UDACITY

NANODEGREE PROGRAM SYLLABUS

Introduction to Cybersecurity

Overview

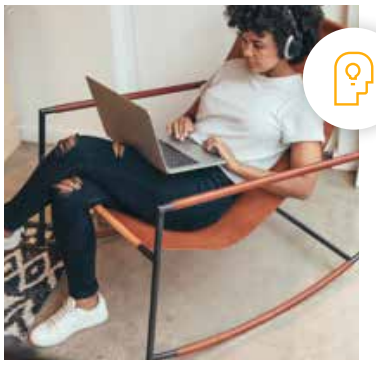
Cybersecurity is a critically important field for businesses in every industry, especially given the proliferation of data breaches (more than 3.2 million records were compromised in the 10 biggest data breaches in the first half of 2020 alone). To reduce risk and improve security, businesses are rushing to hire for cybersecurity roles, yet there's projected to be 3.5 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.
- And much more!

Estimated Time: 4 months at 10hrs/week

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



Flexible Learning: Self-paced

Need Help? udacity.com/advisor

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 Final 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.

	LEARNING OUTCOMES	
LESSON ONE	**Cybersecurity Fundamentals**	• Understand the relevant role of cybersecurity and whyit is important • Describe how business stakeholders play a role in cybersecurity • Become familiar with cybersecurity tools, environments and dependencies
LESSON TWO	**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 THREE	**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 FOUR	**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 FIVE	**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 SIX	**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 Final 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.

	LEARNING OUTCOMES	
LESSON ONE	**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
LESSON TWO	**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 THREE	**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
LESSON FOUR	**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.

Course Final 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.

	LEARNING OUTCOMES	
LESSON ONE	**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 TWO	**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 THREE	**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 FOUR	**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.

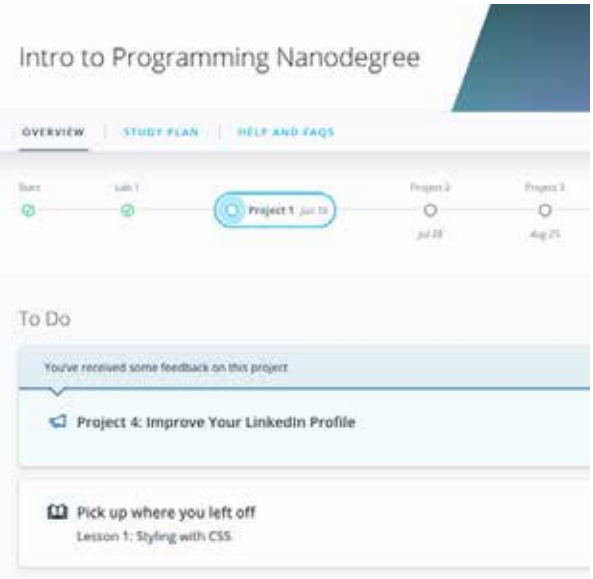
Course Final Project
Create the SwiftTech GRC Program

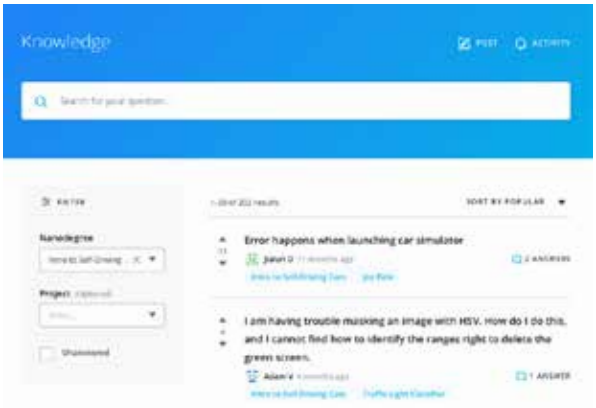
SwiftTech is a company in transition - they are accelerating product development while trying to maintain a high standard for flexibility and responsiveness with customers, and doing all this while migrating their infrastructure to the cloud. This fast paced environment creates challenges for the organization's 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.

		LEARNING OUTCOMES
LESSON ONE	**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
LESSON TWO	**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 THREE	**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 FOUR	**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 FIVE	**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

Our Classroom Experience





REAL-WORLD PROJECTS
Build your skills through industry-relevant projects. Get personalized feedback from our network of 900+ project reviewers. Our simple interface makes it easy to submit your projects as often as you need and receive unlimited feedback on your work.

KNOWLEDGE
Find answers to your questions with Knowledge, our proprietary wiki. Search questions asked by other students and discover in real-time how to solve the challenges that you encounter.

STUDENT HUB
Leverage the power of community through a simple, yet powerful chat interface built within the classroom. Use Student Hub to connect with your technical mentor and fellow students in your Nanodegree program.

WORKSPACES
See your code in action. Check the output and quality of your code by running them on workspaces that are a part of our classroom.

QUIZZES
Check your understanding of concepts learned in the program by answering simple and auto-graded quizzes. Easily go back to the lessons to brush up on concepts anytime you get an answer wrong.

CUSTOM STUDY PLANS
Work with a mentor to create a custom study plan to suit your personal needs. Use this plan to keep track of your progress toward your goal.

PROGRESS TRACKER
Stay on track to complete your Nanodegree program with useful milestone reminders.

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 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.

All Our Nanodegree Programs Include:

EXPERIENCED PROJECT REVIEWERS

REVIEWER SERVICES

- Personalized feedback & line by line code reviews
- 1600+ Reviewers with a 4.85/5 average rating
- 3 hour average project review turnaround time
- Unlimited submissions and feedback loops
- Practical tips and industry best practices
- Additional suggested resources to improve

TECHNICAL MENTOR SUPPORT

MENTORSHIP SERVICES

- Questions answered quickly by our team of technical mentors
- 1000+ Mentors with a 4.7/5 average rating
- Support for all your technical questions

PERSONAL CAREER SERVICES

CAREER SUPPORT

- Resume support
- Github portfolio review
- LinkedIn profile optimization

Frequently Asked Questions

PROGRAM OVERVIEW

WHY SHOULD I ENROLL?

Cybersecurity is a critically important field for businesses in every industry, especially given the proliferance 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 Nanodegreep 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.

WHAT JOBS WILL THIS PROGRAM PREPARE ME FOR?

While this is an introductory course that may not necessarily prepare you for a specific job, it will prepare you with the right foundation with which to pursue more specialized cybersecurity training. It also serves as a great supplement for professionals in IT, Risk Management, and Consulting to bolster their current skillset with a strong grasp of cybersecurity fundamentals.

HOW DO I KNOW IF THIS PROGRAM IS RIGHT FOR ME?

This program is a great fit for anyone interested in building fundamental skills and knowledge in cybersecurity, such as system and network security, threat assessment, and incident response. Whether you're looking to move into a career in the field of cybersecurity, or just want to improve your own understanding of core cybersecurity skills, the Introduction to Cybersecurity Nanodegree program is for you.

ENROLLMENT AND ADMISSION

DO I NEED TO APPLY? WHAT ARE THE ADMISSION CRITERIA?

No. This Nanodegree program accepts all applicants regardless of experience and specific background.

FAQs Continued

WHAT ARE THE PREREQUISITES FOR ENROLLMENT?

To be best prepared to succeed in this program, students should have basic familiarity or experience with:

- Principles of network connectivity
- Basic operating system fundamentals including Windows or Linux

IF I DO NOT MEET THE REQUIREMENTS TO ENROLL, WHAT SHOULD I DO?

We recommend this **Linux Command Line Basics** course if you'd like to learn more about the Linux OS.

TUITION AND TERM OF PROGRAM

HOW IS THIS NANODEGREE PROGRAM STRUCTURED?

The Introduction to Cybersecurity Nanodegree program is comprised of content and curriculum to support four projects. Once you subscribe to a Nanodegree program, you will have access to the content and services for the length of time specified by your subscription. We estimate that students can complete the program in four months, working 10 hours per week.

Each project will be reviewed by the Udacity reviewer network. Feedback will be provided and if you do not pass the project, you will be asked to resubmit the project until it passes..

HOW LONG IS THIS NANODEGREE PROGRAM?

Access to this Nanodegree program runs for the length of time specified in the payment card above. If you do not graduate within that time period, you will continue learning with month to month payments. See the **Terms of Use** and **FAQs** for other policies regarding the terms of access to our Nanodegree programs.

CAN I SWITCH MY START DATE? CAN I GET A REFUND?

Please see the Udacity Program **Terms of Use** and **FAQs** for policies on enrollment in our programs.

SOFTWARE AND HARDWARE - WHAT DO I NEED FOR THIS PROGRAM?

WHAT SOFTWARE AND VERSIONS WILL I NEED IN THIS PROGRAM?

For this Nanodegree program, you will need a desktop or laptop computer running recent versions of Windows, Mac OS X, or Linux and an unmetered broadband Internet connection.