Microsoft Sentinel: Microsoft Defender XDR Integration

Overcast makes migrations simple and straightforward.

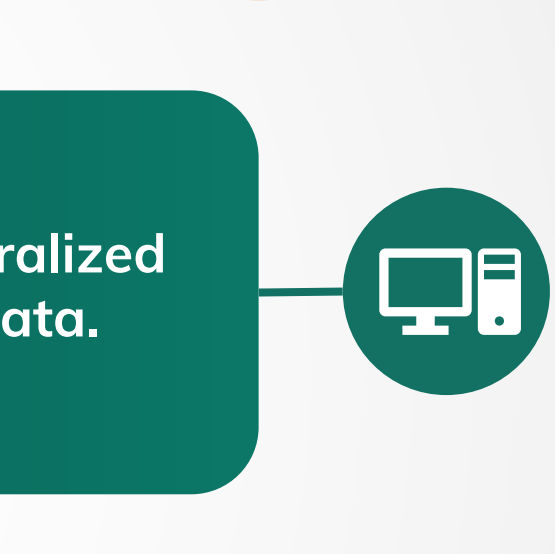
Microsoft XDR incident integration allows you to transmit all XDR incidents from Microsoft Defender to Microsoft Sentinel and keep them synchronized between the two portals.

Maintain the usual security workflow, thereby automating security procedures.

You can use tools like Microsoft Power BI or Microsoft Sentinel workbooks to create your own visualizations of discovery data that fit your organizational needs.

This integration enables centralized monitoring of alerts and detection data.

Longer data retention provided by Log Analytics.



Establish correlations between cloud-based events and on-premises events.

Microsoft Defender XDR incidents include all associated alerts, entities, and relevant information, providing sufficient context to perform triage and preliminary investigation in Microsoft Sentinel.

Overcast UP Your Business. | Microsoft Solutions Partner