UDACITY
FOR ENTERPRISE

THE SCHOOL OF CYBERSECURITY

Enterprise Security

NANODEGREE SYLLABUS

Overview

Enterprise Security Nanodegree Program

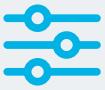
The goal of the Enterprise Security Nanodegree program is to equip learners with the foundational skills of security engineering within an enterprise setting. This program addresses security topics related to corporate environments, which are often distinct from production environments and center around the devices, identities, and infrastructure used by the company's personnel on a daily basis.

Graduates of this Nanodegree program will be able to:
Build a siem and implement enterprise network security best practices to monitor and control network traffic into an enterprise
Develop an asset and patch management to increase security posture of endpoints
Design a security baseline for application development as well conduct an internal application security assessment consisting of threat modeling, vulnerability scanning, and code review.
Establish data integrity checks as well data loss prevention mechanisms that control the types of data that can be transferred out of an enterprise

Program Information

TIME
4 months
Study 5-10 hours/week

LEVEL
Intermediate

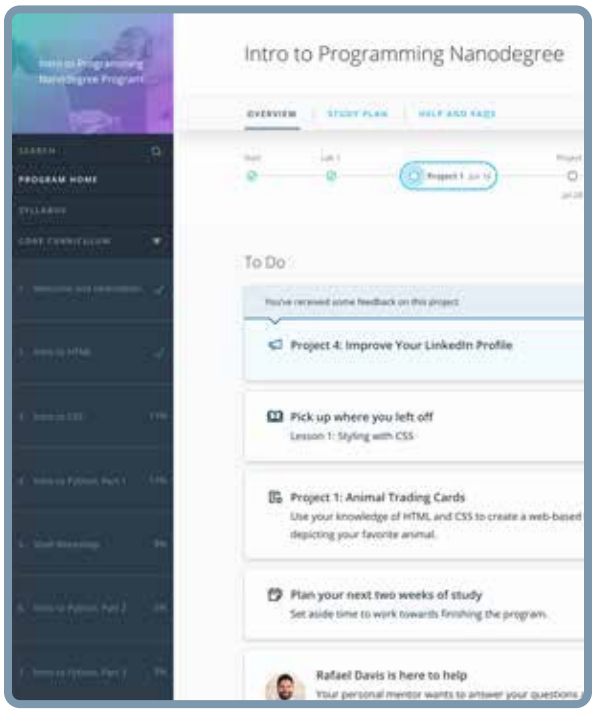


PREREQUISITES
Linux and Azure

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

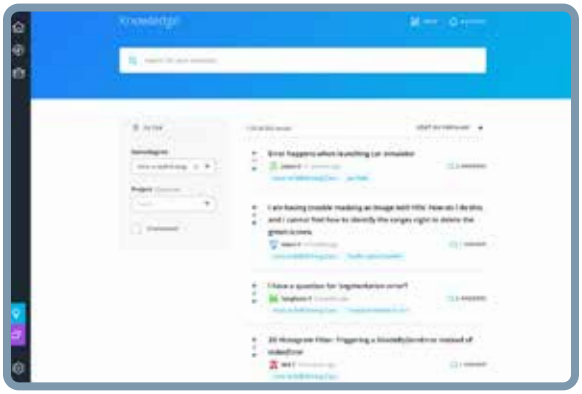
Learners leverage the power of community through a simple, yet powerful chat interface built within the classroom. Learner Hub connects learners with their technical mentor and fellow learners.

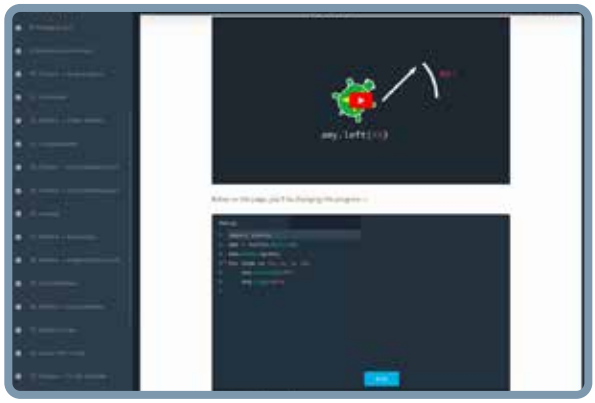
WORKSPACES

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

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 while educating students and professionals in cybersecurity.

Jerry Smith

INFORMATION SECURITY ENGINEER

Jerry is a member of the Security Operations Center for the University of Alabama at 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.

Vamsee Kandimalla

CYBERSECURITY ARCHITECT, HEAD OF PRODUCT TECHNOLOGY

Vamsee has wide-ranging security experience, including in sectors such as defense, consumer electronics, and automotive. He studied electrical engineering, then focused on cybersecurity during graduate school at Carnegie Mellon. He enjoys working on the latest technologies and high-impact solutions.

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.

Course 1: Enterprise Perimeter and Network Security

This course is designed to take you through the perspective of an enterprise and how they design a secure network architecture. The topics in this course will cover current enterprise perimeter and network security, network security architecture, building an enterprise network, continuous monitoring with a SIEM, and Zero Trust.

Project: Securing the Perimeter

Students will get hands-on experience in building a secure enterprise network. They will segment the network across different security topologies and employ the principle of least privilege to restrict access across the various segmentations. Students will then build a VPN to access the enterprise network from a remote location, then set up a SIEM and a web server. Students will monitor web server logs and build alerts to help identify security incidents. Students will then write incident response playbooks for certain attack scenarios. Lastly, students will design a Zero Trust model and write a comparative analysis between current network architecture and Zero Trust.

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
NETWORK SECURITY ARCHITECTURE	• Identify weaknesses in network topologies • Design the placement of security devices in an enterprise network • Use the SABSA framework to align enterprise business and security needs
BUILDING AN ENTERPRISE NETWORK	• Connect from public to private network over a NAT gateway • Partition a virtual network into multiple segments • Build a VPN solution to connect to an enterprise network
CONTINUOUS MONITORING WITH A SIEM	• Deploy a SIEM • Set up alerts and monitor traffic • Build an Incident Response Playbook
ZERO TRUST	• Define the principles of Zero Trust • Identify key components in Zero Trust architecture • Design a Zero Trust model

Course 2: Enterprise Endpoint Security

With data being a core driver of today's growth and the number of devices increasing, businesses have seen a rise in the number of types of endpoints. These factors make enterprise endpoint security more difficult since there are more potential vulnerable channels of cyberattack, and they have been compounded by remote work and the growing number of connected devices (i.e. mobile phones, tablets, etc). Moreover, 89% of security leaders believe that mobile devices will serve as your digital ID to access enterprise services and data. This course covers best practices for safeguarding the data and workflows associated with the individual devices that connect to your enterprise network.

Project: FedF1rst Security Assessment

You are a security engineer for Fed F1rst Control Systems. Fed F1rst has recently spun out of a larger organization into a stand-alone company. You have been tasked with implementing the endpoint portion of the organization's security policy.

The tasks that follow represent real tasks that would be performed on a scheduled and on an as-needed basis (for instance, server hardening is typically performed upon installation). You will recommend hardening strategies on a Windows 10 desktop as well as a Windows 2016 server. In the exercises you performed during the course, you performed these tasks on a CentOS Linux server. Those skills will come in handy here.

Next, you will create several security policies for the organization. As with hardening, you also performed this activity, but for different areas of the Information Technology department areas during the course.

Additionally, you will create build sheets for Windows and Linux cloud servers using the knowledge you have gained throughout the course.

Finally, you will conduct a subset of a server self-assessment that is common during pre-work for compliance audits.

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
SYSTEM HARDENING	• Identify Assets in an Organization • Recommend mitigation of discovered vulnerabilities • Recommend hardening strategy for commonly used operating systems • Recommend a security configuration for IoT and Control Systems
POLICIES AND COMPLIANCE	• Define BYOD Strategy • Create an NDA Policy • Conduct a compliance self-assessment • Create a remote work policy
CLOUD MANAGEMENT	• Recommend a public access configuration strategy • Recommend a configuration for cloud broker • Recommend a management solution for cloud deployments

Course 3: Enterprise Wide Application Security

Application security is a critical part of any enterprise security plan. Similar to the application security course in the Security Engineer Nanodegree, we will be covering how to perform a threat assessment but will get more granular by doing threat modeling and looking at how to harden applications. This course will teach students mitigation and defensive strategies in an application software development lifecycle. The focus will be on covering how enterprises bake security into their lifecycle by shifting security left and the different ways they enhance their security posture across on prem, cloud, containers, and APIs.

Project: CryptoV4ULT Enterprise Security Assessment

In this project, the students are the lead security engineers for a newly released application. The applications backend has recently stood up a new infrastructure to offer new features to its base of over 1 million users. Students will be tasked with reviewing the security for this new application technology stack and helping identify areas of concern with threat models. After pinpointing vulnerabilities, students will run scans against the enterprise application and attempt to exploit these potential issues.

Students' scope includes a variety of entities within the architecture, such as the application itself, the containers running services, and the external-facing API. Finally, students will create a remediation plan to help prevent these vulnerabilities and harden your existing security standards.

LESSON TITLE	LEARNING OUTCOMES
DESIGNING SECURITY ARCHITECTURE	• Identify all steps of enterprise DevSecOps • Plan all stages of the SDLC lifecycle • Design security architecture with specific constraints

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
THREAT HUNTING	• Conduct threat modeling to identify architecture vulnerabilities • Exploit vulnerabilities to prove they exist • Run industry-standard application vulnerability scanners with Nessus • Create pen-testing roadmap to secure solutions
CONTAINER VULNERABILITIES	• Scan containers to identify vulnerabilities • Research container vulnerabilities • Create plans to mitigate container vulnerabilities
API VULNERABILITIES	• Identify coding vulnerabilities in APIs • Research coding vulnerabilities in APIs • Mitigate coding vulnerabilities in APIs

Course 4: Enterprise Data Security

Cyber threats continue to evolve and grow, and each day we are reminded that all it takes is one lucky strike for a malicious hacker to breach a company.

On the other hand, cybersecurity professionals have to try and get it right every time to protect a company from breaches. This means that tackling cyber risk requires a very strategic approach and it starts with securing one of the greatest assets within the enterprise — data.

To begin mastering data security, during this course we'll start by exploring the concept of data governance so that students can build the foundation for understanding, classifying, and protecting data. Students learn to navigate the variety of compliance regulations that apply to data security and create policies that prevent unauthorized disclosure of information.

In the bulk of the course, students focus on protecting confidentiality, integrity, and availability of data through concepts like encryption, auditing, file integrity monitoring, and back-up strategy.

Project

Data Security Analysis in Online Payment Processing

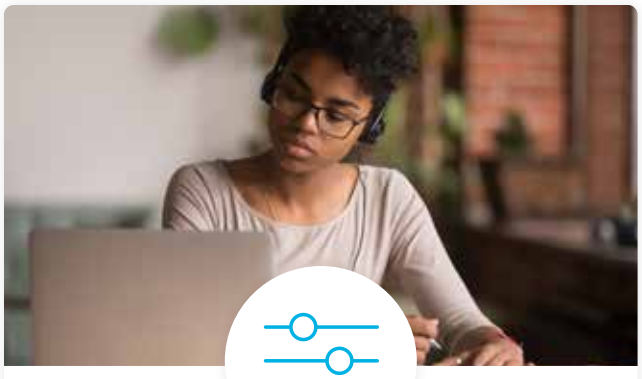
In this project, students will apply the skills they have acquired in this security course to ensure data security.

Students will be provided a realistic case study, company profile, and resource database. They'll work to classify data and justify which regulations apply to the data. They'll use post-breach evidence to perform a file integrity monitoring audit and determine if integrity was impacted. Students will also make recommendations for ensuring data integrity in the future, such as creating a data security policy, mapping out a data storage architecture and new encryption plan based on the data types, and establishing a backup and recovery policy and testing it to protect the company in the future. The deliverable will be an enterprise data security update delivered to the executive team detailing the security program established within the enterprise. The final implementation of the project will showcase students' data security management skills, including their ability to make and justify recommendations to key stakeholders and implement changes.

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
DATA GOVERNANCE	• Justify which compliance regulations apply to the data of your business or industry • Build data security policy to address compliance requirements • Determine typical compliance requirements with standard regulations • Distinguish appropriate regulations for each data type • Analyze enterprise data in order to classify data types based on risk. • Design information rights management policies to prevent intellectual property theft and stop unauthorized file sharing and editing • Analyze enterprise data in order to classify data types based on risk.
DATA CONFIDENTIALITY	• Apply the appropriate encryption system for enterprise data at rest and data in transit • Demonstrate encryption of data • Identify and distinguish methods for determining the right encryption solution for data at rest and data in transit • Analyze and distinguish encryption types, applications, and fundamentals (cert authority, PKI, key management)
DATA INTEGRITY	• Implement data protection and auditing controls that ensure data integrity across the organization • Map out a data storage architecture that supports data integrity and security • Conduct an audit to confirm compliance with key security controls • Distinguish major types of audit • Execute hashing in order to confirm data integrity • Apply the principles of identity and access management
DATA AVAILABILITY	• Establish a backup and recovery solution for critical systems across the organization • Create a disaster recovery plan • Run a back-up and restore test in the cloud • Build a backup and recovery strategy • Justify what data to back up • Distinguish backup and recovery best practice methods

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