HUNTRESS

Huntress Managed Detection and Response for Microsoft 365

Your business runs on the cloud—protect it 24/7 from incoming and ongoing cyberattacks with MDR for Microsoft 365 by Huntress.

Cut through the noise to find and kick hackers out of your cloud.

DETECT THREATS FASTER

Huntress leverages common behavior baselines to receive active threat actor detections from their key early entry and persistence activity.

RESPOND AND REMEDIATE QUICKER

The Huntress SOC team analyzes detections 24/7, filtering out false positives and providing remediation steps.

GAIN TIME BACK

Huntress' MDR for Microsoft 365 minimizes alert fatigue and reduces overall noise from false positives to enable your already-busy technicians to refocus their efforts towards critical tasks.

24/7 PEACE OF MIND

24/7 Managed Detection and Response without needing to hire additional staff to manage the platform.

Protect your cloud by stopping cyberattacks earlier with Huntress.

A single stolen credential or compromised account can be used to launch a crippling cyberattack against modern, cloud-based infrastructure. Identifying user behaviors and detecting malicious activity early, like unauthorized access or email manipulation, enables rapid response to a nascent intrusion even before serious damage may occur. Use Huntress Managed Detection and Response (MDR) for Microsoft 365 to detect and respond to early signs of a cyberattack to shut down hackers fast.

Give your 24/7 cloud the 24/7 protection it deserves.

Huntress Managed Detection and Response (MDR) for Microsoft 365 secures your Microsoft 365 users, applications and environment by leveraging the 24/7 Huntress Security Operations Center (SOC). Our SOC experts interpret threat detections and deliver incident reports with actionable remediations for recovery. A Huntress human will review every detection for you, filtering out the noise and only escalating customized reports when malicious activity is suspected. MDR for Microsoft 365 protects you 24/7 with no gaps or lags in coverage during the peak seasons, off hours, or holidays.

Gain time back while improving long-term security strategy.

MDR for Microsoft 365 integrates with your Microsoft Cloud environment, collecting user, tenant and application data which is enriched using organic and external threat feeds to supply information like geolocation and IP reputation. The Huntress SOC utilizes this context-added data to provide the most accurate and precise incident reports and the best remediation options to neutralize threat actors quickly.

Features and Threats Detected

SUSPICIOUS LOGIN IDENTIFICATION

Threat actors usually access victim accounts from different geographic locations, utilizing different computer and web browser fingerprints.

SUSPICIOUS MAIL FORWARDING CONFIGURATION

Threat actors can use compromised user accounts for several malicious purposes, the main ones being the ability to forward users' emails out to an external, malicious account and to obfuscate email.

PRIVILEGE ESCALATION

Threat actors will often need to change, add or alter the permissions of the compromised account or other accounts in the domain.

ACCOUNT ISOLATION

When a threat actor compromises and accesses an account, their access must be shut down immediately. Account Isolation allows the Huntress SOC to disable an account and log them out from all applications or devices.

24/7 SECURITY OPERATIONS CENTER (SOC)

Threats can occur at any time, but attackers target off-hours and holidays to catch their targets unaware. Huntress' 24/7 SOC team of security experts is constantly reviewing incidents, removing false positives and investigating threats, providing remediation directions so you don't receive any vague alerts.

ASSISTED RULE REMOVAL

Malicious inbox rules remain a threat actor's tool of choice for data exfiltration and obfuscation. MDR for Microsoft 365 introduces an Assisted Remediation for malicious inbox rule removal. With one click, this feature allows you to automatically remove a malicious rule without needing to hunt down the rule in your Azure environment.

"Having a true managed service for email security is a game changer. We were able to resolve an issue within minutes with the help of the 24/7 Security Operations Center Team. Partnering with Huntress has exceeded our expectations, and we can feel the impact they've made in our work."

Matt Robins

Security Analyst | Rudick Innovation and Technology

GREAT LAKES TECH SERVICES

Contact Mark Mullarky

2607 N Grandview Blvd Suite 160E

Waukesha, WI 53188

262.720.3668

info@GreatLakesTS.com

www.GreatLakesTS.com