

AI-Power in Action: Cybersecurity Workflows

A demonstration-led generative AI workshop

FA-0574 · 1 day

Cybersecurity · Agentic & Generative AI

Practise AI-assisted alert review, log interpretation, incident/risk reporting and security communication with verified evidence and human review.

Introduction

This one-day demonstration-led workshop explores generative AI assistance for cybersecurity, IT, audit and risk teams. It covers selected prompts, tool comparisons and illustrative alert, log, vulnerability and reporting tasks.

Participants complete a small set of guided exercises rather than every example in the source. The emphasis is evidence checking, confidentiality, bounded tool access and analyst responsibility. AI explanations, remediation suggestions and risk scores are drafts or hypotheses, not verified findings or authorised response actions.

Use prepared fictitious or appropriately sanitised data. The course does not connect to a production SOC, automate containment or guarantee faster or more accurate investigations.

Learning outcomes

The workshop teaches participants to:

- Explain basic AI/LLM concepts, capabilities and limitations relevant to security work.
- Write scoped prompts with context, assumptions, output format and verification criteria.
- Review selected alert/log summaries, possible causes and incident timelines against underlying evidence.
- Draft vulnerability, risk and stakeholder communications for technical review.
- Identify hallucination, injection, leakage, automation-bias and excessive-trust risks.

- Outline a bounded analyst-reviewed workflow and a low-risk adoption pilot.

Prerequisites

- Basic familiarity with IT, cybersecurity, risk, or business operations.
- No prior AI, machine learning, or programming experience is required.
- An open-minded approach to using AI tools responsibly and practically.
- A Google account or access to commonly available Generative AI tools is recommended.
- Participants should avoid using real confidential company, customer, or security incident data during demos and exercises.

Training outline

1. 1 — AI foundations and security boundaries

- AI, machine learning, deep learning, LLMs, generative models, agents and copilots: accessible distinctions.
- Selected capabilities: summaries, classification assistance, pattern explanation, reports, policy and awareness drafts.
- Limitations: hallucinations, technical errors, outdated information, missing context and overconfident output.
- Potential productivity benefits must be measured; security conclusions require human evidence review.

2. 2 — Tool selection and prompt practice

- Compare selected ChatGPT, Gemini, Copilot, Claude, Perplexity and source-notebook workflows where available.
- Gemini Notebook (formerly NotebookLM): source synthesis and traceability, not automatic correctness.
- Understand how assistance may sit alongside SIEM, SOAR, EDR/XDR, network detection, scanners, ticketing, GRC and intelligence portals; no automatic integration assumed.
- Prompt structure: objective, source data, context, constraints, assumptions, audience, format and validation.
- Practise asking about uncertainty, alternatives, missing information and checks; refine and compare outputs.
- Avoid confidential uploads, unsupported conclusions and unreviewed remediation.

3.3 – Threat and incident-support exercises

- Alert triage: checked summaries, severity context, candidate causes and next investigation questions.
- Log/event review: timelines, possible patterns, correlation and noise, verified against the sample.
- Threat-report synthesis: indicators, techniques, business context and briefing notes with source checks.
- Draft incident, containment-note and lessons-learned reports; distinguish confirmed facts from hypotheses.
- Adapt analyst, operations, management and customer-facing language without inventing findings.
- Selected guided exercise: a synthetic alert/log sample through an incident and executive summary.

4.4 – Vulnerabilities and risk communication

- Interpret a selected advisory/CVE and affected-system context against authoritative sources.
- Discuss severity, exposure, asset criticality, exploitability, compensating controls and operational constraints.
- Draft patch/mitigation checklists and testing/change-management notes for specialist review.
- Draft risk statements and possible acceptance wording; AI scores or 'audit-ready' prose are not assurance evidence.
- Selected demonstration or exercise: a prepared vulnerability report translated into a checked management summary.

5.5 – Responsible and secure AI use

- Review before action, verify output, assign responsibility and document AI assistance.
- Prompt injection, unsafe output handling, false positives/negatives, fabricated explanations and tool misuse.
- Sensitive logs, incident/customer data, credentials, internal policies and architecture: data-handling and access boundaries.
- Approved tools, acceptable use, validation, human approvals, auditability and escalation.
- Privacy, fairness, transparency, regulatory awareness and staff readiness; safeguards reduce risk but do not guarantee safety.

6.6 – Policy, awareness and documentation

- Draft selected policies/procedures, plain-language summaries, checklists and FAQs.
- Prepare phishing-education, password/MFA, safe-AI and role-based awareness material.
- Check statements against the relevant policy or standard before publication.
- Selected exercise: an awareness message, procedure checklist or safe-use draft.

7.7 — A bounded security workflow

- Map alert intake, context enrichment, analyst review, response planning, documentation, reporting and lessons learned.
- Identify permissions, review checkpoints and where AI is unsuitable.
- Evaluate reporting time, quality, consistency, communication and manual rework without assuming improvement.
- Plan a low-risk pilot, user training, monitoring and evidence-based expansion.

8.8 — Final review and action plan

- Outline a simple AI-assisted workflow and safe-use checklist.
- Review unresolved evidence, data-handling and operational questions.
- Prepare personal next steps for appropriate organisational review.