Microsoft 365 Incident Response

SERVICES:

Urgent Incident Response

Cyber IR Services include:

- Active Intruder/Breach
- Business Email Fraud
- Ransomware
- Insider Threat Investigations

Microsoft 365 Investigations/ Forensic Investigation

Microsoft 365 Electronic Discovery/Litigation Support

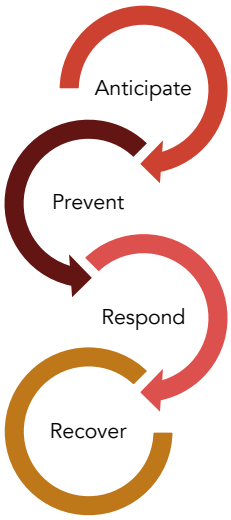
IR Project Services

Microsoft 365 Incident Response Plan Creation/Review

Microsoft 365 Digital Forensics and Incident Response (DFIR) Readiness Assessment

855-404-8324
cyderes.com

Microsoft 365 technologies are the de-facto standard for business cloud services. Entra ID is present in over 90% of the Digital Forensics and Incident Response (DFIR) incidents handled by Cyderes. Microsoft 365 services can be a bastion of safety for business continuity or a point of entry for an attacker depending on an enterprise's ability to understand, configure, and respond to threats in the Microsoft 365 environment.



Cyderes DFIR projects and services encompass the full security motion but emphasize your ability to respond.

- **Early identification of threats and assets** anticipates the most likely or most damaging attacks and aids the development of prevention efforts.
- **Well-planned, rational allocation of prevention resources** can prevent an incident entirely or allow for timely detection to minimize or contain damage from a determined attacker.
- There will always be **unanticipated attacks based on newly discovered vulnerabilities** like Log4j. Planning a capability to respond to such threats is part of the full security motion.
- **Resilience is the ability to recover quickly, even seamlessly, from attacks.** Microsoft 365 services can be accessed independently of internal resources as part of business continuity planning.

Cyderes offers resources throughout the full security motion. The Cyderes Threat Analysis Center (TAC) teams with Cyderes SOC Threat Intelligence to gather the latest indicators from hundreds of client telemetry and commercial providers. Cyderes Offensive Security Teams study the attacker's methods and tools to provide up-to-the-minute anticipation of threat actors. DFIR investigates and studies attackers' actions in live environments to test and confirm conclusions from the analysis of these sources.

The Cyderes TAC analyzes these inputs to deliver actionable advisory services in business-oriented terms, grounded in your industry, service and technology profile.

Examples of value delivered through Cyderes' Microsoft 365 expertise includes:

- Containment of an active threat through Microsoft Services while simultaneously allowing continuity of business-critical services and communication through Microsoft 365.
- Investigation of an intrusion exploiting credentials of privileged accounts.
- Providing vigilance over uncontained areas through Microsoft Defender and Sentinel to minimize operational impact during a ransomware attack.
- Advisory services to correct a litigation hold strategy for Multi-District Litigation supported by expert testimony (if needed).
- Planning an electronic discovery strategy through Microsoft 65 capabilities.

We look forward to helping you on your Microsoft 365 Incident Response journey. If you have any questions, please reach out to your Cyderes representative.