swisscom

☎ 24/7 CSIRT Hotline 0800 850 000

Next-Gen IR: Swisscom’s Framework for Microsoft 365

October 28, 2025, Angelo Violetti

C1 Public

Who am I – Angelo Violetti

Experience

5+ of experience in Digital Forensics and Incident Response

Job

Senior DFIR Analyst @Swisscom CSIRT

Contribution

Threat Intelligence Analyst and Contributor @ The DFIR Report

Degree

BSc in Computer Engineering and MSc in Cyber Security

Certifications

AWS & Azure Incident Response Certifications, Certified Forensic Analyst (GCFA) and Red Team Operator (CRTO)

Speaker

Speaker at Defcon 32 Blue Team Village, SANS Ransomware Summit 2025, etc.

Microsoft 365 Cyber Threats

Microsoft 365

Emerging and Main Cyber Threats

Adversary in The Middle

Internal and External Spear phishing

Financial Frauds

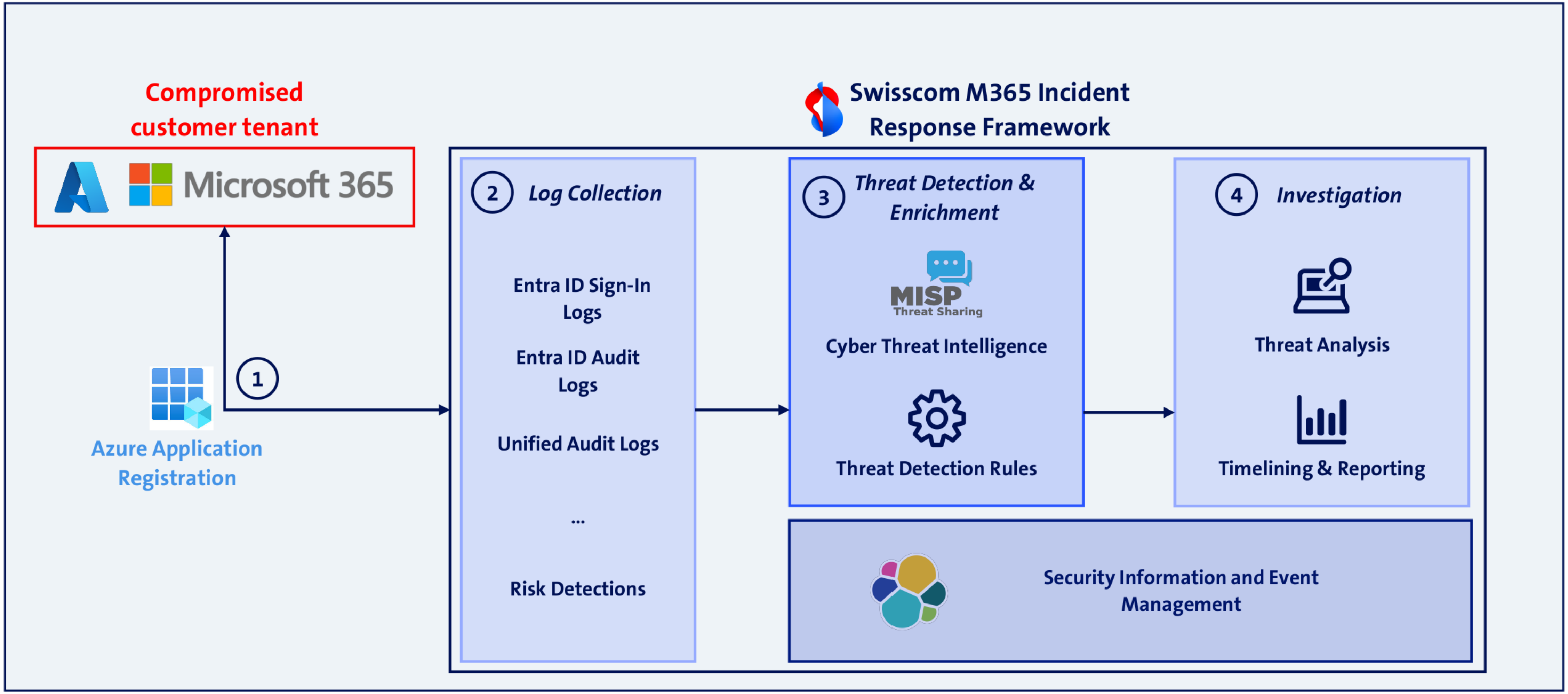
Data Exfiltration

M365 Copilot Vulnerabilities

Reference: Aim Security - Breaking down 'EchoLeak', the First Zero-Click AI Vulnerability Enabling Data Exfiltration from Microsoft 365 Copilot

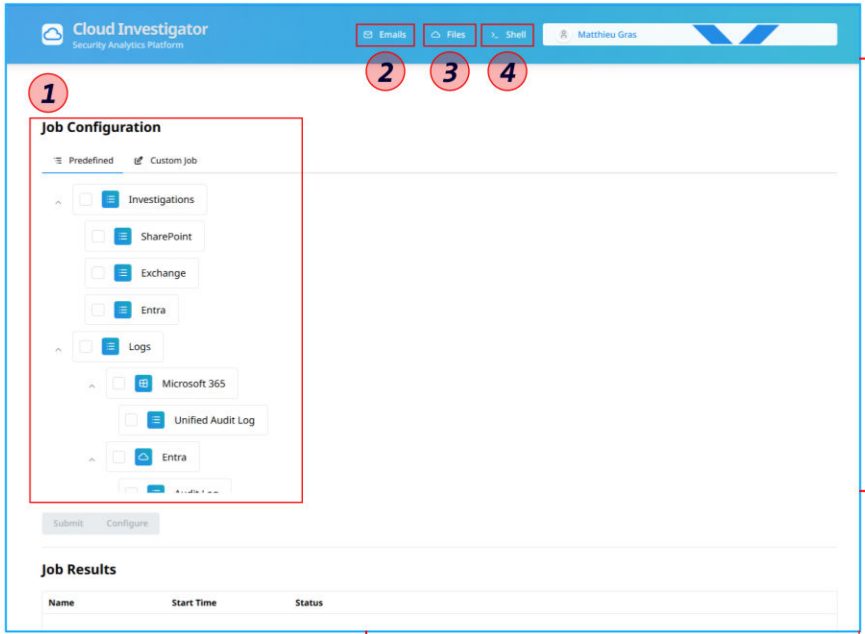
Swisscom IR Framework for Azure & Microsoft 365

M365 Incident Response Workflow

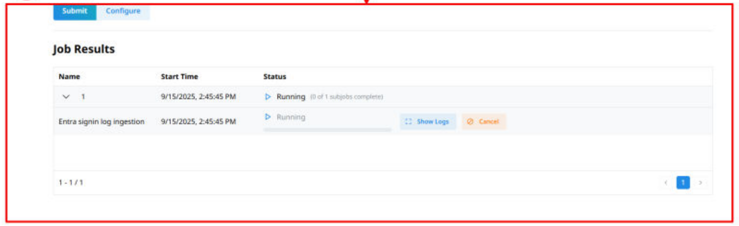


Angelo Violetti, October 28, 2025, Next-Gen IR: Swisscom's Framework for Microsoft 365, C1 Public

Cloud Investigator – Features Overview



1 Log Collection

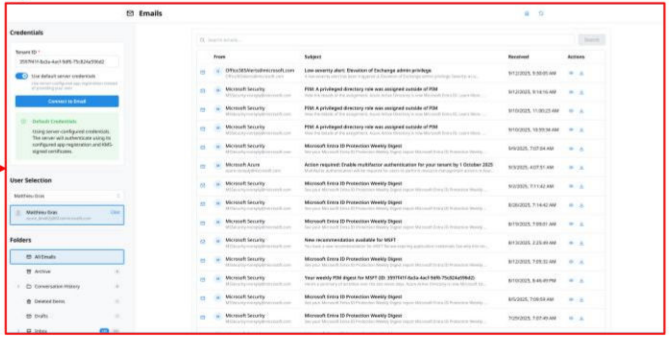


Job Results

Name	Start Time	Status
⌄ 1	9/15/2025, 2:45:45 PM	▷ Running (0 of 1 subjobs complete)
Entra signin log ingestion	9/15/2025, 2:45:45 PM	▷ Running Show Logs Cancel

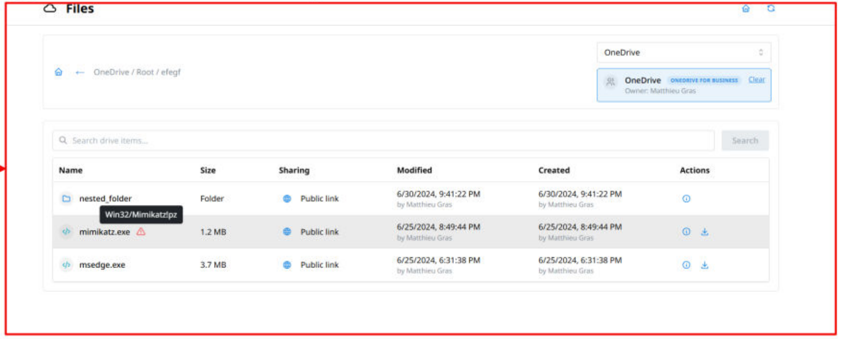
1 - 1 / 1

2 E-Mail Client


Emails
Credentials
Tenant ID *
3597f41f-8a3a-4acf-9df6-75c824a596d2
Use default server credentials
Connect to Email
Default Credentials
Using server-configured credentials. The server will authenticate using its configured app registration and KMS-signed certificates.
User Selection
Matthieu Gras
Matthieu Gras
Clear
Folders
All Emails
Archive
Conversation History
Deleted Items
Drafts
Inbox
Search emails...
Search

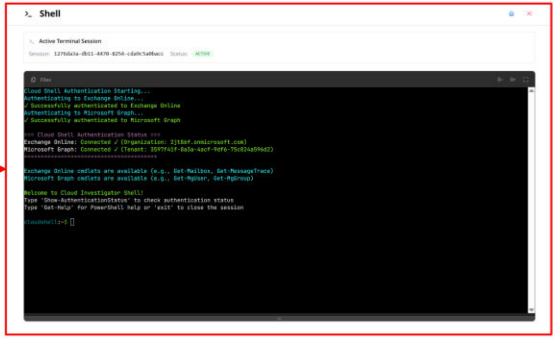
From	Subject	Received	Actions
Office365Alerts@microsoft.com	Low severity alert: Elevation of Exchange admin privilege	9/12/2025, 9:30:05 AM	
Microsoft Security	PIM: A privileged directory role was assigned outside of PIM	9/12/2025, 9:14:16 AM	
Microsoft Security	PIM: A privileged directory role was assigned outside of PIM	9/10/2025, 11:00:23 AM	
Microsoft Security	PIM: A privileged directory role was assigned outside of PIM	9/10/2025, 10:59:34 AM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	9/9/2025, 7:07:04 AM	
Microsoft Azure	Action required: Enable multifactor authentication for your tenant by 1 October 2025	9/3/2025, 4:07:51 AM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	9/2/2025, 7:11:42 AM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	8/26/2025, 7:14:42 AM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	8/19/2025, 7:09:01 AM	
Microsoft Security	New recommendation available for MSFT	8/13/2025, 2:25:49 AM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	8/12/2025, 7:09:32 AM	
Microsoft Security	Your weekly PIM digest for MSFT (ID: 3597f41f-8a3a-4acf-9df6-75c824a596d2)	8/10/2025, 8:46:49 PM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	8/5/2025, 7:09:59 AM	
Microsoft Security	Microsoft Entra ID Protection Weekly Digest	7/29/2025, 7:07:49 AM	

3 OneDrive Files Navigation



Name	Size	Sharing	Modified	Created	Actions
nested_folder	Folder	Public link	6/30/2024, 9:41:22 PM by Matthieu Gras	6/30/2024, 9:41:22 PM by Matthieu Gras	
mimikatz.exe ⚠	1.2 MB	Public link	6/25/2024, 8:49:44 PM by Matthieu Gras	6/25/2024, 8:49:44 PM by Matthieu Gras	
msedge.exe	3.7 MB	Public link	6/25/2024, 6:31:38 PM by Matthieu Gras	6/25/2024, 6:31:38 PM by Matthieu Gras	

4 Cloud Shell

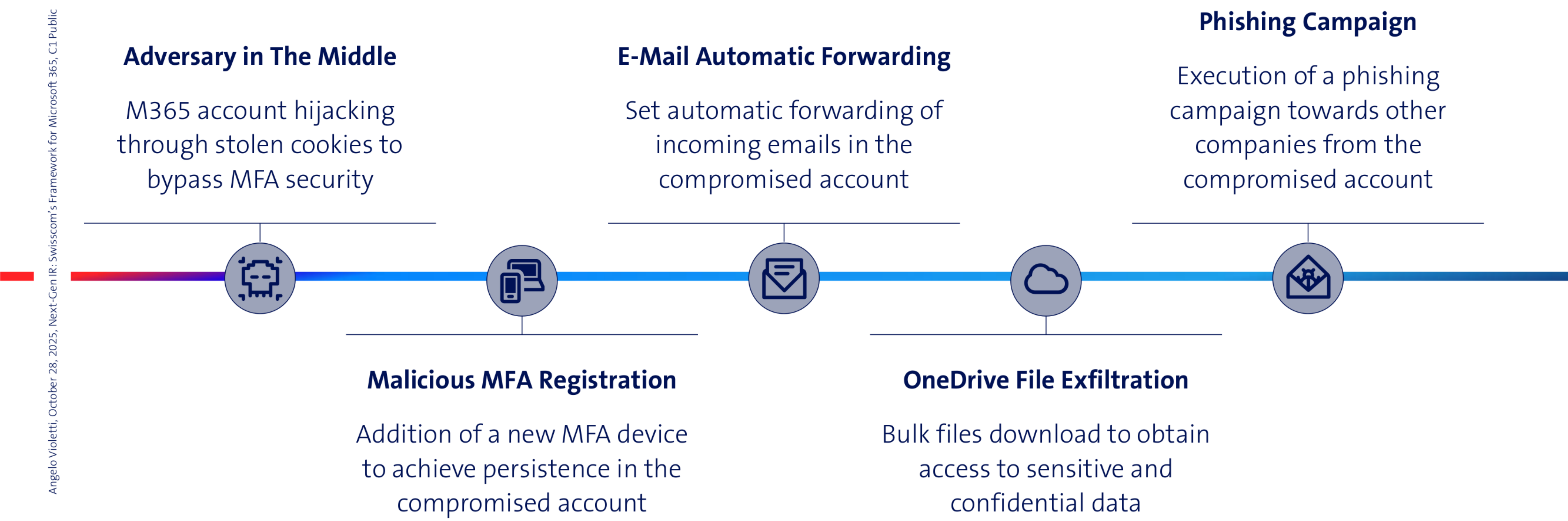


Active Terminal Session

Session: 1276da3a-db11-4470-8254-cda0c5a0bacc Status: ACTIVE

```
Cloud Shell Authentication Starting...
Authenticating to Exchange Online...
✓ Successfully authenticated to Exchange Online
Authenticating to Microsoft Graph...
✓ Successfully authenticated to Microsoft Graph

=== Cloud Shell Authentication Status ===
Exchange Online: Connected ✓ (Organization: 2jt86f.onmicrosoft.com)
Microsoft Graph: Connected ✓ (Tenant: 3597f41f-8a3a-4acf-9df6-75c824a596d2)
========================================

Exchange Online cmdlets are available (e.g., Get-Mailbox, Get-MessageTrace)
Microsoft Graph cmdlets are available (e.g., Get-MgUser, Get-MgGroup)

Welcome to Cloud Investigator Shell!
Type 'Show-AuthenticationStatus' to check authentication status
Type 'Get-Help' for PowerShell help or 'exit' to close the session

cloudshell:~$ 
```

Real-World Microsoft 365 Incident Response Scenario



Adversary in The Middle

M365 account hijacking through stolen cookies to bypass MFA security

Malicious MFA Registration

Addition of a new MFA device to achieve persistence in the compromised account

E-Mail Automatic Forwarding

Set automatic forwarding of incoming emails in the compromised account

OneDrive File Exfiltration

Bulk files download to obtain access to sensitive and confidential data

Phishing Campaign

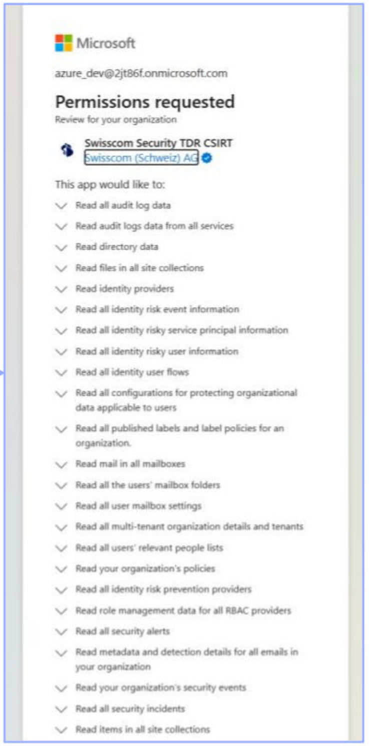
Execution of a phishing campaign towards other companies from the compromised account

Azure Application Registration

Swisscom TDR CSIRT Application Registration

Azure Application Registration

Global Admin clicks on a URL provided by CSIRT



Microsoft

azure_dev@2jt86f.onmicrosoft.com

Permissions requested

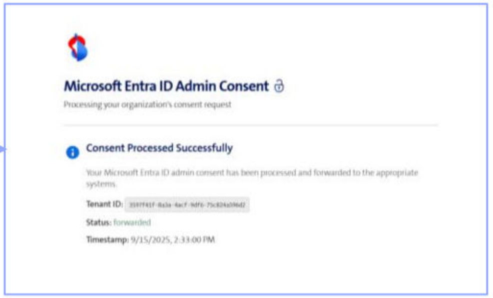
Review for your organization

Swisscom Security TDR CSIRT
Swisscom (Schweiz) AG

This app would like to:

- Read all audit log data
- Read audit logs data from all services
- Read directory data
- Read files in all site collections
- Read identity providers
- Read all identity risk event information
- Read all identity risky service principal information
- Read all identity risky user information
- Read all identity user flows
- Read all configurations for protecting organizational data applicable to users
- Read all published labels and label policies for an organization.
- Read mail in all mailboxes
- Read all the users' mailbox folders
- Read all user mailbox settings
- Read all multi-tenant organization details and tenants
- Read all users' relevant people lists
- Read your organization's policies
- Read all identity risk prevention providers
- Read role management data for all RBAC providers
- Read all security alerts
- Read metadata and detection details for all emails in your organization
- Read your organization's security events
- Read all security incidents
- Read items in all site collections

Global Admin registers the CSIRT application



Microsoft Entra ID Admin Consent

Processing your organization's consent request

Consent Processed Successfully

Your Microsoft Entra ID admin consent has been processed and forwarded to the appropriate systems.

Tenant ID: [illegible]

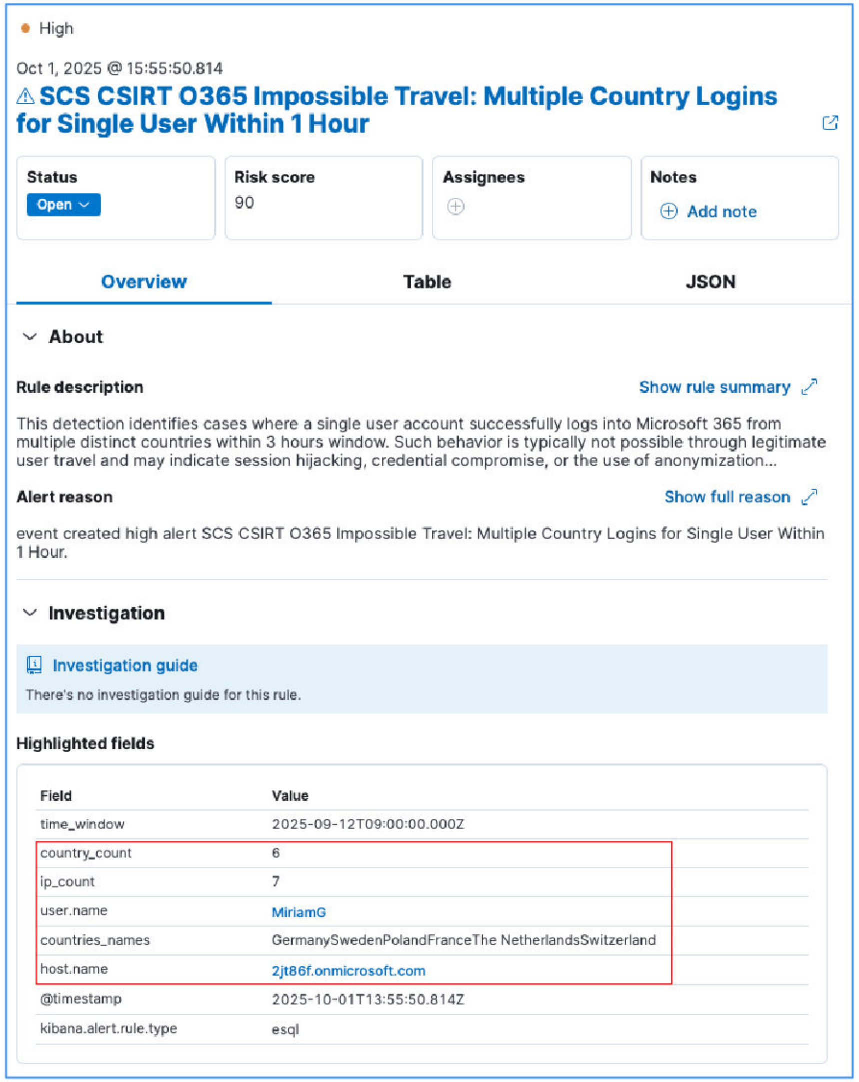
Status: forwarded

Timestamp: 9/15/2025, 2:33:00 PM

AiTM (Adversary-in-the-Middle) is a cyberattack that takes place when a threat actor acts as a proxy between a user and a service (like Microsoft 365) to bypass multi-factor authentication and steal session cookies.

Adversary in The Middle

M365 Incident Response – Adversary in The Middle (1/2)



● High

Oct 1, 2025 @ 15:55:50.814

⚠ SCS CSIRT O365 Impossible Travel: Multiple Country Logins for Single User Within 1 Hour

Status	Risk score	Assignees	Notes
Open	90	⊕	⊕ Add note

About

Rule description — Show rule summary

This detection identifies cases where a single user account successfully logs into Microsoft 365 from multiple distinct countries within 3 hours window. Such behavior is typically not possible through legitimate user travel and may indicate session hijacking, credential compromise, or the use of anonymization...

Alert reason — Show full reason

event created high alert SCS CSIRT O365 Impossible Travel: Multiple Country Logins for Single User Within 1 Hour.

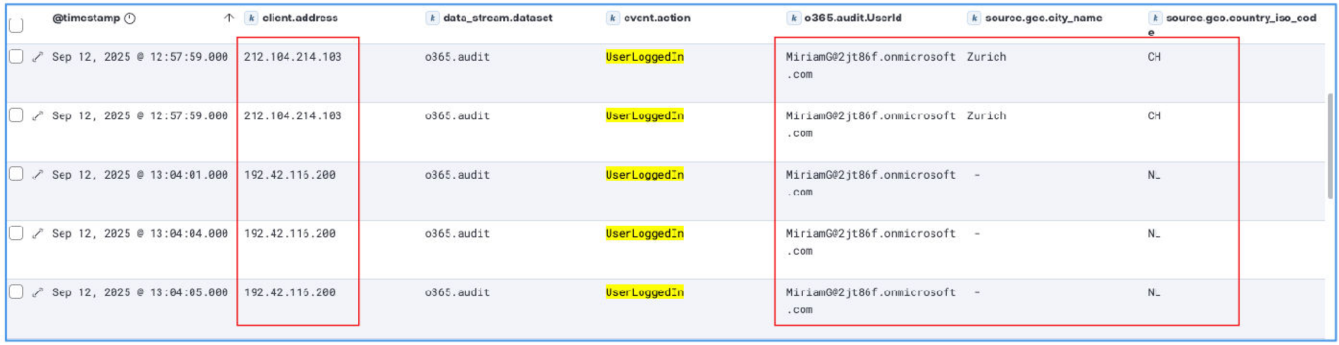
Investigation

Investigation guide

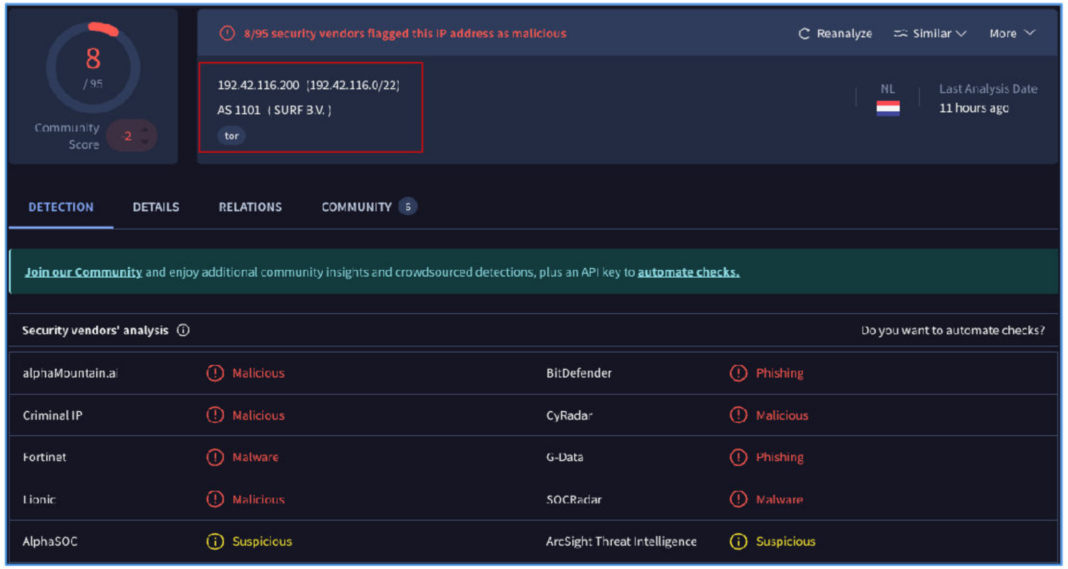
There's no investigation guide for this rule.

Highlighted fields

Field	Value
time_window	2025-09-12T09:00:00.000Z
country_count	6
ip_count	7
user.name	MiriamG
countries_names	GermanySwedenPolandFranceThe NetherlandsSwitzerland
host.name	2jt86f.onmicrosoft.com
@timestamp	2025-10-01T13:55:50.814Z
kibana.alert.rule.type	esql



@timestamp	client.address	data_stream.dataset	event.action	o365.audit.UserId	source.geo.city_name	source.geo.country_iso_code
Sep 12, 2025 @ 12:57:59.000	212.104.214.103	o365.audit	UserLoggedIn	MiriamG@2jt86f.onmicrosoft.com	Zurich	CH
Sep 12, 2025 @ 12:57:59.000	212.104.214.103	o365.audit	UserLoggedIn	MiriamG@2jt86f.onmicrosoft.com	Zurich	CH
Sep 12, 2025 @ 13:04:01.000	192.42.116.200	o365.audit	UserLoggedIn	MiriamG@2jt86f.onmicrosoft.com	-	N_
Sep 12, 2025 @ 13:04:04.000	192.42.116.200	o365.audit	UserLoggedIn	MiriamG@2jt86f.onmicrosoft.com	-	N_
Sep 12, 2025 @ 13:04:05.000	192.42.116.200	o365.audit	UserLoggedIn	MiriamG@2jt86f.onmicrosoft.com	-	N_



8/95 security vendors flagged this IP address as malicious

192.42.116.200 (192.42.116.0/22)
AS 1101 (SURF B.V.)
tor

NL

Last Analysis Date
11 hours ago

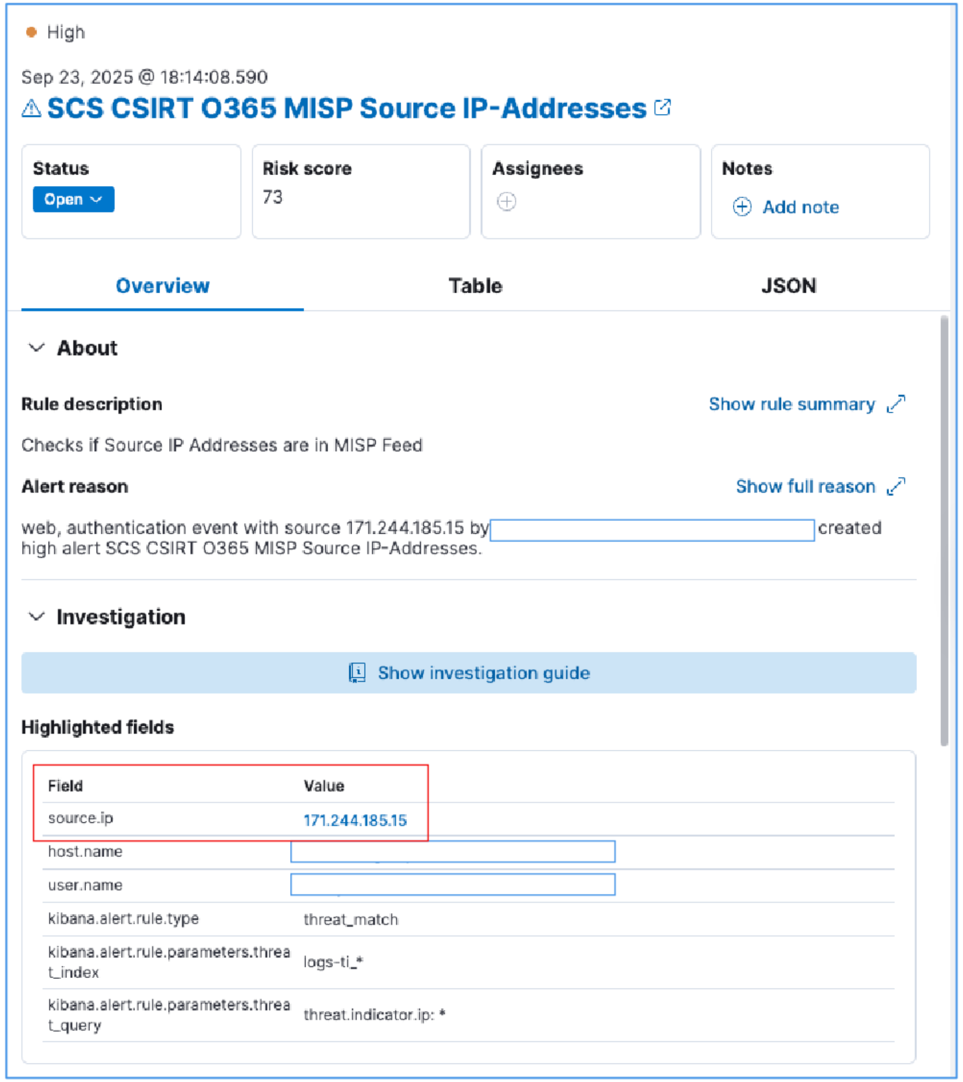
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Phishing
Criminal IP	Malicious	CyRadar	Malicious
Fortinet	Malware	G-Data	Phishing
Lionic	Malicious	SOCRadar	Malware
AlphaSOC	Suspicious	ArcSight Threat Intelligence	Suspicious

M365 Incident Response – Adversary in The Middle (2/2)



● High

Sep 23, 2025 @ 18:14:08.590

⚠ SCS CSIRT O365 MISP Source IP-Addresses

Status	Risk score	Assignees	Notes
Open	73	⊕	⊕ Add note

About

Rule description Show rule summary

Checks if Source IP Addresses are in MISP Feed

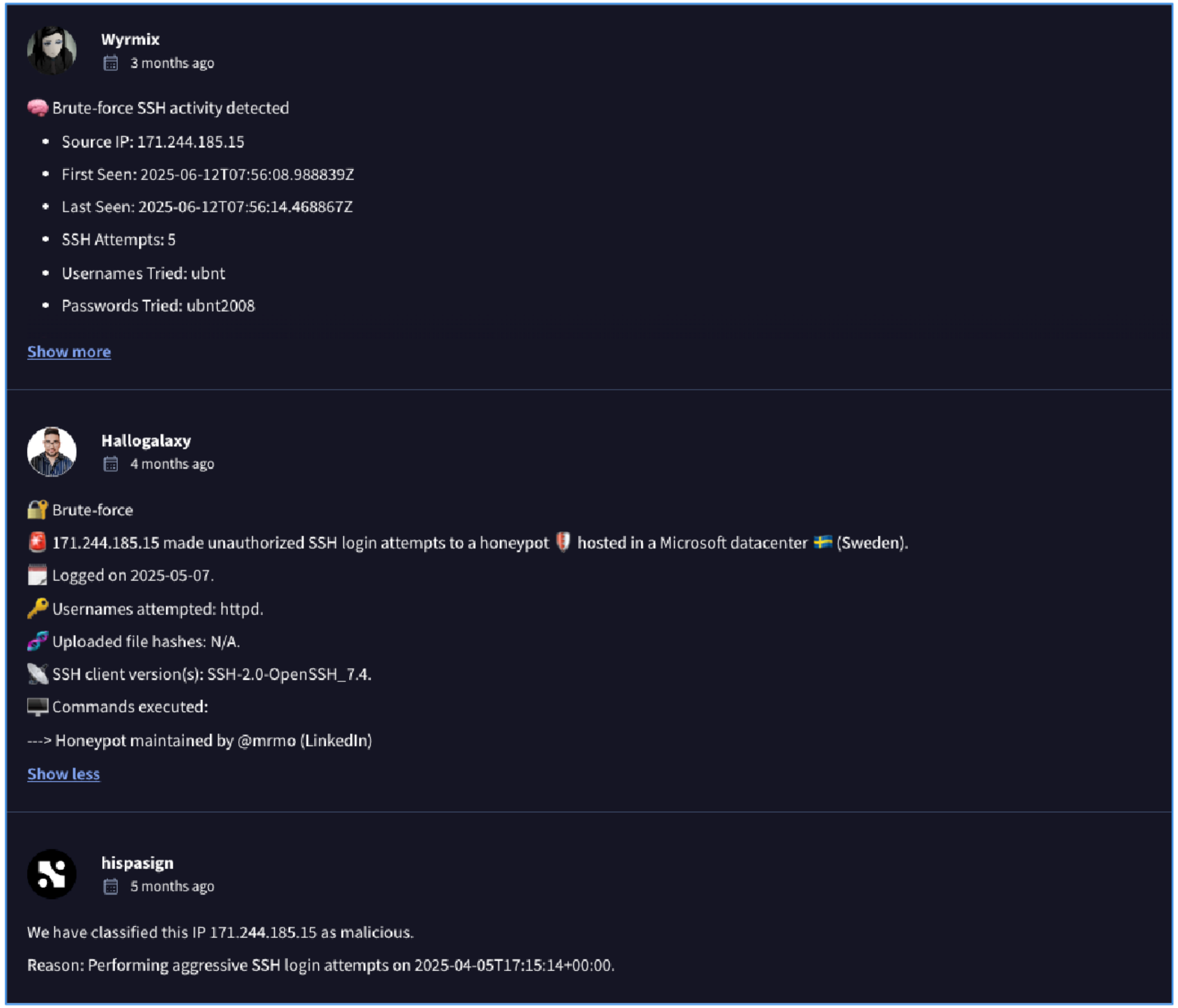
Alert reason Show full reason

web, authentication event with source 171.244.185.15 by [redacted] created high alert SCS CSIRT O365 MISP Source IP-Addresses.

Investigation

Highlighted fields

Field	Value
source.ip	171.244.185.15
host.name	[redacted]
user.name	[redacted]
kibana.alert.rule.type	threat_match
kibana.alert.rule.parameters.threat_index	logs-ti_*
kibana.alert.rule.parameters.threat_query	threat.indicator.ip: *



Wyrmix
🗓 3 months ago

🧠 Brute-force SSH activity detected

- Source IP: 171.244.185.15
- First Seen: 2025-06-12T07:56:08.988839Z
- Last Seen: 2025-06-12T07:56:14.468867Z
- SSH Attempts: 5
- Usernames Tried: ubnt
- Passwords Tried: ubnt2008

Show more

Hallogalaxy
🗓 4 months ago

🔐 Brute-force

🚨 171.244.185.15 made unauthorized SSH login attempts to a honeypot 🛡 hosted in a Microsoft datacenter 🇸🇪 (Sweden).

🗓 Logged on 2025-05-07.

🔑 Usernames attempted: httpd.

🧬 Uploaded file hashes: N/A.

📡 SSH client version(s): SSH-2.0-OpenSSH_7.4.

🖥 Commands executed:

---> Honeypot maintained by @mrmo (LinkedIn)

Show less

hispasign
🗓 5 months ago

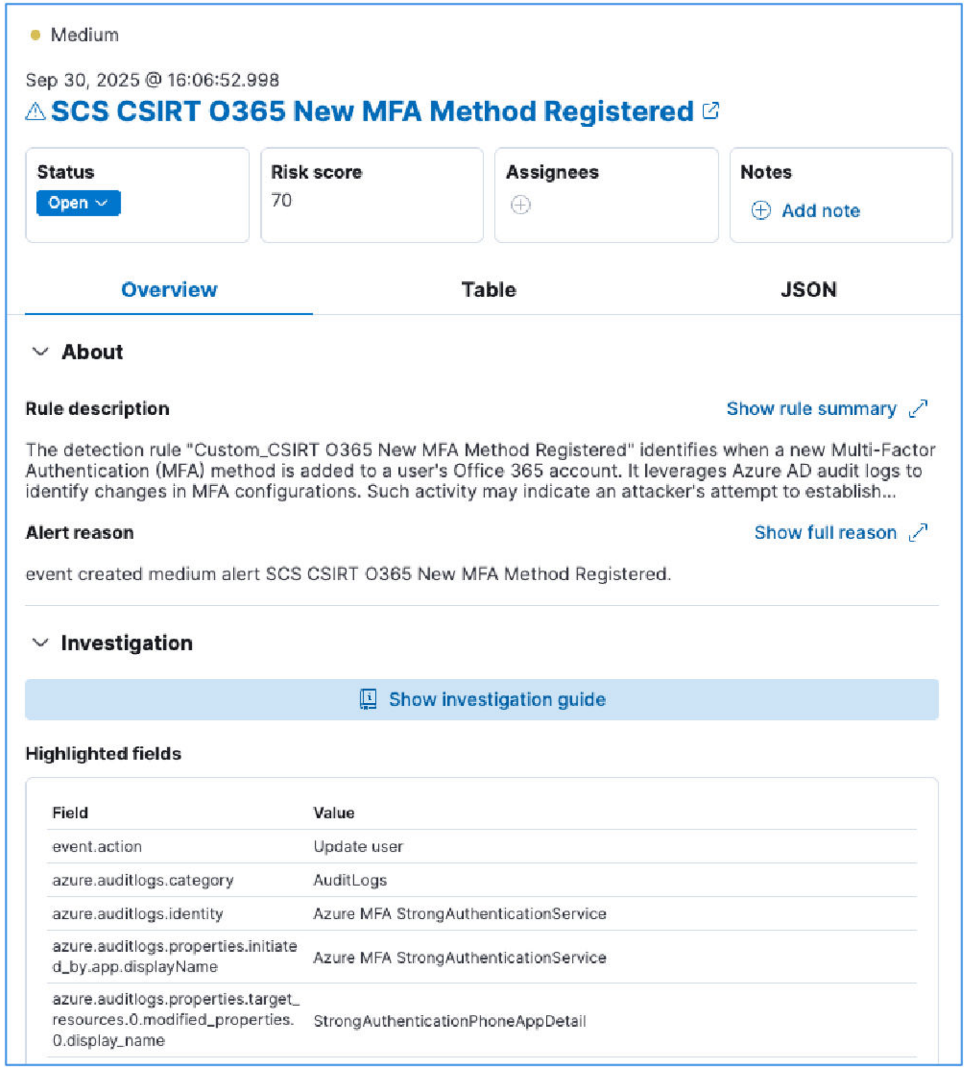
We have classified this IP 171.244.185.15 as malicious.

Reason: Performing aggressive SSH login attempts on 2025-04-05T17:15:14+00:00.

Threat actors exploit a stolen session to register a new MFA device they control by creating a persistent backdoor. This allows them to bypass the user’s legitimate MFA, gaining long-term access to the account.

MFA Registration

M365 Incident Response – MFA Registration



● Medium

Sep 30, 2025 @ 16:06:52.998

⚠ **SCS CSIRT O365 New MFA Method Registered**

Status	Risk score	Assignees	Notes
Open	70	⊕	⊕ Add note

About

Rule description Show rule summary

The detection rule "Custom_CSIRT O365 New MFA Method Registered" identifies when a new Multi-Factor Authentication (MFA) method is added to a user's Office 365 account. It leverages Azure AD audit logs to identify changes in MFA configurations. Such activity may indicate an attacker's attempt to establish...

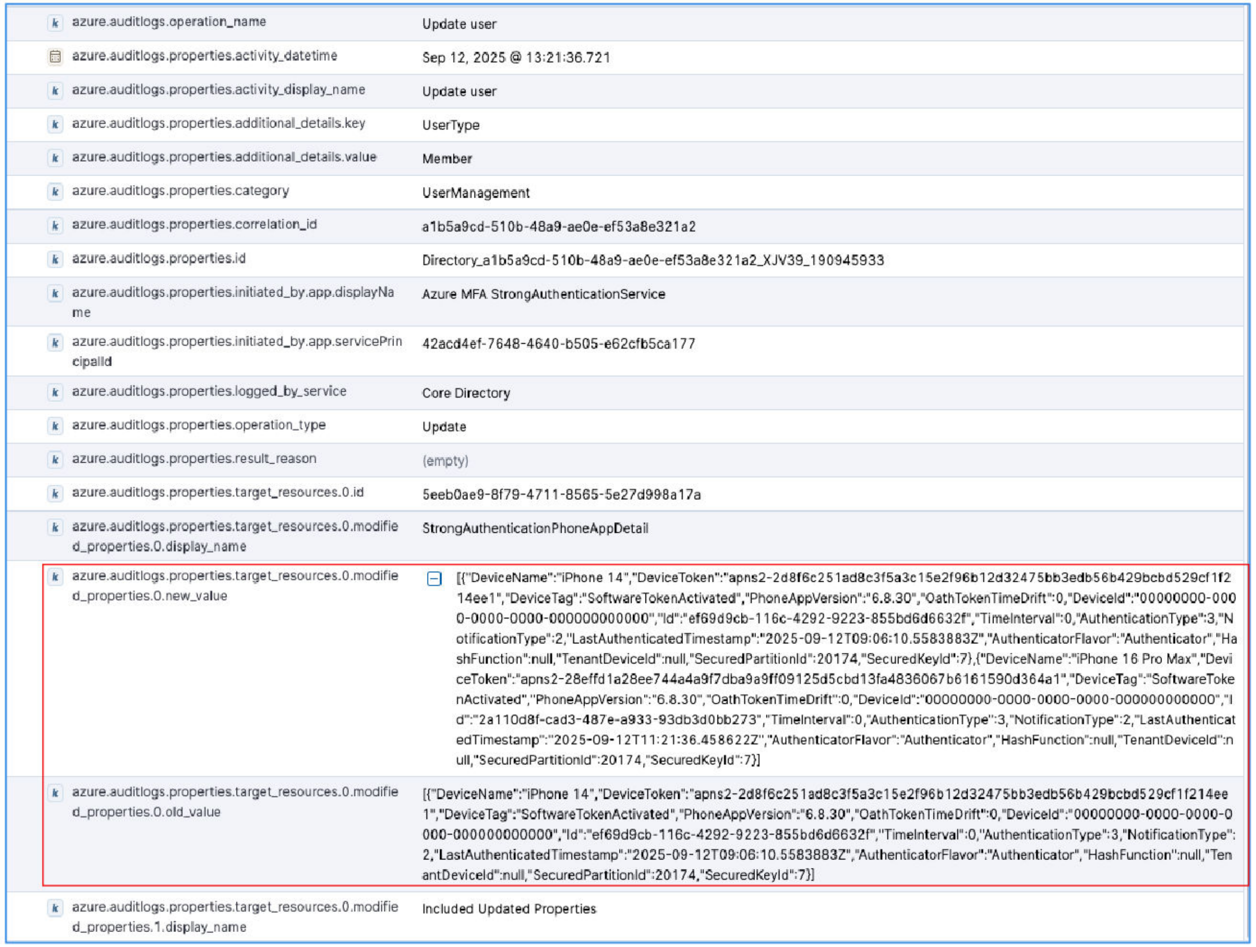
Alert reason Show full reason

event created medium alert SCS CSIRT O365 New MFA Method Registered.

Investigation

Highlighted fields

Field	Value
event.action	Update user
azure.auditlogs.category	AuditLogs
azure.auditlogs.identity	Azure MFA StrongAuthenticationService
azure.auditlogs.properties.initiated_by.app.displayName	Azure MFA StrongAuthenticationService
azure.auditlogs.properties.target_resources.0.modified_properties.0.display_name	StrongAuthenticationPhoneAppDetail

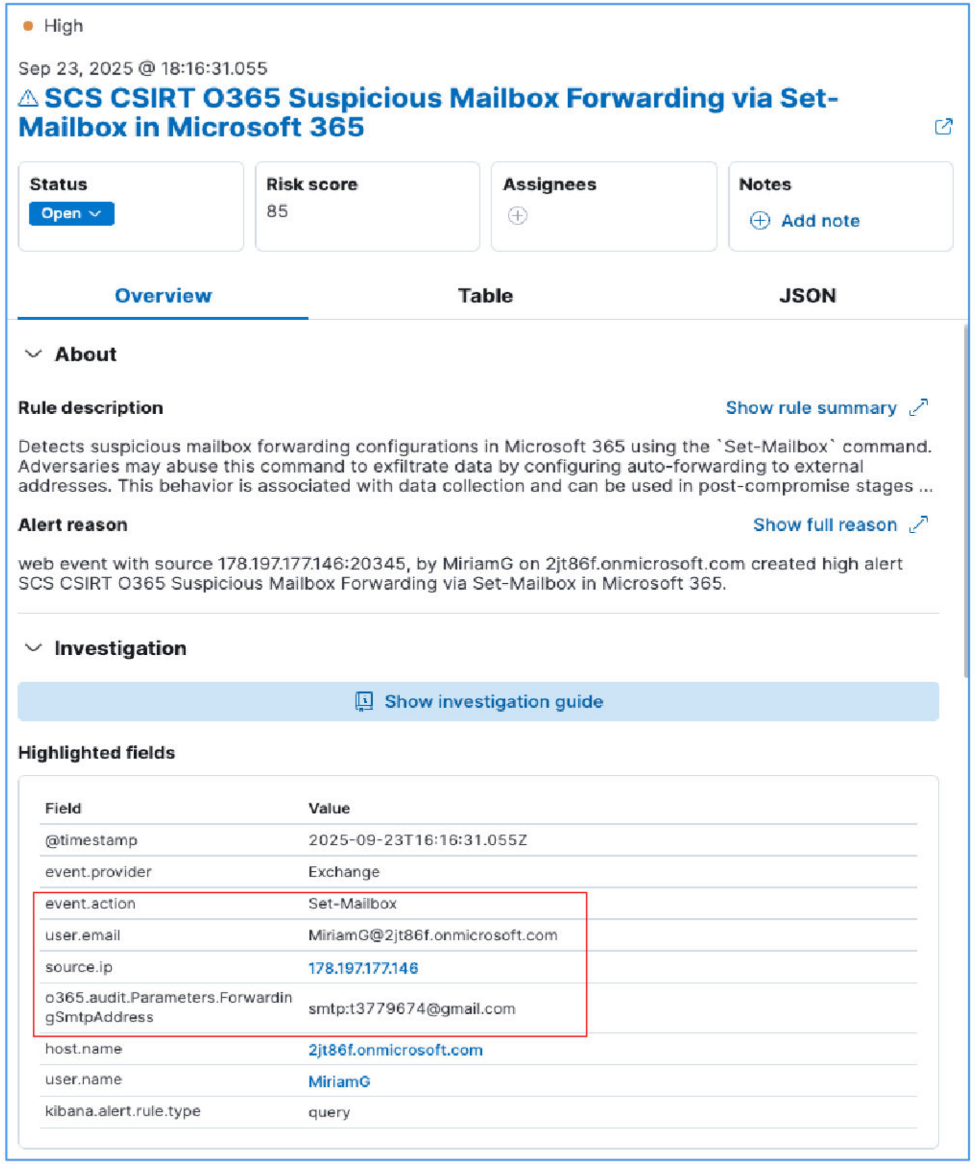


azure.auditlogs.operation_name	Update user
azure.auditlogs.properties.activity_datetime	Sep 12, 2025 @ 13:21:36.721
azure.auditlogs.properties.activity_display_name	Update user
azure.auditlogs.properties.additional_details.key	UserType
azure.auditlogs.properties.additional_details.value	Member
azure.auditlogs.properties.category	UserManagement
azure.auditlogs.properties.correlation_id	a1b5a9cd-510b-48a9-ae0e-ef53a8e321a2
azure.auditlogs.properties.id	Directory_a1b5a9cd-510b-48a9-ae0e-ef53a8e321a2_XJV39_190945933
azure.auditlogs.properties.initiated_by.app.displayName	Azure MFA StrongAuthenticationService
azure.auditlogs.properties.initiated_by.app.servicePrincipalId	42acd4ef-7648-4640-b505-e62cfb5ca177
azure.auditlogs.properties.logged_by_service	Core Directory
azure.auditlogs.properties.operation_type	Update
azure.auditlogs.properties.result_reason	(empty)
azure.auditlogs.properties.target_resources.0.id	5eeb0ae9-8f79-4711-8565-5e27d998a17a
azure.auditlogs.properties.target_resources.0.modified_properties.0.display_name	StrongAuthenticationPhoneAppDetail
azure.auditlogs.properties.target_resources.0.modified_properties.0.new_value	⊟ [{"DeviceName":"iPhone 14","DeviceToken":"apns2-2d8f6c251ad8c3f5a3c15e2f96b12d32475bb3edb56b429bcbd529cf1f214ee1","DeviceTag":"SoftwareTokenActivated","PhoneAppVersion":"6.8.30","OathTokenTimeDrift":0,"DeviceId":"00000000-0000-0000-0000-000000000000","Id":"ef69d9cb-116c-4292-9223-855bd6d6632f","TimeInterval":0,"AuthenticationType":3,"NotificationType":2,"LastAuthenticatedTimestamp":"2025-09-12T09:06:10.5583883Z","AuthenticatorFlavor":"Authenticator","HashFunction":null,"TenantDeviceId":null,"SecuredPartitionId":20174,"SecuredKeyId":7},{"DeviceName":"iPhone 16 Pro Max","DeviceToken":"apns2-28effd1a28ee744a4a9f7dba9a9ff09125d5cbd13fa4836067b6161590d364a1","DeviceTag":"SoftwareTokenActivated","PhoneAppVersion":"6.8.30","OathTokenTimeDrift":0,"DeviceId":"00000000-0000-0000-0000-000000000000","Id":"2a110d8f-cad3-487e-a933-93db3d0bb273","TimeInterval":0,"AuthenticationType":3,"NotificationType":2,"LastAuthenticatedTimestamp":"2025-09-12T11:21:36.458622Z","AuthenticatorFlavor":"Authenticator","HashFunction":null,"TenantDeviceId":null,"SecuredPartitionId":20174,"SecuredKeyId":7}]
azure.auditlogs.properties.target_resources.0.modified_properties.0.old_value	[{"DeviceName":"iPhone 14","DeviceToken":"apns2-2d8f6c251ad8c3f5a3c15e2f96b12d32475bb3edb56b429bcbd529cf1f214ee1","DeviceTag":"SoftwareTokenActivated","PhoneAppVersion":"6.8.30","OathTokenTimeDrift":0,"DeviceId":"00000000-0000-0000-0000-000000000000","Id":"ef69d9cb-116c-4292-9223-855bd6d6632f","TimeInterval":0,"AuthenticationType":3,"NotificationType":2,"LastAuthenticatedTimestamp":"2025-09-12T09:06:10.5583883Z","AuthenticatorFlavor":"Authenticator","HashFunction":null,"TenantDeviceId":null,"SecuredPartitionId":20174,"SecuredKeyId":7}]
azure.auditlogs.properties.target_resources.0.modified_properties.1.display_name	Included Updated Properties

Threat actors can set automatic forwarding of e-mails to exfiltrate them from a compromised user account. This behavior is aimed at collecting sensitive data into an external email address.

Email Automatic Forwarding

M365 Incident Response – Email Automatic Forwarding



● High

Sep 23, 2025 @ 18:16:31.055

⚠ SCS CSIRT O365 Suspicious Mailbox Forwarding via Set-Mailbox in Microsoft 365

Status	Risk score	Assignees	Notes
Open	85	⊕	⊕ Add note

About

Rule description — Show rule summary

Detects suspicious mailbox forwarding configurations in Microsoft 365 using the `Set-Mailbox` command. Adversaries may abuse this command to exfiltrate data by configuring auto-forwarding to external addresses. This behavior is associated with data collection and can be used in post-compromise stages ...

Alert reason — Show full reason

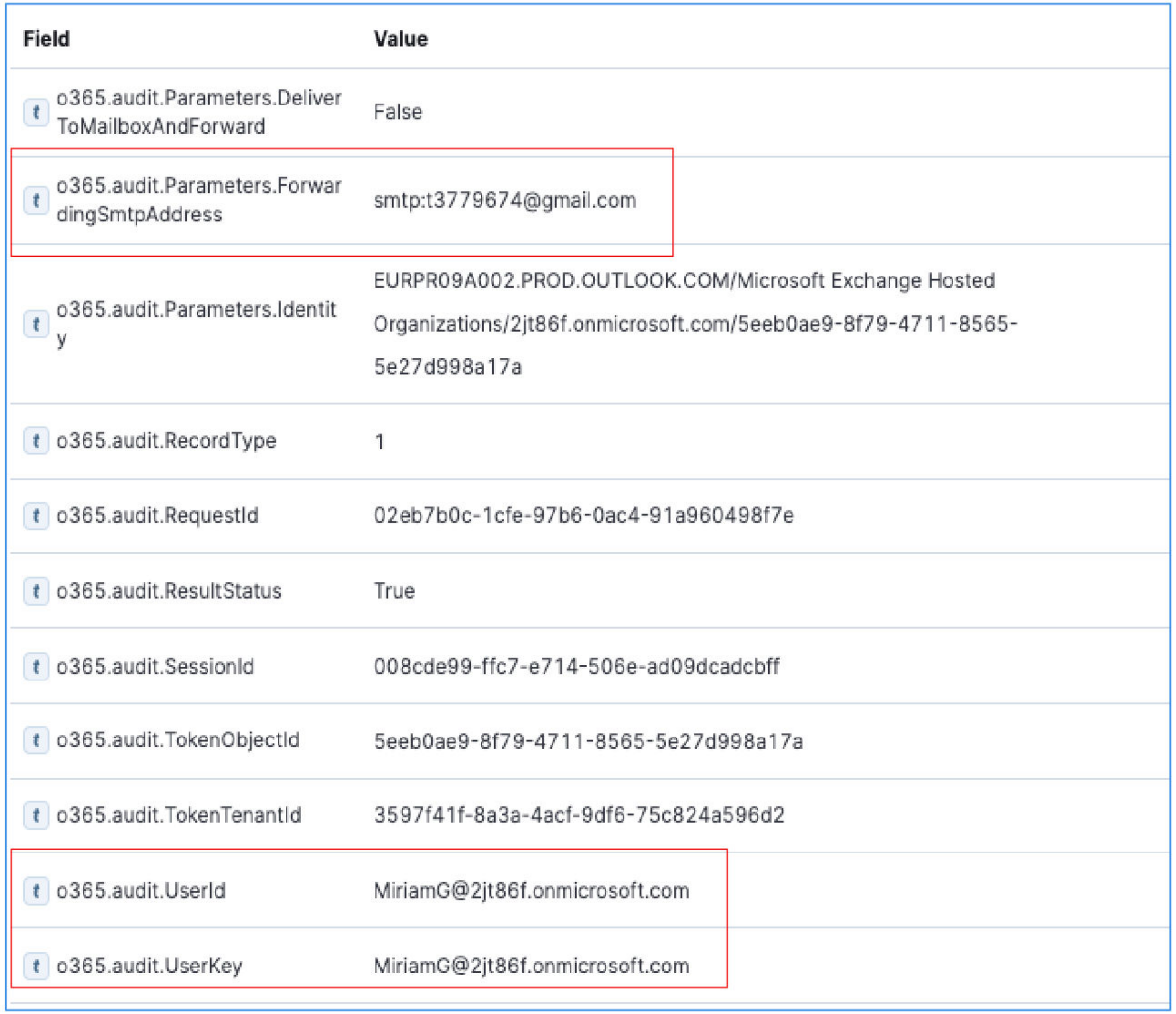
web event with source 178.197.177.146:20345, by MiriamG on 2jt86f.onmicrosoft.com created high alert SCS CSIRT O365 Suspicious Mailbox Forwarding via Set-Mailbox in Microsoft 365.

Investigation

Show investigation guide

Highlighted fields

Field	Value
@timestamp	2025-09-23T16:16:31.055Z
event.provider	Exchange
event.action	Set-Mailbox
user.email	MiriamG@2jt86f.onmicrosoft.com
source.ip	178.197.177.146
o365.audit.Parameters.ForwardingSmtpAddress	smtp:t3779674@gmail.com
host.name	2jt86f.onmicrosoft.com
user.name	MiriamG
kibana.alert.rule.type	query

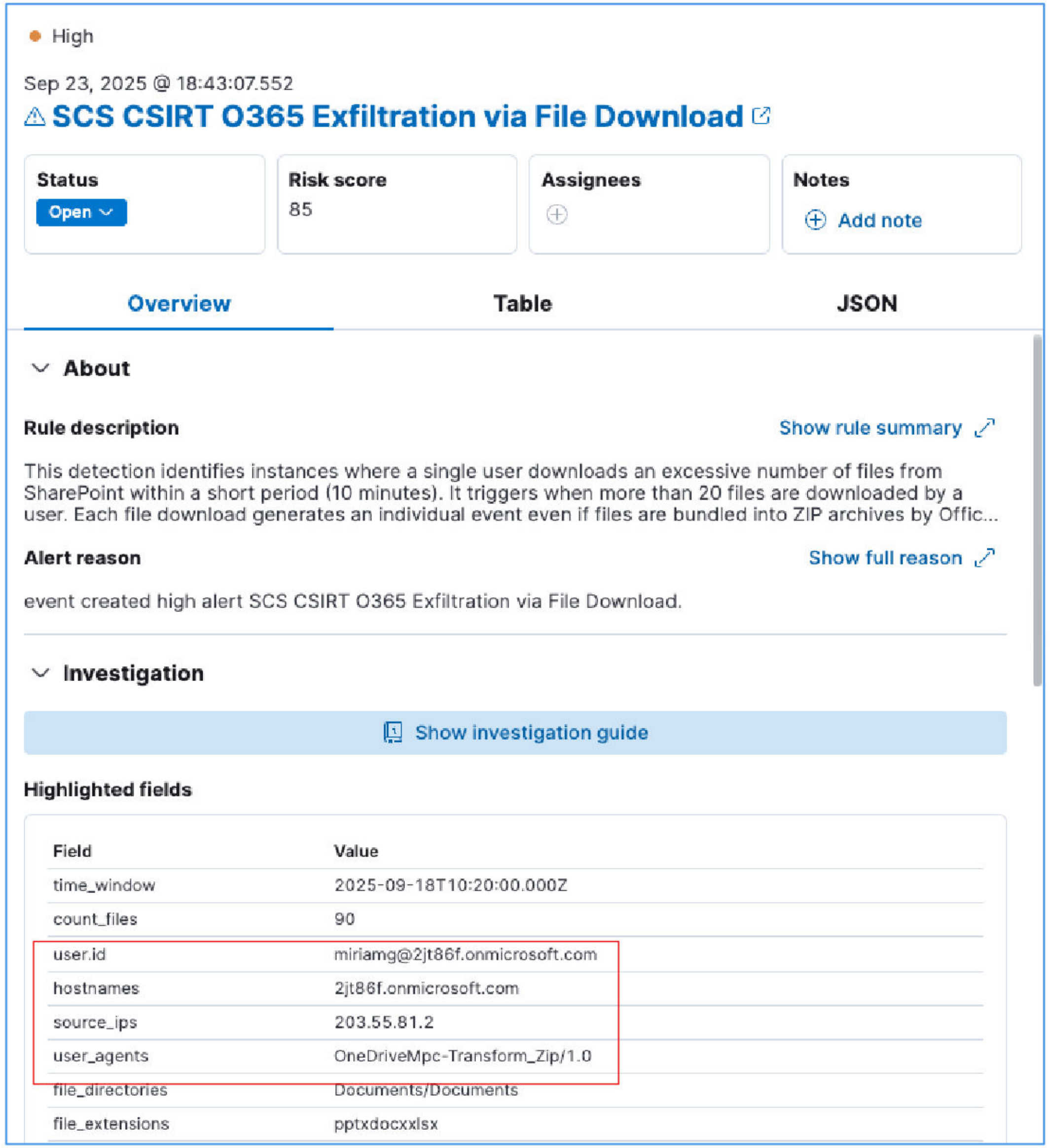


Field	Value
o365.audit.Parameters.DeliverToMailboxAndForward	False
o365.audit.Parameters.ForwardingSmtpAddress	smtp:t3779674@gmail.com
o365.audit.Parameters.Identity	EURPR09A002.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/2jt86f.onmicrosoft.com/5eeb0ae9-8f79-4711-8565-5e27d998a17a
o365.audit.RecordType	1
o365.audit.RequestId	02eb7b0c-1cfe-97b6-0ac4-91a960498f7e
o365.audit.ResultStatus	True
o365.audit.SessionId	008cde99-ffc7-e714-506e-ad09dcadcbff
o365.audit.TokenObjectId	5eeb0ae9-8f79-4711-8565-5e27d998a17a
o365.audit.TokenTenantId	3597f41f-8a3a-4acf-9df6-75c824a596d2
o365.audit.UserId	MiriamG@2jt86f.onmicrosoft.com
o365.audit.UserKey	MiriamG@2jt86f.onmicrosoft.com

The unauthorized transfer of sensitive files from a user's OneDrive or a SharePoint site to a location controlled by an attacker, often using a compromised session or stolen credentials.

OneDrive File Extraction

M365 Incident Response – OneDrive File Exfiltration



● High

Sep 23, 2025 @ 18:43:07.552

⚠ SCS CSIRT O365 Exfiltration via File Download

Status	Risk score	Assignees	Notes
Open	85	⊕	⊕ Add note

About

Rule description — Show rule summary

This detection identifies instances where a single user downloads an excessive number of files from SharePoint within a short period (10 minutes). It triggers when more than 20 files are downloaded by a user. Each file download generates an individual event even if files are bundled into ZIP archives by Offic...

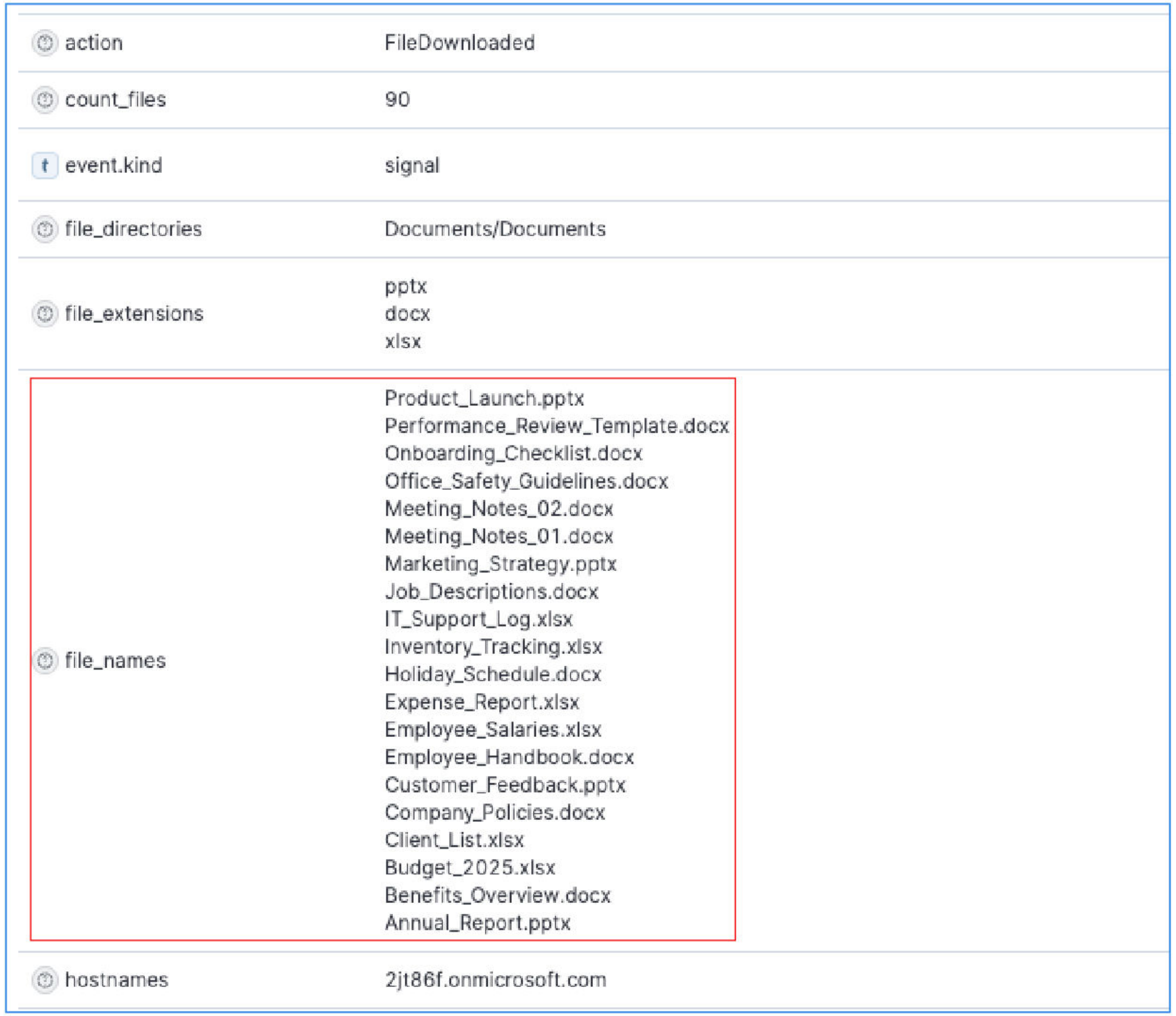
Alert reason — Show full reason

event created high alert SCS CSIRT O365 Exfiltration via File Download.

Investigation

Highlighted fields

Field	Value
time_window	2025-09-18T10:20:00.000Z
count_files	90
user.id	miriamg@2jt86f.onmicrosoft.com
hostnames	2jt86f.onmicrosoft.com
source_ips	203.55.81.2
user_agents	OneDriveMpc-Transform_Zip/1.0
file_directories	Documents/Documents
file_extensions	pptxdocxxlsx

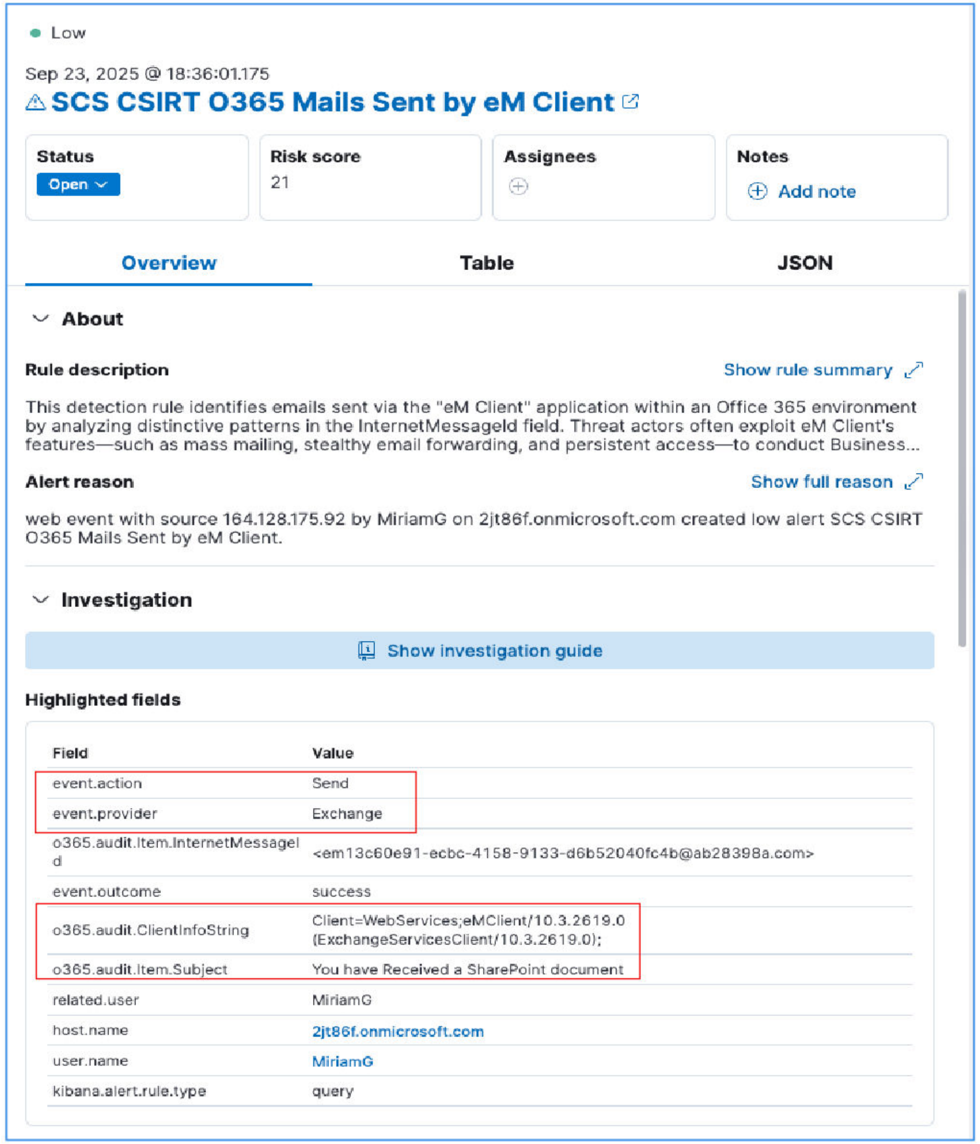


action	FileDownloaded
count_files	90
event.kind	signal
file_directories	Documents/Documents
file_extensions	pptx docx xlsx
file_names	Product_Launch.pptx Performance_Review_Template.docx Onboarding_Checklist.docx Office_Safety_Guidelines.docx Meeting_Notes_02.docx Meeting_Notes_01.docx Marketing_Strategy.pptx Job_Descriptions.docx IT_Support_Log.xlsx Inventory_Tracking.xlsx Holiday_Schedule.docx Expense_Report.xlsx Employee_Salaries.xlsx Employee_Handbook.docx Customer_Feedback.pptx Company_Policies.docx Client_List.xlsx Budget_2025.xlsx Benefits_Overview.docx Annual_Report.pptx
hostnames	2jt86f.onmicrosoft.com

A threat actor uses a hijacked M365 account to send convincing phishing emails to other employees. The emails appear legitimate as they come from a trusted colleague, dramatically increasing the chances of success.

Phishing Campaign

M365 Incident Response – Phishing Campaign



● Low

Sep 23, 2025 @ 18:36:01.175

⚠ SCS CSIRT O365 Mails Sent by eM Client

Status	Risk score	Assignees	Notes
Open	21	⊕	⊕ Add note

Overview | Table | JSON

About

Rule description — Show rule summary

This detection rule identifies emails sent via the "eM Client" application within an Office 365 environment by analyzing distinctive patterns in the InternetMessageId field. Threat actors often exploit eM Client's features—such as mass mailing, stealthy email forwarding, and persistent access—to conduct Business...

Alert reason — Show full reason

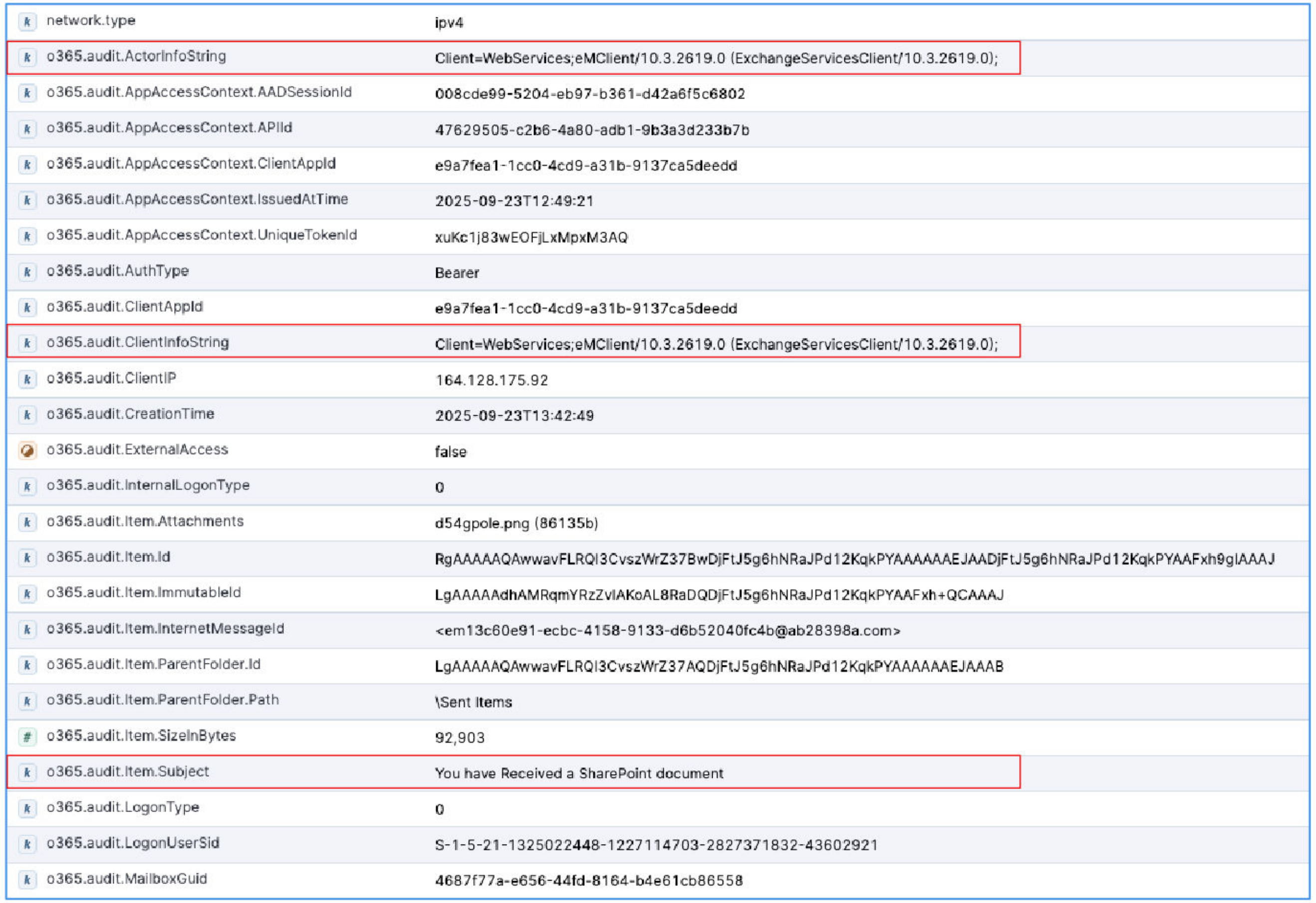
web event with source 164.128.175.92 by MiriamG on 2jt86f.onmicrosoft.com created low alert SCS CSIRT O365 Mails Sent by eM Client.

Investigation

Show investigation guide

Highlighted fields

Field	Value
event.action	Send
event.provider	Exchange
o365.audit.Item.InternetMessageId	<em13c60e91-ecbc-4158-9133-d6b52040fc4b@ab28398a.com>
event.outcome	success
o365.audit.ClientInfoString	Client=WebServices;eMClient/10.3.2619.0 (ExchangeServicesClient/10.3.2619.0);
o365.audit.Item.Subject	You have Received a SharePoint document
related.user	MiriamG
host.name	2jt86f.onmicrosoft.com
user.name	MiriamG
kibana.alert.rule.type	query



network.type	ipv4
o365.audit.ActorInfoString	Client=WebServices;eMClient/10.3.2619.0 (ExchangeServicesClient/10.3.2619.0);
o365.audit.AppAccessContext.AADSessionId	008cde99-5204-eb97-b361-d42a6f5c6802
o365.audit.AppAccessContext.APIId	47629505-c2b6-4a80-adb1-9b3a3d233b7b
o365.audit.AppAccessContext.ClientAppId	e9a7fea1-1cc0-4cd9-a31b-9137ca5deedd
o365.audit.AppAccessContext.IssuedAtTime	2025-09-23T12:49:21
o365.audit.AppAccessContext.UniqueTokenId	xuKc1j83wEOFjLxMpxM3AQ
o365.audit.AuthType	Bearer
o365.audit.ClientAppId	e9a7fea1-1cc0-4cd9-a31b-9137ca5deedd
o365.audit.ClientInfoString	Client=WebServices;eMClient/10.3.2619.0 (ExchangeServicesClient/10.3.2619.0);
o365.audit.ClientIP	164.128.175.92
o365.audit.CreationTime	2025-09-23T13:42:49
o365.audit.ExternalAccess	false
o365.audit.InternalLogonType	0
o365.audit.Item.Attachments	d54gpole.png (86135b)
o365.audit.Item.Id	RgAAAAAQAwwavFLRQI3CvszWrZ37BwDjFtJ5g6hNRaJPd12KqkPYAAAAAAEJAADjFtJ5g6hNRaJPd12KqkPYAAFxh9gIAAAJ
o365.audit.Item.ImmutableId	LgAAAAAdhAMRqmYRzZvIAKoAL8RaDQDjFtJ5g6hNRaJPd12KqkPYAAFxh+QCAAAJ
o365.audit.Item.InternetMessageId	<em13c60e91-ecbc-4158-9133-d6b52040fc4b@ab28398a.com>
o365.audit.Item.ParentFolder.Id	LgAAAAAQAwwavFLRQI3CvszWrZ37AQDjFtJ5g6hNRaJPd12KqkPYAAAAAAEJAAAB
o365.audit.Item.ParentFolder.Path	\Sent Items
o365.audit.Item.SizeInBytes	92,903
o365.audit.Item.Subject	You have Received a SharePoint document
o365.audit.LogonType	0
o365.audit.LogonUserSid	S-1-5-21-1325022448-1227114703-2827371832-43602921
o365.audit.MailboxGuid	4687f77a-e656-44fd-8164-b4e61cb86558

Main Security Recommendations for Microsoft 365

Enforce Phishing-Resistant MFA for all administrators to prevent AiTM attacks by implementing solutions like: FIDO2 security key, Windows Hello for Business or Certificate-based authentication. The enforcement of those superior levels of authentication is accomplished through Conditional Access policies.

Adopt Continuous Access Evaluation (CAE) to evaluate a user’s session in near-real time when certain conditions change, such as their IP address.

Implement strict Conditional Access policies to secure the registration of additional MFA devices for a user, such as requiring MFA for registering security information, blocking any attempts outside of trusted locations (e.g., the corporate network), and ensuring the action is performed from a managed and clean device.

Main Security Recommendations for Microsoft 365

Configure outbound spam policies to restrict the automatic forwarding of email to external recipients or set an external message limit.

Configure the **auditing** of Microsoft 365 activities (Unified Audit Logs) and **collect** the Azure and M365 **logs** into a SIEM platform for monitoring the events and automatically generate alerts, also through a **SOC service which runs 24/7**.

Angelo Violetti

Senior CSIRT Analyst @ Swisscom | Threat Intelligence Analyst @ The DFIR Report

Angelo Violetti

Senior DFIR Analyst @ Swisscom CSIRT

Angelo.Violetti@swisscom.com

24/7 CSIRT Hotline 0800 850 000