The SOC Analyst Level-1 Playbook

Copyright Notice

© 2025 Codelivly / Rocky. All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission from the publisher, except for brief quotations in reviews or educational use.

Unauthorized reproduction or distribution of this book is prohibited.
All trademarks, product names, and logos mentioned are the property of their respective owners.

Who This Book Is For

This book is for anyone who wants to break into Security Operations without getting lost in buzzwords or fake “elite hacker” nonsense.
Straight up — it’s for:

- Beginners trying to land their first SOC Level-1 job.
- Students studying cybersecurity who want practical, real-world clarity.
- IT professionals shifting into cyber defense and needing a structured path.
- Junior analysts who are tired of scattered YouTube tutorials and want a real playbook.
- Self-learners who want to understand monitoring, alert triage, and incident handling in a practical, applied way.
- Anyone preparing for SOC interviews and needing to understand what L1 analysts actually do day to day.

If you want hand-holding or theoretical fluff, this book isn’t for you.
If you want clarity, practicality, and a reality check on real SOC work, you’re in the right place.

Table Of Contents

Chapter 1: Welcome to the Glass House: SOC Truths vs. Hype..... 17
The Mission: Not Finding Needles, Protecting the Haystack..... 18
The SOC Team: Where You Fit (L1, L2, Intel, Management)..... 19
How You're Measured: KPIs That Matter (MTTD, MTTR) & Shift Survival..... 21
The Two Clocks That Never Stop Ticking..... 21
Shift Survival: The Unwritten Rules..... 21
A Day in the Life: Two Tickets, Two Different Outcomes..... 23
Scenario 1: The Burnout Spiral (The Wrong Way)..... 23
Scenario 2: The Efficient Rhythm (The Right Way)..... 23
The Lesson in the Grind..... 24
Chapter 2: The Adversary's Playbook (For Busy Analysts)..... 26
The Cyber Kill Chain & MITRE ATT&CK: Your New Mental Map..... 27
1. The Cyber Kill Chain: The "Big Picture" View..... 27
2. MITRE ATT&CK: The "Tactical Playbook"..... 27
Why This Makes You Better..... 29
Top 5 Threats You'll Actually Face (Phishing, Ransomware, Credential Theft, etc.).. 30
1. Phishing: The Digital Con Artist..... 30
2. Credential Theft & Account Takeover..... 30
3. Ransomware & Destructive Malware..... 31
4. Insider Risk (Malicious or Compromised)..... 31
5. Web Application Attacks..... 32
The Common Thread: Your Job Isn't to "Stop" Them..... 32
Blue Team Tale: "The One-Liner That Broke Everything"..... 34
Chapter 3: Logs & Signals: The Raw Material of Triage..... 38
The Trinity: Network, Endpoint, and Identity Logs..... 39
1. Network Logs: The Traffic Camera..... 39
2. Endpoint Logs: The Body Cam..... 39
3. Identity Logs: The Security Badge Reader..... 40
Putting It All Together: The Story Emerges..... 40
Extracting the "So What?": From Event to Evidence..... 42
Step 1: Understand What You're Actually Looking At..... 42
Step 2: Correlate Immediately (The "Who Asked You?")..... 42
Step 3: Apply the "So What?" Filter (The Three Questions)..... 43
Practical Example: From Event to Evidence..... 43
Your New Habit..... 44
Hands-On Drill: Read this Apache Log. What just happened?..... 45

Step 1: Parse the Log (What are we looking at?)..... 45
Step 2: Apply the "So What?" Filter..... 45
Step 3: Correlate & Build the Story..... 46
Your Action as L1:..... 46
Chapter 4: Network Triage for the Time-Starved..... 48
The 20% of Networking That Solves 80% of Alerts (IPs, Ports, DNS, HTTP/S)..... 49
1. IP Addresses: The "Who" and "Where"..... 49
2. Ports: The "Why"..... 49
3. DNS: The "What Did They Ask For?"..... 50
4. HTTP/S: The "What Did They Say?"..... 50
The 60-Second Network Triage Drill..... 50
Quick Wins with Command Line & Wireshark (Focus on Filters, not Theory)..... 52
Command Line: Your First 30 Seconds..... 52
1. netstat -ano (Windows) or ss -tunap / netstat -tunap (Linux)..... 52
2. tasklist /svc (Windows) or ps aux (Linux)..... 52
3. nslookup or dig (Any OS)..... 53
Wireshark: Your Packet Microscope (When You Have 5 Minutes)..... 53
The Life-Changing Filter Bar..... 53
Follow the TCP Stream (The "Aha!" Button)..... 54
The 90-Second Wireshark Triage Protocol..... 54
Lab: Spot the Beacon in the Noise..... 56
Your Mission..... 56
Step-by-Step Guide..... 56
What You Should Find..... 57
Analysis & Takeaway..... 58
Chapter 5: Endpoint Essentials: Windows & Linux Under the Hood..... 59
Processes, Persistence, and Handles – The Holy Trinity..... 60
1. Processes: What's Alive Right Now?..... 60
2. Persistence: How It Survives Reboot..... 60
3. Handles: What It's Touching..... 61
The Triage Flow in Action..... 61
The Mindset Shift..... 62
EDR Alerts vs. OS Telemetry: Correlating the Story..... 63
EDR Alerts: The Expert Witness..... 63
OS Telemetry: The Raw Footage..... 63
The Triage Workflow: Correlating the Sources..... 64
Practical Example: Correlating a "Living-Off-The-Land" Alert..... 65
The Key Takeaway..... 66

Lab: Triage a "Suspicious Process" Alert Using Built-in OS Tools..... 67
Step 1: Initial Recon - What's Running?..... 67
Step 2: Process Tree & Parentage - How Did It Start?..... 68
Step 3: Network Activity - Is It Communicating?..... 69
Step 4: Persistence Check - Will It Survive Reboot?..... 69
Step 5: Quick Forensic Artifact Check..... 70
Step 6: Containment & Evidence Collection..... 70
Your Investigation Summary..... 71
Key Skills Demonstrated:..... 73
Chapter 6: SIEM Mechanics: How Alerts Are Born (and How They Lie)..... 75
Correlation Rules Demystified: Logic, Thresholds, and Blind Spots..... 76
The Anatomy of a Correlation Rule..... 76
The Three Components That Control Everything..... 76
The Five Blind Spots Every L1 Must Know..... 77
Your New Superpower: Rule Reverse-Engineering..... 78
Practical Example: Decoding a "Malware Download" Alert..... 78
The Analyst's Mantra..... 79
Alert Prioritization: Severity vs. Criticality vs. Your Time..... 80
Severity vs. Criticality: The Life-Changing Difference..... 80
The Criticality Calculator: Five Questions to Ask Immediately..... 80
The Prioritization Matrix: Your Decision Framework..... 82
Time Allocation: Your Shift in Percentages..... 82
The Escalation Threshold: When to Pull the Andon Cord..... 82
Common Traps to Avoid..... 84
The Mindset Shift..... 84
The Triage Loop: A Repeatable 6-Step Methodology..... 85
Step 1: Classify & Contextualize (The 30-Second Triage)..... 85
Step 2: Gather & Observe (The Evidence Collection)..... 85
Step 3: Analyze & Correlate (The "So What?" Phase)..... 86
Step 4: Decide & Act (The Point of No Return)..... 86
Step 5: Document & Notate (Your Professional Legacy)..... 87
Step 6: Feedback & Improve (Breaking the Cycle of Noise)..... 87
The Loop in Action: A 5-Minute Phishing Triage..... 88
The Non-Negotiable Rule..... 88
Chapter 7: Hands-On Triage: From Click to Conclusion..... 89
Step-by-Step Walkthrough: Investigating a Phishing Alert..... 90
Step 1: Classify & Contextualize (0:00-0:30)..... 90
Step 2: Gather & Observe (0:30-2:30)..... 90

Step 3: Analyze & Correlate (2:30-4:30)..... 91
Step 4: Decide & Act (4:30-5:30)..... 92
Step 5: Document & Notate (5:30-6:00)..... 93
Step 6: Feedback & Improve (6:00-6:30+)..... 94
The Alternative Path: No Click Scenario..... 94
Key Takeaways from This Walkthrough..... 94
Asking the Killer Questions: Who, What, When, Where, Why?..... 96
1. WHO? (Identity & Attribution)..... 96
2. WHAT? (Action & Impact)..... 97
3. WHEN? (Timeline & Pattern)..... 97
4. WHERE? (Location & Scope)..... 98
5. WHY? (Intent & Motivation)..... 99
The Bonus Question: HOW? (Method & Technique)..... 99
Putting It All Together: The 60-Second Assessment..... 100
The Mindset Shift..... 100
False Positive Factory: How to Identify, Document, and Move On..... 101
The False Positive Mindset Shift..... 101
Step 1: Identification - The False Positive Decision Tree..... 101
Step 2: Verification - The "Prove It's Benign" Checklist..... 102
Step 3: Documentation - The Art of the Closure Note..... 102
Step 4: Feedback - Breaking the Cycle..... 103
Special Case: The "Benign True Positive"..... 104
The False Positive Hall of Fame (Common Examples)..... 104
The Professional's Approach to False Positives..... 105
The Bottom Line..... 105
Chapter 8: Building Your Own Hunts: Intro to Proactive Detection..... 106
Using ATT&CK to Guide Your SIEM Searches..... 107
The Mindset Shift..... 107
The Translation Method: From Technique to Query..... 107
Practical Examples: From ATT&CK to SIEM..... 107
Example 1: Hunting for Obfuscated PowerShell (T1059.001 + T1027)..... 108
Example 2: Hunting for Credential Dumping (T1003)..... 108
Example 3: Hunting for Persistence via Scheduled Tasks (T1053.005)..... 109
Building Your ATT&CK Hunting Calendar..... 109
The Query Builder Template..... 110
Operationalizing Your Hunts..... 111
The Analyst's Edge..... 111
Crafting a Basic Anomaly Detection Query..... 113

The Philosophy: Normal is Boring, Rare is Interesting....113
The 3-Step Process to Build Any Anomaly Query....113
Step 1: Pick Your Entity and Define "Normal"....113
Step 2: Choose Your Deviation Metric....113
Step 3: Build the "Baseline vs. Current" Query....114
Example 1: The "After-Hours Server Activity" Hunt....114
Example 2: The "Data Exfiltration Spike" Hunt....115
Example 3: The "First-Time Connection" Hunt....116
The Anomaly Hunter's Toolkit: Four Essential Query Patterns....117
Making It Operational: From Hunt to Alert....118
The Golden Rule: Context is Everything....118
Your First Anomaly Hunt Assignment....118
The Takeaway....119
Lab: Find All Users Who Logged In After Midnight from a New City....120
Step 1: Understand the Data Model....120
Step 2: Build the Query Logic....121
Step 3: The Splunk SPL Query....121
Step 4: Alternative Query (Simpler, No Subsearch)....122
Step 5: Run and Analyze Results....123
Step 6: The False Positive Filter....124
Step 7: Operationalize the Hunt....124
Step 8: Follow-up Investigation Playbook....125
Common Pitfalls & Solutions....126
The Bigger Picture: What You're Really Hunting....126
Your Lab Deliverable....126
Key Takeaway....127
Chapter 9: The IR Playbook for L1: Contain, Document, Escalate....129
Initial Containment Actions You're Allowed to Take (Reset, Block, Isolate)....131
1. RESET: Account & Access Actions....131
2. BLOCK: Network & Connectivity Actions....132
3. ISOLATE: Host & Endpoint Actions....133
The Containment Decision Matrix....134
Containment vs. Evidence: The Golden Rule....134
What You're NOT Allowed to Do (Without Escalation)....135
The 5-Minute Containment Drill....135
The Art of the Note: Writing for L2, Auditors, and Future You....136
The 5-Line Incident Summary (Do This FIRST)....136
The Complete Note Structure....136

1. Timeline (The Story)....136
2. Evidence (The Proof).... 137
3. Actions Taken (What You Actually Did).... 138
4. Context & Analysis (The "So What?").... 138
5. Next Steps Recommended (For L2).... 138
What L2 Actually Hates (The "Bad Note" Hall of Shame).... 139
What L2 Actually Loves (The "Good Note" Hall of Fame).... 139
The "Future You" Test.... 140
Special Cases.... 140
The Professional's Habit.... 141
Your Note-Writing Superpower.... 142
The Escalation Checklist: What to Include So They Don't Send It Back.... 143
Pre-Escalation Verification: The 5-Minute Self-Check.... 143
✅ 1. Containment Verification.... 143
✅ 2. Evidence Collection.... 143
✅ 3. Basic Triage Completed.... 143
The Escalation Package: What to Actually Include.... 144
📋 Part 1: The Executive Summary (First thing they read).... 144
🔍 Part 2: The Technical Brief.... 144
🛡️ Part 3: Response Actions (What You Did).... 145
🎯 Part 4: What You Need from L2 (The Ask).... 145
The "Don't Send It Back" Formatting Rules.... 146
1. Ticket Title Convention.... 146
2. The First Comment is Everything.... 146
3. Attach, Don't Describe.... 146
4. Use Bullets, Not Paragraphs.... 146
Common Escalation Failures & Fixes.... 147
Failure 1: The "You Figure It Out".... 147
Failure 2: The "Maybe".... 147
Failure 3: The "Everything Bagel".... 147
Failure 4: The "Black Box".... 147
The Escalation Readiness Test.... 147
The Professional Handoff Script.... 148
When They Still Send It Back.... 148
Your New Reputation.... 148
Chapter 10: The Big Five Incidents – Deep Dive Playbooks.... 150
1. Phishing: Email Headers, URL Analysis, User Action.... 151
Key IOCs to Hunt: The 5-Second Scan.... 151

Triage Steps: The 8-Minute Drill..... 151
Decision Points: The Triage Crossroads..... 152
Sample Notes: The Professional Documentation..... 153
Why This Matters..... 153
2. Malware: Hash Analysis, Process Tree, Network Callouts..... 156
Key IOCs to Hunt: The Execution Triangle..... 156
Triage Steps: The 10-Minute Containment Drill..... 157
Decision Points: From Single Host to Major Incident..... 158
Sample Notes: Malware Incident Documentation..... 158
Why This Matters..... 158
3. Credential Attacks: Brute Force, Impossible Travel, Token Theft..... 161
Key IOCs to Hunt: The Authentication Anomalies..... 161
Brute Force Patterns:..... 161
Impossible Travel Indicators:..... 161
Token Theft Signals:..... 161
Triage Steps: The Authentication Forensics Drill..... 162
1. Map the Attack Pattern (2 minutes):..... 162
2. Validate Geography & Timing (3 minutes):..... 162
3. Check for Success (The Critical Step) (2 minutes):..... 162
4. Immediate Containment (2 minutes):..... 162
5. Scope the Compromise (1 minute):..... 163
Decision Points: From Alert to Incident..... 163
Scenario A: Failed Attempts Only..... 163
Scenario B: Single Account Compromised..... 163
Scenario C: Multiple Accounts Compromised..... 163
Scenario D: Impossible Travel with Legitimate Explanation..... 163
Sample Notes: Credential Attack Documentation..... 164
Special Case: Token Theft Incident Notes..... 166
The Credential Attack Mindset..... 166
4. Web App Attacks: SQLi, XSS in the Logs..... 168
Key IOCs to Hunt: The Attack Patterns in Logs..... 168
SQL Injection (SQLi) Signatures:..... 168
Cross-Site Scripting (XSS) Indicators:..... 168
Other Common Web Attacks:..... 168
Triage Steps: The Web Log Analysis Drill..... 169
1. Identify the Attack Type (1 minute):..... 169
2. Determine Success vs. Attempt (3 minutes):..... 169
3. Trace the Attacker's Actions (2 minutes):..... 169

4. Immediate Containment (2 minutes):.....169
5. Scope the Impact (2 minutes):.....170
Decision Points: From Probe to Breach.....170
Scenario A: Blocked Attempt (WAF caught it).....170
Scenario B: Attempt, No Clear Success (200 but no follow-up).....170
Scenario C: Successful Exploit (Data accessed/exfiltrated).....170
Scenario D: Reconnaissance Only.....170
Sample Notes: Web App Attack Documentation.....171
Quick Reference: Log Search Patterns.....173
The Web Attack Mindset.....173
5. Insider Risk: Data Exfiltration & Privilege Misuse Patterns.....174
Key IOCs to Hunt: The Behavioral Red Flags.....174
Data Exfiltration Patterns:.....174
Privilege Misuse Indicators:.....174
Behavioral & Contextual Signals:.....175
Triage Steps: The Delicate Investigation Drill.....175
⚠️ CRITICAL FIRST STEP: CONSULT YOUR INSIDER THREAT PROTOCOL...175
1. Verify Anomaly Against Role (2 minutes):.....175
2. Gather Context Discreetly (3 minutes):.....175
3. Preserve Evidence Meticulously (2 minutes):.....175
4. Contain Strategically (2 minutes):.....176
5. Document Everything (1 minute):.....176
Decision Points: From Policy Violation to Criminal Act.....176
Scenario A: Policy Violation Only.....176
Scenario B: Data Misuse Without Malice.....176
Scenario C: Active Data Theft.....176
Scenario D: Sabotage/Immediate Harm.....177
Sample Notes: Insider Risk Documentation.....177
Special Considerations for Insider Investigations.....179
Legal & Privacy Boundaries:.....179
The Discreet Triage Approach:.....179
The Escalation Path:.....179
The Insider Risk Mindset.....180
The Big Five Incidents – Complete Playbook Reference.....181
1. Phishing Playbook.....181
Key IOCs:.....181
Triage Steps (8-Minute Drill):.....181
Decision Points:.....181

Sample Notes:..... 181
2. Malware Playbook..... 182
Key IOCs:..... 182
Triage Steps (10-Minute Containment):..... 182
Decision Points:..... 182
Sample Notes:..... 183
3. Credential Attacks Playbook..... 183
Key IOCs:..... 183
Triage Steps:..... 183
Decision Points:..... 183
Sample Notes:..... 184
4. Web App Attacks Playbook..... 184
Key IOCs:..... 184
Triage Steps:..... 184
Decision Points:..... 184
Sample Notes:..... 185
5. Insider Risk Playbook..... 185
Key IOCs:..... 185
Triage Steps:..... 185
Decision Points:..... 185
Sample Notes:..... 186
Universal Playbook Principles..... 187
Common Across All Incidents:..... 187
The Professional Mindset:..... 187
Chapter 11: The Analyst's Swiss Army Knife..... 189
Threat Intel Enrichment (VirusTotal, AbuseIPDB, etc.) – Automate It..... 190
Step 1: The Browser-Based Speed-Up (Zero Setup)..... 190
Step 2: SIEM/EDR Native Integrations (The Built-In Boost)..... 191
Step 3: The API-Powered Workflow (Next-Level Automation)..... 192
Step 4: SOAR/Playbook Automation (Enterprise Level)..... 194
Step 5: The Analyst's Toolkit - Practical Implementation..... 195
Critical Caveats & Best Practices..... 196
Immediate Action Items..... 198
Packet Analysis with Zeek & Wireshark – Just the Useful Bits..... 199
Zeek (Formerly Bro): Your Automated Network Notetaker..... 199
The 4 Zeek Logs That Actually Matter:..... 199
Zeek in 60 Seconds: Your Quick-Check Commands..... 201
Wireshark: Your Packet Microscope..... 201

The 6 Wireshark Filters That Solve 90% of Cases:.....202
Wireshark in 90 Seconds: The Triage Protocol..... 203
Real Example: Finding a C2 Beacon..... 204
The Combined Workflow: Zeek → Wireshark → Conclusion..... 204
Command-Line Magic: tshark (Wireshark without the GUI).....205
The Analyst's Packet Cheat Sheet..... 206
The Reality Check.....206
Lightweight Forensics: Automated Toolkits & Live Response Scripts..... 208
Part 1: The Quick Assessment Tools (Built-In & Free).....208
Windows: Built-In Arsenal.....208
Linux: The Essential Commands.....209
Part 2: Automated Toolkits (Download & Run)..... 209
KAPE (Kroll Artifact Parser & Extractor) - Your Forensic Swiss Army Knife.....209
FleetDM/osquery - Live Query Engine.....210
Part 3: Live Response Scripts (Copy-Paste Ready)..... 211
Windows Live Response Collector (Save as collect.ps1):.....211
Linux Live Response Script (Save as collect.sh):.....213
Part 4: The Practical Workflow - When to Use What.....214
Scenario 1: Suspected Malware, Need Quick Answers..... 214
Scenario 2: Ransomware Alert - SPEED IS EVERYTHING.....214
Scenario 3: Insider Threat Investigation (Discreet).....215
Part 5: Evidence Handling 101..... 215
The Lightweight Forensics Mindset.....216
Chapter 12: Leveling Up Your Game..... 218
Common L1 Pitfalls & How to Sidestep Them..... 219
Pitfall 1: The Rabbit Hole (Analysis Paralysis)..... 219
Pitfall 2: The "Containment Cowboy"..... 219
Pitfall 3: The "It's Probably Nothing" Bias..... 220
Pitfall 4: The SIEM Prisoner.....221
Pitfall 5: The Lone Wolf.....221
Pitfall 6: The Note-Nobody-Can-Use..... 222
Pitfall 7: The Tool Tyrant.....222
The Professional's Mindset Shift..... 223
Your Anti-Pitfall Checklist..... 223
Thinking Like an Attacker (and Then Like an L2).....224
Part 1: Thinking Like an Attacker (The Adversary Mindset).....224
The Attacker's Playbook for Common Scenarios:..... 224
The Attacker's Golden Rules (That You Should Know):..... 226

Part 2: Thinking Like an L2 (The Senior Analyst Mindset)....226
The L2 Mental Checklist:.... 226
How to Practice L2 Thinking Today:.... 227
The Dual-Mindset Workflow.... 228
From Mindset to Action: Your Growth Plan.... 229
The Mindset Shift That Changes Everything.... 229
Building a Home Lab That Doesn't Suck Your Time.... 230
Principle 1: Start Virtual, Stay Virtual.... 230
The Minimal Viable Lab (30 Minutes Setup):....230
The "I Have a Little More Time" Lab (2 Hours Setup):....230
Principle 2: Pre-Built Over DIY.... 230
Ready-to-Go Environments:.... 230
Principle 3: Focused Learning Sprints.... 232
Weekly Lab Schedule (Total: 3-5 hours/week):.... 232
Principle 4: Cloud Labs When Needed....232
Principle 5: The Tool Strategy....233
Essential Tool Categories (Pick ONE from each):....233
Principle 6: The "Production" vs. "Sacrificial" Split.... 234
Principle 7: Realistic Scenarios, Not Just CTFs.... 234
Practical Lab Scenarios:.... 234
The 1-Hour Incident Drill:.... 235
Principle 8: Document Everything (Like a Pro).... 235
The "I Only Have 30 Minutes" Lab.... 237
Common Time Traps to Avoid....237
Your First Week Plan.... 237
The Mindset Shift.... 238
Chapter 13: The Career Launchpad.... 240
Certifications Decoded: What's a Signal vs. Noise.... 241
The Certification Reality Check.... 241
Tier 1: Foundation Signals (Get ONE).... 241
CompTIA Security+.... 241
GIAC Security Essentials (GSEC)....242
Microsoft SC-200: Security Operations Analyst.... 242
Tier 2: Specialization Signals (Choose ONE Path)....242
Blue Team Path:.... 242
CompTIA CySA+.... 242
GIAC CyberDefense (GCDA).... 242
Blue Team Level 1 (BTL1).... 242

Incident Response Path:..... 243
GIAC Certified Incident Handler (GCIH)..... 243
GIAC Certified Forensic Analyst (GCFA)..... 243
Cloud Path:..... 243
AWS Certified Security - Specialty..... 243
Microsoft Certified: Azure Security Engineer Associate..... 244
Tier 3: Advanced Signals (Wait Until Ready)..... 244
CISSP..... 244
OSCP (Offensive Security Certified Professional)..... 244
GIAC Security Expert (GSE)..... 244
The Noise: Certs to Question..... 244
CEH (Certified Ethical Hacker)..... 245
CompTIA PenTest+..... 245
Multiple Entry-Level Certs..... 245
The Strategic Certification Roadmap..... 245
For Career Changers (0 experience):..... 245
For SOC L1 Analysts (1 year experience):..... 246
For L2 Aspiring (2-3 years experience):..... 246
When to Skip Certs Entirely (And What to Do Instead)..... 246
The Certification Decision Matrix..... 247
Pro Tips No One Tells You..... 248
The Final Verdict..... 248
Building a "Break-In" Portfolio with Personal Projects..... 249
The Mindset Shift: From Consumer to Creator..... 249
Tier 1: The "I Have a Laptop" Projects (Start Here)..... 249
1. The Phishing Simulation & Analysis Platform..... 249
2. DIY SIEM with Elastic Stack..... 250
3. Malware Analysis Sandbox..... 251
Tier 2: The "I'm Getting Serious" Projects..... 252
4. Threat Intelligence Feed Aggregator..... 252
5. Incident Response Playbook Simulator..... 253
6. Security Dashboard for Home Network..... 253
Tier 3: The "Hire Me Now" Projects..... 254
7. Automated Threat Hunting Platform..... 254
8. Cloud Security Misconfiguration Scanner..... 255
9. Live Attack/Defend CTF Environment..... 256
Timeline: Build Your Portfolio in 90 Days..... 256
Where to Share Your Portfolio..... 257