PETER'S TECH ONBOARDING GUIDE

Cybersecurity and Security+

4-week detailed curriculum | Target: CompTIA Security+ (SY0-701)

A message to you, Peter

Peter, I built this guide to give you a clear path into technology without expecting you to already know the language. You are not supposed to understand everything on day one. Your job is to show up consistently, practice, ask questions, and keep evidence of what you build. I will help you connect the pieces, but the hands-on work is where the confidence will come from.

Study rule: Do not only watch videos. Type the commands, build the labs, break things, fix them, and explain what happened in your own words.

Your outcome for this phase

Build a practical security foundation across threats, architecture, operations, identity, cryptography, risk, and incident response.

Expected pace: 2-3 hours Monday through Friday, 3-4 hours Saturday, and Sunday reserved for rest or catch-up. Each week ends with something you can demonstrate.

Phase learning resources

Resource	How to use it
Professor Messer SY0-701 playlist	Free Security+ objective-aligned course.
TryHackMe Pre Security	Guided browser-based beginner cybersecurity labs.
PortSwigger Web Security Academy	Free interactive web security lessons and labs.
CyberDefenders	Blue-team investigation and incident-response challenges.
AWS Security Workshops	Hands-on cloud security workshops.

How to prove you learned it

- Explain the concept without reading notes.
- Complete the lab twice: once with instructions and once from memory.
- Push scripts, diagrams, screenshots, or written reflections to GitHub.
- Write down one failure, the cause, and the fix each week.
- Answer practice questions only after performing hands-on work.

Week 1 - Security concepts and threats

Weekly deliverable: Complete the assigned lab, update your GitHub notes, and record a 3-5 minute explanation of what you learned.

Day	Exact learning assignment	Proof of work
Mon	CIA triad, authentication, authorization, accounting, non-repudiation, zero trust.	Notes + commands/screenshots
Tue	Threat actors, motivations, attack surfaces, social engineering and phishing.	Notes + commands/screenshots
Wed	Malware: ransomware, trojans, worms, rootkits, spyware, fileless attacks.	Notes + commands/screenshots
Thu	Vulnerabilities: misconfiguration, injection, XSS, insecure design, supply chain.	Notes + commands/screenshots
Fri	Threat intelligence, CVE, CVSS, indicators of compromise, MITRE ATT&CK; overview.	Notes + commands/screenshots
Sat	TryHackMe lab: introductory security rooms; create a threat-to-mitigation mapping sheet.	Completed lab + weekly recap

End-of-week questions

1. What problem does this technology or concept solve?
2. What are the most important commands, services, or components?
3. What broke during the lab, and how did you identify the cause?
4. How does this week connect to cloud or DevOps work?

Week 2 - Secure architecture and identity

Weekly deliverable: Complete the assigned lab, update your GitHub notes, and record a 3-5 minute explanation of what you learned.

Day	Exact learning assignment	Proof of work
Mon	Network segmentation, DMZ, firewalls, proxies, IDS/IPS, NAC, VPN.	Notes + commands/screenshots
Tue	Cloud and virtualization security; shared responsibility; containers and serverless.	Notes + commands/screenshots
Wed	IAM: least privilege, RBAC, ABAC, MFA, federation, SSO, PAM.	Notes + commands/screenshots
Thu	Cryptography: symmetric/asymmetric, hashing, salting, certificates, PKI, TLS.	Notes + commands/screenshots
Fri	Data classification, encryption at rest/in transit, backups, retention, DLP.	Notes + commands/screenshots
Sat	Lab: design a secure three-tier cloud architecture and explain each control.	Completed lab + weekly recap

End-of-week questions

1. What problem does this technology or concept solve?
2. What are the most important commands, services, or components?
3. What broke during the lab, and how did you identify the cause?
4. How does this week connect to cloud or DevOps work?

Week 3 - Security operations and incident response

Weekly deliverable: Complete the assigned lab, update your GitHub notes, and record a 3-5 minute explanation of what you learned.

Day	Exact learning assignment	Proof of work
Mon	Logging, SIEM, SOAR, EDR/XDR, baselines, alerting, time synchronization.	Notes + commands/screenshots
Tue	Vulnerability scans, penetration testing concepts, remediation, patching.	Notes + commands/screenshots
Wed	Incident response phases: preparation, detection, containment, eradication, recovery, lessons learned.	Notes + commands/screenshots
Thu	Digital forensics basics: evidence, chain of custody, acquisition, timelines.	Notes + commands/screenshots
Fri	Business continuity, disaster recovery, RTO, RPO, tabletop exercises.	Notes + commands/screenshots
Sat	CyberDefenders or TryHackMe blue-team lab; write a one-page incident report.	Completed lab + weekly recap

End-of-week questions

1. What problem does this technology or concept solve?
2. What are the most important commands, services, or components?
3. What broke during the lab, and how did you identify the cause?
4. How does this week connect to cloud or DevOps work?

Week 4 - Governance, risk, and exam readiness

Weekly deliverable: Complete the assigned lab, update your GitHub notes, and record a 3-5 minute explanation of what you learned.

Day	Exact learning assignment	Proof of work
Mon	Risk identification, likelihood, impact, treatment, register, qualitative vs quantitative.	Notes + commands/screenshots
Tue	Policies, standards, procedures, guidelines, audits, compliance, third-party risk.	Notes + commands/screenshots
Wed	Security awareness, change management, secure development, vendor management.	Notes + commands/screenshots
Thu	Performance-based question practice and command/tool review.	Notes + commands/screenshots
Fri	Full practice exam and objective gap analysis.	Notes + commands/screenshots
Sat	Final review, flashcards, lab recap, and exam readiness decision.	Completed lab + weekly recap

End-of-week questions

1. What problem does this technology or concept solve?
2. What are the most important commands, services, or components?
3. What broke during the lab, and how did you identify the cause?
4. How does this week connect to cloud or DevOps work?

Final phase assessment

Do not move forward based only on time spent. Move forward when you can perform and explain the following:

- Complete the main project without copying every step.
- Troubleshoot at least three intentionally introduced failures.
- Explain the architecture or workflow using a diagram.
- Score at least 80% on two separate practice assessments when a certification is targeted.
- Teach the core concepts back to another person in plain language.

Certification note

Target: **CompTIA Security+ (SY0-701)**. Certification dates should be adjusted based on readiness. Passing quickly is less important than retaining the skill and being able to use it in a real environment.