COGNISYS
Smarter Cyber Security

Attack Path Management

Active Directory and Azure are hot targets for threat actors.

In a world where identities are the new security perimeter, compromising identity platforms like AD and AAD provides the greatest payoff for attackers, ultimately giving them control of all users, systems and data within the organisation.

Misconfigurations in these services can create 'Attack Paths', or chains of abusable privileges and user behaviours, which can provide attackers with a route to sensitive data and / or administrator access.

The primary goal of our Attack Path Management service is to provide a way of highlighting potential vulnerabilities in identity services, which in turn will allow organisations to mitigate the associated risks.

Continued overleaf...

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk

Organisations often don't have properly defined identity management processes in place, which means that users and devices can end up accumulating unnecessary access permissions.

Using our Attack Path Management (APM) service, organisations can chart relationships and connections within Active Directory and Azure Active Directory to gain a comprehensive understanding of the permissions given to individual objects, computers, and users. We also assess the impact that specific privileges have on overall security posture.

Method

Our APM toolset is non-invasive, meaning we can run the assessment without interrupting any normal activities. Our aim is to discover attack paths towards domain administrator privileges.

We can tailor the service to identify methods of access to areas containing sensitive data and methods to access sensitive applications, including:

- Scoping to understand exact requirements.
- Analysis of AD and AAD environment including:
  - Users, groups, devices and properties.
  - Security groups and domain trusts.
  - Abusable rights on AD objects.
  - Group Policies and OU structure.
  - SQL admin links, active sessions and privileges.
- Vulnerabilities and misconfigurations.

As a result of the analysis, you will gain a thorough understanding your identity environment including misconfigurations, credentials and user activities, which attackers can combine to create attack paths. This allows you to foresee an attack, and mitigate against it, before it happens.

Overview

Key benefits:

- Comprehensive mapping of relationships and connections within Active Directory and Azure Active Directory.
- Empirical, or practical, measurement of the impact that particular privileges have on the security posture of your organisation, systems and network.
- Precise and safe remediation advice.

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk