

No. 155

CERTIFICATION GUIDE

GIAC GSEC Study Guide

A plain-language guide to GIAC Security Essentials

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 155

GIAC GSEC Study Guide

A plain-language guide to GIAC Security Essentials

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

GIAC GSEC Study Guide

A plain-language guide to GIAC Security Essentials

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. GIAC and GSEC are trademarks of GIAC Certifications. SANS is a trademark of the SANS Institute. This guide is independent and is not affiliated with, sponsored by or endorsed by GIAC or SANS. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this guide 1

PART I · THE CERTIFICATION

1 What GSEC is 4
2 Exam format 5
3 The objective areas 6
4 CyberLive questions 7
5 Building an index 8
6 Renewal 9
7 A study plan 10

PART II · NETWORKS, CRYPTO AND DEFENSE

8 Defense in depth 12
9 Access control and passwords 13
10 Security frameworks and CIS Controls 14
11 Networking and protocols 15
12 TCP and packet analysis 16
13 Defensible network architecture 17
14 Network security devices 18
15 Wireless and web communication security 19
16 Cryptography 20
17 Applying cryptography 21
18 Endpoint security and malware mitigation 22
19 DLP, mobile, containers and macOS 23

PART III · PLATFORMS AND OPERATIONS

20 Windows security infrastructure 25
21 Windows access controls 26
22 Enforcing Windows security policy 27
23 Windows as a service and Microsoft cloud 28

FREE SAMPLE · ojayo.com

24 Windows automation, auditing and forensics 29
25 Linux fundamentals and hardening 31
26 Virtualization, cloud and AI essentials 32
27 Log management and SIEM 33
28 Vulnerability scanning and penetration testing 34
29 Incident handling and response 35
30 Incident handling in practice 36
31 Building a home lab 37
32 Bringing the themes together 38

PART IV · EXAM SUCCESS

33 Practice questions 40
34 Answers 42
35 CyberLive tips 43
36 Exam day 44
37 Common mistakes 45
38 GSEC and Security+ 46
39 Next steps 47
Checklists 48
Glossary 49
Further reading 50

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this guide

What this guide covers, who it is for, and how to use it.

GIAC Security Essentials (GSEC) is a practitioner certification that proves you understand core security technical skills, from networking and cryptography to Windows, Linux, cloud and incident handling. It is known for hands-on CyberLive questions and is widely used for government and defence roles.

This guide explains GSEC in plain language: exam facts, the 26 objective areas grouped into eight themes, diagrams, a study plan, index advice, original practice questions and exam-day tips.

What this guide is, and is not

- An independent study companion written in its own words.
- **Not** official GIAC or SANS material; it does not reproduce exam questions or objectives text.
- Use GIAC's published objective areas as your checklist.

Who this guide is for

- **IT and network administrators** moving into security.
- **Security analysts** who want a respected hands-on credential.
- **Career changers** after Security+ who want more depth.

How the guide is organized

- **Part I — The certification** (Chapters 1–7): what GSEC is, format, objective areas, CyberLive, the index, renewal and a study plan.

FREE SAMPLE · ojayo.com

- **Part II — Networks, crypto and defense** (Chapters 8–19): foundations, networking, cryptography and endpoints.
- **Part III — Platforms and operations** (Chapters 20–32): Windows, Linux, cloud, logging, vulnerability management and incident handling.
- **Part IV — Exam success** (Chapters 33–39): practice questions, labs and next steps.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical study and exam advice.

IN PRACTICE

How a concept looks in real security work.

WATCH OUT

Common traps and misunderstandings.

KEY IDEA

The one thing to remember from a section.

A note on screens

Screens are **illustrations**, not real GIAC exam screens or product screens.

FREE SAMPLE · ojayo.com

PART I

The certification

These chapters explain what GSEC is and how to prepare.

FREE SAMPLE · ojayo.com

CHAPTER 1

What GSEC is

A hands-on security essentials certification.

A definition

GSEC validates that a practitioner understands information security beyond simple terminology and can apply it to real systems. GIAC exams are closely aligned with SANS training, and GSEC lines up with the SANS security essentials course, though you can sit the exam without taking the course.

Why people choose it

- **Depth**: more technical than most entry certifications.
- **Hands-on**: CyberLive questions run in real virtual machines.
- **Recognition**: used in many government and defence workforce frameworks.

KEY IDEA

GSEC asks whether you can do security, not only define it.

FREE SAMPLE · ojayo.com

CHAPTER 2

Exam format

The exam.

Item	Detail
Questions	106
Time	4 hours
Passing score	72% (versions from April 6, 2026)
Question types	multiple choice plus CyberLive labs
Delivery	proctored: ProctorU or Pearson VUE
Attempt window	120 days from activation

Figure 2.1 GSEC exam at a glance

The passing score changed

GIAC set the GSEC passing score at 72% for exam versions released on or after April 6, 2026, after a standard-setting study; earlier versions used 73%.

WATCH OUT

Many websites still describe the older 180-question, 5-hour format. Always check your GIAC account for the format that applies to your attempt.

FREE SAMPLE · ojayo.com

CHAPTER 3

The objective areas

The objective areas.

GIAC lists 26 objective areas for GSEC. This guide groups them into eight themes to make study easier.

Theme (this guide)	GIAC objective areas it covers
Foundations	access control, defense in depth, CIS Controls
Networks	protocols, architecture, devices, wireless, web
Crypto	cryptography and its application
Endpoints	endpoint, malware mitigation, DLP, mobile, containers, macOS
Windows	six Windows and Microsoft cloud areas
Linux	fundamentals, security and hardening
Operations	logs and SIEM, vulnerability testing, incident handling
Cloud and AI	virtualization, cloud and AI essentials

Figure 3.1 26 objective areas grouped into 8 themes

New-style areas

Recent areas include containers and macOS, and virtualization, cloud security and AI essentials, which reflect where organizations now run their systems.

> **TIP**
> Windows has six areas of its own, so it deserves a big share of your study time.

FREE SAMPLE · ojayo.com

CHAPTER 4

CyberLive questions

Hands-on questions.

CyberLive questions put you in a lab with real virtual machines, tools and code, and ask you to find an answer by doing the task.

How to prepare

- Practise on the command line in Windows and Linux.
- Read logs and packet captures.
- Use common tools such as packet analysers, scanners and PowerShell.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide (you are reading this)
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

GIAC GSEC Study Guide

Enjoyed it? The full book has 55 pages and 39 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.