

Remediate Windows Server Security Issues with Azure Services



Tim Warner

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



Overview



Monitor on-premises servers and Azure IaaS virtual machines (VMs) by using Microsoft Sentinel

Identify and remediate security issues for on-premises servers and Azure IaaS VMs by using Microsoft Defender for Cloud



Windows Server 2022: Secure On-premises and Hybrid Infrastructure

Secure the Windows Server Operating System

Secure Hybrid Active Directory Accounts

Configure Hybrid Active Directory Account Security

Remediate Windows Server Security Issues with Azure Services

Secure Windows Server Networking

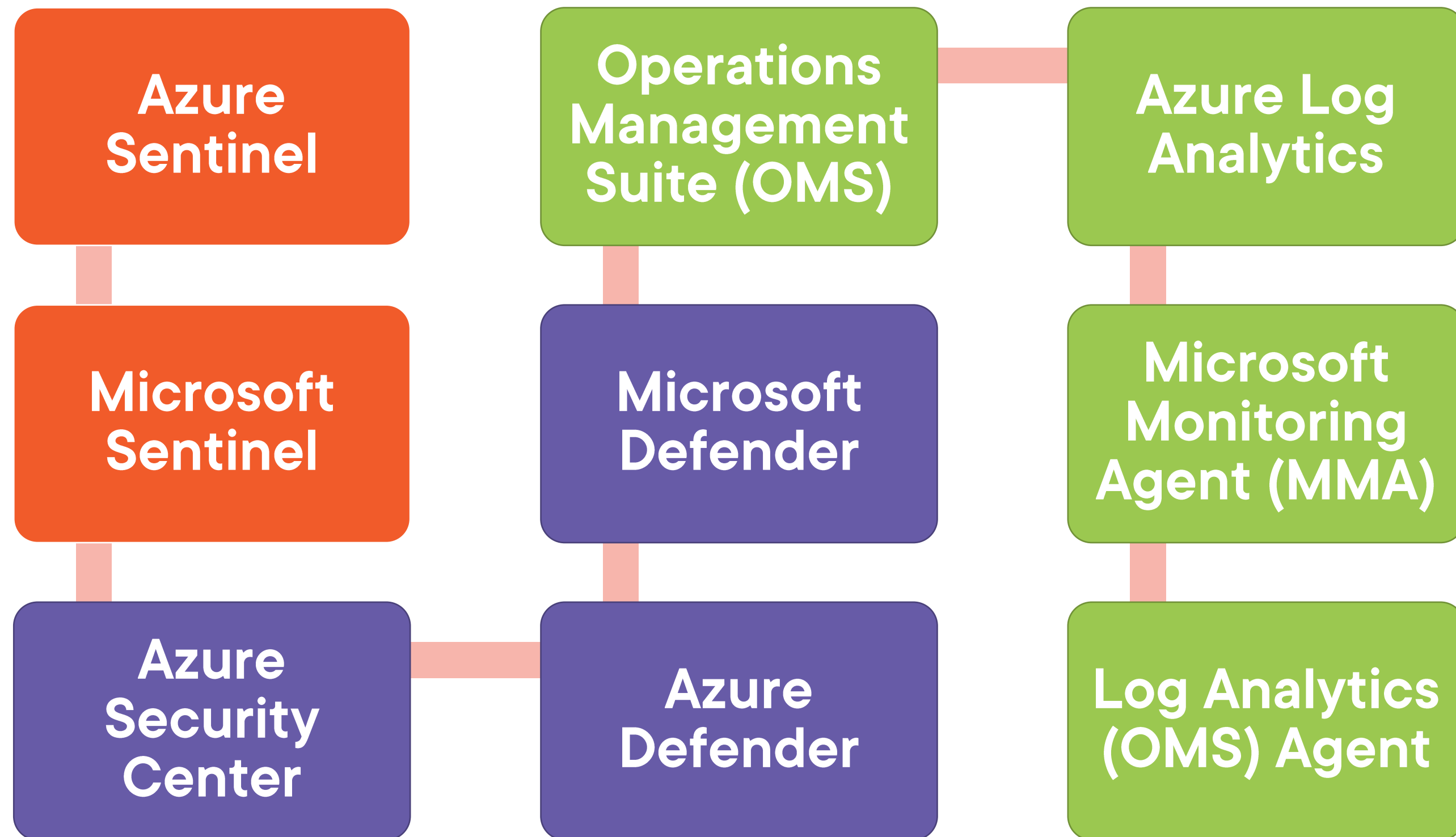
Secure Windows Server Storage



Microsoft Sentinel



A Word About Azure Product Naming



SIEM/SOAR

Security Information and Event Management / Security Orchestration, Automation, and Response. Examples: Splunk Enterprise Security; SolarWinds Security Event Manager; OSSEC



Microsoft Sentinel

Formerly called Azure Sentinel

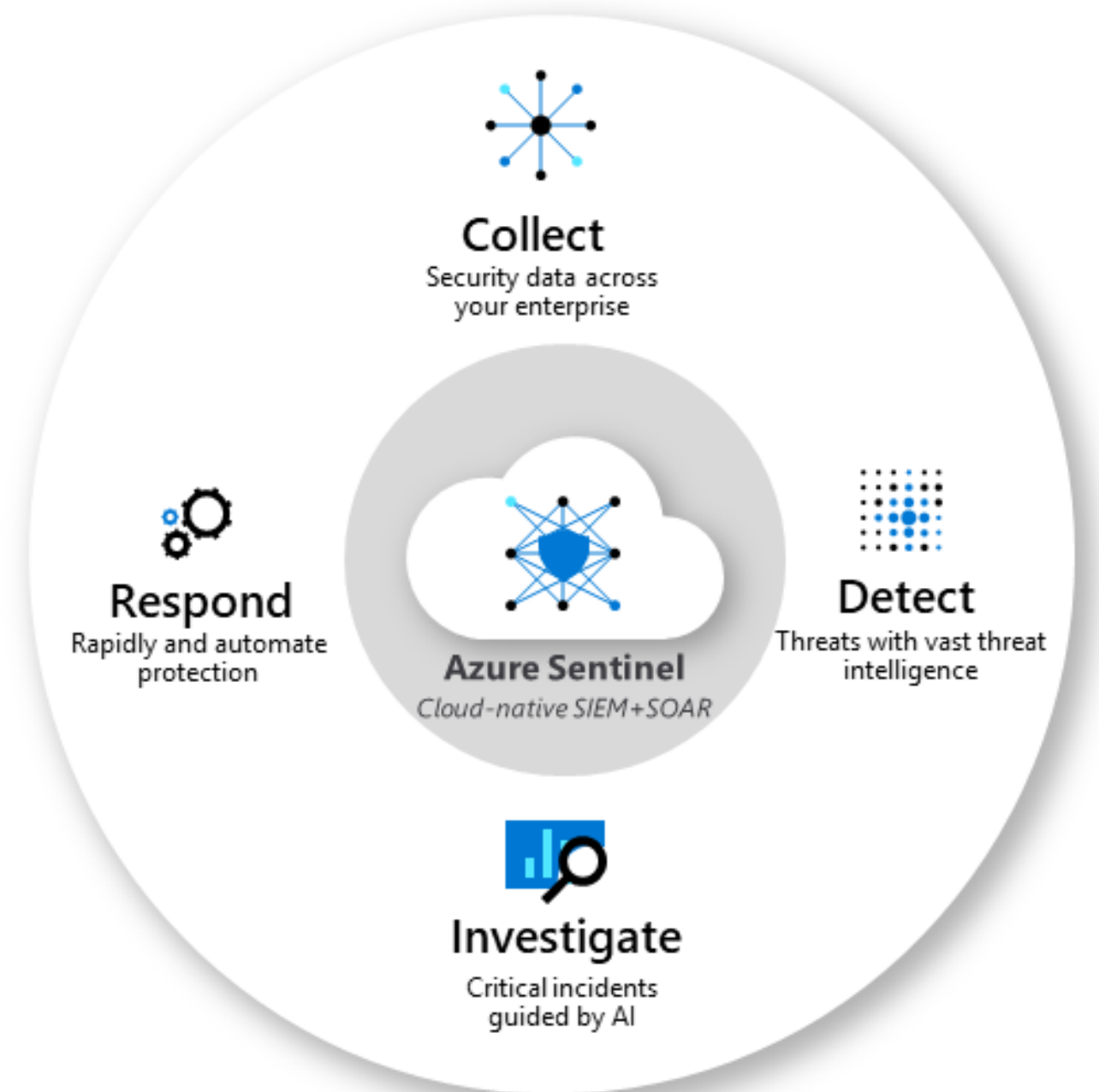
Cloud-native, autoscaling SIEM/SOAR solution

Supports cloud-native, hybrid cloud, and multi-cloud scenarios

Intended for dedicated infosec staff

Extensible connector model

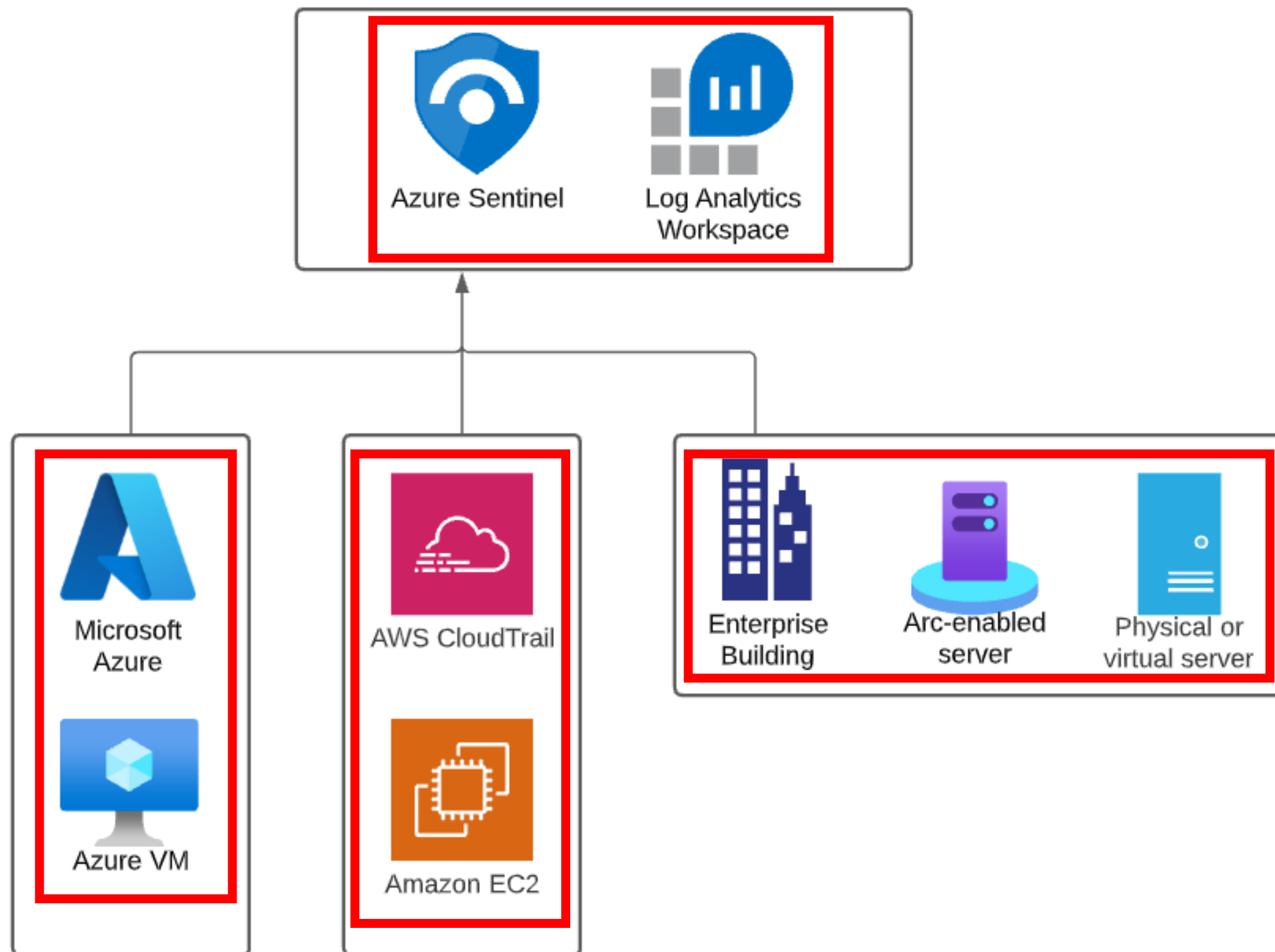
Integration with Azure Monitor and Azure Logic Apps (playbooks)



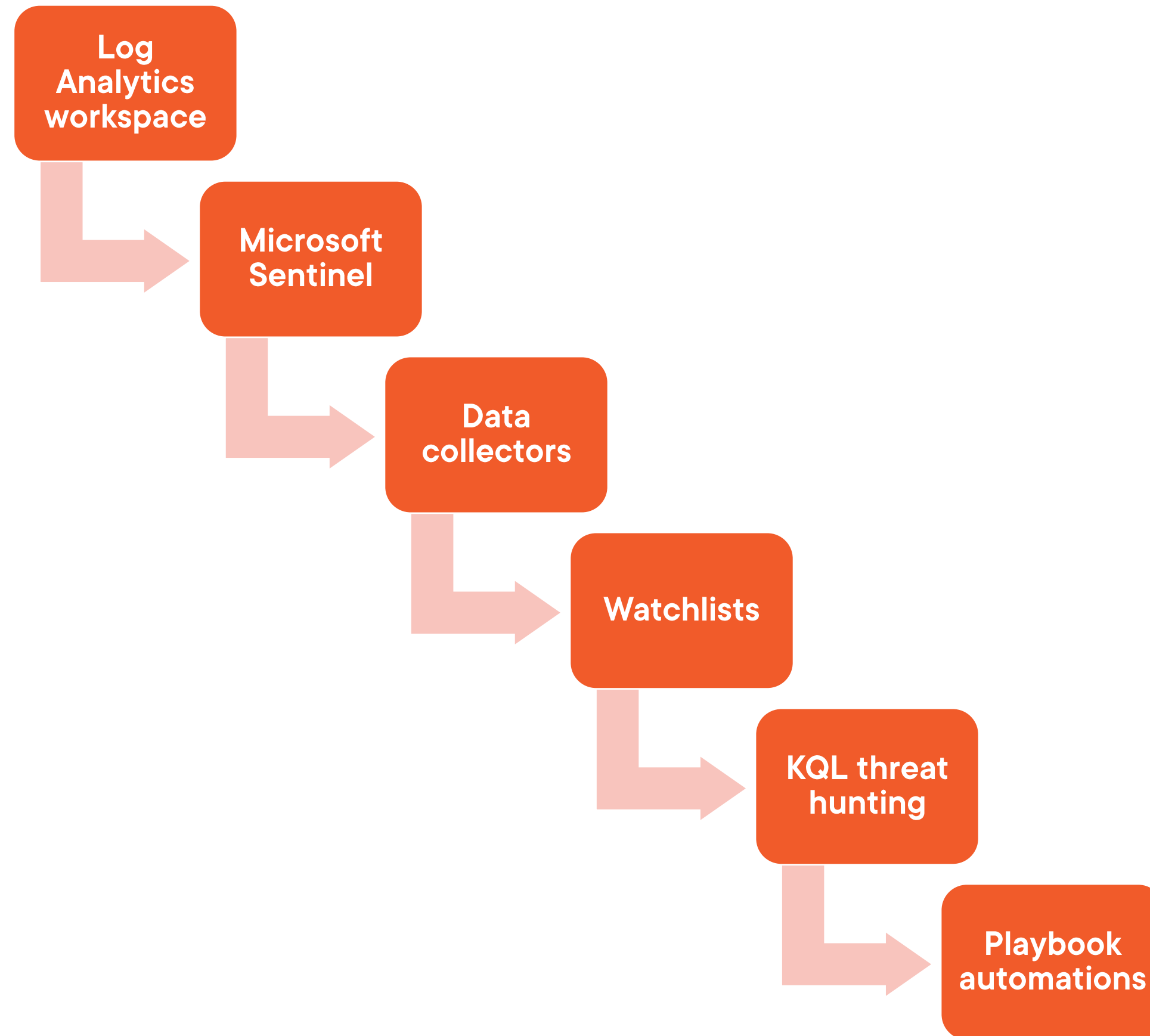
timw.info/v2e



Microsoft Sentinel



Microsoft Sentinel Setup Workflow



Microsoft Defender for Cloud



Microsoft Defender for Cloud



**Hybrid cloud/multi-cloud security posture
management solution**

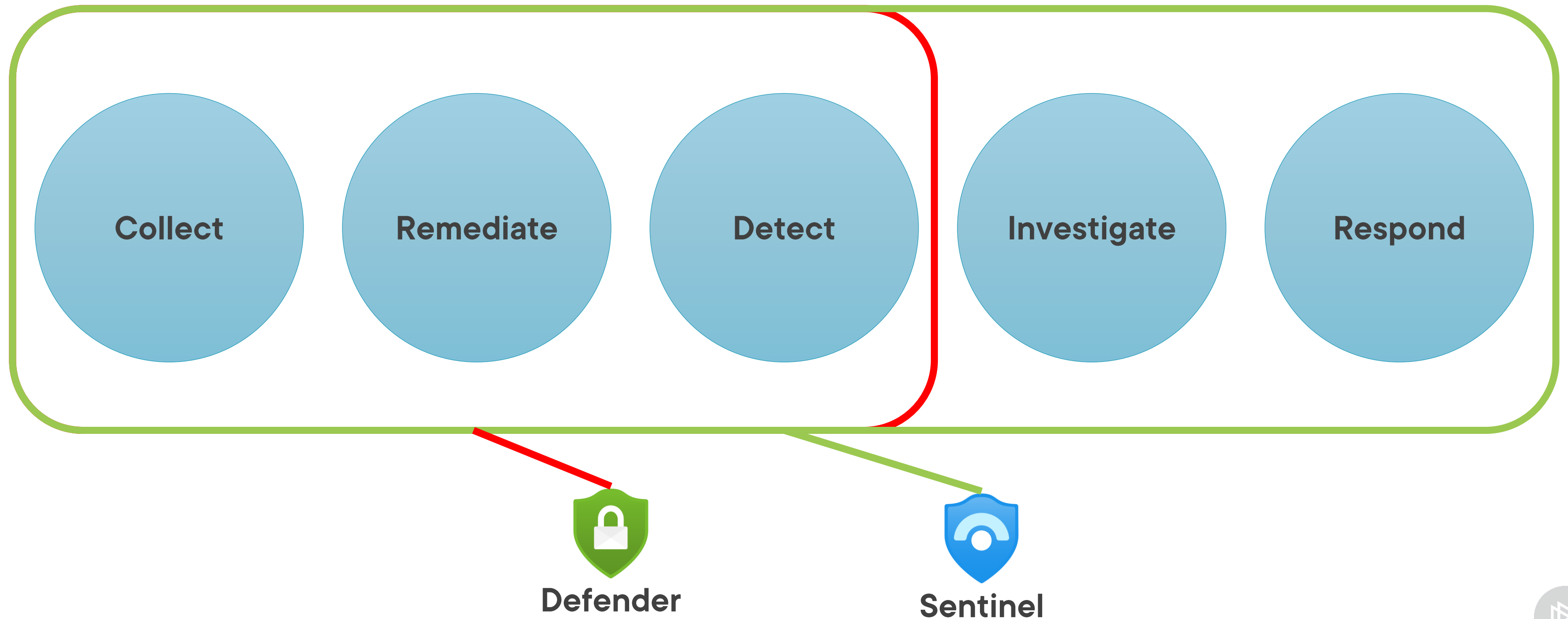
Secure score

Security recommendations

Security alerts



MDC vs. Microsoft Sentinel



Demo



1

Log Analytics workspace

Microsoft Sentinel

Microsoft Defender for Cloud



Summary



Microsoft Defender for Cloud is aimed at most IT professionals

Microsoft Sentinel is a more specialized solution

- Separate Log Analytics workspace



Up Next:

Secure Windows Server Networking

