

IT ISAC

FOUNDED 2000

MEMBERSHIP BROCHURE

IT-ISAC.ORG



Who We Are

The Information Technology-Information Sharing and Analysis Center (IT-ISAC) is the largest and longest established private-sector partnership for information sharing in the IT Sector. Founded in 2000, we are a non-profit organization that provides a trusted forum for IT companies and those that leverage IT for core business functions to share information, manage risks, and collaborate on cyber incident response and strategy.

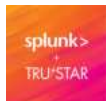
Our mission is to grow a diverse community of companies that leverage information technology and have in common a commitment to cybersecurity, to serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat information, effective security policies and practices for the benefit of all.

We are the only ISAC that supports three critical infrastructure sectors - Information Technology, Food and Agriculture, and Elections. Our membership is comprised of security leaders from leading technology companies across the globe. We have built a network of relationships with trusted partners across the critical-infrastructure community and through this multidirectional sharing, we help companies manage risks to their enterprises and to the critical infrastructure community.

**The attackers share with each other.
The defenders share with us.**

PRODUCTS AND SERVICES

IT-ISAC membership is a cost-effective resource that helps companies to scale their cybersecurity programs. Our experienced Operations Team provides analysis, intelligence, and effective practices that organizations otherwise may not be able to procure. Additionally, IT-ISAC membership comes with the following benefits:



Automated Sharing of Threat Intelligence: Access to the Community Edition of the Splunk Intelligence Management platform which stores, aggregates, and contextualizes, thousands of indicators each week. The platform enables automated sharing and members can leverage custom API and STIX/TAXII integrations to pull indicators into their security tools.



Adversary Attack Playbooks: Over 200+ playbooks that enable members to share tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs) surrounding specific threat actors and their individual campaigns. The playbooks incorporate MITRE's ATT&CK framework and bolster our member's ability to view and share historical and current adversarial information.



Strategic and Tactical Analysis: Curated reports developed by IT-ISAC analysts including daily reports that highlight and link to key security incidents, events, and vulnerabilities, weekly reports that highlight major events from throughout the week, weekly Vulnerability and Exploitation Reports (VEAR), breaking news reports, incident analysis reports, and quarterly trending malware reports.



Incident Response: Timely, incident-specific alerts developed by the IT-ISAC, security partners, and members. Members can also issue Requests for Assistance and Requests for Information to the IT-ISAC team, peer analysts in IT-ISAC member companies, and our global network of security professionals.



Analyst to Analyst Exchanges: Collaboration with analysts from peer companies to address common security challenges and threats. Your concern immediately becomes the concern of other members and partners.



Ransomware Tracker: Since 2021, the IT-ISAC team has maintained a robust ransomware tracker with information being sourced from open-source sites, the dark web, member input, and information shared through the National Council of ISACs (NCI). As of 2024. As of September 2024, the ransomware tracker has recorded over 6,600 events.



Education and Training: 24/7 access to the Notion platform that serves as a repository for past meetings, resources, and best practices. In addition to discounts on various certifications and trainings through partners including CompTIA.

HOW WE SHARE

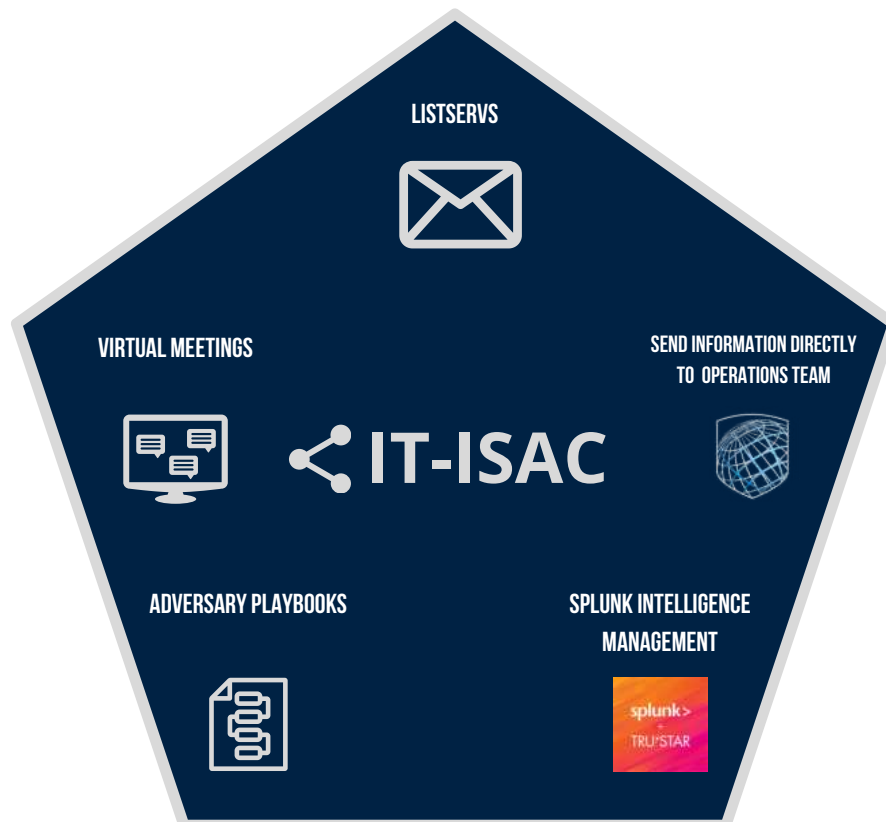
INTELLIGENCE MANAGEMENT PLATFORM

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.



IT ISAC SPECIAL INTEREST GROUPS

A core feature of membership is the ability to collaborate with subject matter experts from other companies on common security topics. Special Interest Group (SIG) members are able to collaborate through virtual meetings and work on impactful projects related to the group's concentration.

CRITICAL SaaS*

The Critical SaaS (CSaaS) 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 to share intelligence information, such as cyber threat intelligence and security practices, with the industry. This SIG is designed for security managers, analysts, and senior level security executives from Critical SaaS companies.

Meets every other Tuesday.



DATA CENTER*

The Data Center SIG (DC-SIG) facilitates operational sharing of cyber threat intelligence, best practices, and effective mitigations among leaders of SIG member companies, enabling members to maintain and protect the integrity and security of information hosted in data centers. This SIG is designed for individuals in member companies who operate within or directly oversee data centers, or provide third-party support to data centers.

Meets on the 3rd Tuesday of every month.



ELECTION INDUSTRY*

The Election Industry SIG supports voting technology providers by giving them an industry-only forum to share information about threats to their enterprises and systems while collaborating on election security and voting challenges. This SIG is designed for participation from senior-level employees at election technology companies, such as those that operate in government affairs or security.

Meets every other Friday.



INSIDER THREAT

The Insider Threat SIG enables members to collaborate on how to identify malicious and non-malicious threats within their organizations, providing a forum for sharing tools and processes used to identify and mitigate insider threats. This SIG is designed for those who are responsible for building and managing insider threat programs within their companies.

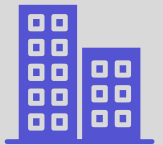
Meets once per quarter.



PHYSICAL SECURITY

The Physical Security SIG provides a forum for members to discuss physical security and business continuity issues and share effective practices to mitigate or respond to threats, as well as to distribute information about natural disasters, accidents, international attacks, and other incidents impacting physical security and business continuity. This SIG is designed for physical security subject-matter experts.

Operates via listserv and meets when requested.



SECURITY INTELLIGENCE

The Security Intelligence SIG brings together senior level analysts from our member companies to exchange ideas, strategies, techniques, and information regarding advanced threat detection and enterprise risk management. This SIG is designed for discussion among senior-level security analysts.

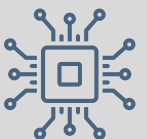
Meets every other Thursday.



SEMICONDUCTOR INDUSTRY*

The Semiconductor SIG facilitates operational sharing of cyber threat intelligence, best practices, and effective mitigations among analysts of member companies in the interest of collaboration and improved security. This SIG is designed for organizations that design or manufacture computer chips or memory devices; develop software used to design or manufacture chips and memory devices; or build machines that make chips or memory devices.

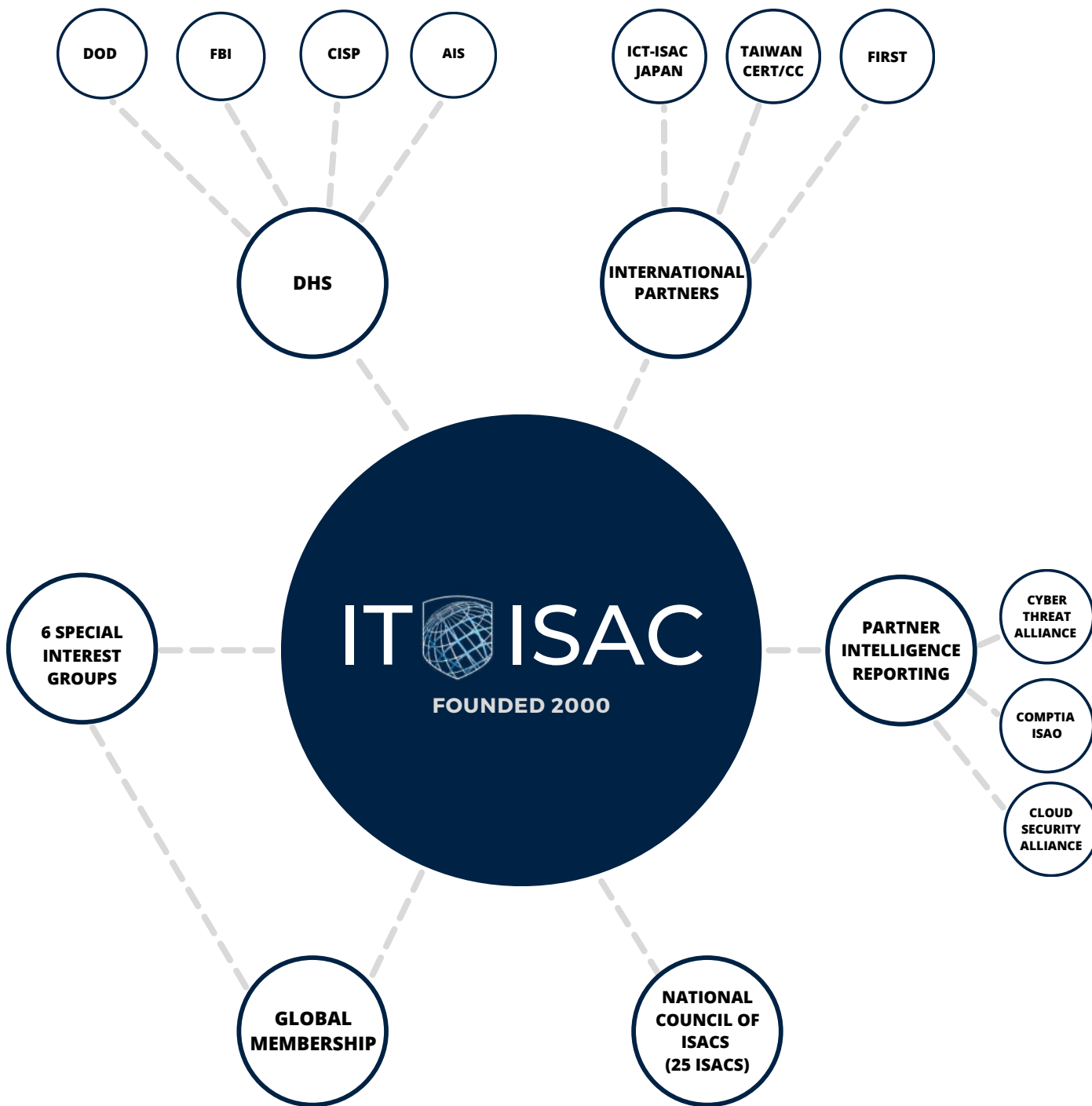
Meets every other Wednesday.



**Requires separate application to the SIG.*

VISIT US AT WWW.FOODANDAG-ISAC.ORG

INFORMATION SHARING RELATIONSHIPS



GET MORE FOR YOUR INVESTMENT

IT-ISAC membership provides companies with a cost effective way to scale their security capabilities and stay on the cutting edge of threat awareness.

For a modest yearly investment, the returns are immense. On average, IT-ISAC membership provides companies with access to **over \$100,000 worth of benefits each year** – that's a huge cybersecurity bang for your buck.

This value is provided through:

- **Daily Threat Reports:** We keep you up-to-date every single day with threat reporting that provides curated analysis and mitigation options - saving your analysts or team multiple hours of work daily.
- **Access to Analysts:** Engage with 600+ leading analysts within the IT-ISAC, instantly broadening and enhancing your organization's cybersecurity program at a fraction of the time and cost.
- **Trusted Data from Experts:** Get access to high-fidelity, verified Indicators of Compromise (IOCs) and intelligence feeds from IT-ISAC members, partners, and the IT-ISAC team.
- **Discounts:** Take advantage of discounts for products and employee education, as well as training with select partners like CompTIA.
- **Learning Opportunities:** Learn from real experiences shared by peer companies on successful (and unsuccessful) security practices deployed by their teams, saving your company time and money.
- **Intelligence Management:** Enjoy no-cost access to an industry-leading intelligence management platform through Splunk.

An investment in IT-ISAC membership will return thousands back in threat intelligence, analysis, data, and community support– and even more in time and resources by helping your team prevent, mitigate and manage cybersecurity incidents.

MEMBERSHIP LEVELS

*We offer three annual membership packages -
designed for small businesses to large enterprises.*

MEMBERSHIP BENEFITS	FOUNDATION GOLD \$25,000	PREMIUM SILVER \$8,000	BRONZE \$3,000
Guaranteed Board Seats	2	0	0
Persons with Access to Weekly IT-ISAC Technical Committee Meeting	15	10	5
Persons Who Receives Analytical Reports	15	10	5
Access to Adversary Attack Playbooks	5	3	1
# of Special Interest Groups Your Company Can Participate In	Unlimited	3	1
Company Listed on Website and Brochure	✓		
Splunk Intelligence Management - Community Edition Credentials	20	10	7
Daily API Calls	1000	600	300
Splunk Intelligence Management STIX/TAXII Integration	✓	✓	✓
Discount on Splunk Intelligence Management Services	✓	✓	✓
Discounts on IT Training & Certifications from Partners	✓	✓	✓

BOARD MEMBERS



As of September 2024

IT ISAC

FOUNDED 2000

Join the IT-ISAC today!



MEMBERSHIP@IT-ISAC.ORG
IT-ISAC.ORG