



# The OffSec for Education Academic Catalog

Academic Year 2023 - 2024



## About OffSec



OffSec, the creators of Kali Linux, is the world's most trusted provider of cybersecurity training and certification. Our rigorous training programs are industry-standard and our certified alumni highly sought-after.



We help businesses, governments and educational institutions become more secure. We help individuals enter or advance their career in cybersecurity.



Built upon the belief that the only way to achieve sound defensive security is to take an offensive approach, we help people develop the necessary mindset with hands-on, real-world like labs, and equip them with the skills to succeed in tackling the challenges of cybersecurity in everyday life and work. Our mission is to empower the world to fight cyber threats.

# Table of Contents

Education Partner Impact	4
OffSec Solution to Workforce Readiness	5
OffSec's Unique Learning Methodology	6
Our Leadership's Commitment to Education	7
Education Partner Program Overview	8
Program Application Process	9
Education Partner Program Requirements	10
Instructor Certification & OffSec Instructor Bootcamp (OSIB)	11
OffSec for Education Platform	12
Learner Progress Reporting	13
Instructor, Admin & Student Support	14
Academic Pathways	15
Vertical & Horizontal Product Alignment	16
Instructor Subscriptions	17
Student Licenses - Penetration Testing Academia Stack	18
Security Operations Academia Stack	19
Web Application Security Academia Stack	20
Student Group Support	21
NICE Framework	22
NICE Framework	23
Case Study: University of Tulsa	24

# Education Partner Impact

Becoming an OffSec for Education Partner can quickly accelerate program, institution, and/or system-center maturity leading to increased visibility and funding to support increased economic impact and student success.



## Features

- Competency based approach
- Off-the-shelf delivery models sequenced to traditional academic semesters
- Mapped to National Initiative for Cyber Education (NICE) Framework
- Pathway to instructor/faculty certification
- Network of OffSec Authorized Instructors for mentorship and best practices



## Short Term Objectives

Cost effectively and efficiently build or augment and accelerate existing programs by providing:

- Industry relevant content and labs developed and curated through our ever-growing training library
- Measures of effectiveness and performance against student learning objectives through our OffSec Instructor Platform and integrated LMS
- Training toward a credible, performance based certification from a well-known and highly regarded training organization
- Access to a global network of professional security practitioners spanning the spectrum of experience from “hire to retire”



## Benefits

- Allows students to build a portfolio of experience during the course of their academic career through practical application of knowledge, skills, and abilities (KSAs) aligned to specific work roles
- Easy integration into new and existing programs
- Language ready to integrate into grant proposals and CAE applications
- Facilitate instructor/faculty professional development and capacity to infuse real-world application of job role specific KSAs into their courses



## Long Term Objective

- To develop and measurably improve student success outcomes leading to increased faculty and administrative program resources to support growth and scale



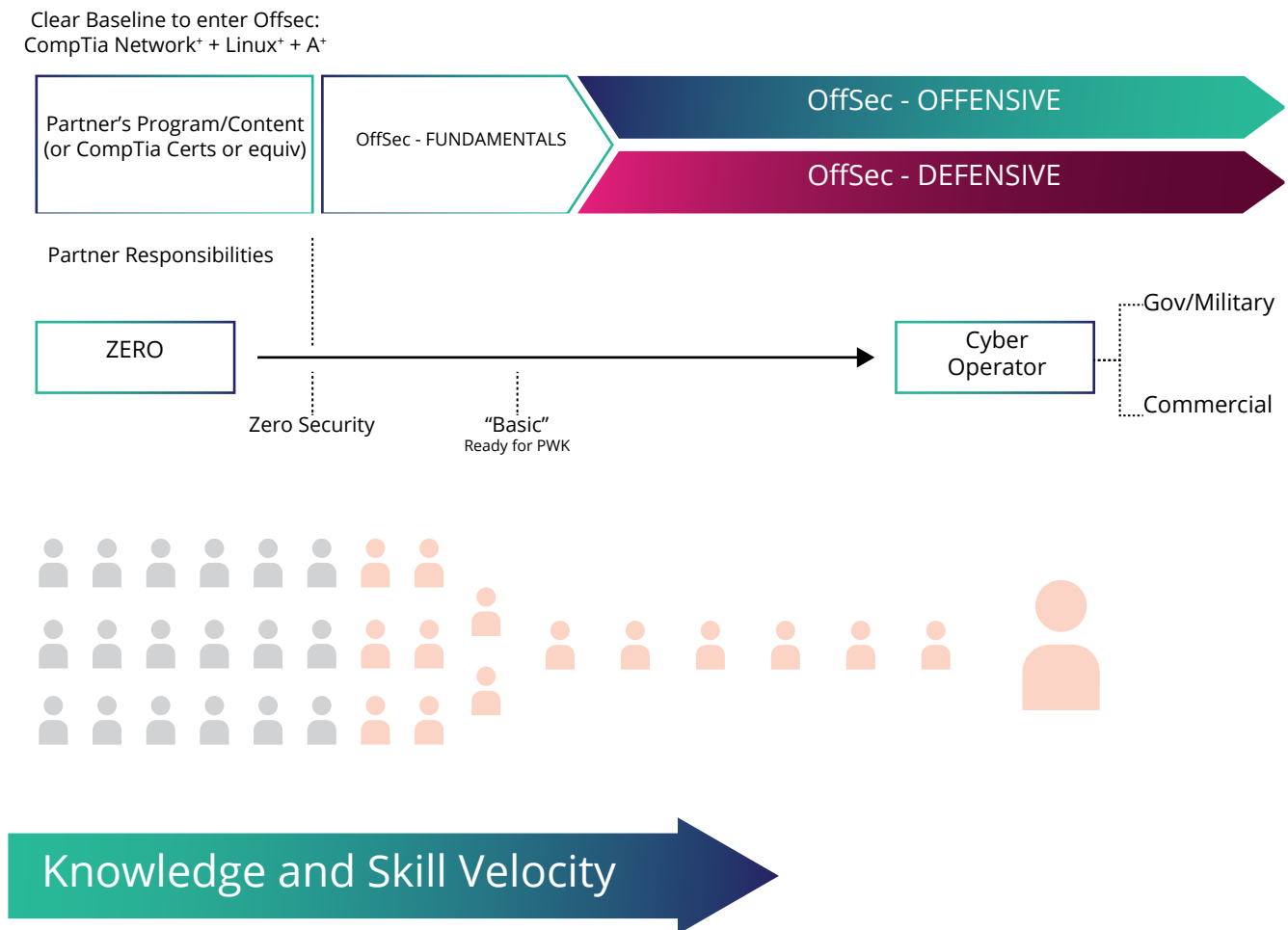
## Combined Overall Objectives

- To initiate, validate, sustain, and continuously improve public/private partnerships to address the global cyber security workforce shortage by building pathways for individuals and organizations aspiring to build a career or practice in cybersecurity.

# OffSec Solution to Workforce Readiness

OffSec believes in the integration of education and training across the spectrum of experience from “Hire to Retire”. Our program has been designed to integrate into the existing cybersecurity workforce development value chain, creating on-ramps and pathways to specific job roles in the cybersecurity industry.

## OffSec Solution to Workforce Readiness

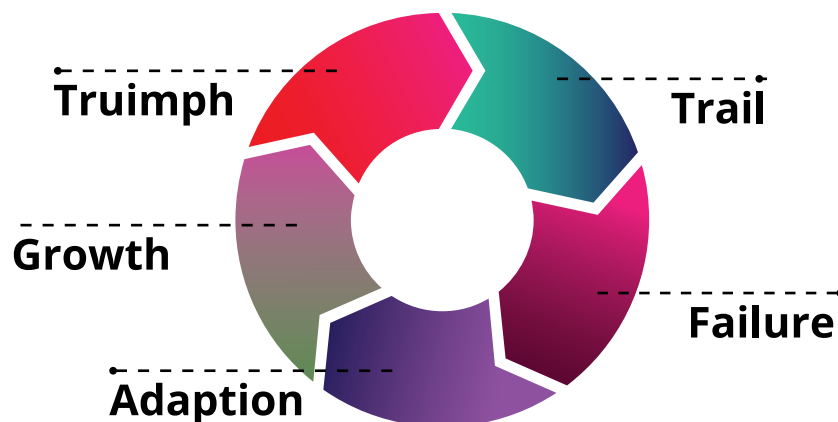


# OffSec's Unique Learning Methodology

OffSec is known for the Try Harder mindset. It is our belief that tenacity, grit, determination and perseverance will help solve problems. It's the realization that security requires trying things that will inevitably fail. We're training not only security skill sets, but also developing and training a security mindset...which is what differentiates us from our competitors.

Our approach is hands-on, skills-based, and competency driven.

When someone earns an OffSec certification or passes an assessment - it's a big indicator that this individual has gone through rigorous training and has proven that they have the knowledge, skills, and abilities to perform the job.



OffSec develops this mindset through an interactive process of trial, failure, adaptation, growth, and triumph.

This model of pedagogy describes how students continuously try, fail, adapt, grow, and ultimately win.

By providing students with opportunities to triumph repeatedly and reliably, we give them the tools to become better security practitioners.

An explicit emphasis in our development practices on this model makes us different and distinct from our competitors.

## Commitment to Education

OffSec is dedicated to educating, training and developing aspiring professionals and students with the knowledge and mindset needed to thrive in cybersecurity. Cyber Security risk is one of the leading concerns of Enterprise Businesses and Governments around the world, and according to Cyberseek, there are more than 714,000 job openings in the industry waiting to be filled by skilled professionals.

What better way is there to help build the pipeline of greatly needed Cyber security professionals than by partnering with accredited colleges and universities? Our Education Partners have a constant flow of new students eager and ready to learn, secure their first job and/or advance in their existing careers. Many Cyber security and IT Faculty members are familiar with OffSec, hold us in high regard and are certified in our trainings.

At OffSec, we have the most highly-sought after hands-on training in the industry. Employers actively seek job candidates with OffSec training and certifications. Where our competitors offer multiple choice exams, we ask our students to prove they have the mindset and skills needed to perform the tasks at hand by demonstrating their competencies through real-life labs and challenges.

We very much look forward to exploring a partnership together. We have a dedicated team that is here to support, guide and mentor you through the process of implementing OffSec content into your program curriculum. We hope this catalog provides a great overview of the service and offerings you can expect by partnering with OffSec.

**Let's work  
together to  
build the next  
generation of  
Cybersecurity  
Professionals!**



**Sean Donnelly**

Head of Global Partnerships

# OffSec Education Partner Program

OffSec partners with accredited colleges and universities to provide live, instructor-led classes to students based on our world-renowned curriculum and labs.

Education Partners are provided with instructor training and resources, including an instructor onboarding process, knowledge transfer of OffSec's best practices, and access to OffSec instructor materials. In addition, support is provided for student registration, reporting and curriculum development. Through OffSec's Partner Program and Partner Portal partners are provided with the benefits, support and resources they need to succeed.

## Education Partner Benefits are based on program level and can include:



### Instructor Authorization & Live-Training Support

- Special Instructor & Student Products
- Instructor Training & Authorization
- Instructor LMS Access
- Course Planning Support
- Student Registration Support
- Customized Instructor Slideware
- Detailed Syllabi for 8, 16 and 30 Week Course Delivery Methods
- Student Cohort Reporting



### Sales Enablement

- Co-brandable One-Pagers
- Course Catalog
- Pricebooks



### Communications & Support

- Monthly Partner Newsletter
- Partner and Instructor Discord Channels & Forums
- Dedicated Customer Success Representative
- Student Mentor Support
- Roadmap Reviews



### Business Planning

- Joint Strategy Alignment
- KPI Creation/Partner Portal Dashboards
- Best-Practice Knowledge Transfer

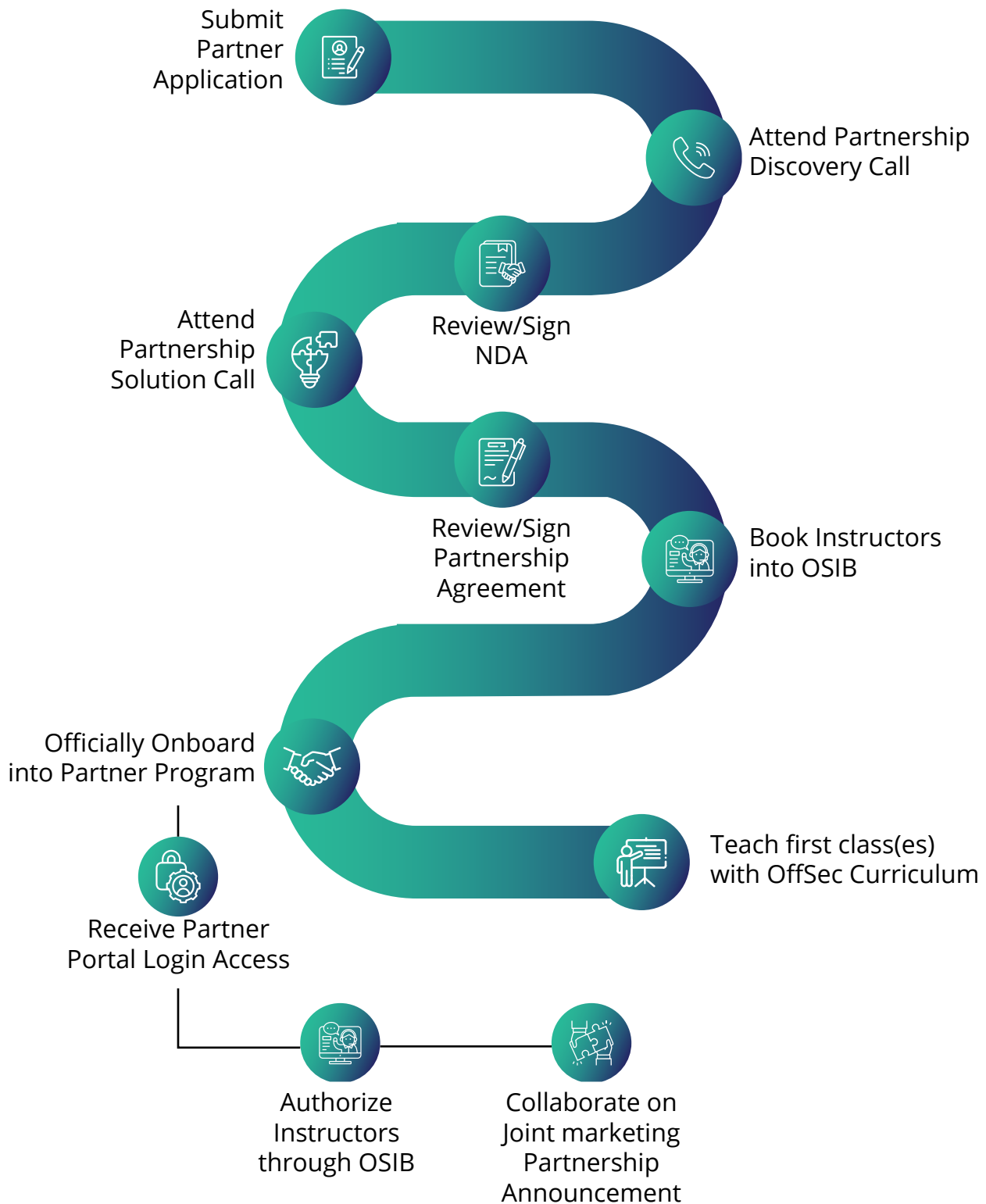


### Marketing Assets & Activities

- Access to OffSec Logos & Course Icons
- Partner Locator Inclusion
- Partnership Announcement Media Kits
- Campaigns in a Box
- Co-Marketing Activities: White Papers, Webinars & Podcasts



# Education Partner Program Application Process



# Education Partner Program Requirements

In an effort to maintain high student experience and protect the OffSec brand we do ask that our partners and partner instructors/faculty meet minimum requirements to maintain their authorization and get access to updated instructor resources and materials.



## Institutional Requirements

1. Accredited, Degree Granting Institution
2. Existing or aspiring NSA/DHS Center of Academic Excellence in Cyber Defense, Research or Operations (or international equivalent)
3. Commit to appointing a Program Champion and Lead Instructor that either already holds an OffSec Certification or is willing to earn
4. Commitment to having at least two authorized instructors on staff for each course being taught
5. Professor to Student Ratio of 1:15



## TA Requirements

1. Holds or is preparing for the certification of the course they will TA for
2. Could be a top performing student from a prior class
3. Personality traits: extrovert, personable and empathetic
4. Team player



## Instructor Requirements:

1. Technical Skills
  - Hold the associated badge aligned with 100 level content with 3 to 5 years of industry experience, in addition to any OffSec certification
  - Hold the certification associated with the 200 level content or above with 3 to 5 years of industry experience
2. Soft Skills
  - Good communication skills, extrovert personality, passion for helping others/teaching, and engineering mindset for problem solving
3. Maintaining Authorized Instructor Status
  - >30 Student survey NPS (instructor and course)
  - 50% percentile OffSec Student engagement (completing topic exercises and course labs)
  - 25 students taught annually per instructor (minimum)

# Instructor Certification & OffSec Instructor Bootcamp (OSIB)

## Pathway to Certification

We offer discounts and incentives to partners on a case by case basis, to facilitate instructor and faculty professional development in pursuit of program launch and scale.

## OffSec Instructor Bootcamp

Eligible Instructors of Education Partners can get authorized to teach live Offensive Security courses by attending the OffSec Instructor Bootcamp.

OffSec's Instructor Bootcamp is an instructional course that enables and empowers Instructors to teach OffSec content by utilizing curriculum resources required to deliver an interactive, engaging and hands-on class.

### Live Online

We offer the option to attend our OSIB, live online, quarterly. This provides instructors with the ability to interact in real time with our OffSec Academy Team and Instructors from other partner organizations.

### 2023 Live Online OSIB Schedule

February 6 - 9 from 10am - 1pm EST  
Deadline to Register: January 23

May 8 - 11 from 2pm - 5pm EST  
Deadline to Register: April 24

September 11 - 14 from 10am - 1pm EST  
Deadline to Register: August 28

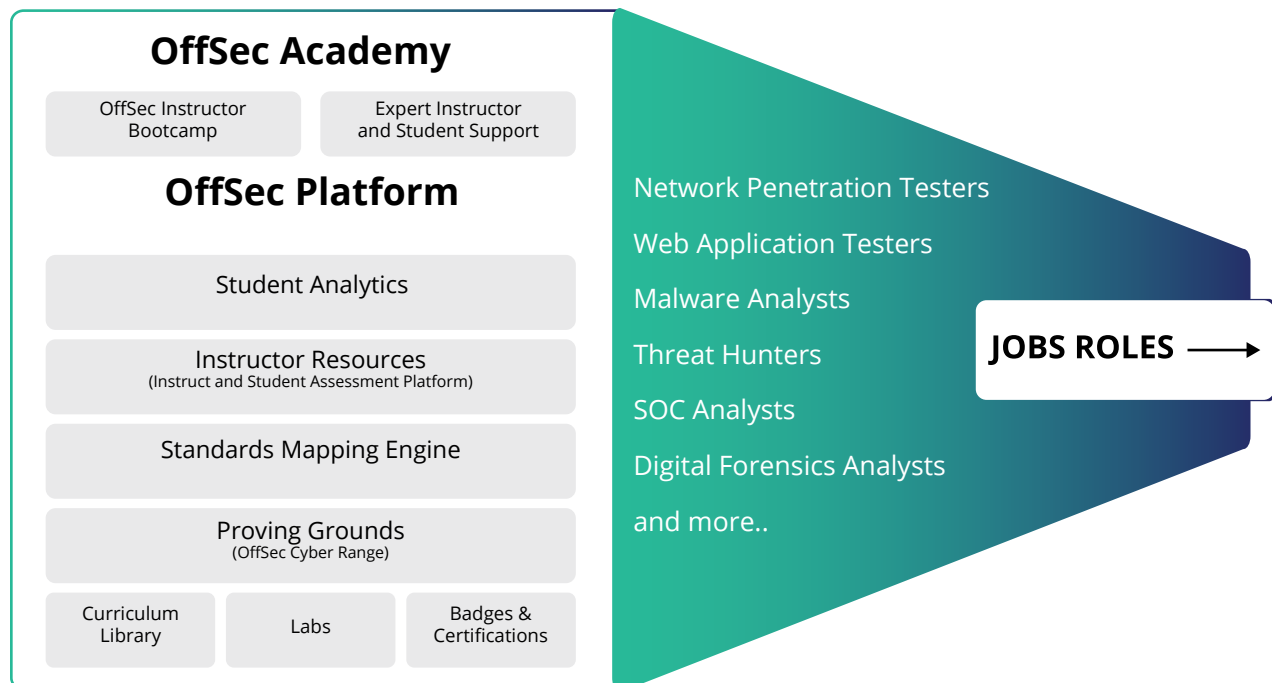
November 13 - 16 from 2pm - 5pm EST  
Deadline to Register: October 30

### Prefer an On-demand Option?

- Instructors can obtain the same training as our live course, during the dates and times that work best for their schedule by booking our self-paced OSIB.
- Instructors attending the OSIB on-demand, will schedule a live teaching demo once they have fully completed their online course, which totals about 5-6 hours of video content.

# OffSec for Education Platform

OffSec understands that establishing and growing impactful cybersecurity programs requires resources. In today's economic environment, measures of effectiveness and performance can mean the difference between a large grant award or a budget cut. Via the OffSec Platform (OSPL) we have developed a single pane of glass for instructors/Faculty to manage the end-to-end student experience and measure outcomes.



## Goals


- More predictable student outcomes
- Best-in-class content across Defensive and Offensive cybersecurity roles
- Professional labs researched and designed by Offsec experts
- End-to-end learning paths "zero-security" to Cybersecurity Professional
- Provide learning stepping stones so novices have a known path to more advanced courses. Better outcomes.
- Evidence-based assessments to improve student outcomes

# Learner Progress Reporting

Accredited colleges and universities will receive access to reporting for their students, instructors and employees. Specialized reporting is provided for each instructor/semester/cohort.

Reporting will be reviewed at a regular cadence through our Client Success team. Reporting will allow you to track progress on exercises, labs, books, video content, total engagement and exam status.

Similar reporting is available in our Platform to be accessed in real time.



Library


Courses ▾

Buy More

My Kali

VPN



Manage my team

Admin ▾

OffSec – Admin

LICENSESGROUPSREPORTS

Download CSV



COURSES4 active users on 11 courses

LEGEND

PEN-200

PEN-300

WEB-200

WEB-300

SOC-200

EXP-301

EXP-312

PEN-210

OSA - PEN - 200

PEN-200 (2023)

ALL

NAME	START DATE	END DATE	EXERCISE PROGRESS	LAB PROGRESS	BOOK PROGRESS	VIDEO PROGRESS	TOTAL PROGRESS	EXAM	DOWNLOADED MATERIALS
Jerry Schrute	Aug 10, 2021	Aug 10, 2024	0/126 exercises (0%)	0/75 labs (0%)	61/735 pages (8%)	9/425 videos (2%)	70/1361 total (5%)	Not scheduled	✗
Damian Simons	Feb 14, 2022	Feb 14, 2023	0/126 exercises (0%)	0/75 labs (0%)	17/735 pages (2%)	1/425 videos (0%)	18/1361 total (1%)	Expired	✗
Lisa McNeil	Feb 16, 2022	Feb 16, 2023	0/126 exercises (0%)	0/75 labs (0%)	1/735 pages (0%)	6/425 videos (1%)	7/1361 total (1%)	Expired	✗

FUNDAMENTALS4 active users on 7 courses

LEGEND

PEN-100

WEB-100

SOC-100

CLD-100

EXP-100

SSD-100

ALL

NAME	START DATE	END DATE	EXERCISE PROGRESS	BOOK PROGRESS	TOTAL PROGRESS	DOWNLOADED MATERIALS
Jerry Schrute	Aug 10, 2021	Aug 10, 2024	833/863 exercises (97%)	1303/1337 pages (97%)	2136/2200 total (97%)	✗
Damian Simons	Feb 14, 2022	Feb 14, 2023	11/863 exercises (1%)	43/1337 pages (3%)	54/2200 total (2%)	✗
Lisa McNeil	Feb 16, 2022	Feb 16, 2023	8/863 exercises (1%)	49/1337 pages (4%)	57/2200 total (3%)	✗
Daryl James	Apr 24, 2022	Apr 24, 2023	0/863 exercises (0%)	0/1337 pages (0%)	0/2200 total (0%)	✗

# Instructor, Admin & Student Support

OffSec believes that instructors should be spending as much time as possible teaching in the classroom... not troubleshooting connectivity issues, labs, or equipment. As such, we offer a suite of support services to ensure just that.



## Student mentors/helpdesk:

- Live chat support
- Helpdesk tickets
- Challenge tickets
- Exam grading
- Testing (PG machines and Topic Exercises)



## OffSec Academy:

- Deliver classroom and virtual training
- Create, update and maintain teaching material and lab exercises
- Adjust, customize, and deliver training
- Development of corporate-class training material















## Partner Support:

- Bug reports
- Reports of academic policy violations
- Reports of leaked materials and spoilers
- System messages indicating new registrations
- Student did not download course material
- Student updated file via website
- Course information & registration inquiries
- Account change requests
- Payment inquiries

# Academic Pathways

OffSec's off-the-shelf "Pathways in a Box" allows education partners to introduce concentrations and/or specializations into existing programs at the vocational, undergraduate, or graduate level. By integrating skills-based, practical training into the cybersecurity curriculum, education partners can ensure their graduates stand ready with "Doorstep Competencies" upon graduation and when reporting for their first assignment.

	Security Operations	Cloud Security	Network Penetration Testing	Web Application Security	Exploit Development
Terminal (PhD)			PEN-210 		
Graduate (Masters)	SOC-200 Part 2 		PEN-200 Part 2 	WEB-200 Part 2 	
Undergrad (4 Yr. Bachelors)	SOC-200 Part 1 		PEN-200 Part 1 	WEB-200 Part 1 	
Vocational (2 Yr. Associates)	SOC-100 	CLD-100 	PEN-100 	WEB-100 	EXP-100 
High School (9-12)			KLR/PEN-103 Proving Grounds Play & Practice	KLR/PEN-103 Proving Grounds Play & Practice	KLR/PEN-103 Proving Grounds Play & Practice
Elem. & Middle School (K-8)					

# Vertical & Horizontal Product Alignment

Via the OffSec Platform (OSPL), authorized instructors/faculty can leverage a suite of products comprising the OffSec Content Library to support:

- The establishment and growth of student cybersecurity clubs, preparing students to compete in Capture the Flag (CTF) competitions
- Faculty professional development
- Balancing out theory heavy courses and programs with practical, skill centric training aligned with specific job roles
- Immersive workforce development programs to increase the pipeline of students into traditional academic programs as well as create pathways for career changers, displaced workers, and veterans

## Vertical & Horizontal Product Alignment

		Student Groups & Clubs (OffSec Achieve)	Traditional Program Augmentation (OffSec Education Partner)			Continuing Education Immersives/Bootcamps (OffSec Learning Partner)			
Terminal (PhD)	OffSec Achieve Learn One	OffSec Achieve Proving Grounds Teams, Practice, Play							
Graduate (Masters)			EDU SOC-200-2	EDU PEN-200-2	EDU WEB-200-2	Defensive Cybersecurity BC	Penetration Testing BC	Web App Penetration Testing BC	
Undergrad (4 Yr. Bachelors)			EDU SOC-200-1	EDU PEN-200-1	EDU WEB-200-1				
Vocational (2 Yr. Associates)	OffSec Achieve Learn Fundamentals		EDU SOC-100	EDU PEN-100	EDU WEB-100	Intro to Defensive Cybersecurity BC	Intro to Penetration Testing BC	Web App Penetration Testing BC	
High School (9-12)									
Elem. & Middle School (K-8)									



## Instructor Subscriptions & Resources

Instructors are provided all of the resources they need to deliver an interactive, engaging and hands-on class, including access to OffSec's online labs. All courses have been created in a format that allows for live, online, or in-person training.



**Syllabus**



**Demo  
Instructions**



**Instructor  
Slides**



**Discussion  
Questions**

## Student Licenses

Our academia series provides students in traditional academic programs access to OffSec's renowned training in an instructor led format. By adopting OffSec's academia series, instructors are able to augment traditional, theory based curriculum with practical labs aligned with an industry recognized certification.

### Penetration Testing Academia Stack

PEN-100 is designed to prepare students with the necessary prerequisites to enter into Penetration Testing with Kali Linux (PWK), also known as PEN-200.








#### EDU\_PEN100

1. Introduction to PEN-100
2. Linux Basics - I
3. Linux Basics - II
4. Windows Basics - I
5. Windows Basics - II
6. Networking Fundamentals
7. Bash Scripting Basics
8. Python Scripting Basics
9. PowerShell Scripting Basics
10. Linux Networking and Services I
11. Linux Networking Tools II
12. Windows Networking and Services
13. Network Scripting
14. Working with Shells
15. Troubleshooting
16. Cryptography
17. Web Applications
18. Introduction to Active Directory

PEN-200 (PWK) is our foundational penetration testing course. Students learn the latest tools and techniques, and practice them in a virtual lab that includes recently retired OSCP exam machines. This course prepares students for the industry-leading OffSec Certified Professional (OSCP) certification.

### Resources

-  Student Text
-  Student Labs
-  Student Videos
-  Assessments & Challenge Labs
-  Proving Grounds Practice



#### EDU\_PEN200-1

1. Penetration Testing with Kali Linux: General Course Information
2. Getting Comfortable with Kali Linux
3. Command Line Fun
4. Practical Tools
5. Bash Scripting
6. Passive Information Gathering
7. Active Information Gathering
8. Vulnerability Scanning
9. Web Application Attacks
10. Introduction to Buffer Overflows
11. Windows Buffer Overflows
12. Linux Buffer Overflows
13. Locating Public Exploits
14. Fixing Exploits
15. File Transfers



#### EDU\_PEN200-1

1. Client-Side Attacks
2. Antivirus Evasion
3. Privilege Escalation
4. Password Attacks
5. Port Redirection and Tunneling
6. Active Directory Attacks
7. The Metasploit Framework
8. PowerShell Empire
9. Assembling the Pieces: Penetration Test Breakdown
10. Trying Harder: The Labs

# Security Operations Academia Stack






SOC-100 is designed to prepare students with the necessary prerequisites to enter into Security Operations and Defensive Analysis, also known as SOC-200.



## EDU\_SOC-100

1. Linux Basics I
2. Linux Basics II
3. Windows Basics I
4. Windows Basics II
5. Networking Fundamentals
6. Python Scripting Basics
7. PowerShell Scripting Basics
8. Linux Networking and Services I
9. Windows Networking and Services
10. Enterprise Network Architecture
11. Linux Networking and Services II
12. SOC Management Processes
13. Troubleshooting
14. Introduction to Active Directory
15. Data Manipulation in Python

## Resources

-  Student Text
-  Student Labs
-  Student Videos
-  Assessments & Challenge Labs
-  Proving Grounds Practice



## EDU\_SOC-200-1 & 2

SOC-200 is OffSec's new Security Operations and Defensive Analysis course on Security Operations. This course prepares students for the OffSec Defense Analyst (OSDA) certification.

1. Introduction to SOC-200
2. Attacker Methodology Introduction
3. Windows Endpoint Introduction
4. Windows Server Side Attacks
5. Windows Client-Side Attacks
6. Windows Privilege Escalation
7. Windows Persistence
8. Linux Endpoint Introduction
9. Linux Server Side Attacks
10. Linux Privilege Escalation
11. Network Detections
12. Antivirus Alerts and Evasion
13. Network Evasion and Tunneling
14. Active Directory Enumeration
15. Windows Lateral Movement
16. Active Directory Persistence
17. SIEM Part One: Intro to ELK
18. SIEM Part Two: Combining the Logs
19. Trying Harder: The Labs

# Web Application Security Academia Stack

WEB-100 is designed to prepare students with the necessary prerequisites to enter into Web Attacks with Kali Linux, also known as WEB-200.



## EDU\_WEB-100

1. Linux Basics II
2. Networking Fundamentals
3. Bash Scripting Basics
4. Python Scripting Basics
5. Troubleshooting
6. Web Applications
7. JavaScript Basics
8. Cryptography
9. Web Attacker Methodology
10. Introduction to Web Secure Coding
11. Web Session Management
12. Input Validation
13. Introduction to Encoding, Serialization, XML, JSON, and YAML
14. Introduction to Templating Engines
15. Getting Started with Git
16. Git Branching and Merging
17. Introduction to Git Security






Learn the foundations of web application assessments. WEB-200 is OffSec's new course, Web Attacks with Kali Linux. Students will discover and exploit common web vulnerabilities, learn how to exfiltrate sensitive data from target web applications and prepare for the OffSec Web Assessor (OSWA) certification.



## EDU\_WEB-200

1. Introduction to WEB-200
2. Tools
3. Cross-Site Scripting Introduction and Discovery
4. Cross-Site Scripting Exploitation and Case Study
5. Cross-Origin Attacks
6. Introduction to SQL
7. SQL Injection
8. Directory Traversal Attacks
9. XML External Entities
10. Server-side Template Injection Discovery and Exploitation
11. Command Injection
12. Server-side Request Forgery
13. Insecure Direct Object Referencing
14. Assembling the Pieces: Web Application Assessment Breakdown

## Resources

-  Student Text
-  Student Labs
-  Student Videos
-  Assessments & Challenge Labs
-  Proving Grounds Practice

## Student Group Support

### **Achieve**

For University Students

**Up to 10% Off**  
Learn One annual subscription

OffSec learners who are currently enrolled university students may be eligible for the Achieve discount program.

### **Aspire**

For certification holders\*

**Up to 20% Off**  
Learn One annual subscription

Save 10% with 1 OffSec certification  
Save 15% with 2 OffSec certifications  
Save 20% with 3 or more OffSec certifications

Find more information on the Achieve and Aspire Programs at:  
[offsec.com/discounts/#AspireAndAchieve](https://offsec.com/discounts/#AspireAndAchieve)

\*Aspire Discount automatically applied at checkout. Those with only an OSWP or KLCP certification are not eligible for the discount. Individual accounts only. Business, Channel Partners and Government Accounts have a separate discount program. Please inquire at [sales@offensive-security.com](mailto:sales@offensive-security.com) to see if you qualify.

## NICE Framework

OffSec has mapped its evolving content library to NIST Special Publication 800-181 revision 1, in order to enable alignment of workforce development activities across the spectrum of a student's journey from their initial academic career, to entry into the industry, through to retirement.

"NIST Special Publication 800-181 revision 1, the Workforce Framework for Cybersecurity (NICE Framework), provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills."

From NIST.gov

The Framework is categorized into 7 sections, of which OffSec courses provide a wide overlap. The primary NIST Specialty Areas, Specialty Area Descriptions, Work Roles and Work Role Descriptions applicable to OffSec are detailed with full mapping in Appendix A.



# NICE Framework

## Protect and Defense (PR)

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

### Role 01: Cyber Defense Analyst (PR-CDA-001)

- NICE Specialty Area Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.
- Work Role: Cyber Defense Analyst
- Work Role Description: Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

### Role 2: Incident Response (CIR)

- NICE Specialty Area Description: Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
- Work Role: Cyber Defense Incident Responder
- Work Role Description: Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

### Role 3: Vulnerability Assessment and Management (VAM)

- NICE Specialty Area Description: Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.
- Work Role: Vulnerability Assessment Analyst
- Work Role Description: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

## Analyze (AN)

Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

### Role 1: Exploitation Analysis (EXP)

- NICE Specialty Area Description: Analyzes collected information to identify vulnerabilities and potential for exploitation.
- Work Role: Exploitation Analyst
- Work Role Description: Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

## Collect and Operate (CO)

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

### Role 1: Cyber Operations (OPS)

- NICE Specialty Area Description: Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- Work Role: Cyber Operator
- Work Role Description: Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.

# Case Study: University of Tulsa

For more than two decades, the University of Tulsa has been at the forefront of cybersecurity research and education – as a Center of Academic Excellence in Cyber Defense Education, it's one of the first 14 institutions awarded this distinction. Tulsa alumni are employed in leading roles in the private and public sectors as well as academia.

To continue stimulating and supporting individuals with roles that strengthen national and global security, the University of Tulsa partnered with OffSec.

With this formal partnership, the University of Tulsa and OffSec are striving to educate and train the next generation of cybersecurity professionals and equip them with a practical set of skills needed to meet today's demand for skilled operators.

As part of the partnership, OffSec provides TU professors and instructors with an instructional course that enables them to teach OffSec content by utilizing the curriculum resources required to deliver an interactive, engaging, hands-on class.



## Undergraduate

Students of an Introduction to Penetration Testing class at Tulsa University can enroll in PEN-100 training by OffSec. This part of the program was designed to support individuals that have just completed their high school education and are looking to start learning toward a cybersecurity specialization. In the PEN-100 curriculum, students are able to learn the basics of Linux, scripting, networking, Active Directory, and more.



## Graduate

The renowned PEN-200 course was adapted and delivered in two parts. PEN-200 is a unique course that combines traditional course materials with hands-on simulations using a virtual lab environment. It's a foundational penetration testing course that teaches the skills and mindset required to be a successful penetration tester.

The first part was included in the TU graduate-level program as part of the Practical Penetration Testing course. Part two can be found in the Advanced Penetration Testing course.



## Non-Degreed training

Partnering with OffSec allows the University of Tulsa to leverage the OffSec Instruct Platform and OffSec Academy expertise to build and launch immersive bootcamp programs supporting workforce development. These bootcamps for PEN-100 and PEN-200 are designed to provide support and high-intensity, hands-on training for those transitioning to cybersecurity from other careers or those that need to advance their skill sets and get relevant industry-recognized training.



## Result

TU offers multiple programs for students who want to advance in cybersecurity education. Students from disciplines across the university can pursue a minor in cybersecurity at the undergraduate level. Graduate students can earn Master's degrees in cybersecurity. As the curriculum aligns with the OffSec Certified Professional (OSCP) designation, students can now get training toward a credible, performance-based certification from a highly regarded training organization while at university.

OffSec materials allowed TU students to improve their success outcomes in their career development and obtain job-ready skills that will allow them to grow.

"My students and I love the hands-on, practical, and real-world labs. OffSec gives me the support and resources I need to teach PEN-200 to my Graduate-level Advanced Penetration Testing class. Some of my students are employed as IT directors and they are applying the skills at work that they learned in class."

- Michael Oglesby, Adjunct Professor at the University of Tulsa

OffSec has a continuous commitment to improve public/private partnerships and to address the global cybersecurity workforce shortage by building pathways for individuals aspiring to build a career or practice in cybersecurity.