AXIA LEARNING / CYB

Diploma in Cybersecurity

Five months. Practical learning. A clear next step.



20 weeks | **220 hours** | **Live classes**

Developing Talent. Building Intelligent Solutions.

Your pathway



Focus and scope. Foundational defensive cybersecurity with a junior security-operations focus. Students learn to secure systems, investigate evidence and report risks in authorised, isolated environments.

Entry requirements. Computer literacy and willingness to work with operating systems and technical documentation. A pre-course diagnostic checks files, command-line familiarity and basic networking concepts.

Pre-course preparation. Required for learners who do not pass the diagnostic: 20–30 hours of IT preparation in operating systems, IP addressing, virtual machines and basic terminal commands before Week 1.

Primary tools. Core: browser-accessible isolated lab or virtual machines, Linux and Windows logs, Wireshark, an entry-level SIEM such as Wazuh, and Python or shell basics. Use supplied packet captures and logs. No public-target testing.

Career direction. Foundation for junior SOC/security-operations, IT security support and cybersecurity internship applications; not a claim of advanced penetration-testing competence.

What you'll be able to do

LO1. Explain common threats and map a small organisation's assets, exposures and controls.

LO2. Apply basic identity, endpoint, network and data-protection controls.

LO3. Interpret packet captures and system logs to triage a suspected incident.

LO4. Document and prioritise vulnerability findings from an authorised lab.

LO5. Execute a basic incident-response and recovery procedure with an evidence trail.

LO6. Communicate technical findings and practical remediation to a non-technical stakeholder.

Five-month overview

Month	Focus	Main assessment
1	Security, networks and operating-system foundations	Network/OS baseline and hardening evidence for an assigned environment.
2	Defensive controls and vulnerability management	Defensive vulnerability assessment with prioritisation and remediation retest.
3	Security monitoring and incident investigation	Incident investigation using supplied SIEM, endpoint and network evidence.
4	Risk, cloud basics and response operations	Risk treatment, detection and recovery tabletop pack for a separate scenario.
5	Capstone investigation and practical defence	Final capstone and individual practical

MONTH 1 / 05

Security, networks and operating-system foundations



1. Security foundations and lab boundaries

Skills & concepts

Explain confidentiality, integrity, availability, threat actors and written authorisation.

Practical evidence

Sign lab rules, inventory a small environment and complete a baseline risk exercise.

2. Networks and traffic

Skills & concepts

Understand TCP/IP, DNS, HTTP/TLS, ports and common traffic patterns.

Practical evidence

Inspect a supplied packet capture and explain normal client/server communication.

3. Linux and command-line skills

Skills & concepts

Navigate files, permissions, processes and relevant system logs.

Practical evidence

Harden a lab user account and document permission checks.

4. Windows, identity and baseline defence

Skills & concepts

Explain accounts, authentication, MFA, updates and endpoint protection.

Practical evidence

Submit Month 1 environment-hardening checklist with before/after evidence.

MONTH 2 / 05

Defensive controls and vulnerability management



5. Network security controls

Skills & concepts

Apply segmentation, firewall concepts, secure remote access and least privilege.

Practical evidence

Design and test a small network policy in the isolated lab.

6. Identity and access management

Skills & concepts

Review account lifecycle, privileged access, password practices and access reviews.

Practical evidence

Audit a supplied access list and propose least-privilege corrections.

7. Vulnerability management

Skills & concepts

Identify assets, understand scanner limitations, validate findings and prioritise remediation.

Practical evidence

Review a supplied scan or scan an assigned lab target and validate selected findings.

8. Web and data security foundations

Skills & concepts

Recognise common web weaknesses, encryption basics, backups and data classification.

Practical evidence

Submit Month 2 defensive assessment and retest a remediated lab issue.

MONTH 3 / 05

Security monitoring and incident investigation



9. Logs and security monitoring

Skills & concepts

Identify useful events, timestamps, fields and sources; distinguish signal from noise.

Practical evidence

Ingest supplied logs and construct a basic investigation timeline.

10. Alert triage and SIEM searches

Skills & concepts

Query events, assess severity and distinguish a suspicious signal from a false positive.

Practical evidence

Triage a supplied alert set and document escalation decisions.

11. Phishing and endpoint investigation

Skills & concepts

Inspect safely provided messages, attachments metadata and endpoint evidence.

Practical evidence

Produce a phishing/endpoint investigation report without interacting with live malicious content.

12. Incident response fundamentals

Skills & concepts

Apply preparation, analysis, containment, recovery and communication through a simulation.

Practical evidence

Submit Month 3 incident case file with evidence references and response recommendations.

MONTH 4 / 05

Risk, cloud basics and response operations



13. Cloud and application security basics

Skills & concepts

Understand shared responsibility, cloud permissions, storage exposure and secret handling.

Practical evidence

Review a supplied cloud configuration and recommend concrete controls.

14. Risk, policy and governance

Skills & concepts

Build a risk register, classify assets and map practical controls to business impact.

Practical evidence

Write a small-organisation risk treatment plan and two usable policy procedures.

15. Scripting for defenders and AI verification

Skills & concepts

Parse logs with a small script and independently verify AI-assisted summaries and indicators.

Practical evidence

Build a repeatable log-triage script with documented checks.

16. Detection and recovery exercises

Skills & concepts

Tune a simple detection, rehearse escalation and verify backup/recovery readiness.

Practical evidence

Submit Month 4 tabletop exercise and detection/recovery evidence; approve capstone scenario.

MONTH 5 / 05

Capstone investigation and practical defence



17. Capstone environment assessment

Skills & concepts

Establish authorised scope, assets, baseline controls and investigation questions.

Practical evidence

Deliver an assessment plan and evidence-handling log.

18. Capstone investigation

Skills & concepts

Review staged logs and traffic, validate findings and reconstruct a timeline.

Practical evidence

Submit an interim incident analysis with uncertainty and alternative explanations.

19. Capstone remediation and retest

Skills & concepts

Prioritise fixes, test selected controls and exercise escalation and recovery.

Practical evidence

Deliver a remediation matrix, retest evidence and response runbook.

20. Security briefing and practical test

Skills & concepts

Present risk clearly and triage an unseen lab incident independently.

Practical evidence

Submit final report, technical appendix and individual practical defence.

Your assessment checkpoints

Checkpoint	Assessed project	Outcome coverage
Week 4	Network/OS baseline and hardening evidence for an assigned environment.	LO1, LO2
Week 8	Defensive vulnerability assessment with prioritisation and remediation retest.	LO2, LO4
Week 12	Incident investigation using supplied SIEM, endpoint and network evidence.	LO3, LO5
Week 16	Risk treatment, detection and recovery tabletop pack for a separate scenario.	LO5, LO6

The capstone and final individual practical together verify all six outcomes. Instructors use the weekly evidence to identify gaps early; the mapping above does not limit remediation to those weeks.

Your final capstone

Assess and investigate a staged incident in an isolated small-business environment. Deliver an asset/control assessment, incident timeline, evidence-backed findings, prioritised remediation and recovery guidance.

Capstone acceptance criteria

Work only within documented lab scope and maintain a timestamped evidence log. Correlate at least two evidence sources and identify a plausible incident timeline. Validate at least five findings; label confirmed findings, hypotheses and false positives separately. Demonstrate three defensive improvements and provide retest evidence. Present an executive summary and technical appendix, then triage an unseen alert independently.

Evidence pack. Include a short brief, source/permissions record, versions, practical artefact, testing or user-research evidence, limitations, handover instructions and a record of material AI assistance. Include a 5–8-minute demonstration and an individual 15-minute defence inside the final week's facilitated schedule.

How the programme works

Programme model and delivery

Programme structure. Six separate pathways, each lasting 20 teaching weeks, organised into five four-week learning blocks. A student enrols in one diploma. The five-month calendar should be confirmed against holidays and local delivery dates. This is a proposed institutional curriculum blueprint, not an accreditation decision.

Audience and admission. Mixed cohort: beginners and career changers can enter the non-coding tracks after an orientation. Technical tracks use practical entry checks and pre-course bridging where required. AI Engineering requires Python/API/Git competence before Week 1. Assess applicants by demonstrated skills rather than degree title alone.

Weekly workload: 11 hours. 3 hours of interactive teaching; 2 hours of supervised practical work; 1 hour of critique, review or mentoring; 5 hours of independent reading, building and assessment preparation. Total: 220 learning hours per diploma, including 120 facilitated hours and 100 independent hours. Projects and assessment preparation are included, not added on top.

How each week runs. Begin with a concrete work problem and a short retrieval exercise; teach the relevant concepts; demonstrate a worked example; complete a supervised lab; finish an individual deliverable and receive feedback. Use a different dataset or brief for independent work so students cannot pass by copying the demonstration.

Shared foundation without losing track time. Week 1 in each course includes AI limitations, data privacy, responsible tool use and evidence checking through a track-specific exercise. Communication, version history, documentation and critical thinking recur throughout. Do not add a separate generic month that displaces the core discipline.

Progression gates. Week 4: demonstrate foundational work independently. Week 8: complete a usable core project. Week 12: show role-specific AI application and evaluation. Week 16: demonstrate integrated work and obtain approval for a separate capstone. Weeks 17–20: deliver, test and defend the capstone. Learners who miss a gate receive targeted remediation and a reassessment plan.

AI use in assessment. Allow AI in normal labs if students disclose material use and verify outputs. Keep a brief record of prompts, generated material and corrections. Do not accept fabricated interviews, invented datasets, unrun tests or unsupported impact claims. The final practical uses a fresh task, allows reference documentation and excludes AI-generated solutions; the oral defence verifies individual understanding.

Data and lab practice. Use public, licensed, synthetic or appropriately consented data. Do not place confidential organisational or personal data in external AI tools. Cybersecurity practice takes place only in written-scope isolated labs; automation uses sandbox accounts and approval before external side effects. Students keep a source and permissions register.

Capstone format. Prefer individual work for a five-month part-time diploma. If a team of up to three is approved, each learner keeps a contribution log and submits an individually assessed component and defence. A cross-track showcase is optional; a

learner's grade must not depend on another track delivering its component.

Portfolio and employability. Career preparation is embedded in project write-ups and mentor review. Each student finishes with four graded monthly project artefacts, one capstone case study, a concise CV/profile and a rehearsed demonstration. Describe evidence of competence honestly; the curriculum does not promise employment or advanced professional expertise.

Assessment and progression

Assessment	Weight	Evidence
Weekly practical work, Weeks 1–16	20%	Sixteen individual practical submissions; mark correctness, reasoning and verification. Each contributes 1.25%.
Four monthly projects, Weeks 4, 8, 12 and 16	30%	Each contributes 7.5%. Grade the integrated project against its outcome map; do not award the same points twice for a weekly lab.
Capstone, Weeks 17–20	35%	A separate brief with implementation/prototype, evaluation evidence, documentation and individual defence. Reusing earlier techniques is allowed; copied project submissions are not a new capstone.
Final individual practical, Week 20	15%	An unseen role-specific task, normally 90 minutes, followed by a short explanation of decisions. Scheduled inside the weekly facilitated hours.

Proposed capstone rubric (100 points within the capstone component):

Criterion	Points
Problem understanding and scope	10
Discipline-specific execution	35
Testing, evaluation and evidence	20
User/business relevance	10
Responsible practice and risk controls	10
Documentation and reproducibility/handoff	10
Presentation and defence	5

The discipline-specific acceptance criteria in each course are additional gates. A polished presentation cannot compensate for missing core functionality, unsupported findings or lack of individual understanding.

Delivery & learning support

Delivery preparation and quality assurance

Before enrolment. Publish entry requirements, assessment rules, actual tool/API charges and device requirements. Run the diagnostic and bridge. Check access to every compulsory tool on the learner's device. No learner should discover a mandatory paid subscription halfway through the course.

Teaching assets required. For every week prepare one instructor plan, a worked example, a supervised lab brief, an independent task, starter files or data, an answer/review guide and a marking checklist. For each project prepare a brief, rubric, sample acceptable evidence and an individual-defence prompt.

Instructor and mentor support. Use a named practitioner lead per track and approximately one practical mentor per 20–25 learners; reduce the ratio for engineering or complex lab sessions. Offer a recorded session or equivalent guided task for

learners with connectivity constraints.

Device and access baseline. Recommend a laptop with at least 8 GB RAM; provide browser labs or a higher-memory option for virtualisation-intensive work. Cybersecurity learners need isolated lab access; Power BI learners need compatible Windows access or a preselected cohort-wide alternative. AI Engineering does not require students to purchase a GPU.

Tool-cost control. Choose one main tool per capability. Provide sandbox datasets, shared lab infrastructure, bounded API quotas and a mock/offline fallback where feasible. Approve spending limits before live integrations. Verify current pricing and licences before each cohort rather than printing unverified prices in the syllabus.

Feedback and quality assurance. Return weekly feedback within seven days. Moderate a sample of marked work across instructors, verify final individual competence and gather feedback at Weeks 4, 8, 12, 16 and 20. Update tool-specific instructions before the next cohort while keeping learning outcomes stable.

Completion rules proposed for adoption. Require at least 60% overall, 60% in the capstone and 60% in the final practical, plus satisfactory evidence for every core learning outcome. Offer targeted resubmission for unmet outcomes. Require participation in 80% of facilitated activities or approved equivalent tasks; publish any local policy changes before enrolment.

Award and recognition. The provider must approve the final award title, hours and assessment policy. These documents do not establish equivalence to a regulated qualification or

endorsement by the reference organisations. Any accreditation or external-certification claims require a separate, verified approval process.

Reference guidance and curriculum maintenance

These are reference resources used to inform the proposed scope, not course endorsements or a claim of formal certification alignment. Reviewed 17 November 2026. Tool versions, access and pricing must be rechecked before delivery. Human–AI interaction design. Microsoft Research: Guidelines for Human-AI Interaction — https://www.microsoft.com/en-us/research/project/guidelines-for-human-ai-interaction/ AI product risk and evaluation. NIST AI Risk Management Framework and GenAI profile resources — https://www.nist.gov/itl/ai-risk-management-framework Analytics data preparation. Microsoft Learn: Prepare data for analysis with Power BI — https://learn.microsoft.com/en-us/training/paths/prepare-data-power-bi/ Cybersecurity work and skills. NIST NICE Framework Resource Center — https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center AI automation components and evaluation. n8n: Integrate AI — https://docs.n8n.io/build/integrate-ai.md LLM foundations and technical prerequisites. Hugging Face LLM Course — https://huggingface.co/learn/llm-course/chapter1/1 Predictive-model evaluation. scikit-learn: Model selection and evaluation — https://scikit-learn.org/stable/model_selection.html AI application security. OWASP GenAI/LLM application security project — https://owasp.org/projects/top-10-for-large-language-model-applications Human–AI interaction guidance informs expectations, correction and recovery in Design. NIST AI risk guidance informs product evaluation and governance. NICE informs task-based cybersecurity planning. Microsoft data-preparation guidance supports analytics sequencing. n8n and Hugging Face documentation inform automation and engineering capability boundaries. scikit-learn and OWASP inform evaluation and security practice.

Questions? Contact info@axia.africa.