The KeepNet Labs

Solution Datasheet

keepnet LABS

Solution Datasheet

The Keepnet Labs platform gives you the power to stop and mitigate the damage of cyber-based attacks. Complementing other products that give you the tools to take action against cyber-attacks, Keepnet adopts a continuous lifecycle approach—fortifying your infrastructure, fostering secure behaviors, joining trusted threat sharing communities, and enabling rapid response to combat cyber threats head-on.

Smishing Simulator
- Collection of over 600+ smishing scenarios to simulate real-world SMS attacks
- Create custom smishing message
- Advanced smishing report

Vishing Simulator
- Voice AI technology
- Create custom voice messages
- Record your own mp3 files for vishing campaigns

Phishing Simulator
- Up-to-date attack scenarios
- Create custom tailored scenarios
- Multi scenario campaigns
- MFA-themed Phishing Scenarios

Quishing Simulator
- Realistic quishing attack scenarios with option to target users for data submission
- Create custom QR code scan scenarios
- Automate campaigns with ease

Email Threat Simulator
- Test your current security solutions including email gateway
- Detailed reports on breached threats
- Attack vectors are updated regularly

Awareness Educator
- Wide selection of videos, presentations, brochures, e-books
- SCORM compliant for any LMS integration
- Target users based on phishing campaign results
- Advanced reporting

Incident Responder
- Integrate existing technologies to boost threat detection
- Fully automated by Playbooks or manually triggered to find suspicious emails
- Automatic removal of threats
- Enable employees to immediately report suspicious emails using the Phishing Reporter

Threat Intelligence
- Dark Web Monitoring
- Real-time Intelligence
- No integration required

Vishing Simulator
- Share and benefit from common threats
- Share threats anonymously
- See suspicious email addresses, domains, URLs, attachments

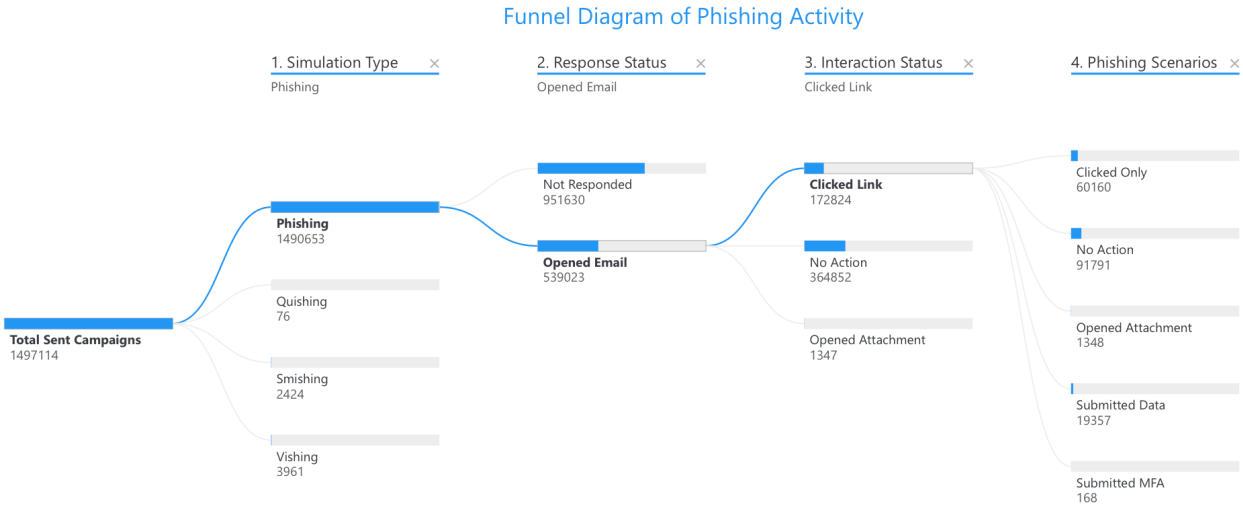
Advanced Reporting

Through launching multiple phishing campaigns over time, you may develop benchmark data that gives insight into your riskiest users, by utilizing our Advanced Reports feature. Our Advanced Reports feature allows you to generate multiple reports ranging from the different types of simulation activity down to an Executive Summary.

Example of an Executive Summary:

***Personal Identifiable Information in the below figures have been redacted.**

Funnel Diagram of Phishing Activity provides a further breakdown of each type of campaign's response status, interaction status, and scenario method.



Based on the target users' interaction with each phishing campaign, *User Stats on Phishing Activity by Type* classifies each target user's security behavior, ranging from **Secure** to **Moderate** to **Low** to **Risky**.

User Stats on Phishing Activities

Full Name	Email	Department	Risky Behaviours	Total Campaign	Opened Mail	Answered Call	Clicked Link
[redacted]	[redacted]	[redacted]	Secure	1	0		0
[redacted]	[redacted]	[redacted]	High	1	1		1
[redacted]	[redacted]	[redacted]	High	1	1		1
[redacted]	[redacted]	[redacted]	Secure	1	0		0
[redacted]	[redacted]	[redacted]	Low	1	1		0
[redacted]	[redacted]	[redacted]	Low	1	1		0
[redacted]	[redacted]	[redacted]	High	1	1		1
[redacted]	[redacted]	[redacted]	High	1	1		1
[redacted]	[redacted]	[redacted]	Low	1	1		0
[redacted]	[redacted]	[redacted]	High	1	1		1
[redacted]	[redacted]	[redacted]	Low	1	1		0

*Columns not pictured in above figure: **Submitted/Vished, Opened Attachment**

Derived from *User Stats on Phishing Activity by Type, Department Stats on Phishing Activity by Type* generalizes each department's security classification, with the same scale of **Secure** to **Risky.**

Department Stats on Phishing Activities

Department	Risky Behaviours	Total Campaign	Opened Mail	Answered Call	Clicked Link	Scanned QR	Submitted Data	Submitted MFA
[redacted]	Secure	2	0		0		0	0
[redacted]	Low	9	3	0	0	0	0	0
[redacted]	High	128	85		31		31	0
[redacted]	High	292	215		74		74	0
[redacted]	High	155	103		29		29	0
[redacted]	High	162	122		39		39	0
[redacted]	High	136	94		34		34	0

Benefits of Advanced Reports Feature

At a glance, System Users may identify the riskiest users and departments via a scale rating their security behavior, thus allowing for security personnel to appropriately prioritize and deploy security measures and targeted training accordingly. Keepnet Labs' solution pinpoints cyber security challenges and proactively trains organizations' employees to foster a secure environment.

Additional Key Features

Multi-Language Support

Keepnet improves your users' experience with translated training content, phishing templates, vishing templates, notifications, and more.

Direct Email Creation

Connects to your O365 with a few required API permissions. This feature creates the phishing simulation email directly in the user's inbox instead of sending the emails over SMTP protocol.

White Labelling

Our product supports brandable customization for training content, notifications, training certificates, enrollment emails, phishing reporter and the platform interface.

LMS Integration

Upload any or all training content to be managed through your own LMS. Our training is SCORM compliant allowing you to integrate with any LMS provider. API Call and Support: We have API calls for all products on the platform from launching Simulations and training to pulling detailed reports.

About Keepnet Labs

Keepnet Labs has simplified the way organizations secure themselves by enabling the human element of cybersecurity. Our solution includes essential email, voice, and SMS security controls - with seamless LMS integration, along with comprehensive reporting. Trusted by thousands of organizations to stay secure and reduce risk.

Find out more information on www.keepnetlabs.com