Managing and Investigating Incidents

Muhammad Sajid
CLOUD ARCHITECT

@sajid_nazeer www.msajid.cloud

Overview

Security Incidents in Azure Sentinel

Managing an Incident

- Incident management lifecycle

Investigating an Incident

- Graphical Investigation

Hunting

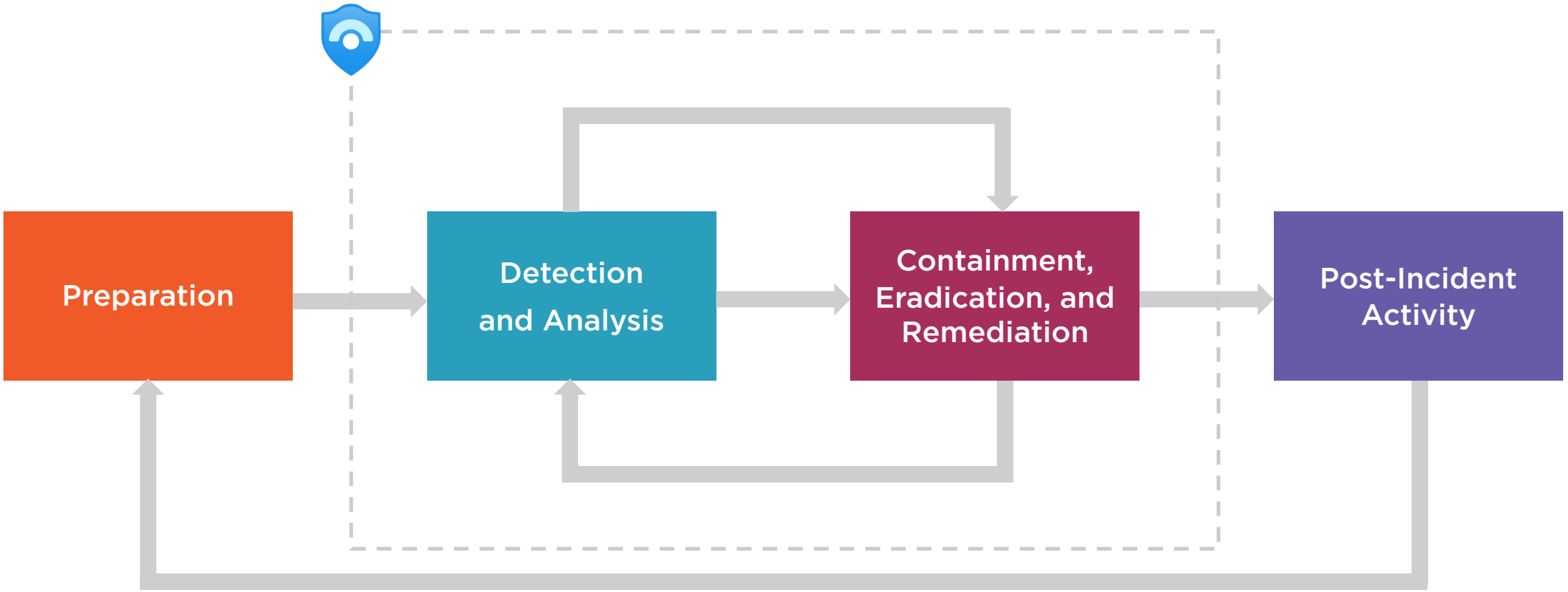
- Queries
- Bookmark Investigation

Managing and Investigating Incidents

Security Incidents in Azure Sentinel

- An incident is created based on alerts
- An incident can be based on first-party analytics from Microsoft Security Solutions
- An incident can also be created via a bookmark
- An incident can include one or multiple alerts
- An incident contains evidence that can be used for further investigation

Incident Management Lifecycle



Demo

Incident management

Investigating incidents

- Graphical Investigation

Threat Hunting and Bookmark Investigation

Threat Hunting

Threat hunting is the process of iteratively searching through a variety of data with the objective to identify threats in the systems.

SOC Using a Three-tiered Approach

Tier 3
Proactive Hunting and Advanced Forensics

Tier 2
Deeper Analysis and Remediation

Tier 1
High Speed Remediation

Automation
Automated Investigation and Remediation

Demo

Hunting queries

Working with Livestream

Working with Bookmarks

- Graphical Investigation
- Creating Incidents from Bookmarks

Summary

Summary

Security Incidents in Azure Sentinel

Managing and Investigating Incidents

Threat Hunting and Bookmark Investigation

Up Next:
Integration and Automation