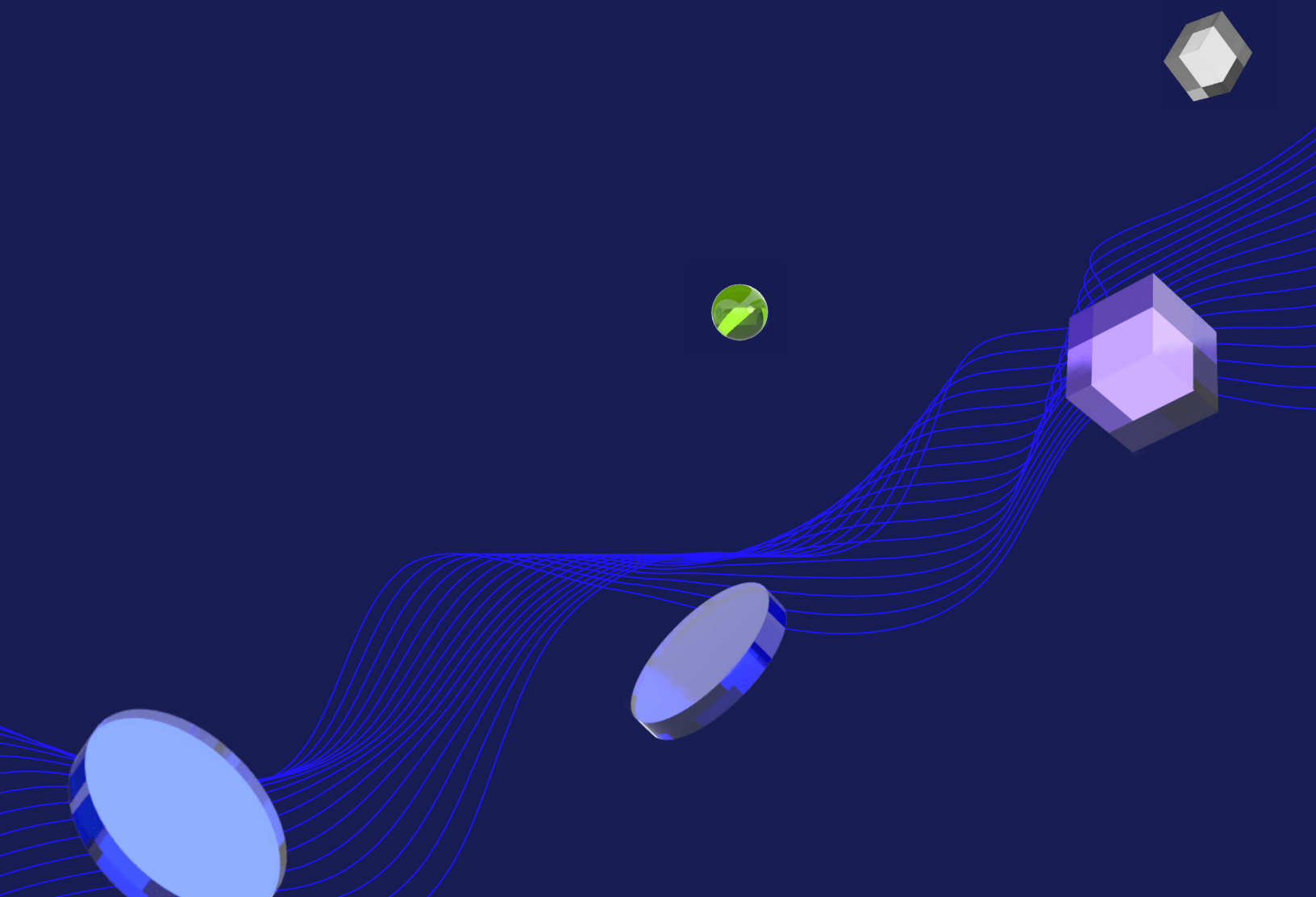
ENTERPRISE

UDACITY

SCHOOL OF CYBERSECURITY

Enterprise Security

Nanodegree Program Syllabus



Overview

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.

Learning Objectives

A graduate of this 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

Estimated Time

4 months at 10hrs/week*

Skill Level

Intermediate

Prerequisites

A well-prepared learner is familiar with relevant platforms (Linux and Azure) and has some experience conducting administration with those platforms such as:

- Setting up a Linux server and perform system configuration/management (Udacity free course: Linux Server Configuration).
- Setting up an Azure environment and perform cloud configuration/management.
- Exposure to networking, cloud, and hardware systems relevant to courses being taught (e.g. if a course teaches on Linux security, students should know the basics of how Linux works).
- Identify the most common networking protocols used (HTTP, TCP, DNS, SSH).
- Distinguish different hardware components in a network (desktop, server, firewall, etc.).
- Explain the relationship between client and server within an architecture.
- Identifying the different encryption protocols (AES, RSA, PGP).

Required Hardware/Software

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.

*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.

Course 1

Enterprise Perimeter and Network Security

This course is designed to take learners 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.

Course Project

Securing the Perimeter

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

Lesson 1

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.

Lesson 2

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.

Lesson 3

Continuous Monitoring with a SIEM

- Deploy a SIEM.
- Set up alerts and monitor traffic.
- Build an incident response playbook.

Lesson 4

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 a digital ID to access enterprise services and data. This course covers best practices of safeguarding the data and workflows associated with the individual devices that connect to an enterprise network.

Course Project

FedF1rst Security Assessment

Acting as a security engineer for Fed F1rst Control Systems, implement the endpoint portion of the organization's security policy. Recommend hardening strategies on a Windows 10 desktop as well as a Windows 2016 server. Next, create several security policies for the organization and create build sheets for Windows and Linux cloud servers. Finally, conduct a subset of a server self-assessment that is common during pre-work for compliance audits.

Lesson 1

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.

Lesson 2

Policies & Compliance

- Define BYOD Strategy.
- Create an NDA Policy.
- Conduct a compliance self-assessment.
- Create a remote work policy.

Lesson 3

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 program, 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.

Course Project

CryptoV4ULT Enterprise Security Assessment

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

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

Lesson 1

Designing Security Architecture

- Identify all steps of enterprise DevSecOps.
- Plan all stages of the SDLC lifecycle.
- Design security architecture with specific constraints.

Lesson 2

Threat Hunting

- Conduct threat modeling to identify architecture vulnerabilities.
- Identify vulnerabilities and their risk levels.
- Run industry-standard application vulnerability scanners with Nessus.
- Create pen-testing roadmap to secure solutions.

Lesson 3

Container Vulnerabilities

- Scan containers to identify vulnerabilities.
- Research container vulnerabilities.
- Create plans to mitigate container vulnerabilities.

Lesson 4

API Vulnerabilities

- Identify coding vulnerabilities in APIs.
- Mitigate coding vulnerabilities in APIs.
- Apply metrics monitoring.

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 learners 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, learners focus on protecting the confidentiality, integrity, and availability of data through concepts like encryption, auditing, file integrity monitoring, and backup strategy.

Course Project

Data Security Analysis in Online Payment Processing

In this project, apply the skills acquired in this security course to ensure data security. Learners will be provided a realistic case study, company profile, and resource database. Work to classify data and justify which regulations apply to the data. Use post-breach evidence to perform a file integrity monitoring audit and determine if integrity was impacted. 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 learners' data security management skills, including their ability to make and justify recommendations to key stakeholders and implement changes.

Lesson 1

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.

Lesson 2

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.

Lesson 3

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.

Lesson 4

Data Availability

- Establish a backup and recovery solution for critical systems across the organization.
- Create a disaster recovery plan.
- Run a backup 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.

Meet your instructors.

Milind Adari

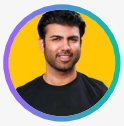
Security Engineer

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.

Jerry Smith

Information Security Engineer

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

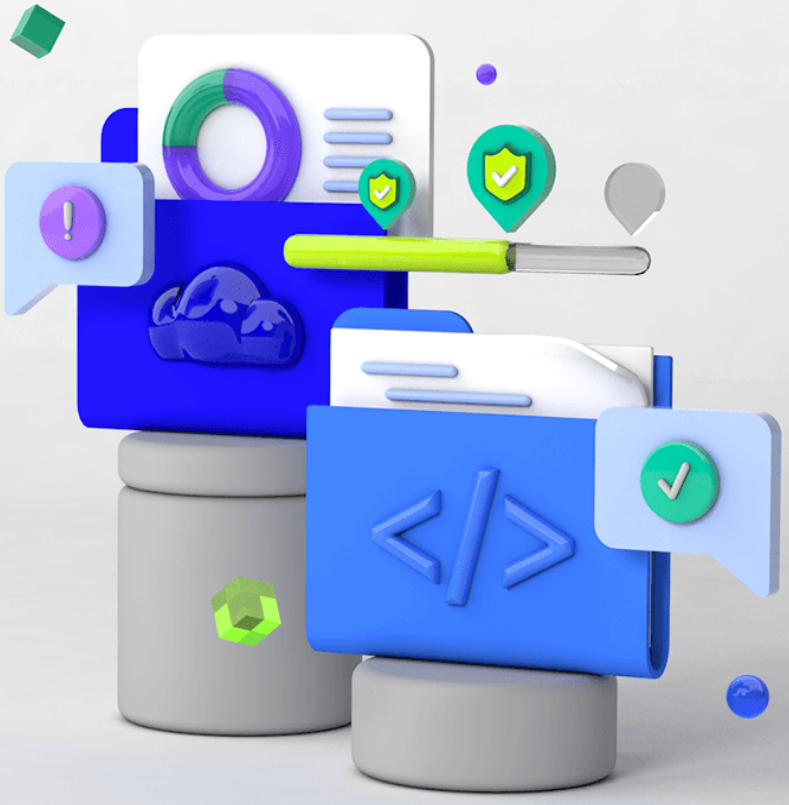
Vamsee has wide-ranging security experience in sectors such as defense and automotive. He studied electrical engineering, then focused on cybersecurity during graduate school at Carnegie Mellon. He enjoys working on latest technologies and high-impact solutions.

Christine Izuakor, PhD, CISSP

Founder & CEO at 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.

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.

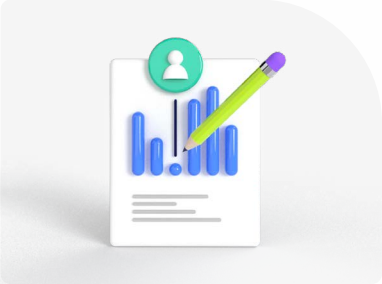
Workspaces

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.

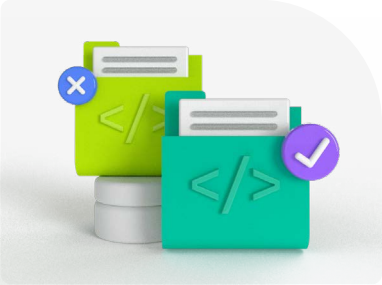
Our proven approach for building job-ready digital skills.



Pre-Assessments

Identify skills gaps.

- In-depth assessments benchmark your team's current level of knowledge in key areas.
- Results are used to generate custom learning paths.



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.

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.

Dashboard & Reporting

Track course progress.

- Udacity's enterprise management console simplifies management of bulk enrollments and employee onboarding.
- Interactive views help achieve targeted results to increase retention and productivity.
- Maximize ROI while optimizing job readiness.

UDACITY

Learn more at

udacity.com/enterprise →

01.06.23 | V1.0