BUILDING A FOUNDATION FOR SUCCESSFUL CYBER THREAT INTELLIGENCE EXCHANGE

KEY CONSIDERATIONS FOR CORPORATIONS SEEKING TO COLLABORATE ON SECURITY INCIDENTS IMPACTING THE CLOUD ENVIRONMENT

cloud security alliance®

Table of Contents

Acknowledgements

CYBER INCIDENT SHARING WORKING GROUP CO-CHAIRS

Dave Cullinane
Brian Kelly

LEAD CONTRIBUTORS

Ramsés Gallego
Krishna Narayanaswamy
Edgar Odenwalder
Rich Phillips

ADDITIONAL CONTRIBUTORS

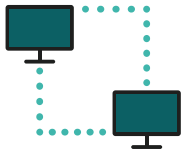
Mariano J. Benito
Ryan Bergsma
Olivier Caleff
Elvis Hover
Leo Magallan
Christine Mullaney
David Neuman
Kavya Pearlman
Codina Ramon
Carlos Samaniego
Stacy Simpson
Jeff Valdes
John Yeoh
Richard Zhao

Overview

No organization is immune from cyber attack. Malicious actors collaborate with skill and agility, effectively moving from target to target at a breakneck pace. New attacks are directed at dozens of companies within the first 24 hours and hundreds within a few days.[1] A few years ago, visibility into the threat environment was essential if cybersecurity was to have any hope of being preventive. Today, visibility into what is coming next is critical to simply staying alive.

Sophisticated organizations, particularly cloud providers, know that the difference between a minor incident and massive breach lies in their ability to quickly detect, contain, and mitigate an attack. As increasing their speed of response has grown into a top priority, cloud providers are increasingly participating in programs that allow them to exchange information on cyber events with others in the industry. Sometimes known as threat intelligence exchange or cyber incident exchange, these programs enable cloud providers to share cyber event information with others who may be experiencing the same issue or at risk for the same type of attack.

There is no denying that cyber security information sharing has in the past been of somewhat limited value for security teams. While this was due in part to past legal and cultural obstacles to the free exchange of cyber threat data, the primary challenge was the manual and reactive design of legacy information sharing programs. These programs were more focused on sharing information about cyber security incidents after the threat was vetted, scrubbed and mitigated more as a public service to others than a tool to support rapid incident response. While this data served a purpose and had a place, as the speed and number of attacks increased, its value was diminished and information sharing was not widely adopted outside of a few critical infrastructure sectors.



Cloud providers are not alone their interest in cyber threat exchange. Security executives and thought leaders across industries are taking a fresh look. In the U.S., cyber threat information sharing is included in the U.S. National Institute for Standards and Technology (NIST) voluntary framework for reducing risks to cyber infrastructures as both a risk assessment and incident response activity, and highlighted as a means to support and facilitate cyber risk management in the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

NIST Cybersecurity Framework

US Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

1 2017 Data Breach Investigations Report 10th Edition by Verizon, April 27, 2017

Overview cont.

Fast forward to today's security environment and the exchange of information about cyber incidents is practically unrecognizable from the information sharing programs of the past. As Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) have matured, new tools and technologies in threat intelligence, data analytics and security incident management have created new opportunities for faster and actionable threat intelligence exchange. Incident data -- more accurately described as suspicious event data -- can now be rapidly shared and analyzed across teams, tools and even companies as part of the immediate response process. In fact, it can be said that if an organization waits to share information until they have an "incident", they've waited too long. Now the focus is on sharing suspicious event data as soon as it is identified, which materially speeds remediation and provides an early and actionable warning to those not yet affected.

The positive impact of this new model for threat intelligence exchange was demonstrated during the Wannacry Crisis in May 2017. Though the first reports of infection originated in Spain on May 12, the UK and Scotland were hit far harder by the malware. This was due in large part to the Spanish Government's incident response scheme for critical infrastructures, such as warnings from the National Cryptology Centre[2], which quickly identified the malware and its vectors, provided mitigation tools, and encouraged organizations to share this information. Spanish companies were able to quickly protect themselves against Wannacry even as the malware continued to spread in other countries. Threat intelligence spread by the United Kingdom's National Cyber Security Centre (NCSC)[3] to understand and share the best mitigation guidance provided the eventual killswitch to the Wannacry virus.

Cloud providers have a unique role to play in threat intelligence exchange because they not only own and manage a massive amount of the world's IT infrastructure, but they also operate some of the most advanced CSIRTs/SOCs seen in the technology world. Due to this investment, they are arguably in the best position to operationalize shared intelligence to defend their systems. Further, because they can do this at scale and involve a significant part of the industry in the effort, they have a tangible opportunity to help level the playing field with malicious actors. CSA also has initiatives underway to help its members do both.

2 https://uk.reuters.com/article/us-spain-cyber/telefonica-other-spanish-firms-hit-in-ransomware-attack-idUKKBN1881TJ
3 https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0

Overview cont.

This paper, the first in a series, provides a framework to help corporations seeking to participate in threat intelligence exchange programs that enhance their event data and incident response capabilities. It is primarily written for corporations beginning to explore, or who have already begun, the exchange of cyber security event data. It is designed to be helpful to security teams with both emerging and mature internal threat intelligence capabilities. In fact, any organization with at least one person dedicated to threat intelligence should consider participation in an exchange to enhance its own data. To this end, this paper will provide high-level practical guidance to support companies in three key areas:

- Connecting with sharing partners and exchange platforms that best meet their needs
- Identifying the capabilities and business requirements that will form the foundation for a value-driven threat intelligence exchange program
- Understanding the basics of the exchange process so they can efficiently share event data they are seeing and more efficiently operationalize any intelligence they collect

The guidance in this paper was developed by members of the Cloud Security Alliance (CSA) **working group**[4] on cyber incident sharing. The work has been instrumental to the design, development, and operation of the **Cloud-CISC**[5] (Cloud Cyber Incident Sharing Center), a threat intelligence exchange platform for CSA members. The recommendations are based largely on the lessons learned through the development and operation of Cloud-CISC, as well as individual experiences in managing threat intelligence programs for large companies. Some common challenges identified through this work include:

1. Organizations that struggle to understand their internal event data have difficulty determining what event data to share.
2. Even when threat intelligence is provided by others, its value is often limited because it is delivered in an email format that cannot be easily integrated into the response process.
3. Organizations want the means to scale laterally to other sectors and vertically within their supply chains.
4. Perhaps most surprising, the motive for sharing is not necessarily helping others, but rather to provide better support for internal response capabilities.

The intent for this paper is to directly address these challenges and help establish a basic framework of key considerations for those getting started with threat intelligence exchange. We hope to work with others in the industry to further develop this guidance and define the associated best practices to make threat intelligence exchange a valuable resource and community for all organizations facing increasing threats from cyber attacks.

4 CSA Cyber Incident Sharing Working Group **https://cloudsecurityalliance.org/group/cloudcisc/#_overview**
5 CloudCISC **https://www.csa-cloudcisc.org/**

Finding Your Fit

Evaluating Sharing Programs

A well-designed sharing program can provide a great deal of support to members and enable organizations of different maturity levels to both participate and derive value from external threat intelligence exchange. While legacy information sharing programs still exist and have their place, the focus today should be on new models for threat intelligence exchange that do more than enable sharing after a threat has passed. Rather, cyber incident exchange should accomplish three key goals:

1. **Enable Sharing** Share meaningful cyber event data safely, easily and early in the response process, in order to leverage external data during remediation efforts and provide early warning to help others reduce their own exposure.
2. **Expand Expertise** Collaborate with skilled security analysts from vetted cloud providers and cloud customers in order to analyze attack indicators, develop defensive strategies and decrease time to mitigation.
3. **Provide Context and Support Decision-Making** Avoid duplication of effort and benefit from what others have already learned.

LEGACY INFORMATION SHARING PROGRAMS	THREAT INTELLIGENCE EXCHANGE PROGRAMS
Share data about incidents after events are vetted, analyzed and often mitigated	Share suspicious event data as soon as it is identified
Data often shared via email, listservs and other manual	Data shared in many different formats, including via APIs
Often rely on trusted third party to manually scrub shared data of confidential information or submitter identity	Leverage encryption and other technologies to provide automation, anonymity, and sensitive or proprietary data redaction

This chapter will review the role of an exchange platform and sharing programs (like, but not limited to, CloudCISC) and how these help support participants. For the purposes of this document, an exchange platform is defined as the underlying system that supports the exchange of incident information and allows companies to form sharing relationships with industry peers, governments, and other relevant outside organizations.

Establishing Sharing Relationships

There are numerous opportunities for companies to develop sharing relationships with outside organizations. While there are a number of threat intelligence platforms that assist companies in facilitating direct sharing relationships with their peers, many organizations new to threat intelligence exchange start with relevant industry groups, particularly sector Information Sharing and Analysis Centers (ISAC), Information Sharing and Analysis Organizations (ISAO) and/or Sectorial Computer Security Incident Response Teams (CSIRTs)/Computer Emergency Response Teams (CERTs) where they exist. ISACs/ISAOs/CSIRTs/SERTs have a long history of facilitating sector-specific cyber security information and many of them have modernized their infrastructure to run on exchange platforms that offer robust automation and data analysis capabilities. Depending on its needs, a company may also choose to share with the **Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) service**[6], a DHS-facilitated ecosystem of private and public sector partners sharing threat intelligence, or with Malware Information Sharing Program (MISP)-based services offered by sectorial CSIRTs.

Evaluating Exchange Platform Capabilities

CSA believes that the cloud industry has a mandate to lead in threat intelligence sharing given its unique and near ubiquitous footprint in the global IT infrastructure. A sharing program for cloud providers, Cloud-CISC, was formed as a pilot project in 2015 and launched in beta a year later. The goal was to develop a threat intelligence exchange program that could fully take advantage of the latest advancements in threat intelligence and "big data" analytics and would concretely and seamlessly support our members' incident response workflows.

CSA is proud to offer its members one the most advanced threat intelligence exchange programs available. The CloudCISC was designed with our members to power real-time incident sharing and analysis that delivers immediate value to the incident response efforts of CSA members.

Once an incident report is shared, the CloudCISC platform's unique algorithms provide near real-time correlation with reports supplied by other vetted members. If similarities are discovered, members can be alerted and provided with the related reports that contain additional attack indicators, valuable context and mitigation advice. Members might also decide to collaborate in other ways, such as joining in on response efforts.

For a limited time, all CSA corporate members can sign up for two CloudCISC licenses at no cost. We encourage all our corporate members to sign up today at **https://www.csa-cloudcisc.org/**.

6 Department of Homeland Security's Automated Indicator Sharing (AIS) service **https://www.us-cert.gov/ais**

The decision to participate in a specific sharing program should be driven foremost by an organization's individual business and security requirements. Further, sophisticated organizations should not limit threat intelligence sharing to one group or system and will find value in establishing partnerships with multiple sharing organizations. That said, CSA has learned many lessons about how the design and capabilities of sharing programs, and the exchange platforms that support them, directly impact the participation rates of users and the value they receive in return for their efforts. Describing the operational capabilities of CloudCISC essential to achieving the stated goals for threat intelligence sharing will assist companies in their efforts to evaluate sharing programs and exchange platforms.

Establishment of Trust

In order for sharing to occur there should be a level of trust established both with the program operator and its participants. This can be accomplished through a standard non-disclosure agreement (NDA) or memorandum of agreement that could be shared by both the provider and all participants, who understand that the information is only to be shared within the members of the threat intelligence exchange. Further, the program operator should vet all prospective members to ensure that they are legal entities with a legitimate purpose for exchange membership.

For cases where the exchange program offers member-led smaller groups, sometimes referred as enclaves, the exchange operator should offer a standard NDA and vetting support to the members for their use in driving those smaller group collaborations.

Prospective participants should also ensure they understand whether the exchange provides incentives for contributing data and consequences for non-participation. Incentive-based participation benefits the exchange and its participants by encouraging active participation from all members.

Anonymity of Participants and Data Sanitization

One essential lesson learned from legacy information sharing efforts is that companies must have a way to ensure their brand, customer trust, and core business is not damaged by the inadvertent disclosure of confidential incident data. This is achieved in threat intelligence exchange through member anonymity and data sanitization.

It is worth highlighting that the experiences with CloudCISC have underscored the benefits of providing anonymity through the exchange platform. By ensuring that the event data being shared cannot be attributed to its source, the risk to the enterprise of sharing information has been greatly reduced. This has allowed CloudCISC members to share richer data earlier in the response process and enabled the rapid initiation of collaborative response efforts.

Participants should have the capability to anonymize their submissions to protect their identities. The threat intelligence exchange should know that the submitter is an authorized member and perhaps be able to obtain limited demographic information about the sender, such as its sector, but no further information should be needed. The exchange provider and other exchange participants should not be able to determine which company submitted what data.

While only the submitter knows what data/info should be obfuscated to ensure that the submission is anonymous, different exchange platforms offer varying levels of support, automation and protection to participants. One recommended approach is obfuscation by hashing. This method allows the data from various submitters to be correlated, without revealing their specific identities. If four companies submit the same hashed value, this data can be correlated and used to help those four companies better respond to what may be happening.

Information feeds ingested into a threat intelligence exchange platform should be stripped of any pertinent company data. While it would be incumbent on the reporting entity to perform this action, different exchange platforms will offer varying degrees of support to participants and may offer different ingestion formats. It is critically important that participants understand how data sanitization is achieved so they can ensure all confidential corporate information remains protected.

Finally, some exchange platforms offer a "preview" capability that allows companies to input their own data and see what correlations exist, prior to exposing the inputs to a larger audience.

Open Standards

The more participants in an exchange, the more incident data it can collect and correlate to benefit of its members. Ideally, the exchange platform used should not limit participation through commercially restrictive technologies or single ingestion formats. For instance, while the Structured Threat Information eXpression (STIX)[7] and the Trusted Automated eXchange of Indicator Information (TAXII) are rapidly gaining acceptance as information sharing specifications, many companies have not implemented them, especially smaller businesses. The ability to enable a broad base of participation is especially important to companies that wish to use threat intelligence exchange as a way to understand risks and incidents within their supply chains.

Thus, an exchange platform should use open protocols and non-commercially restrictive infrastructure. This includes the ability to accept data in virtually any format. In cases where a more restrictive platform is being evaluated, the participant should understand its limitations and ensure that it will integrate smoothly into the more restrictive environment.

7 International in scope and free for public use, TAXII and STIX are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis. More information: **https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity**

Automation

Incident response teams are busy so ease-of-use has to be a consideration. It must be fast and easy for an analyst to input data and to ensure the submission is scrubbed of company-specific confidential data. Threat intelligence exchanges should offer automated tools that facilitate quick and easy data submission.

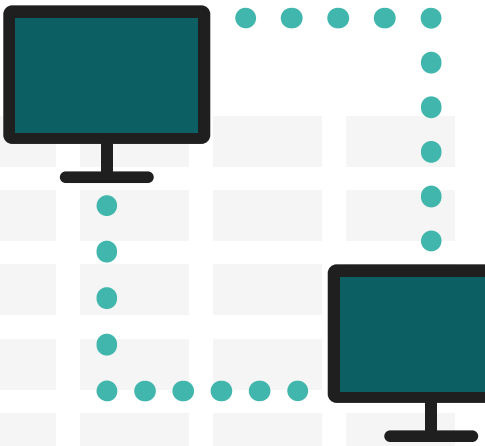
Further, the ability to integrate with Security Incident Event Management (SIEM) systems is essential. SIEM's should be able to leverage application programming interfaces (APIs) from the threat intelligence exchange. Other automation capabilities include email ingestion and notification, which can help incident response personnel more quickly notify and collaborate with peer organizations when an incident occurs..

Analysis at Scale

Response times must be in minutes, not hours or days. When an incident response team identifies a potential attack they have numerous actions to take and relatively little time to make decisions. Suspicious events submitted to a threat intelligence exchange must be quickly and accurately correlated, and actionable data must be rapidly returned in a format that is easy for the analyst to examine and manipulate.

To achieve this, a threat intelligence exchange must be able to efficiently perform large scale analysis. Understanding how an exchange platform correlates and manages "Big Data" is essential to evaluating the level of real-time assistance it will be able to provide when an incident occurs.

Information returned by the CIE should be actionable and contextual. Data visualization capabilities can be extremely helpful in enabling participants to quickly see how incident data relates to their organization and its environment. Ideally, an exchange platform should have the capability to show correlated information from the feeds shared by participating members. For instance, information provided by one entity should alert an associated entity within the threat intelligence exchange whenever and wherever their information is contained in correlated Incident Operation Centers (IOCs).



Collaboration

Receiving an early warning on new threats is beneficial. However, threat intelligence exchange becomes a strategic part of the incident response process when it enables teams to work with others in real-time as they manage identified and potential threats. If someone in the community has already found the fix, it should be rapidly communicated so no member of the exchange has to reinvent the wheel. Such collaboration allows organizations to leverage the expertise of others in hunting threats and mitigating attacks as they are occurring. This can be especially beneficial to small and midsize companies who sometimes struggle to hire and retain top talent in threat intelligence. Specific tools the exchange can offer via its chosen platform include: the ability to chat/message either anonymously or with attribution; the sharing of SIEM scripts or other methods that could assist the common community; shared or appended notes from members that travel in the same feed as incident data; and a standard digest report to report daily, weekly or monthly exchange activity.

Industry/Peer Organization Enclaves

Controlled, secure, and approved sub-groups allow industry peer members to share information between each other and resolve issues prior to releasing the data to a wider audience. Organizations within sub-groups are often approved between with non-disclosure agreements (NDAs). In this document, we refer to these sub-groups as enclaves. The inclusion of enclaves would allow a smaller group with common interests to participate on a separate exchange to share data amongst themselves. For example, an enclave of airline companies can resolve issues amongst each other prior to releasing the information and data related to a given threat to a larger audience outside the airline industry. Information that is shared within an enclave remains proprietary until the group decides to release it to the broader community of interested organizations in their exchanges.

Time Syncing

Time synchronization is essential to troubleshooting and even more critical for correlating events. All devices and peers within a threat intelligence exchange should be synced through a common NTP hierarchical solution, which would be sourced by a standard NTP Stratum.[8]

8 See **www.ntp.org** for more information on NTP Stratum

Before You Join

Building a Foundation for Success

Given the advanced capabilities of threat intelligence exchange, particularly in the areas of automation and collaboration, successful participation in cyber incident sharing does not need to be limited to organizations with highly mature intelligence and response capabilities. Any company with at least one person dedicated to threat intelligence should consider participation in an intelligence sharing program to enhance its own data.

Threat intelligence exchange can be a valuable asset for both threat intelligence management and incident response functions. Increasingly, we are seeing both of these functions come together in the SOC, where analysts manage multiple tools, products, and workflows including SIEMs, ticketing and orchestration platforms, threat feeds, vulnerability scans and endpoint detection products. Whether a corporation has one analyst or thirty, the idea of adding yet another tool to the mix can be daunting. However, when used correctly, threat intelligence can be a force multiplier to accelerate and streamline investigations saving security teams valuable time. To achieve this, organizations should take a few steps to help ensure successful integration of threat intelligence exchange into their SOC workflow.

Capture Internal Event Intelligence

Many security analysts monitor a large universe of tools, storage systems, and data feeds even before joining a threat intelligence exchange. Many providers have SOCs monitoring issues across containers, hybrid architectures, and deep into the supply chain. Organizations should create and maintain a common repository of the event data they are capturing across their own systems. By seeing how events reported in the repository correlate within events in their own organization, companies will be better positioned to understand how new data from a threat intelligence exchange may impact them. Performing this internal analysis enables them to quickly determine how and when to share event data with an external exchange. In this way, intelligence sharing complements their existing threat intelligence operations, rather than adding just another new feed to monitor.

Consider How to Use Intelligence Insights

Joining a threat intelligence exchange will enrich an organization's event data, but only if consideration is paid to how this data will be used. Companies have discovered they often can't easily integrate external threat feeds from proprietary threat providers or sharing centers. Sometimes this is a result of poor incident reporting and correlation from the external threat intelligence exchange, but it can also be the result of a lack of planning and support for security analysts. Manually sifting through emails containing lists of suspicious IP addresses is not only time-consuming and of questionable value, but it can also burn out talented staff.

To avoid these issues, organizations should develop a plan for how they will operationalize threat intelligence they receive from an exchange. Their plan to integrate threat intelligence from an exchange should identify ways the intelligence can be utilized in alerting, triage, investigation and mitigation of internal events. This includes automating key processes and selecting a tool to help analysts correlate data in real-time and more easily extract key indicators. Automation and tooling should also include careful consideration as to how a selected threat intelligence exchange delivers data to the organization.

Measure Participation and Value

Any new investment of time and resources should be subject to an ongoing review of the value it returns to security operations. Organizations should define their expectations and goals to be achieved through their participation in a threat intelligence exchange and consider how they will measure the return on investment. Common goals are to fine tune SIEMs, obtain better or more operational intelligence related to a relevant sector, and gain more tactical intelligence regarding specific threat vectors.

Organizational objectives should include clear goals for the security teams' activities around sharing and operationalizing data, obtaining and providing feedback on how shared data supports mitigation processes, and some consideration of the cyber risk reduction that results from receiving earlier indicators of attack.

Develop Policy

After these considerations related to participation in a CIE are made, it can be useful to document them in an incident exchange policy that places them in context within the broader incident response plan and overall security policy of the organization. Such a documented policy may include:

- Purpose of use
- Roles and Responsibilities (e.g., may include who is authorized to input data, who is authorized to see results, who is authorized to conduct research on the data, etc.)
- Provider requirements for the exchange relative to the security of data
- Data input requirements
- Data retention requirements
- Responsibilities in the event of an incident

Getting Started

Operational Guidance on Threat Intelligence Exchange

The guidance in this section is designed to help companies better understand the threat intelligence exchange workflow so they can more effectively integrate it into their existing security operations. Our goal is to help companies efficiently share information with the exchange platform and more effectively ingest and operationalize threat intelligence they receive.

There are some guiding principles for exchanging incident or threat information the working group used in the development of this guidance. While business and technical requirements vary for different organizations based on several characteristics including industry vertical, risk appetite, technology, and operational maturity, the working group found that there were several important expectations shared among Cloud-CISC members. These expectations drove the development of this model for threat intelligence exchange and the associated best practices. They include:

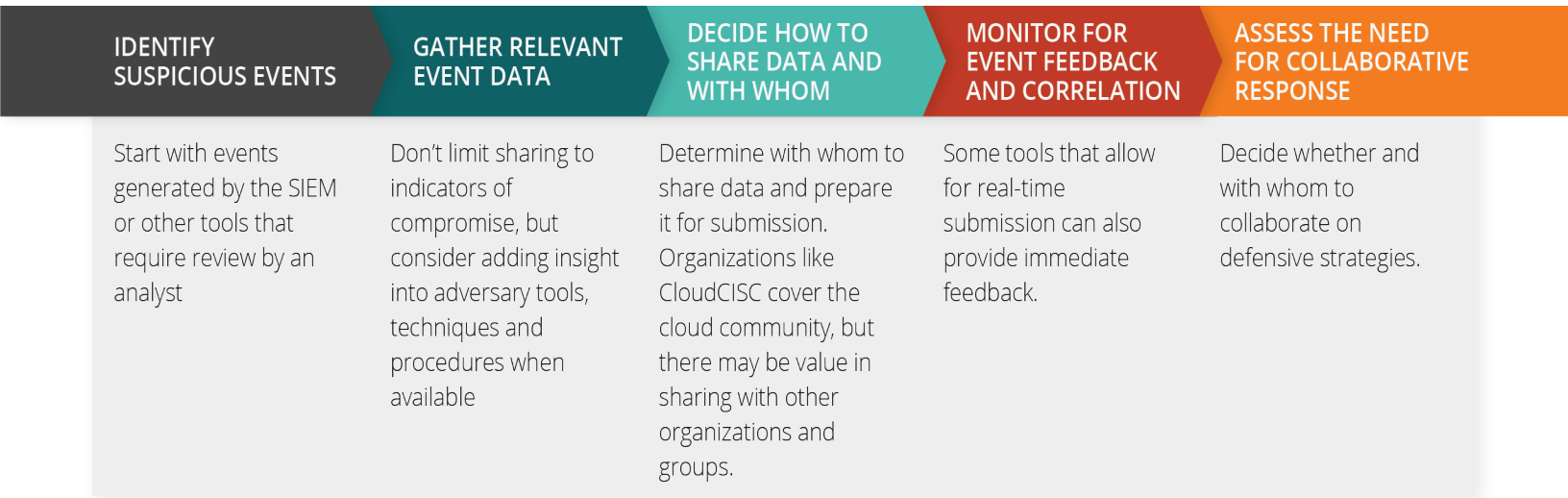
- Security (or incident) information without context is incomplete. Context is necessary to develop informed operational and business decisions..
- The taxonomy of the information must offer agility in the way it is served and/or digested for timely decisions and action.
- More data is better and enables better analysis for evidence-based information and risk assessment.
- Make no assumptions regarding legal, policy, and risk constraints and involve subject matter experts to enable sharing.

This paper delivers a model for the threat intelligence exchange process and includes some high-level best practices that CloudCISC members have found effective to date. However, our goal is to continue to support companies at each phase of the exchange process with more detailed practical guidance. As such, this paper is only the first in a planned series on threat intelligence exchange.

This effort is being led by CSA's CloudCISC working group. We are actively seeking feedback and volunteers to help drive future guidance in this area. If you are interested in contributing, please visit https://cloudsecurityalliance.org/group/cloudcisc/#_join

A Framework for Threat Intelligence Exchange

While automation drives much of the threat intelligence process, the human role in evaluating and understanding the data must not be underestimated. It is the job of the security analyst to determine what is important and how to act. Automation provides them with the data they need; but ultimately the decision-making process belongs to them. This framework specifically focuses on identifying key points in the threat intelligence process where these decisions are made. As such, the focus is not on the method (technology platform, tooling, etc.) organizations are using to consume or generate information, as these may differ, but rather how the information can be used to make decisions and take action to protect the environment and data these custodians are held to defend.



Identify Suspicious Events

The foundation for cyber incident exchange starts with understanding internally-gathered information to better understand the potential likelihood and impact of identified events. Given the sheer number of events being monitored, the ability to prioritize response activities is crucial.

An entry point for prioritization is to start with data surfaced by a SIEM for review by a security team or events that triggered the creation of a ticket in a case management system.

The next step is determining potential likelihood and impact based on the organization's relative understanding of its information technology ecosystem. For example, knowing what IT assets (databases, networking components, identity assets, etc.) process, store, or transfer specific data types that could result in an impact to the business (financial, health, personal information, etc.). This combined knowledge forms the baseline for the security team to define the qualification process and determine prioritization based on potential likelihood and impact.

Once an event is prioritized for review, security teams then prepare the relevant information to share with the community.

Gather Relevant Event Data

In the purest sense, security analysts seek to uncover an adversary's capability, intent, and possible course of action against defined valued assets so they can take the best possible action to counter the attack. While information sharing has often focused on indicators of compromise, which are useful, security teams often have far richer data available to them to drive decision-making. This rich data involves the tactics, techniques and procedures (TTPs) used by the adversary. It has been observed that low level indicators change rapidly. However, the adversary's tactics, techniques and procedures (TTP) change over a longer period of time, in part because they take a higher level of effort and resources to develop.

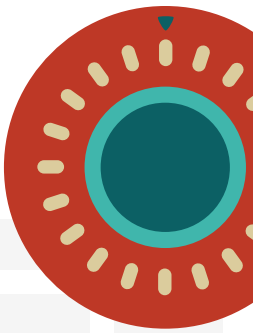
This can be illustrated using the example of spear phishing attacks. The method of spear phishing itself is considered a TTP, but the content of the email is the indicator of potential compromise. In this example, the content of the phishing email (i.e., the indicator) is easy to change and may still be very successful against softer targets, but the TTP remains the same.

It is useful to share information on both adversary TTPs and adversary indicators. However, each drives different activities and requires a different tempo for those responding to incidents.

The indicators change more frequently in order to bypass defense infrastructure. Indicators require rapidly deployed defensive actions to identify, contain, and eliminate them. In the spear phishing example, the indicators can be added to the anti-spam platform to mitigate the threat as soon as they are discovered. In contrast, the TTPs can and should drive broader, longer-term activities and instrumentation of defense infrastructure. In spear phishing, these activities might include employment or configuration of anti-spam platforms to remove these angles of attack before they gain access. Such configurations would typically be implemented by an infrastructure team and be available as effective defenses for years.

In addition to indicators and TTPs, security analysts often have access to other information about an incident. This may include information elements such as where was the activity seen, what activities precede and follow this specific indicator, who is the specific target or group of targets, and was this unique to a specific industry vertical. These elements of information allow classification of behaviors for which defensive actions can be designed and built.

One piece of often discussed, but less relevant information, is attribution. Attribution is difficult and time-consuming and, from a practical perspective, is less useful to the response process than identifying behaviors that characterize capability, intent, and possible course of action. In most cases, attribution will not need to be dealt with in the context of threat intelligence exchange.



In summary, given the richness of incident data has improved beyond indicators of compromise, the goal should be to share as much context as possible with the threat intelligence exchange. By doing so, organizations are not only providing other companies with a rich set of data to drive decision-making, but ideally they are also providing more clues that may help assist them and others in filling any gaps in data which aid their own decision-making and response.

The value of contextualizing data can be shown using the events surrounding the Wannacry attacks. When news broke of the release of exploits used by the U.S. government, teams who followed and began to contextualize the threat were in a position to internally share information and make definitive recommendations to their organizations. As a result, they reduced the attack surface within their organizations and were better prepared when the Equation Group exploits were weaponized as ransomware and against further threats related to the Wannacry exploits.

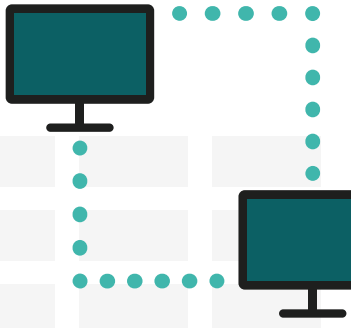
Appendix A provides an example of incident information to be shared via a CIE that includes context and evidence-based decision recommendations.

Decide How to Share Data and with Whom

There are many technology platforms, formats and processes for sharing information both internally and externally. Selecting the method of sharing information may be unique for each organization, but there are some additional topics to consider when implementing information sharing operations. As discussed in previous sections, exchange platforms can lend support and automation to various aspects related to the mechanics of sharing data. Further, having a documented policy around threat intelligence exchange governing aspects of this process will streamline decision-making for the response to individual incidents. Key considerations are outlined below.

Authorizing Access and the Approval Process

Authorized access to information sharing and approval process should be defined in policy rather than having to review the decision for each incident is highly recommended. Further, organizations must keep in mind that threat intelligence exchange is most valuable when data is shared rapidly to get the value of more minds examining the threat and provide the value of early warning to others. Long approval processes are typically counter-productive to achieving both objectives. In our experience, anonymity and data redaction can greatly speed the process of information sharing by ensuring that all organizations' identity and confidential data are not at risk in the sharing process.



Sharing to the Community

Many organizations may participate in multiple sharing programs. Some may even participate in sub-groups, or enclaves, within an individual sharing program. For each incident, security teams will need to decide whether to share event information broadly across all of their representative sharing programs, with only one or two sharing programs, or even only within certain enclaves. In general, the best practice should be to share suspicious event information as broadly as possible. However, in some cases, the sensitivity around an incident may require organizations to limit its distribution. For instance, an organization may determine that an incident can only be shared with a threat intelligence exchange able to take the submission anonymously. Or it may want to limit sharing only with industry members until more information about the event is known.

Anonymous Submissions

Data around suspicious event and incidents will often contain information considered sensitive to the source organization. At the same time, this data may be needed for effective contextualization of the event. The ability to submit incidents to an exchange anonymously can best manage this risk. In some cases, the exchange platform itself will provide anonymity. It is important for the organization to understand exactly what data is revealed to others on the exchange. By ensuring that the incident data being shared cannot be attributed to its source, the risk to the enterprise is greatly reduced, if not altogether eliminated.

Confidential and Sensitive Data

Often there is information related to cyber incidents that is sensitive but not relevant for taking action on the consumption side. This sensitive information could include personally identifiable information for customers or intellectual property. It is ultimately the responsibility of the submitting organization to ensure this information is protected. As such, it should be "scrubbed" from incidents before they are reported to a threat intelligence exchange. This process of redaction can sometimes be automated with the help of client-side support from the exchange platform. However if not, organizations will need a method to manage data redaction. This can be very straightforward where the field information is replaced by a specific character (e.g. x. replacing X with Y). Redaction can be done on an entire field or on partial field contents. For example the leading 'n' or trailing 'm' characters can be left in the clear and the remaining characters can be redacted. One other technique used to avoid inadvertent disclosure is to obscure the length of a field by always replacing the text with a fixed or random number of redacted characters.

Data Formats

Data formats used for information exchange range from binary representation on one end to verbose natural language constructs on the other. The verbose type of representation would be better suited for cyber incident information exchange. It should also be noted that there is a high level of automation being built in SOCs where the cyber event information would be consumed. There are certain data formats that are verbose and at the same time amenable for machine consumption. The most commonly used data formats that fall in this category are XML and JSON.

A wide variety of cyber security use cases rely on such cyber event information including event management/logging, malware characterization, intrusion detection/prevention, incident response, and digital forensics. Having a standardized language for cyber incident sharing supports the effective and seamless consumption of information across a broad range of applications. One such standardized language for information exchange is Structured Threat Information eXpression (STIX)[9]. The STIX framework intends to convey the full range of potential cyber threat data elements and strives to be expressive, flexible, extensible, automatable, and human-readable. STIX is being actively worked on by a technical committee under the OASIS[10] open standards group. The STIX specification defines different types of STIX Domain Objects (SDO).

Example of STIX Domain Object

Indicator Object

```
{
 "type": "indicator",
 "id": "indicator--031778a4-057f-48e6-9db9-c8d72b81ccd5",
 "created": "2017-02-09T12:11:11.415000Z",
 "modified": "2017-02-09T12:11:11.415000Z",
 "name": "HTRAN Hop Point Accessor",
 "pattern": "[ipv4-addr:value = '223.166.0.0/15']",
 "labels": [
 "malicious-activity"
 ],
 "valid_from": "2015-05-15T09:00:00.000000Z",
 "kill_chain_phases": [
  {
   "kill_chain_name": "mandiant-attack-lifecycle-model",
   "phase_name": "establish-foothold"
  }
 ]
}
```

STIX is part of a family of threat intelligence specifications designed to help automate and structure cybersecurity information sharing techniques. The other specifications include the Trusted Automated eXchange of Indicator Information (TAXII), which defines a set of services and message exchanges, and Cyber Observable eXpression (CybOX). CybOX is a standardized schema for the specification, capture, characterization, and communication of events or stateful properties observable in all system and network operations. In the past CybOX was developed as an independent project, but it has now been integrated into the STIX 2.0 project.

9 https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications
10 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

STIX and TAXII are well-supported threat intelligence specifications and their use is recommended for organizations with the resources to implement them. However, the inability to use these specifications should not preclude an organization's participation in threat intelligence sharing. Thus, best practice dictates that exchange platforms should allow intake and integration of data in any format, including email and text.

Monitor For Event Feedback and Correlation

Any organization sharing suspicious event data should ensure that information about the event can be returned to them and correlated with the original event data to support its response and mitigation efforts. Some exchange platforms support this process automatically, but organizations should ensure they are prepared to keep the feedback loop open and are able to operationalize any data collected from the community post event resolution.

Assess Need for Collaborative Response

Mitigating some incidents may be straightforward but mitigating others may require expertise or experience found outside the organization. In addition, there may be some incidents where an organization may have a unique insight that it wants to contribute to the mitigation efforts of its peers. Security analysts will need to determine whether outside collaboration is needed to resolve an incident and how to initiate that effort. Often, the exchange platform will assist with establishing collaborative groups via secured chats, etc. Other times direct outreach to other affected organizations may be required.

Next Steps

A Call to Action

CSA believes any company that uses threat intelligence will tangibly benefit from the external exchange of threat intelligence data. No longer are companies being asked to risk their reputations, assets or customers by participating in one-way directional sharing of cyber security information with little return for them. It is time to embrace a new approach.

Because the cloud industry is already taking advantage of many advanced technologies that support threat intelligence exchange and has such a unique and large footprint across the IT infrastructure, there is a real opportunity to make threat intelligence sharing pervasive. Our commitment to the industry is to continue to provide a value-driven threat intelligence exchange for our members and support them in their efforts to participate by developing and publishing relevant guidance and best practices. While the cloud community is our first priority, we believe our efforts will serve as a model for those across the IT landscape seeking to derive value from threat intelligence exchange.

This paper is only the first in a series of planned efforts to provide that guidance and enable new users of threat intelligence exchange to benefit from the lessons learned from with those who already walked the path. We ask those across the community to provide feedback on our work to date and contribute to our ongoing effort by sharing best practices and lessons learned.

Finally, we call on all corporate CSA members to join Cloud-CISC. Our industry cannot afford to let another year pass working in silos while malicious actors collaborate against us. It is time to level the playing field, and perhaps even gain an advantage.

Appendix A

Example of Shared Incident Information

New Shadow Brokers Leak targeting Windows OS and SWIFT banking system

Today, Shadow Brokers, the cyber group noted for several leaks of National Security Agency (NSA) hacking tools since summer 2016, released a new collection of files. These files contained exploits and hacking tools targeting the Microsoft Windows Operating System (OS), and a series of presentations and files relating to collecting data from the SWIFT banking system of several global banks. The group leveraged its Twitter account to dump the files and password, which were subsequently unzipped and posted on GitHub for mass consumption and security researcher analysis. The new release encompassed three folders named 'Windows,' 'Swift,' and 'OddJob' which contained 23 new hacking tools.

Key Points

- The source-code for several new sophisticated hacking tools are available for use by researchers and threat actors
- The dump is likely dated to 2013, however, it is likely some of the exploits are still valid today
- The overall impact to all Windows versions remains unclear
- Targeted banks leveraging the SWIFT system were likely compromised
- The 'Windows' folders contains several Windows hacking tools and executables which appear to differ from those released in December 2016. The 'OddJob' folder contains an implant, named ODDJOB, with detailed configuration files and payload information. The folder purportedly contains a 2013 text file highlighting ODDJOB's successful avoidance of several anti-virus (AV) software platforms offered by well-known AV providers such as Symantec, Kaspersky and F-Secure. The 'SWIFT' folder contains a presentation and files entitled JEEPFLEA_MARKET which discuss Swift Alliance Access (SAA) systems. Additionally, the folder contains SQL scripts that search for SWIFT-specific data, text, and MS Excel files; suggesting operators gained access to several banks across the globe, mainly in Middle Eastern countries. Of note: many of the exploits seem to be memory based, degrading the efficacy of traditional, non-behavior based, indicators.

Recommended Defensive Action(s)

- **DA1** Prioritize patching/updating over the next 30 days for all Microsoft Windows versions used at Company X
- **DA2** Actively monitor releases from media and security research groups pertaining to threat actor adoption of the capabilities and future targeting

References

Medium, Vice, GitHub

Appendix B
Additional Resources

Government References

Department of Homeland Security's Automated Indicator Sharing (AIS) service
https://www.us-cert.gov/ais

National Institute of Standards and Technology (NIST) Cyber Security Framework
https://www.nist.gov/cyberframework

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

MISP
http://www.misp-project.org/features.html

ENISA
https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-first-study-on-cyber-threat-intelligence-platforms

https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

Information Sharing Specifications for Cybersecurity

Overview
https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

About OASIS Cyber Threat Intelligence
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

STIX 2.0 (Include CYBOX)
https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications

TAXII
https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications