cyberDNA

REDUCE CLOUD BREACH RISK BY UP TO 90% IN 90 DAYS

MANAGED CLOUD RESILIENCE

www.cyberdna.com.au

THE REALITY

CLOUD EXPOSURE HAS BECOME THE FASTEST PATH TO BREACH

In modern AWS, Azure, GCP, Kubernetes, and CI/CD environments, risk accumulates silently long before security teams are aware.

- IAM privileges expand unnoticed
- Public storage and services become exposed
- Vulnerabilities remain internet-reachable
- Secrets leak through pipelines
- Attack paths form before alerts appear

THE RISK

WHEN CLOUD EXPOSURE PERSISTS, IMPACT ESCALATES FAST

- Lateral movement occurs across cloud identities
- Privileges are abused rather than stolen
- Data becomes reachable from the internet
- Breach impact grows before detection

Cloud security is no longer a tooling problem.
It is a resilience and engineering problem.

KNOW YOUR REAL CLOUD BREACH EXPOSURE

CLOUD EXPOSURE ASSESSMENT

MCR begins with a Cloud Exposure Assessment that establishes a measurable baseline of exploitable cloud risk.

- Internet-reachable vulnerable workloads
- Over-privileged IAM identities and trust paths
- Public storage, services, and APIs
- Secrets leakage and DevSecOps exposure
- Real attack paths to sensitive data

INTRODUCING MCR

MANAGED CLOUD RESILIENCE

Managed Cloud Resilience (MCR) is a fully managed, engineering-led service that continuously detects, prioritises, and removes exploitable cloud risk across AWS, Azure, GCP, Kubernetes, and CI/CD.

WHAT MCR DELIVERS

MEASURABLE CLOUD RISK REDUCTION IN 90 DAYS

- Up to 90% reduction in exploitable cloud exposure
- Clear visibility across multi-cloud environments
- Rapid remediation of real attack paths
- Continuous resilience improvement through engineering
- Executive-ready reporting and measurable metrics

HOW IT WORKS

FROM CLOUD EXPOSURE TO CLOUD RESILIENCE

Discover

Continuous visibility into exploitable cloud and DevSecOps exposure.

Prioritise

Validation of real attack paths and business impact.

Remediate

Embedded engineering removes high-risk exposure.

Strengthen

DevSecOps guardrails prevent re-exposure.

Prove

Clear measurement of resilience improvement over time.

CONTINUOUS RISK REDUCTION

BEYOND POSTURE MANAGEMENT

Traditional cloud security tools generate findings.
MCR delivers continuous remediation and resilience uplift.

- Weekly exploitability-driven prioritisation
- Ongoing remediation of real exposure
- DevSecOps guardrail improvement
- Biannual adversary simulation
- Executive resilience measurement

This is continuous engineering-led risk reduction, not monitoring.

ENGINEERING-LED DELIVERY

DELIVERED BY CYBERDNA CLOUD SECURITY ENGINEERS

- → Continuous exposure analysis and prioritisation
- → Embedded remediation execution
- → DevSecOps security uplift
- → Adversary simulation and resilience validation
- → Ongoing measurement and executive reporting

WHO MCR IS FOR

DESIGNED FOR ORGANISATIONS THAT...

- Operate multi-cloud or cloud-first environments
- Run active DevOps or CI/CD pipelines
- Face compliance, insurance, or board pressure
- Lack dedicated cloud security engineering capability
- Want measurable resilience, not dashboards

WHY CYBERDNA

SPECIALISTS IN IDENTITY AND CLOUD BREACH RISK

CyberDNA focuses on removing the real paths attackers use.

01 **Engineering-led managed security services**

02 **Identity and cloud resilience specialisation**

03 **Deep Microsoft and multi-cloud expertise**

04 **Trusted by Toyota, Hyundai, 7-Eleven, and growing SMBs**

TOYOTA 7-ELEVEN HYUNDAI

START WITH YOUR CLOUD EXPOSURE ASSESSMENT

Begin with a complimentary Cloud Exposure Assessment and see how quickly exploitable cloud risk can be reduced.

Run Assessment ›

sales@cyberdna.com.au

03 94543 999

www.cyberdna.com.au

linkedin.com/company/cyberdna

CyberDNA PTY LTD
459 Collins St, Melbourne VIC 3000,
Australia