Acronis SCS

FOR IMMEDIATE RELEASE

Contact: Nicole Magney, Public Policy & Communications Manager, Acronis SCS
(202) 531-2527
NM@AcronisSCS.com

Impressive Initial Results for Novel AI-based Software Supply Chain Risk Scoring Model

Spearheaded by Acronis SCS, first round of research yields 41% improvement at detecting CVEs

SCOTTSDALE, AZ – Dec. 9, 2020 – The Acronis SCS research team – led by the company's Senior Director of Research and mathematician Dr. Joseph R. Barr – has partnered with leading artificial intelligence (AI) academics at the University of California, Riverside, to research and develop a novel AI-based model that quantitatively scores software risks for vulnerability. Early results are noteworthy, with the team's first round of analysis demonstrating 41% improvement or "lift" at detecting common vulnerabilities and exposures (CVEs) in software code. This cutting-edge research will have real-world impact on US national security.

America's Software State-of-Play

From power grids and advanced weapons systems to telework-enabling applications, software sits at the heart of nearly all that keeps America running. As more and more products and services rely on the use of unvetted third party code and open source software libraries, cyber risks and opportunities for exploitation have surged. In fact, cyberattacks targeting open source projects have grown 430% year-over-year.

Hiring developers or outside firms to manually validate product source code can cost companies hundreds of thousands of dollars per review. Both the private and public sectors need a more affordable way to score software risk that relies on repeatable, objective processes and quantifiable results.

Novel Model for Source Code Analysis Balances Innovation and Security

Acronis SCS' AI-based model is designed to do just that. The model, which consists of a deep learning neural network, scans through source code (both open source and proprietary) to provide impartial quantitative risk scores that help IT administrators accurately determine whether and how to deploy new software packages, as well as update existing ones.

The first round of analysis, which focused on the Android Bluetooth module known as "Fluoride," resulted in a 41% "lift" or improvement at detecting CVEs over random testing. More details on these promising initial results are available in "Combinatorial Code Classification & Vulnerability," published in IEEE's 2020 Second International Conference on TransAI. Dr. Barr also outlined the team's findings while chairing a session on "AI Applications in Industry" at IEEE's 2020 International Symposium on Multimedia last week.

The research team is now conducting a second round of research centered on the much larger Android kernel code base. Almost complete, this analysis is also tracking at 41% improvement at detecting CVEs over random testing. The team plans to begin its next round of analysis, to include Windows applications, before the new year as well.

A Value Add for All

Once research is complete, Acronis SCS hopes to share the model in order to help all organizations identify and remediate risks within their software code, and in so doing, help the US government hold industry accountable against a set of consistent, objective standards. This AI-based approach ensures software vendors – and the federal contractors and government agencies relying on their products – can take the uncertainty out of software supply chain validation, while spurring cutting-edge innovation and small business opportunity.

Acronis SCS welcomes collaboration on data and threat analysis and is seeking partners with similar goals in order to continue securing the software supply chain. Please contact the company's Vice President of R&D and Engineering Neil Proctor or Senior Director of Research Dr. Joe Barr to discuss potential collaboration opportunities.

About Acronis SCS

Acronis SCS is a US-based, independently operated and governed cyber protection and edge data security company exclusively dedicated to meeting the unique requirements of the US public sector. In contrast, Acronis – Acronis SCS' international parent company – serves private companies, non-US public sectors, and individual consumers. Acronis SCS' innovative and comprehensive cyber protection, backup and disaster recovery, anti-ransomware, and enterprise file sync and share software solutions ensure operational assurance and data security across America's federal, state and local government, education, healthcare, and nonprofit computing environments. All Acronis SCS employees are US citizens.

# # #