



NETWORKS
PLUS

compassONE
by blackpoint cyber

SAMPLE REPORT

Historical Scan Report

MS365 Findings, Risk Summary, and Guidance.

Tenant:

Scan Period: 26 May 2025 - 26 November 2025

Connection: microsoftteam1.onmicrosoft.com

Report Generated: 1 June 2026

Prepared By: Blackpoint Cyber

Report Summary

Historical Scan reviewed your Microsoft 365 audit logs and surfaced **three critical finding types (five detections total), all classified as malicious** — pointing to a likely account compromise with active Business Email Compromise (BEC) activity. Each will generate a Blackpoint Cyber Forensic Report in CompassOne.

The core threat is **mailbox manipulation from VPN-concealed sessions**: a suspicious inbox rule (2 detections) silently moved a specific sender's mail to Junk, and a forwarding rule (1 detection) quietly siphoned correspondence — both classic BEC techniques. Act today: delete the rules, reset credentials, revoke sessions, audit sent mail, and notify affected contacts.

The third finding needs verification: a sign-in to Outlook web from an **unmanaged iPhone in Toronto over a VPN tunnel** (2 detections). Confirm with the user, and escalate as account compromise if unconfirmed.

Overall, this is **active malicious activity requiring immediate response** — and it exposes real gaps: unmanaged devices reaching email and accounts open to silent rule/forwarding attacks. Close these with Conditional Access, MFA, and managed-device requirements.

Scan Outcome

3

Distinct Events Types

8

Total Events

3

⚠️

 Critical Events

5

Informational Events

Scan Scope and Coverage

101

Login Events Analyzed

95

Audit Logs Events Analyzed

112

Exchange Events Analyzed

89

SharePoint Events Analyzed

ⓘ

What this report is?

This is a historical threat analysis, not an incident response report. Historical Scan reviewed your Microsoft 365 environment's audit logs for the period above. No active attacker was detected and no automated remediation was performed. Findings below represent historical activity that warrants your awareness and action. Where we identified past security events, we have included technical detail and prioritized next steps.

**Login from New Device and IP** Critical

Detection ID: cloud-response/61525456-9881-4021-0571-6e8ee0ee8091 4/2/2026 1:09 PM ET

[View Detections](#)

2 detections

DETECTION STATUS

 **Malicious**

A Blackpoint Cyber Forensic Report will be generated for this finding. When ready, the completed report will be available in the Reports section of CompassOne.

 AI SOC Analysis (BROC)

A successful sign-in to Microsoft 365 occurred using a **mobile Safari browser on an iPhone**, accessing Outlook on the web. The login originated from Toronto, Canada (IP 23.162.200.198) via SUPERUNLIMITED_VPN, flagged with TUNNEL risk. The device was not compliant or managed. No failed attempts preceded the login and no downstream mailbox access anomalies were recorded in the session. While the location (Toronto) may align with the user's normal behavior, the combination of an unmanaged device, active VPN tunnel, and first-seen IP warrants review.

 User	 Application
malkan@blackpointcyberdev.onmicrosoft.com	One Outlook Web
 IP Address	 Location
23.162.200.198	Toronto, CA
 ISP / ASN	 Device
GLOBALTELEHOST Corp.	iPhone (iOS) - Safari • Not Managed
 VPN Enrichment	 Auth Result
SUPERUNLIMITED_VPN - Risk: TUNNEL	Success • ResultStatus: Redirect

MITRE ATT&CK mapping

Tactic: **Stealth (TA0005)** Technique: **Valid Accounts (T1078)**

Recommended Next Steps

-  **Toronto Login Verification & Escalation Alert**
Confirm with the user whether they were in Toronto on Nov 13 using a personal iPhone. If the user did not initiate this login, treat as a potential account compromise and escalate immediately.
-  **Exchange Session Activity Review (Post-Login Investigation)**
Review downstream Exchange activity for the session (Session ID: 00a9c79-(2fd-cOa5-1859-dd2489985fab) for any mailbox access, send events, or rule changes following this login.
-  **Conditional Access Policy Enforcement (Device & Location Controls)**
Enforce Conditional Access: Require compliant/managed devices for Outlook Web access. Block sign-ins from known VPN/proxy ranges where feasible.
-  **Mobile Device Compliance via Intune Enrollment**
Consider Intune enrollment for mobile devices used to access M365. The "not compliant, not managed" signal on this device is a policy gap regardless of this specific event. titles to each these messages

 **Suspicious Inbox Rule Created** Critical

Detection ID: cloud-response/61525456-9881-4021-0571-6e8ee0ee80914/2/2026 1:09 PM ET

[View Detections](#)

2 detections

DETECTION STATUS

 **Malicious**

A Blackpoint Cyber Forensic Report will be generated for this finding. When ready, the completed report will be available in the Reports section of CompassOne.

 AI SOC Analysis (BROC)

An inbox rule, "Move all messages from Jordan Bishop to Junk Email," was created on cshaw@llcu.org (Land of Lincoln Credit Union) from a session routed through a GLOBAL_PROTECT_CLOUD_VPN tunnel (Fidium, Waukeg, IA). Auto-filing a specific sender to Junk is a textbook Business Email Compromise technique to hide finance/vendor correspondence from the victim, and the VPN concealment reinforces malicious intent at a financial institution. Act today: delete the rule, reset credentials, revoke sessions, audit sent mail and other hidden rules, and notify affected correspondents.

 Mailbox / Actor	 Source IP
cshaw@llcu.org	74.0.48.83
 Destination Folder	 Policy Name
Junk Email	RFP
 Location	 ISP / ASN
Toronto, CA	Cisco OpenDNS, LLC

MITRE ATT&CK mapping

Tactic: **Stealth (TA0005)** Technique: **Valid Accounts (T1078)**

Recommended Next Steps

-  **Delete the Inbox Rule**
Immediately remove the suspicious rule from the affected mailbox.
-  **Reset Credentials & Revoke Sessions**
Reset the password and revoke sessions to evict the attacker.
-  **Audit Hidden Rules & Sent Mail**
Review for other hidden rules and outbound mail during the window.
-  **Notify Affected Correspondents**
Warn finance and vendor contacts referenced by the rule of possible BEC.
-  **Block Source Range**
Add the VPN/source range to Conditional Access named locations.



Internal Email Forwarding Rule Created Critical

Detection ID: cloud-response/61525456-9881-4021-0571-6e8ee0ee8091

4/2/2026 1:09 PM ET

1

detections

[View Detections](#)

DETECTION STATUS

 **Malicious**

A Blackpoint Cyber Forensic Report will be generated for this finding. When ready, the completed report will be available in the Reports section of CompassOne.

 AI SOC Analysis (BROC)

An inbox rule on mlawrence@ptssite.com (Production Technology and Services) forwards mail to internal addresses lhoff@ and ahoff@ptssite.com, created from Baton Rouge, LA (Cox). Even internal forwarding can be used by an attacker to silently collect a target's correspondence within the tenant. Treat as possible collection activity: confirm the rule was user-created and authorized; if not, remove it, reset the mailbox, and review for additional hidden rules.

 Mailbox / Actor	 Forwarding Address(es)
cshaw@llcu.org	salvarez@22beacon.org
 Location	 ISP / ASN
Toronto, CA	Cisco OpenDNS, LLC
 Source IP	
74.0.48.83	

MITRE ATT&CK mapping

Tactic: **Stealth (TA0005)**

Technique: **Valid Accounts (T1078)**

Recommended Next Steps

-  **Confirm Rule Authorization**
Verify the user created the internal forwarding rule intentionally.
-  **Remove if Unauthorized**
Delete the rule if it was not user-initiated.
-  **Audit for Hidden Rules**
Check the mailbox for additional concealed rules.
-  **Reset if Suspicious**
Reset the mailbox credentials if compromise is suspected.