Exposed Enterprise Data Search & Neutralization

Exposed enterprise data is a critical issue that arises when sensitive corporate information inadvertently or intentionally becomes accessible on the open, deep, or dark web. This can occur due to a variety of reasons, including human error, inadequate security measures, or targeted cyberattacks.

Deny attackers the opportunity to leverage exposed enterprise data by responding quickly to breach data, improving social media OPSEC, and hardening your external attack surface. Picnic employs a multi-faceted approach that encompasses open, deep, and dark web monitoring to identify and mitigate potential risks.

Select Capabilities & Services

- Open, deep, and dark web monitoring
- Red Team reconnaissance
- Corporate and personal social engineering risk scoring
- Social media monitoring for operational security breaches
- Corporate data exposure monitoring

CISO

Safeguard digital identity assets, respect customer privacy, counter social engineering risks, and ensure business continuity.

CIO & CTO

Improve your cybersecurity defenses to stay ahead of emerging threats and protect critical systems, networks, and data.

SOC Professionals

Reduce your MTTD by proactively and continuously managing your organization's human attack surface.

Third-Party Risk Professionals

Get the tools to make informed risk management decisions quickly regarding the companies within your organization’s supply chain.

Schedule a demo