BLACKBIRD FOR TRAINING

SANS-GIAC Security Essentials Certification

12 – 16 September 2027
Istanbul (Turkey)

UK Traininig
PARTNER



www.blackbird-training.com

SANS-GIAC Security Essentials Certification

Ref: 3255610_346224 **Date:** 12 – 16 September 2027 **Location:** Istanbul (Turkey) **Fees:** 4900 GBP

Introduction

The SANS-GIAC Security Essentials Certification is a professional credential focused on building a strong foundation in information security principles and practical protection mechanisms.

It provides structured knowledge covering network security, system protection, risk assessment, and incident response.

The certification bridges technical controls with governance and risk management to ensure security aligns with organizational strategy.

This program is designed for executives, department managers, information security professionals, technology leaders, risk officers, compliance specialists, and project managers.

It supports professionals across financial institutions, energy organizations, telecommunications providers, government entities, industrial sectors, and service-based enterprises.

The practical value of the SANS-GIAC Security Essentials Certification lies in strengthening the ability to identify threats, implement essential security controls, assess vulnerabilities, and improve institutional cyber readiness.

Participants gain structured analytical skills that enhance decision-making and reinforce operational resilience.

Course Objectives

The SANS-GIAC Security Essentials Certification aims to deliver measurable and applicable outcomes, including:

- Understand fundamental information security concepts.
- Identify common cyber threats and attack methods.
- Analyze network structures and potential vulnerabilities.
- Implement essential system and server protection controls.
- Assess technical risks and develop mitigation strategies.
- Apply monitoring mechanisms to detect malicious activity.
- Execute structured incident response procedures.
- Understand encryption principles and data protection methods.
- Manage identity and access control frameworks.
- Prepare security assessment reports for leadership.
- Strengthen integration between security and business continuity.
- Promote an organizational security awareness culture.



Course Outlines

Day 1: Core Foundations of Information Security and Network Architecture

- Principles of confidentiality, integrity, and availability.
- Overview of organizational network components.
- Data transmission fundamentals and communication protocols.
- Identification of architectural weaknesses.
- Risk management at the infrastructure level.
- Practical exercise analyzing a threat scenario.

Day 2: Threat Landscape and Defensive Protection Mechanisms

- Malware types and infection vectors.
- Denial-of-service attack patterns.
- Social engineering techniques and risk exposure.
- Firewall configuration principles.
- Vulnerability management processes.
- Case study analysis of a real security breach.

Day 3: Operating System Security, Access Control, and Encryption

- Securing operating systems against compromise.
- User account and privilege management.
- Principle of least privilege implementation.
- Encryption fundamentals and cryptographic usage.
- Database and sensitive data protection strategies.
- Practical lab on secure access policy configuration.

Day 4: Intrusion Detection and Incident Response

- Monitoring systems for suspicious activity.
- Log analysis methodologies.
- Initial incident response steps.
- Containment and mitigation techniques.
- Digital evidence collection procedures.
- Simulation exercise of a security incident.



Day 5: Comprehensive Security Evaluation and Sustainable Protection Strategy

- Review of core security principles.
- Organizational security posture assessment.
- Development of phased security improvement plans.
- Integration with enterprise risk management.
- Presentation of applied exercises.
- Final case-based evaluation.

Why Attend This Course? Wins & Losses!

- Strengthens institutional cyber defense capabilities.
- Reduces exposure to security breaches.
- Enhances regulatory and compliance readiness.
- Improves structured risk analysis skills.
- Elevates technology team competency.
- Supports informed executive decision-making.
- Improves cyber incident preparedness.
- Reinforces stakeholder trust in digital systems.

Conclusion

The SANS-GIAC Security Essentials Certification provides a structured framework for mastering foundational security principles and applying them within modern organizations. It covers network protection, system hardening, encryption, risk evaluation, and incident response in a methodical manner.

By applying the methodologies learned, organizations can reduce operational risk, strengthen resilience, and enhance governance maturity. Developing strong foundational security knowledge remains a strategic requirement for protecting digital assets and ensuring operational stability.

