IT-ISAC MEMBER PARTICIPATION GUIDE

A core value of IT-ISAC membership is the ability to collaborate with colleagues and subject matter experts from other member companies on common topics. This collaboration is supported by the protection of the IT-ISAC Member Agreement. IT-ISAC offers members many ways to engage with their peers in other member companies.

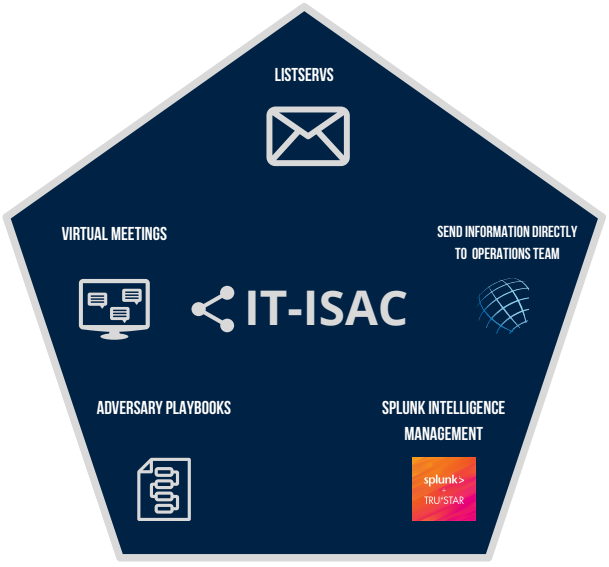
INTELLIGENCE MANAGEMENT PLATFORM

All IT-ISAC members receive access to the Community Edition of the Splunk Intelligence Management platform as part of their membership. Members leverage the platform to identify and prioritize threats and access automated sharing and threat analysis. Members can use custom API and STIX/TAXII integrations to pull indicators from the U.S. Department of Homeland Security, peer members, and IT-ISAC partners across the globe into their internal security tools.

METHODS OF SHARING

The IT-ISAC has various avenues that members can use to share information. These include our Technical Committee and Special Interest Group Listservs, directly with our Operations Team, Splunk Intelligence Management, a secure chat platform, through our Technical Committee and Special Interest Group meetings, and our Adversary Playbooks.

Our Technical Committee meeting is held weekly and is a forum for members to discuss important cybersecurity topics and share mitigation strategies. Most of our Special Interest Groups meet bi-weekly and provide an opportunity for companies to collaborate on issues affecting their specific group's topic of expertise. Our Adversary Attack Playbooks create a collaborative environment where members can share tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs) surrounding specific threat actors and their individual campaigns.



SPECIAL INTEREST GROUPS

Our Special Interest Groups (SIGs) provide members the opportunity to engage with subject matter experts from their specific industry. SIG members collaborate through bi-weekly virtual meetings and work on impactful projects related to the group's concentration.

We currently have six SIGs listed below:

FOOD AND AGRICULTURE

The Food and Agriculture SIG provides a forum for our members in the Food and Agriculture industry to share information on common security threats and collaborate on effective mitigations. The SIG shares information through virtual meetings and through a dedicated enclave in the Splunk Intelligence Management platform.

ELECTIONS INDUSTRY

The Elections Industry SIG supports voting technology providers by giving them an industry-only forum to share information about threats to their enterprises and systems and to collaborate on election security challenges.

CRITICAL SOFTWARE AS A SERVICE

The Critical SaaS SIG serves as a forum for CSaaS companies to collaborate on a collective defense strategy to improve the security and operational resiliency of their services and in turn, increase the level of trust that clients can place in their organizations and the industry at large.

SECURITY INTELLIGENCE

The Security Intelligence SIG brings together the senior level analysts from our member companies to exchange ideas, strategies, techniques, and information regarding advanced threat detection and enterprise risk management.

INSIDER THREAT

The Insider Threat SIG is designed for those who are responsible for building and managing Insider Threat programs within their companies.

PHYSICAL SECURITY

The Physical Security SIG is composed of security and business continuity professionals from our member companies. This group also shares effective strategies for responding to physical security threats relating to natural disasters, accidents, terrorism, and other matters impacting business continuity.

To learn more about IT-ISAC membership, visit **www.it-isac.org** or email **membership@it-isac.org.**