SOC Analyst

10 Hands-On Projects for Skills and Resume

If you're aiming for your first SOC Analyst role, certifications like Security+ or CySA+ are a great start — but hands-on experience is what truly sets you apart. Employers want proof that you can analyze alerts, investigate threats, and document incidents like a real analyst. This guide gives you 10 beginner-to-intermediate level projects that simulate actual SOC tasks.

Project List

SIEM Log Monitoring & Threat Detection
Build a Splunk or ELK Stack lab. Ingest logs and detect simulated attacks.

Simulated Phishing Attack & Incident Response
Recreate a phishing-to-malware scenario and investigate using logs.

IDS Deployment & Packet Analysis
Install Snort or Suricata and analyze alerts and pcap data with Wireshark.

Cloud Security Monitoring with AWS/Azure Logs
Enable and analyze cloud logs from CloudTrail or Azure Defender.

Endpoint Monitoring with Sysmon + Wazuh
Monitor a Windows machine using Sysmon and create detection rules.

Threat Hunting in Real Datasets
Analyze Windows or Zeek logs from real-world datasets to find hidden threats.

Security Automation Script (SOAR Lite)
Write a Python/PowerShell script to automate log parsing or IOC enrichment.

Honeypot Deployment & Threat Intel
Deploy a honeypot and collect/analyze real-world attacker behavior.

Threat Intelligence IOC Research
Investigate malware/APT campaigns, enrich indicators, and write a threat brief.

Phishing Email & Malware Analysis
Analyze phishing emails and malicious attachments in a sandboxed environment.

1. SIEM Log Monitoring & Threat Detection

Summary: Build a Splunk or ELK Stack SIEM lab. Ingest logs (e.g., Sysmon, Linux auth) and detect simulated attacks like brute force or PowerShell misuse.
Skills: SIEM use, log parsing, detection engineering, correlation.
Tools: Splunk Free, ELK Stack, Sysmon, Windows/Linux VMs.
Time: ~20–30 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐ (10/10)

What it simulates:
Real Tier 1–2 SOC alert triage, log analysis, and use case development.
Hands-on detection engineering in a monitored environment.

Add to Resume:

- "Built Splunk SIEM lab to ingest and analyze Sysmon/Windows logs; created custom detection rules for brute force and PowerShell-based attacks."
- "Simulated real-world attacks and investigated events using ELK Stack, improving response skills and detection logic."

2. Simulated Phishing Attack & Incident Response

Summary: Simulate a phishing-to-malware scenario in a lab. Investigate with logs and produce a detailed incident response report.
Skills: IR lifecycle, Windows log analysis, evidence collection, reporting.
Tools: Windows VM, Sysinternals, Event Viewer, Kali, SET.
Time: ~15–25 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐⭐⭐ (9/10)

What it simulates:
A full SOC incident involving phishing, malware, log review, containment, and documentation.
Simulates Tier 1–2 escalation and response workflow.

Add to Resume:

- "Simulated phishing attack in lab and performed full IR process including log review, malware identification, and executive-level reporting."
- "Traced infection path via Windows event logs (Event ID 4688, Sysmon logs) and documented remediation steps in formal IR report."

3. IDS Deployment & Packet Analysis

Summary: Deploy Snort or Suricata. Simulate attacks (e.g., Nmap, SQLi) and analyze alerts and PCAPs using Wireshark.
Skills: IDS/IPS, network protocols, rule tuning, packet analysis.
Tools: Snort, Suricata, Wireshark, Metasploitable, Kali.
Time: ~15–20 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐ (9/10)

What it simulates:
Real-time network intrusion detection tasks.
Alert investigation based on IDS telemetry—common in Tier 1–2 SOC environments.

Add to Resume:

- "Deployed Suricata IDS to monitor test network; generated attack traffic and tuned rules to reduce false positives and detect SQL injection attempts."
- "Investigated PCAPs using Wireshark and correlated alerts with MITRE ATT&CK TTPs."

4. Cloud Security Monitoring with AWS/Azure Logs

Summary: Enable CloudTrail or Defender logs. Simulate events (e.g., IAM abuse, unauthorized S3 access) and analyze them via console or SIEM.
Skills: Cloud security, logging, IAM misconfig detection.
Tools: AWS Free Tier, GuardDuty, CloudTrail, ELK/Splunk.
Time: ~10–20 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐ (9/10)

What it simulates:
Tier 1/2 monitoring of cloud security logs in modern hybrid SOCs.
Detecting IAM privilege escalation, misconfigurations, cloud anomalies.

Add to Resume:

- "Configured AWS CloudTrail/GuardDuty to detect and alert on suspicious IAM events including unauthorized access and misconfigured S3 buckets."
- "Analyzed cloud logs and set up alerting rules to simulate SOC Tier 2 cloud monitoring workflows."

5. Endpoint Monitoring with Sysmon + Wazuh

Summary: Use Sysmon and Wazuh for endpoint log collection. Simulate malware behavior and trigger alerts on suspicious actions.
Skills: Host-based detection, event ID mapping, Sigma/YARA rules.
Tools: Sysmon, Wazuh, Windows VM, PowerShell.
Time: ~10–15 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐⭐ (8/10)

What it simulates:
Tier 1–2 endpoint alert investigation in EDR-like setups (e.g., CrowdStrike, Defender ATP).
Detecting suspicious behavior via host logs (e.g., credential dumping, persistence).

Add to Resume:

- "Ingested Sysmon logs into Wazuh and developed custom alert rules to detect credential dumping and persistence tactics."
- "Simulated malware behavior and validated endpoint alerts via process tree and registry activity."

6. Threat Hunting in Real Datasets

Summary: Analyze log datasets (Windows, Zeek) for anomalies. Build a timeline of attacker activity based on raw logs.
Skills: SPL/KQL, anomaly detection, ATT&CK mapping.
Tools: Splunk, Elastic, CyberDefenders datasets.
Time: ~10–20 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐⭐ (8/10)

What it simulates:
Tier 2 threat hunting workflow: identify suspicious patterns missed by alerts.
Investigation using structured queries and hypothesis-driven analysis.

Add to Resume:

- "Performed threat hunt on Zeek and Windows log dataset; identified lateral movement and brute-force login indicators using SPL queries."
- "Mapped findings to MITRE ATT&CK framework and built a comprehensive attack timeline."

7. Security Automation Script (SOAR Lite)

Summary: Build a Python or PowerShell script to enrich IOCs, parse logs, or auto-tag suspicious events.
Skills: Scripting, API use, automation logic.
Tools: Python, VirusTotal API, AbuseIPDB, log samples.
Time: ~8–15 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐⭐ (7/10)

What it simulates:
Automating Tier 1 enrichment and triage tasks seen in SOAR platforms.
Saves analyst time by streamlining manual processes.

Add to Resume:

- "Developed Python script to enrich IOC indicators via VirusTotal/AbuseIPDB APIs and summarize alert context in JSON reports."
- "Automated noisy log filtering using PowerShell to support faster SOC response."

8. Honeypot Deployment & Threat Intel

Summary: Set up Cowrie SSH honeypot to capture attacker activity. Analyze login attempts, files, and attacker IPs.
Skills: Real attacker interaction, log analysis, OSINT enrichment.
Tools: Cowrie, ELK, VirusTotal, DigitalOcean.
Time: ~15 hrs over 1–2 weeks
Cost: $0–$10
Resume Value: ⭐⭐⭐⭐⭐⭐⭐ (7/10)

What it simulates:
External threat intelligence monitoring, IOC extraction, and attack analysis.
Observing real brute-force and botnet behavior.

Add to Resume:

- "Deployed SSH honeypot in cloud VM; captured and analyzed 5,000+ attacker attempts including common TTPs and password combos."
- "Enriched IPs with OSINT tools and documented findings in threat brief."

9. Threat Intelligence IOC Research

Summary: Research malware/APT, collect IOCs, enrich with tools (e.g., VirusTotal), and build a threat profile.
Skills: IOC research, enrichment, ATT&CK mapping, reporting.
Tools: VirusTotal, OTX, WHOIS, MISP.
Time: ~10–15 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐ (6/10)

What it simulates:
SOC threat intelligence feed handling, watchlist creation, adversary profiling.
Assists Tier 2–3 analysts with threat correlation and prevention.

Add to Resume:

- "Compiled threat report on Emotet malware campaign with enriched IOCs and MITRE TTP mapping; integrated with open-source MISP platform."
- "Correlated indicators across logs and feeds to identify targeted activity."

10. Phishing Email & Malware Analysis

Summary: Analyze phishing email headers, malicious links, and malware attachments in a sandbox. Extract and report IOCs.
Skills: Email forensics, malware sandboxing, IOC extraction.
Tools: Any.Run, VirtualBox, VirusTotal, Wireshark.
Time: ~6–12 hrs
Cost: $0
Resume Value: ⭐⭐⭐⭐⭐⭐ (6/10)

What it simulates:
Tier 1 SOC phishing response—analyzing user-reported suspicious emails.
Triage of email threats and basic malware behavior analysis.

Add to Resume:

- "Analyzed phishing email with malicious doc attachment; performed sandbox detonation and extracted PowerShell-based downloader behavior."
- "Mapped attack to initial access vector and blocked indicators at firewall and EDR levels."