



Cybersecurity Awareness Month

30-Day Cybersecurity Challenge

Build real cyber skills in 30 days.

A daily, self-paced challenge for entry-to associate-level learners and Cisco certification holders.

Each day pairs ~20–60 minutes of learning with a hands-on or reflection task.

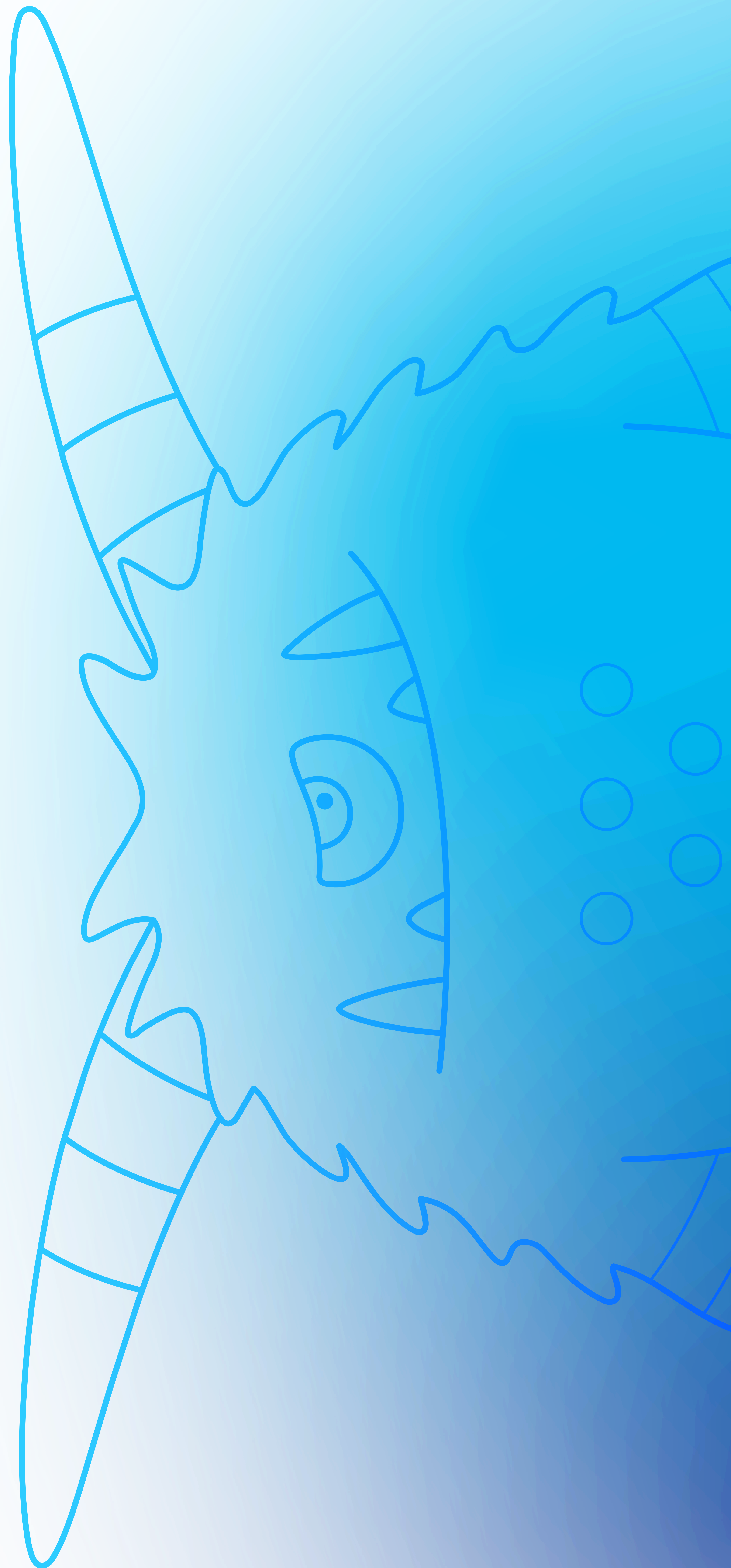
- ✓ **Commit to one day at a time.** Most days take 20–60 minutes. Use the notes section to track your progress for each week.
- ✓ **Learn → Do → Log.** Read/watch the resource, complete the task, and mark each completed day in your 🔥 Streak tracker.
- ✓ **Level up.** Beginners can stop at the core task; certification holders should do the ⚡ Stretch items.
- ✓ Follow us on social and share your progress using **#30DaysofCybersecurity**

Learn with Cisco

[X \(Formerly Twitter\)](#) | [Facebook](#) | [Threads](#) | [LinkedIn](#) | [Instagram](#) | [YouTube](#)

Cisco Networking Academy

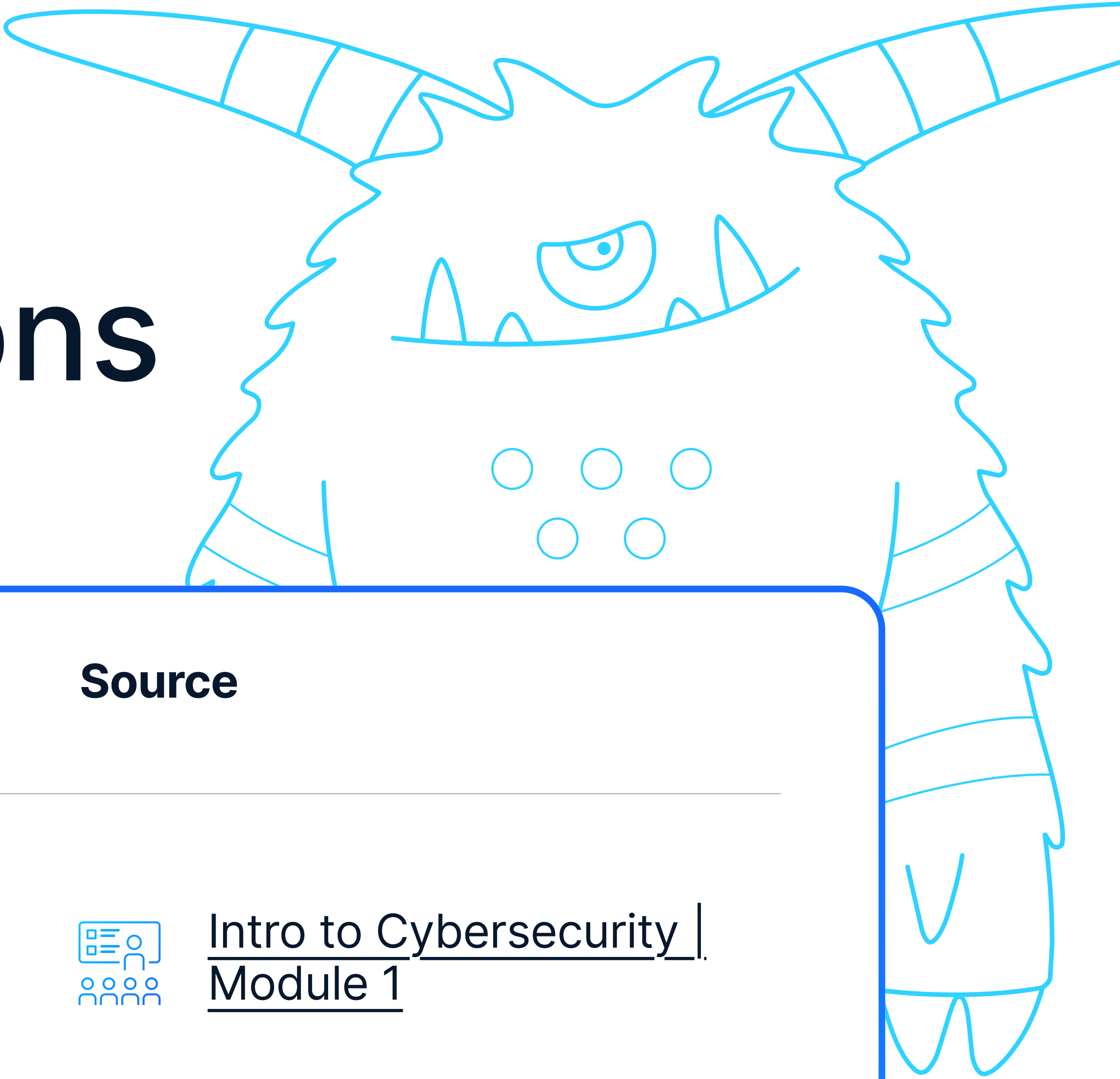
[X \(Formerly Twitter\)](#) | [Facebook](#) | [LinkedIn](#)

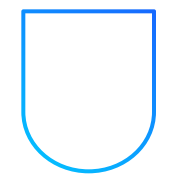
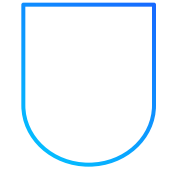
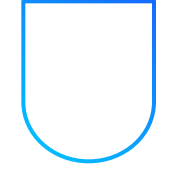
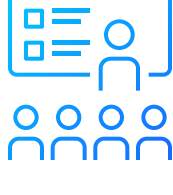




Week 1 — Security Foundations

Think like a defender: understand the threats before you stop them.



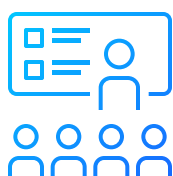
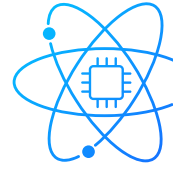
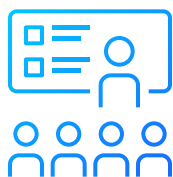
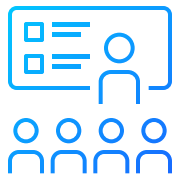
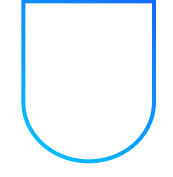
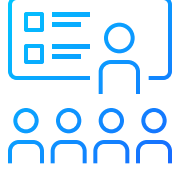
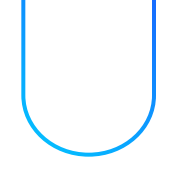
Day	Focus	Task	Source
1	Why Cybersecurity Matters	Enroll in and start Introduction to Cybersecurity . Complete Module 1 and note the three threats that surprised you.	 Intro to Cybersecurity Module 1
2	Threats & Attack Types	Study common threats , malware , and social engineering . Identify one phishing email in your inbox and list its red flags.	 Intro to Cybersecurity Module 2
3	The CIA Triad	Learn Confidentiality , Integrity , and Availability . Write one real-world example of each from your own org.	 Principles of the CIA Triad, Threat Intelligence, and Threat Hunting
4	Passwords & MFA	Audit your own accounts: enable multi-factor authentication on three critical accounts and switch one weak password to a passphrase.	 What is multi-factor authentication (MFA)?
5	Cryptography Basics	Learn hashing vs. encryption . Hash a sample file and verify its integrity. <i>Optional: Packet Tracer - Explore File and Data Encryption</i>	 Endpoint Security 10.1.14 Explore File and Data Encryption
6	Explore Cisco U.	Create a free Cisco U. account and browse a security tutorial or webinar. Bookmark one Learning Path.	 Cisco U.
7	Reflect & Plan	Review Week 1 notes. Pick a target Cisco credential: CCST , CCNA , CCNP , Cisco Certified Specialist , or Cisco Certificate in Ethical Hacking .	 Cisco Cybersecurity Certifications
	Stretch (cert holders)	Skim the 200-201 CCNACBR exam topics and rate yourself 1–5 on each domain.	

Notes:



Week 2 — Network & Endpoint Defense

Protect the devices and networks attackers target first.

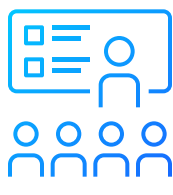
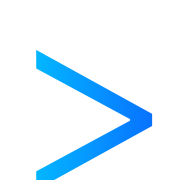
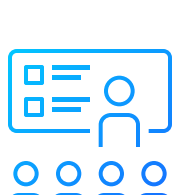
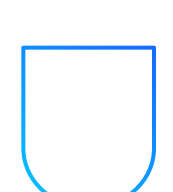
Day	Focus	Task	Source
8	Network Security 101	Learn how networks are defended, then practice hands-on: build a small topology in Cisco Modeling Labs (router, switch, 2 hosts) with basic segmentation.	 Endpoint Security Module 6  CMLLAB Learning Path
9	Defense in Depth	Map the layers of defense for one asset (data → app → host → network → perimeter).	 Network Defense Module 1
10	Endpoint Security	Start the Endpoint Security course. Complete the vulnerability assessment module.	 Endpoint Security Module 1
11	Harden a Network	Harden a network—learn how to monitor and protect your network and evaluate security alerts.	 Network Defense Module 2
12	Access Control	Read the chapter from the <i>CCST Cybersecurity 100-160 Official Cert Guide</i> to learn AAA and least-privilege models. Review permissions on one shared folder or app and remove excess access.	 Access Management
13	Wireless & Mobile	Is your Wi-Fi WPA3-ready? Study wireless and mobile attacks and audit your network.	 Endpoint Security Module 1
14	Access Control Lists	Extend your Cisco Modeling Labs topology: add a firewall/ACLs between segments, test allowed vs. blocked traffic, and log what broke and how you fixed it.	 CCNA: Configure Your First ACL
 Stretch (cert holders)		Perform a security review of your home lab or small network. Document: password policy, MFA status, guest Wi-Fi isolation, software update status, firewall settings, and device inventory. Identify three improvements you can implement immediately.	

Notes:



Week 3 — Security Operations & Threat Detection

Think like a SOC analyst: monitor, detect, investigate.

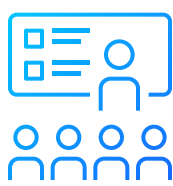
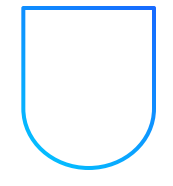
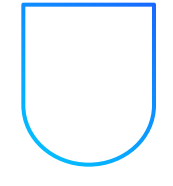
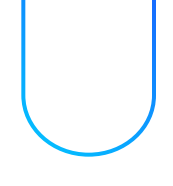
Day	Focus	Task	Source
15	Why You Should Learn Splunk	The demand for pros who know Splunk is increasing. Learn why Splunk skills matter for working with data from firewalls, endpoints, cloud services, and applications.	 Why You Should Learn Splunk in 2026
16	Security Monitoring	Learn what logs and telemetry matter. List five log sources you'd monitor first.	 Get Started with OCSF: Standardize Security Data Across Tools
17	Intro to SIEM	Take Intro to Splunk Security Essentials . Understand how detections and analytic stories work.	 Intro to Splunk Security Essentials
18	Hands-on SPL	Load the free Splunk BOTS dataset (or forward syslog from your CML devices) and run three searches (failed logins, top source IPs, suspicious processes).	 Boss of the SOC (BOTS) Dataset Version 3
19	Automate Response	Take Intro to Splunk SOAR . Sketch a simple playbook for a phishing alert.	 Splunk SOAR
20	Inside the SOC	Step inside the SOC. Complete the Security Operations and the Defense Analyst course to learn how analysts work.	 Security Operations and the Defense Analyst
21	Incident Response	Learn the IR lifecycle . Write a 1-page mini runbook for a malware infection.	 Cisco Talos Incident Response Services
 Stretch (cert holders)		Build a Splunk dashboard with three panels and one correlation search.	

Notes:

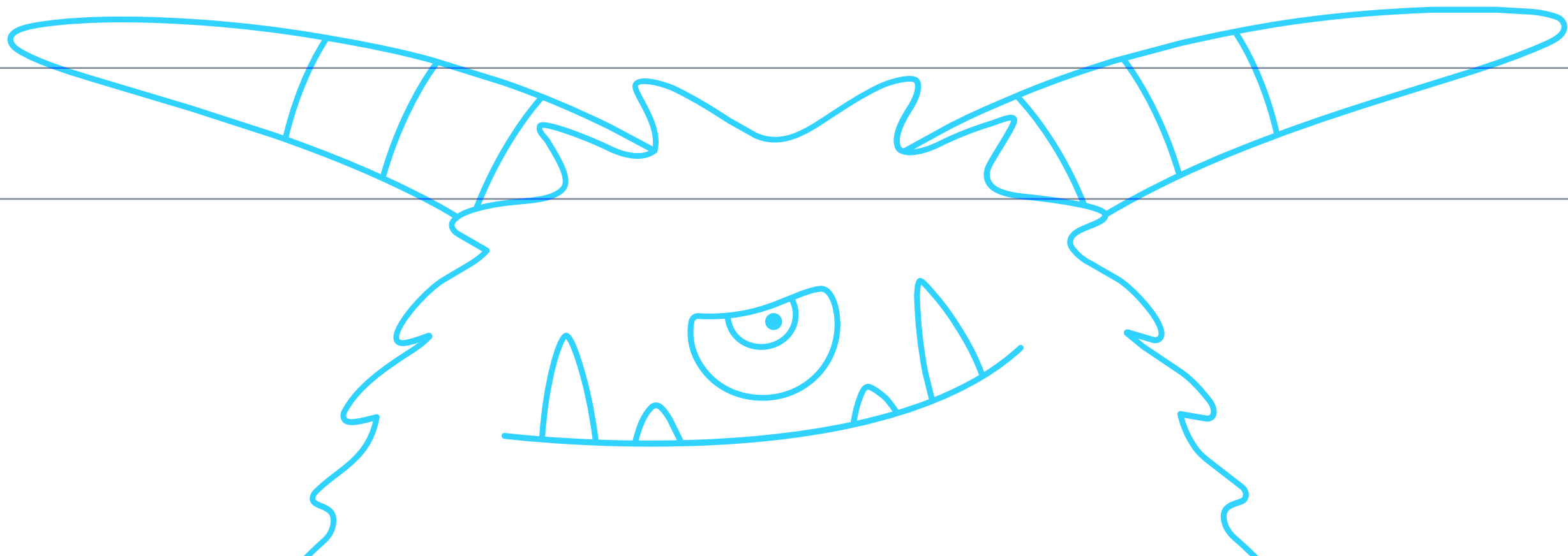


Week 4 — Offense, Cloud & Certification

Think like a SOC analyst: monitor, detect, investigate.

Day	Focus	Task	Source
22	Think Like an Attacker	Start the Ethical Hacker course. Complete the reconnaissance module.	 Ethical Hacker Module 1
23	Vulnerability Assessment	Run a scan against a device in your CML topology (or a VM you own) and triage the top three findings by risk.	 Ethical Hacker Module 3
24	Cloud & Zero Trust	Learn Secure Cloud Access and Zero Trust principles (users, devices, workloads). Read the chapter from <i>Zero Trust in Resilient Cloud and Network Architectures</i> .	 Zero Trust Network Deployment
25	AI & Security	Explore how AI is reshaping defense. Complete one Cisco U. AI tutorial and note one use case.	 Artificial Intelligence Cisco U.
26	Community	Sign into the Cisco Learning Network, follow the Cybersecurity Community, and ask or answer one question.	 Cybersecurity Certifications Community
27	Skill Assessment	Complete the stretch challenge from Week 1. (Already done? Re-rate yourself on each domain to assess your growth.)	 200-201 CCNACBR Exam Topics
28	Commit to a Credential	Commit to a Cisco certification. Build a study plan based on the credentials you explored on Day 7.	 Cisco Cybersecurity Certifications
		Stretch (cert holders)	Map today's controls to CCNP Security (350-701 SCOR) exam topics .

Notes:





Week 5 — Capstone & Next Steps

Day	Focus	Task	Source
29	Capstone	Pick one scenario (phishing, malware, or misconfig) and write an end-to-end response: detect → investigate (Splunk) → contain → remediate → report.	 Your week 1-4 notes  Splunk Free Courses
30	Celebrate Your Skills	You did it! Post your 🔥 Streak Tracker to social using #30DaysofCybersecurity . Then, leave a comment on two (or more) posts to show fellow cyber learners your support.	 #30DaysofCybersecurity

Additional resources

Build your cybersecurity career. Explore Cisco certifications, learning paths, free resources, and career guidance.

www.cisco.com/go/cybercerts



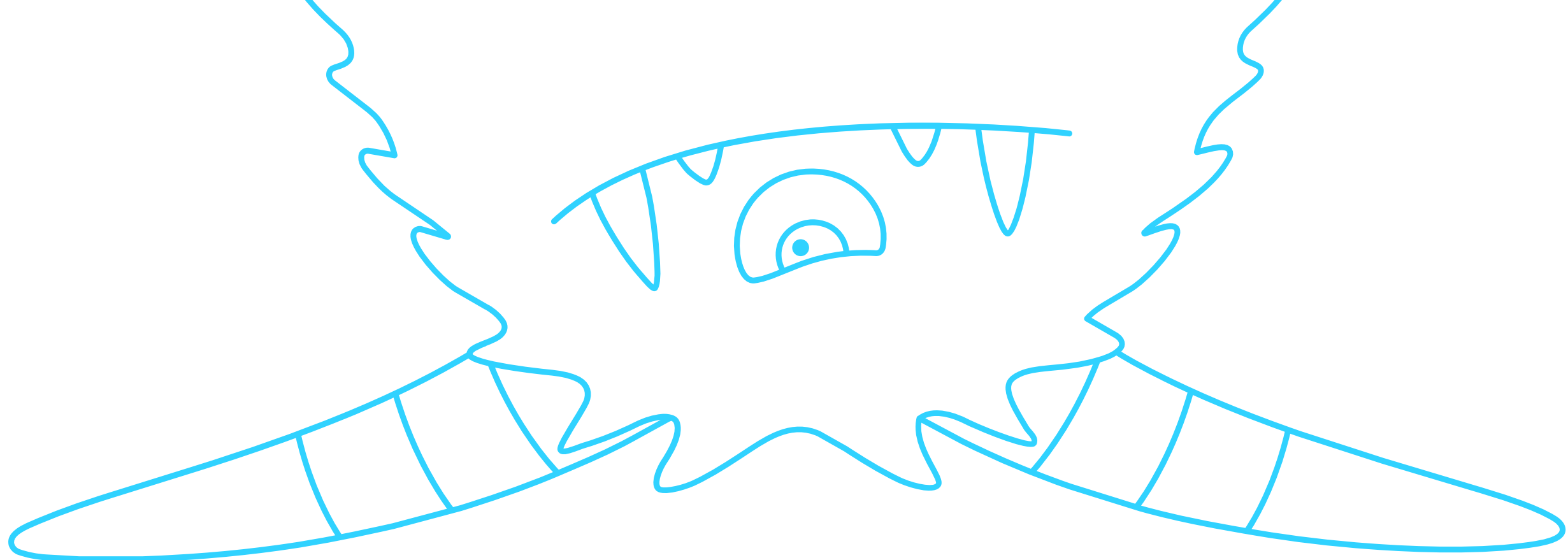
Enter to win

During Cybersecurity Awareness Month, visit the Cybersecurity Certifications Hub for your chance to win a **Cisco Cybersecurity Training Bundle**, including learning resources designed to help accelerate your cybersecurity journey. [Enter giveaway](#)

Available resources

-  [CCST Cybersecurity](#)
-  [CCNA Cybersecurity](#)
-  [CCNP Cybersecurity](#)
-  [Cisco Certificate in Ethical Hacking](#)
-  [Cisco U. - Cybersecurity Learning](#)
-  [Cisco NetAcad - Cybersecurity Training](#)
-  [Cybersecurity Certifications Community](#)





Streak Tracker

Track your learning streak! Once you complete each learning activity, cross off the matching tile below.

1 Why cybersecurity	2 Threats & attack types	3 CIA Triad	4 Passwords & MFA	5 Cryptography basics
6 Explore Cisco U.	7 Reflect & plan	8 Network security 101	9 Defense in depth	10 Endpoint security
11 Harden a network	12 Access control	13 Wireless & mobile	14 ACLs	15 Why Splunk
16 Security monitoring	17 Intro to SIEM	18 Hands-on SPL	19 Automate response	20 Inside the SOC
21 Incident response	22 Think like an attacker	23 Vulnerability assessment	24 Cloud & zero trust	25 AI & security
26 Join the community	27 Skill Assessment	28 Commit to a credential	29 Capstone	30 Celebrate your skills

Finished all 30 days? Congratulations!

You've built foundational-to-operational security skills and a clear path to a Cisco credential.