

No. 120

CYBERSECURITY

Incident Response Planning

Preparing to detect, contain and recover from cyber incidents



oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 120

Incident Response Planning

Preparing to detect, contain and recover from cyber incidents

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Incident Response Planning

Preparing to detect, contain and recover from cyber incidents

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. Product and company names mentioned in this book are trademarks of their respective owners. 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 book 1

PART I · FOUNDATIONS

1 What an incident is 5
2 Why plan 6
3 The lifecycle 7
4 NIST CSF 2.0 and SP 800-61 8
5 Incident types 9
6 Severity levels 10
7 Myths 11
8 Getting leadership support 12

PART II · PREPARING

9 The team 14
10 The plan 15
11 Contacts 16
12 Playbooks 17
13 Tools and access 18
14 Logging readiness 19
15 Backups and recovery readiness 20
16 Third parties 21
17 Retainers and insurance 22
18 For small organizations 23

PART III · RESPONDING

19 Detection and reporting 25
20 The first hour 26
21 Analysis 27
22 Containment 28
23 Eradication 29

FREE SAMPLE · ojayo.com

24 Recovery 30
25 Communication 31
26 Legal and regulatory reporting 33
27 Evidence 34
28 Difficult decisions 35
29 Working with law enforcement 36

PART IV · IMPROVING

30 Exercises 38
31 Lessons learned 39
32 Metrics 40
33 Common mistakes 41
34 Practice scenarios 42
35 A worked example 43
36 A readiness roadmap 44
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

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

Every organization will face a cyber incident sooner or later: a phishing email that works, ransomware on a server, a stolen laptop, a supplier breach or a mistake that exposes data. What separates a bad day from a disaster is usually **preparation**: knowing who does what, having the right contacts and tools ready, and having practised.

Incident response planning is that preparation. This book explains, for beginners, how to build an incident response plan and the capability behind it: roles, severity levels, playbooks, communication, legal reporting, evidence, recovery, exercises and lessons learned. It follows current guidance, including NIST's incident response recommendations revised in 2025 to align with the Cybersecurity Framework 2.0.

What this book covers

- What incidents are and why planning matters.
- The incident response lifecycle and the NIST CSF 2.0 view.
- Building the team, the plan, severity levels and playbooks.
- Detection, analysis, containment, eradication and recovery.
- Communication, legal and regulatory reporting, and evidence.
- Exercises, lessons learned, metrics and a readiness roadmap.

Who this book is for

- **IT and security staff.**

FREE SAMPLE · ojayo.com

- **Managers and executives** who will make decisions in a crisis.
- **Legal, communications and risk professionals.**
- **Small business owners.**

How the book is organized

- **Part I — Foundations** (Chapters 1–8): incidents, why plan, the lifecycle, NIST CSF 2.0, incident types, severity, common myths, and leadership support.
- **Part II — Preparing** (Chapters 9–18): the team, the plan, contacts, playbooks, tools and access, logging, backups, third parties, insurance and retainers, and small organizations.
- **Part III — Responding** (Chapters 19–29): detection, the first hour, analysis, containment, eradication, recovery, communication, legal reporting, evidence, decision-making, and law enforcement.
- **Part IV — Improving** (Chapters 30–36): exercises, lessons learned, metrics, common mistakes, scenarios, a worked example, and a roadmap.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in a real organization.

WATCH OUT

Common mistakes and risks.

FREE SAMPLE · ojayo.com

KEY IDEA

The one thing to remember from a section.

A note on law and screens

This book is not legal advice; reporting rules vary by country and sector and change over time. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what incidents are, why planning matters and the frameworks that guide response.

FREE SAMPLE · ojayo.com

CHAPTER 1

What an incident is

An incident is an event that harms or threatens security.

Events and incidents

An **event** is anything observable, such as a login or an alert. A **security incident** is an event, or series of events, that actually or potentially harms the confidentiality, integrity or availability of systems or data, or breaks security policy.

Examples

A successful phishing attack, malware on a device, unauthorized access to data, a lost unencrypted laptop or a ransomware attack are all incidents.

KEY IDEA

Not every alert is an incident, but every incident deserves a planned response.

FREE SAMPLE · ojayo.com

CHAPTER 2

Why plan

Preparation reduces damage and cost.

- **Speed**: decisions made in advance save critical hours.
- **Less damage**: fast containment limits spread.
- **Lower cost**: well-prepared organizations generally recover faster and spend less.
- **Compliance**: many laws and contracts require incident procedures and reporting.
- **Calm**: a clear plan reduces panic and mistakes.

FREE SAMPLE · ojayo.com

CHAPTER 3

The lifecycle

Response follows a recognizable cycle.

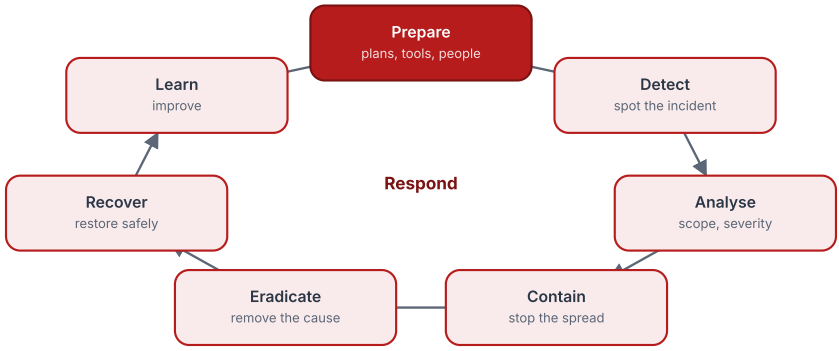


Figure 3.1 The incident response lifecycle

Not strictly linear

Teams often move back and forth, for example discovering more affected systems during recovery and returning to containment.

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 (you are reading this)
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
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

Incident Response Planning

Enjoyed it? The full book has 52 pages and 36 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.