cyberDNA

CONVERSATION ASSET — VOL. 01

Top 12 Identity Attack Paths Every Security Leader Should Understand

Most attackers don't break in anymore. They log in.

Today's attackers increasingly exploit identity rather than relying on traditional malware or noisy intrusion techniques.

Compromised credentials, excessive privilege, stale accounts, and hidden trust relationships often create the fastest path to organisational compromise.

This executive briefing outlines 12 common identity attack paths security leaders should understand to better assess exposure and reduce breach risk.

CYBERDNA EXECUTIVE BRIEFING

THE IDENTITY ERA OF BREACH

Why Identity Attack Paths Matter

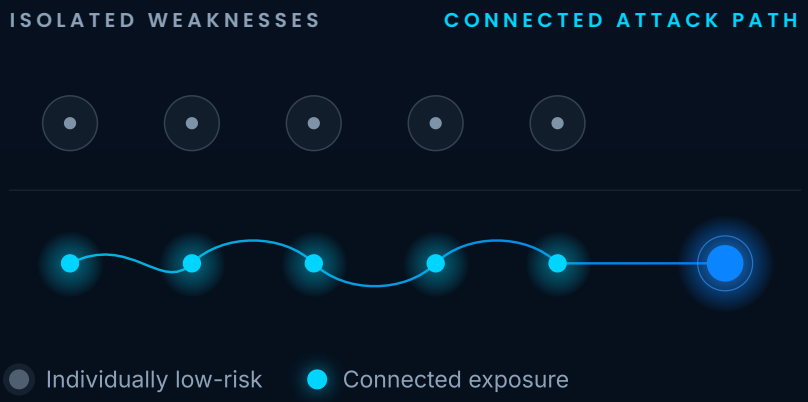
Many organisations focus heavily on endpoint protection, perimeter controls, and alerting.

Yet attackers increasingly succeed by abusing legitimate access instead.

A single compromised credential may not seem critical on its own. Neither might an old admin account, a poorly managed service account, or an over-permissioned cloud identity.

The real risk emerges when these weaknesses connect.

Identity attack paths allow adversaries to move laterally across environments, escalate privileges, establish persistence, and expand compromise while appearing as legitimate users.



> Security leaders need visibility not only into individual identity risks, but into how those risks combine into exploitable attack paths.

Credential & Kerberos Abuse

PATHS **01–04** OF 12

01 Password Spraying

Rather than repeatedly targeting one account and triggering lockouts, attackers test commonly used passwords across many accounts at low volume until valid access is found.

This remains an effective technique in environments with weak password hygiene, incomplete MFA coverage, or legacy authentication exposure.

RISK Stealthy initial access using valid credentials

02 Kerberoasting

Attackers request Kerberos service tickets tied to service accounts, then attempt to crack them offline to recover credentials.

Because service accounts often carry elevated privileges and are poorly managed, this can quickly become a privilege escalation pathway.

RISK Escalation from low access to privileged control

03 Pass-the-Hash

Attackers steal credential hashes from compromised systems and reuse them to authenticate elsewhere without needing to know the actual password.

This technique enables rapid movement across environments, particularly where local admin access is widespread.

RISK Fast lateral movement across systems

04 Golden Ticket

After compromising key Kerberos infrastructure, attackers can forge authentication tickets that grant persistent high-level access.

This effectively gives attackers long-term control over trusted identity infrastructure.

RISK Deep persistence and domain compromise

Privilege, Persistence & Session Risk

PATHS 05–08 OF 12

05 Service Account Abuse

Service accounts often run critical applications and integrations, but many are over-permissioned, shared, poorly monitored, or rarely reviewed.

Attackers frequently target these accounts because they provide quiet access with fewer behavioural anomalies.

RISK Hidden persistence and escalation

06 Stale Privileged Accounts

Accounts belonging to former employees, role-changed administrators, or legacy projects often remain active longer than expected.

These forgotten identities can provide attackers with privileged access that no one is actively monitoring.

RISK Invisible privileged exposure

07 MFA Fatigue / Push Bombing

Attackers repeatedly trigger MFA requests in the hope that users eventually approve one out of confusion, fatigue, or urgency.

Because authentication appears legitimate, compromise can be difficult to distinguish from normal activity.

RISK Socially engineered account compromise

08 Token Theft / Session Hijacking

Instead of stealing passwords, attackers capture authenticated session tokens that allow them to inherit already trusted access.

This can bypass MFA entirely and enable prolonged access without repeated authentication.

RISK Persistent stealth access

Trust, Hybrid & Cross-Environment Chains

PATHS 09–12 OF 12

09 Delegation Abuse

Improperly configured delegation settings can allow attackers to impersonate other users or services.

What appears to be a technical configuration issue can become a powerful privilege escalation mechanism.

RISK Privilege escalation through trust abuse

10 Hybrid Identity Misconfiguration

Many enterprises operate across both on-prem Active Directory and cloud identity platforms such as Entra ID.

Weak trust relationships, sync misconfigurations, or poorly aligned privileges between environments can create attack paths that span both.

RISK Cross-environment compromise

11 Over-Permissioned Cloud Roles

Cloud identities often accumulate excessive access over time, especially where privileged access reviews are inconsistent.

Attackers exploit these permissions to expand impact far beyond the initially compromised account.

RISK Broad cloud compromise

12 Attack Path Chaining

Modern breaches rarely rely on a single weakness.

Attackers combine multiple low-risk identity exposures into a connected pathway that enables broader compromise. A compromised user account, stale privilege, and an exposed service account may appear manageable individually, but together can create a direct route to critical systems.

RISK Full enterprise compromise

FROM ISOLATED RISK TO CONNECTED EXPOSURE

One weak identity control rarely causes a breach. Connected weaknesses do.

Understanding isolated risks is useful.

Understanding how they connect is what reduces breach likelihood.

If helpful, we'd be happy to have an initial discussion about your current approach to identity exposure and attack path risk.

Request an Initial Conversation →

OR

CONTACT
sales@cyberdna.com.au

WEB
cyberdna.com.au

QUESTIONS SECURITY LEADERS SHOULD ASK

Five questions to take to your next leadership conversation.

- Where do privileged attack paths exist today?
- Which stale identities remain active?
- Could an attacker move laterally without detection?
- How quickly would identity abuse be identified?
- Are identity risks assessed individually, or as connected exposure paths?