

No. 117

CYBERSECURITY

Threat Modeling

Finding design flaws before attackers do

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 117

Threat Modeling

Finding design flaws before attackers do

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Threat Modeling
Finding design flaws before attackers do

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 threat modeling is 5
2 Why it matters 6
3 The four questions 7
4 When to do it 8
5 Who takes part 9
6 The Threat Modeling Manifesto 10
7 Myths 11
8 Outputs 12
9 Assets, attackers and assumptions 13

PART II · MODELING AND FINDING THREATS

10 Scoping 15
11 Data flow diagrams 16
12 Trust boundaries 17
13 An example diagram 18
14 STRIDE 19
15 Applying STRIDE 20
16 Attack trees 21
17 Other methods 22
18 Privacy threats 23
19 Attacker techniques 24

PART III · RESPONDING

20 Prioritizing 26
21 Responses 27
22 Common controls 28
23 Documenting 29

FREE SAMPLE · ojayo.com

24 Tracking 30
25 Validating 31
26 Retrospectives 32
27 Communicating risk 33

PART IV · IN PRACTICE

28 Running a session 35
29 Tools 36
30 Threat modeling in agile teams 37
31 Cloud systems 38
32 AI systems and agents 39
33 Scaling 40
34 Metrics 41
35 Common mistakes 42
36 A worked example 43
37 A starter plan 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.

Threat modeling is a structured way of thinking about what could go wrong with a system, before it goes wrong. Teams draw a simple picture of what they are building, ask how it could be attacked or misused, and decide what to do about each risk. It finds design flaws that no scanner can find, at the point where they are cheapest to fix.

This book explains threat modeling for beginners. It uses plain language and simple examples, introduces well-known methods such as STRIDE and attack trees, and shows how to make threat modeling a quick, regular habit rather than a heavyweight exercise.

What this book covers

- What threat modeling is, why it matters and when to do it.
- The four key questions and how to answer each.
- Data flow diagrams, trust boundaries, STRIDE and attack trees.
- Other methods: PASTA, LINDDUN, ATT&CK and approaches for AI systems.
- Prioritizing threats, choosing responses and tracking them.
- Running sessions, tools, scaling across teams and a starter plan.

Who this book is for

- **Developers and architects.**
- **Product managers and testers.**

FREE SAMPLE · ojayo.com

- **Security beginners** and security champions.

How the book is organized

- **Part I — Foundations** (Chapters 1–9): what threat modeling is, why it matters, the four questions, when to do it, who takes part, the Threat Modeling Manifesto, myths, outputs, and assets and assumptions.
- **Part II — Modeling and finding threats** (Chapters 10–19): scoping, data flow diagrams, trust boundaries, a worked diagram, STRIDE, applying STRIDE, attack trees, other methods, privacy threats, and attacker techniques.
- **Part III — Responding** (Chapters 20–27): prioritizing, responses, common controls, documenting, tracking, validating, retrospectives, and communicating risk.
- **Part IV — In practice** (Chapters 28–37): running a session, tools, agile teams, cloud systems, AI systems, scaling, metrics, common mistakes, a worked example, and a starter plan.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in a real team.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens

Screens are **simplified illustrations**. Names in examples are fictional.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what threat modeling is, why it matters, when to do it and who should take part.

FREE SAMPLE · ojayo.com

CHAPTER 1

What threat modeling is

Threat modeling means thinking about what could go wrong.

A simple definition

Threat modeling is the practice of analysing a system to identify potential threats and decide how to address them. A **threat** is something that could go wrong, such as an attacker reading data they should not.

You already do it

When you lock your door and leave a light on before a holiday, you are threat modeling your home: thinking about who might break in, how, and what would stop them.

For software

For software, threat modeling turns that instinct into a repeatable process that a team can share and record.

> **KEY IDEA**
> Threat modeling is structured thinking, not a special tool or a security-only activity.

FREE SAMPLE · ojayo.com

CHAPTER 2

Why it matters

It finds flaws that tools cannot.

Design flaws

Scanners find coding bugs. They cannot tell you that your password reset relies on guessable information or that any user can approve their own refunds. These are **design flaws**, and the OWASP Top 10 lists insecure design as a top risk.

Cheaper early

Changing a design on a whiteboard costs minutes; changing it after release costs weeks.

Shared understanding

Drawing the system together often reveals that team members had different ideas of how it works, which is itself a source of security bugs.

FREE SAMPLE · ojayo.com

CHAPTER 3

The four questions

Four questions frame every threat model.

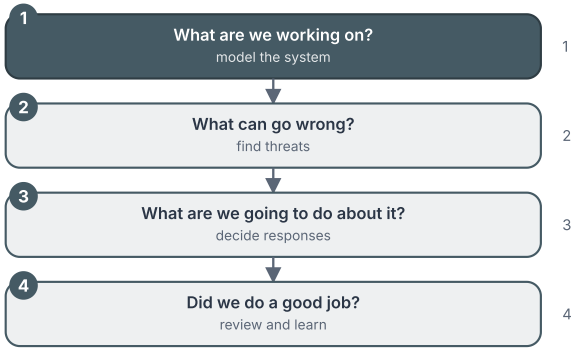


Figure 3.1 The four key questions

A simple framework

Adam Shostack's four questions, widely used in the industry, give every threat model the same structure, whatever method or tool you use. The rest of this book is organized around them.

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 (you are reading this)
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
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

Threat Modeling

Enjoyed it? The full book has 52 pages and 37 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.