

Microsoft Sentinel | Incidents

Selected workspace: 'ar-sentinel-root-92449-ar'

 Search

Create incident (Preview)



Refresh



Last 30 days



Actions



Delete



Security efficiency workbook



Columns



Guides & Feedback

General

Overview

Logs

Guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Summary rules

Watchlist

Automation

Settings

 16
Open incidents 10
New incidents 6
Active incidents

Open incidents by severity

High (6)

Medium (9)

Low (1)

Informational (0)

 Search by ID, title, tags, owner or product

Severity : All

Status : Active

Incident Provider name : All

Alert product name : All

Owner : All

 Auto-refresh incidents

<input type="checkbox"/> Severity ↑↓	Incident number ↑↓	Title ↑↓	Alerts	Incident provider name	Alert product name	Created time ↑↓	Last update ↑↓
<input type="checkbox"/> Medium	22	Shadow Copies Deletion	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:23 PM	11/14/25, 02:00 AM
<input type="checkbox"/> Medium	21	RClone Process Execution	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:19 PM	11/14/25, 02:00 AM
<input type="checkbox"/> High	19	Domain Admin Password Reset	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:18 PM	11/14/25, 02:00 AM
<input type="checkbox"/> Medium	16	Suspicious Download Via Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:17 PM	11/14/25, 02:00 AM
<input type="checkbox"/> High	20	Uncommon Network Connection Initiated By Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:17 PM	11/14/25, 02:00 AM
<input type="checkbox"/> Medium	17	Real-Time Protection in Defender disabled	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:16 PM	11/14/25, 02:00 AM
<input type="checkbox"/> Medium	13	Suspicious Download Via Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:58 AM	11/14/25, 02:00 AM
<input type="checkbox"/> High	12	Uncommon Network Connection Initiated By Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:57 AM	11/14/25, 02:00 AM