Outmaneuver threat actors by using their secret weapon against them

The modern social engineering landscape is complex and evolving. Security investments in areas such as training and awareness, mail gateways, and endpoint protection have not stemmed the tide of human attacks.

Picnic's unique intelligence empowers threat intelligence leaders by exposing how threat actors can compromise your organization's human attack surface so you can identify, detect, prioritize, monitor, and remediate social engineering threats targeting your organization.

Security teams lack the capability to map threat intelligence of TTPs involving social engineering and other personal data exploitations to their employee population. Picnic directly addresses this intelligence gap by automatically combining external threat intelligence with human risk mapping, allowing defenders to prioritize and mitigate corporate and individual risk at scale. The result is a company and workforce that are much less exposed and much less vulnerable to today's threat actors.
Manit Sahib, Director of Global Threat Intelligence, Picnic

Select Platform Capabilities, Services, & Use Cases

Human attack surface management

Prioritize and mitigate corporate and individual risk at scale by combining external threat intelligence with human risk mapping.

High-Value Target protection

Protect the human attack surface for executives, board members and employees with access to sensitive data.

Suspicious domains & accounts detection

Detect attacker infrastructure before it can be used in social engineering attacks against your digital VIPs, their immediate network, or an entire workforce.

Impersonation attack prevention

Proactively prevent impersonation attacks against your employees and your company.

Schedule a demo

www.getpicnic.com