BLACKBIRD FOR TRAINING

Simulation-Based Systematic Troubleshooting & Advanced Incident Investigation Course

28 February – 4 March 2027
Cairo (Egypt)

UK Traininig
PARTNER



Simulation-Based Systematic Troubleshooting & Advanced Incident Investigation Course

Ref: 96_363526 **Date:** 28 February – 4 March 2027 **Location:** Cairo (Egypt) **Fees:** 4900 GBP

Introduction

The Simulation-Based Systematic Troubleshooting & Advanced Incident Investigation course is an intensive two-day course designed to strengthen technical teams' capabilities in diagnosing technical failures, investigating incidents, and making evidence-based corrective decisions. The course follows an integrated practical methodology that guides participants through the complete troubleshooting process, from identifying symptoms and gathering facts to analysing root causes, selecting appropriate actions, and verifying successful resolution.

The course goes beyond theoretical explanations by incorporating an interactive, simulation-based training environment featuring gamified exercises and timed challenges. Participants encounter technical incident scenarios that evolve progressively, with new information becoming available depending on the decisions they make. These exercises allow participants to observe the consequences of their decisions and learn from unnecessary interventions and analytical mistakes.

The course includes up to 12 interactive simulation exercises delivered over two days. These cover individual incident investigations, evidence analysis, root cause identification, critical incident response, cross-team coordination, escalation, and handover management. Participants rotate through different roles, including Incident Lead, Technical Investigator, Evidence Analyst, and Documentation & Communication Officer. Performance is assessed, and results are reviewed following each exercise.

Course Objectives

By the end of the course, participants will be able to:

- Apply a structured and repeatable methodology for troubleshooting and technical incident investigation.
- Distinguish between symptoms, confirmed facts, assumptions, and misleading information.
- Gather and analyse technical evidence, including logs, alerts, timestamps, and system component dependencies.
- Develop root cause hypotheses and prioritise them according to the available evidence.
- Select appropriate corrective actions and establish verification and rollback criteria for unsuccessful interventions.
- Reduce unnecessary actions and improve first-time-fix efficiency.
- Manage technical investigations under time pressure and with incomplete or changing information.
- Improve coordination and information sharing across different technical teams.
- Conduct structured handovers and escalations while maintaining investigation continuity.
- Document decisions, actions, and outcomes, and prepare structured incident reports.



Target Audience

This course is designed for:

- Technical support and systems operations engineers responsible for diagnosing and resolving technical issues.
- Network, server, application, and IT infrastructure engineers.
- Service desk and technical support personnel responsible for receiving, classifying, and routing incidents.
- Problem analysts and technical investigators involved in root cause analysis.
- Incident leads and support or operations team managers responsible for coordinating incident response.
- IT service management specialists involved in escalation, documentation, and incident reviews.

Course Outlines

Day 1: Systematic Troubleshooting – The Core Analytical Process

Focus: Developing structured analytical thinking and applying an evidence-based methodology to diagnose technical failures and select appropriate solutions.

Training Topics:

- Fundamentals of systematic troubleshooting and the stages of incident investigation.
- Distinguishing facts from assumptions and identifying actual symptoms.
- Gathering information and analysing technical logs, alerts, and evidence.
- Developing hypotheses and analysing potential root causes.
- Selecting evidence-based corrective actions.
- Improving troubleshooting efficiency and first-time-fix performance.

Practical Simulation Exercises – Day 1:



1. **Simulation 1: The First Alert** – Participants receive an initial report of a service outage and work to identify symptoms, confirmed information, unknown factors, and investigation priorities.
2. **Simulation 2: Fact or Assumption?** – Teams analyse a collection of conflicting reports, alerts, and observations to distinguish confirmed facts from unverified information and irrelevant details.
3. **Simulation 3: The Missing Information** – Teams face a technical incident with incomplete information and must identify the additional data and checks required before taking any action.
4. **Simulation 4: The Root Cause Challenge** – Teams investigate an incident involving several possible causes. They develop hypotheses, test them against available evidence, and rank the most likely explanations.
5. **Simulation 5: The Wrong Fix** – Teams compare several corrective actions, identify the risks of interventions that are not supported by evidence, and select the most appropriate response.
6. **Simulation 6: First-Time-Fix Challenge** – Teams attempt to resolve a technical incident using the fewest possible investigation and intervention steps while ensuring that the resolution is properly verified.
7. **Simulation 7: The Complete Incident** – Teams conduct a complete investigation, beginning with symptom identification and ending with the identification of the most likely cause, selection of corrective action, verification of the solution, and preparation of an incident summary.

Practical Deliverables – Day 1:

- Symptom and fact assessment sheet.
- Information and evidence requirements checklist.
- Potential root cause analysis matrix.
- Corrective action plan and verification criteria.
- Complete incident investigation summary.

Day 2: Advanced Troubleshooting & Multi-Team Incident Management

Focus: Applying investigation skills under pressure, managing changing information, and coordinating technical teams during complex incidents.

Training Topics:

- Troubleshooting critical incidents under time pressure and prioritising response actions.
- Managing incomplete, conflicting, and changing information during investigations.
- Coordinating investigations and sharing information across technical teams.
- Managing incident handovers and escalations.
- Controlling complex investigations and allocating responsibilities.
- Documenting incidents and preparing timelines, decision logs, and reports.

Practical Simulation Exercises – Day 2:



8. **Simulation 8: The Critical Incident** – Teams face a major service disruption while operations are ongoing. They must assess incident severity, establish priorities, and make decisions within a defined timeframe.
9. **Simulation 9: The Changing Evidence** – Teams receive new technical information that conflicts with their initial hypotheses. They must reassess potential causes, update the investigation plan, and document the reasons behind changes in their decisions.
10. **Simulation 10: Distributed Information Challenge** – Four teams work on different aspects of a single technical incident. Each team holds separate information, and participants must exchange findings and connect the evidence to identify the most likely cause.
11. **Simulation 11: The Escalation and Handover** – Teams deal with an unresolved incident and prepare a structured handover covering actions taken, findings, missing information, risks, and next responsibilities.
12. **Simulation 12: The Major Incident War Room** – All teams participate in a complex and evolving investigation involving multiple technical components, changing information, and several escalation requirements. Participants allocate roles, coordinate the investigation, and prepare a consolidated report of findings and recommendations.

Practical Deliverables – Day 2:

- Incident timeline and decision log.
- Cross-team information-sharing and dependency map.
- Structured handover and escalation template.
- Investigation decision and action register.
- Final investigation report and improvement recommendations.
- Individual and team action plans for applying the acquired skills.

Skills Acquired

Upon completion of this course, participants will be able to:

- Identify symptoms and distinguish confirmed facts from assumptions.
- Gather evidence and analyse technical logs and alerts.
- Develop hypotheses and conduct root cause analysis.
- Evaluate corrective actions and the risks of technical interventions.
- Improve first-time-fix performance.
- Manage investigations under time pressure.
- Handle changing and conflicting information.
- Coordinate investigations and share information across teams.
- Manage structured escalations and handovers.
- Prepare incident timelines, decision logs, and investigation reports.



Why Attend This Course?

- **Learn Through Practice:** Apply troubleshooting methodologies through up to 12 interactive simulations rather than relying solely on theoretical concepts.
- **Respond Under Pressure:** Experience scenarios involving limited time, incomplete information, and decisions with immediate consequences.
- **Improve Investigation Quality:** Develop the ability to gather evidence and evaluate hypotheses before implementing corrective actions.
- **Reduce Unnecessary Interventions:** Build more accurate and efficient approaches to diagnosing technical failures and selecting solutions.
- **Strengthen Teamwork:** Practise collaborative investigations, information sharing, escalation, and handovers between teams.
- **Achieve Practical Outcomes:** Develop templates and practical tools that can be applied to real technical incidents and investigations.

Assessment and Simulation Methodology

Participants' performance is assessed throughout the practical exercises against criteria including analytical accuracy, quality of evidence gathering, root cause identification, corrective action selection, time management, communication, teamwork, documentation, and solution verification.

Each simulation involves presenting an incident scenario, assigning roles, releasing information in stages, making decisions within a defined timeframe, and reviewing the resulting outcomes. This is followed by a structured debrief to discuss effective decisions, mistakes, and opportunities for improvement.

Conclusion

The Simulation-Based Systematic Troubleshooting & Advanced Incident Investigation course provides a hands-on practical experience designed to improve how participants think and respond when facing technical failures, from receiving the initial alert to verifying the solution and closing the investigation.

Through individual and team-based simulations and timed challenges, participants learn how to gather evidence, test hypotheses, avoid unnecessary interventions, and maintain clear communication and investigation continuity across teams.

Following the course, participants will be able to transfer the tools and templates they have practised into their working environment, using them to structure real investigations, improve decision-making, and strengthen collaboration among technical team members.



FAQs

1. What makes the Simulation-Based Systematic Troubleshooting & Advanced Incident Investigation course different?

The course is based on experiential learning through up to 12 interactive simulation exercises involving evolving scenarios, timed challenges, and decisions with clear consequences. Rather than simply studying investigation procedures theoretically, participants practise diagnosing, analysing, correcting, and communicating within working teams.

2. What level of experience is required before attending the course?

The course is designed for professionals with practical experience in technical support, systems, networks, applications, or IT service operations. Basic familiarity with reading technical logs and alerts and understanding technical incidents will help participants gain greater value from the exercises.

3. How many simulation exercises does the course include?

The course includes up to 12 interactive exercises, with up to seven simulations on Day 1 and up to five advanced simulations on Day 2, depending on the session design and the time allocated for practical application and review.

4. How are participants organised during the simulations?

Participants are organised into up to four teams, each consisting of two to four members. Roles are distributed among the Incident Lead, Technical Investigator, Evidence Analyst, and Documentation & Communication Officer. Roles may be combined depending on the number of team members.

5. What practical tools and deliverables will participants receive?

Participants practise using symptom and fact assessment templates, evidence matrices, potential cause analysis tools, incident timelines, decision logs, handover and escalation templates, investigation reports, and action plans. These deliverables are designed to support the application of the methodology in the workplace after the training.

