Identity Threat Detection and Response (ITDR)

todyl

Todyl ITDR delivers critical, 24x7 protection from identity-based attacks, privilege abuse, and cloud security threats for organizations of all sizes.

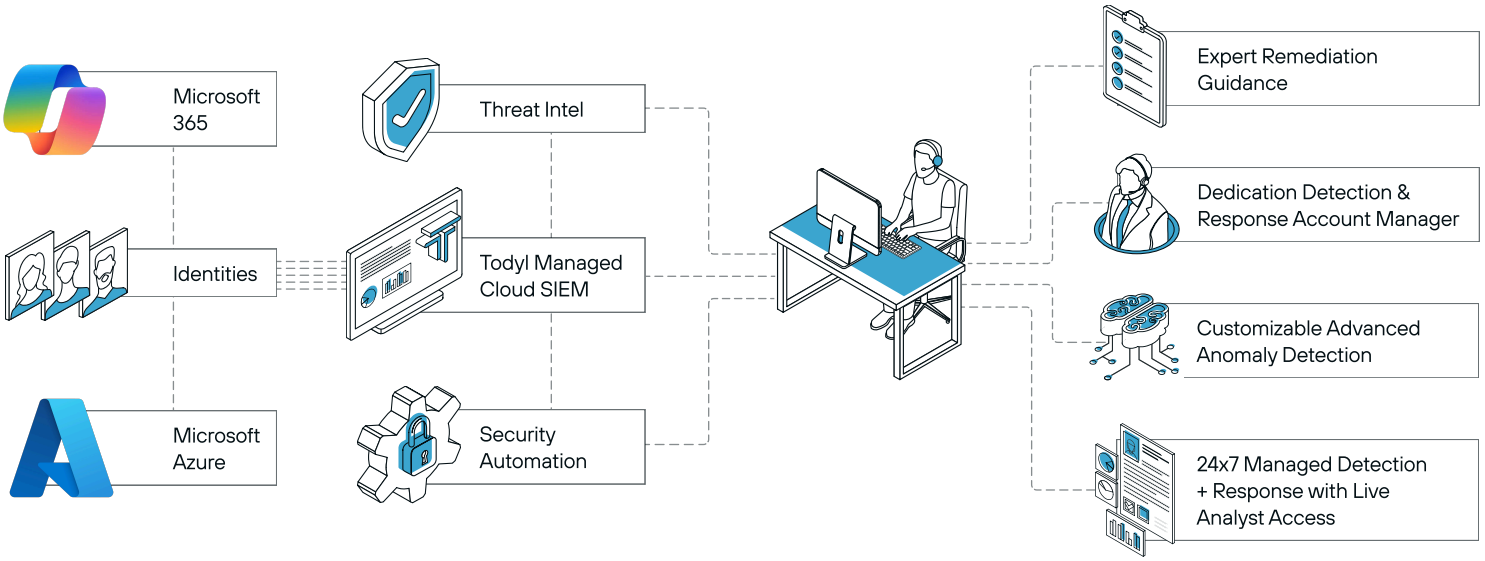
The Challenge

Identity-based threats are one of the most dangerous attack vectors for any organization, but small to mid-sized organizations rarely have the resources and expertise to detect and respond to attacks. Complex cloud architectures, multiple identity stores, and shorter detection windows make ITDR difficult to implement and manage without specialized tools and training. But ITDR is a critical component of any cybersecurity program and is necessary to protect organizations from identity-based threats like credential abuse and insider threats.

The Solution

Todyl's MXDR team delivers 24x7 expert ITDR services for Microsoft 365 and Azure environments, monitoring for anomalous identity usage and account access. Using Todyl SIEM's powerful anomaly detection framework, ML/AI-enabled analytics, and extensive internal and external threat intelligence, MXDR security analysts quickly detect and respond to identity-based attacks around the clock.

ITDR Under the Hood



Todyl ITDR in Action

Todyl's MXDR team delivers expert ITDR at a fraction of the cost of implementing an in-house program. Key capabilities include:

- Continuous monitoring and protection of cloud identities
- Rapid, automated containment of advanced attacks (ATOs, AitM, etc.)
- Herd immunity across all Todyl clients (BECs, Ransomware, etc.)
- Anomalous account access and usage detection

Detecting Business Email Compromises

Challenge
BECs are difficult to detect and respond to because they lack the IoCs (malware, unauthorized access, unusual behavior, etc.) that would typically trigger an alert. EDRs and other point solutions are easily bypassed by the lack of an obvious threat, and many behavioral anomaly detection rules may not have the established baselines needed to detect malicious activity.

Solution
Todyl ITDR analyzes extensive endpoint, network, and user telemetry to identify unique and/or suspicious activity that may be tied to an identity-based attack without requiring a behavioral baseline. IoCs that are investigated by the MXDR team within minutes, correlating data from multiple sources to quickly identify the origination and scope of the BEC.

Additional Todyl Benefit
All Todyl MXDR customers benefit from ITDR services, receiving proactive notification of critical and confirmed identity threats with 24x7 availability to expert analysts and herd immunity from attacks detected anywhere in the install base. Dedicated Detection and Response Account Managers (DRAMs) work with partners to implement SOAR playbooks to automatically prevent attacks like Account Takeovers (ATO) and Adversary-in-the-Middle (AitM) tactics.

Detecting Insider Threats and Stolen Credentials

Challenge
Insider threats and attacks using stolen credentials bypass detection by mimicking legitimate behavior to avoid triggering typical detection rules. Without ITDR in place, MSPs and their clients are blind to identity-based threats, and attacks frequently go undetected until long after the damage has been done.

Solution
Todyl's 24x7 MXDR team analyzes identity-related activity from across the Todyl Platform to quickly detect identity-based threats. Skilled analysts work around the clock to deliver attack context and expert response guidance, and also work with partners to proactively implement automated response playbooks for immediate containment.

Additional Todyl Benefit
Todyl customers have easy access to SASE and LAN Zero Trust, delivering Zero Trust Network Access (ZTNA) for remote users and endpoint micro segmentation for internal users to enforce least privilege to minimize risk and protect against lateral movement in the event of an attack.