Score!

Mapping the National Cyber League Competition Tasks to the Operational Security Testing Job Performance Model

Competitions

What we know

- Encourages ethical practice and skill development in a controlled, legal environment
- Presents authentic circumstances where students can apply theory and protocols skills learned in formal educational environments
- Access to mentoring, resources, potential employers
- Access to scholarships, internships, and job opportunities
- Opportunity to identify talent

What we believe

- Increased knowledge of the work of cyber professionals
- Diverse competitions provide anytime-anywhere learning opportunities for individuals (from high school to college and on to professionals and career changers)
- Contributes to the knowledge-base of practitioners to resolve current issues, develop new tools, technologies, and methodologies
- Contributes to curriculum and educator capacity to meet employer, and national security needs

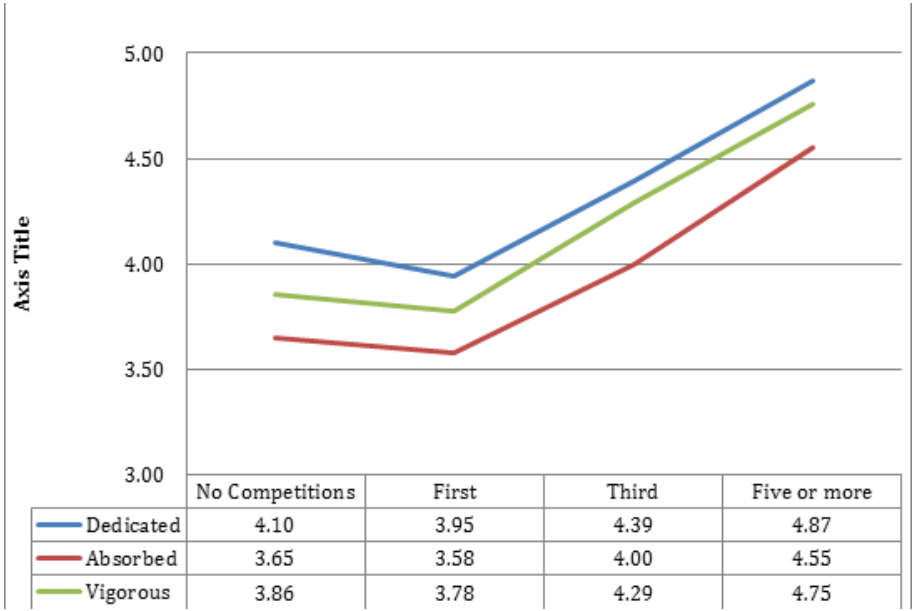
NCL Engagement Study

Approach: Survey participants in the National Cyber League Fall pilot season competitions using the Utrecht Work Engagement (UWE 9) scale (Schaufeli et al., 2006)

"Engagement is a positive, fulfilling, work-related state of mind that is characterized by vigor, dedication, and absorption."

- Source: Tobey, D., P. Pusey, D. Burley. March 2014. Engaging Learners in Cybersecurity Careers: Lessons from the launch of the National Cyber League. ACM Inroads: Special Section on Cybersecurity Education

Engagement - Experience



	No Competitions	First	Third	Five or more
Dedicated	4.10	3.95	4.39	4.87
Absorbed	3.65	3.58	4.00	4.55
Vigorous	3.86	3.78	4.29	4.75

Source: Tobey, D., P. Pusey, D. Burley. March 2014. Engaging Learners in Cybersecurity Careers: Lessons from the launch of the National Cyber League. ACM Inroads: Special Section on Cybersecurity Education

Novice Competitors over 3 Competitions

127 > 105 > 70

Source: Tobey, D., P. Pusey, D. Burley. March 2014. Engaging Learners in Cybersecurity Careers: Lessons from the launch of the National Cyber League. ACM Inroads: Special Section on Cybersecurity Education

NCL Study

The NCL Education Committee in Collaboration with the CyberSecurity Competition Federation and the National CyberWatch Center are mapping the NCL competition structure (competition, graveyard and labs) to the NBISE Job Performance Model (Security Testing Model) to:

- understand the types of skills the competition is involving
- determine the extent to which there is a good overlap of coverage within the preparatory activities versus the competition
- identify the most differentiating tasks within the job model
- discover the competition tasks which have preparatory materials to support them

NCL Long Term Goals

Long-term goals are to understand

- how students skill development can be improved by current workforce development programs.
- where we are vulnerable from a human level. (What attacks are most severe because we don't have the human capacity to address them.)

Job Performance Model

- Enhance the development of the cybersecurity workforce
- Provide a foundation for future certifications
- Guide curriculum, assessments, and development of technical knowledge, skills and abilities
- Identify the position of an individual along the progression through novice, beginner, proficient, competent, expert and master levels of expertise.

Source: Tobey, D. H., Reiter-Palmon, R., & Callens, A. (2012). *Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance. OST Working Group Report.* Idaho Falls, ID: National Board of Information Security Examiners.

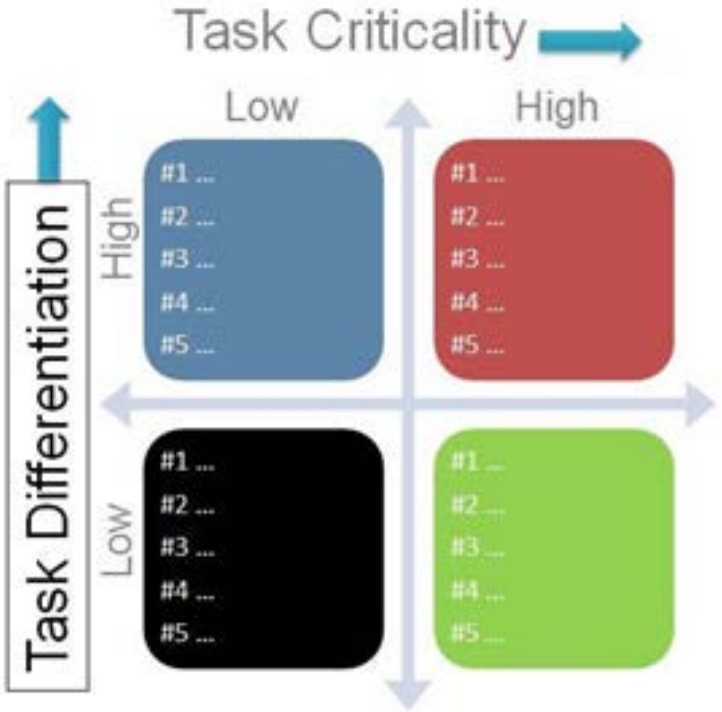
Critical-Differentiation Matrix

Fundamental and differentiating tasks that should best predict job performance

- 83 tasks as fundamental
- 20 indicators of the development of individual competence from novice to beginner, proficient, competition, expert, and master levels of expertise.

Source: Tobey, D. H. (2011). *A competency model of advanced threat response. ATR Working Group Report NBISE-ATR-11-02.* Idaho Falls, ID: National Board of Information Security Examiners.

Critical-Differentiation Matrix



Intrusion Analyst

MAJOR RESPONSIBILITIES

1. Analyze security incidents
2. Develop and manage personnel
3. Identify and mitigate vulnerabilities
4. Log security incidents
5. Respond to intrusions

SOURCE: O'Neil, L. R., Assante, M. J., & Tobey, D. H. (2012). *Snart Grid Cybersecurity: Job Performance Model Report* (Technical Report No. PNNL- 21639). Alexandria, VA: National Technical Information Service.

Intrusion Analyst

National Cybersecurity Workforce Framework Tasks

1. Analyze security incidents
   - Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
   - Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
   - Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
   - Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts
   - Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
   - Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event's history, status, and potential impact for further action
   - Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security

SOURCE: O'Neil, L. R., Assante, M. J., & Tobey, D. H. (2012). *Snart Grid Cybersecurity: Job Performance Model Report* (Technical Report No. PNNL- 21639). Alexandria, VA: National Technical Information Service.

Intrusion Analyst

ES-C2M2 Objectives to Determine Maturity Level

1. Analyze security incidents
   - Detect Cybersecurity Events
   - Identify and Respond to Threats
2. Develop and manage personnel
   - Control the Workforce Lifecycle
   - Develop Cybersecurity Workforce
   - Increase Cybersecurity Awareness
   - Manage WORKFORCE Activities
3. Identify and mitigate vulnerabilities
   - Identify and Respond to Threats
   - Reduce Cybersecurity Vulnerabilities

*capability maturity model for energy systems.

SOURCE: Assante, M. J., Tobey, D. H., Conway, T. J., Leo, R., Januszewki, J., & Perman, K. (2013). *Developing secure power systems professional competence: Alignment and gaps in workforce development programs* (Technical Report No. 2013-SGC-02). Idaho Falls, ID: National Board of Information Security Examiners.

Intrusion Analyst

CERTIFICATION INDICATORS

1. Analyze security incidents
   - Attack Techniques – Discovery (CEH)
   - Incident Handling (CISM)
   - Network Security
   - Networking
   - Risk & Program Management - Business Cont. & Recovery
   - Risk & Program Management - Compliance
   - Risk & Program Management - Governance
   - Security Analysis
   - Security Design
2. Develop and manage personnel
   - Risk & Program Management - Compliance

SOURCE: Assante, M. J., Tobey, D. H., Conway, T. J., Leo, R., Januszewki, J., & Perman, K. (2013). *Developing secure power systems professional competence: Alignment and gaps in workforce development programs* (Technical Report No. 2013-SGC-02). Idaho Falls, ID: National Board of Information Security Examiners.

Intrusion Analyst

EDUCATION COURSES

1. Analyze security incidents
   - Cyber asset vulnerabilities, access, and attack vector identification
     - Advanced SCADA Security Red/Blue Team
   - Incident response
     - Advanced SCADA Security Red/Blue Team

2. Develop and manage personnel
   - Introduction to control systems
   - Course 1450: Advanced SCADA Training (Level II)

3. Identify and mitigate vulnerabilities
   - Architectural security and strategies
   - Control system network security

SOURCE: Assante, M. J., Tobey, D. H., Conway, T. J., Leo, R., Januszewki, J., & Perman, K. (2013). *Developing secure power systems professional competence: Alignment and gaps in workforce development programs* (Technical Report No. 2013-SGC-02). Idaho Falls, ID: National Board of Information Security Examiners.

Intrusion Analyst

2. Develop and manage personnel

Met X	Responsibility	Met X	Task
	Ensure adequate and representative environments exists to train staff and evaluate threats and vulnerabilities and mitigations		Develop a threat analysis testing environment and sandbox where TTPs can be analyzed and considered
			Establish a test lab where tools can be practiced and learned.
	Ensure all security operations staff and stakeholders maintains an understanding of applicable vulnerabilities and threats		Communicate new threats or newly discovered vulnerabilities to the entire security operations staff
			Conduct security drills that incorporate the latest threats and vulnerabilities in the scenarios
			Develop threat awareness content that can be included in security awareness and outreach efforts
			Identify training opportunities that teach methodologies associated with current attack tools such as CEH training and select personnel involved in incident response to take such training.
			Monitor industry groups and forums so that you are able to hear the latest on security vulnerabilities related to smart

Competition Design

Certification » **CEH - Certified Ethical Hacker** ***(EC-Council)***

- NCL Lab » **Abusing SYSTEMS**
  - Denial of Service
  - Website Defacement
- NCL Lab » **Breaking WEP and WPA Encryption**
  - Cracking and Examining Wi-Fi Protected Access (WPA) Traffic
  - Cracking and Examining Wired Equivalent (WEP) Privacy Traffic
  - Examining Plain text Wireless Traffic
  - Wireless Commands and Tools

Certification » **Security+ - CompTIA Security+** ***(CompTIA)***

- NCL Lab » **Access Controls**
  - Configuring Auditing for Object Access
  - Configuring ICMP on the Firewall
  - Viewing The Security Log to Determine Security Incidents
- NCL Lab » **Analyze and Differentiate Types of Application Attacks**
  - Attacking a REmote System Utilizing Armitage
  - Introduction to Metasploit, a Framework for Exploitation
  - Post Exploitation of the Remote System
  - Scanning the Network for Vunerable Systems

Competition Design

Task Type » **Distracting**

Task » **Assign a technical POC for vulnerability remediation and assistance|9624**

- Incident Response Procedures

Task » **Develop appropriate mitigations after consulting with the vendor/integrators and internal system owners |9626**

- Discovering Security Threats and Vulnerabilities
- Incident Response Procedures
- Mitigation and Deterrent Techniques - Anti Forensic
- Mitigation and Deterrent Techniques - Password Cracking
- Secure Implementation of Wireless Networking

Task Type » **Esoteric**

Task » **Document all vulnerability information alerts or disclosures that apply to deployed technology and note the time and responsible party to develop the risk picture and initiate workflow|9623**

- Analyze and Differentiate Types of Application Attacks
- Analyze and Differentiate Types of Attacks Using Window Commands
- Analyze and Differentiate Types of Malware
- Authentication, Authorization and Access Control
- Configuring Backups
- Configuring the pfSense Firewall
- Discovering Security Threats and Vulnerabilities
- Incident Response Procedures

Competition Design

Task Type » **Fundamental**

Task » **Scan all impacted systems to ensure the patch or mitigations are present and the risk associated with the vulnerability has been reduced as expected |9628**

- Conducting Active and Passive Reconnaissance Against a Target
- Discovering Security Threats and Vulnerabilities
- Using Armitage to Attack the Network

Task Type » **Differentiating**

Task » **Decide the risk ratings of the vulnerability based on the technical information and how the technology is deployed/importance of the systems|9625**

- Discovering Security Threats and Vulnerabilities
- Incident Response Procedures

Task » **Implement vulnerability mitigations in accordance with the plan to include patches or additional security controls|9627**

- Analyze and Differentiate Types of Application Attacks
- Configuring the pfSense Firewall
- Discovering Security Threats and Vulnerabilities
- Incident Response Procedures
- Intrusion Detection
- Using Certificates to Encrypt Email