COGNISYS

PENETRATION TESTING

Attack path management

Get a complete understanding of your attack paths through our expert analysis, strengthening your security against potential threats.

Protect your AD, Azure and AWS environments with attack path management

Attack Path Management is crucial for securing modern IT environments, as attackers increasingly target identity-based systems. With platforms like Active Directory, Azure, and AWS spread across various areas, managing attack paths within these systems is essential to prevent security breaches.

Our in-depth analysis identifies vulnerabilities such as privilege escalation, lateral movement, and weak configurations that threat actors can use to access sensitive data or gain admin control.

By replicating real-world attack scenarios, we provide actionable insights and remediation steps to close security gaps before they're exploited. This proactive approach ensures a robust security posture, protecting your assets and data across on-premises and cloud environments.

Scoping and planning

Define objectives

We work closely with you to define the objectives of our attack path management service, focusing on key security concerns and compliance requirements. Whether identifying identity-based vulnerabilities, securing privileged access, or assessing lateral movement risks, our approach is tailored to align with your organisation's security goals.

Requirements

We set up and prepare all necessary environments for a thorough assessment. This includes accessing platforms like Active Directory, Azure AD, and AWS configurations and integrating relevant security tools to map out potential attack paths. This setup enables a controlled and accurate evaluation of security vulnerabilities.

Tailored analysis

Our analysis is customised to meet your organisation's unique security needs, and we communicate regularly throughout the process. This ensures that our findings and recommendations are actionable and directly address potential attack paths, supporting a more robust, resilient security posture.

Core and advanced testing component

Configuration and access review

Our expert team thoroughly reviews permissions, roles, and settings across identity platforms such as Active Directory, Azure AD, and AWS. This foundational step uncovers misconfigurations or excessive privileges that could create potential attack paths, allowing us to fortify these systems against exploitation.

Blast radius analysis

We assess the blast radius of a compromised identity or asset, evaluating how an attacker could move from a single compromised point to reach critical assets like Tier-Zero Assets. Our analysis highlights containment gaps and guides the development of effective isolation strategies to prevent the spread of attacks.

Lateral movement simulation

Our expert team goes beyond permissions by simulating lateral movement to reveal how attackers might navigate between systems once inside. We use advanced techniques like Silver/Golden Ticket attacks, Kerberoasting, and pass-the-hash. We identify hidden pathways attackers could leverage to access high-value assets, strengthening defences across the network.

Why choose Cognisys' attack path management service?

Our Attack Path Management service offers a thorough and practical approach to finding and fixing attack paths across your systems. Using the latest tools and techniques, our experienced team identifies vulnerabilities. We provide clear, actionable steps to reduce risk and strengthen your security.

Partnering with us means you are taking a proactive step towards protecting your organisation. We help you to find potential risks and fix them before they can be exploited, ensuring strong protection against evolving threats. With our expert guidance, your critical systems and data stay secure.

BACK TO CONTENTS