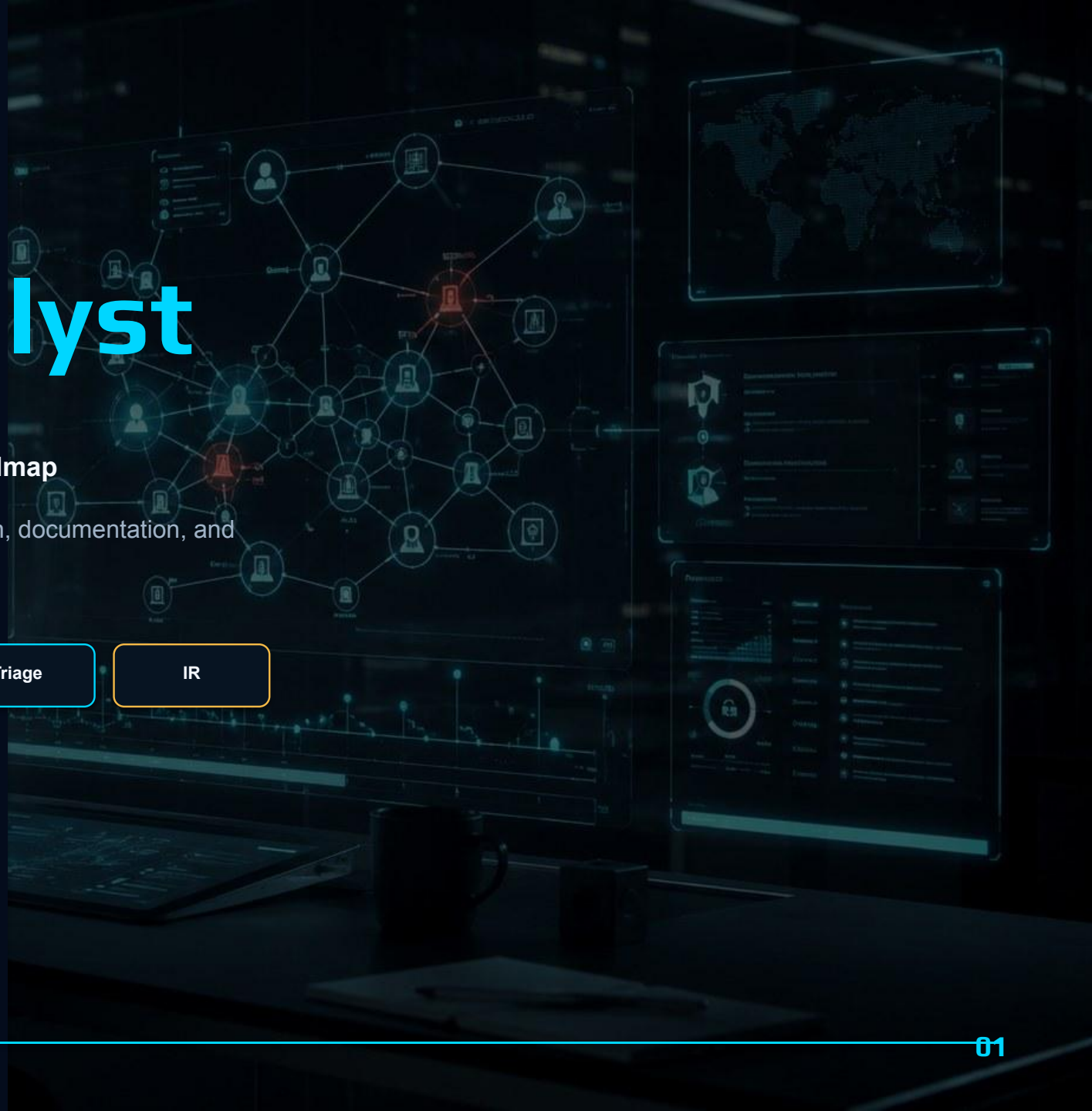
HOW TO BECOME A

Cybersecurity Analyst

12-Week SOC Skills • SIEM • EDR • Incident Response Roadmap

A practical, beginner-friendly path built around evidence, investigation, documentation, and portfolio projects.

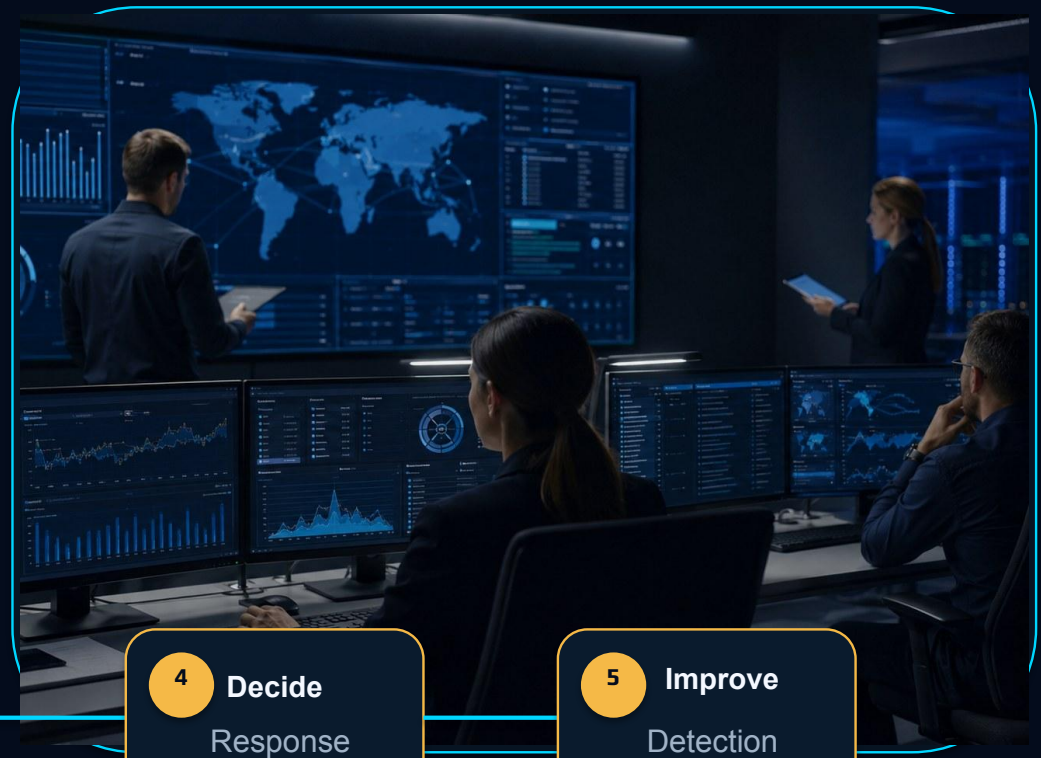
Network | Windows | Linux | SIEM | Triage | IR



Why Cyber Analyst Skills Matter

Cybersecurity work becomes clearer when you learn the investigation workflow.

- The field has many tools, but the core work is practical
- Analysts collect evidence, analyze activity, and make decisions
- Modern work includes endpoint, identity, cloud, SIEM, and response workflows



1 **Understand** Environment

2 **Collect** Evidence

3 **Analyze** Activity

4 **Decide** Response

5 **Improve** Detection

What a Cybersecurity Analyst Actually Does

The analyst converts suspicious activity into evidence-based decisions.

- Reviews alerts from SIEM, endpoint, identity, network, cloud, and email tools
- Collects evidence from users, devices, IPs, logs, files, and timelines
- Escalates incidents, writes reports, and improves detections

Practical example

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

Alert → Evidence → Timeline → Decision

12-Week Roadmap Overview

A focused path from foundations to portfolio evidence.

- Month 1: networking, Windows, Linux, and telemetry basics
- Month 2: SIEM, detections, endpoint, identity, and threat context
- Month 3: triage, incident response, automation, portfolio, and interviews

1 Month 1
Foundations

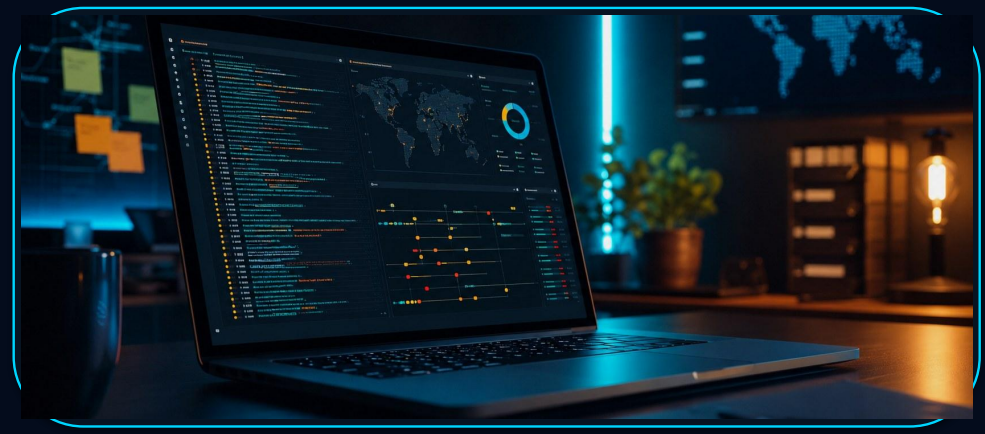
2 Month 2
SIEM + Threat Analysis

3 Month 3
IR + Portfolio

Networking and Core Protocols

Understand how systems communicate and what evidence traffic leaves behind.

- TCP/IP, IPv4, ports, DNS, DHCP, HTTP/S, TLS, VPNs, proxies, and firewalls
- Learn normal versus suspicious connection behavior
- Use packet captures to support investigation conclusions

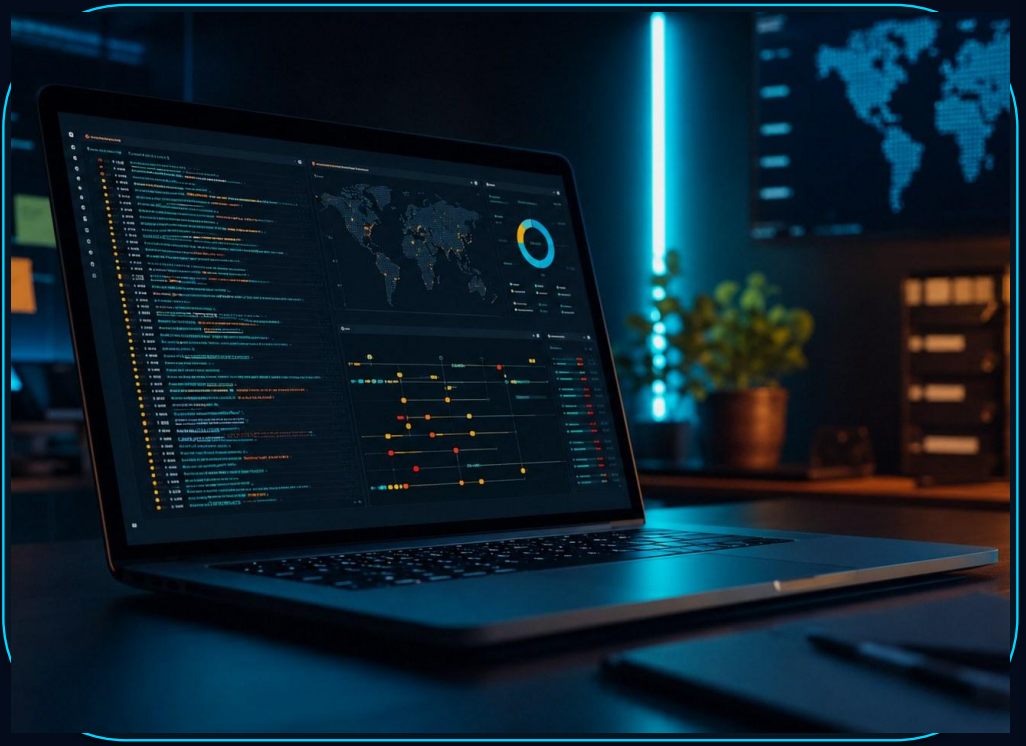


DNS | HTTP/S | TLS | VPN | Firewall

Analyst mindset: What does this traffic mean, and does it fit expected behavior?

Packet Analysis Lab

A PCAP teaches you to ask better questions about network activity.



- Identify DNS lookups, web connections, source and destination IPs
- Separate normal activity from repeated or unusual connections
- Document filters, evidence, timeline, limitations, and conclusion

1 Capture
sample traffic

2 Filter
DNS/HTTP/IPs

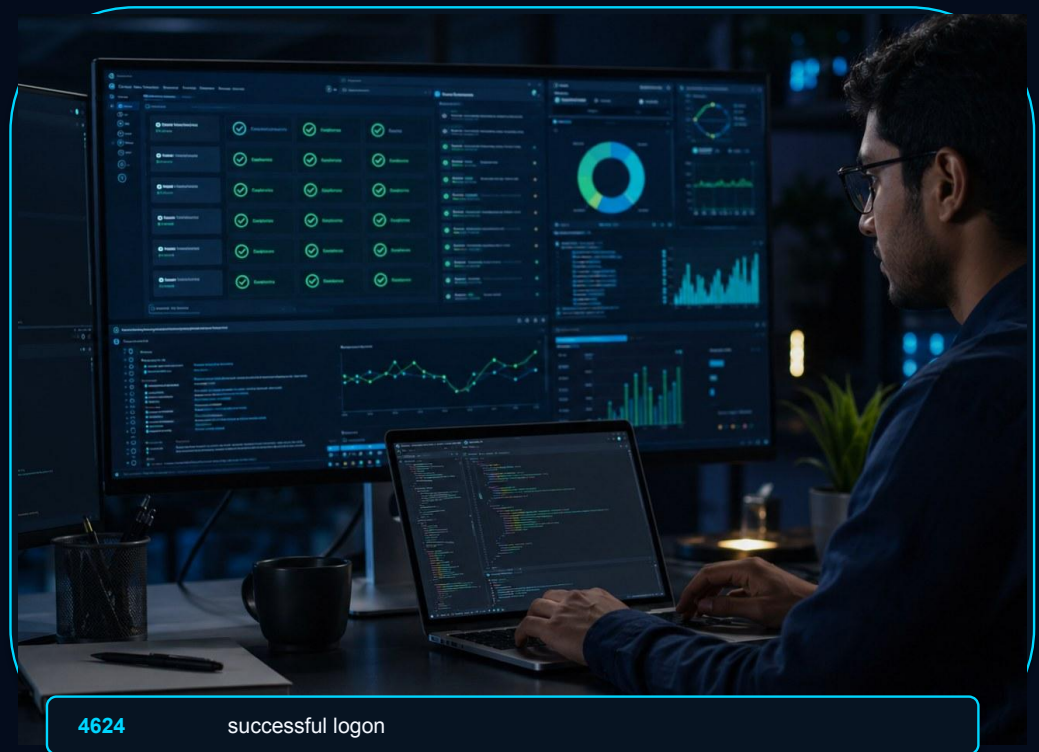
3 Compare
normal vs unusual

4 Report
evidence + limits

Windows Security Evidence

Windows logs show users, processes, authentication, and endpoint behavior.

- Event Viewer: Security, System, and Application logs
- Useful examples: 4624 successful logon, 4625 failed logon, 4688 process creation
- Sysmon can add process, network, and file-activity telemetry



4624	successful logon
4625	failed logon
4688	process creation
Sysmon	extra telemetry

Linux Security Evidence

Linux command-line skills help analysts inspect systems and logs.

- Users, groups, permissions, processes, services, packages, and scheduled jobs
- Authentication logs, syslog, shell history, and journalctl are important evidence
- Practice using grep, tail, ps, ss, find, and journalctl

grep | **tail** | **ps**

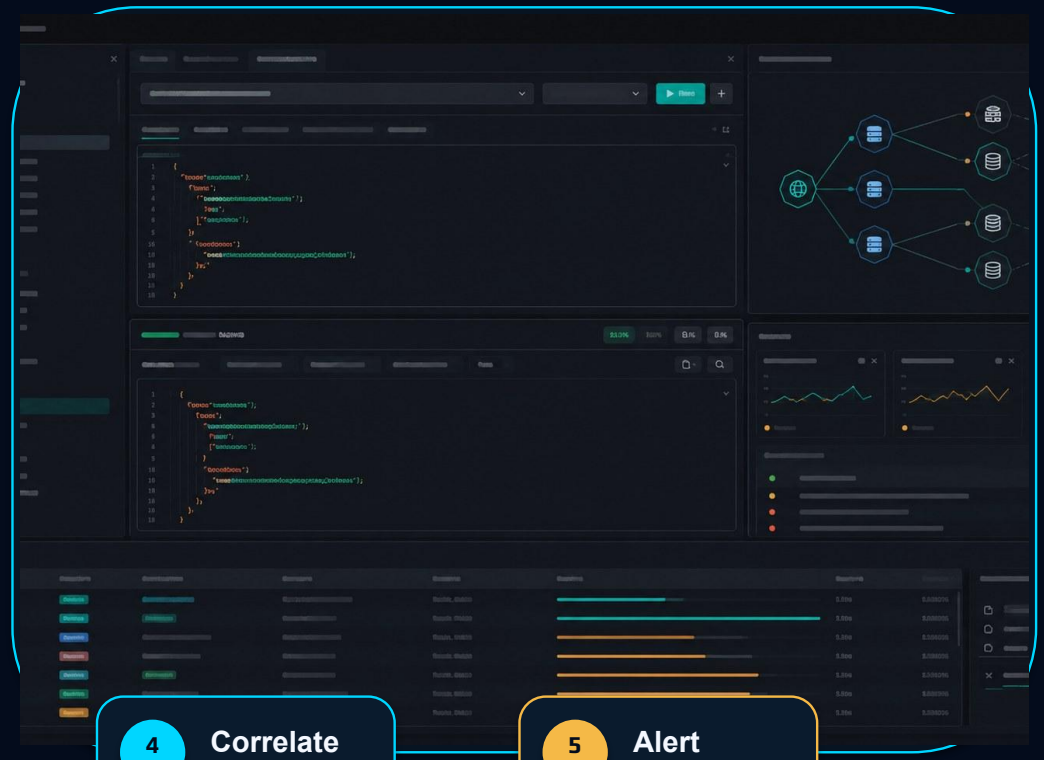
ss | **find** | **journalctl**

Goal: commands + logs + timeline + conclusion

SIEM and Log Analysis

A SIEM helps collect, search, correlate, and investigate security data.

- Start with one platform: Wazuh, Microsoft Sentinel, Splunk, or Elastic
- Understand events, alerts, fields, schemas, timestamps, and parsing
- Build queries for failed logins, new users, admin changes, and suspicious commands



1 **Collect** security data

2 **Parse** security data

3 **Query** security data

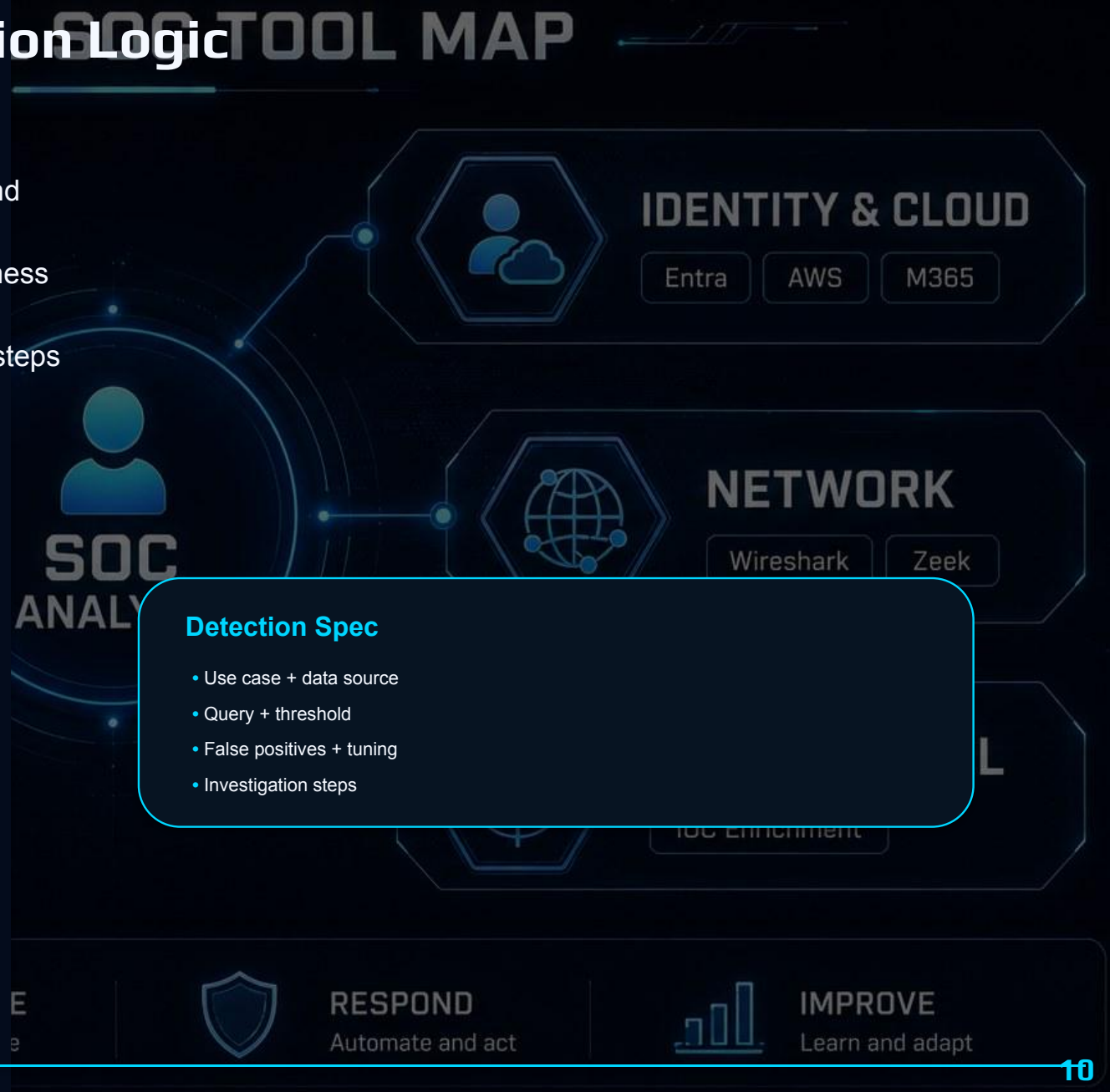
4 **Correlate** security data

5 **Alert** security data

Query Development and Detection Logic

Dashboards are not enough; analysts must understand detection rules.

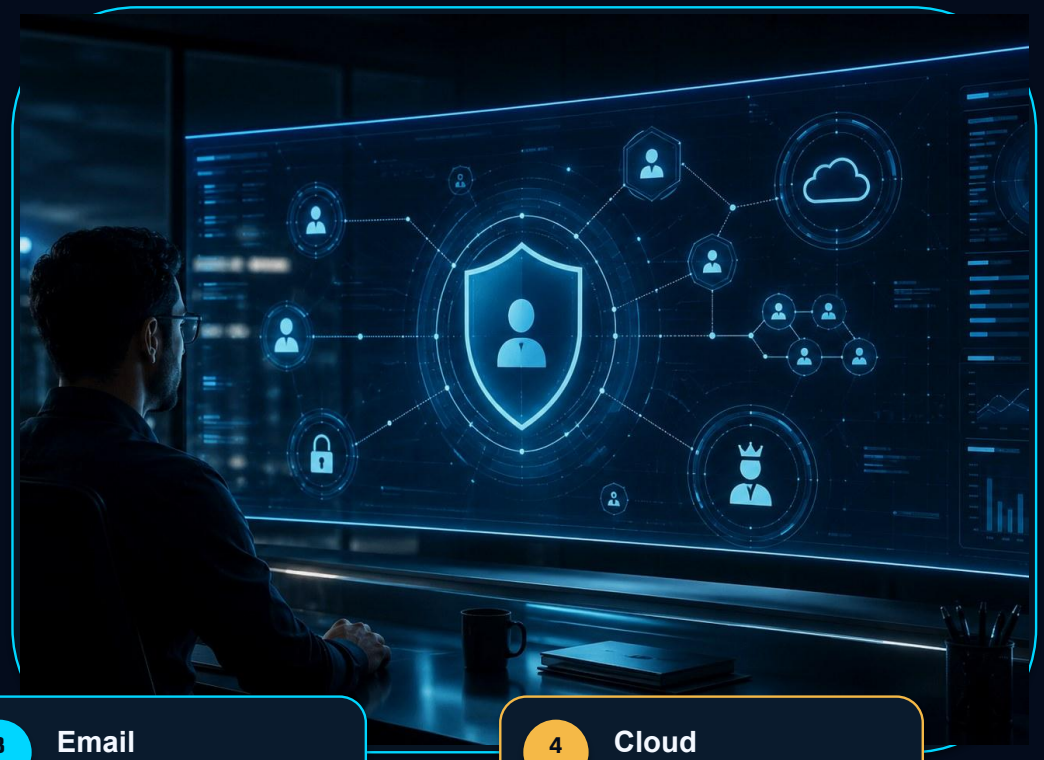
- Define the use case, required data, time window, threshold, and query logic
- Combine indicators with behavior, identity, endpoint, and business context
- Document false positives, tuning decisions, and investigation steps



Endpoint, Identity, Email, and Cloud Monitoring

Modern investigations connect several evidence sources.

- Endpoint: process trees, command lines, files, hashes, network connections
- Identity: sign-ins, MFA, risky activity, roles, and account changes
- Email and cloud logs show phishing, admin actions, and SaaS activity



1 Endpoint
Process trees, command lines

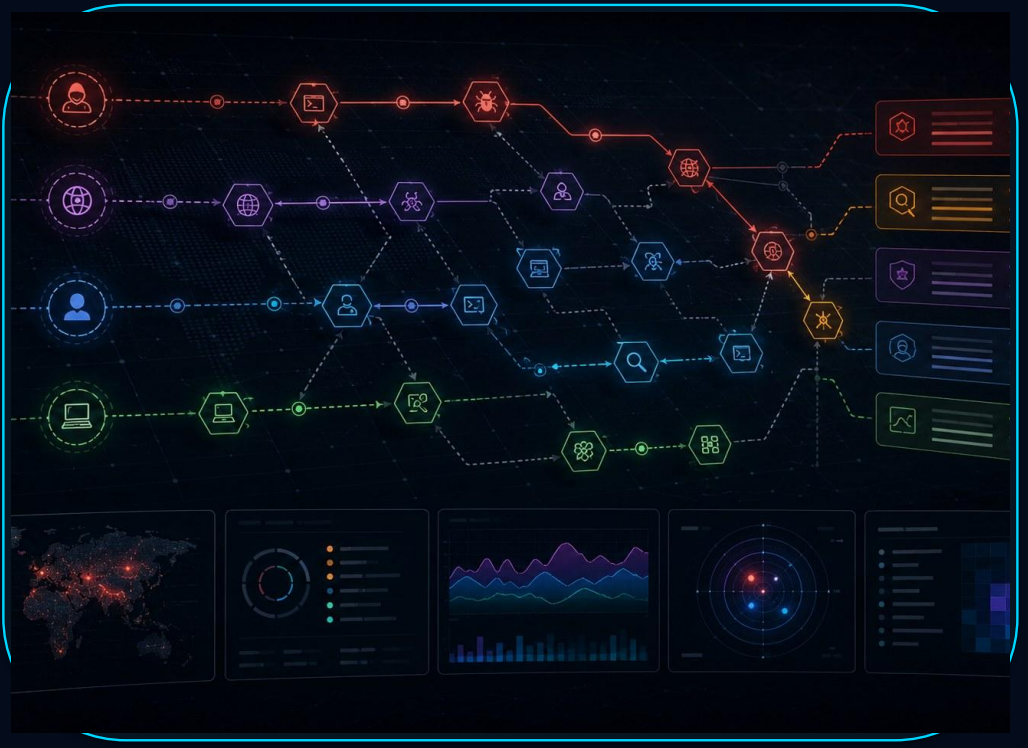
2 Identity
Sign-ins, MFA, roles

3 Email
Links, headers, attachments

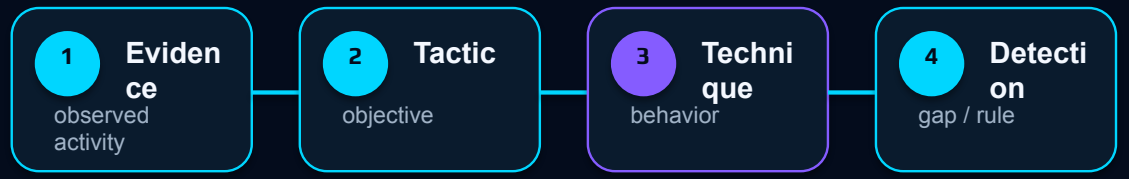
4 Cloud
Audit logs, role changes

MITRE ATT&CK and Threat Intelligence

Use ATT&CK to describe behavior, not to decorate reports.



- Map observed evidence to tactics and techniques
- Understand the difference between indicators and behavior
- Use threat intelligence carefully with confidence and context



Alert Triage Workflow

Triage decides whether suspicious activity needs deeper response.

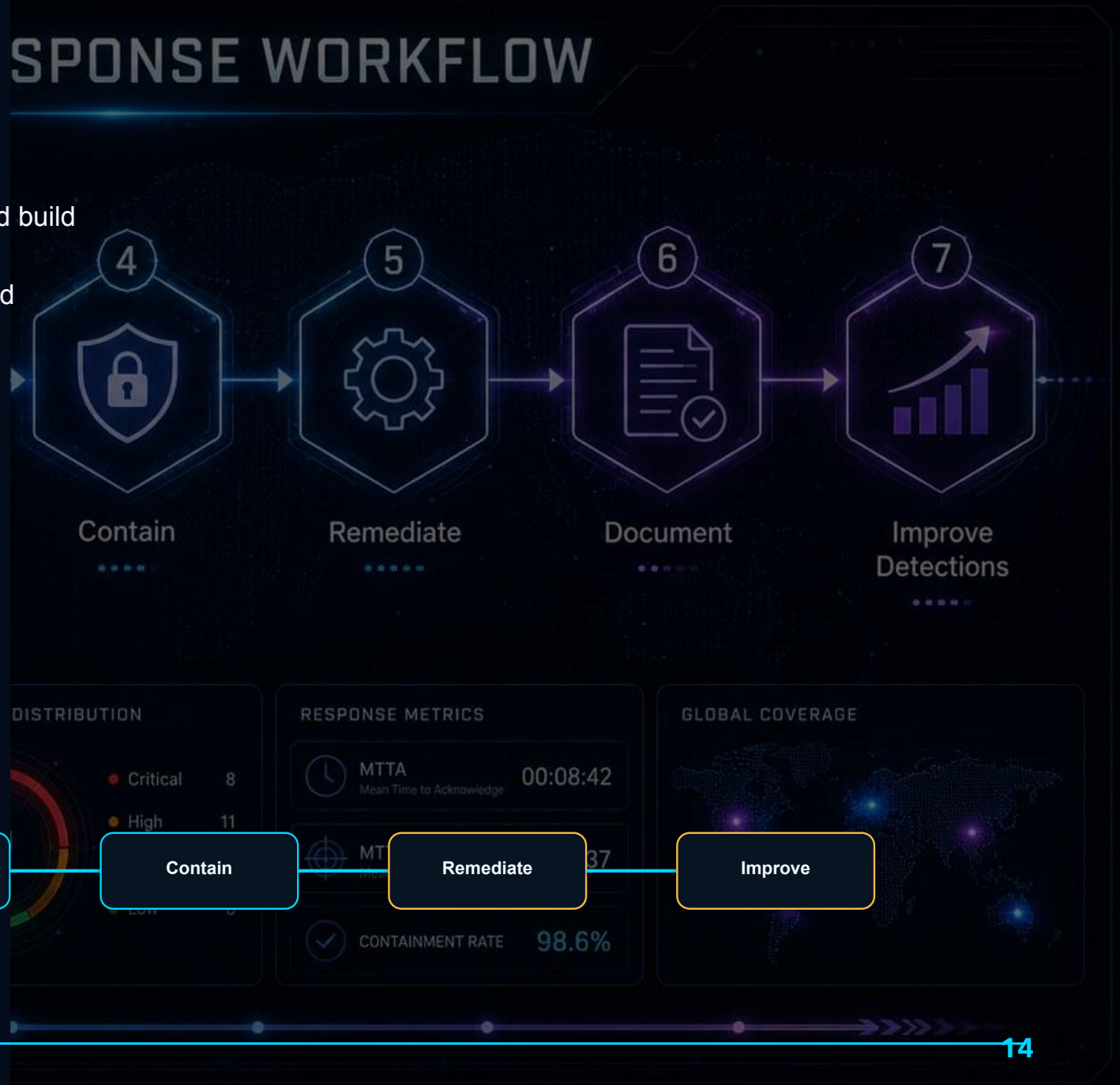
- Validate the alert and enrich the user, device, IP, and process context
- Create an investigation hypothesis and timeline
- Decide whether to close, escalate, or request more evidence

Analyst: “I will validate the alert, enrich the entities, build the timeline, and escalate only if the evidence supports it.”

Incident Response Workflow

Use a repeatable process so investigations stay consistent.

- Validate alert, identify affected resources, collect evidence, and build a timeline
- Determine scope and impact, escalate, contain, remediate, and recover
- Document decisions and improve detections or playbooks

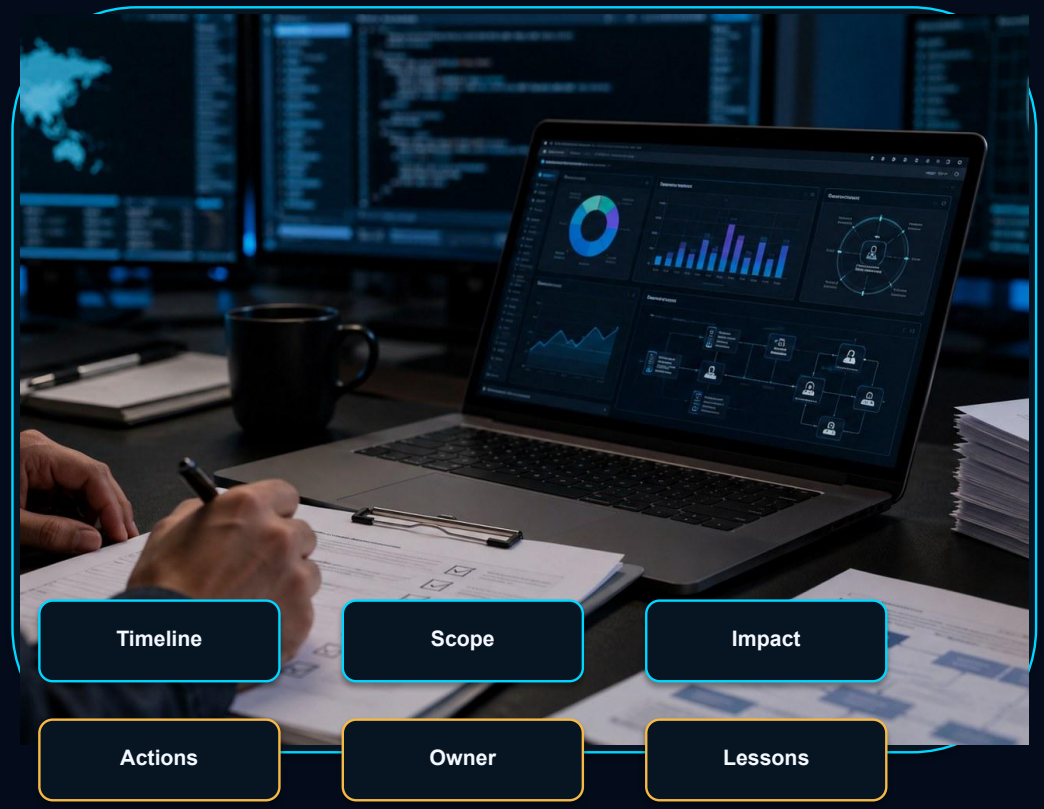


Validate → Scope → Timeline → Contain → Remediate → Improve

Incident Reporting and Ticketing

Good analysts explain technical evidence in business language.

- Write concise incident tickets with timeline, scope, impact, and next actions
- Create executive summaries for non-technical stakeholders
- Track remediation, owners, lessons learned, and detection improvements



Basic Automation and Responsible AI Assistance

Automation and AI can accelerate work, but judgment stays with the analyst.

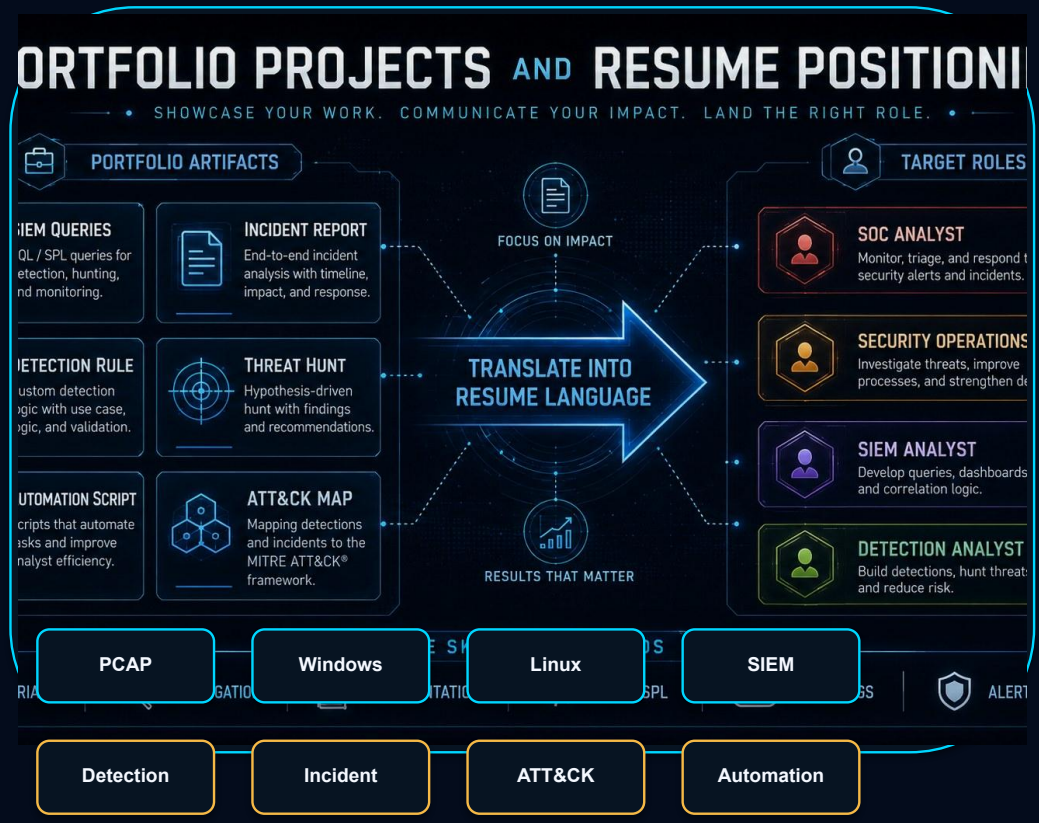
- Use PowerShell or Python for enrichment, CSV/JSON handling, and simple workflows
- Use approved AI tools for summarization, query drafting, and report drafts
- Protect sensitive data and validate every generated conclusion

1. **Use approved tools**
2. **Validate output**
3. **Human decision**

Portfolio Package

Show practical work without exaggerating lab experience.

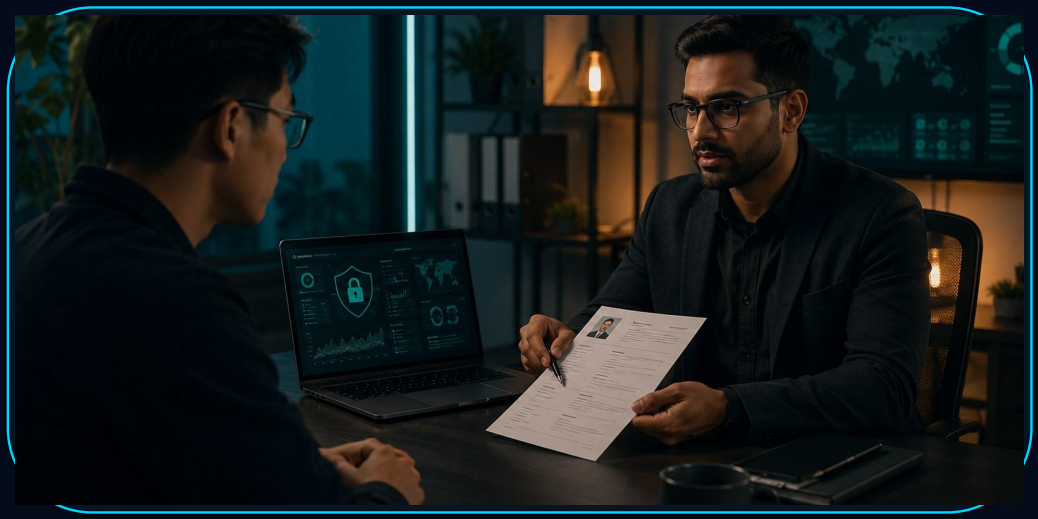
- Network PCAP analysis, Windows and Linux investigations, SIEM query workbook
- Detection rule, ATT&CK mapping, threat-intelligence assessment, incident report
- Automation workflow and validation checklist



Interview Preparation

Be ready to explain how you think through evidence.

- Explain DNS, events versus alerts versus incidents, and alert validation
- Walk through repeated failed logins, endpoint evidence, and SIEM detections
- Explain incident scope, isolation decisions, and missing evidence



Interviewer: “Walk me through a failed-login alert.”
Candidate: “I would validate the pattern, enrich the source, review user context, check endpoint activity, and document the decision.”

Final Roadmap and Next Step

Understand. Investigate. Document. Improve.

- Build foundations, learn one SIEM, investigate endpoint and identity evidence
- Create detections, follow incident-response workflows, and automate carefully
- Start with one lab, document it clearly, and keep building

1 **Understand**
network + OS

2 **Investigate**
logs + evidence

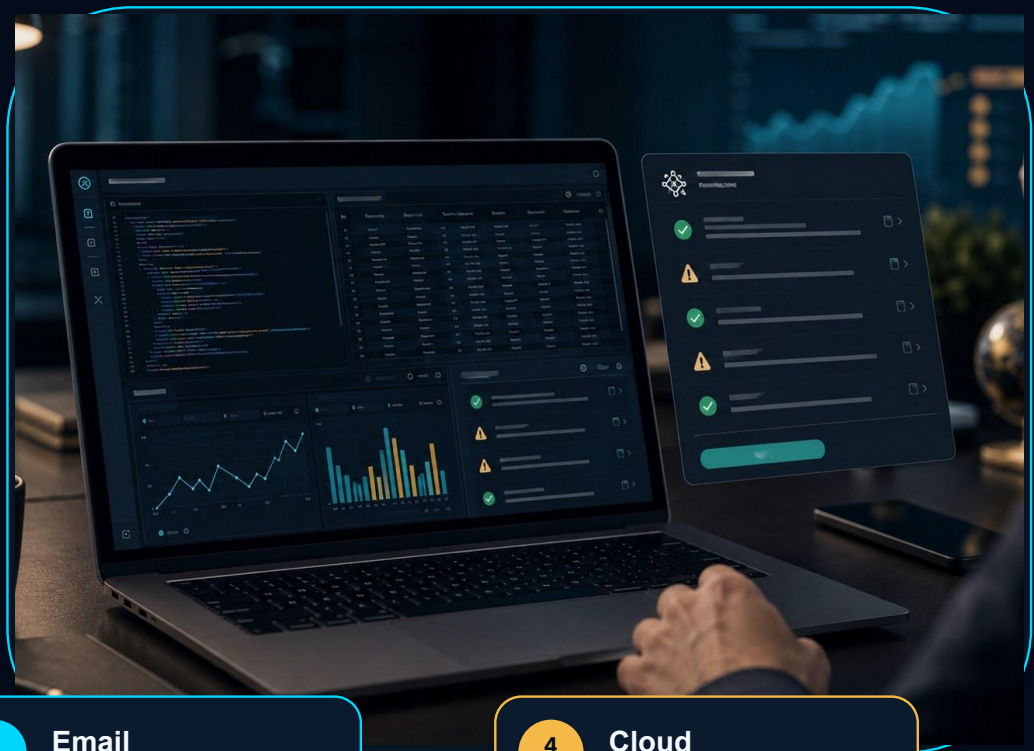
3 **Document**
reports + tickets

4 **Improve**
detections + portfolio

Source and Data Integrity Note

Use current sources, avoid unsupported claims, and keep the message practical.

- Current guidance checked: NIST SP 800-61 Rev. 3, Microsoft Learn, MITRE ATT&CK
- Tools included as examples: Wazuh, Wireshark, Sysmon, Sentinel, Splunk, Elastic
- No salary, job-growth, or guaranteed-employment figures are included



1 **Endpoint**
Process trees, command lines

2 **Identity**
Sign-ins, MFA, roles

3 **Email**
Links, headers, attachments

4 **Cloud**
Audit logs, role changes