Use Watchlists in Microsoft Sentinel

# Watchlists

Watchlists can be used in your search, detection rules, threat hunting and response playbooks. They are stored in your sentinel workspace as name-value pairs and are cached for optimeal query performance and low latency.

Use cases:

* Investigating threats and responding to incidents quickly with the rapid import of IP addresses, file hashes, and other data from CSV files.
* Importing business data as a watchlist. E.g. import user lists with privileged system access or terminated employees then use the watchlist to create allow and blocklists used to detect or prevent those users from logging in to the network.
* Reducing alert fatigue. Create allowlists to suppress alerts from a group of users from authorized IP addresses.
* Enrich event data with name-value combinations derived from external data sources.