Using the NICE Framework as a Metric to Analyze Student Competencies

Jennifer Fowler
Jfowler@anl.gov

Nate Evans
nevans@anl.gov

Argonne National Laboratory
9700 S Cass Avenue, Lemont IL 60439

Abstract - This paper describes how the Department of Energy's CyberForce Competition™ uses anomalies to map collegiate teams' comprehension of different topics in cybersecurity. The competition is currently in its fourth iteration with a fifth planned in November 2019. Anomalies are challenges that collegiate teams must solve in order to receive points and vary in nature, timing, and skillset. All successful teams are able to manage the scale and prioritize which anomalies to complete. This paper identifies which National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework pillars students scored in the upper percentile, and which topics students averaged a lower score. These results may help educators in creating training programs, classes and curriculum to help close these knowledge gaps.

Keywords

NICE Framework, student competencies, competition, red team, blue team, vulnerabilities, anomalies, cyber, cybersecurity, CyberForce, Department of Energy, knowledge, skills, abilities, workforce development, knowledge gaps

1. INTRODUCTION

The Department of Energy's Annual CyberForce Competition™[1] is a one-day event that tests collegiate teams' ability to detect and respond to threat actors and vulnerabilities utilizing a common red vs blue setup. A typical competition has a Blue Team (defenders) that protect a network infrastructure from the Red Team (attackers). A blue team consists of college students who secure and harden their competition system. A red team consists of students or industry professionals that work to cause cyber destruction to the blue teams' network infrastructures. The competition is scored utilizing a point system. The blue team with the most points at the end of the competition is declared the winner of the event.

This event seeks to simulate the current real-world atmosphere that individuals face in cybersecurity by giving students a dynamic environment consisting of a combination of legacy systems and the flexibility to deploy innovative solutions to mitigate vulnerabilities installed on rudimentary systems, such as moving target defense (MTD), defense in depth, custom operating systems or other innovative approaches.

2. TOPOLOGY

Each Blue Team comprises college students that defend their systems against threat actors. The Red Team comprises industry professionals, national laboratory employees, and volunteers who have a background in information technology (IT). Red Team members attempt to infiltrate the Blue Teams' systems and cause disruption or system failure of either the backend interface, customer portal, or industrial control system (ICS). The CFC also adds a "Green Team" element, which consists of members who evaluate the usability of the Blue Teams' customer portal by following provided instructions to perform their given tasks. The White Team comprises the technical staff

[1] For more information, please go to: https://cyberforcecompeition.com

responsible for running and maintaining the competition. All of the aforementioned teams work synchronously to contribute to the competition. Figure 1 shows a diagram of teams and their subsequent responsibilities.

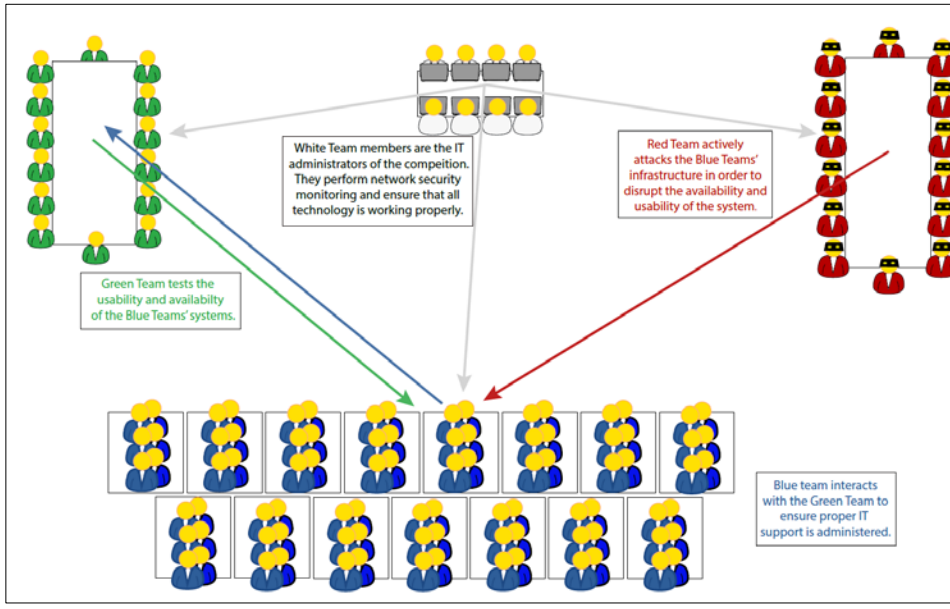

Figure 1: CyberForce Competition Communication Flow

The CyberForce Competition also incorporates anomalies, which are challenges based on different cybersecurity skillsets and are meant as additional challenges to pull attention away from the traditional job of protecting systems from cyber-attack. Over the years the number of anomalies has grown, reaching a point where ideally not every team can accomplish them all.

Anomaly distribution breakdown:

- 2016: 5 total
- 2017: 8 total
- 2018 April: 48 total
- 2018 December: 68 total

As shown above, the anomalies committee has expanded both the type and number of anomalies that are distributed to competitors in order to more accurately gauge proficiencies. Anomalies were created in partnership with seven national laboratories: Argonne National Laboratory (ANL); Brookhaven National Laboratory (BNL); Idaho National Laboratory (INL); Lawrence Berkeley National Laboratory (LBNL); Oak Ridge National Laboratory (ORNL); Pacific Northwest National Laboratory (PNNL); and Sandia National Laboratory (SNL).

3. GOALS

Competition anomalies provide unique challenges for Blue Team competitors. The creation and deployment of anomalies was based on a five-pronged goal.

1. Expose students to real world challenges that may occur within the field of information security;
2. Support the Red Team with added exploits as needed;
3. Measure students' ability to solve a variety of technical problems that are mapped to a widely used framework;
4. Simulate a real-world network where administrators may not be able to focus on monitoring systems due to other challenges or workloads; and
5. Provide a management or task coordination role that successful teams would need to select and prioritize anomalies based on strengths and weaknesses among the team.

The success or failure of the Blue Teams' ability to solve the anomalies allowed for a look into potential knowledge gaps in computer science and cybersecurity comprehension. These anomalies produced metrics that provided insight into the Blue Teams' comprehension of different knowledge, skills, and abilities.

As stated above, one of the goals of this competition is to acquire measurable metrics in order to analyze and identify comprehension gaps. These metrics, applied the NICE Framework, help identify knowledge gaps.

Since these collegiate competitors are likely to enter the workforce within the next few years, comprehension gap identification becomes important in order to aid in workforce development. Through trend analysis, this research can also be applied towards improving K-12 curriculum, post education training needs, and inform colligate class shortfalls in order to prepare the next generation of cyber defenders.

4. METHODOLOGY

The anomalies committee created challenges that mapped to the NICE Cybersecurity Workforce Framework, which is part of the National Institute of Standards and Technology (NIST) 800-181, a national resource that categorizes and describes cybersecurity work. [2] The NICE Framework helps establish capability indicators that can help organizations and educational institutions build formal qualification requirements based off the framework. This framework aids organizations in meeting cybersecurity workforce development goals. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. Figure 2 shows the categories upon which the NICE framework is

Figure 2: NICE Framework Categories

[2] https://csrc.nist.gov/publications/detail/sp/800-181/final

built. The rest of this paper will explore the areas in which students excelled or fell short of solving anomalies that mapped to the NICE Cybersecurity Workforce Framework.

5. FRAMEWORK MAPPING

The NICE Framework has seven high level categories: Securely Provision; Analyze; Operate and Maintain; Oversee and Govern; Collect and Operate; Protect and Defend, and Investigate. The framework has 33 specialty areas that target distinct areas of cybersecurity work. The framework also has 52 work roles that are detailed groupings of cybersecurity work, composed of specific knowledge, skills, and abilities (KSA) required to perform tasks in a work role. The 68 anomalies created for the competition are mapped to the NICE Framework categories as well as the specific KSA ID, as shown in the appendix.

Each lab was responsible for creating anomalies that were defined within a certain framework category. Each anomaly is then mapped to a specific task and work role.

- ANL: Protect and Defend
- BNL: Securely Provision
- INL: Operate and Maintain
- LBNL: Oversee and Govern
- ORNL: Analyze
- PNNL: Collect and Operate
- SNL: Investigate

Some labs decided to create clusters of anomalies, where students had to parse through large swaths of information in order to deduce the answer. BNL required students to find the insider threat within seemingly innocuous (fictions) employee user data. PNNL had students recover answers from a forensics machine in order to receive points. However, a large majority of students were tested on standalone anomalies that tested their knowledge of different tools (Splunk, Wireshark, Ida Pro) and skills (forensic work, reverse

engineering, packet analysis) in order to find the flag or answer and submit it to the scoreboard.

The scoreboard is a multi-functional tool that allows students to submit anomalies, intrusion reports, and documentation. It also checks to see if services (such as ModBus, FTP or other protocols) are up and active. The scoreboard also has a survey area where green team can to interface with the competition and submit the usability scores of the various blue teams.

Due to the complex nature of the scoreboard and the number of requests that it was trying to process, the scoreboard could not handle the number of requests being made across seven different laboratories, and its services (including anomaly submission) were down for a part of the competition. As such, the following anomaly data may not reflect anomalies that students had finished or completed, but did not have a chance to submit.

In the Appendix of this document, Table 1 identifies the following:

- Hour the anomaly was deployed,
- Anomaly question,
- Anomaly answer,
- NICE task and KSA ID,
- Point allocation, and
- Average points and overall percentage of students that received points.

6. GAP ANALYSIS

This section will identify gap analysis and proficiency connections to KSAs for each anomaly. Table 2 shows the anomaly number, and how many teams attempted each anomaly.

Table 2: Number of Teams that Attempted Each Anomaly

Anomaly Number	Number of Teams that Attempted Anomalies
Anomaly 1	50
Anomaly 2	45
Anomaly 3	39
Anomaly 4	40
Anomaly 5	40
Anomaly 6	26
Anomaly 7	25
Anomaly 8	28
Anomaly 9	30
Anomaly 10	28
Anomaly 11	29
Anomaly 12	22
Anomaly 13	27
Anomaly 14	28
Anomaly 15	30
Anomaly 16	12
Anomaly 17	10
Anomaly 18	13

Anomaly Number	Number of Teams that Attempted Anomalies
Anomaly 35	15
Anomaly 36	4
Anomaly 37	4
Anomaly 38	10
Anomaly 39	16
Anomaly 40	6
Anomaly 41	17
Anomaly 42	18
Anomaly 43	6
Anomaly 44	3
Anomaly 45	23
Anomaly 46	13
Anomaly 47	4
Anomaly 48	11
Anomaly 49	2
Anomaly 50	6
Anomaly 51	25
Anomaly 52	2

Anomaly 19	4
Anomaly 20	5
Anomaly 21	2
Anomaly 22	3
Anomaly 23	2
Anomaly 24	5
Anomaly 25	1
Anomaly 26	2
Anomaly 27	1
Anomaly 28	9
Anomaly 29	2
Anomaly 30	3
Anomaly 31	2
Anomaly 32	2
Anomaly 33	1
Anomaly 34	1

Anomaly 53	10
Anomaly 54	6
Anomaly 55	13
Anomaly 56	4
Anomaly 57	2
Anomaly 58	7
Anomaly 59	2
Anomaly 60	2
Anomaly 61	2
Anomaly 62	40
Anomaly 63	1
Anomaly 64	32
Anomaly 65	35
Anomaly 66	2
Anomaly 67	26
Anomaly 68	32

This statistical data indicates that students had hesitancies with the forensics machine anomalies (anomalies 21-31). These anomalies map to the Collect and Operate category. Students seemed to have better success with the network pcap forensics (anomalies 35, 36, 41, 43, 48, 49, 54, 56, 57). This indicates that students have a firm grasp on the following tasks: T0286, T0238, T0396, T0240, and knowledge identifications: K0001, K0179, K0178, K0339, S0004.

Task Identification Numbers:

- T0286: Perform file system forensic analysis
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost)
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools

KSA Identification Numbers:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Students also seemed to struggle with anomaly 32 – 34, 49, anomaly 52, 57, 59-61, 63, and 66.

Anomaly 32 is a forensics anomaly that maps to the Operate and Maintain pillar.

Task Identification Number:

- T0696: Exploit network devices, security devices, and/or terminals or environments using various methods or tools.

KSA Identification Number:

- A0005: Ability to decrypt digital data collections
- A0035: Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.

Anomaly 33 is a password analysis in a memory dump question that maps to the Analyze pillar.

Task Identification Number:

- T0294: Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.

KSA Identification Number:

- K0129: Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).

Anomaly 34 asks the student to identify a bad file, and maps to the Investigate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.

KSA Identification Number:

- K0017: Knowledge of concepts and practices of processing digital forensic data.
- K0060: Knowledge of operating systems
- K0117: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).

Anomaly 49 comprises network pcap analysis, which maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0396: Process image with appropriate tools depending on analyst's goals.

- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 52 comprises malware origin analysis, and maps to the Analyze pillar.

Task Identification Number:

- T0182: Perform tier 1, 2, and 3 malware analysis
- T0288: Perform static malware analysis

KSA Identification Number:

- A0010: Ability to analyze malware
- K0479: Knowledge of malware analysis and characteristics
- S0131: Skill in analyzing malware

Anomaly 57 is a network pcap analysis question that maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).

- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 59 is challenge that asks students to find the key used to encrypt the file and maps to the Investigate pillar.

Task Identification Number:

- T0553: Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.

KSA Identification Number:

- K0017: Knowledge of concepts and practices of processing digital forensic data.
- K0060: Knowledge of operating systems.
- K0117: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).

Anomaly 60 was a trivia-based question that focused on HIPAA and maps to the Oversee and Govern pillar.

Task Identification Number:

- T0419: Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.

KSA Identification Number:

- K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

Anomaly 61 is trivia-based framework question that maps to Oversee and Govern pillar.

Task Identification Number:

- T0419: Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.

KSA Identification Number:

- K0004: Knowledge of cybersecurity and privacy principles.

Anomaly 63 is a trivia-based anomaly based on bloom's taxonomy, and maps to the Oversee and Govern pillar.

Task Identification Number:

- T0419: Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.

KSA Identification Number:

- K0216: Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).

Anomaly 66 is a trivia-based anomaly that asked a question on the U.S. Commerce Control Lists, and operates to the Oversee and Govern pillar.

Task Identification Number:

- T0419: Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.

KSA Identification Number

- K0196: Knowledge of Import/Export Regulations related to cryptography and other security technologies.

Statistical analysis indicates that students have hesitancies towards the Collect and Operate pillar. In order to aid workforce development, students may want to focus on forensic skills and abilities, as well as policy knowledge.

In contrast, students seemed gravitate towards anomalies based on insider threat identification (1-15), mapping to the Securely Provision pillar. This set of anomalies had students parse through logs to try to identify anomalous behavior inside a fictitious company, called Totient, Inc.

Students had to write code to parse and analyze the logfile of Totient's intranet web (HTTP) server farm. The goal is to identify and characterize non-standard browsing behavior of agents residing behind the firewall. Infrequent probing of internal web servers to uncover potential configuration mistakes, for example in document management permissions, is often a precursor to successful industrial espionage. Using histograms or other analysis techniques, you should develop statistical profiles of employees accessing the Totient intranet to determine if these patterns can be leveraged to identify suspicious activity.

Task Identification Number:

- T0708: Identify threat tactics, and methodologies.
- T0433: Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.

KSA Identification Number:

- K0107: Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
- S0120: Skill in reviewing logs to identify evidence of past intrusions

Statistical evidence indicates that students feel comfortable writing code to parse data, and perform data analysis. This is supported by the relatively high scores associated with the completion of these anomalies, as shown in Table 3.

7. ANOMALY SCORING

There is a loose correlation between student hesitancy and the proficiency with which students correctly answered these challenges. In general, Tables 2 and 3 indicate that a lower number of teams attempting anomalies correlates with lower averages for correct submissions. Similarly, the more teams that had more confidence in certain anomalies tended to score higher. This indicates that students have a comfort level with the Securely Provision category, and have the knowledge set to write code, conduct log analysis, and identify threat tactics and methodologies, as shown in Table 3. It is important to note that not all teams attempted every anomaly, and that Table 3 identifies the average points for the teams that decided to participate in each anomaly.

Table 3: Average Points per Anomaly

Anomaly Number	Average Points	Maximum Point Allotment	Percentage
Anomaly 1	2.274509804	4	0.568627451
Anomaly 2	2.166666667	4	0.541666667
Anomaly 3	3.692307692	4	0.923076923
Anomaly 4	3.61	4	0.9025
Anomaly 5	3.512195122	4	0.87804878

Anomaly 6	5.230769231	8	0.653846154
Anomaly 7	6.4	8	0.8
Anomaly 8	4	8	0.5
Anomaly 9	7.2	8	0.9
Anomaly 10	7.428571429	8	0.928571429
Anomaly 11	4.551724138	11	0.413793103
Anomaly 12	5.454545455	12	0.454545455
Anomaly 13	14.28571429	20	0.714285714
Anomaly 14	15	20	0.75
Anomaly 15	19.33333333	20	0.966666667
Anomaly 16	16.66666667	20	0.833333333
Anomaly 17	1.6	8	0.2
Anomaly 18	1.153846154	4	0.288461538
Anomaly 19	1.75	4	0.4375
Anomaly 20	6	8	0.75
Anomaly 21	0	4	0
Anomaly 22	0	4	0
Anomaly 23	0	4	0
Anomaly 24	0	4	0
Anomaly 25	0	8	0
Anomaly 26	0	4	0

Anomaly 27	0	4	0
Anomaly 28	1.333333333	4	0.333333333
Anomaly 29	0	4	0
Anomaly 30	0	4	0
Anomaly 31	0	4	0
Anomaly 32	0	4	0
Anomaly 33	0	4	0
Anomaly 34	0	4	0
Anomaly 35	0	4	0
Anomaly 36	3	4	0.75
Anomaly 37	0	8	0
Anomaly 38	0	4	0
Anomaly 39	2.5	8	0.3125
Anomaly 40	4	8	0.5
Anomaly 41	0.470588235	8	0.058823529
Anomaly 42	2.222222222	8	0.277777778
Anomaly 43	2.5	8	0.3125
Anomaly 44	0	4	0
Anomaly 45	3.826086957	4	0.956521739
Anomaly 46	0.615384615	8	0.076923077
Anomaly 47	0	8	0

Anomaly 48	7.272727273	8	0.909090909
Anomaly 49	0	5	0
Anomaly 50	0	4	0
Anomaly 51	5.12	8	0.64
Anomaly 52	0	20	0
Anomaly 53	0	5	0
Anomaly 54	1.333333333	8	0.166666667
Anomaly 55	2.307692308	5	0.461538462
Anomaly 56	0	20	0
Anomaly 57	0	20	0
Anomaly 58	5	10	0.5
Anomaly 59	10	20	0.5
Anomaly 60	2	2	1
Anomaly 61	1	2	0.5
Anomaly 62	2	2	1
Anomaly 63	2	2	1
Anomaly 64	2	2	1
Anomaly 65	2	2	1
Anomaly 66	2	2	1
Anomaly 67	3	3	1
Anomaly 68	3	3	1

Statistical evidence shows that students scored well in trivia-based challenges, ranking in the highest percentile (Anomalies 60 – 68). Data from Table 2 and Table 3 indicates that not only are students comfortable with writing code and parsing data, but also have solid comprehension in this area, ranking in the higher percentile of the overall competition (Anomalies 1 – 15).

Anomalies 1 – 15 map to the following Task and KSA identification numbers.

Task Identification Number:

- T0708: Identify threat tactics, and methodologies.
- T0433: Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.

KSA Identification Number:

- K0107: Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
- S0120: Skill in reviewing logs to identify evidence of past intrusions.

Students seemed to struggle with anomalies 21-35, 37, 38, 41, 44, 46, 47, 49, 50, 52, 53, 56, 57

Anomalies 21 – 35 are the aforementioned anomalies that students hesitated to complete, and their task and KSA identification can be found in the *Anomalies Attempted* section.

Anomaly 37 is a was a Snort malware analysis anomaly, and maps to the Protect and Defend pillar.

Task Identification Number:

- T0288: Perform static malware analysis.

KSA Identification Number:

- S0025: Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
- S0020: Skill in developing and deploying signatures
- K0472: Knowledge of intrusion detection systems and signature development.
- K0191: Signature implementation impact for viruses, malware, and attacks.

Anomaly 38 is a network analysis anomaly, and maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.

KSA Identification Number:

- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 41 is a network pcap analysis anomaly, and maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 44 is a network pcap anomaly, and maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.

- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 46 is a phishing email analysis anomaly, and maps to the Analyze pillar.

Task Identification Number:

- T0036: Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.

KSA Identification Number:

- S0052: Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).

Anomaly 47 is a image analysis anomaly, and maps to the investigate pillar.

Task Identification Number:

- T0396: Process image with appropriate tools depending on analyst's goals.

KSA Identification Number:

- K0132: Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.

Anomaly 49 comprises network pcap analysis, which maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).

- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 50 is a file analysis anomaly, and maps to the Operate and Maintain pillar.

Task Identification Number:

- T0532: Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.

KSA Identification Number:

- S0109: Skill in identifying hidden patterns or relationships.

Anomaly 52 comprises malware origin analysis, and maps to the Analyze pillar.

Task Identification Number:

- T0182: Perform tier 1, 2, and 3 malware analysis
- T0288: Perform static malware analysis

KSA Identification Number:

- A0010: Ability to analyze malware
- K0479: Knowledge of malware analysis and characteristics
- S0131: Skill in analyzing malware

Anomaly 53 deals with string analysis to dissect iptables, and maps to the Investigate pillar.

Task Identification Number:

- T0615: Conduct in-depth research and analysis
- T0706: Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)

KSA Identification Number:

- K0167: Knowledge of system administration, network, and operating system hardening techniques.

Anomaly 56 is a network pcap analysis anomaly, and maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.

- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

Anomaly 57 is a network pcap analysis question that maps to the Collect and Operate pillar.

Task Identification Number:

- T0286: Perform file system forensic analysis.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

KSA Identification Number:

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0178: Knowledge of secure software deployment methodologies, tools, and practices.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0004: Skill in analyzing network traffic capacity and performance characteristics.

8. CONCLUSION

While it is imperative to continue to educate students on all aspects of cybersecurity, anomaly analysis points out potential gaps in comprehension in the Collect and Operate category and the Investigate category. Additionally this analysis shows strong comfort with the Protect and Defend category demonstrating the Nation's strong coursework and student interest in that area. Continued analysis to grow the dataset and to map performance metrics to individual students is still needed, but helping to understanding this knowledge mapping and closing these knowledge gaps will help the nation's future workforce tasking with securing our cyber infrastructure. Additionally, by addressing these knowledge gaps even earlier in student curriculum, ideally even in K-12, educators can accelerate competencies in students by building a solid foundation of fundamental cybersecurity.

APPENDIX

Table 1: Anomaly Timeline

Timeline	Question	Solution	Task	KSA ID	Point Allotment	Avg. Points	Avg. Percentage
Hour 1 - Anomaly 20	**Anomaly 1**: **CFM Splunk Anomaly** You have been given access to a Splunk instance (Connection information provided separately) that was used to collect and organize logs for a fictitious company, including a website, "imreallynotbatman.com". This website suffered an intrusion that resulted in defacement, and a number of other attacks. For this anomaly, we want you to research the incident and identify logs that show proof of scanning activity that found vulnerabilities. Once you identify the logs, please document aspects of the incident that would be appropriate for sharing with your industry peers to help them defend against a similar attack. At a minimum, please include the following information in your report: o The IP address used to initiate the scanning and attack o The type of Content Management System that was targeted o Using the user agent string, identify the browser that the attacker used. For reference, the attack occurred on August 10th, 2016. You also should be doing all your searches against the following index: index="botsv1".	MANUAL GRADING	T0339, T0161	K0106	Medium - 8 points	6	75%

Hour 3 - Anomaly 37	**Anomaly 2**: **Snort Anomaly** The security team at your company has recently produced a log of network traffic that is particularly troubling, as they believe it might have included the exchange or Malware. Using an intrusion detection system such as Snort, analyze the packet capture they have provided to you (snort_anomaly_capture.pcap). Using the capabilities of this software, determine the name of the first incident of malware present (specifically look at traffic from 192.168.1.135:445 to 192.168.1.112:49759). Submit the name of the malware as your answer (exclude the MALWARE-CNC designation before the name).	Win.Trojan.Doublepulsar	T0288	S0025, S0020, K0472, K0191	Medium - 8 points	0	0%
Hour 4 - Anomaly 45	**Anomaly 3: Wireshark Anomaly** A user at your company was recently seen to be browsing a potentially malicious website. A packet capture was saved from this website visit, and you have been tasked with determining what image the user opened from the website. Analyze this packet capture file (anomaly_packets.cap) with an appropriate tool and provide the answer of what animals (plural noun) are displayed in the file "DSC07858.JPG".	DOLPHINS	T0295, T0240	K0062, K0301, S0156, S0046, K0398	Easy - 4 points	3.82	95.65%
Hour 5 - Anomaly 51	**Anomaly 4**: **Asymmetric Anomaly** Decrypt the following file with my public key. Key ID 2E33D58C	B	T0416	S0138	Medium - 8 points	5.12	64%
Hour 1 - Anomaly 16	**Anomaly 5**: Cryptopuzzle	RED KING	T0049	K0308, K0018	Hard-20	16.66	83.33%

Hour 1 - Anomaly 1	Anomaly 1: Too many login failures in one week (>25/day)	Kurt.Hardy	T0708, T0433	K0107, S0120	Easy - 4 points	2.27	56.86%
Hour 1 - Anomaly 2	Anomaly 2: Too many valid logins in one week (>50/day)	Alice.Rubio	T0708, T0433	K0107, S0120	Easy - 4 points	2.16	54.16%
Hour 1 - Anomaly 3	Anomaly 3: Too many "same page" requests in one week (>50/day)	Wade.Carlson	T0708, T0433	K0107, S0120	Easy - 4 points	3.69	92.31%
hour 1 - Anomaly 4	Anomaly 4: Too many "different page" requests in one week (>50/day)	Keisha.Stafford	T0708, T0433	K0107, S0120	Easy - 4 points	3.61	90.25%
Hour 1 - Anomaly 5	Anomaly 5: Impossibly fast document requests in one day (~1/sec)	Tom.Lowe	T0708, T0433	K0107, S0120	Easy - 4 points	3.51	87.80%
Hour 1 - Anomaly 6	Anomaly 6: Too many logins from too many different machines (>2/day)	Judy.Knight	T0708, T0433	K0107, S0120	Medium - 8 points	5.23	65.38
Hour 1 - Anomaly 7	Anomaly 7: Too many logins from too many different locations (>2/day)	Spencer.Jones	T0708, T0433	K0107, S0120	Medium - 8 points	6.4	80%
Hour 1 - Anomaly 8	Anomaly 8: Too many forbidden HTTP 403 requests for same page (~2/week)	Lori.Roberts	T0708, T0433	K0107, S0120	Medium - 8 points	4	50%
Hour 1 - Anomaly 9	Anomaly 9: Too many uncommon HTTP methods (~2/week)	Brian.Moyer	T0708, T0433	K0107, S0120	Medium - 8 points	7.2	90%
Hour 1 - Anomaly 10	Anomaly 10: Too many void search results in a week (>50/day)	Sally.Beck	T0708, T0433	K0107, S0120	Medium - 8 points	7.43	92.86%
Hour 1 - Anomaly 11	Anomaly 11: Too many unnatural login times (>4/day on Sat & Sun early AM)	Robert.Gross	T0708, T0433	K0107, S0120	Hard - 11 points	4.55	41.38%
Hour 1 - Anomaly 12	Anomaly 12: Non-standard UserAgent (~1/week)	Peggy.Farley	T0708, T0433	K0107, S0120	Hard - 12 points	5.45	45.45%
Hour 1 - Anomaly 13	Anomaly 13: NLB bypass - Direction Connection to Web1 (~1/week)	Mike.Price	T0708, T0433	K0107, S0120	Hard - 20 points	14.29	71.43%
Hour 1 - Anomaly 14	Anomaly 14: Too "consistent in time" searches (~1/day)	Mandy.Steele	T0708, T0433	K0107, S0120	Hard - 20 points	15	75%
Hour 1 - Anomaly 15	Anomaly 15: HTTPS downgrade - HSTS bypass (~1/week)	Dallas.Roth	T0708, T0433	K0107, S0120	Hard - 20 points	19.33	96.67%
Hour 1 - Anomaly 17	Anomaly 2: BruteForceMe	TBD	T0643	K0362	Medium - 8 points	1.6	20%
Hour 2 - Anomaly 32	Anomaly 3: Captain Planet	I'm_like_an_XOR_gate.	T0696	A0005, A0035	Easy - 4 points	0	0%

		I_literally_can't_even.					
Hour 5 - Anomaly 50	Anomaly 6: Sea What?	1_Nibble_	T0532	S0109	Easy - 4 points	0	0%
Hour 2 - Anomaly 33	Anomaly 1: Password analysis in memory dump	predator	T0294	K0129	Medium - 8 Points	0	0%
Hour 3 - Anomaly 39	Anomaly 2: Malware analysis	username:password {Key is: Alphanetworks:wrgn28_dlob_dir412}	T0288	A0010	Medium- 8 Points	2.5	31.25%
Hour 1 - Anomaly 18	Anomaly 3: CVE Analysis Given a CVE that was used against the company what could have been done to prevent it. What measures should be taken in systems and with people.	MANUAL GRADING: {1. Struts} 2: For full points, the written report should describe: 1) A system for keeping track of components used to build each web application; 2) Procedures for checking for vulnerable versions of software frameworks; and, 3) Operational procedures for updating web applications.	T0036, T0047	K0536, T0554, T0085	Easy - 4 Points	115	28.85%
Hour 1 - Anomaly 19	Anomaly 4: Phishing Report Create a report to inform a company of a phishing attack		T0332	K0049, S0120	Easy - 4 Points	1.75	43.75%
Hour 4 - Anomaly 42	Anomaly 5: DLL Tracking	Flag1 OS name: RaspberryPi3 or Raspberry Pi 3 Flag2 Exploited bin file flag: BusyBox	T0286	K0116, K0132	Medium - 8 Points	2.22	27.78%

Hour 4 - Anomaly 46	Anomaly 6: Phishing email	CWT	T0036	S0052	Easy - 4 Points	0.61	7.69%
Hour 5 - Anomaly 52	Anomaly 7: Malware origin analysis	Yautja	T0182, T0288	A0010, K0479, S0131	Medium - 8 Points	0	0%
Hour 7 - Anomaly 60	Anomaly 1: This main regulation was first enacted in 1996 and contains five titles, with the second title known as the Administrative Simplification. It required national standards for electronic health care transactions as well as national identifiers for the providers, insurance plans, and employers. Name this legislation in full.	Health Insurance Portability and Accountability Act of 1996	T0419	K0003	Easy trivia - 2 points	2	100%
Hour 7 - Anomaly 61	Anomaly 2: This voluntary Framework has five functions: Identify, Protect, Respond, Recover, and what?	Detect	T0419	K0004	Easy trivia - 2 points	1	50%
Hour 7 - Anomaly 62	Anomaly 3: This framework provides a six step process that integrates security and risk management into the system development life cycle. It takes into account FIPS 199 & 200 as well as many NIST Special Publications.	Risk Management Framework	T0419	K0048	Easy trivia - 2 points	2	100%
Hour 7 - Anomaly 63	Anomaly 4: In the original Bloom's Taxonomy, knowledge, comprehension, application, analysis, synthesis, and evaluation were the main six categories. In the revised taxonomy, the six categories are: remember, understand, analyze, evaluate, create, and what?	Apply	T0419	K0216	Easy trivia - 2 points	2	100%
Hour 7 - Anomaly 64	Anomaly 5: This framework, which we utilize throughout this competition, provides a blueprint to categorize, organize, and describe cybersecurity work into categories, specialty area, work roles, tasks, and knowledge, skills, and abilities. Most people know it as the NICE Framework. What does NICE stand for?	National Initiative for Cybersecurity Education	T0419	K0233	Easy trivia - 2 points	2	100%
Hour 7 - Anomaly 65	Anomaly 6: Utilizing the Zachman Framework, if I wanted to identify the detailed who of my enterprise architecture, what would I need to provide.	Role Details	T0419	K0199	Easy trivia - 2 points	2	100%

Hour 7 - Anomaly 66	Anomaly 7: Encryption falls under the U.S. Commerce Control List. This list is broken into 10 categories. What category number does encryption fall under? (Please use numbers only).	5	T0419	K0196	Easy trivia - 2 points	2	100%
Hour 7 - Anomaly 67	Freebie – submit your favorite party parrot	N/a			Bonus - 3 points	3	100%
Hour 7 - Anomaly 68	Make your shield or crown and submit to the anomaly table	n/a			Bonus - 3 points	3	100%
Hour 7 - Anomaly 60	Anomaly 1: This main regulation was first enacted in 1996 and contains five titles, with the second title known as the Administrative Simplification. It required national standards for electronic health care transactions as well as national identifiers for the providers, insurance plans, and employers. Name this legislation in full.	Health Insurance Portability and Accountability Act of 1996	T0419	K0003	Easy trivia - 2 points	2	100%
Hour 1 - Anomaly 21	Anomaly 7: Forensics- Angry Employee 1 How much in USD ($) Bob demands to pay in ransom?	$100,000	T0286, T0238	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	0	0%
Hour 1 - Anomaly 22	Anomaly 8: Forensics- Angry Employee 2 What data is written into offset of 110?	6f6c 6c6f 772e 200a 596f 7572 2066 7269	T0286, T0238	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	0	0%
Hour 1 - Anomaly 23	Anomaly 9: Forensics- Log Analysis 1 How many entrees are in the log files for October 20?	3	T0286, T0238	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	0	0%
Hour 1 - Anomaly 24	Anomaly 10: Forensics- Log Analysis 2 How many records are there for the period of October 20 –October 23?	9	T0286, T0238	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	0	0%
Hour 1 - Anomaly 25	Anomaly 11: Forensics- Log Analysis 3 How many entries in each file records, records.1, records.2, records.3, records.4 respectively?	100 109 100 50 15	T0286, T0238	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	0	0%

Hour 1 - Anomaly 26	Anomaly 12: Forensics- Log Analysis 4 How many entries do the logs have in total?	374	T0286, T0238	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	0	0%
Hour 1 - Anomaly 27	Anomaly 13: Forensics- Log Analysis 5 How many calendar days was there no activity recorded?	2	T0286, T0238	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	0	0%
Hour 1 - Anomaly 28	Anomaly 14: Forensics- Log Analysis 6 How many times did the attacker fail to enter correct credentials?	15	T0286, T0238	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	1.33	33.33%
Hour 1 - Anomaly 29	Anomaly 15: Forensics- File Carving 1 Somewhere inside of this raw image there is a JPEG file. What is its MD5 hash?	F6672a8315f1 4ff24a5a a1046585d5f9	T0286, T0238	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	0	0%
Hour 1 - Anomaly 30	Anomaly 16: Forensics- Picture analysis	forensic analysis	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	0	0%
Hour 1 - Anomaly 31	Anomaly 17: Forensics and Cryptography	TBD	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	0	0%
Hour 2 - Anomaly 35	Anomaly 18: Network pcap 1- Heavens to Merge-atroyd	1587296	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	0	0%
Hour 2 - Anomaly 36	Anomaly 19: Network pcap 2 - Pixels	EVER ULTRA	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Easy - 4 Points	3	75%
Hour 3 - Anomaly 41	Anomaly 20: Network pcap 3 - Port Recon	172.20.10.154	T0286, T0238, T0396, T0240	K001, K0179, K0178,	Medium - 8 Points	0.47	5.88%

				K0339, S0004			
Hour 3 - Anomaly 43	Anomaly 21: Network pcap- 4 APIPA	000C29EE1B8C	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	2.5	31.25%
Hour 4 - Anomaly 48	Anomaly 22: Network pcap 5- Ain't nobody got time fo dat	AS8075	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	7.27	90.90%
Hour 5 - Anomaly 49	Anomaly 23: Network pcap 6 - Not so secret message	telnet_is_dangerous	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Hard - 20 Points	0	0%
Hour 5 - Anomaly 54	Anomaly 24: Network pcap 7 - Port Recon 2	FREEMAIL	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Medium - 8 Points	1.33	16.67%
Hour 6 - Anomaly 56	Anomaly 25: Network pcap 8 - It's gonna be Epic	1499816656	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Hard - 20	0	0%
Hour 6 - Anomaly 57	Anomaly 26: Network pcap 9 - Treasure Boat	Redr0v3r!^	T0286, T0238, T0396, T0240	K001, K0179, K0178, K0339, S0004	Hard - 20	0	0%
Hour 2 - Anomaly 34	Anomaly 1: bad_file Find the bad file	TBD	T0286	K0017, K0060, K0117	Easy - 4 Points	0	0%
Hour 6 - Anomaly 59	Anomaly 2: custom_encrypt Find the key used to encrypt the file.	TBD	T0553	K0017, K0060, K0117	Medium - 8 Points	10	50%
Hour 3 - Anomaly 40	Anomaly 3: easy_encrypt Find the key used to encrypt the file.	TBD	T0553	K0019	Easy - 4 Points	4	50%
Hour 4 - Anomaly 47	Anomaly 4: image_challenge	TBD	T0396	K0132	Easy - 4 Points	0	0%

Hour 5 - Anomaly 53	Anomaly 5: iptables Find the string that gets created as the iptables are hit by the traffic.	TBD	T0615, T0706	K0167	Medium - 8 Points	0	0%
Hour 6 - Anomaly 55	Anomaly 6: shell_callback	TBD	T0615	K0301, S0046	Easy - 4 Points	2.31	46.15%
Hour 6 - Anomaly 58	Anomaly 7: web_sploit	TBD	T0294, T0260	K0005, K0077	Medium - 8 Points	5	50%

ACRONYM LIST

ANL	Argonne National Laboratory
BNL	Brookhaven National Laboratory
CFC	CyberForce™ Competition
INL	Idaho National Laboratory
IT	Information Technology
KSA	Knowledge, Skills and Abilities
LBNL	Lawrence Berkeley National Laboratory
ORNL	Oak Ridge National Laboratory
MTD	Moving Target Defense
NICE	National Initiative for Cybersecurity Education
PNNL	Pacific Northwest National Laboratory
SNL	Sandia National Laboratory

REFERENCES

[1] Department of Energy – Cybersecurity, Energy Security, and Emergency Response, CyberForce™ Competition. https://cyberforcecompetition.com.

[2] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, SP 800-181. https://csrc.nist.gov/publications/detail/sp/800-181/final