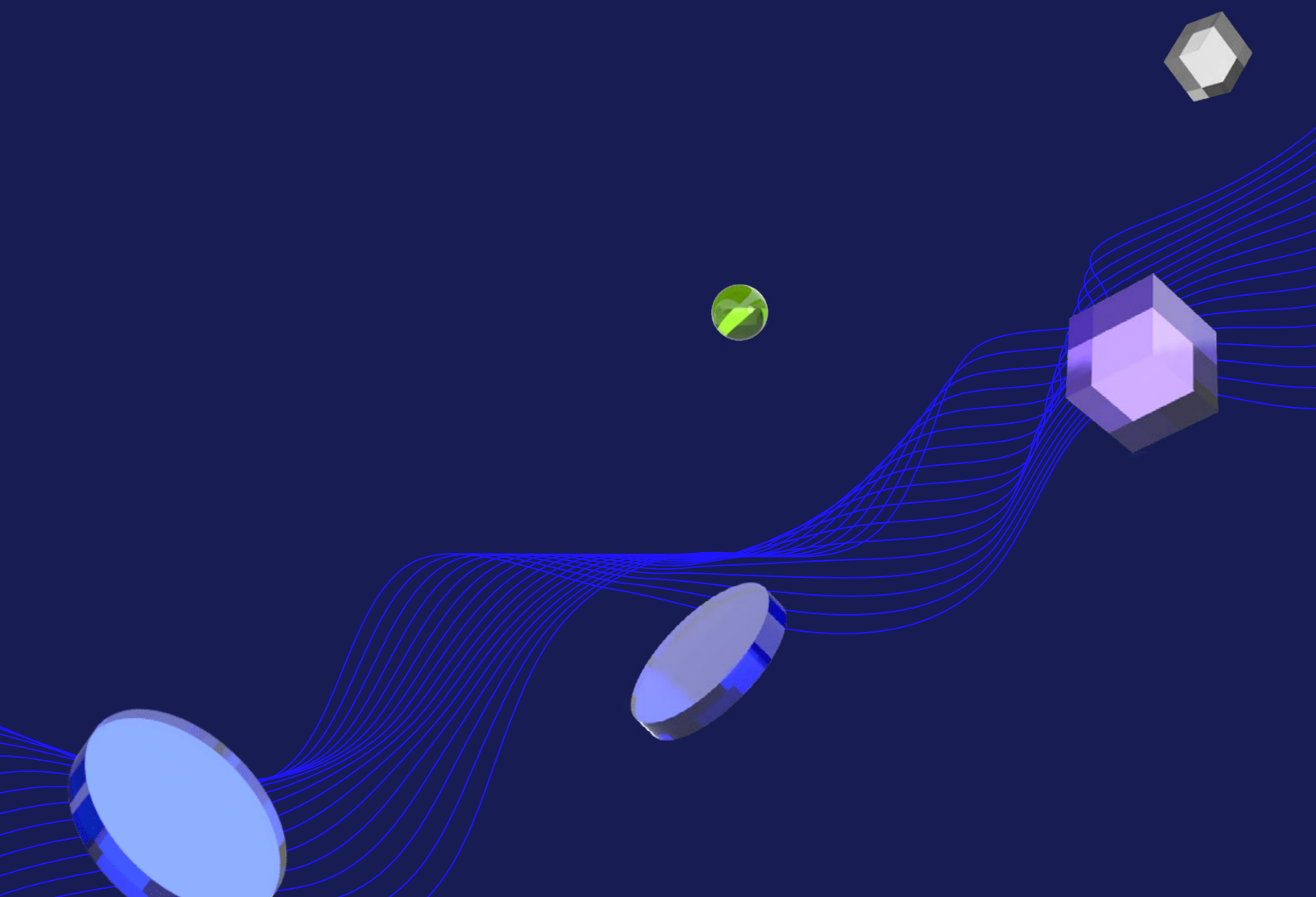
INDIVIDUAL LEARNERS

UDACITY

SCHOOL OF CYBERSECURITY

Introduction to Cybersecurity

Nanodegree Program Syllabus



Overview

Cybersecurity is a critically important field for businesses in every industry, especially given the proliferation of data breaches (more than 3.2 million records were compromised in the 10 biggest data breaches in the first half of 2020 alone). To reduce risk and improve security, businesses are rushing to hire for cybersecurity roles, yet there's projected to be 3.4 million unfilled cybersecurity jobs by 2022. The Introduction to Cybersecurity Nanodegree program will equip learners with the foundational skills to get started in this highly in-demand field.

Learning Objectives

A graduate of this program will be able to:

- Evaluate specific security techniques used to administer a system that meets industry standards and core controls.
- Explain methods for establishing and maintaining the security of a network, computing environment, and application.
- Apply control techniques to secure networks, operating systems, and applications.
- Conduct threat assessments and vulnerability scans to secure the assets of an organization.

Built in collaboration with:

Program information

Estimated Time

4 months at 10hrs/week*

Skill Level

Beginner

Prerequisites

A well-prepared learner should:

- Understand basic principles of network connectivity.
- Understand basic operating system fundamentals including Windows or Linux.

Required Hardware/Software

Learners will need a desktop or laptop computer running recent versions of Windows, Mac OS X, or Linux and an unmetered broadband internet connection.

*The length of this program is an estimation of total hours the average student may take to complete all required coursework, including lecture and project time. If you spend about 5-10 hours per week working through the program, you should finish within the time provided. Actual hours may vary.

Course 1

Cybersecurity Foundations

Security is embedded in all we do online and is a critical job skill and career field. This foundations course explains security fundamentals including core principles, critical security controls, and cybersecurity best practices. Students will also evaluate specific security techniques used to administer a system that meets industry standards and core controls, assess high-level risks, vulnerabilities, and attack vectors of a sample system, and explain ways to establish and maintain the security of different types of computer systems.

Course Project

Securing a Business Network

In this project, students will apply the skills they have acquired in the Cybersecurity Fundamentals course to conduct a hands-on security assessment based on a common business problem. Students will investigate and fix security issues on a Windows 10 client system as a way of demonstrating fundamental cybersecurity knowledge, skills, and abilities.

Lesson 1

Cybersecurity Fundamentals

- Understand the relevant role of cybersecurity and why it is important.
- Describe how business stakeholders play a role in cybersecurity.
- Become familiar with cybersecurity tools, environments, and dependencies.

Lesson 2

What is Cybersecurity

- Identify trends in cybersecurity events and protection techniques.
- Describe careers and skill qualifications of cybersecurity professionals.
- Explain security fundamentals including core security principles, critical security controls, and best practices.

Lesson 3

Maintain Secure Infrastructure

- Apply methods to enforce cybersecurity governance.
- Identify common security regulations and frameworks.
- Explain how current security laws, regulations, and standards applied to cybersecurity and data privacy.
- Recognize components of the NIST Cybersecurity Framework (CSF).
- Recognize components of the Center for Internet Security Critical Security Controls (CSC).

Lesson 4

Think Like a Hacker

- Categorize assets, risks, threats, vulnerabilities, and exploits.
- Identify different types of vulnerabilities in a system.
- Identify the categories of a cyber threat.
- Determine the phase of a cyber attack.
- Recognize common exploits.

Lesson 5

Security Defenses

- Explain how security defenses are layered throughout different system architectures.
- Explain components of identity and access control.
- Identify common identity and access control protection techniques.
- Determine patch levels for common systems/applications.
- Describe the process and technique for applying patches and updates on computing devices.
- Understand protection for email and other communication methods.

Lesson 6

Applying Cybersecurity

- Identify organizational asset(s).
- Analyze vulnerabilities and risks to those organizational assets.
- Recommend and apply basic security controls.

Course 2

Defending and Securing Systems

In this course, students will be exposed to a diverse group of technologies that will provide or enhance the skills needed to enter the cybersecurity field. Students will apply best practices of Defense in Depth to secure computer systems, use outputs from security incidents to analyze and improve future network security, and search internal systems to determine network vulnerabilities. Students will also learn how to recommend mitigations to address common application vulnerabilities and ensure fundamental encryption techniques for securing data at rest and in transit.

Course Project

Monitoring and Securing Douglas Financials Inc.

Douglas Financials Inc. (DFI) has experienced successful growth and as a result is ready to add a security analyst position. Acting as that new analyst, students will analyze Windows and Linux servers and report recommendations on OS hardening, compliance issues, encryption, and network security. Students will also create firewall rules, analyze threat intelligence, and encrypt files and folders for transport to a client.

Lesson 1

Defending Computer Systems & Security Principles

- Explain the Defense in Depth approach to a layered security strategy.
- Explain the NIST 800 framework for defending computer systems.
- Determine if a system has implemented least privileged properly.
- Suggest approaches to correct systems that have inappropriately implemented least privileged principles.

Lesson 2

System Security: Securing Networks

- Differentiate between different types of firewalls.
- Analyze the effectiveness of firewall rules and craft a basic rule.
- Evaluate best practices for securing wireless networks.
- Explain different types of IDS/IPS and craft a basic IDS signature.
- Evaluate documentation to determine proper security settings in Windows.
- Identify the impact of services, permissions, and updates on Windows Security.
- Identify the impact of daemons, permissions, and patches on Linux Security.

Lesson 3

Monitoring & Logging for Detection of Malicious Activity

- Interpret between different types of logs.
- Define the basic parts of network traffic.
- Interpret the output of a firewall and IDS report.
- Explain the importance of a SIEM.
- Explain the pros and cons of open source vs. commercial SIEM.

Lesson 4

Cryptography Basics (Applied Cryptography)

- Define encryption.
- Differentiate different types of encryption techniques.
- Determine the appropriate encryption type for a given scenario.
- Differentiate between data at rest and data in transit.
- Differentiate different types of encryption techniques for data in transit.
- Define and analyze file hashes.

Course 3

Threats, Vulnerabilities & Incident Response

Cybersecurity breaches happen when a threat is able to successfully exploit a vulnerability within a business. To avoid these attacks, security professionals must understand threats the company is facing, including the various threat actors and their motivations. Security professionals must also be able to find vulnerabilities that can enable threats to attack through common practices such as vulnerability scanning and penetration testing. Finally, security professionals should be able to activate and follow incident response procedures to address cybersecurity incidents and breaches. Ultimately, during this course, students will learn how to identify security threats and gaps, fix issues, and respond to inevitable attacks.

Course Project

Navigating a Cybersecurity Incident

Hospital X has seen its worst nightmare become a reality. After several hospitals in its partner network got hacked, the medical establishment has realized that it's likely they are next on the attack hit list. In situations like this, it's important for the cybersecurity team to understand the threats at hand, whether the company is vulnerable, how to close the gaps, and ultimately, how to respond if there is indeed a security incident. In this project, students will apply the skills they have acquired in this security course to navigate a potential cyber incident.

Students will work to identify the type of threat actor involved and potential motivation behind the attack. Based on clues provided throughout the scenario, students will conduct scans to discover and test vulnerabilities that could lead to a successful attack. Students will then assess risk levels associated with the findings and propose a remediation plan. They will also leverage a provided incident response plan to navigate the potential breach and make recommendations for improvements to the plan.

The final implementation of the project will showcase students' vulnerability management and incident response skills, including their ability to prioritize threats and make recommendations to key stakeholders.

Lesson 1

Assessing Threats

- Explain the relationship between threats, threat actors, vulnerabilities, and exploits.
- Utilize event context to identify potential threat actor motivations.
- Identify security threats applicable to important organizational assets.
- Use standard frameworks to assess threats, identify risks, and prioritize.

Lesson 2

Finding Security Vulnerabilities

- Leverage the MITRE ATT&CK framework to understand attack methods.
- Configure and launch scans to find vulnerabilities.
- Explain the steps required to conduct a penetration test.

Lesson 3

Fixing Security Vulnerabilities

- Conduct vulnerability research using industry resources like MITRE CVE framework.
- Validate scan results through manual testing and application of business context.
- Prioritize security gaps and recommend remediation strategies.

Lesson 4

Preparing for Inevitable Attacks

- Explain the relationship between incident response, disaster recovery, and business continuity.
- Distinguish events from incidents and recognize indicators of compromise.
- Explain the incident response lifecycle.
- Recognize the key incident response team roles and core components of an incident response plan.

Course 4

Governance, Risk & Compliance

Cybersecurity governance, risk, and compliance (GRC) has rapidly become a critical part of an effective cybersecurity strategy. While it's important to understand why, how, and where to apply cybersecurity controls, GRC connects cybersecurity controls to business objectives and serves as a safety net to ensure controls are applied efficiently and effectively. In this course, students will learn about the functions of governance, risk, and compliance and how each function operates alongside operational controls to strengthen an organization's security. Students will also learn how to assess control effectiveness, measure security risk, and ensure that organizations are meeting security compliance objectives.

Course Project

Create the SwiftTech GRC Program

SwiftTech is a company in transition—they are accelerating product development while trying to maintain a high standard for flexibility and responsiveness with customers, and doing all this while migrating their infrastructure to the cloud. This fast-paced environment creates challenges for the organization's cybersecurity GRC practice. As a brand new GRC analyst for SwiftTech, you'll need to understand the business quickly and improve their documentation to help support the organization's goals.

Lesson 1

Introduction to Governance, Risk & Compliance

- Understand the historical underpinnings of cybersecurity GRC.
- Explain the key functions of each of the Governance, Risk, and Compliance (GRC) roles.
- Articulate the connection between GRC roles.
- Demonstrate the importance of cybersecurity GRC in accomplishing cybersecurity objectives and business goals.

Lesson 2

Governance

- Understand reliance on governance professionals to align business and security strategy.
- Describe how governance professionals are expected to communicate with the organization.
- Develop organizational security policies and procedures.
- Understand common methods for providing employee security training.
- Explain keys to assessing security controls against expected results.

Lesson 3

Risk

- Explain how organizations measure cybersecurity risk.
- Develop risk measurement documentation.
- Remediate risk and report risk measurement and remediation activities to senior leadership.
- Develop and interpret risk statements.
- Understand the differences between value based risk assessment and traditional risk assessment.

Lesson 4

Compliance

- Describe sources of compliance.
- Locate and assess relevant sources of compliance for your organization.
- Interpret compliance obligations and develop control objectives.
- Measure existing security controls against control objectives.

Lesson 5

Audit Management

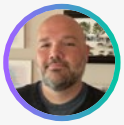
- Understand audit and assessment goals.
- Explain the role governance, risk, and compliance professionals have in ensuring audits achieve expected goals.
- Learn how to facilitate and control audits.
- Develop management responses and remediation plans for audits.

Meet your instructors.

Christine Izuakor, PhD, CISSP

Founder & CEO, Cyber Pop-Up

Dr. Christine Izuakor is the CEO of Cyber Pop-up, an on-demand cybersecurity platform powered by vetted cyber freelancers. She has over a decade of experience leading cybersecurity functions within Fortune 100 companies and has her PhD in security engineering.



Jerry Smith

Information Security Engineer

Jerry is a member of the security operations center for the University of Alabama at Birmingham, where he is the lead threat hunter and a member of the firewall team. Previously he was an information security engineer for Hibbett Sporting Goods.

Ron Woerner, CISSP, CISM

Chief Security Officer

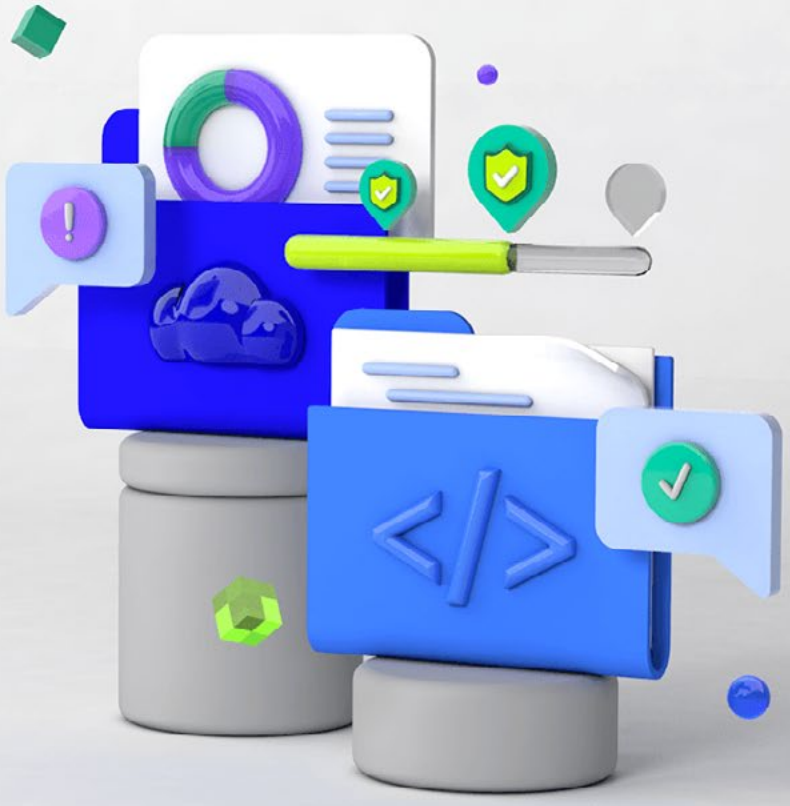
Ron Woerner is a noted consultant, speaker and writer in the security industry. As chief security evangelist at Cyber-AAA, LLC, he delivers training and security risk assessments for small, medium, and large organizations. Woerner also teaches at Bellevue University, an NSA Center of Academic Excellence.

Sean Pike, Esq., M.S.

Sr. Director, Security & GRC

Sean Pike is a cybersecurity and GRC leader with 20+ years of experience leading cybersecurity initiatives in regulated companies. Mr. Pike works with organizations to develop unique, proactive security solutions that follow stringent security principles while accelerating business.

Udacity's learning experience



Hands-on Projects

Open-ended, experiential projects are designed to reflect actual workplace challenges. They aren't just multiple choice questions or step-by-step guides, but instead require critical thinking.

Quizzes

Auto-graded quizzes strengthen comprehension. Learners can return to lessons at any time during the course to refresh concepts.

Knowledge

Find answers to your questions with Knowledge, our proprietary wiki. Search questions asked by other students, connect with technical mentors, and discover how to solve the challenges that you encounter.

Custom Study Plans

Create a personalized study plan that fits your individual needs. Utilize this plan to keep track of movement toward your overall goal.

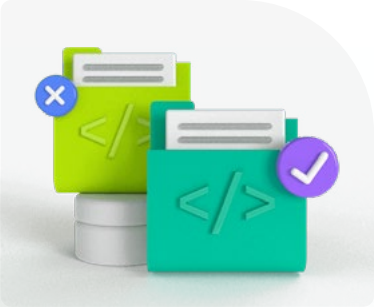
Workspaces

See your code in action. Check the output and quality of your code by running it on interactive workspaces that are integrated into the platform.

Progress Tracker

Take advantage of milestone reminders to stay on schedule and complete your program.

Our proven approach for building job-ready digital skills.



Experienced Project Reviewers

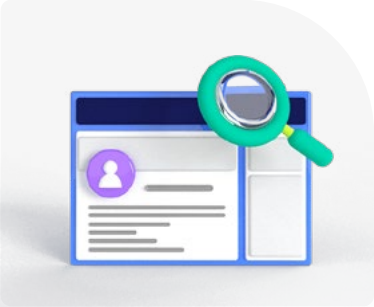
Verify skills mastery.

- Personalized project feedback and critique includes line-by-line code review from skilled practitioners with an average turnaround time of 1.1 hours.
- Project review cycle creates a feedback loop with multiple opportunities for improvement—until the concept is mastered.
- Project reviewers leverage industry best practices and provide pro tips.

Technical Mentor Support

24/7 support unblocks learning.

- Learning accelerates as skilled mentors identify areas of achievement and potential for growth.
- Unlimited access to mentors means help arrives when it's needed most.
- 2 hr or less average question response time assures that skills development stays on track.



Personal Career Services

Empower job-readiness.

- Access to a Github portfolio review that can give you an edge by highlighting your strengths, and demonstrating your value to employers.*
- Get help optimizing your LinkedIn and establishing your personal brand so your profile ranks higher in searches by recruiters and hiring managers.

Mentor Network

Highly vetted for effectiveness.

- Mentors must complete a 5-step hiring process to join Udacity's selective network.
- After passing an objective and situational assessment, mentors must demonstrate communication and behavioral fit for a mentorship role.
- Mentors work across more than 30 different industries and often complete a Nanodegree program themselves.

*Applies to select Nanodegree programs only.

UDACITY

Learn more at

www.udacity.com/online-learning-for-individuals →

12.02.22 | V1.0