ISAO
Standards Organization

ISAO 700-1: Introduction to Analysis

v1.0

June 18, 2018

ISAO 700-1

Introduction to Analysis

V1.0

ISAO Standards Organization
June 18, 2018

Acknowledgments

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from the private, professional, and government communities in an ongoing effort to produce a unified voluntary set of guidelines for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization
Dr. Gregory B. White
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Allen Shreffler
ISAO SO—Deputy Director
LMI

Tommy McDowell
Senior Director
Retail Cyber Intelligence Sharing Center

Working Group 7—ISAO Analysis

David Sula
Signal Processing Engineer
Leidos

Ole Villadsen
Research Liaison, Cybersecurity
& Information Systems
Carnegie Mellon University Libraries

The ISAO SO leadership would also like to acknowledge those individuals who contributed significantly to the development of these guidelines:

Richard Barger, Director of Security Research Security Markets, Splunk Inc.; Tyler Bent, Member Engagement & Programs Coordinator, IT-ISAC; Joy Gumz, Senior Director, Project Auditors LLC; Pierre Lamy, Threat Intelligence Lead, S&P Global; Larry Portouw, NTK Consulting, LLC; David Sula, Signal Processing Engineer, Leidos; Ole Villadsen, Research Liaison, Cybersecurity & Information Systems, Carnegie Mellon University Libraries.

Special thanks from the authors go to the ISAO SO advisors and staff who greatly helped along the way in the development of this document: Marlis C. Cook, Director of Lifecycle Standards Development, and Allen D. Shreffler, Deputy Director.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award No. 2015-PD-128-000001.

Disclaimer: “The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.”

Table of Contents

Figures

Tables

Revision Updates

Item	Version	Description	Date
1	V.01	Initial version	6/18/2018

1 EXECUTIVE SUMMARY

The purpose of analysis is to produce intelligence that decreases uncertainty in decision making and therefore reduces risk. This document provides an introduction to the information analysis process and how an Information Sharing and Analysis Organization (ISAO) can use it to identify, define, and mitigate cybersecurity threats. It is the authors' intent to provide organizations a general understanding of the tools and processes needed for an analysis team to create cybersecurity information and intelligence within their ISAOs.

This document establishes a conceptual framework for an analytical process, including establishing information and intelligence requirements as well as collecting, processing, analyzing, and exploiting relevant data to generate products that provide ISAO members with cybersecurity situational awareness. The objective of sharing cybersecurity analysis is to provide ISAOs with actionable information, reduce uncertainty, and thereby reduce risk to enable decision makers. As a technical overview, this document is meant to foster discussion on both a managerial and an operational level.

2 INTRODUCTION

Analysis is a continuous process and is crucial to understanding the cybersecurity situation. The basis for analysis is knowing where you are, how you see yourself (business/organization), and how adversaries or criminals see you. Data and information in and of itself brings little value; however, the analysis and understanding that is derived provides the decision maker with the necessary context, that is, the intelligence required to act. Analysis is a perishable skill, a combination of art and science, and it must be viewed as a continuous learning process in order to understand the cybersecurity situation. This document will expand on ISAO 300-1, "Introduction to Information Sharing," and provide the reader with the why and the how to apply analysis in an ISAO.

3 BUSINESS IMPACT

Most modern businesses require some form of digital communications to transact in the global marketplace. One must also consider the organization's enterprise and the criticality of its data flowing to and from its customers. As the information age matures, security is increasingly becoming a priority across business.

According to a 2017 IDG Security Priorities Study,[1] 42 percent of organizations expected to see an increase in their security budget over the next 12 months. Mature organizations proactively addressing threat information analysis as a part of a sustained business impact assessment will position themselves procedurally and culturally to routinely make business decisions through the lens of digital risk.

[1] See https://www.idg.com/tools-for-marketers/2017-security-priorities-survey.

The same 2017 IDG study indicates that 28 percent of organizations report that big data analytics is a new or potential area for security investment.

More often than not, organizations struggle with finding cybersecurity approaches that either justify the associated costs or demonstrably enable the business to achieve increased revenues. During the next decade, opportunity exists for organizations to unlock hidden values within their security operations and data that might drive security operations to cost neutrality or become a business enabler.

Business leaders seeking to improve their organization’s cybersecurity will often collaborate with information assurance (IA) teams to align internal strategic, operational, and tactical information technology (IT) programs with external events or business activities to obtain broader situational awareness and to inform risk management processes. For example, in the case of a merger and acquisition, IA teams might be in a position to detect insider threats that could leak sensitive information. Alternatively, IA teams might surge to hunt for remote attackers who may have persistent access to one network, and that could leverage the fissures within corporate bureaucracy to gain access to an overtaking organization’s enterprise during a network migration.

3.1 POOLED RESOURCES

The dynamic nature and complexity of modern digital risks often require an interdisciplinary mix of technical and geo-socio-political expertise. There is simply too much to know and to do in a short amount of time for any one individual contributor or security team to shoulder the burden of reducing organizational risk.

Fortunately, this resource constraint can often become the catalyzing variable to integrate individual contributors and security teams, thus enabling the work product to become greater than the sum of the parts. Organizations seeking to leverage lean, matrixed, cross-functional teams are positioned to achieve greater organizational wins, driving a common security agenda across stakeholders.

The strategy of pooling workforce resources internally can also be extended outside the organization by joining collaborative bodies such as ISAOs, security product user groups, or private security researcher trust groups. It makes little business sense for different organizations within the same vertical to shoulder common burdens or analyze the same risks in isolation. By emulating the efficiencies of distributed processing, groups of individuals and organizations can break down common analytic challenges into shared workflows. By recognizing common threats, organizations can also better prioritize their resources and collaborative efforts, which can lead to a winning strategy for all, such as the collaborative effort to take down the WireX botnet in 2017.

3.1.1 CREATING HISTORIC CONTEXT

Security staff who investigate a security incident such as a spear phishing attempt and later analyze, document, and share details of this incident can retain this information for historical context; any future corporate security staff member or executive now has continuity of the associated details to compare with future security events. This institutional knowledge is now memorialized for the corporation despite any future personnel changes within the security team. This same team will increase the efficacy of future security investigations, saving a new or old analyst time in future investigations.

3.1.2 EXPONENTIAL RETURN ON INITIAL TIME INVESTMENT

If the organization shares details of this event to an analytics community, either internal to the ISAO and its member organizations or an appropriate external group, and a number of analysts respond, each by spending additional time looking into the initial findings and providing additional context, the organization can obtain a far greater amount of distributed analytics time at no additional cost. The investment of the initial time and effort can become the catalyst for others to invest in a common interest area. Moreover, the ability to receive additional viewpoints from others with access to various data sets can be extremely helpful, as can the ability to encourage peers to challenge long-held assumptions.

3.1.3 INCREASED VISIBILITY AND ANALYTICS

The concept of “herd awareness” speaks to the instincts that can be found throughout the natural world. If we look closely, we can admire the beauty in how a flock of birds or a school of fish moves in perfect unison, executing flawless split-second movements as a single unit to avoid a common predator.

As social creatures who crave success, we should consider how we can find success through collaboration. Specifically, leveraging vetted communities whereby individuals having met, worked with, or shared similar problems can enter into a collaborative arrangement, such as regional meetups, email, chat-based trust groups, or conference-based birds-of-a-feather sessions. Recognizing that our natural environment is becoming inextricably bound to our digital environment requires effective communication and orchestration across digital mediums.

As we consider opportunities to matrix our digital and social (personal and professional) networks and create sharing organizations, we can inject raw data, information, knowledge, and intelligence into our communities to increase situational awareness among the group. Other organizations pivoting into their own data sets can often result in additional indicators being shared back, which makes everyone’s response more effective. While not all injections of data or information are “actionable,” they nonetheless promote awareness of a threat or threat actor, improve the quality of data sets, and enable the ability to identify evidence of past, present, or future events.

In addition, multiple organizations and personnel with access to these shared data can also provide value-added context, which in turn expands the scope of the investigation and leads to actionable intelligence to prevent future attacks.

3.1.4 ENABLING DISTRIBUTED DEFENSE

In analytic sharing circles, there is often a clear recognition of which individuals or organizations are the key participants or enablers. Organizations wishing to join and participate actively in such sharing circles will have the peace of mind that the industry recognizes its security program as the key business enabler it strives to be, leading to industry leadership opportunities and the ability to prescribe market-shaping insights and perspectives. Key examples of the latter often include the sharing of best practices and lessons learned, an underappreciated but extremely valuable resource.

3.1.5 SHARED RISK

In 2004, as targeted attacks against the defense industrial base began to increase in frequency, a sober realization fell upon the defense and aerospace market. A market segment that often found itself in cutthroat competition with one another over razor-thin margins would have to change the way it looked at one another and acknowledge that they all faced a shared risk. These organizations realized that while they would compete in the business space, their information technology and security personnel would have to find a means to collaborate against the shared risk if encroachments were made by sophisticated nation-state actors.

In response, we saw the emergence of sharing and collaboration entities such as the National Cyber Investigative Joint Task Force and the Defense Industrial Based Cybersecurity Information Sharing Program. These entities operationalized against the shared risks posed against the national security, defense, and aerospace communities.

Building off the increasing pressures and momentum, the 2015 Cybersecurity Information Sharing Act (CISA) sought to streamline the legal hurdles that private-sector organizations faced while defending their networks and intellectual property. Because many of the same threat groups targeting the private sector were also targeting various departments and agencies across the branches of government, CISA established vehicles for limited liability in sharing cyber-threat information between public- and private-sector organizations dealing with shared risks.

Today, various collaborative models exist that tackle the notion of shared risks such as ISAOs and Information Sharing And Analysis Centers (ISACs)—formed for critical infrastructure—which give individuals and organizations the ability to work in collaboration to identify and reduce shared risks.

4 ESTABLISHING PRIORITIES

4.1 INTRODUCTION

Prioritized information requirements drive all stages of the intelligence cycle, and all stages occur simultaneously. Prioritization provides focus and ensures better, actionable outcomes.[2]

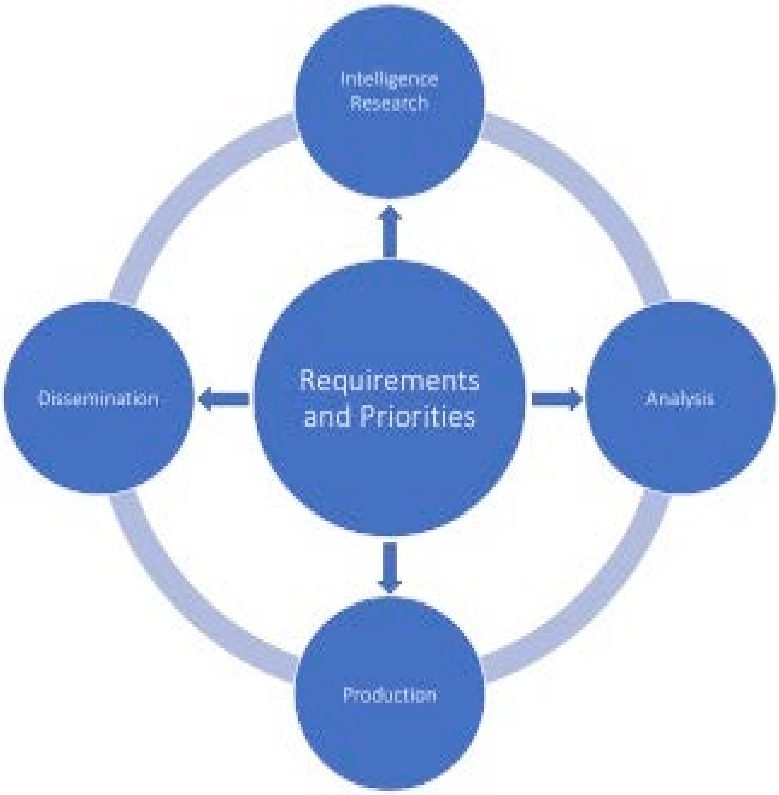
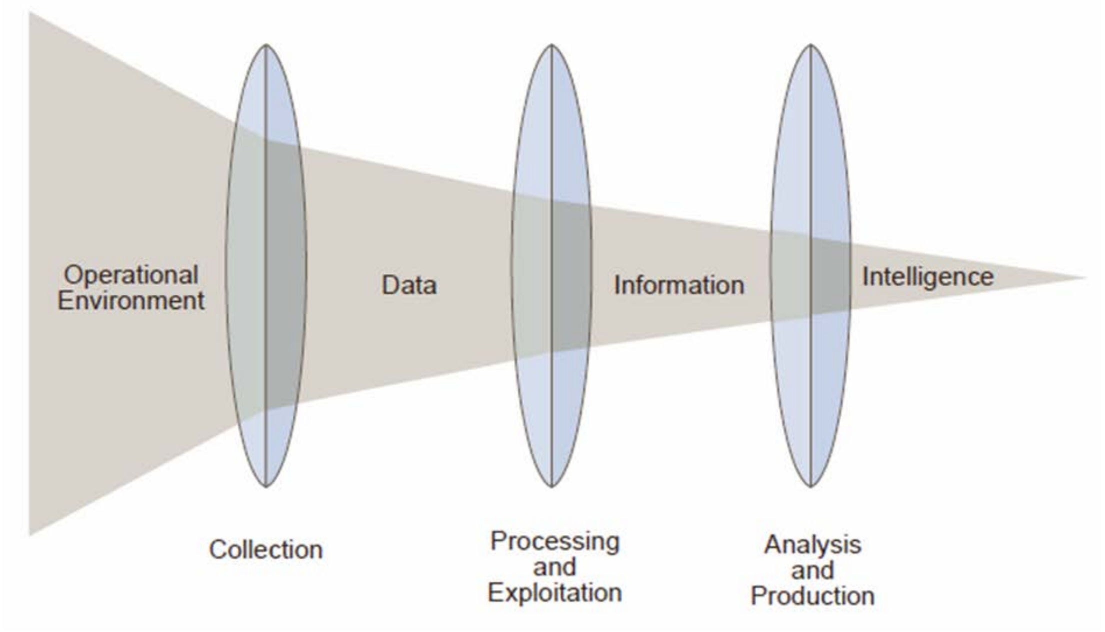


Figure 1. Framework ISAO Intelligence Cycle

Work within each stage of the cycle requires prioritization, with input to prioritization coming from requiring activities and final priorities set by the executing (analytical) activity. Priorities are dynamic and situational and are consumer driven, subject to revision and alteration. The purpose of prioritization is to optimally constrict the volume of inbound data and information leading to relevant, focused intelligence.

[2] ISAO Intelligence Cycle, Larry Portouw, NTK Consulting, LLC.



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Figure 2. Relationship of Data, Information, and Intelligence[3]

4.2 INFORMATION REQUIREMENTS

Data and information requirements are commonly referred to as collection requirements. These requirements can be established anywhere in the intelligence production cycle and they reflect identified knowledge gaps. Requirements are prioritized by ISAO members or by the ISAO analytical team on behalf of its members. The primary driver of the intelligence production cycle is collection requirements. They should not be confused with the requirements definition commonly associated with the achievement of business objectives. Intelligence requirements are focused, time-bounded questions meant to drive intelligence production that reduces ambiguity in decision making in business processes such as acquisition, architecture development, and intellectual property protection.

Information requirements are phrased as questions that are relevant, specific, and achievable. Reporting requirements are the same but are additionally time constrained to establish when the answer is no longer relevant. Note that the example requirements could come from operational activities or internally from the analytical activity (Table 1).

[3] See http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/2-0-Intelligence-Series.

Table 1. Generating Effective Information and Reporting Requirements

Poor Information Requirement	Good Information Requirement	Reporting Requirement
Has XYZ experienced a loss of personable identifiable information (PII)? (Too broad)	Has XYZ lost accountability of PII due to negligence, willful misconduct, or theft? If theft, what attack methods were used and what architectural weaknesses facilitated the penetrations?	Report PII loss immediately upon recognition.
Which critical CVMs have been announced in the past 24 hours? (Too general)	Which issued critical CVMs have not been assessed for their impact on XYZ Company and mitigated within 24 hours of release?	Report CVMs with potential impact to XYZ within 2 hours of publication. Report the CVM mitigation status of XYZ vulnerabilities every 8 hours until complete.
ABC industries' entire client data register was exfiltrated from its network last week. Is XYZ next? (While very specific, this question flunks the feasibility test—it is unlikely it could ever be answered—and is not time bounded.)	Is there a correlation between successful attack or data theft in an industry segment and subsequent attacks in the same segment? (Is threat success an indicator of future attacks in an industry segment?)	Report theft and data type to the ISAO within 24 hours of recognition. Report perpetrator tactics, techniques, and procedures (TTPs).
Is XYZ vulnerable to an insider threat?	Have XYZ network/system administrators increased personal privileges? Are terminated employees' email accounts deactivated immediately?	IT supervisors review and report all user and admin escalated privileges.
Has XYZ lost or had a company laptop stolen?	Has XYZ lost or had company data stolen without encrypted data at rest?	Immediately report all lost or stolen equipment, including data at rest.
Has recently installed software/ hardware conflicted with security protocols?	Are network system configuration changes causing conflicts or rendered security applications non-operational?	Report and resolve all information system conflicts.
When, where, and how have hackers gained access to XYZ data or networks?	When and with what TTPs have unauthorized users gained access to XYZ information systems?	Report unauthorized access to XYZ networks or facilities.

4.3 ANALYSIS REQUIREMENTS

Analytical priorities are established by the organization performing the analysis and are balanced between requiring activities priorities, information requirements, available resources, and ability to answer the requirement. Requirements and priority determinations should be shared regularly with all members of the organization. An analog to setting analytical priorities is medical triage.

Requirements that cannot be feasibly answered or that cannot be answered in the time available will likely receive low priority. Requirements that have high priority from multiple requirement activities, have high impact on operations, and align with available resources and time available will have high priorities. Analytical priorities are not static and are routinely adjusted as new requirements are received and the operational situation changes.

Requirements logs and priorities should be shared regularly with all member activities.

4.4 PRODUCTION REQUIREMENTS

Production priorities are determined by the analytical organization and are driven by analysis priorities, available resources, and operational requirements from requiring activities.

The production of products for dissemination ranges from automated reports (essentially a production pass-through) to formal publications. Production formats should be standardized to minimize production time with a focus on meeting timeliness and accuracy over appearance.

4.5 REPORTING REQUIREMENTS

Cybersecurity information sharing is voluntary and each entity must consider what is to be shared. For more information, see Section 8: Reporting.

Dissemination and reporting are broken into two categories: (1) general or scheduled reporting and (2) ad hoc reporting. In all cases, reporting priorities are driven by information requirements and production priorities.

Priorities for scheduled reports and products are set by the analytical organization and follow a release schedule. These can be periodic, routine reporting and the content is driven by member organizations' needs.

Ad hoc reporting can be triggered when specific conditions are met or can be a one-time publication based upon production requirements and time sensitivity. For example, the first use of an identified vulnerability by a threat actor would trigger a report and in turn might alter priorities for collection and production.

5 DATA/INFORMATION SELECTION

The intelligence cycle referenced in Section 4 introduces the process by which data is converted from a raw format into a finished product that can be used by decision makers and network administrators to best protect their networks. The data required to perform the analysis will change as requirements change, but the basic process of selecting data sources will be similar.

Though not covered in this document, it is important to recognize that the U.S. government has various programs for sharing information with industry groups and government agencies. Some of these programs are detailed in ISAO 600-2, "U.S. Government Relations." These government programs can provide access to large amounts of data from industry and government as well as analytical products that provide context around trends, tactics, techniques, and procedures. However, the process of releasing these data can be lengthy, so the data could be old and of less value by the time released.

5.1 TYPES OF DATA SETS OR INFORMATION (PUSH/PULL)

Generally speaking, arguably the biggest challenge in conducting analysis is identifying and obtaining the right data sets and/or information to analyze which will answer the member requirements. The amount of data/information available for analysis is almost limitless and therefore requires understanding of and prioritizing requirements. This section focuses on potential data/information from external sources although data/information from internal sources (e.g., from a security information and event management [SIEM] system) would also be invaluable for analysis. When selecting what data sets or information to either pull or request from external sources, it is important to consider how it will support the needs of the ISAO and its members. While determining this, it is important to consider that each member company may find different data sets or information to be of value based on factors such as size, sector, and capabilities.

As such, effective analysis is not possible if the ISAO does not understand the needs of its members. Employing an “intelligence requirements” process will help organizations understand and meet their member needs. By understanding member needs, an organization will know not only what type of data is important to members, but also how it can present that data/information in a meaningful way.

For example, a small company without a dedicated IT staff likely will not find a large collection of unanalyzed “raw data” very useful. But a company with a robust dedicated IT team might find such data valuable if it is available at a price it can afford. By partnering with an ISAO, both organizations can benefit through the acquisition of a broader set of data and potentially become able to shift analytic requirements to a centralized body.

5.2 SELECTION SOURCES (PUBLIC/PRIVATE)

ISAOs must consider multiple factors when it comes to selecting which data sources should be used to support analytic efforts. The primary consideration, though, is identifying which sources will provide information relevant to answering requirements established by member organizations.

There are two basic types of “public” sources: (1) those available on public venues such as news sites, blogs, and publicly available raw data feeds that are accessible to all; and (2) data and information from government departments and agencies. More detailed information on what specific types of information can be obtained from these types of sources can be found in ISAO 300-1, “Introduction to Information Sharing.”

The U.S. government has various programs for sharing information with industry and government. These programs are detailed in ISAO 600-2, "U.S. Government Relations, Programs, and Services."[4] The government programs can provide access to large amounts of data from industry and government as well as analytical products that provide context around TTPs. However, the process of releasing these data can be lengthy, so the data could be old and of less value by the time released.

Open-source reporting can be an excellent source of data and information. There are many resources within this category that organizations can access for free. This type of reporting can come from a variety of channels, including blogs, news articles, and presentations made available on public sites. There are also many publicly available data feeds that provide indicators of compromise, such as suspect file hashes, Internet Protocol (IP) addresses, and domain names. The challenge with open-source data/information is the accuracy and veracity of the information as well as its applicability for addressing requirements specific to the ISAO. In all cases, the source of information must be evaluated for accuracy and bias.

Private sources generally refer to information not made available to the general public and provided by a non-government entity. Private sources, including raw data feeds, are often provided by companies with highly advanced capabilities and expert analysts with customized reports that are more likely to relate directly to an ISAO's requirements. There is often a cost associated with such sources, which may be prohibitive to smaller or less-defined organizations. These costs can sometimes be reduced or eliminated through the establishment of a partnership or other reciprocal support arrangement.

In sum, both public and private sources can add value to an organization's analysis. But they can only do so if the services they provide meet the needs of the ISAO and member organizations.

5.3 FREQUENCY OF TRANSMISSION

Generally, it is assumed that the more data shared, the better. While this may be true in many cases, it is not always applicable. The amount of information available grows every day, so it is easy to overwhelm analysts to the point of information overload. Providing so much information that a customer or organization cannot make use of it will have the same effect as not providing anything. Most organizations evaluate data/information based on its usefulness, not on the amount of it. Source selection is key to sending members as much valuable data as possible.

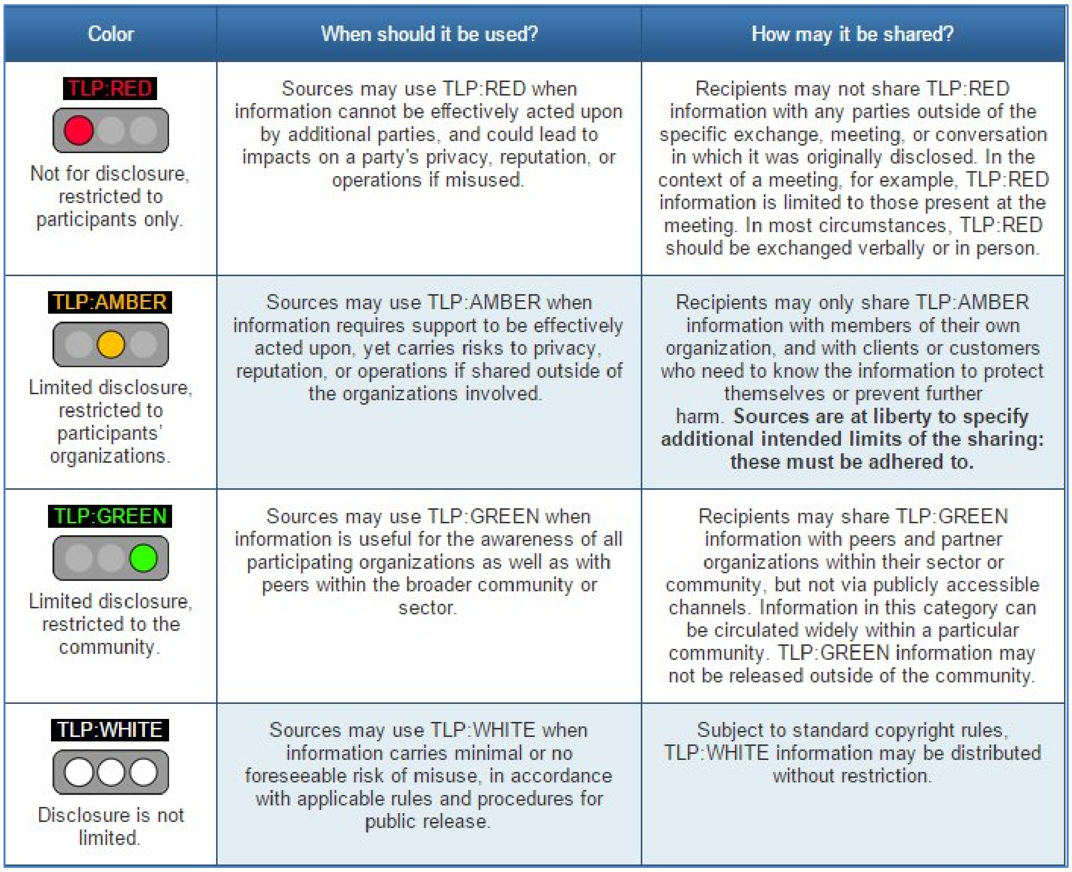
[4] See https://www.isao.org/products/isao-600-2-us-government-relations-programs-and-services.

5.4 DISSEMINATION AND DISCLOSURE

Some data/information cannot be shared broadly or publicly because it contains sensitive or proprietary information, which as a result can degrade the effectiveness of the ISAO. In order to minimize the impact and ensure the widest distribution possible, the members need to identify a method for categorizing information that is being shared to identify who can have access and how it should be protected.

Though there is no perfect system for managing this sharing process, one option which ISAOs may wish to make use of is the Traffic Light Protocol[5] (TLP) which is used by the U.S. Computer Emergency Readiness Team to share intelligence reports to the greatest audience possible. As depicted in Table 2, the TLP uses a color code to identify the appropriate audience and associated conditions for sharing.

Table 2. Traffic Light Protocol Definitions[6]



Color	When should it be used?	How may it be shared?
TLP:RED ● ○ ○ Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER ○ ● ○ Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN ○ ○ ● Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ○ ○ ○ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[5] See https://www.us-cert.gov/tlp.

[6] See https://www.us-cert.gov/tlp.

Widely accepted as an industry standard, the use of the TLP provides a familiar foundation that a majority of ISAO members are likely to be familiar with and understand.

6 ESTABLISHING THE BASELINE

When attempting to address the intelligence research and analysis stages of the intelligence cycle, a key component is having a solid starting point from which data comparisons can be made to determine if activity is normal or out of the ordinary. This starting point is often referred to as a baseline. For most organizations, performing a baseline network survey supports multiple requirements. In general, it is done to establish a benchmark set of metrics defining what normal operations are from a network perspective, to provide administrators with a point of comparison to identify anomalous activity, and to define network performance limitations. As a result of the predictable changes in network utilization based on the time and day of the week, measurements must be captured at multiple points in time to have accurate points of reference.

The type of baseline data necessary to be passed on to the ISAO will depend on the level of analysis the members expect to receive. The ISAO could potentially be acting as the primary analysis element for member networks, which would likely require a complete copy of the data. In contrast, the baselines could simply be used by the members to establish a threshold for when an anomaly needs to be passed along to the ISAO.

6.1 STANDARDIZATION

In order for the ISAO to effectively parse and analyze data provided by member organizations, a standard for data sets should be established for use across the ISAO. Member organizations must agree on multiple points to ensure that a standardized data set has been collected across the ISAO.

The primary areas of concern includes defining what elements of the network need to be monitored, the frequency of collection, and what specific data points are necessary to provide an accurate assessment. Beyond these areas, the ISAO members must all agree on what level of exposure they are willing to accept in terms of the type of data being collected, as well as what anonymizing techniques might be used.

6.2 CONSIDERATIONS

Network baselines can be completed through the use of myriad tools, some of which, like Simple Network Management Protocol, can be used across multiple platforms, while others are tailored to work on specific operating systems and network types. Deciding what tools are necessary to perform the baseline will depend on multiple factors such as the systems involved, the cost of the tool, the time available to review the data, and the level of detail needed to make the data usable.

In terms of detail, ISAOs have two overarching levels of data granularity to choose from as a starting point for operations. The first option is to focus on top-level data, which will indicate changes in network utilization or performance as a leading indicator that a more detailed analysis and data collection must be performed. With this option, there is less upfront work required, but a risk that critical data may be missed. The second option would be to capture a highly detailed set of data each time, which would reduce the chances of data being missed but also increase the time needed to both collect and review the data.

Most ISAOs will likely benefit from a combined approach, collecting more detailed information on key network segments and minimal data on less vulnerable or critical portions. An important consideration will involve costs associated with collecting, storing, and analyzing the collected information, a cost that will grow as the scope of the baseline grows.

7 ANALYSIS

7.1 ANALYZING MEMBER CONTRIBUTIONS

One of the major functions that an ISAO can handle is to ingest community member contributions, de-attribute and sanitize the report, enrich and correlate the data, and report back to the wider community. These reports have the benefit of having been source vetted, are relevant to the wider sector-specific community, and improve the security posture of all members. The process to perform these actions can be broken down into two phases, enrichment and correlation.

7.1.1 DE-ATTRIBUTION

ISAO member reports should be immediately put into a contribution tracking system, with identifying markers stripped off. Identifiers would include unmasked system names, non-RFC1918 IP addresses, domain names, and so on. By working from the beginning on a sanitized data set, the analyst will have a reduced chance of sharing private (and irrelevant) details from the final report. Before the final report is saved and shared, a second analyst should peer review the report to complete an additional check for having stripped off identifiers.

7.1.2 ENRICHMENT AND CORRELATION

Generally speaking, member submissions should include either indicators of compromise (IOCs) or TTPs that were identified in the course of a member’s investigation. The attached IOCs or TTPs should have descriptive information that details the event at a high level and outcome within the member’s environment; the case history as far as what resources have been leveraged to date, to try to enrich and analyze the IOCs and TTPs; any scoping of the threat actors' sophistication; and finally, if possible, tying IOCs or TTPs to the Lockheed Martin Cyber Kill Chain™ model.[7]

A proper analysis of the IOCs and TTPs depends on tying these to prior events in the correlation phase. In order to support expanding and documenting the relationship between indicators from this event and related events, the enrichment phase will provide multiple points of reference that may have been obscured or not been obvious.

Once a member submission has been de-attributed and sanitized, and the IOCs and TTPs extracted and enriched, an ISAO's analysis will require a set of correlation processes. While these processes will be largely tool-dependent, at a high level the analysis should be looking for prior cases involving the same data points. For example, a phishing campaign that leveraged a specific domain may be hosted on an IP address that has likewise been observed to have sent phishing emails to other organizations. By tying these facts together, it can be surmised that the phishing campaign may not be explicitly targeting the member. However, a never-before-seen TTP or IOC may indicate a higher level of attacker sophistication. Documenting these facts will facilitate these judgments.

Analysis teams should develop repeatable workflows for correlation, which may include leveraging the following types of sources:

- Search engines
- ISAO databases, such as prior submissions
- Open-source security resources
- Vendor portals and databases (typically paid)
- Private trust groups
- Person-to-person relationships
- Passive Domain Name System (DNS) (typically paid)
- Domain history databases (typically paid).

ISAOs—especially for sectors that are less advanced in investments for threat intelligence—may find it necessary to use member dues and fees to invest in paid sources of data for correlation. These sources are invaluable for very niche data, such as Passive DNS, Deep and Dark Web data, and domain history. By leveraging a central resource such as an ISAO, even small organizations with a small investment in threat intelligence can benefit.

[7] See https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html.

7.2 DOCUMENTING ANALYSIS PROCESS

During the course of the analysis, both the original submission and enrichments and correlations will be uncovered. It is critical to document the processes that are implemented, as well as storing relevant source information, data points, and raw data. Negative results should likewise be documented under the process as they could indicate that a defensive approach has been successful or that a suspected threat was in actuality a false positive.

These business process logs can be extremely useful during the later phase of documenting findings. While an ISAO may not need to document findings at the same level as in a forensic analysis, the same style of documentation of findings should be followed, as well as documenting the steps that led to the findings.

In the event that third-party sites host the findings, local copies should be made in addition to references to that data. These should all be stored within the case file-tracking system according to ISAO security policies.

Once all analysis processes (de-attribution and sanitzation, enrichment, correlation, and documentation) have been completed, the analyst will be able to begin the potentially most challenging phase—weaving a narrative.

7.3 WEAVING A NARRATIVE

The challenging nature of weaving a narrative to communicate the findings relates to the following:

- The analysis should be timely, relevant, and actionable.
- It should not contain identifying markers relating to the submitter.
- The analysis should be complete—and compelling. A poorly written analysis will not be ingested by other sector members.

Any incident in isolation lacks context with regard to its severity, impact, and scope; providing these individual assessments from members enables the ISAO to generate a big-picture view of events. Weaving together the IOCs, TTPs, scope, impact, and severity and communicating these details effectively allows the member organization to map all of these factors into its own operations.

Of particular interest to most sector members will be the lessons learned, best practices, and recommended steps. For example, a report may contain a list of IP addresses that were used as command and control points for malware; and the recommended actions are to

- search the SIEM and logs for any historical matches,
- block the IP addresses on perimeter gateways, and
- set up alerts for any future matches to this traffic.

In a case where specific vulnerabilities or TTPs were leveraged to conduct the activity, these can likewise be detailed with links to the vendor patches or resources to assist organizations in defending their networks. In a case where an open Remote Desktop Protocol (RDP) host was used as the primary entry point, recommended actions might be to

- scan your organization for an open RDP system,
- implement a hardening guide for RDP hosts if these systems serve a legitimate purpose, and
- ensure that multiple factor authentication is used on RDP hosts.

Any recommendations or observations should be qualified and reference specific third-party resources (links to blog articles, vendor reports, etc.). In recent years, efforts within the threat intelligence community to be precise in estimates and probabilities have gained traction. The Malware Information Sharing Platform (MISP)[8] project documents these taxonomies as follows:

- ***Source Reliability***
  - A. Completely reliable
  - B. Usually reliable
  - C. Fairly reliable
  - D. Not usually reliable
  - E. Unreliable
  - F. Reliability cannot be judged.
- ***Information Credibility***
  - 1. Confirmed by other sources
  - 2. Probably true
  - 3. Possibly true
  - 4. Doubtful
  - 5. Improbable
  - 6. Truth cannot be judged.

By following common taxonomies, analysts can back up their assessments using widely understood terminology.

Finally, it is important to note that while not all products need to be compelling, special efforts should be made to ensure that reports about critical events are compelling. There have been exceeding critical security failures at organizations

[8] See https://github.com/MISP/misp-taxonomies/tree/master/admiralty-scale.

that failed to heed industry warnings about vulnerabilities and high-profile events. A well-written report about high-profile events is arguably more important than a poorly written report that was quickly released.

7.4 STORING COMPLETED WORKS

All products of the initial report, de-attributed and sanitized submission, enrichment, correlation, and other documents must be stored according to ISAO security policies. Furthermore, the finished report and IOCs should be stored in a threat intelligence platform, so that future investigations can leverage these data for their enrichment and correlation phases. Generally speaking, the finished data should be searchable by the ISAO membership.

7.5 ANALYZING OPEN-SOURCE REPORTING

Open-source reports, news, and intelligence are an extremely valuable resource for ISAOs and their membership. While often described as “drinking from the firehose,” several techniques can be used to convert this into a steady stream of actionable intelligence. A consideration with these sources is the validity of the data being presented; sources which provide inaccurate or incomplete data can potentially result in infective guidance being produced.

7.6 PRIORITIZATION—IS IT RELEVANT, TIMELY, AND ACTIONABLE?

Each sector may have different sources of information, but they will all depend on the ISAO analysis team to determine their relevance, timeliness, and assessment about actionability. The relevance of an item can be loosely defined as having the potential to affect member organizations; the timeliness of an item is that it should be observed recently (although some older items may come to light long after they were first observed). The assessment about whether an item can be actioned depends largely on the details that are contained in the report. However, the most important consideration is whether a member organization can detect, block, or otherwise make changes to its environment—or advise other business units about actions that they can take to mitigate against the threat.

7.7 REMARKS ABOUT OPEN-SOURCE REPORTING

It would be fair to assess that half of a threat intelligence analyst’s time is spent researching and reporting about topics that were identified through open sources. This is invaluable work, as it permits an ISAO member organization to stay abreast of developments, vulnerabilities, and findings that may not be available through closed channels. Reporting on these topics in a timely fashion can assist members in updating their decision makers about emerging and high-profile topics.

Often a lesser amount of enrichment and analysis will be performed on these rapidly emerging topics; however, an ISAO analyst can assist the community by providing one- or two-line commentaries about the relevance of the topic. ISAOs should encourage the free discussion on mailing lists about the potential ramifications of new vulnerabilities, observations, and TTPs.

7.8 TOOLS AND RESOURCES

As an ISAO grows its membership and develops business processes to support the community, the ISAO should consider investing resources into tooling and commercial sources for threat intelligence, enrichment and correlation vendors, and data analysis and storage systems. While investing in a variety of tools and vendors, ISAOs should likewise be investing in expanding their teams with a variety of skills and backgrounds.

7.9 ENRICHMENT AND CORRELATION

The following are some of the most common tools to support enrichment and correlation activities:

- Paterva Maltego
- Threat intelligence platforms[9] (examples follow)
  - Anomali Threatstream
  - Collaborative Research Into Threats
  - MISP
  - ThreatConnect
  - IBM X-Force Exchange
- Palantir
- IBM i2 Analyst's Notebook.

The most important features when selecting tools and platforms will vary by organization, budget, and expertise. None of the above tools are endorsed or necessarily recommended; however, they provide a useful starting point to evaluate the market availability of solutions.

As one of the first tools to be used by an ISAO, an enrichment and correlation platform should be extensible to support partner and vendor application programming interfaces (APIs) and feeds. The depth and flexibility of the solution to support these integrations will help the ISAO succeed in long-term sustainability, which is a very important concern. The ability to query historical data over year-long periods is very important, in addition to being able to correlate data points across disparate vendors.

[9] See https://wi2017.ch/images/wi2017-0188.pdf.

7.10 DATA STORAGE

Threat intelligence platforms perform additional functions beyond enrichment and correlation—they provide a platform to share intelligence reports with ISAO members. While the capabilities of various platforms will differ, they will all allow an ISAO analyst team to publish reports and allow for members to consume them manually or programmatically using APIs. Leveraging the platform also allows members to tie in their own enrichment and correlation tooling to this valuable resource. While an ISAO may initially leverage email as a finished intelligence distribution method, this does not allow for new ISAO members to gain access to historical reporting.

While addressed in more detail in Section 10: Security of this document, data storage for case files, investigations, and submissions should be kept separate from the threat intelligence platform (which should be used for finished reports). This separate storage will host highly sensitive data and therefore should be protected by an appropriate set of security policies and tools. Of equal importance is the need to protect certificates, passwords, API keys, and product keys.

7.11 SKILL SETS AND EXPERTISE

Threat intelligence analysts require a broad set of skills to fill their roles; many of which will be specific to the ISAOs unique challenges and focus. As a baseline, an analyst should possess some or all of the following skills:

- An investigation mindset
  - Curiosity
  - The ability to ask questions and pursue lines of inquiry in depth
  - Note taking
  - Noting discrepencies
  - Ingesting facts and synthesizing a narrative or hypothesis
  - Understanding the criminal mindset
- Writing skills
  - The ability to write clearly and concisely for the target audience
  - Differentiating between opinion and fact
  - Supporting facts with evidence
  - Supporting opinion with reference material and historical cases

- Technical competencies
    - Python scripting
        - Other languages such as Ruby, Go, Java, Perl, C, and Assembly are helpful, but Python remains the lingua franca among threat researchers and red teams
    - JSON and APIs
    - DNS, email and web protocols, Secure Sockets Layer, Transmission Control Protocol, User Datagram Protocol, and IP networking.

Given these core skills, some of the most successful threat intelligence analysts will have backgrounds in law enforcement, military, national intelligence, reporting and professional writing, system and network analysis focusing on security issues, and security operations/engineering/architecture. Teams with multiple members should seek to ensure diversity in skill sets and backgrounds, for example, pairing up technical analysts with former law enforcement officers. More so than in most other types of teams, threat intelligence analysts are forced to become instant experts in various subject matter areas during critical incidents, and the fusion of various backgrounds and skill sets enhances the speed, efficiency, and quality of the investigation and recommendations.

Gender, age, ethnic, and cultural diversity are likewise valuable resources for mature threat intelligence teams, for the same reasons as professional diversity. Hiring new threat intelligence analysts is a process where candidates should be considered not only on their technical and professional merits, but also for their ability to bridge any gaps in these areas.

8 REPORTING

Threat intelligence reports are an effective way to communicate the above analysis to decision makers at all levels, including senior executives, mid-level managers, and operational staff. Such reports are typically produced by government agencies, private cyber-threat intelligence firms, or other medium-to-large organizations with sufficient resources to devote to this task. Several ISACs also produce threat intelligence reports, and ISAOs may also wish to deliver threat intelligence reports to their members.

Threat intelligence reports are typically unstructured prose or text as opposed to automated machine-readable information feeds that conform to data exchange standards. Intelligence reports go beyond threat data alone and convey “information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making.”[10] Threat reports

[10] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing.* National Institute of Standards and Technology Special Publication, 800, 150.

may also make use of data visualization techniques to communicate the results of analyzing large data sets.

8.1 REPORT TYPES

Cyber-threat intelligence units prepare several common types of intelligence reports, and ISAOs may wish to consider generating and sharing such reports as part of their services. Before choosing what kind of reports to prepare, ISAOs—or any other threat intelligence component—should consider meeting with or surveying decision makers to determine what information would be most helpful to aid in their decision making.

8.1.1 TREND ANALYSIS AND EMERGING THREATS

These reports aggregate and analyze indicators (e.g., virus signatures, hashes, IP addresses, domain names) across multiple organizations or locations to identify trends over time that point to existing or emerging threats to an organization’s information security. The reports may also include other relavent information that adds context such as information gleaned from the Dark Web that indicates intent or planning. ISAOs may be well positioned to aggregate and examine indicators from member organizations to identify and alert to such trends, as well as provide methods to mitigate or defeat these threats. Such reports emphasize the importance of analyzing aggregated information over rapidly disseminating imminent threats or rapidly evolving events. They are more suited for executives and managers and focus on strategic implications over technical issues.

8.1.2 TARGET OR CAMPAIGN ANALYSIS

Such reports include information on a specific threat actor or campaign, for example, ransomware or phishing campaigns, together with the actors’ TTPs, targets, motivations, and goals. ISAOs may wish to consider generating or disseminating reports on threat actors or campaigns most likely to target member organizations. Such intelligence will help to equip recipients with a better understanding of their threat environment and the threat actors’ capabilities and objectives. These reports are more tactical than trend analysis or emerging threats reports and will contain more technical details.

These reports—particularly trend analyses and target/campaign analyses—may also leverage analytic techniques, such as “data storytelling” and “analytic stories,” to enhance their effectiveness, especially when relying on potentially large volumes of complex data. While opinions vary on the specifics, these methods typically involve addressing a new development that is being analyzed (e.g., a series of phishing attacks against a particular industry); a key question that is being answered or “what’s the so what?” of the new development (e.g., why the campaign is important to an industry); the exploration of data over time through a narrative that adds context and explains events in ways that are easy to follow; and leveraging a series of data visualizations that help to convey this narrative.

In addition, a key component of a threat intelligence analytic story is not only the narrative regarding the cyber threat, but also information and analysis that can help operations personnel and decision makers, such as how the threat can be detected, mitigated, or defeated. Finally, an analytic threat intelligence report should be transparent about the level of confidence in any analytic assessments as well as any specific analytic method that is being used.

8.1.3 IMMINENT THREAT WARNINGS OR SECURITY ALERTS

In response to imminent threats to information security—such as a critical, recently disclosed vulnerability or quickly developing attack campaign—ISAOs may wish to generate or circulate imminent threat warnings or security alerts to members with what is currently known about the threat and what actions are required to protect against it. Imminent threat warning reports may develop over time as more information becomes available about the evolving danger. These reports are completely tactical and focus on security systems, configurations, and specific technical indicators. For additional information on automated threat information sharing, please see ISAO-SO 300-2 (currently in draft).

8.2 REPORTING FREQUENCY

The timing and frequency of report delivery will have a significant effect on the ability to inform decision making. Some report types, such as security alerts or imminent threat warnings, should be delivered on an immediate ad hoc basis to provide recipients sufficient time to act against an impending threat. Other report types with a strategic focus may be delivered on a scheduled or periodic basis.

Threat intelligence components, including ISAOs, should consider working closely with recipients to determine when reports will have the greatest impact on decision making related to information security matters. For example, a strategic report on the cyber threats facing an industry or organization may have the most impact if delivered just ahead of a high-level meeting that will discuss the organization’s information security budget, technology, preparedness, and so forth.

8.3 LESSONS LEARNED

In the aftermath of a security incident, threat intelligence units should consider participating in lessons-learned reviews to determine what knowledge can be gained from the incident to inform future decision making. Such after-action exercises would likely involve a variety of information security personnel from different parts of the organization. ISAOs may wish to participate in these reviews to identify where to make improvements to technology, expertise, or tradecraft related to information sharing and analysis.

9 FEEDBACK AND PRODUCT EVALUATION

After the ISAO has distributed an analytic report to the organization members, a response mechanism is needed in order for the analytic staff to receive feedback from those members on the quality of the information and what changes are needed to improve the reporting process. Initially, there will likely be a need for frequent feedback for the analysts to refine their products to better answer the member requirements, but this will likely decrease over time as the ISAO matures and standardization is reached. Each report type produced will likely require slightly different information to be addressed in the evaluations, but a majority of the feedback should include the same basic elements.

9.1 TIMELINESS

In all evaluations there are three main areas that should be addressed to improve the quality and usability of the reports; the first is timeliness. In most reports, the information that they contain is time-sensitive and the value diminishes the longer it takes to reach the members. Addressing this factor will likely take multiple iterations of changes to work out the trade-off between the time required to prepare a quality report and the window of opportunity to act on it. This assessment may result in the identification of a need for the creation of additional report types to bridge any timeline gaps that can’t be adequately addressed.

9.2 TARGET AUDIENCE

The next factor involves writing the report at a level consistent with the target audience. Depending on the report being prepared, different terminology and depth of explanation is required to ensure that the recipients are able to make use of the information. Reporting that is prepared with excessive jargon may prove unintelligible to decision makers while at the same time a report devoid of a technical explanation may not convey the information necessary for administrators to protect their networks. These challenges can be surmounted, but they will require clear communication between members and the ISAO to understand who will be viewing each report. Additionally, it may be determined that some report formats must be modified to accommodate a wider audience.

9.3 FREQUENCY

Finally, the evaluations should address the frequency at which the reports are being published. While it may be prudent to send out notices of security patches individually as they are discovered, daily reports indicating the absence of threat activity may be detrimental if the administrators become accustomed to the reports having little to no value and as a result become complacent in reviewing them. As with timeliness, this could create a situation where reporting thresholds must be established to determine how often a report is required to be produced and if that timeline should change based on the contents of the report.

9.4 DISTRIBUTION

In addition to determining the proper format for providing feedback, the ISAOs must determine how those evaluations will be distributed. In most instances, the primary audience for the evaluations will be the analytic staff, as they will be responsible for incorporating any changes into their procedures. However, there is also an argument for including all members on the distribution as it may highlight concerns having an impact across the ISAO or encouraging changes that could negatively affect other members. The latter possibility also raises a concern over how the evaluations will be adjudicated and what element of the ISAO will have final say on the correct process.

10 SECURITY

ISAO member organizations' willingness to both consume and share intelligence with the ISAO is predicated on ensuring the confidentiality of communications. To that end, ISAOs must provide for basic communications security mechanisms. In general, one of two methods will be used to share intelligence—email and web portals. Both of these methods are extensively leveraged to collect and disseminate intelligence reports and data. The measures below should be considered as a security floor, and additional security can and should be revisited over time.

As an example of workflows and methods that can demonstrate the need for strong security measures, consider the following:

1. A member organization shares TLP Red details about a data breach, in order for the ISAO to share TLP Amber details about the incident.
2. The ISAO analyst receives a report containing the member organization's details, impact analysis to the member organization, and technical indicators.
3. The ISAO analyst produces a report for the membership containing the relevant indicators and a high-level impact assessment without referencing the specific member organization.

10.1 ENCRYPTION

Websites and email servers should leverage encryption, with web servers only offering Hyper Text Transfer Protocol Secure. Email servers should always use certificate-level security, such as Internet Message Access Protocol over Secure Sockets Layer. The recommended certificate strength will change over the years, and organizations should always renew their certificates with the strongest option at the time of renewal.

In addition to basic encryption methods for securing communications paths, emails containing highly confidential data and shared files that likewise contain this sort of secured data, encryption technology such as Pretty Good Privacy, should always be leveraged. Both email encryption and file encryption will add a layer of trust and confidentiality, ensuring that only the recipients will be able to view the intelligence products.

These encryption technologies and methods should be communicated to new ISAO members during their onboarding process and at regular intervals (e.g., monthly). Members should be strongly encouraged to use encryption to share information with the ISAO.

In the example above, in step #1, the member organization will have a requirement to share a detailed and sensitive report with the ISAO. By leveraging either mail or web encryption as well as encrypting the contents of any files, the member organization can trust that only the ISAO analyst will be able to receive and read the contents of the report.

10.2 DATA-AT-REST

As the ISAO curates new intelligence and receives reports from trusted partners, vendors, and members, it will build up a repository of highly sensitive information. Even as ISAOs serve to address the security needs of the membership, they become a potentially severe source of risk to the sector. The collection of data-at-rest within the ISAO therefore correspondingly requires a very high degree of attention to its confidentiality, availability, and integrity.

At a high level, the following basic security measures should be taken to secure these data:

- A routine of regular backups, which includes offsite encrypted tapes or drives (classic backup approach)
- Offsite encrypted file mirroring and backups using network file systems (cloud approach)
- File integrity monitoring
- A routine of regular tests for restoring files from backup
- Physical security measures to protect access to ISAO servers and offices, such as cameras, swipe access systems, and so on
- Protecting encryption keys and passphrases/passwords; these data should be protected on airgapped, isolated systems
- Host-based on network-based security technologies
- Ensuring the regular maintenance of ISAO computer systems, which includes ensuring that they are kept up to date, with current licenses, and covered by organizational security tools
- Strong organizational policies and training on security practices

- Recurring background checks and administrative checks on access and accounts, including post-separation access
- Business continuity planning exercises.

In the aforementioned example, in step #2, the ISAO analyst will review the contents of the member submission. Having the relevant files and communications encrypted helps the analyst ensure that the confidentiality of the data will be preserved.

10.3 INFORMATION ASSURANCE—TRUST

Earlier in Section 5.4, a standard model for classifying reporting was highlighted. Most often, member submissions will fall under TLP Red, as these reports will contain data attributing to the submitting organization. Trust and intelligence sharing will usually benefit the most from including the most amount of technical threat data while including the least amount of attribution to the source beyond scoping out the legitimacy of the submission.

The data encryption and data-at-rest security measures both contribute to the trust model. Data encryption offers some assurance that the submission was sourced from a trusted sender and contributes to the legitimacy of the submission. Data-at-rest measures help to protect the identity and attribution of the source of intelligence.

The final piece of this equation is the ISAO analyst team and its adherence to intelligence declassification and dissemination practices. All ISAO analyst team members' efforts to provide a finished intelligence product to the rest of the membership should include steps to de-attribute (anonymize) the source, verify and validate the technical indicators, and finally include general impact and severity statements that support their guidance. Once the finished intelligence product is completed, it should be communicated back to the membership using encryption technologies for email or web.

10.4 CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

The protective measures outlined in the section above are only some of several key elements to promoting an ISAO's leadership role within the sector. Of equal importance is for the ISAO to regularly update the membership with details of the protective steps, conduct regular technical and policy security reviews, and collaborate with the member organizations to continually improve.

In summary, confidentiality, integrity, and availability can be achieved by leveraging data-in-transit encryption, data-at-rest encryption, backups, and file integrity or availability monitoring and checks, and by rigorously enforcing best practices for informational handling.

APPENDIX A—GLOSSARY

Selected terms used in the publication are defined below.

Alert: Timely information about current security issues, vulnerabilities, and exploits.

Analysis: A detailed examination of data to identify malicious activity and an assessment of the identified malicious activity to existing threat information to say something greater about the data at hand.

Anomaly: Something that deviates from what is standard, normal, or expected.

Attribute: A quality or feature regarded as a characteristic or inherent part of someone or something. A piece of information that determines the properties of a field or tag in a database or a string of characters in a display.

Automated cybersecurity information sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system utilizing primarily machine programmed methods for receipt, analysis, dissemination, and integration.

Big data analytics: The process of examining large and varied data sets—that is, **big data**—to uncover hidden patterns, unknown correlations, market trends, customer preferences, and other useful information that can help organizations make more informed business decisions.

Campaigns: In the context of cybersecurity, a campaign or attack via cyberspace that targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure, destroying the integrity of the data, or stealing controlled information.

Clustering: The grouping of a particular set of objects based on their characteristics, aggregating them according to their similarities.

Computer security incident: See "Incident."

Computer security incident response team: A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a computer incident response team, computer incident response center, or computer incident response capability.

Crowd sourcing: The practice of obtaining information or input into a task or project by enlisting the services of a large number of people, either paid or unpaid, typically via the Internet.

Cybersecurity information: Data-related risks and practices relevant to increasing the security of an information system. Examples include hardware and software vulnerabilities, courses of action, and warnings.

Cybersecurity information sharing: The exchange of data-related risks and practices.

Cybersecurity threat: An action on or through an information system that may result in an unauthorized effort to adversely affect the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber-threat indicator: Information that is necessary to describe or identify

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or
- any combination thereof.

Cyber-threat information: Information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against IT or operational technology systems.

Data: Facts and statistics collected together for reference or analysis**.**

Data sets: A collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer.

Defensive measure: An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

Enriched cybersecurity information: Cybersecurity information that is combined with multiple different data sets or streams to produce a more comprehensive set of data.

Event: Any observable occurrence in a network or system.

False negative: An instance in which a security tool intended to detect a particular threat fails to do so.

False positive: An instance in which a security tool incorrectly classifies benign content as malicious.

Feeds: An ongoing stream of structured data that provides users with updates of current information from one or more sources. Data feeds are often described in terms of their methods of delivery. Rich Site Summary feeds, for example, use an XML-based file format to deliver content from multiple sources to users.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident handling: The mitigation of violations of security policies and recommended practices.

Incident response: See “Incident handling.”

Indicator: An artifact or observable evidence that suggests that an adversary is preparing to attack, that an attack is currently underway, or that a compromise may have already occurred.

Information: Information is data that have been processed in such a way as to be meaningful.

Intelligence: Intelligence is information gathered within or outside the United States that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security.

Malicious cyber command and control: A method for unauthorized remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system.

Malicious reconnaissance: A method for actively probing or passively monitoring an information system for the purpose of discerning its security vulnerabilities, if such method is associated with a known or suspected cybersecurity threat.

Malware: A program that is covertly inserted into another program or system with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Mitigation: The act of reducing the severity, seriousness, or painfulness of security vulnerability or exposure.

Monitor: To acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.

Operational analysis: Examination of any combination of threats, vulnerabilities, incidents, or practices that results in methods to protect specific data, infrastructure, or functions (e.g., incident analysis, identification of specific tactics, techniques, procedures, or threat actors).

Real-time information sharing: See "Automated cybersecurity information sharing."

Secure portal: A web-enabled resource providing controlled secure access to and interactions with relevant information assets (information content, applications, and business processes) to selected audiences using web-based technologies in a personalized manner.

Security control: The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security vulnerability: Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Situational awareness: Comprehension of information about the current and developing security posture and risks, based on information gathered, observation, analysis, and knowledge or experience.

Social engineering: An attempt to trick someone into revealing information (such as a password) that can be used to attack systems or networks.

Threat: Any circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat actor: An individual or group involved in malicious cyber activity. [Source: MITRE, Structured Threat Information eXpression.]

Threat source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Trend analysis: Examination of data to identify any combination of broad, non-obvious, or emerging actions (e.g., threat actor campaigns and intent, common vulnerabilities and configurations exploited, or merging operational analytics with non-like data streams such as assessments).

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

APPENDIX B—ACRONYMS

API	application programming interface
CISA	Cybersecurity Information Sharing Act
CVE	Critical Vulnerabilities Exposures
DNS	Domain Name System
IA	information assurance
IOC	indicator of compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	information technology
MISP	Malware Information Sharing Platform
PII	personable identifiable information
RDP	Remote Desktop Protocol
SIEM	security information and event management
SO	Standards Organization
TLP	Traffic Light Protocol
TTP	tactics, techniques, and procedures