ANOMALI

ExpertFocus

Brought to you by Anomali

January 2019

THE COMMUNITY APPROACH TO SECURITY

When everyone participates—ISACs can be a vital source of security intelligence

Sharing is caring—and smart

Sharing threat intelligence in an ISAC can make companies stronger when they fully participate.

Evan Schuman explains.

If your organization is involved in critical infrastructure such as public utilities, finance, healthcare, national defense, technology, or a similar field, nation-state attackers have put a huge target on your network. Based on recent industry disclosures, you could be facing daily attacks, many of which are successful. Considering the sophistication and ongoing nature of attacks against your networks, it's important to secure your infrastructure.

A 1998 executive order designed to protect critical infrastructure created Information Sharing and Analysis Centers (ISACs). However, the core natures of these ISACs seem at odds with the security executives who participate in them. For ISACs to be effective, they require companies, and more specifically CISOs, to share critical information about attacks they experience with other ISAC members, including direct competitors. The more detailed information a company can share about an attack or breach, the better. CISOs are known for being extremely protective so participating in an ISAC might seem counterintuitive. That said, when all members submit data about attack vectors, new versions of malware, and new approaches attackers are using to breach a company, it improves the collective intelligence industry-wide.

ISACs are private sector organizations that are sometimes known as Information Sharing and Analysis Organizations (ISAOs). They are one of the most effective weapons against mass cyberattacks. Operating on a similar method to virus detection, properly supported ISACs or ISAOs can alert all participants rapidly to active attacks and the specific details needed to thwart that attack. In theory, this could change the attack landscape—from an attacker being able to compromise dozens of corporations—to one where attacks could be blocked after the first few instances are detected.

This theoretically would force attackers to scale down the number of targets, specialize attack methods for each victim, or push them to assault everyone simultaneously and sharply increase the cost of attack. From the security perspective, increasing the cyberattacker's out-of-pocket costs is always a win for the good guys because it makes the potential target less attractive for exploitation.

Matt LaVigna, the CEO for the National Cyber Forensics & Training Alliance (NCFTA), says he has repeatedly seen companies join ISACs without a firm plan. Organizations "are told that they should join ISACs" and yet they "are often not given guidance on how to interact with the organizations or what return on investment they should expect," LaVigna says.

Some companies "see ISACs as 'I am just going to sign up and plug in and get all of this amazing intelligence,'" says Travis Farral, Director of Security Strategy at Anomali, a Redwood City, California-based threat intelligence service provider. "Although that might be true to a small percentage, getting solid value is a little more complicated. The number [of companies actively sharing] versus those simply digesting is hugely lopsided."

> “The perception is that the ISAC is performing some sort of magic, that it has access to a pool of knowledge and that there’s no work involved on the part of the members”
>
> *– Alex Rifman,Director of Customer Success, Anomali*

Alex Rifman, the Director of Customer Success at Anomali, concurs that many new members of ISACs have unrealistic expectations “I think the perception is that the ISAC is performing some sort of magic, that it has access to a pool of knowledge and that there’s no work involved on the part of the members,” Rifman says. “We call it the consumer versus producer culture.”

A more realistic approach to take is to understand that ISACs can deliver huge security benefits to companies, but they also require cooperation and active participation on the part of its members. For example, such participation could include putting a system in place to alert the ISAC instantly when a company realizes they are under attack. This threat notification to the ISAC would require the technical details of the attack so that other members would know exactly what to look for and how to defend against it if they should suffer the same attack.

The key challenge ISACs face is getting members to understand that the intelligence is only valuable if everyone gives and receives. An ISAC’s effectiveness is predicated on seeing rivals as teammates in fighting attackers. In other words, when one company shares their attack details with a rival and thereby helps that rival thwart the attack, it is a win for both companies—and everyone else in that vertical. But that flies against the competitive nature of many C-levels, who instinctively see information-sharing with rivals as exposing a weakness that the competitor could later choose to exploit.

It also creates a situation that might appear to be anti-competitive, even though lawmakers protect this type of exchange and make it immune from antitrust violations.

Sanitizing the data

Given that this data is being shared with direct rivals, a critical part of an ISAC strategy must be sanitizing the data. This is done so that rivals know everything about the attack but little to nothing about who the specific victim was or anything else that might disclose proprietary information.

Rifman describes this as herd protection, where each member gets indirect benefits from protecting fellow herd members, even if they are competitors. Rifman offers the banking vertical as an example. For banks to convince customers that financial institutions are a safe place to deposit funds, each bank must make sure the customers realize their accounts will be safe. When all banks work together to share information about attacks that one of its members has experienced, they all benefit from being able to protect themselves from the same attack—the bank “herd” is safer because now all member banks can protect themselves without necessarily being attacked, according to Rifman.

But sanitization has its issues. There can be a nuanced line between removing everything that reveals details about your defense systems and your company’s identity to making the information useless to other members of the ISAC. Other times, there exists no such line: To share information helpful to others, the company might have to reveal some sensitive operational details. That’s where the CISO needs to make a difficult decision.

As LaVigna points out, sometimes that decision is not entirely

“There’s got to be a middle ground. Just giving a list of IPs that are knocking on my door is not helpful”

– Matt LaVigna, CEO,
the National Cyber Forensics & Training Alliance

up to the CISO. Some general counsels will refuse to let certain information be shared, even if that information is critical to protecting others in the industry. “The counsel will generally say ‘no.’ It’s safer to say ‘no’ [than] to say not [to] share,” LaVigna says. “Unfortunately, that way of thinking is playing right into our adversary’s hands. That’s what they rely on so they can replay their attacks over and over against new victims.”

The information to be shared can—and should—be sanitized to remove unnecessary details, but it is also easy to go overboard and to sanitize too much. If you sanitize too much you can make information non-actionable for others who receive it, LaVigna says, “There’s got to be a middle ground. Just giving a list of IPs that are knocking on my door is not helpful.”

Rich Schliep, the Chief Technology Officer for the Colorado Department of State, says, “We’ve seen instances where [security staff] shared information that they didn’t have the right to share. When that happened, trust levels plummeted. People then are no longer willing to share information. They’re afraid that it may impact them in a negative way.”

Roberto Sanchez, Director of Threat and Sharing Analysis for Anomali, adds that when sharing attack data, context is crucial. Although essential, it is not solely about what the attacker did and tried to do. It is also important for CISOs to say what they tried to do to counter the attack and what did and did not work. The whole point is to help others defeat—or block—their common attackers.

To do this, CISOs and CSOs must be motivated to prioritize feeding the ISAC. “It’s a question of value. You need to take care of your own house, first and foremost,” Farral says, adding that technology can allow a company to prioritize protecting itself first and then feeding intelligence to the ISAC without asking CISOs to sacrifice the speed of their own defensive actions.

Farral notes that a CISO can “develop a mechanism so that as your SOC (security operations center) is receiving [alerts], they are tagging everything for the ISAC.” This way, a company’s SOC can automatically share data with the ISAC without additional user intervention. “Responders should be doing this as part of the normal process of handling those tickets,” Farral says. “This translates to no heavy lifting for” security teams. “This is a technology problem and is totally solvable.”

Community service

When sharing data with the ISAC, speed is critical. How timely does timely data have to be? “Sometimes, timely is a few minutes,” he says. Indeed, the only viable security conclusion when an ISAC feed sends an attack alert in your region or vertical is to assume that your company is next on the attack list.

Farral points out that this data-sharing is two-way. Let’s say an attack occurs and your system alerts the ISAC while your team is dealing with the event. By sharing the information, “you’re going to get a much broader view, with many different skills and backgrounds and experience levels. You’re going to get a lot more technological visibility than in just your own environment,” he says.

Another argument for sharing is momentum. The actions of one

“If the feeds are out there and you aren’t checking them quickly enough, they won’t do you any good”

– Rich Schliep, Chief Technology Officer, Colorado Department of State

CISO will likely influence the actions of other CISOs. In short, sharing begets sharing and not-sharing begets more not-sharing.

Trusting your fellow ISAC members is only one-half of the battle. CISOs also need to have confidence and faith in the ISAC itself.

“I think one of the biggest misperceptions CISOs or CSOs have is that they look at ISACs as a vendor offering security services. ISACs are a community of owners and operators and other stakeholders within a particular critical infrastructure sector,” says Denise Anderson, President and CEO of the Health Information Sharing and Analysis Center (H-ISAC).

“The community through the ISAC has a trusted forum to share relevant, timely and actionable information about threats and vulnerabilities and a place to share lessons learned and best practices,” she says. “It absolutely is a place where one organization’s defense is another organization’s offense. The more C-suite executives know and understand that they need to work together with their peers to overcome threats, the stronger and better off everyone will be.”

Another point to consider when formulating an ISAC strategy is cost considerations. Sanchez pointed out that some companies have leveraged their ISAC colleagues to share the cost of security analyst resources, with one analyst interacting with the ISAC for multiple companies. This would allow for example, an employee with an annual six-figure salary to cost each company only a small percentage of that amount, Sanchez notes.

Colorado’s Schliep points to staffing as one of his top concerns when discussing how companies are handling their ISAC efforts.

The problem, he says, is that many security operations have too much work and too few employees. “What typically happens is that you only have so many skilled people, and one engineer” is asked to handle too many security tasks. “The first thing the engineer is going to do is defend” their employer by reacting to an attack and not necessarily focus on ISAC reporting.

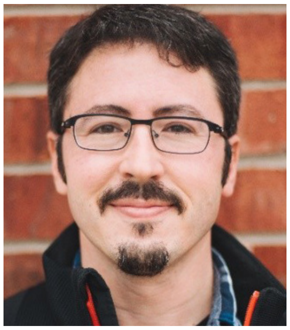
“We need better tools in place for automated reporting,” he continues. That speed concern is twofold: Not reporting an active incident quickly enough and also not checking the ISAC feeds to learn of an imminent attack often enough. “If the feeds are out there and you aren’t checking them quickly enough, they won’t do you any good,” Schliep says.

He also points to customization as critical. That means making sure that the ISAC’s software that interacts with your security information and events management (SIEM) system understands your environment, your employees, your partners, and your customers. “It has to factor in the IPs that are legitimate customers, but you have to have that programmed in ahead of time,” Schliep says.

SMBs: Sharing the wealth

When it comes to arguing for the benefits of security data sharing, various governments are proving helpful, whether it is U.S. Department of Homeland Security’s (DHS), Automated Indicator Sharing (AIS), the DHS Cyber Information Sharing and Collaboration Program (CISCP), or the United Kingdom’s Cyber-security Information Sharing Partnership (CiSP).

But whether the efforts are being pushed by private entities or



“Not all organizations have the resources to stand up full-blown threat intelligence practices capable of producing their own intelligence”

– Travis Farral, Director of Security Strategy, Anomali

government agencies, the biggest obstacle is the budget. To be more precise, it is the flawed perception that the company cannot afford to fully embrace an ISAC strategy, due to budget constraints.

“Not all organizations have the resources to stand up full-blown threat intelligence practices capable of producing their own intelligence,” Farral says. “Although this is not a requirement for sharing indicators or other types of intelligence, it is still a primary reason that organizations feel they have nothing of value to contribute.”

Although two-way information sharing is the most effective means of protecting company assets, not all industry security data sharing efforts go that route. Indeed, unidirectional threat intelligence sharing, where one entity gathers and then shares data with others, is the more common approach, he notes.

Farral points to open source intelligence, “which might involve downloading a publicly available report covering a recent attack that contains indicators and methods used, or ingesting an open source intelligence feed,” as a good example.

Then there is the small and midsize business (SMB) factor, especially for smaller companies. Although ISAC strategies are generally envisioned for large enterprises in a critical infrastructure industry, it is important for enterprise security that a significant number of smaller businesses also participate.

“Organizations with smaller information security teams and smaller budgets may feel like they don’t have anything to contribute that isn’t already being covered by larger organizations or those with bigger budgets,” Farral says, even though it’s decidedly not true.

Indeed, because they are often seen by cyber thieves as having weaker security, smaller businesses are often attacked first. That could be because attackers are using methods that would likely not work against the more robust defenses of a large enterprise or—and this is critical—as a testing ground for a new attack method. Smaller businesses, therefore, have vast amounts of data that is valuable to share, Farral says.

The best place for companies to begin their ISAC efforts are within their own vertical, with similar companies facing similar threats. But the best security efforts should not stop there, as there are powerful reasons to expand beyond one’s own vertical.

“Industries develop muscle memory around specific threats that are commonly seen and attacks from certain actors or groups become easily recognizable,” he continues. “What happens when one of these groups or actors suddenly moves into a new industry, though? The chances are that little may be known about them in that new industry.

“Some information can be carried forward through third-party threat intelligence services, but likely not the full breadth of knowledge that the previous industry has built around that actor or group,” he notes. “The result is that the new industry is caught with little knowledge of the adversary and insufficient means of protecting themselves.” This does not need to be the case.

DHS Fusion Centers

Sometimes determining with whom to share data can be simply a question of geography.

“Finding partners local to your organization’s physical location also has benefits. Not all attacks

“The community through the ISAC has a trusted forum to share relevant, timely and actionable information”

– Denise Anderson, CEO,
Health Information Sharing and Analysis Center (H-ISAC)

are remote in nature. Physical breaches, Wi-Fi attacks, USB drive drops, and hybrid trespassing and information security attacks may indicate local actors with physical access to entities in the local area,” Farral says.

“Additionally, localized events such as weather, terrorist attacks, and accidents would benefit from localized sharing of intelligence that is not dependent upon an industry or vertical. In the United States, DHS Fusion Centers are a great place to start with localized, cross-industry sharing,” he continues. “Networking at local security events is a great place to find good intelligence sharing partners as well.”

Homeland Security’s Fusion Centers differ slightly from ISACs. “Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners,” according to the DHS website.

Unlike ISACs, which are targeted at critical infrastructure industries, “Fusion centers are information sharing hubs that provide comprehensive and appropriate access, analysis, and dissemination that no other single partner can offer,” the agency says. Also, the fusion center is targeted at a geographic location rather than an industry, so sharing is with local companies rather than a room full of potential competitors.

One determining factor as to what type of intelligence sharing a CISO can conduct is as basic as looking at their employer’s business. Currently, there are 20 ISACs that address critical infrastructure industries, but Fusion Centers are geographic and open to any company, regardless of their industry. You can find a list of ISACs here, while details about Fusion Centers can be found here. Whatever option you choose and whatever your organization’s budget, sharing threat intelligence data about a breach attempt you have seen can go a long way to reducing the effectiveness of that attack. ■

ANOMALI®

Anomali® detects adversaries and tells you who they are. Organizations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide. For more information, visit us at www.anomali.com and follow us on Twitter @Anomali.