Pre–Pre New to Purple Team Education Pathway (Blue Team Focused)

A comprehensive, beginner-safe, text-based introduction to defensive cybersecurity

All free resources • No videos • Foundation for Blue → Purple progression

---

Table of Contents

1

Purpose of This Pathway 3

SECTION 1 — Cybersecurity Foundations 4

1.1 Cybersecurity Basics (Text-Based) 4

Cisco – Introduction to Cybersecurity (FREE) 4

IBM SkillsBuild – Cybersecurity Fundamentals 4

Fortinet NSE 1 (Awareness) 4

SECTION 2 — Networking for Defenders 5

2.1 Networking Essentials (No Videos) 5

Cisco Networking Essentials 5

Microsoft Learn — Networking Fundamentals 5

Subnetting Practice Tool 5

SECTION 3 — Operating Systems for Defenders 6

3.1 Linux Foundations 6

Linux Journey 6

OverTheWire – Bandit 6

3.2 Windows Foundations 6

Microsoft Learn – Windows Security Fundamentals 6

Sysinternals Documentation 6

SECTION 4 — Log Analysis & Detection Engineering Basics 7

4.1 SIEM Fundamentals (Text-Based) 7

Splunk Work+ 7

Elastic SIEM Documentation 7

4.2 Defensive Frameworks 7

MITRE D3FEND 7

NIST 800-61 Incident Response (Text PDF) 7

SECTION 5 — Threat Intelligence Foundations (Blue Team Focus) 8

5.1 Real-World Threat Understanding 8

CISA Cybersecurity Advisories 8

CrowdStrike Adversary Library 8

5.2 ATT&CK Literacy 8

MITRE ATT&CK — Enterprise Matrix 8
SECTION 6 — Hands-On Blue Team Practice (Text Only) 9
Project 1 — Build a Basic Detection Lab 9
Project 2 — Event Viewer Log Hunt 9
Project 3 — Sysinternals Defender Exercises 9
Project 4 — MITRE Technique Mapping Exercise 9
SECTION 7 — Blue Team Readiness Check 10
Completion Outcome 10

Purpose of This Pathway

This curriculum is designed for absolute beginners who want to enter cybersecurity through the **Blue Team (defensive)** side before moving toward Purple Team operations.

By the end of this pathway, the learner will: - Understand core cybersecurity concepts - Navigate Windows & Linux as a defender - Analyze logs and detect suspicious activity - Understand SIEM fundamentals - Begin threat analysis & defensive documentation

This prepares them for the next level: the **Pre–New to Purple Team Pathway**.

SECTION 1 — Cybersecurity Foundations

1.1 Cybersecurity Basics (Text-Based)

Cisco – Introduction to Cybersecurity (FREE)

https://www.netacad.com/courses/networking-essentials?courseLang=en-US

Threats

- Cyber hygiene
- Attack types
- Security roles (SOC, IR, Blue Team)

IBM SkillsBuild – Cybersecurity Fundamentals

https://skillsbuild.org

- Security principles
- Controls and safeguards
- Written labs

Fortinet FCA (Awareness)

https://training.fortinet.com

- Internet fundamentals
- Threat actor basics
- Written assessments

SECTION 2 — Networking for Defenders

2.1 Networking Essentials (No Videos)

Cisco Networking Essentials

https://skillsforall.com –

- OSI model
- IP addressing
- Ports and protocols
- Routing and switching

Microsoft Learn — Networking Fundamentals

https://learn.microsoft.com Search: *Networking Fundamentals*

- TCP/IP
- IPv4/IPv6
- Network access controls

Subnetting Practice Tool

https://subnettingpractice.com

- Interactive subnet problems
- Builds packet analysis fundamentals

Blue Team Reasoning: You cannot detect attacks if you don't understand the network they move through.

SECTION 3 — Operating Systems for Defenders

3.1 Linux Foundations

Linux Journey

https://linuxjourney.com

- Command line basics
- Processes
- Permissions
- System navigation

OverTheWire – Bandit

https://overthewire.org/wargames/bandit

- Safe
- text-based Linux challenges
- Builds command familiarity

3.2 Windows Foundations

Microsoft Learn – Windows Security Fundamentals

https://learn.microsoft.com Search: *Windows Security*

- Event Viewer
- Windows logs
- Security baselining

Sysinternals Documentation

https://learn.microsoft.com/sysinternals

- Process Explorer
- TCPView
- Autoruns

Blue Team Reasoning: Windows and Linux make up nearly all enterprise systems—defenders must understand their logs.

SECTION 4 — Log Analysis & Detection Engineering Basics

4.1 SIEM Fundamentals (Text-Based)

Splunk Work+

https://workplus.splunk.com

- Log search basics
- Query writing
- Intro detection concepts

Elastic SIEM Documentation

https://www.elastic.co/guide Search: *Elastic Security*

- Alerts
- Detection rules
- Incident triage

4.2 Defensive Frameworks

MITRE D3FEND

https://d3fend.mitre.org

- Defensive techniques
- Mitigation mappings

NIST 800-61 Incident Response (Text PDF)

https://csrc.nist.gov/publications

- Incident response lifecycle
- Roles and responsibilities

Blue Team Reasoning: Purple Teaming requires understanding how detections work.

SECTION 5 — Threat Intelligence Foundations (Blue Team Focus)

5.1 Real-World Threat Understanding

CISA Cybersecurity Advisories

https://www.cisa.gov/news-events/cybersecurity-advisories

- Vulnerabilities
- Threat actors
- MITRE mapping

CrowdStrike Adversary Library

https://www.crowdstrike.com/adversaries

- Threat actor motivations
- Behavior patterns

5.2 ATT&CK Literacy

MITRE ATT&CK — Enterprise Matrix

https://attack.mitre.org

- Learn tactics
- Study technique descriptions
- Understand defender-relevant logs

Blue Team Reasoning: Purple Teaming starts with understanding attacker **behaviors** before simulating them.

SECTION 6 — Hands-On Blue Team Practice (Text Only)

Project 1 — Build a Basic Detection Lab

Requirements:

- VirtualBox
- Windows 10 VM
- Ubuntu or Security Onion VM

Tasks:

- Observe process creation logs
- Generate network traffic
- Document findings in a detection notebook

Project 2 — Event Viewer Log Hunt

1. Open Event Viewer
2. Trigger activities (PowerShell, file creation)
3. Find corresponding logs
4. Document event IDs

Project 3 — Sysinternals Defender Exercises

Using written documentation only:

- Identify suspicious processes with Process Explorer
- Observe network connections with TCPView

Project 4 — MITRE Technique Mapping Exercise

Pick one technique (e.g., T1059 or T1047). Document:

- What the technique does
- Which logs it leaves
- How defenders detect it

SECTION 7 — Blue Team Readiness Check

Before moving to the **Pre–New to Purple Team Education Pathway**, learners should be able to:

- Read basic Windows logs
- Run basic SIEM searches
- Explain at least 3 MITRE ATT&CK techniques
- Describe how an alert is triaged
- Navigate Linux and Windows confidently
- Identify suspicious vs normal processes

Completion Outcome

Learners completing this Blue Team–focused Pre–Pre Pathway will be fully prepared to:

- Move into the Pre–New to Purple Team Pathway
- Start learning attack simulation and Purple fundamentals
- Understand defensive logging and detection foundations

This path ensures a **defense-first**, structured approach to mastering cybersecurity before entering adversary emulation or Purple Teaming.