FOR IMMEDIATE RELEASE
Contact: IT-ISAC@nahigianstrategies.com

IT-ISAC Publishes New Whitepaper Stressing “Secure by Default” in SaaS Design

Security leaders argue "Secure by Default" enhances security for both software companies and users

WASHINGTON — The **Information Technology - Information Sharing and Analysis Center** (IT-ISAC) Critical SaaS Special Interest Group (CSaaS SIG), today released a white paper authored by leading internet security engineers advocating for Software as a Service (SaaS) companies to adopt “Secure by Default” in system design to help fortify the essential software used by organizations.

Lead authors, **James Dolph, Chief Information Security Officer at Guidewire** and **David Cross, Senior Vice President of SaaS Cloud Security at Oracle**, contend that SaaS companies should leverage their scale and design capabilities to improve the security outcomes for their customers, critical infrastructure, and the internet.

“Securing cloud services isn't just about code – it's about the user experience of security and a focus on secure outcomes for users and consumers. For Critical SaaS providers especially, their products and services are used across hundreds if not thousands of other organizations to accomplish mission-critical functions,” said **James Dolph**. “Secure by Default features in SaaS and other widely used software provide an opportunity to positively impact security outcomes across customers and industries at scale.”

As small, medium, and large enterprises increasingly rely on SaaS and other cloud-computing services to become more efficient, the paper urges services be configured with the most secure settings from the outset (by default) and include guardrails that prevent users from undoing secure settings. Using a system that is insecure or difficult to secure can open organizations up to cybercrime or state-sponsored attacks. This “Secure by Default” approach brings all stakeholders—including engineers, user experience designers, security professionals, and technology providers—to enhance security outcomes for consumers and SaaS users.

Traditionally, “Secure by Design” approaches have assumed that users will want a secure outcome, know what to do, and will do the right thing. While "Secure by Design" is considered a prerequisite for "Secure by Default," it is less opinionated, explicit, or comprehensive. Meaning that “Secure by Design” can discourage deviation from the overall principles and reduce flexibility for the user.

“The real goal for SaaS providers is to make security the default,” said **David Cross**. “It's not necessarily a competition between the two because they can work in tandem to proactively harden the service. Security teams, user experience designers, product managers, and engineers need to

work together to integrate security considerations seamlessly into both the design and default configuration of systems. That is really the key."

The authors outline examples of "Secure by Default" functionalities that are already deployed by popular cloud and SaaS applications, including:

- No access being permitted without explicit addition.
- All user accounts and activations require multi-factor authentication (MFA).
- All user accounts are disabled or adjusted automatically when role changes occur (terminations, org changes, role changes etc.).
- All elevated privileges are time-restricted based on approval.
- All secrets (cryptographic keys, passwords, etc.) are rotated automatically after each usage.
- All roles are segregated and may not be combined.
- All stored data is encrypted.
- All sessions and data in transit is encrypted.
- All interfaces and APIs require authentication and authorization.
- Customer Identity providers are either required or available by default.

"Secure by Design and Secure by Default are two separate principles that often get intermingled," said **Scott Algeier, Executive Director of the IT-ISAC**. "This white paper provides important thought leadership for CSaaS providers, their customers, and policymakers."

In the white paper, users are encouraged to play an active role in promoting "Secure by Default" functionality in their products and services. However, buyers should be aware of it becoming a marketing term used by companies, rather than a SaaS provider's dedication to the principles of "Secure by Default."

The white paper was developed through the IT-ISAC's CSaaS SIG and authored by members, James Dolph and David Cross as SaaS security experts. Members of the CSaaS SIG provide essential services that a vast array of critical infrastructure operators rely on for core operations. Founding members of the SIG include ServiceNow, ZScaler, Guidewire, Okta, Oracle, Workday and MongoDB.

Read the full white paper **here**.

###

About IT-ISAC: Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform and a trusted forum to engage with senior analysts from peer companies.

For more information about IT-ISAC, please visit www.it-isac.org. Twitter: www.twitter.com/ITISAC LinkedIn: www.linkedin.com/company/it-isac