Tech Giants Pledge $30B+ Cybersecurity Investment

Tech giants, Amazon, Google, Microsoft, IBM, and Apple have pledged major investments to bolster private and public cybersecurity infrastructure following a meeting with President Biden. The Biden Administration established voluntary cybersecurity goals and is pushing G7 countries to update NATO cyber policy and to aid in a collective effort to hold nations accountable for harboring ransomware criminals.

Amazon – Will provide its internal employee security awareness training directly to individuals and businesses at no charge. They will offer a multi-factor authentication device to AWS account holders to protect against phishing and password theft and the ability to use that device to access applications such as Gmail, Dropbox, and GitHub.

Google – Investment of $10B over the next five years to expand zero-trust programs, help secure the software supply chain, and enhance open-source security. Google will train 100k Americans for data analytics, privacy, and security jobs through its Google Career Certificate program. Additionally, Google intentionally seeks to close both the skills gap and lack of diversity in the industry by targeting unrepresented groups. Half its certificate program graduates are Black, Latinx, female, and/or veterans.

Microsoft – Will spend $20B over the next five years to advance its own security products and services and pledged $150M to improve government agency security posture and expand cybersecurity training partnerships with community colleges and nonprofits.

IBM – Committed to training 150k people in cybersecurity skills over the next three years and partnering with more than twenty historically Black Colleges and Universities to establish cybersecurity leadership centers, to encourage a more diverse cyber workforce.

Apple – Will establish a new program to drive continuous security improvements throughout the technology supply chain, working with its 9,000 US suppliers to drive mass adoption of multi-factor authentication, security training, vulnerability remediation, event logging, and incident response.