Hacktales

CYBERSECURITY FOUNDATION PROGRAM

Authors:
Chikodili Udeh & Jide Adebayo

Contents

Hacktales

01
Industry Overview

Objectives

Hacktales

01

At the end of this section, students will understand the different categories of organizations within the cybersecurity industry globally.

02

Students will review the roles and responsibilities of each category.

03

Students will be able to identify the opportunities that exist within each category.

Hacktales

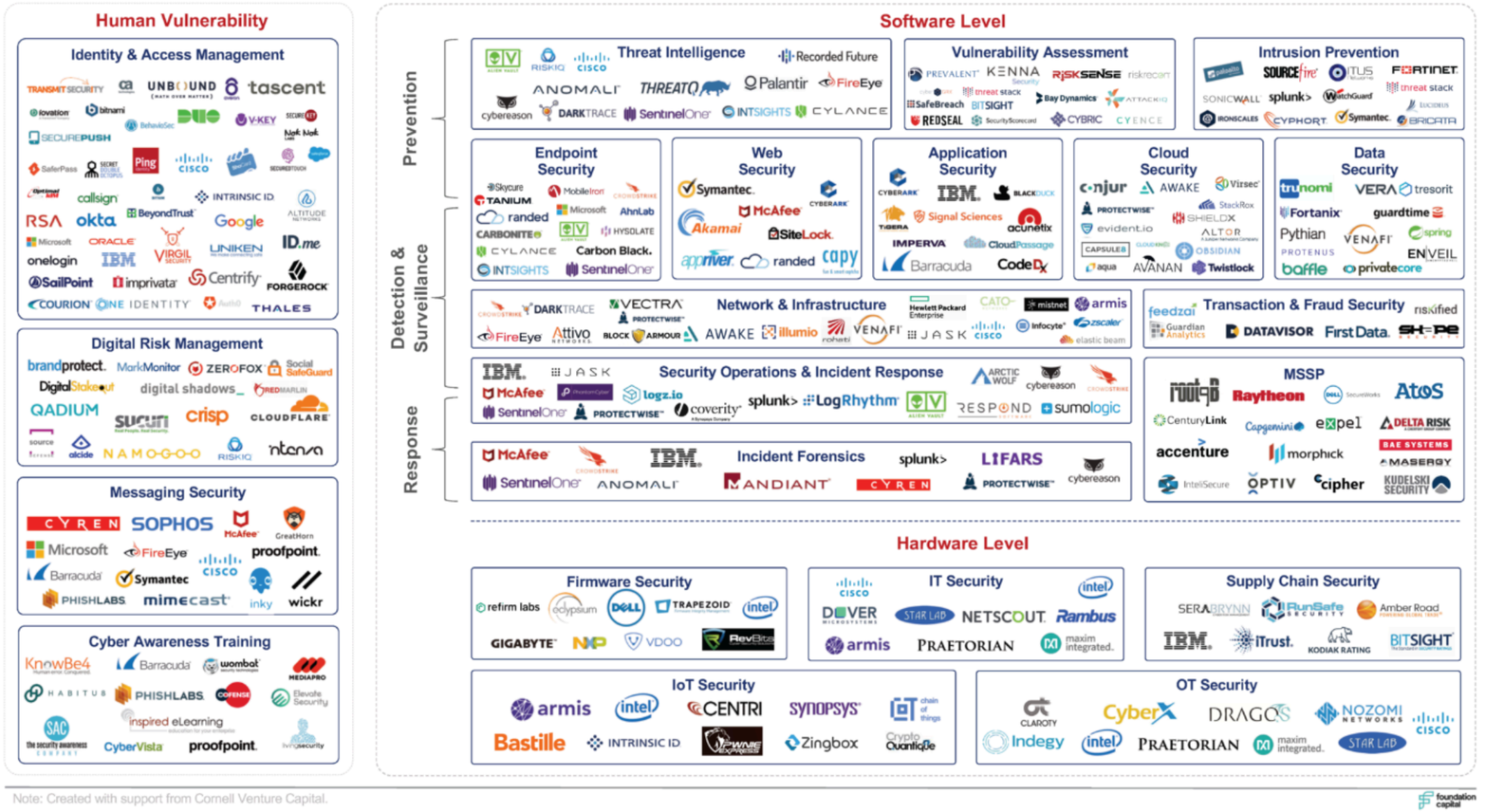
Industry Categories

Original Equipment Manufacturer (OEM)

Technology Partners

Asset Owner / End User

OEMs

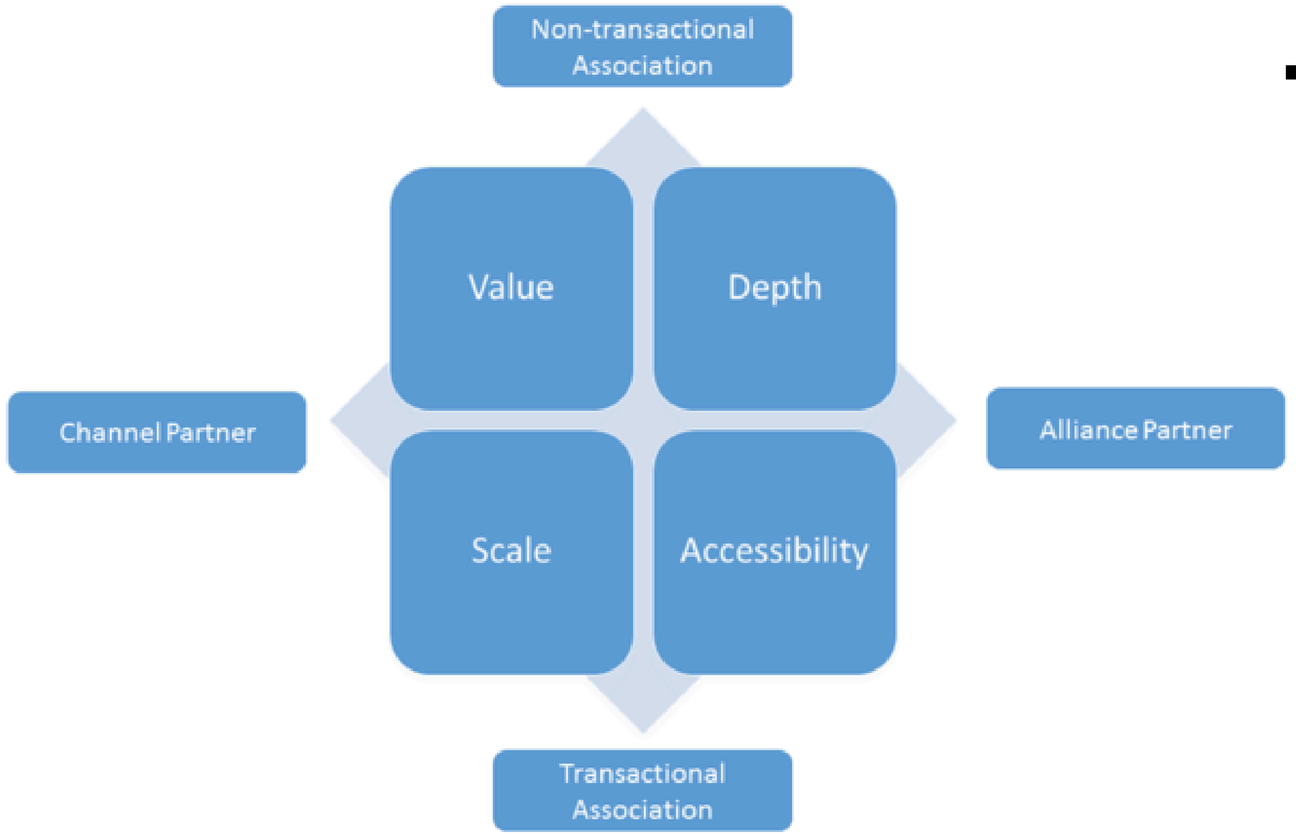


Note: Created with support from Cornell Venture Capital.

foundation capital

Module 6: Cybersecurity Workforce
Cybersecurity Foundation Program

Date:
May 31, 2025



Technology Partners

- Channel Partner - Distributors & Resellers (Alliance Partners)
- Resellers - Business Consultants (Advisory), System Integrators and Independent Software vendors (ISV).

Asset Owners

- Financial Services Industry
- Telecommunications
- Oil & Gas
- Manufacturing
- Energy & Utilities
- Government
- E-commerce
- Healthcare
- Education
- Retail

02
NICE Framework

Objectives

Hacktales

01

At the end of this section, students will understand how cybersecurity teams are built.

02

Students will learn about the different categories which all cybersecurity roles fall under.

03

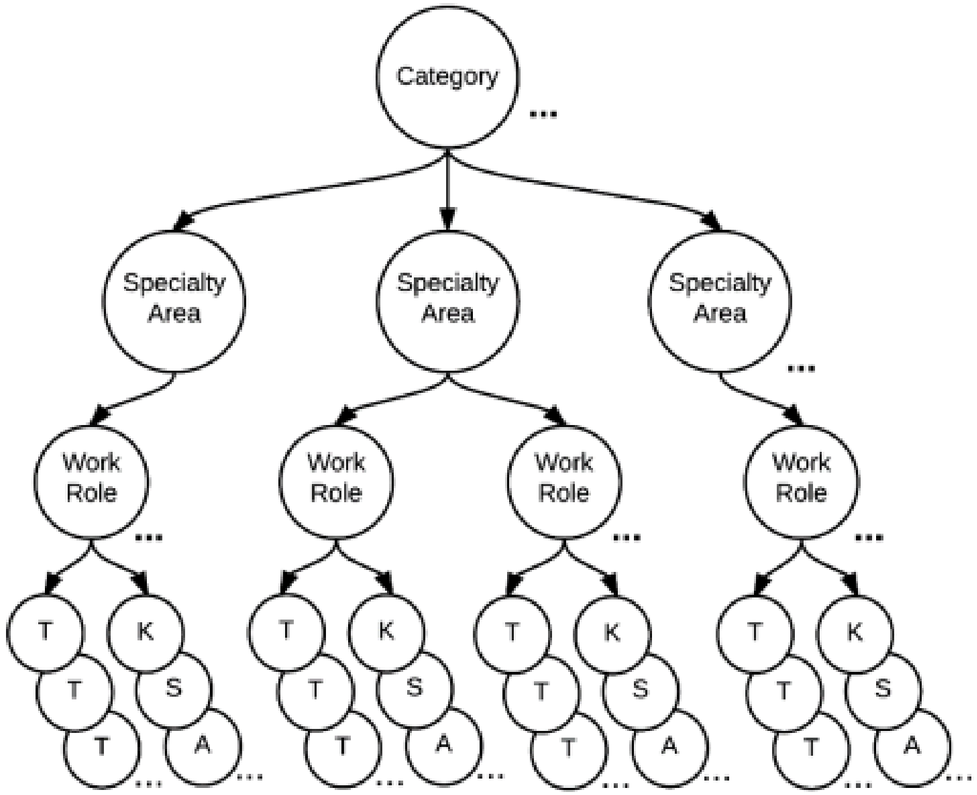
Students will review the tasks, knowledge and skills required for cybersecurity roles.

Workforce Building Blocks

Hacktales

Hacktales

NICE Framework Components



Module 6: Cybersecurity Workforce
Cybersecurity Foundation Program

Date:
May 31, 2025

Workforce Categories

Hacktales

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Hacktales

Work Roles

Work Role Name	**Cyber Defense Analyst**
Work Role ID	**PR-CDA-001**
Specialty Area	**Cyber Defense Analysis (CDA)**
Category	**Protect and Defend (PR)**
Work Role Description	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.
Tasks	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Abilities	A0010, A0015, A0066, A0123, A0128, A0159

Hacktales

NICE Framework Review

NIST.SP.800-181

Module 6: Cybersecurity Workforce
Cybersecurity Foundation Program

03
Internship Program

Objectives

Hacktales

01

At the end of this section, students will gain more insight on the goal of Hacktales Academy.

02

Students will learn about the different specialized roles within the academy.

03

Students will review the tasks, knowledge and skills required for each roles.

R&D Teams

CFP graduates are entitled to a **3-month internship** program.

During this time, you get to hone your hard and soft skills in one of the following teams:

- Purple Team
- Red Team
- Blue Team

Hacktales

Purple Team (GRC Analysts)

They are responsible for corporate-wide Information Security Governance, Risk, and Compliance (GRC) program.

Cybersecurity Analysts work closely with Information Technology, Enterprise Risk Management (ERM), Legal, Human Resources, Internal audit and control, and Procurement to ensure appropriate controls are in place to minimize risk and ensure compliance with Information Security Policy, Standards and Controls, NIST CSF, CIS, PCI-DSS, and data privacy regulations.

Job Description

1. **Perform Gap Assessments:** Examine how well organization meets the requirements of the most common security framework, ISO 27001. Identify where they fall short and what they need to do to meet these standards.
2. **Conduct Risk Assessment:** Evaluate the potential risks to an organization's information security. This involves looking at what could go wrong and how likely it is to happen, as well as the impact if it does.
3. **Develop Risk Register:** Create a list of all the risks identified, along with details about each one, such as how likely it is to occur and what the consequences would be if it did.
4. **Generate Reports:** Put together summaries of our findings from the gap assessments, risk assessments, and risk register. These reports help us understand where we stand in terms of security and what actions we need to take.
5. **Develop Compliance Policies & Train:** Create rules and guidelines that everyone in the organization needs to follow to make sure they meet security standards. These policies help ensure that everyone knows what they need to do to keep information safe.
6. **Participate in Security Meetings:** Take an active role in meetings where we discuss security plans and projects. Sometimes, you'll even lead these discussions, helping to shape the approach to security.

Hacktales

Red Team (Ethical Hackers)

In this role, Engineers assess the security systems within an organization. They conduct tests and purposefully attempt to exploit existing computer systems and software to detect and correct system weaknesses.

Penetration Testers use the test results to develop recommendations which are further used to build the strength of an organization’s information technology (IT) systems.

Job Description

Hacktales

1. **Conduct Penetration Tests**: Perform simulated cyber attacks on an organization's computer systems, networks, and applications to identify vulnerabilities and weaknesses.
2. **Evaluate Security Controls:** Assess the effectiveness of existing security measures by testing how well they withstand different types of attacks.
3. **Analyze Test Results:** Review the findings from penetration tests to understand where systems are vulnerable and how attackers might exploit these weaknesses.
4. **Recommend Security Improvements:** Suggest ways to strengthen defenses based on the results of penetration tests, such as applying patches, changing configurations, or implementing additional security controls.
5. **Document Test Procedures:** Create detailed reports documenting the methods used, vulnerabilities discovered, and recommendations for remediation.
6. **Stay Updated on Security Trends:** Keep abreast of the latest developments in cybersecurity threats and techniques to ensure penetration testing practices remain relevant and effective.

Blue Team (Security Engineers)

Hacktales

A Security Engineer helps in monitoring and analyzing the environment, identifying, and responding to security threats that put the company at risk.

They are responsible for monitoring and handling customers' information security requests, troubleshooting and solving security issues, automating support needs, developing support documentation and runbooks, developing and maintaining tools and infrastructure, and seeking out ways to continuously improve the security experience.

Job Description

Hacktales

1. **Implement Security Measures:** Install and configure security software to protect our systems and networks from cyber threats, such as malware, phishing attacks, and unauthorized access.
2. **Monitor Security Systems:** Keep an eye on our organization's security systems, such as firewalls, intrusion detection systems, and antivirus software, to detect and respond to potential threats.
3. **Investigate Security Incidents:** Investigate any suspicious activities or security breaches to determine the cause and extent of the incident, and take appropriate action to mitigate the damage.
4. **Respond to Security Alerts:** Monitor security alerts and notifications, and respond promptly to any incidents or breaches that are detected.
5. **Stay Updated on Security Trends:** Keep up-to-date on the latest cybersecurity threats, trends, and technologies to help anticipate and mitigate emerging risks.

Academy Roadmap

Hacktales

NEXT

PHASE 1	PHASE 2	PHASE 3
Foundation Program	Internship Program	Capstone Project
(2 months)	(3 months)	(1 month)

What's next?

Hacktales

- Review NICE Framework
- Fill out the Role Placement form
- Sign Internship letter