Microsoft 365 Insider Threat Detection Checklist From Hermathena Labs

The Ultimate Guide to Monitoring Critical Insider Risk Indicators

---

HOW TO USE THIS CHECKLIST

This checklist is designed to help security teams identify and monitor the most important insider threat indicators in Microsoft 365 environments. For each indicator:

1. Check if you're currently monitoring for this activity
2. Note the Microsoft 365 tool that provides this visibility
3. Verify that you have alerts or regular reviews in place
4. Document your current threshold or trigger settings

EMAIL & COMMUNICATION INDICATORS

Unusual Email Forwarding Rules

- ☐ **Monitor for new inbox rules with external forwarding**
- ☐ **Alert on forwarding to personal email domains (Gmail, Yahoo, etc.)**
- ☐ **Review forwarding rules during employee offboarding**
- ☐ **Audit delegation access to executive mailboxes**

Tool: Exchange Admin Center, Audit Logs

Review Frequency: □ Weekly □ Bi-weekly □ Monthly

Unusual Email Attachment Activity

- ☐ **Monitor for spikes in emails with attachments to external recipients**
- ☐ **Alert on emails with sensitive file attachments sent externally**
- ☐ **Track users who send unusual volumes of attachments after hours**
- ☐ **Monitor for encrypted attachments to unauthorized recipients**

Tool: Microsoft Purview DLP, Exchange Online Protection

Review Frequency: □ Daily □ Weekly □ Monthly

Communications with Competitors

- ☐ **Create and maintain list of competitor domains**
- ☐ **Monitor for increasing frequency of communications with these domains**
- ☐ **Alert on internal documents shared with competitor contacts**
- ☐ **Review communications during sensitive business periods**

Tool: Communication Compliance, DLP

Review Frequency: □ Weekly □ Bi-weekly □ Monthly

Communication Pattern Changes

- ☐ **Establish communication pattern baselines for key personnel**
- ☐ **Monitor for sudden changes in tone or language use**
- ☐ **Alert on unusual increases in communication frequency**
- ☐ **Track communication shifts following HR events**

Tool: Communication Compliance, UEBA

Review Frequency: □ Weekly □ Bi-weekly □ Monthly

FILE & DOCUMENT INDICATORS

Mass File Downloads

- ☐ **Monitor for bulk downloads from SharePoint and OneDrive**
- ☐ **Set thresholds for download volumes based on role**
- ☐ **Create alerts for after-hours download activity**
- ☐ **Track downloads of sensitive or restricted documents**

Tool: SharePoint Audit Logs, Microsoft Purview

Review Frequency: □ Daily □ Weekly □ Monthly

Unusual File Access Patterns

- ☐ **Monitor access to files outside of department or role**
- ☐ **Alert on first-time access to sensitive document libraries**
- ☐ **Track users accessing dormant files or archives**
- ☐ **Monitor access to salary, strategy, or IP-related files**

Tool: SharePoint Analytics, Microsoft Purview

Review Frequency: □ Daily □ Weekly □ Monthly

File Manipulation to Evade DLP

- ☐ **Monitor for files being renamed before download**
- ☐ **Alert on document type conversions (especially to image formats)**
- ☐ **Track screenshots of sensitive information**
- ☐ **Monitor for modification of file metadata or properties**

Tool: DLP, SharePoint Audit Logs

Review Frequency: □ Daily □ Weekly □ Monthly

Unusual File Sharing

- ☐ **Monitor creation of anonymous access links**
- ☐ **Alert on sharing to personal email accounts**
- ☐ **Track changes to sharing permissions on sensitive files**
- ☐ **Monitor sharing with external domains after hours**

Tool: SharePoint Admin Center, Microsoft Defender for Cloud Apps

Review Frequency: □ Daily □ Weekly □ Monthly

AUTHENTICATION & ACCESS INDICATORS

Unusual Login Times

- ☐ **Establish baseline login hours for all users**
- ☐ **Alert on authentication outside of normal working hours**
- ☐ **Monitor weekend access for non-IT personnel**
- ☐ **Track access during holidays or company closures**

Tool: Microsoft Entra ID, Microsoft Sentinel

Review Frequency: □ Daily □ Weekly □ Monthly

Geographic Anomalies

- ☐ **Alert on impossible travel scenarios**
- ☐ **Monitor for connections from unusual countries**
- ☐ **Track logins from known VPN exit points**
- ☐ **Alert on logins from sanctioned countries**

Tool: Microsoft Entra ID Identity Protection

Review Frequency: □ Daily □ Weekly □ Monthly

Authentication Failures

- ☐ **Monitor for multiple failed login attempts**
- ☐ **Alert on password resets followed by unusual activity**
- ☐ **Track failed MFA attempts**
- ☐ **Monitor lockout events for privileged accounts**

Tool: Microsoft Entra ID, Microsoft Sentinel

Review Frequency: □ Daily □ Weekly □ Monthly

Privilege Changes

- ☐ **Monitor elevation of user privileges**
- ☐ **Alert on addition of users to administrative groups**
- ☐ **Track self-service role changes**
- ☐ **Monitor creation of service principals with high privileges**

Tool: Microsoft Entra ID, PIM

Review Frequency: □ Daily □ Weekly □ Monthly

CLOUD APPLICATION INDICATORS

Shadow IT Usage

- ☐ **Monitor for uploads to unauthorized cloud storage**
- ☐ **Alert on data transfers to personal accounts**
- ☐ **Track use of unsanctioned collaboration tools**
- ☐ **Monitor for browser extensions that access M365 data**

Tool: Microsoft Defender for Cloud Apps

Review Frequency: □ Weekly □ Bi-weekly □ Monthly

Cross-Service Data Transfers

- ☐ **Monitor for unusual transfers between sanctioned and unsanctioned apps**
- ☐ **Alert on large data moves between services**
- ☐ **Track automated workflows moving data between services**
- ☐ **Monitor API integrations between services**

Tool: Microsoft Defender for Cloud Apps

Review Frequency: □ Weekly □ Bi-weekly □ Monthly

Automation & API Activity

- ☐ **Monitor for new API connections to M365**
- ☐ **Alert on high-volume API calls**
- ☐ **Track creation of automated workflows**
- ☐ **Monitor PowerShell script execution against M365 services**

Tool: Microsoft Defender for Cloud Apps, Microsoft Sentinel

Review Frequency: □ Daily □ Weekly □ Monthly

Security Control Modifications

- ☐ **Monitor changes to security policies**
- ☐ **Alert on modifications to auditing settings**
- ☐ **Track disabling of security controls**
- ☐ **Monitor changes to retention policies**

Tool: Microsoft Purview Compliance Portal, Microsoft Defender for Cloud Apps

Review Frequency: □ Daily □ Weekly □ Monthly

CONTEXTUAL RISK INDICATORS

HR Event Correlation

- ☐ **Create process for HR to notify security of sensitive personnel events**
- ☐ **Enhance monitoring following negative performance reviews**
- ☐ **Track system activity after denial of promotions or raises**
- ☐ **Monitor access patterns during reorganizations**

Tool: Microsoft Purview Insider Risk Management

Review Frequency: □ Daily □ Weekly □ As Needed

Departure Activities

- ☐ **Implement enhanced monitoring upon receipt of resignation**
- ☐ **Alert on increased download, access, or email activity during notice period**
- ☐ **Track email forwards created during last two weeks**
- ☐ **Monitor personal email communications during final days**

Tool: Microsoft Purview Insider Risk Management

Review Frequency: □ Daily during notice period

Organizational Event Correlation

- ☐ **Monitor for unusual activity around major announcements**
- ☐ **Track access to sensitive documents prior to acquisitions or mergers**
- ☐ **Alert on unusual activity before quarterly earnings reports**
- ☐ **Monitor executive account activity during strategy changes**

Tool: Microsoft Purview Insider Risk Management, Microsoft Sentinel

Review Frequency: □ Daily during sensitive periods

Peer Group Comparison

- [ ] **Establish baselines for department and role-based user groups**
- [ ] **Alert on activity that deviates significantly from peer patterns**
- [ ] **Track users whose access patterns differ from their teams**
- [ ] **Monitor for outliers in data access volumes**

Tool: UEBA, Microsoft Sentinel

Review Frequency: □ Weekly □ Bi-weekly □ Monthly

TOOL CONFIGURATION VERIFICATION

Microsoft Purview Insider Risk Management

- [ ] **Configure templates for departing employees**
- [ ] **Enable templates for data leaks**
- [ ] **Set up policy indicators for high-risk users**
- [ ] **Establish case management process**

Microsoft 365 Audit Log

- [ ] **Verify audit logging is enabled for all services**
- [ ] **Confirm retention period meets compliance requirements**
- [ ] **Create saved searches for common investigations**
- [ ] **Establish export process for incidents**

Microsoft Defender for Cloud Apps

- [ ] **Connect all sanctioned cloud applications**
- [ ] **Configure anomaly detection policies**

- [ ] **Enable shadow IT discovery**
- [ ] **Set up session policies for sensitive applications**

Microsoft Entra ID

- [ ] **Enable Identity Protection**
- [ ] **Configure Conditional Access policies**
- [ ] **Enable risk-based authentication**
- [ ] **Implement Privileged Identity Management**

Data Loss Prevention

- [ ] **Create policies for sensitive data types**
- [ ] **Configure endpoint DLP monitoring**
- [ ] **Enable DLP for Teams and other collaboration tools**
- [ ] **Set appropriate notification and blocking rules**

RESPONSE READINESS ASSESSMENT

Documentation

- [ ] **Insider threat response playbooks created and accessible**
- [ ] **Investigation procedures documented**
- [ ] **Chain of custody procedures established**
- [ ] **Escalation paths clearly defined**

Team Preparedness

- [ ] **Security team trained on insider threat investigations**
- [ ] **HR team aware of their role in insider threat response**

- [ ] **Legal team consulted on evidence handling requirements**
- [ ] **Executive sponsors identified for major incidents**

Technical Capabilities

- [ ] **Account suspension procedures tested**
- [ ] **File access revocation capabilities verified**
- [ ] **Forensic tools available for investigation**
- [ ] **Backup procedures in place for relevant logs**

READY TO STRENGTHEN YOUR INSIDER THREAT PROGRAM?

This checklist provides a starting point for monitoring insider threats in Microsoft 365, but implementing a comprehensive program requires expertise and experience.

For assistance in setting up effective monitoring for these indicators, book a free consultation. We'll help you assess your current capabilities and develop a roadmap for enhancing your insider threat detection.

Schedule your free consultation at hermathenalabs.com/booking

---