Whole Cyber “New Security Engineer: Blue Team Field Guide”

MSSP-Focused • NICE Framework Mapped • Free & Non-Video Education Pathway

Entry → Intermediate Defensive Engineering for New Security Engineers

INTRODUCTION

This **Blue Team Field Guide** provides a structured, beginner-safe, text-driven roadmap for new Security Engineers entering **Managed Security Service Provider (MSSP)** environments.

It is:

- 100% **non-video based**
- Aligned to **NICE Framework Work Roles** (PR, DE, OM, AN, IR)
- Built using **free and complementary** public resources

Designed for roles common in MSSPs:

- Tier 1 SOC Analyst
- Tier 2 SOC Analyst
- Security Engineer I
- Threat Analyst / Hunt Support
- Vulnerability Management Support
- Endpoint Monitoring
- SIEM Triage & Escalations

You progress from **entry-level SOC literacy** → **intermediate defensive engineering**.

SECTION 1 — MSSP Role Orientation + NICE Framework Mapping

1.1 Common MSSP Roles

MSSP Functional Role	Description	NICE Role(s)
SOC Tier 1 Analyst	Alert triage, log review, escalation	**PR-CIR-001**, **AN-SOC-001**
SOC Tier 2 Analyst	Incident analysis, correlation, evidence review	**AN-ASA-001**, **IR-INC-001**

MSSP Functional Role	Description	NICE Role(s)
Security Engineer I	SIEM rule tuning, endpoint config, detections	**DE-DPR-001**, **PR-INF-001**
Vulnerability Analyst	Scan review, false positive triage, reporting	**AN-VRA-001**
Threat Intel / Hunt Support	TTP analysis, search creation, enrichment	**AN-TWA-001**, **AN-HNT-001**
MSSP Service Delivery Support	Customer interaction, ticket documentation	**OM-SMG-001**

SECTION 2 — Core Defensive Foundations (Entry Level)

2.1 Security Fundamentals

Cisco Introduction to Cybersecurity
https://skillsforall.com/course/introduction-to-cybersecurity - Threat fundamentals - Basic SOC concepts - Attack categories

IBM SkillsBuild Cybersecurity Fundamentals
https://skillsbuild.org - Authentication & authorization - Controls & defensive strategy - Text-based labs

Fortinet NSE 1 & 2 (Free)
https://training.fortinet.com - Security awareness - Threat actor behaviors

NICE Mapping: PR-DMG-001, PR-INF-001 (defensive understanding)

SECTION 3 — Networking for MSSP Analysts

3.1 Written Networking Foundations

Cisco Networking Essentials
https://skillsforall.com

- OSI model
- Ports
- protocols

- packets
- NAT
- firewalls
- routing

Microsoft Learn — Networking Fundamentals
https://learn.microsoft.com

Search: *Networking Fundamentals*

- TCP/IP
- IPv4/IPv6
- Network segmentation

SubnettingPractice.com
https://subnettingpractice.com - Interactive subnet tasks

NICE Mapping: AN-ASA-001, AN-SOC-001

SECTION 4 — Operating System Literacy (Windows & Linux)

4.1 Linux for Defenders

Linux Journey
https://linuxjourney.com

- Processes
- Permissions
- Services

OverTheWire Bandit
https://overthewire.org/wargames/bandit - Enumeration - File discovery - Safe challenge learning

4.2 Windows for Defenders

Microsoft Learn — Windows Security Documentation
https://learn.microsoft.com Search: *Windows Security*, *Event Viewer*, *Sysmon* - Logs & event IDs - Account activity - Process tracking

Sysinternals Documentation
https://learn.microsoft.com/sysinternals - Process Explorer - TCPView - Autoruns

NICE Mapping: DE-DPR-001, AN-SOC-001

SECTION 5 — Log Analysis & SIEM Foundations

5.1 SIEM Skill Development

Splunk Work+ (Free)
https://workplus.splunk.com

- SPL query basics
- Log parsing
- Alert triage fundamentals

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

- Detection rules
- Alert response
- Investigations

5.2 Understanding Detection Frameworks

MITRE D3FEND
https://d3fend.mitre.org

- Defensive countermeasures
- Mappings to ATT&CK

5.3 Core SOC Log Repositories

Study event types:

- Windows Event Logs
- Sysmon Logs
- Firewall logs
- DNS logs
- Authentication logs

NICE Mapping: PR-CIR-001, AN-ASA-001, DE-DPR-001

SECTION 6 — Threat Intelligence & TTP Literacy

6.1 ATT&CK Familiarity for MSSP Work

MITRE ATT&CK Enterprise Matrix
https://attack.mitre.org Learn:

- Tactics (left→right)
- Techniques (IDs)
- Detection fields

6.2 Intelligence Sources (Free & Written)

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

CrowdStrike Adversary Library
https://www.crowdstrike.com/adversaries

6.3 Daily TI Routine (Beginner → Intermediate)

- Read 1 ATT&CK technique/day
- Skim 1 CISA alert/week
- Maintain a Threat Notebook

NICE Mapping: AN-TWA-001, AN-SOC-001, AN-HNT-001

SECTION 7 — Vulnerability Management Foundations

7.1 CVE Understanding (Text-Only)

NVD — National Vulnerability Database
https://nvd.nist.gov

- CVSS scoring
- CWE categories

7.2 OWASP Cheat Sheets (Text)

https://cheatsheetseries.owasp.org Use:

- Authentication Cheatsheet
- Access Control
- Input Validation
- Logging & Monitoring

7.3 VM Analyst Workflow

From the NICE role **AN-VRA-001**:

- Read scan output
- Identify FP/FN
- Write customer-friendly reports

SECTION 8 — Hands-On Blue Team Exercises (Safe, Text Based)

8.1 Detection Notebook Setup

Track:

- Event IDs
- TTP observations
- Correlation notes
- Detection logic

8.2 Log Hunt Drill

1. Trigger activity on a Windows VM (PowerShell, new user, network connections).
2. Locate relevant logs.
3. Write triage notes.

8.3 SIEM Query Drills

Practice daily:

- Find failed logins
- Find new processes

- Find network anomalies

8.4 Create a Correlation Rule Concept

Define: -

- Trigger condition
- Suspicious indicators
- Recommended response
- MITRE mapping

SECTION 9 — Intermediate MSSP Readiness Checklist

A learner is MSSP-ready when they can:

- Write basic SIEM queries
- Identify suspicious logs quickly
- Map detections to ATT&CK techniques
- Explain findings to customers
- Document incident details
- Understand vulnerabilities & severity
- Follow escalation procedures

MSSP-focused NICE alignment:

AN-SOC-001 – SOC Operations

AN-ASA-001 – Cyber Defense Analyst

IR-INC-001 – Incident Responder

DE-DPR-001 – Detection Engineer

AN-VRA-001 – Vulnerability Analyst

PR-CIR-001 – Cyber Defense Incident Responder

CONCLUSION

This **Blue Team Field Guide** provides:

A full entry → intermediate defensive engineering progression

Free and safe training aligned to the NICE Framework

A roadmap tailored for actual MSSP workflows

A non-video curriculum compatible with SkillBridge, apprenticeships, and WCCSE training

Blue Team Student Guide, Materials, & Assignments

Based on the New Security Engineer: Blue Team Field Guide (MSSP-Aligned)

SECTION 1 — Course Overview

Course Purpose

This training prepares students to begin working in a Managed Security Service Provider (MSSP) environment as an entry-level Blue Team Security Engineer or SOC Analyst. All learning is **text-based**, free, and aligned to the **NICE Framework**.

Students will: - Build foundational Blue Team & SOC skills - Learn how to analyze logs, triage alerts, and document incidents - Understand vulnerability and threat intelligence workflows - Develop SIEM investigation abilities - Prepare for Purple Team & Security Engineering roles

SECTION 2 — Required Student Materials

All materials are **free**:

Required Platforms & Tools

- Cisco SkillsForAll account
- IBM SkillsBuild account
- Microsoft Learn
- Splunk Work+
- Elastic Security documentation
- MITRE ATT&CK & D3FEND
- NVD + CWE (vulnerability references)
- Sysinternals documentation
- VirtualBox + Windows VM (student provided)

Student Notebook Requirements

Students must have: - **Detection Notebook** (digital or physical) - **ATT&CK Technique Log** - **Windows Log Journal** - **SIEM Query Log**

Optional Tools (Free)

- Notion or OneNote for structured learning
- Markdown editor for clean documentation

SECTION 3 — Weekly Student Guide

Below is the structured guide for student progression.

WEEK 1 — Cybersecurity & SOC Fundamentals

Student Learning Goals

- Understand baseline cyber concepts
- Understand MSSP workflows & tickets
- Learn alert triage fundamentals

Reading & Study Material

- Cisco Introduction to Cybersecurity (text)
- IBM Cybersecurity Fundamentals
- Fortinet NSE 1–2

Assignments

4. **Define 10 security terms** in your notebook (CIA Triad, threat actor, SOC, IR, alert, event, firewall, SIEM, etc.)
5. **Write a half-page summary** on how an MSSP functions.
6. **Identify 5 types of alerts** commonly handled by Tier 1 analysts.

WEEK 2 — Networking for Defenders

Student Learning Goals

- Understand how attacks move through networks
- Build packet and protocol awareness

Reading & Study Material

- Cisco Networking Essentials (text)
- Microsoft Learn: Networking Fundamentals
- SubnettingPractice.com drills

Assignments

1. Complete **15 subnetting practice problems**.
2. Create a chart of **20 important ports** (TCP/UDP).
3. Describe **3 network attacks** and their defensive indicators.

WEEK 3 — Linux & Windows for Defenders

Student Learning Goals

- Navigate operating systems used in enterprise security
- Identify malicious vs normal OS activity

Reading & Study Material

- Linux Journey
- OverTheWire Bandit (levels 0–12)
- Microsoft Learn: Windows Security fundamentals
- Sysinternals Documentation

Assignments

1. Document **10 Windows Event IDs** and what they mean.
2. Complete Bandit levels 0–12 and write **what you learned from each level**.
3. Using Sysinternals documentation, explain:
   - What Process Explorer is used for
   - What TCPView reveals about a system

WEEK 4 — Log Analysis & SIEM Fundamentals

Student Learning Goals

- Learn to identify suspicious logs
- Understand how SIEM queries work
- Begin tier 1 triage workflows

Reading & Study Material

- Splunk Work+ text labs
- Elastic SIEM documentation
- MITRE D3FEND

Assignments

1. Write **10 SPL queries** in a SIEM log notebook.
2. Describe **5 common detection rule patterns**.
3. Document a mock investigation using:
   - suspicious process log
   - login failures
   - remote network connection

WEEK 5 — Threat Intelligence & TTP Literacy

Student Learning Goals

- Map attacker behavior to ATT&CK framework
- Understand adversary profiles

Reading & Study Material

- MITRE ATT&CK Enterprise Matrix
- CISA Alerts & Advisories
- CrowdStrike Adversary Library

Assignments

1. Pick **one threat group** and map 5 techniques.
2. Create a **daily TTP tracking log** (minimum 3 entries).
3. Summarize **one CISA alert** and identify its defensive actions.

WEEK 6 — Vulnerability Management Basics

Student Learning Goals

- Read vulnerability reports
- Understand how weaknesses become attacks

Reading & Study Material

- NVD (search 10 CVEs)
- MITRE CWE categories
- OWASP Cheat Sheets (Access Control, Authentication, Input Validation)

Assignments

1. Document **10 CVEs** with severity + affected components.
2. Explain **5 CWE weakness classes**.
3. Create a **simple VM remediation report** identifying:
    - Issue
    - Severity
    - False positive likelihood
    - Recommendation

WEEK 7 — Blue Team Hands-On Labs

Student Learning Goals

- Build detection intuition
- Strengthen triage & documentation habits

Practice Labs

1. Log Hunt:
    - Trigger events (PowerShell, file creation)
    - Locate logs
    - Write findings
2. SIEM Search Drills (daily):
    - failed logins
    - process creation
    - unusual network connections
3. Create a **detection rule concept** for:
    - suspicious PowerShell
    - persistence mechanism
    - abnormal user behavior

Assignments

1. Submit a **full detection notebook** entry with:
    - Triage notes
    - MITRE mapping
    - Evidence collection steps
2. Submit a written **customer-facing summary** (MSSP skill).

SECTION 4 — Final Student Assessment

Students must complete:

- Detection Notebook (20+ entries)
- ATT&CK Technique Log (20+ techniques)
- Windows Log Journal
- SIEM Query Workbook (20 SPL-style searches)
- Final Mini-IR Case Study

Final Exam: Mini Incident Response Report

Students receive a simulated incident with:

suspicious logs

abnormal user behavior

potential malware traces

They must write:

- Summary of incident
- Evidence gathered
- MITRE mapping
- Risk assessment
- Recommended actions

SECTION 5 — Completion Outcome

Students who finish this guide will be ready to perform:

- Tier 1 SOC monitoring
- Tier 1 alert triage and escalation
- SIEM search operations
- Threat intelligence research
- Vulnerability analysis support
- MSSP-style customer communication

This student guide is designed to carry a learner from **zero → competent MSSP-ready Blue Team engineer** in a structured, digestible format.

Blue Team Student Workbook

A Hands-On, Activity-Based Workbook for New Security Engineers (Ages 18–40)

Based on the Blue Team Student Guide + Field Guide

How to Use This Workbook This workbook transforms your Blue Team training into interactive activities, just like a K–8 workbook but designed for adult learners entering SOC, MSSP, or Security Engineering roles.

Each module includes:

- Worksheets
- Fill-in-the-blanks
- Short-answer questions
- Diagramming tasks
- Realistic MSSP ticket simulations
- ATT&CK mapping drills
- SIEM-writing practice
- Log hunts

This workbook is self-paced, beginner-friendly, and requires only free resources.

MODULE 1 — Cybersecurity Foundations

1.1 Vocabulary Builder (Fill-in-the-Blank)

Fill in the missing words:

1. The three parts of the CIA Triad are C____________, I____________, and A____________.

2. A _____________ is any person, group, or entity that attempts to cause harm to systems.
3. A _____________ is a triggered event inside a SIEM based on a detection rule.

4. A _____________ is any log entry captured by a device, application, or system.

5. A _____________ is a security device that filters network traffic.

1.2 Define These Terms (Short Answer)

Write a 1–2 sentence explanation:

Threat actor ____

Vulnerability ____

Exploit ____

SOC ____

Indicator of Compromise

1.3 Scenario Activity

A user reports suspicious login attempts. What five questions would you ask?

1. ________________________________

2. ________________________________

3. ________________________________

4. ________________________________

5. ________________________________

____

MODULE 2 — Networking for Defenders

2.1 Port Matching Activity

Match the protocols:

80 → ________

443 → ________

22 → ________

53 → ________

3389 → ________

2.2 Network Diagramming

Draw the following on paper or tablet:

An external user → firewall → internal network → server

Label:

1. Where an IDS or IPS should go
2. Where logs would be generated

2.3 Subnetting Mini-Quiz

Complete the following:

1. /24 network = how many hosts? __________

2. /16 network = how many hosts? __________

3. IP 192.168.10.37 belongs to the network: ____________________

2.4 Scenario

A sudden spike in outbound traffic occurs. List three possible causes:

1. ________________________________

2. ________________________________

3. ________________________________

____

MODULE 3 — Operating Systems for Defenders

3.1 Linux Commands (Fill-in-the-blank)

- ls lists ____________
- ps aux shows ____________
- cat displays ____________
- chmod changes ____________
- sudo allows ____________

3.2 Linux Activity

Run these commands in a Linux VM and write what they do:

whoami → ___________________________

hostname → ___________________________

netstat -tulnp → ___________________________

3.3 Windows Event Viewer Hunt

Locate these logs:

1. Failed logins (Event ID: ________)

2. Process creation (Event ID: ________)

3. New user created (Event ID: ________)

Write one sentence describing what you found for each.

- 1a____
- 2a____
- 3a____

3.4 Sysinternals Explorer

Using the documentation, identify:

A suspicious process name: __________________________

A legitimate-but-noisy process: ______________________

A network-active process: ____________________________

____

MODULE 4 — Log Analysis & SIEM Fundamentals

4.1 SPL-Style Query Practice

Write queries that:

Find failed logins: ____

Find PowerShell executions: ______________________________________

Find new services created: ______________________________________

4.2 Log Identification Task

Given these logs, decide whether they are benign or suspicious:

1. powershell.exe -nop -enc <base64> → ________________

2. svchost.exe /service → ________________

3. User login attempt failed 10 times in 5 minutes → ________________

4.3 Mini-Investigation Table

- Field Notes
- Alert Description
- Log Source
- Suspicious Indicators
- MITRE Technique
- Recommended Action

MODULE 5 — Threat Intelligence & ATT&CK Mapping

5.1 ATT&CK Technique Worksheet

Pick one technique and fill this in:

Technique ID: ______________

Description: ____

What an attacker does: ________________________________

What logs show it: ____________________________________

MITRE mitigations: ___________________________________

5.2 Threat Actor Profile

Choose a threat group and answer:

Name: _______________________

Country/Origin (if known): _________________________

3–5 known techniques:

1. ______________________

2. ______________________

3. ______________________

What industries they target: _________________________

5.3 CISA Alert Reading Exercise

Read any CISA Alert and answer:

What happened?

What weaknesses were exploited?

What defensive actions does CISA recommend?

____

MODULE 6 — Vulnerability Management

6.1 CVSS Scoring Mini-Quiz

Write the correct severity:

CVSS 9.8 → __________

CVSS 7.4 → __________

CVSS 5.1 → __________

CVSS 3.1 → __________

6.2 CVE Report Builder

Pick one CVE from NVD and answer:

CVE ID: ____________________

Affected system(s): ____________________

Attack Vector (AV): ____________________

Severity: ____________________

Summary: ____

6.3 OWASP Worksheet

Define:

Injection: ____

Broken access control: __________________________________

Misconfiguration: _______________________________________

____

MODULE 7 — Blue Team Lab Exercises

7.1 Log Hunt Challenge

Perform the following in your VM:

1. Open PowerShell and run two commands

2. Create a file named log_test.txt 3. Attempt a failed login

Now in Event Viewer:

- Find the PowerShell events
- Find the file creation logs
- Find the failed login

Document Event IDs + what you learned.

7.2 SIEM Simulation Ticket

Ticket Description: “User reports their system is running slowly and they found a strange PowerShell window opening and closing.”

Fill in:

What logs do you search first? ____________________

What indicators matter? __________________________

What MITRE techniques apply? ____________________

What would you escalate? _________________________

7.3 Detection Rule Drafting

Draft a rule concept:

Trigger: ____

Condition: ______________________________________

Expected False Positives: _________________________

Recommended Customer Action: ______________________

____

FINAL EXAM — Mini Incident Response Case Study

Below is your simulated incident: “A workstation shows multiple failed RDP logins followed by successful login from an unknown source and execution of encoded PowerShell commands.”

Answer: 1. What happened? ________________________________

2. Which logs confirm it? _________________________

3. What ATT&CK techniques were used? _____________

4. What is the risk level? ________________________

5. What should be done next? ______________________

____