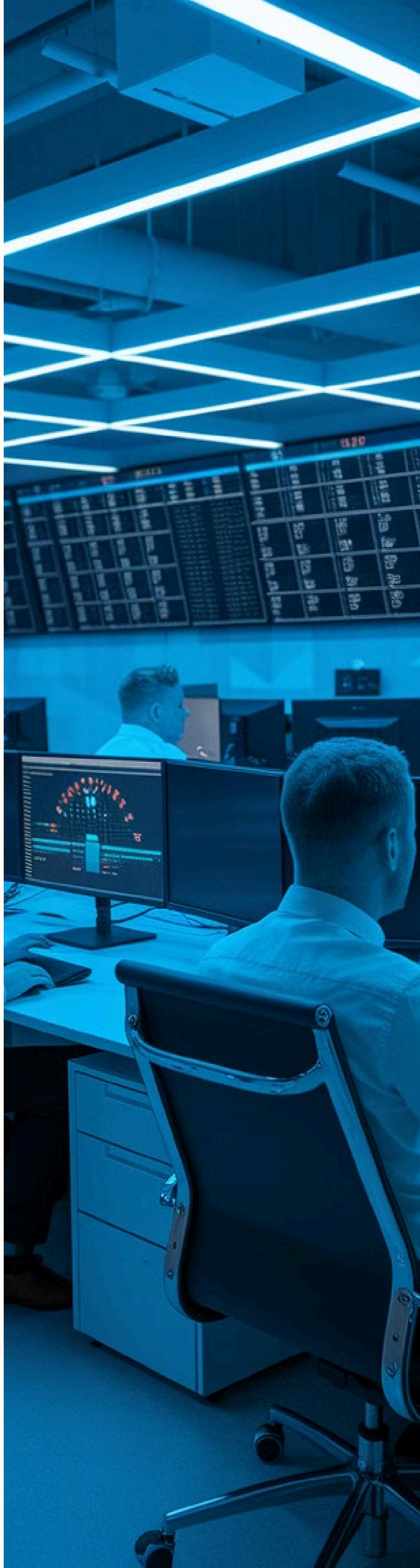
Program Catalog

Cyber Security Responder & Practitioner (CSRP)

Empowering the Next Generation of Cybersecurity Professionals

CYBER SCHOOL



1 **Program Overview**

About the CSRP Program • Preparing You for Cybersecurity Jobs • What You Will Learn • Commitment to Success

2 **Learning Experience**

Program Structure • Teaching Methodologies • CSRP Education Process • Program Flow

3 **Program Benefits**

What's Included • Industry Certifications • The CSRP Advantage

4 **Career Development**

Program Breakdown by Course • Career Services • Program Summary

About the CSRP Program

In today's digital landscape, organizations face increasingly sophisticated cybersecurity threats. As hackers exploit new vulnerabilities faster than ever, the demand for skilled cybersecurity professionals has never been greater.

1000+	3	100%
Total Training	**Industry Recognition**	**Practical Training**
Comprehensive learning journey	Including CompTIA Security+	Real-world simulations

The Cyber Security Responder & Practitioner (CSRP) Bootcamp addresses the global shortage of cybersecurity professionals through:

Comprehensive Learning Experience

Blended learning combining instructor-led sessions with self-paced study and hands-on labs

Industry-Aligned Curriculum

Real-world skills, practical experience, and recognized certifications including LPI Linux Essentials, PCAP, and CompTIA Security+

Career Development Focus

Complete career services including resume building, interview preparation, and job search strategies

Whether you're starting your IT journey or advancing your cybersecurity career, CSRP provides your pathway from beginner to job-ready professional through hands-on experience, CTF competitions, and capstone projects.

Launch Your Cybersecurity Career

Transform your future with CSRP's industry-leading cybersecurity training program. We've engineered every aspect of our curriculum to prepare you for immediate success in the fastest-growing technology sector, with direct pathways to high-paying cybersecurity positions.

$65K

Entry Salary

Average starting compensation for graduates

3.5M

Open Positions

Global cybersecurity job opportunities

35%

Growth Rate

Expected industry expansion by 2025

Security Operations

- SOC Analyst
- Threat Hunter
- Incident Responder

Infrastructure Security

- Technical Help Desk Technician
- Network Security Administrator
- Cybersecurity Analyst

Offensive Security

- Penetration Tester (Ethical Hacker)
- Digital Forensics Investigator
- Red Team/Blue Team Specialist

Graduate job-ready with the perfect blend of practical skills, industry certifications, and hands-on experience that both private and public sector employers demand. Our comprehensive training ensures you're prepared to step into high-impact cybersecurity roles from day one.

What You Will Learn

The CSRP program delivers a comprehensive cybersecurity education through a structured progression of skills and knowledge, from foundational concepts to advanced specializations.

1

Advanced Cybersecurity

Master specialized skills in incident response, malware analysis, digital forensics, and threat hunting

2

Tools & Technologies

Gain hands-on experience with industry-standard security tools, SIEM systems, and cloud platforms

3

Foundational Knowledge

Build a strong foundation in networking, operating systems, and cybersecurity frameworks

🎯 Hands-On Experience

- Virtual labs and cybersecurity simulations
- Red Team vs. Blue Team exercises
- Capture The Flag (CTF) challenges
- Capstone projects for real-world application

🛠️ Technical Skills

- Firewalls, VPNs, IDS/IPS systems
- Cloud security (AWS, Azure, GCP)
- Python programming for cybersecurity
- Penetration testing techniques

🧠 Advanced Topics

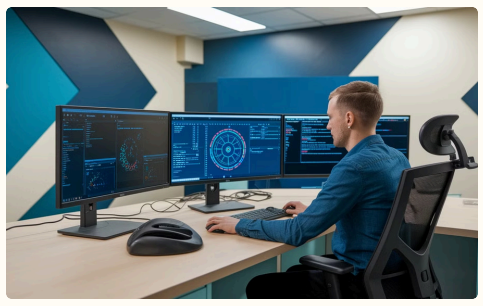
- Malware analysis & reverse engineering
- Digital forensics & memory analysis
- Threat intelligence gathering
- Game theory in attack/defense

Your Path to Cybersecurity Success

At CSRP, we don't just teach cybersecurity—we transform careers and build industry leaders. Our comprehensive support system ensures every student has the tools, guidance, and opportunities needed to thrive in the cybersecurity field.

Expert-Led Training

Learn directly from industry veterans who bring real-world cybersecurity challenges and solutions into the classroom, ensuring you're prepared for actual scenarios you'll face in the field.



Hands-On Experience

Master your skills in state-of-the-art virtual labs that replicate real security environments, giving you practical experience with the latest tools and techniques.

Personalized Growth

Benefit from one-on-one mentorship sessions with cybersecurity experts who guide your learning journey and help you overcome challenges.

Career Launch

Transform your skills into career success with comprehensive career services, including resume crafting, interview preparation, and direct connections to industry opportunities.

Your success is our mission. Whether you're starting fresh or advancing your existing career, CSRP provides the perfect blend of cutting-edge curriculum, personal support, and practical experience to help you achieve your cybersecurity goals.

Program Structure

The CSRP Bootcamp is divided into three distinct phases, each designed to prepare students for specific roles within the cybersecurity industry.

1 Phase 1: Fundamentals

Technical Help Desk Focus

- Introduction to Cybersecurity (Sorting Course)
- Computer Networking
- Operating Systems Security (Windows & Linux)
- Certification Prep: LPI Linux Essentials
- Career Services Week: Resume building & LinkedIn optimization

2 Phase 2: Cybersecurity Technologies

Cybersecurity Practitioner Focus

- Cybersecurity Technologies and Tools
- Artificial Intelligence for Cybersecurity
- DevSecOps (Cloud Security & Automation)
- Python Security (Secure Coding & Automation)
- Certification Prep: PCAP – Certified Associate in Python Programming
- Career Services Week: Interview preparation & job market strategies

3 Phase 3: Advanced Cybersecurity

Cybersecurity Analyst Focus

- Ethical Hacking (Penetration Testing & Exploit Development)
- Game Theory Skills and CTF Challenges (Competitive Cybersecurity)
- Incident Response and Digital Forensics
- Certification Prep: CompTIA Security+
- Career Services Week: Advanced interview prep & leadership training

Teaching Methodologies

The CSRP Bootcamp blends traditional instruction with hands-on learning to ensure maximum skill retention and real-world readiness.

Key Teaching Methods

Live Instruction

Weekly 4-hour instructor-led sessions with industry experts

Self-Paced Study

Flexible asynchronous lessons for deeper exploration

Hands-On Labs

Virtual cybersecurity environments for practical experience

CTF Challenges

Competitive, gamified learning experiences

CSRP Education Process

Our comprehensive Five-Step Cyber Education Process ensures every student is career-ready upon completion:

1

Consultation & Career Planning

Meet with admissions advisors to map out your cybersecurity career goals

2

Introductory Course

Complete the 30-hour sorting course to assess program suitability

3

Hands-On Training

Learn through immersive labs, projects, and real-world simulations

4

Certifications

Earn globally recognized cybersecurity certifications

5

Career Launch

Work with career coaches to build your professional profile and ace interviews

What's Included in CSRP Bootcamp

3

Core Certifications

LPI Linux Essentials, PCAP, and CompTIA Security+

10

Program Courses

From expert training to career services

16

Months

Including career services

Core Program Features

Expert-Led Training

Learn from industry professionals through live instruction and hands-on guidance

Virtual Labs & Simulations

Practice in real-world environments with CTF challenges and team exercises

Career Development

Comprehensive career services including resume building, LinkedIn optimization, and interview prep

Certification Preparation

Structured preparation for industry-recognized certifications with additional resources

Certification Pathway

Certification	Phase	Focus Area
LPI Linux Essentials	Phase 1	Linux Systems & Command Line
PCAP – Certified Associate in Python	Phase 2	Python Programming & Automation
CompTIA Security+	Phase 3	Advanced Cybersecurity Concepts

Advanced Certification Options

- CEH (Certified Ethical Hacker)
- CHFI (Computer Hacking Forensic Investigator)
- OSCP (Offensive Security Certified Professional)

The CSRP Advantage

- Blended Learning Approach with Live & Self-Paced Study
- Hands-On Labs & Real-World Simulations
- Competitive CTF Challenges & Team Exercises
- Career-Focused Curriculum with Dedicated Support
- Global Alumni Network & Employer Partnerships

Full CSRP Pathway - Detailed Lessons

Cyber Security Responder & Practitioner (CSRP) Bootcamp

Phase 1: Cybersecurity Fundamentals

1

Introduction to Cybersecurity

Core Concepts

- Welcome to Cybersecurity
- Understanding the Threat Landscape
- The CIA Triad and Security Concepts
- Risk Management & Compliance

Career Focus

- Cybersecurity Roles and Salaries
- Building Your Career Path
- Resume Building & LinkedIn Optimization
- Job Market Overview

2

Computer Networking

Network Fundamentals

- Networking 101
- OSI Model & TCP/IP Stack
- IP Addressing & Subnetting
- Routing & Switching

Security Components

- Firewalls & VPNs
- IDS/IPS Systems
- Wireless Security
- Cloud Networking

3

Operating Systems Security

Core OS Security

- OS Architecture
- Command-Line Mastery
- User Authentication
- Permissions & Access Control

Platform Security

- Windows Security
- Linux System Hardening
- Network Services Security
- System Monitoring

4

Certification Path

- LPI Linux Essentials Prep
- Multi-OS Security Capstone
- Career Services Support
- Professional Profile Building

Phase 2: Cybersecurity Technologies

Prepare for PCAP Certification

Cybersecurity Technologies and Tools

Master essential security tools including SIEM, firewalls, and cloud security while building practical SOC skills.

AI for Cybersecurity

Learn to leverage AI and machine learning for advanced threat detection and automated security responses.

DevSecOps

Integrate security into the development pipeline using modern tools and cloud-native security practices.

Python Security

Develop secure automation scripts and custom security tools using Python.

Cybersecurity Tools Mastery

- SOC operations and SIEM implementation
- Threat intelligence and security frameworks
- Advanced firewall and IDS/IPS configuration
- Cloud security across AWS, Azure, and GCP
- Capstone: Design a comprehensive secure network

AI-Powered Security

- Machine learning for anomaly detection
- AI-driven threat hunting and malware detection
- Automated incident response systems
- Ethical considerations in AI security
- Capstone: Build AI threat detection system

1

DevSecOps Foundation

Infrastructure as Code and secure CI/CD pipelines

2

Container Security

Docker and Kubernetes security best practices

3

Python Security

Secure coding and security automation

4

PCAP Certification

Final preparation and certification

🎓 Certification Goal

PCAP – Certified Associate in Python Programming

💼 Career Services

Resume building for SOC and Cybersecurity Analyst roles with specialized interview preparation

🏆 Learning Outcome

Hands-on experience with modern security tools, AI integration, and automation through Python

Phase 3: Advanced Cybersecurity (Prepare for CompTIA Security+)

1 Ethical Hacking

Master the art of ethical hacking through hands-on penetration testing, vulnerability assessment, and security auditing. Culminates in a full-scale penetration test project.

- The Penetration Testing Process
- Active & Passive Reconnaissance
- Web Application & Wireless Hacking
- Social Engineering & Physical Security
- Privilege Escalation & Reporting

2 Game Theory & CTF Challenges

Apply game theory principles to cybersecurity through competitive Capture The Flag challenges and red vs. blue team exercises.

- Offensive & Defensive Strategies
- CTF Challenge Solutions
- Red vs. Blue Team Exercises
- Live Fire Drill Scenarios

3 Incident Response & Digital Forensics

Learn comprehensive incident handling and digital forensics techniques, culminating in a full-scale cyber incident simulation.

- Incident Response Lifecycle
- Memory & Disk Forensics
- Malware Analysis
- Threat Intelligence

Career Development & Certification Path

Career Services

- Resume Building & LinkedIn Optimization
- Interview Preparation
- Portfolio Development
- Networking Strategies

Certifications Pathway

- LPI Linux Essentials (Phase 1)
- PCAP Certification (Phase 2)
- CompTIA Security+ (Phase 3)

Program Breakdown by Course

960h

Total Program Hours

Complete cybersecurity training program

840h

Instructor-Led Hours

Direct training with cybersecurity experts

120h

Self-Study Hours

Certification preparation & asynch learning

Our comprehensive cybersecurity program is divided into three phases, each building upon the previous to develop your expertise:

1 Phase 1: Fundamentals

- Introduction to Cybersecurity (84h - Instructor-Led)
- Computer Networking (84h - Instructor-Led)
- Operating Systems Security (84h - Instructor-Led)
- LPI Linux Essentials (40h - Self-Study)

2 Phase 2: Advanced Technologies

- Cybersecurity Technologies & Tools (84h - Instructor-Led)
- Artificial Intelligence for Cybersecurity (84h - Instructor-Led)
- DevSecOps (Cloud Security & Automation) (84h - Instructor-Led)
- Python Security (84h - Instructor-Led)
- PCAP Certification Prep (40h - Self-Study)

3 Phase 3: Expert Skills

- Ethical Hacking (84h - Instructor-Led)
- Game Theory Skills & CTF Challenges (84h - Instructor-Led)
- Incident Response & Digital Forensics (84h - Instructor-Led)
- CompTIA Security+ Prep (40h - Self-Study)

Each phase includes both instructor-led training and self-paced certification preparation to ensure comprehensive learning and industry recognition.

Career Services & Program Overview

Our comprehensive career support ensures you're ready for success in cybersecurity:

Career Development

Professional resume building and LinkedIn profile optimization to showcase your skills

Interview Excellence

Comprehensive technical and behavioral interview preparation with mock sessions

Industry Networking

Access to exclusive networking events and cybersecurity job fairs

Job Strategy

Personalized job search strategies and salary negotiation guidance

1008

Program Hours

Complete program duration

576

Direct Training

Interactive classroom hours

432

Independent Learning

Flexible study time

Industry Certifications

- LPI Linux Essentials
- PCAP – Certified Associate in Python Programming
- CompTIA Security+

Hands-on Capstone Projects

- Red Team/Blue Team Simulation
- CTF Challenge
- Real-World Cyber Incident Response

Join Us in Shaping Tomorrow's Security

> Every expert was once a beginner. In the world of cybersecurity, it's not just about defending systems—it's about defending the future.

Step Forward

Begin your journey into cybersecurity

Stay Curious

Never stop learning and exploring

Make Impact

Become the protector the world needs

Your cybersecurity journey starts here. Are you ready to make a difference?