PICNIC™

HUMAN ATTACK SURFACE MANAGEMENT PLATFORM

Automated risk detection, prioritization and mitigation

getpicnic.com

WHAT IS PICNIC?

The vast majority of cyberattacks today leverage exposed personal and corporate data for social engineering and initial access, resulting in successful ransomware attacks, compromised data, sabotaged business operations, reputational damage, and financial losses. When virtually all cyberattacks are specifically crafted from the data tied to your human attack surface, **imagine the impact of knowing, managing, and reducing your human attack surface**.

Picnic offers a frictionless cybersecurity solution that mitigates the threat of social engineering by proactively disrupting attacker reconnaissance and resource development, effectively reducing the human attack surface at an enterprise-wide scale.

NO HARDWARE. NO AGENTS. NO HEADACHES.

"Social engineering is a key and growing threat to industrial organizations and Picnic offers important innovations to help the community strengthen its defenses. Picnic's team understands how threats perform reconnaissance and initial targeting against companies and has built a privacy-forward platform for organizations looking to strengthen their cybersecurity."

ROBERT M. LEE
CEO at Dragos Inc.

WHY PICNIC?

COST SAVINGS
Reduce the operating costs of the cybersecurity program downstream by denying attackers the most attractive ingress vector to corporate and personal data and devices.

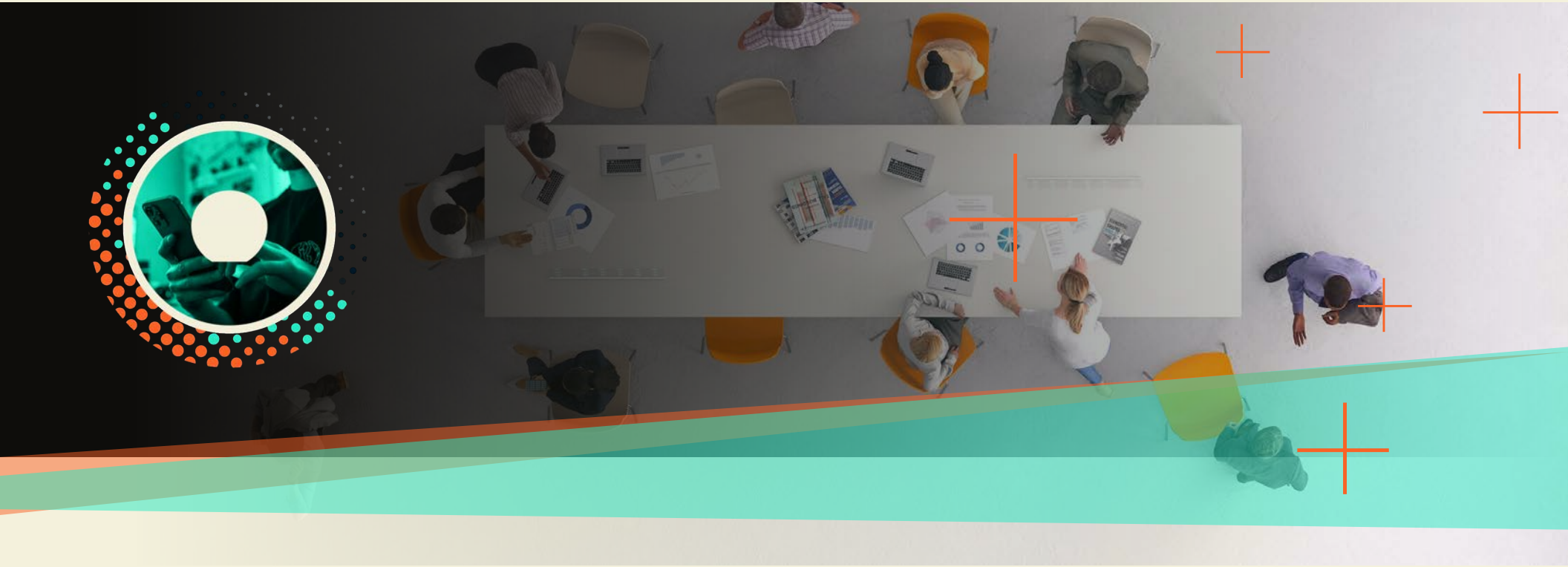
HUMAN RISK VISIBILITY
Identify the assets most at risk and see the human attack surface through the lens of the social engineer to identify high-value targets and pathways to compromise.

HUMAN RISK REDUCTION
Manage risk by controlling your organization's OSINT exposure and reduce exposure for high-value targets such as VIPs and key pesonnel with privileged access, while protecting against credential reuse and credential stuffing attacks.

AUTOMATED PREDICTION & PREVENTION
Eliminate targeting opportunities and attacker motives. Defend forward by preventing the compromise of users with privileged technical and financial access.

FOCUSED DETECTION & RESPONSE
Improve security by automating continuous risk detection for fewer active threats to detect and respond to, and reduce the mean time to detection as a result.

EMPLOYEE PRIVACY & AWARENESS
Enable learning and aha moments through private and personalized risk assessments and recommendations based on actual corporate and personal risks.

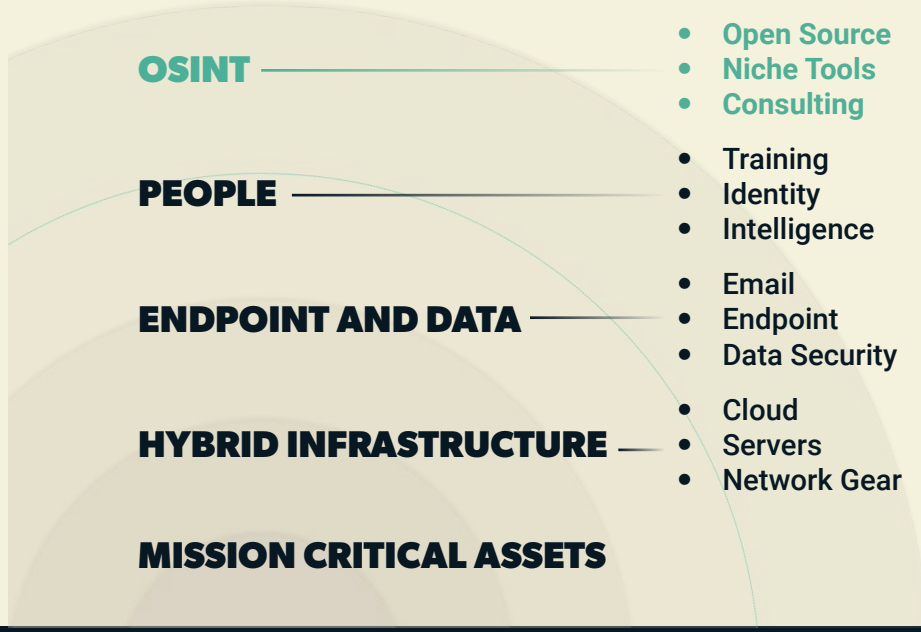


SOCIAL ENGINEERING RISK FRAMEWORK

Cybercriminals use personal information to target employees at home and at work to gain initial access. Credential stuffing, impersonation, spear phishing, and other social engineering attacks lead to organizational compromise. These begin by harvesting exposed personal, corporate, and third-party data.

Cyber defenders across all critical infrastructure sectors lack a holistic and comprehensive cybersecurity framework that **specifically** helps them manage at scale the risks associated with **OSINT and Social Engineering**.

While many cybersecurity best practices and frameworks exist today for specific industry sectors (including some that are integrated into regulatory compliance requirements) most are focused on addressing **technical vulnerabilities** and not **human vulnerabilities**:



- Most cybersecurity controls focus on hardening infrastructure, yet social engineering risk is a data problem related to human vulnerabilities.
- Cybersecurity awareness programs are useful tools for defenders but can be enhanced with personalization that leverages real and relevant corporate and personal risk data.
- Mail gateways, AI/ML-based filters, multi-factor authentication, and others aren't foolproof. They are located downstream of the source of the threat and can be defeated.
- **92% of cyber attacks leverage individuals' public data to craft the attack**, yet paradoxically current security measures do not address OSINT reconnaissance at scale.

CURRENT CYBERSECURITY MEASURES DO NOT ADDRESS THE HUMAN ATTACK SURFACE AT SCALE

A ROADMAP TO REDUCE THE HUMAN ATTACK SURFACE

Picnic offers its customers a **tailored roadmap** to reduce their human attack surface on both an enterprise and personal level, to help them minimize the number of socially engineered attacks impacting their security operations.

Picnic's **Social Engineering Risk Management Framework** was built alongside industry leaders and early Picnic adopters to help manage risks and respond to active social engineering threats originating from OSINT reconnaissance.

This framework, aligned with NIST CSF and MITRE ATT&CK, and reflected in the platform, helps cyber defenders tackle social engineering risk at the source using best practices and Picnic's prediction and prevention capabilities.

Reducing the human attack surface cascades into:

- More compehensive and targeted threat intelligence
- A lower number of active threats
- Less attention fatigue at the SOC
- Reduced cybersecurity operational expenses

Picnic delivers the visibility and automated social engineering risk management capabilities needed to positively impact identity and access management. With Picnic, you take a proactive vs reactive stance against cyber and physical threats towards your VIP, employees, infrastructure, and mission critical assets.

Tackle the social engineering problem at the source with Picnic.

PREEMPT, PREVENT AND DISRUPT SOCIAL ENGINEERING AT SCALE

THE PICNIC PLATFORM

HUMAN ATTACK SURFACE MANAGEMENT AT SCALE

Harnesses OSINT to reduce the human attack surface, preemptively expose social engineering pathways, and automate continuous risk detection.

Command Center is Picnic's cloud-delivered SaaS platform that provides security teams the power to preempt, prevent, and disrupt attacker reconnaissance and resource development at scale.

Ask yourself:

- What if you could see and understand your organization's social engineering risk exposure from the lens of the attacker?
- What if you could mitigate human risk at scale through data-backed risk prioritization and remediation?
- What if you denied the attackers the opportunity and motive and tackled the majority of cyber attacks where they originate?
- What would happen if a single platform could impact the effectiveness and reduce the cost of your overall cybersecurity program?

USE CASES

TACKLE 92% OF CYBERATTACKS AT THE SOURCE

HIGH-VALUE TARGET PROTECTION
Protect 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.

THREAT INTELLIGENCE PRIORITIZATION
Prioritize and mitigate targeted social engineering threats by combining external threat intelligence with human threat mapping.

IMPERSONATION ATTACK PREVENTION
Detect and remediate social media impersonation and detect email spoofing risk.

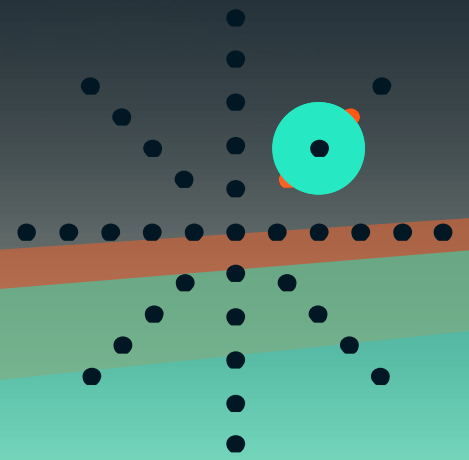
SUSPICIOUS DOMAINS AND ACCOUNTS DETECTION
Neutralize attackers by identifying suspicious domains and accounts and enabling preventive measures.

EXPOSED ENTERPRISE DATA SEARCH AND NEUTRALIZATION
Identify and remediate publicly available sensitive enterprise data that powers social engineering attacks.

SMS ATTACK AND PHISHING RISK NEUTRALIZATION
Remove publicly-available personally identifiable information (PII) to reduce social engineering risk.

SPEARPHISHING SIMULATION AND MITIGATION
Protect employees from targeted phishing attacks through Tigerphish simulation exercises and training.

TAILORED CYBER AWARENESS TRAINING PRIORITIZATION
Prioritize high-risk individuals for training with specifically targeted social engineering risks.



READY TO GET STARTED?

getpicnic.com/schedule-demo

PICNIC™

getpicnic.com

Picnic Corporation
7315 Wisconsin Ave
Suite 400W
Chevy Chase, MD 20815
Sales: +1 (240) 316-4067