



**TECKYGUYS  
ACADEMY**

# CYBERSECURITY

## PATHWAY GUIDE

PREPARED BY: CHROME TECH LLC

**2026 EDITION**

A practical pathway for beginners, career changers, working professionals and experienced technicians.



[www.teckyguy.com](http://www.teckyguy.com)



[info@teckyguy.com](mailto:info@teckyguy.com)

## ABOUT THIS GUIDE

# Welcome to the Cybersecurity Pathway

This standalone guide explains the curriculum, controlled laboratories, assessments, awards and career preparation for all three levels of the TeckyGuys Academy Cybersecurity Pathway.

## What this guide covers

1. Level 1 — Cybersecurity Foundations
2. Level 2 — Security Operations & Threat Defense
3. Level 3 — Advanced Cyber Defense & Ethical Security (planned advanced delivery)
4. Required Cisco Networking Academy courses at each level
5. TeckyGuys practical training, simulations, evidence and assessments
6. Program formats, credentials, certification direction and career opportunities

## What this guide does not replace

- The TeckyGuys Academy Catalog and Student Handbook
- The student's written enrollment agreement and program offer
- Current Cisco course, examination or professional-certification requirements
- Employer-specific experience, screening or work-authorization requirements

**IMPORTANT :** Course access, schedules, included services and Level 3 availability must be confirmed in writing for the applicable enrollment period.

## NAVIGATION

# Contents

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>Welcome to the Cybersecurity Pathway.....</b>             | <b>2</b>  |
| What this guide covers.....                                  | 2         |
| What this guide does not replace.....                        | 2         |
| <b>SECTION 1 .....</b>                                       | <b>5</b>  |
| <b>Pathway Overview .....</b>                                | <b>5</b>  |
| 1.1. Who this pathway is for .....                           | 6         |
| 1.2. Training approach .....                                 | 6         |
| <b>SECTION 2 .....</b>                                       | <b>7</b>  |
| <b>Pathway Learning Outcomes .....</b>                       | <b>7</b>  |
| <b>SECTION 3 .....</b>                                       | <b>8</b>  |
| <b>Three-Level Architecture and Entry Requirements .....</b> | <b>8</b>  |
| 3.1. Direct entry .....                                      | 8         |
| 3.2. Normal progression.....                                 | 8         |
| <b>LEVEL 1.....</b>                                          | <b>9</b>  |
| 3.3. Cybersecurity Foundations .....                         | 9         |
| 3.3.1. Introduction to Cybersecurity.....                    | 9         |
| 3.3.2. Cybersecurity Essentials .....                        | 10        |
| 3.3.3. TeckyGuys Foundational Laboratory Program .....       | 11        |
| 3.3.4 Evidence portfolio.....                                | 11        |
| 3.3.5 Practical Assessment.....                              | 12        |
| 3.3.6 Assessment dimensions.....                             | 12        |
| 3.3.7 Completion, Recognition and Progression .....          | 13        |
| <b>LEVEL 2.....</b>                                          | <b>13</b> |

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| 3.4. Security Operations & Threat Defense .....                         | 13        |
| 3.4.1. Endpoint Security .....                                          | 14        |
| 3.4.2. Network Defense .....                                            | 15        |
| 3.4.3. Cyber Threat Management .....                                    | 16        |
| 3.4.4. CyberOps Associate .....                                         | 16        |
| 3.4.5. Defensive-Security Laboratory Program .....                      | 17        |
| 3.4.6. Simulated Security Operations Center Exercise .....              | 18        |
| 3.4.7. Defensive-Security Capstone .....                                | 19        |
| 3.4.8. Completion, Recognition and Progression .....                    | 20        |
| <b>LEVEL 3 .....</b>                                                    | <b>20</b> |
| 3.5. Advanced Cyber Defense & Ethical Security .....                    | 20        |
| 3.5.1. Ethical Hacker .....                                             | 21        |
| 3.5.2. Advanced CyberOps or Current Advanced Cyber-Defense Course ..... | 22        |
| 3.5.3. Advanced Controlled Laboratory Program .....                     | 23        |
| 3.5.4. Ethics, Authorization and Safe Practice .....                    | 24        |
| 3.5.5. Advanced Capstone, Completion and Award .....                    | 24        |
| <b>SECTION 4 .....</b>                                                  | <b>26</b> |
| <b>Tools and Laboratory Resources .....</b>                             | <b>26</b> |
| 4.1. Use conditions .....                                               | 26        |
| <b>SECTION 5 .....</b>                                                  | <b>27</b> |
| <b>Program Formats and Student Journey .....</b>                        | <b>27</b> |
| 5.1. Typical progression .....                                          | 27        |
| <b>SECTION 6 .....</b>                                                  | <b>28</b> |
| <b>Assessment Evidence, Credentials and Awards .....</b>                | <b>28</b> |
| <b>6.1. Evidence students may produce .....</b>                         | <b>28</b> |
| <b>SECTION 7 .....</b>                                                  | <b>29</b> |

Career Preparation and Opportunities ..... 29

7.1. Career-readiness evidence ..... 29

SECTION 8 ..... 30

Student Readiness and Next Steps ..... 30

SECTION 1

Pathway Overview

*Preparing students to identify risk, protect systems, analyze evidence and support responsible incident response.*

The pathway combines official Cisco Networking Academy coursework with instructor-led practice, controlled security laboratories, simulated workplace scenarios, log and network-traffic analysis, practical assessments, technical documentation and professional development.

## 1.1. Who this pathway is for

- Beginners entering cybersecurity
- IT support, help-desk, networking and data center technicians
- Junior security professionals and SOC candidates
- Career changers entering technical roles
- Professionals preparing for cybersecurity certification
- Business and technical professionals responsible for protecting systems or information

## 1.2. Training approach

Cisco courses provide the structured academic curriculum. TeckyGuys adds guided practical experience, assessment, documentation, feedback and career preparation so students apply that curriculum within realistic but legally controlled environments.

**AUTHORIZED USE ONLY** Every security activity must remain within an approved laboratory, assigned account and documented scope. Training never authorizes access to an external system.

## SECTION 2

### Pathway Learning Outcomes

| Domain                                                                                                                                                                                                | Student capability                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Security foundations                                                                                                                                                                                  | Explain common threats, vulnerabilities, risks, controls and ethical responsibilities.         |
| Endpoint defense                                                                                                                                                                                      | Review approved Windows and Linux security information and recognize suspicious activity.      |
| Network defense                                                                                                                                                                                       | Interpret network evidence and explain segmentation, access-control and monitoring concepts.   |
| Security operations                                                                                                                                                                                   | Review alerts, logs and telemetry; establish priority; and follow defined workflows.           |
| Threat analysis                                                                                                                                                                                       | Identify indicators, develop timelines and distinguish supported findings from assumptions.    |
| Incident response                                                                                                                                                                                     | Recommend authorized containment, escalation and response actions appropriate to the level.    |
| Risk communication                                                                                                                                                                                    | Document technical findings, business impact, evidence limitations and remediation priorities. |
| Professional practice                                                                                                                                                                                 | Protect information, maintain authorization boundaries and communicate responsibly.            |
| <b>PROGRESSIVE DEPTH</b> Expected technical complexity and independence increase at each level. Foundation completion does not substitute for advanced course, laboratory or assessment requirements. |                                                                                                |

## SECTION 3

### Three-Level Architecture and Entry Requirements

| Level   | Entry position                                                             | Primary outcome                                                                       |
|---------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Level 1 | Open to beginners; basic computer literacy is recommended.                 | Security awareness, basic defensive investigation and CCST Cybersecurity preparation. |
| Level 2 | Level 1, CCST Cybersecurity, or approved equivalent knowledge.             | Junior defensive-security and SOC preparation.                                        |
| Level 3 | Level 2, CyberOps Associate, or approved equivalent operations experience. | Advanced cyber-defense and authorized ethical-security preparation.                   |

#### 3.1. Direct entry

TeckyGuys reviews direct-entry requests using previous education, certification, professional experience and, where required, a readiness assessment. Direct entry does not waive the completion requirements of the level entered.

#### 3.2. Normal progression

2. Build security foundations and pass the Level 1 incident-review assessment.
3. Complete the defensive-security sequence, SOC simulation and Level 2 capstone.
4. After activation, complete the advanced courses and controlled Level 3 capstone.

**LEVEL 3 STATUS** Level 3 opens only after TeckyGuys confirms Cisco course access, qualified instructors, laboratory readiness, safe exercise environments and supervision procedures.

# LEVEL 1

## 3.3. Cybersecurity Foundations

Level 1 develops the knowledge required to understand cyber threats, protect devices and information, recognize suspicious activity and apply basic defensive-security practices.

| Component                                                                                                                                       | Requirement                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Cisco curriculum                                                                                                                                | Introduction to Cybersecurity and Cybersecurity Essentials                 |
| Practical work                                                                                                                                  | Approved Windows, Linux, network-traffic and threat-awareness laboratories |
| Evidence                                                                                                                                        | Analysis worksheets, observations, incident tickets and escalation records |
| Final assessment                                                                                                                                | Foundational review of a simulated security incident                       |
| Award                                                                                                                                           | TeckyGuys Academy Cybersecurity Foundations Award                          |
| Certification direction                                                                                                                         | Preparation for the separate CCST Cybersecurity examination                |
| <b>ENTRY</b> Previous cybersecurity experience is not required. Basic computer literacy, ethical judgment and consistent practice are expected. |                                                                            |

### 3.3.1. Introduction to Cybersecurity

Introduces why cybersecurity matters to individuals and organizations and how common threats affect accounts, devices, services and information.

#### Core knowledge and skills

- Personal and organizational information security
- Common cyber threats, malware and attacks
- Vulnerabilities and security weaknesses

- Social-engineering methods
- Protection of accounts, devices and data
- Cybersecurity laws, ethics and career opportunities

### Applied learning

- Classify example threats and likely impacts
- Review a simulated phishing message
- Recommend account and device protections
- Document when escalation is required

**LEARNING FOCUS :** Students learn that curiosity and technical ability must always operate within legal and ethical boundaries.

### 3.3.2. Cybersecurity Essentials

Builds the technical vocabulary and defensive concepts needed for continued cybersecurity study and entry-level support.

#### Core knowledge and skills

- Threats, vulnerabilities and risk
- Endpoint and network-security fundamentals
- Authentication and access control
- Cryptography fundamentals
- Security monitoring and incident-response concepts
- Governance, policies and professional responsibilities

#### Applied learning

- Review approved endpoint and account settings
- Interpret basic system or security information
- Observe network traffic in an approved environment
- Prepare a concise risk or incident record

**LEARNING FOCUS :** The course provides a foundation; students must still demonstrate practical judgment through TeckyGuys activities.

### 3.3.3. TeckyGuys Foundational Laboratory Program

| Laboratory domain   | Required activities                                                                          |
|---------------------|----------------------------------------------------------------------------------------------|
| Threat recognition  | Identify phishing, social engineering, malware indicators and common security weaknesses.    |
| Account protection  | Review passwords, multifactor authentication, users and permissions.                         |
| Endpoint awareness  | Observe approved Windows and Linux security settings and file protections.                   |
| Event review        | Use Windows Event Viewer fundamentals and interpret selected security information.           |
| Traffic observation | Use Wireshark to observe approved network traffic and basic protocol behavior.               |
| Threat intelligence | Use approved VirusTotal resources and document limitations responsibly.                      |
| Documentation       | Prepare risk notes, incident tickets, escalation records and recommended protective actions. |

### 3.3.4 Evidence portfolio

- Threat-classification worksheet
- Phishing-analysis record
- Endpoint or account-security checklist
- Event or traffic observation notes
- Risk and vulnerability summary

- Incident ticket and escalation note

**LAB BOUNDARY :** Students may use only assigned systems, files, accounts and data. Unauthorized scanning, credential use or testing is prohibited.

### 3.3.5 Practical Assessment

Every Level 1 student completes a foundational review of a simulated security incident.

#### The student must

- Identify the affected user, device or service.
- Recognize the potential threat, vulnerability or unsafe behavior.
- Collect only approved evidence and review relevant basic information.
- Recommend reasonable protective actions within assigned authority.
- Escalate conditions requiring greater access or expertise.
- Prepare a clear incident record and explain the ethical considerations.

### 3.3.6 Assessment dimensions

| Dimension     | Evidence of performance                                                |
|---------------|------------------------------------------------------------------------|
| Recognition   | Correctly identifies likely risk and affected assets.                  |
| Investigation | Uses approved information and distinguishes evidence from assumptions. |
| Judgment      | Recommends proportionate action and escalates appropriately.           |
| Documentation | Creates an accurate, clear and usable incident record.                 |
| Conduct       | Protects information and remains within authorization boundaries.      |

### 3.3.7 Completion, Recognition and Progression

#### Completion requirements

- Complete both required Cisco courses
- Complete the required TeckyGuys laboratories and evidence portfolio
- Pass the Level 1 practical assessment
- Meet attendance, participation, conduct and academic-integrity standards
- Follow all authorization and ethical-use requirements
- Resolve applicable academic and administrative requirements

#### Eligible recognition

- Applicable Cisco Networking Academy course-completion certificates
- Applicable Cisco digital badges
- TeckyGuys Academy Cybersecurity Foundations Award

#### Recommended next steps

- Strengthen Windows, Linux and networking fundamentals.
- Prepare separately for the CCST Cybersecurity examination, if desired.
- Progress to Level 2 for security operations and threat-defense practice.

**CERTIFICATION DISTINCTION :** The TeckyGuys award and Cisco course certificates are not the CCST Cybersecurity professional certification. The certification requires a separate provider-controlled examination.

## LEVEL 2

### 3.4. Security Operations & Threat Defense

Level 2 moves students from security fundamentals into applied defensive-security operations. Students monitor systems, analyze logs and network activity, investigate alerts and support incident response within a simulated Security Operations Center.

| Component                                                                                                                                               | Requirement                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Cisco curriculum                                                                                                                                        | Endpoint Security, Network Defense, Cyber Threat Management and CyberOps Associate |
| Practical work                                                                                                                                          | Defensive-security laboratories and simulated SOC activities                       |
| Evidence                                                                                                                                                | Alert triage, timelines, analysis notes, tickets, reports and handovers            |
| Performance events                                                                                                                                      | SOC simulation and defensive-security capstone                                     |
| Award                                                                                                                                                   | TeckyGuys Academy Security Operations & Threat Defense Award                       |
| Professional direction                                                                                                                                  | Junior analyst, SOC and Cisco CyberOps-related preparation                         |
| <b>DEFENSIVE SCOPE :</b> Level 2 emphasizes monitoring, analysis, response support and evidence-based communication—not uncontrolled offensive testing. |                                                                                    |

### 3.4.1. Endpoint Security

Develops the ability to recognize endpoint threats, understand host protections and collect approved evidence for escalation.

#### Core knowledge and skills

- Endpoint threats and vulnerabilities
- Operating-system security
- User, account and host-based protection
- Malware behavior
- System hardening and security controls
- Endpoint monitoring, evidence collection and escalation

### Applied learning

- Review selected Windows and Linux events
- Analyze an endpoint alert
- Identify relevant users, processes or artifacts
- Prepare an evidence-based escalation

**LEARNING FOCUS :** Students must preserve evidence and avoid making unsupported changes to a suspected compromised system.

### 3.4.2. Network Defense

Explains how layered network controls help prevent, detect and contain malicious activity.

#### Core knowledge and skills

- Network threats and attack methods
- Defense-in-depth
- Firewalls, access control and segmentation
- Secure network architecture
- Intrusion detection and prevention
- VPN, network monitoring and defensive response procedures

### Applied learning

- Review an approved firewall or access-control scenario
- Analyze selected packet evidence
- Relate observed traffic to possible controls
- Document a proportionate defensive recommendation

**LEARNING FOCUS :** Configuration concepts are practiced only in approved simulations or assigned laboratory systems.

### 3.4.3. Cyber Threat Management

Connects threat intelligence, vulnerability management, risk, monitoring and incident-response processes.

#### Core knowledge and skills

- Threat intelligence and indicators
- Vulnerability and risk assessment
- Security monitoring and alert analysis
- Incident-response processes
- Digital-evidence awareness
- Policies, governance, compliance and threat reporting

#### Applied learning

- Research approved threat-intelligence sources
- Prioritize a set of vulnerabilities or alerts
- Develop an incident timeline
- Prepare technical and management-facing summaries

**LEARNING FOCUS :** The quality of a finding depends on evidence, context, confidence and clear communication of limitations.

### 3.4.4. CyberOps Associate

Develops knowledge and practical ability for entry-level Security Operations Center responsibilities.

#### Core knowledge and skills

- SOC roles and workflows
- Network and endpoint telemetry
- Security alerts, events and log analysis
- Network-traffic and threat investigation
- Incident-response procedures and evidence handling
- Playbooks, escalation, reporting and operational communication

## Applied learning

- Triage simulated alerts
- Correlate logs and network evidence
- Classify and prioritize an incident
- Prepare a shift handover and incident report

**LEARNING FOCUS :** Cisco may update course titles or structure. TeckyGuys may use a current approved equivalent while preserving published outcomes.

### 3.4.5. Defensive-Security Laboratory Program

| Laboratory domain    | Required activities                                                                    |
|----------------------|----------------------------------------------------------------------------------------|
| Logs and telemetry   | Review Windows and Linux logs, authentication events and endpoint alerts.              |
| Network evidence     | Capture and inspect approved traffic using Wireshark and related resources.            |
| SIEM fundamentals    | Use Splunk demonstrations or an approved equivalent for event search and correlation.  |
| Threat investigation | Review phishing, malicious-file indicators, intelligence and indicators of compromise. |
| Defensive controls   | Analyze firewall, access-control, segmentation and endpoint-protection scenarios.      |
| Incident workflow    | Classify, prioritize, timeline, document, escalate and hand over simulated incidents.  |

## Required evidence

- Alert-triage worksheet
- Log and packet-analysis notes
- Indicator and threat-intelligence record
- Incident timeline
- Containment or escalation recommendation
- Incident report and shift handover

**TOOLS :** Commercial, free, trial, demonstration or education editions may be used. Tool access does not require students to buy the provider's course or certification unless stated in writing.

### **3.4.6. Simulated Security Operations Center Exercise**

Students work individually or in an assigned team through a structured SOC scenario.

#### **3.4.6.1. Operational sequence**

- Receive and review assigned security alerts.
- Identify affected assets, accounts, users and services.
- Establish initial severity and priority.
- Collect relevant logs, telemetry and network evidence.
- Investigate indicators and distinguish likely incidents from false positives.
- Recommend approved containment or escalation actions.
- Document the investigation and prepare a shift handover.
- Present findings to the instructor or assessment panel.

#### **3.4.6.2. Professional behaviors assessed**

- Technical discipline
- Teamwork and role clarity
- Evidence preservation
- Clear operational communication
- Timely escalation
- Respect for privacy and authorization

**SIMULATION PURPOSE:** The exercise evaluates how students work through uncertainty—not simply whether they name a threat correctly.

### 3.4.7. Defensive-Security Capstone

The student reviews a simulated organizational environment and develops a supported incident conclusion.

#### Required performance

- Identify important systems, users, services and security risks
- Analyze assigned alerts, logs and network information
- Investigate suspicious endpoint or network activity
- Develop an incident timeline and identify possible attack methods
- Recommend proportionate containment, response and escalation actions
- Prepare a complete incident report
- Present and defend the findings

#### 3.4.7.1. Evaluation areas

| Technical                                                                                                                                             | Professional                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Monitoring, triage, log analysis, traffic analysis and investigation                                                                                  | Documentation, communication, teamwork, ethics and judgment          |
| Evidence correlation, timeline development and response recommendations                                                                               | Clear limitations, defensible conclusions and appropriate escalation |
| <b>EVIDENCE STANDARD</b> A strong capstone explains what the evidence supports, what remains uncertain and what authorized action should happen next. |                                                                      |

### 3.4.8. Completion, Recognition and Progression

#### Completion requirements

- Complete all four required Cisco courses
- Complete the defensive-security laboratories and required evidence
- Complete the SOC simulation
- Pass the Level 2 capstone
- Meet attendance, participation, conduct and academic-integrity standards
- Follow privacy, authorization and ethical-use requirements

#### Eligible recognition

- Applicable Cisco Networking Academy course-completion certificates
- Applicable Cisco digital badges
- TeckyGuys Academy Security Operations & Threat Defense Award

#### Progression

Graduates may pursue junior defensive-security or SOC opportunities, continue building experience and prepare separately for an applicable Cisco professional-certification examination. Qualified students may request Level 3 entry after it is activated.

**CERTIFICATION DISTINCTION** Completion does not automatically grant Cisco Certified CyberOps Associate or another professional certification.

## LEVEL 3

### 3.5. Advanced Cyber Defense & Ethical Security

Level 3 is the planned advanced stage of the pathway. It prepares qualified students to conduct deeper defensive investigations, analyze attacker behavior, assess controls and perform authorized ethical-security testing.

#### Activation requirements

- Access to the applicable official Cisco courses
- Qualified instructor availability
- Laboratory and cyber-range readiness
- Safe and legally controlled exercise environments
- Documented assessment and supervision procedures

### **Advanced learning purpose**

The program combines defensive and offensive perspectives so students understand how attacks occur and how organizations detect, contain and prevent them. It does not authorize testing, scanning, access or interference outside the written scope of an assigned exercise.

**PLANNED DELIVERY :** TeckyGuys will publish the exact Level 3 course titles, schedule and enrollment terms before accepting students.

## **3.5.1. Ethical Hacker**

Develops controlled practical knowledge of security testing under documented authorization and scope.

### **Core knowledge and skills**

- Ethical-hacking principles and professional ethics
- Legal authorization, scope and rules of engagement
- Reconnaissance and vulnerability discovery concepts
- Network and system assessment
- Web, application and wireless-security concepts
- Evidence, risk reporting and remediation recommendations

### **Applied learning**

- Interpret an authorization and scope statement

- Plan an approved assessment
- Validate assigned findings using controlled procedures
- Prepare technical and executive reports

**LEARNING FOCUS :** All activities remain inside TeckyGuys-approved systems and accounts under applicable supervision.

### 3.5.2. Advanced CyberOps or Current Advanced Cyber-Defense Course

Extends defensive operations into deeper threat analysis, hunting, detection and incident coordination.

#### Core knowledge and skills

- Threat hunting and advanced event analysis
- Endpoint and network telemetry
- Detection-engineering concepts
- Attack-pattern and malware-behavior analysis
- Security-automation concepts
- Incident coordination and operational reporting

#### Applied learning

- Develop and test a threat-hunting hypothesis
- Reconstruct a complex incident timeline
- Evaluate detection coverage
- Present a coordinated response recommendation

**LEARNING FOCUS :** The exact official Cisco title will be confirmed before Level 3 enrollment opens.

### 3.5.3. Advanced Controlled Laboratory Program

| Phase       | Required activities                                                                             |
|-------------|-------------------------------------------------------------------------------------------------|
| Plan        | Review written authorization, scope, assets, restrictions and rules of engagement.              |
| Discover    | Perform approved attack-surface review, scanning, enumeration and vulnerability identification. |
| Validate    | Use controlled procedures to validate findings and assess existing security controls.           |
| Investigate | Conduct advanced traffic, log, telemetry, threat-hunting and timeline analysis.                 |
| Respond     | Develop containment, recovery, detection and remediation recommendations.                       |
| Report      | Classify risk and prepare technical, executive and lessons-learned reports.                     |

#### Evidence portfolio

- Authorization and scope summary
- Assessment or investigation plan
- Evidence register
- Validated findings record
- Risk and remediation matrix
- Technical report
- Executive presentation

**CONTROLLED ENVIRONMENT :** These activities support the Cisco curriculum. They are not separate third-party certifications and do not create authority to test external systems.

#### 3.5.4. Ethics, Authorization and Safe Practice

##### **Before participating, every student must**

- Complete the applicable ethics and acceptable-use agreement
- Understand the written scope and rules of engagement
- Use only approved systems, accounts, tools and data
- Follow instructor directions and stop immediately when directed
- Protect credentials, evidence, personal information and confidential material
- Report unexpected access, exposure or system behavior
- Follow applicable laws, policies and professional standards

##### **Strictly prohibited**

- Unauthorized scanning, access, credential use or exploitation
- Disruption, persistence, data collection or interference outside scope
- Copying or distributing unauthorized tools, data or techniques
- Testing a live organization, customer or public target without documented permission

**CONSEQUENCES :** A serious violation may result in removal from the exercise or program and may be referred to the appropriate authority.

#### 3.5.5. Advanced Capstone, Completion and Award

##### **Capstone performance**

- Review the authorized assessment scope, assets and restrictions.
- Develop an approved assessment and investigation plan.
- Evaluate the assigned environment and analyze relevant evidence.
- Validate findings using approved procedures.

- Assess likelihood, impact and defensive significance.
- Recommend improvements and prepare technical and executive reports.
- Present and defend findings while demonstrating ethical compliance.

### **Completion requirements**

- Complete the published Cisco courses
- Complete advanced laboratories
- Pass the Level 3 capstone
- Meet participation and integrity standards
- Follow every legal, ethical and authorization requirement

### **Eligible recognition**

- Applicable Cisco course certificates and badges
- TeckyGuys Academy Advanced Cyber Defense & Ethical Security Award

**AWARD LIMIT :** The TeckyGuys award is not a Cisco professional certification, penetration-testing license or legal authorization to assess external systems.

## SECTION 4

### Tools and Laboratory Resources

| Purpose                        | Approved examples                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------|
| Network simulation and traffic | Cisco Packet Tracer and Wireshark                                                             |
| Endpoint and operating systems | Windows Event Viewer, Linux command-line tools and virtual machines                           |
| Security monitoring            | Splunk free, trial, demonstration or education resources; approved SIEM equivalents           |
| Threat analysis                | VirusTotal and approved threat-intelligence resources                                         |
| Network assessment             | Nmap demonstrations and approved vulnerability-assessment tools                               |
| Controlled practice            | Endpoint-security demonstrations, firewall simulations and TeckyGuys cyber-range environments |

#### 4.1. Use conditions

- Lawful educational purpose
- Approved laboratory environment
- Systems owned by the student or expressly authorized for assessment
- Applicable instructor supervision
- Provider terms and TeckyGuys policies

**RESOURCE NOTICE** Tools may change with technology, licensing and course requirements. Students are not required to purchase every tool demonstrated unless a written enrollment offer states otherwise.

## SECTION 5

### Program Formats and Student Journey

| Format                    | Cybersecurity pathway experience                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Self-Paced                | Assigned Cisco courses and stated TeckyGuys activities within the access period; does not automatically include the full laboratory, SOC simulation or career-support experience. |
| 12-Week Cohort            | One level with instructor sessions, guided labs, practical assignments, reviews, professional development and the applicable final assessment.                                    |
| 24-Week Career Transition | Level 1 plus Level 2, progressing from foundations into junior defensive-security and SOC responsibilities.                                                                       |
| Level 3 Advanced          | Separate planned delivery after course, instructor, laboratory and supervision requirements are confirmed.                                                                        |

#### 5.1. Typical progression

- Complete official coursework for the selected level.
- Practice inside approved environments and retain required evidence.
- Receive instructor feedback and correct deficiencies.
- Complete the applicable practical assessment, simulation or capstone.

- Receive eligible recognition and plan the next academic or career step.

**ENROLLMENT CONTROL** Only the format, services, tools and supports identified in the written enrollment offer are included.

## SECTION 6

### Assessment Evidence, Credentials and Awards

#### 6.1. Evidence students may produce

- Threat, phishing and vulnerability-analysis worksheets
- Endpoint, log and network-traffic investigation notes
- Alert-triage decisions and incident timelines
- Tickets, escalation records and shift handovers
- Technical and executive incident or assessment reports
- Presentations and capstone defense materials

| Recognition type                  | Meaning                                                                                                               |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Cisco course certificate or badge | Provider-issued recognition subject to Cisco course and platform requirements.                                        |
| TeckyGuys pathway-level award     | Academy recognition that the student met the published course, laboratory and assessment requirements for that level. |
| Professional certification        | A separate provider-controlled credential generally requiring an examination and current eligibility requirements.    |

| Recognition type                                                                                                                                                             | Meaning |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| <b>EXAMINATION COSTS</b> Professional-certification examinations, vouchers and retakes are separate unless expressly included in the student's written enrollment agreement. |         |

## SECTION 7

### Career Preparation and Opportunities

| After level | Illustrative role directions                                                                                                                       |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Level 1     | Cybersecurity or IT security support technician, junior security technician, information-security intern, cybersecurity apprentice.                |
| Level 2     | Junior cybersecurity analyst, junior SOC analyst, security-monitoring analyst, incident-response support, endpoint or network-security technician. |
| Level 3     | Cybersecurity analyst, SOC analyst, threat hunter, incident-response analyst, vulnerability-assessment analyst, junior ethical-security tester.    |

#### 7.1. Career-readiness evidence

- Accurate résumé and LinkedIn profile
- Ethically sanitized portfolio artifacts
- Clear explanation of tools, methods, evidence and limitations
- Interview examples demonstrating judgment, teamwork and escalation
- Certification and continued-learning plan

**CAREER NOTICE** Job titles and requirements differ by employer. Completion does not guarantee certification, internship, employment, promotion or salary, and does not by itself qualify a graduate for a senior or penetration-testing role.

## SECTION 8

### Student Readiness and Next Steps

**A successful cybersecurity student is prepared to**

- Study consistently and practice beyond scheduled instruction
- Build Windows, Linux and networking knowledge as needed
- Handle accounts, evidence and personal information responsibly
- Accept uncertainty and explain the limits of available evidence
- Follow scope, authorization, safety and ethical rules without exception
- Document work clearly and communicate professionally
- Continue learning as threats, tools and certification requirements change

**Before enrolling, confirm**

- Selected level and entry requirements
- Delivery format and schedule
- Included courses, laboratories, tools and support
- Tuition and additional expenses
- Computer and internet requirements
- Assessment and award requirements

**NEXT STEP :** Review the Academy Catalog and Student Handbook, then submit the official inquiry or application form for current availability.

# TECKYGUYS ACADEMY

Powered by Chrome Tech LLC

[www.teckyguy.com](http://www.teckyguy.com) | [info@teckyguy.com](mailto:info@teckyguy.com) | (737) 397-1127

**Explore your pathway. Develop practical skills. Prepare for opportunity.**