AppOmni

10 Key Detections for M365 Security

Microsoft 365 (M365) is essential to business operations, but its broad use makes it a target for account takeovers, data theft, and insider threats. To improve security, Microsoft has expanded logging for Exchange Online, SharePoint, and Teams, providing deeper visibility into user activity.

To make the most of these logs, teams need a proactive monitoring strategy. By tracking key M365 events, organizations can detect unauthorized access, suspicious searches, and potential data exfiltration before threats escalate.

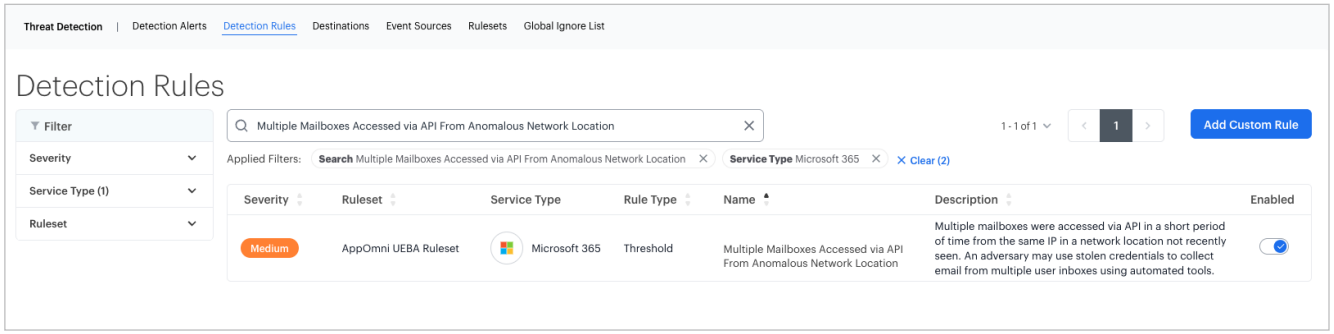
Identify unauthorized access, suspicious searches, and data exfiltration by watching for anomalous or unusual activity in these 10 M365 events:

1 Exchange Online: MailItemsAccessed

Attackers who compromise accounts often read emails to gather intelligence, steal sensitive data, or prepare for phishing and business email compromise (BEC) attacks.

Monitor for:

- An AppID accessing multiple mailboxes in a short time frame, which may indicate automated data theft
- Large spikes in mail access activity from a single user, a common sign of account compromise
- Access to sensitive mailboxes from unusual IPs or devices, suggesting external threat actor activity



Exchange Online:
Send

2

Attackers often use a compromised email account to send phishing emails, forward sensitive information, or communicate with other compromised users within an organization.

Monitor for:

- Emails sent from known suspicious IP addresses
- Unusual attachment types, such as password-protected ZIP files
- Emails sent from accounts that recently logged in at odd hours or from unexpected locations

3

Exchange Online:
SearchQueryInitiatedExchange

Attackers frequently search a compromised mailbox for financial data, credentials, or business-critical information to use for further exploitation.

Monitor for:

- Searches for sensitive terms like “invoice,” “password,” or “wire transfer” by unauthorized users
- Excessive search activity within a short period, which could indicate reconnaissance behavior
- Searches originating from devices or IPs not previously associated with the user

4

SharePoint Online:
SearchQueryInitiatedSharePoint

SharePoint and Teams store critical business documents, including financial records, intellectual property, and confidential reports. Attackers search these repositories for valuable information to steal or exploit.

Monitor for:

- Searches for confidential documents performed outside normal working hours
- Queries for sensitive terms by users who are not part of the authorized team or department
- Repeated searches across multiple SharePoint sites by a single user, potentially indicating an insider threat

Rule Details

M365 SCuBA - Suspicious Search Activity

You're the rule owner.

Description

Detect suspicious search activity in SharePoint or Exchange data.

Severity

Medium

Supported Services

Microsoft 365

This rule will trigger when:

```
All of the following conditions occur in 60 minute(s):
   • event.action equals query_resource
   • any of the following conditions:
      • labels.query contains password
      • labels.query contains securestring
   • any of the following conditions:
      • event.code equals SearchQueryInitiatedExchange
      • event.code equals SearchQueryInitiatedSharePoint
with identical values for the following fields:
   • user.name
When this detection rule is triggered, it won't trigger again for 60 minute(s).
```

5

Microsoft Teams:
MeetingParticipantDetail

Unauthorized access to virtual meetings can expose sensitive discussions, provide attackers with reconnaissance opportunities, or facilitate social engineering attacks.

Monitor for:

- External or unauthorized users joining meetings related to sensitive topics
- Patterns of participants repeatedly leaving and re-joining meetings, which may suggest eavesdropping attempts
- Meeting participant IPs that match known threat actor infrastructure

6

Microsoft Teams:
MessageSent

Attackers often use Teams messages to distribute phishing links, spread malware, or communicate within a compromised organization.

Monitor for:

- High volumes of messages sent to external or guest users
- Messages sent during off-hours or from devices that have not been previously used by the sender

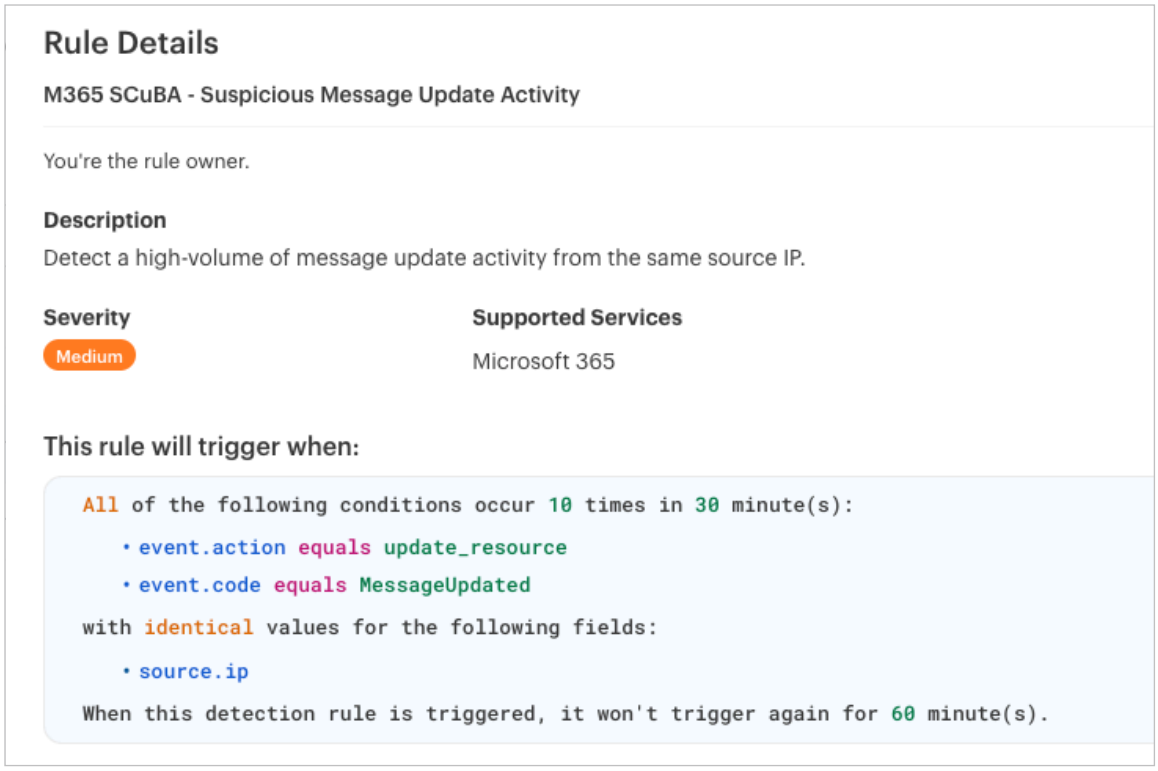
7

Microsoft Teams:
MessageUpdated

Edited messages can be a sign of tampering, an attempt to cover up malicious activity, or an effort to mislead other users.

Monitor for:

- Edits made from unrecognized or suspicious IP addresses
- Messages that are repeatedly edited within a short timeframe



8

Microsoft Teams:
MessageRead

Attackers who gain unauthorized access to an account may read Teams messages to collect intelligence without actively participating in conversations.

Monitor for:

- Bulk reading of multiple messages in a single chat thread
- Message reads from unauthorized applications or devices
- Messages accessed from IP addresses that do not align with the user's historical activity

9

Microsoft Teams:
ChatRetrieved

The Graph API can be used to silently retrieve chat metadata, giving attackers insight into internal communications, team structures, and high-value targets.

Monitor for:

- Automated retrieval of multiple chat threads by the same AppID
- Chat retrieval requests from unauthorized or unrecognized applications
- Patterns that indicate bulk API activity occurring within a short period

10

Microsoft Teams:
MessageHostedContentRead

Attackers may extract files, images, or code snippets from Teams channels to gather sensitive data without triggering standard file download alerts.

Monitor for:

- Access to hosted content by unauthorized external applications
- Repeated retrievals of hosted content from the same chat or channel
- Unusual access patterns related to specific content types, such as proprietary code or financial documents

How AppOmni Can Help

Manually monitoring these risks across M365 can be time-consuming and complex. AppOmni simplifies SaaS security by providing automation, visibility, and intuitive controls for M365 and other SaaS environments.

With AppOmni, security teams can:

Automate monitoring and alerting for security events across M365 and other SaaS applications, reducing manual work.

Apply customizable detection rules without needing complex queries or specialized expertise.

Correlate activity across multiple SaaS platforms to identify meaningful patterns and real threats faster.

Integrate with SIEM and SOAR solutions to streamline workflows and simplify response efforts.

Conduct automated compliance checks that make meeting industry standards like NIST, ISO 27001, and SOC 2 easier.

With built-in expertise, clear guidance, and automation, AppOmni makes securing SaaS environments easier and more effective than ever.

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by 5 of the Fortune 10, AppOmni specializes in securing diverse SaaS environments.

To learn more or request a SaaS security assessment, visit AppOmni.com.