Microsoft Security

Building an AI-powered, Unified SOC

Protect identities

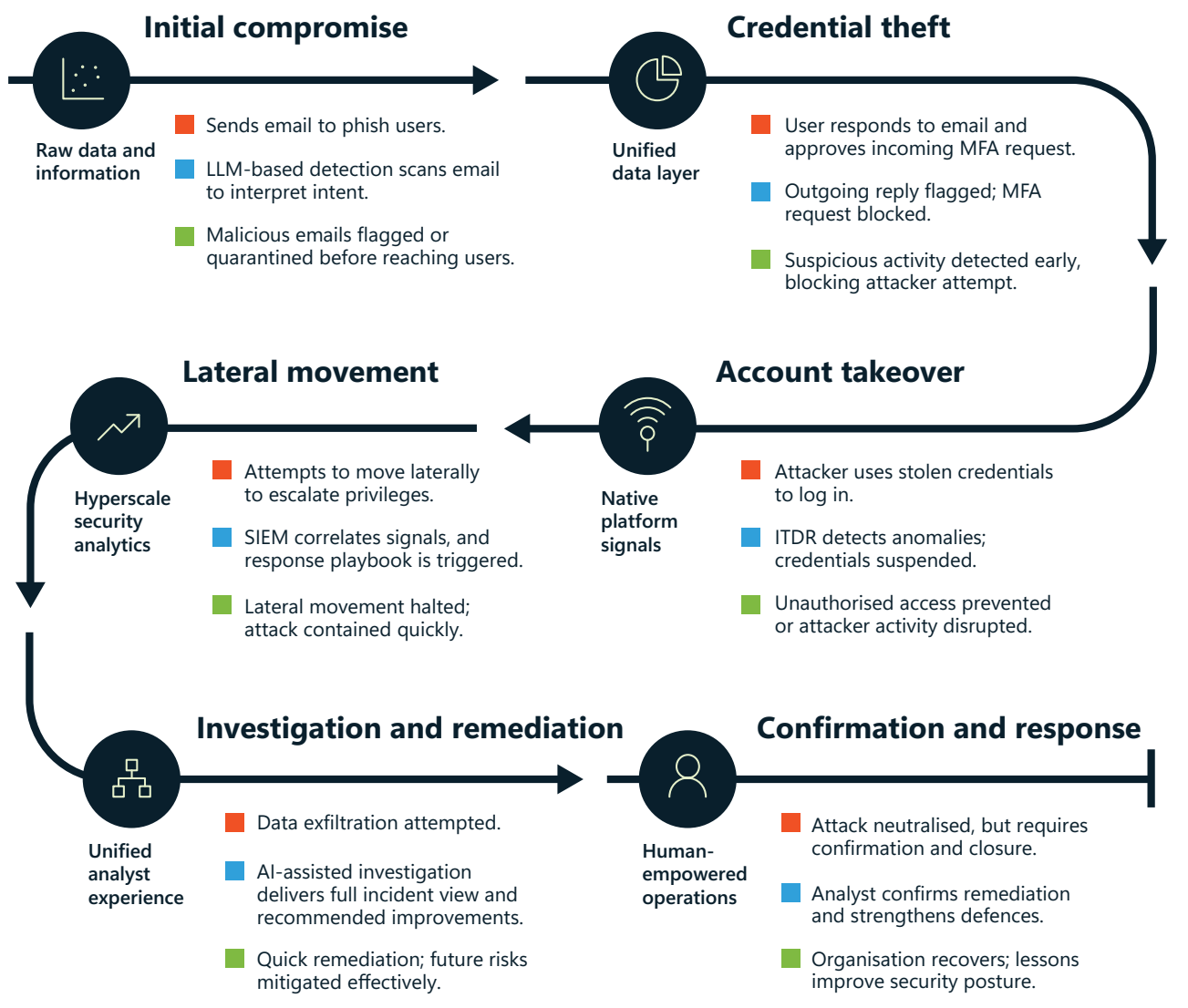
A unified SOC integrates AI-powered tools to deliver coordinated defence across your environment. In the following scenario – one of five that show how a unified approach strengthens defences and closes gaps attackers exploit – you'll see how unifying identity signals can detect phishing attempts, block credential theft and prevent lateral movement to ensure robust protection against account takeovers and insider threats.

Unified identity defence: Disrupting phishing and account takeover

This diagram shows how a unified security platform can disrupt phishing leading to account takeover at various points. It illustrates potential attack paths and the platform's response to specific attacker actions.

LEGEND

- **Attacker Action:** Actions taken by the attacker along potential attack paths.
- **Platform Action:** How the platform responds to specific attacker actions.
- **Outcome:** The result of the platform's response.



Key considerations for identity protection

Understand emerging identity-based threats and learn how unified defences can prevent account takeovers.

Phishing attacks

#5 Phishing attacks rank as the fifth most significant external threat among senior-level IT decision-makers whose primary role is security management.[1]

[1] 'The Unified Security Platform Era Is Here', Microsoft, 2024

Solution: **Microsoft's Identity Threat Detection and Response (ITDR)** solution analyses identity signals across your environment to detect stolen credentials in real time. By correlating signals and automating responses, ITDR unifies identity protection to stop threats quickly. **Microsoft Security Copilot** further strengthens ITDR by containing credential theft incidents and minimising damage with actionable insights.

Prevalence of password-based attacks

99% of daily identity attacks are pass-word-based.[2]

[2] 'Microsoft Digital Défense Report 2024', Microsoft, 2024

Solution: **Microsoft Entra ID Protection**, part of Microsoft's **ITDR** solution, defends against credential-based threats by enabling MFA and passwordless options across your environment. **Security Copilot** enhances this by monitoring adoption rates and providing recommendations to optimise defences, ensuring continuous improvement against password-based attacks.

Rise in AiTM phishing attacks

46% increase in AiTM phishing attacks.[3]

[3] 'Microsoft Digital Défense Report 2024', Microsoft, 2024

Solution: By analysing authentication patterns and identity signals across all identity systems – cloud and on-premises – **ITDR** can detect sophisticated AiTM phishing attempts. **Security Copilot** helps investigate these advanced threats and guides teams through rapid response steps to protect user credentials.

Unify your identity signals and disrupt phishing attempts with **Identity Threat Detection and Response (ITDR),** which integrates capabilities like **Entra ID Protection** for comprehensive account takeover protection

Want the full story? Discover how a unified SOC delivers coordinated defence across five key security domains: endpoints, identities, cloud-native applications, SIEM/XDR and data. Download **Coordinated Defence: Building an AI-powered, unified SOC**