What is Microsoft Sentinel?

Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Insights into threats

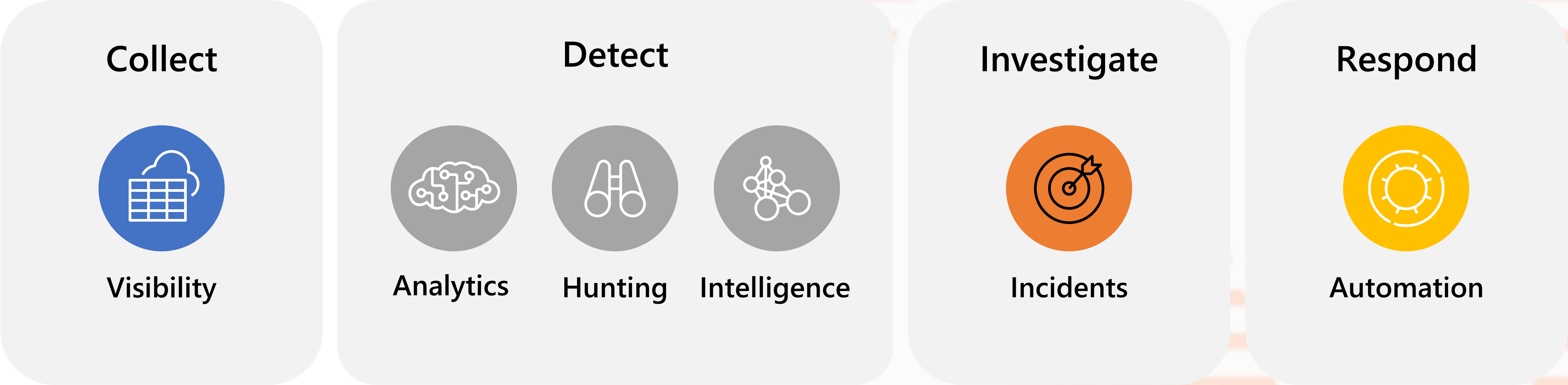
Get a birds-eye view across all data ingested and detect threats using Microsoft's analytics and threat intelligence. Investigate threats with artificial intelligence and hunt for suspicious activities.

In scope for this engagement.

Requirements

Available to organizations with an Azure tenant.

An end-to-end solution for security operations



Collect

Visibility

Detect

Analytics

Hunting

Intelligence

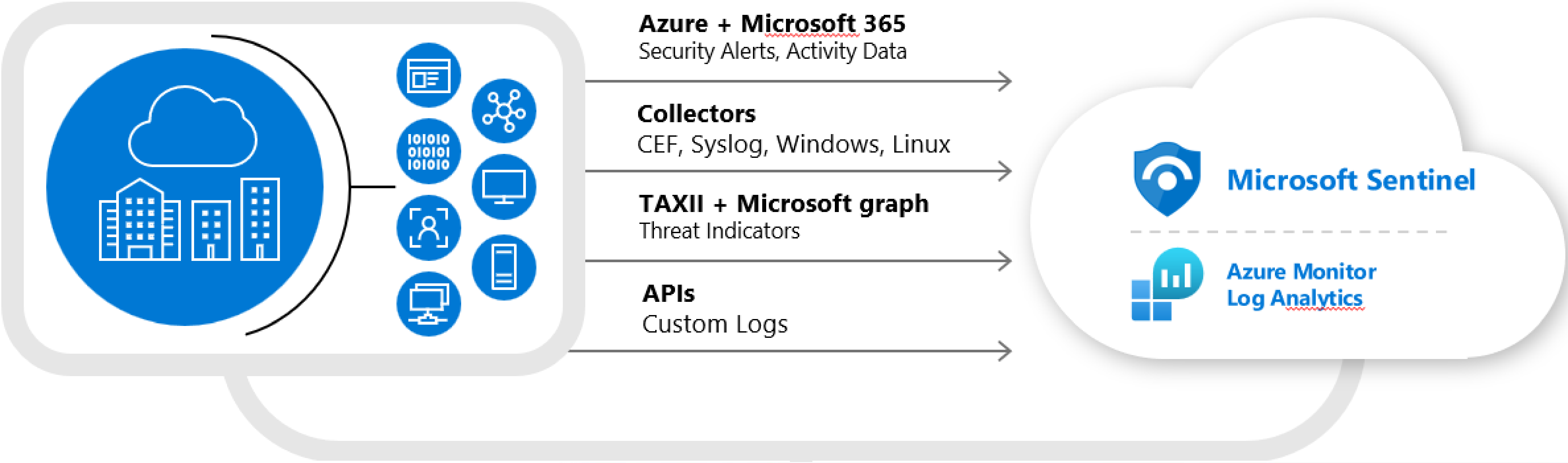
Investigate

Incidents

Respond

Automation

Collect security data at cloud scale from any source



Azure + Microsoft 365
Security Alerts, Activity Data

Collectors
CEF, Syslog, Windows, Linux

TAXII + Microsoft graph
Threat Indicators

APIs
Custom Logs

Microsoft Sentinel

Azure Monitor
Log Analytics