techventive.io
US Engineering Studio

Cohort enrolling now

info@techventive.io · 202-709-6940
5010 Sunnyside Ave, Suite 108, Beltsville, MD 20705
www.techventive.io

CYBER SECURITY BOOTCAMP

Cyber *Security*

6 weeks · Beginner+ to Intermediate · live + recorded

A hands-on, blue-team-first cyber security curriculum covering network and web security, identity, cryptography, OS hardening, incident response, cloud security, and offensive tooling — delivered by senior US-based security engineers who run real production SOCs.

10
CORE MODULES

35+
PRACTICAL SKILLS

5+
PROJECT TRACKS

1:1
CAREER SUPPORT

The *production stack* you'll master

Each tool taught with the workflows and failure modes practitioners actually meet on the job.

01
Linux
Hardened Linux + scripting

02
Wireshark
Packet capture & analysis

03
Nmap
Network reconnaissance

04
Burp Suite
Web application testing

05
Metasploit
Exploitation framework

06
OWASP ZAP
Open web scanner

07
Splunk
SIEM & log analysis

08
Kali Linux
Pentesting distribution

09
AWS Sec
Cloud security controls

10
OpenSSL
Crypto & PKI

Foundation *modules*

First half of the curriculum — core fundamentals and the most common day-to-day skills.

01

Security Foundations

CIA triad, threat models, attack lifecycle (Cyber Kill Chain, MITRE ATT&CK), risk vs. vulnerability, security mindset.

02

Network Security

TCP/IP, firewalls, IDS/IPS (Snort/Suricata), VPNs, network segmentation, packet capture with Wireshark.

03

Cryptography & PKI

Symmetric vs. asymmetric encryption, hashing, TLS handshake, certificates, key management, OpenSSL hands-on.

04

Identity & Access

Authentication vs. authorization, MFA, OAuth/OIDC, SAML, IAM in AWS/Azure, least-privilege, RBAC vs. ABAC.

05

OS & Endpoint Hardening

Linux hardening (CIS), Windows GPOs, EDR basics, patching, secure baselines, host firewalls, audit logging.

Freshers

Enter security from scratch with a hands-on blue-team & ethical hacking path.

IT Professionals

Add security depth — network, web, cloud — to your existing IT skillset.

Developers

Learn to ship secure code: OWASP, threat modeling, secrets management, DevSecOps.

Career Switchers

Move from adjacent fields (sysadmin, support, audit) into SOC / GRC / pentesting roles.

info@techventive.io · 202-709-6940
www.techventive.io

Advanced *modules*

Second half — production patterns, real-world operations, and the senior-level depth.

06

Web Application Security

OWASP Top 10 deep-dive — injection, auth flaws, XSS, CSRF, SSRF, broken access control. Burp Suite labs.

07

Offensive Tooling

Recon (Nmap), enumeration, exploitation (Metasploit), privilege escalation, lateral movement, post-exploitation cleanup.

08

Incident Response

NIST IR lifecycle, triage, containment, eradication, recovery, postmortem writing, SIEM hunting (Splunk).

09

Cloud Security

AWS shared responsibility, IAM, KMS, VPC, GuardDuty, Security Hub, CloudTrail, multi-cloud posture management.

10

GRC & Compliance

SOC 2, ISO 27001, NIST CSF, PCI-DSS, risk frameworks, audit evidence, security policies, vendor risk.

Hands-on project outcomes

- Capture and analyse network traffic to detect malicious activity.
- Run authenticated web app penetration tests against vulnerable targets.
- Harden a Linux server to CIS benchmark standards.
- Triage and respond to a simulated security incident end-to-end.
- Build and tune SIEM detection rules in Splunk.
- Configure AWS IAM, KMS, and GuardDuty for a multi-account org.
- Document an OWASP Top 10 finding with reproducible PoC.
- Map controls to NIST CSF / SOC 2 / ISO 27001 frameworks.

Course learnings

- Adversarial mindset — think like an attacker, defend like an engineer.
- Network, web, and cloud attack surfaces and their defences.
- Incident response lifecycle from detection through postmortem.
- Identity, cryptography, and access control fundamentals.
- SOC and GRC team workflows in real US enterprises.
- DevSecOps — security baked into the SDLC, not bolted on.

Career readiness, *built in.*

techventive.io turns this curriculum into job-ready positioning — project explanation, résumé and LinkedIn rewrites, GitHub portfolio polish, technical interview preparation, and placement-focused guidance through to the offer letter.

- SOC Analyst
- Security Engineer
- Cloud Security Engineer
- GRC Analyst
- Penetration Tester
- Application Security Engineer

Who can *apply*

Freshers, working professionals, managers, career switchers, and aspirants who want a practical, job-focused path.

Freshers

IT Professionals

Developers

Career Switchers

Start your Cyber Security journey with techventive.io.

info@techventive.io · 202-709-6940 · Beltsville, MD