SKUNKWORKS ACADEMY

Individual Development Roadmap

Nkateko Mtembi

SOC Operations · Wazuh SIEM · Threat Detection · Incident Response · Cloud Security

Recommended development placement

Primary: Junior SOC Analyst !’ SOC Analyst / Security Operations Analyst
Secondary growth: Detection Engineering / Cloud Security
Learning mode: self-paced, hands-on and evidence based
Initial execution: 12-week applied sprint
Long-term direction: security operations leadership and subject-matter growth

Executive Summary

Source-based starting point

Nkateko's submitted career assessment identifies strong interest in SIEM platforms, a preference for self-paced learning, willingness to invest substantial weekly time in learning, interest in Cisco, GitHub, Google and professional skills, and a desire to move into employment, increase earning potential and ultimately reach a leadership position.

The supplied professional profile describes an aspiring Junior SOC

Analyst already building a Wazuh SIEM home lab, with practical focus on threat detection, log analysis and incident response. Existing profile strengths include cloud security, security monitoring, Windows fundamentals, networking and several foundation cybersecurity/networking credentials.

Recommended development placement

Primary pathway: Junior SOC Analyst !’ SOC Analyst / Security Operations Analyst

Secondary growth pathway: Detection Engineering / Cloud Security Analyst

Long-term direction: Security operations leadership, subject-matter expertise and mentoring

The secondary and long-term pathways are recommendations derived from the submitted interests, portfolio direction and stated leadership ambition; they are not claims of current role seniority.

Development priorities

1. Windows security telemetry and event-log investigation.
2. Wazuh administration, alert triage, rule tuning and detection logic.
3. Networking and packet-analysis fundamentals for SOC investigations.

4. Incident response, evidence handling and escalation discipline.
5. MITRE ATT&CK mapping, threat intelligence and detection engineering basics.
6. Git/ GitHub workflow and evidence-quality portfolio development.
7. Cloud-security fundamentals with a vendor-neutral control mindset.
8. Professional communication, concise incident writing and regular mentor feedback.
9. Time-management habits that balance work and sustained learning.
10. Interview readiness and visible evidence for junior SOC opportunities.

12-month North Star

By the end of the roadmap, Nkateko should be able to investigate common Windows and network security events, operate and tune a SIEM, document incident decisions, create and test basic detection logic, explain common attacker techniques, demonstrate cloud-security fundamentals, collaborate through GitHub and present a credible evidence portfolio for junior SOC and security-operations roles.

Evidence standard

A course or certificate records learning; it does not ind

ependently prove operational capability. Progress is demonstrated through investigations, lab notes, detection rules, runbooks, GitHub repositories, mentor review and the ability to explain decisions under questioning.

Capability Profile

This public profile is intentionally sanitised. It uses the submitted assessment and professional profile to establish a development baseline without publishing private contact details.

Current profile evidence

- aspiring Junior SOC Analyst;
- hands-on Wazuh SIEM home lab experience;
- practical interest in threat detection, log analysis and incident response;
- stated strengths in cloud security, security monitoring and Windows;
- foundation networking/cybersecurity learning through Cisco and Google programmes;
- public SOC Analyst portfolio already exists on GitHub;
- current interests include SIEM platforms, AI, website building and cybersecurity learning;
- preferred learning mode is self-paced, with regular one-on-one feedback;
- comfortable working independently and collaboratively;
- willing to participate in cross-functional projects.

Existing foundation learning

The supplied profile lists foundation achievements including:

- Networking Devices and Initial Configuration;
- Introduction to Cybersecurity;
- Google Cybersecurity Professional Certificate;
- Networking Basics;
- Cybersecurity and Cloud Fundamentals 1.0.

These provide a useful starting point. The IDR focuses on converting that learning into repeatable investigation and operational evidence.

Strengths to leverage

Strength · How the roadmap uses it

--- · ---

Wazuh home-lab initiative · Becomes the main SIEM/detection laboratory

Security monitoring interest	Drives triage, alert analysis and detection exercises
Windows familiarity	Becomes the foundation for Event Viewer/ Sysmon/ Windows event investigations
Networking fundamentals	Supports packet analysis, source/ destination reasoning and network triage
Problem solving	Applied to incident hypotheses and investigation logic
Creativity	Used in lab design, detection ideas and portfolio presentation
Communication awareness	Developed through incident notes, one-page briefs and mentor

review

High learning commitment · Converted into structured evidence rather than unbounded course consumption

Priority development gaps

Area · Development target · Evidence

--- · --- · ---

SOC triage · Consistent alert-to-decision process · Three complete investigation packs

Windows telemetry · Recognise important authentication/process events · Event 4625/4624/process-creation investigations

Wazuh operations · Understand agents, rules, alerts and tuning · Wazuh detection pack and tuning notes

Incident response · Document severity, containment, escalation and recovery · Incident runbook + tabletop

Threat mapping · Relate detections to attacker behaviour · MITRE ATT&CK mappings

Cloud security · Understand identity, logging, least privilege and monitoring · Cloud-control comparison artefact

GitHub workflow · Professional repositories, branches, commits and README evidence · Reviewed portfolio PRs

Communication · Concise technical writing and verbal explanation · Mentor-reviewed incident summaries

Time mana
gement · Sustain learning without frag
mentation · Weekly plan + sprint completion rate

Capabili
ty proof rule

A capability is treated as developed when Nkateko can explain it, demonstr
ate it safely, document the evidence and respond to review questions. Certificates and learning records support this evidence but do not replace it.

Career Pathway

Primary pathway — Junior SOC Analyst !’ SOC Analyst

This pathway matches the supplied profile and assessment most closely. The immediate goal is employability in security operations, followed by deeper detection, incident response and SIEM ownership.

Entry capability target

Nkateko should be able to:

- explain the purpose and workflow of a SOC;
- triage common endpoint, authentication and network alerts;
- investigate Windows security events using a repeatable method;
- use Wazuh dashboards, agents, alerts and rule concepts confidently;
- document investigation evidence and conclusions clearly;
- map important activity to MITRE ATT&CK where useful;
- distinguish benign activity, suspicious activity and confirmed incidents;
- escalate with the right context instead of forwarding raw alerts;
- use GitHub to publish sanitised lab evidence and investigation notes.

Secondary pathway — Detection Engineering / Cloud Security

The assessment identifies SIEM platforms and AI as areas of interest, while the professional profile highlights cloud security. Once the SOC foundation is reliable, the roadmap introduces detection engineering and cloud-control concepts.

Development signals

- comfortable writing simple Wazuh rules or detection logic;
- understands false positives and detection tuning;
- can explain identity, logging, least privilege and monitoring controls in cloud environments;
- can automate basic evidence-processing or reporting tasks;
- can connect threat behaviour to telemetry requirements.

Long-term pathway — Security Operations Leadership

Nkateko's assessment states a long-term ambition to attain leadership and create a positive work environment. Leadership development therefore begins early through communication, documentation, mentoring habits and evidence ownership rather than waiting for a management title.

Long-term evidence

- leads or facilitates a small security improvement project;
- produces an operational runbook used by others;
- presents a security finding to technical and non-technical audiences;
- mentors a newer learner or explains a lab to peers;

- proposes measurable SOC improvements;
- demonstrates consistent professional communication and follow-through.

Career progression map

```
flowchart LR
A[Home Lab Learner] --> B[Junior SOC Analyst]
B --> C[SOC Analyst]
C --> D{Specialisation}
D --> E[Detection Engineering]
D --> F[Cloud Security]
D --> G[Incident Response]
E --> H[Senior SOC / Security Lead]
F --> H
G --> H
```

Role-selection rule

The first 90 days should remain broad enough to build employable SOC fundamentals. At the Day-90 review, use portfolio evidence and mentor feedback to decide which specialisation deserves more weight.

12-Month Roadmap

Phase · Months · Focus · Required outcome

--- · ---: · --- · ---

Foundation · 1–2 · Windows telemetry, networking, Wazuh, GitHub workflow · Reliable alert triage and evidence habits

Detection & IR · 3–4 · Detection logic, ATT&CK, incident response, threat intelligence · Detection pack + incident runbook

Cloud & automation · 5–6 · Cloud-security fundamentals, Python/PowerShell basics, GitHub Actions · Cloud baseline + small automation artefact

SOC depth · 7–8 · Threat hunting, rule tuning, case management, reporting · Multi-stage investigation portfolio

Professional growth · 9–10 · Communication, interview preparation, cross-functional work · Interview-ready CV/LinkedIn/portfolio evidence

Specialisation · 11–12 · Detection engineering, cloud security or incident response · Capstone and next-role development plan

Months 1–2 — Foundation

- establish a repeatable Windows-event investigation method;
- strengthen TCP/IP, DNS, authentication and endpoint-log reasoning;
- understand Wazuh agent, manager, rules, alerts and decoder concepts;
- use GitHub issues, branches, commits and README files professionally;
- complete the 12-week sprint with evidence rather than attendance.

Months 3–4 — Detection and incident response

- write and test simple detection logic;
- document false positives and tuning decisions;
- map common activity to MITRE ATT&CK;
- complete incident-response tabletop exercises;
- improve incident summaries and escalation writing.

Months 5–6 — Cloud and automation

- learn identity, least privilege, logging, monitoring and network controls in cloud environments;
- compare cloud controls across Google Cloud, Microsoft Azure and AWS at a fundamentals level;
- automate one repeatable SOC task with Python or PowerShell;
- add automated validation to a GitHub repository.

Months 7–8 — SOC depth

- run multi-source investigations;
- practise threat hunting from a hypothesis rather than an alert;
- create a small SOC scorecard;
- improve Wazuh rules and documentation;
- produce a case-study style investigation.

Months 9–10 — Professional growth

- refine CV, LinkedIn and GitHub portfolio around evidence;
- practise concise written and verbal incident explanations;
- complete mock SOC interviews;
- participate in a cross-functional or peer-review activity;
- improve time-management habits around focused learning blocks.

Months 11–12 — Specialisation

Choose one primary direction based on evidence and opportunity:

- Detection Engineering;
- Cloud Security;
- Incident Response / Threat Hunting.

Complete a capstone that combines telemetry, detection, investigation, documentation and presentation.

Formal gates

- Day 30: evidence workflow and first Windows/Wazuh investigations are reliable.
- Day 60: at least one detection and one incident-response artefact are mentor-reviewed.
- Day 90: at least 10 sprint weeks are accepted and three portfolio artefacts are review-ready.
- Month 6: one automation and one cloud-security artefact are complete.
- Month 12: six portfolio items and a capstone support a clear next-role story.

12-Week Applied Sprint

This sprint turns Nkateko's current Wazuh/ home-lab foundation into structured SOC evidence. Each week should end with something inspectable: an investigation, rule, runbook, diagram, test result or written explanation.

Sprint map

Week · Focus · Practical output · Acceptance signal

---: · --- · --- · ---

1 · SOC baseline · Capability matrix + lab inventory · Clear starting point and evidence standard

2 · Networking & Windows telemetry · Event-source map + packet/Windows notes · Can explain where security evidence comes from

3 · Wazuh operations · Wazuh architecture and alert-triage notes · Can trace agent !’ manager !’ rule !’ alert

4 · Authentication investigation · Event 4625 investigation pack · Evidence-based conclusion with timeline

5 · Detection engineering · Two basic detection ideas/rules · Logic, test method and false positives documented

6 · Incident response · Endpoint-compromise tabletop runbook · Severity, escalation and contain

ment decisions clear

7 · GitHub workflow · Clean evidence repository and PR workflow · Work is traceable and reviewable

8 · Cloud security · Cloud-control baseline · Identity/ logging/ least-privilege concepts explained

9 · ATT&CK & threat intelligence · Technique-to-telemetry map · Can connect attacker behaviour to observable evidence

10 · Automation · Small Python/ PowerShell SOC utility · Safe input/ output and clear README

11 · Communication · Executive-style incident summary + mock interview ·

Explains findings clearly without jargon overload

12 · Capstone · Multi-stage SOC case study · Portfolio-ready evidence and next-90-day plan

Week 1 — Baseline and SOC foundations

Objectives

- understand the role of Tier-1/Tier-2 SOC work;
- inventory the current Wazuh lab and available telemetry;
- define a simple evidence standard for every future investigation;
- identify what is already strong and what still needs structured practice.

Practical work

Create a capability matrix covering networking, Windows logs, Wazuh, incident response, Git, cloud security and communication. Draw the current home-lab architecture and identify which logs are available.

Evidence

- capability-matrix.md
- lab-architecture.md or diagram
- first mentor/self-review note

Week 2 — Networking and Windows telemetry

Objectives

- reinforce IP addressing, ports, DNS, DHCP, TCP/UDP and common protocols;
- understand Windows Security log sources and authentication events;
- practise timeline thinking.

Practical work

Create an event-source map for Windows endpoint, authentication and network evidence. Capture safe examples from the home lab and explain what each event proves and what it does not prove.

Evidence

- event-source map;
- short notes on Event IDs 4624, 4625 and a process-creation event source;
- one basic network flow explanation.

Week 3 — Wazuh operations

Objectives

- understand Wazuh agents, manager, decoders, rules, alert levels and dashboards;
- distinguish collection from detection;

- practise alert triage.

Practical work

Take three safe lab alerts and document: source, rule, severity, observable facts, possible explanation, next evidence to collect and final disposition.

Evidence

- Wazuh architecture diagram;
- three alert-triage records;
- one tuning idea.

Week 4 — Event 4625 investigation

Objectives

- investigate failed Windows logons systematically;
- distinguish user error, service/account issues and brute-force indicators;
- document assumptions and uncertainty.

Practical work

Use synthetic or authorised Windows event data. Build a timeline around repeated 4625 events, correlate source information, check successful logons where available and produce a conclusion.

Evidence

- investigation README;
- timeline table;
- evidence screenshots/log excerpts with private data removed;
- conclusion and recommended next steps.

Week 5 — Detection engineering basics

Objectives

- write detections from a threat hypothesis;
- define required telemetry;
- test expected positives and benign activity;
- document false positives.

Practical work

Design two simple detection ideas: one authentication-based and one endpoint/process-based. Implement in Wazuh where safe or provide well-formed rule/pseudocode.

Evidence

For each detection: hypothesis, telemetry, logic, severity, test case, false positives, tuning notes and ATT&CK mapping.

Week 6 — Incident response

Objectives

- understand identify !’ contain !’ eradicate !’ recover !’ lessons learned;
- separate facts from assumptions;
- know when to escalate.

Practical work

Run a tabletop for a simulated suspicious endpoint with failed logons and an unusual process alert. Write the incident timeline, severity rationale, containment options and stakeholder update.

Evidence

- incident-response runbook;
- timeline;
- decision log;
- concise incident update.

Week 7 — Git and GitHub professionalism

Objectives

- use issues, branches, commits and pull requests cleanly;
- organise portfolio evidence;

- protect secrets and sensitive data.

Practical work

Refactor one existing SOC portfolio investigation into a professional repository structure with README, evidence, references and lessons learned.

Evidence

- issue !’ branch !’ PR history;
- improved README;
- privacy/security check.

Week 8 — Cloud-security fundamentals

Objectives

- understand shared responsibility;
- explain identity, MFA, least privilege, logging, storage/network exposure and monitoring;
- connect cloud events to SOC operations.

Practical work

Build a vendor-neutral cloud-security baseline, then map equivalent services/concepts in Google Cloud and one additional major cloud platform.

Evidence

- control matrix;
- simple cloud architecture diagram;
- one logging/detection use case.

Week 9 — MITRE ATT&CK and threat intelligence

Objectives

- use ATT&CK to organise behaviours rather than memorise IDs;
- distinguish indicators from behaviours;
- map detections to useful telemetry.

Practical work

Choose three common behaviours and map tactic, technique, likely data sources, Wazuh/Windows evidence and investigation questions.

Evidence

- technique-to-telemetry matrix;
- one threat-intelligence note explaining source confidence and relevance.

Week 10 — Automation basics

Objectives

- automate a small repetitive SOC task;
- validate inputs and outputs;
- avoid unsafe assumptions.

Practical work

Build a small Python or PowerShell utility such as IOC-list normalisation, failed-logon summary parsing or evidence-file hashing.

Evidence

- source code;
- README;
- test input/output;
- limitations and safety notes.

Week 11 — Communication and interview evidence

Objectives

- improve concise technical communication;
- explain incidents to both technical and non-technical audiences;
- practise junior SOC interview responses using real portfolio evidence.

Practical work

Rewrite one investigation as a one-page incident summary. Prepare three STAR-style stories: investigation, learning challenge and teamwork/initiative.

Evidence

- one-page summary;
- three interview stories;
- mentor feedback notes.

Week 12 — Capstone

Objectives

- combine telemetry, detection, investigation and communication;
- show a complete SOC workflow;
- decide the next specialisation direction.

Practical work

Create a synthetic multi-stage case: suspicious authentication, endpoint alert and supporting network evidence. Triage, investigate, map ATT&CK, document response and present the conclusion.

Evidence

- capstone repository;
- investigation timeline;
- detection logic;
- incident-response decisions;
- 5–10 minute presentation;
- next-90-day plan.

Completion rule

A week is accepted only when Nkateko can explain the evidence, identify limitations, protect sensitive information and respond to review questions. Time spent alone does not equal completion.

Credentials and Skill Milestones

The submitted profile already shows meaningful foundation learning. This IDR does not restart from zero. Credentials are used as structured learning milestones while practical evidence remains the main proof of capability.

Existing profile-listed learning

- Networking Devices and Initial Configuration
- Introduction to Cybersecurity
- Google Cybersecurity Professional Certificate
- Networking Basics
- Cybersecurity and Cloud Fundamentals 1.0

Recommended next milestones

Priority · Milestone · Why it matters · Evidence gate

--- · --- · --- · ---

Core · Wazuh practical proficiency · Directly supports current SIEM portfolio · Three triage cases + one tuned detection

Core · CompTIA Security+ knowledge objectives · Broad junior security baseline · Labs mapped to identity, threats, operations and risk

Core · Cisco cyber security pro gression · Builds on existing Cisco foundation · Networking/ security lab evidence

Core · GitHub workflow proficiency · Makes evidence pr ofessional and reviewable · Issues, branches, PRs, README and clean history

Supporting · Microsoft security operations learning · Introduces Sentinel/ Defender concepts used in many SOC roles · One Sentinel-style detection/

incident comparison

Supporting · Google Cloud security fundamentals · Aligns with stated Google interest and cloud-security profile · Cloud-control baseline

Applied · Python or PowerShell automation · Enables repetitive SOC task automation · Working utility + tests

Applied · MITRE ATT&CK mapping · Strengthens detection/investigation reasoning · Three technique-to-telemetry mappings

Professional · Incident communication · Addresses communication-development request · Mentor-reviewed incident summary

Career · Junior SOC interview

readiness · Converts evidence into employ ability · Two mock interviews + four evidence-backed answers

Suggested credential sequencing

First 90 days

Prioritise Wazuh, Windows events, networking, GitHub and Security+ knowledge objectives. Do not overload the sprint with multiple exam preparations.

Months 4–6

Choose one formal certification target only if it directly supports job applications or exposes a clear knowledge gap. Add cloud-security learning and basic automation.

Months 7–12

Select a specialisation milestone based on portfolio evidence and available roles: detection, cloud security or incident response.

Acceptance rule

A credential milestone counts toward the IDR only when it is backed by practical evidence: a reviewed lab, investigation, detection, automation, architecture/control map or mentor-accepted artefact.

Course Curriculum

The curriculum is organised around employable SOC evidence rather than course completion.

Module 1 — SOC foundations

Outcomes

- explain SOC roles, alert lifecycle, severity, escalation and evidence handling;
- distinguish monitoring, detection, investigation and incident response;
- use an investigation template consistently.

Assessment: capability matrix + one triage record.

Module 2 — Networking for analysts

Outcomes

- reason about IP addresses, ports, protocols, DNS and TCP/UDP;
- interpret source/destination context;
- recognise common network evidence used in investigations.

Assessment: annotated network-flow analysis and packet/log notes.

Module 3 — Windows security telemetry

Outcomes

- use Event Viewer and Windows Security logs;
- interpret authentication activity and process evidence;
- create timelines and correlate related events.

Assessment: Event 4625 investigation pack.

Module 4 — Wazuh SIEM operations

Outcomes

- understand agent/manager/rule/alert relationships;
- triage alerts systematically;
- document rule tuning and false positives.

Assessment: three alert triage cases + one tuning proposal.

Module 5 — Detection engineering

Outcomes

- start from a threat hypothesis;

- define required telemetry;
- implement or describe detection logic;
- create test cases and false-positive guidance.

Assessment: Wazuh Detection Pack.

Module 6 — Incident response

Outcomes

- classify incidents;
- document containment, eradication and recovery options;
- create decision logs and stakeholder updates.

Assessment: incident tabletop and runbook.

Module 7 — Threat intelligence and MITRE ATT&CK

Outcomes

- distinguish indicators, behaviours and techniques;
- map relevant detections to ATT&CK;
- assess source relevance and confidence.

Assessment: technique-to-telemetry matrix.

Module 8 — Cloud security fundamentals

Outcomes

- explain shared responsibility, IAM, MFA, least privilege, logging, network exposure and monitoring;
- compare equivalent security controls across cloud platforms;
- identify cloud events relevant to SOC operations.

Assessment: cloud-security baseline and logging use case.

Module 9 — GitHub and evidence engineering

Outcomes

- use issues, branches, commits and pull requests;
- maintain clean README files and references;
- avoid publishing secrets or sensitive evidence.

Assessment: reviewed portfolio repository.

Module 10 — Automation basics

Outcomes

- automate one repetitive security-analysis task;
- validate inputs and outputs;
- document limitations and safe usage.

Assessment: Python or PowerShell utility with test evidence.

Module 11 — Professional communication

Outcomes

- write concise incident summaries;
- explain technical findings to non-technical audiences;
- practise interview narratives linked to real evidence.

Assessment: one-page incident summary + mock interview.

Module 12 — Capstone

Outcomes

- combine multiple evidence sources;
- perform a complete triage/investigation/response workflow;
- present conclusions and uncertainty clearly.

Assessment: multi-stage SOC case study.

Assessment rubric

Dimension · Weight

--- · ---:

Technical accuracy · 25%

Investigation logic · 20%

Evidence quality and reproducibility · 20%

Security/privacy discipline · 10%

Communication · 15%

Reflection and improvement · 10%

Pass: 75%

Distinction: 90%

Hands-On Labs

All labs must use the existing home lab, local virtual machines, vendor sandboxes or synthetic datasets. Never test third-party systems without explicit authorisation.

Standard lab evidence

Every lab should include objective, authorised scope, environment diagram, steps, evidence, test results, conclusion, limitations, cleanup/rollback and references.

Lab 1 — Windows authentication investigation

Generate or use safe sample failed/successful

logons. Investigate Event IDs 4625 and 4624, build a timeline, identify source context and explain whether the evidence suggests user error, service-account problems or suspicious activity.

Deliverable: event-4625-investigation/README.md plus sanitised evidence.

Lab 2 — Wazuh alert triage

Select three different Wazuh alerts. For each record rule ID/name, alert level, raw facts, hypothesis, next evidence, disposition and tuning recommendation.

Deliverable: three completed triage sheets.

Lab 3 — Wazuh detection rule

Create or safely simulate a simple custom detection. Define the threat hypothesis, log source, logic, test events, expected alert and false positives.

Deliverable: rule/pseudocode, test evidence and tuning notes.

Lab 4 — Network evidence analysis

Use a local packet capture or synthetic flow data. Identify endpoints, protocol, ports, DNS context and whether the traffic is expected.

Deliverable: annotated traffic-analysis note.

Lab 5 — Incident-res

ponse tabletop

Simulate suspicious logons followed by a process alert. Decide severity, containment options, escalation path, evidence collection and recovery criteria.

Deliverable: incident timeline, decision log and stakeholder update.

Lab 6 — Threat mapping

Choose three attacker behaviours relevant to authentication or endpoint activity. Map them to MITRE ATT&CK and identify Wazuh/Windows/network telemetry that could detect or investigate them.

Deliverable: ATT&CK-to-telemetry matrix.

Lab 7 — Cloud-security baseline

Create a small vendor-neutral control baseline covering identity, MFA, least privilege, logging, storage exposure, network controls and monitoring. Map the concepts to Google Cloud and one additional cloud platform.

Deliverable: control comparison and architecture diagram.

Lab 8 — SOC automation utility

Build a small Python or PowerShell utility for one safe task: normalising IOC lists, summarising failed logons,

hashing evidence files or parsing a simple log export.

Deliverable: source, test data, output, README and limitations.

Lab 9 — GitHub evidence workflow

Create an issue, branch, commit series and pull request for one investigation. Ensure no secrets or private data are committed.

Deliverable: traceable GitHub workflow and mentor/self-review note.

Lab 10 — Capstone case

Combine authentication, endpoint and network evidence into a synthetic incident. Triage, investigate, map

relevant ATT&CK techniques, propose response actions and present the case.

Deliverable: full portfolio case study and short pr esentation.

Assignments

Assignments are short, reviewable exercises that strengthen technical reasoning and communication between larger labs and portfolio projects.

Assignment 1 — SOC capability baseline

Create a table covering networking, Windows logs, Wazuh, incident response, cloud security, Git/GitHub, automation and communication. Score current confidence, identify evidence already available and define the next 90-day action for each area.

Assignment 2 — Alert triage worksheet

Build a reusable triage template containing:

- alert name and source;
- timestamp and affected asset/account;
- observable facts;
- initial hypothesis;
- next evidence to collect;
- severity rationale;
- disposition;
- escalation decision;
- false-positive/tuning note.

Use it on three lab alerts.

Assignment 3 — Investigation writing

Write a one-page investigation summary for a failed-logon scenario. The reader should understand what happened, what evidence supports the conclusion, what remains uncertain and what action is recommended.

Assignment 4 — Detection design

Design two detections from threat hypotheses. Include telemetry, logic, severity, test data, false positives and ATT&CK mapping.

Assignment 5 — Cloud control map

Compare identity, MFA, least privilege, logging, network exposure and monitoring controls in Google Cloud and one additional cloud platform. Explain the SOC-relevant telemetry each control can produce.

Assignment 6 — Communication improvement plan

The assessment identifies communication as an area where additional support would help. Create a practical plan with:

- one written communication exercise per week;
- one short verbal explanation/demo every two weeks;
- mentor feedback notes;
- examples of improved before/after wording;
- one mock incident briefing by Day 60.

Assignment 7 — Career evidence audit

Review CV, LinkedIn and GitHub portfolio. For every claimed security skill, link to evidence or mark it as learning-in-progress. Remove vague claims that cannot be supported.

Submission standard

Each assignment should include references, evidence links, a short self-review and the specific mentor/reviewer feedback that was acted on.

Portfolio Projects

The portfolio should show how Nkateko thinks and works, not only screen shots of tools. Every project must be safe to publish and should contain a clear README, evidence, references, limitations and lessons learned.

Project 1 — SOC Analyst Portfolio Index

Create a landing repository/ page that organises all security evidence by capability:

- investigations;
- Wazuh/SIEM work;
- detection engineering;
- incident response;
- networking;
- cloud security;
- automation;

- professional communication.

Acceptance: every claim links to evidence and outdated/duplicate material is removed.

Project 2 — Event 4625 Investigation Pack

Expand the existing failed-logon investigation work into a professional case study with:

- scenario and scope;
- timeline;
- event interpretation;
- source/target context;
- correlation with successful logons where available;
- hypothesis and conclusion;
- false-positive considerations;
- response recommendations;
- references and lessons learned.

Project 3 — Wazuh Detection Pack

Create at least three detection entries. Each should include threat hypothesis, data source, rule/logic, severity, test method, expected result, false positives, tuning notes and ATT&CK mapping.

Project 4 — Incident Response Runbook

Build a junior-SOC-friendly runbook for a simulated suspicious Windows endpoint. Cover intake, severity, evidence collection, containment options, escalation, eradication/recovery considerations and lessons learned.

Project 5 — Cloud Security Baseline

Build a concise control baseline covering identity, MFA, least privilege, logging, storage/network exposure, monitoring and incident evidence. Map concepts to Google Cloud and one additional major cloud platform.

Project 6 — SOC Capstone Case Study

Create a synthetic multi-stage case that combines:

- authentication anomalies;
- endpoint/process evidence;
- network context;
- Wazuh alerts;
- ATT&CK mapping;
- detection logic;
- incident-response decision making;
- final technical and non-technical summaries.

Standard repository structure

```
project-name/
% % %  README.md
% % %  evidence/
% % %  detections-or-scripts/
% % %  references.md
% % %  SECURITY.md
% % %  review-notes.md
```

Portfolio readiness rule

A project is interview-ready when Nkateko can explain the scenario without reading the README, answer why each step was taken, identify limitations and show that all published evidence is sanitised.

Study and Review Calendar

Suggested weekly rhythm

The assessment indicates very high willingness to allocate learning time, but it also identifies time division between work and learning as a challenge. The IDR therefore uses focused core sessions rather than filling every available hour.

Day · Time · Activity · Output

--- · --- · --- · ---

Monday · 18:30–19:30 · Theory / primary documentation

· Notes + one question

Wednesday · 18:30–20:00 · Lab / investigation · Technical evidence

Thursday · 18:30–19:30 · Documentation / GitHub · README, timeline or rule notes

Saturday · 09:00–11:00 · Deep work / portfolio · Completed weekly artefact

Alternate Wednesday · 20:00–20:30 · Mentor / one-on-one review · Feedback + next actions

The core timetable is about 5.5 hours per week, deliberately lower than the maximum time Nkateko said he is willing to invest. Extra learning time should be optional and targeted,

not used to create an unsustainable backlog.

12-week schedule

Week commencing	Focus	Primary output
31 Aug 2026	Baseline and SOC foundations	Capability matrix + lab architecture
7 Sep 2026	Networking and Windows telemetry	Event-source map
14 Sep 2026	Wazuh operations	Three alert-triage records
21 Sep 2026	Event 4625 investigation	Investigation pack
28 Sep 2026	Detection engineering	Two tested detection ideas
5 Oct 2026	Incident response	Tabletop runbook

12 Oct 2026 · GitHub workflow · Reviewed evidence repository

19 Oct 2026 · Cloud security · Control baseline

26 Oct 2026 · ATT&CK and threat intelligence · Technique-to-telemetry matrix

2 Nov 2026 · Automation · Python/ PowerShell SOC utility

9 Nov 2026 · Communication and interviews · Incident brief + interview stories

16 Nov 2026 · Capstone · Multi-stage case study + next-90-day plan

Review checkpoints

- Weekly: record evidence, blockers and learning hours.
- Fortnightly: one-on-one review of one completed artefact.
- Day 30: check investigation method, Wazuh confidence and workload sustainability.
- Day 60: review detection quality, incident-response thinking and communication progress.
- Day 90: assess portfolio readiness and choose the next specialisation emphasis.

Rescheduling rule

Missed time is not recovered by doubling the following week. Move the highest-value activity, preserve the evidence outcome and record the reason. Repeated slippage should trigger a scope reduction rather than hidden backlog.

Goals and KPIs

The IDR measures accepted evidence, not raw course hours.

KPI · 90-day target · 12-month target · Evidence

--- · ---: · ---: · ---

Sprint execution · "e10/12 weeks accepted · N/A · Weekly artefacts

Investigation quality · 3 reviewed cases · 8 reviewed cases · Timelines, conclusions, review notes

Wazuh/ SIEM capability · 3 triage cases + 1 tuning idea · 3+ tested detections and tuning history · Detection pack

Incident response · 1 tabletop · 3

scenarios / one polished runbook · Runbook and decision logs

Networking/ telemetry · Event-source map complete · Multi-source investigation evidence · Lab notes

Cloud security · Baseline control map · One cloud-security portfolio artefact · Control matrix/ diagram

Automation · Plan selected · 2 small SOC utilities · Code + tests + README

GitHub professionalism · 3 clean repos/PRs · Full portfolio index · Git history and README quality

Communication · 3 reviewed summaries · 6 reviewed technical/ non-

technical briefs · Mentor notes

Interview readiness · 3 evidence-backed stories · 2 mock interviews + 6 strong stories · Interview notes

Formal scorecard

Score each dimension from 1–5.

Dimension · 1 · 3 · 5

--- · --- · --- · ---

Investigation logic · Jumps to conclusions · Uses evidence and a repeatable process · Correlates multiple sources and explains uncertainty

SIEM/ detection · Tool navigation only · Can triage and describe logic · Can test, tune and defend detection choices

Networking/ telemetry · Limited protocol/

event under standing · Correctly interprets common evidence · Selects the right telemetry for hypotheses

Incident response · Unstructured reaction · Uses severity/ escalation/ runbook logic · Makes clear, risk-aware response decisions

Communication · Raw technical notes · Clear structured summary · Audience-specific, concise and decision-ready

Evidence quality · Screenshots without context · Reproducible README/ evidence · Professional portfolio-quality case study

Security/ privacy · Inconsistent handling · Safe synthetic/ sanitised evidence ·

Proactively designs privacy/ security boundaries

Day-30 gate

- first two investigations use a consistent method;
- Wazuh lab inventory and alert flow are understood;
- GitHub evidence workflow is in place;
- learning schedule is sustainable.

Day-60 gate

- one detection has been tested/tuned;
- incident-response tabletop is complete;
- communication improvement is visible in at least two revised summaries;
- at least two portfolio artefacts are mentor-review ready.

Day-90 gate

- at least 10 sprint weeks accepted or a documented recovery plan exists;
- three portfolio artefacts are review-ready;
- one clear next specialisation direction is selected;
- CV/LinkedIn/GitHub claims are linked to evidence.

Annual completion gate

Nkateko should be able to explain and defend six portfolio artefacts, complete a realistic SOC case study and demonstrate readiness for junior SOC/security-operations interviews without relying on course-completion claims alone.

Mentor and Review Process

The assessment explicitly requests a mentor/coach and regular one-on-one feedback. The IDR therefore uses frequent evidence review rather than occasional end-of-course evaluation.

Mentor / coach: To be assigned by Skunkworks Academy

Review cadence

- short self-review every week;
- 30-minute one-on-one review every two weeks during the initial sprint;
- formal Day 30, Day 60 and Day 90 reviews;
- quarterly review after the sprint.

Standard 30-minute agenda

Time · Topic · Output

---: · --- · ---

5 min · Workload and progress · RAG status and blockers

10 min · Evidence review · Accepted / revise / re-scope

5 min · Investigation/detection challenge · One technical question to deepen reasoning

5 min · Communication feedback · One concrete writing/presentation improvement

5 min · Next actions · Two highest-value tasks

Mentor review template

```
# Mentor Review — YYYY
## Evidence reviewed
- link / file
## Decision
- Accepted / Revise /
## Scores (1–5)
- Investigation logic:
- SIEM/detection:
- Networking/telemetry
- Incident response:
- Communication:
- Evidence quality:
- Security/privacy:
## Strongest improveme
## Main gap
## Required changes
## Next two-week prior
```

Feedback rule

Feedback is complete only when the next revision shows what changed. Review comments should not accumulate as passive notes.

Communication-development emphasis

Because the assessment identifies co

mmunicatio n as an area needing additional support, every second mentor review should include one short verbal explanation or written incident summary and one specific imp rovement target.

Governance, Privacy and Safety

The public IDR and portfolio must be useful without exposing personal or organisational information.

Never publish

- passwords, API keys, tokens, private keys or connection strings;
- personal phone numbers, email addresses or home addresses;
- employer/customer private data;
- production logs with identifiers or confidential information;
- unauthorised vulnerability details;
- private tenant/account identifiers;
- screenshots that expose sensitive administration details.

Safe lab rule

Use only:

- Nkateko's own home-lab systems;
- local virtual machines;
- synthetic data;
- vendor-provided training sandboxes;
- systems for which explicit testing permission exists.

Evidence sanitisation checklist

Before committing evidence to GitHub:

1. remove personal/contact information;
2. search for secrets and tokens;
3. replace real usernames/hostnames with synthetic examples where practical;
4. crop/redact screenshots that expose irrelevant identifiers;
5. verify repository visibility;
6. check commit history, not only the latest file;
7. include references and explain what was simulated.

Responsible security practice

This roadmap does not require scanning, exploiting, accessing or modifying third-party systems without permission. If lab scope is unclear, stop and clarify before proceeding.

Accidental exposure process

If a secret or sensitive value is committed:

1. stop further sharing;
2. revoke/ rotate the secret if applicable;
3. notify the relevant owner/ mentor;
4. remove the data from the current repository state;
5. assess Git history and published artefacts;

6. document the corrective action.

Quality rule

A technically strong artefact cannot pass review while it contains unsafe or u nauthorised information.

Learning Resources

Use primary vendor and standards sources first. Third-party videos or courses can help explain a topic, but the evidence should be grounded in the official documentation and the lab results.

Resource map

Capability	Primary references
Wazuh / SIEM	Wazuh documentation; Microsoft Sentinel documentation
Windows events	Microsoft Windows Security and auditing documentation
Networking	Cisco Skills for All /

Networking Academy

Detection · Wazuh rules; MITRE ATT&CK; Sentinel analytics concepts

Incident response · CISA; NIST CSF

Cloud security · Google Cloud security docs; Microsoft/AWS security fundamentals as comparison

GitHub · GitHub Skills; GitHub Docs

Junior security breadth · CompTIA Security+ objectives

Learning-to-evidence rule

For every learning resource, record:

1. what was learned;
2. which lab or project used it;
3. what decision or investigation improved

because of it;

4. what remains uncertain.

References and Source Register

This register separates source-derived learner information from recommended technical-development references.

Learner source material

The public IDR was built from:

- the submitted Career Growth and Learning Assessment response for Nkateko Mtembi;
- the supplied professional profile / resume PDF;
- the existing public SOC Analyst portfolio referenced by the supplied profile.

The public website intentionally does not reproduce private contact details or the complete raw questionnaire response.

Source-derived learner facts represented in the IDR

- junior SOC analyst career direction;
- Wazuh SIEM home-lab experience;
- interest in SIEM platforms;
- threat detection, log analysis and incident-response focus;
- cloud security, security monitoring and Windows strengths listed in the supplied profile;
- Cisco, GitHub, Google and professional-skills interests from the assessment;
- self-paced learning preference;
- preference for regular one-on-one feedback;
- willingness to participate in cross-functional work;
- stated long-term leadership ambition;
- communication support need and time-management challenge;
- foundation cybersecurity/networking learning listed in the supplied profile.

Technical-development references

Wazuh

- Wazuh Documentation — https://documentation.wazuh.com/
- Wazuh Ruleset — https://documentation.wazuh.com/current/user-manual/ruleset/index.html

Windows and Microsoft security

- Windows Security documentation — https://learn.microsoft.com/windows/security/
- Windows security auditing — https://learn.microsoft.com/windows/security/threat-protection/auditing/
- Microsoft Sentinel — https://learn.microsoft.com/azure/sentinel/
- Kusto Query Language — https://learn.microsoft.com/kusto/query/

Threat behaviour and incident response

- MITRE ATT&CK — https://attack.mitre.org/
- NIST Cybersecurity Framework — https://www.nist.gov/cyberframework
- CISA — https://www.cisa.gov/

Networking

- Cisco Skills for All — https://skillsforall.com/
- Cisco Networking Academy — https://www.netacad.com/

Cloud security

- Google Cloud Security — https://cloud.google.com/security
- Microsoft Azure Security — https://learn.microsoft.com/azure/security/
- AWS Security — https://docs.aws.amazon.com/security/

GitHub and engineering workflow

- GitHub Skills — https://skills.github.com/
- GitHub Docs — https://docs.github.com/
- GitHub Actions — https://docs.github.com/actions

Broad junior-security framework

- CompTIA Security+ — https://www.comptia.org/certifications/security

Reference-use rules

- Re-check vendor certification pages before booking an exam because names and requirements change.
- Use primary documentation to support technical conclusions.
- Frameworks organise thinking; they do not replace investigation evidence.
- Public portfolio artefacts must use safe, sanitised or synthetic data.

Download, Review and Sign-Off

What the downloadable IDR contains

- source-based learner baseline;
- recommended SOC career pathway;
- 12-month roadmap;
- full 12-week applied sprint;
- curriculum and labs;
- assignments and portfolio projects;
- credential/skill milestones;
- calendar and review cadence;
- goals and KPIs;
- mentor process;
- governance/privacy rules;
- learning references.

First 10 working days

Day range · Action · Evidence

--- · --- · ---

1–2 · Review baseline and target role · Confirmed capability matrix

1–4 · Inventory Wazuh lab and available logs · Lab architecture diagram

3–5 · Standardise investigation template · Reusable triage/investigation worksheet

4–7 · Review GitHub portfolio structure · Portfolio cleanup issue/branch

6–8 · Complete first Windows/Wazuh case · Investigation README

8–10 · Conduct first one-on-one review · Feedback and next actions

Formal review gates

Day 30

- workload and schedule are sustainable;
- Wazuh alert flow is understood;
- at least two investigations follow a repeatable method;
- GitHub evidence is clean and safe to publish.

Day 60

- at least one detection has a documented test and tuning process;
- the incident-response tabletop is complete;
- communication improvement is visible in written summaries;
- at least two portfolio artefacts are review-ready.

- at least 10 sprint weeks are accepted or a recovery plan exists;
- at least three portfolio items are review-ready;
- one next specialisation direction is chosen;
- CV/LinkedIn/GitHub claims are evidence-linked.

Annual sign-off target

The roadmap is complete when Nkateko can demonstrate six strong portfolio artefacts, explain a realistic SOC case end to end, show safe GitHub/evidence practices and defend readiness for junior SOC/security-operations opportunities.

Sign-off

Role · Name · Decision / signature · Date

--- · --- · --- · ---

Learner · Nkateko Mtembi · ·

Mentor / coach · To be assigned · ·

Skunkworks Academy review · · ·

Review questions

- Does the portfolio prove investigation ability rather than only tool familiarity?
- Can Nkateko explain what evidence supports each conclusion?
- Is the Wazuh work tested and documented?
- Is communication becoming clearer and more concise?
- Are learning hours sustainable despite the high stated willingness to study?
- Does every public artefact respect the privacy/safe-lab boundary?