THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW...

THREAT MODELING & SECURITY OPERATIONS

IDENTIFY THREATS. UNDERSTAND ADVERSARIES.
DETECT EARLY. RESPOND FAST. STAY SECURE.

THREAT MODEL
Identify assets, attackers, and attack vectors using proven threat modeling methodologies.

ASSESS RISK
Evaluate likelihood and impact to prioritize threats and focus on what matters most.

DETECT THREATS
Leverage the MITRE ATT&CK® framework, detection logic, and threat hunting techniques.

SECURITY OPERATIONS
Build and optimize SOC processes, monitoring, alerting, and incident response workflows.

RESPOND & CONTAIN
Execute effective incident response, contain threats, and minimize business impact.

IMPROVE & ADAPT
Measure, learn, and strengthen defenses through continuous improvement.

WHAT YOU'LL LEARN

- ✓ Threat modeling frameworks and best practices
- ✓ MITRE ATT&CK® and adversary tactics
- ✓ Vulnerability analysis and risk assessment
- ✓ Security monitoring, detection, and alerting
- ✓ Threat hunting and investigation
- ✓ Incident response and digital forensics overview
- ✓ Metrics, KPIs, and continuous improvement

REAL-WORLD FOCUS

- Practical examples and use cases
- Step-by-step guidance
- Templates and checklists
- Built for SOC analysts, engineers, architects, and security leaders
- Actionable insights you can apply immediately

WHO THIS BOOK IS FOR

Security engineers • SOC analysts • Threat hunters • Incident responders
Security architects • IT leaders • Anyone responsible for protecting systems, data, and users in today's complex threat landscape.

BELSHAW CONSULTING
ENGINEERING. SECURITY. RESULTS.

Just Tell Me What I Need To Know
Threat Modeling & Security Operations

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

Table of Contents

Introduction

Modern cybersecurity is no longer just about building strong defenses—it's about understanding how attackers think, anticipating how they will target your systems, and detecting malicious activity before it becomes a major incident.

Organizations today face increasingly sophisticated attacks that exploit weaknesses in applications, cloud environments, identities, networks, and business processes. At the same time, security teams are expected to monitor massive amounts of data, identify suspicious behavior, investigate incidents, and respond quickly to minimize damage. Success requires more than good technology; it requires understanding both the attacker's perspective and the defender's role.

The challenge is that information about threat modeling and security operations is often scattered across countless frameworks, standards, vendor documentation, and technical resources. Threat modeling methodologies, MITRE ATT&CK, SIEM platforms, threat hunting, digital forensics, and incident response are frequently treated as separate disciplines, making it difficult to understand how they work together.

That's where this book comes in.

The Just Tell Me What I Need to Know… series is designed to cut through the complexity and focus on the knowledge that cybersecurity professionals actually use. Rather than overwhelming you with unnecessary theory or product-specific details, each book delivers practical, real-world concepts in a clear, concise, and easy-to-understand format.

This book focuses on Threat Modeling & Security Operations—understanding how attackers plan and execute attacks, how defenders identify and prioritize risk, and how Security Operations Centers (SOCs) detect, investigate, and respond to security events. You'll learn how to perform threat modeling, use the MITRE ATT&CK framework to understand adversary behavior, engineer effective detections, hunt for threats, investigate incidents, automate security operations, and protect critical data throughout the attack lifecycle.

While the companion book Threat Management focuses on vulnerabilities, attack surfaces, patch management, and reducing organizational exposure, this book begins where prevention ends. It focuses on detecting attacks in progress, understanding attacker techniques, and building security operations that can rapidly identify, contain, and respond to threats.

Whether you're preparing for a cybersecurity certification, interviewing for a SOC, security engineering, or security architecture role, or simply looking to better understand how modern defensive operations work, this book provides the practical knowledge you need to think like an attacker—and defend like a professional.

Our goal is simple:

Give you the knowledge you need, without making you read three books to get it.

The key distinction from Threat Management is:

Threat Management asks: "What threats exist and how do we reduce exposure?"

Threat Modeling & Security Operations asks: "How do we anticipate attacks, detect them, investigate them, and respond?"

This book should teach readers to think like both an attacker and a defender.

So, let’s get started.

STOPPING ATTACKS IS IMPORTANT. DETECTING THEM BEFORE THEY BECOME DISASTERS IS ESSENTIAL.

No security control is perfect. Attackers eventually bypass firewalls, exploit vulnerabilities, steal credentials, or find new ways into enterprise environments. The organizations that recover fastest aren't the ones that prevent every attack—they're the ones that detect threats early, investigate them quickly, and respond effectively.

The problem? Most books treat threat modeling, Security Operations Centers (SOCs), threat hunting, incident response, digital forensics, and detection engineering as separate disciplines. Few explain how they work together to build a modern cyber defense.

This book is different.

Just Tell Me What I Need To Know... Threat Modeling & Security Operations provides a practical, business-focused guide to thinking like both an attacker and a defender. You'll learn how to identify likely attack paths before systems are deployed, understand adversary behavior using the MITRE ATT&CK framework, engineer effective detections, monitor enterprise environments, hunt for hidden threats, investigate incidents, automate security operations, and continuously improve your organization's ability to detect and respond to cyber attacks. Rather than focusing solely on prevention, this book explains how modern Security Operations transforms visibility, intelligence, and rapid response into organizational resilience.

THE MODERN CYBER DEFENSE LIFECYCLE

INSIDE YOU'LL LEARN HOW TO:

- Build and operate an effective Security Operations Center (SOC)
- Perform practical threat modeling using industry-leading methodologies
- Understand attacker tactics, techniques, and procedures with MITRE ATT&CK
- Design and improve detection engineering and security monitoring
- Conduct proactive threat hunting and digital forensics
- Respond to and recover from cybersecurity incidents
- Use automation and AI to strengthen security operations
- Build a mature, threat-informed security operations program that continuously improves over time

CORE DISCIPLINES. ONE UNIFIED DEFENSE.

THREAT MODELING	THREAT INTELLIGENCE	DETECTION ENGINEERING	MONITORING & SOC
THREAT HUNTING	INCIDENT RESPONSE	DIGITAL FORENSICS	AUTOMATION & AI

KEY CAPABILITIES YOU WILL BUILD

END-TO-END VISIBILITY
See more. Know more. Act faster.

EARLY THREAT DETECTION
Detect threats before they become breaches.

FASTER INCIDENT RESPONSE
Reduce dwell time. Limit impact. Recover faster.

STRONGER TEAM COLLABORATION
People, processes, and technology working together.

MEASURABLE IMPROVEMENT
Metrics, reporting, and continuous optimization.

BUSINESS RESILIENCE
Protect what matters. Support the mission. Build trust.

Whether you're a security architect, SOC analyst, engineer, threat hunter, incident responder, CISO, ISSO, consultant, project manager, or aspiring cybersecurity professional, this book gives you the practical knowledge needed to anticipate attacks, detect threats, respond with confidence, and build resilient security operations for today's evolving threat landscape.

ANTICIPATE ATTACKS. DETECT THREATS. RESPOND WITH CONFIDENCE. BUILD RESILIENT SECURITY OPERATIONS.

BELSHAW CONSULTING