THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW ...

THREAT MANAGEMENT

KNOW THE THREATS. UNDERSTAND THE RISK. TAKE ACTION. STAY AHEAD.

IDENTIFY
Discover threats, threat actors, and attack vectors across your environment.

ANALYZE
Understand threat intent, capabilities, and potential business impact.

DETECT
Use continuous monitoring and intelligence to detect threats early and accurately.

RESPOND
Contain, mitigate, and neutralize threats quickly to reduce damage.

RECOVER
Restore operations and strengthen defenses to prevent recurrence.

ADAPT
Learn from every incident and evolve your defenses continuously.

THE THREAT MANAGEMENT LIFECYCLE

IDENTIFY
Assets, threat actors, and attack vectors

ASSESS
Evaluate likelihood and impact

DETECT
Monitor and identify threat activity

RESPOND
Contain and mitigate the threat

RECOVER
Restore services and operations

IMPROVE
Strengthen defenses and reduce risk

KEY THREAT SOURCES

- **CYBER CRIMINALS** — Financial gain, ransomware, theft
- **NATION STATES** — Espionage, disruption, sabotage
- **INSIDER THREATS** — Malicious or negligent actions
- **THIRD-PARTY RISKS** — Vendors, partners, supply chain
- **EMERGING THREATS** — Zero-day exploits, AI-driven attacks

THREAT INTELLIGENCE

- **COLLECT** — Gather data from multiple sources
- **PROCESS** — Normalize and enrich intelligence
- **ANALYZE** — Identify patterns and indicators
- **SHARE** — Disseminate actionable insights
- **APPLY** — Use intelligence to drive decisions

BEST PRACTICES

- Maintain an up-to-date asset inventory
- Leverage threat intelligence feeds
- Implement defense-in-depth
- Use automation to reduce dwell time
- Test incident response regularly
- Measure, report, and improve

YOU CAN'T ELIMINATE ALL THREATS.
BUT YOU CAN MANAGE THEM.

PEOPLE | PROCESS | TECHNOLOGY

BELSHAW CONSULTING

Just Tell Me What I Need To Know

Threat Management

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

Table of Contents

Introduction 5

Part I — Threat Management Foundations 6

Chapter 1 — Introduction to Threat Management 6

Chapter 2 — Understanding Today's Threat Landscape 14

Chapter 3 — Threat Intelligence 22

Part II — Understanding Attack Vectors 31

Chapter 4 — Identity and Authentication Attacks 31

Chapter 5 — Privileged Access Attacks 40

Chapter 6 — Endpoint Attacks 50

Chapter 7 — Network Attacks 60

Chapter 8 — Application and API Attacks 69

Chapter 9 — Cloud and Container Threats 77

Chapter 10 — Emerging Technology Threats 87

Part III — Vulnerability Management 98

Chapter 11 — Understanding Vulnerabilities 98

Chapter 12 — Vulnerability Assessment 105

Chapter 13 — Prioritization and Exposure Management 113

Part IV — Mitigation Strategies 122

Chapter 14 — Patch Management 122

Chapter 15 — Secure Configuration Management 130

Chapter 16 — Reducing the Attack Surface 138

Chapter 17 — Defense in Depth 146

Part V — Advanced Threat Management 155

Chapter 18 — Threats to Critical Infrastructure 155

Chapter 19 — Cyber Warfare 165

Chapter 20 — Building an Enterprise Threat Management Program 174

Appendices 184

Appendix A — Threat Management Review Checklist 184

Appendix B — Common Attack Vectors Reference 191

Appendix C — Vulnerability Prioritization Checklist 201

Appendix D — Patch Management Checklist 207

Appendix E — Configuration Management Checklist 213
Appendix F — Threat Intelligence Sources 220
Appendix G — MITRE ATT&CK Tactics Summary 228
Appendix H — Common CVSS Scores Explained 237
Appendix I — Threat Management Interview Questions 245
Appendix J — Recommended Reading 252

Introduction

Cyber threats are constantly evolving. Every day, organizations face attacks from cybercriminals, nation-state actors, insider threats, hacktivists, and increasingly sophisticated automated tools. New vulnerabilities are discovered, attack techniques change, and emerging technologies create new opportunities for exploitation. For today's cybersecurity professional, understanding threats is no longer optional—it's essential.

The challenge is that there is an overwhelming amount of information available. Threat intelligence feeds, vulnerability databases, security advisories, government publications, vendor documentation, and industry frameworks provide valuable guidance, but finding the information that matters—and understanding how it all fits together—can be difficult.

That's where this book comes in.

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

This book focuses on Threat Management—understanding who attacks organizations, how they attack, what vulnerabilities they exploit, and how defenders reduce risk through sound security practices. You'll learn about threat actors, attack vectors, vulnerability management, configuration management, patch management, attack surface reduction, defense in depth, cyber warfare, and enterprise threat management strategies.

Unlike books that focus on incident response or Security Operations Centers (SOCs), this book concentrates on identifying, understanding, and reducing threats before they become successful attacks. It explains not only what modern threats look like, but also how organizations assess exposure, prioritize remediation, and build resilient security programs that continuously reduce risk.

Whether you're preparing for a certification, interviewing for a cybersecurity role, expanding your technical knowledge, or leading enterprise security initiatives, this book provides the practical understanding you need to confidently discuss and apply modern threat management concepts.

Our goal is simple:

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

So, let's get started.

Part I — Threat Management Foundations

Chapter 1 — Introduction to Threat Management

Cybersecurity is no longer simply about building strong defenses. Modern organizations operate in an environment where cyber threats are continuous, sophisticated, and constantly evolving. Attackers range from lone hackers and organized cybercriminals to nation-state intelligence agencies and insider threats. They exploit technology, business processes, and human behavior to achieve their objectives. As organizations become more connected through cloud computing, remote work, mobile devices, industrial control systems, and the Internet of Things (IoT), the number of opportunities available to attackers continues to grow.

For many years, cybersecurity focused primarily on preventing attacks through firewalls, antivirus software, and access controls. While prevention remains essential, organizations have learned that no defensive control is perfect. Even mature security programs experience successful attacks. The question is no longer whether an organization will be targeted, but how quickly it can identify threats, respond effectively, and recover from an incident.

Threat management provides the structured approach for accomplishing this objective. It combines people, processes, technology, and intelligence to continuously identify, understand, prioritize, and mitigate cyber threats before they become major business disruptions.

This chapter introduces the core concepts that form the foundation for the remainder of this book.

What is Threat Management?

Threat management is the continuous process of identifying, analyzing, preventing, detecting, responding to, and recovering from cybersecurity threats that could affect an organization's systems, data, personnel, or operations.

Rather than focusing on a single security technology, threat management is a comprehensive operational discipline. It integrates intelligence, security monitoring, vulnerability information, incident response, and continuous improvement into a coordinated program designed to reduce the organization's exposure to cyber threats.

Threat management answers several important questions:

- Who may attack us?
- What techniques are attackers currently using?
- Which assets are most likely to be targeted?
- How can attacks be prevented?
- How quickly can attacks be detected?
- How effectively can incidents be contained?
- What lessons can be learned to improve future defenses?

CYBER THREATS NEVER STOP EVOLVING. NEITHER CAN YOUR DEFENSES.

Today's organizations face an endless stream of attacks from cybercriminals, nation-state actors, insider threats, ransomware groups, and increasingly sophisticated AI-enabled adversaries. The challenge isn't just understanding the latest threats—it's knowing how to identify, prioritize, and reduce them before they become successful attacks.

The problem? Most books on threat management focus on a single technology, a specific security product, or the operations of a Security Operations Center. Few explain how all the pieces fit together into a practical enterprise threat management program.

This book is different.

Just Tell Me What I Need To Know... Threat Management provides a practical, business-focused guide to understanding modern cyber threats and reducing organizational risk. You'll learn how attackers operate, the techniques they use, and how organizations defend themselves through threat intelligence, vulnerability management, attack surface reduction, secure configuration, patch management, defense in depth, and enterprise threat management strategies. Rather than concentrating on responding after an attack, this book emphasizes proactively identifying and mitigating threats before they become major business disruptions. It combines proven cybersecurity principles with today's evolving threat landscape to help you build stronger, more resilient security programs.

TODAY'S THREAT LANDSCAPE

CYBERCRIMINALS
Profit-driven attacks targeting data, money, and operations.

NATION-STATE ACTORS
Strategic attacks for espionage, disruption, and advantage.

INSIDER THREATS
Malicious or negligent insiders who can cause major damage.

RANSOMWARE GROUPS
Extortion and encryption attacks that disrupt and demand payment.

AI-ENABLED ADVERSARIES
Using automation and AI to scale, personalize, and evade defenses.

INSIDE YOU'LL LEARN HOW TO:

- Understand today's threat actors and evolving attack landscape
- Analyze common attack vectors and adversary techniques
- Use threat intelligence to make better security decisions
- Prioritize vulnerabilities and reduce organizational exposure
- Strengthen defenses through secure configuration and patch management
- Apply defense-in-depth and attack surface reduction strategies
- Protect cloud, network, application, endpoint, and identity environments
- Build a mature, proactive enterprise threat management program

THREAT MANAGEMENT IN ACTION

CORE PILLARS OF EFFECTIVE THREAT MANAGEMENT

THREAT INTELLIGENCE
Know your enemy.

VULNERABILITY MANAGEMENT
Close gaps before they're exploited.

ATTACK SURFACE REDUCTION
Remove unnecessary exposure.

SECURE CONFIGURATION
Eliminate misconfigurations.

PATCH MANAGEMENT
Keep systems up to date.

DEFENSE IN DEPTH
Layer controls for resilience.

CONTINUOUS IMPROVEMENT
Adapt, learn, and stay ahead.

Whether you're a security architect, engineer, analyst, CISO, ISSO, consultant, project manager, or aspiring cybersecurity professional, this book provides the practical knowledge you need to understand modern cyber threats, reduce risk, and help your organization **stay ahead** of an ever-changing adversary.

KNOW THE THREATS. UNDERSTAND THE RISK. TAKE ACTION. STAY AHEAD.

BELSHAW CONSULTING