
UDACITY
FOR ENTERPRISE
THE SCHOOL OF PROGRAMMING AND DEVELOPMENT
Intro to Cybersecurity
NANODEGREE SYLLABUS

Overview

Introduction to Cybersecurity Nanodegree Program

BUILT IN COLLABORATION WITH

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 3.5 million unfilled cybersecurity jobs by 2021.

The Introduction to Cybersecurity Nanodegree program will equip you with the foundational skills to get started in this highly in-demand field. Graduates 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.

Program Information

ESTIMATED TIME
4 months
Study 10 hours/week

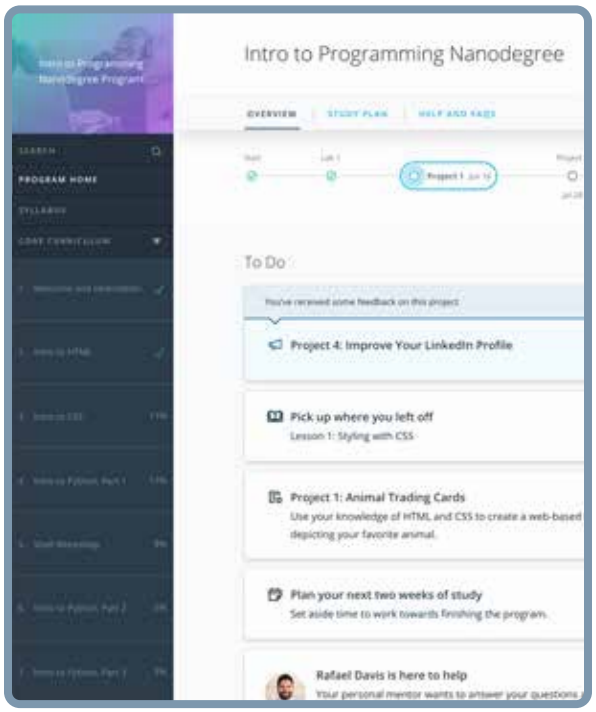
LEVEL
Foundational

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

HARDWARE/SOFTWARE REQUIRED
A computer running recent versions of Windows, Mac OS X, or Linux and an unmetered broadband Internet connection.

LEARN MORE ABOUT THIS NANODEGREE
Contact us at enterpriseNDs@udacity.com.

Our Classroom Experience



REAL-WORLD PROJECTS

Learners build new skills through industry-relevant projects and receive personalized feedback from our network of 900+ project reviewers. Our simple user interface makes it easy to submit projects as often as needed and receive unlimited feedback.

KNOWLEDGE

Answers to most questions can be found with Knowledge, our proprietary wiki. Learners can search questions asked by others and discover in real-time how to solve challenges.

LEARNER HUB

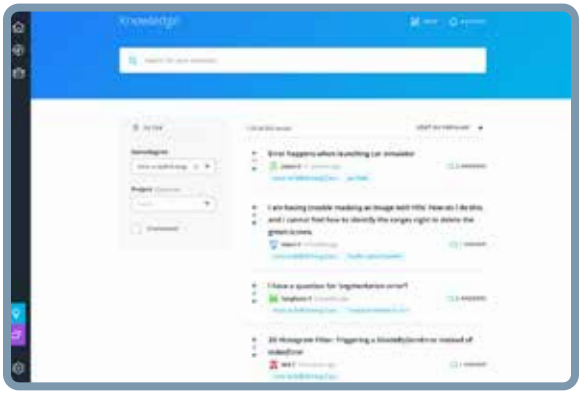
Learners leverage the power of community through a simple, yet powerful chat interface built within the classroom. Learner Hub connects learners with their technical mentor and fellow learners.

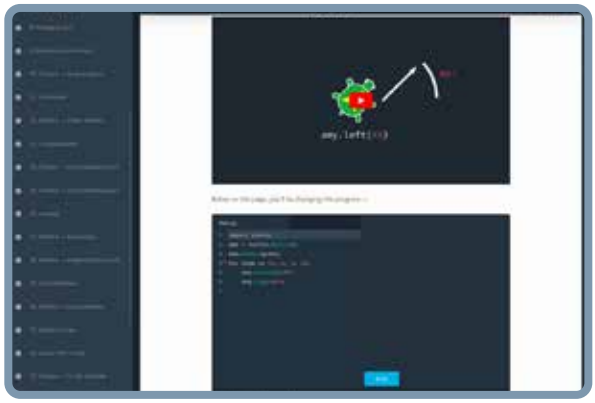
WORKSPACES

Learners can check the output and quality of their code by testing it on interactive workspaces that are integrated into the classroom.

QUIZZES

Understanding concepts learned during lessons is made simple with auto-graded quizzes. Learners can easily go back and brush up on concepts at anytime during the course.





CUSTOM STUDY PLANS

Mentors create a custom study plan tailored to learners' needs. This plan keeps track of progress toward learner goals.

PROGRESS TRACKER

Personalized milestone reminders help learners stay on track and focused as they work to complete their Nanodegree program.

Learn with the Best

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 Birmingham, where he is the lead Threat Hunter and a member of the fi rewall 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.

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. Learners 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.

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 TITLE	LEARNING OUTCOMES
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.
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.
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).

Course 1: Cybersecurity Foundations, cont.

LESSON TITLE	LEARNING OUTCOMES
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.
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.
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.

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 TITLE	LEARNING OUTCOMES
DEFENDING COMPUTER SYSTEMS AND 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.
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.

Course 2: Defending and Securing Systems, cont.

LESSON TITLE	LEARNING OUTCOMES
MONITORING AND 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.
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, and 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.

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.

Course 3: Threats, Vulnerabilities, and Incident Response, cont.

LESSON TITLE	LEARNING OUTCOMES
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.
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.
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.
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, and 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.

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 TITLE	LEARNING OUTCOMES
INTRODUCTION TO GOVERNANCE, RISK, AND 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.
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.

Course 4: Governance, Risk, and Compliance, cont.

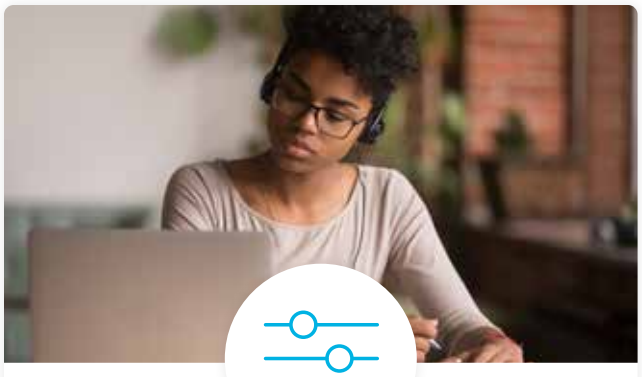
LESSON TITLE	LEARNING OUTCOMES
RISK	• Explain how organizations measure cybersecurity risk. • Develop risk measurement documentation. • Remediate risk and report risk measurement and remediation activities to senior leadership. • Develop and interpret risk statements. • Understand the differences between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

Extracurricular

In this section, there is no project submission. Instead, you will explore a quick overview of the vast world of programming. After this section, you'll have a better understanding of different options you have as a programmer.

LESSON TITLE	LEARNING OUTCOMES
Front-End Programming	• Learn about front-end web developers who create intuitive and responsive websites.
Back-End Programming	• Learn about back-end web programmers who write serverside code to build web apps that serve millions of people worldwide.
Mobile Programming	• Learn about mobile programming and the differences between iOS and Android programming.
Data Analysis Programming	• Learn about data analysts who analyze data to direct growth and make informed decisions.

Our Nanodegree Programs Include:



Pre-Assessments

Our in-depth workforce assessments identify your team's current level of knowledge in key areas. Results are used to generate custom learning paths designed to equip your workforce with the most applicable skill sets.

Dashboard & Progress Reports

Our interactive dashboard (enterprise management console) allows administrators to manage employee onboarding, track course progress, perform bulk enrollments and more.

Industry Validation & Reviews

Learners' progress and subject knowledge is tested and validated by industry experts and leaders from our advisory board. These in-depth reviews ensure your teams have achieved competency.

Real World Hands-on Projects

Through a series of rigorous, real-world projects, your employees learn and apply new techniques, analyze results, and produce actionable insights. Project portfolios demonstrate learners' growing proficiency and subject mastery.

Our Review Process

Real-life Reviewers for Real-life Projects

Real-world projects are at the core of our Nanodegree programs because hands-on learning is the best way to master a new skill. Receiving relevant feedback from an industry expert is a critical part of that learning process, and infinitely more useful than that from peers or automated grading systems. Udacity has a network of over 900 experienced project reviewers who provide personalized and timely feedback to help all learners succeed.

Vaibhav
UDACITY LEARNER

"I never felt overwhelmed while pursuing the Nanodegree program due to the valuable support of the reviewers, and now I am more confident in converting my ideas to reality."

now at
CODING VISIONS INFOTECH

All Learners Benefit From:

- Line-by-line feedback for coding projects
- Industry tips and best practices
- Advice on additional resources to research
- Unlimited submissions and feedback loops

How it Works

Real-world projects are integrated within the classroom experience, making for a seamless review process flow.

- Go through the lessons and work on the projects that follow
- Get help from your technical mentor, if needed
- Submit your project work
- Receive personalized feedback from the reviewer
- If the submission is not satisfactory, resubmit your project
- Continue submitting and receiving feedback from the reviewer until you successfully complete your project

About our Project Reviewers

Our expert project reviewers are evaluated against the highest standards and graded based on learners' progress. **Here's how they measure up to ensure your success.**

900+

Expert Project Reviewers

Are hand-picked to provide detailed feedback on your project submissions.

1.8M

Projects Reviewed

Our reviewers have extensive experience in guiding learners through their course projects.

3

Hours Average Turnaround

You can resubmit your project on the same day for additional feedback.

4.85 /5

Average Reviewer Rating

Our learners love the quality of the feedback they receive from our experienced reviewers.

UDACITY
FOR ENTERPRISE

2440 W El Camino Real, #101
Mountain View, CA 94040, USA - HQ

For more information visit: **www.udacity.com/enterprise**