CISOnow
Your Trusted Cyber Security Partner

Identity Theft Detection and Response (ITDR) for Microsoft 365

Proactive Cyber Defense for Microsoft 365

Catch Cyber Attacks and Defend Your Microsoft 365 Users

With modern cloud-based application services, a single stolen credential or compromised account can be used to launch a crippling cyber-attack. Detecting suspicious logins or activity like new mail forward configurations can identify an emerging intrusion. With Identity Threat Detection and Response (ITDR) for Microsoft 365 you have 24x7 Detection and Response to these and other early signs of an attack.

Give Your Microsoft 365 Environment the 24x7 Protection It Deserves

ITDR for Microsoft 365 secures your Microsoft 365 users and applications by leveraging a 24x7 fully managed service to detect and respond to suspicious user activity, permission changes and anomalous access behavior. ITDR for Microsoft 365 protects you 24x7 with no gaps or lags in coverage during the peak seasons, off hours or holidays.

Real-time Cyber Defense Backed by Human Experts

ITDR for Microsoft 365 integrates seamlessly with AzureAD and collects and combines user, tenant and application data enriched with additional organic and external threat feeds. Together, this data is utilized to detect, analyze and report on suspicious behaviors or dangerous threats and provide remediation options.

Cut through the noise to defend your Microsoft 365 environment.

DETECT THREATS FASTER
Identify threat actor behavior faster and more accurately by detecting early entry and persistence activities.

RESPOND AND REMEDIATE QUICKER
Our SOC analyzes incidents 24x7, removing false positives and providing remediation steps.

BE MORE EFFICIENT
ITDR for Microsoft 365 works quickly and efficiently so you see what truly matters; real threats and the recommended steps for remediation.

HUMAN-POWERED PEACE OF MIND
Our 24x7 human-intelligence-powered detection and response solution saves you time and money, so you can focus on your core business.

Features and Threats Detected

SUSPICIOUS LOGIN IDENTIFICATION

When threat actors gain access to an account, they often leave behind indicators of anomalous behavior. These may include a string of repeated failed login attempts preceding a successful one, as well as instances of unlikely or impossible travel between login locations.

SUSPICIOUS MAIL FORWARDING CONFIGURATION

Threat actors can use compromised user accounts for several malicious purposes, including reading emails in a user's inbox, forwarding emails to external recipients and sending phishing emails.

ACCESS ACTIVITY MONITORING

Threat actors will often need access to systems and services not available or unused by compromised accounts. Novel or unauthorized access to applications, files or data can be a key indicator of a compromised account.

PRIVILEGE ESCALATION AND EXPLOITATION TRIGGERS

Threat actors often need to change, add or alter the permissions for the compromised account or others. Permission changes can include high-level or sweeping privileges, additional mailbox access, creating new accounts, new groups and others.

24x7 SOC

Security threats are ever-present, striking at any time. However, attackers often exploit off-hours and holidays to catch their targets off guard. Utilize a vigilant team of security experts available 24x7 to continuously monitor incidents, filter out false alarms, investigate thoroughly, and provide clear remedial guidance.

ACCOUNT ISOLATION

When a threat actor compromises and accesses an account, the account must be restricted immediately. Account Isolation enables our SOC to log out the account from all applications and devices, including disabling the account from further environment access.

MALICIOUS INBOX RULE REMOVAL

Malicious inbox rules remain a threat actor's tool of choice for data exfiltration. Malicious Inbox Rule Removal enables the our SOC to remove the offending inbox rule without impacting other important business email configurations.

CISOnow

Your Trusted Cyber Security Partner

Ready to have peace of mind?
Contact us today.

1-866-247-CISO
sales@cisonow.com
www.cisonow.com