

Dreamlab Technologies Introduces Industry's First Fully Automated Advanced Honeypot Architecture

Dreamlab Technologies Introduces Industry's First Fully Automated Advanced Honeypot Architecture for Superior Threat Intelligence and Research

BERN, SWITZERLAND, May 11, 2021

/EINPresswire.com/ -- [Dreamlab](#)

[Technologies](#), a leader and source of constant innovation in cyber defence

solutions and services, announced today the rollout of its [automated threat detection](#) and threat intelligence solution. Their new, innovative technology platform, [Honeykube](#), combines traditional deception techniques strategies with advanced data collection and automated analytics, to help organisations focus on higher value activities.



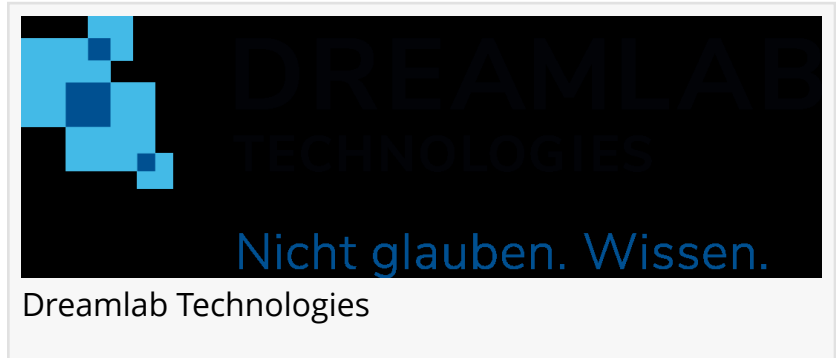
Our latest deception-based threat intelligence security solution is purposeful and advantageous for use cases such as recognising targeted ransomware and identifying nation state hackers"

*Nicolas Mayencourt, Global
CEO of Dreamlab
Technologies*

Traditional ways of defence are becoming less and less effective due to the unprecedented increase in the number of remote workers, along with the changing nature of the cyber criminal's behaviours, tools, and tactics. The only way to stay ahead of today's sophisticated attackers is to implement methods and schemes that go above and beyond traditional solutions and provide advanced attack visibility and investigation.

Previously, these technologies have been focused on automated threat detection. While such methods have been extremely beneficial for rapid response and

remediation, they have left an important gap in the market around automated data collection and analysis. Honeykube addresses this gap by offering a next-generation solution that provides a vast array of information on attacks and the attackers behind them. It also automates the consolidation, integration and harmonisation of the data collected, to assist investigations with an advanced understanding of the diverse threats lurking within our networks.



Sheila A. Berta, Head of Research and Development at Dreamlab Technologies, said: "Security Analysts and Researchers require data that is simplified, comprehensive, and that helps them stay ahead of the evolving threat landscape. However, this is usually a laborious, time-intensive process due to the huge amount of raw data, that can rapidly become overwhelming. With the development of Honeykube, we are helping customers improve their intelligence, hunting and analysis capabilities for new threats and malicious actors, by providing an advanced platform that contextualises collected data to generate business-ready dashboards and reports which are ready to act upon."

"Our latest deception-based threat intelligence security solution is purposeful and advantageous for use cases such as recognising targeted ransomware and identifying nation state hackers" said Nicolas Mayencourt, Global CEO of Dreamlab Technologies. "The conception of Honeykube came from the need for a solution that provided an extensive attack analysis and most importantly, the ability to automatically analyse and identify the attack vectors and criminals behind them. It was developed with analysts-in-mind; facilitate their work, saving time and effort, and allowing them to focus on other tasks that might be more beneficial to the company".

To learn more about Honeykube's new threat intelligence and deception technology, please visit www.honeykube.ch or schedule a demo with our customer success team, who are always available for consultation!

About Honeykube

Honeykube is an advanced platform for honeypot and honeynet management, along with sophisticated adversary analysis. Honeykube leverages a sophisticated approach for identifying the type of attacks performed, providing solid and useable intelligence. For Threat Hunters and Threat Intelligence Specialists who need to understand both the current and new attack techniques being used by real malicious actors, Honeykube provides intelligence and data rich analysis of their tactics, techniques and procedures. The novel honeypot-based security approach employs cutting-edge Kubernetes technology to guarantee the high availability and resilience of its honeypots, whilst ensuring that the information collected through them is reliable.

About Dreamlab Technologies

For over 20 years, Dreamlab Technologies has supported private and governmental organisations. Our main activities include strategic consulting, audit and education.

We also focus on the conception, realisation, integration, operation and the maintenance of cybersecurity solutions based on open standards. We have comprehensive experience in fraud cases, as well as targeted malware attacks.

Since 2003, Dreamlab has officially represented the Institute for Security and Open Methodologies (ISECOM) in Switzerland, France, Germany and Chile. ISECOM is an international

non-profit organisation that develops open standards for IT security and business integrity testing. It is the editor of the Open Standards Security Testing Methodology Manual (OSSTMM), the most widely spread standard for information security testing. Through its close partnership with ISECOM and an active collaboration in setting new standards, Dreamlab is always up-to-date and even ahead of the curve.

Being an honorary member of the security section of the Swiss Informatics Society, a member of the OpenTCPA Research Group and the World Wide Web Consortium (W3C) means we are a part of the newest developments in IT security. Our clients directly benefit from this wealth of knowledge, network of contacts and from the insights into development and future marketplaces.

HONEYKUBE

Dreamlab Technologies

Tel: +41313986666

contact@dreamlab.net

www.honeykube.ch

www.dreamlab.net

This press release was issued through ArabNewswire.com: <http://www.arabnewswire.com>, a newswire service with press release distribution to media in the Arab World, Middle East and North Africa (MENA).

HONEYKUBE

Dreamlab Technologies

+41 313986666

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/540828457>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.