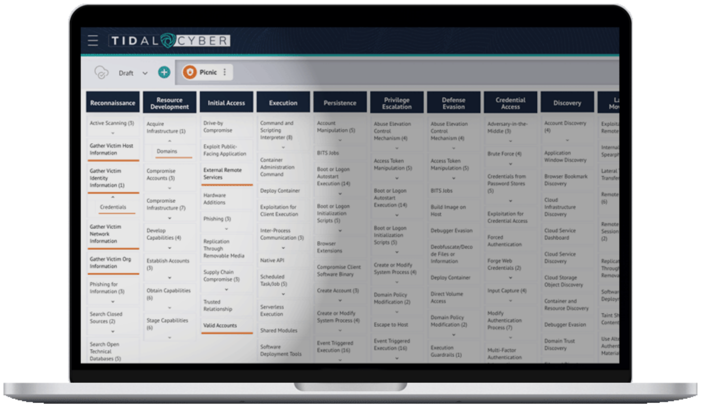
EINPRESSWIRE

Picnic Corporation joins the Tidal Product Registry

WASHINGTON, D.C., U.S., June 20, 2023 /EINPresswire.com/ -- Picnic Corporation, the creators of the industry's first automated enterprise-wide human attack surface protection solution, announced today that the company has joined the Tidal Product Registry™, a Tidal Cyber curated repository of vendor capabilities and data sources, mapped to MITRE ATT&CK®, that helps security professionals see how security vendors and products address adversary behaviors.



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	La Mov
Active Scanning (3)	Acquire Infrastructure (1) Domains	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploita Remote
Gather Victim Host Information	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearph
Gather Victim Identity Information (1) Credentials	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Transfe
Gather Victim Network Information	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote (6)
Gather Victim Org Information	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Session (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replicat Through Remova
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Softwar Deploym
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Sh Content
		Valid Accounts	Shared Modules	Event Triggered Execution (16)		Domain Policy Modification (2)	Multi-Factor Authentication	Debugger Evasion	Use Alt Authent Materia
			Software Deployment Tools			Execution Guardrails (1)		Domain Trust Discovery	

With the current cybersecurity vendor landscape being as extensive and complex as it is, there's certainly no lack of products in the marketplace that provide defenders with threat visibility and security controls. When working towards a threat-informed defense, most companies look to identify which vendors address the adversary tactics, techniques, and procedures (TTPs) being used to target them. Tidal Cyber is helping these companies by offering a curated registry of hundreds of cybersecurity vendors mapped to the widely adopted MITRE ATT&CK framework, which enables comparing vendors' claims within MITRE's matrix. This allows Tidal Cyber's users to easily narrow the scope of their vendor research based on claimed capabilities to mitigate, protect, detect, respond, and test those TTPs that are relevant to their program.

> Participating in the Product Registry empowers users to understand how creative solutions like Picnic can enhance their security stack."
>
> *Frank Duff, Chief Innovation Officer for Tidal Cyber*

Picnic recently partnered with Tidal Cyber and joined the Tidal Product Registry; users of both Tidal Cyber's Enterprise Edition and their freely-available Community Edition can now quickly see Picnic's scope within the MITRE ATT&CK framework and compare it to the TTPs used by specific cyber threats. This high-level view of the vendor landscape mapped to MITRE's matrix of TTPs provides relevancy and focus and demonstrates why Picnic is unique in the marketplace.

Most breaches today are the result of social engineering and credential stuffing attacks that rely on OSINT data tied to the human element. Still, most cybersecurity vendors focus on securing devices, applications, clouds, and other targets, without addressing the human attack surface of employees, contractors, and third parties. This exposed PII is the fuel that powers attackers' social engineering campaigns and initial access.

Picnic fills this critical security gap by delivering enterprise-wide protection of the human attack surface by remediating exposed PII in the wild and integrating with internal controls to break reconnaissance chains used by attackers. Picnic's solution helps customers shift from detection and response to prevention.

“Tidal's Product Registry provides the transparency around how vendors map to the MITRE ATT&CK framework that companies need to make threat-informed cyber defense decisions,” said Picnic CEO Matt Polak. “Picnic addresses the first two stages of this framework and disrupts attacks early in the kill chain to prevent initial access. We're excited to partner with Tidal and showcase the unique capabilities Picnic has to offer.”

"We're excited to welcome Picnic to the Tidal Product Registry," said Frank Duff, Chief Innovation Officer for Tidal Cyber. "Participating in the Product Registry empowers users to understand how creative solutions like Picnic can enhance their security stack."

Learn more about Picnic's platform, its benefits, and its capabilities. Schedule a demo at https://getpicnic.com/schedule-a-demo/.

About Picnic
Picnic Corporation is an innovative cybersecurity firm that provides enterprises with the capability to manage their external human attack surface and to detect, prevent, and protect against social engineering and credential stuffing attacks. Picnic's platform automatically emulates threat actor reconnaissance on the public data footprint of an organization and its people for defensive purposes. Our technology continuously monitors and reduces company and employee OSINT exposure, commonly leveraged for social engineering and initial access, preemptively disrupts attacker reconnaissance and resource development, and proactively neutralizes human risk beyond the corporate perimeter to prevent organizational compromise. For more information, contact Picnic at info@getpicnic.com.

Sara Trammell
Picnic Corporation
marketing@getpicnic.com
Visit us on social media:
Twitter
LinkedIn