JFrog Research Uncovers Weak Links in MLOps & Security Usage within Enterprise Software Supply Chains

New report reveals multiple disconnects between senior executives and hands-on practitioners globally, amplifying gaps in standardized use of AI/ML, security detection and remediation technologies

Sunnyvale, Calif., July 18, 2024 — JFrog Ltd. ("JFrog") (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today unveiled the findings of a new report exposing disparities in MLOps and security perceptions between leadership and frontline teams that is increasing the risk of software supply chain (SSC) attacks around the globe.

Software supply chain security breaches are experiencing a significant uptick, according to a recent IDC survey showing a staggering 241% increase in such attacks year-over-year[1]. Surprisingly, only 30% of the survey respondents identified the need to address vulnerabilities in their software supply chain as a top security concern.

"The complexity of today's software supply chain poses unprecedented risks. Despite leadership efforts to equip frontline teams with the right equipment, developers are struggling to improve efficiency and accelerate productivity due to tool sprawl, lengthy open source and ML model approvals, plus audit and compliance checks," said Moran Ashkenazi, SVP & CISO, JFrog. "This discrepancy highlights the urgency for organizations to rethink their security strategies, focus more on AI/ML components, and align executives and doers on a mission to fortify their software supply chains."

JFrog's new report reveals several disparities between security executives and frontline software teams concerning malicious open-source package detection, AI/ML integration, and code-level security scans, including:

- 92% of executives claim their organizations possess tools to detect malicious open-source packages, while only 70% of developers agree with this statement.
- Over 90% of executives believe they are using ML models in their software applications, but only 63% of developers confirm that is the case.

[1] IDC, "IDC Helps Organizations Navigate Software Supply Chain Security with New Industry-Leading Research," 15 June 2023, https://www.idc.com/getdoc.jsp?containerId=prUS50913123

- 88% of executives believe AI/ML tools are being used for security scanning and remediation processes, however only 60% of DevSecOps teams report they are using these tools.
- 67% of executives believe code-level security scans are conducted regularly, while only 41% of developers confirm such is true.

JFrog's study also delves into regional disparities in software supply chain security, visibility, and use of AI/ML such as:

- **Awareness of Security Solutions**: 14% of EMEA respondents were unaware of tools for identifying malicious open-source packages, in contrast to lower rates in the US (9%) and Asia (1%), highlighting a substantial disconnect in EMEA's security strategies and operational understanding.
- **Adoption of AI/ML Models**: Only 82% of EMEA respondents reported using AI/ML models, compared to 91% in the US and 99% in Asia. This variance may point to Europe's risk-averse environment influenced by strict regulations, while we see faster adoption of AI/ML technologies in the US.

For deeper insights on how executives can augment collaboration with developers, security, and data science teams to better secure their software supply chains download the full report. You can also register to join JFrog's Field CISO, Paul Davis, and JFrog's CIO, Aran Azarzar, for a webinar, ***"Know The Enemy: What Execs Need To Understand To Secure Their Software Supply Chain,"*** detailing the complexities, promising solutions, and recommendations for better managing and securing software supply chains.

###

Like this Story? Share this: @JFrog sponsored research shows critical gaps in visibility between business divisions, execs, & doers increases risk of #softwaresupplychain attacks. Learn more: https://bit.ly/3WplWbl #DevOps #DevSecOps #cybersecurity #CVEs #AI/ML

About JFrog

JFrog Ltd. (Nasdaq: FROG), is on a mission to create a world of software delivered without friction from developer to device. Driven by a "Liquid Software" vision, the JFrog Software Supply Chain Platform is a single system of record that powers organizations to build, manage, and distribute software quickly and securely, ensuring it is available, traceable, and tamper-proof. The integrated security features also help identify, protect, and remediate against threats and vulnerabilities. JFrog's hybrid, universal, multi-cloud platform is available as both self-hosted and SaaS services across major cloud service providers. Millions of users and 7K+ customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely

embrace digital transformation. Learn more at www.jfrog.com or follow us on X @JFrog.

Media Contact:
Siobhan Lyons, Sr. Manager, Global Communications, JFrog, siobhanL@jfrog.com

Investor Contact:
Jeff Schreiner, VP of Investor Relations, JFrog, jeffS@jfrog.com