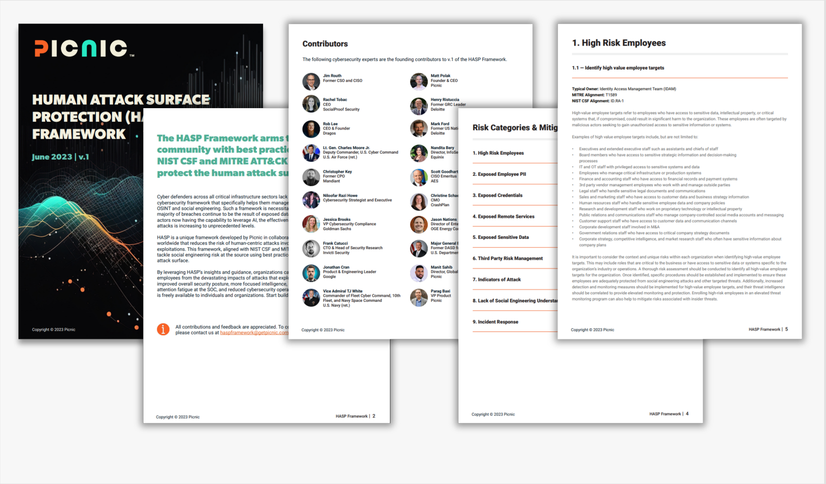
EINPRESSWIRE

Picnic Corporation Launches Practical Framework to Combat Human-Centric Attacks

Company arms the cybersecurity community with best practices aligned to NIST CSF and MITRE ATT&CK to proactively protect human attack surface



PICNIC™

HUMAN ATTACK SURFACE PROTECTION (HA
FRAMEWORK

June 2023 | v.1

Copyright © 2023 Picnic

The HASP Framework arms t
community with best practi
NIST CSF and MITRE ATT&CK
protect the human attack su

Cyber defenders across all critical infrastructure sectors lack
cybersecurity framework that specifically helps them manage
OSINT and social engineering. Such a framework is necessita
majority of breaches continue to be the result of exposed dat
actors now having the capability to leverage AI, the effectiven
attacks is increasing to unprecedented levels.

HASP is a unique framework developed by Picnic in collabora
worldwide that reduces the risk of human-centric attacks invo
exploitations. This framework, aligned with NIST CSF and MIT
tackle social engineering risk at the source using best practic
attack surface.

By leveraging HASP's insights and guidance, organizations ca
employees from the devastating impacts of attacks that expl
improved overall security posture, more focused intelligence,
attention fatigue at the SOC, and reduced cybersecurity opera
is freely available to individuals and organizations. Start build

All contributions and feedback are appreciated. To c
please contact us at haspframework@getpicnic.com

Copyright © 2023 Picnic — HASP Framework | 2

Contributors

The following cybersecurity experts are the founding contributors to v.1 of the HASP Framework.

Jim Routh
Former CSO and CISO

Rachel Tobac
CEO
SocialProof Security

Rob Lee
CEO & Founder
Dragos

Lt. Gen. Charles Moore Jr.
Deputy Commander, U.S. Cyber Command
U.S. Air Force (ret.)

Christopher Key
Former CPO
Mandiant

Niloofar Razi Howe
Cybersecurity Strategist and Executive

Jessica Brooks
VP Cybersecurity Compliance
Goldman Sachs

Frank Catucci
CTO & Head of Security Research
Invicti Security

Jonathan Cran
Product & Engineering Leader
Google

Vice Admiral TJ White
Commander of Fleet Cyber Command, 10th Fleet, and Navy Space Command
U.S. Navy (ret.)

Matt Polak
Founder & CEO
Picnic

Henry Ristuccia
Former GRC Leader
Deloitte

Mark Ford
Former US Nati
Deloitte

Nandita Bery
Director, InfoSe
Equinix

Scott Goodhart
CISO Emeritus
AES

Christine Schae
CMO
CrashPlan

Jason Nations
Director of Ente
OGE Energy Co

Major General
Former DASD f
U.S. Departmen

Manit Sahib
Director, Global
Picnic

Parag Baxi
VP Product
Picnic

Copyright © 2023 Picnic

Risk Categories & Mitig

1. High Risk Employees
2. Exposed Employee PII
3. Exposed Credentials
4. Exposed Remote Services
5. Exposed Sensitive Data
6. Third Party Risk Management
7. Indicators of Attack
8. Lack of Social Engineering Understa
9. Incident Response

Copyright © 2023 Picnic — HASP Framework | 4

1. High Risk Employees

1.1 — Identify high value employee targets

Typical Owner: Identity Access Management Team (IDAM)
MITRE Alignment: T1589
NIST CSF Alignment: ID.RA-1

High-value employee targets refer to employees who have access to sensitive data, intellectual property, or critical systems that, if compromised, could result in significant harm to the organization. These employees are often targeted by malicious actors seeking to gain unauthorized access to sensitive information or systems.

Examples of high value employee targets include, but are not limited to:

- Executives and extended executive staff such as assistants and chiefs of staff
- Board members who have access to sensitive strategic information and decision-making processes
- IT and OT staff with privileged access to sensitive systems and data
- Employees who manage critical infrastructure or production systems
- Finance and accounting staff who have access to financial records and payment systems
- 3rd party vendor management employees who work with and manage outside parties
- Legal staff who handle sensitive legal documents and communications
- Sales and marketing staff who have access to customer data and business strategy information
- Human resources staff who handle sensitive employee data and company policies
- Research and development staff who work on proprietary technology or intellectual property
- Public relations and communications staff who manage company-controlled social media accounts and messaging
- Customer support staff who have access to customer data and communication channels
- Corporate development staff involved in M&A
- Government relations staff who have access to critical company strategy documents
- Corporate strategy, competitive intelligence, and market research staff who often have sensitive information about company plans

It is important to consider the context and unique risks within each organization when identifying high-value employee targets. This may include roles that are critical to the business or have access to sensitive data or systems specific to the organization's industry or operations. A thorough risk assessment should be conducted to identify all high-value employee targets for the organization. Once identified, specific procedures should be established and implemented to ensure these employees are adequately protected from social engineering attacks and other targeted threats. Additionally, increased detection and monitoring measures should be implemented for high-value employee targets, and their threat intelligence should be correlated to provide elevated monitoring and protection. Enrolling high-risk employees in an elevated threat monitoring program can also help to mitigate risks associated with insider threats.

Copyright © 2023 Picnic — HASP Framework | 5

WASHINGTON, D.C., U.S., June 12, 2023 /EINPresswire.com/ -- Most organizational breaches today continue to be the result of human-centric attacks involving social engineering and credential compromise, according to Verizon's 2023 DBIR report. These attacks persist because they rely on exploitation of the largest security gap companies have: the human attack surface of employees, contractors, and third parties. With threat actors now having the capability to leverage AI, the effectiveness and scale of these human-centric attacks is increasing to unprecedented levels.

> As the first framework dedicated to social engineering and human compromise risk reduction, HASP sets the standard for the industry."
>
> *Jim Routh, Former CSO and CISO*

Cyber defenders lack a holistic and comprehensive cybersecurity framework to address the human attack surface, which sits at the intersection of open-source intelligence (OSINT) and social engineering. As the leader in the field of human attack surface protection, Picnic Corporation has taken the lead to bring together thought leaders and create a critical framework to directly address human-centric attacks.

In an effort to fill the defensive gap, the company has just announced the release of the Human Attack Surface Protection (HASP) Framework, an original roadmap to help organizations proactively protect their human attack surfaces and reduce the risk of human-centric attacks involving social engineering and exposed data. The HASP Framework has been developed by Picnic in collaboration with cybersecurity experts worldwide. It is aligned to NIST CSF and MITRE ATT&CK with the goal of arming the cybersecurity community with best practices that directly and proactively reduce the human attack surface.

"As the threat landscape continues to evolve, it's essential that we provide our customers with the most comprehensive solutions," says Matt Polak, Founder and CEO of Picnic. "Our partnership with leading cybersecurity experts and the launch of our HASP Framework underscores our commitment to proactively protecting against attacks that exploit the human element."

Born out of a deep understanding of threat actor reconnaissance techniques and TTPs that leverage the human attack surface, the HASP Framework serves as a North Star for how the industry tackles the problem of human-centric attacks. Its founding contributors include Jim Routh, Former CSO and CISO; Rachel Tobac, CEO of SocialProof Security; Robert M. Lee, Founder and CEO of Dragos; Lt. Gen. Charles L. Moore Jr., Deputy Commander, U.S. Cyber Command (ret.); Timothy J. “TJ” White, Vice Admiral & Commander of Fleet Cyber Command, 10th Fleet, and Navy Space Command (ret.); Chris Key, Former Chief Product Officer of Mandiant and Founder of Verodin; Niloofar Razi Howe, Cybersecurity Strategist and Executive; Ben Fried, Former CIO of Google; Jessica Brooks, VP, Cybersecurity Compliance of Goldman Sachs; Jim Somborovich, Cybersecurity Leader & Veteran (USMC); Jonathan Cran, Product & Engineering Leader at Google; Frank Catucci, CTO & Head of Security Research at Invicti Security, and other leading experts in the field.

By leveraging HASP, organizations can effectively protect their human attack surface, resulting in an improved overall security posture, more focused intelligence, a lower number of active threats, less attention fatigue at the SOC, and reduced cybersecurity operating expenses.

"HASP is specifically designed to provide organizations with the roadmap to preemptively address their human attack surface data and dramatically reduce their risk of falling victim to a breach," says Parag Baxi, VP of Product at Picnic Corporation. "We have utilized this framework in our own product development and, in doing so, we are able to provide our customers with the most advanced human attack surface protection solution possible."

The HASP Framework is a tangible example of Picnic’s thought leadership and expertise in the field of human-based cybersecurity, and its launch marks a major milestone in the industry's efforts to fill the largest defensive void in cybersecurity.

"As the first framework dedicated to social engineering and human compromise risk reduction, HASP sets the standard for the industry," says Jim Routh, Former CSO and CISO. "Picnic is at the forefront of this critical issue and this framework, especially in tandem with Picnic's platform, helps organizations ensure the highest level of protection for their people."

For more information about HASP and how it can help protect your organization from social engineering and credential stuffing attacks, please visit https://getpicnic.com/human-attack-surface-protection-framework/ or contact haspframework@getpicnic.com.

Sara Trammell

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

This press release can be viewed online at: https://www.einpresswire.com/article/638630221