NICE Webinar: Witnessing an Evolution- The NICE Framework and its Role in Building a Better Cybersecurity Workforce

December 15, 2021
CALL FOR COMMENTS – due by January 31, 2022
• Proposed NICE Framework Data Update Process
• Refactored NICE Framework Ability Statements
• NICE Framework Competencies, NISTIR 8355 (Second Draft)

NEW RESOURCE
• NICE Framework in machine-readable JSON Format
The NICE Framework: Evolution and Growth
Karen Wetzel, Manager of the NICE Framework
NICE Framework Evolution: A Quick Recap

2017
NIST 800-181: A National Framework
What started as an effort to align the federal cyber workforce is intentionally expanded as a national framework.

2020
NIST 800-181: First Revision
Name changed in recognition that cybersecurity is a concern across the workforce; other community-suggested adjustments streamline use and increase efficacy.

2021
NICE Framework Data Review
Focusing on reviewing the data to align with the 2020 revision, addressing gaps, and developing process to ensure responsiveness and community input.

2022
Continued Growth
- Competencies list
- Task review and alignment
- Machine-readable
- Update process
- Accessible platform
2020 Revision

• Stakeholder community feedback gathered since 2017 and during 2019 comment period
• National Framework: Government, Private Industry, and Academia
• Most significant changes:
  – Deprecation of Specialty Areas
  – Deprecation of Ability Statements
  – Addition of Competencies
NICE Framework Attributes

**Agility**
Keep pace with a constantly evolving ecosystem.

**Interoperability**
Exchange workforce information using a common language and framework model.

**Modularity**
Communicate about other enterprise risks and workforces (e.g., privacy) within and across organizations and sectors.

**Flexibility**
Account for your organization’s unique operating context.
Evolution and Transformation
Data Review: Ability Statement Refactoring

• Mostly skills, a handful of knowledge and task statements, e.g.:
  – A0016: Ability to facilitate small group discussions.
  – *Becomes*: Skill in facilitating small group discussions.

• Addressing redundancies and duplicates, e.g.:
  – A0010: Ability to analyze malware.
  – S0131 Skill in analyzing malware.

• Alignment with [TKS Authoring Guide](#), e.g.,
  – A0061: Ability to design architectures and frameworks.
  – Skill: Skill in designing architectures
  – Skill: Skill in designing frameworks

---

- 178 Ability Statements...
- 42 Knowledge Statements
- 93 Skill Statements
- 6 Task Statements

[TKS Authoring Guide General Principles]
- Flexible
- Consistent
- Clear
- Affirmative
- Discrete
Data Review: Skill Statements Review

TKS Authoring Guide alignment:

• **Consistent phrasing, e.g.,**
  – Skill in performing sensitivity analysis
  – Skill in performing fusion analysis
    (vs. the original “Skill in fusion analysis”)

• **Observable actions, e.g.,**
  – Skill in recognizing relevance of information.
    • vs.
  – Skill in encrypting network communications.

• **Include only one skill, e.g.,**
  – Skill in identifying and extracting data of forensic interest in diverse media
    • becomes
  – Skill in identifying forensic data in diverse media
    and Skill in extracting forensic data in diverse media.

Also addresses:

– **Redundancies or duplicates:**
  – Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.
  – Skill in applying various analytical methods, tools, and techniques

– **Verbs, e.g., using, utilizing, use** (“Skill in using PKI” becomes “Skill in implementing PKI”)

**Skill:** The capacity to perform an observable action.

**Skill Statements**

• Begin with “Skill in” followed by a verb
• Represent observable actions
• Include only one skill in a single statement
Data Review: Knowledge Statements

• Limited to a single concept
  – Possible exceptions to the rule (e.g., “Knowledge of performance tuning tools and techniques.”)

• Removal of parentheticals
  – Will introduce usage guidance field
  – Ex: Knowledge of key concepts in security management. (e.g., Release Management, Patch Management)
Data Review: Competencies & Update Process

• NICE Framework Competencies NISTIR: Second Draft
  – Clearer definition
  – More clarity on Competencies vs. Work Roles
  – More application information

• NICE Framework Data Review and Update Process
  – Aim to implement in 2022
  – Provides insight into the proposed process
  – Answers questions
NICE Framework: Ongoing Improvements

• **Content Review & Updates**
  – December 2021:
    • Ability statement refactoring
    • Knowledge & Skill statements
    • NICE Framework Competencies (2nd draft)
  – 2022:
    • Task statements
    • Competencies List

• **Machine-readable format**
  – December 2021: JSON & Schema

• **2022: Web access, tools, resources**
  – Framework in Focus
  – Success Stories
  – Guides
  – Filling gaps (OT, Cybersecurity Awareness, etc.)

• **NICE Framework Update Process**
  – December 2021: Overview release
  – 2022 Launch
NICE Framework: Ongoing Improvements

- Content Review & Updates
  - December 2021:
    - Ability statement refactoring
    - Knowledge & Skill statements
    - NICE Framework Competencies (2nd draft)
  - 2022:
    - Task statements
    - Competencies List

- NICE Framework Update Process
  - December 2021: Overview release
  - 2022 Launch

Strategic Plan: Expand Use of the NICE Framework
- Document and disseminate uses
- Align with other frameworks and publications
- Establish regular review and update process
- Explore tool development
- Highlight areas that could be performed by automated techniques
- Expand international outreach

NICE Framework Update Process

- December 2021: Overview release
- 2022 Launch
For More Information

nist.gov/nice/framework

nist.gov/nice/community

NICEFramework@nist.gov

@NISTcyber

Karen Wetzel
Manager, NICE Framework
karen.wetzel@nist.gov
Q & A
Witnessing an Evolution - The NICE Framework and its Role in Building a Better Cybersecurity Workforce at Nova Southeastern University

Yair Levy, Ph.D.
Nova Southeastern University
College of Computing and Engineering
Professor of IS and Cybersecurity
Director of Center for Information Protection, Education, and Research (CIPhER) - https://InfoSec.nova.edu/

Proud NSA National Center of Academic Excellence (NCAE) in Cybersecurity - Cyber Defense (CD) since 2005!
Nova Southeastern University (NSU) - Florida
Nova Southeastern University (NSU) - Florida
Nova Southeastern University (NSU) - Florida

• NSU’s College of Computing and Engineering (https://computing.nova.edu/) is recognized as a national leader in Computer Science, Information Technology, and Cybersecurity Education.
  • BS in Computer Science – ABET Accredited
  • BS in Information Technology
  • BS minors in Cybersecurity or Data Analytics
  • MS in Cybersecurity Management – NSA NCAE-C Designated Program
  • MS in IA & Cybersecurity – NSA NCAE-C Designated Program
  • MS in Computer Science
  • MS programs in Information Technology, Data Analytics, Tech Leadership, and Information Systems
  • Ph.D. in Cybersecurity Management, Computer Science, and Information Systems
Nova Southeastern University (NSU) - Florida

• NSU was among the first in the State of Florida to be designated as a CAE in March 2005 and received CAE re-designation in 2009, 2014, and 2021 (https://infosec.nova.edu/)

• Cybersecurity Programs:
  • *Ph.D. in Cybersecurity Management*
  • *MS in Information Assurance and Cybersecurity* (30cr)
    • Focus on “Network Security Engineering”
      ‣ NICE WF Cat: Protect and Defend
  • *MS in Cybersecurity Management* (30cr)
    • Focus on “Security Policy Development and Compliance”
      ‣ NICE WF Cat: Oversee and Govern
Program(s) of Study (PoS) Validation Requirements

b. NICE Framework crosswalk alignment

The applicant will state the cybersecurity PoS crosswalk alignment with the NICE Framework (a.k.a. NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf). See categories on Table 1, p. 11 of NIST.SP.800.181: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and/or Investigate (IN).

Requirement:

- Identify the NICE Cybersecurity Workforce Framework category(ies) that the PoS is best aligned to (May check more than one).
Nova Southeastern University (NSU)

• Faculty and staff of College of Computing and Engineering (CCE) at NSU and NSU Career Development Office (CDO) staff (https://www.nova.edu/career/) collaboration
• Integration of the NCWF into the student advising process
  • Relevant job roles for the NSA NCAE-C designated programs
  • Identifying and listing NCWF Job Roles for each program
  • Exposure of the framework to the career advisors
  • Creation of a focused Career Development Newsletter
  • Development of sample student resumes
    • Entry level, five, and 10 Years of Experience resume samples
Nova Southeastern University (NSU)

CYBERSECURITY MANAGEMENT
MASTER OF SCIENCE (M.S.)

Future Opportunities
Under the category of Oversee and Govern, within the National Institute of Standards and Technology, explore careers, such as
- chief information security officer (CISO)
- information systems security manager (ISSO)
- cybersecurity program manager (OPM#801)
- information systems security manager (OPM#722)
- IT program manager (OPM#802)
- cyber policy and strategy planner (OPM#752)

Integrating the NICE Framework to academic degree ‘Program Sheet’

Source: https://computing.nova.edu/masters/documents/ms-cybersec-mgmt.pdf
Nova Southeastern University (NSU)

INFORMATION ASSURANCE AND CYBERSECURITY
MASTER OF SCIENCE (M.S.)

**Future Opportunities**
Under the category of Protect and Defend, within the National Institute of Standards and Technology, explore careers such as:
- chief information security officer (CISO)
- information systems security officer (ISSO)
- cyber defense analyst (OPM#511)
- cyber defense infrastructure support specialist (OPM#521)
- cyber defense incident responder (OPM#531)
- vulnerability assessment analyst (OPM#541)

Source: [https://computing.nova.edu/computing/documents/ms-info_assurance_cybersecurity.pdf](https://computing.nova.edu/computing/documents/ms-info_assurance_cybersecurity.pdf)

Integrating the **NICE Framework** to academic degree ‘Program Sheet’
Nova Southeastern University (NSU)

Center for Academic & Professional Success Newsletter

Computing & Engineering Edition

Visit Handshake

The Center for Academic and Professional Success (CAPS) is here to support our sharks by providing virtual advising appointments and communicating weekly updates on job and internship opportunities.

The below newsletter highlights industry specific opportunities, upcoming events, steps to schedule a virtual advising appointment, and information regarding our industry resume books, along with featured events hosted by the College of Computing & Engineering.

NSU College of Computing & Engineering Hosted Events
Nova Southeastern University (NSU)

Hank Pym
3301 College Avenue, Davie, FL, 33314
(954) 262-7201, Hank@nova.edu

EDUCATION
Master of Science in Cybersecurity Management (NSA/DHS designated program for Information Security Policy Development and Compliance, NSU’s Center of Academic Excellence (CAE) in Cyber Defense Education) May 2020
Nova Southeastern University (NSU)
Davie, FL

Bachelor of Science in Computer Science May 2014
Nova Southeastern University (NSU)
Davie, FL

CERTIFICATIONS
• CompTIA Security+ SY0-501 May 2017
• Offensive Security Certified Professional: Offensive Security August 2018
• Certified in essential elements of computer and network security: Access Control and Identity management, Policies, Procedures, and Awareness, Physical Security, Perimeter Defenses, Network Defenses, Host defenses, Application Defenses, Data Defenses, Audits and Assessments

PROFESSIONAL EXPERIENCE
Cybersecurity Analyst January 2020-Present
Company X Fort Lauderdale, FL

• Provide support to the security of company networks.
• Perform studies on customer data sets and infrastructure; document findings in reports, presentations, and technical exchanges.
• Provide forensic analysis of network packet captures, DNS, proxy, Netflow, malware, host-based security and application logs, as well as logs from various types of security sensors.
• Identify gaps in IT infrastructure by mimicking an attacker’s behaviors and responses.
• Compile detailed investigation and analysis reports for internal SOC consumption and delivery to management.
• Develop advanced queries and alerts to detect adversary actions.
• Develop tools to automate security related procedures.
• Scan networks and analyze reports for vulnerabilities, advise on patching and mitigation actions.
• Provides detection, identification, and reporting of possible cyber attacks/intrusions, anomalous activities, and misuse
NICE Framework – Core

Figure 1 - NICE Framework Approach

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1-draft.pdf
Skill Development and Competencies

Figure 1. The Stages of Skill Development and Competency Attainment


Skill Development and Competencies

TestOut – LabSim SecurityPro
Skill Development and Competencies

Intro to Malware – Static Analysis

Overview
A look at what you will be doing in this lab

Learning outcomes
- Demonstrate understanding of basic malware concepts

Awards
Your rivals who are leading the way
Skill Development and Competencies

https://nice-challenge.com/
Witnessing an Evolution - The NICE Framework and its Role in Building a Better Cybersecurity Workforce at Nova Southeastern University (NSU)

The future?
# Future in Skills and Competency Assessments

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Awareness</th>
<th>Training</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Seeks to make users aware of what security is and what to do in some situations</td>
<td>Seeks to train users how they should react and respond when threats are encountered</td>
<td>Seeks to educate users as to why the reactions are needed and what preparations should be in place</td>
</tr>
<tr>
<td>Level</td>
<td>Offers basic information about threats and responses</td>
<td>Offers more detailed knowledge about detecting threats and teaches skills needed for effective reaction</td>
<td>Offers the background and depth of knowledge to gain insight into how processes are developed and enables ongoing improvements</td>
</tr>
<tr>
<td>Objective</td>
<td>Can recognize threats and formulate simple responses</td>
<td>Can respond effectively using learned skills</td>
<td>Can engage in active defense and use understanding of the objectives to make continuous improvements</td>
</tr>
<tr>
<td>Teaching Method</td>
<td>Media videos, Newsletters, Posters, Informal training</td>
<td>Formal training, Workshops, Hands-on practices</td>
<td>Theoretical instructions, Discussions/seminars, Background reading</td>
</tr>
<tr>
<td>Assessment</td>
<td>True/False or multiple-choice questions, (identify learning)</td>
<td>Problem solving (apply learning)</td>
<td>Essay/research paper/presentations (interpret learning)</td>
</tr>
<tr>
<td>Impact timeframe</td>
<td>Short-term</td>
<td>Intermediate</td>
<td>Long-term</td>
</tr>
</tbody>
</table>

Powering the Innovation Ecosystem

The Alan B. Levan | NSU Broward Center of Innovation is a public-private partnership between Nova Southeastern University and Broward County acting as an economic and education development engine linking the South Florida innovation ecosystem.

The Levan Center supports the Founder’s Journey from birth of an idea through successful exit or global expansion providing programs, events, and wraparound services to entrepreneurs and early-stage startups for the buildout and scaleup of their business.

https://www.nova.edu/innovation/
Future in Skills and Competency Assessments
Thank you!

Contact:
levyy@nova.edu

https://www.caecommunity.org/community-of-practice/cyber-defense
Q & A
BUILDING AND MEASURING CYBERSECURITY SKILLS

CyberQ

Mapping Cyber Range activities to the NICE Framework

Steve Graham – Sr. Vice President
EC-Council was founded in 2001. In 2003, the Certified Ethical Hacker (CEH) course and certification were launched. EC-Council became the first federal customer of the Federal Bureau of Investigation (FBI) in 2005. In 2010, EC-Council achieved its first U.S. Department of Defense (DoD) Accreditation for the CEH. From 2004 to 2021, EC-Council developed over 20 hands-on, tactical Cybersecurity certification courses along with several leading cybersecurity education brands. 4 Courses accredited by the U.S. Department of Defense (DoD).

EC-Council Global Brands
Our Programs
How Do We Do It?

THE EC-COUNCIL CONTINUOUS SKILL DEVELOPMENT CAPABILITY
### NCWF JOB ROLE

**Cyber Defense Analyst**

**Job Role Description:** A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

**Maps To:** Certified Ethical Hacker (CEH)

**Mapping Summary:** Performance-based learning and evaluation in CEH imparts specific KSA's that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

<table>
<thead>
<tr>
<th>TASK</th>
<th>ID</th>
<th>Statement</th>
<th>Bloom's Action Verbs</th>
<th>CEH Exam Objectives</th>
<th>NICE Proficiency</th>
<th>Relational Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0020</td>
<td>Develop content for cyber defense tools.</td>
<td>Develop, Synthesize</td>
<td>6.7, 7.9, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.7, 16.2, 17.5, 18.8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0023</td>
<td>Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.</td>
<td>Analyze</td>
<td>2.7, 3.7, 7.7, 14.4</td>
<td>4</td>
<td>90% or .9</td>
<td></td>
</tr>
<tr>
<td>T0043</td>
<td>Coordinate with enterprise-wide cyber defense staff to validate network alerts.</td>
<td>Validate</td>
<td>16.1, 16.2</td>
<td>3</td>
<td>70% or .7</td>
<td></td>
</tr>
<tr>
<td>T0088</td>
<td>Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.</td>
<td>Test, Evaluate</td>
<td>1.6, 1.7, 1.8, 1.11, 6.7, 15.6, 16.1, 16.2, 17.3</td>
<td>4</td>
<td>100% or .1</td>
<td></td>
</tr>
<tr>
<td>T0155</td>
<td>Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.</td>
<td>Generate, Apply, Analyze</td>
<td>1.9</td>
<td>2</td>
<td>50% or .5</td>
<td></td>
</tr>
<tr>
<td>T0164</td>
<td>Perform cyber defense trend analysis and reporting.</td>
<td>Perform</td>
<td>1.1</td>
<td>4</td>
<td>100% or 1</td>
<td></td>
</tr>
<tr>
<td>T0166</td>
<td>Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.</td>
<td>Perform</td>
<td>2, 2, 3, 4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11</td>
<td>4</td>
<td>100% or 1</td>
<td></td>
</tr>
<tr>
<td>T0178</td>
<td>Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.</td>
<td>Perform</td>
<td>1.6</td>
<td>2</td>
<td>70% or .7</td>
<td></td>
</tr>
<tr>
<td>T0187</td>
<td>Plan and recommend modifications or adjustments based on exercise results or system environment.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0198</td>
<td>Provide daily summary reports of network events and activity relevant to cyber defense practices.</td>
<td>Provide</td>
<td>7.1</td>
<td>2</td>
<td>50% or .5</td>
<td></td>
</tr>
<tr>
<td>T0214</td>
<td>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.</td>
<td>Analyze</td>
<td>16.2</td>
<td>3</td>
<td>90% or .9</td>
<td></td>
</tr>
</tbody>
</table>

---

**Program Level NICE Framework Mapping**
Knowledge gained from real-world experience that updates the process over time.
Experiences with target ranges, flags, and guides are presented as simple thumbnails.
Flags presented to students with simple Q&A Format (all complexities and data mapping is done by the platform)
Skills Report maps directly to NICE Framework KSAT’s and showed measured results of performance-based activity at the individual KSAT Level.
Task Mastery Report maps directly customizable Course/Module/Task showing learning objective coverage and completion.

<table>
<thead>
<tr>
<th>Course</th>
<th>Module/Task</th>
<th>Time</th>
<th>Attempts</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEHv11</td>
<td>Module 02: Footprinting and Reconnaissance</td>
<td>0:00:35</td>
<td>1</td>
<td>Completed</td>
</tr>
<tr>
<td>CEHv11</td>
<td>Module 03: Scanning Networks</td>
<td>0:08:47</td>
<td>1</td>
<td>Completed</td>
</tr>
<tr>
<td>CEHv11</td>
<td>Module 14: Hacking Web Applications</td>
<td>0:02:23</td>
<td>3</td>
<td>Completed</td>
</tr>
<tr>
<td>CEHv11</td>
<td>Module 03: Scanning Networks</td>
<td>0:01:10</td>
<td>3</td>
<td>Completed</td>
</tr>
<tr>
<td>CEHv11</td>
<td>Module 15: SQL Injection</td>
<td>0:06:46</td>
<td>6</td>
<td>Completed</td>
</tr>
<tr>
<td>CEHv11</td>
<td>Module 02: Footprinting and Reconnaissance</td>
<td>0:03:18</td>
<td>1</td>
<td>Completed</td>
</tr>
<tr>
<td>CEHv11</td>
<td>Module 14: Hacking Web Applications</td>
<td>0:00:27</td>
<td>1</td>
<td>Completed</td>
</tr>
</tbody>
</table>
Flag Reports provide information on the Flag Question, Answer provided, Time on Task, Attempts, Hints and overall score.
Building Custom Range Activities

Instantly launch any of hundreds of exercises

- Solve Puzzles
- Capture flags
- Conduct Forensic Investigations
- Hack Web Servers
- Root Machines
- Crack Passwords
- Investigate breaches
- And much, much more!
CyberQ SKILLS-FIRST Approach

Skill mapped targets and flags are the building blocks of CyberQ – Not the Range

Target
- Anything that can be virtualized (Windows, Linux, iOS, Android, etc.)
- Software Packages
- Vulnerable apps, sites, configs
- Files (offline Targets)
- Re-usable across Experiences

Flag
- Mapped to Skills
- Mapped to NICE Job Roles
- Mapped to Courses

Experience
- Single Target
- Collection of Targets
- Attack Console (Kali, Parrot, Custom, OVPN)
- Cold Storage > Live deployment in minutes, on-demand

Train | Practice | Assess | Compete | Execute
One Platform | Many Solutions

- Single Target Experiences
- Multi Target Experiences
- Cyber Competitions
- Skill Based Flag Management
- Exercise Library
- Course & Exercise Management
- Marketplace for cyber exercises
- Full Cloud Orchestration
- Comprehensive Analytics

TRAIN | PRACTICE | ASSESS | COMPETE | EXECUTE
Target: Internal DoS Attack

Tags:
- denial of service
- insider threat
- log analysis
- network investigation

Public?:
- Yes
- No

Flag Type: PCap

Team:
- Red
- Blue

Flag Question:
What is the IP Address of the Attacker?

Answer: 10.0.0.8

Duration: 10

Course:
- CHIRID

Module:
- CHIRID Module 95 L

Task:
- Identifying and Investigating

Category: Investigate

Speciality Area: Digital Forensics

Work Role: Cyber Defense

Points:
- Skill in analyzing network data.
- Skill in identifying obfuscation techniques.
- Skill in interpreting results of debugger to ascertain tactics...
- Skill in analyzing malware.
- Skill in conducting bit-level analysis.
- Skill in processing digital evidence, to include protecting an...
- Skill in performing packet-level analysis.

Select Skill

Copyright © 2021 IC-Council (Patent Pending)
Official Digital Forensics Essentials v1 - CyberQ Labs

The Official Digital Forensics Essentials v1 - CyberQ Labs map directly to the content involved in EC-Council’s Digital Forensics Essentials (DFE) Program. Purchasing this job upgrade gives the student 6 months access to to the lab exercises that accompany the DFE certification program.

Digital Forensics Essentials (DFE) program covers the fundamental concepts of computer forensics. Equips students with the skills required to identify an attacker’s footprint and to properly gather the necessary evidence to prosecute in the court of law. This program gives a holistic overview of the key components of computer forensics. The course is designed for those interested in learning the various fundamentals of computer forensics and wishes to pursue a career in the computer forensics field.

You can play all the experiences for 180 Days.

<table>
<thead>
<tr>
<th>INDEX</th>
<th>LOGO</th>
<th>NAME</th>
<th>RATING</th>
<th>DIFFICULTY</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td>DFEv1 Module 01 Computer Forensics Investigation Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td>DFEv1 Module 02 Understanding Hard Drives and File Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td>DFEv1 Module 03 Data Acquisition and Duplication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td>DFEv1 Module 04 Defeating Anti-forensics Techniques</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td>DFEv1 Module 05 Windows Forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td>DFEv1 Module 06 Linux and Mac Forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td>DFEv1 Module 07 Network Forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td>DFEv1 Module 08 Investigating Web Attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thank you!
Q & A
Complete Survey

https://www.surveymonkey.com/r/decnicewebinar
Thank You for Joining Us!

**Upcoming Webinar:** Mentorship Models to Enhance Diversity and Increase Persistence in Cybersecurity Careers

**When:** January 19, 2022, at 2-3pm ET

**Register:** [https://nist-secure.webex.com/nist-secure/onstage/g.php?MTID=e5b026381618d86baa3431c0ca400ef0e](https://nist-secure.webex.com/nist-secure/onstage/g.php?MTID=e5b026381618d86baa3431c0ca400ef0e)

[nist.gov/nice/webinars](https://nist.gov/nice/webinars)