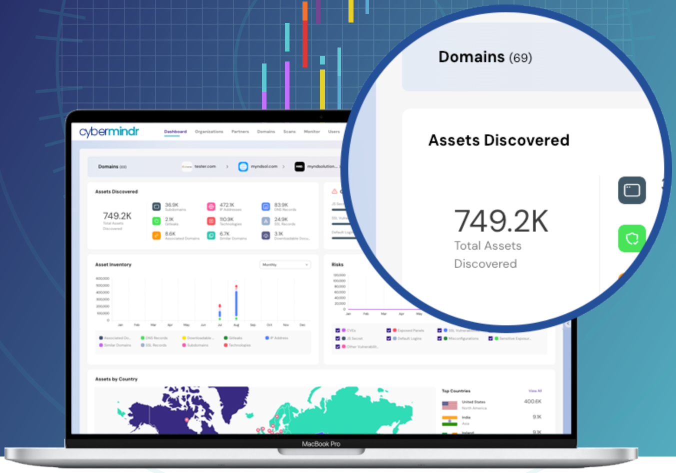
POWERED BY WATI

cybermindr

Automated Attack Path Discovery

CyberMindr is a cloud hosted, external solution to discover and tests for things that can allow an attacker to gain access to or exploit your organization.

We call this
Automated Attack Path Discovery



WHAT IS AN ATTACK PATH?

An attack path is a sequence of steps or actions that an attacker may take to gain unauthorized access to a system, network, applications, cloud, etc. In other words, this is how the bad guys get in.

Automating knowledge of experienced red teamers, bug bounty hunters and ethical hackers, **CyberMindr** discovers these attack paths so you can close them before they are exploited.

The platform leverages millions of data points from across the deep, dark and surface web. Many external assessment tools gather data through passive methods, using Open Source INTelligence (OSINT) as well as broad internet scanners as data sources. In many cases this information is older and may represent a picture of how you were and not how you are. By adding in a variety of active assessment techniques, the **CyberMindr** provides more current and more granular data. This provides a better picture of the true state of your cyber posture.

CyberMindr results will show what asset has the issue and wherever applicable, provide detailed information as how to reproduce the problem. This will typically be enough information to help quickly plan out the remediation effort.

15,000+ ATTACK TEMPLATES

300+ HACKER FORUMS MONITORED

Providing organisations with unprecedented insight into the breadth and depth of potential compromises on both the deep and surface webs.

CAPABILITIES:

— **Asset Enumeration:**
- Domains: Corporate domain information, Similar or Related Domains
- Subdomains: Subdomains as well as Orphaned Subdomains
- Deployed technologies
- Ports

— **Corporate email hygiene:** Check for the proper configuration of your email servers to improve your email security hygiene (DMARC, SPF, DKIM, BIMI settings)

— **Indicators of compromise:**
- Botnet Leaks - See evidence of sensitive company information, including user credentials, being exfiltrated via botnet infections.
- Leaked credentials that are currently being sold or traded in the hacker markets.

— **External vulnerabilities:**
- Misconfigurations that happen during the server or database setup, network configuration, or application settings stages of the application development and deployment process.
- SSL related issues
- Unintended exposed portals
- Common vendor specific vulnerabilities (CVEs)
- Commonly seen platform vulnerabilities
- Vulnerability validation - Custom vulnerability scripts validate exploitability.

— **Concerning exposures:**
- Surface exposed API keys in webpages and GitHub
- Downloadable documents
- Filetypes not typically exposed visible externally
- Publicly accessible code that may contain privileged account information or exposed keys.

BENEFITS

☑ **Cloud-based SaaS Platform:** No Hardware, No Agent, No Deployment.

☑ **Eliminate attack paths:** Actionable intelligence from i-Radar will help you remediate real issues faster.

☑ **We monitor the forums so you don't have to:** Our security teams go to the places that you don't want to.

☑ **Distributed Global Bot Network:** Identify more by leveraging our global bot network built to automatically detect, fingerprint, and identify exposed digital assets.

☑ **Multi-Stage attacks templates:** Increase the visibility of easily exploitable attack paths.

☑ **Comprehensive Risk Analysis:** Detect data exposures, authentication and encryption vulnerabilities, misconfigured services, architecture flaws, phishing attacks, and other risks. This is in addition to the common vulnerabilities and exposures (CVEs).

☑ **Remediation prioritization:** Gain actionable intelligence of what needs to be addressed: CyberMindr results will show what asset had the issue and wherever applicable, provide detailed information as to how to reproduce the problem.

Need help with remediation?
Let our experts help.

We maintain a team of security experts that can be engaged as needed.

CLICK HERE FOR **DEMO**