Learn Faster with Victrics Career Based Security Training

“Be where your enemy is not.”
-Sun Tzu

Technical Foundations Networking Basics (Network+)

Cybersecurity is built on a foundation of core technical skills, and Module 1 of this curriculum establishes those essentials. We begin with understanding computer components—motherboards, CPUs, and memory—and move to operating systems and virtualization, forming the groundwork for managing IT environments. Networking fundamentals, including the OSI model and network devices like firewalls, are introduced to build confidence in designing and securing networks.

Students also explore internet architecture, database basics, and encryption concepts, from hashing to public-private key systems. These are paired with an introduction to security principles like the CIA triad—Confidentiality, Integrity, and Availability—forming a bridge to more advanced topics.

Through practical, hands-on learning, this module ensures that whether you're entering the workforce or pursuing further cybersecurity education, you'll have a strong grasp of essential skills. This foundation is critical as we dive into specialized roles, such as Information Systems Security Officers and Security Controls Assessors, in subsequent modules.

1. **Networking Computer/Network Technology Foundations ($500 USD)**
    - **Week 1**
      Focus: Explore computer hardware and electronic components such as motherboards, CPUs, memory, and virtualization. Learn the basics of operating systems and servers.
    - **Week 2**
      Focus: Master networking fundamentals, including the OSI model, networking technologies, and devices like firewalls. Understanding networking topologies, cabling. and IP introduction

- **Week 3**
  ***Focus*: Understand internet architecture (DNS, HTTP, TCP/IP) and web server concepts. Gain foundational database knowledge, including structure, SELECT statements, and security.**
- **Week 4**
  ***Focus*: Understanding Network devices and virtualization, understanding protocols and services.**
- **Week 5**

  Focus: Understanding VLANS and Cloud concepts, Data centers and architectures
- **Week 6**

  Focus: Network access controls, redundancy and wireless concepts

---

Cybersecurity Fundamentals Security+ Aligned Training

This **six-week course** is designed for beginners with general computer or networking knowledge. **No prior cybersecurity experience required**—we use real-world scenarios to make complex security concepts easy to understand and apply.

You'll gain essential skills in threat identification, risk management, cryptography, and security operations. Our hands-on approach ensures you're not just learning theory, but developing practical abilities that employers value.

- **Week 1**
  ***Focus*: Review computer hardware, electronic component, networking hardware and how cyber security concepts protect physical (and virtual) IT assets**
- **Week 2**
  ***Focus*: Security concepts.** Understand security concepts pertaining to Internet architecture (DNS, HTTP, TCP/IP) and web server concepts. Gain

foundational database knowledge, including structure, SELECT statements, and security. devices like firewalls.

- **Week 3**
  ***Focus*: Threats, Vulnerabilities, and Mitigation.** Understand the threats arrayed against information systems, how vulnerable systems can lead to data loss, financial loss and more. Learn how to blunt the attacks and minimize their risks.
- **Week 4**
  ***Focus*: Security Architecture,** Learn encryption basics, including public/private keys and hashing. Grasp core security principles, such as the CIA triad and physical/logical/management security.
- **Week 5**

  Focus: Security operations Learn encryption basics, including public/private keys and hashing. Grasp core security principles, such as the CIA triad and physical/logical/management security. Operations center, incident response, backup and recovery, and contingency planning and testing
- **Week 6**

  Focus: Tying it all together. Work on ocumenting issues, reporting, planning, and best practices. Work on using live exercises tied to exam questions and security officer responsibilities

---

Cybersecurity Analyst (CySA+) Aligned Training ($1,000 USD)

This module continues with security technology fundamentals but uses that platform to move the student into the job of helping secure information systems by utilizing information assurance principles for government systems. This **intensive, lab heavy,**

instructor-led six-week course is built for individuals with prior computer, network, or helpdesk experience who want to develop in-demand cybersecurity analysis skills. Dive deep into the techniques used by security professionals to defend against modern cyber threats.

This class takes a multifaceted approach that combines network traffic analysis, process monitoring, endpoint detection, and proactive threat hunting. Analysts must develop a deep understanding of their organization's normal behaviors to spot anomalies that may indicate malicious activities. Utilizing tools like SIEM and EDR enhances detection capabilities, while structured threat hunting methodologies empower analysts to actively seek out potential threats before they can cause harm.

You'll master critical skills in behavioral analytics, threat intelligence gathering, robust vulnerability management, and effective incident response strategies. This advanced training qualifies you for specialized roles such as Cybersecurity Analyst, Security Analyst, and Information Security Analyst.

- **Week 1:**
  ***Focus*: Review cybersecurity terminology and revisit internet/network security concepts to understand their application in ISSO roles. Learn how to confidently interpret network diagrams.**
- **Week 2:**
  ***Focus*: Cybersecurity analysts focus on recognizing malicious activities within network communications.** Study access control protection (passwords, tokens, MFA) and advanced cryptography (steganography, data infiltration/exfiltration).
- **Week 3:**
  ***Focus*: Spotlight on Process Anomalies, Process injection, Process Masquerading Alerts, Registry Modification Analysis,** Learn to interpret security policies and contingency planning, including Business Impact Analysis (BIA) and recovery technologies like backups.

- **Week 4:**
  Focus: Endpoint Detection and Response (EDR), Script Execution Analysis, Behavioral Correlation and Application Logs, Web Server Log Analysis. Dive into effective incident response strategies.
- **Week 5**

  Focus: SQL Injection Detection, XSS Detection, Leveraging SIEM for Threat Detection, Log aggregation, and **Proactive Threat Hunting,**
- **Week 6**

  Focus: Hypothesis-driven investigations, Threat Intelligence-Based Hypotheses, Behavioral Analysis Hypotheses

---

Certified Information Systems Auditor (CISA) course ($1,000 USD)

The Certified Information Systems Auditor (CISA) course represents the pinnacle of our Victrics learning pathway. As a Security Auditor, you'll evaluate information systems against rigorous standards such as NIST SP 800-53A, conducting objective assessments that identify security gaps and vulnerabilities.

This module takes the ISSO training, security controls assessor, PCI auditing and all that you know so far and will use that knowledge to evaluate IT systems against the criteria found in the NIST SP 800-53A; this is the assessment companion to the NIST SP 800-53 used by the ISSO's. Due to FISMA, all government IT systems must be evaluated (assessed) and accredited (authorized). Preparing the system for this evaluation is the job of the ISSO.

You'll learn to clearly document findings, communicate risks to stakeholders, and provide actionable recommendations that help organizations strengthen their security posture and maintain compliance with regulatory requirements.

This **six-week instructor-led course** requires completion of our earlier courses or substantial equivalent experience in cybersecurity analysis.

Evaluating the information system is the job of the security control assessor. This module will leverage the previous module skills development in security plan writing and interpreting agency IT policies. However, this module will be ***heavy*** on “relearning” on how to read and write.

- **Week 1**
  Focus: Understand the role of SCAs and how to evaluate IT systems using NIST SP 800-53A. Learn how to assess system controls based on ISSO-prepared plans.
- **Week 2**
  Get hands-on with NIST SP 800-53 controls. Practice writing Systems Security Plans (SSPs) for Major Applications (MA) and General Support Systems (GSS).
- **Week 3**

  Focus: Hone skills in reading and interpreting guidance, requesting artifacts, and synthesizing findings into Security Assessment Reports (SARs) and Accreditation Letters.
  .
- **Week 4**
  Focus: Learn the major auditing frameworks; NIST, ISO, and PCI

- **Week 5**

Focus: Build effective communication and interviewing skills. Learn to collaborate with SMEs, eliminate unnecessary noise, and focus on pertinent details during evaluations

- **Week 6**

  Focus: Transition into job preparation. Learn to interpret job boards, tailor resumes, and rebrand yourself for roles in IT security.

This breakdown clearly identifies the focus of each week across the four modules and ensures structured, progressive learning.