Codevirus

BLUE TEAM - FULL PATH

Complete Learning Roadmap + Study Material

Codevirus

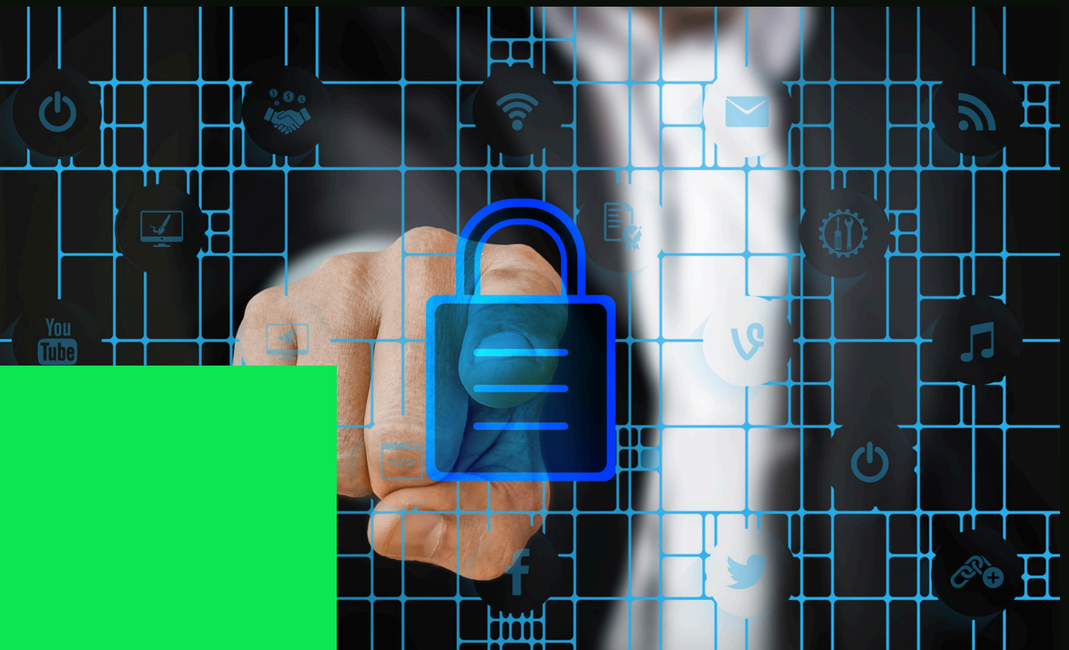
INTRODUCTION

The Blue Team is responsible for defensive cybersecurity

Primary Goals: To monitor, detect, analyze, respond, and prevent cyber attacks across networks, systems, cloud, and applications.

Codevirus

BLUE TEAM FOCUS AREAS



The Blue Team focuses on five core pillars:

- Threat detection
- Incident response
- Monitoring and logging
- Hardening systems
- Continuous defense

Codevirus

CAREER ROLES IN BLUE TEAM

Common professional roles include:

- SOC Analyst (L1/L2/L3)
- Incident Responder
- Threat Hunter
- Detection Engineer
- Blue Team Security Engineer
- Cloud Security Analyst

LEARNING PATH OVERVIEW (PART 1)

Foundational Modules

- Module 1: IT & Networking Fundamentals
- Module 2: Operating Systems (Windows & Linux)
- Module 3: Cyber Security Fundamentals
- Module 4: SOC Analyst (Level 1 – Level 3)
- Module 5: SIEM & Log Analysis
- Module 6: Incident Response & DFIR

Codevirus

LEARNING PATH OVERVIEW (PART 2)

Advanced & Specialization Modules:

- Module 7: Endpoint Detection & Response (EDR)
- Module 8: Threat Intelligence
- Module 9: Threat Hunting
- Module 10: Blue Team Automation & Scripting
- Module 11: Cloud & Blue Team Security
- Module 12: Compliance, Governance & Reporting

Codevirus

MODULE 1 — IT & NETWORKING FUNDAMENTALS

Importance: Most attacks leave network footprints; understanding traffic helps detect intrusions

Key Concepts:

- IP Addressing
- TCP vs UDP
- DNS, HTTP/HTTPS
- Ports and Protocols
- Firewalls and Routers

Codevirus

MODULE 2 — OPERATING SYSTEM FUNDAMENTALS

Windows Security Basics: Users & Groups, NTFS permissions, Event Logs, and Windows Defender.

Linux Security Basics: Users & permissions, Processes, Logs (/var/log), and File system security.

Codevirus

MODULE 3 — CYBER SECURITY FUNDAMENTALS

Core Security Concepts:

- CIA Triad
- Authentication vs Authorization
- Defense in Depth
- Least Privilege

Common Threats: Malware, Phishing, Ransomware, and Insider threats.

Codevirus

MODULE 4 — SOC ANALYST FUNDAMENTALS (L1 ⟶ L3)

SOC Level 1: Alert monitoring, log review, false positive analysis, and escalation.

SOC Level 2: Deep investigation, correlation analysis, and root cause analysis.

SOC Level 3: Advanced incident response, threat hunting, and malware/forensic analysis.

Codevirus

MODULE 5 — LOG ANALYSIS & SIEM

What is SIEM? SIEM collects and correlates logs from Firewalls, Servers, Endpoints, and Cloud services

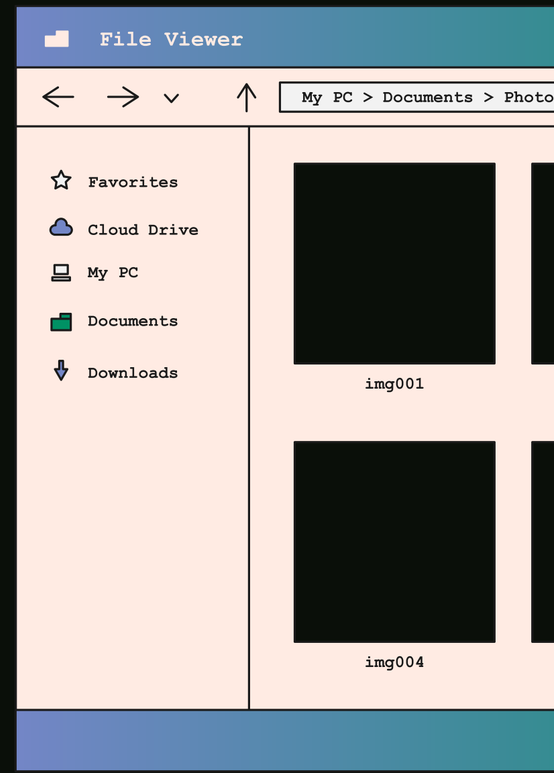
Blue Team Tasks: Alert triage, rule tuning, and creating dashboards/reports

Codevirus

MODULE 6 — INCIDENT RESPONSE & DFIR

IR Lifecycle: Detection, Analysis, Containment, Eradication, Recovery, and Lessons Learned.

Digital Forensics Basics: Disk, Memory, and Log forensics.



Cod virus

MODULE 7 — ENDPOINT SECURITY & EDR

Endpoint Security Includes: Antivirus, EDR/XDR, and Host-based firewalls.

Blue Team Responsibilities: Detecting malicious processes, isolating infected endpoints, and investigating alerts.

Codevirus

MODULE 8 — THREAT INTELLIGENCE

Definition: Information about malicious IPs, Domains, Hashes, and Threat actor techniques

- Types of Intelligence:
  - Strategic
  - Tactical
  - Operational

Codevirus

MODULE 9 — THREAT HUNTING

Definition: Proactively searching for hidden threats that bypass automated tools.

Threat Hunting Steps:

- Hypothesis creation
- Data collection
- Analysis
- Validation

Codevirus

MODULE 10 — BLUE TEAM AUTOMATION

Why Automation Matters: Faster detection, reduced manual work, and improved accuracy

Useful Skills: Python basics, Bash scripting, and Log parsing.

Codevirus

MODULE 11 — CLOUD SECURITY

Cloud Threats: Misconfigurations, account compromise, and insecure APIs.

Blue Team Cloud Tasks: Monitoring cloud logs, detecting abnormal access, and securing IAM (Identity and Access Management).

Codevirus

MODULE 12 & 13 — COMPLIANCE & BEST PRACTICES

Compliance Concepts: Data privacy, security policies, audits, and incident documentation.

Why it Matters: Legal protection, trust, and accountability.

Best Practices: Continuous monitoring, regular patching, least privilege, incident drills, and documentation.

Cod©virus

SUMMARY & QUIZ

Final Note: Blue Team is about detecting early, responding fast, and improving continuously.

Q1: Goal? Defending system

Q2: First line of defense? SOC Analyst L1

Q3: SIEM use? Log collection and analysis

Q4: IR first phase? Detection

Q5: Log for login attempts? Authentication log.

Codevirus

QUIZ

Q6: Threat hunting is? **Proactive**

Q7: Tool for endpoints? **EDR.**

Q8: Cloud monitoring focus? **Cloud logs and IAM activity.**

Q9: Minimum required access? **Least privilege.**

Q10: Automation benefit? **Reduce manual effort.**

Codevirus

THANK YOU!

Thank you for being part of the secure digital journey.
Together, we create a safer internet for everyone.