



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

The increasingly dynamic threat landscape has security operations and incident response teams being bombarded with an increasing number of security alerts every day. Threat actors are constantly evolving their tactics, techniques, and procedures (TTPs), which requires SOC teams to adapt quickly to new threats and risks, such as Generative AI.

Picnic's Threat Intelligence sources data from the most relevant OSINT and Darknet channels, marries it to customer's business needs, and provides valuable insights directly to security workflows to enhance alert prioritization, threat detection, and blocking.



Attackers today are leveraging data from employees' personal accounts to breach organizations. In this threat environment, companies need to know what data is out there that poses a risk and be able to reduce and proactively neutralize the data before it can be exploited. Picnic's platform allows security teams to do exactly this. Carlos Neto, VC Investor and Entrepreneur, Bright Pixel



Select Platform Capabilities, Services, & Use Cases

High-Value Target protection

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



Automated credential stuffing protection

Prevent reuse throughout the organization of compromised corporate and personal passwords that could be used in credential stuffing attacks.



Human attack surface management

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



SMS attack & phishing risk neutralization

Tackle smishing and phishing risk comprehensively before attacks even happen by reducing the human attack surface and addressing exposed data.



[Schedule a demo](#)