Global Information Assurance Certification Paper

Cyber Threat Intelligence Support to Incident Handling

GIAC (GCIH) Gold Certification

Author: Brian P. Kime, bkime@mastersprogram.sans.edu
Advisor: Sally Vandeven
Accepted: November 2017

Abstract

Recent research has shown increased awareness of Cyber Threat Intelligence (CTI) capabilities. However, CTI teams continue to be underutilized and have had difficulty demonstrating the value they can add to digital forensics incident response (DFIR) teams. Meta-analysis of multiple surveys will identify where the gaps in knowledge exist. The paper will suggest how CTI can support DFIR at each level of intelligence and operations – tactical, operational, and strategic – and during each phase of the incident response lifecycle – preparation; detection and analysis, containment, eradication, and recovery; and lessons learned. CTI teams should have priority intelligence requirements (PIRs) and a collection plan that supports answering those PIRs. In return, DFIR needs to share investigations and incident reports with the CTI team to reduce risk to the organization, decrease the time to detect an incident and decrease the time to remediate an incident. This paper builds on previous work by the author to develop CTI processes to support CTI planning.

1. Introduction

Organizations face a deluge of security alerts. The teams responsible for handling security alerts and incidents are often overwhelmed and suffer from alert overload. This paper explores the information gaps in the incident handling process and presents solutions for how cyber threat intelligence can reduce risk at the tactical, operational, and strategic levels of cybersecurity.

1.1. The Incident Response Life Cycle

Four major phases comprise the NIST Incident Handling Process which serves as a guide for an incident handler. The preparation phase is where the organization collects the people, policies, data, and tools necessary to remediate an incident quickly and completely. The second phase of the process is detection and analysis and involves triaging security events from the organization's network perimeter, host perimeter, system-level activity, application-level activity, or users; it also involves declaring an incident. Upon declaration of an incident, the organization will begin the containment, eradication, and recovery phase. During this phase, the threat may continue its course of action. Often, incident handlers will move back and forth between the second and third phases during an incident response as new information becomes available about the threat. Lastly, in the post-incident activity phase, the incident response team prepares the post-incident report and applies solutions to improve the process for the next incident (Cichonski, Millar, Grance, & Scarfone, 2012). A visual depiction of the cycle is in Figure 1 below. The faster incident handlers can move through the cycle the less damaging cyber-attacks are upon a targeted organization.

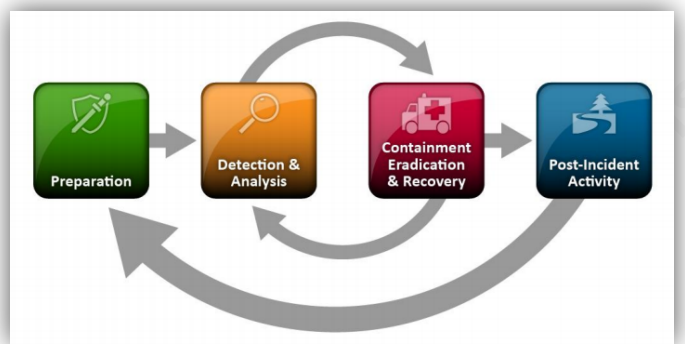

Figure 1: The NIST Incident Response Life Cycle (Cichonski, Millar, Grance, & Scarfone, 2012)

1.2. The Intelligence Cycle

The basic intelligence process is, in many ways, like the incident response lifecycle. Briefly, the Intelligence Cycle is a continuous five-step process conducted by intelligence teams to provide leadership with relevant and timely intelligence to reduce risk and uncertainty. The five steps are: planning and direction; collection; processing and exploitation; analysis and production; and dissemination and integration. A graphical depiction of the Intelligence Cycle is below in Figure 2. Throughout the intelligence cycle, teams require feedback and evaluation from management (Kime, 2016). As during the incident handling process, Intelligence teams often move back and forth between the second through fourth steps of the cycle as new information and requirements are identified.

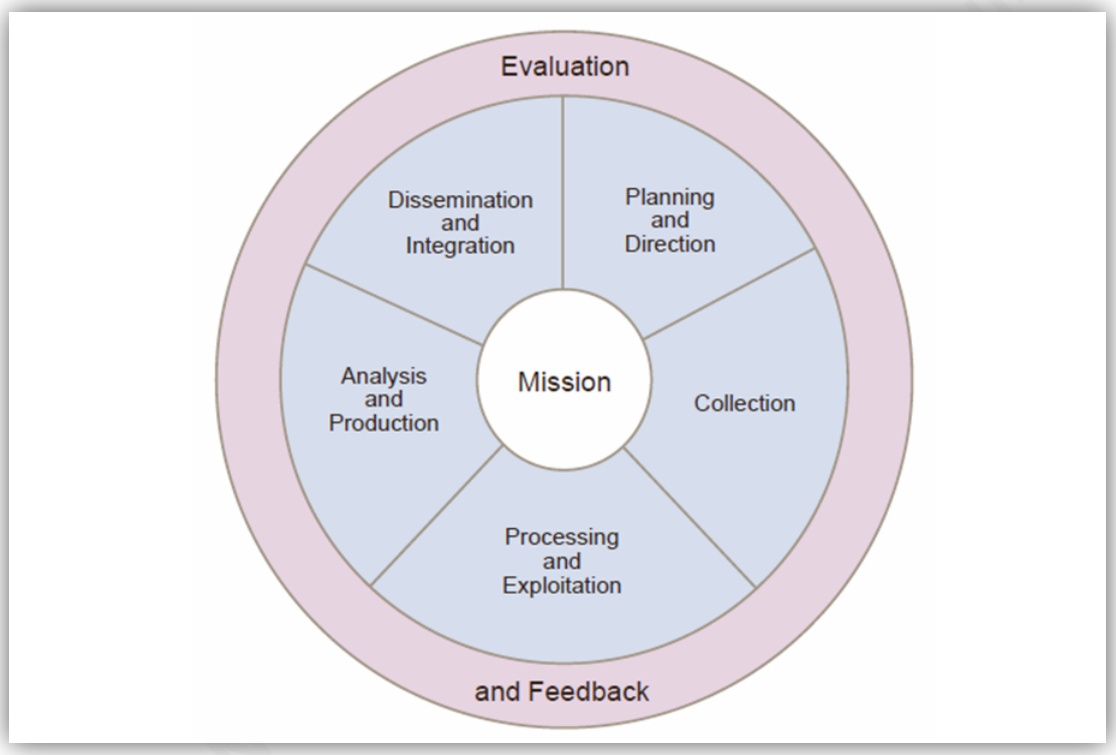

Figure 2: The Intelligence Cycle ("JP 2-0", 2013)

1.3. Intelligence Preparation of the Cyber Operational Environment

Intelligence Preparation of the Cyber Operational Environment (IPCOE) is a systematic, continuous process of analyzing potential threats to detect a suspicious set of activities that might threaten the organization's systems, networks, information, employees, or customers. The process provides a means of visualizing and assessing numerous specific intrusion sensor inputs and open source information to infer specific threat courses of action ("ATP 2-01.3", 2014).

IPCOE supports the organization's risk management strategy and the information security group's decision-making. Applying IPCOE identifies potential threats' courses of action and helps the security and risk management leaders selectively apply and maximize a defense in depth strategy via a greater understanding of the organization's cyber threats at critical points in time and space in the operational environment. The

process has four steps depicted in Figure 3 below (Kime, 2016). Step 1, Define the Operational Environment, identifies for further analysis the significant characteristics of the operational environment that may influence the organization's defense-in-depth strategy and tactics (Kime, 2016). Step 2, Describing the Operational Environment's effects on Network Defense, determines how significant characteristics of the operational environment can affect defensive operations and threat operations (Kime, 2016). Step 3, Evaluate the Cyber Threats, determines threat capabilities and the doctrinal principles and tactics, techniques, and procedures threats prefer to employ (Kime, 2016). Step 4, Developing Cyber Threat Courses of Action, identifies and describes threat courses of action that can influence information security operations (Kime, 2016). Upon completion of IPCOE, the intelligence team has the necessary information to recommend Priority Intelligence Requirements (PIRs) and build an intelligence collection plan capable of answering management-approved PIRs

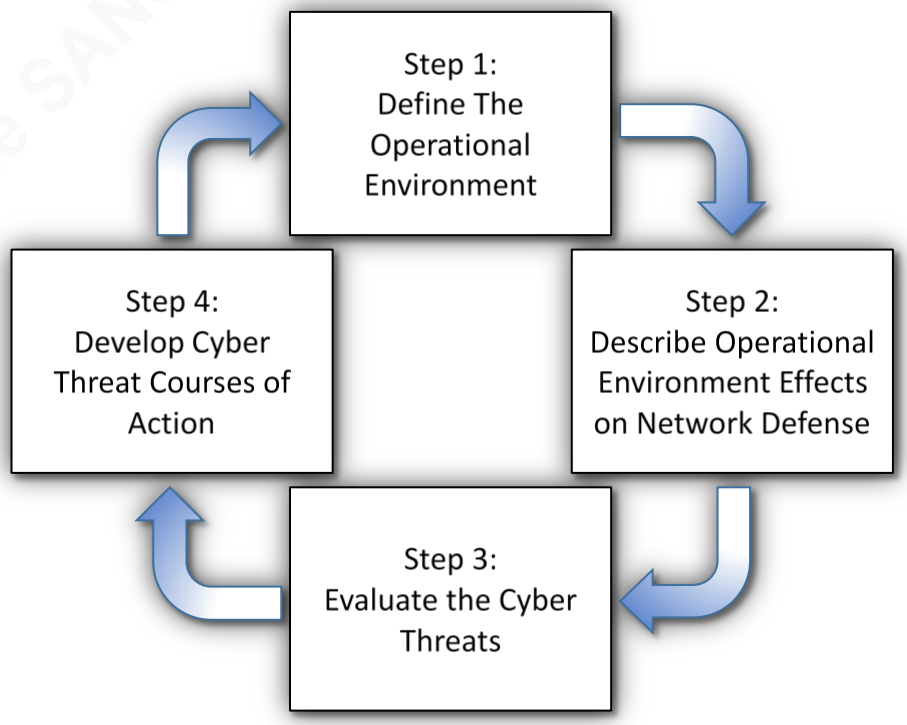

Figure 3: Intelligence Preparation of the Cyber Operational Environment (Kime, 2016)

1.4. The Levels of Intelligence

Cyber operations occur at the tactical, operational, and strategic levels. Thus, the intelligence that supports a leader's decision-making must also exist at those same levels. As the tactical level is where defenders and threat actors engage each other. Intelligence at this level is focused mostly on indicators of compromise (IOCs), rules, and signatures that enrich security controls to detect or prevent specific malicious activity. Multiple tactical events (port scanning, exploit delivery, establishing backdoors, exfiltration of data.) are combined to conduct operations or campaigns against a target. Intelligence at the operational level reveals adversary trends, expanding capabilities, operational cycles, and more which enables decision-makers to configure security controls and network architecture to achieve strategic goals of preventing data breaches and attacks. Multiple operations or campaigns are conducted to fulfill strategic goals. At the strategic level, intelligence helps decision makers determine security objectives and how to resource to accomplish those objectives (INSA, 2013). Figure 4 shows the interrelationships between each level of cyber threat intelligence. Intelligence at all three levels is necessary for security organizations to set the right policies, budgets, people, process, and tools to successfully defend an enterprise.

Figure 4: Cyber Threat Intelligence Responsibilities and Interrelationships (INSA, 2013)

2. Identified Gaps in CTI Support to Incident Handling

Multiple organizations, including the SANS Institute and Ponemon Institute, have surveyed information security leaders in recent years regarding their usage of cyber threat intelligence. These survey results have been analyzed to identify patterns and gaps in the information security community's usage of CTI to support incident handling. Ponemon picked up on a general theme in 2015 when they asked how accurate, timely, and actionable threat intelligence is for a company. See Figure 5 below. Their survey queried participants on a scale of 1(lowest) to 10 (highest) the accuracy, timeliness, and actionability of their intelligence. The results skewed heavily towards the low (immature) end of the spectrum. Furthermore, only about 10% of respondents felt their intelligence was at the upper end of the scale (Ponemon, 2015). For CTI to be add value and reduce risk in an organization, it must be accurate, timely, and actionable.

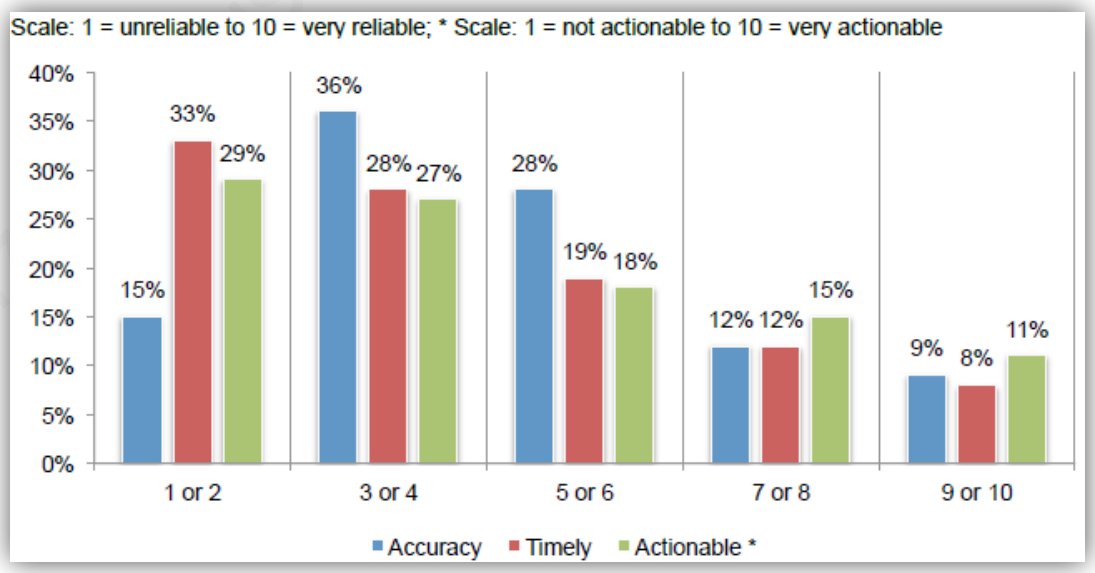

Figure 5: How accurate, timely, and actionable is an organization's threat intelligence? (Ponemon, 2015)

2.1. Tactical level gaps

At the tactical level, the SOC needs timely, accurate, and actionable information to detect malicious activity and confirm security events as true or false positives. According to Ponemon, an average of 35 percent of all cyber attacks are undetected.

Eighty-six percent of respondents say detection of a cyber attack takes too long and 85 percent say there is little or no prioritization of incidents (Ponemon, 2014). Forty percent of respondents said none of their security products support the import of threat information from other sources while only 17 percent reported that all of their security products did support importing threat information. (Ponemon, 2014). Security tools need to be able to ingest various types and formats of tactical threat information to detect a wide range of modern cyber threats. Without accurate, timely, and actionable intelligence information, security tools are less likely to detect indications of a breach or attack.

There are many vendors and free sources for tactical threat information. Unsurprisingly, 32 percent of organizations responding in 2014 had plans to onboard a dedicated threat intelligence service according to Cyberedge Group (Cyberedge, 2015). That survey also showed that primary uses for threat intelligence are detecting and blocking threats and less for investigating threats (Cyberedge, 2015). The key justification for tactical threat intelligence usage appears to be a further hardening of the perimeter. Conversely, Ponemon reported that security operations are the primary or secondary users of threat intelligence in 44% and 41% of organizations that responded (Ponemon, 2016). While threat intelligence vendors appear to be focusing on monetizing IOCs, organizations are not necessarily prioritizing integrating tactical intelligence into security operations. The plethora of standards (ex: STIX, OpenIOC) may be increasing the challenges of integrating tactical threat intelligence data into security controls.

2.2. Operational level gaps

Assessing risk from specific threat groups is one of the most challenging tasks for analysts functioning at the operational level. In 2016, Ponemon, asked respondents to enumerate their primary and secondary users of threat intelligence. Security leaders (Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs)) and incident response teams were the top two primary users suggesting a focus on CTI at the operational level (Ponemon, 2016). However, Cyberedge's respondents rated zero-day vulnerabilities as their second highest extreme concern – trailing only phishing (Cyberedge, 2015). This result shows a lack of awareness of which threats are most likely

to target an organization. As Rob Joyce, chief of NSA's Tailored Access Operations said at USENIX Enigma 2016, "A lot of people think that nation states are running their operations on zero days, but it is not that common. For big corporate networks, persistence and focus will get you in without a zero-day. There are more vectors that are easier, less risky, and more productive" (Joyce, 2016). To summarize, those organizations which concern themselves disproportionally with the "zero-day threat" are not producing actionable operational level intelligence for the CISO and CSO.

2.3. Strategic level gaps

To help drive the overall cyber risk management process, business leaders need actionable strategic cyber threat intelligence. However, Ponemon discovered strategic level decision makers were the least likely to be primary users of CTI (Ponemon, 2016). Only 3% of responses named the C-suite as primary users, and none named the Board of Directors (Ponemon, 2016). As secondary users of CTI, the C-suite was ahead of the Board of Directors, procurement, non-IT management, and business continuity management. The Board of Directors ranked only above procurement (Ponemon, 2016). As recently noticed in the massive Equifax incident, the lack of strategic cybersecurity planning by Boards and C-suites will lead to unprepared organizations caught in the middle of significant data breaches.

3. Opportunities for CTI Support to Incident Handling

3.1. Tactical Level

At the tactical level of intelligence, organizations are primarily concerned with supporting those individuals and teams on the 'front lines' of defending the network. These teams typically include the SOC, NOC, and service desk as they are the first to see reports of possible malicious activity. In the case of a data breach, the incident response team is the CTI team's primary customer at the tactical level.

A table broadly depicting the items CTI teams should be tasked with at the tactical level can be found in Table 3 in Appendix 1.

3.1.1. Preparation

Collection of threat information is not enough to prepare for an incident and to reduce risk by itself. Mature threat intelligence teams assess each source of threat information for reliability and information content. For technical sources, they determine whether the data source is current, updated frequently, and if it is free of false positives. An Admiralty System (also known as an intelligence source and information reliability matrix) can greatly aid in the evaluation of CTI information sources. For human sources (e.g. journalists, industry peers, vendor researchers, cyber personas) the US Army Human Intelligence Collector Operations manual offers an easy solution. Each source is evaluated on reliability (from cannot be judged to reliable) and information content (from cannot be judged to confirmed). See Table 1 for a full description of the admiralty system for human sources. It is wise to also rate technical sources (ex: internal logs, free threat information feeds, paid threat information feeds) as well. Table 2 is an option for rating technical feeds and can be used to rate a technical source's frequency of updates and false positive rate. Knowing which sources are more timely, accurate, and actionable allows for better intelligence analysis and more efficient and complete assessment of security alerts by the SOC.

Source Reliability		
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 basis** exists for evaluating the reliability of the source
Information Content		
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 basis** exists for evaluating the validity of the information

Table 1: Admiralty System for Human Sources (FM 2-22.3, 2006)

	Update Frequency	
A	**Real-time**	The actual time during which a process or event occurs; within **milliseconds**
B	**Near real-time**	Delay of **several seconds to several minutes** between the event and availability of the information
C	**Daily**	Source of information updated **daily**
D	**Weekly**	Source of information updated **weekly**
E	**Monthly**	Source of information updated **monthly or less often**
F	**Cannot be Judged**	**No basis** exists for evaluating the reliability of the source
	Information Accuracy	
1	**Completely Free of False Positives**	**100%** true positives
2	**Almost Free of False Positives**	**90 - 99%** true positives
3	**Mostly Free of False Positives**	**75 - 89%** true positives
4	**Some False Positives**	**50 - 74%** true positives
5	**Mostly False Positives**	**< 50%** true positives
6	**Cannot be Judged**	**No basis** exists for evaluating the validity of the information

Table 2: Admiralty System for Technical Sources

Analysts should consider hash values, IP addresses, domains, and rules like Snort and Yara tactical threat information. They should consider integrating the sources with the most reliable and trustworthy data (see Admiralty Systems above) into active tools (ex: IPS, email gateways, content filtering) to block malicious activity outright. Security teams should then integrate less reliable and trustworthy data into passive tools (IDS, SIEM) to detect possible malicious activity that requires additional human analysis to determine the nature of the threat. To block a greater amount of true malicious activity, analysts must use admiralty systems to determine which information sources to use in active tools.

Brian P. Kime

Automating enrichment of IOCs is another area where tactical CTI can reduce risk and decrease the time between detection and remediation of a security event. Many useful sources of threat information make use of application programming interfaces (APIs) to integrate with other tools. Organizations should consider using APIs and paid subscriptions for those services which automatically provide a SOC analyst with the data needed to make quicker decisions on the level of threat observed. For example, if a SOC analyst is assessing an alert for a blocked website he or she would benefit from having WHOIS data – to include the age of the domain and hosting history – and any history of malware related to the domain in the case without having to manually query that additional data. Presenting a more holistic picture of the threat to the analyst will reduce the time an analyst spends on an alert and increase the events per analyst per hour in the SOC.

A security organization should consider user awareness and training as a part of the preparation phase of incident handling (Cichonski, Millar, Grance, & Scarfone, 2012). As intelligence teams represent the threat in planning for incident handling, organizations should consult with CTI teams when running phishing exercises. If a CTI team includes the organization's internal red team, then consider directing CTI to manage the phishing program. Security teams should represent current threats with intelligence-driven phishing exercises to ensure users identify and report relevant malicious activity.

3.1.2. Detection and Analysis

Prevention should not be the only goal of consuming tactical threat intelligence. While CTI activities in the preparation phase improve the SOC's performance in the detection and analysis phase, there is important work for intelligence teams in the detection and analysis steps. Not easily automated at scale is threat hunting. It takes a human analyst's intuition and tenacity to find what malicious activity may be lurking undetected in a network. While the SOC is triaging security alerts and the incident response team is investigating true positive breaches of confidentiality, integrity, and availability, CTI teams should actively hunt for unknown malicious activity. Relationships with peer organizations, information sharing and analysis centers, trust

groups, and law enforcement partners are critical to informing the CTI team of incidents outside of the organization. The intelligence shared via these relationships should drive hunting activities by the CTI team to detect unknown malicious activity.

In US Army infantry battalions and brigades, tactical intelligence officers must understand tactics or risk becoming irrelevant. The same truths are present in the cybersecurity world. For CTI analysts to accurately represent the threat during security event analysis, the analyst must have a keen knowledge of cyber threat actor (CTA) tactics. To overcome any lack of confidence, intelligence analysts should understand that despite their lack of reverse engineering and volatile memory analysis experience compared to their DFIR counterparts, they make up for it with access to the organization's vast intelligence data and singular focus on cyber threat actors. CTI, therefore, must ensure a shared understanding of the cyber threat actors targeting the organization to guarantee accurate analysis of security events and proper escalation of potential breaches of confidentiality, integrity, or availability. The team should own and maintain a platform for storing, enriching, and correlating internal and external intelligence data using taxonomies like the Lockheed Martin Cyber Kill Chain, the Diamond Model of Intrusion Analysis, and MITRE ATT&CK.

Computer security incidents can vary greatly from routine commodity malware to sophisticated incidents that combine several attacks and exploits. For many organizations, the most challenging part of the lifecycle of an incident is accurately assessing the magnitude and tailoring the response (Cichonski, Millar, Grance, & Scarfone, 2012). From the intelligence team's robust database of threats and security events, they are in great position to help plan the incident response team's containment, eradication, and recovery actions to reduce the risk of an ineffective response. CTI analysts should consult with trusted contacts who may have knowledge of the threat actor and potential threat courses of action. Security teams should always involve a member of their CTI team during the detection and analysis steps of the incident handling lifecycle.

3.1.3. Containment, Eradication, and Recovery

The SOC, NOC, or service desk will usually resolve security events that do not breach confidentiality, integrity, or availability without engaging the incident responders. However, some events may still warrant containment actions. For example, a threat using an open source vulnerability scanner will likely trigger an IDS alert. CTI can find or create rules to block that open source vulnerability scanner at the organization's perimeter to reduce the number of alerts in the future and the threat's visibility.

Containing a breach is a delicate manner and incident handlers need to be respectful of the threat. It is natural for security teams to want to block IPv4 ranges and remove malware immediately. However, mature threats are likely to have multiple backdoors and change hop points to connect to their victims. As the CTI team should have a robust database of threat templates and infrastructure, they need to advise the SOC and IR team during the containment step or risk losing visibility of the threat and triggering unplanned responses from the threat. For example, if a threat is siphoning data it may be useful to plant false data or documents laced with tracking pixels to raise the risk to the threat and increase the likelihood of attribution. At the same time, rate limiting the connection siphoning data helps to contain the threat's actions on the objective. An intelligence-driven containment plan should reduce the impact of breaches and simultaneously not tip off threats to their discovery by the incident responders.

Sometimes, eradicating adware and potentially unwanted programs (PUPs) may not thoroughly remove all risks using operating system uninstall tools. Often installed in bundles with other free software, PUPs may continue to generate low priority alerts on an affected endpoint. In those scenarios, CTI should ensure its customers have the information needed to identify and eradicate all risks that have not resulted in a data breach.

Eradicating a well-resourced and intelligent threat is orders of magnitude more complicated than eradication of PUPs. Again, as the keepers of the organization's intelligence information, the CTI team should drive eradication of threat actors in the wake of a data breach. The CTI team should aggressively hunt for indicators of the

specific threat actor in all available data sources – internal and external – to ensure comprehensive eradication of the threat. Only through robust data collection and enumeration of indicators can an organization effectively eradicate a threat from their environment.

There are several recovery actions where CTI can play a role. Before administrators return affected systems to production, the CTI team should be consulted to ensure the exploited vulnerabilities – software, hardware, configuration, and human – are scheduled to be addressed. Monitoring of threat actor communications channels can help confirm all vulnerabilities have been remediated.

3.1.4. Post-Incident Activity

As the SOC closes event cases and the IR team closes incidents, CTI should identify what information analysts and responders could have used to reduce the time to detection and remediation and assess new sources of information. Identifying missing or late information should occur during the lessons learned meetings with the incident responders. For example, if free passive DNS sources did not provide current or complete data, the CTI team should consider a paid passive DNS service that can provide the SOC the robust data needed to assess security events accurately and quickly. Reassessing IOC and rule sources for reliability and trustworthiness and regularly evaluating tactical data sources, what those data sources feed, and how the SOC analysts use that information ensures the organization is tactically prepared to assess malicious activity.

Having a robust database of events and incidents is important for linking other malicious activity, forecasting, reporting metrics to management and evaluating the reliability and fidelity of IOC and rule sources. Once a security event is assessed as a true positive and the case is closed, relevant information (to include hash values, IP addresses, domains, network artifacts, and tools) should be cataloged automatically in a threat intelligence platform. Tactical data collection supports the production of operational and strategic intelligence.

3.2. Operational Level

At the operational level of cyber threat intelligence, organizations move beyond individual events and incidents to create holistic assessments of cyber threat actors. In creating operational intelligence, analysts build upon events and incidents to identify campaigns. Campaigns are then, if possible, attributed to cyber threat actors. Teams and individuals working at the operational level are typically the security leaders (e.g. CISOs and CSOs).

A table broadly depicting the items CTI teams should be tasked with at the operational level can be found in Table 3 in Appendix 1.

3.2.1. Preparation

Military leaders use processes like the Military Decision-Making Process (MDMP) to prepare operations orders with the lowest acceptable risk and highest chances of success. Central to MDMP is the intelligence team representing the threat during the process. Intelligence Preparation of the Cyber Operational Environment is a process adapted from the military that provides security leaders with the relevant intelligence to design a security program and respond to threats. The process identifies potential threat courses of action and helps the security and risk management leaders selectively apply and maximize a defense in depth strategy via a greater understanding of the organization's cyber threats at critical points in time and space in the operational environment. The process has four steps: defining the operational environment, describing the operational environment's effects on network defense, evaluating cyber threats, and developing cyber threat courses of action (Kime, 2016).

The outputs of the Intelligence Preparation of the Cyber Operational Environment are useful to many teams in the security organization. Each step produces detailed products that help design a defense-in-depth infrastructure (Security Architecture), identify the organization's high-value targets (Security Architecture/SOC/DFIR), prioritize security patches (Vulnerability Management), provide context to security alerts (SOC), and drive the incident handling lifecycle (DFIR). Additionally, the intelligence

team uses those same outputs to recommended PIRs and an intelligence collection plan that helps analysts answer management's PIRs (Kime, 2016). Preparing to defend an organization must be driven by timely, accurate, and actionable intelligence .

Testing incident response plans is a critical function that ensures an organization is prepared when a data breach or attack occurs. As the intelligence team represents the threats an organization is facing, CTI should be intimately involved in blue team exercises. The intelligence team should develop the testing scenario that is based on real security events relevant to the organization. Additionally, CTI teams with a red teaming capability can represent the threat during the actual exercises – tabletop or with real exploits. Cyber threat intelligence drives successful incident handling lifecycles.

3.2.2. Detection and Analysis

The intelligence community trains analysts to detect indications and warnings of threat courses of action. NIST uses the term precursors rather than indications and warnings, but the meaning is the same. A precursor is simply a sign that an incident may occur in the future or that a threat has chosen a course of action. Detecting precursors falls squarely in the mission of cyber threat intelligence as they occur "left of hack." Two recent events where CTI can contribute to incident handling via detecting precursors were the WannaCry and Petya ransomware attacks in May 2017 and June 2017, respectively. In both cases, reliable security researchers began sharing information about the attacks on Twitter as it became available. Soon after the initial reports of each attack information sharing and analysis centers shared initial assessments of the attacks. CTI teams trained and connected with the right sources will quickly observe precursors of events like WannaCry and Petya. From those sources, CTI can push IOCs to the organization's security stack, request emergency patches, and advise SOCs where to look for the expected attack to reduce risk to the organization.

As intelligence teams are concerned with CTAs and their respective campaigns at the operational level of cyber threat intelligence, we need robust data to correlate security events and incidents. As in counterinsurgency operations like the US military and its allies have been conducting in Afghanistan and Iraq since 2001, data needed to assess

threat groups and campaigns flows upward from the tactical level. Ensuring event and incident case data is stored into a database provides CTI analysts working at the operational level the information needed to identify CTA campaigns. Multiple free and paid threat intelligence platforms exist to help CTI teams identify, catalog, assess, and prioritize CTAs. Awareness of an organization's most relevant threats is critical to completing Step 3 (Evaluate the Cyber Threats) of Intelligence Preparation of the Cyber Operational Environment.

3.2.3. Containment, Eradication, and Recovery

Often, there is a debate in the middle of an incident whether to contain and eradicate a threat as soon as it is detected. While most organizations choose to expel the CTA immediately, mature security teams may consider the intelligence gain or loss from kicking a miscreant out of their networks. Prematurely eradicating an adversary off the network may decrease visibility into that particular threat and increase the risk of not detecting the next campaign. Mature threats will shift command and control infrastructure which likely will not be in the organization’s threat intelligence platform that feeds IOCs to the security controls. Deciding when, how, and whether to contain and eradicate a CTA off the network should be a risk-based decision. CTI, representing the threat in all planning and operations of a security team, should drive the intelligence gain and/or loss discussion during containment and eradication.

Recovering from a data breach should involve more than technical actions. As mature CTI teams will have many good information sources outside the organization, these sources should be used to monitor relevant threat actor communications channels when possible to validate recovery efforts, collect information for possible law enforcement actions, and to hunt for the organization’s data in criminal marketplaces.

3.2.4. Post-Incident Activity

As intelligence analysts are concerned with campaigns and CTAs at this level of intelligence, our post-incident activities should focus on mid-term solutions. CTI should compare their threat models and courses of action (from Steps 3 and 4 of IPCOE) to the

actual tactics, techniques, and procedures used by the threat actor and update the models to reflect the observed data. By updating threat actor models and assessments with the latest incident data, CTI can identify successes and areas to improve. Additionally, reviewing and refining the team's intelligence collection plan based on recent incidents ensures the collection plan does not become stagnant or irrelevant.

3.3. Strategic Level

Strategic intelligence in the private sector reduces risk to the organization by providing the assessments and forecasting for leadership to plan company cybersecurity objectives and create policies. Intelligence must be included so that strategic-level decision makers can understand the threats that may impact strategic business objectives (INSA, 2013). Adapting from a quote often attributed to Chinese military strategist Sun Tzu, "[Cybersecurity] strategy without tactics is the slowest route to [a secure environment]. [Cybersecurity] tactics without strategy is the noise before [a data breach]." In cybersecurity, strategic intelligence must be informed by operational intelligence. For strategic leaders, like the C-Suite and Board of Directors, to get the information security strategy correct, it must be influenced by strategic cyber intelligence.

A table broadly depicting the items CTI teams should be tasked with at the strategic level can be found in Table 3 in Appendix 1.

3.3.1. Preparation

A lack of preparation for the future is often the cause of failure. At Kodak's peak, it sold about 70 percent of the photographic film in the US (Brachmann, 2014). Despite a Kodak engineer building the first digital camera prototype, they went bankrupt in 2012. Kodak executives never considered that digital photography could one day replace traditional film cameras (Brachmann, 2014). To avoid becoming the next Kodak, scenario planning and strategic forecasting are two methodologies organizations can use to help predict the future.

In today's hyper-connected environment, senior leaders need to consider the future cybersecurity threat landscape when developing strategic plans. A forecast is a long-term estimative product. For example, the US Intelligence Community releases a National Intelligence Estimate yearly to provide the US Congress and Executive Agencies their coordinated judgment of the long-term threats facing the United States. A yearly cyber threat intelligence estimate coinciding with organizational reporting can add significant value to an organization's risk management processes.

Alternatively, scenario planning for future cyber threats should contain multiple narratives that are unique, but plausible – similar to developing CTA courses of action during IPCOE. Stratfor – the geopolitical firm whose name is shorthand for the term 'strategic forecasting' uses the process in Figure 6 (below) to develop potential future scenarios for its clients. The intelligence community uses a similar process called alternate futures analysis. A sample alternate futures exercise for a critical infrastructure organization can be found in Figure 7. Scenario planning, or alternate futures analysis, adds value to an organization's strategic planning by providing an effective means of weighing multiple unknown or unknowable factors, identifying plausible combinations of uncertain factors, and providing a broad analytic framework for calculating costs, risks, and opportunities for policymakers (CIA, 2009).

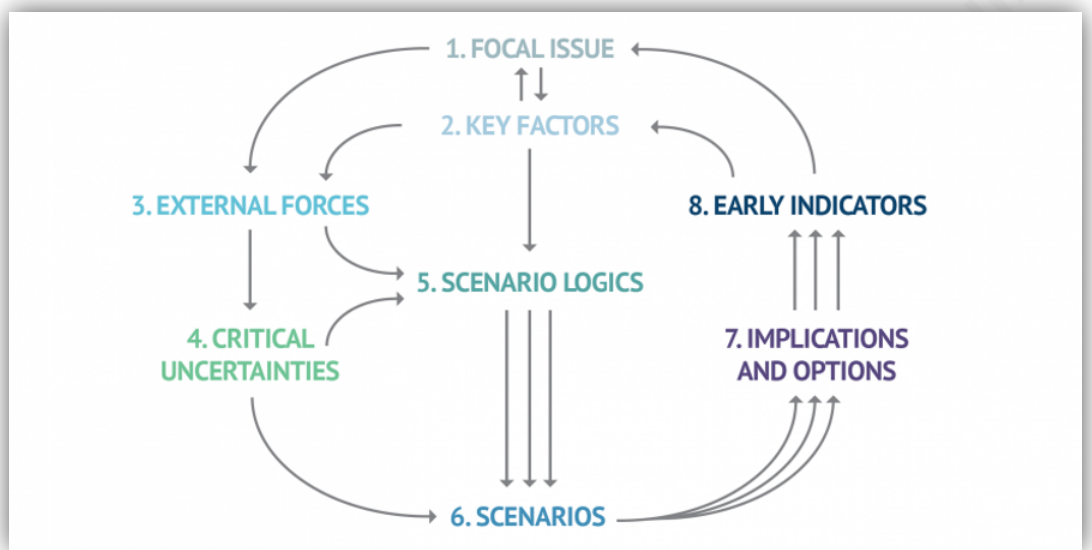

Figure 6: Stratfor's Eight-Step Scenario Planning Process (Ogilvy, 2015)

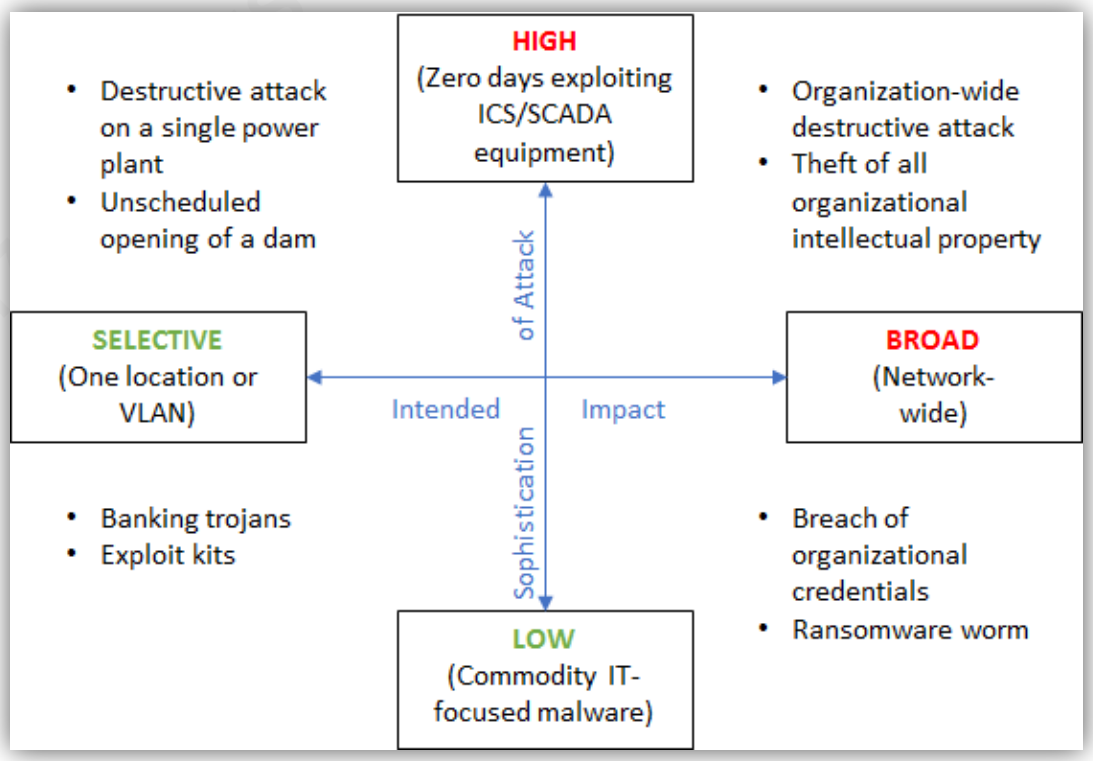

Figure 7: Alternate futures exercise sample for an electric utility

Strategic forecasting, by describing potential threat scenarios in the years to come, has multiple use cases in an organization. For example, many industries and organizations lobby for or against legislation and regulations. Organizations regularly plan for new technology acquisitions and talent acquisition and retention. By providing strategic leaders with actionable, threat-focused forecasts, an organization's long-term cyber risk can be managed more effectively than by relying on tactical CTI alone. Forecasting and scenario planning can significantly help increase the probability that an organization is prepared to counter cyber threats in the long-term.

CTI teams should proactively support legislative and regulatory efforts of their organization. CTI teams should forecast the likelihood and impact of future security breaches and attacks, emerging threat actor courses of action, and provide policy recommendations that the organization's executives and lobbyists can present to legislative bodies. The intelligence team will have to work with lawyers and other non-technical customers to craft assessments that support the external affairs mission. As many in government lack a technical background, providing policymakers with threat-based policy recommendations can help tailor legislation and regulations that encourage good security practices and reduce the incentives of miscreants to use the Internet for criminality.

In addition to the above tasks CTI can do to help an organization strategically prepare for CTAs, mergers and acquisitions can introduce significant risk to the parties involved. Until recently, many organizations did not consider cybersecurity risks during the due diligence period of an acquisition or merger. For example, in 2013 IBM acquired hosting provider Softlayer – which itself had acquired another hosting provider, The Planet Internet Services. In 2010, Brian Krebs did an analysis of bad ISPs and hosting providers and had found that both Softlayer and The Planet were listed very prominently (Krebs, 2015). A cyber intelligence analysis of mergers and acquisitions is beyond the scope of this paper. However, IBM's leadership may have negotiated from a different place had they used their cyber threat intelligence capability to assess the threat the Softlayer acquisition may pose to IBM's reputation and security posture. An organization's intelligence team should be used during mergers and acquisitions to assess

the target organization's cybersecurity vulnerabilities and the impact the acquisition could make upon the gaining organization to reduce strategic cyber risk.

3.3.2. Detection and Analysis

Detecting strategic shifts by the main types of threat groups (nation-states, criminals, hacktivists) relies on the strategic intelligence estimates prepared in the preparation phase. Stratfor, the private intelligence company, reviews its strategic forecasts each year. Stratfor clients benefit by this honest appraisal of Stratfor products. By regularly comparing past strategic estimates to current reporting, CTI teams can detect long-term changes to broad categories of threats and enumerate successes and areas for improvement.

3.3.3. Containment, Eradication, and Recovery

At the strategic level of incident handling, an organization will need to communicate effectively to assuage the concerns of customers, employees, partners, regulators, shareholders, and other constituents. The default response from most public relations teams tends to be something along the lines of, "an advanced, highly sophisticated criminal attacked our organization." In reality, most data breaches are the handiwork of medium-skilled CTAs, and most breaches could be prevented by implementing frameworks like the Center of Internet Security's 20 Critical Security Controls. CTI can monitor threat actor communications channels to anticipate how a CTA will react to various PR strategies during the containment, eradication, and recovery phases. By monitoring these communications channels, CTI can contribute to a threat-focused public relations response that minimizes risk to the breached organization and better allocates resources.

An increasing number of cyber threat actors focus their energy on exploiting human and client-side vulnerabilities rather than exploiting server-side vulnerabilities. However, much security awareness training has not been updated in 10-15 years and lacks consideration of modern cyber threats. CTI teams have a unique perspective and should ensure security awareness training educates different cohorts of users on the

threats likely to target them. For example, engineers working for a nuclear power plant will likely see different tactics used against them than what an accountant would observe. As "the threat gets a vote", security awareness training that is informed by CTI assessments ensures the right messages and training gets to the right users.

3.3.4. Post-Incident Activity

Policies and standards are directed by an organization's leadership. In the wake of an incident, there may be a consideration to review and update security policies and standards. For example, NIST recently released new Digital Identity Guidelines that prescribe a radical change for password policies. These new guidelines were created due to the knowledge of how threats steal, collect, monetize, and use stolen user credentials. After a credential breach of employees or customers, organizations will likely review their password policies. As the threat intelligence team has visibility into all cyber threats known and emerging, an organization can ensure policies and standards are respective of the relevant cyber threats.

A major security breach may encourage a victim organization to lobby for changes to cybersecurity laws and regulations. In the wake of a major incident, strategic CTI should be brought to bear by an organization's lobbyists and industry relations teams to help formulate policy recommendations to legislators that are based on current and emerging threats, and that will reduce risk to the organization and industry. As in the preparation phase, CTI teams should forecast the likelihood and impact of future security breaches and attacks, emerging threat actor courses of action, and provide policy recommendations that the organization's executives and lobbyists can present to legislative bodies.

4. Conclusion

Moving beyond the tactical level of cyber threat intelligence is critical to an organization's ability to prevent data breaches, intrusions, and denial-of-service attacks. Intelligence Preparation of the Cyber Operational Environment is a robust process that

substantially helps an organization understand the threat landscape they conduct business in. Additionally, intelligence support to governmental affairs, mergers and acquisitions, incident communications, and more are potential areas where organizations can consume strategic cyber threat intelligence to make better business and policy decisions for long-term effects and risk management. Providing public, private, and academic sector senior leaders with tactical, operational, and strategic cyber threat intelligence ensures all decision-makers have the information needed to reduce risk in the short-, mid-, and long-term.

References

Brachmann, S. (2014, November 1). The Rise and Fall of the Company that Invented Digital Cameras. Retrieved September 27, 2017, from http://www.ipwatchdog.com/2014/11/01/the-rise-and-fall-of-the-company-that-invented-digital-cameras/id=51953/

Bromiley, M. (2016). Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey (Rep.). SANS Institute.

Central Intelligence Agency (CIA). (2009). A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis [Pamphlet]. Washington, DC: United States Government (USG).

Cichonski, P, Millar, T., Grance, T., & Scarfone, K. (2012, August). SP 800-61r2 Computer Security Incident Handling Guide (U.S. Department of Commerce, National Institute of Standards and Technology). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cyberedge Group. (2015, January). 2015 Cyberthreat Defense Report North America & Europe (Rep.).

Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force. (2013, September). Operational Levels of Cyber Intelligence (Rep.). Retrieved from https://www.insaonline.org/wp-content/uploads/2017/04/INSA_OperCyberIntelligence_WP.pdf

Joyce, R. (2016, January 27). Disrupting Nation State Hackers. Lecture presented at USENIX Enigma in Hyatt Regency San Francisco, San Francisco. Retrieved May 25, 2017, from https://www.youtube.com/watch?v=bDJb8WOJYdA

Kime, B. (2016, March 26). Threat Intelligence: Planning and Direction (Unpublished master's thesis). SANS Technology Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/threat-intelligence-planning-direction-36857

Krebs, B. (2015, October 21). IBM Runs World's Worst Spam-Hosting ISP? Retrieved June 26, 2017, from https://krebsonsecurity.com/2015/10/ibm-runs-worlds-worst-spam-hosting-isp/

Malik, J. (2016). *Threat Intelligence Déjà Vu* (Rep.). Alien Vault.

Ogilvy, J. (2015, January 8). Scenario Planning and Strategic Forecasting. Retrieved August 24, 2017, from https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/print/

Ponemon Institute LLC. (2014). *Threat Intelligence & Incident Response: A Study of U.S. & EMEA Organizations* (Rep.).

Ponemon Institute LLC. (2015). *The Importance of Cyber Threat Intelligence to a Strong Security Posture* (Rep.).

Ponemon Institute LLC. (2015). *Second Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way* (Rep.).

Ponemon Institute LLC. (2016). *The Value of Threat Intelligence: A Study of North American & United Kingdom Companies* (Rep.).

Shackleford, D. (2015). *Who's Using Cyberthreat Intelligence and How?* (Rep.). Bethesda, MD: SANS Institute.

Shackleford, D. (2016). *The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing* (Rep.). Bethesda, MD: SANS Institute.

US Department of the Army, Headquarters. (2014, November). *Intelligence Preparation of the Battlefield/Battlespace* (Army Techniques Publication (ATP) 2-01.3).

US Department of the Army, Headquarters. (2006, September). *Human Intelligence Collector Operations* (Field Manual (FM) 2-22.3).

US Department of Defense, Joint Chiefs of Staff. (2013, October 22). *Joint Intelligence* (Joint Publication (JP) 2-0).

5. Appendix 1

Table 3: CTI mapped to Incident Handling Lifecycle Phase

Level of Intell-igence / Incident Response Life Cycle Phase	Tactical (SOC, DFIR Team)	Operational (CISO, CSO)	Strategic (C-Suite, Board of Directors)
Preparation	Deploy IOCs and rules (i.e., Snort, Yara) to controls and tools; Represent the threat in blue team exercises (i.e., phishing exercises)	Intelligence Preparation of the Cyber Operational Environment, Develop PIRs and collection plan; Represent the threat in blue team exercises	Strategic forecasting; Scenario Planning/Alternate Futures; Support to Governmental Affairs; Support to Acquisitions & Mergers
Detection and Analysis	Hunt for emerging threats elsewhere in environment; Share tactical information with peers and trust groups	Indications and Warnings (Precursors) CTA/Campaign analysis	Reviews of prior forecasts to detect strategic changes by CTAs
Containment, Eradication, and Recovery	Recommend countermeasures for containment; Enumerate threat indicators to ensure comprehensive eradication. Enumerate vulnerabilities exploited to ensure comprehensive recovery	Conduct intel gain/loss analysis to drive IR actions; Monitor possible threat actor communications channels and perimeter logs; Hunt for stolen data in dark web	Support to Incident Communications (PR, Social Media); Support to Security Awareness; evaluate threat actor responses to incident response actions
Post-Incident Activity	Reassess IOC and rule sources for reliability and trustworthiness	Update threat models and assessments; Identify intelligence gaps and refine collection plan	Evaluate new policies, standards, and controls for effectiveness in reducing risk from known and potential threats; Support to governmental affairs