Collaborate (CSAP)

Share real-time early threat warning advisories for malware, vulnerabilities, threat actors, and attack campaigns with security teams.

BENEFITS & CAPABILITIES

- Enable enterprises assign SecOps priorities to their varied security teams by sharing early warning threat advisories.
- Enable Business units & ISAC members build an intelligence-powered defensive posture.
- Support ISAC members improve threat hunting processes, risk management practices, and overall cybersecurity strategy by sharing intelligence-rich advisories.
- Protect critical infrastructure sectors by enabling cross-sectoral threat advisory sharing amongst different ISACs.
- Boost cyber resilience of all stakeholders in the ecosystem likely to be affected by cyber threats.
- Get exposure to threat intelligence providers’ premium content via participating trial plans.
USE CASE 1: Enterprise to Business Unit Advisory Sharing

A large enterprise can share specific early threat warning advisories with their security teams based on role, location, and business units.

- Enterprises can equip their security stakeholders with the latest insights on emerging threats facing their business operations & infrastructure.
- Different kinds of threats such as malware, vulnerabilities, and threat actors can be prevented using strategic intel from early warning advisories.
- Each business unit can implement necessary defensive measures using insights gained from shared advisories to manage their cyber risks.

USE CASE 2: ISAC to Member Advisory Sharing

An ISAC belonging to a specific industry sector can share early warning advisories with its members.

- ISACs can direct their members to take specific preventive actions based on the threats revealed by shared advisories.
- ISACs can improve the operational collaboration with their member organizations by sharing advisories on threats facing their industry.
- ISAC member organizations can augment their security operations with actionable insights on malware, vulnerabilities, threat actors, attack campaigns, and other critical threats.

USE CASE 3: ISAC to ISAC Advisory Sharing

ISACs from different industry sectors can share advisories amongst themselves to operationally collaborate against cyber threats.

- Different industry ISACs can share advisories amongst each other to promote cross-sectoral cybersecurity collaboration.
- Retrospective lessons learnt from threats faced by one industry can be incorporated to defend another industry by sharing threat advisories among ISACs.
- ISACs can collectively prevent threats facing their hardware & software supply chains by sharing threat advisories with each other.