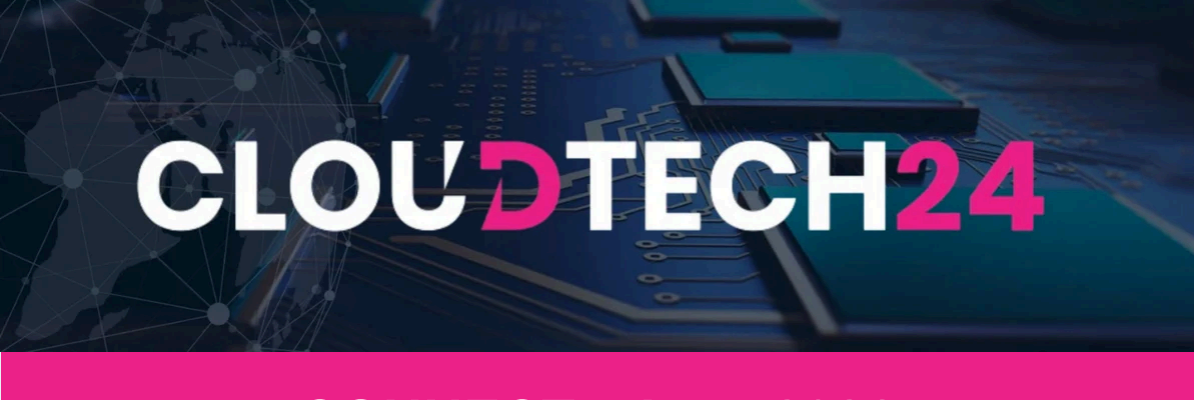




CONNECT - June 2026

NEW SERVICE

IDENTITY THREAT DETECTION AND RESPONSE (ITDR)

LAUNCHING OUR NEW ITDR SERVICE

Identity is now the primary attack path for cybercriminals.

Attackers are no longer focused on breaking through the perimeter. Instead, they are using compromised identities to gain legitimate access and move undetected across systems.

CloudTech24's Identity Threat Detection & Response (ITDR) is designed as a seamless extension of our Managed Detection & Response (MDR) service for clients using Microsoft 365, AWS or Okta platforms. While MDR focuses on detecting and responding to threats across endpoints, cloud and networks, **identity protection adds a critical layer focused on the one control attackers rely on most, user access.** Together, they provide a complete solution.

What ITDR delivers

- Real-time identity threat detection and prevention
- Reduced identity attack surface
- Rapid response to identity compromise
- Reduced operational burden

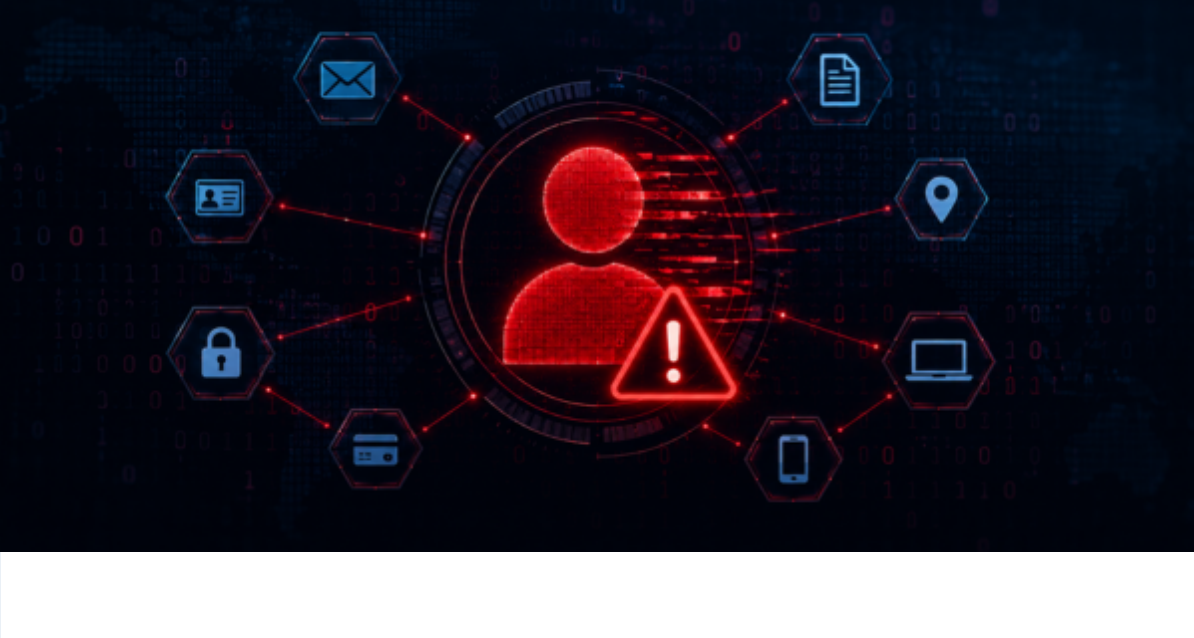
Key benefits

- **Lower risk of breach and faster incident containment** - ITDR identifies and stops identity-based attacks early.
- **Improved visibility and control** - Provides clarity over identity risks and how they are being managed.
- **Stronger compliance posture** - Demonstrate adherence to regulatory expectations and best practice frameworks.
- **Immediate value** - Deploy quickly with best practice controls in place from day one.

Click here to learn more

KEY CYBERSECURITY TREND

Increase in identity attacks



Each month, we'll take a look at a major cybersecurity trend and what this means for your organisation.

What's happening?

Cyber attackers are shifting from breaking into systems to simply logging in as legitimate users. A large proportion of breaches now involve stolen or compromised credentials. Instead of exploiting technical vulnerabilities, attackers target human identity and access points.

Key impacts of identity attacks

- **Data breaches and loss of sensitive information** - Attackers gain access to confidential customer, financial, or business data using valid credentials.
- **Financial loss** - Fraudulent transactions, ransomware payments, and recovery costs can be significant.
- **Reputational damage** - Loss of customer trust and brand credibility following a breach.
- **Prolonged exposure** - Because attackers "log in" as legitimate users, they can remain undetected for long periods.

Priorities for action

- **Adopt Zero Trust approach** - Apply least privilege access and regularly review permissions.
- **Implement Zero Trust architecture** – Continuously verify users and devices instead of trusting them by default.
- **Monitor and detect suspicious behaviour** - Use tools to flag unusual logins (location, device, time) and respond quickly.

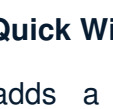
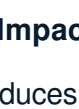
If you want to discuss the implications for your organisation, simply book a discovery call at a time that suits you.

Book a Discovery Call

THIS MONTH'S QUICK WIN

Enforce Multi-Factor Authentication (MFA)



 Threat	 Quick Win	 Impact
Most identity attacks rely on compromised passwords obtained through: - Phishing attacks - Credential stuffing - Brute force attacks - Malware/keyloggers - Social engineering	MFA adds a second verification step, such as phone code or app approval. This can often be enabled centrally via identity providers (eg. Microsoft and Google) and doesn't require major system re-design.	MFA reduces account takeover risk because even if attackers have the password they can't access the second factor.

EXCITING TIMES AT CLOUDTECH24

MEET OUR NEW TEAM MEMBERS

Our client-base is growing and so is our team

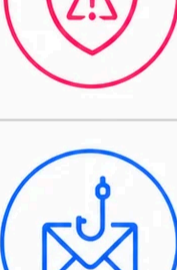
We're proud to be bringing more talented people into the business, adding even more expertise, experience and energy to what we do every day.

In the past month, we've welcomed Matthew (IT Security Engineer), Paul (Senior Account Manager), Lordine, John and Francis (IT Support Engineers), Nicole (Client Services Manager) and Sean (Account Manager). Take a look at our [Meet the Team](#) page to put names to faces!

It's great to be moving forward, and to be continuing to strengthen the level of support and service we provide.

MAY 2026

SECURITY MONITORING STATS



733

Real-world security events handled by **our team**



3,887

Phishing emails identified and remediated for **our clients**



747,100

Vulnerabilities patched, updated or remediated by **CT24 cybersecurity specialists**