With advanced hunting, there is also advantage of the following capabilities:

- *Powerful query language with IntelliSense* – It is built on top of query language which gives the flexibility that is needed to take hunting to the next level.
- *Query the stored telemetry* - The telemetry data is accessible in tables for the query. For example, query process creation, network communication, and many other event types.
- *Links to portal* –Consolidating the Advanced Hunting query experience and the existing portal investigation experience links directly to the machine names and file names to the portal.
- *Query examples* - A welcome page provides examples designed to get started and get familiar with the tables and the query language.

### Threat Analytics

Windows Defender ATP research and development team identifies the emerging threats and their outbreaks. The reports helps in the assess impact of threats in the environment and provides recommended actions to contain, increase organizational resilience, and prevent specific threats.

Each threat report provides a summary which describe the details like where the threat is coming from, where it's been seen, or techniques and tools that were used by the threat.

The dashboard of the ATP shows the impact in the organization through the following tiles:

- *Machines with alerts* – It shows the current distinct number of impacted machines in the organization.
- *Machines with alerts over time* -It shows the distinct number of machines impacted over time.
- *Mitigation recommendations* – It lists the measurable mitigation solutions and also the number of machines that do not have each of the mitigations in place.
- *Mitigation status* – It shows the number of mitigated and unmitigated machine.
- *Mitigation status over time* – It determines the distinct number of machines that have been mitigated, unmitigated, and unavailable over time over the organisation.

### Automated investigation and Remediation

Automated Investigations significantly reduces the volume of alerts that need to be investigated individually. The Automated investigation feature leverages various inspection algorithms, and processes used by analysts to examine alerts and take immediate remediation action to resolve breaches. This significantly reduces the volume of alerts, which allows security operation experts to focus on more sophisticated threats and other high value initiatives. The Automated Investigations list displays all the investigations that have been initiated automatically with other details such as its status, detection source, and the date for when the investigation was initiated.

## Windows Defender ATP Preview Feature

The Windows Defender ATP service is constantly being updated to include new feature enhancements and capabilities to threat detection and protections. Some of latest and important features are as follows:

- Information Protection