UDACITY
FOR ENTERPRISE

THE SCHOOL OF PROGRAMMING AND DEVELOPMENT

Security Analyst

NANODEGREE SYLLABUS

Overview

Security Analyst Nanodegree Program

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.

Program Information

TIME
4 months
Study 10 hours/week

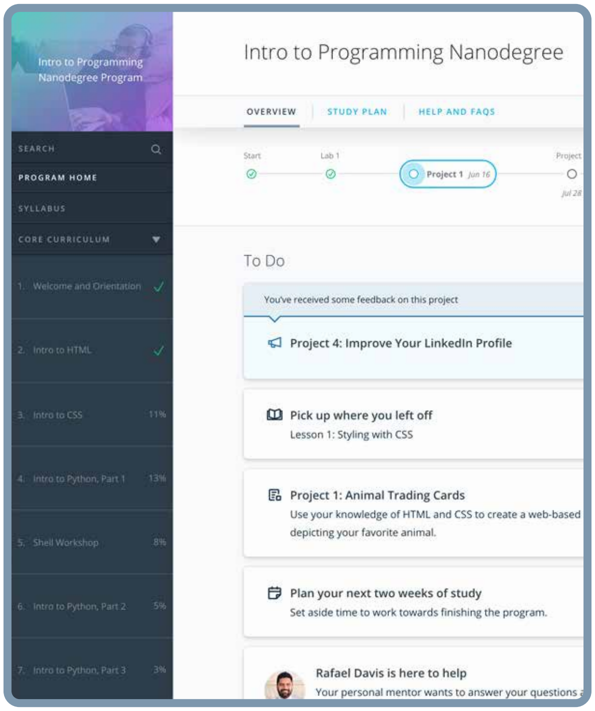
LEVEL
Practitioner

PREREQUISITES
Experience with Python, SQL, security fundamentals, database design, and networking and operating systems.

HARDWARE/SOFTWARE REQUIRED
Access to the internet and a 64-bit computer.

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

Our Classroom Experience



Intro to Programming Nanodegree Program

Intro to Programming Nanodegree

OVERVIEW | STUDY PLAN | HELP AND FAQS

Start · Lab 1 · Project 1 Jun 16 · Project Jul 28

SEARCH

PROGRAM HOME

SYLLABUS

CORE CURRICULUM

1. Welcome and Orientation ✓

2. Intro to HTML ✓

3. Intro to CSS 11%

4. Intro to Python, Part 1 13%

5. Shell Workshop 8%

6. Intro to Python, Part 2 5%

7. Intro to Python, Part 3 3%

To Do

You've received some feedback on this project

Project 4: Improve Your LinkedIn Profile

Pick up where you left off
Lesson 1: Styling with CSS

Project 1: Animal Trading Cards
Use your knowledge of HTML and CSS to create a web-based depicting your favorite animal.

Plan your next two weeks of study
Set aside time to work towards finishing the program.

Rafael Davis is here to help
Your personal mentor wants to answer your questions

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

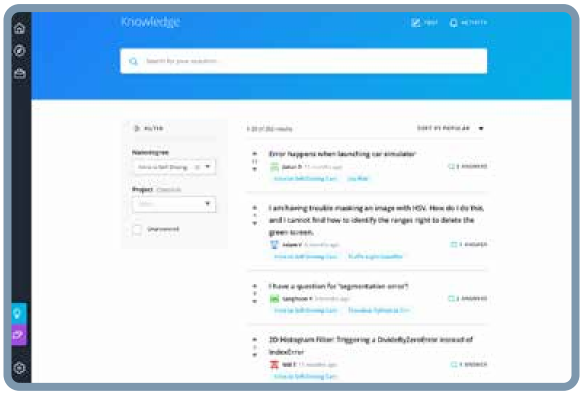
Learners leverage the power of community through a simple, yet powerful chat interface built within the classroom. Learner Hub connects learners with their technical mentor and fellow learners.

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.



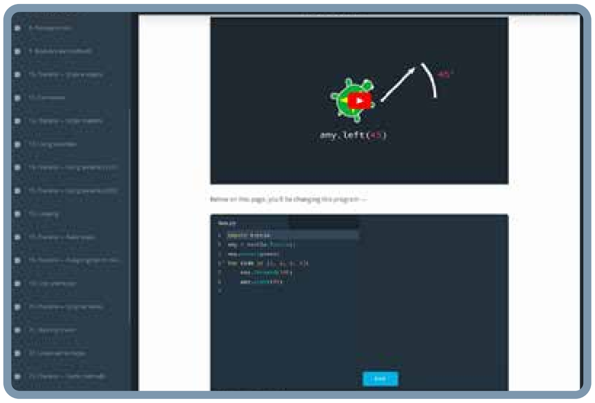
Knowledge

Error happens when launching car simulator

I am having trouble masking an image with HSV. How do I do this, and I cannot find how to identify the ranges right to delete the green screen.

I have a question for "segmentation error"

2D Histogram Filter: Triggering a DivideByZeroError instead of IndexError



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

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.

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 — 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.

LESSON TITLE	LEARNING OUTCOMES
CORE FRAMEWORKS AND PRINCIPLES	• Explore the underlying goals of information security. • Discover the Defense-in-Depth approach to security. • Identify common network attack vectors.
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.
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 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.

LESSON TITLE	LEARNING OUTCOMES
IDENTIFYING SECURITY THREATS	• Explore cybersecurity landscape. • Identify internal & external threats. • Analyze the OWASP Top 10. • Identify threat actors and TTPs.
MITIGATING THREATS	• Explore mitigation strategies for internal threats. • Dive into mitigation strategies for external threats. • Develop mitigation plans for OWASP Top 10.
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

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.

LESSON TITLE	LEARNING OUTCOMES
UNDERSTANDING VULNERABILITIES	• Identify common vulnerabilities. • Examine the vulnerability lifecycle. • Explore vulnerability databases and documentation methods.
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.

Course 3: Assessing Vulnerabilities and Reducing Risk

LESSON TITLE	LEARNING OUTCOMES
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.
MANAGING AND MITIGATING RISK	• Prioritize remediation/mitigation efforts. • Communicate risk to stakeholders. • Provide strategic guidance for leadership to effectively reduce risk.

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 — 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.

LESSON TITLE	LEARNING OUTCOMES
INCIDENT DETECTION	• Identify threats and aAerts. • Understand Intrusion Detection Systems (IDS). • Create a custom Snort IDS rule. • Analyze IDS alert data. • Evaluate and categorize IDS alerts.
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.

COURSE 4: Monitoring, Logging and Responding to Incidents, cont.

LESSON TITLE	LEARNING OUTCOMES
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 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

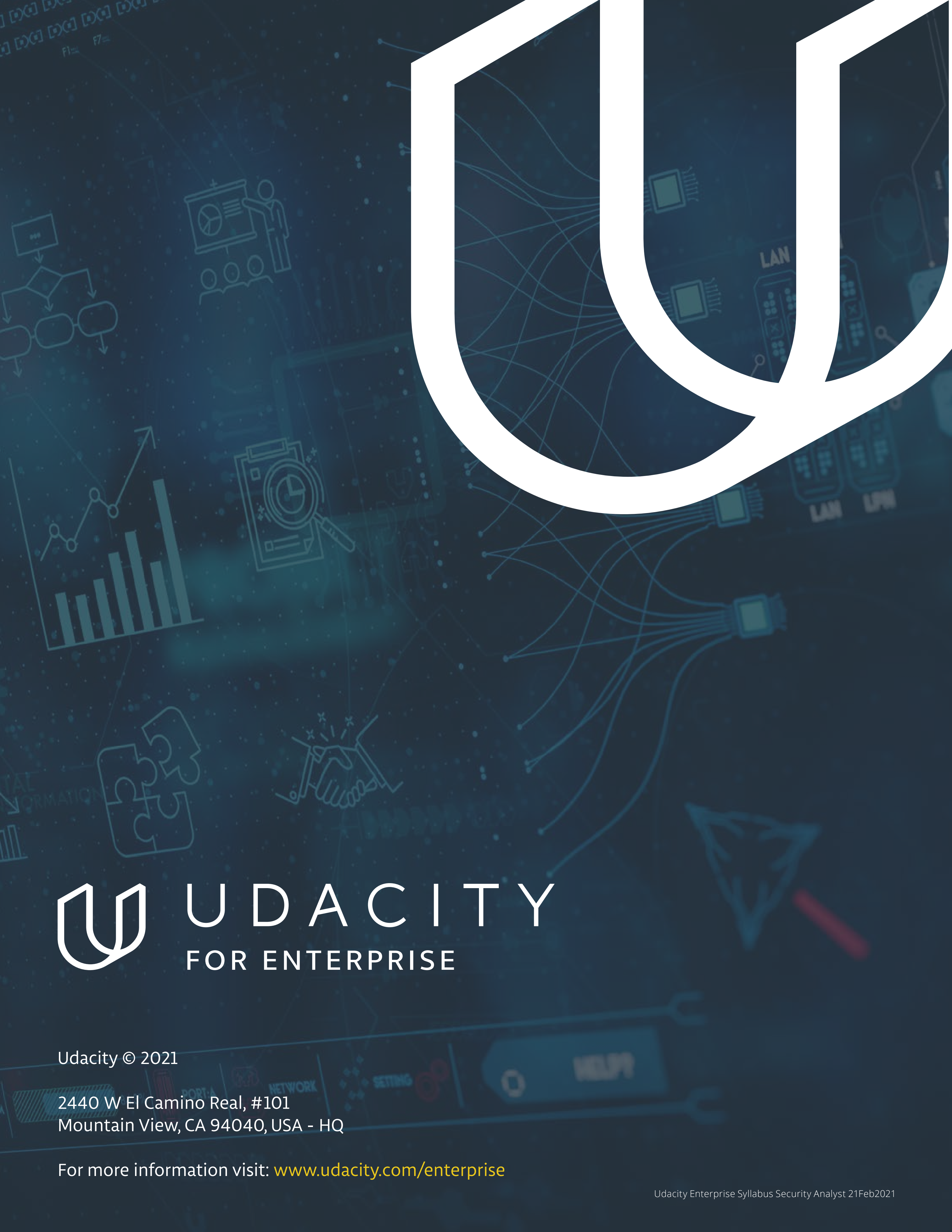
Hours Average Turnaround

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