CYBERSECURITY

Professional Program

AMERICAN UNIVERSITY
WASHINGTON, DC

AMERICAN UNIVERSITY
WASHINGTON, DC

CYBERSECURITY

Professional Program

Table of Contents

About the Cybersecurity Professional Program

Imagine the following scenario. You arrive at work, ready to start your day. You open a browser and navigate to your company's website, only to find that a hacker group's logo has replaced the content your team has worked so hard to build. The damage to your company's reputation doesn't stop with the obvious fact that it was vulnerable to a security breach. The trust that your company has built with its clients is gone in an instant, as any sensitive information that was stored in the website's database is now in the hands of the malicious attackers and is most likely already on the dark web.

Information theft is continually on the rise and can cost businesses untold sums of hard-earned revenue, but another alarming target is our critical infrastructure. While many businesses are improving their ability to implement effective preventative measures, by the time they have caught up with the latest attacks, "in the shape-shifting world of cybersecurity, attackers have already moved on to indirect targets, such as vendors and other third parties in the supply chain," a recent report states. "It is a situation that creates new battlegrounds even before they have mastered the fight in their own backyard."[1] To add to the list of threats, cybercriminals also target the growing array of IoT devices, pacemakers, and automobiles, posing a threat not only to our finances and privacy but also to our health and safety.

Now more than ever, we must address the growing shortage of qualified cybersecurity professionals, not only to protect our sensitive data and personal safety but also to defend our livelihood and ensure the integrity of the systems we rely upon every day. The need for more qualified cybersecurity professionals is not only linked to the increase in the types of attacks but also the sheer volume. According to the Herjavec Group, "2020 was the worst year on record in terms of the data breaches that occurred[...] A staggering 36 billion records were exposed, many of which were vulnerable due to poor hygiene, and a rise in social engineering threats."[2]

The cutting-edge **Cybersecurity Professional Program** was developed in partnership with thought leaders in the industry to address these needs. This program prepares you to enter the workforce in under a year as a highly qualified, entry-level professional with the in-demand experience employers are looking for to help defend our most vital assets.

The 400-hour program offers a fully immersive experience with comprehensive virtual training labs that allow you to benefit from hands-on, digital simulation exercises in online classes taught by cybersecurity professionals. Thought leaders and industry experts work together to develop state-of-the-art course materials to ensure that you always receive the most current information. Instructors are insiders with a wealth of industry knowledge and expertise who guide you through everything you need to know, preparing you to sit for top industry certification exams* and enter an exciting, fast-paced field that is constantly evolving.

A unique Introductory Course allows you to gain a foundational understanding of cybersecurity so that you can determine whether or not it is the right career path for you before committing to the full program. This 30-hour course teaches the fundamentals of cybersecurity, and an assessment is provided at the end to determine your suitability for the field. At the culmination of the intro course, you will consult with your Admissions Advisor to determine whether or not you will continue to the full 400-hour program.

You will also have access to a full suite of career services to help you build resumes, create professional online profiles, and develop interview skills and techniques. Integrated throughout the program, this valuable guidance prepares you to enter the workforce empowered with the knowledge you need to enter a rapidly growing, in-demand field and build a successful career.

* The program includes an extra four dedicated sessions for test preparation. Certification exams are not conducted as part of the program and require additional costs not included in tuition. While the curriculum provides the knowledge needed to perform well on industry exams, the American University Cybersecurity Professional Program is not a test preparation program, where the primary focus is your performance on the exam. This program is designed to teach in-demand knowledge for today's workforce.

1. Accenture. 2020. Innovate for Cyber Resilience: Lessons from Leaders to Master Cybersecurity Execution.
2. Herjavec Group. 2021. Cybersecurity Conversations for the C-Suite: Securing the Post-COVID Paradigm Shift.

Preparing You for Cybersecurity Jobs

Designed for beginners with little to no technical background, as well as those with some prior knowledge, the American University Cybersecurity Professional Program provides you with the skills and experience that hiring departments look for in qualified cybersecurity personnel. If you are a gifted problem-solver, are good at puzzles, love figuring out how things work, or have a strong affinity for technology, cybersecurity could be the right field for you.

This program qualifies you for a variety of cybersecurity and IT roles,* including:

- Network Security Engineers
- Network and System Security Administrators
- Systems Security Managers
- Systems Security Engineers
- Cyber Network Defenders
- Vulnerability Assessment Analysts
- Cybersecurity Operations Specialists
- Network Security Technicians
- Cybersecurity Crime Investigators
- Cybersecurity Analysts
- Security Operations Center (SOC) Analysts
- IT Security Managers
- IT Support Engineers
- Network Operations Center (NOC) Technicians

* Job titles listed do not necessarily reflect entry-level positions.

Experts predict that the global cybersecurity market will be worth $300B by 2024.[3]

3. Columbus, Louis. 2020. "2020 Roundup of Cybersecurity Forecasts and Market Estimates." Forbes, April 5, 2020.

The accelerated programs powered by ThriveDX help reskill and upskill learners in today's fast-growing digital economy. With over a decade of experience as the world's premier digital skills and cybersecurity education provider, ThriveDX works with top-tier academic institutions, government organizations, and global enterprises to offer advanced workforce and professional development programs in digital technology.

What You Will Learn

The Cybersecurity Professional Program provides you with the knowledge and skills that will prepare you to enter the cybersecurity workforce.

The Foundations

- Principles of cybersecurity research
- Networking and network attacks
- Installing and operating Windows and Linux Operating Systems (OSs)
- Windows Client, Windows Server 2012, and Enterprise
- Domain name system (DNS)
- Shares and permissions
- Disk management
- iOS fundamentals
- File system and error handling

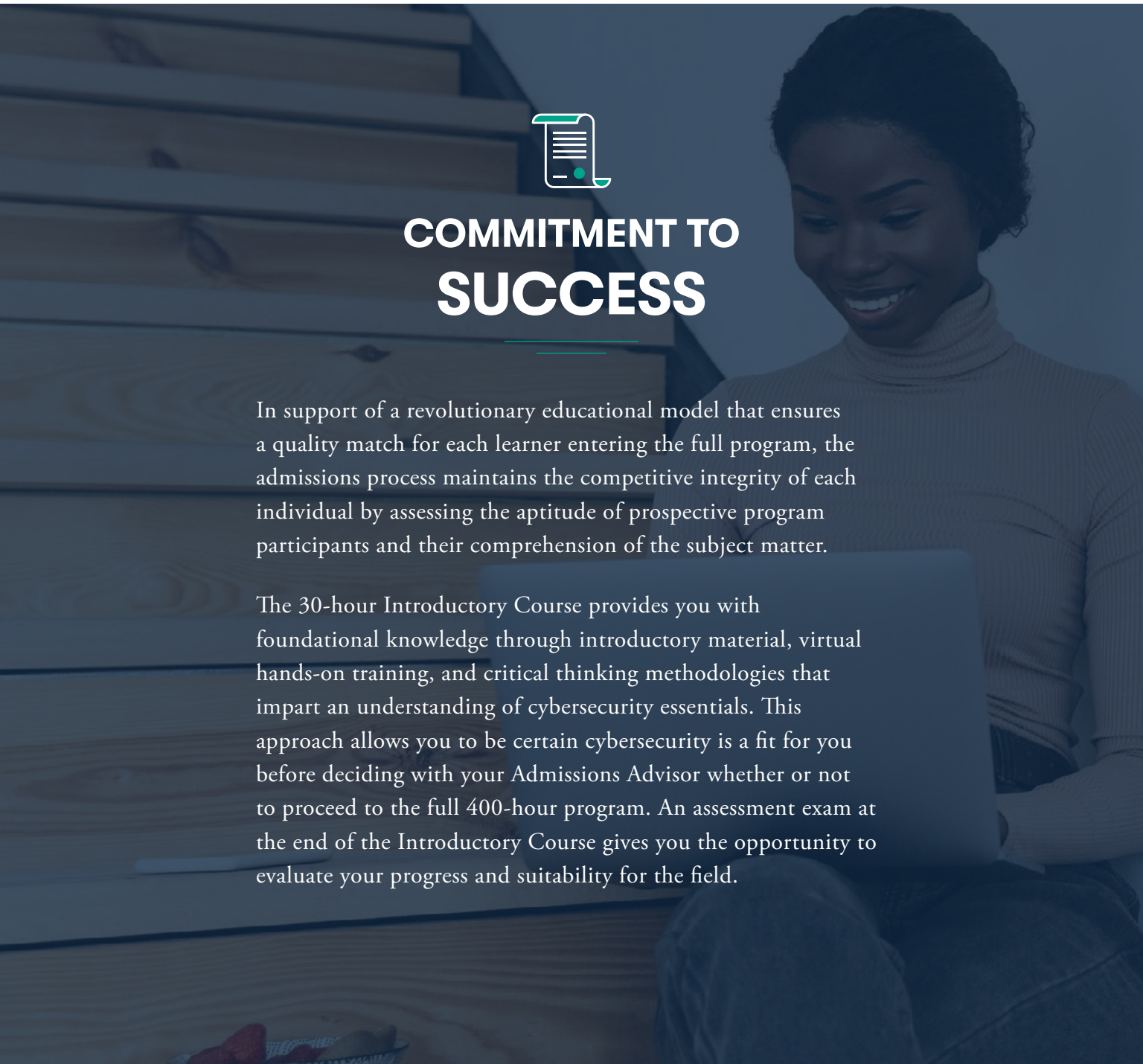
Mitigation, Tools & Security Measures

- Network security, traffic analysis, and communications
- Windows and Linux OSs and security
- The cyberattack cycle, countermeasures, and defense techniques
- Active Directory (AD), PowerShell, group policy
- Endpoint security and switch security
- IPv4 and IPv6 static routing procedures
- Dynamic routing procedures
- Security policies and authentication
- Dynamic Host Control Protocol (DHCP), Internet Protocol (IP), routing, and subnetting
- VLAN and Trunk
- Cloud security and advanced cloud computing
- Virtualization and containers
- Command-line interface (CLI), bash scripting, host security
- Practical cryptography
- Firewalls and VPN technologies
- Intrusion Protection Systems (IPSs) and Intrusion Detection Systems (IDSs)
- Honeypots and data loss prevention
- Mail security
- Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)
- Industrial Internet of Things (IIoT) and Industrial Control Systems (ICSs)
- Secure architecture implementation
- Programming and scripting with Python
- Creating Python automations for security and operations
- Data types and conditions, loops, and functions
- Ethical hacking concepts
- Network scanning, cross-site scripting (XSS), and file inclusion
- Mitigating On-Path attacks, Brute-Force attacks, social engineering, infrastructure attacks, structured query language (SQL) injection, and Windows and Linux privilege escalation
- Web application security
- Game theory to prevent and mitigate attacks

What You Will Learn

Data Analysis & Forensics

- Digital forensics, incident response, and data acquisition
- Windows live and dead analysis
- Network forensics
- Linux forensics
- Memory analysis, log analysis, and timeline
- Digital forensics and incident response (DFIR) simulation
- Threat hunting procedures
- Static and dynamic malware analysis
- Malware defense and persistence



COMMITMENT TO SUCCESS

In support of a revolutionary educational model that ensures a quality match for each learner entering the full program, the admissions process maintains the competitive integrity of each individual by assessing the aptitude of prospective program participants and their comprehension of the subject matter.

The 30-hour Introductory Course provides you with foundational knowledge through introductory material, virtual hands-on training, and critical thinking methodologies that impart an understanding of cybersecurity essentials. This approach allows you to be certain cybersecurity is a fit for you before deciding with your Admissions Advisor whether or not to proceed to the full 400-hour program. An assessment exam at the end of the Introductory Course gives you the opportunity to evaluate your progress and suitability for the field.

Program Structure

Structured around evening and weekend course schedules, this intensive 400-hour program is designed for working professionals.

The American University Cybersecurity Professional Program teaches you everything you need to defend digital information, implement security measures, respond to cyberattacks, and protect business and consumer data. The curriculum provides a comprehensive education in the fundamentals of cybersecurity through virtual lectures and participation in virtual cyber labs, real-world digital simulations, and individual and group exercises.

The program provides you with the foundational understanding and the practical, immersive experience that will help you gain entry into the field of cybersecurity. You will put foundational theories and methodologies into practice through projects and virtual hands-on training exercises that are designed to provide you with the skill set and foundational understanding you need to succeed in the field of cybersecurity.

30-Hour Introductory Course

To allow you to determine your suitability for the field before committing to the full program, the 30-hour Introductory Course provides you with an understanding of the fundamental principles of cybersecurity. This approach also ensures classroom success by facilitating the advancement of only those who have the passion and skills that are necessary to ultimately succeed in a cybersecurity career.

Cyber Labs

You will learn to identify vulnerabilities on web, server, mobile, and desktop platforms and create secure defenses that protect against a variety of threats through immersive cyber labs and real-world simulations. This virtual hands-on environment provides you with the knowledge, training, and experience that make you a highly qualified candidate who is prepared to enter the field of cybersecurity.

Global Certification

The Cybersecurity Professional Program at American University prepares you for the following IT and cybersecurity certifications:*

- CompTIA Network+
- CompTIA Security+
- AWS Certified Cloud Practitioner
- CompTIA CySA+
- LPI Linux Essentials
- (ISC)² SSCP**
- Cisco Certified CyberOps Associate

Career Outcomes

Because education alone may not be sufficient to help you get the job you are looking for, the Cybersecurity Professional Program provides you with the knowledge, skills, and hands-on experience through digital simulations and virtual hands-on labs that prepare you for a successful career in cybersecurity. Career Outcomes services include a full self-study curriculum to help you build your professional brand, LinkedIn profile, technical resume, job search strategy, interview skills, and more. You can connect with a career coach for additional support, and also attend exclusive live virtual events centered on career readiness, networking, and industry-focused panel discussions.

* The program includes an extra four dedicated sessions for test preparation. Certification exams are not conducted as part of the program and require additional costs not included in tuition. While the curriculum provides the knowledge needed to perform well on industry exams, the American University Cybersecurity Professional Program is not a test preparation program, where the primary focus is your performance on the exam. This program is designed to teach in-demand knowledge for today's workforce.

** You must have a minimum of one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK) in order to be certified.

Teaching Methodologies

The program is nimble and adaptable, much like the cybersecurity industry itself. Classes are conducted in live, synchronous, virtual classroom environments. This innovative teaching style provides you with the opportunity to learn in an environment that is aligned with the profession and allows you to balance your education with your other responsibilities. We have applied foundational elements from our advanced teaching methodologies that include:

Advanced Remote Education Technologies

You can take advantage of industry-leading remote technologies that increase the comprehension level of course material. The ability to instantly message instructors, virtually raise your hand during class, and collaborate with peers via remote workspaces ensures you have the tools you need to learn even the most intricate concepts.

Online Q&A Sessions with Instructors

You can request clarification on challenging concepts or ask for feedback from instructors through virtual, instructor-led question-and-answer sessions. This community environment promotes teamwork and collaboration that translate outside of the classroom.

Synchronous, Virtual, Live Classrooms

Expert instructors lead online classes, which are structured on real-time interactions and are held on a regular basis. Lessons stem from top-tier instructional methodologies and are enhanced with cloud-based chat software that allows live, virtual, hands-on interaction between you and your instructors.

A Library of Recorded Classroom Sessions

Curated by industry professionals, course materials are consistently updated to reflect new technologies, tools, and developments and are made available for you to review at your convenience. Recorded classroom sessions provide you with the opportunity to revisit any topics that were discussed during a lesson.

Live, Hands-on Practice Labs

Real-time, monthly lab exercises allow you to practice the skills you learn in the virtual classroom by yourself and alongside your instructor to ensure in-depth comprehension. Virtual lessons provide you with the opportunity to apply the skills from real-world scenarios to solve problems in a remote working environment.

Extended Virtual Office Hours

Instructors offer extended virtual office hours to provide you with additional support outside of lectures. You are encouraged to prepare your own questions regarding lessons as well as any concerns about your progress in the course.

Live Events & Workshops

Career Outcomes offers you exclusive access to a variety of live virtual events that include alumni panels, industry-focused discussions with subject matter experts, networking opportunities, career readiness talks, and pop-up company info sessions with potential employers. A workshop focused on helping you successfully prepare for technical job interviews is also available.

Taught by Experts in the Field

Classes are taught by instructors who are leaders in the industry and who bring a wealth of knowledge and expertise to the learning environment. You will benefit from instructors' current industry expertise as well as from their unique insiders' understanding of the fast-paced field of cybersecurity.

Five-Step
Cyber Education Process

The Five-Step Cyber Education Process combines unique teaching methodologies with a continually updated curriculum to ensure you receive the highest caliber of education. The process is the result of over a decade of proven research conducted by global cybersecurity experts. This revolutionary model ensures that you finish the program armed with the competitive skill set you need to enter today's job market as a competitive candidate.

01
Talk to Us

To assess your aptitude as a prospective learner and determine the most appropriate placement in our programs, schedule a consultation with a Cybersecurity Admissions Advisor.

02
One-on-One Meetings

Upon determination of placement, you will meet with an assigned advisor to further discuss the program, career expectations, and job opportunities. Meetings can be held over the phone or through videoconferencing.

03
Introductory Course

In the 30-hour Introductory Course, you will learn the fundamentals of cybersecurity and explore your expectations of working in cybersecurity versus the reality. This course provides an opportunity for you to determine your suitability for the field. At the end of the course, a summary exam and instructor evaluation are used to determine your future in the program.

04
The Program

A well-rounded instructional approach instills the fundamentals of theory and practical experience that provides immersive, experiential training through digital simulation. The program is led by cybersecurity experts and is the product of over a decade of research, teaching, and best practices.

05
Career Outcomes

Career Outcomes services are built into the program and provide you with interview training, advice on personal branding, job search strategy tips, professional networking opportunities, and more. Career coaches offer one-on-one feedback on your professional resume and LinkedIn profile. This integrated support increases your chances of success as you prepare to enter the field of cybersecurity.*

* Career Outcomes services are consultation-based only and do not guarantee job placement.

Program Flow

The Fundamentals Courses

You will already have a grasp of basic technological concepts from the Introductory Course, such as common operating systems, communication over a computer network, and the cloud environment. From the first day, instructors teach content from a security perspective that is explored in depth in each course. These essential courses provide you with a foundational understanding of cybersecurity.

Microsoft Security
This course provides an in-depth understanding of Microsoft systems and the security concepts that ensure system protection, from the management and operation of a Microsoft domain environment (including the Windows Server 2012 OS) to the differences between newer OS versions, such as Windows Server 2016 and 2019.

Computer Networking
This course provides an in-depth understanding of fundamental networking concepts essential for cybersecurity professionals, such as those surrounding protocols, topologies, and network devices. This course prepares you to take the CompTIA Network+ exam.*

Cloud Security
The concepts taught in this course, such as the growing use of cloud platforms and how environments are managed and secured in the cloud, provide an essential understanding that paves the way for the practices and labs in the advanced courses that follow. This course prepares you for the AWS Certified Cloud Practitioner certification.

Linux Security
This course provides an understanding of the security and hardening aspects of Linux environments with specific emphasis on the Kali Linux cybersecurity distribution. You will also learn how to manage and operate a Linux environment. The curriculum taught in this course prepares you for the LPI Linux Essentials certification exam.*

Cybersecurity Infrastructure Courses

After completing the courses above, you will be prepared to start searching for entry-level jobs that will allow you to gain experience in the field, and you will be ready to apply for at least one relevant certificate.

The courses in this category lay the groundwork for a deeper understanding of the security measures and technologies cybersecurity professionals use every day. These courses provide essential expertise that prepares you to enter the world of cybersecurity.

Network Security
In this course, you will learn to secure, manage, and operate network communication equipment and systems and to implement the network security tools and technologies that are key to protecting an organization. This course prepares you to take the Cisco Certified CyberOps Associate exam.* In this course, you will learn to secure, manage, and operate network communication equipment and systems and to implement the network security tools and technologies that are key to protecting an organization. This course prepares you to take the Cisco Certified CyberOps Associate exam.*

Cyber Infrastructure & Technology
This course provides you with the knowledge and practical training you need to design and maintain secure infrastructures and technologies. Security countermeasures such as SIEM, SOAR, endpoint security, and more provide an essential understanding of how to effectively protect organizations. This course begins to cover the CompTIA Security+ and CySA+ certificate objectives.

Introduction to Python for Security
This course provides you with an introduction to Python, the advanced programming language used by cybersecurity professionals to write scripts and automate security-related tools. The information you learn in this course also gives you a fundamental understanding of object-oriented programming.

Advanced Cybersecurity Courses

The courses until this point have established the practical knowledge, cybersecurity best practices, and the tools you need to prevent cyberattacks. To prepare you to address an attack that has already occurred, the advanced concepts in this category provide you with an understanding of different types of attacks, the attack kill chain, how to implement an attack, how to respond to an assault that is already underway, and how to mitigate it.

Offensive Security - Ethical Hacking
To train you to discover and exploit system vulnerabilities, penetrate organizational infrastructures, hack into web interfaces, and execute and defend against a variety of cyberattacks, this course provides you with knowledge, tools, and an understanding of a hacker's perspective. This skill set will help you to be a better defender as you prepare for a future career in ethical hacking and penetration testing.

DFIR & Threat Hunting
This course, as an introduction to digital forensics and incident response, provides a foundational understanding of the dynamics of working on a Security Operations Center (SOC) team and how to handle cyberattacks in real time. The material taught in this course prepares you for the CompTIA Security+, CompTIA CySA+, and (ISC)² SSCP** certification exams.*

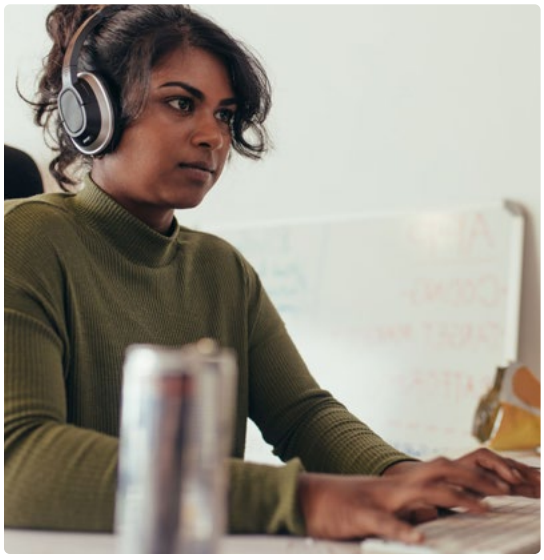
Game Theory Strategy in Cybersecurity
As you implement game theory fundamentals and apply them to cybersecurity defense, you will also begin to understand how a hacker thinks. This course teaches you a creative approach to problem-solving and a method of decision-making that helps you solve cybersecurity problems on your own.

---

* Certification exams are not conducted as part of the program and require additional costs not included in tuition. The program meets the objectives of the certificate throughout the program. Additionally, we are offering two non-mandatory extra sessions per certificate for Network+, Linux Essentials, CyberOps, and Security+ exam preparation.
** You must have a minimum of one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK) in order to be certified.

What's Included

- Experiential Learning
- Professional Networking
- 12 Specialized Courses
- 4 Dedicated Test Preparation Workshops
- Career Outcomes Events and Workshops
- 400 Program Hours
- Library of Recorded Classroom Sessions



Prerequisites

- While you should be technically inclined, no background in the field is needed.
- Professional evaluation

Industry Certifications

The American University Cybersecurity Professional Program sets you up for success by providing you with the fundamental knowledge you'll need to prepare for the industry's most recognized exams. The preparation and experience you receive in this intensive program help you stand out to employers while training you for an exciting career in cybersecurity defense.*

Preparation assistance for certification exams includes the following:†**

- CompTIA Network+
- AWS Certified Cloud Practitioner
- LPI Linux Essentials
- Cisco Certified CyberOps Associate
- CompTIA Security+
- CompTIA CySA+
- (ISC)² SSCP††

Learners who complete the Cybersecurity Professional Program are prepared for a career defending the world's most sensitive information, critical infrastructures, and digital assets for business and industry. The knowledge gained in this program also prepares you to take essential industry certifications. The extensive opportunities in cybersecurity extend to the private and governmental sectors. For those who wish to enter the Information Assurance (IA) workforce, the following baseline certifications from the list above have been approved by the Department of Defense‡ (DoD):

- CompTIA Network+
- CompTIA Security+
- CompTIA CySA+
- Cisco Certified CyberOps Associate
- (ISC)² SSCP††

The above certifications are considered by the DoD to be among the necessary qualifications for IA personnel. Opportunities for the DoD include various roles, such as Information Assurance Technicians (IATs), Identity and Access Management (IAM), Information Assurance System Architects and Engineers (IASAEs), and Cybersecurity Service Providers (CSSPs). Opportunities are available for Analysts, Infrastructure Support, Incident Responders, Auditors, and Managers.‡‡

---

* While the curriculum provides the knowledge needed to perform well on industry exams, this program is not a test preparation program, where the primary focus is your performance on the exam. The program is designed to teach in-demand knowledge for today's workforce.
**Certification exams are not conducted as part of the program and require additional costs not included in tuition.
† The test preparation workshops are not mandatory and are not part of the program curriculum. The workshops are designed to provide extra resources and help for learners who wish to take specific exams.
†† You must have a minimum of one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK) in order to be certified.
‡ The certifications are DoD-Approved 8570 Baseline Certifications: https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/.
‡‡ DoD guidelines listing certification requirements for various IA roles can be found at https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/. DoD guidelines are subject to change. It is the individual's sole responsibility to check DoD documents for changes.

The ThriveDX Difference

American University's Cybersecurity Professional Program was developed in partnership with ThriveDX (formerly known as HackerU). Originally founded in Israel, ThriveDX is one of the world's premier digital education providers with more than 15 years of global experience powering career-change programs that help adult learners join the digital economy. This program leverages industry leaders to develop and teach curriculum tailored to today's job market, including hands-on simulation labs that support individuals aspiring to build a career in technology. ThriveDX partners with many top-tier universities to offer accelerated professional development programs for learners from all backgrounds.

Program Breakdown
by Course

Course 1

Introductory Course

30 Hours

The primary objective of the Introductory Course is to introduce you to the cybersecurity industry and the multitude of opportunities that exist within the current landscape. In addition, the course provides you with an overview of some of the core concepts in cybersecurity and previews how those concepts will be covered within the extended program. When the course ends, you will complete an assessment exam and consult with an admissions advisor who can help you make an informed decision on whether you are a good fit to continue on to the extended program and if pursuing a career in cybersecurity is the best choice for your future.

The course begins with the fundamentals of information security and risk management, ensuring that you understand the business context of cybersecurity. You are then introduced to networking and network security fundamentals, the Linux and Microsoft platforms and related security, and unique considerations for software security. The concept and role of offensive security are introduced, and the course concludes with an explanation of how to contextualize threats and threat actors within the previous topics.

The course includes the following modules:

1. **Introduction to Cybersecurity**
2. **Information Security and Risk Management**
3. **Network Security**
4. **System Security: Linux**
5. **System Security: Microsoft**
6. **Application Security**
7. **Offensive Security**
8. **Threats and Threat Actors**

Course 2

Microsoft Security

40 Hours

Companies around the world manage their computers and networks with Group Policy Objects on Windows Server 2012. This course teaches you how to set up domain environments with Active Directory to enable central control of all computers and users in a domain. You will also learn the differences between Windows Server 2012 and newer versions, how to manage network services such as DNS and DHCP servers, and how to configure security servers to harden systems.

The following topics are covered in the course:

1. **Introduction to Windows Client**
2. **Windows Server 2012 and Enterprise Creation**
3. **Domain Name System**
4. **Active Directory**
5. **PowerShell**
6. **Group Policy**
7. **Shares and Permissions**
8. **DHCP**
9. **Disk Management**
10. **Microsoft Endpoint Security**
11. **Security Policies and Authentication**

Course 3

Computer Networking

50 Hours

Networking is a major part of nearly every industry, including government, finance, transportation, technology, healthcare, manufacturing, hospitality, and more, as almost every business sector worldwide operates with networked devices. In this course, you will learn the various protocols, network layers, and devices that are essential to understanding a computer network.

Because it is vital for cybersecurity professionals to have an in-depth understanding of networking, in this course, you will learn the networking concepts surrounding protocols, topologies, and network devices. This course also prepares you to take the CompTIA Network+ exam.*

The following topics are covered in the course:

1. **Introduction to Networks**
2. **Network Fundamentals**
3. **IOS Fundamentals**
4. **Switch Security**
5. **IP and Routing Concepts**
6. **Subnetting**
7. **IPv4 and IPv6 Static Routing**
8. **Dynamic Routing**
9. **VLAN and Trunk**
10. **Diagnostics and Troubleshooting**
11. **Access-Control List**
12. **Infrastructure Services**

Course 4

Cloud Security

15 Hours

Cloud platforms provide centralized managed solutions that house organizational infrastructures. More and more companies are migrating their servers and databases to platforms such as Amazon's AWS, Google Cloud, and Microsoft Azure. Services range from basic physical servers to completely managed solutions. An essential understanding of cloud platforms includes knowing how to leverage, work with, and secure them.

In this course, you will learn how environments are managed and secured in the cloud and understand the rationale and scope of the growing use of cloud platforms. This course also provides you with the knowledge base and skill set that will prepare you for the AWS Certified Cloud Practitioner exam.*

The following topics are covered in the course:

1. **Cloud Fundamentals**
2. **Virtualization and Containers**
3. **Securing the Cloud**
4. **Advanced Cloud Computing**

Course 5

Linux Security

30 Hours

Linux's growing increase in popularity can be attributed to its use in IoT products, as well as the benefits it offers information security personnel. With specific emphasis on the Kali Linux cybersecurity distribution, this course focuses on the management and operation of the Linux open-source operating system. You will learn to navigate the Linux file system, run basic commands, configure network services, handle access permissions, and exploit mitigations. This course provides you with an understanding of the security aspects and hardening of Linux environments and prepares you for the LPI Linux Essentials certification exam.*

The following topics are covered in the course:

1. **Introduction to Linux**
2. **CLI Fundamentals**
3. **Users and Permissions**
4. **Networking and System Management**
5. **Services and Hardening**
6. **Bash Scripting**
7. **Host Security**
8. **Network Security**

Course 6

Network Security

35 Hours

This course provides you with the knowledge you need to specialize in technological fields and business operations and stand out to potential employers with an understanding of how to secure, manage, and operate network communication equipment and systems for different organizations. This course helps to prepare you for the Cisco Certified CyberOps Associate exam.*

The following topics are covered in the course:

1. **Network Security Systems and Architecture**
2. **Secure Management and Access**
3. **Network Attacks and Mitigation**
4. **Network Traffic Analysis**
5. **Practical Cryptography**
6. **Firewall Fundamentals**
7. **VPN Technologies**
8. **Network Monitoring**
9. **IPS and IDS Concepts**

*Certification exams are not conducted as part of the program and require additional costs not included in tuition.

Course 7

Cyber Infrastructure & Technology

40 Hours

This course teaches you to design and maintain secure infrastructures, implement various security countermeasures, and build the knowledge base required to take the CompTIA Security+ certification exam.* Through an in-depth examination of various defensive infrastructures, you will learn how to design a secure architecture and understand the security measures that can be used to harden networks, devices, and cloud infrastructures. You will also learn how to work with Security Information and Event Management (SIEM) solutions through an emphasis on Splunk, a widely used open-source solution.

The following topics are covered in the course:

1. **Endpoint Security Measures**
2. **Honeypots**
3. **Data Loss Prevention**
4. **Mail Security**
5. **SIEM Introduction**
6. **Advanced SIEM**
7. **SIEM and SOAR**
8. **IIoT and ICS**
9. **Physical Security**
10. **Secure Architecture**

Course 8

Introduction to Python for Security

25 Hours

This course teaches you the essential concepts of Python, the industry's leading programming language. Immersive training exercises provide you with firsthand experience as you learn to work with tools to automate cybersecurity tasks. In a virtual hands-on integration, you will set up a Python environment in Windows and Linux and discover how to use external libraries.

In this course, you will receive guidance on how to find a position as a cybersecurity practitioner, how to work with IT and Network Operations Center (NOC) teams across a variety of organizations, and how to become the cybersecurity specialist for those teams.

The following topics are covered in the course:

1. **Introduction to Programming**
2. **Data Types and Conditions**
3. **Loops**
4. **File System and Error Handling**
5. **Functions**
6. **Network Communication**
7. **Python for Security**

Course 9

Offensive Security: Ethical Hacking

50 Hours

In this course, you will learn how to execute and defend against various attacks, such as network, application, cryptographic, and social engineering attacks. Hands-on digital labs provide you with the knowledge and tools you need to discover and exploit system vulnerabilities. You will also gain an understanding of how unethical hackers think so that you can anticipate their intentions and stay ahead of impending threats. The material presented in this course further prepares you for the CompTIA Security+, CompTIA CySA+, and (ISC)^2 SSCP** certification exams.*

The following topics are covered in the course:

1. **Introduction to Ethical Hacking**
2. **Network Scanning**
3. **On-Path Attacks**
4. **Brute-Force**
5. **Social Engineering**
6. **Infrastructure Attacks**
7. **Windows Privilege Escalation**
8. **Linux Privilege Escalation**
9. **Web Application Security Fundamentals**
10. **XSS and File Inclusion**
11. **SQL Injection**
12. **Vulnerability Scanners and Reporting**

* Certification exams are not conducted as part of the program and require additional costs not included in tuition.
** Learners must have a minimum of one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK) in order to be certified.

Course 10

DFIR & Threat Hunting

60 Hours

Through an understanding of digital forensics and incident response (DFIR), this course instills advanced threat hunting techniques such as situational awareness, machine learning, intelligence, and user behavior analytics. You will learn how to identify elusive threats that evade existing security countermeasures, how to implement successful threat hunting procedures, and how to handle cyberattacks as they occur. With an understanding of digital forensics techniques, you will investigate network attacks and host attacks and learn how to reverse engineer malware to understand its purpose and execution on vulnerable systems.

The curriculum seeks to familiarize you with the dynamics of working on a Security Operations Center (SOC) team and the role of SOC teams across a variety of organizations. This course also prepares you for the CompTIA Security+, CompTIA CySA+, and (ISC)^2 SSCP** certification exams.*

1. **Introduction to DFIR**
2. **Incident Response Preparation**
3. **Incident Response Implementation**
4. **Data Acquisition**
5. **Windows Live Analysis**
6. **Windows Dead Analysis**
7. **Memory Analysis**
8. **Linux Forensics**
9. **Log Analysis and Timeline**
10. **DFIR Simulation**
11. **Threat Hunting**
12. **Static Malware Analysis**
13. **Dynamic Malware Analysis**
14. **Network Forensics**
15. **Network Defense and Persistence**

Course 11

Game Theory Strategy in Cybersecurity

10 Hours

Our only defense against hackers, who always seem to be a step ahead, is to anticipate impending threats by becoming experts at divergent thinking and understand the unethical hacker mindset. This course introduces you to game theory—a tool that is essential to a solid comprehension of the thinking and rationale of attackers, how players interact, and how to creatively secure networks. To broaden your perspective on a variety of strategic topics, you will use game theory to model real-world scenarios and apply these methods to create solutions that will defend an organization.

The following topics are covered in the course:

1. **Introduction to Game Theory**
2. **Game Theory Application in Cybersecurity**

Course 12

Career Outcomes

15 Hours

The career planning, training, and tools you need to enter the field of cybersecurity—along with personalized interview coaching, professional networking, and one-on-one consultations devoted to perfecting LinkedIn profiles and resumes—help you to put your best foot forward as you prepare to seek entry into the field of cybersecurity. Career Outcomes covers the following subjects:

1. **Resume and LinkedIn Profile Building**
2. **Interview Skill Building**
3. **Job Search Strategies and the Power of Networking**

* Certification exams are not conducted as part of the program and require additional costs not included in tuition.
** You must have a minimum of one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK) in order to be certified.

Program Summary

Courses	In-Class Hours
Introductory Course	30
Microsoft Security	40
Computer Networking	50
Cloud Security	15
Linux Security	30
Network Security	35
Cyber Infrastructure & Technology	40
Introduction to Python for Security	25
Offensive Security: Ethical Hacking	50
DFIR & Threat Hunting	60
Game Theory Strategy in Cybersecurity	10
Career Outcomes	15
Total	**400**

AMERICAN UNIVERSITY
WASHINGTON, DC

(202) 888-4202

4400 Massachusetts Ave. NW
Washington, D.C. 20016

digitalskills.american.edu