JUMPSEC

WHY ATTACK PATH MAPPING IMPROVES YOUR CYBER DEFENCES

www.jumpsec.com

Content

Many organisations fail to generate real cyber security improvement because they repeat the same types of activities each year. For most organisations, the level of security never truly improves over time. At best it stays the same, and at worst it declines as attackers effectively invest more than defenders.

Much of this challenge stems from the industry standard approaches to security testing and monitoring, which were designed for simpler networks than those of today. Lacking the complexity and scale of modern environments, they required minimal traversal required for an attacker to move from perimeter breach to the point of being able to complete an attack.

Networks today are much larger in size and scale, are much more diverse in terms of technologies implemented and the complexity of the assets, and are subject to more frequent development. This means that fixing every vulnerability, or monitoring for every adversarial tactic, technique, and procedure (TTP) is unfeasible and fails to reflect how an attacker will actually target a digital network.

An effective solution must focus on truly exploitable issues which enable an attacker to progress toward their objective. By building targeted controls against the most pivotal attacker actions, organisations can maximise the security value of their investment. We believe attack paths can be used to realise this outcome.

What are attack paths?

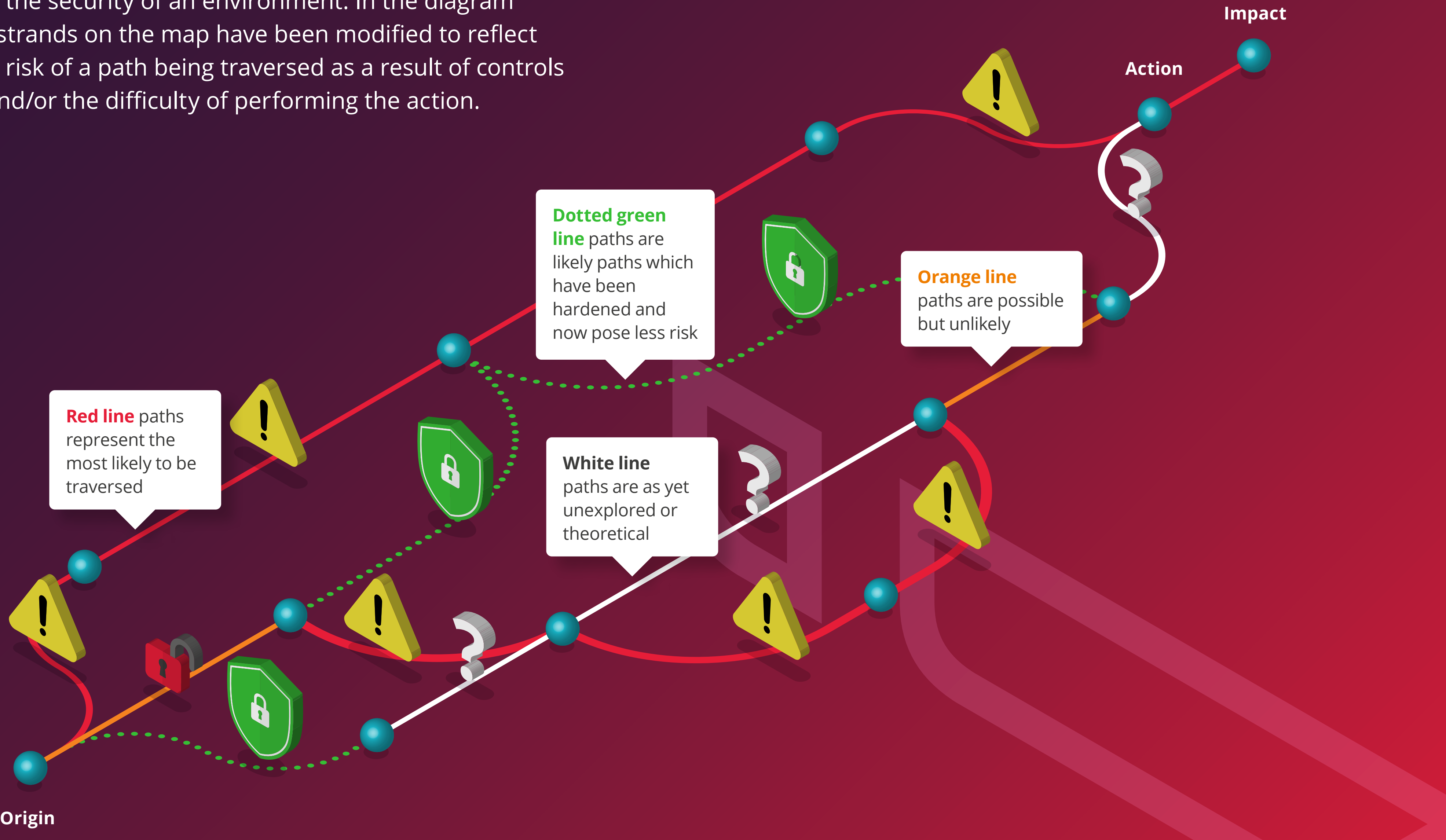
An attack path is a graph of an organisation and its digital assets based on how a cyber attacker will seek to target them. It describes the component actions which an attacker must complete in order for them to achieve their malicious objectives.

Understanding what an organisation must defend using attack paths facilitates an accurate understanding of which business processes, systems, technologies, and users are most likely to be targeted by an attacker, and how they are most likely to be abused. Once these paths are understood and mapped, they can be used to drive security operations activities through the implementation of prevention, detection, and response controls.

By nature, the process of mapping these attack paths is highly tailored and context-dependent. While attackers will often use similar tooling and tradecraft, we've observed that many out-of-the-box monitoring solutions fall short here. Generic detections often fail to afford the right level of coverage or pick up the most reliable indicators of malicious activity, because the severity of an action in one environment can be wildly different in another.

Many security monitoring vendors today claim to track attack logic and chain together events. But by starting with generic detections and attempting to link isolated events rather than building controls for specific attack paths, gaps in coverage and missed detections are all too common.

We see attack paths as a living representation of the impact of controls on the security of an environment. In the diagram below, the strands on the map have been modified to reflect the relative risk of a path being traversed as a result of controls deployed and/or the difficulty of performing the action.



Dotted green line paths are likely paths which have been hardened and now pose less risk

Orange line paths are possible but unlikely

Red line paths represent the most likely to be traversed

White line paths are as yet unexplored or theoretical

Building effective security controls

Attack paths provide defenders with a tactical advantage over adversaries. Hardening key nodes on the path where multiple strands converge can help organisations to control the battlefield; preventing or reducing the ability for actions to be performed, and funnelling attackers down known, predictable paths with effective monitoring controls to enable high-fidelity detection and response.

Closing or hardening every possible path is not an effective cyber defence strategy as it encourages motivated and well-resourced attackers to find novel methods of achieving their goal. By tactically increasing the complexity and cost of some actions but leaving others open, live threats can be more reliably detected, contained, and neutralised before real harm can be caused.

As a result of additional hardening activities, the relative risk of an attacker traversing a particular path or performing certain actions will be modified. This insight can be used to better contextualise and qualify the actual risk posed to an organisation of a specific scenario becoming a reality, clearly demonstrating the impact of cyber security investment upon business risk reduction.

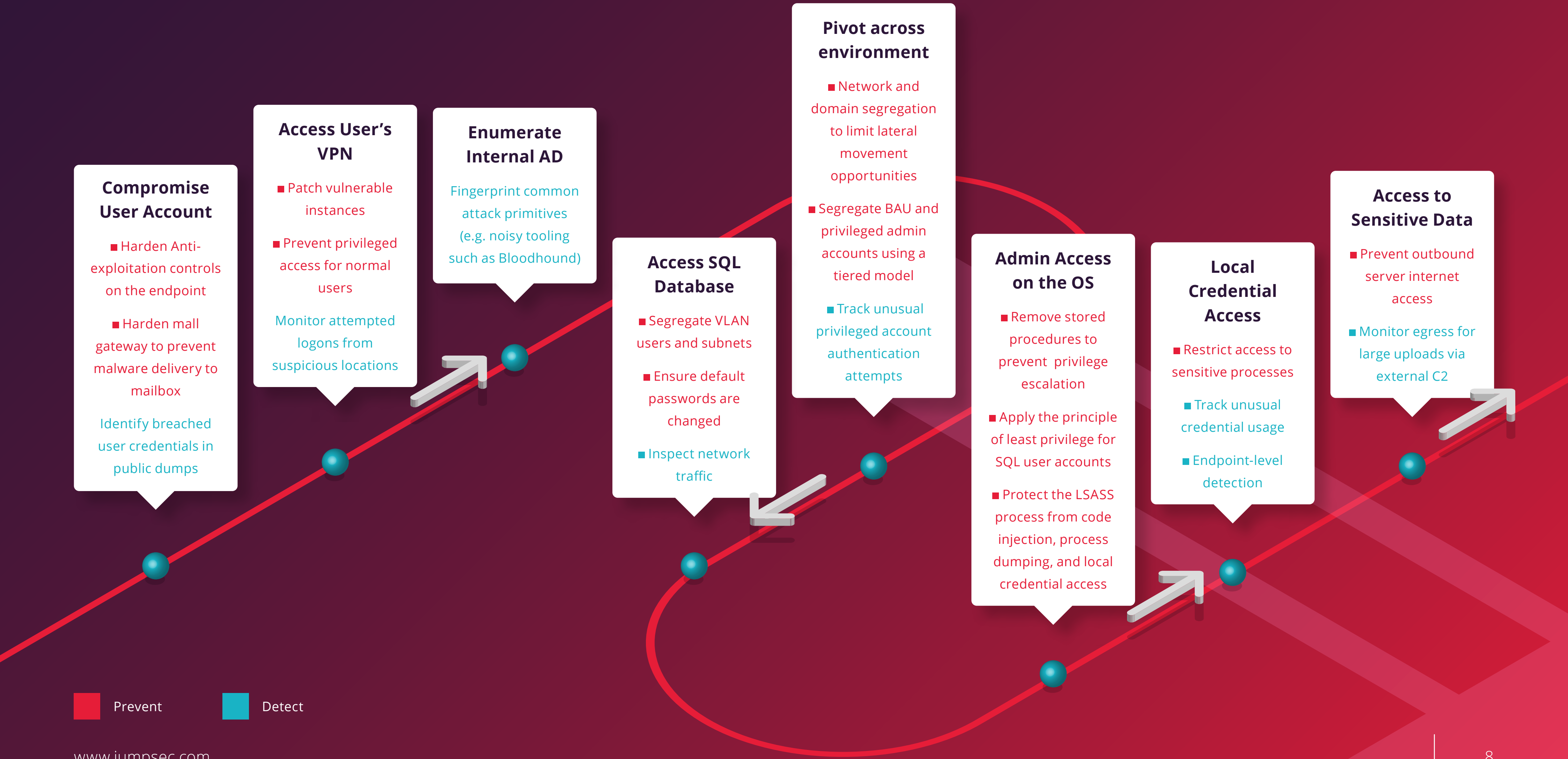
To be truly effective, cyber security controls should always be aligned with the desired level of risk reduction, and the nature of the threats faced by the organisation. Risk is typically understood as a calculation of the likelihood of an scenario occurring, multiplied by its potential impact. However, the cyber world is nuanced from an actuarial approach in that the value to an attacker (and therefore their motivation to perform an action) does not directly equate with its impact upon the business.

> Likelihood can be challenging to gauge in cyber security without understanding the context of the environment being targeted. Objective measures such as CVSS are not entirely reliable indicators of relative severity. This means understanding the attacker's viewpoint of an environment is vital to measuring risk.

Whilst it can be tempting to begin with the most destructive and damaging scenarios facing the business, these are not always the most likely when considering an attacker's objectives. **The most damaging scenario for you does not always reflect the most viable or profitable for an attacker.**

Attack path mapping in action

The diagram below illustrates how attack path mapping can be used to build targeted detection and response controls for an example environment, across a single thread of an attack path.



Compromise User Account

🟥 Harden Anti-exploitation controls on the endpoint

🟥 Harden mall gateway to prevent malware delivery to mailbox

Identify breached user credentials in public dumps

Access User's VPN

🟥 Patch vulnerable instances

🟥 Prevent privileged access for normal users

Monitor attempted logons from suspicious locations

Enumerate Internal AD

Fingerprint common attack primitives (e.g. noisy tooling such as Bloodhound)

Access SQL Database

🟥 Segregate VLAN users and subnets

🟥 Ensure default passwords are changed

🟦 Inspect network traffic

Pivot across environment

🟥 Network and domain segregation to limit lateral movement opportunities

🟥 Segregate BAU and privileged admin accounts using a tiered model

🟦 Track unusual privileged account authentication attempts

Admin Access on the OS

🟥 Remove stored procedures to prevent privilege escalation

🟥 Apply the principle of least privilege for SQL user accounts

🟥 Protect the LSASS process from code injection, process dumping, and local credential access

Local Credential Access

🟥 Restrict access to sensitive processes

🟦 Track unusual credential usage

🟦 Endpoint-level detection

Access to Sensitive Data

🟥 Prevent outbound server internet access

🟦 Monitor egress for large uploads via external C2

🟥 Prevent

🟦 Detect

Not all of these controls are particularly novel or advanced, and many organisations will implement them already. However, they might not know why these controls are important, or the impact that their existence – or failure – can have on security posture.

This insight can be used to inform the priority and criticality of alerts generated. It can also prompt organisations to invest in maintaining these vital controls, and testing their effectiveness at regular intervals.

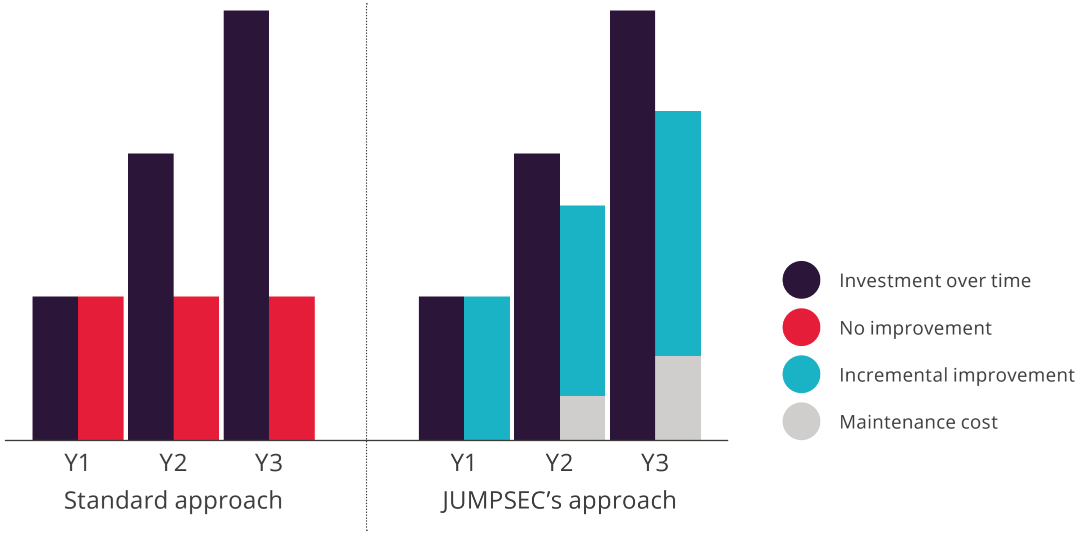
> Understanding the most prevalent paths across an environment and identifying the key prevention and detection opportunities at each node ensures that any investment in implementing, testing, and maintaining controls provides a clear security advantage, improving resilience and reducing susceptibility to attack.

Cumulative investment over time

Using attack paths means that, rather than repeating the same projects, organisations can spend their time and money building upon retained knowledge and exploring new threats each year.

Once a path is fully explored, hardened, and monitored, it can be maintained for a fraction of the initial investment. This enables the remainder of the annual budget to be allocated to further enhancing the security baseline and covering new ground, rather than fighting to maintain the same standard of security.

Comparison of a standard security spending model with JUMPSEC's incremental improvement model.



Using attack paths facilitates the creation of prioritised, threat- and risk-based cyber defences which will yield genuine security advantages in terms of preventing, detecting, and responding to malicious activity threatening to cause real harm to the business.

Beginning with the highest risk paths enables an organisation to build resilience against the most damaging attack scenarios as priority in year one, rapidly reducing risk exposure and ensuring that maximum resources are allocated to securing the most critical and prevalent paths.

Once the priority paths are mapped and secured, further paths can be covered to achieve a level of coverage and depth that makes sense for the business in question. It's important that this is tailored to the needs of the business in question, based on its threat profile and overall exposure to cyber security risk.

> It isn't possible to eliminate repeated investment entirely, as controls naturally must be maintained and updated in line with natural evolution (as a result of developmental changes, and emerging attacker tooling and tradecraft). That said, structured spending can enable the security bar to be raised over time without radically increasing the cost.

Getting started with attack path mapping

The starting point for any successful attack path mapping exercise is effective threat modelling; considering who, why, and how the organisation could be targeted by an attacker. Without this, the likelihood of a particular attack occurring, and its potential impact, cannot be gauged.

Why would an attacker target your business?

- What motivations would an attacker have for targeting your business?
- In what ways can an attacker benefit by attacking your business?
- What would the impact be if an attacker achieved their objectives?

What does your network look like to an attacker?

- What hosts have you exposed to the internet?
- What technologies have you deployed on your external facing hosts?
- What digital and information assets would present a risk to your business if compromised?

How is an attacker likely to execute an attack?

- How can an attacker manipulate your digital assets?
- How can your business processes be abused using legitimate / intended functionality?
- How can an attacker traverse your network to achieve their goals?

Where will an attacker look to breach your network?

- Where are the most likely and pivotal entry points to your network?
- Which technologies are you exposing to the internet that may be susceptible?
- Which users / user types pose the highest risk?

Once the most susceptible points of breach are identified to determine the potential origin of an attack, and the highest risk attacker objectives have been determined, organisations can begin to map the paths across their network that an attacker can take to achieve their objectives.

At this point, many organisations will have a lot of the required knowledge to build attack paths across their network, as they essentially rely upon understanding network topology, business processes, data flows, and system configuration – something that nobody knows about your business better than you. Speak to JUMPSEC about how you can transform your security operations using attack paths.

JUMPSEC
Unit 3E – 3F,
33 – 34 Westpoint,
Warple Way,
Acton W3 0RG

T: 0333 939 8080

E: hello@Jumpsec.com

www.jumpsec.com