CCNP CYBERSECURITY

CBRCOR 350-201

Complete Learning Guide

Performing CyberOps Using Cisco Security Technologies

4 domains · 29 chapters · 145 practice questions
hands-on labs · case studies · quick reference · glossary

Jozef Baroš

EXAM-PREP STUDY GUIDE

CBRCOR 350-201

Complete Learning Guide

Performing CyberOps Using Cisco Security Technologies

A structured, exam-focused study guide for the CCNP Cybersecurity certification

Four domains · 29 chapters · 145 knowledge-check questions

Hands-on labs · worked case studies · quick reference · glossary

Jozef Baroš

CBRCOR 350-201 Complete Learning Guide

Performing CyberOps Using Cisco Security Technologies

Disclaimer. This book is an independent study guide and is not sponsored by, endorsed by, or affiliated with Cisco Systems, Inc. Cisco, CCNP, and related marks are trademarks or registered trademarks of Cisco Systems, Inc. All other trademarks are the property of their respective owners. The exam objectives referenced are published by Cisco and may change without notice; always confirm the current blueprint on the official Cisco certification site.

Use at your own risk. The information is provided for educational purposes "as is," without warranty of any kind. The code and commands in this book are illustrative; test them in a safe, isolated environment and never run security tooling against systems you do not own or have explicit permission to assess. The author assumes no liability for any loss or damage arising from the use of this material.

First edition · 2026

About This Book

This guide prepares you for the **CBRCOR 350-201** exam — *Performing Cybersecurity Using Cisco Security Technologies* — the core exam of the CCNP Cybersecurity certification. It is organized to mirror the official exam blueprint exactly, so your study maps one-to-one onto what you will be tested on.

What is inside

- **Four sections**, one per exam domain, divided into **29 focused chapters** that together cover every published objective.
- **145 knowledge-check questions** with full explanations — the correct answers are distributed evenly across choices so you learn the material, not the pattern.
- **Five hands-on labs** with runnable Python and Bash, **two worked case studies** that integrate all four domains, an **exam-strategy and study-plan** chapter, a **quick-reference** appendix, and a **glossary**.

How to use it

Read the sections in order — each builds on the vocabulary of the last. Take every knowledge check and, crucially, make sure you can explain *why each wrong option is wrong*. Run the labs rather than just reading them; the Automation domain rewards hands-on familiarity. Finish with the case studies and the exam-strategy chapter, then revisit your weak areas.

The callout boxes

Throughout the book, colored callouts flag the most useful asides. Learn to spot them:

> ✅ **Exam Tip — Exam Tip**
>
> A concrete pointer to what the exam tests and how to answer it — the highest-value boxes for passing.

> 💡 **Did you know? — Did you know?**
>
> Context and background that make a concept stick and reveal why it matters.

You will also see **Common Pitfall** boxes (frequent mistakes and wrong answers to avoid) and **From the Field** boxes (how the concept plays out in a real SOC). Each chapter ends with a **Summary** and **Key Takeaways** for fast revision.

Exam Blueprint

The CBRCOR 350-201 exam is a 120-minute exam associated with the CCNP Cybersecurity certification. It certifies knowledge of core cybersecurity operations: fundamentals, techniques, processes, and automation. The four domains and their weightings are below; this book devotes one section to each.

Domain	Weight	Covered in
1.0 Fundamentals	20%	Section 1 (chapters 1.1–1.5)
2.0 Techniques	30%	Section 2 (chapters 2.1–2.10)
3.0 Processes	30%	Section 3 (chapters 3.1–3.8)
4.0 Automation	20%	Section 4 (chapters 4.1–4.6)

Domain 1 — Fundamentals covers playbooks and tooling, compliance standards, cyber risk insurance, risk analysis, the incident-response workflow and its metrics, and cloud environments. **Domain 2 — Techniques** covers AI analytics and threat intelligence, system and network hardening, security posture, DevSecOps, data loss prevention, SIEM and detection tuning, SOAR, and behavioral and traffic analysis. **Domain 3 — Processes** covers threat modeling, case investigation, malware analysis, predictive analysis, endpoint intrusion, indicators, data-loss investigation, and vulnerability triage. **Domain 4 — Automation** covers SOAR mechanisms, Python, data formats, REST APIs, Bash, and CI/CD, DevOps, and Infrastructure as Code.

Cisco notes that related topics outside this list may appear on any delivery of the exam, and that the blueprint may change without notice. Understand the concepts — do not merely memorize the objectives — and confirm the current blueprint on Cisco's official certification site before your exam.

Table of Contents

Section 1 — Fundamentals

Welcome to the foundation of the CBRCOR 350-201 exam. This first domain accounts for **20% of the exam** and establishes the vocabulary, workflows, and mental models that every later domain assumes you already own. Before you can recommend a SOAR workflow (Domain 4) or run a malware investigation (Domain 3), you must be fluent in how a Security Operations Center (SOC) thinks: how it codifies its response in playbooks, which compliance regimes constrain it, how it quantifies risk, how it walks an incident from alarm to lessons learned, and how all of this changes when the workload lives in the cloud.

Treat this section as the grammar of cybersecurity operations. The topics here are described and applied rather than configured, so the exam questions tend to be scenario-based: you will be given a situation and asked which playbook applies, which standard governs it, or which incident-response phase you are in. Master the distinctions and the rest of the book becomes far easier.

Sub-section	Focus	Exam topics
1.1	Playbooks: components, tool selection, and common scenarios	1.1, 1.2, 1.3
1.2	Compliance standards and cyber risk insurance	1.4, 1.5
1.3	Risk analysis: assets, vulnerabilities, and threats	1.6
1.4	The incident response workflow and IR metrics	1.7, 1.8
1.5	Cloud environments and SecOps considerations	1.9, 1.10

> ✅ **Exam Tip — Read the verb in every objective**
>
> Cisco writes each exam objective with a deliberate verb: *interpret, determine, apply, infer, describe, analyze, compare*. A “describe” objective wants recognition of a concept; an “apply” objective wants you to choose the right action for a scenario. Matching your answer to the verb is one of the easiest ways to gain points in this domain.

1.1 Playbooks: Components, Tooling & Common Scenarios

Exam topics covered: 1.1 Interpret the components within a playbook · 1.2 Determine the tools needed based on a playbook scenario · 1.3 Apply the playbook for a common scenario such as unauthorized privilege escalation, DoS/DDoS, and website defacement.

What a playbook actually is

A **playbook** is a documented, repeatable, end-to-end response to a category of security event. Where an analyst's instinct is fast but inconsistent, a playbook makes the SOC's response *deterministic*: the same trigger produces the same investigative steps, the same decision points, and the same escalation path every time, regardless of which analyst is on shift at 3 a.m. In modern operations a playbook is often partially or fully automated inside a **SOAR** (Security Orchestration, Automation, and Response) platform, but the concept predates automation — it is fundamentally a structured plan.

It helps to separate two terms the exam likes to blur. A **runbook** is a low-level, often single-tool procedure ("how to pull a packet capture on this firewall"). A **playbook** is the higher-level orchestration that *strings runbooks together* into a complete response to a scenario such as a ransomware outbreak. One playbook calls many runbooks.

The components within a playbook

Objective 1.1 asks you to **interpret the components** of a playbook — so memorize the anatomy. A well-formed playbook contains:

- **Trigger / initiating condition** — the alert, detection, or request that starts the playbook (e.g., a SIEM correlation rule firing on multiple failed privilege escalations).
- **Scope and classification** — the incident type and severity, which determine urgency and who must be notified.
- **Roles and responsibilities** — who runs the playbook (Tier 1 vs Tier 2/3 analyst, incident commander), and who is informed.
- **Workflow steps** — the ordered investigative and response actions, usually expressed as a flow with **decision points** (if/then branches).
- **Required inputs and tools** — the data sources and platforms each step depends on (covered in 1.2).
- **Escalation criteria** — the conditions that promote the incident to a higher tier or invoke the formal IR process.
- **Evidence handling and documentation** — what to capture, where, and how to preserve chain of custody.
- **Closure / exit criteria** — the conditions that allow the incident to be declared resolved, plus post-incident notes.

> 💡 **Did you know? — Playbooks grew out of aviation and the military**
>
> The term "playbook" migrated into security from sports and, before that, from military operations orders — standardized responses rehearsed so heavily that execution under stress is automatic. That heritage is the whole point: a SOC playbook exists so that a stressed analyst at 3 a.m. performs like a

> rehearsed one.

Determining the tools a scenario needs

For objective 1.2 you must map playbook steps to the **category of tool** that performs them. You are rarely asked for a product name; you are asked for the *function*. The table below is the mapping the exam tests most.

Playbook need	Tool category	Example function
Centralized detection & correlation	SIEM	Aggregates logs, fires correlation rules, raises alerts
Automated, orchestrated response	SOAR	Runs the playbook, calls APIs, opens tickets, contains hosts
Endpoint visibility & containment	EDR / XDR	Isolates a host, kills a process, collects endpoint artifacts
Enriching indicators with context	Threat Intelligence Platform (TIP)	Looks up reputation, maps IOCs to actors/TTPs
Tracking the incident	Case / ticketing system	Records timeline, tasks, evidence, and closure
Deep packet / traffic inspection	NDR / packet capture	Reconstructs sessions, extracts files from PCAP
Forensic preservation	Forensic imaging / sandbox	Captures memory/disk, detonates samples safely

> 🌍 **From the Field — How a real SOC chooses tools mid-incident**
>
> In practice the SIEM is the front door: it raises the alert and provides the first correlation. The analyst pivots to EDR to confirm what ran on the host, enriches the indicators in a TIP, and — if the playbook is automated — lets the SOAR platform isolate the endpoint and open the case automatically. Knowing this pivot order is exactly what objective 1.2 is testing.

Applying playbooks to common scenarios

Unauthorized privilege escalation

Trigger: a standard account suddenly gains administrative rights, or a process spawns with higher privileges than its parent. The playbook validates whether the escalation was sanctioned (a change ticket?), identifies the technique (token manipulation, exploited service, misconfigured sudo), contains by disabling the account and isolating the host, then eradicates the persistence mechanism and reviews how the privilege was obtained.

Denial of Service (DoS) and Distributed DoS (DDoS)

Trigger: a sharp drop in availability or a flood of traffic. The playbook distinguishes a single-source **DoS** from a many-source **DDoS**, characterizes the attack (volumetric, protocol, or application-layer), engages

upstream mitigation (ISP scrubbing, CDN/anti-DDoS service, rate limiting), and protects business continuity. Note the emphasis on **availability** — the goal is to keep the service up, not to dissect malware.

Website defacement

Trigger: unauthorized modification of public web content. The playbook preserves the defaced state as evidence, restores from a known-good backup, identifies the entry vector (often an unpatched CMS, web-app vulnerability, or stolen credentials), and closes the gap. Reputation and public communication are part of this playbook in a way they are not for the others.

> ⚠️ **Common Pitfall — Don't confuse playbook components with IR phases**
>
> Students frequently answer a "what is a component of a playbook?" question with an incident-response *phase* (e.g., "Containment"). Phases belong to the IR lifecycle in 1.4. A playbook *component* is structural — trigger, roles, decision points, escalation criteria. Keep the two vocabularies separate.

> **Summary**
>
> A playbook is a structured, repeatable response to a class of security event, often automated in a SOAR platform. Its components are structural — trigger, scope, roles, workflow with decision points, required tools, escalation criteria, evidence handling, and closure. Tool selection maps each step to a function (SIEM for detection, EDR for endpoint action, TIP for enrichment, ticketing for tracking). The three named scenarios each have a distinct emphasis: privilege escalation centers on how access was gained, DoS/DDoS centers on availability and upstream mitigation, and website defacement centers on evidence preservation, restoration, and reputation.

> **Key Takeaways**
>
> **Playbook ≠ runbook:** a playbook orchestrates many runbooks. **Components are structural, not phases. Tool questions test function, not brand** — know SIEM/SOAR/EDR/TIP roles. **DoS vs DDoS** is single-source vs distributed, and both are about **availability**. **Defacement** uniquely involves reputation and restore-from-backup.

Knowledge Check — 1.1 Playbooks

Q1. Which item is a structural *component* of a playbook rather than a phase of incident response?

- **A.** Eradication of the threat
- **B.** Recovery of affected systems
- **C.** A decision point that branches the workflow
- **D.** Post-incident lessons learned

Correct answer: C. Decision points are part of a playbook's structure. Eradication, recovery, and lessons learned are phases of the IR lifecycle, not playbook components.

Q2. During a playbook step you must isolate a compromised laptop and kill a malicious process. Which tool category performs this?

- **A.** EDR/XDR
- **B.** SIEM
- **C.** Threat Intelligence Platform

D. Ticketing system

Correct answer: A. Endpoint Detection and Response (EDR/XDR) provides host isolation and process termination. A SIEM detects, a TIP enriches, and ticketing tracks — none of them act on the endpoint.

Q3. A flood of traffic from thousands of distinct source addresses overwhelms a web service. Which scenario and primary concern apply?

A. DoS — confidentiality

B. Defacement — integrity

C. Privilege escalation — access

D. DDoS — availability

Correct answer: D. Many distinct sources make this a Distributed DoS, and the impacted security property is availability. A single-source DoS would not show thousands of origins.

Q4. What best distinguishes a runbook from a playbook?

A. A runbook is automated and a playbook is always manual

B. A runbook is a low-level single procedure; a playbook orchestrates several into a full response

C. A runbook is for executives and a playbook is for analysts

D. They are synonyms with no meaningful difference

Correct answer: B. A playbook is the higher-level orchestration that strings together multiple runbooks (low-level procedures) into an end-to-end response.

Q5. In a website-defacement playbook, which action is uniquely emphasized compared with the other common scenarios?

A. Preserving the defaced page as evidence before restoring from backup

B. Isolating the user's endpoint

C. Engaging the ISP for traffic scrubbing

D. Disabling the privileged account

Correct answer: A. Defacement uniquely centers on preserving the altered public content as evidence and restoring from a known-good backup, alongside reputation management. Host isolation, scrubbing, and account disabling belong to the other scenarios.

1.2 Compliance Standards & Cyber Risk Insurance

Exam topics covered: 1.4 Infer the industry for various compliance standards such as PCI, FISMA, FedRAMP, SOC, SOX, GDPR, Data Privacy, and ISO 27001 · 1.5 Describe the purpose of cyber risk insurance.

Why compliance lives in a security operations exam

Compliance standards dictate *what* a SOC must monitor, log, retain, and report. A breach of cardholder data triggers different obligations than a breach of EU citizens' personal data. Objective 1.4 does not ask you to recite every control — it asks you to **infer the industry or domain** a standard governs. So the winning study strategy is a clean mapping of standard → who it applies to.

Standard	Applies to / industry	In one line
PCI DSS	Anyone storing/processing payment card data	Protects cardholder data; mandated by the card brands
FISMA	US federal agencies and their contractors	Requires a risk-based security program for federal systems
FedRAMP	Cloud services sold to US government	Standardized security authorization for cloud providers
SOC 1 / SOC 2 / SOC 3	Service organizations (esp. SaaS/hosting)	AICPA attestation of controls; SOC 2 covers security/availability
SOX	US publicly traded companies	Integrity of financial reporting and related IT controls
GDPR	Any org handling EU residents' personal data	EU data-protection and privacy law with global reach
ISO/IEC 27001	Any organization, any sector	International standard for an Information Security Management System (ISMS)

> ✅ **Exam Tip — Anchor each standard to one keyword**
> PCI → *cards*. FISMA/FedRAMP → *US federal* (FedRAMP specifically *cloud*). SOX → *financial reporting / public companies*. GDPR → *EU privacy*. SOC → *service-provider attestation*. ISO 27001 → *ISMS, any industry*. If a scenario mentions credit cards, the answer is PCI; if it mentions a US agency buying a cloud service, it is FedRAMP.

The traps the exam sets

Several of these standards are deliberately easy to confuse, and the exam exploits that.

- **SOC vs SOX.** SOC (System and Organization Controls) is an AICPA *audit/attestation* for service providers. SOX (Sarbanes–Oxley) is *US law* about financial-reporting integrity. They sound alike and are unrelated in purpose.

- **ISO 27001 vs 27002.** 27001 specifies the *requirements* of an ISMS and is the **certifiable** standard; 27002 is a *guidance* catalog of controls. The blueprint's "27101" is a typo — the standard you need is **27001**.
- **FISMA vs FedRAMP.** FISMA governs federal *systems* generally; FedRAMP is the specific program for authorizing *cloud services* used by the government.

> ⚠️ **Common Pitfall — "Data Privacy" is broader than GDPR**
>
> The objective lists GDPR *and* "Data Privacy" separately. Treat data-privacy as the broad category (which also includes laws like CCPA/CPRA in California). GDPR is the flagship example, but a scenario set in the United States may point to a different privacy regime.

> 💡 **Did you know? — GDPR fines scale with global revenue**
>
> GDPR's top administrative fine is the greater of €20 million or **4% of total worldwide annual turnover**. That revenue-linked ceiling is why GDPR reshaped logging and breach-notification practice far beyond Europe — and why it is a favorite exam example of a privacy regime with teeth.

Cyber risk insurance

No control set eliminates risk entirely. After an organization mitigates what it can, a **residual risk** remains. **Cyber risk insurance** is a *risk-transfer* mechanism: for a premium, the insurer absorbs a defined portion of the financial loss from a cyber event. Its purpose, in the language objective 1.5 wants, is to **transfer residual financial risk** that the organization has chosen not to (or cannot) eliminate.

Coverage typically splits into two buckets. **First-party** coverage pays the insured's own costs — incident response, forensics, data restoration, business interruption, extortion/ransom, and breach notification. **Third-party** (liability) coverage pays claims brought *by others* — affected customers, partners, or regulators. Crucially, insurance does not reduce the likelihood of an incident; it cushions the financial impact, and most policies *require* baseline controls (MFA, EDR, backups) before they will pay.

> 🌍 **From the Field — Insurers now drive security baselines**
>
> Because insurers price risk, cyber-insurance questionnaires have effectively become a security checklist. Many organizations deployed MFA and EDR not because an auditor demanded it but because their insurer refused to renew without it. On the exam, remember the *purpose*: insurance treats risk by **transferring** it — it is one of the four classic risk responses, alongside accept, avoid, and mitigate (see 1.3).

Summary

Compliance standards tell a SOC what to protect, log, and report, and the exam tests your ability to infer which industry each one governs: PCI for payment cards, FISMA/FedRAMP for US federal (FedRAMP specifically for cloud), SOX for public-company financial reporting, GDPR for EU privacy, SOC for service-provider attestations, and ISO 27001 for an ISMS in any sector. Cyber risk insurance is a risk-transfer mechanism that absorbs residual financial loss — first-party coverage pays the insured's own costs and third-party coverage pays liability claims — but it does not lower the probability of an incident.

Key Takeaways

> **Map each standard to one keyword. SOC ≠ SOX**; **ISO 27001** is the certifiable ISMS standard (not 27101). **FedRAMP = cloud for US government. GDPR = EU privacy**, fines up to 4% of global revenue. **Insurance transfers residual financial risk**; first-party = your costs, third-party = liability; it requires, not replaces, controls.

Knowledge Check — 1.2 Compliance & Insurance

Q1. A scenario describes a SaaS vendor that must demonstrate its security and availability controls to enterprise customers via an independent attestation. Which standard fits?

- **A.** SOX
- **B.** SOC 2
- **C.** PCI DSS
- **D.** FISMA

Correct answer: B. SOC 2 is the AICPA attestation service organizations use to demonstrate controls (including security and availability) to customers. SOX governs financial reporting, PCI governs card data, and FISMA governs federal systems.

Q2. What is the primary purpose of cyber risk insurance?

- **A.** To eliminate the likelihood of a breach
- **B.** To replace the need for security controls
- **C.** To certify compliance with ISO 27001
- **D.** To transfer residual financial risk to an insurer

Correct answer: D. Insurance is a risk-transfer mechanism; it cushions financial loss but does not reduce the probability of an incident and does not replace controls — most policies require them.

Q3. A US federal agency wants to procure a cloud-hosted application. Which program authorizes the cloud service for government use?

- **A.** FedRAMP
- **B.** PCI DSS
- **C.** GDPR
- **D.** SOX

Correct answer: A. FedRAMP standardizes security authorization for cloud services sold to the US government. FISMA is the broader federal mandate, but the cloud-specific program is FedRAMP.

Q4. Which statement about ISO/IEC 27001 is correct?

- **A.** It is a US law governing financial reporting
- **B.** It applies only to payment-card environments
- **C.** It specifies the requirements for an ISMS and is the certifiable standard
- **D.** It is guidance only and cannot be certified against

Correct answer: C. 27001 defines ISMS requirements and is certifiable; 27002 is the guidance/controls catalog. It is sector-agnostic, not card- or finance-specific.

Q5. Which coverage type would pay for lawsuits brought by customers whose data was exposed?

- **A.** First-party coverage
- **B.** Business-interruption coverage