Threat Detection Using Analytics

Muhammad Sajid

CLOUD ARCHITECT

@sajid_nazeer   www.msajid.cloud

Overview

KQL Refresher

- Basic commands, functions and operations

Understanding Analytic Rules

- Classification of Analytic Rules

Creating and Validating Analytic Rules

- Types of analytic rules

Detecting Threats

KQL Refresher

Kusto Query Language (KQL)

The Kusto Query Language (KQL) is a plain-text, read-only language that is used to query data consumed by Azure Sentinel.

Services That Make Use of KQL

Azure Data Explorer

Azure Sentinel

Log Analytics

Microsoft Defender ATP

Simple KQL Commands

Count

Where

Take

Sort and Top

Extend

Summarize

Demo

Using KQL in Azure Data Explorer

Understanding Analytic Rules

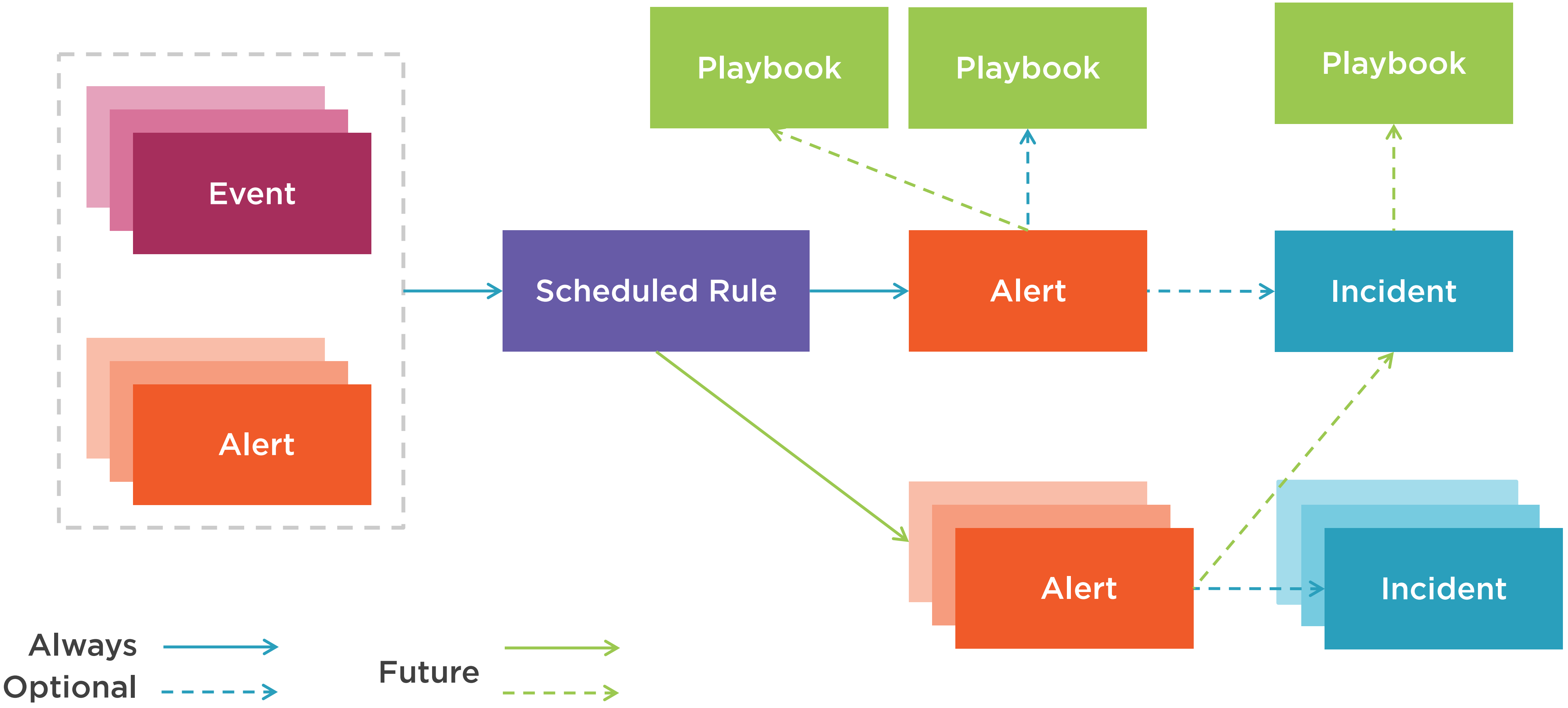
Analytic Rule

The rules users create are called analytic rules

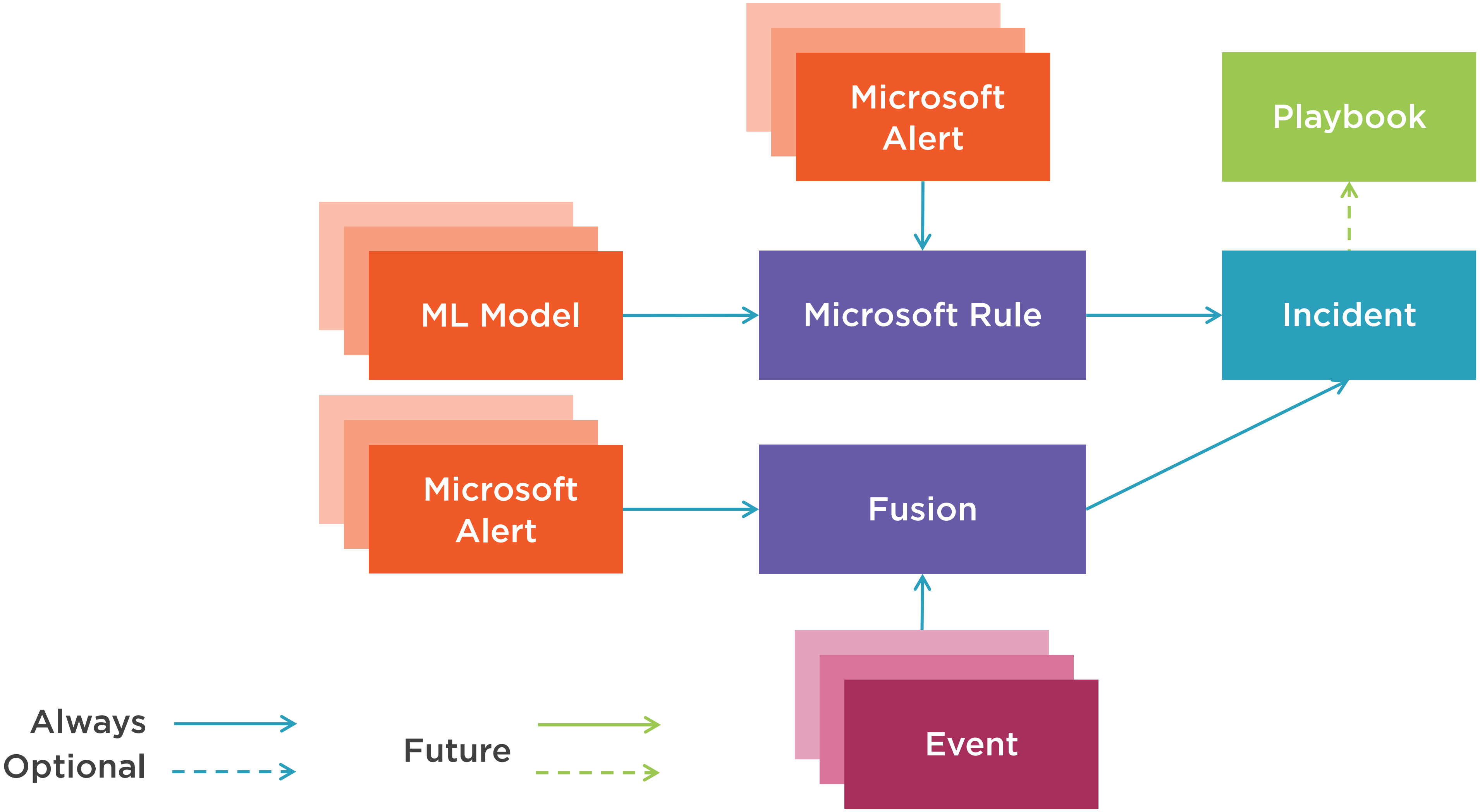
Types of Analytic Rules

- Scheduled
- Microsoft Security
- Machine learning behavioral analytics
- Fusion

Scheduled Alerts



Fusion and Microsoft Rule



Creating Incidents from Microsoft Security Alerts

Demo

Creating Incidents from Microsoft Security Alerts

Creating Scheduled Rules and Detecting Threats

Demo

Create Scheduled Rules and Detecting Threats

Summary

Summary

KQL Basics

Understanding, Creating and Validating Analytic Rules

Threat Detection using Analytic Rules

Up Next:
Managing and Investigating Incidents