
# 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.

## TECHNICAL COMMITTEE

The IT-ISAC Technical Committee provides a forum for members to receive briefings on current and emerging cybersecurity threat information and trends from top subject-matter experts within IT-ISAC, as well as from outside member companies. Such topics include presentations on new attack trends and tactics, vulnerabilities and company-specific risk-management processes. The Technical Committee is also the primary forum IT-ISAC uses to coordinate responses to cyber incidents and to share cyber-threat information.

## SECURITY INTELLIGENCE SPECIAL INTEREST GROUP

This group is focused on bringing together the "APT hunters" from our member companies so that they can exchange ideas, strategies, techniques, and information regarding advanced threat detection. It is designed and reserved for member company employees who specialize in identifying advanced threats on their networks.

## INSIDER THREAT SPECIAL INTEREST GROUP

The IT-ISAC Insider Threat Special Interest Group (SIG) exists to enable IT-ISAC members to collaborate on how to identify malicious and non-malicious threats within their organizations. The Insider Threat SIG provides a forum where members can share information about tools, processes, technologies and policies used to identify and mitigate insider threats.

## FOOD AND AGRICULTURE SPECIAL INTEREST GROUP

The IT-ISAC Food and Agriculture Special Interest Group (Food and Ag SIG) facilitates trusted information-sharing and collaborative analysis among IT-ISAC members who operate in, or who have business units that operate within, the food and agriculture sector. The goal is to better enable members to identify attack, incident and threat indicators that they might have in common and to share effective mitigation strategies. The Food and Ag SIG is focused on, but not limited to, examining indicators from persistent adversaries who use multiple attack vectors to achieve their goals.

## ELECTIONS INDUSTRY-SPECIAL INTEREST GROUP

With a mission to collaborate information and improve the safety of our voting systems, the EI-SCC (Election Infrastructure Sector Coordinating Council) and the IT-ISAC formed a Special Interest Group for companies in the Elections Infrastructure Subsector. The Elections Industry Special Interest Group (EI-SIG) provides a dedicated forum for companies with common lines of business to proactively facilitate and support the sharing of threats (cyber and physical) in a trusted environment and to explore solutions driven by industry needs. In contrast with the government focused EI-ISAC, this group is led by corporate members, who participate with the same benefits available to other IT-ISAC members. Election companies who are a part of the SIG have valuable peer access to major IT and cybersecurity companies, which helps elevate the cybersecurity posture of their respective companies, and the Elections Subsector as a whole.

## PHYSICAL SECURITY AND BUSINESS CONTINUITY GROUP

This group provides a forum for subject-matter experts from within our membership to discuss physical security and business continuity issues and share effective practices to mitigate or respond to threats. This group provides an efficient way to distribute information we receive on physical security threats and incident reports from natural disasters, accidents, intentional attacks, and other matters impacting physical security and business continuity.

## THREAT INTELLIGENCE PLATFORM

All indicators shared by IT-ISAC are imported into IT-ISAC's threat intelligence platform, hosted by TruSTAR Technology, which all members have access to. In addition to information uploaded by the IT-ISAC staff and members, this platform receives automated feeds as part of the DHS CISCP and AIS programs and provides actionable context to the indicators. This platform leverages the STIX-TAXI framework that members can easily integrate with their existing tools. In addition, Silver and Gold members are able to utilize an API for integrations with SIEMs and Case Management tools.

## DAILY AND WEEKLY MEMBERS REPORT

IT-ISAC produces a daily report that summarizes important cyber incidents and vulnerabilities discovered by or reported to IT-ISAC during the previous 24 hours. This includes information shared by members, partners and identified through open sources and priority indicators or analysis available in the threat-intelligence platform. The weekly report is issued every Friday and summarizes key open source reporting from the week.

## PARTNER REPORTS AND ANALYSIS

IT-ISAC partners often share indicators and analytical reports with IT-ISAC. We then share those with members. Such reporting includes analysis from the Department of Homeland Security, the FBI, other industry specific ISACs and security vendor partners.

## INCIDENT RESPONSE AND COORDINATION

In addition to regular reporting, IT-ISAC issues incident specific reports that provide members with enhanced situational awareness and mitigation strategies. These reports are often developed in collaboration with members, ensuring they reflect the consensus recommendation of our members and enable members to coordinate mitigation activities. These incident reports are issued for cyber and physical incidents alike.

## THOUGHT LEADERSHIP

IT-ISAC represents member interests in information sharing and incident response public policy discussions. This includes the National Cyber Incident Response Plan, standards development, and through leadership in the IT Sector Coordinating Council.

## VULNERABILITY AND EXPLOITATION ACTION REPORT

The IT-ISAC Vulnerability and Exploitation Action Report is shared with members on a weekly basis. This report shows active exploitation vulnerabilities through JPGs, videos and GIFs.

To learn more about membership, visit **www.it-isac.org** or contact our Executive Director, Scott Algeier, at **salgeier@it-isac.org** or **703-385-4969**.

20TH ANNIVERSARY OF THE IT-ISAC
FOUNDED 2000

it-isac.org

@ITISAC

02/06/2020