LSU Online | In Collaboration With Fullstack Academy

#1 University in Louisiana*

Cybersecurity Bootcamp

Overview & Syllabus

CompTIA Authorized Partner | DELIVERY PARTNER | CompTIA Security+ CERTIFICATION Plus Series

CourseReport BEST CYBER SECURITY BOOTCAMP 2025

*The Wall Street Journal

TABLE OF CONTENTS

About the Cybersecurity Bootcamp

As cybercrime increases and evolves on a global scale, cybersecurity industry employers are seeking qualified individuals to fill exciting, impactful tech roles. With over **600,000 job openings nationwide**, demand for cybersecurity experts is surging–according to CyberSeek. Technology insights company Gartner also predicts that by 2027, **17% of cyberattacks will leverage generative AI**, adding new layers of complexity to security challenges.

As a result, the cybersecurity workforce in the U.S. is projected to grow **33% through 2030**—more than **three times faster than the average job market**—driven by the rapid expansion of digital technologies and stronger data privacy regulations. Now is the perfect time to build **AI-enhanced cybersecurity skills** and position yourself for a rewarding and future-proof career.

The **Louisiana State University Online Cybersecurity Bootcamp**, in collaboration with Fullstack Academy, equips learners with the skills to meet this demand. Through live online classes, hands-on labs, projects, and assessments, you'll build knowledge in **GenAI for Cybersecurity, Red Team, Blue Team, Operating Systems, Network Security, Scripting, Governance, Risk & Compliance, Cloud Security, Cyber Threat Intelligence**, and much more—while developing a portfolio of industry-relevant projects that showcase your abilities.

Upon completing this bootcamp, you will earn a **certificate of completion** from Louisiana State University Online and Fullstack Academy, validating your ability to implement AI-driven security solutions and respond to modern cyber threats.

To help you translate skills into career success, the program includes **personalized 1:1 career coaching during the bootcamp and for up to a year following graduation**. From resume and LinkedIn profile optimization, mock interviews, and access to curated job boards, you'll have the resources needed to **stand out in the job market and launch a successful career in cybersecurity**.

Key Features

- Go from **cybersecurity beginner to job-ready in just 13-21 weeks** with no prior tech experience required.
- Discover the cutting-edge applications of **generative AI in cybersecurity.**
- **Prepare for the CompTIA Security+ certification and receive the exam voucher** at no extra cost.
- Leverage our **comprehensive career coaching services** to build or optimize the ideal cybersecurity career for you, and enhance your visibility with top hiring companies.
- Join a network of success—**over 1,500 companies across the U.S. have hired graduates** from Fullstack Academy Tech Bootcamps.
- Study with Fullstack Academy, a trusted trailblazer in tech education with **600+ cohorts delivered**, plus gain access to a vast network of **13,000+ alumni** who can help open doors to new career opportunities.
- Pursue a high-quality bootcamp program **rated 4.8 stars out of 5** by students and alumni (Course Report).
- Earn a **certificate of completion** jointly issued by Louisiana State University Online and Fullstack Academy, validating your industry-ready skills.
- Learn through **100% online classes** taught live by industry-experienced professionals.
- Engage in **15+ real-world, hands-on projects** for your cybersecurity career preparation, including a comprehensive capstone project you can use to demonstrate your skills to potential employers.
- Experience an immersive **genAI-powered cybersecurity bootcamp** with **25+ of the latest tools & technologies** like Splunk, Metasploit, Nmap, Wireshark, and Nessus.

Louisiana State University Online and Fullstack Academy Partnership

#1 University in Louisiana*

Louisiana State University Online (LSU Online)—consistently ranked among Kiplinger's Top 100 Public Colleges—is one of the highest-rated public universities in Louisiana. It has proven to be a place where students can get an exceptional education with a great return on investment. LSU graduates earn $20,000 more annually than the national average.

LSU Online has chosen Fullstack Academy to power its Cybersecurity Bootcamp. Fullstack Academy is one of the longest-running and most reputable tech bootcamps in the nation. Its graduates are equipped to succeed in the professional world through a foundational, active-learning teaching method, which prepares students to thrive in their first job and every job after. Bootcamp graduates also gain the assistance of the Fullstack Academy career services team and leave as members of the LSU Online and Fullstack Academy communities—with a supportive alumni network of over 13,000 graduates that can help open doors to future career opportunities.

*The Wall Street Journal

The Fullstack Academy Difference

Founded in 2012, Fullstack Academy is a pioneering and top-rated bootcamp provider that has helped over 13,000 graduates through 600+ cohorts to launch or accelerate their careers in tech.

Fullstack Inclusion

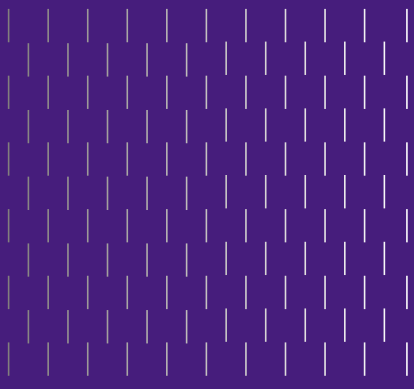
Fullstack can help make your career goals possible, no matter your background. We're committed to providing a welcoming, diverse, and flexible learning environment.

Fullstack Experience

Fullstack's rigorous curriculum focuses on the skills top-tier tech employers are seeking. Guided by passionate instructors and a caring career success team to assist with everything from interview prep to salary negotiations, you'll gain the confidence you need to build a fulfilling career.

Fullstack Outcomes

We're obsessed with helping our students succeed, and it shows: 1,500+ companies across the U.S. have hired our graduates — including notable companies like Google, Amazon, LinkedIn, Bloomberg, Facebook, Capital One, and many more.



Cybersecurity Industry Trends

The US cybersecurity industry is expanding rapidly as organizations confront increasingly complex digital threats, driving a surge in demand for skilled cyber professionals and competitive salaries. The global talent shortage—which spans nations, states, and industries—could reach 85 million workers by 2030, causing approximately $8.5 trillion in unrealized annual revenue (WEF). Some key statistics highlighting the demand for cyber expertise in today's workforce are:

$106,000

is the median salary for cybersecurity analysts in 2025 (Indeed)

500,000+

Job postings for cybersecurity-related positions in 2025 (CyberSeek)

29%

Projected job growth rate of Information security analysts from 2024-2034 (U.S. Bureau of Labour Statistics)

10%

of cybersecurity job listings specifically reference AI skills as a requirement in 2025 (Cyberseek)

67%

of organizations report a moderate-to-critical skills gap in cybersecurity (Global Cybersecurity Outlook 2025, World Economic Forum)

70,000+

Job openings requesting CompTIA Security+ certification (Cyberseek)

As organizations continue to digitize operations and contend with escalating cyber risks, the time has never been better to upskill for a secure and high-impact future in cybersecurity.

Cybersecurity Job Roles & Salaries

Explore cybersecurity job titles and their potential annual average salaries, according to data from Indeed and Glassdoor.

Job Title	Average Salary (USD)	Salary Range (USD)
Cybersecurity Analyst	$90,000	$75,000 - $105,000
Incident Responder	$90,000	$75,000 - $120,000
Network Security Engineer	$110,000	$90,000 - $130,000
Penetration Tester	$110,000	$90,000 - $130,000
Application Security Engineer	$115,000	$95,000 - $135,000
Security Engineer	$120,000	$100,000 - $140,000
Security Consultant	$130,000	$110,000 - $150,000
Security Architect	$130,000	$130,000 - $190,000
Cloud Security Engineer	$140,000	$120,000 - $160,000
Chief Information Security Officer	$245,000	$220,000 - $277,000

Fullstack Academy Graduates' Achievements

Top-Reported Salary: $350,000

This is the maximum salary among graduates who have disclosed their post-bootcamp salaries.

Average Salary: $76,038

This represents the average salary of Fullstack Academy graduates who provided post-bootcamp salaries. However, the salary increases up to $350,000 for some graduates, depending on various factors such as skills, experience, location, and employer.

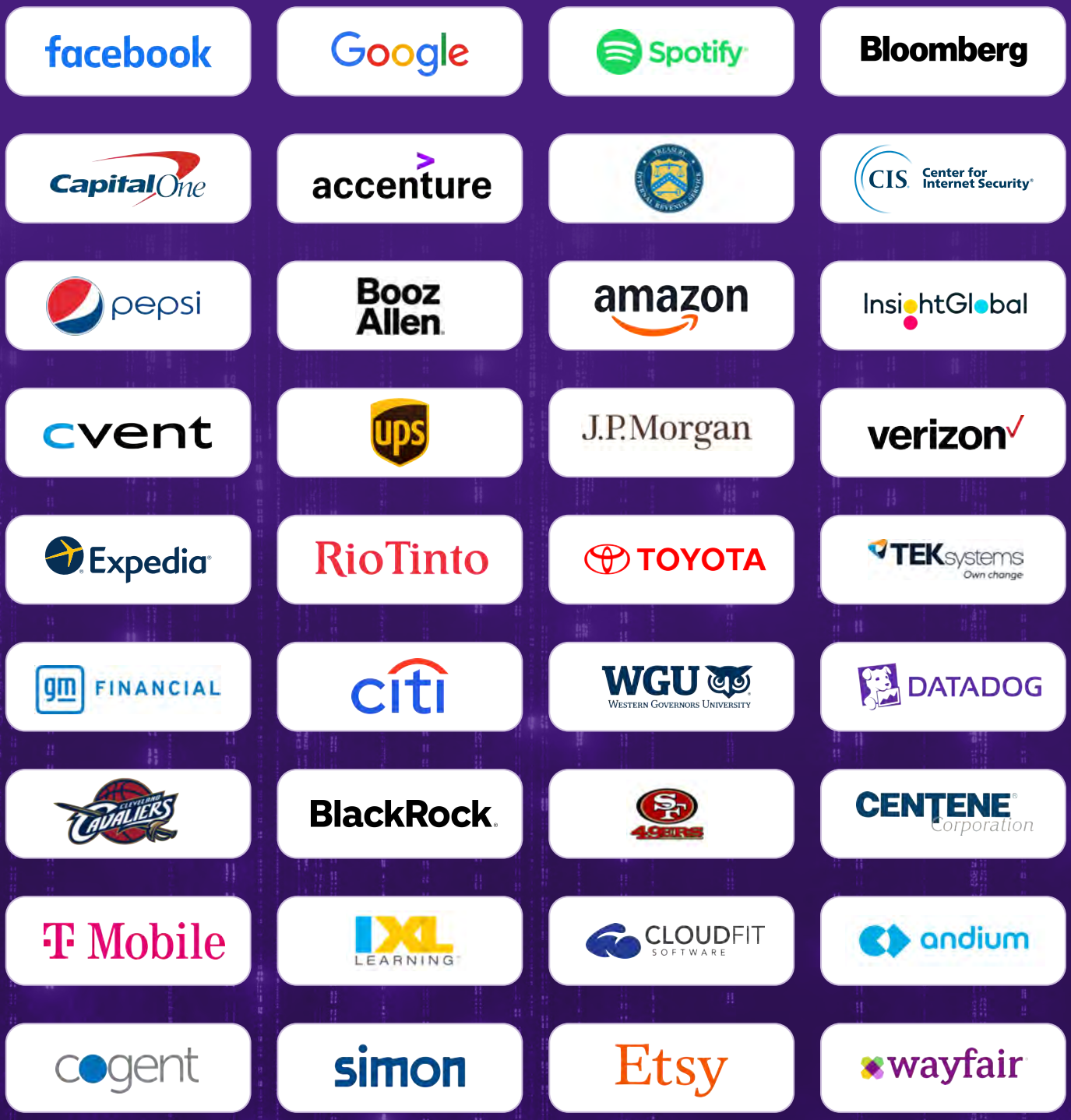
Alumni Network: 13,000+ graduates

Join over 13,000 students who have benefited from Fullstack Academy's industry-relevant curriculum and career preparation for in-demand tech roles.

Graduation Rate: 89%

This statistic is the percentage of students who have graduated from bootcamp or are close to graduation.

Prominent Companies That Have Hired Fullstack Academy Graduates:



...and many more

Career Success Services

During bootcamp and for a full year after graduation, you can access the Fullstack Academy Career Success Program to help achieve your desired career outcomes.

1,500+ companies across the U.S. have hired Fullstack Academy graduates—everywhere from large tech firms to mid-size companies and innovative start-ups. You'll also join our expansive network of alums—building lasting connections to support you throughout your career.

Our career success support includes:

- **Access to a Curated Career Success Platform:** Integrated services to build a professional profile, optimize your resume & LinkedIn profile, explore a curated job board, attend events, and connect with coaches
- **Career Practicum Lessons:** Step-by-step career curriculum lessons and tools
- **Workshops & Webinars:** Live and on-demand interactive sessions with Career Coaches on job search, networking, interviewing, and more
- **1:1 Career Coaching:** Personalized sessions during the program and up to 12 months after your graduation for guidance on resumes, networking, interviews, and salary negotiation
- **Alumni & Industry Events:** Panels, guest experts, and networking opportunities to expand professional connections
- **Ongoing Support:** Resources, tools, and expert advice to support career readiness and job search

Student Testimonials

"Initially, it felt overwhelming, but I learned to tackle each section methodically, which turned the challenge into a rewarding growth opportunity."

Chad Sider

Information Technology Help Desk Technician, ParaTech LLC

"The bootcamp showed me how to think like an analyst and apply cybersecurity tools in practical, meaningful ways."

Kelly Johnson

Command and Control Engineer, CloudFit Software

"Bootcamp has enabled me to not only learn a variety of programs and their purpose, but it has prepared me for real-world application of parsing data and identifying suspicious activity."

Carnesia Jackson

System Support Specialist, Coast Professional, Inc.

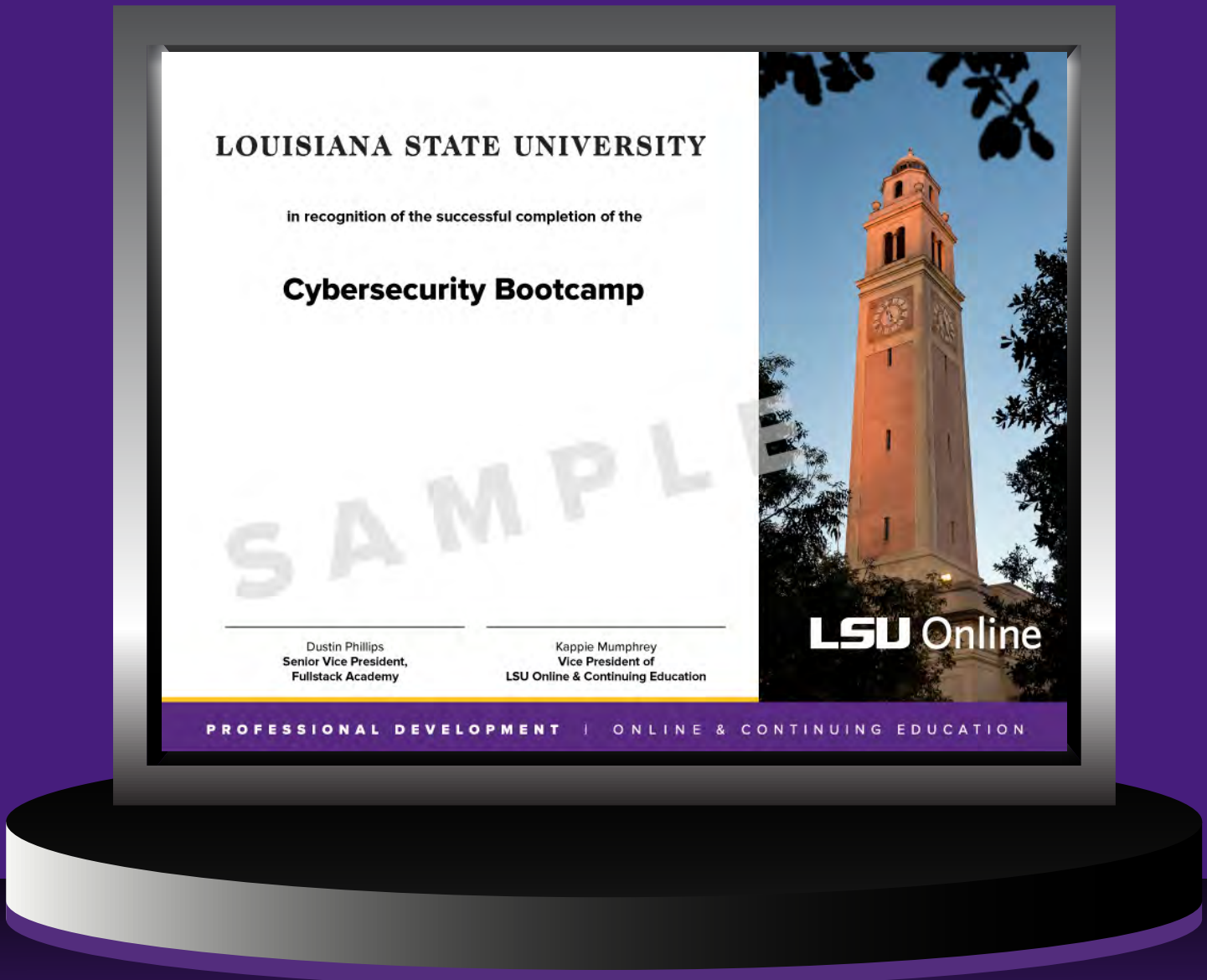
"The hands-on simulations and team projects allowed me to apply my knowledge in many different aspects. It was like a revelation to myself—that I can do this and be successful."

Tyler Blocker

Asset Management Configuration Technician, CapitalOne

Certificate of Completion

Upon completing the Cybersecurity Bootcamp, you'll receive a Certificate of Completion jointly issued by LSU Online and Fullstack Academy. These credentials will validate your skills as an industry-ready cybersecurity professional.



Curriculum Unit Overview

Elective: CompTIA Security+

Tools & Technologies Covered

Windows
Linux
splunk>
Metasploit
NMAP
WIRESHARK
ChatGPT
Nessus
SHODAN
aws
FTK® Imager
Scapy
hPing
Windows Server
Tor
OWASP
7ZIP
spiderfoot
Cmder
HxD Hex Editor
njRAT
Noriben
pestudio
RanSim
Whois
Identify for everyone
attify
beebox SYSTEMS
crunch
7 UFHTCRACK

...and many more

Sample Projects

Securing Linux Servers Using Honeypots and IP Blocking

Deploy a honeypot and defensive mechanisms like SSH hardening and automated IP blocking to detect, analyze, and mitigate SSH brute-force attacks.

Digital Forensics and Steganography: Recovering Hidden Data from a JPG Image

Utilize FTK (Forensic Toolkit) to recover a deleted file from its disk image and extract the hidden text from the recovered JPG.

Uncovering Digital Information for Security Analysis Using Footprinting, Reconnaissance, and Scanning

Utilize tools to identify open ports, services, and vulnerabilities—developing practical skills in ethical hacking and cybersecurity risk assessment.

Exploiting Android with Metasploit

Establish a remote shell connection from a target device to a control system, while exploring common Android vulnerabilities and defense techniques.

Secure File Storage and Access Management for Project Teams

Implement role-based access control to prevent unauthorized modifications and maintain audit compliance.

Performing a Vulnerability Assessment Using Kali and Metasploitable

Conduct a Kali Linux vulnerability assessment to gain practical network-scanning and vulnerability-analysis skills in a secure lab.

Executing Social Engineering Attacks with The FatRat and Metasploit

Simulate a social-engineering attack in a safe lab: craft a benign payload, send a phishing message, analyze the compromise, and perform email forensics.

Simulating and Analyzing a DoS Attack on a Web Server

Simulate a DoS attack in a controlled lab, then apply and verify basic mitigation using Windows Firewall.

Performing End-to-End Penetration Testing on Metasploitable2 Using GenAI (Gemini)

Perform a full black-box penetration test on Metasploitable2 targeting FTP, exposed directories, and vulnerable web apps.

Exploiting vsftpd Vulnerability Using Metasploit and GenAI

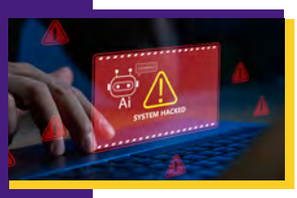
Simulate a red-team operation against a vulnerable FTP service using Metasploit and GenAI to guide exploit selection and avoid brute-force methods.

Performing AI-Powered SQL Injection Analysis and Report Generation Using SQLMap and TinyLLama via Ollama

Simulate a SQL injection assessment on DVWA using SQLMap for automated enumeration and data extraction.

Monitoring File Integrity Using Batch and GenAI on Windows

Build a file integrity monitoring system with Windows tools. Practice scripting, hash checks, tamper detection, and automation offline.



Running an Offline AI-Powered Malware Detection Workflow on Windows

Simulate a real-world Windows malware detection and response system using PowerShell and AI-style reasoning.

*The projects listed above are for illustrative purposes only and may be subject to change based on curriculum updates and industry relevance.

Eligibility Criteria

For admission into the LSU Online Cybersecurity Bootcamp, candidates must meet the following qualifications:

- Be at least 18 years old
- Have earned a high school diploma or GED equivalent

Application Process

The application process consists of three simple steps:

Fill out the online application form → Schedule a call with your Student Advisor → Receive an entrance decision

Talk to a Student Advisor

Our team of dedicated student advisors will guide you through your bootcamp journey. They are available to:

- Address your questions about the application process
- Discuss available payment options, discounts, and scholarships
- Provide insight into the curriculum, program outcomes, and more

Curriculum

Unit 1

Operating Systems and Networking Essentials

Lay the groundwork for your cybersecurity journey. This unit introduces essential operating system (OS) concepts (Windows and Linux), fundamental networking principles, and an overview of cryptography and wireless security.

Key Learning Objectives

- Understand OS architecture
- Apply file system management techniques in Windows
- Demonstrate user and group account management
- Compare various network topologies
- List the layers and functions of the TCP/IP and OSI models
- Improve network efficiency and reliability
- Describe Public Key Infrastructure components
- Apply wireless security measures to safeguard data

Key Skills

- Operating Systems
- Networking Concepts
- Network Topologies
- Cryptography Basics
- TCP/IP Model
- Public Key Infrastructure
- WLAN Security

Tools & Technologies

Windows

Linux

*Curriculum is subject to change.

LSU Online | In Collaboration With Fullstack Academy

Unit 2

Enterprise Infrastructure Security

Understand the core facets of enterprise security. This unit covers fundamental security concepts, network defense mechanisms, Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), an overview of Zero Trust Network, and Identity and Access Management (IAM).

Key Learning Objectives

- Analyze key security concepts
- Evaluate network defense mechanisms
- Implement SOAR and SIEM tools
- Analyze log types, formats, and collection methods
- Configure SIEM components for data storage optimization
- Develop SIEM rules and use cases
- Manage alerts and incident response workflows
- Design secure authentication and access control strategies

Key Skills

- Network Security
- Log Management
- Zero Trust Concepts
- SIEM
- Security Fundamentals
- Incident Response Basics
- Identity & Access Management
- SOAR

Tools & Technologies

Windows Server | splunk> | Tor

*Curriculum is subject to change.

Unit 3

Application Security and Cyber Resilience

This unit explains the essentials of web application security. Learn core concepts like encryption and Public Key Infrastructure (PKI), address the OWASP Top 10 threats, and integrate security into development using threat modeling.

Key Learning Objectives

- Identify core principles of web application security
- Apply secure coding practices
- Analyze threat modeling techniques
- Integrate security measures into the software development life cycle
- Understand the role of cyber resilience in continuity, threat mitigation, and trust

Key Skills

- Web Application Security
- OWASP Top 10
- Server-Side Request Forgery
- Threat Modeling
- Cyber Resilience Concepts

Tools & Technologies

*Curriculum is subject to change.

LSU Online | In Collaboration With Fullstack Academy

Unit 4

Web Application Vulnerabilities

Get hands-on experience with understanding and identifying weaknesses in web applications. This unit explores common application vulnerabilities and the techniques and tools used to find system vulnerabilities.

Key Learning Objectives

- Classify application vulnerabilities
- Analyze the security implications
- Analyze the impact of regular updates
- Analyze and demonstrate secure coding practices
- Integrate security measures for minimizing vulnerabilities

Key Skills

- Application Vulnerabilities
- Privilege Escalation
- Command Injection Attacks
- SQL Injection Attacks
- Cross-Site Scripting (XSS) Attacks
- Vulnerability Identification Concepts
- Attack Vectors and Methods

Tools & Technologies

Metasploit

*Curriculum is subject to change.

LSU Online | In Collaboration With Fullstack Academy

Unit 5

Ransomware and Malware—Defense, Analysis, and Response

Learn techniques to combat modern malware threats. This unit introduces various types of malware, with a specific focus on ransomware, and covers malware analysis tools and techniques, digital forensics, and malware protection.

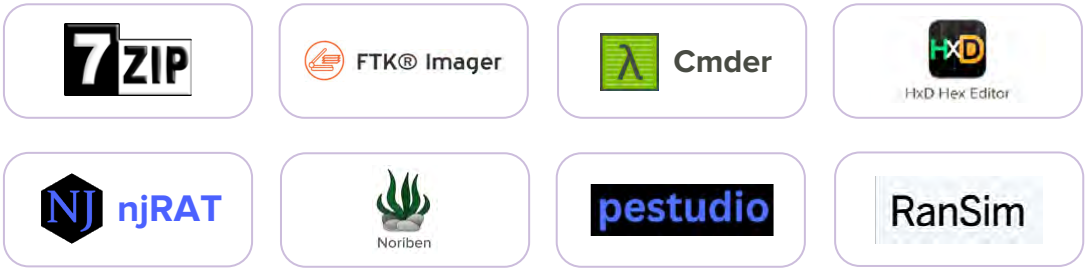
Key Learning Objectives

- Analyze different types of malware
- Apply malware analysis techniques
- Evaluate malware naming conventions
- Implement digital forensics strategies
- Examine ransomware attack campaigns and operators

Key Skills

- Malware Identification
- Malware Analysis
- Digital Forensics
- Incident Response Basics
- Cyber Threat Intelligence
- Ransomware Understanding and Mitigation
- Static Analysis Techniques
- Dynamic Analysis Techniques

Tools & Technologies



*Curriculum is subject to change.

Unit 6

Ethical Hacking: From Recon to Attack

Step into the shoes of an ethical hacker. This unit provides the foundation for ethical hacking, introduces the Cyber Kill Chain methodology, and covers essential reconnaissance and footprinting techniques used to gather information about target systems.

Key Learning Objectives

- Perform DNS enumeration
- Conduct active footprinting
- Apply advanced scanning techniques
- Utilize Metasploit for user account enumeration
- Explain the Cyber Kill Chain methodology and its stages
- Implement network enumeration, mapping, and OS identification

Key Skills

- Passive Footprinting
- DNS Enumeration
- Passive Reconnaissance
- Active Footprinting
- Active Reconnaissance
- Network Scanning
- Cyber Kill Chain Methodology
- Ethical Hacking & Reconnaissance

Tools & Technologies

*Curriculum is subject to change.

Unit 7

Vulnerability Assessment and Penetration Testing (VAPT)

Develop the skills to identify and exploit vulnerabilities in systems and networks. This unit covers vulnerability analysis and assessment, penetration testing, security scanning, social engineering, and denial-of-service attacks. Cloud and container security are also discussed.

Key Learning Objectives

- Apply vulnerability assessment techniques
- Implement the vulnerability management lifecycle
- Implement cloud and container security strategies
- Assess infrastructure and network-layer vulnerabilities
- Conduct penetration testing activities
- Evaluate social engineering and identity-based attack vectors

Key Skills

- Vulnerability Analysis
- Security Scanning
- Penetration Testing
- Social Engineering
- Cloud Security
- Containerization
- Everything as a Service (XaaS)
- Denial of Service and DDoS Attacks

Tools & Technologies

*Curriculum is subject to change.

Unit 8

Essentials of Generative AI

Explore the core concepts of Generative AI. This unit provides a fundamental understanding of Generative AI and Large Language Models (LLMs), focusing on prompt engineering and fine-tuning.

Key Learning Objectives

- Learn key concepts of generative AI and LLMs
- Utilize ChatGPT and domain-specific GPTs for practical use cases
- Demonstrate the ability to construct effective prompts
- Develop hands-on skills in leveraging multimodal capabilities and customized GPTs

Key Skills

- Generative AI Fundamentals
- Prompt Engineering
- Fine-tuning

Tools & Technologies

ChatGPT

*Curriculum is subject to change.

Unit 9

Generative AI in Cybersecurity

Understand how AI and Generative AI are transforming cybersecurity. This unit explores the applications of GenAI in threat analysis, incident response, forensics, penetration testing, and defense, while also addressing the ethical implications of using GenAI in cybersecurity.

Key Learning Objectives

- Analyze the role of GenAI in cyber operations
- Apply GenAI to real-world cyber scenarios
- GenAI-driven defensive techniques
- Ethical implications of GenAI in cybersecurity

Key Skills

- Cybersecurity Analytics using GenAI
- Cybersecurity Triage Process with GenAI
- Penetration Testing Using GenAI
- Introduction to Generative AI in Cybersecurity
- Risks and Vulnerabilities of GenAI in Cybersecurity
- Incident Response and Cyber Playbooks with GenAI
- Guarding Against Risks in LLMs with GenAI
- Vulnerability Management with GenAI
- Defensive Techniques Using GenAI
- Forensics Analysis with GenAI
- Threat Detection Using GenAI in SIEM
- GenAI-Driven SOAR

Tools & Technologies

ChatGPT

*Curriculum is subject to change.

Unit 10

Capstone Project

Put your cybersecurity skills to the test! You'll create a comprehensive cybersecurity solution or analysis, applying the knowledge and skills gained throughout the bootcamp.

Key Learning Objectives

- Integrate knowledge from various units to solve a unique cybersecurity challenge
- Collaborate effectively in a team environment
- Design a cybersecurity solution or analysis, and present your findings and recommendations

Key Skills

- Problem-Solving in Cybersecurity
- Integration of Cybersecurity Concepts
- Teamwork and Collaboration
- Technical Presentation Skills

*Curriculum is subject to change.

CompTIA Security+ (Elective)

This optional elective unit will prepare you with essential knowledge and skills to take the CompTIA Security+ certification exam. The elective focuses on core security principles, risk management, incident response, cryptography, identity and access management, and securing networks, systems, and applications.

The CompTIA Security+ certification is a globally recognized credential that validates your foundational knowledge and skills in cybersecurity. The certification demonstrates competency in core concepts required for career advancement in cybersecurity.

Eligible students can receive a voucher for one CompTIA Security+ exam attempt at no additional cost.

Key Learning Objectives

- Understand and apply cybersecurity risk management concepts
- Identify and mitigate common threats, vulnerabilities, and attacks
- Respond to security incidents and perform basic digital forensics
- Implement identity and access controls
- Secure network architecture and endpoint systems
- Understand compliance, governance, and security auditing principles

Key Skills

- Threat Analysis and Vulnerability Assessment
- Network and Endpoint Security Configuration
- Secure Protocol Implementation
- Basic Penetration Testing and Incident Response
- Familiarity with Cloud and Mobile Security Best Practices
- Identity and Access Management

LSU Online

In Collaboration With Fullstack Academy

APPLY NOW

http://bootcamp.online.lsu.edu/programs/cybersecurity

info.lsu@fullstackacademy.com