BELLSTECH ACADEMY

PURDUE UNIVERSITY | Delivered by simplilearn

Professional Certificate Program in Cybersecurity

In Collaboration With Microsoft

- Master O ensive and Defensive Cybersecurity
- 60+ Hands-on Projects, 20+ Tools
- Specialized Module on GenAI with Cybersecurity

BELLSTECH ACADEMY

Cybersecurity Industry Trends

The global cybersecurity market is projected to grow at a CAGR of 7.92% from 2024 to 2029, reaching a market volume of US$ 271.90 billion by 2029.

Source: Statista

US Market

The US leads the global cybersecurity market and is on track to generate $81.4 billion in revenue in 2025.

Source: Statista

Career Growth

62% increase in cybersecurity job roles over the past five years.

Source: LinkedIn

Ransomware Growth

Ransomware costs are projected to reach $265 billion annually by 2031, with increasing attacks targeting critical industries.

Source: Cobalt

AI in Cybersecurity

AI will enhance detection and predictive insights, shifting from reactive to proactive security approaches.

Source: ISACA

BELLSTECH ACADEMY

About the Program

Welcome to the Professional Certificate Program in Cybersecurity, a collaboration between Purdue University and Simplilearn. This comprehensive program is designed to equip individuals with the skills and knowledge to safeguard systems, protect sensitive data, and defend against cyber threats in today's increasingly digital world.

You'll gain hands-on experience with industry-standard tools to assess vulnerabilities, implement security protocols, manage operations, and respond to incidents. The curriculum covers essential cybersecurity topics, including network security, threat detection, incident response, and risk management, ensuring you are prepared to counter malware, ransomware, and other common threats. Whether you are an IT professional, security analyst, consultant, or simply looking to develop your

expertise in cyberse curity, this program is designed for you. Our expert instructors will guide you through real-world scenarios and provide the knowledge and resources you need to succeed in the dynamic and high-demand field.

Key Features of the Program

Learn and Build Credibility With Recognized Certifications

- Earn a program completion certificate from Purdue University Online and Simplilearn.
- Attend online masterclasses by Purdue faculty and sta and instructor-led sessions by top industry experts.
- Access the Microsoft Learn portal and get O icial Microsoft Azure-branded certificates courses.

Hands-On Learning with an Industry-Aligned Curriculum

- Gain 100+ hours of live expert-led training covering foundation to red and blue team concepts.

Foundations Module
Build expertise in operating systems, networking, and security fundamentals.

Defensive Security
Learn to secure enterprise infrastructure, protect applications, and mitigate cyber threats. Develop skills in firewalls, SIEM, IAM, and malware analysis.

O ensive Security
Master ethical hacking, vulnerability assessment, and penetration testing. Perform reconnaissance, network scanning, and exploit simulations using industry tools.

- Get three industry-relevant capstone projects and 60+ hands-on projects with seamless access to integrated labs.

Accelerated Career Advancement & Professional Network

Exclusive Access to the Purdue Alumni Association Upon Program Completion.

Dedicated Career Services:

- One-on-one interview service by TopInterview
- Resume makeover assistance from TopResume
- Access to the Resume Rabbit employer network
- 30-day premium subscription to career.io

Learning Path Visualization

Program Modules

Electives

- Academic Masterclass
- Essentials of Generative AI, Prompt Engineering & ChatGPT
- GenAI with Cybersecurity
- Azure Fundamentals (AZ-900)
- Security, Compliance, and Identity Fundamentals (SC-900)
- Azure Security Engineer Associate (A Z-500)

Module 1

Induction for Professional Certificate Program in Cybersecurity

- Kickstart your journey with our Professional Certificate Program in Cybersecurity, covering all essential concepts in the cybersecurity field
- Explore everything about this unique program covering fundamental and advanced cybersecurity concepts

Module 2

Operating Systems and Networking Essentials*

- Gain a solid understanding of operating systems, including memory management, file systems, and system architecture
- Acquire essential networking skills, including protocols, topologies, and security practices, with hands-on experience using tools like PowerShell, Wireshark, and Packet Tracer

Module 3

Enterprise Infrastructure Security

- Gain advanced cybersecurity knowledge and skills focused on enterprise and infrastructure security, essential for managing complex digital environments
- Develop a deep understanding of the NICE framework, security controls, firewalls, SIEM, VPNs, and identity and access management

*This module is optional

Module 4

Application Security, Vulnerability Management, and Cyber Resilience

- Learn essential principles of application security, including web architecture, encryption, OWASP vulnerabilities, and security testing practices
- Get hands-on experience with security, monitoring, and logging tools while using frameworks like NIST and ISO/IEC 27001 to mitigate vulnerabilities and improve cybersecurity

Module 5

Ransomware and Malware - Defense, Analysis and Response

- Explore various types of malware and ransomware, how they spread, and ways to protect against them
- Gain hands-on experience in conducting malware analysis and incident response to detect and manage cyber threats e ectively

Module 6

Ethical Hacking - From Recon to Attack

- Understand the fundamentals of cybersecurity, including defensive and o ensive security, hacker classifications, and attack methodologies like the Cyber Kill Chain and MITRE ATT&CK®
- Learn hands-on techniques for network scanning, footprinting, and enumeration techniques using real-world tools and methods to enhance o ensive and defensive security

BELLSTECH ACADEMY

Module 7

Vulnerability Assessment and Penetration Testing (VAPT)

- Understand vulnerability management techniques, including vulnerability assessment, scoring systems like CVSS, and how to use tools like Nessus and Nmap for e ective scanning and reporting
- Learn about advanced network security threats such as sni ing, DoS/DDoS attacks, and social engineering, and how to deploy defense strategies like honeypots, AAA, and Wireshark-based analysis

Module 8

Capstone Project

- Apply the cybersecurity skills you learned throughout the program in this culminating project
- Solve real-world, industry-based challenges and showcase your abilities to employers with a Capstone completion certificate from Simplilearn

Electives:

Module 1

Academic Masterclass

Attend an online interactive masterclass to gain insights about advancements in cybersecurity technology and techniques.

Module 2

Essentials of Generative AI, Prompt Engineering & ChatGPT

- Explore cutting-edge topics in generative AI, prompt engineering, and ChatGPT
- Gain hands-on skills and practical insights into real-world business applications of GenAI
- Learn to apply generative AI e ectively and leverage prompt engineering for customized outputs

Module 3

Generative AI with Cybersecurity

- Explore the role of Generative AI in cybersecurity, including its impact on threat intelligence, playbooks, and combating phishing, malware, and deep fakes
- Understand how Generative AI can enhance defense strategies and threat prediction
- Investigate NLP strategies to improve cybersecurity defenses and anticipate threats

Module 4

Microsoft Certified: Azure Fundamentals (AZ-900)

- Explore Microsoft Azure's core services, including compute, networking, and storage
- Understand Azure's architectural components and tools for security, governance, and administration
- Investigate how Azure supports cloud computing concepts and prepares you for a career in cloud technology

Module 5

Microsoft Certified: Security, Compliance, and Identity (SCI) Fundamentals (SC-900)

- Explore the fundamentals of security, compliance, and identity in Microsoft environments
- Understand key concepts and tools for securing identities, managing compliance, and protecting information
- Investigate how Microsoft solutions integrate security, compliance, and identity management to enhance organizational protection

Module 6

Microsoft Certified: Azure Security Engineer Associate (AZ-500)

- Explore advanced security features and tools in Microsoft Azure to protect cloud environments
- Understand identity and access management, platform protection, and data security in Azure
- Investigate how to manage security operations and implement threat protection to secure your Azure infrastructure

BELLSTECH ACADEMY

Skills Covered

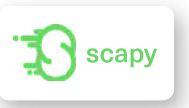
- Operating Systems Fundamentals
- System Architecture
- Virtual Memory Concepts
- Networking Concepts
- Network Protocols
- Firewalls and Security Protocols
- SIEM Systems
- MITRE ATT&CK Framework
- Cybersecurity Threats and Vulnerabilities
- Ethical Hacking
- Penetration Testing
- Secure Coding Practices
- Incident Response
- Risk Management
- Prompt Engineering

Integrated Labs & Tools

Students will get access to the following VM:

Students will get hands-on experience working with the tools below, but they won't be required to install them on their computers. They can access them through virtual machines (VMs) in our secure, integrated lab environment.

Foundations:



Defensive Security:

Semgrep

pestudio

splunk>

OWASP ZAP

OWASP Threat Dragon

exterro

Offensive Security:

metasploit

Nessus

spiderfoot

SHODAN

Crunch

BEE BOX

Binwalk

Capstone Project

Project 1

A Day in the Life of a System Administrator

Set up a secure file storage system for Globex Financial's finance teams. Configure user accounts, manage ACLs, and customize the command history (10 or 50 commands). Ensure settings persist and monitor security violations via logs accessible through a secure web interface for IT security.

Project 2

A Day in the Life of a Security Operations Center (SOC) Analyst

Conduct a vulnerability assessment on SecureBank's Windows Server 2016 environment. Identify and exploit vulnerabilities using tools like Metasploit, assess the impact on confidentiality, integrity, and availability, and perform root cause analysis to strengthen security and prevent future threats.

Project 3

A Day in the Life of a Network Security Engineer

Deploy and manage Active Directory (AD) for TechCorp using Windows Server 2019. Set up a secure AD domain, configure client systems, create organizational units, and manage user accounts. Implement security policies aligned with NIST and CIS standards to enhance centralized network administration, enforce security, and ensure compliance.

Disclaimer - The projects have been built leveraging real publicly available data-sets. Data may be tweaked to enable learners to get maximum advantage of their learnings in the course

Learning Outcomes

Upon successful completion of the program, you will:

- Gain a comprehensive understanding of system architecture, virtual memory, and networking fundamentals across Windows and Linux platforms.
- Develop proficiency in vulnerability assessment, penetration testing, and network monitoring tools to secure networks e ectively.
- Acquire specialized knowledge in ethical hacking, threat analysis, incident response, and secure coding practices to protect against cyber threats.
- Learn to implement and manage Security Information and Event Management (SIEM) systems for real-time security event monitoring and incident handling.
- Understand and apply the principles of risk management and compliance to safeguard organizational information systems and comply with regulatory standards.
- Apply cybersecurity skills through capstone projects that simulate industry-relevant security challenges, demonstrating your ability to solve real-world problems.
- By the end of this program, you'll be prepared to take on roles such as cybersecurity analyst, SOC specialist, consultant, and more, with opportunities at leading companies.

University Certificate

Upon completing the Professional certificate program in Cybersecurity you will receive a program completion certificate from Purdue University Online and Simplilearn.

Microsoft Certificate

Receive Industry-recognized Microsoft certificates for Microsoft courses.

Career Opportunities After Completion

The program is ideal for professionals aspiring to fill various cybersecurity job roles, including:

Cybersecurity Analyst

An analyst's responsibilities include analyzing security incidents, monitoring security infrastructure, and implementing security measures to protect data and systems.

Security Operations Center (SOC) Analyst

This position focuses on monitoring, detecting, and responding to security events and incidents within an organization's SOC.

Threat Intelligence Analyst

They gather, analyze, and interpret threat data to provide actionable intelligence and enhance the organization's security posture.

Malware Analyst

Specializes in analyzing and reverse-engineering malware to understand its behavior, functionality, and mitigation techniques.

Vulnerability Analyst

Identifies, evaluates, and mitigates security vulnerabilities within an organization's systems and applications.

Cybersecurity Consultant

Provides expert advice and solutions to organizations on cybersecurity strategies, policies, and best practices.

Network Security Administrator

Manages and secures an organization's network infrastructure, including firewalls, routers, and switches, to prevent unauthorized access and threats.

Compliance Analyst

Ensures the organization's security policies and procedures comply with relevant laws, regulations, and standards.

Red Team Specialist

Simulates cyberattacks to test and improve the organization’s defenses, identify weaknesses, and recommend enhancements.

Blue Team Specialist

This person defends the organization’s systems against cyberattacks, focusing on detection, response, and recovery.

These job roles reflect the diverse opportunities available in the cybersecurity field, catering to various specializations and expertise.

Suite 15-04, Menara Tan & Tan, 207, Jalan Tun Razak,
50400 Kuala Lumpur, Malaysia

Email: support@bellstechacademy.com

www.bellstechacademy.com