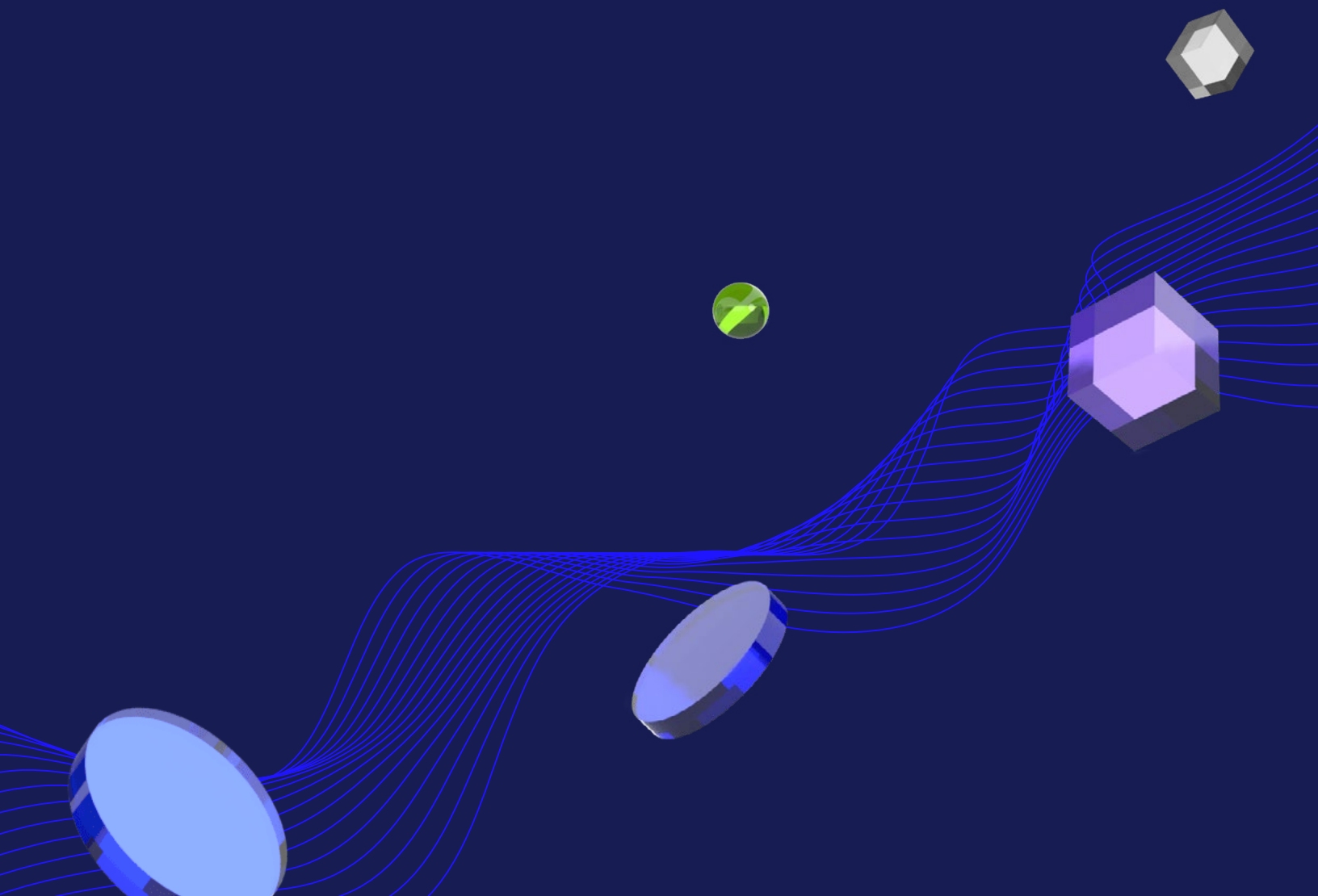




SCHOOL OF CYBERSECURITY

Security Analyst

Nanodegree Program Syllabus



Overview

Prepare to meet the demand for cybersecurity professionals who are trained to play a critical role in protecting an organization's computer networks and systems. Learn to identify, correct, and respond to security weaknesses and incidents by determining appropriate security controls to secure a network, system, or application and assessing security threats through vulnerability scanning and threat assessments. Learners will also monitor network traffic, analyze alert and log data, and follow incident handling procedures in this program.



Learning Objectives

A graduate of this program will be able to:

- Design the appropriate administrative, physical, and logical controls to secure a network, computer system, or application.
- Recommend improvements to the security controls of an existing network, computer system, or application.
- Conduct a threat assessment and build an appropriate threat model.
- Conduct risk analysis and develop mitigation plans that address threats and vulnerabilities of a system.
- Use vulnerability detection utilities and scanning tools to execute a vulnerability assessment.
- Use the Snort Intrusion Detection System to automatically generate alerts based on suspicious network traffic.
- Analyze alerts for false positives and follow appropriate incident handling procedures.
- Use an SIEM to search and correlate security log data across multiple sources.

*Students who do not feel comfortable in the above may consider taking Udacity's Introduction to Cybersecurity course to obtain prerequisite skills.

Program information



Estimated Time

4 months at 10hrs/week*



Skill Level

Intermediate



Prerequisites

A well-prepared learner should:

- Be able to use Python as scripting language and SQL in order to run queries from log data.
- Be familiar with security fundamentals including core security principles, critical security controls, and best practices for securing information.
- Be knowledgeable in database design, large database systems, networking, and operating systems.
- Have experience using Unix or Linux command line.
- Have a basic understanding of client-server architecture.
- Have familiarity with reading and creating simple network architecture diagrams.



Required Hardware/Software

None

*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.

Fundamentals of Defending Systems

In this course, learners will begin their exploration into the role of a security analyst. They will learn about the core principles and philosophy that drive work in the security field. Then, they will discover physical, logical, and administrative controls, their industry recognized frameworks, and how to apply them to secure a network, system, or application. Lastly, learners will apply security concepts to create defensible, resilient network architecture.



Course Project

Planning for Security Controls

In this project, learners will assume the role of a security analyst working on the infrastructure team for a sample company. They will receive detailed sample technical schematics for how they manage their internal information systems and will be tasked with evaluating the company's business structure and needs, assessing their security controls, and making recommendations to improve their security program. As the company evolves to meet security challenges, they will be asked to design a deployment plan for incorporating new controls and new technologies to ensure its viability and long-term success.

Lesson 1

Core Frameworks & Principles

- Explore the underlying goals of information security.
- Discover the defense-in-depth approach to security.
- Identify common network attack vectors.

Lesson 2

Controls

- Examine numerous physical, logical, and administrative controls.
- Evaluate controls necessary to secure a network, computer system, or application.
- Interpret the security controls from an industry-recognized control framework.

Lesson 3

Defensible Network Architecture

- Evaluate methods of deploying security controls using a layered security approach.
- Incorporate security techniques to enhance existing controls.
- Articulate security concepts to appropriate audiences and stakeholders.

Course 2

Analyzing Security Threats

In this course, learners will start by exploring the current threat landscape and identifying both threats and threat actors that organizations face. They will learn about the OWASP Top 10 and that they pose a critical threat to organizations. Then, they'll learn all of the ways to mitigate threats, including the OWASP Top 10. Lastly, they'll learn what threat modeling is and build their own threat models.



Course Project

Insecure Juice Shop

Udajuicer is the biggest juice shop in the world, and learners will help them analyze their new online application. In this project, learners will work to identify the threat actor and attack that is taking down their website. From there they will perform a threat assessment, analyzing their architecture and building a threat model. Learners will then perform a vulnerability analysis to identify OWASP vulnerabilities and exploit those vulnerabilities themselves. Afterwards, they will conduct a risk analysis and build a mitigation plan for all of the threats and vulnerabilities discovered.

Lesson 1

Identifying Security Threats

- Explore cybersecurity landscape.
 - Identify internal and external threats.
 - Analyze the OWASP Top 10.
 - Identify threat actors and TTPs.
-

Lesson 2

Mitigating Threats

- Explore mitigation strategies for internal threats.
 - Dive into mitigation strategies for external threats.
 - Develop mitigation plans for OWASP Top 10.
-

Lesson 3

Threat Modeling

- Define threat modeling.
- Explore different threat models.
- Build a threat model.

Course 3

Assessing Vulnerabilities & Reducing Risk

Learn how security analysts address system vulnerabilities in order to reduce organizational risk. First learn about vulnerabilities, their characteristics, and their dynamic lifecycle. Then explore the ways analysts assess vulnerabilities, including reviewing and administering scanning tools and utilities. Learn how to measure the risks associated with discovered vulnerabilities. Lastly, review ways to communicate risk in order to plan remediation and mitigation activities.



Course Project

Juice Shop Vulnerabilities Report

In this project learners will execute a vulnerability assessment, prioritize risk, and communicate findings to stakeholders and leadership. They will receive a purposefully flawed and vulnerable web application. As they assume the role of a security analyst, they will execute any number of vulnerability detection utilities and scans of their choice against this web application to determine its flaws. Then, they will perform a vulnerability assessment and a risk analysis. Finally, learners will communicate their analysis of system vulnerabilities by creating an executive report suitable for executive leadership.

Lesson 1

Understanding Vulnerabilities

- Identify common vulnerabilities.
- Examine the vulnerability lifecycle.
- Explore vulnerability databases and documentation methods.

Lesson 2

Assessing Vulnerabilities

- Appropriately scope and administer a vulnerability assessment engagement.
- Review and select the appropriate assessment tools and strategies.
- Execute assessment activities.
- Analyze and interpret assessment results.

Lesson 3

Determining Risk & Business Impact

- Analyze the probability of compromise given vulnerability data.
- Analyze the potential for impact of identified vulnerabilities.
- Evaluate the risk of vulnerabilities using industry frameworks.

Lesson 4

Managing & Mitigating Risk

- Prioritize remediation/mitigation efforts.
- Communicate risk to stakeholders.
- Provide strategic guidance for leadership to effectively reduce risk.

Monitoring, Logging & Responding to Incidents

In this course, learners will discover the importance of incident detection and use the Snort Intrusion Detection System to automatically generate alerts based on suspicious network traffic. They will learn to analyze automated alerts for false positives and determine if they represent a real security threat. They will analyze network traffic using Wireshark and capture live traffic using tcpdump. They will also use Splunk to search and correlate security log data across multiple sources. Finally, they will follow incident handling procedures to respond and recover from security incident scenarios.



Course Project

Intrusion Detection & Response

In this project, learners will be acting as a security analyst, filling in for an analyst on vacation. They'll be provided with a network diagram, incident handling playbooks, and network log and host log data to analyze. During the network log analysis, learners will uncover a security incident. They'll use Wireshark to dive deep into the data to understand the scope of the issue and follow the appropriate incident handling playbook to handle the issue. They'll develop an Intrusion Detection System (IDS) rule to help alert on similar malicious network traffic and create Splunk dashboards and reports to further identify events of interest.

Lesson 1

Incident Detection

- Identify threats and alerts.
- Understand Intrusion Detection Systems (IDS).
- Create a custom Snort IDS rule.
- Analyze IDS alert data.
- Evaluate and categorize IDS alerts.

Lesson 2

Monitoring & Logging

- Understand the key features of centralized logging.
 - Describe the advantages of a SIEM platforms.
 - Correlate network alerts and host log data.
 - Capture live network traffic.
 - Create Splunk dashboards and reports.
 - Develop SIEM functionality using Splunk.
-

Lesson 3

Incident Handling

- Describe the phases of the incident handling process.
- Evaluate incident handling playbooks.
- Identify factors that contribute to incident severity.
- Recommend an effective incident remediation plan.

Meet your instructors.



Richard Phung

Information Security Analyst

Richard is an SSCP and CISSP with over a decade of enterprise systems administration experience. He is dedicated to empowering businesses and their people to meet the demands of a continually evolving threat landscape. Richard holds a BA in psychology from Hendrix College and a Master of Education (EdM) from Lesley University.



Milind Adari

Security Engineer

Milind Adari is a security engineer at The Associated Press and an adjunct instructor at Columbia University. He is responsible for protecting journalists all around the world from malicious threat actors and state-sponsored attacks, all the while educating students and professionals in cybersecurity.

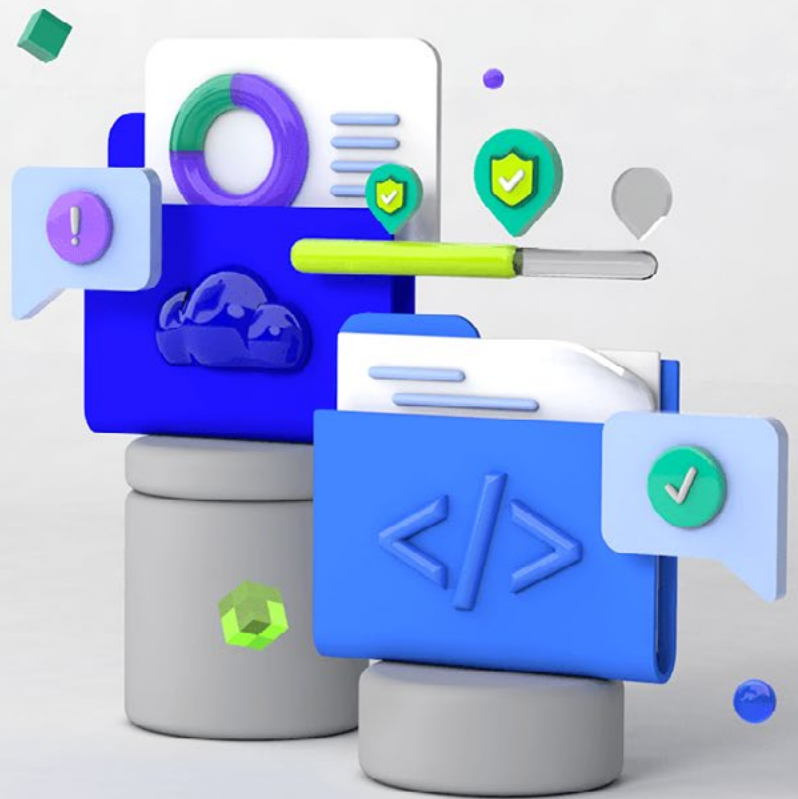


Chris Herdt

Security Analyst III

Chris Herdt is a security analyst at the University of Minnesota and an adjunct instructor at Dunwoody College. In addition to network security, his other specialties are web application security and Linux operating system security. Chris has a master's in computer and information technology from the University of Pennsylvania.

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

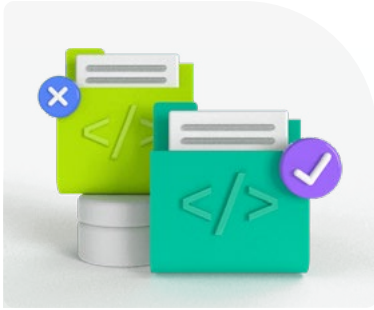
See your code in action. Check the output and quality of your code by running it on interactive workspaces that are integrated into the platform.



Progress Tracker

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

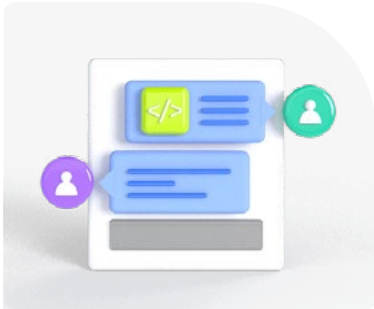
Our proven approach for building job-ready digital skills.



Experienced Project Reviewers

Verify skills mastery.

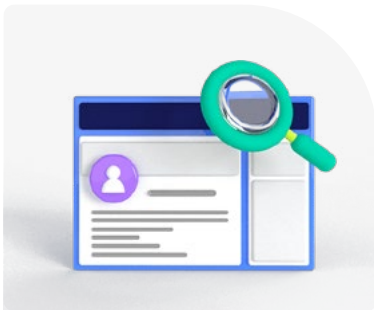
- Personalized project feedback and critique includes line-by-line code review from skilled practitioners with an average turnaround time of 1.1 hours.
- Project review cycle creates a feedback loop with multiple opportunities for improvement—until the concept is mastered.
- Project reviewers leverage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



Technical Mentor Support

24/7 support unblocks learning.

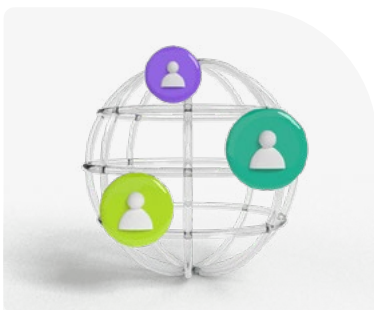
- Learning accelerates as skilled mentors identify areas of achievement and potential for growth.
- Unlimited access to mentors means help arrives when it's needed most.
- 2 hr or less average question response time assures that skills development stays on track.



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.



Learn more at

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