Intelligence Sharing and Partnerships

If an organization has an established threat intelligence team, someone will likely be responsible for connecting with other organizations to join or form an **Information Sharing and Analysis Center** (ISAC). These are typically industry-specific groups comprised of multiple organizations in order to share actionable intelligence such as indicators of compromise, precursors, and information about attacks and threats.

For example, if Organisation A operates in the aviation industry, and so does Organisation B, they could form an intelligence sharing partnership, and recruit in other organizations that also operate in the same industry. Together they can share information to help each other defend against threats that target the aviation industry. If Organisation B suffers a damaging cyber attack, they can share information about the attack with other members of the ISAC so they can take proactive defensive measures so the same doesn't happen to them. ISACs can be extremely beneficial if members are active, regularly share intelligence, and have online meetings to discuss trends and strategic intelligence surrounding threats.

An example of an ISAC is the Aviation ISAC, or a-isac. This is a collective of organizations that operate within the aviation industry, and come together to share threat intelligence to help each of the member partners to better defend themselves. You can view their website for more information, and an insight into a real ISAC here – https://www.a-isac.com/.

AVIATION ISAC

Having someone that focuses on strategic intelligence to manage and maintain relationships with not only ISAC and industry partners, but also government contacts and agencies could bring valuable intelligence into the organization so it can be used to power defenses and keep team members updated with trends and campaigns that they could have to deal with in the future.