THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW...

ARTIFICIAL INTELLIGENCE

AI-POWERED DEFENSE. SMARTER DETECTION. STRONGER SECURITY.

HOW AI STRENGTHENS CYBERSECURITY

THREAT DETECTION
AI analyzes vast amounts of data in real time to identify threats faster and with greater accuracy.

BEHAVIOR ANALYSIS
Machine learning models detect anomalies and suspicious behavior across users, systems, and networks.

AUTOMATION & RESPONSE
AI automates incident response and remediation, reducing response time and analyst workload.

PREDICTIVE INTELLIGENCE
AI predicts and prioritizes risks by learning from historical data and emerging threat patterns.

PHISHING & MALWARE PREVENTION
AI detects and blocks malicious emails, links, and unknown malware before damage occurs.

DATA PROTECTION
AI helps classify sensitive data, detect exfiltration risks, and enforce access controls automatically.

WHERE AI MAKES AN IMPACT

- ✓ Security Operations Centers (SOC)
- ✓ Endpoint Detection & Response (EDR)
- ✓ Network Monitoring & IDS/IPS
- ✓ Vulnerability Management
- ✓ User & Entity Behavior Analytics (UEBA)
- ✓ Cloud Security & DevSecOps
- ✓ Fraud Detection & Risk Scoring

KEY AI TECHNOLOGIES

MACHINE LEARNING (ML)
Finds patterns and detects anomalies

NATURAL LANGUAGE PROCESSING (NLP)
Analyzes text, alerts, and threat intel

DEEP LEARNING (DL)
Detects complex threats with neural networks

GENERATIVE AI (GENAI)
Enhances threat hunting, reporting, and analyst productivity

BEST PRACTICES FOR USING AI IN CYBERSECURITY

START WITH CLEAR GOALS
Define the problem you want AI to solve and the outcomes you expect.

USE QUALITY DATA
AI is only as good as the data it learns from.

HUMAN + AI TOGETHER
Combine AI speed with human expertise and context.

VALIDATE & TUNE CONTINUOUSLY
Continuously test models to reduce false positives and improve accuracy.

ENSURE ETHICAL & SECURE USE
Address bias, ensure privacy, and protect AI systems from adversarial attacks.

MEASURE & IMPROVE
Track performance, learn from results, and adapt to new threats.

THE FUTURE IS INTELLIGENT SECURITY

“AI won’t replace cybersecurity experts. But experts who use AI will lead the future of cybersecurity.”

LEARN > ADAPT > AUTOMATE > PROTECT

BELSHAW CONSULTING

Just Tell Me What I Need To Know

Artificial Intelligence

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

Table of Contents

Introduction

Artificial Intelligence is no longer a technology of the future—it's a technology of the present.

From search engines and recommendation systems to cybersecurity, healthcare, software development, and business analytics, AI is transforming how organizations operate and how professionals perform their jobs. It is changing the way we write software, analyze data, detect cyber threats, make decisions, create content, and solve complex problems. Whether you realize it or not, you're already interacting with artificial intelligence every day.

The challenge is that AI is evolving at an extraordinary pace. New models, tools, platforms, and capabilities appear almost daily, making it difficult to separate meaningful advances from marketing hype. Many resources either oversimplify AI or dive so deeply into mathematics and programming that they become inaccessible to the average professional.

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 professionals actually need. Rather than overwhelming you with algorithms, complex mathematics, or vendor-specific implementations, each book delivers practical, real-world concepts in a clear, concise, and easy-to-understand format.

This book focuses on Artificial Intelligence—what it is, how it works at a conceptual level, and how it is being applied across business, engineering, cybersecurity, healthcare, education, government, and countless other industries. You'll learn about generative AI, large language models, prompt engineering, retrieval-augmented generation (RAG), AI agents, enterprise AI, governance, ethics, security, and the practical skills needed to use AI effectively and responsibly.

Unlike the companion book Machine Learning, which explores how AI systems are trained and built, this book focuses on how professionals can understand, evaluate, and apply AI to solve real-world problems. The goal is not to make you an AI researcher—it is to help you become an AI-enabled professional who knows when and how to use these technologies effectively.

Whether you're an engineer, architect, cybersecurity professional, project manager, executive, educator, student, or simply someone who wants to understand the technology reshaping our world, this book provides the practical foundation you need to work confidently with artificial intelligence.

This book should answer the questions:

"How do I understand, govern, and effectively use Artificial Intelligence in the enterprise?"

And

"What does every technology and cybersecurity professional need to know about Artificial Intelligence?"

Our goal is simple:

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

So, let's get started.

ARTIFICIAL INTELLIGENCE IS CHANGING EVERY PROFESSION—AND THE PEOPLE WHO UNDERSTAND IT WILL HELP SHAPE THE FUTURE.

Whether you're using AI to write code, improve cybersecurity, analyze data, automate business processes, create content, or make better decisions, understanding the technology behind today's AI revolution has become an essential professional skill.

Just Tell Me What I Need to Know... Artificial Intelligence provides a practical, vendor-neutral guide to understanding and applying AI in the real world. Instead of focusing on complex mathematics or programming, this book explains the concepts, technologies, and best practices that professionals need to confidently evaluate and use modern AI systems.

INSIDE YOU'LL LEARN ABOUT:

- Artificial Intelligence fundamentals
- Generative AI and Large Language Models (LLMs)
- Prompt engineering and AI-assisted productivity
- Retrieval-Augmented Generation (RAG)
- AI agents and intelligent automation
- Enterprise AI strategy and governance
- AI security, privacy, and ethics
- Responsible AI and regulatory considerations
- Practical AI applications across industries
- Preparing for the future of AI

CLEAR EXPLANATIONS.
No jargon. No fluff.

REAL-WORLD APPLICATIONS.
Practical examples. Proven use cases.

ACTIONABLE INSIGHTS.
Make better decisions with confidence.

Whether you're an engineer, architect, cybersecurity professional, manager, executive, educator, student, or business leader, this book provides the practical knowledge needed to understand AI, evaluate its capabilities, and use it responsibly to solve real-world problems.

HOW AI HELPS YOU

ENHANCE SECURITY
Detect threats, analyze behavior, respond faster.

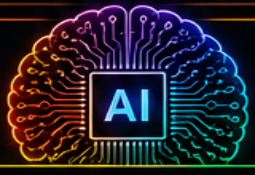
DRIVE EFFICIENCY
Automate tasks, reduce costs, improve outcomes.

GAIN INSIGHT
Analyze data, find patterns, uncover opportunities.

BOOST CREATIVITY
Generate ideas, content, and better solutions.

EMPOWER PEOPLE
Augment skills, expand capabilities, increase impact.

BUILD THE FUTURE
Innovate responsibly, stay competitive, lead the change.



LESS HYPE.
MORE PRACTICAL KNOWLEDGE.
JUST TELL ME WHAT I NEED TO KNOW.

BELSHAW CONSULTING