

The Blue Team Field Manual

An Introductory Arsenal for Cyber Defenders

Powered by Bugitrix



Bugitrix



The Defender's Mission

If hackers are thieves, Blue Teamers are the guards, CCTV operators, and investigators.



- **Monitor Systems:** Continuously watch over networks and devices for signs of trouble.
- **Detect Attacks:** Identify malicious activity as it happens.
- **Stop Breaches:** Intervene to block threats and minimize damage.
- **Learn & Harden:** Analyze incidents to strengthen defenses for the future.

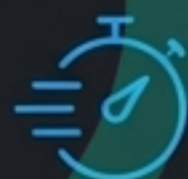
The Defender's Mindset

“Tools don’t make you a defender—
thinking like one does.”



Visibility:

Seeing what’s happening



Speed:

Acting on it quickly

“A skilled analyst with basic tools can outperform an untrained analyst with expensive software.”

At Bugitrix, we focus on both: empowering the analyst and mastering the tools.

The Core Arsenal: Your Toolkit at a Glance



SIEM

The Central Brain
(Logs + Alerts)



EDR

The Endpoint Bodyguard
(Laptops, Servers)



IDS / IPS

The Network Alarm
System



Log Analysis

The Digital Forensics
Notebook

A stylized graphic of a human brain in profile, facing right. The brain is rendered in a dark blue color with intricate white circuitry lines tracing its surface. Overlaid on the brain is a large, semi-transparent green shield with a white outline. The shield is positioned centrally, partially obscuring the brain's features.

SECTION 01: SIEM

The Central Brain of Your Security Operations Center

Splunk (SIEM)

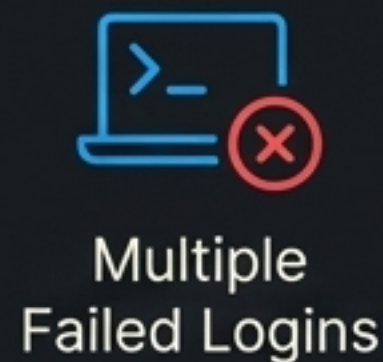
WHAT IT DOES

Collects, searches, and correlates log and event data from virtually any source across your entire infrastructure.

WHY DEFENDERS LOVE IT

It transforms millions of raw, disparate logs into a single source of truth, enabling the creation of meaningful, high-fidelity alerts.

IN ACTION



+



HIGH-PRIORITY
ALERT TRIGGERED

4. YOUR FIRST MISSION

Get hands-on by practicing with basic log searching, building simple alerts, and creating dashboards.

The SIEM Landscape: Flexible & Cloud-Native Options

Elastic SIEM

The Open-Source Powerhouse



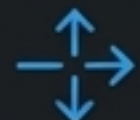
WHAT IT DOES

A free and open SIEM built on the high-speed Elasticsearch stack.



WHY DEFENDERS LOVE IT

Highly flexible, customizable, and budget-friendly for labs or full deployments.



IN ACTION

Detects brute-force attacks by correlating authentication logs over time.



FIRST MISSION

Learn Elasticsearch (ELK Stack) basics and practice building dashboards in Kibana.

Microsoft Sentinel

The Cloud-Native Brain



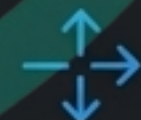
WHAT IT DOES

A cloud-native SIEM tightly integrated with the Microsoft Azure ecosystem.



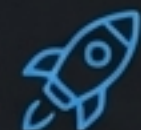
WHY DEFENDERS LOVE IT

Leverages powerful, built-in automation (SOAR) and AI to analyze threats at cloud scale.



IN ACTION

Automatically identifies and flags malicious PowerShell commands on Azure VMs.



FIRST MISSION

Spin up a free instance and experiment with the built-in analytics rules in an Azure lab environment.



SECTION 02: EDR

The Bodyguard on Every Endpoint

Endpoint Protection: Real-Time & OS-Integrated

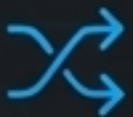
CrowdStrike Falcon

Real-Time Threat Prevention



WHAT IT DOES

A cloud-based platform providing next-gen antivirus, EDR, and threat hunting.



IN ACTION

A ransomware process attempts to execute; Falcon instantly blocks the process and quarantines the file.



WHY DEFENDERS LOVE IT

Excels at stopping malware and ransomware *before* significant damage occurs.



FIRST MISSION

Study endpoint telemetry and learn to recognize patterns of malicious behavior.

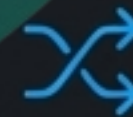
Microsoft Defender for Endpoint

Deep Operating System Visibility



WHAT IT DOES

Microsoft's native EDR solution for Windows environments.



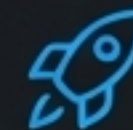
IN ACTION

Detects a suspicious process attempting to inject malicious code into a legitimate Windows service.



WHY DEFENDERS LOVE IT

Offers unparalleled, deep visibility into the Windows OS kernel and system processes.



FIRST MISSION

Begin by analyzing Windows Security Event Logs to understand baseline activity.

Wazuh

Your Open-Source Security Lab



WHAT IT DOES

An open-source security platform combining a Host-based Intrusion Detection System (HIDS) with SIEM capabilities.



WHY DEFENDERS LOVE IT

It's the perfect free tool for building a home lab to learn log analysis, file integrity monitoring, and endpoint security fundamentals.




IN ACTION

An attacker modifies a critical system file (`/etc/passwd`); Wazuh immediately generates an alert for an unauthorized file change.



YOUR FIRST MISSION

Install Wazuh on a Virtual Machine (VM) and learn to configure agents and rules.



SECTION 03: NETWORK SECURITY

The Unblinking Eye on the Wire

Network Intrusion Detection: The Classic vs. The Contender

Snort

The Industry Classic



WHAT IT DOES

A signature-based Intrusion Detection System (IDS) that analyzes network traffic for known attack patterns.



WHY DEFENDERS LOVE IT

It's the foundational IDS that many professionals learned on. The principles are timeless.



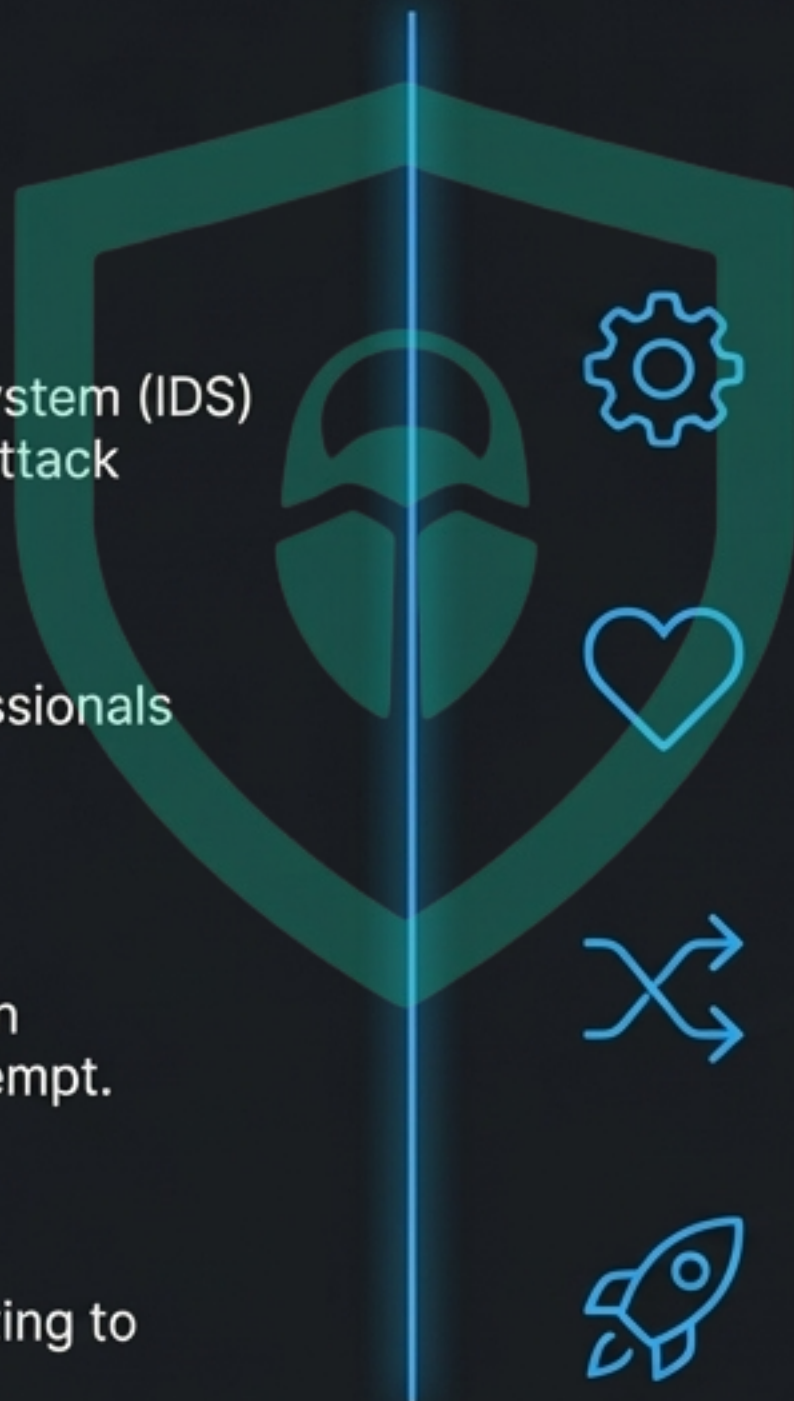
IN ACTION

Detects network traffic matching a known signature for an SQL injection exploit attempt.



FIRST MISSION

Learn the fundamentals of Snort rule writing to detect specific patterns.



Suricata

Modern & High-Performance



WHAT IT DOES

A modern, high-performance IDS/IPS engine that supports multi-threading for faster processing.



WHY DEFENDERS LOVE IT

It's fast, modern, and can handle high-volume traffic on today's networks.



IN ACTION

Identifies suspicious DNS queries indicative of a DNS tunneling command-and-control channel.



FIRST MISSION

Practice analyzing network traffic captures (PCAPs) with Suricata to hunt for threats.

Zeek (formerly Bro)

See the Story in Your Traffic



WHAT IT DOES

A network security monitor that analyzes traffic behavior, creating high-fidelity, transactional logs of all activity (e.g., every HTTP request, every DNS query).



WHY DEFENDERS LOVE IT

It goes beyond alerts. Zeek logs provide rich context that is invaluable for deep investigations and threat hunting.



IN ACTION

An analyst, reviewing Zeek logs, notices a single host making unusual SMB connections to multiple other workstations, indicating lateral movement.



YOUR FIRST MISSION

Dive into protocol analysis and learn to interpret Zeek's detailed log files (`conn.log`, `http.log`, etc.).

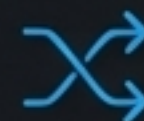
Graylog

Log Analysis Made Accessible



WHAT IT DOES

A centralized log management platform designed for collecting, indexing, and analyzing log data from any source.



IN ACTION

A defender uses Graylog's dashboard to visualize a sudden spike in error logs from a web server, leading to the discovery of an attack.



WHY DEFENDERS LOVE IT

Its powerful search capabilities and easy-to-use User Interface (UI) make it a favorite for quickly spotting anomalies in massive datasets.



YOUR FIRST MISSION

Set up a Graylog instance and practice creating streams and parsing different log formats.

Your First Mission Debrief: An Action Plan

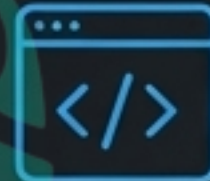
Learning is doing. Here is a practical roadmap to begin building your skills.



VM & LAB SETUP: Install Wazuh or Graylog on a Virtual Machine.



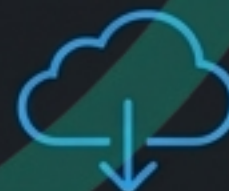
LOG ANALYSIS: Practice log searching in Splunk or Elastic. Learn to parse logs.



RULE WRITING: Learn the basic syntax for writing a Snort rule.



LOG ANALYSIS: Practice log searching in Splunk or Elastic. Learn to parse logs.



CLOUD PRACTICE: Use a free tier to explore Microsoft Sentinel in an Azure lab.



NETWORK ANALYSIS: Download sample PCAPs and analyze them with Suricata and Zeek.

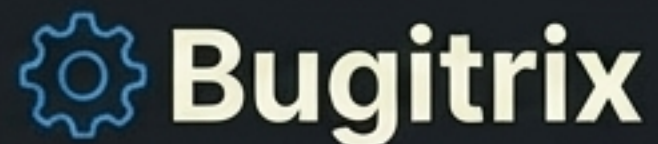


ENDPOINT FUNDAMENTALS: Study Windows Event Logs to understand what 'normal' looks like.

The Defender's Code

All tools discussed are for educational and defensive purposes only. Use them only on systems you own or have explicit permission to monitor.

Bugitrix stands for ethical cybersecurity education and responsible defense.



bugitrix.com

Blue Team Learning Made Simple