MICROSOFT 365 DECEPTION MONITORING

TrapLine

Meridian Health Partners

Monthly Security Report · June 1–30, 2026

Action required — canary interaction confirmed

Four decoy assets were accessed this period, three of them within a single 12-hour window on June 5. Combined with a 183% rise in file modification volume, this pattern warrants credential review for the affected account before the next reporting cycle.

AUDIT EVENTS	SIGN-INS	CANARY HITS	DETECTIONS	DECOYS LIVE
7,265	4,118	4	3	11
▲ 6.2% vs. May	– 1.1% 12 failed	▲ 4 from zero	1 med · 2 low	100% healthy

01 June in review

30 OF 30 DAYS COVERED

TrapLine collected and analyzed **7,265 Microsoft 365 audit events** and **4,118 Entra ID sign-ins** across the Meridian Health tenant, with unbroken telemetry for all 30 days of the period. Eleven deception assets remained deployed and healthy throughout.

The period's defining event was **four canary interactions** — the first recorded for this tenant since deployment. All four traced to a single mailbox, `r.okafor@meridianhealth.org`, with three occurring inside a twelve-hour window on June 5. Three additional detections were raised and triaged; one remains open pending client confirmation.

ANALYST ASSESSMENT

> Canary access is a high-confidence signal by design — no legitimate business workflow touches these assets. The clustering of three hits on a single day, against a single mailbox, is more consistent with mailbox enumeration by an automated tool than with accidental user access. The parallel spike in extended file modifications on the same account strengthens that read.
>
> We have not observed data exfiltration, admin role changes, or anomalous sign-in geography. This is an early-stage signal, not a confirmed breach — but it is exactly the point at which intervention is cheapest.
>
> Reviewed and finalized by a Vortacity Cyber analyst · Jul 4, 2026

RECOMMENDED ACTIONS

P1	**Force credential reset and revoke sessions for the affected mailbox** Revoke all refresh tokens for r.okafor@meridianhealth.org and require re-authentication with MFA. Audit any inbox rules created in the last 45 days.	48 HRS
P1	**Review and disposition the suspicious inbox rule detection** A forwarding rule created June 5 remains active. Confirm with the user whether this was intentional; if not, treat as a business email compromise indicator.	48 HRS
P2	**Close out 23 carryover items from prior periods** The oldest dates to March 27. Sustained carryover reduces signal quality and delays triage on new events. We recommend a scheduled review session.	30 DAYS
P3	**Extend deception coverage to OneDrive** OneDrive currently holds zero canaries, leaving a coverage gap in the workload most associated with bulk data staging.	NEXT CYCLE

02 Deception & response

4 INCIDENTS · 11 ASSETS

DECEPTION COVERAGE BY WORKLOAD

Outlook	SharePoint	OneDrive
4	7	0
4 HEALTHY · 3 TRIGGERED	7 HEALTHY · 1 TRIGGERED	COVERAGE GAP · SEE P3

CANARY INCIDENTS

INC-01 "Urgent: Wire Transfer Confirmation Needed" — ACTIVE

ASSET	Outlook mailbox canary	ACCOUNT	r.okafor@meridianhealth.org
FIRST SEEN	Jun 5, 2026 · 10:25 AM ET	ACTION	MessageRead · client not recorded

10:25:14	10:25:31	10:41:00	PENDING
Canary opened	Alert raised	Analyst triage	Client confirmation

INC-02 "New VPN credentials attached" — ACTIVE

ASSET	Outlook mailbox canary	ACCOUNT	r.okafor@meridianhealth.org
FIRST SEEN	Jun 5, 2026 · 10:25 AM ET	ACTION	MessageRead · attachment not opened

10:25:52	10:26:08	10:41:00	PENDING
Canary opened	Alert raised	Correlated to INC-01	Client confirmation

INC-03 "New VPN credentials attached" — ACTIVE

ASSET	Outlook mailbox canary	ACCOUNT	r.okafor@meridianhealth.org
FIRST SEEN	Jun 5, 2026 · 8:19 PM ET	ACTION	MessageRead · outside business hours

20:19:03	20:19:20	20:44:00	PENDING
Canary re-opened	Alert raised	Escalated to P1	Credential reset

INC-04 "Q3 Payroll Reconciliation — DRAFT.xlsx" — MONITORING

ASSET	SharePoint document canary	ACCOUNT	r.okafor@meridianhealth.org
FIRST SEEN	Jun 18, 2026 · 2:07 PM ET	ACTION	FileAccessed · no download

14:07:41	14:08:02	15:30:00	OPEN
Document accessed	Alert raised	Low confidence — monitoring	Watchlisted 30 days

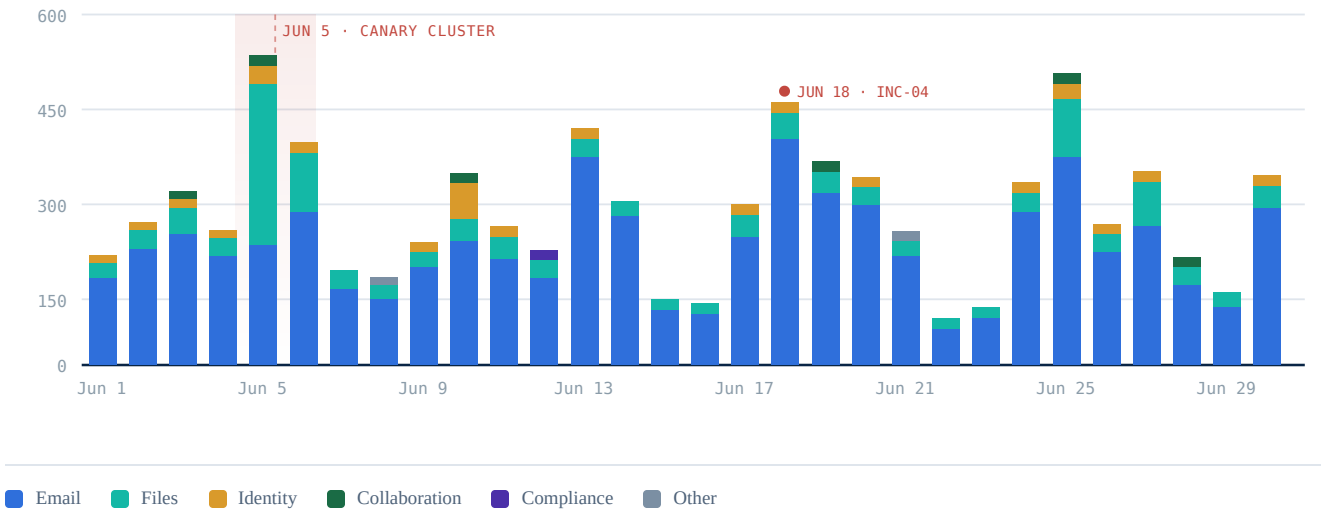
CARRYOVER ITEMS

23 items from prior periods remain active, all classified high severity. The oldest was first seen **March 27, 2026** — 95 days open as of this report. Full detail is tracked in the client portal. Carryover at this volume degrades triage quality on new signals; see recommended action P2.

03 What we examined

7,265 EVENTS · 5 WORKLOADS

DAILY AUDIT ACTIVITY BY WORKLOAD



NOTABLE MOVEMENT VS. YOUR BASELINE

▲ 183%

Extended file modifications

Sustained modification spikes are monitored for encryption-like patterns. This increase correlates with the June 5 canary cluster on the same account.

51 → 18
PRIOR PERIOD

▲ 50%

Files downloaded

Download volume is tracked against the tenant's rolling 90-day baseline. Within tolerance, but trending upward for a third consecutive period.

15 → 10
PRIOR PERIOD

▲ 39%

Full folder sync downloads

Bulk sync activity can indicate data staging ahead of exfiltration. All events traced to managed devices with compliant status.

25 → 18
PRIOR PERIOD

▼ 22%

Failed sign-in attempts

Reduction follows the Conditional Access policy tightening deployed in May. No password-spray patterns observed.

12 → 154
PRIOR PERIOD

04 Detections & coverage

3 DETECTIONS THIS PERIOD

DETECTION	SEVERITY	COUNT	DISPOSITION
Suspicious inbox rule	MEDIUM	1	Open — forwarding rule created Jun 5 on the affected mailbox, still active. Awaiting client confirmation of intent.
Impossible travel	LOW	1	Closed — benign. Traced to corporate VPN egress reassignment on Jun 12.
Legacy authentication attempt	LOW	1	Closed — blocked by Conditional Access. Source was an unmanaged mobile mail client.

COVERAGE & COLLECTION HEALTH

Telemetry days observed	30 / 30	Collector freshness	Jul 4, 11:05 AM ET
Unified Audit Log ingestion	Healthy	Entra ID sign-in ingestion	Healthy
Admin role changes	0 this period	Canary asset health	11 / 11 responding
High-signal operations tracked	13 daily	Mean time to alert	19 seconds

GLOSSARY

Canary — a decoy file or mailbox item that no legitimate workflow should touch. Access is a high-confidence signal of unauthorized activity.

Unified Audit Log — Microsoft 365's consolidated record of user and administrator activity across workloads.

Sign-in log — Entra ID's record of authentication attempts, including outcome, location, and client application.

Baseline — a rolling 90-day statistical profile of tenant activity, used to identify meaningful deviation.

Report limitations. Audit and sign-in data availability depends on Microsoft 365 telemetry latency and tenant collection health. Display times use Eastern Time; UTC query boundaries are retained in the report record. Findings reflect activity observable through Vortacity-held service telemetry and do not constitute a comprehensive assessment of tenant security posture.

BEHIND THIS REPORT

7,265	4,118	13	11
audit events scanned	sign-ins screened	high-signal operations tracked daily	deception assets maintained

vortacitycyber

REVIEWED AND FINALIZED BY A VORTACITY CYBER ANALYST
REPORT 4b5734f6-54dc-48e6-9616-fd87894e956d · REVISION 2 · TRAPLINE v0.2.0
GENERATED JUL 4, 2026 11:08 AM · FINALIZED JUL 4, 2026 11:10 AM ET
QUESTIONS? CONTACT YOUR VORTACITY CYBER ANALYST.