Integration and Automation

Muhammad Sajid
CLOUD ARCHITECT

@sajid_nazeer www.msajid.cloud

Overview

What is SOAR?

Azure Logic Apps Refresher

Automation Playbooks in Azure Sentinel

- Real-time Automation
- On-demand Automation

Azure Sentinel APIs

- Management API
- Http Data Collector API

Further learning

What Is SOAR?

Security Orchestration, Automation and Response (SOAR)

A solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance.

Orchestration, Automation, Response

Each component performs a different SOC function

Orchestration

Integrates different technologies and connects between security tools

Automation

Provides automated detection and response

Response

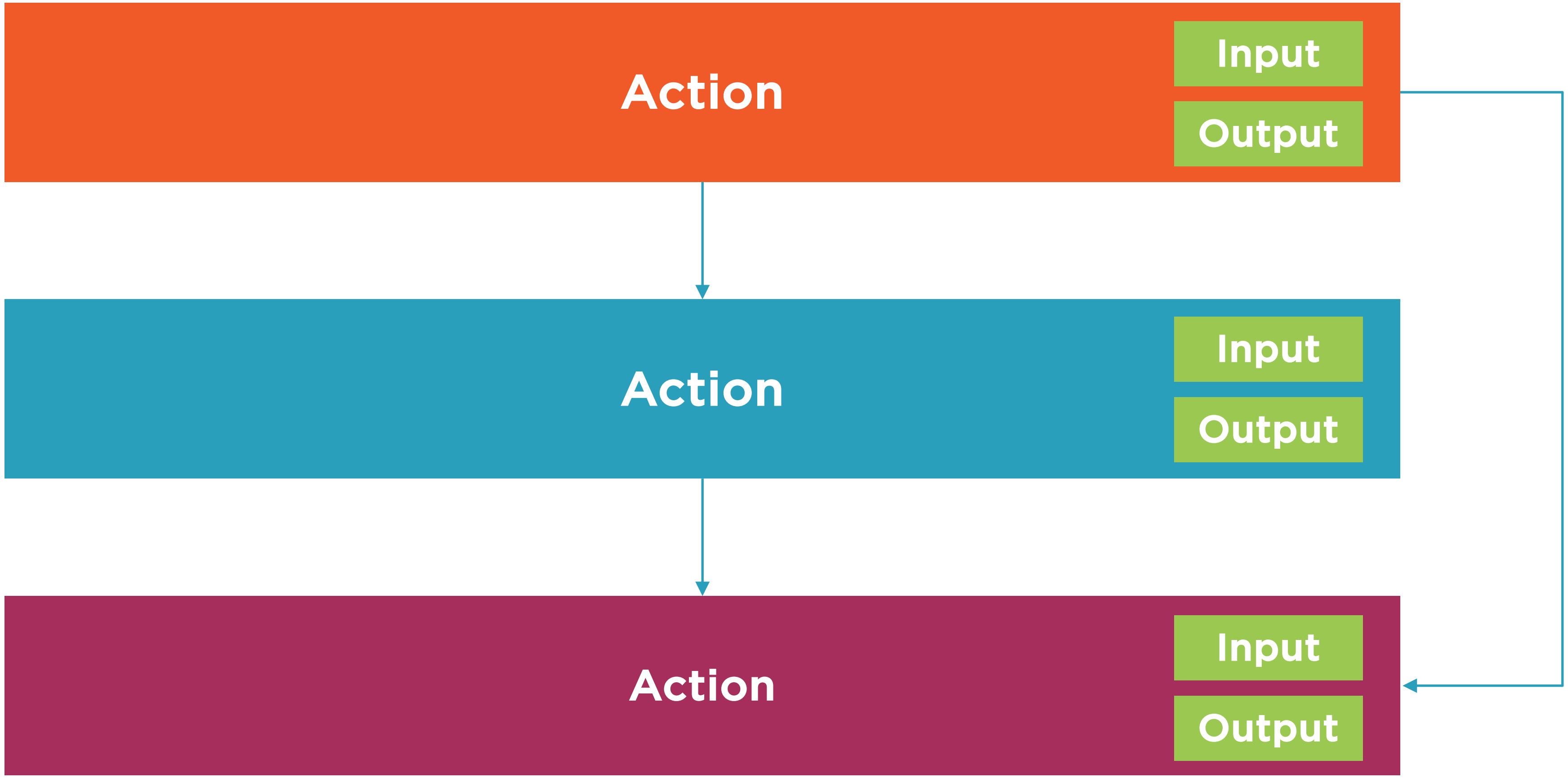
Security teams can use playbooks to run automated workflows

Azure Logic Apps Refresher

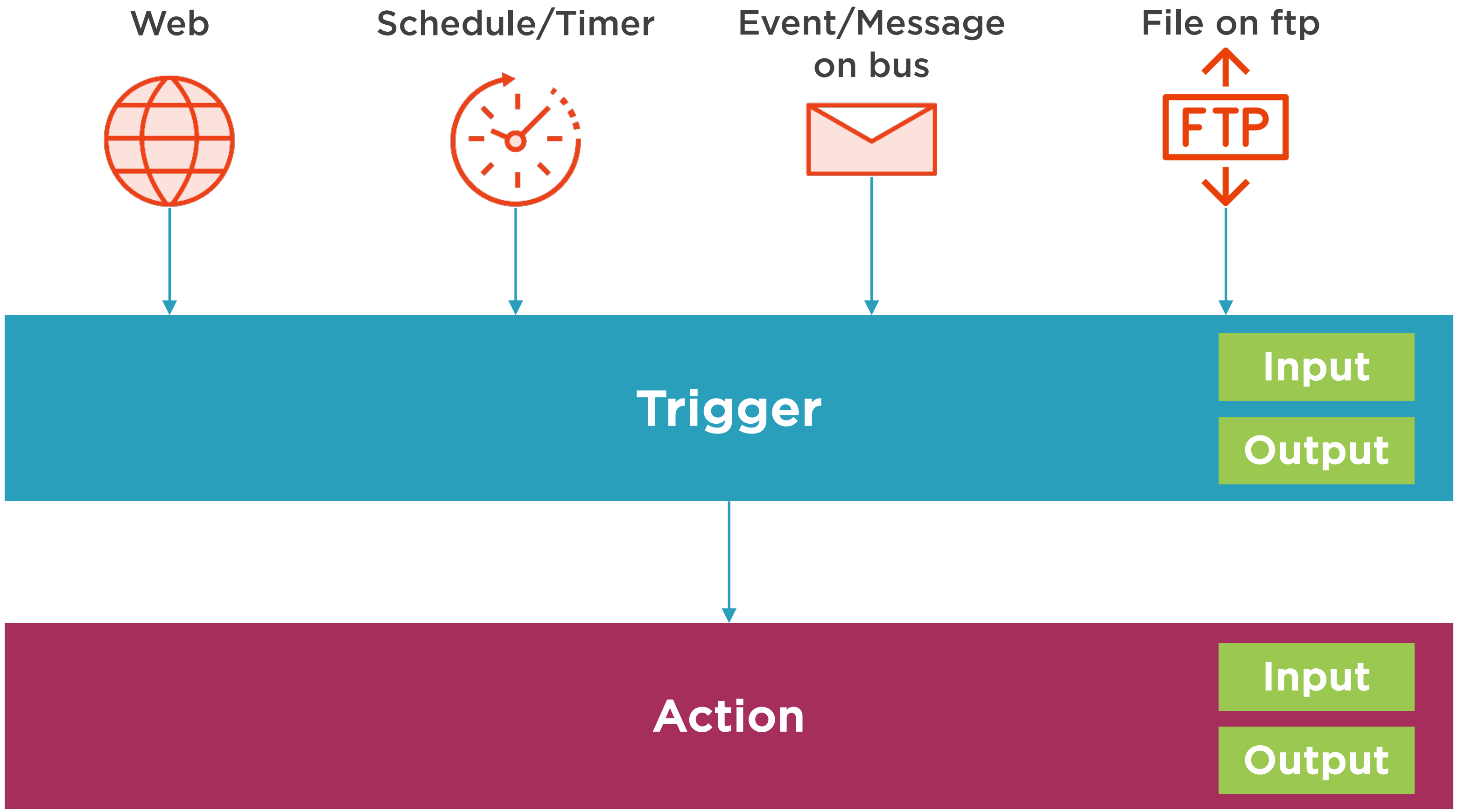
What Is a Logic App?

Azure Logic Apps is a cloud service that helps you schedule, automate, and orchestrate tasks, business processes, and workflows.

How a Logic App Works?



How a Logic App Works?



Demo

Creating Logic Apps

- A basic addition app

Automation Playbooks in Azure Sentinel

What Is a Security Playbook in Azure Sentinel?

A security playbook is a collection of procedures that can be run from Azure Sentinel in response to an alert.

Two Ways to Leverage Logic Apps

Real-time Automation

Calls the Playbook automatically when the incident is created

On-demand from the Incident

Manually call a Playbook from the incident on-demand

Demo

Using Security Playbooks in Azure Sentinel

- Real-time Automation
  - Simulate a break glass account usage alert

Demo

Using Security Playbooks in Azure Sentinel

- On-demand Automation
  - Enrich break glass account usage incident with IP location information

Azure Sentinel APIs

Overview of Azure Sentinel APIs

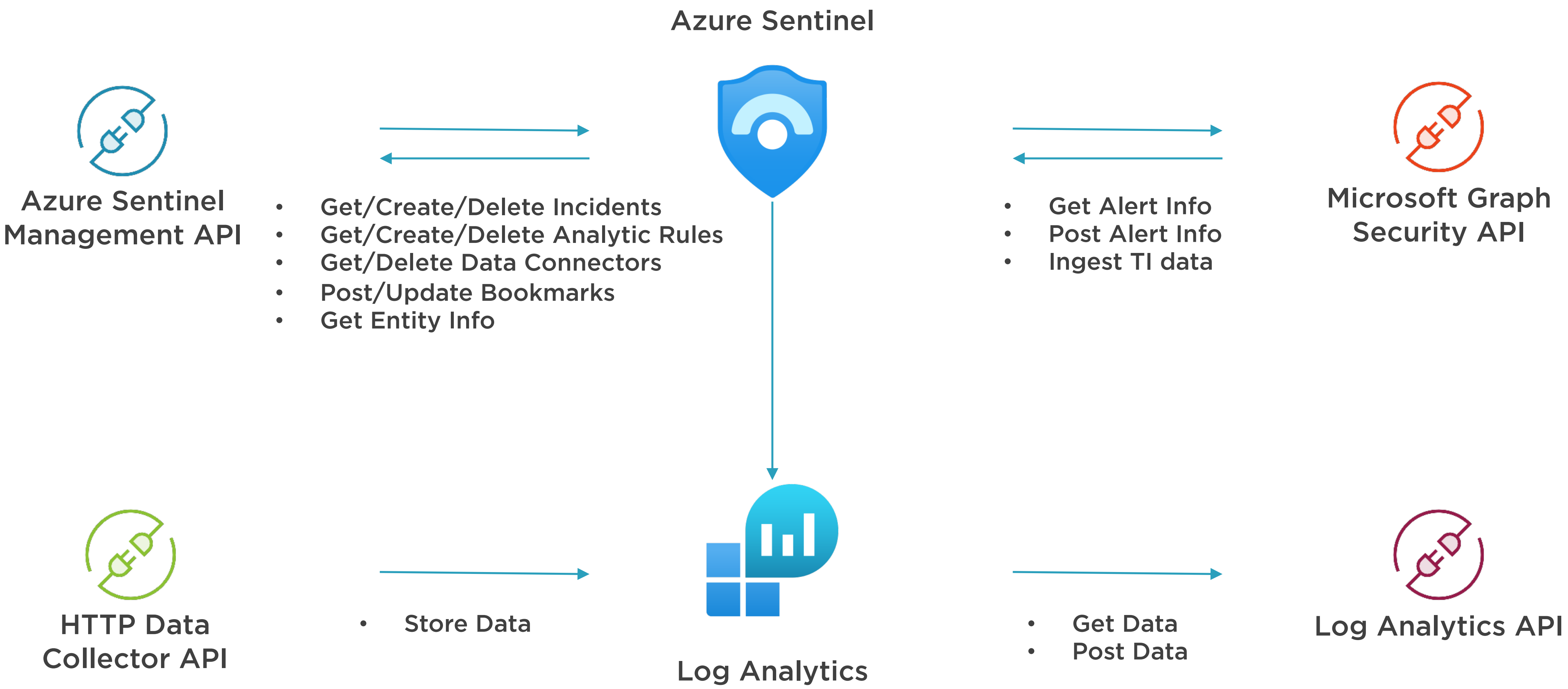
Azure Sentinel Management API

Microsoft Graph Security API

Log Analytics API

HTTP Data Collector API

Overview of Azure Sentinel APIs



Azure Sentinel

Azure Sentinel Management API

- Get/Create/Delete Incidents
- Get/Create/Delete Analytic Rules
- Get/Delete Data Connectors
- Post/Update Bookmarks
- Get Entity Info

Microsoft Graph Security API

- Get Alert Info
- Post Alert Info
- Ingest TI data

HTTP Data Collector API

- Store Data

Log Analytics

- Get Data
- Post Data

Log Analytics API

Demo

Using Azure Sentinel Management API

- Listing Incidents
- Fetching Incident by Id
- Creating an Incident

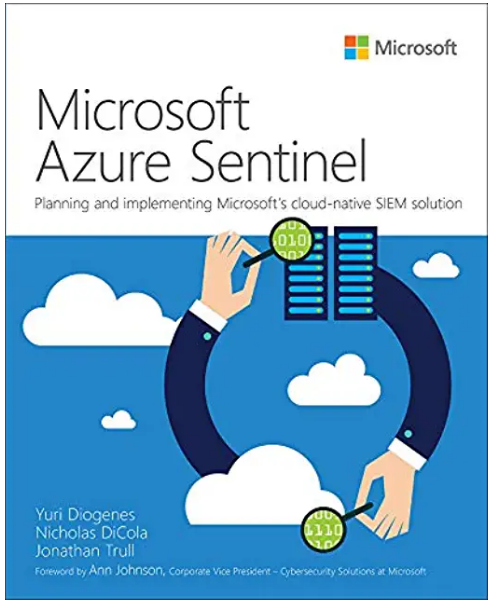
Demo

Using HTTP Data Collector API

- Ingest data into Azure Sentinel

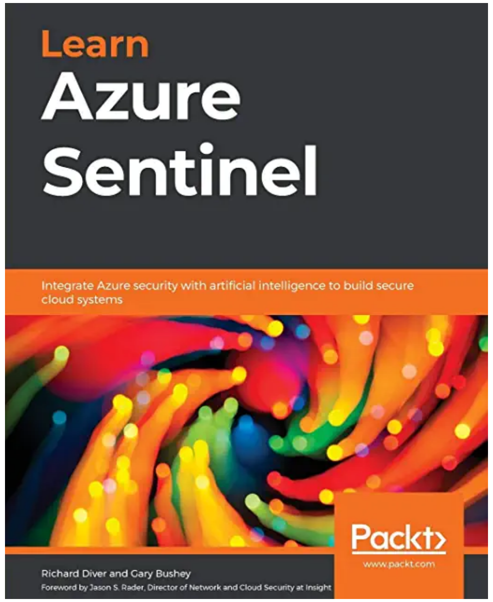
Further Learning

Books


Microsoft
Microsoft Azure Sentinel
Planning and implementing Microsoft's cloud-native SIEM solution
Yuri Diogenes
Nicholas DiCola
Jonathan Trull
Foreword by Ann Johnson, Corporate Vice President – Cybersecurity Solutions at Microsoft

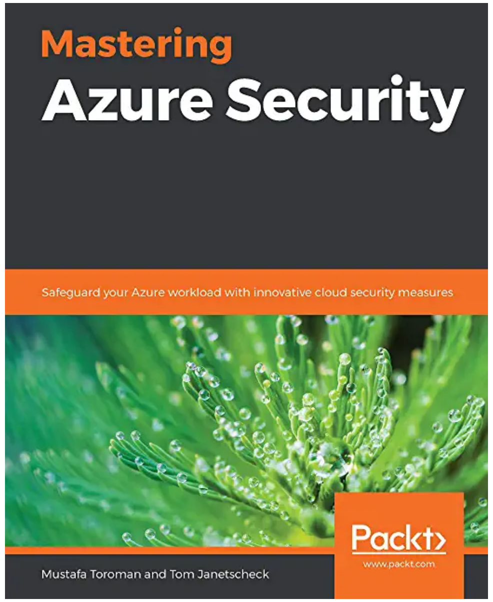
Microsoft Azure Sentinel

http://bit.ly/msazsent


Learn
Azure Sentinel
Integrate Azure security with artificial intelligence to build secure cloud systems
Packt>
www.packt.com
Richard Diver and Gary Bushey
Foreword by Jason S. Rader, Director of Network and Cloud Security at Insight

Learn Azure Sentinel

http://bit.ly/learnazsent


Mastering
Azure Security
Safeguard your Azure workload with innovative cloud security measures
Packt>
www.packt.com
Mustafa Toroman and Tom Janetscheck

Mastering Azure Security

http://bit.ly/masterazse
c

This training program includes 16 modules.

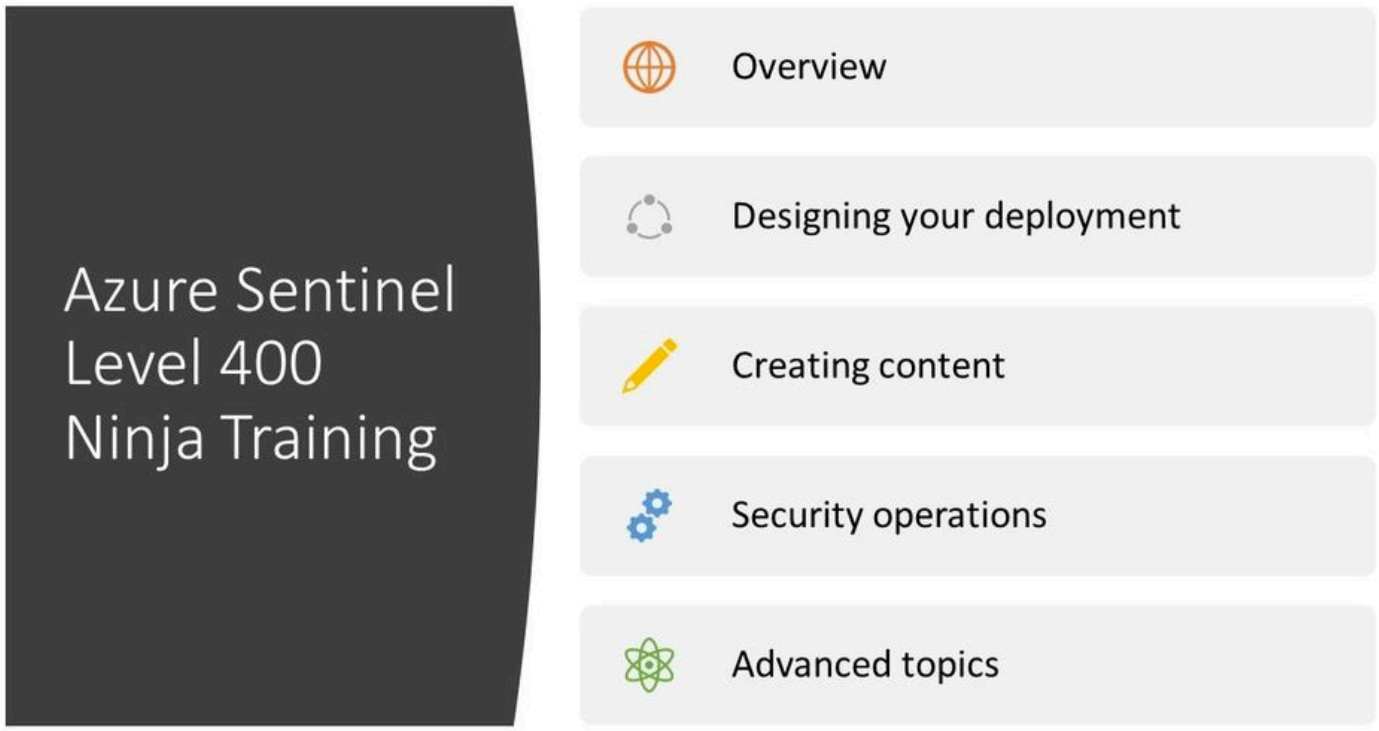
The post includes

Presentation

Recording

Product docs

blog posts

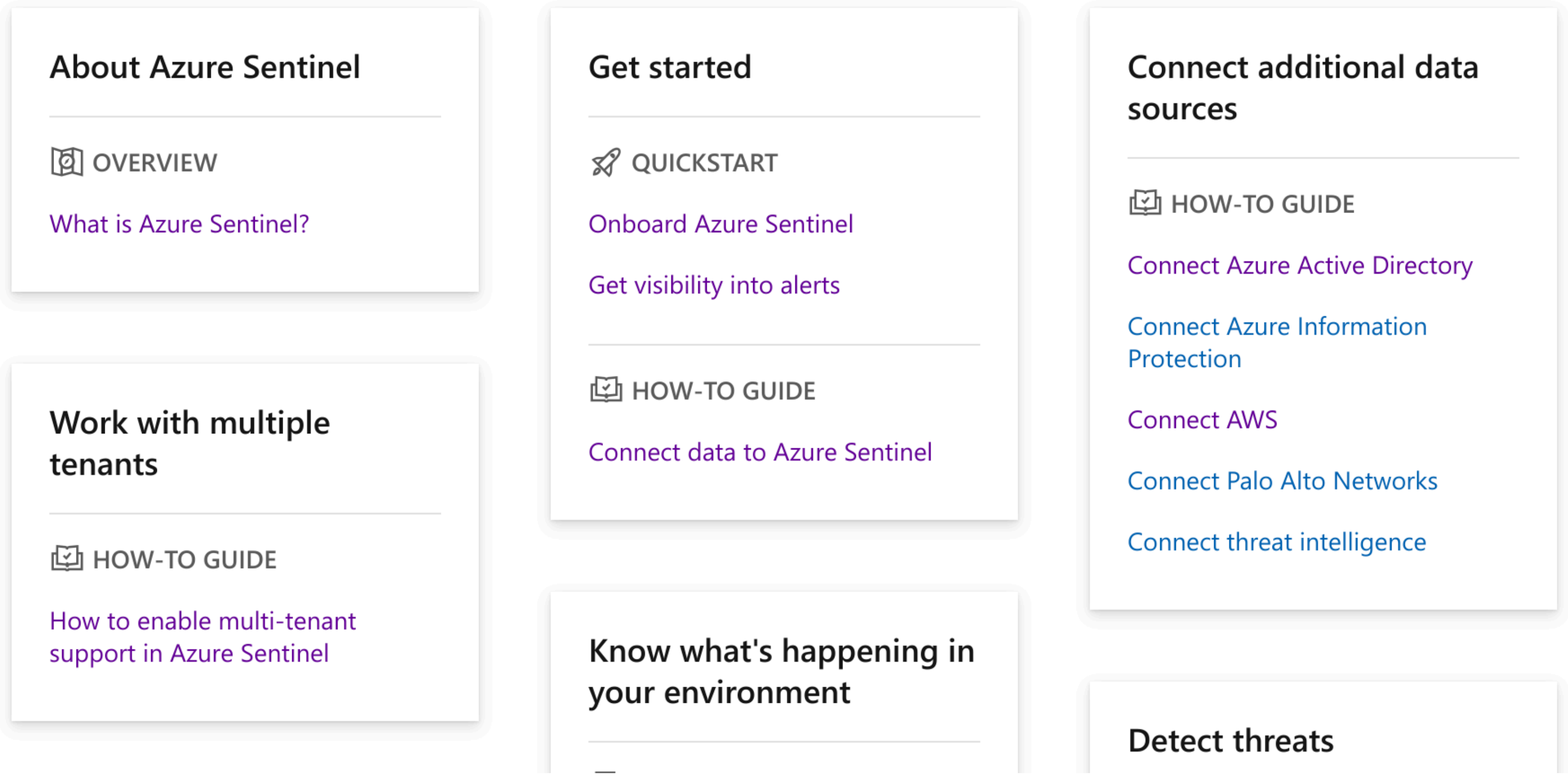


Azure Sentinel Level 400 Ninja Training

- Overview
- Designing your deployment
- Creating content
- Security operations
- Advanced topics

http://bit.ly/azsentninja

Azure Sentinel Documentation



About Azure Sentinel

OVERVIEW

What is Azure Sentinel?

Work with multiple tenants

HOW-TO GUIDE

How to enable multi-tenant support in Azure Sentinel

Get started

QUICKSTART

Onboard Azure Sentinel

Get visibility into alerts

HOW-TO GUIDE

Connect data to Azure Sentinel

Know what's happening in your environment

Connect additional data sources

HOW-TO GUIDE

Connect Azure Active Directory

Connect Azure Information Protection

Connect AWS

Connect Palo Alto Networks

Connect threat intelligence

Detect threats

http://bit.ly/azsentdoc

Module and Course Summary

Summary

Enabling Azure Sentinel

Data Ingestion options

- Connector types

Workbooks

Analytic Rules and Threat Detection

Incident Management, Investigation and Threat Hunting

Integration and Automation options

- Security Playbooks
- Azure Sentinel APIs