PENNSYLVANIA STATE UNIVERSITY

CYBERLIONS-B

November 9, 2024

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
94	9153	1350	6115.31	10,000

TEAM 67 SCORECARD

This table highlights the *team's* efforts for the 2024 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	839	41.95%	26
Security Documentation	825	82.50%	52
C-Suite Panel	527	52.70%	89
Red Team	1681	67.24%	21
Blue Team	2000	100.00%	1
Green Team Surveys	1420	94.67%	24
Deductions	0		
Overall	**7292**	**72.92%**	**24**

ANOMALY SCORING

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. These carefully crafted challenges not only test technical skills but also emphasize daily time management skills that professionals must demonstrate to effectively perform their roles. Most anomalies are mapped to the NIST NICE Framework and fall into one of seven work role categories: *Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defense, Investigation, Cyberspace Intelligence, and Cyberspace Effects. Some anomalies may also be categorized as Energy or "Other".* For those mapped to the NIST NICE Framework, their will include the mapping to associated knowledge, skill, ability, and task roles within its respective category, offering students with a comprehensive idea of the wide range of responsibilities cybersecurity professionals face while in the field.

Anomaly Score	839

Below highlights whether the anomaly was correct or incorrect for your team.

1	yes
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	no
10	yes
11	no
12	Not Answered
13	yes
14	no
15	yes
16	yes
17	yes
18	yes
19	yes
20	no
21	yes
22	yes
23	yes
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	no
29	Not Answered
30	no
31	no
32	yes
33	Not Answered
34	yes
35	yes
36	no
37	no
38	no
39	yes
40	no
41	yes
42	Not Answered
43	no
44	Not Answered
45	no
46	yes
47	no
48	yes
49	yes
50	yes
51	yes
52	yes
53	no
54	Not Answered
55	yes
56	yes
57	no
58	yes
59	yes
60	yes
61	yes
62	yes
63	yes
64	no
65	Not Answered
66	no
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	yes
72	yes
73	Not Answered
74	yes
75	Not Answered
76	yes
77	yes

ORANGE TEAM

Security Documentation

Blue team participants should use the Security Documentation section as an opportunity to highlight unique approaches to securing their infrastructure.

Security Documentation Score	825

Strong Points	*Areas of Improvement*
• Overall, the report is well done, especially the sections on the system overview and known vulnerabilities, which were completed effectively. Good job! • The team employed a multi-layered hardening approach • Your team did a very good job preparing this document. Your system overview describes the system very well and uses the language suitable for both technical and executive audience. You identified many vulnerabilities and your mitigation steps are appropriate. Your system hardening approach shows that you have a good understanding of hardening, you think methodically, and you apply layered mitigation approach to first protect the perimeter and external access and then focus on security weaknesses inside the system. You did a very good job there. • Good overview, worded in a way senior executives could understand. Vulnerabilities were sufficiently identified, and mitigations were well explained. Good justifications for each hardening step.	• The network diagram and system hardening sections present potential for improvement. Incorporating a legend into the network diagram would enhance its clarity, and adding a bit more technical detail would make it more robust. Furthermore, including justification for the steps taken by the team would significantly improve the document, ensuring that the rationale is clear and reasonable. • While the diagram includes main elements, it lacks logical connections and details, limiting clarity • Your Asset Inventory is missing open ports for Windows Server 2016. • No ports or protocols were identified for CNC on the asset list. A legend would be ideal for the network diagram.

C-Suite Panel

C-Suite Panel will be a pre-recorded video based on the task outlined in this document. This video should be recorded and placed somewhere accessible to judges.

C-Suite Panel Score	527

Strong Points	*Areas of Improvement*
• Very good cost estimations • Adding the industry average security posture score and how your recommendation result in a higher than average score was a nice touch. • Full notes on next answer. Really appreciated the specific figures given.	• Security posture math isn't explained. Facts were thrown at us, without introduction or context. • Consider font size and color choice, the bar graph was tough to read. Include and clearly define the risks related to business concerns and your high priority recommendations.

• Professional presentation with contributions from all team members.	• REQUIRED ELEMENTS - 4/4 • RISKS TO CORE BUSINESS- 2/4 • quantified security postures are good, but please explain which metric this is, and how this was determined (internal audit, external audit, internal analysis, etc) • if this is a timeline, please show some specific dates. at minimum, probably want 1 month out, 3 months out, 6 months, 1 year, 5 years • minimal jargon • no discussion of risk of degraded energy output in AOR • STRATEGY TO REDUCE RISKS - 3/4 • establishing a SOC is good, but expensive and time consuming (not to mention staffing it). would have liked to see discussion of these factors • trainings - again, no details on what trainings cover. identifying phishing emails? consequences of breaches at similar orgs? SANS trainings for the cybersecurity team? • cybersecurity tools - SIEM mentioned, and it feels like this section might be better called "deploy SIEM" than "Cybersecurity Tools", as the main argument I heard for SIEM is the ability to concentrate alerts behind "a single pane of glass". However, again, no discussion of timeline, cost, or risks (setting up a SIEM is one of the major hurdles in setting up a SOC) • compliance - no discussion beyond "it is good to comply". i promise that all of these regulated entities have well-funded compliance departments. in order to give a point for this, i'd have to hear what they ought to be doing differently (establish dedicated NERC CIP compliance team, provide content for training program connecting compliance requirements to mitigating security risk, etc) • Overall, each of these items has good potential, but needs to be developed further. 2/4 at this point but - • Bumping this a point for the specific numbers given on the Cost slide, especially like the breakdown between employees and software. In the future, be sure to distinguish between operational

	and capital expenses, this is very very important to C-Suite and money types. Good that this broadly maps to the risks on the previous slide (Cybersecurity Tools, SIEM, Cybersecurity Training, that's 3; not sure what Infosec Department is, how it connects to Compliance if at all, and how it differs from Cybersecurity Tools) • FUTURE EVENTS - these are not risks, these seem to be responses to possible risks or possible benefits of adopting the recommendations on the previous slides. in that sense they're quite good • HIGH PRIORITY RECOMMENDATIONS - 1/4 I do not see a High Priority Recommendations section. Some recommendations were given in the Risk Reduction Strategy, but at no point is a distinction made between short-term wins and long-term goals. • QUALITY - 3/4 • many of the audio clips feel like they're starting a couple seconds late. transitions are extremely abrupt, no discussion after Maguire regarding people's names and roles • OVERALL - You are missing several sections of the rubric. I like that you included specific figures for Risks to Core Business and Strategy to Reduce Risks: Cost, but no sources were given for these. Audio quality is also questionable and certain clips feel like they're starting 1-2 seconds in. • More clearly identify business risks and impact with transition to strategy that directly speaks to the risks. More practice would likely result in more effective use of executive time.

RED TEAM SCORING

RED TEAM FLAG INPUTS (ASSUME BREACH & WHACK A MOLE)

This year we will be using ***Assume Breach*** for part of your Red team score. This will be worth *1000 points*. The purpose of the assume breach model is for your team to investigate and accurately report back incident details after experiencing a successful execution of an attack chain. The **Whack a Mole** portion of the Red team score will be worth *750 points*. This will be done in a traditional method of “hacking” through holes created through known vulnerabilities in the system.

Assume Breach

AB1	AB2	AB3	AB4	AB5	AB6	AB7	AB8	AB9	AB10
75	100	0	75	25	25	25	50	100	100

Whack a Mole	
WAM1	WAM2
375	281

Automated Script Check – Vulnerability

This portion of the Red team score will be worth *750 points*. This will be done via an automated scripted check.

Automated Script Score	450

BLUE TEAM SCORE

The Blue team scoring (service scans) is completely based on the Blue team's ability to keep services active. In an industry environment, every security professional's primary responsibility is to keep business operational and secure. 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 scoreboard polling system. Each service is scored and weighted the same, which means availability is scored purely on the service being operational.

Service Scans	AI Algorithm Score
1600	400

GREEN TEAM SCORE

The Green team will review and complete surveys to evaluate each Blue team system's usability and user experience. Points will be awarded based on the user's ability to complete the tasks outlined in the user acceptance testing guide at the end of this document. The Green team will assess their ability to validate these tasks. The guide that will be provided to Green team users is available in the Rubrics section. It is in your best interest to run through this user testing to ensure that you can complete all the steps they are.

Green Team Score
1420