SECURITY ALERTS

Fabrikam Dental Group

Harbour IT

PREPARED BY	DATE	DATA COLLECTED	MICROSOFT 365 TENANT
Harbour IT	16 Oct 2026	16 Oct 2026, 14:48 UTC	fabrikam.onmicrosoft.com

What Microsoft Defender has flagged: open incidents and alerts, how severe, who is dealing with each, the accounts and devices they name, and what was resolved recently.

Open alerts	High severity	Not picked up	Open incidents	Recently resolved
4	1	3	2	1
Not resolved in Defender	Open alerts Defender rates high	Still new and assigned to nobody	Related alerts grouped by Defender	Alerts resolved, last 30 days

Open incidents 2 2 to review

Defender groups related alerts into an incident, so one attack shows once. Work through these from the most severe: assign each to someone, and close it in Defender with what it turned out to be.

Flag	Incident	Severity	Status	Assigned to	Alerts	Created (UTC)	Last updated (UTC)	Link
High	Phishing involving one user	High	Active	–	1	14 Oct 2026, 14:48	14 Oct 2026, 14:48	Open in Defender
Medium	Execution incident on one endpoint	Medium	In progress	helpdesk@msp.example	1	12 Oct 2026, 14:48	12 Oct 2026, 14:48	Open in Defender

Open alerts 4 2 to review

Alerts nobody has resolved yet. One that's still new and assigned to nobody hasn't been looked at. Check what each names: for an account, its recent sign-ins, inbox rules and MFA methods; for a device, what Defender found on it. Then resolve it in Defender, saying whether it was a real threat.

Flag	Alert	Severity	Status	Picked up	Source	Category	Accounts	Devices	Assigned to	Created (UTC)	Link
High	Email messages containing malicious URL removed after delivery	High	New	No	Defender for Office 365	Initial access	anna.kowalski@fabrikam.example	–	–	14 Oct 2026, 14:48	Open in Defender
Medium	Suspicious PowerShell command line	Medium	In progress	Yes	Defender for Endpoint	Execution	LAPTOP-OKAFOR\bob	LAPTOP-OKAFOR	helpdesk@msp.example	12 Oct 2026, 14:48	Open in Defender
Low	Unfamiliar sign-in properties	Low	New	No	Entra ID Protection	–	carl.svensson@fabrikam.example	–	–	15 Oct 2026, 14:48	Open in Defender
	eDiscovery search started or exported	Informational	New	No	Defender XDR	–	–	–	–	13 Oct 2026, 14:48	Open in Defender

Recently resolved 1

Alerts resolved in the last 30 days, and what whoever closed each said it was.

Alert	Severity	Source	Outcome	Accounts	Devices	Resolved (UTC)
User clicked a malicious link	High	Defender for Office 365	Real threat (phishing)	daniel.frost@fabrikam.example	–	11 Oct 2026, 14:48

From Microsoft Defender's alerts and incidents. Which services report to it depends on the tenant's licences: Defender for Office 365 for email, Defender for Endpoint or Business for computers, Entra ID Protection for sign-ins. Office Sentry keeps the accounts and devices an alert names, never the email, file or command behind it. Times are UTC.

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 16 Oct 2026, 14:48 UTC.