Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats

By: Robert M. Lee , Ben Miller, and Mark Stacey

Executive Summary

The Industrial Control Systems industry has arrived at a recognition point. It has become clear to most asset owners and operators that consistent monitoring and the establishment of defensible networks within process environments is required to ensure safe and reliable operations. Like the need to monitor processes, a need exists for increased awareness of process data that can be rapidly analyzed and acted upon to ensure integrity and reliability.

Today, many organizations have pursued the development of asset hardware and software inventories, as well as collecting information from various asset types. Many organizations are looking to move beyond asset inventory and basic logging capabilities. Much of the focus on the need for asset inventories is around architecture and passive defense purposes, including segmentation, vulnerability identification and patching, secure configuration, and controlling access.[1] This approach is important to security but does not fully address the needs of security personnel, such as incident responders and security operations staff who must prepare for and conduct investigations into adversary activity in their environments. Thus, defenders need to go beyond asset inventories in the traditional sense and develop and utilize an internally-focused collection management framework.

A collection management framework (CMF) is a structured approach to identifying data sources and determining what information can be obtained from each source. The concept of collection management is rooted in intelligence work. In the intelligence field, it is routine to identify requirements and determine where sources exist to collect information to satisfy those requirements. Various styles of collection management exist and can incorporate attributes such as a reliability rating of the data and measurements of trustworthiness, accuracy, and completeness.[2] In cyber threat intelligence work, as an example, a CMF could include external data sources such as

---

1 The CIS 20 Critical Controls are widely-used and provide effective guidance for security programs. Building off these controls allows defenders to actively seek out and disrupt attackers in their networks. https://www.cisecurity.org/controls/

2 For example, the NSA and CIA offer different approaches and focuses of collection management, stemming from cultural differences and, largely, the difference in data sources. Evaluating collection from signals and communications is inherently different than evaluating data collected from human sources. Even if the data source is the same, different styles can exist. For example, the U.S. Army's Field Manual 2-22.3 on human intelligence collector operations offers a slightly different but still structured view of collection management: https://fas.org/irp/doddir/army/fm2-22-3.pdf. Further, the U.S. Army also prepared Field Manual 34-2 on Collection Management: https://fas.org/irp/doddir/army/fm34-2/Ch3.htm

malware repositories, domain registrar databases, and malware indicator feeds to identify where analysts can go and what they can collect to satisfy the requirements or questions they have.[3] An important concept in collection management is developing an effective framework to meet the requirements of analysts as it relates to collecting data and producing information from it—not necessarily subscribing to others' exact models.

Defenders should prepare a CMF focused on internal data sources. This will enable defenders to effectively identify and structure their data sources to prepare for and respond to cyber threats. For this purpose, an internally-focused CMF should contain information about the defenders' assets, so they can evaluate preparedness for various threat scenarios, while also facilitating a more effective investigation post adversary activity. Each organization can create its CMF differently, but the core questions driving a collection management framework are:

- What data is collected and from where?
- How long is the data stored?
- What types of questions can the data answer as it relates to detection and response?

This paper will present one approach to creating a CMF with examples in industrial networks.

Leveraging Existing Missions

A CMF standardizes and strengthens how defenders detect and respond to intrusions across assets and their data; however, every organization will have pursued similar inventories and management systems that can be leveraged by defenders and fed into the collection management framework structure. For instance, many organizations will have a business continuity criticality rating identifying critical business processes and the systems and applications that support those critical business processes. Defenders' understanding of which assets are the highest severity can inform and allow them to better recognize what security controls surround these systems and make required adjustments.

There are many ways to measure and understand an environment. The mission of understanding visibility, detectability, and ability to respond to an incident is the core value of a CMF. Existing data sets that can directly feed into the framework include: asset inventory systems, vulnerability management systems, change control systems, ticketing systems, work management systems, capital project steering committees, risk committees, mergers and acquisitions, regulatory reporting, and network topographies.

Phases of Collection Management Framework

The challenge for defenders today, particularly those defending industrial environments, is understanding the visibility and blind spots that exist from both a detectability and response perspective. The CMF offers a repeatable process to understand environment visibility. Once this visibility is understood, gap analysis can then be factored into the risk management process for

3 In the SANS Institute class FOR578 – Cyber Threat Intelligence co-authors Robert M. Lee and Rebekah Brown have introduced various views of CMFs for intelligence work. Rebekah's work highlights how an analyst can utilize tools such as VirusTotal and public databases to enrich an understanding of adversary activity found in the network. In each construct of a CMF the focus is on a structured approach to answering questions. The class and its materials can be found at: www.sans.org/for578

improvements. The following phases follow a Deming cycle approach and largely reapply the U.S. Army's FM34-2 collection cycle to the topic of cyber security.[4,5]

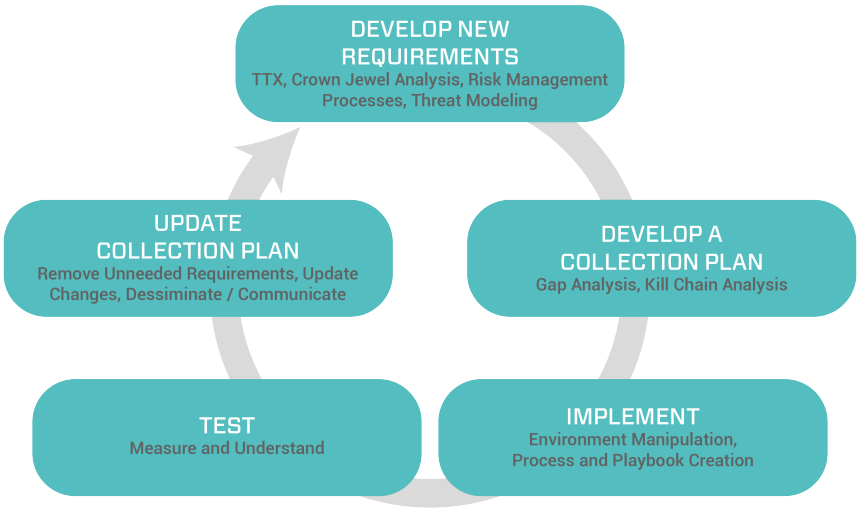

Figure 1: CMF Development and Improvement Model

Develop Requirements

An organization's defenders are often challenged with getting requirements. "Defend the organization" must be broken down beyond service-level agreements and into understanding the business risks. Once these business risks are understood, a set of requirements can be formed.

Forming Initial Requirements

Gaining an understanding of what matters to the business can be challenging. Interviews with business owners or business continuity owners, performing table top exercises, and using existing documentation such as risk registrars can serve as sources and methods to obtain enough data and to begin building an initial set of requirements. Initial requirements are often formed to protect mission-critical systems and business units; they are also key to understanding that different parts of the organization will have different mission requirements, and they will often not apply to one another. As an example, the mission requirements of the corporate network are vastly different from the industrial operations of a power generation station.

Method: Incident Response Table Top Exercise

Table top exercises (TTXs) are beneficial for testing all aspects of incident handling and response processes. During a TTX, a risk-based scenario is generally described and response is played out with all involved parties participating. An organization's CMF plays a crucial role in each TTX by allowing the IR team to quickly identify data available for triage, as well as where that data is located.

It is generally preferred for all actions to be completed during a TTX. Rather than simply saying analysts will pull and review memory, have the team extract a memory image from a sample server and review the image as if in an active investigation. If this is not possible, due to time or other

4 https://deming.org/explore/p-d-s-a
5 https://fas.org/irp/doddir/army/fm34-2/Ch3.htm

constraints, the CMF can be referenced to provide context and better estimate time involved for the action to complete by stating what resources are available. As the IR team discusses which artifacts would be valuable to the investigation, the CMF can ascertain where this data may reside and identify other potential gaps in visibility.

For example, if the mock adversary is believed to have touched multiple HMIs from the business network, the CMF may identify that the firewall logs are being aggregated to a centralized Syslog server, but gathering event logs for host analysis requires touching each HMI. This will increase the resources required to triage each device. A follow-on action would be to identify whether these host logs could be aggregated through a host agent. The CMF can be a reference to any already deployed solution (NXLog, Snare, or other COTS) elsewhere in the environment. The CMF should be updated following every TTX to ensure it is complete and correct.

Method: Crown Jewel Analysis

Crown Jewel Analysis is a methodological approach to understanding what assets can have the most consequence to the business. In the realm of ICS, this crosses into physical processes, such as the safety of rotating or pressurized equipment (including turbines or boilers). Crown Jewel Analysis allows an organization to prioritize the assets or environments that can directly or indirectly lead to severe consequences.

Once these "Crown Jewels" are identified, many organizations apply protective controls and architectures around them; this is needed, but insufficient. Understanding and increasing visibility and detectability around these assets is required for the defense team to properly protect them and put them in a continuous defensive posture. From this perspective, Crown Jewel Analysis not only prioritizes the most critical assets, but also understands likely (easiest) "kill chains" that could lead to a particular outcome.

Method: Threat Model

A threat model is a representation of what threats, or what threat tradecraft, could reasonably impact an organization.[6] Many approaches to threat modeling exist, but one valuable method is to extend the Crown Jewel Analysis approach to add in active threats to your industry or tangential industries.[7] Determining what threats have already caused impact to your industry is key to determining how they achieved their success. Organizations should not just protect against the known threat, but also the methods of success, which could be used by currently unknown threats. Focusing on the threat behaviors, or tradecraft, allows the organization to prepare for similar incidents, regardless of the aggressor.

Known threat tradecraft should be layered against the Crown Jewel Analysis to determine requirements for collection. As an example, consider a threat that caused impact by compromising a virtual private network (VPN) in a control center of an electric distribution provider where the adversary then leveraged the distribution management system to disrupt power to distribution

6 Many approaches to threat models exist including Adam Shostack's excellent work framing threat modeling as a proactive approach to determine what is important, what could go wrong, and what should be done about it. The approach taken in this paper is more aligned with threat intelligence in understanding what styles of attacks have been seen before and how to prepare for those in the future.

7 Some industries have very similar threat landscapes. If not much is known about pharmaceutical-based threats, as an example it can be useful to investigate larger manufacturing threats. Once the scenarios are exhausted, the organization could look at similar styles of attacks regardless of industry that could reasonably work in the organization.

substations. Knowing this type of threat has previously occurred in electric power would help defenders identify the need to prepare for similar activities and ensure they have the required people, processes, and technology to counter the attack across its various steps. In this case, requirements may form to collect VPN logs, achieve network security monitoring in the operations technology (OT) networks where the distribution management system is located, and have logging at the substations.

Outputs

The primary output of this phase is a list of prioritized requirements. These prioritized requirements are essentially a subset of specific questions the overall organization may have that influence the defenders' security posture.

Example requirements include:

- What cyberattacks or activity groups can cause an impact to refinery A?
    - How would they cause an impact?
    - Would the organization be successful in detecting and responding to the attack?
- What is the exposure to MS17-010 across our fleet of manufacturing sites?
- Our city is hosting a nationally significant event (Super Bowl, presidential visit, political party convention, etc.). Is there a change to our threat landscape during this time?

These requirements are fed into the collection plan where the team decides what information is available to answer these questions on an operational basis.

Generating New Requirements

Requirements will and should change over time. Creating both ad hoc and scheduled mechanisms and feedback mechanisms to generate new requirements can help the defenders stay current--not only against evolving threats, but also against changing business requirements.

Creating explicit "triggers" that generate new or influence current requirements help maintain a dynamic and up-to-date CMF. Triggers for ad hoc requirements gathering may include new public or private reporting, such as a new threat targeting a particular industry, an exploit in the wild, or a changing business landscape (such as new partners, customers, mergers and acquisitions, or new investments). Below are two examples of creating triggers around both incident response and hunting.

Trigger: Incident Response

Resources required for incident response are proportional to the resources required to gather and analyze information. Centralized log management streamlines the investigation process by having artifacts readily available and avoids delays from accessing devices directly. Referencing the CMF during an investigation allows analysts to identify what information is centrally located and what information is also accessible directly from the host.

Does that device store local logs? How long are these logs available? Knowing the answers to these questions will save valuable time and prevent analysts from chasing volatile information that may no longer be present. If the activity of these devices is not available locally, is network traffic stored somewhere, and how is this information accessed?

Contractors or junior analysts may not be aware of additional logs or data available outside of centralized tools. (Do your SOC analysts know all forensic data available outside of the primary

SIEM?) A complete CMF will make these sources known to all analysts and expedite the retrieval process by defining not only what devices have useful data locally, but the type of data as well. Additionally, the CMF should allow the investigation lead to ensure analysis was complete and all available artifacts were leveraged.

Trigger: Threat Hunting

Threat hunting allows analysts the freedom to search across a network to identify adversaries not detected by existing security controls. To be successful, hunting should involve analysis of the entirety of all devices and traffic across the network. Several adversaries use HTTP and DNS for command and control (C2) of compromised hosts. This is because these protocols are almost always required for most networks' operation. Adversaries are additionally "living off the land," which means leveraging built-in tools and functionality within the host operating system wherever possible. Abusing allowed protocols and using standard software alleviates the need for additional tools or malware that may be detected by host agents or antivirus.

Detection of adversary activity becomes much more difficult when the tradecraft consists of standard protocols and programs common on the network. Identifying malicious activity among valid behavior requires increased visibility to provide context of what is normal or approved.

The art of threat hunting is learning what is expected for the network and creating detection capabilities to identify adversary misuse. Hunters can leverage CMFs to identify visibility gaps and focus efforts on activity not visible from existing security controls. Part of the return on investment for a hunting program is training and knowledge gained by the analysts, as it requires a thorough understanding of normal operations. Once the traffic or system behavior is understood, it can then be centralized and added to the CMF with thresholds and other behavioral analytics. Threat hunting and a CMF are complimentary; the CMF is used to identify new potential areas of investigation and hunting should lead to an improved, more complete CMF.

Develop a Collection Plan

Once a new list of prioritized requirements is received, the team must formulate an understanding of what data sources are available internally to the enterprise that can feed into the collection plan. The above example requirement "What is our exposure to MS17-010 across our fleet of manufacturing sites?" can be broken down into a variety of elements to be considered, including:

- Where are the sites(s) located?
- What is the pervasiveness of SMB across these sites?
- What is the pervasiveness of the MS17-010 patch across the Purdue Model stack?
- What security controls exist to enable visibility into SMB communications, network traffic in general, and our ability to instrument escalations of known behavior such as WannaCry?
- Are there follow-on collection opportunities if needed?
- Where is the data stored?
- How long is the data stored?

The data can be structured in any method that is useful to the analyst. This could take the form of hyperlinked pages on an internal knowledge management system, or something as simple as an Excel spreadsheet. The size of the system, how many analysts are using it, and analysts' personal preferences will all dictate the final template.

A simple example can be observed in Figure 2 in the form of an Excel spreadsheet filled out at an electric grid control center and its transmission level substation. Here, the question type is structured against the intrusion kill chain phases, noting that the analyst can answer the types of questions related to that phase of the kill chain, such as exploitation of the system.

	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

Figure 2: Sample CMF of a Hypothetical Electric Company

With only a few rows and columns filled out in the above CMF, we can make observations that would be useful for the defender. As an example, the oldest data source is 120 days in the form of Alarms on the Windows Human Machine Interface (HMI). That data type can only answer information about Actions on Objectives, such as how the adversary is utilizing the system. If a defender received notification of adversary activity, they would only be able to answer questions back as far as 120 days, and not reliably, unless the activity is specifically related to actions on the HMI. It is also apparent that the network monitoring appliance only stores alerts for 30 days; therefore, correlating the Windows HMI event logs with the network monitoring alerts can only be done for 30 days at a time. Additionally, we can determine that a defender would have a difficult time completing an investigation that dealt with an adversary compromising the control center and the transmission substation, because the data from the transmission substation is only stored locally, whereas the control center data is mostly in the Enterprise SIEM.

There are numerous ways to prepare a CMF, and likewise, there are various use cases that can be identified to include threat hunting, incident response, and security operations.

CMF Examples

Standard Baselines for Asset Locations

Categorizing each asset type and location each time they are needed in the CMF can be extremely time consuming for larger organizations. An effective strategy for reducing workload is to maintain standard baseline options that can create a grouping of all the appropriate information for the CMF.

As an example, there might be two common builds of an electric transmission substation the organization wants to maintain. The first could include Windows HMIs, remote terminal units (RTUs), and network monitoring appliances that each have centralized logging and are maintained for 30 days each. The second standard baseline might include only Windows HMIs and RTUs that have local logging for 7 days. Instead of the organization creating a column for each of its substations, which could include numerous sites, it could categorize assets into Transmission Substation A and Transmission Substation B profiles and keep a second record of what substations fall into either Group A or Group B; any outliers would need documented or grouped as well. An example of this is shown in Figure 3.

	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION B	TRANSMISSION SUBSTATION B
ASSET TYPE	Windows Human Machine Interface	Network Monitoring Appliance	Remote Terminal Units	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alerts	Syslog	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Installation, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Packet Capture	Controller Logic	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise Log Server	Enterprise Log Server	Enterprise Log Server	Local	Local
DATA STORAGE TIME	30 Days	30 Days	30 Days	30 Days	30 Days

Figure 3: CMF with Standard Baseline Asset Locations as Groups

Standard Baselines for Asset Types

One approach to CMF building is to build a standard profile for the type of assets to include their various follow-on collection opportunities. This is a similar approach to the standard baselines for asset locations and can be combined with it as well.

With this approach, defenders might find there is a wealth of information available on a Windows HMI. Follow-on collection could include volatile memory acquisition, network cached information, and various types of logs. Instead of writing that information out each time the Windows HMI is put into the CMF, defenders could assign it a group base; multiple groups could still be used for different base profiles of what type of logging is enabled. Additionally, the network monitoring appliance might be configured differently based on data types in the environment available. Network Monitoring Appliance Group A might consume the network traffic, process historian, and the RTU syslog into it, directly allowing its alerts to have a wider breadth of coverage. Networking Monitoring Appliance Group B might just consume network traffic. Building standard profiles into groups allows the easy understanding of what capabilities are available at each site. An example is shown in Figure 4.

	CONTROL CENTER	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION B
ASSET TYPE	Windows Historian Group B	Network Monitoring Appliance Group A	Remote Terminal Units	Windows Human Machine Interface Group A
DATA TYPE	Windows Event Logs	Alerts	Syslogs	Windows Event Logs
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Installation, Actions on Objectives	Exploitation, Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Group B	Group A	Controller Logic	Group A
DATA STORAGE LOCATION	Enterprise Log Server	Enterprise Log Server	Enterprise Log Server	Local
DATA STORAGE TIME	30 Days	30 Days	30 Days	30 Days

Figure 4: CMF with Standard Baseline Builds as Groups

MITRE ATT&CK Matrix-Focused Questions

MITRE's ATT&CK matrix is a commonly used framework for exploring adversary behaviors, including tactics and techniques.[8] Instead of using kill chain phases for the question type, the ATT&CK lifecycle can be used supplementally as an additional row. The choice will ultimately come down to the use-case of the CMF and whether the organization is already using ATT&CK, the intrusion kill chain, or both of them. ATT&CK is very useful in its ability to also help defenders align prevention, detection, and response capabilities to the tactics and techniques of threats. Leveraging ATT&CK with a CMF and a good threat model can lead to very successful threat hunting and incident response capabilities.

8 MITRE's ATT&CK is sometimes seen as a substitute for using the kill chain phases. However, the intrusion kill chain is more appropriately used for the description of adversary phases, usually for the purposes of tagging such data and performing intrusion analysis by identifying patterns. ATT&CK is much more focused on how the adversary achieved their objectives. It is perfectly fine to utilize both of them together for the unique strengths of each. More on ATT&CK may be found here: https://attack.mitre.org/wiki/Main_Page

Implement

So far, we have gained an understanding of our defensive requirements from the business in the form of prioritized questions, such as "What is our exposure to MS17-010 across our fleet of manufacturing sites?" Now a collection plan can be created to identify the data sources available to defenders across the enterprise that can help operationally answer these questions. During the implementation phase, the defenders focus on two deliverables: creating new procedures and identifying new data sources that can be leveraged internally.

Institutionalizing Data Sources

CMFs will quickly identify opportunities to improve existing data sources to be better institutionalized by defense. This can range from lengthening data retention of the data sources and centralizing logging, to tuning configurations to allow for more optimal logging. Streamlining existing data sources includes simplifying access across operations and giving autonomy to the defenders to prevent bottlenecks and reduce the level of effort. It also may include adding new capabilities for pivoting or follow-on collection. Documenting connected data sources allows an analyst to quickly pivot from one data set to another knowing that there may be relevancy to the search they are performing.

As an example, an endpoint protection system may generate an alert on a new piece of malware. Additionally, it records the digital hash of the malware. The CMF may show that endpoint protection alerts are available and note data that can be pivoted to, such as the hash, or otherwise link the datasets together. Additionally, follow-on collection could be documented for a system in which the data that is not yet collected to be collected if needed. As an example, a CMF may note that on a Windows system the event logs are being collected. Follow-on collection could be highlighted as the capability to capture volatile memory off of the system by the incident response team. Analysts who understand what data they have, what data is available to them on an as-needed basis, and what follow-on collection exists can better institutionalize their data sources.

In addition, the identification of new data sources can be a desired outcome. These data sources may range from existing data in the environment not previously accessible to the defenders, to gaps that simply do not currently exist in an environment. While the collection cycle does not stop to wait for implementation of new data sources (such as enabling NetFlow or changing Group Policy Settings within a Microsoft Active Directory to enable additional logging), it can be the impetus for such changes and new data sources in the future.

Procedures: Security Operations

Refinement of procedures on how these data sources are used is also important for operations. Security operation centers (SOCs) are responsible for correlating data from multiple sources and platforms, while adding enrichment from external sources. Organizing data sources, location, and value is a valid use of a CMF. SOCs are often tasked with quick triage of multiple events. Ensuring consistent data gathering and analysis for each investigation is imperative.

Duplicative data can convolute analytic efforts by creating noise and increasing the amount of data for analysts to review. Every SOC is tasked with automating as much of their daily processes as possible, while maintaining a dependable output. CMFs can facilitate this by recognizing an authorized source for each specific data type, as well as facilitating automation of common tasks by

identifying the location and format of the data. This streamlines the triage process by either aggregating data of value or automating the retrieval of logs.

As an example, while signature-based detection is limited in successfully detecting adversaries, trending in antivirus alerts can indicate a larger issue on the network. If a single heuristic alert fires, there may not be cause for much concern. If multiple heuristic alerts fire throughout a subnet, an IR effort may be justified. Having this aggregative reporting is useful for correlation. With a complete CMF, analysts can identify where other alerts may be firing but not reported to the SOC. Additionally, it is useful to provide context to otherwise benign notices.

Procedures: Indicator Sweeps

Retroactively searching for known indicators of compromise is a common task for any network security team. The accuracy of the results is based on the data queried. Analysts must understand what data they are querying and ensure that the indicator could return a true positive. As an example, scoping indicators for an industrial threat, while not collecting data from the industrial networks, should stand out as wasted time and effort.

Creating an asset inventory through multiple avenues (passive network monitoring, Group Policy, vulnerability scanning, network discovery, etc.), then comparing the CMF against these asset inventories allows analysts to identify coverage with each retroactive search. Without a CMF, the source data pool is unknown, and therefore, the results cannot be considered complete.

As an example, consider a threat report containing multiple hash values of known Windows malware associated with the alert. Searching through a host-agent security control will only return results from systems that have the agent deployed. If Group Policy was used to deploy the agent, it will only be installed on those systems correctly configured to adhere to Group Policy. There are multiple instances where devices performing critical functions cannot have additional software or agents installed. These devices commonly do not have additional security controls or adhere to any domain-management software. In this example, these devices are not included in the results from the IOC scan.

Procedures: Embedded Playbooks

Another approach to utilizing a CMF is to embed playbooks for analysts to use. As an example, if there are certain data types that are foreign to the analyst, it can be useful to document the procedures on collecting and analyzing that data set; this way senior analysts can capture their knowledge to make a checklist-styled approach available to junior analysts. Playbooks can also allow cross-learning between analysts of different strengths and can be applied to different components of the CMF, including common use-cases, suspected attacks, or interlinking with high confidence threat detections in the environment.

Test

Operationalizing new data sources and defining new procedures does not make them effective for an organization. Testing and understanding the implications of these changes is important not only to ensure they are effective, but also to prevent them from being a detriment and a step back from prior operations. Two big measures of success are in both quantification and qualification of coverage. Finally, while we have changed and improved our collection plan during implementation,

our new understanding of these changes in this phase may lead to prioritizing additional security controls.

Quantify Coverage

It is common for larger organizations to have multiple self-governing networks with shared resources and/or domain trust for network communications. In these instances, it is difficult to evaluate coverage of protections and detections across each subnet. This issue is compounded when there is a central SOC for the organization, but independent oversight and budget allocated for remote sites and networks.

For example, transmission substation A may operate in Texas and have full visibility of all asset communications through passive monitoring, while transmission substation B in New Mexico has no visibility outside of perimeter firewall logs. Both substations have domain trust with the enterprise network and each other for reporting, backups, and hot-site management. In this case, substation B has weaker detection capabilities and may be an unknown infection vector for A. Because of the lack of security controls and visibility available to analysts, substation B may remain compromised until the adversary pivots into substation A.

A complete CMF allows the organization to quantify the visibility of the entire network and determine where additional resources are required for protection, detection, and triaging events.

Qualify Coverage

Some devices offer substantial configuration options for logging and alerting. Enabling logging on a device with the default configuration may not provide the greatest return. Extending logging to store everything possible may limit retention, due to additional resources required. To get the greatest return on investment for each device's logging options, an analyst should review the entirety of a network's visibility to identify gaps.

For example, an SEL Real-Time Automation Controller (RTAC) has options available to refine logging based on the function of the device (data concentrator, PLC, HMI). Additionally, if a device is controlled through software that has been installed on top of the Windows Operating System and there is a local Endpoint Detection and Response (EDR) agent deployed to monitor kernel and user space, additional logging through the device software may not return additional value. An analyst can use the EDR logs to forensically triage the host and the device; however, the CMF should also take into consideration the agent configuration to ensure all important data is captured.

Prioritize Additional Security Controls

Organizational budgets in network security have grown substantially, due to a necessity to protect critical assets and information; however, unless a company knows *what* it is trying to protect, there is no way to calculate the return on investment for a new security control. The evaluation of new security controls should include a comparison against the existing CMF to determine new investigative capabilities and potential enhancements to existing processes.

Defense in depth means there are multiple safeguards to protect a network. If one is subverted by an adversary, there are more that stand in the way relating to protecting, detecting, and mitigating the adversarial actions. Establishing a CMF allows an organization to confirm defense in depth is in place by organizing protection and detection capabilities throughout the network(s) into a single pane.

Additionally, large organizations may have multiple networks managed by local teams. It is not uncommon for an organization to purchase multiple tools that perform the same function, due to a lack of awareness around what licenses the parent or sibling networks have already obtained.

Update Collection Plan

The challenge with collection requirements and collection plans is that they continually grow and do not get pruned down. A key factor for long-term success is to review requirements and collection sources that are no longer relevant. For instance, a company may acquire an existing refinery and determine its requirement is to deploy additional monitoring capabilities between the refinery and the rest of the enterprise network. This enhanced monitoring may be reduced after a set period of time. Going back and updating the collection plan to account for this is critical. This includes removing the collection requirement, as well as updating the method of collection. Procedures should exist to disseminate this information to all teams to communicate and challenge assumptions of the collection plan.

Conclusion

To ensure an industrial network is defensible, defenders must understand what assets are on the network, as well as what information those assets can offer during an incident. Data location, type, and retention are key to streamlining an investigation and ensuring triage of a potential incident is complete. Creating this knowledge base should be inwardly-focused and does not need to be done in adherence to a specific standard. More importantly, the data needs to be usable, extensible, and managed over time to ensure it is accurate.

The collection management framework is a process that documents, institutionalizes, and operationalizes data sources that are available to defenders. This allows them to understand their visibility and, critically, the lack of visibility in their environments. This visibility ultimately influences an organization's ability to proactively detect intrusions and respond to them.