Microsoft 365 Forensic Triage Report

Generated: 2026-01-10T22:57:33.452502+00:00 • Coverage: ? → ? • Mode: deep • Case: INC-2026-001 • Client: EVILCORP • Analyst: MR ROBOT

This report is **read-only** and intended for **forensic preservation**. See the **Evidence** section for provenance, parameters, and export artifacts.

Overall risk

100

Score (0–100)

CRITICAL

Severity → weighting (Critical/High/Medium/Low)

Findings

126

Total

Critical: **0**

High: **59** Medium: **67** Low: **0**

Impacto

5

Usuarios afectados

7

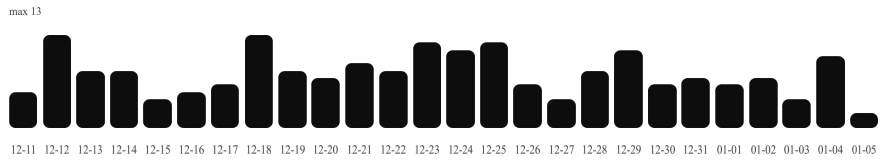
IPs involucradas

Dataset

7

Archivos

Volume per day (eventos)



Sign-ins, UAL and aggregated findings per day (when timestamps are available).

Severity distribution

Note: Only embedded findings are included (top severities + Critical: **0** High: **59** Medium: **67**

Findings (priority & evidence)

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Risky sign-in flagged by Entra risk fields** • risky_signin

HIGH **Legacy authentication / risky client protocol** • legacy_auth

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

HIGH **Suspicious Unified Audit Log operation** • ual_suspicious_operation

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Suspicious Unified Audit Log operation** • ual_suspicious_operation

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Suspicious Unified Audit Log operation** • ual_suspicious_operation

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Risky sign-in flagged by Entra risk fields** • risky_signin

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

MEDIUM **Suspicious Unified Audit Log operation** • ual_suspicious_operation

MEDIUM **Legacy authentication / risky client protocol** • legacy_auth

Note: This report embeds a subset (up to ~1500) to stay lightweight. Full datasets remain in findings.csv / triage.sqlite.

Timeline (hallazgos)

Events (chronological)

Time	Sev	Title	User
2025-12-11T12:09:00+00:00	high	Risky sign-in flagged by Entra risk fields	alice@acme.example
2025-12-11T12:09:00+00:00	medium	Legacy authentication / risky client protocol	alice@acme.example
2025-12-11T15:19:00+00:00	high	Legacy authentication / risky client protocol	cfo@acme.example
2025-12-11T18:24:00+00:00	medium	Legacy authentication / risky client protocol	cfo@acme.example
2025-12-11T21:25:00+00:00	high	Risky sign-in flagged by Entra risk fields	bob@acme.example
2025-12-11T21:25:00+00:00	medium	Legacy authentication / risky client protocol	bob@acme.example
2025-12-12T00:03:00+00:00	high	Risky sign-in flagged by Entra risk fields	cfo@acme.example
2025-12-12T00:03:00+00:00	medium	Legacy authentication / risky client protocol	cfo@acme.example
2025-12-12T02:32:00+00:00	medium	Legacy authentication / risky client protocol	svc.backup@acme.example
2025-12-12T04:49:00+00:00	high	Legacy authentication / risky client protocol	alice@acme.example

Heatmap (Sign-ins)

Day of week × hour (0–23). Useful to spot anomalous spikes.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	2
Sun	2	1		1	1	1		1	2	2	2	1	1	1	1	2	3		2	1	
Mon			2	3	1					1	1	3		3		1				1	
Tue	1	2		1	1		1	1		1		1		1	3	3		1		1	
Wed		1		3		1	1		1	1					1	1	1	1	1	1	
Thu	2	2			1	1	2	2	1	2	2	1	1			2	1		3	2	
Fri	2		3	2	3	3	2	1	2		1	1		1				1	3	2	
Sat	1	1			1					1	2					3		2	2		

Sign-ins

Top IPs con fallos

IP	Fails	Users
20.190.128.12	17	6
2.139.88.10	16	6
83.45.12.33	16	5
104.26.12.88	12	6
83.45.12.34	12	5
5.62.41.22	11	6
185.199.110.42	9	6

Typical password-spray indicator: one IP → many users.

Top users with failures

User	Fails
cfo@acme.example	20
it.admin@acme.example	19
alice@acme.example	14
svc.backup@acme.example	14
bob@acme.example	13

Typical brute-force indicator: one user → many IPs.

Audit (UAL) — BEC checklist

Forwarding / Redirect

4

Eventos

Top external domains

acme.example 8 **evil.example** 1

Inbox Rules sospechosas

1

Eventos

Revisa reglas de delete/hide/redirect/move.

Delegaciones / permisos

0

Eventos

Cambios de permisos y delegaciones s

BEC events (sample)

Time	User	IP	Operation	Ref
2025-12-21T23:32:00+00:00	alice@acme.example	83.45.12.33	Set-Mailbox	1:11
2025-12-22T03:59:00+00:00	bob@acme.example	185.199.110.42	Set-Mailbox	1:3
2025-12-26T00:47:00+00:00	bob@acme.example	83.45.12.33	New-InboxRule	1:25
2025-12-26T00:47:00+00:00	bob@acme.example	83.45.12.33	New-InboxRule	1:25
2026-01-04T07:24:00+00:00	alice@acme.example	5.62.41.22	Set-Mailbox	1:18

Evidence / Integridad

Inventario de archivos (hashes)

Conserva estos archivos en modo solo lectura. Verifica SHA-256 si haces copia/traslado.

Family	File	Rows	Start	End	SHA-256
signin	ApplicationSignIns_2025-11-22_2025-12-22.csv	20			cf51b97965d5725088774ef3643529c57245df2bd902cbe4c87a91b1
signin	InteractiveSignIns_2025-11-22_2025-12-22.csv	30			db7af86d9de0d3b6dd9b4eb4e16ed02638de66c194fdedc917fafb8eb
signin	InteractiveSignIns_AuthDetails_2025-11-22_2025-12-22.csv	30			6502d77d750cb193db12d0ee1373afe57eaaac084652b54791b2e038
signin	MSISignIns_2025-11-22_2025-12-22.csv	20			e4907fa5d1e695ac0ce96036e8225c9004bf23d7477a746e66c99565

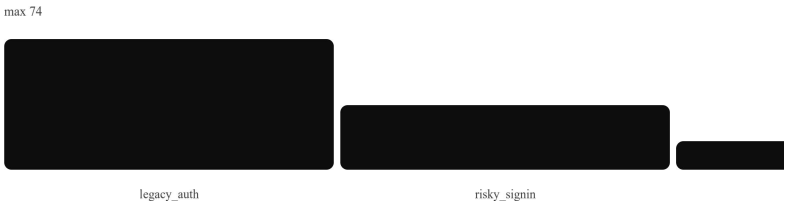
Family	File	Rows	Start	End	SHA-256
signin	NonInteractiveSignIns_2025-11-22_2025-12-22.csv	30			60cc65ee8cfd12678e2b88d281e24384ddb31e6439b5225ef480e903
signin	NonInteractiveSignIns_AuthDetails_2025-11-22_2025-12-22.csv	30			1edd7db6707c2f819d84545204843c0fde56501ef22bd04384cc9659
ual	14c46140-fbea-4e73-8385-a22688bc16e4.csv	40			f726c1273d2815c385796503b4222995566d8a6f015eb2a0c5219b82

Note: Raw identifiers may be partially redacted in the embedded dataset to reduce inadvertent disclosure. Full values are available in report_data.json if required.

Exports (para SOC / IR)

Archivos clave

Top categorías



Raw (Markdown)

Para copiado rápido, envío o anexado a ticket. También disponible como report.md.

```
# M365 Offline Forensic Triage Report

## Coverage
- Global start (UTC):
- Global end (UTC):

## Findings summary
| severity | count |
| -------- | ----- |
| medium   | 67    |
| high     | 59    |

## Top categories
| category               | count |
| ---------------------- | ----- |
| legacy_auth            | 74    |
| risky_signin           | 36    |
| ual_suspicious_operation | 16  |

## High severity findings (top 50)
| timestamp | category | title | user | ip | details |
| --- | --- | --- | --- | --- | --- |
| 2026-01-01T18:23:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | svc.backup@acme.example | 5.62.41.22 | risk_level=high risk_state=atRisk risk_detail=tokenIssuerAnomaly app=Azure Portal client=M |
| 2025-12-26T03:16:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | svc.backup@acme.example | 5.62.41.22 | risk_level=medium risk_state=atRisk risk_detail=tokenIssuerAnomaly app=Microsoft Teams c |
| 2025-12-14T14:07:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | cfo@acme.example | 5.62.41.22 | risk_level=medium risk_state=atRisk risk_detail=passwordSpray app=SharePoint Online client=B |
| 2025-12-21T11:21:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | bob@acme.example | 83.45.12.34 | risk_level=high risk_state=remediated risk_detail=passwordSpray app=Exchange Online client=( |
| 2025-12-11T21:25:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | bob@acme.example | 83.45.12.33 | risk_level=medium risk_state=remediated risk_detail=tokenIssuerAnomaly app=Azure Portal clie |
| 2026-01-03T15:01:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | bob@acme.example | 83.45.12.33 | risk_level=high risk_state=atRisk risk_detail=impossibleTravel app=SharePoint Online client=IM |
| 2025-12-29T02:40:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | cfo@acme.example | 20.190.128.12 | risk_level=high risk_state=atRisk risk_detail=passwordSpray app=Exchange Online client=Exch |
| 2025-12-20T17:18:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | it.admin@acme.example | 2.139.88.10 | risk_level=medium risk_state=remediated risk_detail=passwordSpray app=Azure Portal client= |
| 2025-12-19T19:10:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | bob@acme.example | 20.190.128.12 | risk_level=medium risk_state=confirmedSafe risk_detail=passwordSpray app=Azure Portal clie |
| 2025-12-12T00:03:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | cfo@acme.example | 104.26.12.88 | risk_level=medium risk_state=confirmedSafe risk_detail=tokenIssuerAnomaly app=Azure Portal |
| 2025-12-16T04:16:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | alice@acme.example | 20.190.128.12 | risk_level=medium risk_state=remediated risk_detail=anonymousIPAddress app=Microsoft 365 |
| 2025-12-13T21:36:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | bob@acme.example | 83.45.12.34 | risk_level=medium risk_state=confirmedSafe risk_detail=passwordSpray app=Microsoft Teams c |
| 2025-12-21T18:14:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | it.admin@acme.example | 104.26.12.88 | risk_level=medium risk_state=remediated risk_detail=tokenIssuerAnomaly app=Graph Explorc |
| 2025-12-24T21:00:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | bob@acme.example | 2.139.88.10 | risk_level=medium risk_state=atRisk risk_detail=anonymousIPAddress app=Exchange Online cl |
| 2025-12-11T12:09:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | alice@acme.example | 20.190.128.12 | risk_level=medium risk_state=atRisk risk_detail=impossibleTravel app=Microsoft Teams client |
| 2025-12-23T11:39:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | svc.backup@acme.example | 104.26.12.88 | risk_level=medium risk_state=remediated risk_detail=unfamiliarFeatures app=Azure Portal c |
| 2025-12-18T19:04:00+00:00 | risky_signin | Risky sign-in flagged by Entra risk fields | svc.backup@acme.example | 104.26.12.88 | risk_level=medium risk_state=remediated risk_detail=passwordSpray app=Azure Portal clien |
| 2025-12-12T21:47:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | bob@acme.example | 5.62.41.22 | legacy_client='Other clients' app='Graph Explorer' success=True |
| 2025-12-23T15:16:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | svc.backup@acme.example | 185.199.110.42 | legacy_client='Exchange ActiveSync' app='Azure Portal' success=True |
| 2026-01-03T00:56:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 185.199.110.42 | legacy_client='POP3' app='Microsoft 365 Admin Center' success=True |
| 2026-01-04T03:10:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | alice@acme.example | 185.199.110.42 | legacy_client='POP3' app='Exchange Online' success=True |
| 2025-12-29T13:12:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 185.199.110.42 | legacy_client='IMAP4' app='Microsoft 365 Admin Center' success=True |
| 2025-12-20T10:32:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 185.199.110.42 | legacy_client='Other clients' app='SharePoint Online' success=True |
| 2025-12-30T14:11:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 2.139.88.10 | legacy_client='Other clients' app='Exchange Online' success=True |
| 2025-12-20T17:18:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 2.139.88.10 | legacy_client='IMAP4' app='Azure Portal' success=True |
| 2025-12-18T08:10:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 5.62.41.22 | legacy_client='Other clients' app='Azure Portal' success=True |
| 2025-12-16T20:04:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 83.45.12.34 | legacy_client='Exchange ActiveSync' app='SharePoint Online' success=True |
| 2025-12-11T15:19:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 185.199.110.42 | legacy_client='IMAP4' app='Exchange Online' success=True |
| 2025-12-16T04:16:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | alice@acme.example | 20.190.128.12 | legacy_client='Exchange ActiveSync' app='Microsoft 365 Admin Center' success=True |
| 2025-12-28T21:32:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | bob@acme.example | 185.199.110.42 | legacy_client='Other clients' app='Microsoft Teams' success=True |
| 2025-12-16T15:07:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 5.62.41.22 | legacy_client='Other clients' app='Microsoft 365 Admin Center' success=True |
| 2025-12-20T15:55:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 83.45.12.33 | legacy_client='Other clients' app='Azure Portal' success=True |
| 2025-12-24T03:59:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | svc.backup@acme.example | 83.45.12.34 | legacy_client='Other clients' app='Exchange Online' success=True |
| 2025-12-13T18:42:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 83.45.12.34 | legacy_client='Other clients' app='Microsoft 365 Admin Center' success=True |
| 2025-12-13T04:05:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | bob@acme.example | 20.190.128.12 | legacy_client='Exchange ActiveSync' app='SharePoint Online' success=True |
| 2025-12-24T03:17:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 83.45.12.34 | legacy_client='POP3' app='Microsoft Teams' success=True |
| 2025-12-31T15:18:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 104.26.12.88 | legacy_client='IMAP4' app='Microsoft Teams' success=True |
| 2025-12-12T04:49:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | alice@acme.example | 83.45.12.34 | legacy_client='IMAP4' app='SharePoint Online' success=True |
| 2025-12-24T03:36:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | svc.backup@acme.example | 2.139.88.10 | legacy_client='Exchange ActiveSync' app='Graph Explorer' success=True |
| 2025-12-24T06:24:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | alice@acme.example | 185.199.110.42 | legacy_client='IMAP4' app='Exchange Online' success=True |
| 2025-12-12T17:02:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 5.62.41.22 | legacy_client='Exchange ActiveSync' app='Azure Portal' success=True |
| 2025-12-21T00:41:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | cfo@acme.example | 185.199.110.42 | legacy_client='Other clients' app='Microsoft 365 Admin Center' success=True |
| 2026-01-02T03:48:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | bob@acme.example | 83.45.12.34 | legacy_client='Exchange ActiveSync' app='Graph Explorer' success=True |
| 2025-12-23T07:31:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | it.admin@acme.example | 83.45.12.34 | legacy_client='POP3' app='Graph Explorer' success=True |
```

| 2025-12-28T21:51:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | alice@acme.example | 2.139.88.10 | legacy_client='Exchange ActiveSync' app='Microsoft Teams' success=True
| 2025-12-25T07:03:00+00:00 | legacy_auth | Legacy authentication / risky client protocol | alice@acme.example | 5.62.41.22 | legacy_client='IMAP4' app='Azure Portal' success=True
| 2025-12-22T03:59:00+00:00 | ual_suspicious_operation | Suspicious Unified Audit Log operation | bob@acme.example | 185.199.110.42 | operation=Set-Mailbox workload=Exchange record_type=1 forwarding_indicator=true
| 2025-12-13T21:30:00+00:00 | ual_suspicious_operation | Suspicious Unified Audit Log operation | svc.backup@acme.example | 20.190.128.12 | operation=Add service principal workload=AzureActiveDirectory record_type=8 dang
| 2025-12-12T15:14:00+00:00 | ual_suspicious_operation | Suspicious Unified Audit Log operation | bob@acme.example | 2.139.88.10 | operation=Consent to application workload=AzureActiveDirectory record_type=8 dangerc
| 2025-12-14T19:05:00+00:00 | ual_suspicious_operation | Suspicious Unified Audit Log operation | svc.backup@acme.example | 83.45.12.33 | operation=Consent to application workload=AzureActiveDirectory record_type=8 dang

Sign-in failures: top IPs
ip	fails
20.190.128.12	17
2.139.88.10	16
83.45.12.33	16
104.26.12.88	12
83.45.12.34	12
5.62.41.22	11
185.199.110.42	9

Sign-in failures: top users
user	fails
cfo@acme.example	20
it.admin@acme.example	19
alice@acme.example	14
svc.backup@acme.example	14
bob@acme.example	13

BEC indicators (summary)
- Forwarding-related events: 4
- Inbox-rule-related events: 1
- Delegation/permissions events: 0

Top external domains seen in forwarding artifacts
domain	count
acme.example	8
evil.example	1

Notes / Next steps
- Review HIGH findings first, then correlate with mailbox content checks, inbox rules, and suspicious OAuth consents.
- If you have additional logs (Defender for Office 365, Mailflow, EDR), ingest them for better correlation.

Generated by m365_triage v2.0.0 • 2026-01-10T22:57:33.452502+00:00