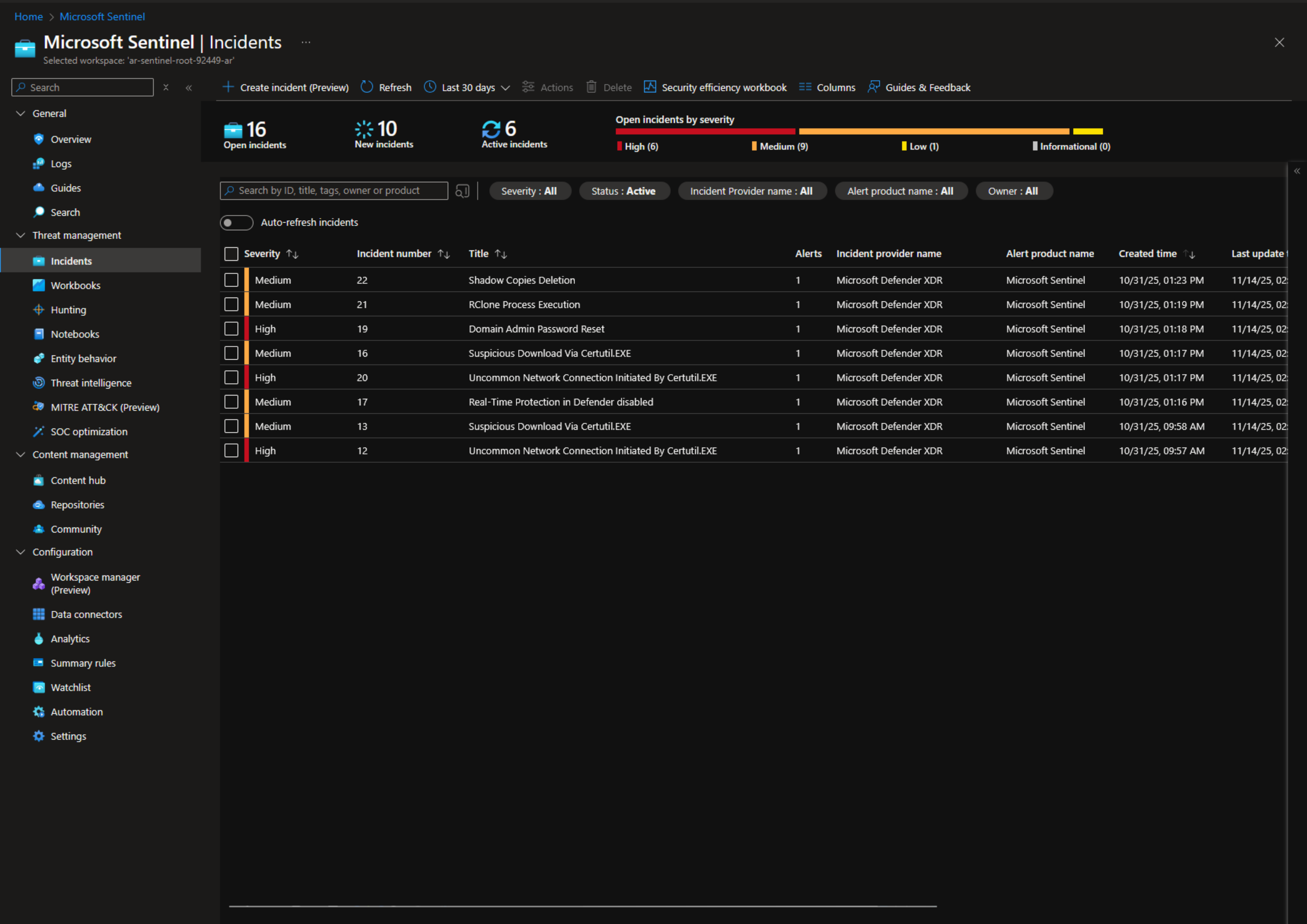

Microsoft Sentinel | Incidents

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

16 Open incidents

10 New incidents

6 Active incidents

Open incidents by severity

High (6) Medium (9) Low (1) Informational (0)

Severity : **All** Status : **Active** Incident Provider name : **All** Alert product name : **All** Owner : **All**

Severity	Incident number	Title	Alerts	Incident provider name	Alert product name	Created time	Last update t
Medium	22	Shadow Copies Deletion	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:23 PM	11/14/25, 02
Medium	21	RClone Process Execution	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:19 PM	11/14/25, 02
High	19	Domain Admin Password Reset	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:18 PM	11/14/25, 02
Medium	16	Suspicious Download Via Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:17 PM	11/14/25, 02
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
Medium	17	Real-Time Protection in Defender disabled	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 01:16 PM	11/14/25, 02
Medium	13	Suspicious Download Via Certutil.EXE	1	Microsoft Defender XDR	Microsoft Sentinel	10/31/25, 09:58 AM	11/14/25, 02
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