

Microsoft Sentinel

Planning and implementing Microsoft's cloud-native SIEM solution

Second Edition



Yuri Diogenes
Nicholas DiCola
Tiander Turpijn

Foreword by Sarah Fender

Partner Director of Product Management – Microsoft Sentinel

Microsoft Sentinel

Planning and implementing
Microsoft's cloud-native SIEM solution
Second Edition

Yuri Diogenes
Nicholas DiCola
Tiander Turpijn

- **Alerts** As defined by the sending source, alerts are normalized in nature, and schemas are validated and enforced.
- **Incidents** As defined by the sending source, incidents are normalized in nature, and schemas are validated and enforced. Technically, incidents are created in Microsoft Sentinel upon ingestion.

An incident in Microsoft Sentinel is created in one of the following ways:

- A scheduled analytics rule (as described in Chapter 3), based on either one or more alerts or notable events
- An incident created by one of the data connectors based on one or more alerts
- A Fusion incident based on fused and correlated events
- An incident based on a Machine Learning (ML) behavior analytics rule
- An incident based on a match with one or more threat indicators
- An incident based on a hunting query
- A manually created incident through the SecurityInsights API, PowerShell, or the Azure portal

What all these incidents have in common is that a notable event has been created as a data source. This can be through an agent, Azure resource or service, AWS, GCP event, or any ingested data stream. A notable event converts to an alert if certain (rules) conditions are matched, which will result in the creation of an incident, which by itself can contain one or more alerts. The exception is that the source can also send alerts or incidents directly. This is most common with first-party data connectors, which cover Microsoft sources like Azure Active Directory Identity Protection, Azure Information Protection, and so on. Another example would be incidents sent through the **Microsoft 365 Defender** connector (M365D), which contains alerts as well.

The benefit is that alerts and incidents created by these data connectors already contain correlated entities, such as a host, account, IP address, and the like. Scheduled analytics rules are flexible in the sense that you can define which entities should be associated with the incident. In Sentinel, this concept is called *entity mapping*.

Exploring and configuring the Incidents view

The incidents blade, which shows all incidents, can be customized to fit the needs of the analyst. A time and date range can be configured so that it is retained for the duration of the analyst session, even if the analyst navigates to another Sentinel blade. Figure 4-1 shows the **Last 24 Hours** default selection, which can be customized using a **Custom Range**.

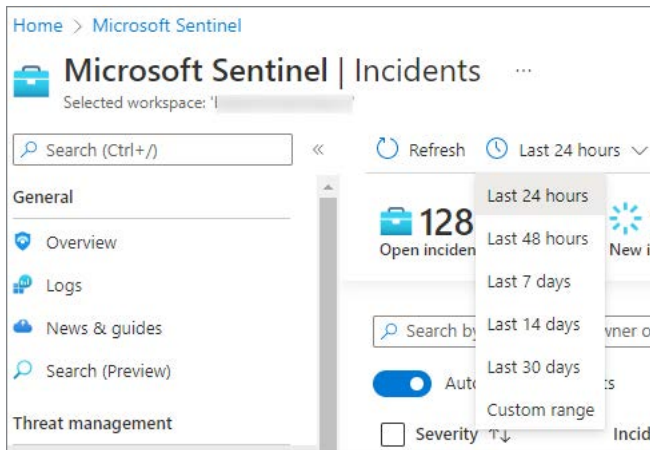


FIGURE 4-1 Selecting the time and date range for viewing incidents

To select the time and day range of incidents to view, follow these steps:

1. Open the **Azure portal** and sign in as a user who has Microsoft Sentinel Reader privileges.
2. Under **Threat Management**, select **Incidents**.
3. Collapse the arrow next to **Last 24 Hours** and make your selection based on the default choices, or select **Custom Range** to select your **From (UTC)** and **To (UTC)**, as shown in Figure 4-2.

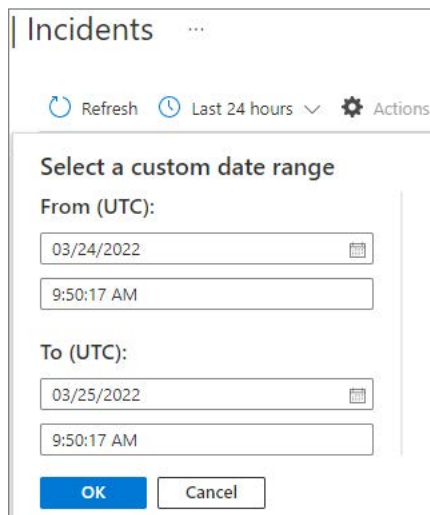


FIGURE 4-2 Selecting a custom range for viewing incidents

NOTE Custom date ranges will always be shown in UTC.

Your selection will update the **Open Incidents**, **New Incidents**, and **Active Incidents** count to reflect the time and day range. The filters for **Severity**, **Status**, **Product Name**, and **Owner** allow you to further filter incidents according to your needs. Figure 4-3 shows incidents being filtered by **Product Name**.

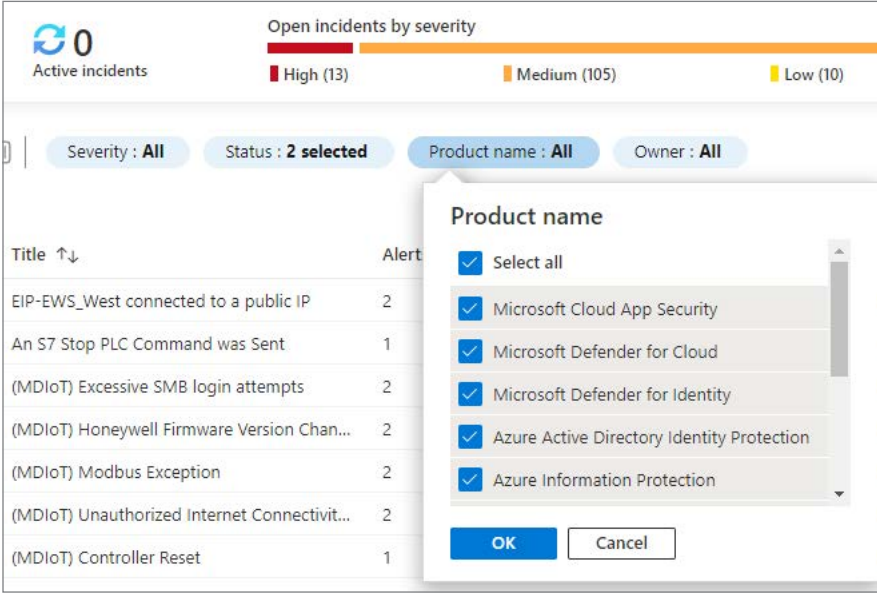


FIGURE 4-3 Filtering the incidents view by Product Name

In the top-middle area of the incidents view (next to the time and day range filter) are the **Actions** that can be taken. You can use the checkboxes to select multiple incidents. When multiple incidents are selected, clicking the **Actions** button enables you to change the **Severity**, assign an owner or group, change the status, or add Tags for multiple incidents at once.

As shown in Figure 4-4, next to the **Actions** button is the **Security Efficiency Workbook** option, which helps you monitor your SOC Key Performance Indicators (KPI), such as the mean-time to triage, meantime to closure, and so on.



FIGURE 4-4 Options available for incidents

Follow the steps below to access the **Security Efficiency Workbook**:

1. While still on the **Incidents** blade, select the **Security Efficiency Workbook** button.
2. Select your **Subscription** and **Workspace**.
3. Filter according to your criteria, such as by owner, tactics, or product name.
4. The Workbook shows different KPIs, such as **Time To Triage** and **Time To Closure**, which can be found if you scroll down through the Workbook (see Figure 4-5).

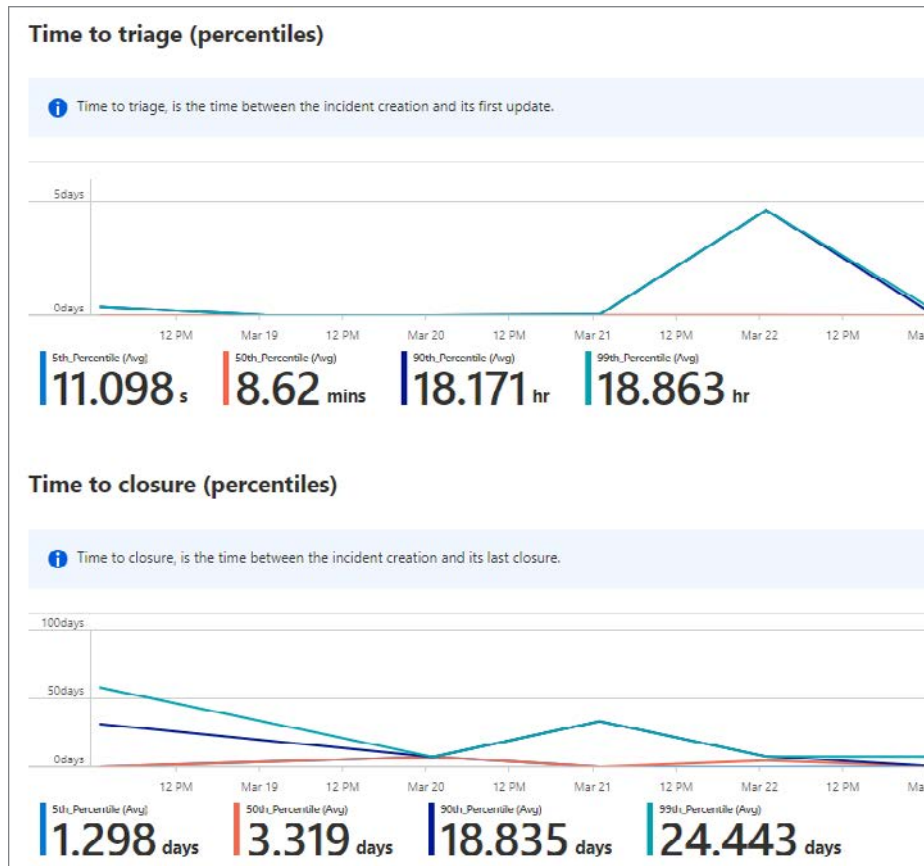


FIGURE 4-5 The Security Efficiency Workbook, showing the Time To Triage and Time To Closure

Back in the **Incidents Overview** blade, you will see the **Columns** option to the right of the **Security Efficiency Workbook** option. After clicking **Columns**, you can unhide or hide certain columns, and you can change the order. Figure 4-6 shows an example of unhiding the **Tactics** column and reordering it so it appears next to the **Incident ID** column.

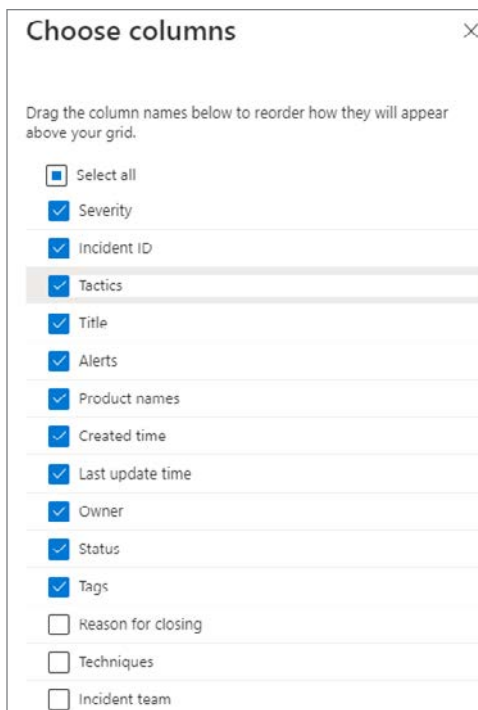


FIGURE 4-6 Choosing to hide, unhide, or reorder columns

After you click **Apply**, the incident column view will be updated based on your selection, as shown in Figure 4-7.

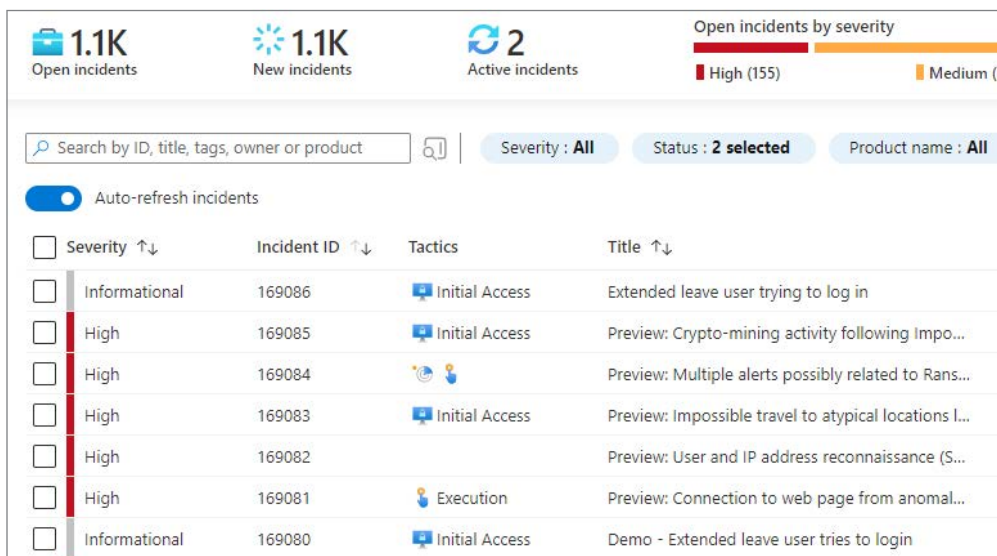
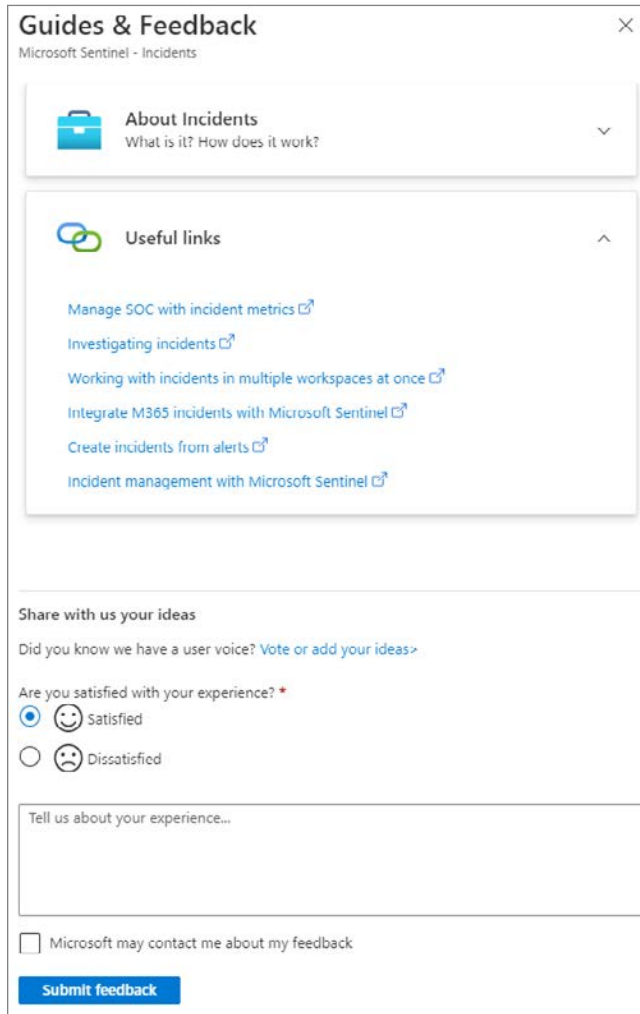


FIGURE 4-7 Tactics column added and reordered to appear next to the Incident ID column


Guides and feedback


The **Incidents** blade also offers you an opportunity to provide valuable feedback to the Sentinel Product Group, which is always considered when developing new features and improving the product. Here, you will find guidance on how incidents work in Sentinel, valuable links to explore, and the Sentinel community forum to share your ideas and suggestions. Figure 4-8 shows the **Guides & Feedback** pane with **Useful Links**, the **Vote Or Add Your Ideas** link, and a **Tell Us About Your Experience** text box, where you can share your experience with Sentinel.



Guides & Feedback ×

Microsoft Sentinel - Incidents

 **About Incidents**
What is it? How does it work? ▼


 **Useful links** ^


- [Manage SOC with incident metrics](#)
- [Investigating incidents](#)
- [Working with incidents in multiple workspaces at once](#)
- [Integrate M365 incidents with Microsoft Sentinel](#)
- [Create incidents from alerts](#)
- [Incident management with Microsoft Sentinel](#)

Share with us your ideas

Did you know we have a user voice? [Vote or add your ideas](#)

Are you satisfied with your experience? *

☒  Satisfied

☐  Dissatisfied

Tell us about your experience...

☐ Microsoft may contact me about my feedback

Submit feedback

FIGURE 4-8 The Guides & Feedback pane

You can provide feedback or explore useful links by clicking **Guides & Feedback** in the upper middle part of the **Incidents Overview** pane. This is also the place to provide feedback or **Share With Us Your Ideas**.