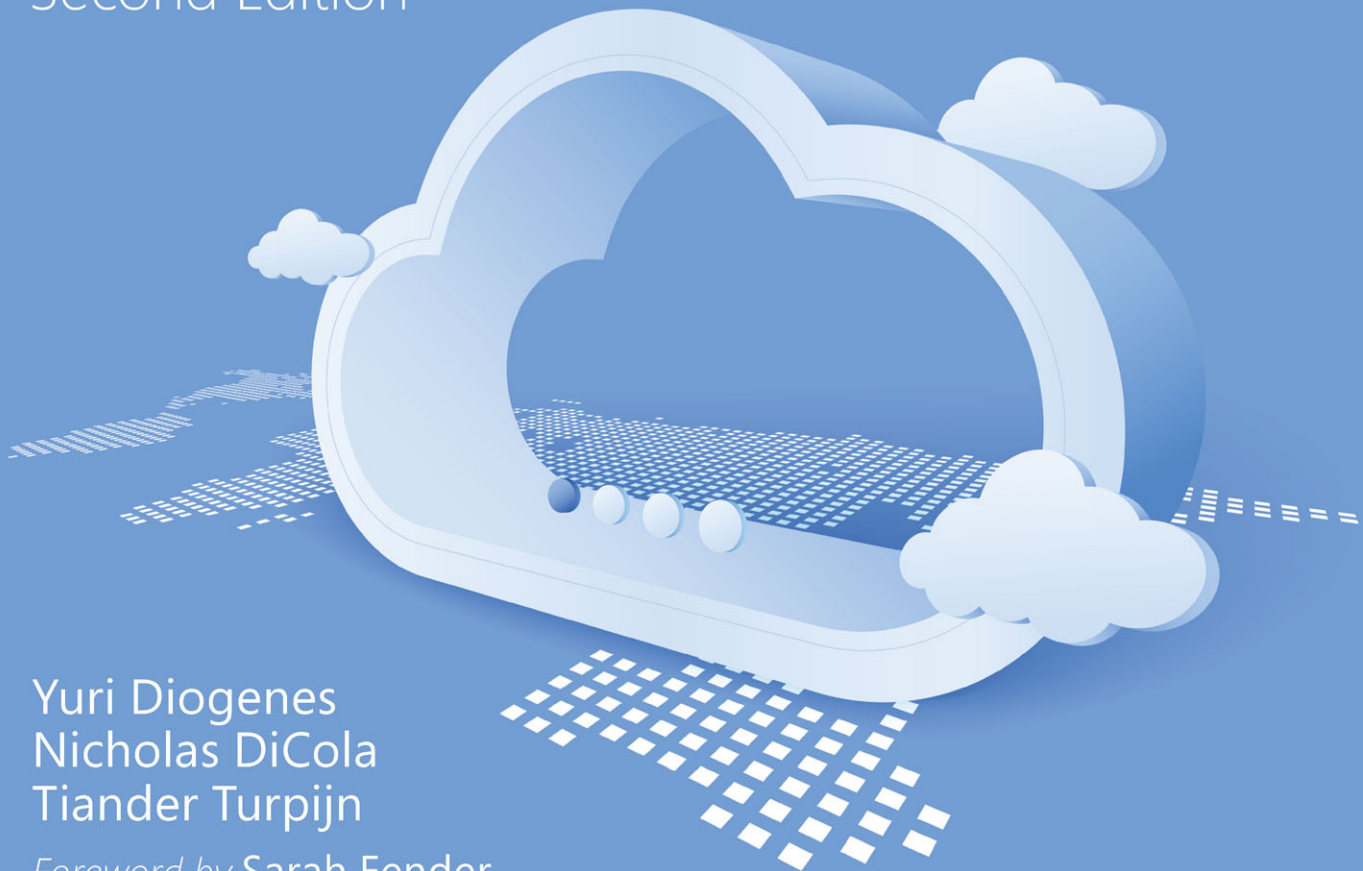


Microsoft Sentinel

Planning and implementing Microsoft's cloud-native SIEM solution

Second Edition



Yuri Diogenes
Nicholas DiCola
Tiander Turpijn

Foreword by Sarah Fender

Partner Director of Product Management – Microsoft Sentinel

Microsoft Sentinel

Planning and implementing
Microsoft's cloud-native SIEM solution
Second Edition

Yuri Diogenes
Nicholas DiCola
Tiander Turpijn

Microsoft Sentinel: Planning and implementing Microsoft's cloud-native SIEM solution

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Contents

Foreword

Acknowledgments

About the authors

Introduction

Chapter 1 Security challenges for SecOps

- Current threat landscape

 - The history of a supply-chain attack

- Security Challenges for SecOps

 - Resource challenges

 - Finding the proverbial needle in the haystack

- Threat intelligence

- Introducing Microsoft Sentinel

 - Core capabilities

Chapter 2 Introduction to Microsoft Sentinel

- Architecture

Table of Contents

- Roles and permissions

- Workspace design considerations

- Hardening considerations

- Additional considerations

- Enabling Microsoft Sentinel

- Ingesting data from Microsoft solutions

 - Connecting Microsoft Defender for Cloud

 - Connecting to Azure Active Directory

- Accessing ingested data

Chapter 3 Analytics

- Why use analytics for security?

- Understanding analytic rules

 - Configuring analytic rules

 - Types of analytic rules

- Creating analytic rules

- Validating analytic rules

Chapter 4 Incident management

- Understanding Microsoft Sentinel incidents

- Exploring and configuring the Incidents view

- Guides and feedback

- Triaging incidents

- Searching for specific incidents

- Incident details

- Teams integration

- Graphical investigation

Chapter 5 Hunting

- Understanding threat hunting

Table of Contents

Knowing your environment and data

Threat hunting in Microsoft Sentinel

Running your first hunting query

Hunting hypothesis example

Livestream

Using Livestream with Azure Key Vault honeytokens

Understanding cyberthreat intelligence

Threat intelligence in Microsoft Sentinel

Configuring the TAIL data connector

Enabling the threat intelligence rules

Creating a custom threat indicator

Interactive TI and hunting dashboards

Chapter 6 Notebooks

Understanding Microsoft Sentinel Notebooks

Configuring an AML workspace and compute

Configuration steps to interact with your Microsoft Sentinel workspace

The MSTICpy library

Hunting and enrichment examples

Sign-ins that did not pass the MFA challenge

Creating interactive cells

Chapter 7 Automating response

The importance of SOAR

Understanding automation rules

Creating an automation rule

Advanced automation with Playbooks

Post-incident automation

Chapter 8 Data visualization

Table of Contents

Microsoft Sentinel Workbooks

Creating custom Workbooks

Creating visualizations in Power BI and Excel

Creating visualizations in Power BI

Exporting data to Microsoft Excel

Chapter 9 Data connectors

Understanding data connectors

Ingestion methods

The Codeless Connector Platform

Preparing for a new data connector

Enabling and configuring a data connector

The Microsoft 365 Defender connector

Understanding the Amazon Web Services S3 connector

The AWS S3 configuration process

Data connector health monitoring

The Microsoft SentinelHealth table

The Content Hub

Appendix A: Introduction to Kusto Query Language

The KQL query structure

Data types

Getting, limiting, sorting, and filtering data

Summarizing data

Adding and removing columns

Joining tables

Evaluate

Let statements

Suggested learning resources

Table of Contents

Appendix B: Microsoft Sentinel for managed security service providers

Accessing the customer environment

- Azure Lighthouse

- Azure Active Directory B2B

Cross-workspace features

- KQL Queries

- Analytics rules

- Hunting

- Incident management

- Automation/SOAR

- Workbooks

Security content management

- How to adopt CI/CD?

- Microsoft Sentinel repositories

Index