



WHAT IS IDENTITY THREAT DETECTION & RESPONSE (ITDR)?

Identity Threat Detection and Response (ITDR) is a dedicated security discipline focused on protecting identity infrastructure – such as Microsoft 365, Google Workspace, and Identity and Access Management (IAM) systems from credentials-focused attacks.

While Endpoint Detection and Response (EDR) monitors devices, ITDR monitors credentials, session tokens, and identity behaviour across cloud and SaaS environments to stop attackers who log in rather than hack in.

Why ITDR Has Become Essential

- ✓ MFA can be bypassed
- ✓ No malware is needed for an attack
- ✓ Traditional antivirus can't see an attack

How Does Managed ITDR Work?

While standalone ITDR software generates alerts, Managed ITDR pairs detection capabilities with 24/7 human analysis to validate threats and take direct action.

Continuous Visibility: Ingests live data from identity providers, cloud workspaces, and SaaS applications such as Microsoft 365 and Google Workspace.

Contextual Analysis & Human Validation: Filters out false positives by analysing whether an anomaly represents legitimate user travel or an active adversary.

Active Response: Automatically action to isolate the compromised user, terminate active sessions, block rogue app permissions, and reset credentials within minutes.



Protect Your Accounts With ITDR

To learn more about ITDR, please email jon@systemagic.co.uk.