External Threat Exposure Assessment

If an attacker targeted your organisation today, what would they see - and what could they exploit?

Many cyber incidents no longer begin with sophisticated attacks. Instead, attackers increasingly exploit exposed internet-facing systems, misconfigurations, leaked data, and publicly accessible services.

Kordia's External Threat Exposure Assessment provides an outside-in view of an organisation's cyber risk, identifying weaknesses across its external digital footprint that could be discovered and exploited by a threat actor.

What we assess

- External attack surface
- Internet-facing domains, subdomains, web applications and APIs
- Shadow IT and unmanaged or forgotten assets
- Exposed services, vulnerabilities, and high-risk configurations
- Dark web and threat intelligence
- Targeted dark web searches for organisational data or credentials
- Validation of whether exposed information is current and exploitable
- Indicators of potential or emerging threat actor interest

What you'll gain

- Executive summary outlining key risks and business impact
- Risk-rated findings across external exposure
- Clear distinction between theoretical and exploitable risk
- Prioritised, actionable remediation roadmap

Best suited for

- Organisations with internet-facing portals, applications, or APIs
- Healthcare, government, and critical service providers
- SOC customers seeking assurance beyond monitoring
- Executive teams seeking clarity on real-world cyber exposure

How it's delivered

- Lightweight, non-disruptive assessments
- No credentialed access required
- Delivered by Kordia's DFIR and CTEM specialists
- Typical delivery timeframe: 1–2 weeks

Optional follow-on services:

- Incident Response Retainer
- Threat Hunting
- Dark Web Monitoring
- Continuous Threat Exposure Monitoring

Understand what attackers can see and exploit - before they do.

CONTACT US AT:

0800 kordia | kordia.co.nz

kordia®