Microsoft

# Technology Integration Scenarios with Azure Sentinel

Building with Azure Sentinel

# Contents

## Introduction – Adding customer value.

Azure Sentinel is a next-generation, cloud native SIEM that re-imagines, threat detection, investigation and response powered by the limitless speed and scale of the Azure Cloud and the advance services Azure delivers including AI, Automation and ease of deployment.

Security Operations teams use Azure Sentinel to generate detections as well as investigate and remediate threats. Offering your data, detections, automation, analysis and packaged expertise, to customers via integration with Azure Sentinel enables security teams with the right information at the right time to execute informed security responses.

Azure Sentinel Solutions make it easier than ever for joint customers to discover, deploy, and maximize the value of the partner integrations that you create. With solutions, partners can:

**Unlock more value for your current customers and create new use cases.** When you build an Azure Sentinel solution, you're giving your customers everything they need to start maximizing the security value that your product or service already gives them – by building detections on top of that data, enabling them to cross-correlate it with the rest of their ecosystem, streamline investigation via the investigation graph, automate responses, and more. By delivering solutions you have an opportunity to deeply integrate with each of these Azure Sentinel SIEM and SOAR capabilities to not only deliver combined value for your current offerings but also expand to newer use cases that Azure Sentinel has to offer currently and in the future.

**Reach new customers.** Broaden discoverability and reach a new customer base through the Azure Sentinel solutions marketplace. Azure Sentinel solutions integrate with Azure Marketplace, and the solutions you deliver is showcased both in Azure Sentinel solutions blade as well as the Azure Marketplace. Hence delivering solutions gives you a direct connection to a potentially new and broad customer base.

**Productize your integration investments.** Enable customers to deploy integrations with just a few clicks by combining content into one single, easily discoverable, easily deployable package - consolidating value across data connectors, analytics, playbooks, and more. With solutions, you are delivering a combined productized value for your offerings in Azure Sentinel to deliver end-to-end scenarios in Azure Sentinel for our mutual customers.

This article outlines

- Mutual Scenarios and how to decide which make sense.
- What technical features are needed to enable each scenario.
- Where to go for instructions on building and publishing
- What Microsoft programs can help you with getting to customers.

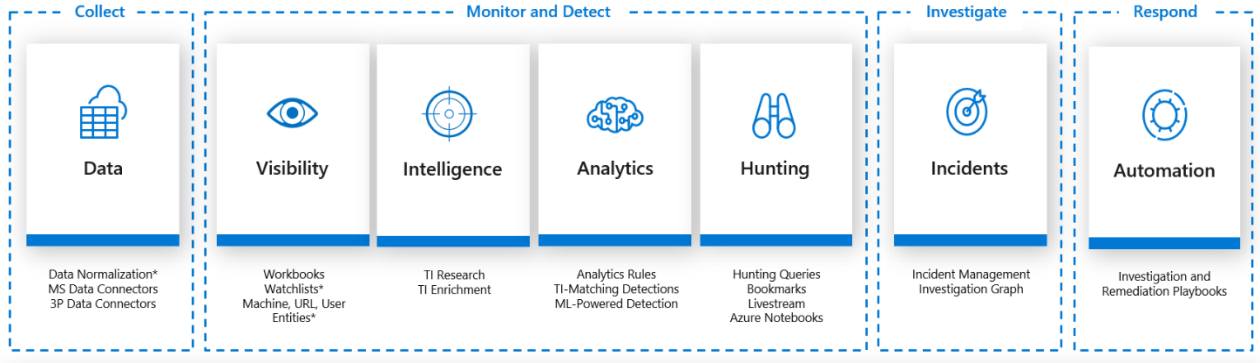
## Scenarios Overview – Use cases that resonate with customers

Azure Sentinel is designed to provide Security Operations teams with an integrated platform in which they can execute the daily activities of Collecting information, Detecting threats, Investigating and Responding to security incidents.

Creating Detections via the SIEM (Bring Log Data, Actionable Intelligence, Analytics rules, Hunting Rules, Guided hunting experiences, ML Analysis) to create detections out of semi-structured data.

Contributing to Azure Sentinel Investigation (Bring your detections, Queries, Historical data and supporting data like HVA DB's, VIP DBs, Vulnerability data, Compliance data, etc.)

Automating tasks in Azure Sentinel (Write automation rules for enrichment, remediation or orchestrating security activities within the customer's environment and infrastructure)




Each of these activity areas contain Azure Sentinel artifacts that technology partners can contribute and combine to deliver magnified value to Azure Sentinel customers.

## Collect - Bringing Data

Almost every Azure Sentinel technology partnership scenario begins with data. At the heart of Azure Sentinel are both a flexible and powerful general detection engine, and a full featured investigative engine. Both operate over data ingested into Azure Sentinel's data repository.

Sentinel works with four classes of data: Unprocessed Data, Security Conclusions, Reference Data and Threat Intelligence. It is very common for security products to simultaneously include more than one of these classes of data and each enable different activities within Azure Sentinel.

***Unprocessed Data - Facilitating Detections and Enabling Hunting.*** Analysis of raw operational data in which signs of malicious activity may be present is critical to the success of security teams. Azure Sentinel includes a cloud native, automatically scaled, SIEM. Bringing unprocessed data to Azure Sentinel enables you to bring Azure Sentinel's Hunting and detection capabilities (both query and ML based) to identify new threats and automate detection of already identified threats evidenced in the data you supply.

Examples of this class of data are Syslog, CEF over Syslog, application logs, firewall logs, authentication logs, access logs, etc.

***Security Conclusions - Creating alert visibility and opportunity for correlation***. Alerts and Detections are conclusions that have already been made about threats. Putting detections in context with all the activities and other detections visible in Azure Sentinel investigations, saves time for analysts and creates a more complete picture of an incident, resulting in better prioritization and better decisions.

Examples of detections include anti-malware alerts, suspicious processes, communication with known bad hosts, network traffic that was blocked and why, suspicious logons, detected password spray attacks, identified phishing attacks, data exfiltration events, and much more.

***Reference Data - Building Context and saving investigators time and effort by making information gathering more efficient***. Much time is spent by SOC Investigators gathering additional information from other systems to inform both investigation and remediating detected threats. Delivering Enrichment automation, the process of adding addition meaningful related data to Azure Sentinel incidents, is a highly valuable way to help the SOC improve their speed and completeness with investigations.

Examples of enrichment data include CMDBs, high value asset databases, application dependency databases, IP assignment logs, TI collections for enrichment and more.

***Threat Intelligence – Contributing Indicators of known threats to power threat detection***. TI can consist of current indicators, representing immediate threats, or historical indicators that are documented and retained for future prevention. Azure Sentinel supports both via different integration patterns.

- **Delivering current threat indicators** to Azure Sentinel, in the form of observables such as IP addresses, domains, etc. used in Azure Sentinel's detection engine for the purpose of finding sightings in customer log data. Current indicators can be the output from a Threat Intelligence Platform or other scoped feed and can be directed, not only to Azure Sentinel but to any Microsoft Product that can accept customer supplied TI.
- **Consuming Historical Indicators and/or Reference datasets** are also valuable to Azure Sentinel customers. In practice these data sets are often extremely large and best referenced ad hoc, in place, rather than being directly imported into Azure Sentinel.

## Monitoring and Detecting

The activities of the Monitoring and Detection capabilities in Azure Sentinel, are fundamentally about creating automated detections that help customers scale their security team's expertise.

***Threat Detection Rules – Enabling sophisticated detection to create accurate, meaningful alerts***.
Supplying your expertise and insights around what activities can be detected in the data you deliver can be encoded as Azure Sentinel Analytics making it easy for customers to gain the benefit of your experience. Analytics are query-based rules, operating over the data in a customer's Azure Sentinel workspace(s). Analytics can output alerts (notable events), incidents (unit of investigation), and fire off automation playbooks.

Threat detection rules can be included in Azure Sentinel Solutions as well as via the Azure Sentinel ThreatHunters community. Contributing Azure Sentinel Analytics rules via the community can help encourage community creativity over partner sourced data and help customers with more reliable and effective detections.

An example of a detection rule scenario might be to "Find the IP addresses of successful sign-ins that were also used in attempts to sign into disabled accounts."

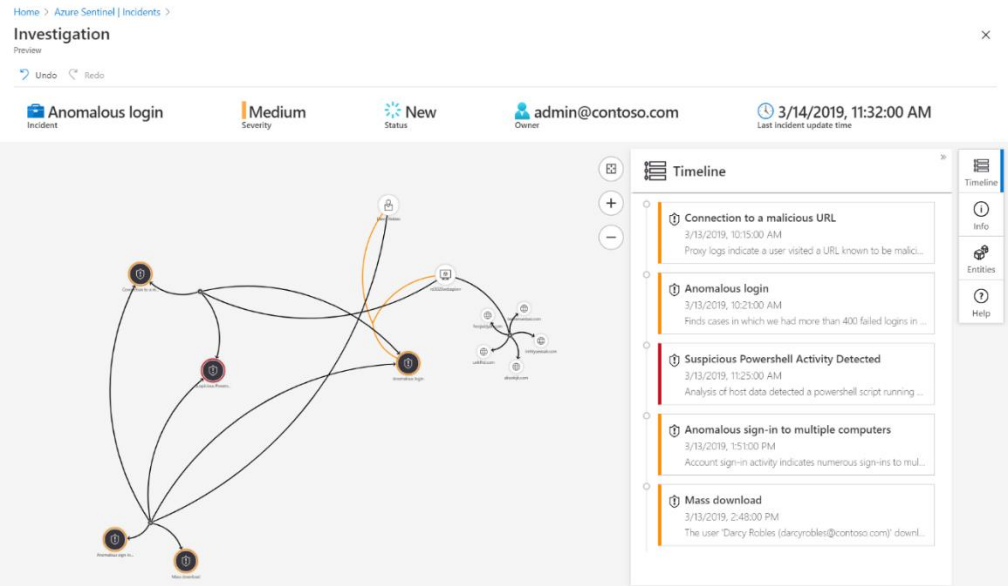
***Enabling Hunting – Helping customers find the "unknown" threats in their data.*** Azure Sentinel enables a rich set of hunting abilities that enable you to contribute your expertise to empower Azure Sentinel Hunters directly in the Azure Sentinel UI.

Helping customers hunt over the data that you supply enables customers in the process of discovering, as yet, undetected threats evidenced in the data you supply. You can deliver tactical hunting queries that highlight specific knowledge and/or complete guided hunting experiences in the form of Azure Sentinel Notebooks.

***Visualization – Helping customers manage and understand your data.*** Azure Sentinel customers invest in bringing vast amounts of data to Azure Sentinel. Creating graphic views of how well data is flowing and how effectively it contributes to detections highlights partner value to customers, by providing easy to use, customer customizable dashboards.

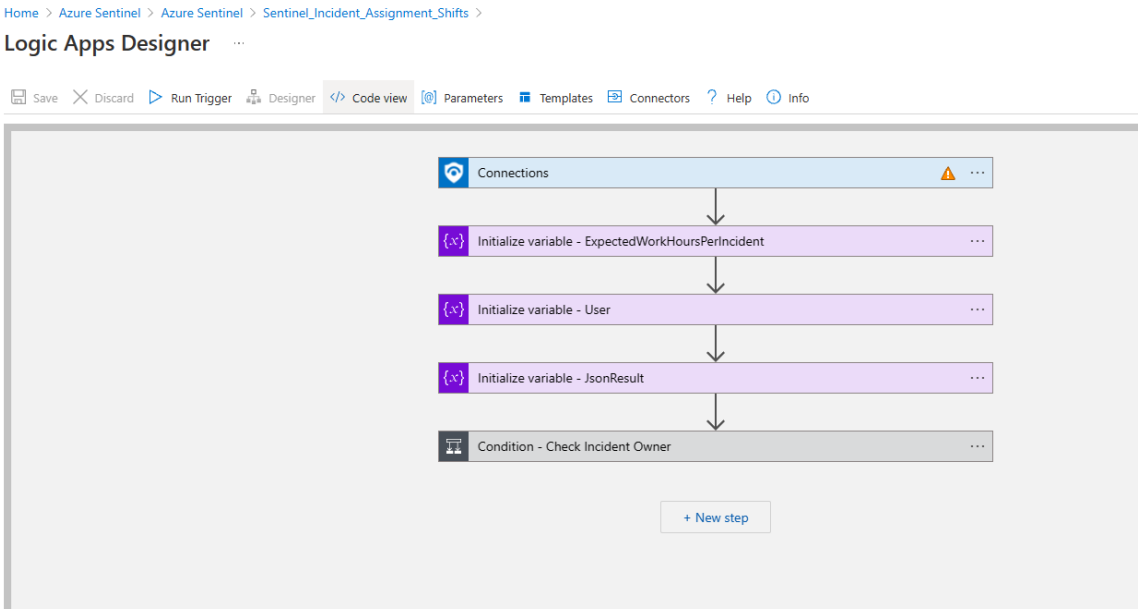
## Investigating

***Contributing to Investigative Graph – Giving investigators the right data, right when they are looking for it.*** The Azure Sentinel Investigation Graph allows investigators to view security incidents and alerts via the lens of connected entities to find relevant or related things that contributed to the event. Partners contribute to this experience in one of two ways. First, Azure Sentinel Alerts and incidents, either delivered by partner solutions, or created in Azure Sentinel via Analytics rules are automatically included. Secondly, partners can also extend the Azure Sentinel Investigation UI with Exploration Queries allowing custom queries into partner supplied data, enabling rich exploration, and linking of information and insights for the Security Investigator.



## Responding

***Coordination and Remediation. Enabling Azure Sentinel users to orchestrate and effect remediations quickly and accurately.*** Azure Sentinel Playbooks support a partner extensible workflow environment that allow for creation of rich automations which execute security related tasks across customer environments. Enabling Azure Sentinel customers with the ability to configure partner product security policies, gathering additional data to inform investigative decisions, linking Azure Sentinel Incidents to external incident management systems, and integrating alert lifecycle management across partner solutions are all high value customer scenarios that enable quicker and more reliable responses to security incidents.



## Deciding what to build – What to include in your Azure Sentinel Solution

There is a rich set of building blocks that partners can craft and combine, and understanding what to build depends on what scenarios apply. Below is a table that links the scenarios discussed in this paper with the essential and optional Azure Sentinel technical components to include in your Azure Sentinel Solution, that contribute to each scenario. Multiple scenarios are common and encouraged.

| Scenarios – Pick all that apply | Examples | How data is used in Azure Sentinel | What to build |
|---|---|---|---|
| *Your solution generates data that can inform or is important to security investigations. May or may not include detections* | Solutions that supply some form of log data: Firewalls, Cloud Application Security Brokers, Physical Access Systems, Syslog output. Commercially available and enterprise-built LOB applications, Servers, Network Metadata, anything deliverable over Syslog in Syslog of CEF format or REST API in JSON format. | Import Data into Azure Sentinel via data connector to enable analytics, hunting, investigations, visualizations, etc. | **Azure Sentinel Data Connector -** Deliver data and link to other customizations in our UI.<br>❑ Workbooks (Recommended)<br>❑ Sample Queries (Mandatory)<br>❑ Analytics – Build detections on your data in Azure Sentinel. (Recommended)<br>❑ Hunting Queries - Enable hunters with pre-built queries they can use in hunting(Optional)<br>❑ Azure Notebooks – Deliver fully guided, repeatable hunting experience. (Optional) |
| *If you provide detections…* | Antimalware, Enterprise Detection and Response solutions, Network Detection and Response solutions, Mail Security solutions including anti Phishing products, Vulnerability scanning, Mobile Device Management, UEBA Solutions, Information protection, products, etc. | Making your detection, alert or incident available in Azure Sentinel enables your detections to appear in context with other alerts and incidents.<br>Consider also delivering the log or metadata that powers your detections as customers routinely ask for it as additional context during investigation. | **Build an Azure Sentinel Data connector as above plus:**<br>❑ Analytics – Create Azure Sentinel Incidents from your detections so they become useable in incident investigations (Recommended) |
| *Supplying Threat Intelligence Indicators* | TIP platforms, STIX/TAXII Collections, public or licensed TI Sources.<br><br>Reference data: WhoIS, GeoIP, Newly observed Domains, etc. | Current indicators should be delivered to Azure Sentinel for use in Microsoft detection platforms including Sentinel and Defender<br>Very Large scale or Historical datasets should be used for enrichment scenarios and are best accessed remotely. | **Current TI**<br>❑ Build GSAPI connector to push indicators to Azure Sentinel<br>❑ Provide STIX 2.0,2.1 TAXII Server, customers will use built in TAXII data connector.<br><br>**Historical indicators and/or reference datasets**<br>❑ Logic app Connector and enrichment workflow playbook |
| *Additional Context* | CMDB, High value Asset DB, vIP DBs, Application dependency DBs, Incident Management Systems, Ticketing Systems | Alert and Incident Enrichment. | ❑ Logic App connector<br>❑ Enrichment workflow playbook<br>❑ Potentially external Incident lifecycle management workflow |
| *You can implement security policies* | Firewalls, NDR, EDR, MDM, Identity solutions, Conditional Access solutions, physical access solutions, other products that support block/allow or other actionable security policies | Azure Sentinel actions and workflows enabling remediations and responses to threats | ❑ Logic App connector<br>❑ Action workflow playbook |

## Getting Started

All Azure Sentinel Technical integrations begin with the Azure Sentinel Github Repository and Contribution Guidance.

When you are ready to begin work on your Azure Sentinel Solution. instructions for submitting, packaging and publishing are found in the Guide to Building Azure Sentinel Solutions

## Getting to market

Microsoft offers a number of programs to help partners approach Microsoft customers.

- Microsoft Partner Network The primary program for partnering with Microsoft is the Microsoft Partner Network. Membership in MPN is required to become an Azure Marketplace publisher where all Azure Sentinel Solutions are published.

- Azure Marketplace Azure Sentinel Solutions are delivered via the Azure Marketplace where customers go to discover and deploy both Microsoft and partner supplied general Azure integrations. Azure Sentinel Solutions are one many offer types that customers will find. Azure Sentinel also references your Azure Sentinel Solution Marketplace offers in an embedded Azure Marketplace experience in the Azure Sentinel UI.

- Microsoft Intelligent Security Association is the program specifically designed to provide Microsoft Security Partners with help creating awareness of partner created integrations with Microsoft customers and helps provide discoverability of your Microsoft Security product integrations.

  Joining the MISA program requires a nomination from a participating Microsoft Security Product Team and building the following integrations qualify partners for nomination

  - ✓ Azure Sentinel Data Connector and associated content – Workbooks, Sample Queries, Analytics Rules
  - ✓ Published Logic Apps Connector and Azure Sentinel Playbooks.
  - ✓ API integrations – on a case by case basis.

  To request a MISA nomination review or for questions please contact:
  AzureSentinelPartner@microsoft.com