Cloud Automated Threat Response: Microsoft 365

Written By Merium Khalid – Director, SOC Offensive Security

Purpose of Automated Threat Response:

The primary objective of Automated Threat Response (ATR) is to address security threats in real time by reducing the time to respond (TTR) and therefore the impact of a compromise. By analyzing logs from Microsoft 365, our Machine Learning (ML) detection rules meticulously examine authentication logs. When potential malicious activity is identified, ATR promptly responds by connecting into your Microsoft 365 environment via API integration. This process neutralizes the threat automatically, requiring no intervention from the customer and ensuring continuous security.

How it works:

Barracuda's Managed XDR platform provides rapid and intelligent protection for compromised Microsoft 365 accounts by automatically suspending affected users and terminating all active sessions. Leveraging advanced machine learning models and proprietary anomaly detection algorithms, the platform continuously monitors and correlates activity patterns within Microsoft 365 to identify potential account compromises. By integrating ATR (Automated Threat Response), threat intelligence, and cutting-edge analytics, Barracuda XDR delivers a comprehensive approach to detecting and responding to suspicious behavior. Upon confirmation of a compromise, the platform initiates an automated response to suspend the user within the Microsoft 365 cloud environment, ensuring swift containment and protection against advanced threats. Please note that in hybrid environments, changes are not applied to on-premise systems; your IT department must implement those updates locally.

Actions We Take

To detect and respond to potentially compromised Microsoft 365 accounts, we use several anomaly indicators. When multiple of these indicators are triggered, a high severity alert is generated, and the user account is automatically suspended via API to prevent further unauthorized access. While we will still alert on anomalies regardless of the type of account, please note admin accounts (User Type 2 and 3) are excluded from this functionality due to their high criticality and business impact within an organization.
Here's a breakdown of the indicators we monitor:

Login Activity Indicators

1. Last 24h Login Counts: Monitors the count of successful logins in the past 24 hours, identifying unusual login behaviors.
2. Geo and IP-Based Anomalies:
    a. Missing Geo Flag: Indicates logins with missing geographical information.
    b. Speed in KMPH: Calculates speed between consecutive logins; high speed may indicate unusual behavior.
    c. Distance from Typical Geo: Measures the distance between the login location and the user's typical location (FP threshold: 200 KM).
    d. Risky Geo Country: Flags logins from high-risk countries (e.g., Russia, China) and medium-risk countries (e.g., Israel, Vietnam).
    e. Geo Rarity Score: Scores the rarity of the login location; a high score implies unusual access locations.
    f. Impossible Travel Flag: Indicates logins where the speed between locations is over 1000 KMPH with high geo-rarity.
3. Source IP Rarity Score: Ranks the rarity of login IPs based on 90-day history; higher values suggest rare or unusual IPs.

4. Same Region Login Indicator: Checks if the login is from the user's usual region; a different region may indicate compromise.

Behavioral Anomaly Indicators

5. Low Login Indicator: Detects if a user has low login frequency, potentially increasing FP likelihood.
6. Midnight Login: Monitors logins during midnight hours but is excluded due to timezone inconsistencies.
7. Different Audit Device ID Indicator: Flags logins from different devices within a 30-minute window.

Account Change Indicators

8. Recent MFA Change/Disable Indicator: Detects if a user recently changed or disabled MFA within 24 hours.
9. Recent Password Reset Indicator: Flags if a password reset occurred in the last 24 hours.

Aggregate Anomaly Indicators (24h)

10. Impossible Travel Flag Breach: Counts impossible travel incidents within the last 24 hours.
11. Speed Breach: Counts instances of abnormal login speeds in 24 hours.
12. Geo Rarity Breach: Tracks geo-location rarity breaches in the last 24 hours.
13. Source IP Rarity Breach: Records instances of unusual source IPs within 24 hours.
14. Login Time Rarity Breach: Monitors login time irregularities based on historical data.

When multiple indicators are triggered, we immediately escalate to a high alert and suspend the user account to prevent unauthorized activity, ensuring swift, automated response to potential compromises in Microsoft 365.

Reducing False Alerts

Some patterns are less likely to indicate a threat, like multiple logins from the same region or low travel distances which are designated as medium and low alerts.

Alert Levels

We classify alerts by severity based on the likelihood of a true compromise:

- High: When several indicators point to a high likelihood of compromise, an alert is generated, and we may disable the account to prevent unauthorized access.
- Medium: Alerts with moderate risk may require additional information from you before we take further action.
- Low: Low-severity alerts highlight unusual but low-risk activities that generally do not need immediate attention.

Characteristics of True and False Positives

Certain features make a compromise more likely (True Positives), while others decrease its likelihood (False Positives). This helps in refining accuracy and reducing false alerts.

Dynamic Severity Levels

- High: Numerous True Positive indicators plus risky device. High alerts may trigger automatic account lockdown, excluding admin accounts.
- Medium: Multiple True Positive indicators.
- Low: Limited True Positive indicators.

When Alerts Are Not Triggered

- The login occurs from a user's typical location.
- The user has logged in fewer than 50 times over the last 90 days.
- Two or more false positive indicators are detected.
- Travel speed is below 800 KMPH, and the login is within 200 KM of the user's usual location; both thresholds must be exceeded to qualify as an impossible travel scenario

Our approach minimizes unnecessary alerts, focusing on high-confidence, actionable events to ensure security while reducing noise.

What You Will See on Your End

If our XDR team identifies activity suggesting a potential account compromise, the affected user account will be immediately suspended within your Microsoft 365 environment. Locking down a user account will terminate the user's active session in ALL Microsoft 365 applications and prevent further sign-ins.

Upon detection, you will receive one of the following alerts if user is suspended (High alerts):

- Microsoft 365 Impossible Travel User Suspended
- Microsoft 365 Anomalous Login User Suspended

Upon detection, you will receive one of the following alerts if not suspended (Low and Medium alerts):

- Microsoft 365 Impossible Travel
- Microsoft 365 Anomalous Login

Each alert will be accompanied by a detailed incident, including the following information:

- Description of suspicious activities, such as impossible travel, unusual login location, or high-risk geo access.
- Indicators triggered that led to the account lockdown.
- Details of the automatic remediation action, confirming the account's suspended status and providing next steps, if needed.
- Barracuda AI Insights: AI-generated summary of the flagged activity presented in a clear, easy-to-read, and actionable format.

The comprehensive alert enables you to review the incident swiftly, understand the nature of the detected anomalies, and take any further action as required.

Automated Threat Response (ATR) is more than just a feature; it's a transformative approach to cybersecurity. Here's why:

- Real-Time Responses: ATR promptly addresses threats, significantly reducing attackers' window of opportunity and minimizing the impact of potential security breaches.
- Customer-Focused Approach: By automating threat responses, ATR enables customers to maintain seamless business operations without the complexities of managing security incidents.
- Improved Security Posture: ATR strengthens overall security, making it an essential tool for MSPs and partners to safeguard their clients.

Conclusion

Automated Threat Response reflects our commitment to pioneering cybersecurity solutions. With real-time threat mitigation and automated responses, ATR empowers MSPs and partners to deliver enhanced security. In today's evolving threat landscape, ATR embodies innovation, boosting operational efficiency and reinforcing security resilience. We are excited to see the impact of ATR on the cybersecurity industry as we work towards building a safer digital ecosystem for all.

Call to Action

Discover the transformative potential of Cloud Automated Threat Response: Microsoft 365. Enhance your cybersecurity solutions and join us in advancing cybersecurity. Don't miss the opportunity to revolutionize your security strategy with next generation technology!

1. Existing XDR Cloud Security Customers: ATR for Cloud is included at no extra cost. Set it up easily in your XDR Customer Security Dashboard.
2. Not Subscribed to XDR Cloud Security? We strongly recommend protecting your Microsoft 365 and cloud apps. Contact our sales team for options.
3. New to XDR? Learn more about ATR, Threat Intelligence, and our XDR & SOC capabilities. Contact sales at sales@barracudamsp.com.