9 Steps

Creating a New Cyber Threat Intelligence Team

8 May 2020

Authors
Carly Harris
Heather Manganello
Vidya Murthy
Kyle Rota
Susan Vagell

Graphic Designer
Sarah Schreck

Advisor
Kyle O'Meara

Capstone Project for Master's of Science Degree in Information Security Policy and Management from Heinz College, Carnegie Mellon University

Carnegie Mellon University
Heinz College
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Table of Contents

List of Figures

Executive Summary

This report is a framework that a company could use as a guide to create a cyber threat intelligence team. Companies with cyber threat intelligence teams claimed that their average return on investment three years after creating the team was 284%, according to a survey conducted by Recorded Future, and the companies' risk was reduced by approximately 10 times due to identifying threats sooner.[1] The intended audience for this paper is a company with an existing cyber security function, such as a Security Operations Center (SOC), and seeks to add cyber intelligence capabilities to better inform its senior leaders' decisions. The team's primary outputs would be reports and briefings that identify emerging cyber threats and analyze potential impact to the company.

Our approach offers nine steps to institute a new, small cyber threat intelligence team. For each step, we provide its goal, scope of implementation, best practices based on personal experiences and literature reviews of US Government and private sector company methodologies, and recommendations for improving the team's performance over time. Our intent is that the framework is practical, such that it outlines methods to accomplish each step rather than merely identifying lofty goals without any explanation of how to achieve them.

In addition to providing a procedure to set up a cyber threat intelligence team, we have included a workflow of the team's daily operations, including how the team could integrate with senior leaders. Each component in the workflow refers back to the detailed descriptions contained within the nine steps, which should aid a manager in tailoring the team's processes to match the company's vision for the cyber threat intelligence team.

Introduction

We derived our framework from a foundational report written in 2019 by the Software Engineering Institute (SEI) titled *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States,*[2] and our report builds on SEI's work by detailing how a company could create and develop a cyber threat intelligence team. The SEI authors surveyed approximately 30 private company's cyber threat intelligence teams and focused on improving an existing cyber threat intelligence team's capabilities to become "high performance." Accordingly, we view the two reports to be complementary, and a company could use them in tandem to form, institute, and hone a cyber threat intelligence team.

9 Steps

Drawing from 33 "assessment factors" that SEI used to evaluate the teams it interviewed, we selected, combined, and modified approximately half of the assessment factors to create nine steps to forming a new team. Our paper describes each step in detail and suggests opportunities to improve the team's performance in that area over time. We ordered the nine steps, listed in Figure 1, such that the team's manager could develop processes for the broadest sets of activities first, then identify additional resources that the team could leverage from across the company, and finally hire the team only after the manager had clearly defined roles and responsibilities for each member. We expect the process to be iterative, with the manager regularly refining workflows.

1. Leadership Involvement
2. Cyber Intelligence Reporting
3. Strategic Analysis Workflow
4. Technical Analysis Workflow
5. Intelligence Requirements Process
6. Threat Prioritization Process
7. Organization Information Sharing Process
8. Staffing a New Cyber Threat Intelligence Team
9. Technology for Data Collection

Figure 1. 9 Steps to create a cyber threat intelligence team

First, we advocate that a manager should obtain senior leaders' approval, acquire resources (e.g. budget), and solicit leaders' views on the team's mission; vision; and scope. Second, with leadership, the manager should determine the team's outputs, such as by jointly outlining a couple of types of written reports and establishing a briefing schedule. Third, the manager should design a procedure for conducting strategic analysis to produce those reports for leaders using sophisticated critical thinking. Fourth, a technical analysis workflow should be created to ensure that Technical Analysts strengthen strategic analysis by conducting the underpinning technical assessments, collaborating on reports, and coordinating with the company's SOC.

After designing the team's overarching analytic functions, the manager should involve other parts of the organization in the fifth step to establish procedures identifying the company's most pressing questions—"Intelligence Requirements"—that the cyber threat intelligence team strives to answer. This step, and the next, should include senior leaders, mid-level managers, and the risk management team. Sixth, company representatives should institute a process, incorporating Intelligence Requirements, to prioritize the multitude of threats facing the company to list the most important projects for the cyber threat intelligence team. Seventh, the manager should seek opportunities to obtain and share data across the company and potentially with external organizations.

After having collaborated with teams across the company to develop multiple procedures, the manager should know which roles the cyber threat intelligence team should staff to fulfill each process as well as identify any resources (e.g. Data Scientists) that the manager could leverage from elsewhere in the company, making it easier to draft specific hiring requirements. Ninth, after staffing a small team, the manager should defer to the analysts to select their preferred commercial tools to collate information.

Team Workflow

This framework would be incomplete without outlining the workflow for a cyber threat intelligence team once formed; although related, the steps that a manager follows to develop procedures is different from the team's order of operations. Accordingly, we designed a team workflow that is premised on the Intelligence Cycle workflow developed by the US Intelligence Community.[3] The Intelligence Cycle lists six categories of intelligence activities that are repeated iteratively: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and evaluation.[4] The Intelligence Cycle model also is consistent with

the SEI's recommendations for improving the performance of cyber threat intelligence teams. In the Team Workflow section, we include a graphic of our recommended workflow that reflects the cyclical, iterative nature of cyber threat intelligence.

Scope

Recognizing that every company faces a plethora of threats, we deem it necessary for a new cyber threat intelligence team to limit its scope. Not only do analysts need to build expertise, but the team should quickly demonstrate its utility beyond commercially-available cyber intelligence reports, which typically are general and not tailored to specific companies or industry sectors. The team's analysts need to both add specific context on threats as well as offer insights on how that threat could impact the company. Analysts are likely to add the most utility when they are allowed to specialize on a particular country, for instance.

In this paper, we recommend that a new, small cyber threat intelligence team focus only on a few top nation-state adversaries as well as the company's top three critical assets. To cover these topics, we recommend hiring Strategic Analysts of two types: geopolitical and functional. Geopolitical Strategic Analysts specialize in the culture and, if possible, the language of one or two foreign adversaries. Functional Strategic Analysts specialize on the company's critical assets and work closely with geopolitical Strategic Analysts to learn more about the capabilities of foreign threat actors targeting those critical assets.

As the cyber threat intelligence team demonstrates its utility to leadership and obtains more resources, we recommend that the manager consider broadening the team's scope to cover additional topics, such as more nation states, criminal groups, emerging technologies, or the company's supply chain.

For the purposes of this paper, we define cyber attacks and cyber operations as any offensive actions that an adversary attempts against an organization, including data exfiltration, network intrusions, and phishing.

Step 1: Leadership Involvement

Overview

For a cyber intelligence program to be effective, leadership support and involvement is essential. Senior company leaders should work with the team to provide topics of interest, such as cyber issues that could affect upcoming business decisions, which the team could research and analyze in written reports and briefings. These priorities also should be reflected in Executive Intelligence Requirements, which will be defined in Step 5 (Intelligence Requirements Process). Furthermore, leaders should suggest improvements for tailoring the products—both content and layout—to their needs.[2] Given that the team's mission is to provide assessments for senior leaders, leaders should be involved in approving the team's workflows, take an active interest in and engage the team, and make use of its products.

Scope

This section outlines best practices in leadership involvement and communication channels. The recommendations in this section aim to combat common challenges, such as reactionary involvement or lack of involvement from leadership. Leaders often get involved only during a crisis, which might be too late to produce the result that leaders seek. Teams who have reactionary involvement from their leaders typically want their leaders to be more active in setting strategy and workflows.[2] The best practices and recommendations outlined in this section are applicable to cyber threat intelligence teams of all performance levels; they could be implemented by either a new team or by an established highly-functioning team. This section includes recommendations on methods to include leaders in the cyber threat intelligence team process and suggestions for instituting specific communication channels.

Industry Best Practices

Incorporating Senior Leaders

One best practice is to periodically involve leaders, and even the company's board of directors, in a cyber threat intelligence team's planning, direction, production, and feedback. It is important that the board of directors understand the importance and value of cyber intelligence and cyber security; if the board is unfamiliar with those concepts, the team's manager could brief the board on its purpose and capabilities. Some organizations have a senior member of the cyber intelligence or cyber security team sit on the board, like the Chief Information Security Officer

(CISO), Chief Security Officer (CSO), or Chief Technology Officer (CTO). Cyber intelligence teams could send some or all of their reports, such as Threat Priority Lists, to the board in addition to senior leaders.[2] As described below, the cyber intelligence team should institute defined communication channels for providing relevant information to leaders and the board as deemed appropriate for the company.

A large portion of senior leaders' responsibilities includes risk management. CISO's need to assess risk, identify risk mitigation strategies, and communicate risk to other senior managers. To do so well, a CISO requires having pertinent information from the cyber threat intelligence team. Because the cyber threat intelligence team's primary customer probably is the CISO, the team's manager should work closely with the CISO in establishing the team's mission, scope, and processes. The cyber threat intelligence team should sharpen their leaders' focus by providing general trends. Topics on which the team could report include frequent types of cyber attacks, cyber operations generally requiring the most expensive responses, emerging threats, new cyber adversaries and the assets that they are targeting, and successful cyber security practices and new technologies.[5]

An effective way to involve leaders is to create a feedback loop, as shown in Figure 2. A company's cyber threat intelligence team should receive guidance from its CISO and leadership and possibly its SOC or business unit directors on threats of interest and prioritized assets. Using this background, the cyber threat intelligence team should provide leaders with related information like prevalent cyber attacks, costly cyber operations, emerging cyber threat actors, and successful security practices and technologies. Business leaders could then use this information to communicate the impact of potential threats and justify the return on investment of countermeasures to the company's Board of Directors. This flow could be adapted depending on the company's organization chart.

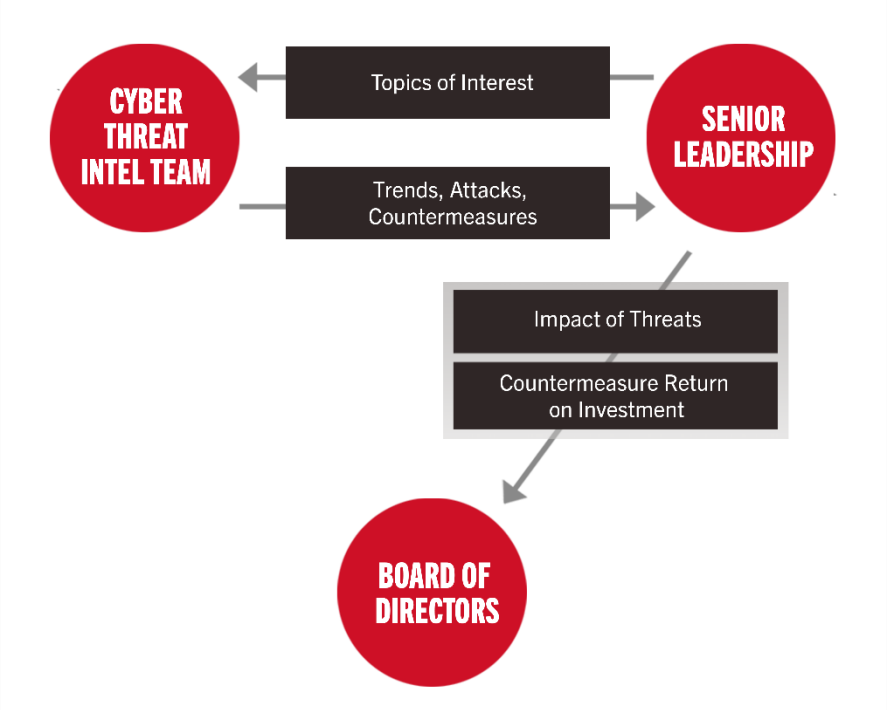

Figure 2. Flow of leadership involvement

Communication Channels

When communicating across an organization, it is important that the content shared is appropriate and necessary for its various categories of recipients. With this goal in mind, many organizations identify groups of stakeholders and create communication channels based on these groups. Some examples of communication channels include emails, presentations, reports, and meetings. Creating targeted communication channels prevents leaders from receiving irrelevant information or the cyber threat intelligence team inappropriately distributing information that is deemed sensitive. Leaders should approve distribution lists and establish the maximum classification levels of materials transmitted via those channels.[6] As described Step 8 (Staffing a New Cyber Threat Intelligence Team), the team's Collection Coordinator could help disseminate the team's published reports using such procedures.

To prevent overwhelming stakeholders with irrelevant information, a company should create communication channels based on different groups of stakeholders. Possible groups include senior leadership, business unit CISOs, business unit leaders, risk managers, and corporate cyber security teams (e.g. the SOC). Specifically, a company could create two levels of communication channels for reporting to their leaders.

(1) General Business-Relevant Information: This communication channel would focus on generic cyber hygiene and threats likely to impact all of a company's business units. Leaders should be informed of actionable business-relevant information that is relevant to the company as a whole but might not affect subordinate business units directly. For instance, the Chinese Government is likely to release its next Five-Year Strategic Plan in Spring 2021; if aerospace is listed as the top industry China seeks to grow, a defense contractor should expect aggressive cyber attacks from China through at least 2026.[7]

(2) Targeted Information: This communication channel is focused on targeted information that pertains specifically to a manager's unit. This includes any information that is pertinent to a leader's product, technology, or people, such as, threat analysis reports, vulnerability reports, and incident response reports. A cyber threat intelligence team could create a targeted information channel to a specific business unit's CISO to share cyber threats specific to the latter's critical assets. Similarly, a cyber threat intelligence team could institute a targeted information channel with the SOC to obtain network logs listing attacks targeting a business unit's manufactured products.

Recommendations for Improving Performance

As the cyber threat intelligence team grows and develops, the team should work to develop new ways to involve leadership. As new cyber intelligence-related teams develop within the company—such as a collection management team, a data science team, or more specialized cyber threat intelligence branches—feedback loops similar to the ones suggested above should be created for each team to ensure that leadership receives relevant information. In addition, communication channels should be added and refined across the company and between new teams, such as delivering information to additional individuals or groups. The goal is to create an interactive process that becomes second nature to the team and senior leaders that is reviewed and updated periodically.

Conclusion

We propose a variety of suggestions to incorporate leaders into the cyber threat intelligence process effectively. Leadership endorsement and support for a new cyber threat intelligence team are key elements to the successful implementation of the intelligence process. Creating a

feedback loop between leadership and the cyber threat intelligence team would ensure that leaders receive the information they need to make decisions and that it is in their preferred format. The team's products should provide valuable information to leaders and the board of directors, informing them on cyber operations and actors that could affect the company as well as providing useful assessments of those potential impacts, justifying expenditures on both cyber intelligence and cyber security. In addition, instituting communication channels based on specific groups of recipients would ensure that each stakeholder receives relevant information. Following these best practices and suggestions would result in effective leadership involvement in a new cyber threat intelligence team.

Step 2: Cyber Intelligence Reporting

Overview

To transform information collected and analyzed into actionable operations or decisions, analysis should be distributed in different forms of reports to customers. A variety of cyber threat intelligence report types should be used to address immediate needs, leadership requests, and analysis useful to other business units (e.g. a SOC). When building a cyber threat intelligence team, it is important to identify the specific types of reports useful to leaders. High-performing organizations create a strategy for their cyber intelligence product line that includes identifying recipients for particular reports, layouts for cyber intelligence reports, and timelines for the distribution of the reports.[2]

In addition to writing reports for decisionmakers, reports could help a team to retain knowledge as team members change; new teammates could use these papers as background. Furthermore, reports listing their published dates allow a team to compare cyber actors' changes in methodology and targets over time, enabling the team to assess cyber actors' evolution over years. To preserve its reports, as mentioned later in this paper, the team should select a knowledge management database—which could be as simple as a shared folder or SharePoint—allowing all team members and other stakeholders access to the team's published papers. Additionally, disseminating these reports would facilitate information sharing between a cyber threat intelligence team and its parallel cyber security units (e.g. a SOC), such as by sharing the technical details of cyber actors' tactics, techniques, and procedures.

Scope

This section outlines best practices in intelligence reporting, including writing style, confidence levels, and estimates of probability. In addition, a suggested structured distribution system and formalized schedule for reporting is provided.

The report types described in this section are customized for a newly-developed cyber intelligence team. To have the capacity to produce these reports on a regular timeline, a company would require sufficient resources and a formalized schedule. For instance, the US Intelligence Community has specific report types corresponding to timelines of 4 hours, 24 hours, 1 week, or 1 month. For reports published within 24 hours, such as the President's Daily Brief (PDB) produced by the US Intelligence Community, an analyst and up to four tiers of

editing managers often work long hours into the night. While a company's editing chain almost certainly would not be as rigorous, senior leaders and the cyber intelligence team's manager should determine under what conditions the company would want analysts to work overtime to meet certain deadlines. As mentioned in Step 3 (Strategic Analysis Workflow), in some scenarios, leaders might be willing to accept a short paper that highlights a current development with low confidence levels within one day when followed by a longer paper with higher confidence levels published a week later.

However, organizations that do not have enough people or time allocated to producing reports typically use their limited resources to focus merely on cyber security issues, losing opportunities to obtain predictive assessments.[2] As mentioned in Step 1 (Leadership Involvement), leadership buy-in is essential to drive a strategy behind producing reports. Organizations that do not have leadership support typically receive no feedback on requirements, timelines, or layouts for reports.

Industry Best Practices

Report Types

Threat News

To spread awareness throughout the organization of cyber threats, the cyber threat intelligence team should provide weekly Threat News reports listing brief summaries of important external intelligence products. These reports could be distributed via email and should contain information on security events that are directly relevant to the company, the defense industry, or the cyber security field. A report template is provided in Appendix A and is based on Recorded Future's Weekly Threat Intelligence Report Template.[8] These reports could be highlights copied from cited external intelligence reports that are collated by the team's Collection Coordinator.

Threat Analysis Reports

Following the identification of an adversary, an actionable summary report should be created and shared with relevant stakeholders, based on the previously described distribution protocol. This report should include a description of the adversary's actions and tactics, including the adversary's capabilities; the adversary's infrastructure; and the victims and/or affected assets. In addition, the report should contain a course of action that summarizes steps to be taken to respond to any immediate threats. A report template is provided in Appendix B and is loosely

based on Zelster's Report Template for Threat Intelligence and Incident Response.[9] Strategic and Technical Analysts should collaborate to draft this report.

Senior Leadership Briefings

The cyber threat intelligence team should provide senior leadership with updates on the team's activities and findings. This can be accomplished in a variety of forms, including weekly meetings with the team's immediate chain of command, monthly briefings to business unit department leaders, and bi-annual CISO and senior-leader briefings. The team could host two types of Senior Leadership Briefings. The first type could be assessments pertinent to a specific business unit. This should focus on specific information that directly affects a leader's product, technology, or people, such as a cyber actor seeking to modify a particular product built by a specific business unit. When briefing department leaders, the team should prepare a PowerPoint presentation or handouts with a summary of findings directly related to that department. The second type could be assessments that affect all business units to inform company leaders and could be actionable but not specific to one business unit. This could include a new cyber actor seeking to exfiltrate intellectual property from other defense contractors. Strategic Analysts should give these briefings, focusing on the potential impact to the company or executives' future decisions, but it might be appropriate for Technical Analysts to attend the briefings to answer any technical questions.

Geopolitical Events

Geopolitical events that impact nation states could instigate adversaries to conduct malicious cyber operations against companies that are perceived to be close to the US Government.[10] Therefore, it is essential for the cyber threat intelligence team to publish papers identifying such events and assessing possible actors who might target the company and list their most common tactics. Following a geopolitical event that could have implications for the company, Strategic Analysts—with substantive assistance from Technical Analysts—should write a paper to be produced and distributed using the previously-described distribution protocol. The report should contain details on the country and, if applicable, the specific group likely to respond to the event. In addition, it should contain details on why the event is important and what is the probable impact. Other details that should be included, if known, are the nation state's motivation and whether this motivation is connected to the company in any way. Additionally, analysts should include their judgements on the potential for long-term impact. A report template is provided in Appendix C.

Threat Priority List

Following the completion of the Threat Prioritization Process outlined in Step 6, as well as after periodic reviews, the cyber intelligence team's manager—and possibly Analytic Tradecraft Expert—should create a Threat Scorecard. This scorecard will produce a list of numerous threats that are prioritized by the likelihood that the actors have the means and motivation to attack the company. These threats are mapped to specific assets that the actors could target and include the assessed potential impact on those assets. Derived from the scorecard, the Threat Priority List should be a shorter description of the top threats. In addition to the list, the report should contain key judgements resulting from the Threat Prioritization Process. A report template is provided in Appendix D.

Writing Style

> ***"Good intelligence depends in large measure on clear, concise writing….The information [the Central Intelligence Agency] CIA gathers and the analysis it produces mean little if we cannot convey them effectively."***
> *- Style Manual and Writers Guide for Intelligence Publications, CIA*[11]

Senior leaders have little time, and analysts should write such that their readers could quickly skim the product and glean the important information without stumbling over confusing wording, grammar, or jargon. *The Analytic Thinking and Presentation for Intelligence Producers Analysis Training Handbook*[12] outlines the following principles:

Conclusion First: To make the "big picture" clear, reports should begin with important conclusions. Most reports start with a Bottom Line Up Front (BLUF), which is a military communication standard that is meant to enforce speed and clarity.[13] The BLUF should contain the most important conclusions that are found in the report. Providing this information up front clearly conveys your main point and saves the reader time. In PDBs, the US Intelligence Community bolds and italicizes each BLUF to make them easily visible. Following the BLUF, the report should contain a logical flow of key judgements that support the conclusions outlined in the BLUF.[14]

Organize

Information should be provided in a logical order using summary sentences and bullets to convey

details. This structure will avoid confusing or slowing the reader. Under each paragraph's BLUF, the US Intelligence Community lists supporting pieces of information using bullet points, clearly delineating the portions of a paragraph that are analytic versus informational.

Formats

Each report type should have its own structured design that effectively conveys information and is customized to the preferences of its recipient, such as the CISO. A clear understanding of the similarities and differences between report types and purposes will allow analysts to quickly determine which report type should be used in each situation.

Precision

Precise language throughout reports is required to eliminate ambiguity or misinterpretation by the intended customers. Each person who reads the report should understand the same message.

Economize

Remember that those reading reports probably are busy and have little time. Therefore, the products should be brief, concise, and use familiar, simple terms—avoiding the use of jargon. Sentences should be pithy and short by making each word count.

Clarity

Aim for clear, transparent logic. This goal can be achieved by using precise language and structure and simple sentences that avoid unnecessary adjectives and adverbs.

Active Voice

When writing reports, use active voice instead of passive voice. Active voice makes the content direct and concise, and therefore, more analytical. Sentences structured using passive voice can confuse readers who are skimming papers, forcing them to reread those passages. Using active voice involves structuring sentences to have the subject perform an action that the object receives. For example, "Heather ran the race" not "The race was run by Heather."

Edit

No reports should be distributed without first being edited. Revise your own work first to improve its quality. A manager or analytic tradecraft expert should edit papers for senior leaders

to ensure consistency. If available, also have another editor in your company review products prior to distribution.

Know Your Readers

When writing, remember the reader will be asking "So what?". Everyone who reads the report needs to be able to understand and apply your report's message and rely on your insights and judgements.

Patience

When working with a team to develop a report, have patience. Work together to produce a well-written report that will impress leadership. A paper's writing style can influence leaders' impressions of a team's capabilities as much as, or more than, the paper's content; without writing clearly, a leader won't understand or remember the substance.

Confidence Level and Probability Estimates

Confidence levels assigned to conclusions are needed to help provide transparency and convey uncertainty when the underlying information is conflicting, unavailable, or potentially misleading. According to the Office of the Director of National Intelligence (ODNI)'s *Guide to Cyber Attribution,*[15] confidence levels should be based on the timeliness and reliability of the evidence, the strength of the logic linking the evidence, and the type of evidence (direct, indirect, circumstantial, or contextual). The *Guide to Cyber Attribution* outlines the three confidence levels depicted in Figure 3, and we provide examples for each.

CONFIDENCE LEVEL	DESCRIPTION	EXAMPLE
HIGH CONFIDENCE	This level of confidence is used when analysts judge the totality of evidence and context to be beyond a reasonable doubt and with no reasonable alternative.	We judge with high confidence that the Chinese nation-state group APT10 is targeting US defense contractors to steal sensitive information on missiles used by the US Army.
MODERATE CONFIDENCE	This level of confidence is used when analysts judge the totality of evidence and context to be clear and convincing, with only circumstantial cases for alternatives.	We assess with medium confidence that APT10 includes employees of a Chinese company named Huaying Haitai Science and Technology Development Group.
LOW CONFIDENCE	Analysts use this level of confidence when they judge that more than half of the body of evidence points to one thing, but there are significant information gaps.	We assess with low confidence that APT10 will change its malware tools after recent reports publicly identified the group's methodology.

Figure 3. Descriptions of confidence levels[15]

In addition to assigning confidence levels to conclusions, include an assessment of probability; each analytic judgement should contain a probability estimate, which makes it clear that the statement is an assessment rather than a fact. According to the ODNI's *International Community Directive 203,*[16] assessments should indicate any uncertainties in judgements and explain the basis behind the uncertainty. In addition, analysts should explain how their uncertainty affects the analysis. This includes what types of information would change their analysis, and how this new information would affect their certainty. For instance, a clear conclusion with probability estimate and an explanation of uncertainty might be, "Russia probably conducted these cyber attacks, but our assessment of the cyber actor would change if the Syrian Government also were targeted." The ODNI's *International Community Directive 203* outlines the set of terms for likelihood or probability shown in Figure 4.

ALMOST NO CHANCE	VERY UNLIKELY	UNLIKELY	ROUGHLY EVEN CHANCE	LIKELY	VERY LIKELY	ALMOST CERTAIN(LY)
REMOTE	HIGHLY IMPROBABLE	IMPROBABLE (IMPROBABLY)	ROUGHLY EVEN ODDS	PROBABLE (PROBABLY)	HIGHLY PROBABLE	NEARLY CERTAIN
01 - 05%	05-20%	20 - 45%	45 - 55%	55 - 80%	80 - 95%	95-99%

Figure 4. Descriptions of probability estimates[166]

Distribution

Reports should be disseminated as quickly as possible—most organizations find that 24 hours is ideal; however, this timeframe is difficult to achieve. Often, four days is considered unusually fast.[2]

The distribution of reports is likely to depend on the type of report and the information outlined in the report. To maintain a consistent system for distributing reports, we suggest that companies follow the Traffic Light Protocol (TLP) chart shown in Figure 5, developed by the Department of Homeland Security (DHS), that we modified for a cyber threat intelligence team, for internal information sharing.[17] A manager should assign one of the TLP sensitivity levels to each report produced by the cyber threat intelligence team, based on the most sensitive information contained in the report, which should restrict the paper's distribution. Furthermore, the manager could specify certain individuals or units that are allowed access to the report.

COLOR	WHEN SHOULD IT BE USED?	HOW COULD IT BE SHARED?
TLP: RED Extremely limited disclosure, restricted to preauthorized individuals only. **Clearance Level** Top Secret	Reports and information should be assigned TLP:RED when distributing the information is likely to severely harm an individual's privacy or group's reputation or it contains exclusive information, such as sensitive information shared by senior leadership.	Recipients should not share TLP:RED information with any unauthorized parties who were not privy to the specific exchange, meeting, or conversation in which it was originally disclosed. In most circumstances, TLP:RED should be exchanged verbally, in person, or over encrypted channels.
TLP: AMBER Limited disclosure, restricted to certain teams. **Clearance Level** Secret	Reports and information should be assigned TLP:AMBER when it poses moderate risk to an individual's privacy or group's reputation or it should not be shared broadly across the company.	Recipients may only share TLP:AMBER information with members of their own business unit. Leaders should determine when to distribute it outside of their departments to other sections of the company
TLP: GREEN Limited disclosure, restricted to the company. **Clearance Level** Confidential	Reports and information should be assigned TLP:GREEN when information probably is useful for the majority of the company but should not be shared externally without senior leaders' approval.	Recipients may share TLP:GREEN information with other departments in the company. The information probably is permissible to share with other organizations, but that process should be approved by leadership.
TLP: WHITE Disclosure is not limited	Reports and information should be assigned TLP:WHITE when it contains minimal or no foreseeable sensitive information.	Subject to standard copyright rules, TLP:WHITE information may be distributed outside of the company without restriction, in accordance with applicable rules and procedures for public release.

Figure 5. Traffic Light Protocol data classification system[17]

Recommendations for Improving Performance

As a company' cyber intelligence team evolves, so should its reporting capabilities. The more analysts on the team, the more reports could be written. High-performing organizations have a varied cyber intelligence product line.[2] Therefore, as the program evolves, a company should introduce new report types. Some additional report types to consider: Targeting Packages as described in Step 3 (Strategic Analytic Workflow), tactical reports on actors; indicators of compromise; and behavior summary, incident response reports, and malware analysis.

In addition, as the team grows, companies should aim to improve efficiency in disseminating reports. Improvements are possible in many parts of the cycle, and the manager should periodically review the team's publication process to identify opportunities to improve efficiency and collaboration. For instance, a Collection Coordinator could be charged with delivering papers to leaders and soliciting feedback. As the coordination process outlined in Step 3 (Strategic Analysis Workflow) becomes more routine, the time designated for allowing other teams to review the team's papers might be shortened. If leaders seek to have papers delivered sooner, the paper formats could be shortened or analysts authorized additional overtime. If editing becomes a bottleneck, the team could hire a dedicated editor.

Conclusion

We propose a variety of suggestions in order to implement an effective reporting strategy for most companies. Following industry best practices in writing style results in conveying important information in a clear and concise manner. Using Confidence Levels and Estimations of Probability provide context to key judgements. Following the Traffic Light Protocol for information sharing within the organization will ensure all relevant stakeholders are informed. Finally, the variety of report types proposed provides a starting point to eventually build a range of cyber intelligence products.

Step 3: Strategic Analysis Workflow

Overview

Corporate leaders are concerned with multiple business areas that could be affected by cyber intrusions, and Strategic Analysts seek to provide forewarning of or damage assessments on cyber activities to decision makers, drawing connections between the cyber and business worlds. When providing assessments to leaders, however, it is important to provide thoughtful analysis to demonstrate the team's utility. A Strategic Analysis Workflow is a defined and repeatable process[2] that ensures that reports are of high quality and representative of the views of all pertinent stakeholders in the company, providing thorough products from which leaders can make more informed decisions.

What does a Strategic Analyst do on a typical day? This workflow outlines expectations for a Strategic Analyst, proposing a specific order of operations. The workflow should be customized to a company, but these concepts—based on the process that intelligence agencies use to write reports for the US President—should be incorporated.

Scope

As stated above, this workflow is based on an assumption that—in a new cyber intelligence cell—Strategic Analysts would focus only on enumerating nation-state adversaries and protecting critical assets. Ideally, an intelligence cell would have one geopolitical Strategic Analyst each covering Chinese, Democratic People's Republic of Korea (DPRK), Russian, and Iranian cyber adversaries. It is helpful for analysts to be divided by countries because some government-sponsored cyber groups overlap in methodology and infrastructure. Additionally, at least one functional Strategic Analyst could focus on cyber threats that could impact a company's critical assets. For situations in which a foreign adversary monitored by a geopolitical analyst conducts a cyber campaign targeting a company's critical asset covered by a functional analyst, crossing analytic lines of responsibility, analysis will be enriched by integrating both analysts' perspectives.

Most of this section is derived from the CIA's strategic analysis methodologies, which have been developed and refined for over 70 years. CIA created and drives the President's Daily Brief, which is the US Intelligence Community's premier venue for strategic intelligence papers and is written for the US President.[18] CIA's Sherman Kent School for Intelligence Analysis has set the

standards for analysis across the US Intelligence Community.

Industry Best Practices

Establishing an effective Strategic Analysis Workflow is challenging. Of the few-dozen companies with cyber threat intelligence teams that the SEI interviewed, the SEI evaluated only one-quarter as being "high performing" in this category.[2]

What is Strategic Analysis?

Strategic cyber intelligence analysis is culling through a mass of incomplete data to make "big-picture" assessments on threats to an organization, such as by identifying threat actors, interpreting their motives, and suggesting opportunities to deter, prevent, or detect attacks.[2,33]

When aligned with corporate risk management and informed by technical analysis, strategic analysis should be a core activity of a cyber intelligence program. Strategic Analysts' reports have two primary consumers: corporate leadership and Technical Analysts. Accordingly, Strategic Analysts should provide leadership with assessments on potential impacts of geopolitical events (e.g. whether a foreign adversary is likely to target the company as a result of an action taken by the US Government) and provide Technical Analysts detailed information on the methods that the same cyber actors are likely to use to attack the organization. One way to delineate between strategic analysis and technical analysis that the former could focus more on future and the latter more on present. Strategic Analysts should be all-source or intelligence analysts, whereas Technical Analysts more often are malware or reverse engineering analysts who work closely with the company's cyber security functions, such as its SOC.

Srategic Analysts can serve as intermediaries between leaders, who are responsible for making a wide array of decisions, and Technical Analysts or cyber security engineers, who probably are focused on ongoing incidents and unable to dedicate time to predictive analysis. Strategic Analysts' goals are to review a mass of disparate types of information—from foreign governments' strategic documents to technical indicators, interpret linkages between those data, use critical thinking to derive assessments and explain their confidence in those assessments, identify key gaps in information that could alter their assessments, and report their assessments to senior leaders and technical staff in papers tailored to each customer set.

Ideally, Strategic Analysts also will hold regular meetings with senior leaders to brief on the cyber threat landscape and actions of US adversaries, always focusing the briefings on the potential impact to the organization's operations and its critical assets. In turn, these discussions should enlighten analysts on their leaders' concerns, better enabling them to tailor their analysis and products. Leaders also could "task" analysts to conduct further research on specific topics important for their decision-making.

In parallel, Strategic Analysts should also provide Targeting Packages to Technical Analysts that note the methodologies and infrastructures used by prospective adversaries. In return, Technical Analysts should feed their own technical reports on ongoing attacks to Strategic Analysts, which Strategic Analysts should incorporate, with additional context such as identifying possible threat actors or malware trends in a specific industry, into their assessments for leaders.

Tailored Products for Consumers: Engaging with Leaders and Technical Analysts

Strategic Analysts' primary output is a variety of analytic reports and briefings for different customers that each contain sophisticated critical thinking, identify gaps in information that reduce confidence in assessments, highlight potential impact on the company, and provide actionable recommendations. It is important that analytic products surpass summarizing collected data by analyzing possible consequences on an organization's interests.

A new cyber intelligence team probably should focus on providing tailored products to only two consumer groups initially: senior leaders and Technical Analysts, who both have different requirements.

In practice, a new cyber intelligence team probably would not endure or receive continued funding unless it quickly demonstrated its utility to senior leadership. As outlined in the scope, focusing on two topics—nation states and a company's critical assets—probably are most likely to garner leaders' attention. For instance, Strategic Analysts could highlight emerging

vulnerabilities or attack vectors to an organization's critical assets from a specific foreign adversary after a geopolitical event. Alternatively, analysts could identify a redundant or outdated cyber security expenditure to protect critical assets that could be cut. Additionally, the team should seek to brief leaders regularly on these topics, as depicted in Figure 6.

In return, when faced with business decisions, senior leaders should consider whether their cyber intelligence team could provide additional information. For instance, if the company considered opening a branch in a foreign country, the cyber intelligence team could research whether any nation-state adversaries have penetrated computer networks there. As senior leaders discover the utility of a cyber threat intelligence team, the team's managers should ensure that leadership's "taskings" are limited to those topics covered by the team to ensure that the cell develops sufficient expertise in certain areas. Accepting taskings that are outside the scope are likely to reduce the strength of the team's analysis and overwhelm analysts, hurting morale.

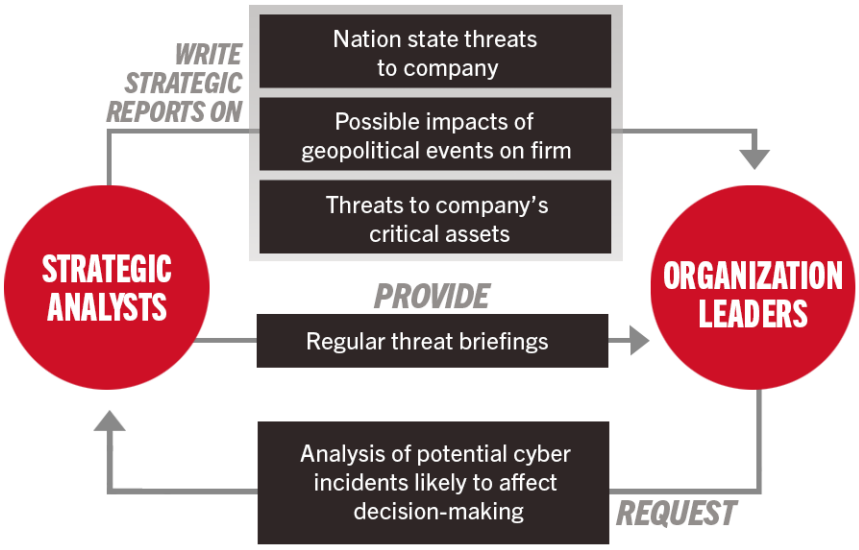

Figure 6. Strategic Analyst's interactions with senior leaders

Separately, Strategic Analysts should work closely with Technical Analysts, as shown in Figure 7. Technical Analysts should help brainstorm, contribute language to, and review each paper written by Strategic Analysts to verify its technical underpinnings. We recommend that each cyber threat intelligence team hire its own Technical Analysts, who could provide summaries of technical details to the team's Strategic Analysts as well as interface both with the company's SOC. Their primary responsibility should be to collect and synthesize technical data to help

derive strategic assessments for senior leaders, rather than augmenting the company's SOC. Unless it is explicitly stated in their job requirements, we assume that cyber security engineers in the SOC would not willing to write or contribute language to papers that require the level of diligence outlined in this Strategic Analysis Workflow. More information about Technical Analysts's responsibilities is in Step 4 (Technical Analysis Workflow).

When new threats to the organization or industry emerge from nation states or to critical assets, Strategic Analysts could prepare Targeting Packages for Technical Analysts. Based on the Diamond Model of Intrusion Analysis framework,[19] Targeting Packages could include detailed information about the adversary, capability (methodology), infrastructure (IP addresses, websites, servers, and malware signatures), and victims. Technical Analysts within the cyber threat intelligence team could incorporate that information into their more technical Threat Profiles, which detail cyber threat actors' tactics and infrastructure. Cyber security engineers could use Targeting Packages or Threat Profiles as parameters for penetration testing to evaluate the company's defenses against those threats.

Conversely, Technical Analysts should provide technical assessments to Strategic Analysts to include in reports for leadership. For instance, after receiving a Targeting Package, Technical Analysts could report back that they had tested their defenses and assess that the company is fully protected against it, information that might interest a CISO. Alternatively, Technical Analysts might uncover an ongoing attack, and Strategic Analysts could write a report for leadership that identifies the most likely perpetrators to use that infrastructure or methodology.

Additionally, Technical Analysts might discover a new attack methodology for a known adversary, a topic on which Technical and Strategic Analysts could jointly publish a report. Furthermore, the company might ask the analysts to share the report with law enforcement or Information Sharing and Analysis Centers (ISACs).

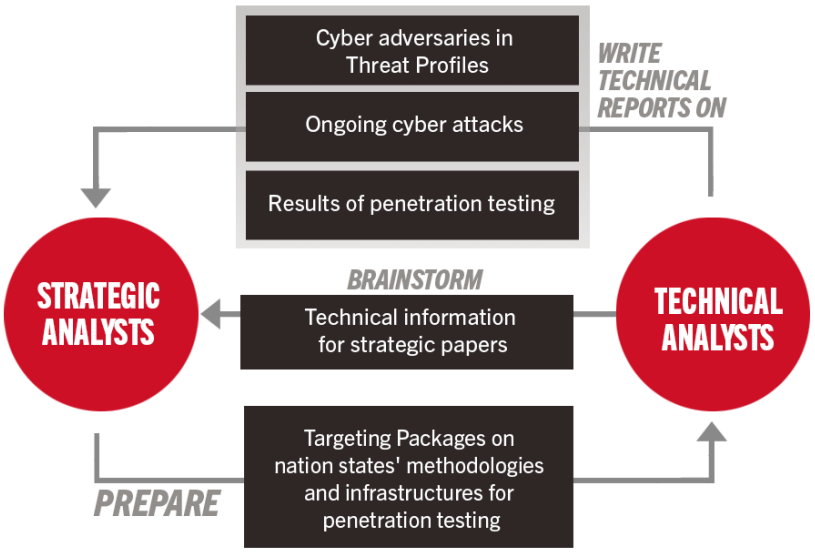

Figure 7. Products exchanged by Strategic and Technical Analysts

Proposed Strategic Analysis Workflow

This section provides a possible "day in the life of" workflow of a Strategic Analyst and is based heavily on the work practices of intelligence analysts at CIA. A Strategic Analyst's goal is to synthesize a large amount of data while considering the needs of his or her customer. When writing for senior leaders, for instance, analysts should not be sidetracked by threats of little consequence to the company or details more appropriate for technical analysis. Our proposed workflow is given in Figure 8.

Figure 8. Recommended Strategic Analysis Workflow

(1) Identify Intelligence Requirements

When a Strategic Analyst starts work on a new topic, he or she should first identify several clear questions that he or she seeks to answer. These questions should be drawn from the company's list of Executive or Priority Intelligence Requirements, as explained in more detail in Step 5 (Intelligence Requirements Process). Some examples of such questions are what threats do Advanced Persistent Threat (APT) 29 currently pose to this company? Is our company's intellectual property susceptible to Iran's Silent Librarian attacks? Such focus and planning ensure that an analyst's research is targeted and efficient.

Subsequently, the analyst should identify information that would help fill gaps in his or her knowledge or confirm or refute tentative hypotheses and relay those Specific Intelligence Requirements to the team's Collection Coordinator. For example, a Strategic Analyst might learn of a new hacking group called "Red Panda Rises" comprising Chinese individuals. One of the analyst's Specific Intelligence Requirements could be whether the Chinese individuals are linked to the Chinese Government. Collection Coordinators then seek additional sources of information that could fill these gaps, such as data from other ISACs on the infrastructure (e.g. Internet Protocol, IP, addresses) that Red Panda Rises used in its attacks, which the Strategic Analyst could compare against known Chinese Government infrastructure.

As analysts learn more about a topic, they should periodically update their Specific Intelligence Requirements. Because analysts inevitably have limited time and technical resources to synthesize the multitudes of open-source data available, it is necessary that analysts prioritize and drive information collection to address their most important questions.

(2) Review and synthesize data

A Strategic Analyst is likely to start his or her day by reading through information published since the day before, including commercial intelligence reports compiled in the Threat Intelligence Platform described in Step 9 (Technology for Data Collection). As the analyst reviews that material, he or she should consider whether any it of fills an intelligence gap or reveals a new threat and is worth highlighting to either leadership or Technical Analysts. For instance, if the relationship between the US Government and a foreign country soured overnight, the analyst could produce a report for leaders assessing whether that country is likely to attack their organization using cyber operations and—furthermore—whether the attack is likely to be

successful. In addition to providing an overarching assessment for leadership, analysts also could prepare a Targeting Package for Technical Analysts on methodologies typically used by that country's cyber actors for penetration testing or vulnerability analysis.

Strategic Analysts should review a wide array of reporting, from press reports on international affairs to recently disclosed software vulnerabilities. Many analysts focus on cyber threats emanating from a particular country and should monitor that government's press releases and any government-backed media sites. Analysts should be aware that foreign cyber actors are also likely to monitor US websites revealing new vulnerabilities, such as Krebs on Security[20] or MITRE's common vulnerabilities and exposures (CVE),[21] and attempt to develop exploits to take advantage of those vulnerabilities before the software is patched. Analysts probably would also have access to some vendor intelligence reports (e.g. Recorded Futures or the CyberWire) that highlight breaking cyber news. Companies should also hire reputable third parties to search the dark and deep networks for information on cyber actors targeting the company or industry, such as looking for indications that cyber actors have exfiltrated and are selling the company's intellectual property.

It is beneficial if geopolitical analysts covering nation-state actors cultural have cultural awareness and native language capabilities, although Google Translate[22] and Linguee. Companies also could consider sponsoring language training; Duolingo is considered one of the best language instruction programs offered for free.[23] Resources to learn more about a country's culture include The CIA's World Factbook,[24] BBC's country profiles,[25] the RSF Press Freedom Index, and PEW Research's Global Attitudes Project. As mentioned previously, the industries mentioned in China's Five-Year Plan historically have matched those from which Chinese actors attempt to steal intellectual property,[7] demonstrating the utility of reviewing political documents. Geopolitical analysts would evaluate both foreign leaders' intentions to conduct cyber activities as well as the capabilities of their state-sponsored cyber units.

Separately, functional analysts monitoring threats to the company's critical assets should also review internal risk management reports outlining the company's primary concerns and consider the most probable avenues of attack. Functional analysts should also work with geopolitical analysts to identify threat actors with relevant intent and sufficient capabilities to target the top critical assets. Both sets of analysts should review reports on ongoing attacks issued by the company's Technical Analysts and cyber security engineers and add additional context when possible, such assessing the most likely perpetrators.

(3) Log critical information

As analysts read new material, it is important to note key information in a shared repository accessible to Strategic and Technical Analysts, Collection Coordinators, Data Scientists, and other involved entities. Each company needs a shared knowledge management system (either commercial or proprietary) that ingests flagged open-source reports, internal logs and other raw technical data, and the company's published technical and strategic analysis reports. Although proprietary, customized tools might be the easiest method for analysts to use to find and sort important data, Microsoft OneNote could serve this purpose. Some companies attempt to use email to share and retain knowledge across the company, but email is difficult to search, might not be sent to all the relevant stakeholders, and could not incorporate multiple analysts' notes in one shared location.[2] Furthermore, retaining institutional knowledge is a common downfall of cyber intelligence teams and hurts analysis over the long term, particularly as teams expand and analysts change topics or become managers.

Collecting a variety of information in one centralized database is especially important for a cyber threat intelligence team. If a breaking report about a critical CVE were posted in the shared database, people in multiple roles could review the report and tag pertinent information to it. Technical Analysts and SOC engineers could test the company's defenses against that vulnerability to determine whether it poses a threat. Collection Coordinators could seek additional information about the vulnerability by contacting MITRE or other companies. Reading colleagues' notes, geopolitical analysts could quickly write a paper for leadership assessing which foreign nation states have the capabilities to exploit the vulnerability before a patch were issued. Functional analysts could contribute to the paper by determining whether the company's assets were at risk. Sharing all this information in one database, tagged to one report, is much more efficient than sending pieces of information via email, during which some individuals forget to include others and some people miss emails.

In addition to recording text-based information in a shared database, it often is helpful to display key data in a visualization tool like a link chart. Displaying a picture showing links between two attacks that used the same IP address is a quick and effective way to explain analysis, such as that two attacks might have been conducted by the same group, to leaders. Furthermore, link charts often are easily searchable and useful repositories for information. i2's Analyst Notebook is a commercial tool popular in the US Intelligence Community that creates link charts,[26] which

could display cyber actors, their infrastructure, and their victims.

(4) Identify topic for report

What is the threshold for writing a paper? Typically, a cyber intelligence team produces a product for one of three reasons: (1) senior leaders task the team to analyze a certain issue, (2) analysts observe something noteworthy (e.g. a geopolitical event) to highlight for leadership, or (3) Strategic and Technical Analysts seek to document information (e.g. about a cyber adversary or operation) using a formal mechanism to retain knowledge over time. Each paper should aim to answer one broad, key question that addresses a customer's concern. For instance, to what extent is a specific critical asset vulnerable to a new malware attack? If the overarching question is complex, the paper should be divided into sections, each addressing one subcomponent of the primary question.

The selected topic should have clear impact to the organization; the purpose of writing the report—and utility of reading it—needs to be evident to all readers. It is important that each product includes analysis and not merely summarize reports; analysts are hired to augment the company's critical thinking on the cyber landscape. Analysis should include short term and long-term impact and may include some projections based on trends in data—but not opinions. If analysts cannot agree on one most likely outcome, papers could list several feasible scenarios with supporting data for each possible outcome.

(5) Analyze information

Analysts should strive to both collect and process data without bias to avoid skewing collection such that it would lead to a predetermined assessment. Additionally, analysts should observe and interpret data or events and inductively draw generalizations, rather than finding data to fit a theory. Accordingly, it is important to work closely with Collection Coordinators to acquire a range of useful data to fill gaps.

We highly recommend that analysts undergo training on critical thinking, conducting unbiased analysis, and becoming aware of cognitive biases; CIA analysts receive four months of training on critical thinking, writing, and briefing when they enter the organization and more as they progress through their careers.[27] Some retired CIA analysts have become Independent Contractors and offer similar training that could be tailored to a company's products. The following is a list of good books on intelligence analysis written by former senior CIA analysts.

- Psychology of Intelligence Analysis is written by Richards J. Heuer, Jr. and covers

cognitive biases and Structured Analytic Techniques;[28]

- Analyzing Intelligence: Origins, Obstacles, and Innovations is edited by Roger Z. George and James B. Bruce and discusses methods for improving analysis;[29]
- Intelligence: From Secrets to Policy is written by Mark M. Lowenthal, a former Assistant Director at CIA, and focuses on analyzing the significance of a topic for a customer and specifically covers cyber security and cyber intelligence;[30] and
- The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving is written by Morgan D. Jones to simplify problem solving and decision-making.[31]

All four books are available electronically for free (links are in the endnotes). Information about how to conduct intelligence analysis, as well as some declassified examples of old reports, also is available in CIA's peer-reviewed academic journal, *Studies in Intelligence*.[32] According to former Principal Deputy Director of National Intelligence and CIA analyst Susan Gordon, "Intelligence is about colloquially knowing the truth, seeing beyond the horizon, and allowing the leaders to act before events dictate. . . . It is about having a tradecraft around being able to deal with fundamentally uncertain information with certainty."[33]

(6) Draft outline of report

After selecting a topic for a report, but before writing the full paper, an analyst should select the paper format, such as described in Step 2 (Cyber Intelligence Reporting), and draft a short outline. The outline should have one key, tentative assessment per paragraph, which should consist of one to two sentences each. Beneath the assessment, in bullet format, the analyst should list supporting evidence. If possible, these assessments should include actionable recommendations for the company's leadership.

(7) Hold brainstorm

Strategic Analysts should hold a brainstorm with relevant parties to ensure that all pertinent information is considered before an assessment is finalized. For instance, Technical Analysts might be aware of technical details that could change or augment an assessment. In advance of the brainstorm, the analyst should send his or her outline to stakeholders so that attendees come prepared with additional information. These stakeholders include a broad range of colleagues, including Technical Analysts, Data Scientists, SOC officers, Collection Coordinators, risk management officers, and lawyers.

The brainstorm itself should be limited to 30 to 60 minutes, offering other experts an opportunity to share data and debate—and potentially adjust—the tentative assessments. A few minutes at the end of the brainstorm should be devoted to updating Specific Intelligence Requirements. Attendees should discuss and highlight key information gaps that could confirm or change their assessment. Often, these key gaps should be incorporated into the paper itself, using language such as, "This assessment would change if we were to uncover that . . ." because leaders probably would benefit from understanding the limitations of available data.

If not in attendance, gaps should be relayed to Collection Coordinators for further collection. Obtaining information that fills such gaps also could become the basis of writing subsequent reports, such as to inform leaders that analysts have higher confidence in their assessment or are modifying their assessment based on new data.

(8) Write report

With preapproved assessments and key supporting data listed in the outline, writing the report should be straightforward. As mentioned in Step 2 (Cyber Intelligence Reporting), each sentence that contains any analysis should also include the assessed likelihood of that conclusion (using estimative language or confidence levels), with the following ranges from high likelihood to low likelihood: almost certainly, probably, possibly, might.[16] For instance, "China **almost certainly** will launch [malware] against our company within the next week," or "Russia **might** try to exploit [vulnerability] against [critical asset]." Each piece of supporting data should be described and cited so that customers could locate and review the original data source. For instance, "In January, our antivirus platform detected [malware] installed on several administrator's computers, **according to a review of [antivirus] logs on [date].**"**[log citation]**

Analysts should seek to add graphics, such as maps, link charts, or pictures, to augment or simplify the content and draw or maintain readers' attention. For instance, when writing papers for Technical Analysts, Strategic Analysts could include a graphic evaluating an adversary using the MITRE ATT&CK framework.[34]

(9) Coordinate report with colleagues

Other stakeholders, such as those who attended the brainstorm, should have an opportunity to review the report before it is sent to management. The US Intelligence Community often holds a "coordination period" in which an analyst emails a paper to other analysts and offers them a

certain time period, which depends on the immediacy of the report, to review and comment on the piece.[35] For papers with a 24-hour deadline, the coordination period is often only two hours long; for papers with a one-week deadline, the coordination period could be one or two days. Coordination is useful because other stakeholders might be aware of a supporting piece of information that was released while the author wrote the report or might request rewording of an assessment to better reflect technical data. Because of the brainstorming step, the coordination review should be efficient.

A risk of not holding a brainstorm previously is that analysts might need to rewrite the entire paper if colleagues produce data contradicting the core assessments. If some officers firmly disagree with the main assessment—which should become clear during the brainstorm—the authors could add a short "dissent" or "alternative analysis" at the end of the piece, explaining the differing interpretation and some of its key supporting information.
We also recommend coordinating and/or brainstorming on briefing slides with other stakeholders, particularly when the briefing will be on a topic not previously reviewed by colleagues to prevent providing outdated or inaccurate information to leadership.

(10) Request managerial review

After the stakeholders have agreed on the content of the report, management should review it for two primary reasons. First, managers should ensure that customers' perspectives are considered. For instance, managers might attend meetings with senior leaders and understand how to frame the report in a certain way to better address leaders' concerns or explain the information such that its applicability to an upcoming decision is clearer.

Second, managers should edit the paper for grammar. A *Style Guide* written by the CIA in 2011 is publicly available[11] and could be used to standardize grammar; poor grammar could distract customers or confuse readers about the underlying message. If a manager has too many responsibilities to also edit papers, the company could hire an editor focused on ensuring high quality and consistency across products, such as the Analytic Tradecraft Expert described in Step 8 (Staffing a New Cyber Threat Intelligence Team).

A company's Strategic Analysis Workflow might include a series of individuals who review papers, particularly those written for senior leaders. The PDB typically requires at least five managers to edit a paper, with some editors conducting multiple revisions. A best practice is to

carbon copy (cc) all individuals who previously reviewed the piece when sending back edits so that the others can learn from the changes, making editing future papers more efficient.

(11) Publish

Once all requisite individuals have reviewed a report, it should be published via a mechanism internal to the company. If the company has an editor, that editor could lead this process. Publication could include a variety of steps, such as assigning a number to the report so that it could be easily referenced in future papers. Additionally, reports should be assigned a classification (e.g. Confidential) that dictates the level of sharing for that report, derived from the sensitivity of the information, considering proprietary, legal, personnel, or other restricted data.

(12) Disseminate

After publication, the paper should be disseminated (e.g. posted in a shared knowledge management database and emailed) and made available to relevant individuals in the company. The company might also seek to share some reports with external bodies, such as law enforcement or ISACs. The individual who is responsible for distributing the paper, both internally and/or externally, should be identified, have clear procures, and receive authorization from senior leaders to ensure that the paper is sent only to appropriate customers.

After completing the full cycle, analysts should note any significant intelligence gaps that they identified during the process and add them to the team's Specific Intelligence Requirements as discussed in Step 5 (Intelligence Requirements Process). Analysts should work with Collection Coordinators to increase collection on those topics.

Getting Started

The team's manager should consider arranging training opportunities for new analysts on the cyber threat intelligence team to learn core critical thinking, writing, and briefing skills and best practices. This training could vary in duration, and we recommend that a company choose a program that is approximately one month long, and possibly broken into different segments, due to the complexity of producing sophisticated analysis. The core training could be offered twice a year as a company starts staffing the team. Over time, the team could add more advanced training classes, such as detecting denial and deception activities, such as those used in false flag cyber operations. More information about training is available in Step 8 (Staffing a New Cyber Threat Intelligence Team).

Ideally, the instructor—possibly an Independent Contractor—should have experience teaching for a problem similar to the Career Analyst Program of CIA's Directorate of Analysis (formerly Directorate of Intelligence); that curriculum is directly transferrable to a private company's cyber threat intelligence team. The same instructor could also train managers, editors, or publication staff on editing, publishing, and disseminating reports. Alternatively, a company could hire a former, or retired, CIA or Intelligence Community analyst as a part-time employee to fulfill these duties. The team's Analytic Tradecraft Expert referenced in Step 8 (Staffing a New Cyber Threat Intelligence Team) also could fill this role.

Short-Deadline Products

When faced with a breaking issue (e.g. a major geopolitical event), a cyber threat intelligence team might receive pressure to provide an update to leadership before completing the entire Strategic Analysis Workflow. We highly recommend pushing back on leadership and not providing any briefings or products until the assessments are fully vetted by all stakeholders and management. Not only is it unlikely that analysts could produce long, detailed papers within one day for senior leaders, but frequent, unexpected overtime is likely to burn out Strategic Analysts and possibly the manager or other individuals who stay late to review the papers; the team's goal should be to complete tasks, including writing reports, only during standard eight-hour business days.

A worst-case scenario is that an analyst might quickly review readily available information, make an initial assessment, and share it with leaders but further analysis and coordination disproves that assessment. In such a case, leadership might have already acted, based on the inaccurate analysis, further endangering the company or wasting funds. Furthermore, this type of experience—even if an anomaly—probably would undermine leadership's trust in the intelligence unit, reducing leaders' confidence in the team's future products.

One solution for handling short-turnaround taskings from leadership is to provide two fully coordinated products with different levels of detail, one within 24 hours and a second within one week. For instance, analysts could provide a short, high-level product to leaders within one day. The format could be one paragraph comprising a primary, general assessment (BLUF) and a few key pieces of data supporting that assessment in bullet format. Analysts should complete the full Strategic Analysis Workflow (including brainstorming and paper coordination) for that initial

product to ensure consensus with their top-line assessments. Because the product is short, the process should be relatively fast. It should be acceptable for analysts to note their lack of certainty, particularly if they plan to conduct a more thorough review, by including language such as, "we **tentatively** assess that . . ."; "the adversary **might be** China"; "with **low confidence**, we assess that . . . , **although** . . . ".

If analysts cannot agree on a particular assessment, instead of compromising or picking one assessment that might be incorrect, authors should include all feasible assessments in the summary product to inform leadership that the issue is complex and requires more time for additional analysis. The paper's language could include, "While the **majority** of analysts assess . . . , **some** analysts assess . . . **because** . . . ".

In addition to producing a short-turnaround, high-level paper, analysts could provide a more detailed product for leaders (e.g. one to two pages) within one week. This paper also should proceed through the full Strategic Analysis Workflow but allow more time for research as well as coordination to resolve any analytic differences. As explained in depth in Step 2 (Cyber Intelligence Reporting), each assessment in the paper (BLUF) should list a few supporting pieces of data or, if analysts have low confidence in the assessment, some contradicting information. Additionally, the paper should note intelligence gaps or scenarios that could either strengthen or alter the top-level assessment.

It also is important to set expectations for these timelines with leadership during discussions described in Step 1 (Leadership Involvement). For instance, the cyber threat intelligence team's manager should explain to senior leaders that there is a tradeoff between time and complete, thorough analysis. The manager could explain that because the team always takes the time necessary to complete the full Strategic Analysis Workflow, the products that the leaders receive will always reflect the comprehensive expertise of all relevant analysts and officers throughout the company. Managers should agree on standard deadlines for papers of a certain format or detail, and the cyber threat intelligence team should not reduce quality but instead shorten the length of the paper to meet those deadlines. Over time, the company's leaders should develop more confidence in the team's products because the papers were vetted both horizontally and vertically across the organization, rather than receiving assessments that could change significantly because they were hastily analyzed and written.

Recommendations for Improving Performance

Incorporate Structured Analytic Techniques

Much scholarship has been published on various types of cognitive biases and predilections, and it is important for Strategic Analysts to be aware of and counter such commonplace critical thinking issues. Structured Analytic Techniques were designed by CIA to help analysts to analyze data objectively. It is a best practice to conduct Structured Analytic Techniques on topics that are especially important to the company or that are unusually complicated, such when analysts disagree significantly or new, credible information contradicts a previous assessment. A brainstorm is one type of Structured Analytic Technique because it invites more perspectives than just the author's, but brainstorms probably would not prevent groupthink. A more objective Structured Analytic Technique is an "Analysis of Competing Hypotheses" (ACH), which is used to identify the least likely scenarios (hypotheses) based on available data. Another type of Structured Analytic Technique that leaders and corporate risk management officers are likely to deem valuable is High-Impact/Low-Probability Analysis, which generates low-probability scenarios that could have significant impact on the company.

The team could hire consultants to provide training on Structured Analytic Techniques and other analytic methods, which are excellent opportunities to improve the team's sophistication of analysis. CIA's thorough backgrounder on Structured Analytic Techniques with examples is available online.[36] A detailed book, written by retired CIA analysts Richards J. Heuer, Jr. and Randolph H. Pherson, is Structured Analytic Techniques for Intelligence Analysis and is available for free download (links are in endnotes).[37]

Hire Editor

As previously mentioned, hiring an in-house editor could make report production more efficient. The editor would review grammar and then publish and disseminate reports. If the team hired an Analytic Tradecraft Expert, that individual could edit; train the team on critical thinking, writing, briefing; and run SAT exercises.

Expand Topics

We recommend that a cyber threat intelligence cell initially research only adversarial nation states and a company's critical assets. Over time, the cell should seek to hire additional analysts

to cover additional topics, such as threats to the company's supply chain, criminal groups, insider threats, physical threats, and emerging technologies that could impact the company's network. The order in which other topics are adopted should be consistent with the company's risk management evaluations and leadership's most significant concerns.

Add Customers

Some papers written by a cyber threat intelligence team would be of interest to entities outside the company, such as to law enforcement, the US Intelligence Community, ISACs, vetted partners that adhere to sensitive reporting guidelines, or trusted cyber intelligence vendors. A next step would be to identify certain types of reports that could be shared with other entities and set up appropriate mechanisms, including classification and dissemination systems. An additional step would be to invite other organizations to participate in the coordination process (e.g. brainstorms or paper coordination) so as to enrich the company's analysis with additional data and expertise.

Separate Strategic Analysis Team

According to SEI's review of cyber threat intelligence teams in private industry, it is a best practice for high-performing companies to separate strategic analysis from other types of analysis to ensure that Strategic Analysts are allowed to focus on big picture topics rather than ongoing cyber incidents or other cyber security tasks.[2] Furthermore, having a separate team encourages a company to hire an adequate number of Strategic Analysts, rather than requiring a couple of analysts to cover such a broad range of topics that the analysts cannot build deep expertise. This concept is reflected in the "Dream Team" scenario listed in Step 8 (Staffing a New Cyber Threat Intelligence Team)

Conclusion

The Strategic Analysis Workflow mirrors the US Government's Intelligence Cycle, pictured in the Team Workflow section, in that the cyber threat intelligence team identifies information gaps, analyzes potential emerging trends or future cyber threats, provides leaders with assessments of the cyber threat landscape to inform decision-making, and disseminates assessments to pertinent customers. The basic process should be: identify Intelligence Requirements; collect, record, and synthesize data; select a topic for a report; analyze data, prepare outline of a report, and hold a brainstorm with other stakeholders; write the report and coordinate it with stakeholders; request managers review the report; and publish and disseminate

the report.

In addition to instituting a clear process, it is important to set expectations with leaders on the turnaround deadlines for specific types of products and ensure that the process is streamlined to meet those timelines. Over time, the team should focus on establishing consistency across products and authors, building the sophistication of the team's analysis, and expanding its topics and customer groups.

Step 4: Technical Analysis Workflow

Overview

Leaders periodically will need to make quick decisions on issues pertaining to cyber activities and operations. Some of these decisions almost certainly will rely on various technical assessments, such as vulnerability scan reports, network logs, malware samples, or adversary methodology reports. Each of these types of detailed assessments fall under the broad umbrella of technical analysis.

Technical analysis uses specialized data about cyber activities to make assessments on threats relevant to organizations. The mission of technical analysis in companies typically is to inform cyber security actions and operations and to assist in the decision-making process on topics related to cyber hygiene, cyber security, or incident response.[2] However, across industries and organizations, the responsibilities of Technical Analysts on cyber security and cyber threat intelligence units is likely to vary significantly. We are cognizant of these differences and offer examples of two different ways that technical analysis could be performed for a company's cyber threat intelligence team. For such a team, we recommend that Technical Analysts's primary goal should be to inform Strategic Analysts, who write strategic papers for policymakers. In doing so, Technical Analysts conduct detailed technical analyses on the topics listed in the team's Intelligence Requirements.

We encapsulated the concept that technical analysis roles typically are fluid in our Technical Analysis Workflow. The cyber intelligence team's technical analysis should depend on the specific data gathered and analyzed by the company's other units performing technical analysis. Accordingly, organizations would need to define a repeatable Technical Analysis Workflow specific to their cyber threat intelligence team.[2] This workflow requires that a cyber intelligence team define clear expectations of roles, responsibilities, and timelines with the goal of providing pertinent analysis quickly.

Scope

To deliver valuable and actionable analysis to Strategic Analysts and leadership, the Technical Analysis Workflow requires that Technical Analysts possess a range of technical skills and obtain a variety of threat-specific data. To help determine the responsibilities of a Technical Analyst on a cyber threat intelligence team, technical analysis could be divided into two

categories: tactical analysis and operational analysis, which are described in depth below. The structure of a company's cyber environment—such as any technical gaps that need to be filled—could determine whether the cyber threat intelligence team provides tactical and/or operational analysis.

Tactical analysis includes examining specific threats, vulnerabilities, incidents, attacks, or unusual activity based on information typically collected by a SOC.[2] This analysis assists in decision-making for incident response, network defense, and protecting computers associated with the organization's cyber security. Decisions on threats requiring tactical analysis usually require analysts to respond to leaders' questions in a short timeframe, such as within minutes, a day, or occasionally a week.

On the other hand, operational analysis involves identifying and researching specific threats, threat actors, and threat actor campaigns—projects that probably are longer term and are more anticipatory than reactionary.[2] This includes assessing relevant threat actors' intentions and capabilities and whether their cyber operations could impact the organization or industry. Operational analysis uses the priorities set in Step 5 (Intelligence Requirements Process) and Step 6 (Threat Prioritization Process) of creating the team. One product employing operational analysis that Technical Analysts could produce for the team is a "Threat Profile" that includes assessments on threat actors primarily derived from technical data. Threat Profiles are a venue for a cyber threat intelligence team to record information on adversaries' tactics and infrastructure and allows Technical and Strategic Analysts to note changes in adversaries' methodologies over time. Threat Profiles also could become the basis of strategic papers written for leaders interested in details on specific cyber actors. A sample Threat Profile is provided in Appendix E. Technical and Strategic Analysts should collaborate closely to identify other opportunities for joint projects for policymakers.

We provide a sample Threat Analysis Workflow below, for which we integrated both tactical and operational analysis. However, we reiterate that a cyber threat intelligence team should customize its workflow based on whether either function is already fulfilled by other units, such as the SOC. To be effective, the team would need to consistently collect the technical data necessary to sustain technical analysis. Additionally, as previously mentioned, this workflow focuses on protecting a company's critical assets and actively identifying threats from nation-state adversaries to an organization.

Industry Best Practices

Establishing an expedient Technical Analysis Workflow requires a sufficient understanding of current threat intelligence techniques and the advantages of frameworks used in industry. Some well-known frameworks for threat intelligence provide organizations with guidelines on collecting, processing, and identifying potential attacks and adversaries. The two frameworks outlined below offer detailed methods of how attackers think, operate, and persistently threaten organizations using cyber operations, helping defenders to better anticipate vulnerabilities and attacks. These frameworks complement our Technical Analysis Workflow by assisting analysts to identify potential threats from nation-state adversaries and to critical assets.

Lockheed Martin Cyber Kill Chain

First implemented in 2011 by Lockheed Martin, the Cyber Kill Chain is a threat intelligence framework based on the "kill chain" military concept of deconstructing an attack into stages.[38] This distinction of stages assists an organization's defenders in identifying possible attacks and generating corresponding mitigation strategies or countermeasures to build a defense-in-depth model. Specifically, the Cyber Kill Chain decomposes a cyber attack into seven stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions and Objectives.

The MITRE ATT&CK™ Framework

The ATT&CK™ Framework provides a matrix of cyber threat actors' tactics, techniques, and procedures that analysts could use to describe adversaries and their behaviors.[34] This framework not only complements, but also builds on, the Cyber Kill Chain. If an organization were attacked, its analysts could use the ATT&CK™ Framework to distinguish specific indicators from the operation that they could then use to identify possible perpetrators. The matrix also could be customized for specific platforms, including Windows, macOS, Linux, AWS, GCP, Azure, AzureAD, SaaS, and Office365 platforms.

The MITRE ATT&CK™ Framework for Enterprises identifies 12 unique tactics used by adversaries: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact.

For each of the tactics, MITRE defines various techniques that adversaries could use in a cyber operation, and in some cases provides examples of procedures that cyber actors have employed, such as types of malware sets or other actions leveraging the technique. Additionally, MITRE maintains a repository of tactics and techniques commonly used by particular threat actors, allowing analysts to correlate from behavior to adversaries. This framework could be used by Technical Analysts on a cyber threat intelligence team, incident response teams, or SOCs to identify adversaries or record details of a cyber operation.[34]

Two Variations of Technical Analysis

As mentioned above, we acknowledge that each company has a different structure of cyber security teams. The responsibilities of a SOC in one organization might be dispersed across various components or teams in another organization. For instance, some companies might have an independent vulnerability management or analysis team that collaborates with a SOC, whereas that role might be part of a SOC's duties in another company. We assume that for most organizations, the full range of tactical analysis as described above is performed in its SOC, and those functions do not need to be replicated in its cyber threat intelligence team. However, the cyber threat intelligence team probably would have technical analysis requirements that a SOC could not fulfill. It is important that each company review its tactical and operational analysis capabilities, determine whether it needs one or both types within its cyber threat intelligence team, and then establish an appropriate Technical Analysis Workflow. We define two possible scenarios for a cyber threat intelligence team's technical analysis as only-op technical analysis and tac-op technical analysis.

Only-Op Technical Analysis

A cyber threat intelligence team with only-op technical analysis would incorporate operational analysis exclusively. It would have entirely different responsibilities than the organization's SOC, which traditionally performs tactical analysis; the organization should have other teams with defined processes to examine ongoing cyber activity, threats, vulnerabilities, incidents, and attacks and that also collect information necessary for the cyber threat intelligence team's op-only technical analysis.

Technical Analysts performing only-op technical analysis would focus on identifying potential threats, threat actors, and threat actor campaigns as well as threat actors' tactics, techniques, and procedures. In doing so, they should collaborate with Strategic Analysts, answer Intelligence

Requirements, and determine relevant threats to an organization, with the goal to inform senior-level decision-making. In this scenario, Technical Analysts on the cyber threat intelligence team should communicate with other teams in the organization that perform tactical analysis or cyber security functions to procure data.

Tac-Op Technical Analysis

Another scenario is that a cyber threat intelligence team might incorporate both tactical and operational analysis. While tac-op Technical Analysts would still focus on identifying threat actors and tactics and answering Intelligence Requirements, they would also have responsibilities that are commonly conducted on teams like a SOC, Red Team, or Vulnerability Management Team. A cyber threat intelligence team with tac-op technical analysis should hire Technical Analysts with more tactical specializations, such as in malware analysis, reverse engineering, penetration testing, or vulnerability analysis.

Figure 9 outlines duties for both only-op and tac-op technical analysis:

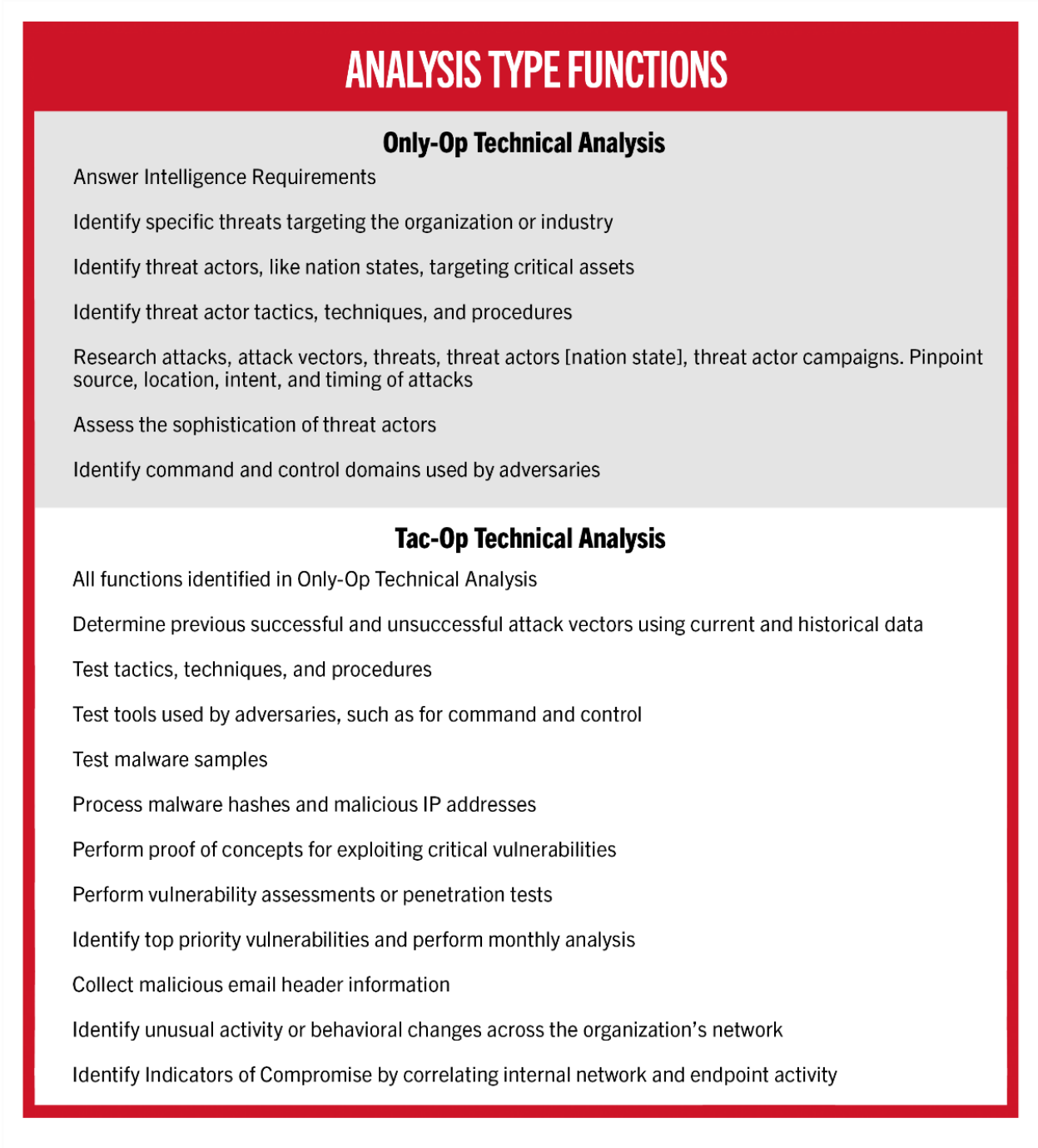

Figure 9. Responsibilities of two types of Technical Analysts

Sample Technical Analysis Workflow

This section provides a sample workflow for a Technical Analyst, as shown in Figure 10; the workflow could be applied to only-op or tac-op technical analysis. Having a Technical Analysis Workflow would assist the team in efficiently providing leaders with information for their

decisions. Depending on the team's type of technical analysis and the data being processed and analyzed, Technical Analysts might not only share assessments with Strategic Analysts but also with other teams, like the SOC. A Technical Analyst's goal is to identify and examine technical data to ultimately inform cyber security operations or strategic analysis for decision-making.

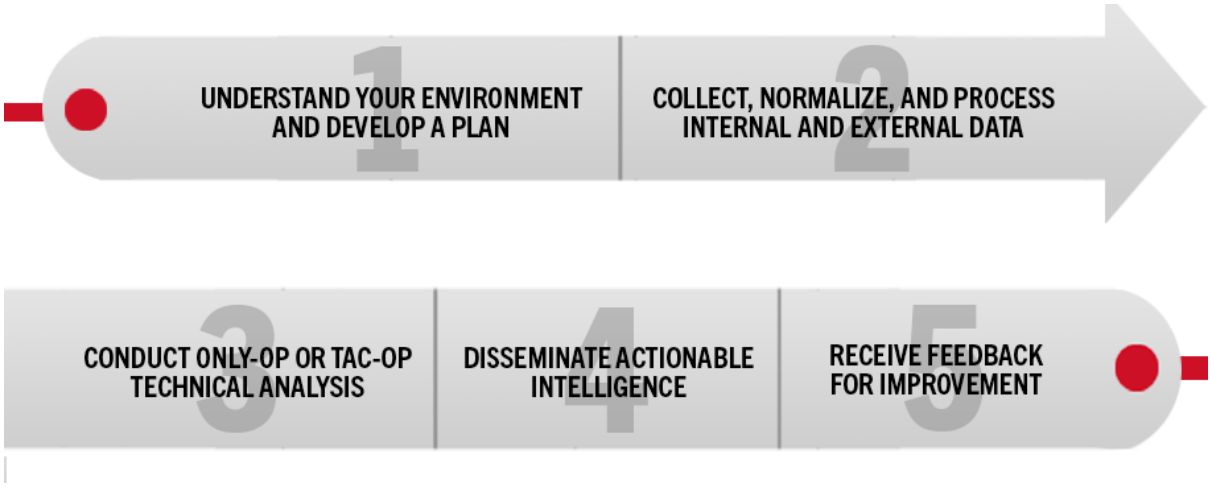

Figure 10. Recommended Tactical Analysis Workflow

(1) Understand your environment and develop a plan

First, Technical Analysts should identify specific projects, based on the topics generated from Step 5 (Intelligence Requirements) and Step 6 (Threat Prioritization Process). Technical Analysts should ensure that their projects align with business needs and coordinate with Strategic Analysts. For example, if a Strategic Analyst is working on Advanced Persistent Threat (APT) 10, a Technical Analyst might also concentrate on APT10 throughout one iteration of this workflow. Technical Analysts should also identify indicators to monitor and establish procedures in case those indicators are flagged, such as to identify emerging cyber threats.

(2) Collect, normalize, and process internal and external data

In the second phase, Technical Analysts should acquire internal and external data related to the project identified in the first phase, probably with assistance from the team's Collection Coordinators. Information that Technical Analysts could collect includes internal organization data, external technical data, and external open-source reports as detailed in Figure 11. Analysts would identify the types of information to gather, obtain that data from Collection Coordinators and/or organization's cyber security teams, normalize the data to analyze it more efficiently, and process the data. The type of information that a Technical Analyst would need depends on

whether he or she is performing only-op or tac-op technical analysis. For the former, Technical Analysts should liaise with their company's SOC to retrieve pertinent internal data.

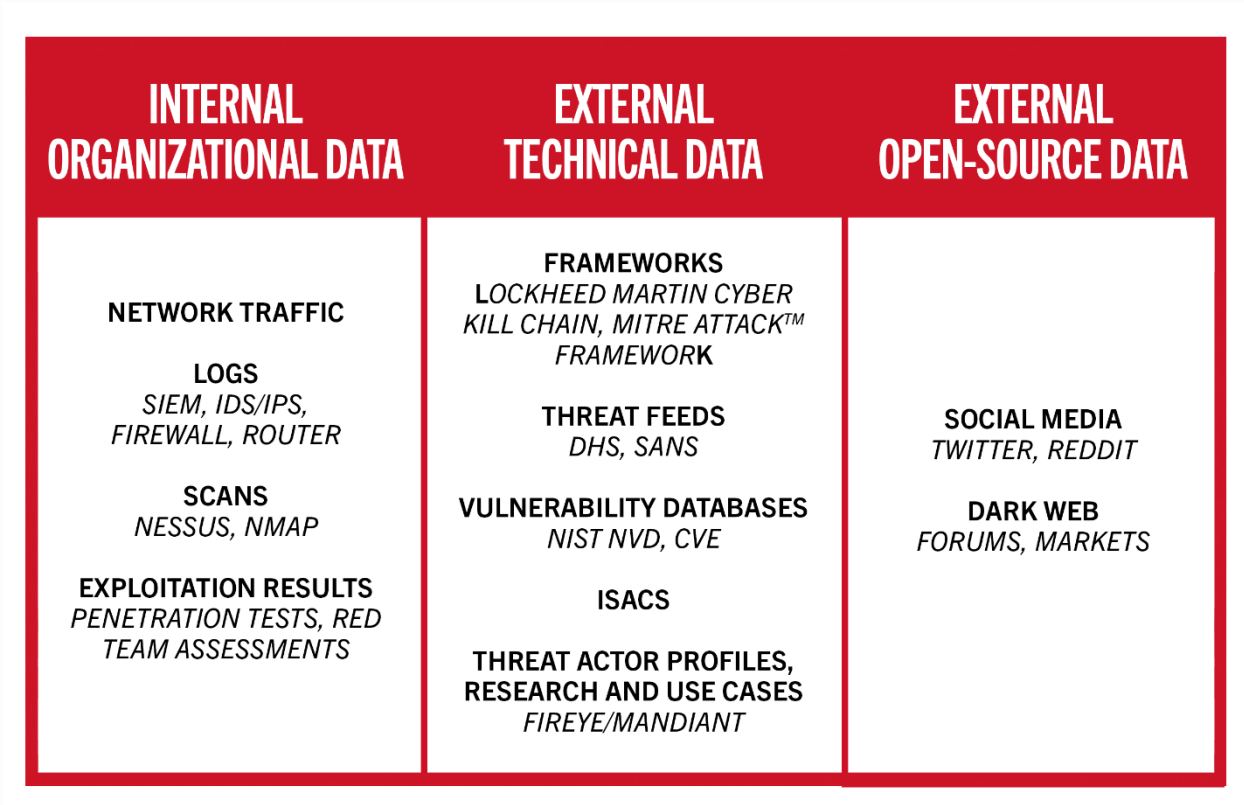

Figure 11. Technical information Technical Analysts should seek

Once this data is collected and normalized, it should be processed either manually or by using automation. There are many methods for processing data, and Data Scientists could help Technical Analysts to filter and sift through bulk data.

An example of this phase is that an organization might prioritize a list of vulnerabilities and then scan its workstations and network for those vulnerabilities monthly. Technical Analysts could automate scans of subnets, asset managers, and workstations and correlate the results to identify exploitable vulnerabilities. Another example is that Technical Analysts could extract malicious IP addresses from commercial threat feeds to which the organization subscribes, as outlined in Step 9 (Technology for Data Collection), and import them into intrusion detection or event management products to identify or alert on potentially malicious activity.

(3) Conduct only-op or tac-op technical analysis

Third, Technical Analysts should perform either only-op or tac-op technical analysis, depending on the type previously identified to be appropriate by an organization's cyber threat intelligence team. In either case, analysts should leverage the frameworks discussed above to thoroughly assess relevant data, attempt to identify the perpetrators of cyber operations, and produce technical intelligence for cyber security engineers or Strategic Analysts.[2]

As outlined above, only-op (only operational) analysis involves identifying and investigating specific threats, threat actors, and threat actor campaigns.[2] Specifically, only-op Technical Analysts should answer the Priority Intelligence Reports and Specific Intelligence Reports discussed in Step 5 (Intelligence Requirements Process) to assist senior leaders, such as the such as the CSO and CISO, in making decisions. To do so, only-op Technical Analysts should investigate and inform Strategic Analysts of attacks' sources, intents, motives, or timing. Technical Analysts should also prepare Threat Profiles on adversaries threatening the organization using both internal and external information, which Collection Coordinators could help obtain. Technical Analysts would compare processed data on cyber attacks, campaigns, and events to technical indicators collected on specific adversaries. Examples of information that Technical Analysts should review includes threat actors' attack vectors or common command and control platforms.

Tac-op (tactical and operational) analysis includes the functions outlined above for only-op analysis in addition to examining network, packet, or file ("tactical") data on specific threats, vulnerabilities, incidents, attacks, or unusual activity.[2] Tac-op Technical Analysts would compare a company's network and endpoint information to adversaries' "indicators of compromise," meaning certain pieces of data suggesting that a cyber threat actor is attacking or has attacked the company. Indicators of compromise include domain names, IP addresses, email header information, hash values, or malware signatures, each of which might be specific to an adversary. Analysts should examine tactical data to identify tactics, techniques, and procedures of potential threat actors[39] as well as those used in attacks against the company. Additionally, Technical Analysts should research the organization's vulnerabilities and be aware of the most commonly-used, successful exploits at that time. Analysts should understand opportunities for adversaries to attack an organization and suggest defensive measures and share their tactical assessments to appropriate cyber security units, such as the SOC, and operational findings to Strategic Analysts.

Differentiating between tactical and operational technical analysis would help analysts to identify their consumers, their responsibilities, and the types of decisions they should inform; both types are critical to an organization. Managers should provide guidance to Technical Analysts on the format and writing style of their assessments to ensure that their products communicate technical details effectively and clearly highlight actionable opportunities. Because Strategic Analysts and senior leaders receive Technical Analysts' operational analysis, such as their Threat Profiles, it should be concise, avoid using technical jargon, and directly relate to the organization's business processes.[2]

(4) Disseminate actionable intelligence

The next phase focuses on disseminating intelligence produced by Technical Analysts. After completing their analyses, Technical Analysts should determine the appropriate consumers, such as cyber security operations teams for tactical technical analysis or Strategic Analysts for operational technical analysis.

To retain knowledge and ensure consistency, Technical Analysts should record their operational analysis and key supporting data in Threat Profiles. These profiles would contain the **technical details** of important information, unlike the strategic papers written by Strategic Analysts for leadership. Threat Profiles should be shared with Strategic Analysts, and we recommend that Technical Analysts also meet with Strategic Analysts to verbally relay information in the Threat Profiles and answer any questions. Ideally, Strategic Analysts's reports for leadership would incorporate the Technical Analysts's overarching assessments, and Technical Analysts would attend brainstorms on paper outlines as explained in Step 3 (Strategic Analysis Workflow).

Technical Analysts must also determine deadlines for their analyses, which would affect the depth of their examinations. Frequently, cyber security teams would have short turnaround times for analysis. However, Strategic Analysts probably would have more flexible deadlines, such as from days to weeks. Furthermore, Strategic Analysts and leadership probably would find value in Technical Analysts conducting longer reviews of key adversaries' tactics and infrastructure, such as by updating Threat Profiles every year to highlight changes over time. Technical Analysts are responsible for determining the time sensitivity of their intelligence analysis.

(5) Receive feedback for improvement

Finally, because Intelligence Requirements are likely to change several times a year, it is critical

that Technical Analysts receive feedback frequently from Strategic Analysts, cyber security engineers, and incident responders. When requirements or priorities change, Technical Analysts might need to change projects, but the Technical Analysis Workflow should still hold.[39] The manager of the cyber threat intelligence team is responsible for establishing feedback channels with each of the Technical Analysts's consumers, defining efficient processes for receiving feedback regularly, and relaying the feedback to Technical Analysts. A feedback channel could be email, an organization's chat forum, online surveys, or in-person meetings.

Getting Started

Because we recommend that a company's cyber threat intelligence team initially focus on threats posed by nation-state adversaries and protecting its critical assets, the team would need to collect technical data appropriate for those two topics. For nation-state actors, this information should include details on their tactics, techniques, and procedures for cyber operations. Because some nation-state actors are likely to target a ocompany's critical assets, certain technical data would be pertinent for both topics. Overlaying a company's internal technical data on the MITRE ATT&CK™ Framework could help Technical Analysts identify the actors behind cyber attacks or identify common tactics used by cyber actors targeting a company. Additionally, Technical Analysts could use the Lockheed Martin Cyber Kill Chain model to anticipate other strategies and approaches that nation-state actors might employ to target the company. For example, Russia often uses phishing attacks to gain access to its targets, and phishing attacks "represent 90 percent of all sophisticated nation-state attacks,"[40] suggesting that a company's critical assets are likely to be targeted using phishing attacks. Technical Analysts should correlate intelligence from external technical and open-source data with a company's internal data.

The team should establish methods for saving and maintaining important data and Threat Profiles so that the team could refer to older data, which might contain additional information that Technical Analysts did not immediately recognize. To help institute such a process, Technical Analysts should determine whether the internal data on which it relies is collected by the company, such as its SOC. Technical Analysts should also seek opportunities to collect more internal data from the company's networks, such as IP addresses; subnets; infrastructure; or assets. It could consider acquiring additional data by conducting its own penetration tests or vulnerability management assessments.

Collecting relevant technical data from business units in the company probably would also be

beneficial. Technical Analysts and their manager should work with the team's Collection Coordinators to identify relevant information to obtain from business units. Such data might include other teams' threat feed findings, results of penetration tests, or lists of malicious domain names and IP addresses. Over time, coordinating collection efforts with other teams could be added to the Technical Analysis Workflow as discussed in Step 7 (Organization Information-Sharing Process).

Recommendations for Improving Performance

Incorporate Automation and SOAR Technologies

Depending on the size of an organization and the quantity of its assets, data processing is likely to be time intensive. Although it is common for Technical Analysts to manually process technical data, we recommend that they incorporate automation with Data Scientists' assistance. Companies interviewed by SEI claimed that automating technical analysis notably increased their cyber threat intelligence teams' performance.[2] With appropriate tools, most of the processing requirements in the Technical Analysis Workflow could be automated. For instance, writing a basic Python program to examine a company's internal data could save a Technical Analyst a significant amount of processing time, allowing the analyst more time to focus on analysis.

In addition to automating repetitive tasks, some high-performing organizations use Security, Orchestration, Automation, and Response (SOAR) technologies in technical analysis.[2] SOAR technologies integrate multiple cyber security tools, threat intelligence platforms, and various non-security tools into a single dashboard. SOAR has not only shown promise in automating data processing but also in executing tasks or identifying indicators of compromise. As a cyber threat intelligence team develops, we recommend it consider adopting SOAR technologies.

Conclusion

The Technical Analysis Workflow feeds into and mirrors the larger intelligence cycle in that it provides analysis to inform cyber security actions, operations, and strategic analysis; in this construct, technical analysis would inform leadership's decisions. We differentiate between only-op and tac-op technical analysis to help clarify the responsibilities of Technical Analysts on a cyber threat intelligence team, noting that that it should have a different mission than cyber security units. The workflow's core phases are to understand the company's environment and

create a plan, collect; normalize; and process internal and external data, conduct only-op or tac-op technical analysis, disseminate actionable intelligence, and receive feedback for improvement.

Step 5: Intelligence Requirements Process

Overview

A vast amount of information is available on the Internet, and a company needs to sift through large quantities of data to identify relevant intelligence. In coordination with Step 6 (Threat Prioritization Process), which ranks a company's most significant threats, setting Intelligence Requirements would help an organization to efficiently acquire information to answer its pressing questions. The utility of Intelligence Requirements hinges on the organization understanding its environmental context, such as its vulnerabilities.

Intelligence Requirements should drive a company's strategic and technical analysis, identifying specific topics and questions for analysts to research. We recommend having three levels of Intelligence Requirements, from broad to detailed: Executive Intelligence Requirements, Priority Intelligence Requirements, and Specific Intelligence Requirements. Publishing and regularly updating Intelligence Requirements would help a cyber threat intelligence team to focus on the company's greatest threats, resulting in a more proactive, business-driven posture.

Scope

As mentioned previously, to ensure that a new cyber threat intelligence team is successful and not overwhelmed, we initially limited the scope of this step to Intelligence Requirements pertaining to nation-state adversaries and protecting critical assets. Over time, the team could expand to other topics, such as supply chain threats, criminal groups, insider threats, physical threats, and emerging technology.

Much of this Intelligence Requirements section is derived from the best practices published by industry leaders, including SEI, MITRE, Recorded Future, and the System Administration, Networking, and Security (SANS) Institute.

Industry Best Practices

Intelligence Requirements are questions posed by a decisionmaker, manager, or analyst that could impact the future of a company. They serve as a baseline for the organization's collection plan. Collection Coordinators, as described in Step 8 (Staffing a New Cyber Threat Intelligence Team), typically are responsible for managing Intelligence Requirements, such as organizing

regular brainstorms to create and update Intelligence Requirements, finding data from a variety

of sources that could partially answer those questions, and providing that information to analysts. Strategic Analysts, and sometimes Technical Analysts, then seek to answer the Intelligence Requirements for leadership and relay their assessments in papers or briefings. It is important that the company create a formal process for identifying Intelligence Requirements that is reviewed periodically to ensure that the company's cyber threat intelligence team continues to assist decisionmakers.[41]

As proposed in SEI's *Cyber Intelligence Tradecraft Report*,[2] we recommend establishing as many as three tiers of Intelligence Requirements to address different levels of granularity. For instance, a broad Executive Intelligence Requirement could successively lead to a few Priority Intelligence Requirements, each of which could be further deconstructed into several Specific Intelligence Requirements. Many of these concepts are outlined in more detail in the SEI report, which draws from the US Intelligence Community's requirements process.

Executive Intelligence Requirements

Executive Intelligence Requirements are the broadest category of Intelligence Requirements and reflect the questions that a company's leadership and board have on threats and risks to the organization's mission, operations, and revenue.[2] These requirements are general and should be approved at senior levels, such as by the Chief Executive Officer (CEO) or President, to ensure that they accurately represent the company's current concerns. Because these questions are so comprehensive, they probably should be updated only once a year. Furthermore, because the questions are so extensive, Strategic Analysts are unlikely to write papers covering an entire Executive Intelligence Requirement and instead focus on subordinate questions, such as Priority or Specific Intelligence Requirements.

Examples of Executive Intelligence Requirements:

- What are the predominant internal and external cyber threats targeting our organization?
- What are the most significant cyber threats impacting our industry?
- Which nation states targeting our organization are the most capable?
- What might be the most significant cyber threats to our company in one year?

Priority Intelligence Requirements

Executive Intelligence Requirements should be broken down into Priority Intelligence Requirements, which are more detailed.[2] Priority Intelligence Requirements are concise questions that focus on a specific actor, event, or activity[42] and are intended to provide information to support a single decision. They should be approved by another senior manager—such as the CSO, CISO, or designated manager—and updated approximately every six months to maintain currency. Strategic Analysts typically write assessments to answer Priority Intelligence Requirements. As subject matter experts, Strategic Analysts could suggest new Priority Intelligence Requirements. Collection Coordinators should be responsible for obtaining approval from senior officers, often at biannual collection management meetings.

Examples of Priority Intelligence Requirements:[2]

- Which cyber threat actors are targeting—or might target—our organization's critical assets?
- What is a (particular) nation state's motives in targeting our industry?
- Is our company being targeted with phishing attacks? If so, which cyber actors are using this tactic and what types of employees are they targeting?
- Which of our critical assets is being targeted most heavily? What would be the impact if an attack were successful?
- Do we think a (specific) foreign country will target our company because of a (certain) geopolitical event?

Specific Intelligence Requirements

More detailed than Priority Intelligence Requirements, Specific Intelligence Requirements often are tactical and best answered by Technical Analysts in collaboration with Strategic Analysts. The manager of a cyber threat intelligence team should deconflict with the company's cyber security teams, such as the SOC, to determine which team takes the lead on addressing Specific Intelligence Requirements. Because the questions are so detailed, Collection Coordinators should arrange meetings to reevaluate Specific Intelligence Requirements roughly every two months. Technical Analysts across the company, as well as the cyber threat intelligence team, could propose Specific Intelligence Requirements, which should be approved by a mid-level manager.[2]

Examples of Specific Intelligence Requirements:

- Has a (particular) country conducted a specific attack against us within the past week?
- Were any of our critical assets attacked today?
- What is the command and control infrastructure used by a (specific) threat actor?
- Does our network have a critical vulnerability that was disclosed today?
- Did we observe any anomalies on our network this week?

Figure 12 demonstrates the correlation between Executive, Priority, and Specific Intelligence Requirements.

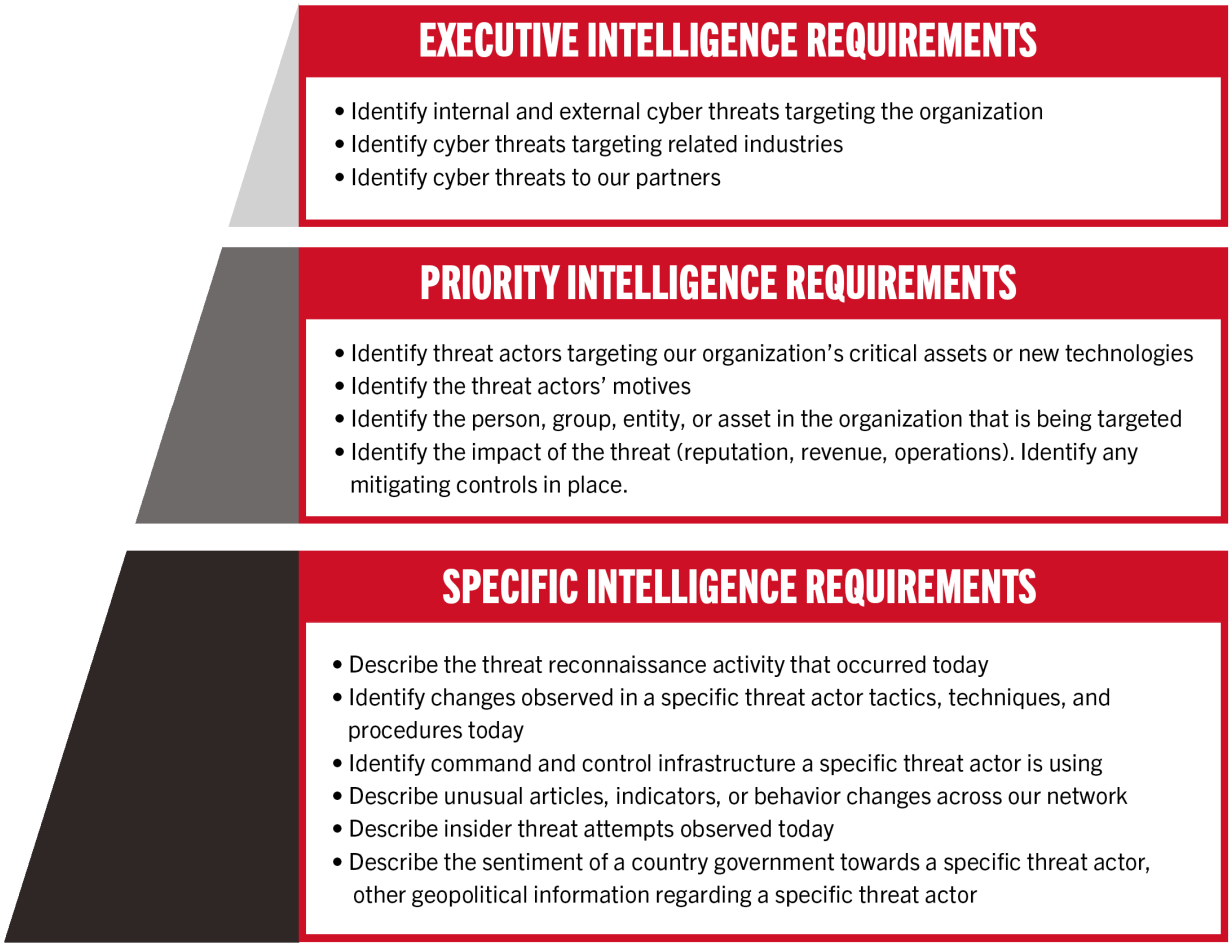

Figure 12. Intelligence Requirements selected from SEI's report[2]

A cyber threat intelligence team should establish procedures for three components related to Intelligence Requirements: drafting, monitoring, and updating Intelligence Requirements.

Drafting Procedure

The cyber threat intelligence team's Collection Coordinators should organize a separate meeting with all relevant, appropriate stakeholders for each tier of Intelligence Requirements.[43] The Collection Coordinators should guide the discussions to formulate questions whose answers could impact decisions made by senior leaders or other managers. Initially, these questions could focus the cyber threat intelligence team's initial scope, such as nation states and critical assets.

In brainstorming the first round of Intelligence Requirements, the Collection Coordinators could reference the DHS's Homeland Security Standing Information Needs as examples.[2] The Standing Information Needs provide a formal, structured framework of Intelligence Requirements on "all threats and all-hazards information needs of the U.S. Department of Homeland Security (DHS) and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners,"[44] suggesting that the team could use or modify some of DHS's Standing Information Needs for its own Intelligence Requirements.

Monitoring Procedure

The team should create a mechanism to track Intelligence Requirements, which the cyber threat intelligence team's Collection Coordinators and manager would maintain. The database should list all the approved Intelligence Requirements, state whether Collection Coordinators had obtained information on that topic and note whether the cyber threat intelligence team had published any reports addressing the requirement. SEI's survey of private companies revealed that numerous organizations did not have a centralized storage mechanism to track their Intelligence Requirements and often used emails instead.[2] Developing a database containing all the Intelligence Requirements also would help the manager and analysts prioritize their projects.

In addition to creating a database, we recommend that the cyber threat intelligence team create a version of an Organizational Intelligence Priorities Framework (OIPF) as outlined in *Intelligence Community Directive 204: National Intelligence Priorities Framework*.[45]

> ***"The OIPF informs future planning, budgeting, programming, and allocation of resources to data collection and analysis. The OIPF should be actively managed so that it reflects organization-wide stakeholder priorities, and the***

> ***entire OIPF should be reviewed quarterly. Organizations should consider imposing expiration dates on intelligence requirements to force reevaluation. To increase visibility, organizations should consider providing access to the OIPF to all departments that may be able to use it."***
> *- Cyber Intelligence Tradecraft Report, SEI*[2]

The cyber threat intelligence team's Collection Coordinators would be responsible for creating an Organizational Intelligence Priorities Framework, which should be scaled to the company's needs and limited to its predetermined scope.

Updating Procedure

To ensure that analysts are aware of leaders' priorities and are not focused on outdated issues, the team's Collection Coordinators should periodically organize meetings to update all three tiers of Intelligence Requirements using the timeframe guidelines provided above. Between meetings, Collection Coordinators should solicit and record suggestions from analysts and leaders. Many of these will come in the form of intelligence gaps, which should be discussed in brainstorms and noted in published reports as detailed in Step 3 (Strategic Analysis Workflow).[2]

Recommendations for Improving Performance

Because it is time consuming to track Executive, Priority, and Specific Intelligence Requirements across numerous topics and identify new sources of information for each, companies could create a collection management team to lead the entire Intelligence Requirements process. As explained in Step 8 (Staffing a New Cyber Threat Intelligence Team), we recommend that a new team initially hire only one Collection Coordinator. As the team adds analysts and Intelligence Requirements multiply, however, we recommend that a company devote a team—separate from the cyber threat intelligence team—to collection management. According to SEI's research, high-performing organizations often have a standalone collection management team.[2] That team would be responsible for the full Intelligence Requirements process, including coordinating, publishing, and finding information to address Executive, Priority, and Specific Intelligence Requirements. If possible, the collection management team also should record the rationale for each data source it collects and evaluate whether its information is accurate and credible.

Conclusion

Leadership priorities should be reflected in Intelligence Requirements, and in turn, Intelligence Requirements should drive an organization's strategic threat intelligence analysis. Having clear Intelligence Requirements would focus Strategic and Technical Analysts on the topics most important to the company and help them to sift through large quantities of data to identify relevant information. Establishing an Intelligence Requirements process is a critical step in creating an efficient cyber threat intelligence team.

Step 6: Threat Prioritization Process

Overview

There is no shortage of threat actors, and a cyber threat intelligence team has limited resources. Having a repeatable process that focuses on protecting an organization's most important assets against the most significant threats would enable companies to use their resources most efficiently. Prioritization helps to define Intelligence Requirements, focus a cyber threat intelligence team, and determine which reports to share with the SOC.

Scope

This section assumes that companies are aware of their network environment, including all its access points, the software used across the enterprise, and the vulnerabilities of its assets and networks.

Best Practices

An effective threat prioritization process should analyze asset value, threat actor potential, and an organization's vulnerabilities together, determining the threat actors most likely to target assets critical to an organization's function. We recommend initially prioritizing critical assets and nation-state actors separately to ensure that both topics have sufficient consideration. As described in Step 3 (Strategic Analysis Workflow), Functional Strategic Analysts could select their projects based on the ranked critical asset list whereas geopolitical Strategic Analysts could choose topics based on ranked threat actor list.

High-performing organizations use a repeatable process that is regularly reviewed by leadership to prioritize risk, ensuring that analysts work on the most meaningful threats. Companies could use frameworks such as MITRE ATT&CK, which was outlined in Step 4 (Technical Analysis Workflow) and catalogues the tactics, techniques, and procedures used by the most active APTs, to identify methods that a cyber actor might use to target an asset.[2] In our prioritization process, a company's risks are ranked by their likelihood of occurrence and impact; ideally, this criteria is quantitative and calculated using methods like those found in risk management frameworks such as OCTAVE Allegro or Factor Analysis of Information Risk (FAIR). The company's risk assessors would consider threat actors' tactics, techniques, and procedures in determining both probability and impact of cyber operations.[46]

In large organizations with mature information security risk management teams, threat prioritization is often driven by—or at least heavily influenced by—the risk management team.[47] As part of its core duties, the risk management team should have already determined the probable impact of an asset's security controls failing and is best postured to estimate the likelihood that its security controls will fail.[48] In addition to the risk management team, other entities who could participate in the Threat Prioritization Process are senior leaders, Collection Coordinators, and cyber intelligence; information technology; and information security teams.

Proposed Process

We recommend following the series of steps below to set up a Threat Prioritization Process that is repeatable and effective. Recognizing that conducting the Threat Prioritization Process for all of a company's assets would be a gigantic undertaking, instead, we propose that the company conduct its first prioritization process with only a few of its high-value assets. After completing the process once, and all participants understand their roles, the company could then expand its scope. We designed these steps to be used and integrated with the MITRE ATT&CK Framework, but other public frameworks also could be used to prioritize threats efficiently.

Below, we suggest four prioritization exercises. The first two exercises focus on prioritizing a company's critical assets, which should especially benefit the cyber threat intelligence team's functional Strategic Analysts. This third exercise focuses on prioritizing the company's cyber adversaries, which should benefit geopolitical Strategic Analysts. The fourth exercise merges the results from the first three exercises.

Step 1

A team of subject matter experts, asset owners, and managers should identify the company's key assets and highest-impact information security risks and produce a table listing assets and the potential impact to the organization if each asset were breached or shut down. This table is called the Assets and Impact Table, as detailed in Figure 13. Senior leaders should make the final decision on the assets' ranking in importance to ensure that the prioritized list aligns with organizational strategy.

ASSETS AND IMPACT TABLE

SUBJECT MATTER EXPERTS (SME)				MANAGEMENT
ASSET	ASSET FUNCTION	IMPACT OF ASSET FAILURE	VALUE OF INFORMATION IN ASSET (ASSET FUNCTION COLUMN)	ASSET IMPORTANCE SCORE
Identify assets; In the interest of time management, it is recommended that the team starts with assets they intuitively feel are high value.	Qualitative description of what information in contained with other accessible by a particular asset.	Consider failures of confidentiality, integrity, and availability.	This could be done quantitatively (using a sytem like FAIR) or a 1-5 rating.	This can be done based on the quantitative value of the asset, or Leadership can rank these based on a holistic understanding of how the asset supports the business goals of the company.

Figure 13. Assets and Impact Table instructions

Step 2

A group composed of asset owners, information technology, cyber security, information security risk management, and cyber intelligence employees should determine the most significant risks for each of the company's assets. Using the MITRE ATT&CK framework, they should determine the vulnerability for each asset that, if exploited, would cause the most damage. They also should list each asset's existing security controls for both hardware and software. This exercise should produce an Organization Exposure Table for each asset listed in the Assets and Impact Table, shown in Figure 14.

ORGANIZATION EXPOSURE TABLE

MANAGEMENT, RISK ANALYSTS, OR SMEs						
ASSET	HARDWARE ASSOCIATED WITH ASSET	SOFTWARE ASSOCIATED WITH ASSET	VULNERABILITIES ASSOCIATED WITH HARDWARE	CONTROLS FOR HARDWARE VULNERABILITY	VULNERABILITIES ASSOCIATED WITH SOFTWARE	CONTROLS FOR SOFTWARE VULNERABILITY
Take the assets from the Assets and Impact Table and populate this column with them (sorted by impact/priority) - multiple rows per asset may be required	Depending on the asset defined in the Asset column, evaluate the asset and determine what hardware makes up the asset.	Depending on the asset defined in the Asset column, evaluate the asset and determine what software is used by the asset	List any known vulnerabilities associated with the hardware identified (ie "CVE-2017-5754 / Meltdown").	What controls exist? It may be helpful to also think about the effectiveness of those controls	List any known vulnerabilities associated with the software identified	What controls exist? It may be helpful to also think about the effectiveness of those controls

Figure 14. Organization Exposure Table instructions

Step 3

The cyber threat intelligence team and company's cyber security entities should identify cyber threat actors who have targeted the company's industry, employ tactics; techniques; and procedures that could successfully exploit the weaknesses listed in the Organizational Exposure Table, and could be motivated to target the company. For simplicity, this overarching prioritization exercise should identify cyber adversaries only to specific countries; Intelligence

Requirements drafted from this table could include more detail like a particular cyber threat actor (e.g. APT10). The cyber intelligence team should create the Threat Actor Potential table with threats ranked by the likelihood that they have the capabilities and motivation to attack the company. The Threat Actor Potential table is described in Figure 15.

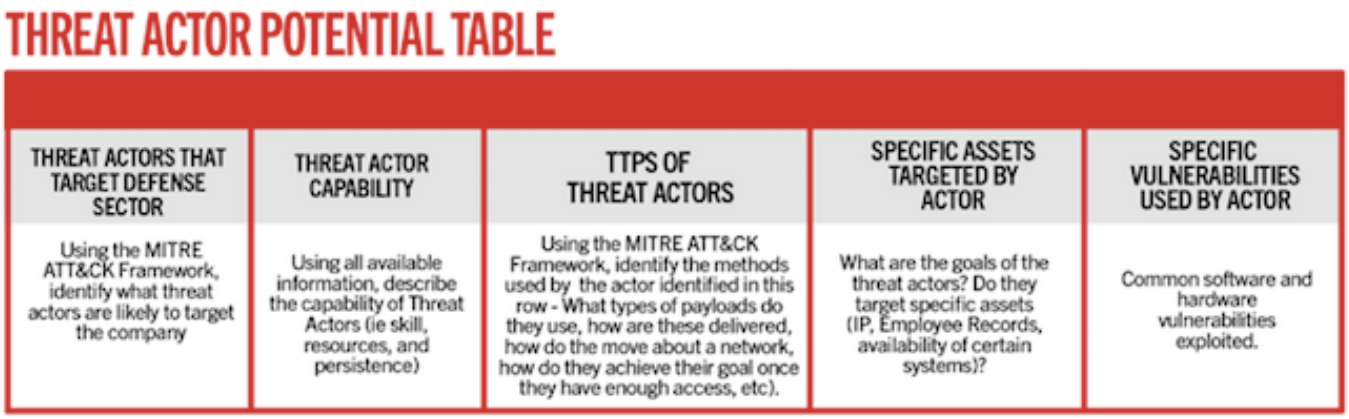

Figure 15. Threat Actor Potential Table instructions

Step 4

The cyber threat intelligence team should merge the Assets and Impact Table, the Organizational Exposure Table, and the Threat Actor Potential Table to form a comprehensive list of threats called the Threat Scorecard, which is not prioritized in this step. While this chart is organized by threat actors (i.e. countries), the chart also lists each asset's priority rank. Combining these tables into one scorecard would allow a company to understand the relationships between their most important assets and the most significant threats to those assets. Figure 16 shows how all three tables described in earlier steps feed into the Threat Scorecard, with a fictious example provided for clarity.

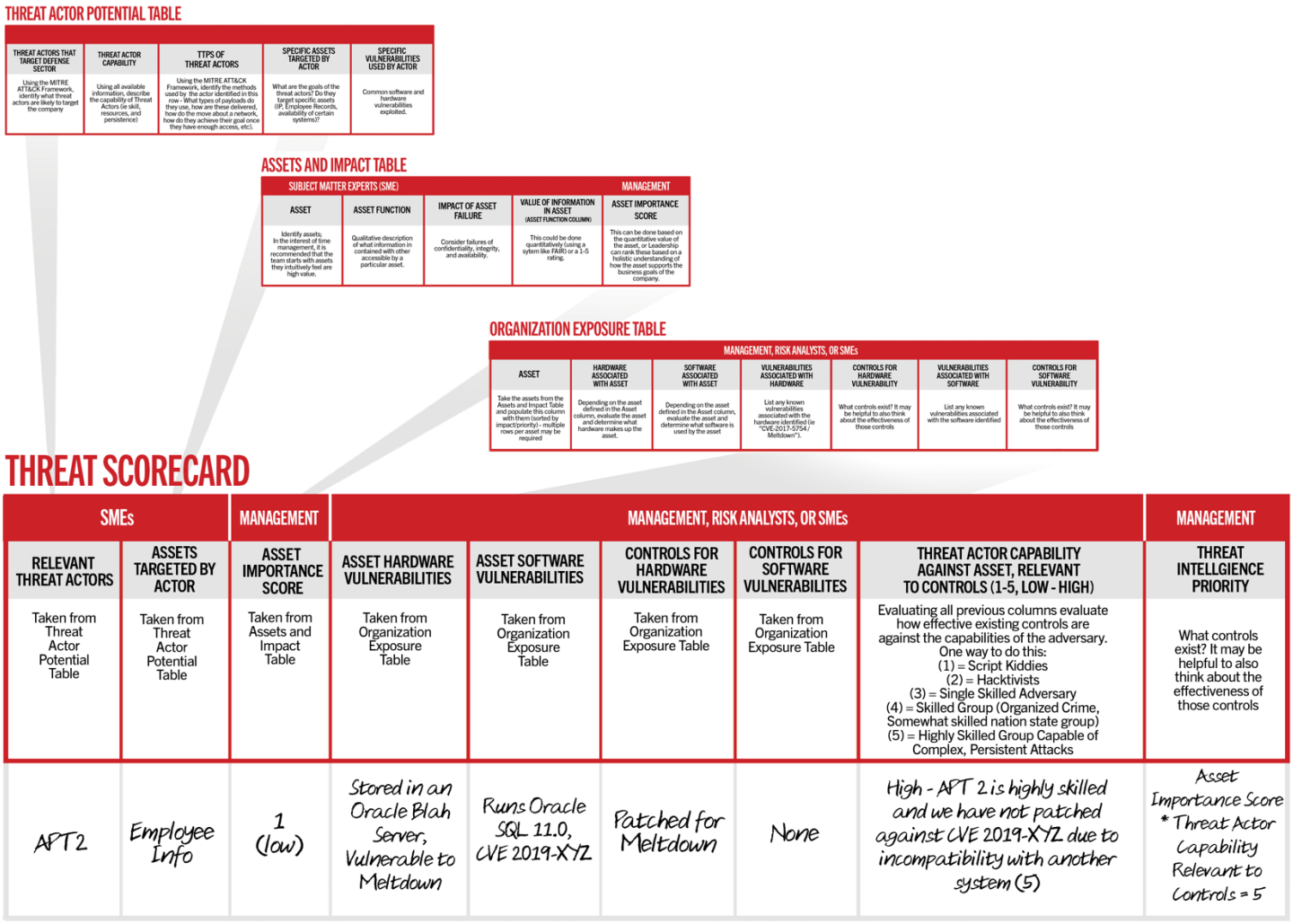

Figure 16. Threat Scorecard instructions

Step 5

The risk management team should prioritize the Threat Scorecard by combining the asset importance score with the estimated ability of all threat actors to target that asset, using a methodology such as OCTAVE Allegro. Alternatively, leadership could review the Scorecard and prioritize it according to business priorities.

Step 6

The risk management team should distribute the prioritized Threat Scorecard to stakeholders, such as the cyber threat intelligence team and SOC. The cyber intelligence team should use the scorecard to prioritize its intelligence collection, analysis, and production.

Recommendations for Improving Performance

The first time that a company prioritizes its threats using this process is likely to be long and resource intensive, but further iterations of the process should require fewer resources. The process could be improved in three ways: increasing the scope by looking at more assets and more threat actors, increasing the frequency of conducting the process, and improving the company's methods for quantifying threats. We recommend that organizations focus on expanding their scope until the cyber threat intelligence team's scorecard contains all critical assets within the organization. At that point, companies could improve the rigor of the scorecard by using more quantitative analysis for the inputs in the tables. Lastly, the company's goal should be to iterate this process regularly to incorporate emerging threats and new information. The Threat Actor Potential Table and the Organizational Exposure Table probably would need to be updated far more frequently than the Assets and Impact Table; the former should be updated roughly quarterly and the latter annually.

Conclusion

We provide a Threat Prioritization Process that is repeatable, customized to the business needs of an organization, and potentially quantifiable. Prioritizing threats requires coordination between information technology, information security, information security risk management, cyber intelligence, and management to ensure that the process supports the organization's mission. While the Threat Prioritization Process probably would require a significant investment of resources upfront, it would help the cyber intelligence team to focus on protecting the company's most important assets from the organization's most significant threats.

Step 7: Organization Information-Sharing Process

Overview

It is crucial for organizations to have both formal and informal processes for sharing information and analysis on protecting critical assets against nation-state threat actors. These processes establish a bi-directional method of exchanging information between organizations, government entities, and cyber security teams to actively prevent, protect, respond, and recover from the nation's largest threats. In a study on the evolution of cyber threat intelligence conducted by the SANS Institute, 95% of organizations who shared information both internally and externally reported substantial value gained during the process.[49] Benefits included acquiring timely and relevant threat information, developing contacts in related organizations, and improving security awareness. Through collaborative communication, a company should find opportunities to strengthen its abilities to collect relevant data, prioritize threats, and manage risks, adding tangible value to the organization's mission.

Scope

This process includes identifying data that could be shared within an organization and, separately, with external entities as well as instituting mechanisms to exchange information. We intended for this step to be generalized because information-sharing processes are highly dependent on an organization's structure and business practices. Furthermore, the types of organizations with which a company would share information is likely to vary across industries.

Best Practices

Identify Valuable Data

A company should initially establish information-sharing processes across its internal business units and later expand to external partners. The cyber threat intelligence team's manager, and possibly Collection Coordinators, should identify other teams within the company that collect information on internal networks, conduct cyber security, own information technology assets, and perform risk management. With each internal partner, the manager should identify specific, valuable information that the teams could exchange and institute formal procedures to regularly share data. Data sought by the manager might include network logs of detected cyber attacks or analyses of malware samples. In return, other teams might appreciate receiving the cyber threat intelligence team's weekly highlights or strategic analysis reports, particularly if the report cited data that they had provided.

Once the cyber threat intelligence team's manager has networked throughout the company, with leadership's approval, the manager and Collection Coordinators should consider contacting other organizations that might have information beneficial to the team. Primary goals of information sharing are to build relationships with other organizations and across sectors as well as to be proactive in protecting infrastructure, assets, and business goals.[2] External entities that are likely to share useful information include the US Government—such as federal, state, and local law enforcement, DHS, and the Department of Defense (DoD)—and ISACs and other industry partners. Additionally, other companies in the same industry might have been attacked by the same cyber actors and be willing to share their analysis on potential adversaries' tactics, techniques, and procedures. All information shared should be relevant and actionable.

Information sharing is most beneficial when organizations are transparent, and many types of data could be shared with internal and/or external customers. A company should be careful not to release information that is compartmentalized, however, and prevent sharing information that is classified or proprietary.[2] Information that could be exchanged includes, but is not limited to, the list in Figure 17.

Figure 17. Information to consider sharing with internal or external partners

Having a dedicated individual, such as a Collection Coordinator, oversee this process and draft information-sharing policies would help to ensure consistency and protect an organization's private information and critical assets. Ideally, an organization would have an entire collection management team lead the information-sharing processes both internally and externally.

Information-Sharing Models for the Defense Industrial Base

As an example, we investigated the defense sector for its information-sharing practices. Government organizations, specifically those within the DoD, are generally considered to have high-performing information-sharing processes due to multi-directional collaboration, use of federal resources and oversight, and their abilities to identify meaningful information. Defense industry entities and suppliers have excelled at collaborating with ISACs and other partners to enhance information sharing.

Peder Jungck, BAE Systems's Vice President and Chief Technology Officer emphasized the benefit of joining an ISAC. In a testimonial he stated,

> ***"Collaborating through [Information Technology] IT-ISAC provides an effective force-multiplier for us. Learning from each other enables everyone to more quickly adjust strategies and tactics. Plus, IT-ISAC's global network of members and partners provides us regular access to sensitive indicators. These trusted relationships also ensure that the information we share quickly reaches key communities so that they can protect their enterprises well."***
> - Peter Jungck[49]

Information sharing across companies varies; it depends on the data that each company collects and the industry. Many government organizations have reported considerable benefit from information-sharing resources, such as the DHS's free Automated Indicator Sharing (AIS) capability, the DoD's information-sharing program, and the National Cyber-Forensics and Training Alliance. Additionally, the National Council of ISACs comprises various sharing centers unique to specific industries and sectors. Below, we identified several programs and information-sharing resources that work specifically with members of the DoD and from which defense contractors could benefit significantly.

DIB-CS Program

The Defense Industrial Base (DIB) Cybersecurity Information Sharing Program (CS) is a voluntary, public-private cyber security partnership in which DoD and participants share information on cyber threats and mitigation and remediation strategies. The program provides a collaborative environment in which members voluntarily report cyber operations conducted against them as well as details on how to most effectively mitigate or handle those threats.

DHS AIS

The Department of Homeland Security provides an Automated Information Sharing capability in which organizations can receive and share cyber threat indicators that have been anonymized to maintain companies' privacy.

IT-ISAC

The Information Technology-ISAC's mission is to strengthen information security infrastructure through sharing information on cyber threats. It facilitates communication between members' SOCs and offers Non-Disclosure Agreements to promote exchanges.

ND-ISAC

The National Defense-ISAC offers defense industry entities and suppliers access to security data, high-performing tools and technology, and best practices. Through ND-ISAC, members share intelligence on cyber security, insider threats, vulnerabilities, and associated threat mitigation strategies. Members are provided with many opportunities to develop and continually mature the security of their enterprises. This specific ISAC has a collaborative environment and serves as the defense sector's primary focal point for all cyber threats. It also partners with the DIB-CS.

Proposed Process

Below are a series of steps to set up information-sharing processes. Although we recommend that a company eventually institute bi-directional processes for external information sharing, we assumed that a new cyber threat intelligence team would initially only **receive** applicable information.

(1) Define relevant business units

The cyber threat intelligence team manager should determine which internal business units

collect and analyze cyber information that could assist the cyber intelligence team. The primary unit probably is the company's SOC.

(2) Identify useful information

The manager should identify areas within these business units from which to acquire useful information. The cyber threat intelligence team should also communicate with other business units to solicit data on threats, vulnerabilities, and research relevant to the company's strategy to protect its critical assets against nation-state adversaries.

(3) Determine shareable data

The team's manager should clarify which of the team's data could be collected, analyzed, and disseminated to other internal units. This step would include identifying data that could be useful to other business units and considering what types of data could be shared across the entire company versus being restricted to only some.

(4) Establish contact

The manager should contact the selected business units to establish an ongoing communication channel on cyber security practices, technical analysis, and mitigation strategies. If possible, the manager should draft an information-sharing procedure or policy.

(5) Join external information-sharing centers

After networking internally, the cyber threat intelligence team manager or Collection Coordinators should join an external information-sharing program.

(6) Build team resources

The company should form a collection management team and designate roles and responsibilities for proactively engaging with internal teams and external programs, collecting information, and relaying relevant information to the cyber threat intelligence team.

Recommendations for Improving Performance

A company's information-sharing process should evolve with its cyber intelligence team. Over time, an organization would benefit from not only receiving relevant information but also providing it; the more information that a company gives, the more likely it will receive in return.

Organizations with a standalone collection management team are more likely to have successful internal and external information sharing, which would greatly improve the quality and accuracy of the cyber threat intelligence team's analysis.[2] Responsibilities of such a team also could include understanding an organization's cyber team structure, researching and locating new resources that might improve cyber intelligence analysis, and developing more efficient processes to send and receive information.

One of the most crucial tasks of a collection management team is identifying and sharing the right information. In high-performing organizations, Collection Coordinators on a collection management team review a company's internal data and reports to determine whether the information contains some type of threat pertaining to others, and if so, relays that information after evaluating it and removing proprietary or sensitive company data. Information evaluation, which could be done by either Collection Coordinators or analysts, includes rating information—called a confidence rating—for both reliability (" source reliability") and utility ("information content").[2] A company should not share information that has a confidence rating of less than average in either source reliability or information content; a lower rating indicates that the information's source is more untrustworthy than trustworthy or the information is not important or relevant. Figure 18 below is a sample rubric from the US Government that could be used to evaluate source reliability and information content; using letters for one scale and numbers for the other easily differentiates the two criteria.

SOURCE RELIABILITY EVALUATION CRITERIA		
A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot be Judged	No bias exists for evaluating the reliability of the source

INFORMATION RELIABILITY EVALUATION CRITERIA		
1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot be Judged	No bias exists for evaluating the validity of the information

Figure 18. Rubrics for information source and content

Conclusion

We propose the methods detailed above for information sharing, which we assess would ultimately benefit any company's cyber intelligence analysis through acquiring more relevant data both from other teams within the company as well as from external partners. Organizations should follow the steps outlined above to find opportunities to collect relevant data, prioritize threats, manage risks, and align with the company's mission. To prevent accidental sharing of sensitive or proprietary information, it is imperative for companies to establish both formal and

informal procedures for sharing information and analysis.

Step 8: Staffing a New Cyber Threat Intelligence Team

Overview

Organizations often have difficulty selecting the best positions for a cyber threat intelligence team; SEI evaluated 60% of the private companies that it interviewed as not being staffed effectively for cyber intelligence, especially strategic analysis.[2] SEI found that most companies instead expect cyber threat intelligence analysts to perform technical analysis. It is important to note that cyber intelligence is a separate discipline than cyber security, and cyber intelligence analysts require different—if complementary—skills.[50]

The key difference between the two fields is that cyber intelligence analysts seek to anticipate future threats and identify nonobvious trends, producing papers and briefings on these topics for leadership, whereas cyber security operators handle ongoing cyber incidents. Accordingly, companies should hire individuals with strong critical thinking and communication skills for cyber intelligence (strategic analysis) positions and solicit people with cyber security and networking expertise for cyber security (technical analysis) jobs. Even within the field of cyber intelligence, however, a good team needs a variety of skills that are rarely found in a single individual. While this paper suggests positions to hire, it is important that each team recruit individuals whose expertise and skills fill the team's gaps.[51]

Scope

The goal of this section is to identify key roles and traits for staffing a "lean," startup-style cyber threat intelligence team. It also suggests how a company could expand into successively larger "mean" and "dream" teams, suggesting three levels of staffing that a company could adopt as it increases its analytic sophistication and coverage. As previously mentioned, the topics of these proposed teams are limited to foreign nation states and the company's critical assets; companies might choose to broaden to other topics (e.g. cybercrime) when they reach "dream team" status.

The "lean team" is cross functional—meaning that it includes employees whose work supplements analysts, such as Data Scientists—and comprises seven members. The "mean team" also is cross functional and contains nine members. Finally, the "dream team" shifts Data Scientists and Collection Coordinators into their own teams and replacing them with analysts, leaving the cyber threat intelligence team with 10 members.

Industry Best Practices

The highest-performing organizations have diverse teams of employees with a variety of skillsets, such as expertise in intelligence analysis or networking.[2,52] Possibly counterintuitively, many companies have found it more challenging to teach their employees critical thinking, writing, and briefing—traditional intelligence analysis skills—than technical skills, such as computer networking.[2]

Staffing Roles

We identified six important positions on a cyber intelligence team. To assist with hiring, we selected several specific jobs listed in National Institutes of Standards and Technology (NIST)'s Special Publication 800-181, the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,[53] which contains cyber-related jobs and corresponding expertise and skills. The Cybersecurity Workforce Framework is a helpful reference for distinguishing the exact hiring requirements that companies need for a wide range of cyber security roles. Our recommendations below are based on correlating recommendations from SEI's *Cyber Intelligence Tradecraft Report* with the Cybersecurity Workforce Framework.

Strategic Analysts

Strategic Analysts use a variety of analytic tools and techniques to understand the "big picture" of cyber activity, such as to determine the cyber actors posing a cyber threat, adversaries' motivations, and a threat's potential impact to the company.[2] These individuals review a pile of disparate and sometimes conflicting information, evaluate the information based on its context, consider leaders' pending decisions, and provide recommendations and answers to leadership.[54] Strategic Analysts also relay technical details to cyber security engineers to improve the company's defenses, such as by identifying methodologies that emerging cyber threat actors might use to attack the organization's computer networks.

The team should have enough Strategic Analysts, and a sufficiently limited scope, such that each analyst can specialize and build expertise, which would allow that analyst to write reports quicker and attribute cyber threats to actors. Given that this framework is scoped to address threats only from foreign nation states and to a company's critical assets, the team should strive to eventually hire one analyst covering each of the following: Chinese, Russian, North Korean, and Iranian cyber threat actors as well as the company's three most important critical assets.

Analysts focused on foreign nation states ("geopolitical analysts") could be selected in part based on their language skills or cultural understanding of a country, either from travel or graduate studies. Analysts focused on critical assets ("functional analysts") could be chosen because of their cyber threat risk management backgrounds or experience using or developing a specific asset.

The most relevant Strategic Analyst role listed in the Cybersecurity Workforce Framework is All-Source Analyst (AN-ASA-001). Figure 19 lists desirable qualifications, based on NIST's Cybersecurity Workforce Framework.

SKILLS AND ATTRIBUTES FOR STRATEGIC ANALYSTS
Skill in evaluating a variety of information for reliability, validity, and relevance to determine most likely scenario, key assumptions, and gaps in information
Skill in critical thinking, such as to identify alternative analyses to predict unanticipated events
Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality products
Ability to clearly articulate intelligence requirements as well-formulated research questions
Skill in using analytic tools, databases, and structured analytic techniques (e.g. Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.)
Skill in using search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and other tools for open-source research
Knowledge of how to extract, analyze, and use metadata
Skill in writing, reviewing, and editing cyber-related papers
Skill in briefing analysis to leadership
Ability to participate in a collaborative environment, consulting with other analysts and experts—both internal and external to the company—to leverage analytical and technical expertise

Figure 19. Criteria for Strategic Analysts[53]

Recruiting Strategic Analysts

Personnel in a strategic cyber threat intelligence team should possess different skills than those in technical cyber security teams; SEI notes that successful Strategic Analysts in cyber threat intelligence often do not initially possess any cyber security or networking expertise.2 Instead, SEI recommends hiring individuals with intelligence analysis expertise, strong critical thinking skills, and awareness of geopolitics and, once hired, train the analysts on technical topics. SEI notes that most companies that they interviewed found it easier to teach technical topics to intelligence analysts than to teach intelligence analysis tradecraft to network engineers. Companies should consider hiring Strategic Analysts who have worked for the US Intelligence Community—and have geopolitical awareness of key foreign adversaries—and subsequently train them on cyber security fundamentals.

SEI suggests that hiring managers seek the following skills for Strategic Analysts: critical thinking, problem solving, strong written and oral communication, successful collaboration, experience in intelligence analysis, data collection and prioritization, and knowledge of geopolitics and possibly cyber security. 2 Additionally, SEI recommends searching for the following traits: intellectual independence, adaptability, curiosity, persistence, ability to learn quickly, high emotional intelligence, good interpersonal skills, open mindedness, creativity, humility, ability to self-critique, healthy skepticism, intuit the "big picture," and self-motivated.

To objectively evaluate a candidate, a company could give candidates short tests to determine their critical thinking and writing capabilities. To test critical thinking, candidates could solve logic problems, such as identifying patterns, similar to problems on the Law School Admission Test (LSAT). To test analytic and writing skills, candidates could be given approximately five reports on a (fake) geopolitical crisis—or a cyber attack for those with a cyber background—and asked to write a one-page paper assessing the scenario, identifying key intelligence gaps (i.e. gaps in information), and offering recommendations to the company. These tests might also reveal other traits of the candidates, such as their ability to learn quickly, persistence, and adaptability. A hiring manager could judge whether candidates possess other traits, such as emotional intelligence and effective oral communication, during behavioral-based interviews.

Technical Analysts

While Strategic Analysts provide big picture assessments, Technical Analysts use their computing expertise to examine the details of cyber activity, such as hunting through malware to determine its intended purpose or possible authors.[55] On a cyber threat intelligence team, Technical Analysts are especially useful for communicating effectively between Strategic

Analysts and the company's cyber security engineers, such as those in a SOC.[54] Technical Analysts should also consult with Strategic Analysts as necessary to provide technical explanations and interpretations. For every paper written by Strategic Analysts, Technical Analysts should ensure that its technical details are accurate and support the overarching conclusions. Ideal Technical Analyst candidates would have a broad knowledge of network analysis, malware analysis, and reverse engineering.

Some companies might call this role a "Cyber Threat Analyst." However, we consider that term too vague to distinguish between Strategic Analysts and Technical Analysts, both of which analyze cyber threats using different methodologies. Similarly, the position "Cyber Intelligence Analyst" could refer to either a strategic or tactical role, so we also avoid using that term.

We also caution that a Technical Analyst might be drawn into other technical teams' work unless that analyst's performance evaluation is clearly based on his or her support to the cyber threat intelligence team's products. Performance criteria typically correlate strongly to an officer's work effort, and this role is focused on extrapolating technical data that is pertinent for strategic analysis prepared for company leaders.

The most pertinent positions for a Technical Analyst listed in the Cybersecurity Workforce Framework is Threat/Warning Analyst (AN-TWA-001), Target Network Analyst (AN-TGT-002), and Target Developer (AN-TGT-001). Figure 20 is a list of corresponding qualifications, based on NIST's framework.

SKILLS AND ATTRIBUTES FOR TECHNICAL ANALYSTS
Knowledge of system and application security threats and vulnerabilities (e.g. buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)
General knowledge of networking, malware analysis, reverse engineering, and forensics analysis
General knowledge of cyber adversaries (e.g. script kiddies, insider threat, non-nation state sponsored, and nation sponsored)
Knowledge of cyber attack stages (e.g. reconnaissance, scanning, enumeration, gaining access, privilege escalation, maintaining access, network exploitation, covering tracks)
Skill in recognizing and categorizing types of vulnerabilities and associated attacks

Figure 20. Criteria for Technical Analysts[53]

Collection Coordinators

The overarching responsibility of this position is to identify and obtain documents and data to fill Intelligence Requirements identified by Strategic or Technical Analysts or leadership. Such information could include a foreign nation state's strategic statements, which might provide clues on its cyber targets, or specific malware samples from another company. These individuals have deep expertise on data collection tools and Internet-searching methodologies and general knowledge of—or could be trained on—computer security and geopolitical issues.[55] Similar to Strategic Analysts, some companies have found it more efficient to hire someone with previous collection expertise and instruct them on cyber security principles than to convert a cyber security engineer into a collection manager.

Collection Coordinators should work closely with Strategic and Technical Analysts to understand, prioritize, and find information on Intelligence Requirements. These individuals could also evaluate the utility of new commercial sources of information, external intelligence reports, or tools. Additionally, they could act as liaisons to organizations that exchange information on cyber threats, such as ISACs.

While the US Government's equivalent of this position—a Collection Management Officer—does not have a technical role, we envision that a company could seek to hire individuals with

some computer coding capability to help analysts cull through data. For instance, Collection Coordinators who know the Python programming language could perform SQL queries to locate specific information contained within a database.[55] Similarly, while the US Government's Collection Management Officers do not perform analysis, Collection Coordinators could triage external cyber intelligence reports for the team or prepare a daily cyber intelligence report to leaders that summarizes key external cyber intelligence products.

Possible positions for a Collection Coordinator listed in the Cybersecurity Workforce Framework are All-Source Collection Manager (CO-CLO-001), All-Source Collection Requirements Officer (CO-CLO-002), and Exploitation Analyst (AN-EXP-001). Some corresponding qualifications are, based on NIST's framework, are given in Figure 21.

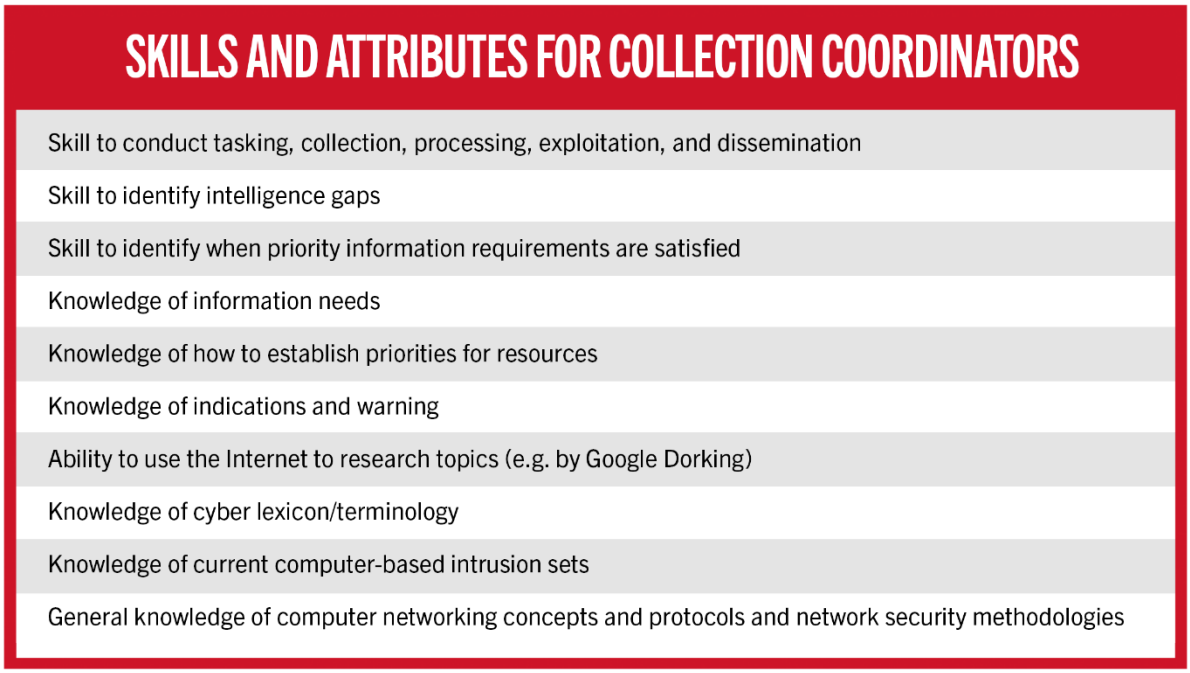

Figure 21. Criteria for Collection Coordinators[53]

Data Scientists

These individuals are highly skilled in data analysis tools and ideally have expertise in machine learning to automate tasks.[2] They support Strategic and Threat Analysts by sorting through large data sets as well as uncovering new patterns. They do not need a background in cyber security to be effective, although they probably could benefit from some training to better interpret data.

Data Scientists could assist Strategic and Threat Analysts by building data profiles and searching for anomalies. Furthermore, they could use machine learning to automate some technical tasks performed by Technical Analysts. Data Scientists are prized in the US Government because they develop methodologies to cull through mass amounts of data, helping to identify and link threat actors. In some instances, their work probably shortened the time to identify foreign adversaries by up to one year, judging by the time an analyst probably would need to correlate numerous reports.

Because Data Scientists are not specific to cyber security roles, NIST's Cybersecurity Workforce Framework does not list the position.

Manager

The manager interfaces with senior leaders to identify pending decisions that could be better informed by the cyber threat intelligence team, relays leadership's needs to the team, and solicits executives' feedback on the team's papers and briefings. To provide effective oversight, the team's manager should have some experience with strategic intelligence analysis. Regarding candidates with government experience, some companies noted that intelligence officers with military or tactical backgrounds often were not interested in managing or reviewing analytic products and instead preferred operations, driving strategic intelligence teams more towards tactical technical analysis,[2] suggesting that intelligence experience in the US Intelligence Community differs from that in the Military and the former probably are preferable for this role. The Cybersecurity Workforce Framework lists one similar managerial role as Information Systems Security Manager (OV-MGT-001).

Analytic Tradecraft Expert

To free up time for the manager to focus on personnel issues and coordinating with other managers, we recommend that a team hire a senior expert to develop the team's analytic skills and ensure the quality of its products. This individual should edit all of the team's papers and instruct team members on critical thinking, writing, and briefing. This expert should be a former analyst—and ideally instructor—from one of the better-known strategic US intelligence agencies, whose training courses are directly applicable to cyber threat intelligence analysis. The expert should have strong communication and organization skills. Relevant positions in the Cybersecurity Workforce Framework are Cyber Instructor (OV-TEA-002) and Cyber

Instructional Curriculum Developer (OV-TEA-001), although they do not capture the full range of responsibilities described above.

Creating and Expanding the Team

Recognizing that a new cyber threat intelligence team is likely to have limited resources, we recommend creating, growing, and institutionalizing the team in a series of three steps, which we refer to as the Lean, Mean, and Dream Teams.

Lean Team

This team would rely on existing capabilities within the company and might initially hire generalists over specialists, as shown in Figure 22. Two Strategic Analysts would cover the four most-dominant cyber nation-state adversaries (e.g. China, Russia, North Korea, and Iran). One Strategic Analyst would focus on the company's three most-critical assets, relying heavily on the geopolitical analysts to provide context on threat actors from the four countries followed by the geopolitical analysts. One Analytic Tradecraft Expert, Technical Analyst, Collection Coordinator, and Data Scientist would round out the team.

LEAN TEAM

ANALYTIC TRADECRAFT EXPERT	Trains all team members in critical thinking; instructs Strategic Analysts on writing and briefing. Edits all reports written by the team and ensures thorough, sophisticated analysis. Possesses general knowledge of all disciplines and helps Collection Coordinators to brainstorm intelligence requirements
STRATEGIC ANALYST NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from China and North Korea
STRATEGIC ANALYST NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from Russia and Iran
STRATEGIC ANALYST CRITICAL ASSETS	Analyzes, writes on, and briefs about cyber threats to the company's top three critical assets
TECHNICAL ANALYST	Provides technical analysis to all Strategic Analysts. Liaises with technical security teams (e.g. SOC).
COLLECTION COORDINATOR	Seeks information to address all of the Strategic and Technical Analysts's intelligence gaps
DATA SCIENTIST	Provides data analysis support to all Strategic and Technical Analysts

Figure 22. Members of a new cyber threat intelligence team

Mean Team

As described in Figure 23, this team would specialize further. Adding two more Strategic Analysts would allow each of the geopolitical Strategic Analysts to focus on only one nation state. However, if the Strategic Analysts sought more assistance, the team might need to hire another Technical Analyst, Collection Coordinator, or Data Scientist.

MEAN TEAM	
ANALYTIC TRADECRAFT EXPERT	Trains all team members in critical thinking; instructs Strategic Analysts on writing and briefing. Edits all reports written by the team and ensures thorough, sophisticated analysis. Possesses general knowledge of all disciplines and helps Collection Coordinators to brainstorm intelligence requirements
STRATEGIC ANALYST NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from China
STRATEGIC ANALYST NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from Russia
STRATEGIC ANALYST NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from North Korea
STRATEGIC ANALYST NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from Iran
STRATEGIC ANALYST CRITICAL ASSETS	Analyzes, writes on, and briefs about cyber threats to the company's top three critical assets
TECHNICAL ANALYST	Provides technical analysis to all Strategic Analysts. Liaises with technical security teams (e.g. SOC).
COLLECTION COORDINATOR	Seeks information to address all of the Strategic and Technical Analysts's intelligence gaps
DATA SCIENTIST	Provides data analysis support to all Strategic and Technical Analysts

Figure 23. Members of a developing cyber threat intelligence team

Dream Team

The cyber intelligence team would focus exclusively on analysis, as shown in Figure 24. Collection Coordinators and Data Scientists would form one or two separate teams to enable them to further develop expertise in their fields and potentially become corporate resources, assisting management or other teams as needed. In high-performing organizations, analysis, collection, and data science are split into separate roles, and each role develops unique skills.[2]

One additional geopolitical Strategic Analyst would cover cyber threats posed by all nation states other than the original four countries. Another functional Strategic Analyst would share responsibility for identifying threats to the company's top three critical assets. Furthermore, each Strategic Analyst should be assigned to back up another analyst's account, such that there would be no interruption of coverage were an officer to take leave. A second Technical Analyst could better support the team's seven Strategic Analysts, increasing the depth of the technical assessments underpinning the team's papers and improving communication with the company's technical analysis and SOC teams.

DREAM TEAM	
ANALYTIC TRADECRAFT EXPERT	Trains all team members in critical thinking; instructs Strategic Analysts on writing and briefing. Edits all reports written by the team and ensures thorough, sophisticated analysis. Possesses general knowledge of all disciplines and helps Collection Coordinators to brainstorm intelligence requirements
STRATEGIC ANALYSIS NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from China
STRATEGIC ANALYSIS NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from Russia
STRATEGIC ANALYSIS NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from North Korea
STRATEGIC ANALYSIS NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from Iran
STRATEGIC ANALYSIS NATION STATES	Analyzes, writes on, and briefs about cyber threats emanating from all other countries
STRATEGIC ANALYSIS CRITICAL ASSETS	Analyzes, writes on, and briefs about cyber threats to the company's top critical assets
STRATEGIC ANALYSIS CRITICAL ASSETS	Analyzes, writes on, and briefs about cyber threats to the company's top critical assets
TECHNICAL ANALYST	Provides technical analysis to all Strategic Analysts. Liaises with technical security teams (e.g. SOC).
TECHNICAL ANALYST	Provides technical analysis to all Strategic Analysts. Liaises with technical security teams (e.g. SOC).

Figure 24. Members of a mature cyber threat intelligence team

A summary of the team's development is shown in Figure 25.

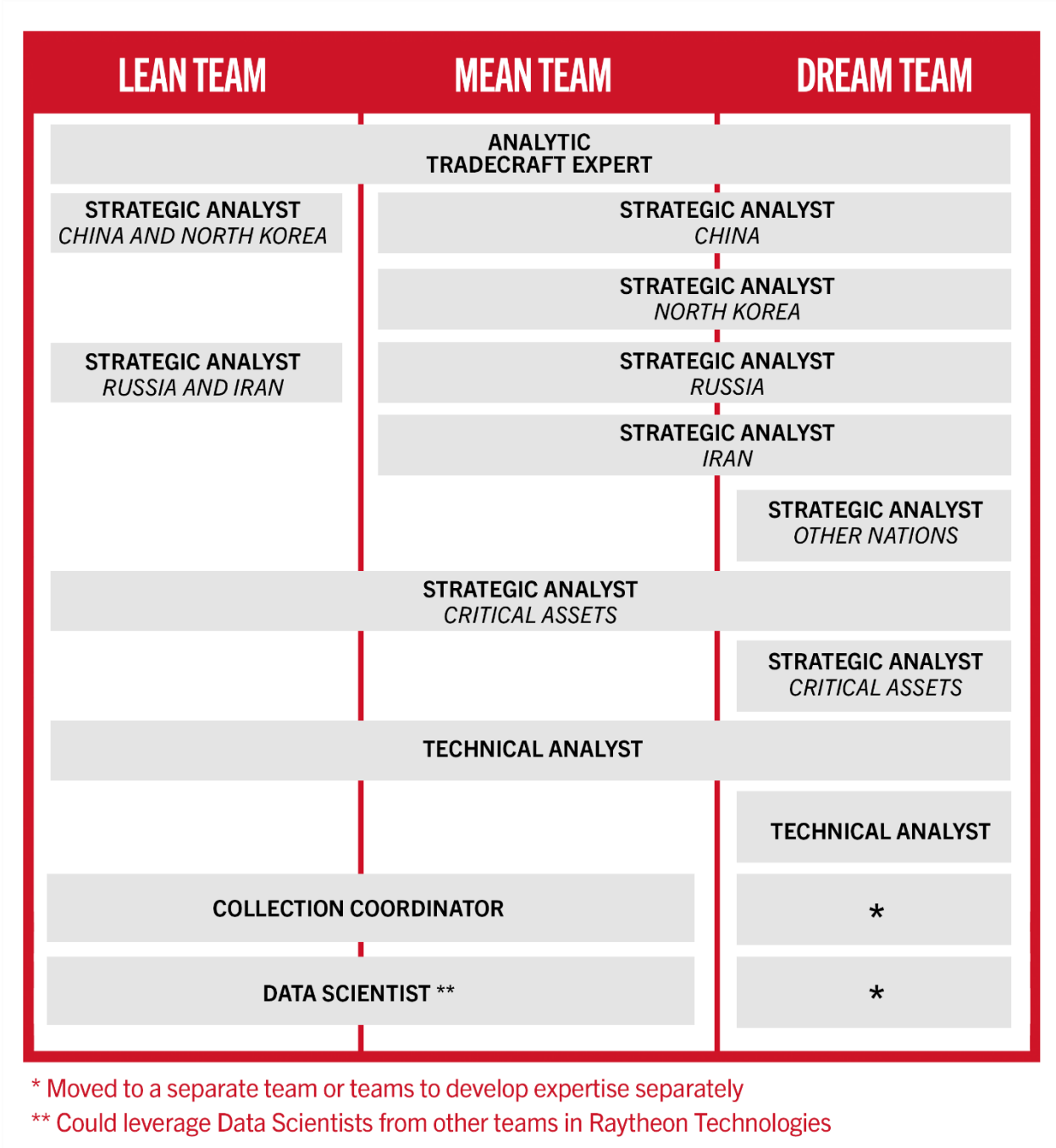

Figure 25. Proposed evolution of cyber threat intelligence team

Budgeting

Three key budget items for a cyber threat intelligence team are salaries, training, and tools. Recommendations for tools are listed in Step 9 (Technology for Data Gathering).

Training

We recommend two types of training: analytic (e.g. critical thinking, writing, and briefing) and technical (e.g. cyber intelligence, vulnerability analysis, and networking).

Training Strategic Analysts

It is important that a company institute a career development path, and that path probably would be different across specialties. For Strategic Analysts, we recommend investing in two pillars: analytic tradecraft and cyber security expertise.

Within the analytic tradecraft pillar, analysts should take an introductory training course on writing, briefing, and critical thinking, as described in Step 3 (Strategic Analysis Workflow). Later in their careers, they should undergo training on Structured Analytic Techniques, intelligence failures, and denial and deception.

Within the cyber security expertise pillar, each analyst should be expected to attend commercial training, such as the SANS Institute's Cyber Threat Intelligence Course, as well as common information security conferences, such as DEF CON Hacking Conference, BlackHat USA, Security BSides, DerbyCon, or Women in Cybersecurity.

Depending on the needs of individuals on the team, Figure 26 is a list of possible courses that a company could offer. Analytic training might not be useful for some roles, some individuals might need to learn basic cyber security principles, and Collection Coordinators and Data Scientists might need specialized training. A well-known commercial vendor is the SANS Institute, which offers a variety of technical courses. A company could offer several courses a year, rotating its employees through all the applicable training over the course of a few years. The following are training courses that the company could consider, some of which could be divided in two segments and offered twice a year for continued development.

COURSE	LENGTH	COST
Critical Thinking (Independent Contractor)	2 Weeks	$6,000
Writing (Independent Contractor)	2 Weeks	$6,000
Briefing (Independent Contractor)	3 Days	$1,800
Structured Analytic Techniques (Independent Contractor)	1 Week	$3,000
Denial and Deception (Independent Contractor)	3 Days	$1,800
Introduction to Cyber Security (SANS, SEC301)	1 Week	$6,090.00 / person
Cyber Threat Intelligence (SANS, FOR578)	1 Week	$6,090.00 / person

Figure 26. Costs of possible training courses

Recommendations for Improving Performance

Expand Topics

Each new analyst should be assigned only one topic to ensure that analysts can develop expertise and are not overwhelmed. Leadership should know that a team's scope could expand only if it were to acquire more personnel. However, analyzing only nation states and threats to critical assets is limited and could leave leaders with blind spots when making decisions. As budgeting allows, the team should broaden its topics, such as to cover cyber criminals or to evaluate how new technology could challenge a company's cyber security.

The cyber threat intelligence team manager should reevaluate coverage twice a year to confirm that the team's scope includes the company's most pressing cyber concerns. This assessment could be timed to follow the corporate risk management team's periodic reviews, which should produce a prioritized list of the company's risks.

Create Additional Teams

As mentioned previously, over time, the company is likely to benefit from separating Data Scientists and Collection Coordinators into their own team or teams to develop their expertise separately. By having their own teams and managers, those officers could have distinct evaluation criteria and more easily share best practices with each other to improve their own tradecrafts.

Conclusion

We propose three different tiers of staffing to support strategic analysis of cyber threats posed by foreign nation states and targeting the company's three most critical assets. In doing so, we emphasize the importance of analysts building expertise with a limited scope of responsibility. Strategic Analysts alone are insufficient for producing high-quality assessments and papers, however. The team should supplement Strategic Analysts with a tradecraft coach to hone the analysts' critical thinking, writing, and briefing skills; Technical Analysts to investigate malware and other types of technical data; Data Scientists to extrapolate emerging trends; and Collection Coordinators to obtain key data.

Step 9: Technology for Data Collection

Overview

A plethora of information on cyber threats is available from a broad array of sources, both free and with paid subscription. It is vital for organizations to aggregate reports and technical data from a wide range of public, paid, and technical sources to obtain multiple perspectives and amass sufficient context on actors targeting the organization, actors' motivations and capabilities, and indicators that the actors have compromised company systems.[56] Having collected multitudes of data, however, it is important to organize it in such a way that the data is easily discoverable. Organizations use data collection tools, such as threat intelligence platforms, to collate, add structure to, and assign priorities to data from various sources to make querying more efficient for analysts. Vendors who sell threat intelligence platforms often include their own threat intelligence feed, which typically is raw technical data on cyber operations but could include intelligence reports. This step pertains to acquiring cyber threat data, including from external sources, as opposed to a Security Incident and Event Management system, which collects a company's event logs and monitors its network and endpoint devices.

Typically, Technical Analysts, and sometimes Strategic Analysts, use a threat intelligence platform to correlate raw data from a couple of sources. Many threat intelligence platforms provide data only collected its by vendor, but some might also include data from organizations of which the vendor is member. Data provided by threat intelligence platforms includes information on cyber hygiene practices, cyber campaigns, and cyber actors' tactics, techniques, and procedures. Most threat intelligence platforms also offer data visualization, allowing analysts to create "dashboards" for a particular threat. This method of filtering information should quicken and improve analysis. However, other members of a cyber threat intelligence team also could use threat intelligence platforms. For instance, the tool is likely to contain bulk data useful for a Data Scientist. Additionally, Collection Coordinators could use it to determine whether Specific Intelligence Requirements were met; most threat intelligence platforms can generate reports based on the user's preferences, including timeframe and specific actors.

Scope

This workflow assumes that new cyber intelligence teams initially require only one data collection tool—such as a threat intelligence platform—to function effectively. Our recommendations are limited to this paper's scope of collecting data on nation-state adversaries

and protecting critical assets. As the team expands and covers more topics, the team almost certainly would need additional threat intelligence platforms to have a more holistic intelligence feed.

We evaluated numerous threat intelligence platforms, with details of some listed in Appendix F, based on open-source data available on vendors. This step also includes best practices outlined in reports published by industry leaders, such as SEI, MITRE, Recorded Future, Forrester, and the SANS Institute.

Industry Best Practices

It is important to clarify the differences between a threat intelligence provider and threat intelligence platform: threat intelligence providers sell threat intelligence platforms. Threat intelligence providers are companies that produce mostly raw cyber threat data and some analysis. Providers share content with customers in the form of feeds via e-mail, portal download, RSS feed, or tweet that can be ingested into threat intelligence platforms, which is that displays cyber information. Threat intelligence providers typically have limited scope; some vendors provide reports on cyber actors and others have a specific theme, such as cyber espionage. Separately, threat intelligence platforms are complex content management systems designed for cyber data that allow organizations to aggregate, organize, and search for data.[57]

Organizations often subscribe to multiple threat intelligence providers—typically purchasing multiple threat intelligence platforms—based on their needs and priorities. According to Forrester, companies with 1,000 or more employees subscribe to an average of 4.2 commercial threat intelligence vendors.[58] Companies assess that one provider alone is unlikely to offer sufficient information to fulfill all their Intelligence Requirements on potential threats and threat actors. Based on a report by Forrester, organizations subscribe to feeds based on the following factors: collection, reputation, workflow management, dissemination, support, and cost.[59]

Most vendors offer free demonstrations for short time periods, often two to four weeks. We recommend that a company obtain trial versions of programs and information services to determine whether a particular threat intelligence platform or provider is suitable for its business needs and analysts find it beneficial. We recommend that a company form a working group to evaluate tools and technology, such as threat intelligence platforms, that periodically examines and tests new products. Regular evaluations would ensure that the company's tools meet

industry standards. A Collection Coordinator could head this group to incorporate the organization's collection requirements in addition to analysts' perspectives.

Recommendations for Improving Performance

Different Threat intelligence platforms and providers offer distinct information. Over time, as the threat intelligence team grows, we recommend subscribing to additional threat intelligence platforms and providers based on team's capabilities and requirements. To evaluate threat intelligence vendors, we assessed that the list of questions prepared by Ed Tittel and available on TechTarget.com displayed in Figure 27 to be the most comprehensive.

FACTORS TO CONSIDER WHILE EVALUATING TIPS

DATA FEED

- ☐ Multiple SIEM Ingestions
- ☐ Industry protocols for ingestion
- ☐ How many data feeds are available, and what is their focus? Feeds may cover IP/domain URLs, reputation, security risks, vulnerabilities and more.
- ☐ What platform does the provider use to process data? Does it require proprietary equipment?
- ☐ Which file formats are the data feeds? Formats are typically CSV, XML, STIX and JSON. Many service providers accommodate API management, which enables customers to pull data through a web service.
- ☐ From how many different data sources does the company draw?
- ☐ What are the sources? Most providers are willing to disclose their sources of threat intelligence data upon request, while others can't or won't do so because it's considered confidential information.

THREAT INTELLIGENCE ALERTS AND REPORTS

- ☐ Does the company provide real-time alerts?
- ☐ How frequently are reports or summaries issued?
- ☐ Are they industry-specific?
- ☐ Are organization-specific reports available?

REPUTATION

- ☐ Automated IOC Enrichment
- ☐ Vulnerability Prioritization
- ☐ Threat Correlation
- ☐ Named Threat Attribution
- ☐ Anonymized/Sanitized Threat Sharing/Community

WORKFLOW MANAGEMENT

- ☐ Custom Dashboards
- ☐ Visual Threat Correlation

DISSEMINATION

- ☐ Weekly Threat Landscape Reports by Vendor
- ☐ STIX 1.x/TAXII/MISP, etc Framework Support
- ☐ ServiceNow Records & Updates Integration
- ☐ Private/Public Communities
- ☐ Splunk Integration & App
- ☐ Cloud/remote client login/portal support
- ☐ Monitoring
- ☐ Brand monitoring (OSINT/Deep/DarkWeb)
- ☐ YARA/Retro Hunts

SUPPORT

- ☐ Technical Support
- ☐ Assigned Engineer/Account Manager & Advisory Consultation
- ☐ Intel Analyst Q&A
- ☐ Universal Shared Accounts Supported
- ☐ Flexible Pricing and Support
- ☐ Free Playbook Configuration/Integration Use Case Development
- ☐ Cloud Solution
- ☐ On-Premise (remember costs associated)

PRICING

- ☐ Total users
- ☐ API usage rate
- ☐ GB Data Transfer rate
- ☐ Product/Flat Rate

Figure 27. Checklist for Threat Intelligence Platforms and Providers[60]

Conclusion

Threat intelligence platforms are crucial for collating and sifting through cyber intelligence data feeds, a necessary starting point to developing an effective threat intelligence analysis process. This type of platform offers an efficient method to store, categorize, and access information, and analysts could find data easily using the software's data visualization dashboards. Using threat intelligence platforms could add structure to a cyber threat intelligence team's processes, enabling repeatable procedures important to scaling for future growth. Additionally, threat intelligence platforms could also help overcome silos within organizations and across industries.[61]

Team Workflow

Having described nine steps to create a cyber threat intelligence team, we also propose a process for the team's daily routine. As mentioned previously, our goal is to help a company to establish a team that would operate similarly to cyber intelligence units in the US Intelligence Community. Accordingly, our framework contains the same, core intelligence activities as the Intelligence Community and SEI's models. As shown in Figure 28, the Intelligence Community's Intelligence Cycle delineates six categories of intelligence activities: Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, Dissemination and Integration, and Evaluation.[3,4]

Figure 28. US Intelligence Cycle[62]

SEI translated this concept into five "components" specific to cyber intelligence as displayed in Figure 29. In SEI's workflow, Environmental Context includes identifying a company's vulnerabilities, prioritizing threats, and planning; Data Gathering is equivalent to collection; Threat Analysis refers to technical analysis and incorporates processing and exploitation; Strategic Analysis pertains to analysis and production; and Reporting and Feedback includes production, dissemination, and evaluation.[2]

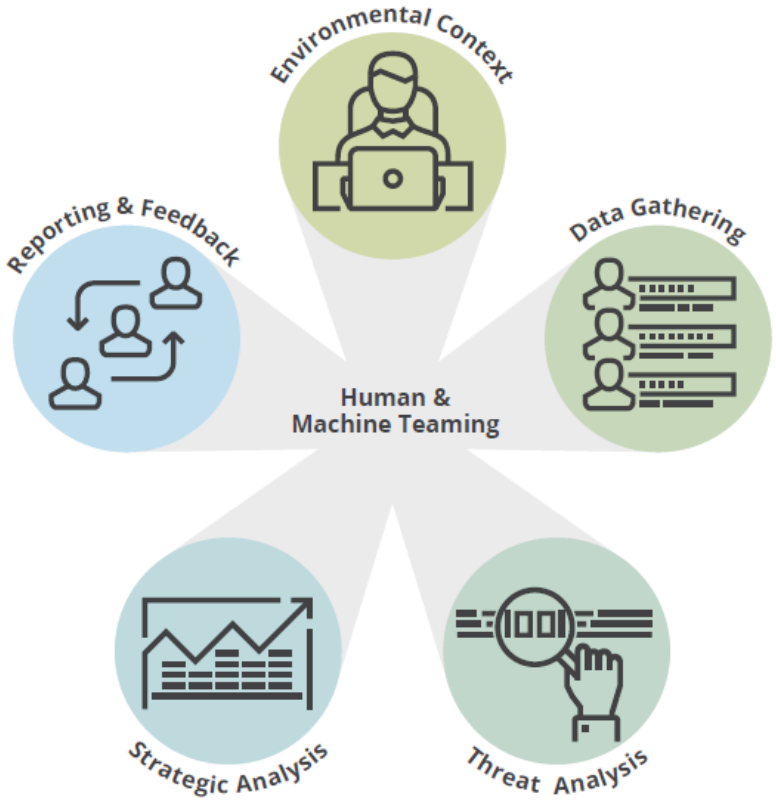

Figure 29. SEI's cyber intelligence workflow[2]

The workflow that we designed for a cyber threat intelligence team comprises all these elements but in more detail, as shown in Figure 30.

Figure 30. Possible workflow for entire cyber threat intelligence team

When identifying a topic to investigate, a team member should consider the company's vulnerabilities, critical assets, ranking of threats, and Intelligence Requirements, which were all determined in collaboration with the company's risk and collection management teams. With assistance from the company's collection management, cyber security, and information technology teams, that team member would collect relevant information from sources within and external to the company.

Strategic and Technical Analysts would analyze intelligence reports and technical data while Data Scientists would analyze bulk data sets, all seeking to answer the Intelligence Requirements pertinent to their topics as well as to identify new threats and vulnerabilities. Strategic Analysts would write papers and brief leaders on their assessments, incorporating Technical Analysts's insights.

The team's manager would solicit feedback from senior leaders on the team's assessments. Furthermore, leadership would periodically reevaluate the company's Intelligence Requirements, which would ensure that the cyber threat intelligence team continued to focus on executives' top priorities.

Instead of this process being linear and ending when leadership receives an assessment, the process should be a cycle that iteratively feeds back into itself. The results of many of these actions should inform other activities. For instance, a new threat that analysts identify during the analysis phase could be considered in the next reviews of the company's threat priorities and Intelligence Requirements, which in turn would drive more collection on the threat.

Across the nine steps described above, we outline each of the actions contained in the team workflow. Drawing on the US's Government's best practices for performing cyber intelligence, we assess that this workflow would benefit most cyber threat intelligence teams.

Future Work

We do not expect that a company would build an advanced, sophisticated cyber threat intelligence team using only the nine steps we discussed above. Instead, our intent is to identify the most important steps to building a functional cyber intelligence team that could quickly add value to an organization's decisions on cyber threats as well as to its cyber security teams. Once an organization has made satisfactory progress on creating the team and instituting a team workflow, the organization should plan its next steps to improve the capabilities and performance of the existing team.

We selected nine subsequent steps, referencing specific assessment factors listed in SEI's *Cyber Intelligence Tradecraft Report*,[2] that an organization could follow after its new cyber intelligence team has started producing actionable intelligence.

Data Collection

- Using past, present, and future data (Environmental Context 8)
- Intelligence Requirement and data source alignment (Data Gathering 2)
- Data source validation (Data Gathering 5)

Analysis

- Timeliness and accuracy of threat analysis (Threat Analysis 2)
- Diversity in technical disciplines (Threat Analysis 3)
- Relationship between cyber intelligence and inside threat teams (Environmental Context 9)

Feedback

- Feedback mechanisms for analysts (Reporting and Feedback 5)
- Influence of feedback on data gathering and analysis (Reporting and Feedback 6)
- Capturing return on investment (Reporting and Feedback 8)

These steps are intended to complement each other and guide the team towards three enduring goals.

Improve Quality of Analysis

A team could improve the sophistication and accuracy of its analysis by improving how the organization collects, validates, and analyzes data. The team should develop or purchase a tool to retain the team's reports and data that map the products to Intelligence Requirements.

Ensure Value of Analysis

Feedback is likely to offer the team the greatest opportunities to develop its tradecraft and increase its impact on the organization. The team should solicit opinions on the content and format of its products both from executives and team members.

Develop Technical Expertise

We expect that a cyber threat intelligence team is likely to experience some difficulty both in distinguishing itself from and exchanging information with a company's pre-existing cyber security teams. It is important that the cyber intelligence team not exist in a silo and instead work through these challenges to ensure that it develops sufficient technical expertise to inform leadership about cyber threat actors' methodologies and share information about emerging cyber threats with security teams. To be successful, the team should strive to improve its technical knowledge and collaboration techniques.

Incorporating Machine Learning

One emerging trend in the cyber intelligence industry is the use of machine learning to improve efficiency. The team's Data Scientist might be able to integrate some machine-learning techniques into the team's workflow to identify additional insights from data sources, such as cyber threat information written in foreign languages, malicious anomalies, and potential vulnerabilities. We identified three types of machine-learning applications that a cyber threat intelligence team should consider incorporating.

Natural Language Processing (NLP)

A lot of the information, especially technical information, that would be useful to a cyber intelligence team is distributed across millions of websites. Strong NLP systems can collect and analyze data irrespective of language or format, with constant advancements so that the system can understand jargon, slang, or abbreviations.[63] NLP systems could help analysts find cyber threat information written in foreign languages.

Pattern Recognition

Intelligence analysts seek to find patterns in large sets of unstructured or inconsistently-formatted data. As an example, MIT's Computer Science and Artificial Intelligence Laboratory created a machine-learning platform called AI^2 that can improve anomaly detection and group data into patterns for human analysts to review.[64,65] Pattern recognition could help analysts to uncover new types of cyber threats.

Predictive Analytics

Similarly to entertainment companies using machine learning to suggest television shows to a viewer, some companies already are using machine learning to predict the probability that a particular vulnerability could be exploited or assess the risk of a currently-benign actor turning malicious.[66] A threat intelligence team could use predictive analytics to ensure that its analysts have not overlooked any potential risks.

Conclusion

In this report, we have created a framework in which we identified nine steps to a guide an organization in establishing a cyber threat intelligence team. Additionally, we suggest a team workflow that would integrate the processes and policies formulated during the team's creation. Using both of these models, we judge that a company could form and develop a cyber threat intelligence team that produces actionable assessments for leadership to better protect the company's critical assets and identify the most significant nation-state adversaries, ultimately adding substantial value to the company's overall mission.

To create a cyber threat intelligence team, we recommend that a company perform the nine steps below:

(1) Leadership Involvement

Develop best practices in leadership involvement and communication channels.

(2) Reporting and Feedback

Identify best practices in intelligence reporting, including writing style, confidence levels, and estimates of probability. Institute a distribution mechanism and schedule for the team's products.

(3) Strategic Analysis Workflow

Produce sophisticated analytic reports on cyber threats to inform leadership's decisions.

(4) Technical Analysis Workflow

Collect and assess technical data and communicate and disseminate it to Strategic Analysts.

(5) Intelligence Requirements Process

Determine business-focused Intelligence Requirements, which should drive the cyber threat intelligence team's collection and production.

(6) Threat Prioritization Process

Establish the most important threats to an organization, which should help the cyber threat intelligence team to identify and prioritize topics to assess.

(7) Organization Information-Sharing Process

Suggest bi-directional processes for sharing information across a company's cyber security and cyber intelligence teams and, separately, with external organizations.

(8) Staffing a New Cyber Threat Intelligence Team

Provide hiring and budgeting recommendations for specific positions on a cyber threat intelligence team, divided into three successive stages of development.

(9) Technology for Data Collection

Analyze numerous commercial tools that organizations could use to collate and structure data obtained from multiple sources.

Cyber threat intelligence is an enabler; it enables organizations to anticipate attacks, prevent harm, become aware of new threats, and make better business decisions. This framework proposes methods that offer organizations opportunities to think ahead, prepare, innovate, and thwart adversaries before they could threaten the company's most valuable assets.

> ***"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."***
>
> - Sun Tzu[67]

Appendices

Appendix A: Weekly Threat News Report Template

Distribution: *[Clearance Level]*

DEFENSE INDUSTRY THREAT DIGEST: WEEK OF [Day, Month, Year]

Published On:

Author:

EXECUTIVE SUMMARY

Highlight the news reports you discuss in the digest. Simply list the title of the News Piece.

THIS WEEK'S HIGHLIGHTS

Industry

Three to five industry related news reports

[Defense Industry Related News Reports]

General

Three to five general cybersecurity awareness news reports

[General Cybersecurity Awareness News Reports]

PROMINENT INFORMATION SECURITY EVENTS

Descriptions on the news report highlighted/listed in the Executive Summary.
[Title]
[Source]
[1 Paragraph description – can be copy/pasted from the news report itself]
Anaylst Comment: *How the news impacts or relates to the company*

Descriptions on the news report highlighted/listed in the Executive Summary.
[Title]
[Source]
[1 Paragraph description – can be copy/pasted from the news report itself]
Anaylst Comment: *How the news impacts or relates to the company*

Descriptions on the news report highlighted/listed in the Executive Summary.
[Title]
[Source]
[1 Paragraph description – can be copy/pasted from the news report itself]
Anaylst Comment: *How the news impacts or relates to the company*

Appendix B: Threat Analysis Report Template

Distribution: *[Clearance Level]*

THREAT ANALYSIS REPORT: [Title of Incident]

Published On:
Author:

BLUF

Communicate key points because this might be the only part of the paper that busy leaders read. Brief 1-paragraph analysis that includes the who, what, where, when, why, how, and impact of the threat event

KEY JUDGEMENTS

Ordered based on importance. Best to use in papers that are longer than one to two pages

[Key Judgements - using either a confidence level or estimation of probability]

ADVERSARY'S ACTIONS & TACTICS

Analysis of Incident

Identify important or unusual tactics in the incident (what, when, where), focusing on analysis rather than listing technical data, in a couple of sentences. If possible, highlight the attributes of the cyber actor, potential cyber actors (who), intentions (why), and motivations (why).

[Supporting data]

Adversary's Capabilities & Infrastructure

Describe the adversary's capabilities in terms of tactics, techniques and procedures (how), focusing on analysis, in a couple of sentences. Address the tools and tradecraft employed by the perpetrators, such as exploits, backdoors, and staging methods. Brief description of the adversary's infrastructure (technical details should go in the appendix).

[Supporting Data - Could be a one-sentence description of tools , tradecraft, infrastructure, etc.]

IMPACT

Potential Victims and Affected Assets

Describe the possible victims that could have been affected by the adversary's actions in a couple of sentences. Also outline the potential affected assets, such as networks, systems, and applications.

[Supporting Data]

Long-Term Effects

Describe the long-term impacts of this cyber incident in a couple of sentences; this could include a couple of plausible scenarios. Describe whether you think the cyber actor will conduct another attack and, if so, would it be with the same methodology or would the cyber actor probably adjust tactics?

[Additional Scenario Information]

INTELLIGENCE GAPS

Describe any gaps in analysis or missing pieces of information that could change the analysis. Collection Coordinators use these gaps to seek additional information.

[Intelligence Gap Information]

APPENDIX: TECHNICAL DETAILS

Describe the infrastructure, such as IP addresses, domain names, program names, etc. used by the adversary.

Distribution: *[Clearance Level]*

Appendix C: Geopolitical Event Report Template

Distribution: *[Clearance Level]*

GEOPOLITICAL EVENT REPORT: [Title of Event]

Published On:

Author:

Country:

Threat Group (if known):

BLUF

Communicate key points because this might be the only part of the paper that busy leaders read. Brief 1-paragraph analysis that includes the who, what, where, when, why, how, and possible impact of the geopolitical event

EVENT

Description of the event (who, what, where, when, how) in a couple of sentences.

[Suporting Data Points]

SIGNIFICANCE

Description of how the event could impact the company, why it is important, and the potential long-term impact of the event in a couple of sentences. Include nation state (who), reasons that the country might retaliate against or target the company; industry; or US Government (why), and possible methodology (how).

[Supporting Data Points / Scenarios]

INTELLIGENCE GAPS

Describe any gaps in analysis or missing pieces of information that could change the analysis. Collection Coordinators use these gaps to seek additional information.

[Intelligence Gaps]

Appendix D: Threat Priority List Report Template

Distribution: *[Clearance Level]*

CYBER THREAT INTELLIGENCE TEAM THREAT PRIORITY LIST

Published On:

Author:

BLUF

Brief 1-paragraph description of the contents of the list, including any key judgements determined or intelligence gaps identified during the threat prioritization process

THREATS TO CRITICAL ASSETS

In order of significance

1. [Threat 1] - Brief description and impact the threat has on the organization.

2. [Threat 2] - Brief description and impact the threat has on the organization.

3. …

NATION-STATE THREATS

In order of significance

1. [Threat 1] - Brief description and impact the threat has on the organization.

2. [Threat 2] - Brief description and impact the threat has on the organization.

3. …

Appendix E: Sample Threat Profile

THREAT PROFILE

Adversary Type: Nation State

Threat Type: APT

Target Types:

Sector: Government, Aerospace

Attribution: China

Platform: Windows

TECHNICAL ANALYIST: Marina B.

OVERVIEW

[Insert Summary and impact of this Threat Profile –discuss motivation and goals of adversary executing this threat]

THREAT EXPOSRE SCORES

1 2 3 4 5 6 (7) 8 9 10

LIKELIHOOD

1 2 3 4 5 6 7 (8) 9 10

IMPACT

ASSOCIATED MALWARE

Anel
Haymaker
Snugride
Bugjuice

TTPs

Tactics

Initial Access, Reconnaissance, Lateral Movement, Data Exfiltration

Techniques

Spear Phishing emails that install UPPERCUT backdoor.

Procedures

This APT10 technique sends malicious Microsoft Office documents as part of spear phishing campaigns via email.

TOOLS

TOOL	DISCOVERED TECHNIQUES	PURPOSE	ATTACK LIFECYCLE STAGE
HAYMAKER	Code Signing Credential Dumping File and Directory Discovery Standard Application Layer Protocol Spear Phishing with .lnk files within archive files having double extensions (.dox.exe)	Backdoor	Initial Compromise
UPPERCUT (ANEL)	Malicious VBA Macro attached to email with .doc file	Backdoor	Initial Compromise

INDICATORS OF COMPROMISE

FILE NAMES	FILE SIZE	MD5 HASH
Government Recommendations from the Liberal Democratic Party's Comprehensive Strategic Maritime Subcommittee.doc		4f83c01e8f7507d23c6 7ab085bf79e97
North Korean interior swayed by the approach of the United States.doc		cca227f70a64e1e7fcf5 bccdc6cc25dd

IP ADDRESS ORIGINS		DOMAINS	C2 SERVERS
82.221.100.52 153.92.210.208	151.106.53.147 167.99.121.203	Update.kapersky.com Download.kapersky.com Cloud-king.com Incloud-co.com	Eservake.jetos.com

ATTACK METHODOLOGY

TECHNIQUE	DETECTION STRATEGY
Phishing Attachments	Anti-virus / Anti-malware
	Network Intrusion Prevention
	User Training
Command Line Executions	Execution Prevention
File and Directory Discovery	Monitor process executions and command line arguments for data exfiltration
Remote File Copy	Monitor network activity over SMB, FTP, or other file transfer utilities

ATTACK PATH

HIGH-LEVEL SUMMARY

Attacker sends an email that contains an attached malicious document

Clicking on the document allows it to exploit Microsoft Office vulnerabilities

Abuse of the vulnerabilities leads to the download of "Koadic", a post-exploitation tool, on the victim's machine

Koadic scans the victim's system environment and downloads UPPERCUT backdoor from the C2 server

DETAILED PROCESS

STEP	FIGURE/SCREENSHOT
1. *First discovered step in adversary attack path*	*[Image from attacker's point of view]*
2.	
3.	
4.	
5.	
6.	
7.	
8.	

Appendix F: Data Analysis Tools

FACTORS TO CONSIDER - TOOL APPENDIX

The appendix is divided into 5 categories. The categories are Organizational Details, Pricing, Capabilities, Support and Additional Insights. These categories are further divided into subcategories. This document briefly expands on each category and their importance.

ORGANIZATIONAL DETAILS

WEBSITE - A link to the vendors website
YEAR FOUNDED - This is to serve as an indication about the maturity of an organizations processes.
COUNTRY OF ORIGIN- Based on the nature of their businesses, some organizations or industries have preferences for the country of origin of their technology.

PRICING

SUBSCRIPTION - This category addresses the license structure of various vendors. The pricing varies based on factors such as the number of users, time period of subscription and amount of data consumed

CAPABILITIES

The vendors considered for this whitepaper were not tested. The following section in the appendix will only address if the capability exists, not the quality of the capability.

SERVICES PROVIDED -This category lists the services provided by the vendor. Often companies have multiple security products that are designed so that the products integrate well with each other within an enterprise environment. By subscribing to vendors with multiple products and subsequently using these products, an increased efficiency in performance may be observed. Additionally, purchasing a bundle of products and services may come at a discounted price.

CUSTOM DASHBOARD - A customized dashboard will allow analysts to create dashboards based on their priorities. Some vendors do not offer this to their clients. In such cases, the analysts will have access to a common dashboard developed by the vendor. The analyst can run certain processes and create reports based on this dashboard. We recommend selecting a vendor that offers customized dashboards as they make visualization and data centralization faster – enabling the analysts to make decisions and reports efficiently.

ZERO DAY DETECTION - This category examines whether vendors are capable of publishing advisories on zero-day exploits. This capability typically is a combination of dynamic and static analysis techniques. This technique would allow vendors to rapidly identify zero-day exploits and publish advisories to their clients.

DARK WEB RESEARCH CAPABILITIES - Adversaries typically use the dark web to sell stolen information. A threat intelligence vendor must have resources and capability of scouring the dark web searching for possible sale of client IP.

TAILORED THREAT INTELLIGENCE - Some vendors do not offer tailored threat intelligence. This is an important capability to have in order to sift through the noise. Organizations in different sectors will be targeted by different organizations and have different priorities. For example, a company in the healthcare sector will have different priorities that a company in finance. If a vendor does not offer tailored intelligence, the quality of the intelligence may not be on par with the needs of RMD.

MALWARE ANALYSIS CAPABILITIES - Everyday, an increasing number of malwares and their variations are being detected. This category addresses whether the vendor has a dedicated team to identify new malwares, create signatures and publish advisories. In case of an attempt or a successful malware attack, some vendors also offer reverse engineering services. We recommend RMD select their vendor based on their needs and current in-house capabilities.

DELIVERY MECHANISM - There are various delivery mechanisms by which threat intelligence can be delivered to an organization. Some common methods are a SaaS based delivery mechanism, API based, some organizations periodically deliver reports via email. While deciding between threat intelligence vendors, RMD has to consider the delivery mechanism best suited for their needs.

SUPPORT

STIX AND TAXXI SUPPORT - STIX (Structured Threat Information eXpression) is a standardized a programming language that is used to define and add structure to threat intelligence. TAXII (Trusted Automated eXchange of Indicator Information) is a collection of services and message exchanges that allows cross platform information exchange. Compliance with STIX and TAXII will ensure faster data ingestion and sharing. It is important that vendors provide intelligence that is supported by STIX and TAXII so that intelligence from various sources can be stored and accessed efficiently.

NOTES

This section mainly provides information that is not pertinent to any of the above categories, but is of importance while making a decision regarding threat intelligence vendors.

FACTORS TO CONSIDER WHILE EVALUATING THREAT INTELLIGENCE PLATFORMS

		CROWDSTRIKE	FIREYE	BAE SYSTEMS	PALO ALTO NETWORKS
ORG. DETAILS	WEBSITE	https://www.crowdstrike.com/endpoint-security-products/falcon-x-threat-intelligence/	https://www.fireeye.com/solutions/cyber-threat-intelligence/threat-intelligence-subscriptions.html	https://www.baesystems.com/en-us/home	https://www.paloaltonetworks.com/cortex/threat-intelligence
	FOUNDED	2011	2004	1971	2005
	COUNTRY OF ORIGIN	USA	USA	United Kingdom	USA
PRICING	SUBSCRIPTION	Varies based on customer *	Subscriptions range from $100,000 to $500,000.	1 Year	Licensed as a per-user annual subscription or available as an unlimited user enterprise-wide license.
CAPABILITIES	SERVICES PROVIDED	Incident response, Adversary Emmulation, Red Team/Blue Team excercises. Tabletop excercises, Live Fire Services, cloud security, M&A Assessments **	Programmatic CTI Consumption and Integration Strategy and Process Threat Awareness and Skill Enhancement Threat Intelligence Foundations (TIF) Cyber Threat Diagnostic (CTD) Intelligence Capability Assessment (ICA) Intelligence Capability Uplift (ICU) Analytic Tradecraft Workshop (ATW) Hunt Mission Training (HMT)	Managed Security, Incident Response,Malware Analysis , Email analysis, Log analysis, Network traffic analysis, Disk image analysis	Native integration with the WildFire data set researcher-curated context from Unit 42 the Palo Alto Networks threat research team (including information on malware family, adversaries, campaigns, malicious behaviors and exploits used) aggregation and correlation of any third-party threat intelligence provider via the Palo Alto Networks MineMeld app for AutoFocus, integration into third-party systems
	CUSTOM DASHBOARD AVAILABLE	Yes	Yes	No	Yes
	ZERO DAY DETECTION	Yes	Yes	Yes	Yes
	DARK WEB RESEARCH CAPABILITIES	No Data Available	Yes	Yes	No*
	TAILORED THREAT INTEL	Yes	Yes	No	Yes
	MALWARE ANALYSIS CAPABILITIES	Yes	Yes	Yes	Yes
	DELIVERY MECHANISM	SaaS based	Delivered by API integration, intellgience portal & email	Signature Feeds, Reports and briefings, Analysis Services	SaaS-based security services
SUPPORT	STIX &TAXXI SUPPORT	Data Unavailable	Yes	Not Applicable	Yes
NOTES		*Details about Crowdstrike prices can be found at https://www.cybersecuritypricing.org/tag/crowdstrike-pricing/ ** Crowdstrike offers a variety of threat intelligence products. The above listed are some common solutions offered across products	Large customer base in North America. Used across sectors like Finance and Government Fireye also provides a dedicated point-of-contact for every customer. Useful for emergent threats and zero-days Fireye also provides a dedicated POC	BAE systems has partnered with various govermnet agenicies in the past. Established a repution for providing suitable and actionable intelligence to customers.	*Palo Alto Network teamed up with another vendor Intsights so that IntSights can integrate with the Palo Alto TIP. IntSights has darkweb capabilities, Palo Alto does not have a dark web capabilities by itself.

FACTORS TO CONSIDER WHILE EVALUATING TIPS (CONTINUED)

	RECORDED FUTURE	ANAMOLI	SECUREWORKS	MCAFEE
ORG. DETAILS				
WEBSITE	https://www.recordedfuture.com/	https://www.anomali.com/products/threatstream	https://www.secureworks.com/services/threat-intelligence	https://www.mcafee.com/enterprise/en-us/solutions/advanced-threat-management.html
FOUNDED	2009	2013	1999	1987
COUNTRY OF ORIGIN	USA	USA	USA	USA
PRICING				
SUBSCRIPTION	Offers four different licence types with varying capabilities	Varies based on customer	Annual subscription. Actual price depends on the size of the organization	1 Year Licenses
CAPABILITIES				
SERVICES PROVIDED	Brand Protection Third-party risk Secops and Response Geopolical Risk	Data collection from multiple sources and formats Normalization, enrichment, removal of duplicates and false positives Integration with security tools such as SIEMs, firewalls, etc. Workflows and functionalities to analyze and share data Brand monitoring (automatic search for typosquatted domains & compromised credentials) Sandboxing (research malicious indicators within the platform) Extracting data from suspected phishing emails for immediate blocking	Malware analysis, reverse engineering, managed security, security and risk consulting, incident response, and cloud security, end point security, security orchestration, network security	McAfee VirusScan, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager, and from third party vendor products sending information over McAfee Data Exchange Layer, Global Threat Intelligence, Enterprise Security Manager, Threat Intelligence Exchange *
CUSTOM DASHBOARD AVAILABLE	Yes*	Yes*	No	Yes
ZERO DAY DETECTION	Yes	Yes	Yes	Yes
DARK WEB RESEARCH CAPABILITIES	Yes	Yes	No Data Available	No Data Available
TAILORED THREAT INTEL	Yes	Yes	Yes	Yes
MALWARE ANALYSIS CAPABILITIES	Yes*	Yes	Yes	Yes
DELIVERY MECHANISM	SaaS based**	Available as a SaaS, on-premises, or hybrid solution	SaaS	On premises or SaaS based
SUPPORT				
STIX &TAXXI SUPPORT	Yes	Yes	Yes	Yes
NOTES	A review done by Matthew Hreben by SC Magazine rated Recorded Future 5/5 in the fields of Features, Documentaion, Performance, Integration and Support. Recorded Future provides Malware Hashes ** Integrates well with REST based APIs	Anamoli also has a custom splunk app, integrating their feed into the enterprise Splunk instance. This will make ingestion and analysis easy.	Does not have dedicated point of contact	McAfee Threat Intelligence products leverage their wide array of security products for seamless integration and data ingestion. This provides a considerable advantage for the customer in terms of timing, efficiency and structure of intelligence. McAfee also provides situational awareness intelligence

References

[1] Pokorny, Zane, et al. *The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program.* 2nd ed., CyberEdge Group LLC, 2019, https://go.recordedfuture.com/hubfs/ebooks/threat-intelligence-handbook-second-edition.pdf?utm_campaign=THR-EBO-1019&utm_source=hs_automation&utm_medium=email&utm_content=78663535&_hsenc=p2ANqtz-8QzMolYUnF4j4oi6GXtPmfQm1MNaBMckwUrgUQ75fu7uqJrwttjE58gSsPaU3xTWK7rVHeaRJyCZSc1gtCV_qt-wI2QQ&_hsmi=78663535. Accessed 17 April 2020.

[2] Ettinger, Jared, et al. *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States.* Software Engineering Institute (SEI), 2019, resources.sei.cmu.edu/asset_files/EducationalMaterial/2019_011_001_546699.pdf. Accessed 23 February 2020.

[3] Office of the Director of National Intelligence. *U.S. National Intelligence: An Overview*. US Government, 2011, https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf. Accessed 17 April 2020.

[4] Central Intelligence Agency. *The Intelligence Cycle*. US Government, 2013, https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html. Accessed 17 April 2020.

[5] *The Threat Intelligence Handbook Second Edition.* Recorded Future, https://go.recordedfuture.com/hubfs/ebooks/threat-intelligence-handbook-second-edition.pdf?utm_campaign=THR-EBO-1019&utm_source=hs_automation&utm_medium=email&utm_content=78663535&_hsenc=p2ANqtz-8QzMolYUnF4j4oi6GXtPmfQm1MNaBMckwUrgUQ75fu7uqJrwttjE58gSsPaU3xTWK7rVHeaRJyCZSc1gtCV_qt-wI2QQ&_hsmi=78663535. Accessed 27 March 2020.

[6] Townsend, Troy, et al. *SEI Innovation Center Report: Cyber Intelligence Tradecraft Project Summary of Key Findings.* Software Engineering Institute, January 2013, https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf). Accessed 27 March 2020.

[7] PricewaterhouseCoopers and BAE Systems. *Operation Cloud Hopper*. PWC, 2017, April, https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf. Accessed 19 April 2020.

[8] Crucq, Parker. *Threat Analysis Insights: Weekly Threat Intelligence Report Template.* Recorded Future, 5 March 2019, https://www.recordedfuture.com/threat-intelligence-report-template/. Accessed 16 February 2020.

[9] *Cyber Threat Intelligence and Incident Response Report.* Zelster, https://zeltser.com/media/docs/cyber-threat-intel-and-ir-report-template.pdf. Accessed on 23 February 2020.

[10] Camacho, Chris. *Don't Overlook Geopolitics in Threat Intelligence.* Infosecurity Magazine, 4 April 2019, https://www.infosecurity-magazine.com/opinions/geopolitics-threat-intelligence-1-1-1/. Accessed on 23 February 2020.

[11] Directorate of Intelligence. *Style Manual & Writers Guide for Intelligence Publications*. Central Intelligence Agency, 2011, https://fas.org/irp/cia/product/style.pdf. Accessed 26 April 2020.

[12] *Analytical Thinking and Presentation for Intelligence Producers: Analysis Training Handbook.* Office of Training and Education, http://index-of.co.uk/Tutorials-2/CIA%20%20Analytic%20Thinking%20and%20Presentation%20for%20Intelligence%20-%20Analysis%20Training%20Handbook.pdf. Accessed 16 February 2020.

[13] Asplund, Jan-Erik. *BLUF: The Military That Can Make Your Writing More Powerful.* Animalz, 9 September 2019, https://www.animalz.co/blog/bottom-line-up-front/. Accessed 3 February 2020.

[14] Paredes, Christian. *Pen to Paper& the Finished Report: The (Often Overlooked) Key to Generating Threat Intelligence.* Sans Institute, https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492113075.pdf. Accessed 3 February 2020.

[15] *A Guide to Cyber Attribution.* Office of the Director of National Intelligence, 14 September 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf. Accessed 16 February 2020.

[16] Clapper, James. *Intelligence Community Directive 203.* Office of the Director of National Intelligence, 2 Jan. 2015. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf. Accessed 23 February 2020.

[17] Cybersecurity and Infrastructure Security Agency (CISA). *Traffic Light Protocol (TLP) Definitions and Usage*. US Department of Homeland Security, N.D., https://www.us-cert.gov/tlp. Accessed 27 April 2020.

[18] Central Intelligence Agency. *President's Daily Brief*. CIA, 2016. https://www.cia.gov/library/readingroom/presidents-daily-brief. Accessed 23 February 2020.

[19] Caltagirone, Sergio, Pendergast, Andrew, and Betz, Christopher. *The Diamond Model of Intrusion Analysis*. US Department of Defense, 2013, apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf. Accessed 22 February 2020.

[20] Krebs, Brian. *Krebs on* Security blog. krebsonsecurity.com. Accessed 23 February 2020.

[21] MITRE. *CVE List Home*. cve.mitre.org/cve. Accessed 23 February 2020.

[22] Google. *Google Translate*. translate.google.com. Accessed 23 February 2020.

[23] Duolingo. *Learn a language for free. Forever.* Duolingo, 2020, https://www.duolingo.com/. Accessed 24 April 2020.

[24] Central Intelligence Agency. *The World Factbook.* US Government, 2020, https://www.cia.gov/library/publications/the-world-factbook/. Accessed 24 April 2020.

[25] BBC News. *Country Profiles.* BBC News, 2019, http://news.bbc.co.uk/2/hi/country_profiles/default.stm. Accessed 24 April 2020.

[26] IBM. *IBM i2 Analyst's Notebook.* IBM, 2020, https://www.ibm.com/us-en/marketplace/analysts-notebook. Accessed 22 April 2020.

[27] Central Intelligence Agency. *Offices of CIA*. CIA, 2015. https://www.cia.gov/offices-of-cia/intelligence-analysis/careers-1. Accessed 23 February 2020.

[28] Heuer, Jr., Richards J. *Psychology of Intelligence Analysis*. Washington, D.C., Central Intelligence Agency, 2012. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf. Accessed 23 February 2020.

[29] George, Roger Z. and Bruce, James B. *Analyzing Intelligence: Origins, Obstacles, and Innovations.* Washington, D.C., Georgetown University Press, 2008. https://epdf.pub/analyzing-intelligence-origins-obstacles-and-innovations.html. Accessed 23 February 2020.

[30] Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, Eighth Edition. Thousand Oaks, California, CQ Press, 2020. https://www.ebookphp.com/intelligence-from-secrets-to-policy-epub-pdf/. Accessed 23 February 2020.

[31] Jones, Morgan D. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. New York City, New York, Three Rivers Press, 1998. https://www.nwcbooks.com/get/ebook.php?id=oYojFVG7UqgC. Accessed 23 February 2020.

[32] Center for the Study of Intelligence. *Studies in Intelligence*. CIA, 2020. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html. Accessed 23 February 2020.

[33] Morell, Michael and Gordon, Susan. "Former top DNI official Sue Gordon discusses circumstances of her departure from ODNI." *Intelligence Matters,* CBS News, 14 Feb. 2020. https://www.cbsnews.com/news/former-top-dni-official-sue-gordon-discusses-circumstances-of-her-departure-from-odni-transcript/. Accessed 23 February 2020.

[34] MITRE. *ATT&CK*. Mitre, 2019. https://attack.mitre.org/. Accessed 23 February 2020.

[35] Smith, R.J. *Coordination and Responsibility.* CIA, 1993. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol1no4/html/v01i4a03p_0001.htm. Accessed 23 February 2020.

[36] Central Intelligence Agency. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. U.S. Government, 2009. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf. Accessed 23 February 2020.

[37] Heuer, Jr., Richards J. and Pherson, Randolph H. *Structured Analytic Techniques for Intelligence Analysis.* Washington, D.C., CQ Press, 2011. https://all-med.net/get/ebook.php?id=R6qiDwAAQBAJ&file=Structured%20Analytic%20Techniques%20for%20Intelligence%20Analysis. Accessed 23 February 2020.

[38] Cyber Kill Chain. (n.d.). Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[39] Threat Intelligence: Everything You Need to Know. (n.d.). Retrieved from https://www.recordedfuture.com/threat-intelligence/

[40] News Team. (2019, August 13). Nation State Threats. Retrieved from https://www.cyberdefensemagazine.com/nation-state-threats/

[41] *Defining Threat Intelligence Requirements*. (n.d.). SANS Internet Storm Center. Retrieved April 19, 2020, from https://isc.sans.edu/forums/diary/Defining+Threat+Intelligence+Requirements/21519/

[42] *Developing Priority Requirements*. (n.d.). Retrieved April 19, 2020, from https://fas.org/irp/doddir/army/fm34-2/Appd.htm

[43] *Threat Analyst Insights: How to Develop Effective Intelligence Requirements.* (2018, November 07). Retrieved April 19, 2020, from https://www.recordedfuture.com/effective-intelligence-requirements/

[44] Department of Homeland Security. *Performance Measures Definitions Gujde: Measuring the Performance of the National Network of Fusion Centers*. US Government, April 2014.

[45] Clapper, James. *Intelligence Community Directive 204.* Office of the Director of National Intelligence, 2 January 2015, https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf. Accessed 23 February 2020. Accessed 26 April 2020.

[46] Nickels, Katie. *Getting Started with ATT&CK: Threat Intelligence*. 10 June 2019. https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f.

[47] Kure, Halima Ibrahim, Shareeful Islam and Mohammed Abdur Razzaque. "An Integrated Cyber Security Risk Management." 30 May 2018. *MDPI*

[48] Recorded Future. *How Security Intelligence Enables Risk-Prioritized Vulnerability Management* . 18 March 2020. https://www.recordedfuture.com/vulnerability-management-prioritization

[49] Lee, R. (2019). SANS CTI. Retrieved from https://www.domaintools.com/content/SANS_CTI_Survey_2019.pdf

[50] https://www.darkreading.com/vulnerabilities---threats/how-to-roll-your-own-threat-intelligence-team/a/d-id/1326445

[51] https://www.recordedfuture.com/threat-intelligence-analyst-job-description/

[52] https://www.bankinfosecurity.com/building-cyber-intelligence-team-a-4185

[53] Newhouse, William, et al. *NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. Nation Institute of Standards and Technology, August 2017, https://doi.org/10.6028/NIST.SP.800-181. Accessed 17 March 2020.

[54] https://www.crowdstrike.com/epp-101/threat-intelligence/#types

[55] https://cyber-edge.com/wp-content/uploads/2018/11/Recorded-Future-eBook.pdf#p90

[56] *Recorded Future*. (n.d.). Recorded Future for Threat Intelligence. Retrieved April 19, 2020, from https://www.recordedfuture.com/solutions/threat-intelligence/

[57] *The 'REAL' Distinction of Threat Intelligence Platforms*. (2019, May 09). Retrieved April 19, 2020, from https://www.threatq.com/threat-intelligence-platforms-distinction/

[58] *How to choose the right threat intelligence services.* (n.d.). Retrieved April 19, 2020, from https://www.kaspersky.com/blog/threat-intelligence-forrester-wave/24740/

[59] Cole, D. (2020, January 02). *How to Choose the Right Threat Intelligence Platform for You* - ThreatConnect: Intelligence-Driven Security Operations. Retrieved April 19, 2020, from https://threatconnect.com/blog/how-to-choose-the-right-threat-intelligence-platform-for-you/

[60] Tittel, E. (2017, April 04). *Five criteria for purchasing from threat intelligence providers.* Retrieved April 19, 2020, from https://searchsecurity.techtarget.com/feature/Five-criteria-for-purchasing-threat-intelligence-services

[61] *How to Evaluate Threat Intelligence Platform Features ...* (n.d.). Retrieved April 19, 2020, from https://www.msspalert.com/cybersecurity-services-and-products/threat-intelligence/how-to-evaluate-platforms/

[62] Chairman of the Joint Chiefs of Staff. *Joint Publication 2-0: Joint Intelligence.* U.S. Military, 2013, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf. Accessed 17 April 2020.

[63] Recorded Future. *Machine Learning: Practical Applications for Cybersecurity.* Recorded Future, March 2018, https://www.recordedfuture.com/machine-learning-cybersecurity-applications/. Accessed 26 April 2020.

[64] Drinkwater, Doug. *5 Top Machine Learning Use Cases for Security.* CSO Online, December 2017, https://www.csoonline.com/article/3240925/5-top-machine-learning-use-cases-for-security.html. Accessed 26 April 2020.

[65] Connor-Simons, Adam. *System predicts 85 percent of cyber-attacks using input from human experts*. MIT News, April 2016, http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418. Accessed 26 April 2020.

[66] Truve, Staffan. *4 Ways Machine Learning is Powering Smarter Threat Intelligence*. Recorded Future, No Date, https://go.recordedfuture.com/hubfs/white-papers/machine-learning.pdf?utm_campaign=ML-WP&utm_source=hs_automation&utm_medium=email&utm_content=53413311&_hsenc=p2ANqtz-8DKtuQZF6pqCD96M7CkvCkHmNXuZinR0V7akb019bR8dodN_my6hwsHUz2pRLE89AabOFxUMcG5KbKpxIxUHsNaz-P1g&_hsmi=53413311. Accessed 26 April 2020.

[67] A quote from The Art of War. (n.d.). Retrieved April 22, 2020, from https://www.goodreads.com/quotes/17976-if-you-know-the-enemy-and-know-yourself-you-need