Attack Path Mapping

How to cut your pentesting budget in half while increasing the value ten-fold.

Attack Path Mapping (APM) acts as the cost effective and complementary bridge between pentesting and Red Team simulated attacks. You'll get to understand the characteristics of the most likely attacks and how to prioritize and structure your defenses, so you can focus your time and effort to protect what matters most to your organization.

What is Attack Path Mapping?

For decades, organizations have been relying on penetration testing to find vulnerabilities that could be exploited by adversaries. But as cyber criminals become more entrepreneurial and disruptive in their nature of attack - your defensive strategy should equally become more thorough, sophisticated and robust.

Attack Path Mapping (APM) is a new type of security testing, and it goes above and beyond the typical scanning and testing services you may be receiving without always having to invest in a full simulated attack exercise (Red Teaming).

APM quickly identifies and practically maps as many routes as possible through an environment that could be taken by a skilled attacker as they try to exploit vulnerabilities and enter computer systems or networks. It provides a widespread deployment of depth-first techniques to help our clients remove as many pathways as possible that could be exploited by a threat actor.

It is designed to chain attacks in a similar goal-oriented depth-first manner to Cyber Attack Simulation services, but its focus is not on actively avoiding alerts generated by Anti-Virus or Endpoint Detection and Response products, instead APM exercises generate a bounty of data for defenders to build detection rulings and alerts around.

While a Cyber Attack Simulation (Red Team) exercise is successful if the operator can reach the goal (or flag), an APM exercise will attempt to identify as many routes as possible for a threat actor to reach that same goal, but with the same impunity from detection/response that is granted to typical penetration testing activities.

Why APM should form a part of your cyber security strategy

- Addresses the real-world problems you face in a cost-effective manner compared to red teaming or simulated attacks
- Visibility of your network through a hacker's eyes to reveal overlooked weak spots
- Identification of choke points you can monitor to detect attacks in progress
- Prioritization of which vulnerabilities to fix first, so you're able to stop the most dangerous attacks. You'll also receive a thorough technical report with strategies and recommendations on fixes
- Creation of the most accurate simulated attacks, with the latest Threat Intelligence relevant to your sector and location, helping you to maximize investments in your security spend
- Informs continuous testing and evolution of defenses against new attack methods

+61 (0) 2 9552 4451 response@nccgroup.com www.nccgroup.com

How Attack Path Mapping Works

APM combines the tactics of pentesting with the goal-oriented approach of attack simulations. The key phases include:

In Phase

Identifies how hackers gain initial access to your network through tactics like credential stuffing.

Tests entry points like email, VPNs, cloud apps, and public web apps.

Through Phase

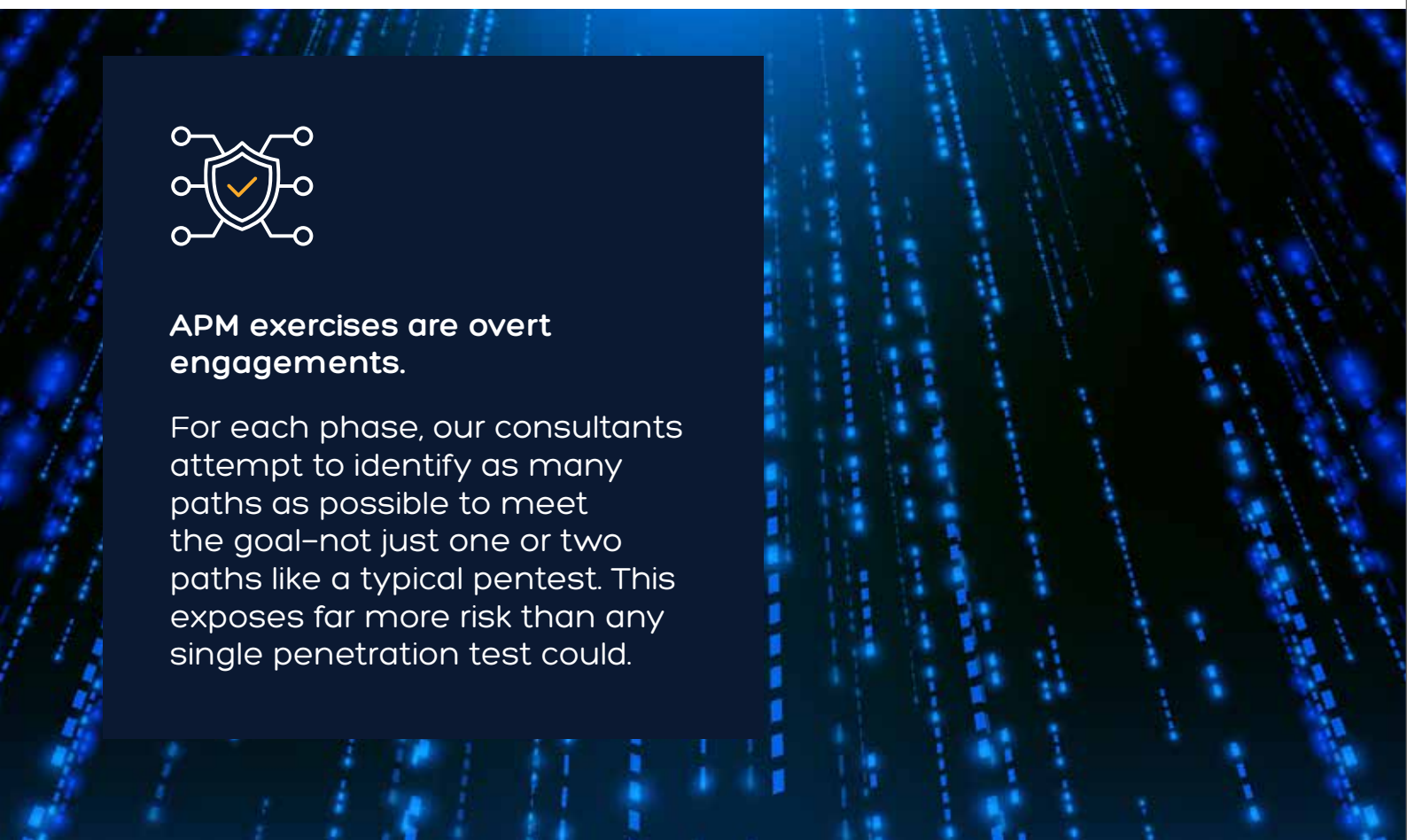
Maps how hackers could escalate privileges and move laterally between systems once inside your network.

Reveals vulnerabilities hackers use to expand access.

Out Phase

Determines how hackers could steal data or disrupt operations to achieve their objectives.

Focuses on vulnerabilities that lead to data exfiltration, command and control, and other critical impacts.



APM exercises are overt engagements.

For each phase, our consultants attempt to identify as many paths as possible to meet the goal–not just one or two paths like a typical pentest. This exposes far more risk than any single penetration test could.

How does APM compare to Penetration Testing?

We enable our clients to cost effectively understand the characteristics of their most likely attacks and how to prioritize and structure their defenses.

In Phase

The **"In"** phase focuses on assessing the technical controls in place to protect the environment from the typical methods used by threat actors looking to gain an initial foothold on the system and the activities utilised on the target devices. This includes:

- **Initial Access -** the techniques used by various threat actors and their associated entry vectors. This is how the attacker gains their initial foothold.
- **Execution -** the techniques used to achieve code execution on the targets host.
- **Persistence -** the techniques used to maintain or re-establish access following interruption.

Through Phase

The **"Through"** phase aims to identify the vulnerabilities typically exploited by threat actors to move through the network, increase permissions and identify high value targets on the network. This includes:

- **Privilege Escalation -** the techniques employed by threat actors attempting to increase their permissions on the target environment.
- **Credential Access -** the techniques threat actors use to gain access to account names and passwords.
- **Discovery -** the techniques used by threat actors to understand the target environment.
- **Lateral Movement -** the techniques utilised by threat actors to move from system to system in pursuit of achieving the objectives.

Out Phase

The **"Out"** phase is where the specific objectives for the target system are performed, what the impact is in the Confidentiality, Integrity or Availability aspects relevant to that system. This includes:

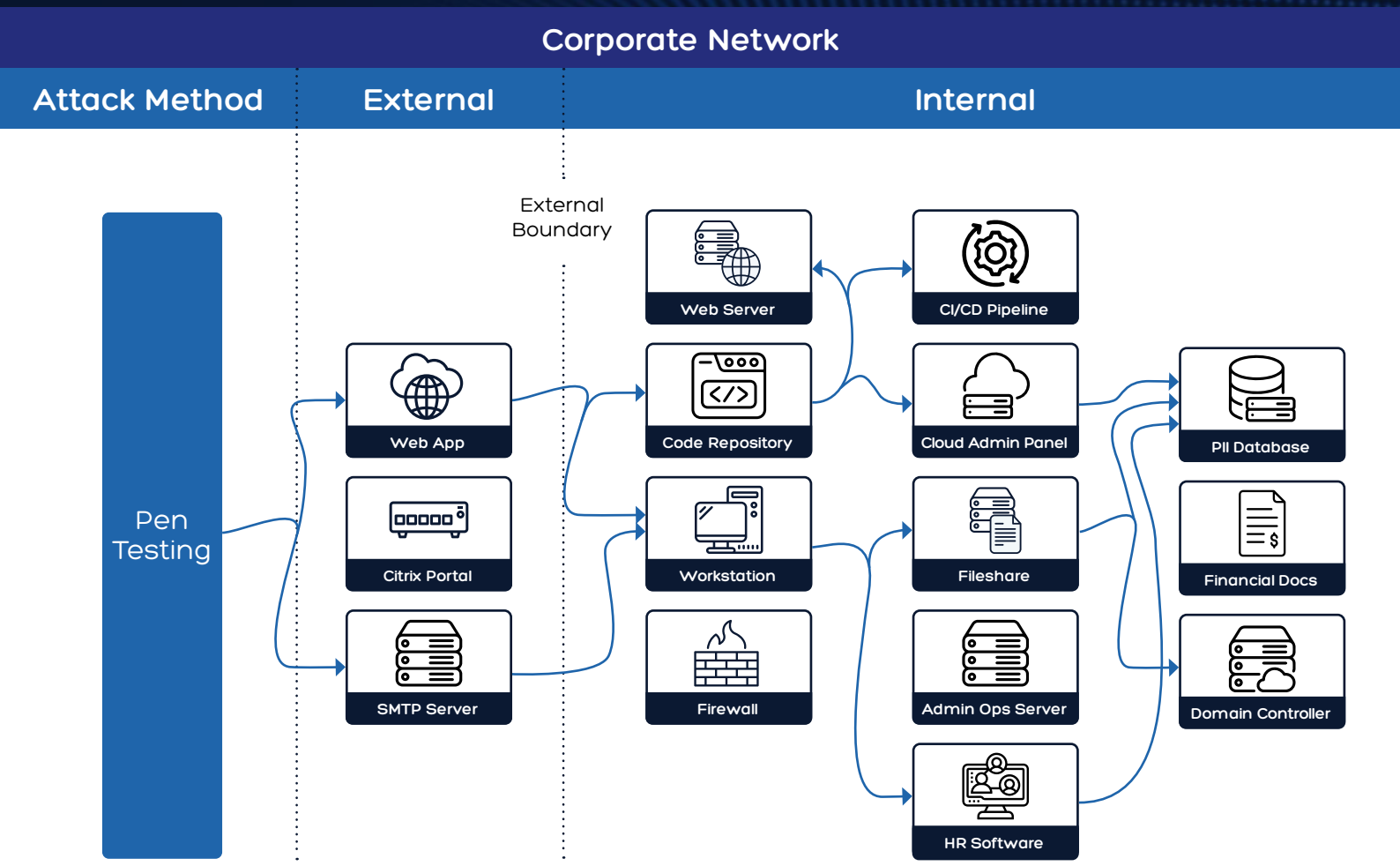
- **Collection -** the techniques utilised by attackers to identify and collect information.
- **Command & Control -** the techniques the threat actors use to communicate with the compromised environment and execute further attacks.
- **Exfiltration -** the techniques performed to get the data out of the comprised network.

+61 (0) 2 9552 4451 response@nccgroup.com www.nccgroup.com

How APM compares to Penetration Testing?

APM illustrates multiple paths an attacker could take to fully compromise your environment. It allows you to collaborate with us to list and execute specific tests that measures your resilience to compromising attack paths.

The key difference is that APM builds its value on your knowledge of your greatest cyber risks, and our ability to map multiple attack paths to those risks.

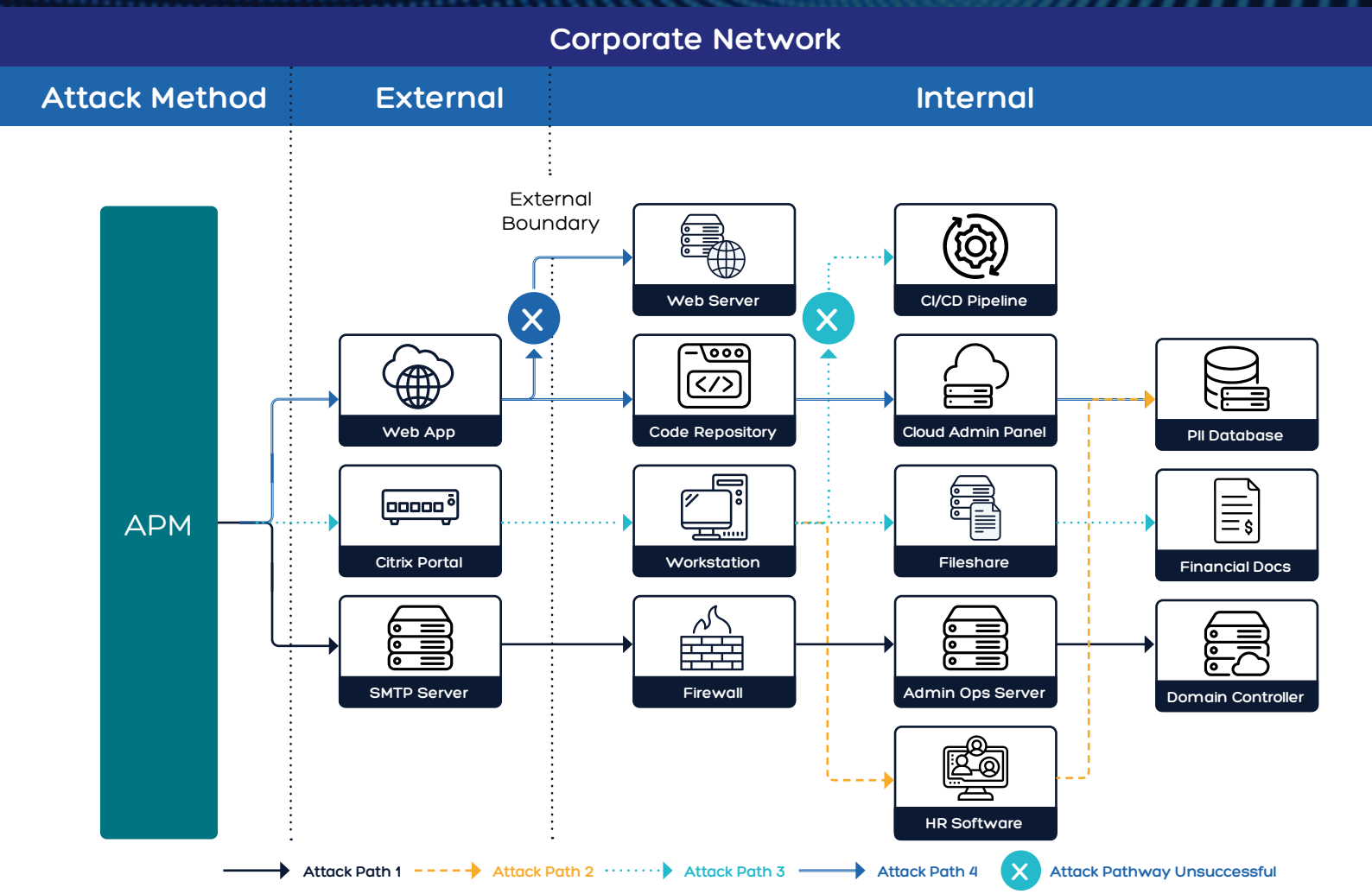


Pentesting typically uses an open-ended scope and relies on the realism of a 'zero-knowledge' approach to discover a subset of potential vulnerabilities and attempt to chain potential exploits together in a fixed time frame. Pentests can miss the larger context of an organization's most relevant threats, and only provides a snapshot of your overall risk with one or two attack-paths.

Know Your Attack Surface

NCC Group will identify the vulnerabilities and configurations that a threat actor can chain together to achieve compromise of your environment. APM shows more than just vulnerabilities, it shows you the art of the possible.

This will empower your teams to use attack paths as the best form of building your defense.



As you can see above, APM strives to show you all the ways a hacker could "get in, move through, and get out" of your network. This reveals more vulnerabilities than pentesting alone, and helps your organization prioritize which vulnerabilities to fix first and how to disrupt the most dangerous and impactful of attack chains.

+61 (0) 2 9552 4451 response@nccgroup.com www.nccgroup.com

What To Expect

Our APM exercises identify numerous dynamic attack paths. These may include:

Targeting your publicly accessible services such as email and web servers, VPNs, Virtual Desktop Environments, Microsoft365 instances and other public and hybrid cloud environments.

Simulating phishing attacks to assess the effectiveness of your security controls around communications.

Assessing if your workstation and server lockdowns are effectively restricting access to sensitive data as well as preventing unauthorised applications and custom payloads that may allow privilege escalation.

Determining to what extent lateral movement is possible within your network.

Identifying choke points within the attack chains that can be remediated to remove multiple pathways quickly and efficiently.

People powered, tech-enabled, Cyber Security

At the **heart** of cyber for over 30 years

NCC Group is a global cyber and software resilience business, operating across multiple sectors and geographies.

We're a research-led organization, recognised for our technical depth and breadth; combining insight, innovation, and intelligence to create maximum value for our customers.

As society's dependence on connectivity and the associated technologies increases, we help organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With over 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific.

Jordan LaRose
Global Practice Director for Infrastructure Security
jordan.larose@nccgroup.com

Kevin Dunn
Global Technical Assurance Lead
kevin.dunn@nccgroup.com

Our experts are here to help you.

Scan the QR code to discover how Attack Path Mapping can help protect your organization.