UDACITY
FOR ENTERPRISE

THE SCHOOL OF CYBERSECURITY

Security Architect

NANODEGREE SYLLABUS

Overview

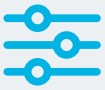
Security Architect Nanodegree Program

The goal of the Security Architect Nanodegree is to equip learners with the necessary skills required to advance their careers in the field of cybersecurity. As a security architect, you'll be charged with designing security systems to thwart malware, hacker intrusions and denial-of-service attacks. The program addresses security topics related to architectural and implementation skills required by a skilled cybersecurity professional for critical use-cases like identity and access management, infrastructure security, threat detection and, incident response.

Program Information

TIME
4 months
Study 10 hours/week

LEVEL
Intermediate

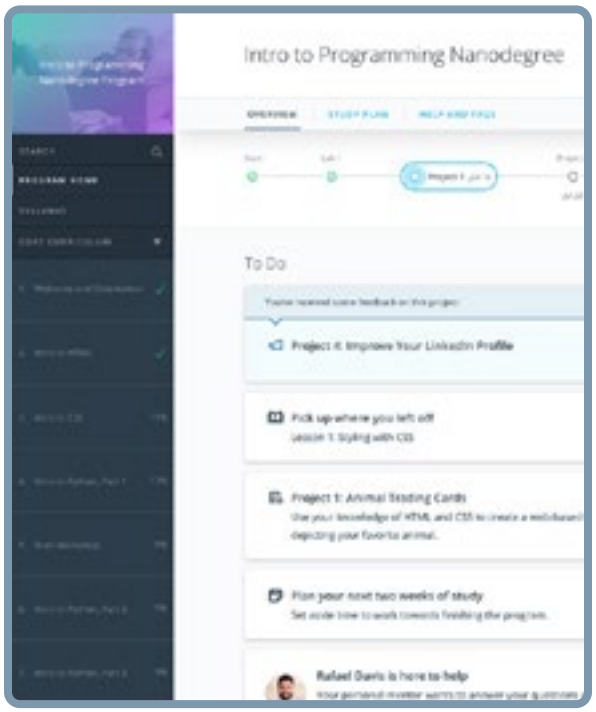


PREREQUISITES
Linux and AWS

HARDWARE/SOFTWARE REQUIRED
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. Udacity's basic tech requirements can be found at https://www.udacity.com/tech/requirements.

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

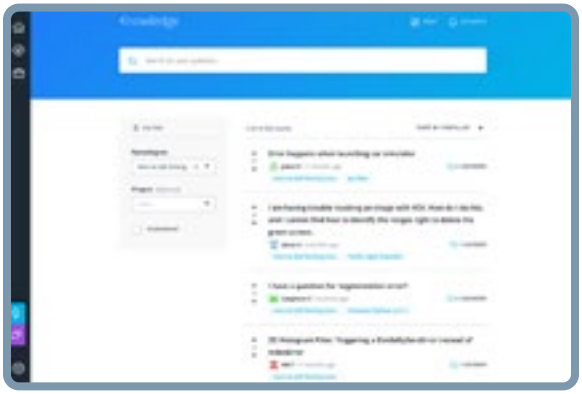
Learners leverage the power of community through a simple, yet powerful chat interface built within the classroom. Learner Hub connects learners with their technical mentor and fellow learners.

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

Erick Galinkin

PRINCIPAL AI RESEARCHER RAPID7

Erick Galinkin is a hacker and scientist specializing in applying artificial intelligence to cybersecurity. He also conducts academic research on machine learning theory and the interplay between algorithmic game theory and information security.

Sjon-Paul Brown

SENIOR DEVOPS ENGINEER

Sjon-Paul Brown is a DevOps engineer and DevOps consultant who helps companies streamline and secure their cloud environments and development processes. He has formally worked with varying startups and enterprises to ensure to that software can be securely developed and deployed in an agile manner.

Abhinav Singh

CYBERSECURITY RESEARCHER

Abhinav is a cybersecurity researcher with nearly a decade of experience working for global leaders in security technology, financial institutions and as an independent consultant. He is the author of Metasploit Penetration Testing Cookbook and Instant Wireshark Starter, as well as many papers, articles and blogs.

William O. Ferguson

CLOUD ARCHITECT

William serves as a subject matter expert for complex information assurance and security engineering efforts worldwide. He helps foster a better view into the globalized challenges of secure computing worldwide as a global digital professional with intimate knowledge of both domestic and foreign network infrastructures.

Course 1: Security Architecture Planning & Design

This course introduces the fundamental security planning, design and systems thinking concepts that are used throughout security architecture. As networks and applications grow more complex, the need to identify potential sources of weakness that are a product of that complexity becomes crucial. Students who complete this course will be equipped with the skills to identify and evaluate risks in systems, assess whether or not risks are acceptable, and work alongside stakeholders to prioritize remediation efforts.

Project: Conduct an Application Security Review

Conducting application security reviews is an important part of planning, building and deploying secure systems. As part of a security process, we conduct a technical security assessment for each newly deployed application or service. For applications that haven't had a security review, your job includes making sure they meet the standards of the organization. In this project, students review a customer information management system (CIMS) for security vulnerabilities and write up their findings in a technical report.

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
INTRODUCTION TO SECURITY PLANNING & DESIGN	• Categorize risks by severity based on impact and likelihood • Identify risks in application architectures by considering the details of the system • Create architecture diagrams using diagramming software • Identify threats to a system by examining its exposure and value to attackers
SECURITY AND REGULATORY FRAMEWORKS	• Determine the applicability of security frameworks to their organization by considering the types of data managed by the organization • Distinguish between different security frameworks and identify their commonalities and differences • Distinguish between different regulatory frameworks and identify their commonalities and differences
DESIGNING SECURE SYSTEMS	• Prioritize risk reduction by evaluating the severity of a risk and the cost to remediate it. • Design architectures that are highly usable by identifying key stakeholders and prioritizing their needs • Assess security problems within trust models by applying risk minimization principles • Balance business needs with security needs by conducting analysis of security controls

Course 2: Enterprise Identity and Access Control

Identity and access control management is fundamental to the security of any organization. This course introduces the fundamentals needed to create and implement access control within an organization. Specifically, this course teaches the fundamentals of managing access control within cloud environments such as AWS. Students who complete this course will be equipped with the skills to design, implement and enforce access control using different access control models. In doing so, they will be prepared to implement access control that is maintainable and aligns with the principle of least privilege.

Project: Architecting IAM Implementation with Enforcement

Creating and enforcing a role structure is critical to the success of access control within an organization. In this project, students will implement a role structure with policies that will be evaluated and enforced. Using an access control matrix that outlines the appropriate roles, resources and actions to be implemented, students will create the role structure within AWS. They will ensure that least privilege is maintained by evaluating the access defined in the policies to ensure that it aligns with the access defined in the matrix. Upon implementation of the policies and permissions, they will be leveraging AWS Config to evaluate IAM policies to ensure that the organizational requirements are maintained.

LESSON TITLE	LEARNING OUTCOMES
IAM ACCESS CONTROL MODELS AND AWS	• Identify and justify the correct Access Control Model given a scenario • Define and employ RBAC and determine the use cases in which it should be employed • Define and employ ABAC and evaluate the benefits of its use in given scenarios
BUILDING ACCESS CONTROL MATRIX AND MAPPING PERMISSIONS	• Identify access control components • Translate access control components from requirements • Create access control matrix from predefined requirements

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
BUILDING ORGANIZATIONAL ROLE STRUCTURE	• Create IAM roles from subjects in access control matrix • Create scoped IAM policies from permissions in access control matrix • Create IAM restrictions from restrictions defined in access control matrix
BUILDING ORGANIZATIONAL ROLE AND ACCESS VISUALIZATION	• Identify elements and resources to be visualized from the access control matrix • Create visualization for IAM roles • Create visualization for IAM policies • Create visualization for each resource and permissions
ENFORCING IAM POLICY CONFIGURATIONS	• Identify and employ use cases for AWS Config • Evaluate IAM requirements from the access control matrix that must be enforced • Create AWS Config rules for alerting on non-compliant IAM policies

Course 3: Infrastructure & Network Security Architecture Planning & Design

This course covers infrastructure and network security concepts essential for designing and implementing secure infrastructure. Complex infrastructures can have multiple moving components connected over a network. A multi-layered security architecture is required to provide complete visibility of system and service behavior. This course covers aspects of architecting and building security alerting and monitoring services that are scalable throughout the enterprise.

Project: Watertight Security

The Water & Power Organization (WPO) audits and maintains the billing and usage of its customers with an application that allows its field agents to upload the picture of the meters attached in customers' houses. Lately, WPO engineers started noticing a lot of binary files getting uploaded through the application which are actually malware files. It is possible that either someone is deliberately trying to attack the application by uploading malware files or one of the field agent's devices is infected and is being used to target WPO's application. As a security architect, you have been called onboard to help improve the overall security of the service and mitigate possible disruption to WPO and its customers.

LESSON TITLE	LEARNING OUTCOMES
INFRASTRUCTURE & NETWORK SECURITY ARCHITECTURE PLANNING & DESIGN	• Understand framework types and implement them to security problems • Build network boundaries and define access types for the infrastructure. • Map security services with network and infrastructure • Identify, quantify and rectify cybersecurity risks associated with the business or infrastructure

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
BUILDING INTELLIGENCE DRIVEN, DEFENSE-IN-DEPTH ARCHITECTURE	• Implement Defense-in-Depth (DiD) on your infrastructure and network • Secure an organization with a threat-driven Approach • Map the various stages of a cyber attack with the Cyber Kill Chain model
THREAT SURFACE ANALYSIS & BUILDING SCALABLE DETECTION SERVICE	• Use the STRIDE methodology to complete threat modeling • Integrate security best practices into existing business and application process flow • Plan and build scalable services that can detect certain types of threats for the business or application • Integrate an alert pipeline for security teams to monitor for security incidents
THREAT TRIAGE AND DETECTION ENRICHMENT	• Describe detection and response processes and frameworks • Implement the MITRE ATT&CK framework to map our threat landscape against different attack scenarios • Design playbooks to triage and remediate security incidents quickly and efficiently

Course 4: Incident Response & Business Continuity Architecture Planning, Design & Implementation

This course introduces the fundamental incident response planning, design and architecture concepts that are used in the cloud. As cloud solutions grow more complex so must the related incident response capabilities. Students who complete this course will be equipped with the skills to plan, design and execute a strong set of foundational cloud incident response capabilities.

Upon completion of this course students will be able to:

- Plan incident response roles, conduct asset inventories and configure logging and monitoring
- Plan and implement artifact collection, containment and isolation, and automated response procedures in runbooks
- Plan, implement and validate business continuity actions in runbooks

Project: Incident Response and Business Continuity for Micro-Assurances

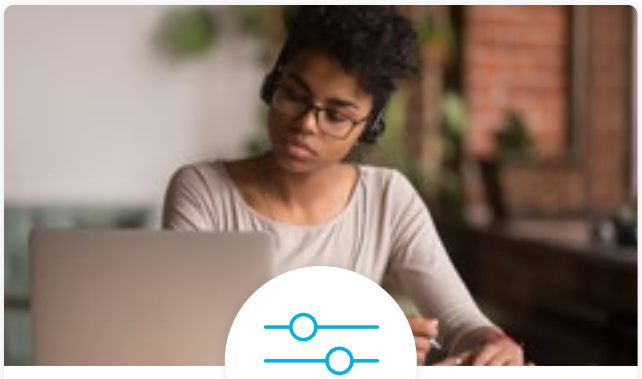
It is your first day as the incident response and business continuity manager for a small insurance company called Micro-Assurances. They have a small but important deployment in the AWS cloud and this deployment supports their primary business function which is processing insurance policy claims. If both of their servers are unavailable the company will incur fines, lose customers and possibly have to shut down.

An architecture diagram was provided to you depicting a public-facing AWS elastic load balancer, Linux, Apache, MySQL, and PHP (LAMP) server in a primary availability zone and LAMP server in a secondary availability zone. In addition, you were informed that the AWS platform team consists of a database administrator, system administrator, network engineer, application owner, security analyst and incident responder. You will now have to create and execute a cloud incident response runbook for a compromised database administrator account.

Nanodegree Program Overview

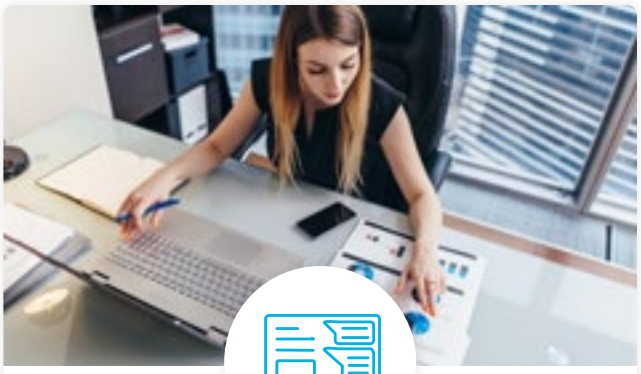
LESSON TITLE	LEARNING OUTCOMES
INCIDENT RESPONSE & BUSINESS CONTINUITY ARCHITECTURE PLANNING, DESIGN & IMPLEMENTATION	• Plan incident response roles, conduct asset inventories and configure logging and monitoring • Plan and implement artifact collection, containment and isolation, and automated response procedures in runbooks • Plan, implement and validate business continuity actions in runbooks
INCIDENT RESPONSE RUNBOOKS FOR CLOUD INFRASTRUCTURE	• Identify and document incident response roles and responsibilities • Document an asset inventory for incident response • Configure logging and monitoring for cloud incident response
INCIDENT RESPONSE PLAYBOOKS AND AUTOMATION	• Collect artifacts for incident response in a cloud environment • Contain and isolate infected resources for incident response in a cloud environment • Automate incident response scripts in a cloud environment
BUSINESS CONTINUITY	• Perform business continuity analysis • Automate business continuity actions • Validate and document business continuity

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

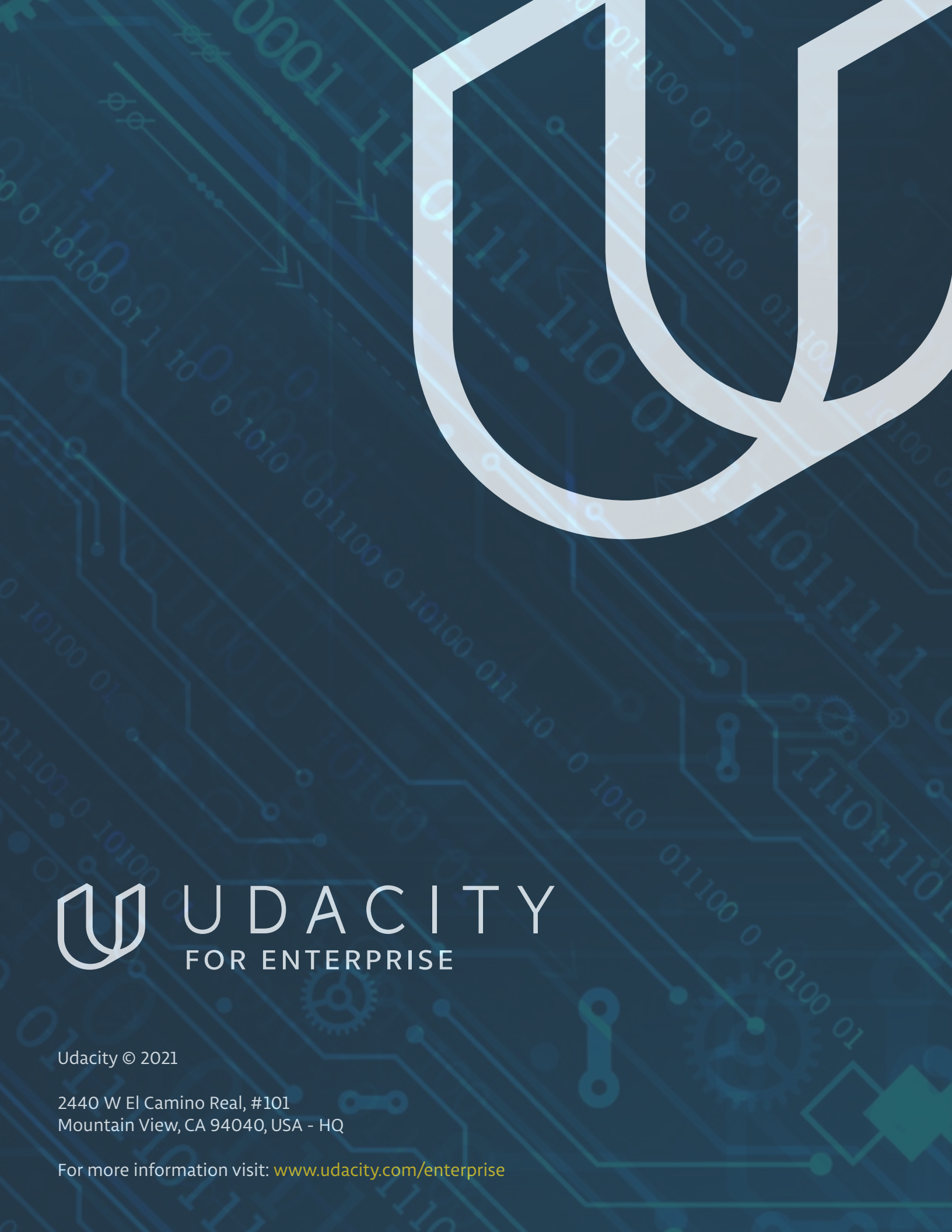
Our expert project reviewers are evaluated against the highest standards and graded based on learners' progress. **Here's how they measure up to ensure your success.**

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.



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

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