blue team Azure and VPN PDF.
- Make use of only freely available or free trials of software. Paid software and paid Azure images are prohibited from use.

- Configure the DNS service for name resolution by all machines on your subnet.
- Create a webmail service that supports SMTP and POP3 access.
- Create a help desk service for your green team users to request assistance. Asking green team users to use their personal email or phone numbers is strictly prohibited.
- Configure the NTP service for time synchronization of all machines on your subnet.
- Protect and maintain the continuous operations of the ICS device your team has been entrusted with to ensure your company and its consumers are satisfied.
- Input the scored services into the sCOARboard prior to competition day.
- Keep your services online, on their standard ports, for the duration of the competition.
- Ensure all users specified in the provided **REQUIRED USERS** list are created. These users will be provided to the Green team in order to login to any services needed to complete their tasks.
- Submit Green team users and passwords to the sCOARboard prior to the competition.
- Keep Green team user passwords updated in the sCOARboard.
- Create and submit the User Guide to the sCOARboard for Green team members on how to use services hosted on your website. Reminder, Green team scores are based on surveys of the usability of your hosted services.
- Create and deploy innovative defense strategies within the constraints of other rules.
- Submit Security Documentation by November 8, 2019 by 11:59pm PST to the sCOARboard.
- Bring all laptops, adapters, extra cables, extra mice/keyboards, monitors, etc. that your team will need to compete. Laptops should have an Ethernet port or come with required adapter to connect to Ethernet or be wireless enabled.

THE DO NOT'S

- Do not create more than 9 total virtual machines (VMs) in your environment (including all the VMs provided). White team will delete the last machine(s) created if more than 9 machines are present.
- Do not delete the provided machines or the required services from the machines.
- Do not change the IP addresses to the following provided VMs: your VPN or debian9.
- Do not change the name of your provided machines in Azure. If restoring from a snapshot or redeploying an image, ensure it is renamed to the original name.
- Do not use paid or trial Azure images.
- Do not specifically block or ban IP addresses or ranges. Automated systems that block connections after N failed login attempts (e.g., fail2ban) are NOT allowed.
- Do not physically tamper with any other team's physical devices.
- Do not perform offensive actions toward any other teams, your host laboratory, or Azure.
- Do not modify the logic for the ICS components in RexDraw. Altering the logic of these devices may result in damage to the physical model during the competition.
- Do not modify any of the provided VPN machines.
- Any attempts to hack or compromise the sCOARboard will result in disqualification.

COMPETITION REQUIREMENTS

REQUIRED SERVICES AND PORT NUMBERS

All Blue teams are required to establish and maintain the following services on the listed ports during the competition. If one of these services is on a provided VM, it must remain on that VM. This pre-existing service will be scored.

SERVICE	PORT NUMBER
HTTP	80
SSH	22
FTP	21
DNS	53

SERVICE	PORT NUMBER
NTP	123
SMTP	25
POP3	110

REQUIRED USERS

The following users are required to have administrative privileges to the ICS and must be used to login to any authenticated services. The passwords you provide for them should also be inputted into the sCOARboard prior to the competition on November 16, 2019 and be updated during the competition.

REQUIRED DOCUMENTATION

SECURITY DOCUMENTATION

Blue teams must develop a Security Document detailing their security strategy for assessing the threats to their environment, hardening and monitoring their network, and responding to incidents. This documentation must be submitted to the sCOARboard as a PDF by November 8, 2019 at 11:59pm PST. Details on requirements can be found in the Scoring guidelines. Examples of high scoring documentation will be provided via the Slack channel.

USER GUIDE

Blue teams must develop a User Guide for their users. This manual must be uploaded to the sCOARboard prior to the start of the competition on November 16, 2019. 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.

Green teams will be provided a Windows 10 machine with Firefox and an OpenVPN client connected to your VPN. Note that Firefox has a built-in FTP client and Green team members will not have administrative access to their machines. The following are the required and scored steps of your users.

1. Access your team's website
2. View your ICS device's status on your ICS Human Machine Interface (HMI)
3. Add an engineering note on the website
4. Access the FTP file share
5. Download a sample file from the share
6. Check company email on the website
7. Request support from the Help Desk

SCORING BREAKDOWN

Red Team	2000 points	20%
Blue Team	2000 points	20%
Green Team	2000 points	20%
White Team	2000 points	20%
Anomaly Scoring	2000 points	20%
Total	**10000 points**	**100%**

RED TEAM SCORING

TOTAL POINTS: 2000

During the competition, Red team will be mounting attacks against Blue team's systems, networks, and software. Red team's goal is to achieve and maintain persistence on Blue teams' systems for the purposes of disrupting confidentiality, integrity and availability.

Scoring will be broken into three categories:

1. Exploitability of known vulnerabilities.
2. Vulnerabilities introduced through Blue team build-outs.
3. Sportsmanship

Category 1 scores will be deducted on a pre-determined set of points per vulnerability. Categories 1 and 2 will comprise 90% of the Red team scoring and will lose points with each successful compromise. Category 3 will comprise 10% of the scoring using the rubric provided below. Category 1 and 2 scores will be updated every two hours. Category 3 points will only be provided at the end of the day.

BLUE TEAM SCORING

TOTAL POINTS: 2000

The Blue team scoring is completely based on the Blue team's ability to keep services active and available based on the parameters in the Azure/VPN document. In a professional environment, every security professional's primary responsibility is to keep business operational and secured as best as possible. Service uptime is based on the required services and their respective uptimes. Teams earn points for each availability scan that results in positive service uptime for a total of 2000 points. Throughout the day, services will be validated as operational by the sCOARboard polling system. Each service is scored and weighted the same, which means availability is scored purely on the service being operational. Blue teams are responsible for their services in the sCOARboard.

GREEN TEAM SCORING

TOTAL POINTS: 2000

The Green team will review and fill out surveys which evaluate each Blue team system's usability and user experience and submit points based on documentation, overall performance, and helpfulness. The Green team will assess a fictitious employee's ability to perform routine business tasks by attempting to access and use the User Guide on the sCOARboard.

Blue teams should develop a User Guide for their Green team members. This manual must be uploaded as a PDF to the sCOARboard. 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. The User Guide should include how to:

1. Access your team's website
2. View your ICS device's status on your ICS Human Machine Interface (HMI)
3. Add an engineering note on the website
4. Access the FTP file share
5. Download a sample file from the share
6. Check company email on the website
7. Request support from the Help Desk

WHITE TEAM SCORING

TOTAL POINTS: 2000

SECURITY DOCUMENTATION

POINTS: 1100

Security documentation provides your team the opportunity to highlight what your approach to security was for this competition. Examples of high scoring documentation will be provided via Slack in the #security-doc-q-a channel. Your document must be submitted on or before **NOVEMBER 8, 2019 AT 11:59PM PST** on the sCOARboard as a PDF. Documentation submitted after the deadline will result in the loss of 15% of the scored document per day. 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.

INFORMATION SHARING

POINTS: 600

Information sharing is the process of sharing a technical account of a cyber-attack against your protected services with your peers. Despite the competitive nature of business, most organizations have recognized that participation in trusted communities where cyber defense information is shared has proved more beneficial to them in the long run than trying to defend alone. For the purpose of this event, information sharing will be accomplished through one or more team members logging into your team's assigned Malware Information Sharing Platform (MISP) server and submitting the details of the identified attack including event attributes. Each team will be assigned to a MISP server for each two hour block of the competition and will be connected to sharing groups based on your team's dependencies. The purpose of the MISP server is for your team to share and collect attack information on attacks that may be targeted at your team or those within your dependency chain.

Your team must submit six cyber incidents each worth 100 points throughout the competition (minimally three in each half). If your team submits more than three events per half, the three submissions that yield the most amount of points will be chosen. Each team is encouraged to submit as many relevant events as they are able to. Points are awarded based on the completeness of the information and the attributes submitted to the MISP server.

CISO PANEL BRIEF

POINTS: 300

The CISO panel allows your team to experience having to explain real world examples of challenges in the modern day workforce. For this effort your team will be provided a scenario of a cyber-related event on Friday,

November 15, 2019 via Slack. A representative from your team must explain the details of the event to the CISO leadership team. The senior leadership team will want to know details surrounding the described event and your representative's ability to identify and articulate the incident related data elements.

ANOMALY SCORING

TOTAL POINTS: 2000

In the real world of information security, there is never a dull moment. Anomalies simulate the stream of requests that IT employees and cybersecurity professionals 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. Teams that do not submit a response will not be awarded any points for that anomaly. Blue team members are responsible for ensuring that responses to anomalies are submitted on time with complete documentation (if necessary) in order to earn points. Although the sCOARboard is not case sensitive, please ensure proper spelling upon submitting, as the sCOARboard has to match your answer with the master key. Blue teams will be able to download the zipped anomaly folders on November 15, 2019 from the White team FTP server. It is highly recommended to download these folders immediately on Friday as not to incur any time lost waiting for your download to complete on the day of the competition.

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 by White Team = 250 points per reinstall per box
- Failure to comply with naming guidance during competition = 250 points per misnamed VM
    - Will be assessed by White team throughout competition.
- Receiving help from your teams mentor = Verbal Warning then Disqualification
- Offensive action towards other teams' networks or hardware and/or network = Disqualification

RUBRICS

RED TEAM CATEGORY 1 & 2 RUBRIC

	Low	Moderate	High
Difficulty to Exploit	Exploit was by the book, exactly as expected per CVE or vulnerability report.	Some mitigations were put in place, but service was still exploitable.	Blue team made exploitation extremely difficult.
Difficulty to Discover/Remediate	Minimal hardening steps taken. This is a vulnerability that needs to be patched.	Patching or remediating was non-trivial, required some skill and investigation into individual services, applications, or configurations.	Vulnerable services required deep knowledge of system and/or network design, extensive remediation, or were unfixable without extraordinary measures.
Consequences of Exploit	Non-account or privilege related information leakage, read only access, etc.	Ability to drop files on the system, potential for pivot or attack setup, provides lower privileged account or system access.	Administrative access, full shell/command access.

RED TEAM CATEGORY 3 RUBRIC

	Description	Low Performer	Moderate Performer	High Performer
SPORTSMANSHIP				
Secure the team network in a manner practicable in a real-world environment, both technically and politically	Team defenses are not overly heavy-handed (e.g., realistic limits on user accounts, appropriate intervention in user activities, banning/blocking is targeted and justified, not breaking required functionality, etc.)	Many or major issues.	Few or minor issues.	No issues.
Demonstrate professional and ethical conduct during the competition	Team does not provoke or respond to the red team in a manner inconsistent with behavior acceptable for the spirit of the competition.	Many or major issues.	Few or minor issues.	No issues.

SECURITY DOCUMENT SCORING RUBRIC

	Network Diagram	Security Write Up	Professionalism and Formatting
100%	• Diagrams include all assets located on competition network including logical connections and interconnects • Appropriate and accepted symbols and terminology	• 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% - 99%	• Diagrams omit minor components of competition environment • 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 • 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 completed 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

INFORMATION SHARING RUBRIC

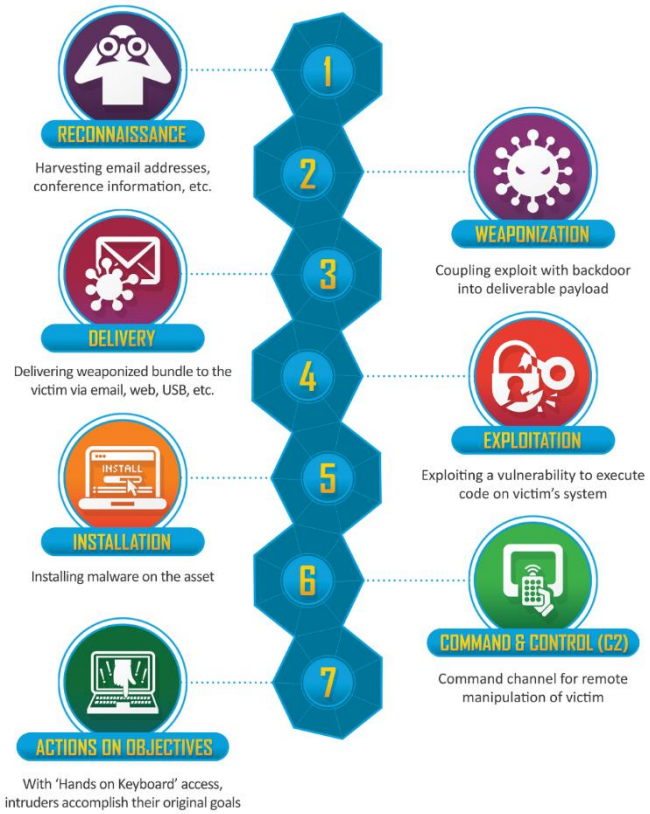
Each event MUST contain the following base set of fields (worth 16 points):

- Time: The time that the event was first observed.
- Description: A textual description of the cyber attack
- Actionable Attribute: A piece of information that helps identify the observed activity

By providing additional detail, as shown below, you can increase the value of a submission to 50 points.

Points	Fields within the MISP server that represent a security event
12	Kill Chain = What step within the kill chain does the identified attack represent
12	Recommended Mitigation = What steps are needed to protect or remediate the cyber event
12	One or more ADDITIONAL Actionable Attributes
12	Attack Type = buffer over flow, compromised service, stolen/cracked credentials
12	Number affected = how many systems had the same attack attempted
12	Recommended action = what or how to protect yourself and others
12	Impact level = low, moderate, severe, or critical

Further documentation will be provided at the competition to indicate the specific named attributes that should be used to convey the information above.



Additional Information

- MISP documentation: https://misp-project.org/documentation/
- Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

CISO PANEL RUBRIC

Points Awarded	Basic Data Elements B.1	Incident Handler Data Elements B.2	Post-Incident Activity Suggestions
100%	All the elements listed in **B.1** for this scenario have been included.	All the incident handler data elements listed in **B.2** for this scenario have been included.	Provided a post-incident plan that included more than three different options to remove the future risk
75%	More than 50% of the listed elements in **B.1** have been included	More than 50% of the incident handler data elements listed in **B.2** have been included	Provided a post-incident plan that included more than two different options to remove the future risk
50%	Less than 50% of the listed elements in **B.1** have been included	Less than 50% of the incident handler data elements listed in **B.2** have been included	Provided a post-incident plan that included one option to remove the future risk
0%	Did not follow the recommended NIST SP 800-61 standard or simply repeated the scenario paragraph	Did not follow the recommended NIST SP 800-61 standard or simply repeated the scenario paragraph	No after action plan provided

B.1 Basic Data Elements	B.2 Incident Handler Data Elements

• Incident Details
  ○ Status Change date/time
  ○ Physical location of incident
  ○ Current status of the incident
  ○ Source/cause of the incident
  ○ Description of the incident
  ○ Description of affected resources
  ○ Indicators related to incident
  ○ Prioritization factors
  ○ Response actions performed
	• Current status of the incident response
	• Summary of the incident
	• Incident handling actions
	• Incident handler comments
	• Cause of the incident
	• Cost of the incident
	• Business impact

GREEN TEAM SURVEY

1. I was able to access my team's website.
    a. Yes
    b. No
2. I was able to check the status of the Industrial Control System (ICS) Human Machine Interface (HMI).
    a. Yes
    b. No
3. I had the ability to add an engineering note on the website.
    a. Yes
    b. No
4. I was able to access file share.
    a. Yes
    b. No
5. I had the ability to download a sample file from the file share.
    a. Yes
    b. No
6. I had the ability to check email.
    a. Yes
    b. No
7. I felt the Blue team was responsive and helpful.
    a. Strongly Agree
    b. Agree
    c. Disagree
    d. Strongly Disagree
8. I was able to easily follow the instructions provided.
    a. Strongly Agree
    b. Agree
    c. Disagree
    d. Strongly Disagree
9. I felt the Blue team ensured I understood my tasks.
    a. Strongly Agree
    b. Agree
    c. Disagree
    d. Strongly Disagree
10. I felt the design of the website was user friendly.
    a. Strongly Agree
    b. Agree
    c. Disagree
    d. Strongly Disagree
11. The User Guide provided by the Blue team allowed me to complete all my tasks within the time allotted.
    a. Strongly Agree
    b. Agree
    c. Disagree
    d. Strongly Disagree
12. The documentation provided looked professional and was well-written.
    a. Strongly Agree
    b. Agree
    c. Disagree
    d. Strongly Disagree
13. Comments