# Global Information Assurance Certification Paper

# Threat Intelligence: Planning and Direction

*GIAC (GSEC) Gold Certification*

Author: Brian P. Kime, bkime@mastersprogram.sans.edu
Advisor: Christopher Walker
Accepted: March 26, 2016

Abstract

Not understood well by most organizations outside the military and government is Cyber Threat Intelligence – one of the latest areas of information security. Many practitioners of Cyber Threat Intelligence are technologists by trade and are unfamiliar with the Intelligence Cycle. Often overlooked by business leaders and private sector Cyber Threat Intelligence Teams is planning and direction, one of the steps in the Intelligence Cycle. Intelligence teams must be requirements focused in order to generate results that lead to reductions in risk. Those Priority Intelligence Requirements – approved and resourced by management – focus tactical/technical, operational, and strategic collection and analysis of intelligence information. This paper will discuss how to plan and direct a cyber threat intelligence team's operations towards reducing an organization's risk with the Intelligence Preparation of the Cyber Operational Environment process and the difference between Intelligence and Counterintelligence.

# 1. Introduction

Many celebrated leaders like Ben Franklin and Winston Churchill have said, in various forms, “Failing to plan is planning to fail.” That notion is relevant to the still new information security subfield of Cyber Threat Intelligence (CTI). Few, if any, CTI vendors offer to help clients plan and direct their CTI team (the “Team”). A lack of planning often leads Teams into irrelevancy, answering questions about irrelevant threats leadership did not ask.

This paper heavily references Joint Publication (JP) 2-0: Joint Intelligence, 22 October 2013 and Army Techniques Publication (ATP) 2-01.3: Intelligence Preparation of the Battlefield/Battlespace, November 2014 and aims to adapt military intelligence tradecraft to private sector CTI management, planning, and operations. The processes described in these two unclassified US military publications illustrate how analysts take raw data and information and apply analytical tradecraft to create a “new understanding of the information, which may be called “intelligence”” ("JP 2-0", 2013).

Contrary to many other white papers on CTI, this paper will not focus on adapting military intelligence collection or analysis steps of the Intelligence Cycle to the private sector. The focus here will be on the planning and direction step of the cycle and incorporating business leaders into the Intelligence Cycle and a Team’s operations. Also, contrary to Yuill, et al.’s 2000 journal article, “Intrusion-detection for incident-response, using a military battlefield-intelligence process”, the goal of the process described here is to identify threat courses of action, not compromised devices (that may happen as a result of The Process, though).

Management and integration of intelligence is an enormous challenge even in military organizations that have been integrating Intelligence since the advent of warfare. An intelligence team in an infantry battalion, for example, will typically have one threat to model and determine courses of action for at one point in time in one location. Cyber Threat Intelligence Teams, however, must model and assess a diverse range of threats attempting to attack the business or steal information 24 hours a day, seven days a week. The challenges are daunting for Teams.

Brian P. Kime, bkime@mastersprogram.sans.edu

In fact, at the recently concluded 2016 RSA Conference in San Francisco, the big topic of interest was CTI. According to the experts consulted by the Salted Hash blog, CTI lacks context. Alarmingly, the consensus is most CTI vendors are not selling intelligence that organizations can use to trigger some action in their environment. In addition, the experts said vendors take a one-size-fits-all approach to their CTI services (Ragan, 2016).

## 1.1. Demystifying Intelligence

First, a moment to demystify intelligence. Indicators of Compromise (IOCs), by themselves, are not intelligence. An IOC, by itself, is simply one data point. Add to that IOC the type of malicious activity observed (ex: recon, spam, command and control (C2)) and now an analyst has information. In reality, threat information is what many CTI vendors are selling. While useful for network defense, threat information is still not intelligence. When an analyst, responding to management-directed intelligence requirements, takes information and relates it to their operational environment (i.e. their organization), applies context, and assesses the threat, that is intelligence. Intelligence products provide customers answers to their requirements. Those answers should drive business decisions.

Furthermore, as with military intelligence, CTI operations and products should address tactical/technical, operational, and strategic levels of cybersecurity. Strategically, Teams can support organizational-wide security and risk management strategy, policies, budgeting, technology acquisition, and staffing. At the operational level, CTI can support the information security group's understanding of the overall threat landscape to support digital forensics management, incident response management, security architecture, security awareness training, and the CISO's interactions with the C-suite and board of directors. Lastly, at the tactical/technical level, CTI can reduce risk by hunting for unknown threats, recommending countermeasures, and feeding IOCs to security tools.

Often confusing is the term "counterintelligence". Simply defined, counterintelligence is denying a threat or adversary the ability to collect accurate information on your organization. counterintelligence operations identify spies and

deceive adversaries' understanding of an organization's intent, capabilities, and knowledge. Traditional military intelligence is outward looking, focused on discerning the threat's intent, capabilities, and knowledge. For cyber threat intelligence, we must address the entire spectrum of threats by using intelligence and counterintelligence tradecraft, often simultaneously.

## 1.2. The Intelligence Cycle

Briefly, the Intelligence Cycle is a five step, continuous 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 (the focus of this Gold Paper); collection; processing and exploitation; analysis and production; dissemination and integration. Throughout the intelligence cycle, Teams require feedback and evaluation from management.

Overlooked for a variety of reasons is the planning and direction step. Most often, business leadership is not aware of the capabilities of a robust, resourced, and well-managed Team. Business leaders may also be intimidated by the technical aspects of information security or intelligence operations and unwilling to participate in the planning step. In order to deliver the most value, Teams must work with the leadership and expend much energy on the planning step. It is during planning and direction when management and The Team collaborate to determine intelligence requirements, develop an intelligence architecture, create a collection plan, and generate requests for information.

As business leaders are the consumers of Intelligence, it is vitally important for The Team to work with them to define Priority Intelligence Requirements (PIR). PIRs then drive all other intelligence operations. CTI analysts will chase what is interesting to them when management does not set their requirements, often leading to a mismatch between intelligence products and business needs. Intelligence Preparation of the Cyber Operational Environment is a process to help Teams recommend PIRs, intelligence architecture, a collection plan, and requests for information.

Brian P. Kime, bkime@mastersprogram.sans.edu

## 1.3. Intelligence Preparation of the Cyber Operational Environment - Introduction

Intelligence Preparation of the Cyber Operational Environment ("The Process") 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 by providing a means of visualizing and assessing a number of specific intrusion sensor inputs and open source information to infer specific threat courses of action ("ATP 2-01.3", 2014). The Process supports the organization's risk management strategy and the information security group's decision-making. Applying 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 by:

1. Defining the operational environment
2. Describing the operational environment effects on network defense
3. Evaluating the cyber threats
4. Developing cyber threat courses of action

Figure 1 is a graphical representation of the Intelligence Preparation of the Cyber Operational Environment.

Brian P. Kime, bkime@mastersprogram.sans.edu

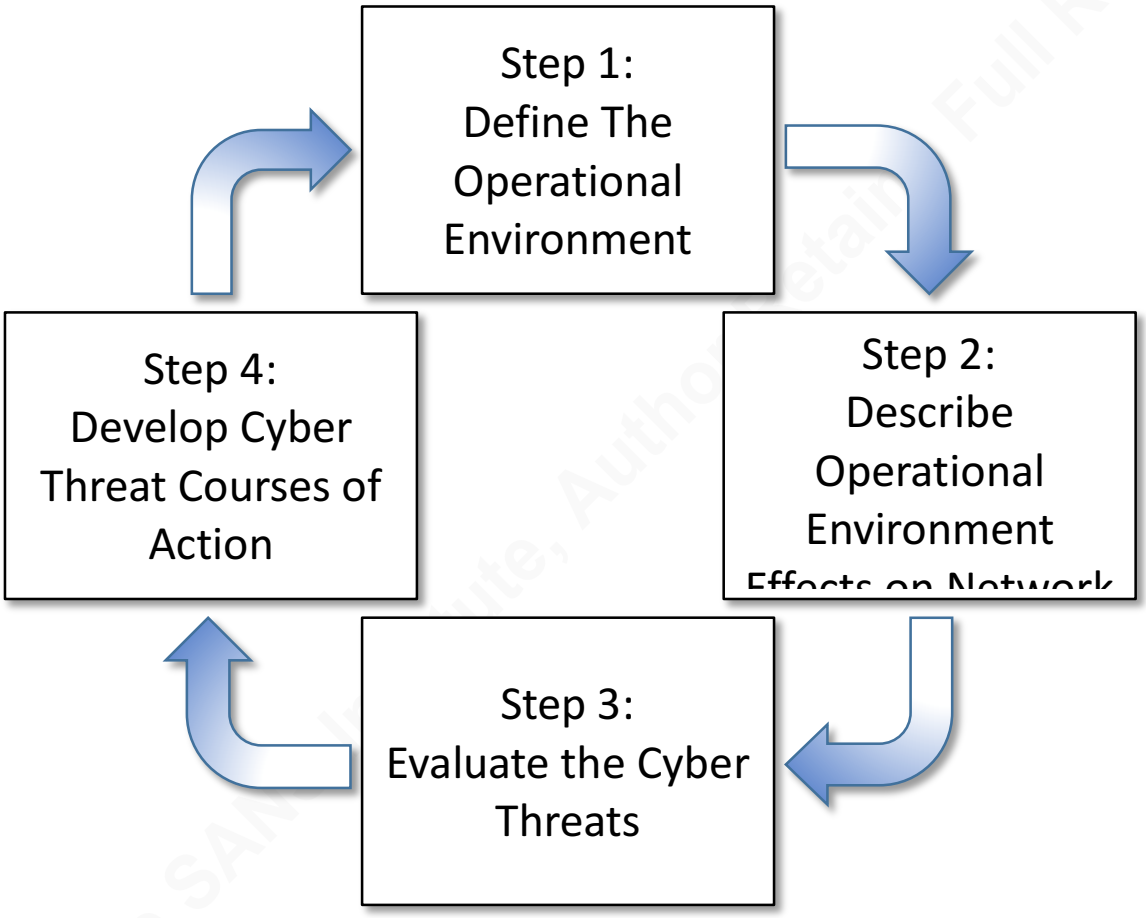


*Figure 1: Intelligence Preparation of the Cyber Operational Environment*

Like the related Intelligence Cycle, Teams should continually conduct The Process to ensure that The Process's products remain complete and valid, and to support the planning and direction of cyber intelligence collection, analysis, and production. The Process helps security and risk management leaders know what the threat landscape looks like, where to look, when to look, what to expect, what to defend, and helps identify critical information and key assets.

The Process is a translation of the US Army's Intelligence Preparation of the Battlefield (IPB) methodology from kinetic and physical warfare into cybersecurity. Intelligence concepts are the basis for IPB and easily adapted for use in The Process. Military intelligence is used to describe existing and previously existing conditions or estimate future possibilities and probabilities to reduce risk and uncertainty. The first three steps of The Process are largely descriptive. The fourth step is principally estimative.

Brian P. Kime, bkime@mastersprogram.sans.edu

Note that the threat may not necessarily be a foreign government, criminal organization, terrorist group, or hacktivist. We need to consider the necessity to perform predictive intelligence analysis against corporate espionage, chaotic actors, and the insider threat. The Process allows the analyst to consider the business's mission, vulnerabilities, and peculiarities while developing courses of action against a number of notional threats which may have different goals and related doctrines, methods, tactics, techniques, and procedures (tactics, techniques, and procedures).

The result of The Process is a suite of products that queue the collection step of the Intelligence Cycle and are useful during incidents to support business decisions. Examples of The Process's products are area of operation and area of interest graphics, lists and graphics of the organization's key assets/information, narratives and graphics describing potential threat objectives, threat models, threat course of action narratives and graphical overlays, detection point overlays, and recommended Priority Intelligence Requirements.

# 2. Intelligence Preparation of the Cyber Operational Environment

## 2.1. Step 1. Defining the Operational Environment

Step one of Intelligence Preparation of the Cyber Operational Environment ("The Process") identifies for further analysis the significant characteristics of the operational environment that may influence the organization's defense in depth strategy and tactics and the business's risk management decision making ("ATP 2-01.3", 2014). This section is adapted from Chapter 3 of ATP 2-01.3. Figure 2 is a diagram of step 1.

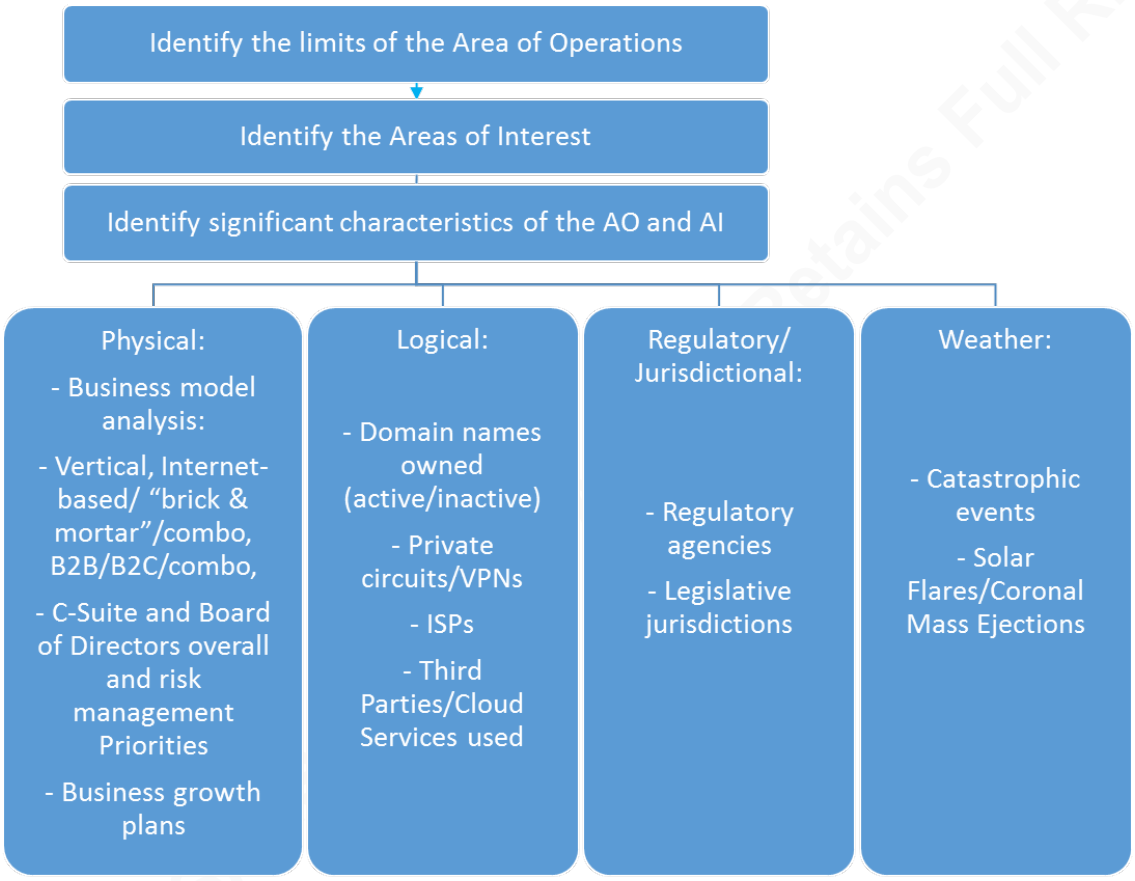


*Figure 2: Sub-steps of step 2 of Intelligence Preparation of the Cyber Operational Environment*

### 2.1.1. Desired End State

Step 1 of The Process focuses The Team's effort on the characteristics of the operational environment that can influence the organization's network defense and threat operations. The Team acquires the intelligence needed to complete The Process in the degree of detail required to support the organization's defense in depth strategy. The primary outputs of step one are the determination of the area of operations and area of interest, identification of general characteristics of the area of operations that could influence the organization's business, and identification of gaps in current intelligence holdings, translating them into requirements for collection or information in order to complete The Process ("ATP 2-01.3", 2014).

### 2.1.2. Identify the Limits of the Business' area of operations

The executives and boards of directors define the area of operations for a private sector business. The area of operations will include where the business operates physically and logically. We define the area of operation as the defended environment.

### 2.1.3. Identify the Limits of the Business's area of interest

The area of interest is the broader area outside the area of operations that contains features, assets, and threats that can influence the business's ability to protect the organization's information, networks, customers, and employees. The area of interest is the area from which information and intelligence are required to defend the organization's physical and logical environment.

Relevant questions (not all-inclusive) for identifying the business's area of interest include, but are not limited to, where are the business's customers; and where may threats plan malicious activities against the organization?

### 2.1.4. Identify Significant Characteristics within the area of operations and area of interest for Further Analysis

The network is neither homogeneous in its security, architecture, administration, use, or assets. As a result, it is necessary to identify the primary aspects of the environment, which will influence the threat's courses of action and The Process. To facilitate planning, examine these characteristics at a high level, initially. Further examination takes place in later steps. Primary aspects of the environment include the business/operating model, executive and board priorities, expansion/growth plans, private circuits connecting offices, VPNs for remote access, domain names the business owns, ISPs and backup/redundant connections, cloud services used by the organization, regulatory bodies and actions affecting the organization, legislative jurisdictions the organization operates in, and weather that may affect network operations.

### 2.1.5. Evaluate Current Defensive Posture and Intelligence Holdings to Determine Additional Information Needed to Complete Intelligence Preparation of the Cyber Operational Environment

Due to the nature of the business, the information security group may not be aware of all security assets, logs, or networks. Identify information gaps early and prioritize based on the business leadership's guidance and intent.

Given the available resources and the Identify, Protect, Detect, Respond, and Recover incident response process requirements, the purpose of this step is to plan and focus The Process's efforts. These plans should identify the places within the area of operations and AI, which has the most promising sources of information to answer the leadership's intelligence requirements.

Relevant questions should answer which logs The Team needs to be able to assess threats and discover anomalies and which people, processes, and tools the business has that affect security and information risk.

After determining which information gaps exist, The Team submits requests for access to log repositories, points of contact for people, process, and tools. Fulfilling requests will close information gaps and update The Process's products. New information gaps are determined and prioritized.

## 2.2. Step 2. Describing the Operational Environment effects on Network Defense

Step 2 of Intelligence Preparation of the Cyber Operational Environment ("The Process") determines how significant characteristics of the operational environment can affect defensive operations and threat operations ("ATP 2-01.3", 2014). This section is adapted from Chapter 4 of ATP 2-01.3. Figure 3 is a diagram of step 2.

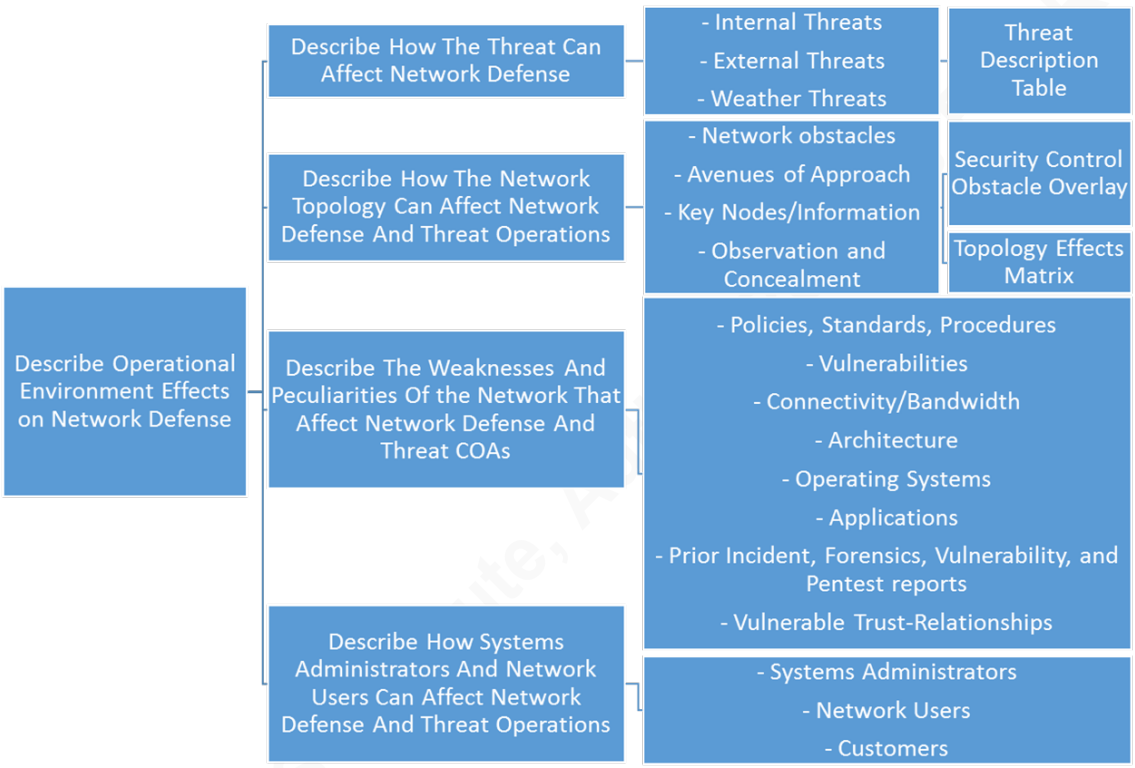


*Figure 3: Sub-steps of step 2 of Intelligence Preparation of the Cyber Operational Environment*

### 2.2.1. Desired End State

Identify how the operational environment influences the organization's network defense and threat courses of action. The primary outputs associated with step 2 of The Process may include network topology analysis, threat avenues of approach, network key nodes/information, potential threat objectives, detection points, and refined/updated requests for information ("ATP 2-01.3", 2014).

### 2.2.2. Describe How Threats Affect Network Defense

We break down insider threats by intent – malicious or unintentional. A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems (CMU, n.d.).

Brian P. Kime, bkime@mastersprogram.sans.edu

Unintentional insider threats are users, administrators, programmers, etc. who harbor no malicious intent but through their lack of security awareness, carelessness, negligence, or poor technical skills introduce risk into the company.

Capabilities and intent of external threats varies dramatically. Most cyber criminals deal in commodity malware and spam and target all Internet users. However, there are exceptionally talented and resourced cyber criminals paid to target specific organizations. Industry competitors, criminal organizations, or foreign intelligence services may conduct cyber espionage. Chaotic actors ("hacking for lulz") may attack a target with little warning and unclear objectives. Hacktivists (ex: Anonymous) often attack a target out of real or imagined grievances or transgressions. Often they use social media to draw more attention to their cause and to recruit more participants. Extortionists threaten attacks or data theft in order to get organizations to pay, usually via cryptocurrency, for the threat to go away. Governments and regulatory agencies can be threats as sudden changes in legislation or enforcement may force an organization to alter dramatically how it protects customer data or conducts business.

Extreme weather events, like Hurricane Sandy, can cause a loss of power data centers or force abnormally high usage of VPNs for remote access – affecting the availability of an organization's information.

Solar flares can temporarily alter the upper atmosphere creating disruptions with signal transmission from, say, a GPS satellite to Earth causing it to be off by many yards. Another phenomenon produced by the sun could be even more disruptive. Known as a coronal mass ejection (CME) these solar explosions propel bursts of particles and electromagnetic fluctuations into Earth's atmosphere. Those fluctuations could induce electric fluctuations at ground level that could blow out transformers in power grids. A CME's particles can also collide with crucial electronics onboard a satellite and disrupt its systems (Dunbar, n.d.).

The threat description table supports the threat overlays by classifying the type of threats identified to the organization and describing the broad capabilities of each threat type. See Table 1 in Appendix 1 for an example of a threat description table.

Brian P. Kime, bkime@mastersprogram.sans.edu

### 2.2.3. Describe How the Network Topology Can Affect Network Defense and Threat Operations

Analyzing the defensive aspects of network topology involves the collection, processing, evaluation, and interpretation of features of a computer network, combined with other relevant factors, to determine effects of the network topology on network defense and threat operations. Network topology analysis is a continuous process as changes in the operational environment may alter the analysis of its effect on network defense ("ATP 2-01.3", 2014).

In military intelligence, Intel analysts enhance maps by applying overlays depicting characteristics of the environment, e.g., obstacles and key terrain. Analysts use overlays to visualize the combined effects of the battlefield's characteristics. We can use similar constructs for The Process. A map of the network architecture and components provide the framework for analysis of the operational environment effects. The primary features should include networking devices, network management tools (like SNMP managers), systems (servers, workstations, mobile), and content (software and sensitive data).

This sub-step of step 2 summarizes the elements of the network topology that affect the operational environment. The tactical aspects of network topology are network obstacles, avenues of approach (AA), key nodes and information, observation, and concealment.

An obstacle in a network path is any network or host feature that denies, degrades, or delays the threat in their attempt to get from one point to another in the environment. Evaluation of obstacles helps to identify AAs. An obstacle can be a device or policy that dissuades the threat from using a network path such as in intrusion prevention system. Some examples of network obstacles are firewalls, router access control lists (ACL), host intrusion prevention systems (HIPS), antivirus, virtual local area networks (VLAN), email security appliances, network intrusion prevention systems, web proxies, and physical controls.

AAs are routes the threat can take to reach their objectives. Determining AAs requires some understanding of the threat's likely courses of action. In particular, it requires some understanding of where he is coming from and where he is going. Determining the threat's courses of action is the fourth step in The Process. The threat's tactics, techniques, and procedures and an organization's defensive posture will influence the threat's choice of AAs. Assessment of these tactics, techniques, and procedures occurs in the third step of The Process - evaluate the threat. As more becomes knows about threat courses of action and tactics, techniques, and procedures, update the products from step two.

AAs are primarily the paths established by network obstacles and by routing devices. Classify AAs according to the degree of obstruction encountered along the path as unrestricted, restricted, or severely restricted. Threats will favor paths with fewer obstacles and with less likelihood of detection. Features of the threat's most appealing AAs are available entry points, directness to the objective, lack of obstacles, low likelihood of detection, and sustainable access.

Key nodes, in network security, are any resource, the seizure of which affords a marked advantage to either the offense or defense. Evaluate key nodes by assessing the impact of its control by either the organization or a threat. In network defense, key nodes are those network devices that control the network or those that detect anomalous activity. Domain controllers, log repositories, firewalls, and servers that hold an organization's most sensitive information are examples of key nodes.

Key information is, but not limited to, administrator credentials, PII, PHI, trade secrets, or sensitive business plans. In other words, key information is any information that has value to criminals, nation-states, or to an organization's competitors.

Observation is the condition that permits the network defenders to see threat activities or the threat to see a target. In traditional military intelligence, the highest terrain normally provides the best observation. One analogy to this construct is the central log repository that provides network defenders the ability to observe threats throughout the operational environment. As part of the reconnaissance phase, a threat can use open sources of information, like Shodan or Censys to observe their target.

Brian P. Kime, bkime@mastersprogram.sans.edu

A detection point is a point along a path that data must pass through to reach the destination. Detection points can be useful for observation, especially along AAs. One of the outputs of Step 4 is identification of detection points.

Concealment provides a threat protection from observation. Concealment is useful when a threat desires persistence in the target network. Threats use a variety of tactics, techniques, and procedures to deter an organization's observation of them. For example, a threat can block a system administrator's remote access to a device, thereby concealing himself until the system administrator has regained access to the device. Using stolen credentials may cause defenders to overlook malicious logins, for example. Data exfiltration data via encrypted channels also conceals a threat's activities. Deleting logs can conceal a threat's presence in the network. A threat may use aliases on social media to conceal their information collection on an organization.

The security control obstacle overlay is a graphic product that portrays the effects of the network topology on defensive and threat operations. The overlay normally depicts significant aspects of the network topology that affect offense and defense. Though not all-inclusive, some of these aspects are AAs, obstacles, and key nodes. We divide the effects on network paths into three categories – unrestricted, restricted, and severely restricted. Unrestricted network paths are free of any restrictions to data-flow such as an area of a network attached directly to the Internet (ex: DMZ). Restricted network paths hinder data flow to some degree. Severely restricted network paths hinder data flow to a degree where it is impossible or impractical to the threat.

Collectively assess the effects of multiple obstacles along an AA. If a path contains many obstacles that restrict passage, the overall effect could be severely restricted topology. An obstacle's effect on network paths can vary depending upon the direction of traffic, the specific path, the available bandwidth (ex: a low bandwidth link may be severely restricted for a packet flood attack, but unrestricted for a telnet session), the type of traffic (ex: a proxy firewall may only permit connections to Web servers), and the threat's skill (ex: what is impossible for a low skilled threat may be easy for a skilled threat). In cybersecurity, skilled threats have traversed network topology the defender

assessed impassable to carry out many successful attacks. Figure 4 is an example of a security control obstacle overlay.

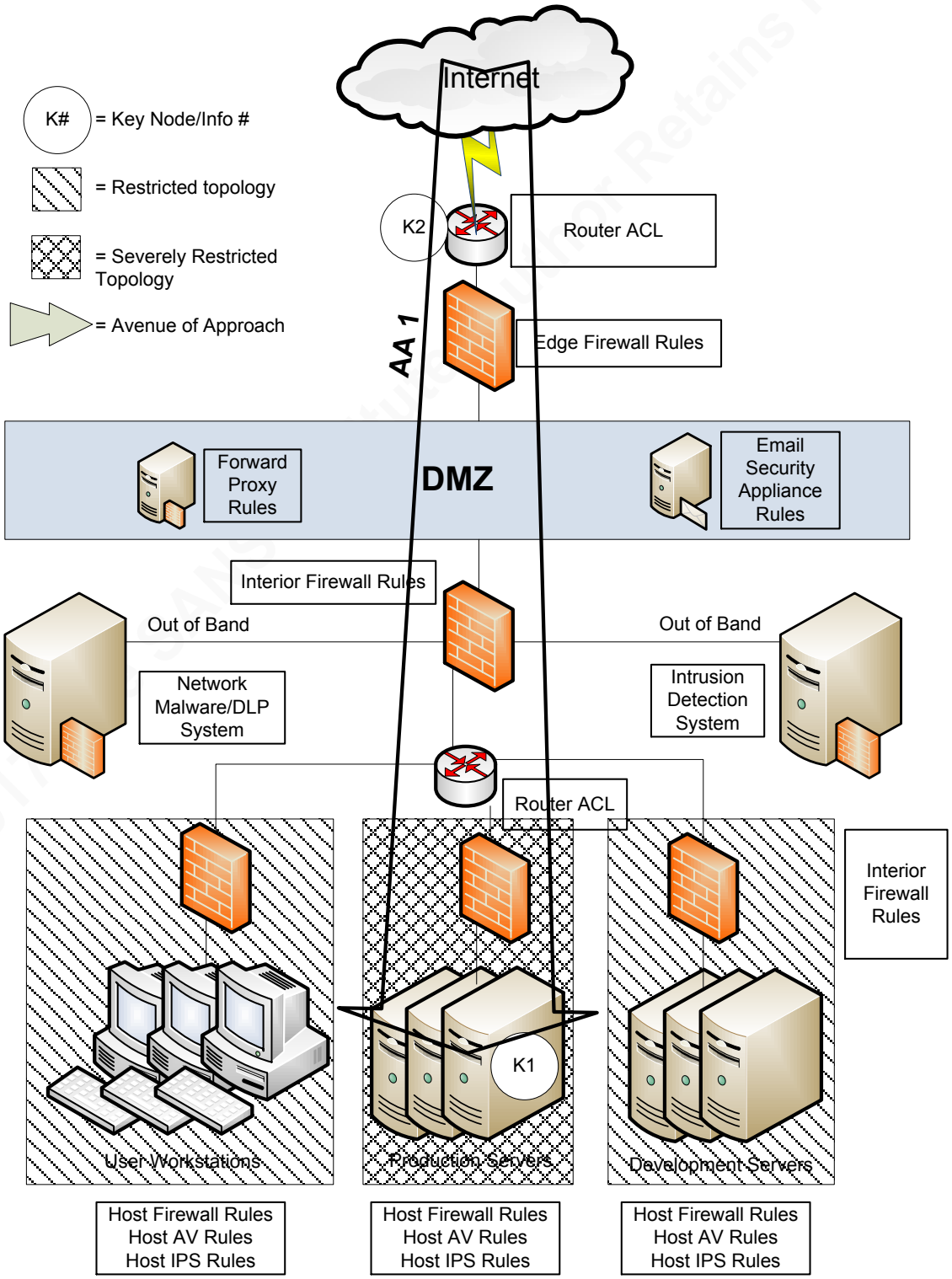


*Figure 4: Security Control Obstacle Overlay*

Brian P. Kime, bkime@mastersprogram.sans.edu

Subsequent, the topology effects matrix describes the effect each aspect of the network topology has on network defense and threat operations. Use the security control obstacle overlay as a guide when creating the topology effects matrix. Table 2 in Appendix 1 is an example of a topology effects matrix.

### 2.2.4. Describe The Weaknesses and Peculiarities of the Network That Affect Network Defense and Threat courses of action

After people, processes are an organization's most important aspects. As tactics fail when strategies are not well designed or employed, procedures will fail when security policies are obsolete, have gaps, or are not enforced. Assess the organization's policies, standards, and procedures to ensure coverage across the spectrum of threat courses of action. Assess the leadership's willingness and ability to hold individuals and management accountable for enforcing policy.

Describe and assess the vulnerabilities in the operational environment to include network devices, hardware (servers, workstations, mobile), software (internally developed and externally sourced), human, and trust relationships. Describe and assess exploits for those vulnerabilities if a threat were to choose a particular exploit.

Describe and assess the organization's connections to the Internet (ex: are there redundant circuits?), connections between business units, data centers, general offices, and remote employees. Within the perimeter, describe the connections and the network's

baseline traffic load. Figure 5 is an example of ISP and intrasite connectivity.

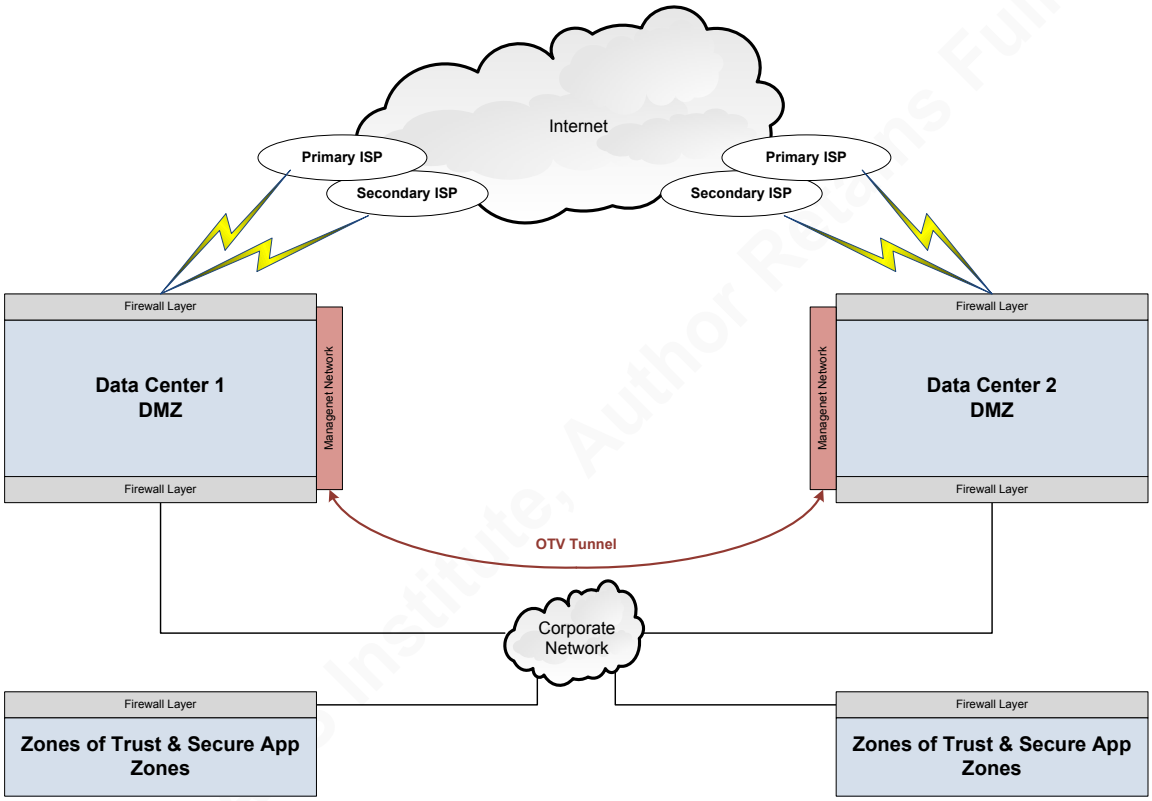


*Figure 5: Example of ISP and intrasite connectivity*

An organization's network and security architecture plays a significant role in how network defenders and threats operate. Having a complete understanding of an organization's network and security architecture due to their particular operating model will facilitate the design and implementation of security controls and assist analysts in identifying detection points for threat observation. Figure 6 is an example of a high-level network topology diagram.

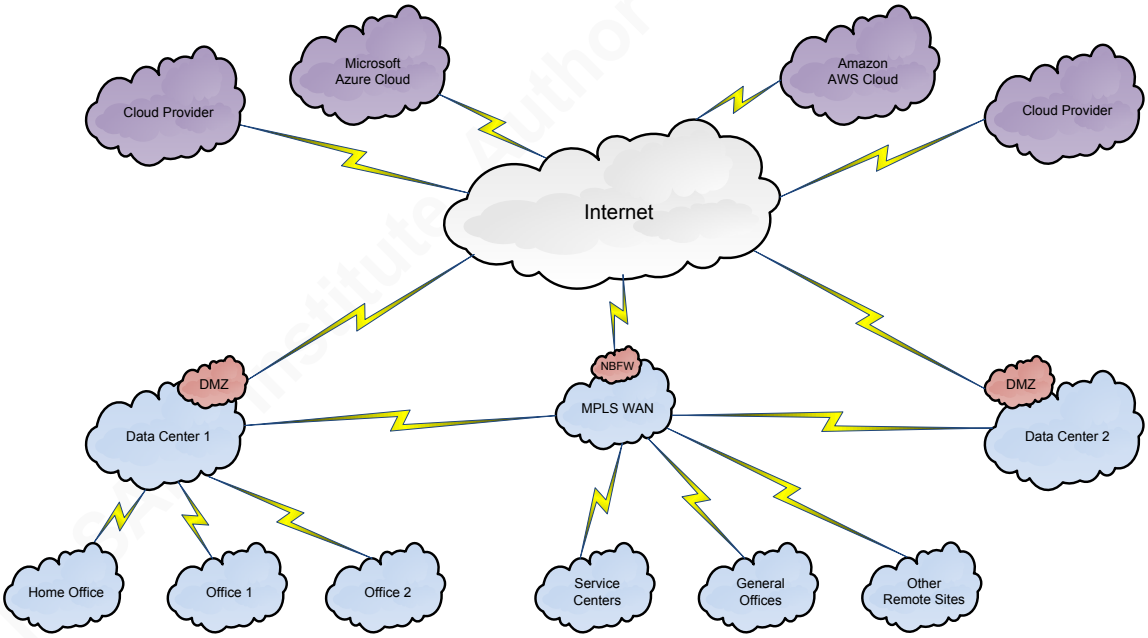


*Figure 6: Example of high-level network topology*

Analysts should break down operating systems into three categories to assess their impact on the operational environment. Those three categories are servers, workstations, and mobile devices. Describe the level of patching and maintenance on those, whether they are centrally managed by the business or not, what - if any - key nodes/information use a particular OS, and how threats view each operating system.

Greatly influencing network defense is the applications in the operational environment. Describe and assess the effects on threat courses of action and network defense from both internally developed applications and externally sourced (on premise or cloud) applications.

Brian P. Kime, bkime@mastersprogram.sans.edu

Historical reporting from supporting/supported information security teams helps the analyst assess the weaknesses, peculiarities, and threats in and around the organization's operational environment.

Describe and assess trust relationships between the DMZ, subdomains, and VLANs inside the organization's operational environment. Describe and assess how those relationships affect threat courses of action and network defense. Figure 7 in Appendix 1 depicts exploitable trust-relationships. Nodes in the graph represent devices. Arrows represent exploitable trust relationships. An arrow pointing from node A to node B represents "B trusts A, and B can be compromised from A". Teams should identify vulnerable trust relationships. In the below figure, node B is a compromised device. A could have been the means by which B was compromised. Therefore, the threat may compromise C now or in the future. By compromising C, a threat can compromise D (Yuill, et al., 2000).

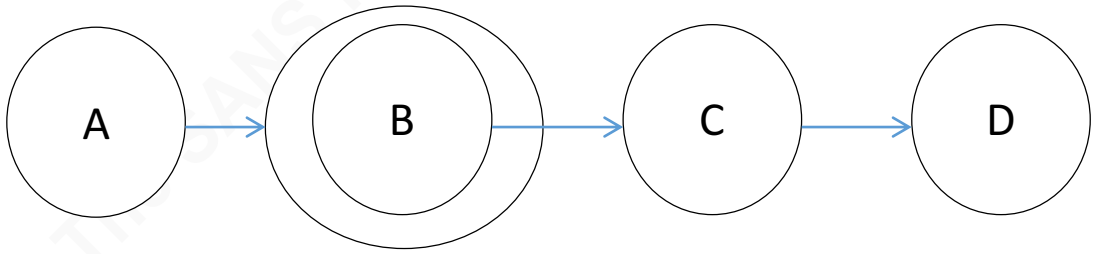


*Figure 7: Diagram of exploitable trust relationships (Yuill, et al, 2000)*

### 2.2.5. Describe How Systems Administrators, Network Users and Customers Can Affect Network Defense and Threat Operations

System-administration is the implementation and operation of the network. In practice, it has a controlling influence over security and over The Process itself. For example, individual departments may have their own system-administrators and the corporate IT department its own system-administrators. For the realms of administrative control, identify those aspects of network administration which affect the threat's operations and which affect network defenders' operations. Primary aspects are resources and abilities for secure administration (ex: the system administrator has little time for, and training in, security), prior performance of security efforts, resources available for assisting with The Process (systems administrators and networking teams may need to be

educated to see the value in assisting The Team with The Process), and security policy and its actual implementation.

A network's users play a key role in security and risk management, despite general users' lack of awareness of security concepts. Teams should collectively or individually, analyze the network's users. The analysis should identify those aspects of user behavior that affect the threat's operations and network defense. The primary aspects of user behavior include user accountability, security awareness training, and attitudes toward security. Teams should also know which users have elevated privileges on the network or greater access to key nodes and information

Analyze the different cohorts of users to assess their impact on network defense and threat operations. In addition, each business unit's users may affect network defense in ways different from the greater network user population. Furthermore, the business must know its individual customers and assess how they affect network defense and threat operations.

In order to reduce fraud, it is critical to understand a business's customers and how they interact with the network. Cyber threats are likely to target the same servers customers use to conduct business. If applicable to an organization, call centers must be aware of threat's masquerading as legitimate customers.

## 2.3. Step 3. Evaluating the Cyber Threats

Step 3 of Intelligence Preparation of the Cyber Operational Environment ("The Process") determines threat capabilities and the doctrinal principles and tactics, techniques, and procedures threats prefer to employ. This may include threats that create multiple dilemmas for network defenders by simultaneous employment of attacks and exploits ("ATP 2-01.3", 2014). This section is adapted from Chapter 5 of ATP 2-01.3. Figure 8 for a diagram of step 3.

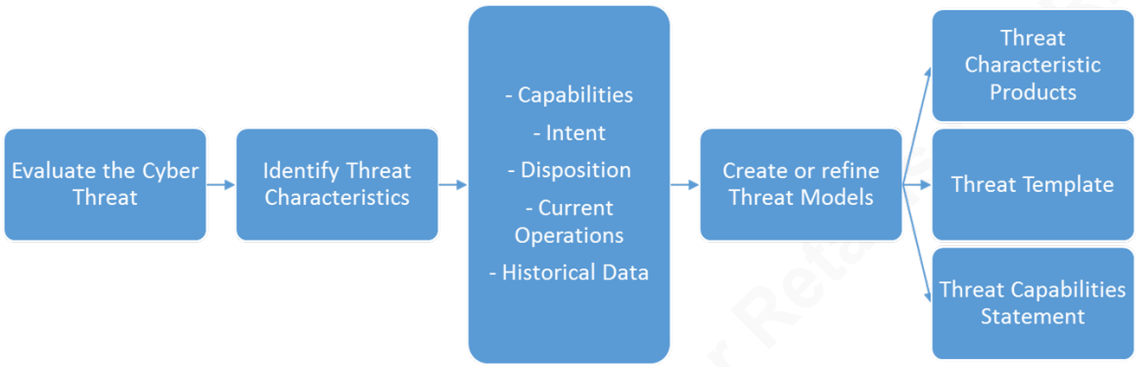


*Figure 8: Sub-steps of step 3 of Intelligence Preparation of the Cyber Operational Environment*

### 2.3.1. Desired End State

The Team develops threat models that accurately portray how cyber threats normally execute operations and how they have reacted to similar situations in the past. The primary output of step three of The Process is a compilation of threat models for each identified threat in the area of operations that The Team uses to guide the development of threat courses of action. This may include, creating and updating threat characteristics products, developing situation models, creating threat capabilities statements, updating the intelligence estimate, and refining and updating requests for information or requests for collection ("ATP 2-01.3", 2014).

### 2.3.2. Identify Threat Characteristics

In step three, The Team seeks to develop a model of the threat. In particular, The Team seeks to learn the threat's capabilities, intentions, and disposition, which govern the threat's behavior on the network. The Team derives this analysis from information about the threat's current and historical operations. Knowledge of the threat's capabilities, intentions, disposition, doctrine, and tactics provide the basis for developing a threat model and discovering the threat's vulnerabilities to detection.

Capabilities are the broad courses of action and supporting operations that the threat can take to achieve its goals and objectives. A threat's prior actions may reveal the threat's capabilities. The following two broad tactical cyber courses of action are generally open to cyber threats: attack and information collection.

Attack courses of action are further broken down into deny courses of action and manipulate courses of action. Within the deny courses of action, the US military considers three more specific courses of action: degrade, disrupt, and destroy. Degrade courses of action are those that deny access to, or operation, of a target to a level represented as a percentage of capacity. Disrupt courses of action are those that completely, but temporarily deny access to, or operation of, a target for a period of time. Destroy courses of action permanently, completely, or irreparably deny access to, or operation of a target. Attack courses of action affect the availability of information, systems, and networks. Manipulate courses of action control or change the target's information, systems, or networks (JP 3-12(R), 2013). Manipulate courses of action affect the integrity of information systems or networks.

Information collection courses of action are those that affect the confidentiality of information and typically support a threat's objectives and end-state. Information collection courses of action can occur in or outside the target network. One threat course of action is to collection information from sources (generally open, like Shodan) outside the target network in preparation for further courses of action. Information collection courses of action inside the target network include exploitation of human vulnerabilities (ex: social engineering), exploitation of software or hardware vulnerabilities (ex: installing a remote access tool), and exploitation of poorly configured systems to steal data (ex: SQL injection).

Cyber threats have varying intent. Teams should understand the various objectives of the threats facing their organizations. Evaluate a cyber threat's historical data to assess the intent of a threat's prior attacks or intrusions. Assessing a threat's intent regarding your organization also relies on having a robust understanding of the business model and key information contained in the networks. For example, if a known cyber threat sells PII in the underground markets, the organization's customer and employee PII may be that threat's objective.

A cyber threat's disposition comprises the arrangement or placing of their infrastructure and the threat's mental and technical tendencies and attitudes. An attack or breach may reveal the threat's personality traits. For The Process, CTI analysts are

interested in traits that govern the threat's behavior on the network. Those traits include judgment (the degree to which the threat thinks clearly and can be impaired by vices like greed, arrogance, obsession, and vengeance age and maturity, morality (the degree to which he is willing to inflict loss), patience, cautiousness (the risk the threat is willing to accept), and culture (Yuill, et al., 2000)).

In general, it is easier to profile behavior than it is to profile psychological attributes like knowledge, personality, motive, and asset-appraisement. Analysts can objectively observe behavior. However, analysts must subjectively assess a threat's psychological attributes. Strengthen assessments of psychological attributes by using multiple reliable sources of information for corroboration. Patterns of behavior can indicate intention, (ex: repeated nmap scans of a IP range may indicate the threat has a special interest in it).

Doctrine is overall how an organization employs its resources. Tactics, on the other hand, are parts of a strategy. While tactical doctrine refers to the threat's accepted organization and employment principles, tactics refer to the threat's conduct of operations toward a strategic goal. Based on knowledge of a threat's tactical doctrine, The Team can determine how the cyber threat may employ its resources against their organization under various conditions. Analysts integrate tactics in threat models and other intelligence products.

Doctrine and tactics for cyber threats refer to the tactics, techniques, and procedures that guide threat operations. Understanding how the threat prefers to operate aids the defender's awareness of potential threat courses of action. tactics, techniques, and procedures to consider in step 3 include: exploits used, tools used, techniques for avoiding detection, the degree of caution exercised in avoidance of detection, attack technique, time spent on the network (both duration and patterns-of-occurrence), use of a device or data once access is obtained. Knowing the amount of time the threat spends on information collection and attack is helpful for predicting future courses of action.

Patterns in the use of techniques and in the times-of-occurrence can be useful for predictive analysis. These patterns can reveal the threat's preferred tactics, techniques, and procedures. Pattern analysis time wheels are an excellent tool to profile a threat's

work habits. In addition, there are several popular books and security vendor reports (free and subscription) describing cyber threats tactics, techniques, and procedures and patterns that can help provide a means of discerning threat doctrine and tactics and future courses of action.

Some elements of tactics, techniques, and procedures analysis depend upon knowledge of the threat's capabilities, intentions, and likely courses of action. For example, if The Team knows the threat's likely targets, then they can identify the possible AAs to the target. Additional identifying attributes are the threats peculiar work habits. For example, malware compile time stamps can help an analyst estimate which time zone a threat operates.

Current operations are those operations currently engaged in by a threat. This includes operations against your organization or those within your vertical. Analyzing current cyber threat operations provides up-to-date information on the threat's characteristics.

Collecting the history of any cyber threat involves conducting research necessary to gather all relevant information regarding the threat and producing materials needed to communicate that information to the CISO and staff. Slide decks and papers are the two most commons methods for this purpose. The history component of the threat profile should include the original sources of information used to compile slide decks and papers. The entire Team should be familiar with these products.

Collect historical data from external sources – both open and closed – and from internal incident and forensics reports. In addition, using internal information, perform robust analytics on security events collected from all the sensors within the security stack to break down the malicious activity into categories that give the leadership a greater idea of the types of cyber threats observed by the information security group.

The Diamond Model of Intrusion Analysis may be useful to organize historical data. The model establishes the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim (Caltagirone, et al. 2013).

Brian P. Kime, bkime@mastersprogram.sans.edu

Attack evidence varies from being certain to being highly speculative. The evidence can be incorrect or incomplete. Revise any analysis based on uncertain, incomplete, or incorrect information when better information becomes available. Analysts need procedures and techniques for accommodating such revisions throughout The Process.

### 2.3.3. Create or Refine Threat Models

Threat models accurately portray how threats normally execute operations and how they have reacted to similar situations in the past. This also includes knowledge of threat capabilities based on the current situation. Create initial threat models by analyzing information collected from various sources ("ATP 2-01.3", 2014).

A threat model is a two-part analytical work aid designed to assist in the development of situation models during step 4 of The Process. The two parts are convert threat doctrine or patters of operation to graphics and describe the threat's tactics, techniques, and procedures and options ("ATP 2-01.3", 2014).

In this step, the analyst builds doctrinal models consisting of organizational, tactics, techniques, and procedures, and behavioral characteristics. Threat doctrinal models are how the threat operates regardless of time, operational environment, or the target's reaction. To achieve a threat objective like privilege escalation or data exfiltration, a Team can sequence multiple models into an attack or breach scenario.

The Cyber Kill Chain describes a basic intrusion model consisting of the following steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. Reconnaissance is the research, identification, and selection of targets. Weaponization refers to the packaging of exploit or attack code into a payload. Transmitting the weaponized payload to a target is the delivery phase. Exploitation occurs when the payload runs on the victim host. Command and control is necessary for the threat to send instructions or more malware to a compromised host. Actions on the objective are the intent of the cyber intrusion or attack (Hutchins, et al, 2010). The Cyber Kill Chain model is useful across a wide spectrum of cyber threats.

Brian P. Kime, bkime@mastersprogram.sans.edu

Threat models portray how the threat might utilize its capabilities to perform the functions required to accomplish its objectives. Scale threat models to depict the threat's disposition and actions for a particular type of operation (for example, denial of service or remote code execution). When possible, graphically depict models as an overlay, on a supporting system or through some other means. Tailor threat models to the needs of the business or staff creating them.

The analyst constructs threat models through an analysis of the intelligence database and an evaluation of the threats' past operations. The analyst also determines how the threat normally employs and deploys their tradecraft and infrastructure. Modeling requires continuous refinement to portray threat patterns and practices accurately. Some threat models will consider the threat as a whole while other products depict pattern analysis, time event charts, and association matrices.

The threat model includes a description of the threat's preferred tactics. The analyst should describe the threat's preferred tactics even if the analyst depicted them in graphic form. The description lists the options available to the threat should the operation fail or succeed (branches or sequels), prevents the threat model from becoming more than a "snapshot in time", and aids in analyzing the organization's defense in depth strategy during the development of threat courses of action and situation models.

When identifying threat capabilities and courses of action, start with a full set of threat models and consider the threat's ability to conduct each operation based on the current situation and the threat's own constraints. Most situations will not present the threat with ideal conditions envisioned by their doctrine. As a result, the threat's actual capabilities usually will not mirror the ideal capabilities represented by the complete set of threat models.

Analysts should avoid overstating the threat model and threat capabilities. The proper use of findings and recommendations developed from threat assessments will in turn develop realistic threat models. During any discussion of the threat, cultural awareness is an important factor. By developing an awareness of the threat's culture, the information security group can better anticipate a threat's course of action. Analyzing the impacts of geopolitical, religious, and social events will help discern threat operational

tempos. For example, threats under official or unofficial control of a foreign government will respond to geopolitical events. Religious and social holidays will also affect when cyber threats area active. Another example, Chinese cyber threat activity drops significantly during the Chinese Lunar New Year.

Threat doctrinal models show the deployment pattern and disposition preferred by the threat when not constrained by the effects of the operational environment. These models are normally scaled depictions of threat dispositions for a particular operation. Threat models graphically portray how the threat prefers to utilize its capabilities to perform the functions required to accomplish its objectives. Scale threat models to depict the threat's disposition and actions for a particular type of operation (for example, DDoS or data exfiltration).

When possible, models depict graphically as an overlay, on a supporting system, or through some other means. Teams tailor threat models to the needs of the business. They may depict – but are not limited to – obstacles. threat infrastructure, target infrastructure, and stages of Kill Chain.

Threat models allow the information security group to fuse all relevant threat information, assist in identifying intelligence gaps, predict threat activities, adapt courses of action, and synchronize information collection. Tables 3 and 4 in Appendix 1 are examples of threat models.

The analyst describes and makes a determination of what goal or goals the threat is trying to achieve. Threat objectives are often, but not always, what the information security group is trying to prevent. Threat objectives will be specific to the type of threat and the organization's operational environment. The analyst should also describe the threat objective in terms of purpose and end state.

Two characteristics of the threat's tactical options are exploitability and sustainability. Exploitability is the degree of difficulty in appropriating the use of some network feature. Sustainability is how long and exploited vulnerability can be compromised.

Brian P. Kime, bkime@mastersprogram.sans.edu

A threat capabilities statement is a narrative that identifies a particular action for which the threat has the capability to complete and the tactics, techniques, and procedures the threat prefers to use to accomplish its objectives. It addresses operations portrayed in the threat doctrinal model. Below is an example of a threat capability statement:

> *Threat A is capable of using open source tools to reconnoiter potential targets. The threat is able to identify vulnerable SQL databases and write scripts to exploit those vulnerabilities. The threat can deliver the exploits over anonymity networks or other means of obfuscating the threat's true location. The threat can run the exploit script and exfiltrate data from said SQL databases. If the threat is unable to breach a target SQL database, they will shift tactics and resort to spear phishing database administrators in hopes of harvesting database credentials.*

## 2.4. Step 4. Developing Cyber Threat Courses of Action

Step 4 of Intelligence Preparation of the Cyber Operational Environment ("The Process") identifies and describes threat courses of action (course of action) that can influence information security operations. Determining threat courses of action is a two-step process consisting of developing courses of action and developing event models and matrices ("ATP 2-01.3", 2014). This section is adapted from Chapter 6 of ATP 2-01.3. Figure 9 is a diagram of step 4.

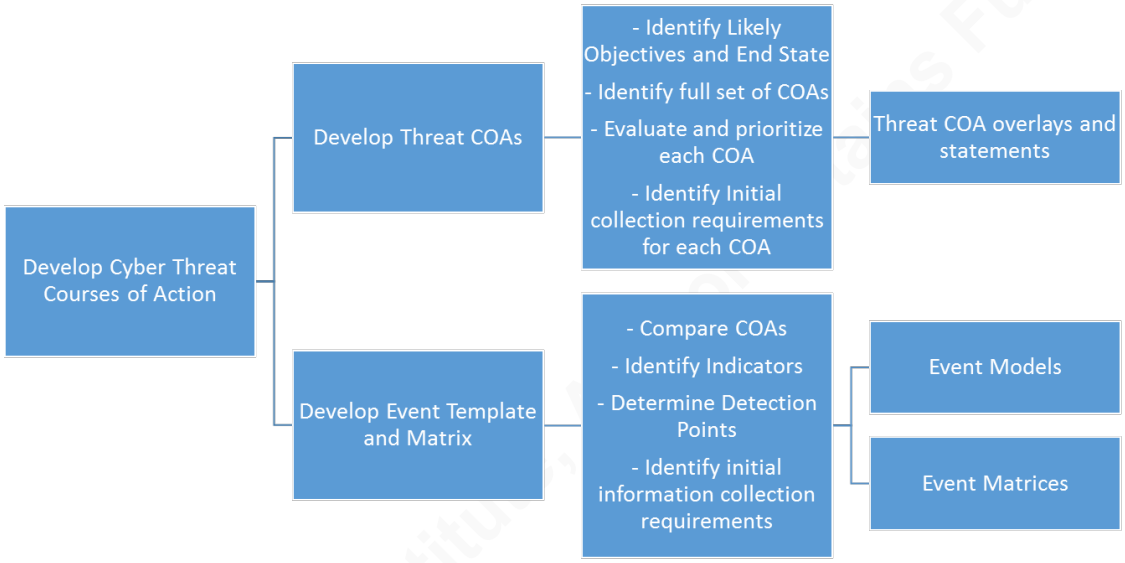


*Figure 9: Sub-steps of step 4 of Intelligence Preparation of the Cyber Operational Environment*

### 2.4.1. Desired End State

The desired end state of step 4 of The Process is the development of graphic overlays (threat situation models) and narratives (threat course of action statements) for each possible threat course of action. The information security group uses these products while conducting defense in depth tactics, operations, and strategy. The Team replicates the set of courses of action that the threat is considering; identifies all courses of action that will threaten the organization's operations, networks, information, employees, or customers; and identifies those areas and activities that, when observed, will discern which course of action the threat has chosen. The primary outputs associated with step 4 may include threat course of action models with associated course of action statements, event models and associated event matrices, input into the collection plan, an updated intelligence estimate, recommended PIRs, and input into security staffing, policy, and budgetary planning ("ATP 2-01.3", 2014).

### 2.4.2. Develop Threat Courses of Action

Cyber threat course of action development is a four-step process that requires an understanding of the threat characteristics and the effects of network topology. The most important element in determining threat courses of action is in understanding threat operational art and tactics, techniques, and procedures. The example threat description table in step two lists nine threat types. The spectrum of an organization's cyber threats may change over time. Regardless of threat, the process to determine threat courses of action is identical: (1) identify likely objectives and end state; (2) identify the full set of courses of action available to the threat; (3) evaluate and prioritize each threat course of action (most likely to least likely & most dangerous to lease dangerous); (4) identify initial collection requirements for each course of action ("ATP 2-01.3", 2014).

In order to plan for all possible contingencies, the network defender understands all courses of action a threat can use to accomplish their objectives. To aid in this understanding, The Team determines all valid threat courses of action and prioritizes them from most to least likely. The Team also determines which threat course of action is the most dangerous to the organization. "To be valid, threat courses of action should be: feasible, acceptable, suitable, distinguishable, and complete" ("ATP 2-01.3", 2014).

Feasibility refers to the threat's ability and time to carry out a course of action. Acceptability discusses the risks a threat is willing to accept). The potential for accomplishing the threat's likely objective is a course of action's suitability. Distinguishable means each course of action must be significantly different. Lastly, to be complete, course of action must answer who, what, when, where, why, and how.

### 2.4.3. Identify Likely Objectives and End States

The Team identifies the threat's likely immediate and subsequent objectives and desired end state based on the results earlier in The Process. These elements are included in the threat course of action statement developed for each course of action.

An objective is a clearly defined, decisive, and attainable goal. The end state is a set of required conditions that define achievement of the threat's objectives. Threat objectives can be political, criminal, information, or a combination. For example, a threat

may attack to deny a business' customers access to their accounts or exploit a vulnerable web application for "lulz."

### 2.4.4. Identify the Full Set of Course of Action Available to the Threat

Regardless of the type of threat group and the type of operation, threats may plan operations based on task, purpose, method, and end state. Teams identify the tasks, purpose, and end state for each course of action developed. By identifying these for each course of action, The Team will be better able to determine the chosen threat course of action during the conduct of operations. Regardless of the type of threat, when developing a threat course of action, Teams determine the mission, objectives, capabilities, vulnerabilities to detection, decision points, branches (a contingency plan), sequels (a course of action that follows another course of action), and how the operational environment will affect a threat course of action.

Once The Team has identified all valid threat courses of action, it compares each one to the others and prioritizes them by number. For example, if a Team develops four courses of action, course of action 1 is the most likely and course of action 4 is the least likely. Additionally, Teams determine which course of action is the most dangerous to their organization. The most likely course of action may also be the most dangerous.

### 2.4.5. Evaluate and Prioritize Each Threat Course of Action

Information security groups should optimize their defense in depth strategy to counter the most likely threat courses of action, while allowing for contingency options should the threat choose another course of action. Therefore, Teams evaluate each threat course of action and prioritize it according to how likely it is that the threat adopts that option. Generally, cyber threats are more likely to use a course of action that offers the greatest advantage while minimizing risk. However, based on the situation and its objectives, the threat may choose to accept greater risk to achieve a desired end state. Teams develop and prioritize as many valid threat courses of action as time allows but at a minimum develops the most likely and most dangerous courses of action.

### 2.4.6. Situation Model for Each Threat Course of Action

When constructing situation models, Teams use the threat doctrine models developed during step three of The Process as a base. Modify those models based on the significant effects the operational environment will have on the threat course of action. For example, a threat may not be able to access a target server directly from the Internet and must compromise other resources first to gain access to the target.

A threat situation model is a depiction of a potential threat course of action as part of a particular threat operation. Develop situation models using the threat's current situation, based on threat doctrine and the effects of the operational environment. Situation models can be simple sketches, reserving in-depth development and analysis for later when more time is available. Each threat course of action has a corresponding situation model. Figure 10 is an example of a Threat Situation Model.

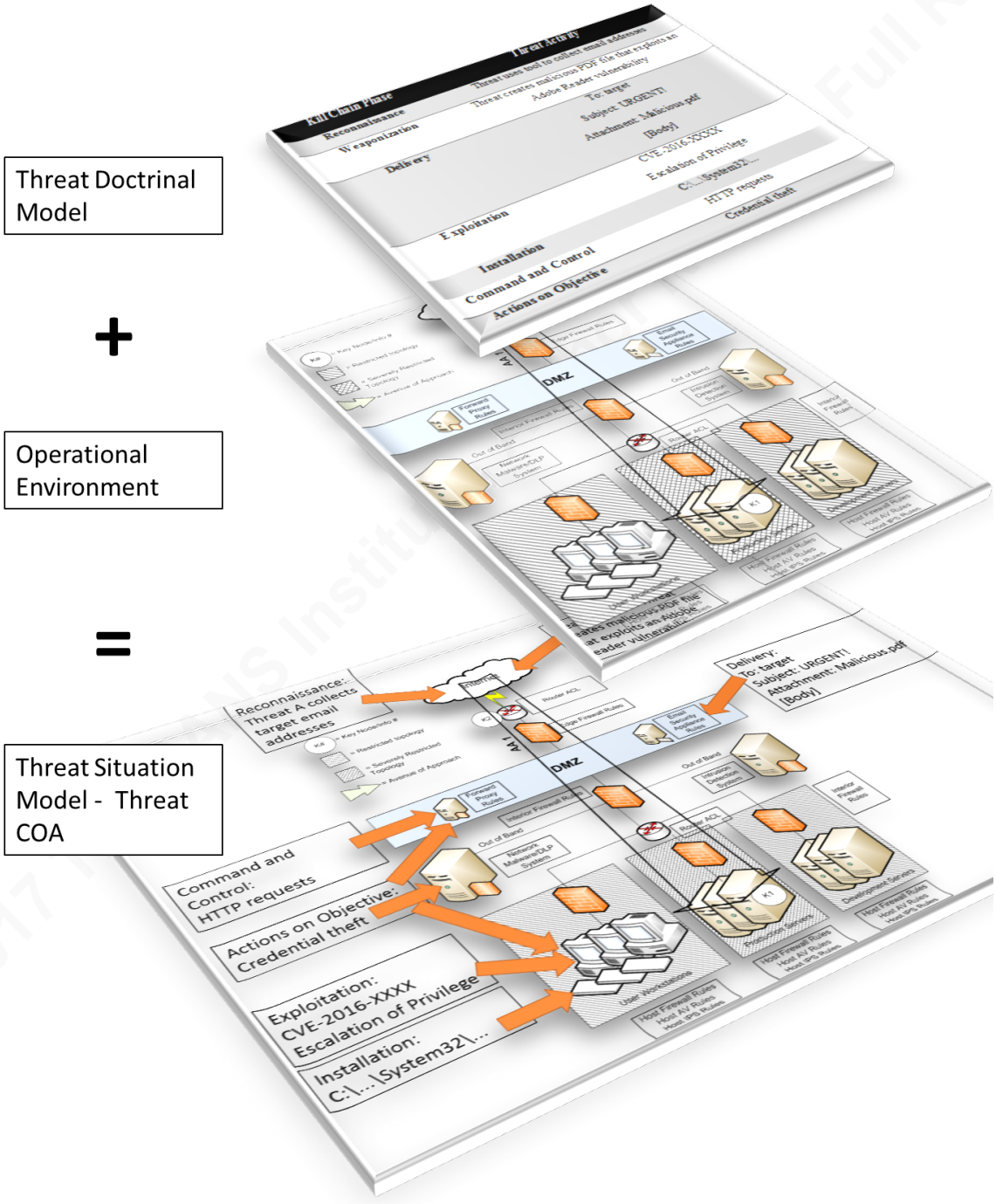


*Figure 10: How to create a threat situational model.*

Brian P. Kime, bkime@mastersprogram.sans.edu

### 2.4.7. Threat Course of Action Statement

As stated previously, every threat course of action includes a threat course of action statement, which is a narrative that describes the situation model. Figure 11 is an example of a threat course of action statement.

**Current Threat Situation:** Threat A is a criminal for hire that sells illegal services on an underground market.

**Threat Mission:** Threat A will exploit vulnerabilities in Adobe Reader to install a keylogger on user workstations in the short term in order to steal credentials.

**Threat Objectives and End State:** Threat end state is to have acquired valid network credentials.

**Threat Capabilities:** Threat is a capable of acquiring email address of current employees, and weaponizing PDF documents.

**Threat Vulnerabilities to Detection:** Threat must deliver payload via email that an email security appliance will analyze for violation of rules for mail servers, sender address, and attachments. HIPS has rules to detect installation of keyloggers. Web proxy has rules to block HTTP visits to risky websites.

**Branches:** If the targeted users do not open the weaponized PDF, the threat will have to attempt another COA.

**Sequels:** If the threat acquires legitimate network credentials, they can use them to sustain and increase access to the target or sell the credentials on an underground market.

*Figure 11: Example of a Threat course of action statement*

### 2.4.8. Identify Initial Collection Requirements for Each Course of Action

After identifying the full set of potential threat courses of action, Teams develop the tools necessary to determine which course of action the threat will implement. Teams assign threat assessments a level of confidence (low, medium, or high) because the threat always "has a vote." However, Teams can develop the intelligence requirements and indicators necessary to support the construction of an intelligence collection plan that can

provide the intelligence necessary to confirm or deny threat courses of action and locate threats in the operational environment. To meet the intelligence requirements of the business, Teams collect and process indicators. An indicator is an item of information that reflects the intention or capability of a threat to adopt or reject a course of action. Teams should generally relate intelligence requirements to confirming or denying a threat course of action.

### 2.4.9. Develop the Event Template

An event template is a graphic overlay used to confirm or deny threat courses of action. The Computer Security Incident Response Team (CSIRT) can also use the event template during the incident handling process to aid in determining which course of action the threat has adopted. An event template always accompanies an event matrix.

Constructing an event template is an analytical process that involves comparing the multiple threat courses of action developed earlier in step four of The Process to determine the place or condition in which the threat must make a decision on a particular course of action. Figure 12 is an example of the basic process of generating an event template.

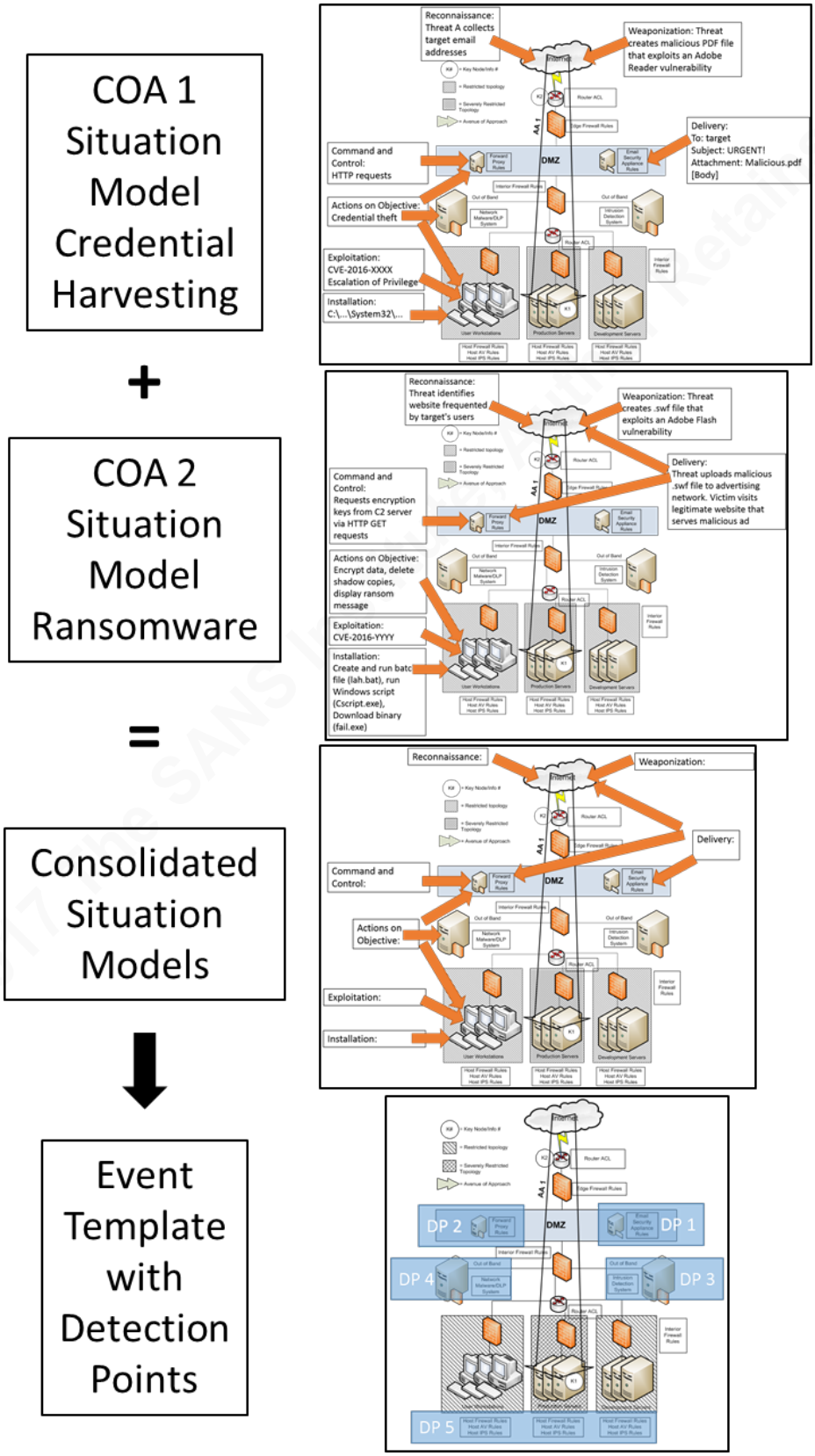


*Figure 12: How to create an event template with detection points*

Brian P. Kime, bkime@mastersprogram.sans.edu

The event template is comprised of detection points and the security control obstacle overlay. Normally, select detection points to capture indications of threat courses of action, but, at times, may be related to conditions of the operational environment.

An event template with detection points shows the business where in the operational environment Teams expect to observe threats as they pursue a particular course of action. Careful selection of detection points can make it possible to distinguish among courses of action to tell which one of a set of possible courses of action might actually be in play. Detection points include – but are not limited to – firewalls, intrusion detection/prevention systems, breach detection systems, email gateways, web proxies, DNS servers, VPN systems, customer portal authentication systems, 3rd party threat reports, social media, and IRC.

### 2.4.10. Develop the Event Matrix

An event matrix is a table that associates the detection points identified in the event template with indicators to aid in determining which course of action the threat is implementing. An indicator is an item of information that reflects the intention or capability of a threat to adopt or reject a course of action. Constructing an event matrix is an analytical process that involves determining the indicators of threat activity that aid in identifying the decisions the threat has made. Table 5 in Appendix 1 illustrates the basic mechanics of this process.

## 3. Planning and Direction

Upon completion of all Process steps and products, Teams will have a robust understanding of the operational environment and the threat landscape. The Team is now ready to present the products from The Process to the leadership and begin involving them in planning and directing CTI operations. Within the planning and direction step of the Intelligence Cycle, Teams should strive to develop PIRs, an intelligence architecture, a collection plan, and any necessary requests for information with the organization's leadership.

Brian P. Kime, bkime@mastersprogram.sans.edu

## 3.1. Intelligence Requirements and the Collection Plan

An intelligence requirement is any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence or a requirement for intelligence to fill a gap in the business' knowledge or understanding of the operational environment or threats ("JP 2-0", 2013). Any team within the information security group may recommend intelligence requirements for designation by the leadership as PIRs. The Team, however, should have overall responsibility within the information security group for consolidating intelligence requirements and submitting the recommendations to the leadership for prioritization.

PIRs are those intelligence requirements approved by the organization's leadership. Successfully (or even partially) answering PIRs provides the leadership with the intelligence necessary to make strategic, operational, or tactical changes to the people, process, and tools that reduce risk to the organization.

To help answer PIRs, Teams should use the event matrix from step 4 of The Process. The event matrix includes a column of indicators. Teams match the indicators from the event matrix to a PIR. For each indicator, create a Specific Information Requirement. Next, link each Specific Information Requirement to a detection point, also in the event matrix. This new matrix becomes The Team's intelligence collection plan. As the information security group may not have operational access to every detection point, the intelligence collection plan (with management support) will give The Team authority to collect logs and reports from tools managed by groups outside of the information security group. Table 6 in Appendix 1 is an example of an Intelligence Collection Plan.

## 3.2. Intelligence Architecture

As there are many papers on cyber threat intelligence architectures, this paper is not going to address intelligence architectures in much detail. In general, however, any intelligence architecture should be dynamic and capable of answering PIRs at all levels of intelligence. People and processes must be accounted for as much, if not more so, than the technology part of an intelligence architecture.

Brian P. Kime, bkime@mastersprogram.sans.edu

The outputs from The Process should help a Team and information security leadership design an intelligence architecture that processes and exploits the right information in order to provide CTI analysts with the necessary information. This architecture should also support the analysis and production of finished intelligence. Any intelligence architecture should also provide robust processes to share information and finished intelligence with trusted third parties and internal customers.

## 4. Conclusion

Cyber Threat Intelligence Teams do not have to plan to fail if their organization's senior leadership supports and resources them appropriately. The Intelligence Preparation of the Cyber Operational Environment products and an intelligence collection plan may be the "marketing collateral" that influences boards of directors and C-suite executives to see that a robust CTI program adds value beyond traditional information security. Implementing a CTI program in an organization can and should be an information security and risk management force multiplier if that organization's management is involved throughout the Intelligence Cycle. To be sure, educating C-suite executives and board members to support a Team, and specifically The Process, will not be easy.

Furthermore, fusing counterintelligence strategies, operations, and tactics with traditional external threat focused intelligence operations will greatly enhance an organization's visibility into all cyber threats. Lastly, it was the goal of this Gold Paper to give the struggling Team the tools needed to provide an organizations' senior leadership the "so what" of CTI.

Brian P. Kime, bkime@mastersprogram.sans.edu

# References

Caltagirone, S., Pendergast, A., & Betz, C. (2013, June 24). *The Diamond Model of Intrusion Analysis* [Scholarly project]. The Center for Cyber Intelligence Analysis and Threat Research. Retrieved from https://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf

Carnegie Mellon University (CMU), Software Engineering Institute. (n.d.). Insider Threat. Retrieved February 18, 2016, from https://www.cert.org/insider-threat/index.cfm

Dunbar, B. (n.d.). Impacts of Strong Solar Flares. Retrieved February 18, 2016, from https://www.nasa.gov/mission_pages/sunearth/news/flare-impacts.html

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010, October 24). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* [Scholarly project]. Lockheed Martin Corporation. Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Ragan, S. (2016, February 29). Threat intelligence programs lack context experts say. Retrieved February 29, 2016, from http://www.csoonline.com/article/3038833/security/threat-intelligence-programs-lack-context-experts-say.html

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

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

US Department of Defense, Joint Chiefs of Staff. (2013, February 5). *Cyberspace Operations* (Joint Publication (JP) 3-12(R)).

Yuill, J., Wu, F., Settle, J., Gong, F., Forno, R., Huang, M., & Asbery, J. (2000). Intrusion-detection for incident-response, using a military battlefield-intelligence process. Computer Networks, 34(4), 671-697.

Brian P. Kime, bkime@mastersprogram.sans.edu

# 5. Appendix 1

*Table 1: Example of threat description table*

| Threat type | Disposition | Description |
|---|---|---|
| Malicious insider | Already in the operational environment via FTE or as a contractor/consultant; may hold a grudge against the company or individuals | Motivated to compromise the organization over grievances or manipulated by external party; can use internal tools |
| Unintentional insider | Already in the operational environment via FTE or as a contractor/consultant; lacks training, attention to detail, or a desire to protect the company | In the course of everyday business, increases risk to the organization via ignoring security policies, carelessness, and ignorance. |
| Commodity criminals | Financially motivated, commonly located outside US | Trade malware and access to botnets in underground or closely held forums/markets. |
| Criminals-for-hire | Financially motivated, commonly located outside US | Higher skilled and resourced than commodity criminals, often sells services on specialized underground markets/forums. |
| Corporate espionage | Business competitors. Stealing trade secrets and intellectual property or disrupting operations to strengthen their market position; | Technical abilities vary greatly; may outsource cyber operations to third parties. |
| Foreign espionage | Located outside US; To support local competitors, steal PII/PHI of potential spies, influence | Highly trained and resourced cyber operators acting on orders from a foreign government; may |

Brian P. Kime, bkime@mastersprogram.sans.edu

| | | |
|---|---|---|
| | media, "diplomacy by other means" | use custom tools/malware or commodity malware and a target's own tools |
| Hacktivists | Located worldwide; communicate via social media and IRC; To right a perceived wrong or influence media narrative | Skills and tools vary as hacktivists are usually disorganized. May use commodity tools. Commonly "defaces" vulnerable websites to spread messages. Often announces target prior to delivery stage |
| Chaotic actors | Located worldwide; Known to attack online gamers or easy targets; motivation for attacks is often "for the lulz". | Capabilities vary greatly; Often uses "stresser" or "booter" services to attack online video game adversaries. Uses free or open source tools to find easily exploitable vulnerabilities in order to "deface" a web page. |
| Extortionists | Financially motivated; located worldwide; attempts to coerce targets into paying them to go away | Capabilities vary greatly; will often conduct a test attack to scare targets into paying. Often uses "stresser" or "booter" services for DDoS attacks. May also threaten use of destructive malware. |

*Table 2: Example Topology Effects Matrix*

| Topology Aspect | Topology Effects |
|---|---|
| **Network Obstacles** | Network is segmented into different zones, NIDS and network malware/DLP are not in place to block malicious activity |

| | |
|---|---|
| **Avenues of Approach** | There is one route into the network; all traffic must pass through border router, edge firewall, and DMZ; no reverse proxy |
| **Key Nodes/Information** | Production servers host PII/PHI |
| **Observation** | DMZ and NAT prevents direct observation of production servers; all threats can be observed at edge firewall |
| **Concealment** | Using stolen credentials and SFTP could conceal data exfiltration |

*Table 3: Example Threat Model 1*

| Kill Chain Phase | Threat Activity |
|---|---|
| **Reconnaissance** | Threat uses tool to collect email addresses |
| **Weaponization** | Threat creates malicious PDF file that exploits an Adobe Reader vulnerability |
| **Delivery** | To: target<br>Subject: URGENT!<br>Attachment: Malicious.pdf<br>[Body] |
| **Exploitation** | CVE-2016-XXXX<br>Escalation of Privilege |
| **Installation** | C:\...\System32\... |
| **Command and Control** | HTTP requests |
| **Actions on Objective** | Credential theft |

*Table 4: Example Threat Model 2*

| Kill Chain Phase | Threat Activity |
|---|---|

| | |
|---|---|
| **Reconnaissance** | Threat identifies website frequented by target's users |
| **Weaponization** | Threat creates .swf file that exploits an Adobe Flash vulnerability |
| **Delivery** | Threat uploads malicious .swf file to advertising network. Victim visits legitimate website that serves malicious ad |
| **Exploitation** | CVE-2016-YYYY |
| **Installation** | Create and run batch file (lah.bat), run Windows script (Cscript.exe), Download binary (fail.exe) |
| **Command and Control** | Requests encryption keys from C2 server via HTTP GET requests |
| **Actions on Objective** | Encrypt data, delete shadow copies, display ransom message |

*Table 5: Example of an Event Matrix*

| Detection Points | Indicators | Threat course of action indicated |
|---|---|---|
| **1, 2, 3, 4, 5** | • Malspam<br>• HTTP requests to risky websites<br>• HIPS/AV alerts<br>• IDS alerts | Course of action 1 -<br>Credential Theft |
| **2, 3, 4, 5** | • HTTP requests from legit websites to risky ad networks<br>• HTTP requests to risky websites<br>• HIPS/AV alerts<br>• IDS alerts | Course of action 2 -<br>Ransomware |

Brian P. Kime, bkime@mastersprogram.sans.edu

| | | |
|---|---|---|
| | • Suspicious pattern of file modification | |

*Table 6: Example of an Intelligence Collection Plan*

| PIR # | Priority Intelligence Requirement | Indicator | Specific Information Requirement | Detection Point |
|---|---|---|---|---|
| 1 | Who are the threats or groups who may attempt to attack or exploit the organization? | The organization's employees' unusual or unauthorized attempts by to exfiltrate confidential the organization's data | Who are the organization's employees, in an unusual or unauthorized manner, attempting to exfiltrate confidential the organization's data? | Data Loss Prevention tools |
| | | Emails received by non-public, non-advertised, test accounts (honey email accounts) | Who are the threats sending emails received by the organization's honey email accounts? | Email security appliance |
| | | Talk on social media, chat rooms, paste sites, etc. about targeting the | Who is talking on social media, chat rooms, paste sites, etc. about targeting the organization logically? | Social Media/Paste sites/IRC rooms/Anonymity networks/social media accounts falsely claiming to |

| | | | | |
|---|---|---|---|---|
| [redacted] | | organization logically | | be the organization's employees |
| | | Talk on social media, chat rooms, paste sites, etc. about targeting the organization physically | Who is talking on social media, chat rooms, paste sites, etc. about targeting the organization physically? | Social Media/Paste sites/IRC rooms/Anonymity networks |
| | | IRL data linked to known threat/group infrastructure | Who are the IRL people linked to known threats who may attempt to exploit or attack? | OSINT/Cyber HUMINT |
| | | Reconnaissance conducted on newyorklife.com | What activity on newyorklife.com appears to be threats reconnoitering the organization? | Web marketing analytics |
| | | The organization's BIN/IINs found on Internet (Any CC's with the organization's name are only affinity cards) | Who is sharing/talking about the organization's BIN/IINs on the Internet | OSINT/Cyber HUMINT |

Brian P. Kime, bkime@mastersprogram.sans.edu

| | | | | |
|---|---|---|---|---|
| | | IOCs known to have targeted industry vertical | What are the IOCs/threats/groups known to have targeted the organization's life insurance/retirement competitors | ISACs/subscription threat intelligence |
| **2** | Who provides support to cyber threats and groups who wish to attack or exploit the organization? | Sponsoring organizations supporting cyber threats targeting the organization | Who are the sponsoring organizations supporting cyber threats targeting the organization? | Social Media/Paste sites/IRC rooms/Anonymity Networks/OSINT |
| | | Front companies or Internet properties supporting any cyber threat. | What are the front companies or Internet properties supporting any cyber threat? | Domain registrations/Social Media/OSINT |
| | | Buyers of the organization's confidential data | Who are the threats who are interested in buying confidential organizational data? | Social Media/Paste sites/IRC rooms/Anonymity Networks |
| **3** | What are the tactics, techniques, procedures, infrastructure, | Known threats or groups indicators of compromise in the organization's logs | Which indicators of compromise in the organization's logs belong to cyber threats or groups? | SIEM/log repositories |

| | | | | |
|---|---|---|---|---|
| | resources, and indicators of compromise of any threat or group that may target the organization? | Emerging threat tactics, techniques, and procedures that may be used against the organization | What are the emerging tactics, techniques, and procedures of cyber threats around the world that may be used against the organization? | Vendor threat reports/paid TI/OSINT/etc. |
| | | Unusual amount of data leaving the organization's environment | Is an unusual amount of data leaving the organization's environment? | Data Loss Prevention tools |
| | | LinkedIn profiles falsely claiming to be current the organization employees | What LinkedIn profiles falsely claim to for current the organization employees? | Custom script to query LinkedIn and HR records |
| | | Domains created to mimic legitimate the organization's domains | What are the domains mimicking the organization's legitimate domains? | Domain registrations |
| **4** | Which vulnerabilities – including but not limited to application, software, | Attacks or exploit attempts against the organization's honeypots | What attacks or exploit attempts observed against the organization's operated honeypots? | the organization's honeypots |
| | | Known unpatched, | What are the known, unpatched, | Automated vulnerability |

| | | | | |
|---|---|---|---|---|
| | network, and human – may threats or groups use to attempt to exploit or attack the organization? | vulnerable software on the organization's production networks for which exploits are publicly available. | vulnerable software on the organization's production networks for which exploits are publicly available? | scanning + OSINT + paid TI |
| | | Known unpatched, vulnerable hardware on the organization's production networks for which exploits are publicly available. | What are the known, unpatched, vulnerable hardware on the organization's production networks for which exploits are publicly available? | Automated vulnerability scanning + OSINT + paid TI |
| | | The organization's Executives being talked about negatively in social media/anonymity networks | Whom are the threats talking about the organization's executives? | OSINT/Cyber HUMINT |
| | | The organization's employees exhibiting | Which of the organization's employees are exhibiting behavior | Data Loss Prevention tools |

| | | | | |
|---|---|---|---|---|
| | | behavior consistent with signs of internal threats | consistent with signs of internal threats | |
| **5** | What changes to any regulatory guidance or mandates will affect the organization's information security policies? | SEC rules regarding cyber | What new or proposed SEC rules may affect the organization's information security policies? | www.sec.gov, OSINT |
| | | Changes to the USA PATRIOT Act regarding money laundering | What changes are being considered/approved to the USA PATRIOT Act that would change the way the organization's shares information regarding suspicious financial transactions? | OSINT |
| | | Changes to the US Dept. of Treasuries OFAC sanctions list. | What changes are being considered/approved to the list of countries on the US Dept. of Treasury sanctions list? | www.treasury.gov |

Brian P. Kime, bkime@mastersprogram.sans.edu

| | | | | |
|---|---|---|---|---|
| [redacted] | | HIPAA rules regarding cyber | What new or proposed HIPAA rules may affect the organization's information security policies? | OSINT |
| | | FFIEC rules regarding cyber | What new or proposed FFIEC rules may affect the organization's information security policies? | www.ffiec.gov, OSINT |



Brian P. Kime, bkime@mastersprogram.sans.edu

# 6. Appendix 2

## Glossary of Acronyms

| | |
|---|---|
| AA | Avenues of Approach |
| ACL | Access Control List |
| ATP | Army Techniques Publication |
| C2 | Command and Control |
| CIA | Confidentiality, Integrity, Availability |
| CISO | Chief Information Security Officer |
| CME | Coronal Mass Ejection |
| course of action | Courses of Action |
| CSIRT | Computer Security Incident Response Team |
| CTI | Cyber Threat Intelligence |
| DDOS | Distributed Denial of Service |
| DMZ | De-Militarized Zone |
| DNS | Domain Name Service |
| FTE | Full Time Employee/Employment |
| HIPS | Host Intrusion Prevention System |
| HUMINT | Human Intelligence |
| IDS | Intrusion Detection System |
| IOC | Indicator of Compromise |
| IPB | Intelligence Preparation of the Battlefield |
| IPS | Intrusion Prevention System |

Brian P. Kime, bkime@mastersprogram.sans.edu

| | |
|---|---|
| IRC | Internet Relay Chat |
| JP | Joint Publication |
| NAT | Network Address Translation |
| OPSEC | Operational Security |
| OS | Operating System |
| OSINT | Open Source Intelligence |
| PDRR | Prevent, Detect, Restore, And Respond |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| PIR | Priority Intelligence Requirement |
| SIR | Specific Information Requirement |
| SNMP | Simple Network Management Protocol |
| tactics, techniques, and procedures | Tactics, Techniques, Procedures |
| US | United States |
| VLAN | Virtual Local Access Network |

Brian P. Kime, bkime@mastersprogram.sans.edu