Relay Hosts 'State of Cybersecurity Industry' Panel; Pre-Registration Now Open

TORONTO, June 02, 2021 (GLOBE NEWSWIRE) -- Relay Medical Corp. ("**Relay**" or the "**Company**") (CSE: RELA, OTC: RYMDF, Frankfurt: EIY2) - will be hosting their inaugural Cybersecurity panel discussion later this month on Tuesday, June 22, 2021.

The Company will be streaming the first webcast on June 22nd; guest speakers will be respected influencer and Forbes writer Chuck Brooks,[1] and Chris Blask,[2] the innovative creator of the firewall and Digital Bill of Materials. The discussion will include Dmitry Raidman, CTO of Cybeats and moderated by Evgeniy Kharam. After the event, video recording will be available for viewing on the company's youtube channel. To attend the live event or submit questions ahead of time, please email events@cybeats.com.

The panel will be discussing the prevalent cybersecurity topics addressed by United States President, Joe Biden, in the Executive Order (EO)[3] and the greater Internet of Things (IoT) industry issues with connected devices sector examples focusing on the significance of mission critical systems and various connected devices applications.

"The Order calls for an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response," shares Chuck Brooks, Strategic Advisor. "Both industry and government will require better capabilities of detection of vulnerabilities throughout manufacturing and deployment of connected devices, especially in supply chains."

The Presidential Cybersecurity Timeline

> The presidential order timeline is set to publish a definition of the term "critical software" by the end of June and publish a list of software categories meeting this definition of "critical software" by end of July.
>
> In mid July the director of National Institute of Standards and Technology (NIST) will publish guidance outlining security measures for "critical software", and guidelines for minimum standards for vendors' testing of their software source code. The Secretary of Commerce will publish the minimum elements for a Software Bill of Materials (SBOM).
>
> On February 6, 2022 (270 days from the EO) the director of NIST will publish guidance on practices that enhance software supply chain security that will include tools to check for and remediate vulnerabilities and manage SBOMs and identify Internet of Things (IoT) cybersecurity criteria for a consumer labelling program.
>
> On March 8, 2022 (300 days from the EO) the administrator of the Office of Electronic Government will require that all agencies comply with the NIST guidelines with respect to software procured after the date of the Executive Order.

"The inevitability of SBOMs means that those with responsibility for security operations centers need to begin determining how SBOMs will get integrated into real time operations," said by Chris Blask, Strategic Advisor. "Solutions like Cybeats SBOM Studio and IoT Platform would be key to operationalizing this new feed of supply chain intelligence."

Cybeats

Cybeats' SBOM Studio product allows for the monitoring and analysis of cybersecurity on all components during the design and manufacturing stage ensuring connected devices have been developed with secure software components.

Cybeats' IoT security platform's capabilities span across detecting and mitigating attacks on devices while they are operational, to enabling device makers to identify and fix security flaws during the product's design phase and empowering end users with fleet management tools such as secure firmware updates.

Recent Global Cybersecurity News

On May 30th, 2021, JBS Foods,[4] the world's largest meat processing company, suffered a coordinated cyberattack[5] that forced it to close 10 processing plants, pause operations in North America and Australia[6], and cancel shifts for thousands of workers. The attack wipes out nearly a fifth of America's meat production for the duration of this incident as investigations are still ongoing.

Other large American meat producers have paused slaughtering in fear of similar and imminent potential attacks.[7] From food shortages to redirecting cattle for slaughter, the gravity of this debilitating attack is not yet fully known. This attack increases the ongoing pressure on the Whitehouse to prioritize the nation's cybersecurity earlier in May which led to the May 12th EO.

For Media Inquiries, please contact: Destine Lee media@relaymedical.com | 647-872-9982

SUBSCRIBE: For more information on Relay or to subscribe to the Company's mail list visit:

https://www.relaymedical.com/news

About Relay Medical Corp.
Relay Medical is a MedTech innovation Company headquartered in Toronto, Canada focused on the development of novel technologies in the diagnostics and AI data science and IoT security sectors.

Website: www.relaymedical.com

Contact:
W. Clark Kent
President
Relay Medical Corp.
Office. 647-872-9982 ext. 2
TF. 1-844-247-6633 ext. 2
investor.relations@relaymedical.com

Bernhard Langer
EU Investor Relations
Office. +49 (0) 177 774 2314
Email: blanger@relaymedical.com

Forward-looking Information Cautionary Statement

Except for statements of historic fact, this news release contains certain "forward-looking information" within the meaning of applicable securities law. Forward-looking information is frequently characterized by words such as "plan", "expect", "project", "intend", "believe", "anticipate", "estimate" and other similar words, or statements that certain events or conditions "may" or "will" occur. Forward-looking statements are based on the opinions and estimates at the date the statements are made, and are subject to a variety of risks and uncertainties and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements including, but not limited to delays or uncertainties with regulatory approvals, including that of the CSE. There are uncertainties inherent in forward-looking information, including factors beyond the Company's control. There are no assurances that the commercialization plans for the technology described in this news release will come into effect on the terms or time frame described herein. The Company undertakes no obligation to update forward-looking information if circumstances or management's estimates or opinions should change except as required by law. The reader is cautioned not to place undue reliance on forward-looking statements. Additional information identifying risks and uncertainties that could affect financial results is contained in the Company's filings with Canadian securities regulators, which filings are available at www.sedar.com

---

[1] https://www.relaymedical.com/blog/2021/5/4/relay-welcomes-global-cybersecurity-thought-leader-expert-and-influencer-chuck-brooks-to-cybeats-advisory-board
[2] https://www.relaymedical.com/blog/2021/5/20/relay-welcomes-renowned-cybersecurity-expert-digital-bill-of-materials-inventor-chris-blask-to-advisory-board
[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[4] https://jbs.com.br/en/
[5] https://www.nbcboston.com/news/local/worlds-largest-meat-producer-jbs-hit-by-cyberattack-in-us-australia/2394375/
[6] https://www.reuters.com/world/us/some-us-meat-plants-stop-operating-after-jbs-cyber-attack-2021-06-01/
[7] https://www.marketscreener.com/quote/stock/JBS-S-A-6499588/news/JBS-S-A-nbsp-Large-North-American-meat-plants-stop-slaughter-after-JBS-cyberattack-35490180/