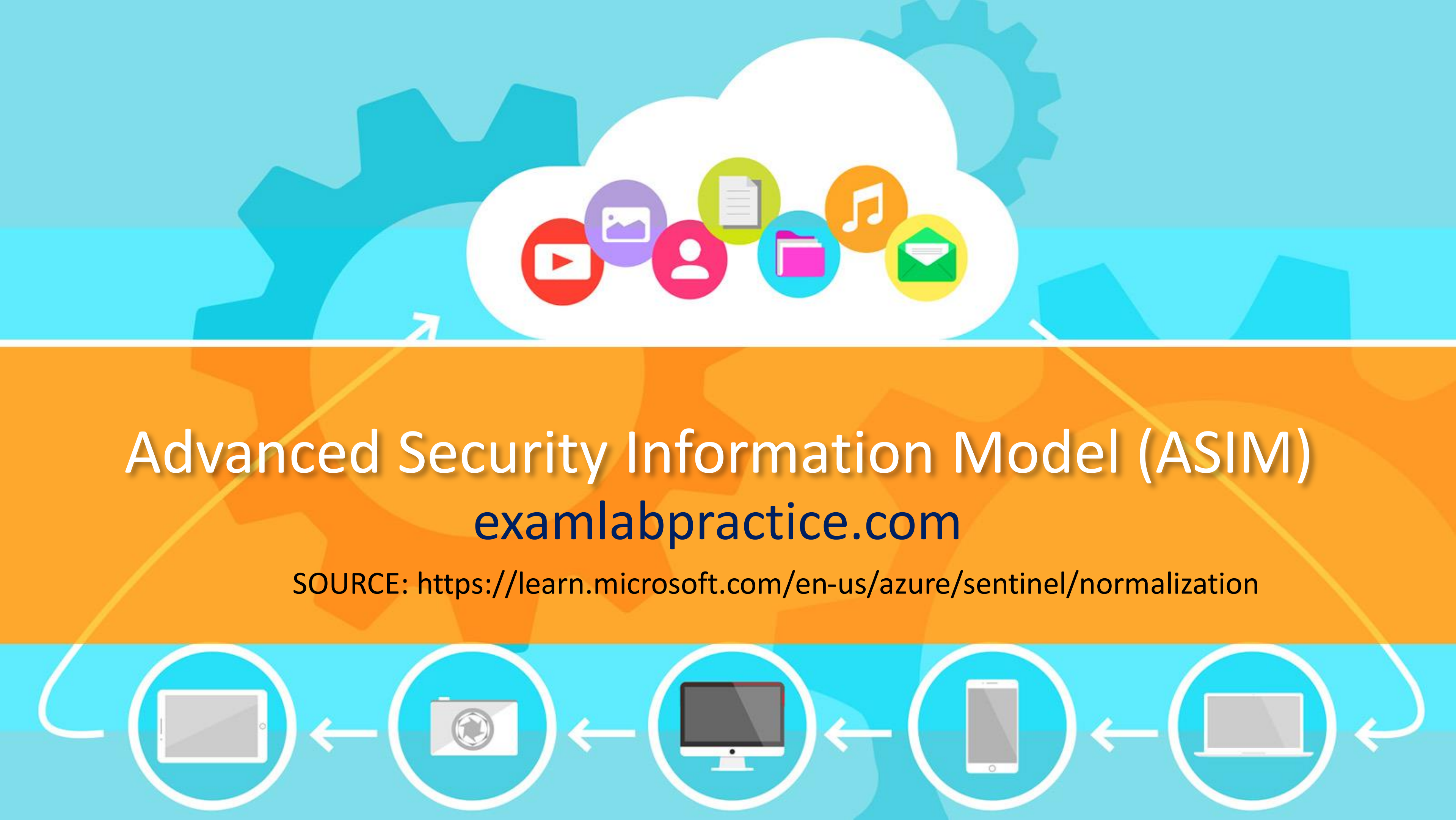


Advanced Security Information Model (ASIM)

examlabpractice.com

SOURCE: https://learn.microsoft.com/en-us/azure/sentinel/normalization

Why is ASIM important?

- Microsoft Sentinel gathers information from a diverse range of sources. To effectively work with this assortment of data, you must be familiar with each distinct type and table. This involves crafting and utilizing specialized data sets for analytics rules, workbooks, and hunting queries tailored to each specific type or schema.
- There are instances where you might require distinct rules, workbooks, and queries for different data types, even when there are shared elements, like in the case of firewall devices. Moreover, correlating various data types during investigative and hunting activities can present additional complexities.
- The Advanced Security Information Model (ASIM) acts as an intermediary layer between the user and the various data sources. Adhering to the robustness principle as its guiding design pattern, ASIM converts the unique telemetry data gathered by Microsoft Sentinel into user-friendly information. This transformation is aimed at simplifying data exchange and integration.

Common ASIM Usage

ASIM provides a seamless experience for handling various sources in uniform, normalized views, by providing the following functionality:

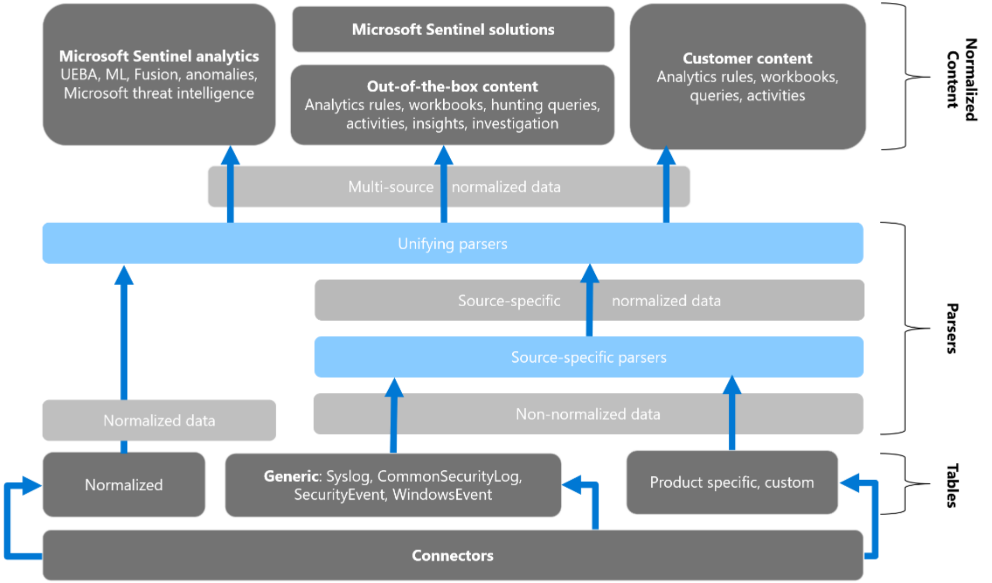
- Cross source detection. Normalized analytics rules work across sources, on-premises and cloud, and detect attacks such as brute force or impossible travel across systems, including Okta, AWS, and Azure.
- Source agnostic content. The coverage of both built-in and custom content using ASIM automatically expands to any source that supports ASIM, even if the source was added after the content was created. For example, process event analytics support any source that a customer may use to bring in the data, such as Microsoft Defender for Endpoint, Windows Events, and Sysmon.
- Support for your custom sources, in built-in analytics
- Ease of use. After an analyst learns ASIM, writing queries is much simpler as the field names are always the same.

ASIM and the Open Source Security Events Metadata (OSSEM)

- ASIM is in harmony with the Open Source Security Events Metadata (OSSEM) common information model, enabling consistent correlation of entities across standardized tables.
- OSSEM, driven by community efforts, concentrates on standardizing and documenting security event logs from a variety of data sources and operating systems.
- Additionally, it offers a Common Information Model (CIM), assisting data engineers in the data normalization process.
- This model is instrumental for security analysts to efficiently query and analyze data from multiple sources.

ASIM components

The image below illustrates the process of converting non-normalized data into a standardized format for use in Microsoft Sentinel. This involves beginning with a unique, product-specific, non-standardized table and employing a parser along with a normalization schema to transform this table into normalized data. Once normalized, this data can be utilized in various Microsoft and custom analytics, rules, workbooks, queries, and beyond.



Microsoft Sentinel analytics UEBA, ML, Fusion, anomalies, Microsoft threat intelligence

Microsoft Sentinel solutions

Out-of-the-box content Analytics rules, workbooks, hunting queries, activities, insights, investigation

Customer content Analytics rules, workbooks, queries, activities

Normalized Content

Multi-source normalized data

Unifying parsers

Source-specific normalized data

Source-specific parsers

Non-normalized data

Normalized data

Parsers

Normalized

Generic: Syslog, CommonSecurityLog, SecurityEvent, WindowsEvent

Product specific, custom

Tables

Connectors

Normalized Schemas

Normalized schemas encompass a range of consistent event types that are useful for developing unified capabilities. Each schema specifies the fields characterizing an event, adheres to a uniform column naming convention, and establishes a standard format for the values of these fields.

ASIM currently defines the following schemas:

- Audit Event
- Authentication Event
- DHCP Activity
- DNS Activity
- File Activity
- Network Session
- Process Event
- Registry Event
- User Management
- Web Session

Query Time Parsers

- ASIM employs parsers at query time to align existing data with the normalized schemas, utilizing KQL functions.
- Microsoft Sentinel provides numerous ASIM parsers as built-in features.
- Additionally, a variety of parsers, including customizable versions of the built-in ones, can be implemented from the Microsoft Sentinel GitHub repository.

Ingest Time Normalization

Query time parsers offer several benefits:

- They maintain the original data format, ensuring the source's integrity is not compromised.
- Their development is straightforward as they provide a representation of the data rather than altering it.
- This makes the processes of developing, testing, and repairing parsers more efficient since they work on pre-existing data.
- If issues arise, they can be rectified promptly, with the corrections applying retroactively to existing data.

However, despite their optimized nature, ASIM parsers may cause query slowdowns, particularly with large datasets. To counteract this, Microsoft Sentinel employs ingest time parsing alongside query time parsing. This approach involves transforming the events during ingestion into a normalized table format, thereby speeding up queries that utilize this normalized data.