protiviti®
*Face the Future with Confidence*

# Microsoft 365 Incident Response Readiness Assessment

## Assessing the Advanced Security Capabilities of Microsoft 365

Organizations are managing a growing volume of data and alerts, all while dealing with tight budgets and vulnerable legacy systems. In this environment, minimizing security risks is a massive challenge. At Protiviti, we believe confidence in cybersecurity and privacy does not come from knowing nothing will happen; it is achieved by knowing all the things that can happen and preparing both proactive and reactive solutions.

As a Microsoft Gold Partner, Protiviti can help your organization protect your environment from an ever-evolving threat landscape with a Microsoft 365 Incident Response Readiness Assessment. The objective is to assess your incident response readiness as it relates to your Microsoft 365 and Azure Active Directory environments and provide industry leading recommendations for deployment and configuration of Microsoft Cloud security tools and incident response protocols.


## Microsoft 365 Incident Response Readiness Assessment Deliverables

- Microsoft 365 Attack Simulation; Incident Response Table-Top Exercise in the Client's Production Microsoft 365 environment
- Documented Attack Simulation and Incident Response Findings and Recommendations
- Guided Data Governance Review in the Client's Production Microsoft 365 environment, with Documented Findings and Recommendations
- Configuration of a POC (Trial) Microsoft 365 environment with recommended Microsoft 365/AAD Security Tooling

INNOVATE. TRANSFORM. SUCCEED.

# Microsoft 365 Incident Response Readiness Assessment

Protiviti's Microsoft 365 Incident Response Readiness Assessment will help secure your business by providing the below activities and actionable insights to help you establish the right processes for cyber-risk reduction.

## Conduct M365 Attack Simulations

- Utilize M365 Attack Simulator in the client's Production
- M365 environment to conduct:
  - Spear Phishing Attacks (credential harvest & malware)
  - Brute Force Password Breach, Password Spray Account Breach
- Analyze & review simulation results
- Compare to expected/past results & industry standards

## Conduct Incident Response Simulation

- Conduct table top incident response simulation
- Observe/analyze response protocols & discuss gaps
- Demonstrate in a Protiviti M365 demo environment the industry leading practices for M365/AAD incident response: log analysis, content search/purge, inbox rule inspection, analysis tools, end user communications/training, automated investigation & response (AIR), Advanced Hunting & Azure Sentinel

## Additional Data Governance Review

In the customer's Production M365 environment:

- Review the Know Your Data/Data Classification page
- Configure Cloud App Discovery (snapshot report)
- Configure DLP Policies (in monitor mode)
- Review discovery & policy outcomes
- Provide recommendations for DLP, MIP, MCAS, Retention

## Configure Microsoft 365/AAD Security POC

Build a new POC M365 environment (trial tenant) including:

- Conditional Access (standard & risk based)
- Multi-factor Authentication/Disable Legacy Auth
- Privileged Identity Management (PIM)
- Defender for O365 (EXO, SPO/ODFB, Teams)
- Defender for Endpoints (limited endpoints)
- Microsoft Cloud App Security policies (monitor mode)
- Automated Investigation & Response

## Contact us today to schedule a Microsoft 365 Incident Response Readiness Assessment!


 Protiviti.com/Microsoft

 MicrosoftSolutions@Protiviti.com

 TCblog.Protiviti.com


Gold Microsoft Partner

Microsoft

protiviti®

*Face the Future with Confidence*