

# 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 : New

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	11	RClone Process Execution	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:54 AM	10/31/25, 09:
<input type="checkbox"/> High	9	HackTool - Bloodhound/Sharphound Execution	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:50 AM	10/31/25, 09:
<input type="checkbox"/> Medium	8	RClone Process Execution	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:45 AM	10/31/25, 09:
<input type="checkbox"/> Medium	7	Suspicious Download Via Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:43 AM	10/31/25, 09:
<input type="checkbox"/> High	6	Uncommon Network Connection Initiated By Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:42 AM	10/31/25, 09:
<input type="checkbox"/> High	5	HackTool - Bloodhound/Sharphound Execution	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:39 AM	10/31/25, 09:
<input type="checkbox"/> Medium	4	Suspicious Download Via Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:38 AM	10/31/25, 09:
<input type="checkbox"/> High	3	Uncommon Network Connection Initiated By Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:37 AM	10/31/25, 09:
<input type="checkbox"/> Medium	1	Real-Time Protection in Defender disabled	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:36 AM	10/31/25, 09:
<input type="checkbox"/> Low	2	Suspicious Group And Account Reconnaissance Activity Using Net.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:35 AM	10/31/25, 09: