HOW TO BECOME A

SOC Analyst

in 2026

Skills • Tools • AI • 12-Week Roadmap

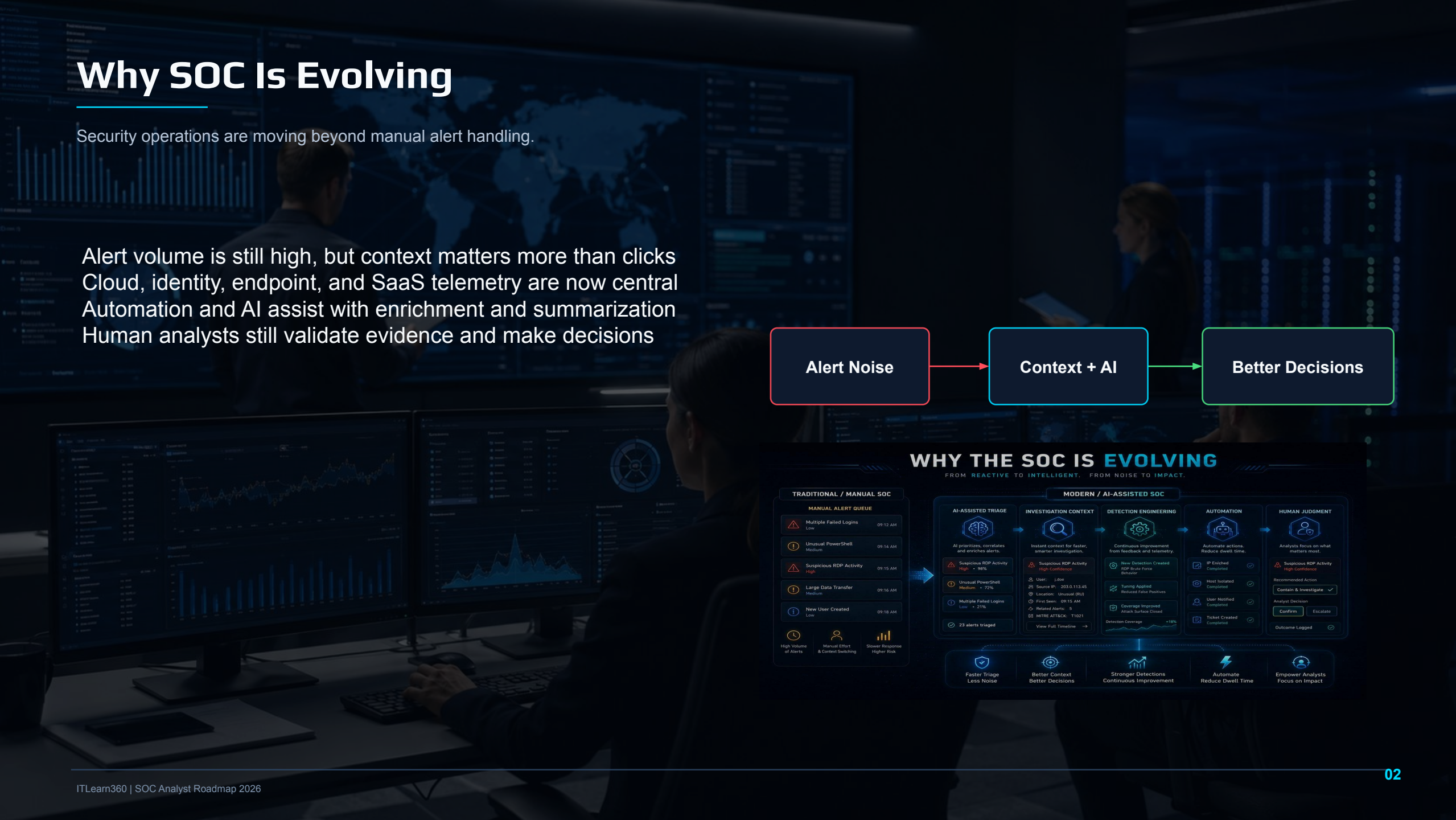
A practical, beginner-friendly path into modern security operations.

Alert | Investigate | Detect | Automate

Why SOC Is Evolving

Security operations are moving beyond manual alert handling.

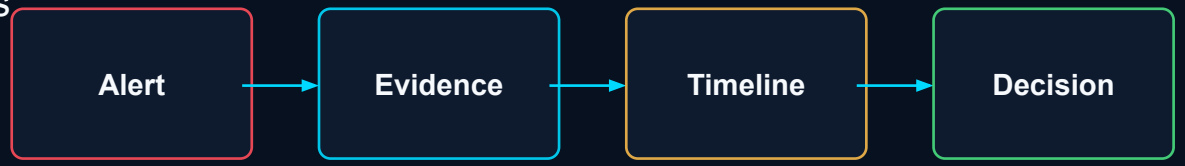
Alert volume is still high, but context matters more than clicks
Cloud, identity, endpoint, and SaaS telemetry are now central
Automation and AI assist with enrichment and summarization
Human analysts still validate evidence and make decisions



What a SOC Analyst Actually Does

The analyst turns alerts and evidence into decisions.

Reviews alerts from SIEM, EDR, identity, cloud, network, and email tools
Collects evidence from users, devices, IPs, files, processes, and logs
Builds timelines, determines scope, and escalates real incidents
Documents findings and recommends detection or response improvements



Practical example

A suspicious login alert becomes an investigation: user, location, device, MFA status, recent activity, and business impact.

SOC Responsibility Levels

Tiers are common, but every organization structures SOC work differently.

Entry / Triage

Validate alerts, collect context, follow playbooks, document notes, and escalate when criteria are met.

Investigation Analyst

Scope incidents, reconstruct timelines, analyze endpoint and identity evidence, and write incident reports.

Senior / Proactive Defense

Threat hunting, detection engineering, automation, tuning, mentoring, and process improvement.

Progression moves from guided triage to independent investigation
Senior roles usually require stronger query, detection, and response skills
Titles vary: SOC Analyst, Security Operations Analyst, MDR Analyst, Detection Analyst

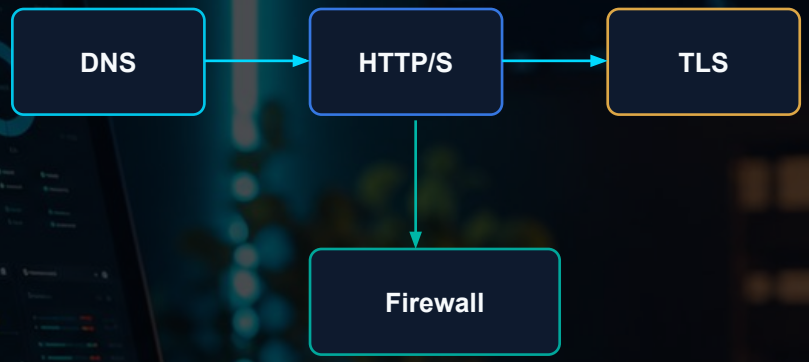
Core Foundations for SOC Analysts

Tools change, but these skills keep you useful.

Networking and Packet Analysis

Understand how traffic creates evidence.

TCP/IP, DNS, HTTP/HTTPS, TLS, ports, proxies, VPNs
Firewall, DNS, proxy, and VPN logs reveal movement and access
Wireshark helps inspect packet captures and protocol behavior
Zeek can produce structured network-security telemetry



Analyst mindset

Do not only read IPs and ports. Ask what the traffic means and whether it fits expected behavior.

Windows and Linux Endpoint Evidence

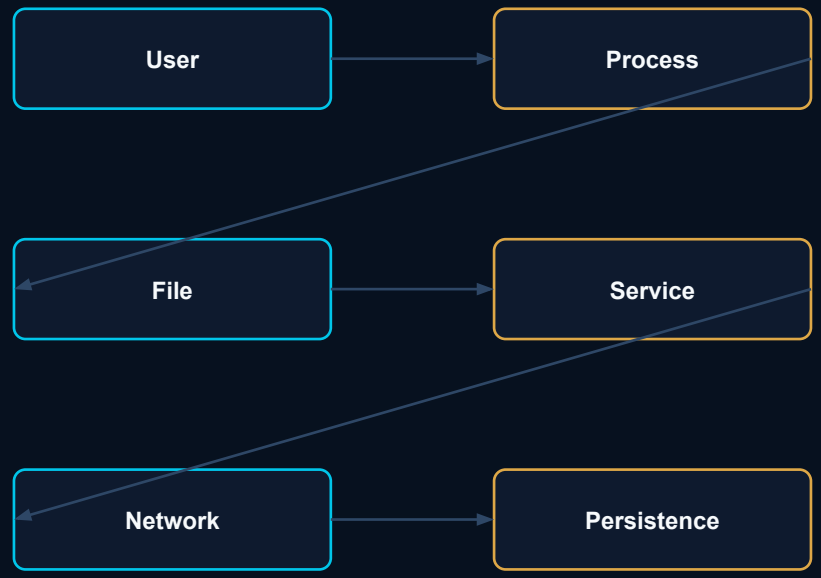
Endpoints show what actually happened on the device.

Windows Evidence

Event Logs, authentication events, process creation, PowerShell, services, scheduled tasks, registry activity, Sysmon telemetry.

Linux Evidence

Authentication logs, users and groups, permissions, processes, services, cron jobs, shell history, syslog, package changes.



Logs, SIEM, and Query Skills

Modern SOC work depends on searching the right data correctly.

- Understand events, fields, timestamps, schemas, parsing, and normalization
- Learn one query language deeply: KQL, SPL, Elastic KQL, ES|QL, or SQL basics
- Use queries to validate alerts, hunt, tune detections, and write reports
- Always ask what data may be missing or misleading

Example query goal

Find failed sign-ins followed by a successful login from a new location or device.

Essential SOC Tool Map

Learn categories first, then pick one platform deeply.

SIEM

Sentinel • Splunk • Elastic • Wazuh
Collect, correlate, detect, investigate

EDR / XDR

Defender • CrowdStrike • Elastic Defend
Endpoint timelines and containment

Network

Wireshark • Zeek • DNS • Firewall
Traffic and connection evidence

SOAR / Case

Playbooks • tickets • enrichment
Automate repeatable response steps

Identity + Cloud

Entra • M365 • AWS • GCP
Sign-ins, audit logs, roles, SaaS

Strategy: one SIEM deeply + basic familiarity across the stack

EDR and XDR Investigation

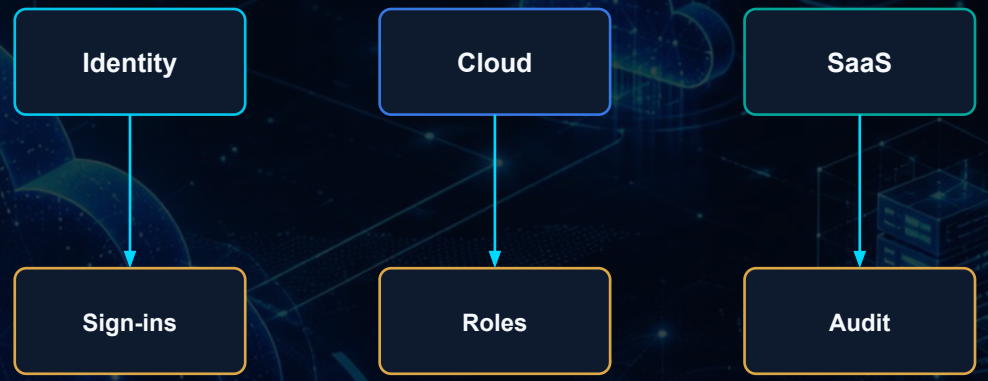
Endpoint timelines help prove what ran, when, and under which user.

Investigate process trees, command lines, files, hashes, and network connections
Review device timelines and related user activity
Look for persistence, suspicious scripts, lateral movement, and impact
Containment actions require approved procedures and careful validation

Cloud and Identity Monitoring

Identity is often the control plane for modern attacks.

Review sign-in logs, audit logs, MFA events, and risky activity
Monitor privileged roles, service principals, workload identities, and admin changes
Use cloud logs such as Azure Activity, AWS CloudTrail, and Google Cloud audit logs
Correlate identity, endpoint, cloud, SaaS, and email evidence



Incident Response Workflow

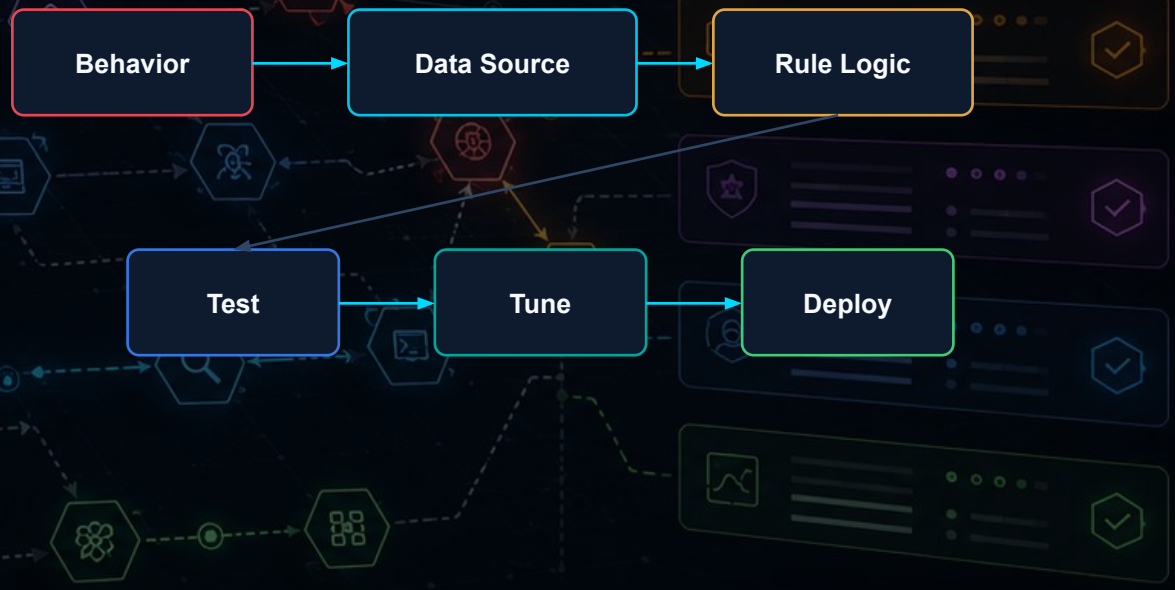
Use a repeatable process so investigations stay consistent.

Confirm whether the alert is real and collect evidence
Identify affected users, devices, systems, and cloud resources
Contain using approved procedures; preserve important evidence
Document decisions, remediation, and detection improvements

MITRE ATT&CK and Detection Engineering

Map behavior to evidence, then build better detections.

ATT&CK helps describe adversary tactics and techniques
Use evidence before mapping a technique
Detection engineering turns suspicious behavior into testable logic
Good detections include data source, query, guidance, tuning notes, and ATT&CK mapping



Threat Hunting

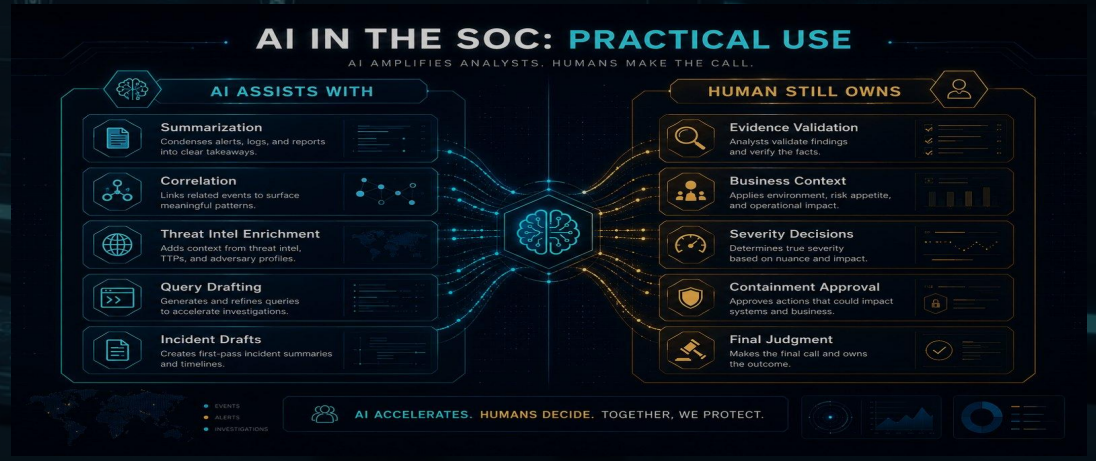
Search proactively when alerts are not enough.

Start with a hypothesis: what behavior are we looking for?
Identify the data needed before writing queries
Pivot across users, devices, IP addresses, files, and cloud resources
Convert useful hunt logic into detections when appropriate

AI in the SOC: Reality vs. Hype

AI can accelerate investigation, but it does not own the decision.

Useful for summarization, enrichment, query drafting, and preliminary reports
Can suggest investigation steps and help correlate related signals
May assist with supported alert triage depending on platform capabilities
Analysts must validate results against original evidence



Responsible AI Workflow

Use AI as an assistant, not as an unchecked authority.

Approved Tool

Use only approved services

Protect Data

Never expose confidential logs

Validate Output

Compare with original evidence

Check Queries

Review generated logic first

Human Approval

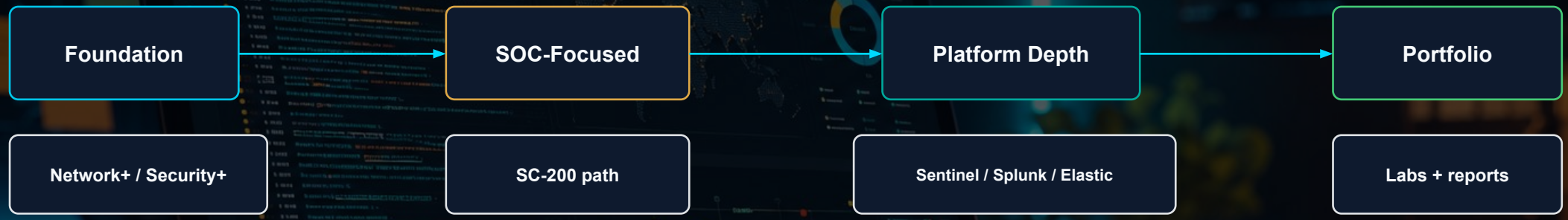
Keep high-impact actions human-led

Document Use

Record AI assistance when required

Certification Path

Use certifications to structure learning, not replace projects.



Verify current exam objectives, pricing, and retirement dates before registering
Pick platform training based on the jobs and tools you are targeting
Your strongest proof is a documented SOC portfolio

12-Week SOC Analyst Curriculum

A practical path from fundamentals to capstone portfolio.

Week 1
SOC workflow

Week 2
Networking

Week 3
Windows

Week 4
Linux

Week 5
SIEM queries

Week 6
Triage

Week 7
EDR/XDR

Week 8
Cloud + identity

Week 9
ATT&CK + detections

Week 10
Threat hunting

Week 11
SOAR + AI

Week 12
Capstone

Final deliverable: investigation report + queries + detection + hunt + automation + AI validation note

Portfolio Projects and Resume Positioning

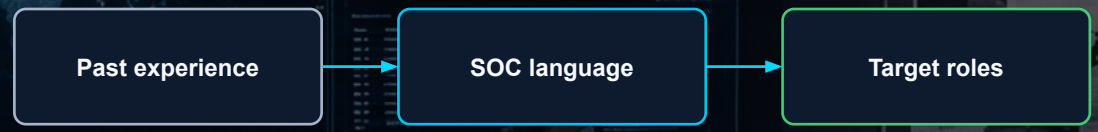
Show evidence of work without exaggerating experience.

Portfolio Projects

SIEM diagram, query workbook, triage worksheet, incident report, detection rule, ATT&CK map, threat-hunt report, SOAR workflow.

Resume Language

Describe labs as hands-on projects. Use terms such as triage, logs, SIEM queries, investigation, detection, and incident report.



Search: SOC Analyst, Security Operations Analyst, SIEM Analyst, MDR Analyst
Transferable skills: tickets, troubleshooting, evidence, documentation, reporting
Never present lab work as enterprise production experience

Final Roadmap and Next Step

Understand. Practice. Prove. Apply.

Start with one lab. Document it clearly. Keep building.

For structured technology learning and career-focused guidance, explore ITLearn360.

Source notes: Microsoft Learn • NIST • MITRE ATT&CK • Wireshark • Wazuh • Splunk • Elastic