UDACITY

NANODEGREE PROGRAM SYLLABUS

Security Analyst

UDACITY

Overview

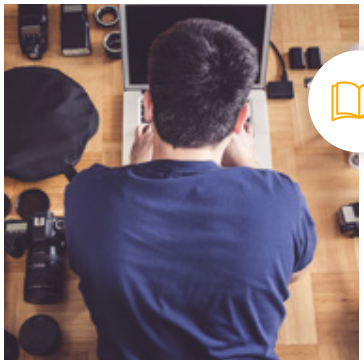
Prepare to meet the demand for cybersecurity professionals who are trained to play a critical role in protecting an organization's computer networks and systems. Learn to identify, correct and respond to security weaknesses and incidents by determining appropriate security controls to secure a network,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

Prerequisites:

- 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

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

Length of Program*:
4 months



Textbooks required:
None

Frequency of Classes:
The program is flexible, self-paced with suggested project deadlines

Need Help?
udacity.com/advisor
Discuss this program with an enrollment advisor.

*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 10 hours per week working through the program, you should finish within the time provided. Actual hours may vary.

Course 1: Fundamentals of Defending Systems

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

Project 1
Planning for Security Controls

In this project, you will assume the role of a security analyst working on the infrastructure team for a sample company. You 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, you will be asked to design a deployment plan for incorporating new controls and new technologies to ensure its viability and long-term success.

	LEARNING OUTCOMES	
LESSON ONE	**Core Frameworks and Principles**	• Explore the underlying goals of information security. • Discover the Defense-in-Depth approach to security. • Identify common network attack vectors.
LESSON TWO	**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 THREE	**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, you'll start by exploring the current threat landscape and identifying both threats and threat actors that organizations face. You will learn about the OWASP Top 10 and that they pose a critical threat to organizations. Then, you'll learn all of the ways to mitigate threats, including the OWASP Top 10. Lastly, you'll learn what threat modeling is and build your own threat models.

Project 2
Insecure Juice Shop

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

	LEARNING OUTCOMES	
LESSON ONE	**Identifying Security Threats**	• Explore cybersecurity landscape. • Identify internal & external threats. • Analyze the OWASP Top 10. • Identify threat actors and TTPs.
LESSON TWO	**Mitigating Threats**	• Explore mitigation strategies for internal threats. • Dive into mitigation strategies for external threats. • Develop mitigation plans for OWASP Top 10.
LESSON THREE	**Threat Modeling**	• Define threat modeling. • Explore different threat models. • Build a threat model.

Course 3: Assessing Vulnerabilities and Reducing Risk

In this course, you will learn how security analysts address system vulnerabilities in order to reduce organizational risk. You will first learn about vulnerabilities, their characteristics and their dynamic lifecycle. You will then explore the ways analysts assess vulnerabilities, including reviewing and administering scanning tools and utilities. You will learn how to measure the risks associated with discovered vulnerabilities. Lastly, you will review ways to communicate risk in order to plan remediation and mitigation activities.

Project 3
Juice Shop Vulnerabilities Report

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

	LEARNING OUTCOMES	
LESSON ONE	**Understanding Vulnerabilities**	• Identify common vulnerabilities. • Examine the vulnerability lifecycle. • Explore vulnerability databases and documentation methods.
LESSON TWO	**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 ONE	**Determining Risk and 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 TWO	**Managing and Mitigating Risk**	• Prioritize remediation/mitigation efforts. • Communicate risk to stakeholders. • Provide strategic guidance for leadership to effectively reduce risk.

UDACITY

Course 4: Monitoring, Logging and Responding to Incidents

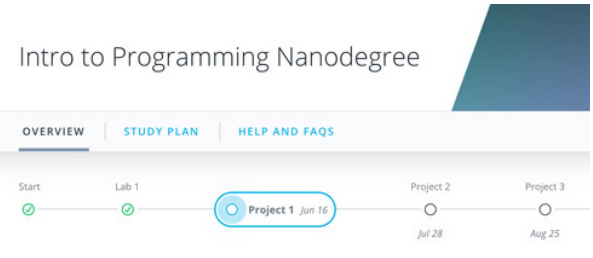
In this course, you will discover the importance of incident detection and use the Snort Intrusion Detection System to automatically generate alerts based on suspicious network traffic. You will learn to analyze automated alerts for false positives and determine if they represent a real security threat.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

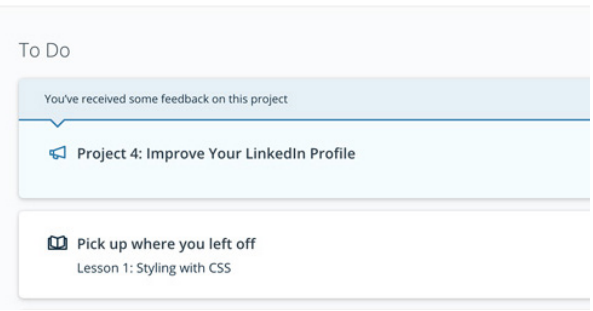
Project 4
Intrusion Detection and Response

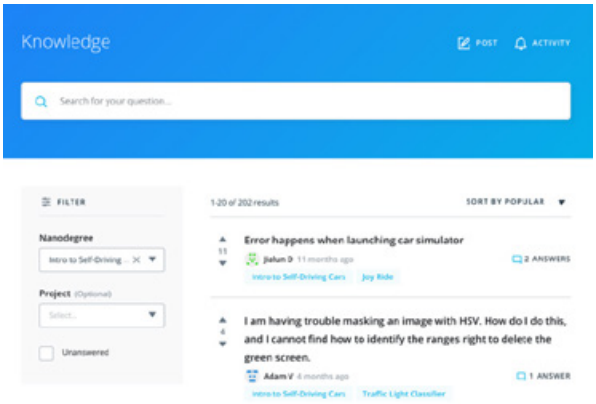
In this project, you will be acting as a security analyst, filling in for an analyst on vacation. You'll be provided with a network diagram, incident handling playbooks, and network log and host log data to analyze. During your network log analysis, you'll uncover a security incident. You'll use Wireshark to dive deep into the data to understand the scope of the issue and follow the appropriate incident handling playbook to handle the issue. You'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.

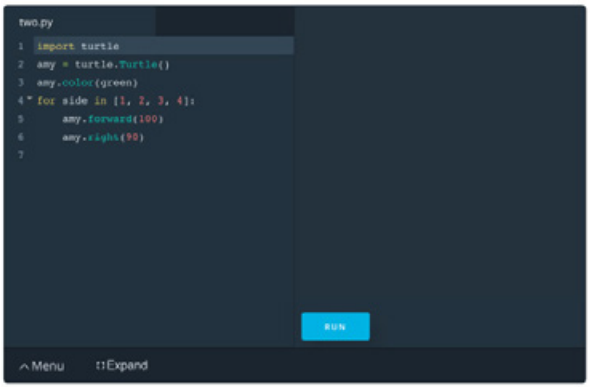
	LEARNING OUTCOMES	
LESSON ONE	**Incident Detection**	• Identify threats and alerts. • Understand Intrusion Detection Systems (IDS). • Create a custom Snort IDS rule. • Analyze IDS alert data. • Evaluate and categorize IDS alerts.
LESSON TWO	**Monitoring and Logging**	• Understand the key features of 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 THREE	**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.

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

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 of Computer and Information Technology from the University of Pennsylvania.

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

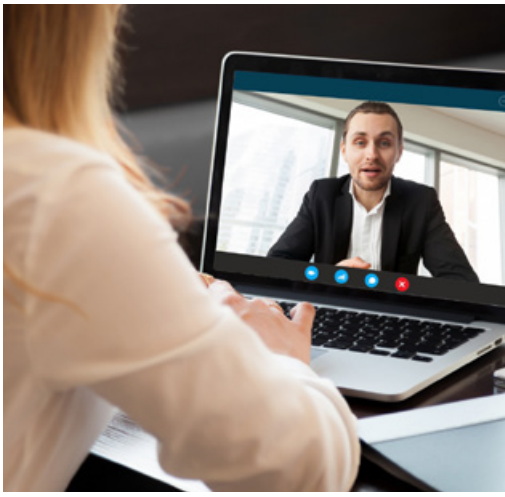
PERSONAL CAREER SERVICES

CAREER SUPPORT

- Resume support
- Github portfolio review
- LinkedIn profile optimization

Frequently Asked Questions

PROGRAM OVERVIEW



WHY SHOULD I ENROLL?

The global cybersecurity market is currently worth $173B in 2020, growing to $270B by 2026. This program was designed to help you take advantage of the growing need for skilled security analysts. 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.

WHAT JOBS WILL THIS PROGRAM PREPARE ME FOR?

The need for a strong cybersecurity culture in an enterprise organization is greater than ever. The skills you will gain from this Nanodegree program will qualify you for jobs in several industries as countless companies are boosting security protocol.

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

The course is for developers who already use SQL and Python and have a basic understanding of network infrastructure, but want to advance their career and increase their earning potential.

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.

WHAT ARE THE PREREQUISITES FOR ENROLLMENT?

The Security Analyst Nanodegree Program is an intermediate course for developers. Learners should:

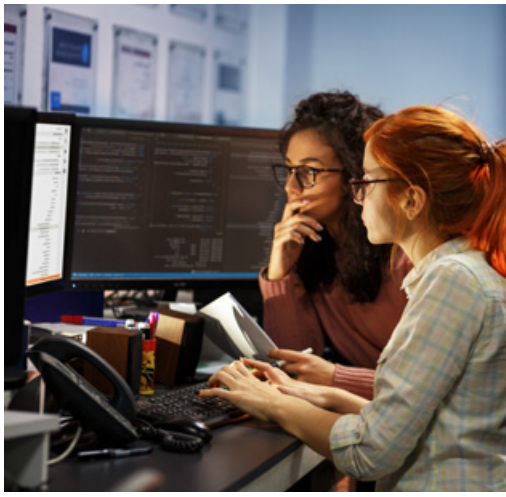
- Be able to use Python as scripting language and SQL in order to run queries from Log data
- Be familiar with security fundamentals including core security principles, critical security controls, and best practices for securing information.
- Be knowledgeable in database design, large database systems, 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

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

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

FAQs Continued

TUITION AND TERM OF PROGRAM



HOW IS THIS NANODEGREE PROGRAM STRUCTURED?

The Security Analyst Nanodegree program is comprised of content and curriculum to support four projects. We estimate that students can complete the program in four months, working five to ten 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 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 SOFTWARE AND VERSIONS WILL I NEED IN THIS PROGRAM?

There are no software and version requirements to complete this Nanodegree program. All coursework and projects can be completed via Student Workspaces in the Udacity online classroom.