CompTIA Security+ SY0-701 Exam Prep

UWF CyberSkills2Work

Offered by the University of West Florida Center for Cybersecurity

Cyber Defense Analyst Pathway

Course Overview

Dates: March 9 – May 8, 2026

Length of Completion: 40 contact hours

Prerequisites: Recommended (CompTIA) minimum 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts and networking.

Recommended Schedule: 8 weeks instruction | 1 week testing

Learning Setting: Hybrid Asynchronous Online / Instructor-led Zoom sessions

Target Audience: Individuals seeking entry-level to mid-career cybersecurity role.

DoD 8140.03M Compliance: Approved for the following Cyberspace Workforce Element, Cybersecurity Workforce roles: Cyber Defense Analyst (511), Cyber Defense Infrastructure Support Specialist (521), Cyber Defense Incident Responder (531), Vulnerability Assessment Analyst (541).

Level of instruction: upper division undergraduate; suitable for master's-level graduate

Type of Instruction per Week: Material covers at least 5 lessons per week; lectures (live & recorded), reading 40-50 pages of condensed, technical information per week, 5-6 hands-on labs, 2-4 activities, quizzes, and reviews)

Commitment Required: **Minimum effort is 20 hours per week** for students with either 2 years on-the-job experience; completed bachelor's degree in IT or cybersecurity, or 600+ hours of structured, hands-on technical training. **Entry-level students can expect 30 hours+**

No-Show / Fail to Persist

Students receive a temporary, two-week access code to CertMaster Learn+Labs on the first day of class. Students who complete all of the required assignments will be given a permanent access code for the duration of the course. Students who fail to meet this requirement may be performance dropped from the class. Students who do not login during the first two days of class or login and do not complete any of the required assignments shall be declared as "no-shows" for the course and performance dropped.

STUDENTS ARE REQUIRED TO TAKE THE CERTIFICATION EXAM

Course Instructor

Instructor	Email Address
Guy Garrett, M.S., M.B.A.	ggarrett@uwf.edu

Course Description

Prepare to pass the Security+ (SY0-701) exam and step confidently into a cyber defense role. This course delivers focused, hands-on training built around real-world tasks and CompTIA's updated exam objectives. You'll get what you need to succeed on test day—and in the field.

What is Sec+?

Sec+ is a global industry certification, compliant with ISO 17024, that validates the foundational cybersecurity skills necessary to perform core security functions and pursue an IT security career. Security+ establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.

What should a successful candidate know and be able to do?

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

CompTIA Exam Objectives

The table below lists the domains measured by this examination and the extent to which they are represented.

Domain #	Domain	% Weight on Exam
1	General Security Concepts	12
2	Threats, Vulnerabilities, and Mitigations	22
3	Security Architecture	18
4	Security Operations	28
5	Security Program Management & Oversight	20

Certification Test Details

Required exam	SY0-701
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes

DCWF Mapping

This course aligns to the Department of Defense Cyber Workforce Framework per DoD Directive 8140.01 as follows:

Workforce Element: Cybersecurity

Work Role: Cyber Defense Analyst
Work Role ID: 511 (NIST: PR-DA-001)

Core KSATs
** Required for every work role. Other Core KSATs are work role specific.*

KSAT ID	*Description*	*KSAT*
19	*Knowledge of cyber defense and vulnerability assessment tools, including open-source tools, and their capabilities.*	*Knowledge*
22	** Knowledge of computer networking concepts and protocols, and network security methodologies.*	*Knowledge*
59A	*Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.*	*Knowledge*
66	*Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.*	*Knowledge*
70	*Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).*	*Knowledge*
81A	*Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.*	*Knowledge*
87	*Knowledge of network traffic analysis methods.*	*Knowledge*
92	*Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open*	*Knowledge*

KSAT ID	Description	KSAT
	System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	
108	** Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).*	*Knowledge*
150	*Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.*	*Knowledge*
214A	*Skill in performing packet-level analysis.*	*Skill*
433	*Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.*	*Task*
823	*Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.*	*Task*
895	*Skill in recognizing and categorizing types of vulnerabilities and associated attacks.*	*Skill*
958	*Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.*	*Task*
959	*Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.*	*Task*
984	*Knowledge of cyber defense policies, procedures, and regulations.*	*Knowledge*
990	*Knowledge of the common attack vectors on the network layer.*	*Knowledge*
991	*Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).*	*Knowledge*
1069A	*Knowledge of general kill chain (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).*	*Knowledge*
1111	*Identify applications and operating systems of a network device based on network traffic.*	*Task*
1157	** Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.*	*Knowledge*

KSAT ID	Description	KSAT
1158	* Knowledge of cybersecurity principles.	Knowledge
1159	* Knowledge of cyber threats and vulnerabilities.	Knowledge
6900	* Knowledge of specific operational impacts of cybersecurity lapses.	Knowledge
6935	* Knowledge of cloud computing service models Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).	Knowledge
6938	* Knowledge of cloud computing deployment models in private, public, and hybrid environment and the difference between on-premises and off-premises environments.	Knowledge

Additional KSATs

KSAT ID	Description	KSAT
3C	Skill in recognizing vulnerabilities in information and/or data systems.	Skill
8	Knowledge of authentication, authorization, and access control methods.	Knowledge
21	Knowledge of computer algorithms.	Knowledge
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	Knowledge
27	Knowledge of cryptography and cryptographic key management concepts.	Knowledge
43A	Knowledge of embedded systems.	Knowledge
49	Knowledge of host/network access control mechanisms (e.g., access control list).	Knowledge
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Knowledge

KSAT ID	Description	KSAT
61	Knowledge of incident response and handling methodologies.	Knowledge
63	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Knowledge
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	Knowledge
88B	Knowledge of new and emerging control systems technologies.	Knowledge
90	Knowledge of operating systems.	Knowledge
95A	Knowledge of penetration testing principles, tools, and techniques.	Knowledge
98	Knowledge of policy-based and risk adaptive access controls.	Knowledge
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Knowledge
110	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Knowledge
111	Knowledge of security system design tools, methods, and techniques.	Knowledge
130A	Knowledge of systems security testing and evaluation methods.	Knowledge
139	Knowledge of the common networking protocols (e.g., TCP/IP), services (e.g., web, mail, Domain Name Server), and how they interact to provide network communications.	Knowledge
148	Knowledge of Virtual Private Network (VPN) security.	Knowledge
175	Skill in developing and deploying signatures.	Skill
177B	Knowledge of countermeasures for identified security risks.	Knowledge
179A	Skill in assessing security controls based on cybersecurity principles and tenets.	Skill

KSAT ID	Description	KSAT
181A	Skill in detecting host and network-based intrusions via intrusion detection technologies.	Skill
199	Skill in evaluating the adequacy of security designs.	Skill
212A	Knowledge of network mapping and recreating network topologies.	Knowledge
233	Skill in using protocol analyzers.	Skill
234B	Knowledge of the use of sub-netting tools.	Knowledge
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup).	Knowledge
277	Knowledge of defense-in-depth principles and network security architecture.	Knowledge
278	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	Knowledge
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	Knowledge
342A	Knowledge of operating system command line/prompt.	Knowledge
593A	Assess adequate access controls based on principles of least privilege and need-to-know.	Task
717A	Assess and monitor cybersecurity related to system implementation and testing practices.	Task
992C	Knowledge of threat environments (e.g., first generation threat actors, threat activities).	Knowledge
1033	Knowledge of basic system administration, network, and operating system hardening techniques.	Knowledge
1034A	Knowledge of Personally Identifiable Information (PII) data security standards.	Knowledge
1034B	Knowledge of Payment Card Industry (PCI) data security standards.	Knowledge
1034C	Knowledge of Personal Health Information (PHI) data security standards.	Knowledge

KSAT ID	Description	KSAT
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	Knowledge
1072	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Knowledge
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Knowledge
1103	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Task
1104	Examine network topologies to understand data flows through the network.	Task
1111	Identify applications and operating systems of a network device based on network traffic.	Task
1113	Identify network mapping and operating system (OS) fingerprinting activities.	Task
1114	Knowledge of encryption methodologies.	Knowledge
1119	Knowledge of signature implementation impact.	Knowledge
1120	Ability to interpret and incorporate data from multiple tool sources.	Ability
1121	Knowledge of Windows/Unix ports and services.	Knowledge
1142	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Knowledge
3431	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Knowledge
3461	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	Knowledge

KSAT ID	Description	KSAT
6210	Knowledge of cloud service models and possible limitations for an incident response.	Knowledge

GRADING

Course completion: All assigned work through week 6 (This is not sufficient to pass your exam).
Grading Scale: 0-100% with points given for correct answers/tasks.
Penalties: This course has no additional penalties for late work.
Incomplete assignments: Receive an automatic grade of 0.

Course Details

Materials & Resources

- Canvas Learning Management System
  - Primary tool for assigning work, recording grades.
  - Built-in email system for use by students and faculty.
- CertMaster Perform (access to CertMaster Learn+Labs)
  - Official online learning platform with student assignments.
  - Official CompTIA eBook. PDF version of the official exam guide.
- CertMaster Practice
  - Online, interactive testing platform used for review.
- Zoom
  - Used for faculty-student meetings.

Course Outline
Each week covers 2 lessons and multiple exam objectives.

Week	Lessons	CompTIA Objectives
1	01A Security Concepts 01B Security Controls 02A Threat Actors 02B Attack Surface 02C Social Engineering	1.2 1.1 2.1 2.2 2.2
2	03A Cryptographic Algorithms 03B Public Key Infrastructure 03C Cryptographic Solutions 04A Authentication 04B Authorization	1.4 1.4 1.4 4.6 4.6

	04C Identity Management	4.6
3	05A Enterprise Network Architecture 05B Network Security Appliances 05C Secure Communications 06A Cloud Infrastructure 06B Embedded Systems & Zero-Trust Architecture	3.1, 3.2 3.2 3.2 3.1, 3.2 1.2, 3.1
4	07A Asset Management 07B Redundancy Strategies 07C Physical Security 08A Device & OS Vulnerabilities 08B Application & Cloud Vulnerabilities 08C Vulnerability Identification Methods 08D Vulnerability Analysis & Remediation	3.4, 4.2 1.2, 3.4 1.2 2.3 2.3 4.3 4.3
5	09A Network Security Baselines 09B Network Security Capability Enhancement 10A Implement Endpoint Security 10B Mobile Device Hardening	4.1, 4.5 4.5 2.5, 4.1, 4.5 4.1
6	11A Application Protocol and Cloud Vulnerabilities 11B Cloud & Web Application Security Concepts 12A Incident Response 12B Digital Forensics 12C Data Sources 12D Alerting & Monitoring Tools	4.5 4.1 4.8 4.8 4.9 4.4
7	13A Malware Attack Indicators 13B Physical & Network Attack Indicators 13C Application Attack Indicators 14A Policies, Standards, & Procedures 14B Change Management 14C Automation & Orchestration	2.4 2.4 2.4 5.1 1.3 4.7
8	15A Risk Management Processes & Concepts 15B Vendor Management Concepts 15C Audits & Assessments 16A Data Classification and Compliance 16B Personnel Policies	5.2 5.3 5.5 3.3, 5.4 5.6
9	**Exam Week**	**ALL**