Microsoft Sentinel In Action: A Cybersecurity Masterclass for the Modern Threat Landscape

In today's rapidly evolving digital world, organizations face an unprecedented barrage of cyber threats. To effectively combat these threats, it is imperative to embrace advanced cybersecurity solutions that provide comprehensive protection, real-time visibility, and actionable insights.

Microsoft Sentinel in Action: Architect, design, implement, and operate Microsoft Sentinel as the core of your security solutions, 2nd Edition by Richard Diver

4.8 out of 5

Language	: English
File size	: 63777 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 478 pages

Microsoft Sentinel, a cloud-native security information and event management (SIEM) platform, has emerged as a game-changer in the cybersecurity arena. Through its powerful capabilities, Sentinel empowers security teams to monitor, detect, investigate, and respond to threats in real-time, ensuring the safety of their networks and data.

Microsoft Sentinel In Action is an indispensable guide for cybersecurity professionals seeking to harness the full potential of this transformative

platform. This comprehensive book provides practical insights, step-by-step instructions, and real-world examples that will equip you with the knowledge and skills to:

- Configure and customize Microsoft Sentinel to meet your organization's specific needs
- Ingest and analyze security data from a wide range of sources
- Create and manage custom threat intelligence to identify potential risks
- Detect and investigate security incidents using advanced analytics and machine learning
- Automate response actions to mitigate threats and minimize their impact

Why Microsoft Sentinel?

Microsoft Sentinel stands out as the preferred SIEM solution for organizations of all sizes due to its numerous advantages:

- **Cloud-native architecture:** Sentinel is built on Microsoft Azure, providing scalability, reliability, and global availability.
- **Comprehensive threat intelligence:** Sentinel integrates with Microsoft Threat Intelligence, offering real-time access to the latest threat information.
- **Advanced analytics and machine learning:** Sentinel uses machine learning algorithms to detect and prioritize threats, reducing the risk of false positives.
- **Seamless integration with Microsoft ecosystem:** Sentinel seamlessly integrates with other Microsoft security products, such as

Azure Active Directory, Azure Security Center, and Microsoft 365 Defender.

- **Cost-effective pricing:** Sentinel offers flexible pricing models that scale with your organization's needs.

Book Contents

Microsoft Sentinel In Action is structured into three parts:

1. **Getting Started:** This part introduces Microsoft Sentinel, its architecture, and key components. It provides step-by-step guidance on installation, configuration, and data ingestion.
2. **Threat Hunting and Detection:** This part delves into the advanced threat hunting and detection capabilities of Sentinel. Readers will learn how to create custom threat intelligence feeds, develop analytics rules, and use machine learning for threat detection.
3. **Incident Response and Automation:** This part focuses on the incident response process, including triage, investigation, and remediation. Readers will learn how to automate response actions, integrate with external systems, and streamline threat mitigation.

Who Should Read This Book?

Microsoft Sentinel In Action is written for cybersecurity professionals of all skill levels who are tasked with the responsibility of protecting their organizations from cyber threats. This book is particularly valuable for:

- Security analysts and incident responders
- IT administrators responsible for security operations
- Cloud engineers looking to enhance security posture

- Cybersecurity students and researchers

Benefits of Reading This Book

By reading Microsoft Sentinel In Action, you will gain the following benefits:

- A comprehensive understanding of Microsoft Sentinel's architecture, capabilities, and use cases
- Proven strategies and techniques for configuring and customizing Sentinel
- Hands-on experience in setting up threat intelligence, analytics, and automation
- In-depth knowledge of threat hunting, detection, and investigation techniques
- Proven methods for incident response and threat mitigation

About the Authors

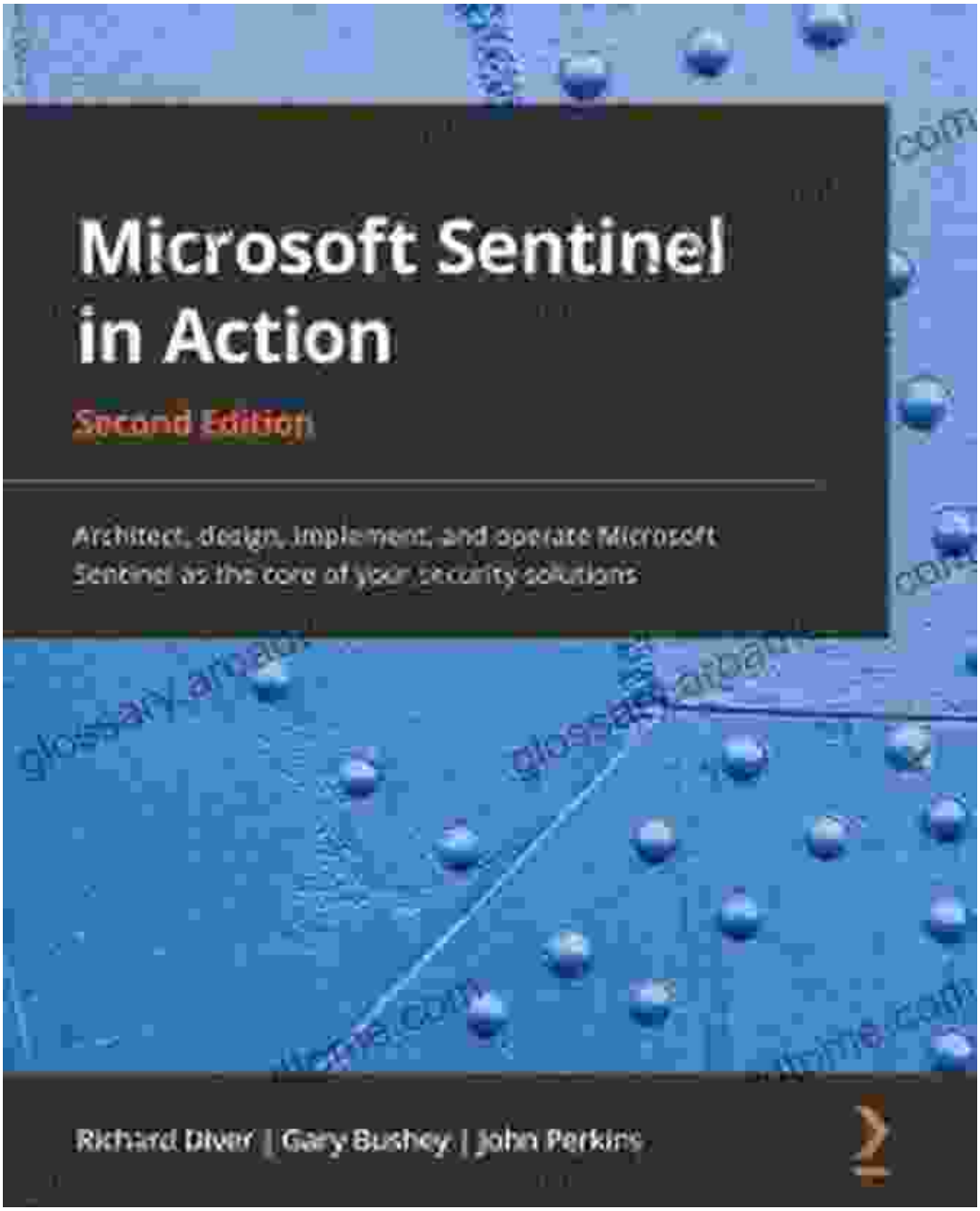
Microsoft Sentinel In Action is authored by a team of experienced cybersecurity experts:

- **Jason Shirk:** A Microsoft Cloud Security MVP and Security Analyst at Medtronic.
- **Brandon Weisman:** A Senior Security Analyst at Aegis Digital.
- **Steven Meighen:** A Security Evangelist at Microsoft.

Microsoft Sentinel In Action is an essential resource for cybersecurity professionals who seek to elevate their organization's protection against cyber threats. This comprehensive guide provides practical insights and

step-by-step instructions that will empower you to harness the full potential of Microsoft Sentinel and safeguard your organization from harm.

Free Download your copy of Microsoft Sentinel In Action today and begin your journey towards creating a more secure and resilient cyber defense.

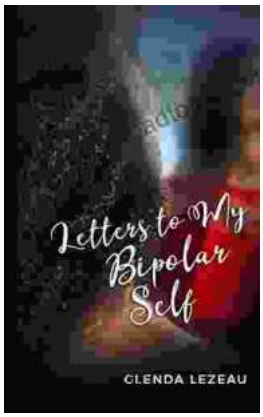


Microsoft Sentinel in Action: Architect, design, implement, and operate Microsoft Sentinel as the core

of your security solutions, 2nd Edition by Richard Diver

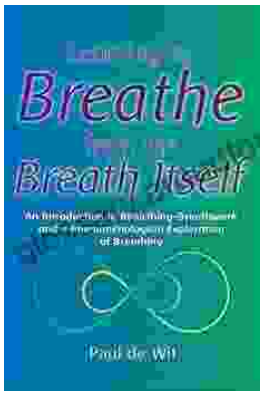
4.8 out of 5

Language	: English
File size	: 63777 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 478 pages



Letters to My Bipolar Self: A Journey of Hope, Healing, and Acceptance

Bipolar disFree Download is a serious mental illness that can cause extreme mood swings, from mania to depression. It can be a devastating...



Learning to Breathe from the Breath Itself: A Transformative Guide to Mindfulness and Well-being

In the whirlwind of modern life, finding moments of peace and tranquility can seem like a distant dream. However, within the depths of our own being lies a tool that holds...