Intelligence-Driven Incident Response. Cyber Threat Intelligence:

Knowing how to identify and understand the attacker as well as how to use that information to protect networks is the fundamental concept behind a more recent addition to the incident responder's toolkit: cyber threat intelligence. Threat intelligence is the analysis of adversaries — their capabilities, motivations, and goals; and cyber threat intelligence (CTI) is the analysis of how adversaries use the cyber domain to accomplish their goals.

Analysis of an intrusion, either successful or failed, can provide a variety of information that can be used to better understand the overall threat to an environment. The root cause of the intrusion and the initial access vector can be analyzed to inform an organization of weaknesses in network defenses or of policies that attackers may be abusing.

The way an attacker moves laterally through a network can be analyzed and used to create new ways to monitor for attacker activity in the network. There is essentially no part of an incident-response engagement that cannot be used to better understand the threats facing an organization.

Cyber-threat intelligence isn't a new concept, simply a new name for an old approach: applying a structured analytical process to understand an attack and the adversary behind it.

Intelligence-driven incident response allows us to learn from attackers; to identify their motivations, processes, and behaviors; to identify their activities even as they seek to outwit our defenses and detection methods. The more we know about attackers, the better we can detect and respond to their actions.

This is the basic premise of intelligence: taking in external information from a variety of sources and analyzing it against existing requirements in order to provide an assessment that will affect decision making.

Data is a piece of information, a fact, or a statistic. Data is something that describes something that is. In information security, an IP address or domain are data. Without any additional analysis to provide context, they are simply facts. When various data points are gathered and analyzed to provide insight around a particular requirement, it becomes intelligence.

The difference between data and true intelligence is analysis. Without analysis, most of the data generated by the security industry remains as data. That same data, however, once it has been properly analyzed in response to requirements, becomes intelligence, as it now contains the appropriate context needed to answer questions and support decision making.

One of the most referenced military concepts in security is OODA, an acronym for "observe, orient, decide, act."

- The **Observe** phase centers around the collection of information. If the individual is trying to catch a network attacker, the observation includes gathering logs, monitoring systems, and collecting any outside information that could help identify the attacker.

- The **Orient** phase puts the information collected during the Observe phase into context with already known information. In the example of a network attacker, orientation takes the telemetry

pulled from the logs and combines it with knowledge about the network, relevant attack groups, and previously identified artifacts such as specific IP addresses or process names.

- The **Decide** phase: at this point, information has been collected (observed) and contextualized (oriented); thus it's time to determine a course of action. In the case of dealing with a network attacker, it means deciding whether to wait and continue to observe the attacker's actions, whether to start an incident-response action, or whether to ignore the activity.

- The **Act** phase is relatively straightforward: the individual follows through with the chosen course of action. OODA is a generalization of the basic decision-making process that everyone goes through thousands of times a day. It explains the process a network defender or incident responder goes through when gathering information and figuring out how to use it.

The intelligence cycle is the formal process for generating and evaluating intelligence. The first step in the intelligence cycle is direction. Direction is the process of establishing the question that the intelligence is meant to answer.

The next step is collection of the data necessary to answer the question. This is a wide-ranging exercise that should focus on gathering as much data as possible from many sources. It's difficult to know exactly what data might eventually prove useful, so building a broad capability to collect a wide variety of information is important. The focus at this point is not understanding how the data relates but simply developing as much information as possible.

Data is not always immediately usable in its raw format or in the format in which it was collected. The processing neccesary to make data usable is often an overlooked task, but without it, generating intelligence would be nearly impossible.

Here are some of the most common ways to process data related to cyber threats:

- **Normalization**: Processing includes normalizing collected data into uniform formats for analysis.
- **Indexing**: Large volumes of data need to be made searchable.
- **Enrichment**: Providing additional metadata for a piece of information is important.
- **Filtering**: Not all data provides equal value, and analysts can be overwhelmed when presented with endless streams of irrelevant data. Algorithms can filter out information known to be useless
- **Prioritization**: The data that has been collected may need to be ranked so that analysts can allocate resources to the most important items.
- **Visualization**: Designing a visualization based on what analysts need can assist in reducing cognitive load.

Analysis, as much an art as it is a science, seeks to answer the questions that were identified in the Direction phase. In intelligence analysis, data that has been collected is characterized and considered against other available data, and an assessment is made as to its meanings and implications.

Analysis is not a perfect science and must often be conducted with incomplete information. It is important that analysts identify and clearly state any information gaps in their analysis. This allows for decision makers to be aware of potential blind spots in the analysis, and can also drive the collection process to identify new sources in order to reduce those gaps.

A report with an answer is useless until it's shared with the relevant stakeholders: those who can use this intelligence. In plenty of documented intelligence failures, analysis was spot-on but dissemination failed. Intelligence must be shared with relevant stakeholders in the form they find the most useful.

Often forgotten, the Feedback phase is key to continuing intelligence efforts. The Feedback phase asks whether the intelligence that was generated answers the direction successfully.

The quality of intelligence relies primarily on two things: collection sources and analysis.

Collection method: It is important to understand whether the information is collected primarily from incidents or investigations, or whether it is being collected from an automated collection system such as a honeypot or a network sensor.

Date of collection: The majority of cyber-threat data that is collected is perishable. The lifespan of that data varies from minutes to potentially months or even years, but there is always a period of time when this information is relevant. Understanding when data was collected can help defenders understand how it can be acted upon.

Context: The more context that is available, the easier it will be to analyze. Context can include additional details, such as specific activities related to the information and relationships between pieces of information.

Bias: All analysts have biases, and identifying and countering those biases so that they do not influence analysis is a key component of quality intelligence. Some biases that analysts should seek to avoid include confirmation bias, which seeks to identify information that will support a previously formulated conclusion, and anchoring bias, which leads analysts to focus too heavily on a single piece of information while disregarding other, potentially more valuable information.

Tactical intelligence is low-level, highly perishable information that supports security operations and incident response. This usually includes IOCs and observables as well as highly granular TTPs describing precisely how an adversary deploys a particular capability.

Operational intelligence is a step up from tactical. In CTI, this usually includes information on campaigns and higher-order TTPs. It may also include information on specific actor attribution as well as capabilities and intent.

Strategic intelligence. In CTI, we think of this as supporting C-level executives and boards of directors in making serious decisions about risk assessments, resource allocation, and organizational strategy.

Intelligence typically has different confidence levels associated with it. These confidence levels reflect the analysts' trust that the information is correct and accurate. It is important to identify confidence in two important areas: confidence in the source of the information, and confidence in an analyst's conclusions.

Intelligence-Driven Incident Response. Basics of Incident Response:

Incident response encompasses the entire process of identifying intrusions (whether against a single system or an entire network), developing the information necessary to fully understand them, and then developing and executing the plans to remove the intruders.

Preparation is the defender's chance to get ahead of the attacker by deploying new detection systems, creating and updating signatures, and understanding baseline system and network activity.

Preparation should focus on four key elements, two technical and two nontechnical:

- **Telemetry**: Specialized systems are required for incident responders to identify and investigate intrusions. These systems range from network to host and should provide the ability to investigate a wide variety of activities at multiple levels.

- **Hardening**: Ensuring that patches are deployed, configurations are locked down, and tools that limit attacks such as virtual private networks (VPNs) and firewalls are in place.

- **Process and documentation**: Along with processes (such as an incident-response plan, notification plan, and communications plan), having documentation for common questions such as network configurations, system configurations, and system owners will also speed up responses.

- **Practice**: The best incident-response teams are those that have been through incidents together, and the best way to do that is practice.

The Identification phase is the moment where the defender identifies the presence of an attacker impacting their environment. This can occur though a variety of methods: • An incoming phishing email • Noticing command-and-control traffic from a compromised host • Seeing the massive traffic spike when the attacker begins exfiltrating data

The identification phase typically leads to an investigation, identifying even more information about the attack and the attacker, before beginning to respond directly.

The first two phases of the cycle can be considered primarily passive and are focused on information gathering. The first phase of actual response, meaning that specific actions are being taken in response to a specific attack, is containment. Containment is the initial attempts to mitigate the actions of an attacker, stopping them in the short term while preparing a longer-term response.

Containment tends to be most effective against less-sophisticated adversaries that make limited changes to their approach, such as commodity malware threats. So what about sophisticated adversaries? In many cases, the Containment phase can tip them off. They may set up new tools, establish secondary backdoors, or even just start being destructive. For this reason, most of these incident responses may move straight into eradication.

Eradication consists of the longer-term mitigation efforts meant to keep an attacker out for good. These actions should be well thought out and may take a considerable amount of time and resources to deploy.

Containment and eradication often require drastic action. Recovery is the process of going back to a nonincident state. If an entire network is compromised, the Recovery phase involves undoing any actions taken by the attacker across the entire network, and can be a lengthy and involved process.

The Lessons Learned phase evaluates the team's performance through each step. The goal of the Lessons Learned phase is to discover how to make the next incident response go faster, smoother, or ideally never happen at all. Basically, this takes the incident report and answers some basic questions: 1. What

happened? 2. What did we do well? 3. What could we have done better? 4. What will we do differently next time?

The kill chain provides an ideal abstraction for the phases an attacker moves through when exploiting a target. Whereas the incident cycle is focused on the defender's actions, the kill chain focuses on the attacker's actions.

After deciding what and who to target, the attacker begins conducting reconnaissance. In the Reconnaissance phase (or simply recon), the attacker develops as much information as possible about the planned victim. Reconnaissance can fall into multiple categories based on the type of data sought (hard data versus soft data) and collection methods (passive versus active).

Hard data includes information about technical aspects of a network and the systems attached to it. Soft data includes information about the organization behind the network and its systems.

Attackers may use different methods of collecting information. We can categorize these methods as active or passive:

- Active methods require interacting directly with the target.
- Passive methods are based on collecting information without interacting directly with the target, often by gathering information from a third-party information service.

The goal for attackers is to find places where the intention and implementation don't match — a vulnerability. This vulnerability must then be exploited reliably and packed into a form that's ready to be delivered to a target (for example, a malicious document or exploit kit). The process of finding this vulnerability, crafting an exploit, and combining it with a payload is Weaponization.

The exploitability process is all about finding a method to trigger the vulnerability and turn that into actual control of program execution. Generally, the goal of an exploit includes delivering some sort of payload for the attacker to then use to further their goals (such as data exfiltration). The implant will allow the attacker to maintain access to the exploited system without having to continually exploit the device.

There are two primary types of implants. The first is a beaconing implant that calls out to a commandand-control server and will receive commands to be carried out on the target system. The second is an implant that does not beacon, but waits to receive a command and then begins to communicate with a command-and-control server.

Once the attacker has gathered enough information to craft an attack, the next kill chain stage is Delivery. Common delivery scenarios include but are not limited to the following:

- **Spear phishing**: The attacker sends a weaponized resource, either as an attachment or as a link, via direct communications (often email) to a specific target.

- **SQL injection**: The attacker sends a command to a web application that is passed to the database server and interpreted directly.

- **Strategic web compromise (watering hole)**: The attacker first compromises a secondary resource, usually a website, and places a browser exploit on it.

Exploitation is the point where the attackers gain control of code execution and begin executing their own code. From this point forward, the attacker has control of at least one process on the target's system. This foothold is the start of the attacker's move into the network.

Once attackers have code execution, their first move is typically to solidify their foothold. There are two types of persistence:

- **System persistence**: Most attackers begin by solidifying their hold on a small number of hosts by deploying a root kit or remote-access Trojan (RAT) style of implant.

- **Network persistence**: Gathering credentials that allow access to broadly utilized network resources. This often means VPNs, cloud services, or other internet-exposed systems such as web mail.

Once an attacker has established persistence they need a method to send commands. Communication can come in a variety of methods and using multiple types of channels.

In most cases, all of this is not the ultimate goal, but rather the setup. Attackers go through the process of setting up access in order to give themselves the capability to affect the target in a way they didn't have before. We call this new capability the actions on objective. The most common actions on target were categorized by the US Air Force as follows:

- Destroy: The attacker destroys a physical or virtual item. This could mean destroying data, overwriting or deleting files, or otherwise making a system unavailable until it is completely rebuilt.

- Deny: The attacker denies usage of a resource (such as a system or information) by the target, such as in the case of denial-of-service attacks that do not permit access to a site.

- Degrade: The attacker degrades the utility of the target's resources or capabilities. This most often refers to the target's ability to control and command resources.

- Disrupt: By interrupting the flow of information, an attacker can disrupt the target's ability to carry out normal operations.

- Deceive: The attacker seeks to cause the target to believe something that is not true.

Intelligence cycles shouldn't just lead to more intelligence: they should lead to meaningful operations. This means threat intelligence shouldn't just lead us to more threat intelligence but instead to aggressive incident-response actions.

Operations cycles shouldn't end after the objective is completed. The information gained during any operation should start feeding a new intelligence cycle. When an incident response is concluded, the information developed during it should be fed into the intelligence apparatus to start developing new intelligence, learn from previous incidents, and be better prepared for future intrusion attempts.

To facilitate this process, F3EAD uses a modified version of a combined intelligence and operations cycle: Find, Fix, Finish, Exploit, Analyze, Disseminate. As you'll see, this means going through the incident-

response cycle and feeding the results into the intelligence cycle, and then connecting those results back into a new incident-response cycle.

The Find phase includes the targeting phase of the operation, which is where you determine the threats that you will address. This can come from many sources, such as intelligence from a vendor or open source. This parallels the Preparation phase of the incident-response cycle.

Based on the information from the Find phase, the Fix phase establishes telemetry and determines where an adversary is on the network as well any external presence we can detect. This involves taking available information and figuring out which systems, services, or resources an adversary may have compromised, what their channels of communications are, and how they're moving around your network.

The Finish phase includes the actual incident-response action. This is when you take decisive action against the adversary, carrying out the containment, mitigation, and eradication phases of the incident-response cycle. The end of the Finish phase starts the beginning of the Exploit phase. The intelligence half of the F3EAD process then begins.

The Exploitation phase maps directly to the Collection phase of the intelligence cycle. The goal is to gather as much information as possible that might be useful.

During the Analyze phase, the overall goal is to develop a complete picture of the actor and his tactics, techniques, and procedures, with a focus on how to detect, mitigate, and remediate his actions.

Disseminate: Regardless of the level of intelligence or the audience you are addressing, you will want the information you disseminate to be clear, concise, accurate, and actionable.

Intelligence-Driven Incident Response. Fix:

Intelligence supports incident response in a few key ways: • Providing better starting points by creating improved alerting criteria • Contextualizing information identified in the response process • Understanding attackers, methodologies, and tactics

In the Fix phase of F3EAD, all the intelligence you gathered in the Find phase is put to work tracking down signs of adversary activity on your networks.

The two primary ways to detect intrusions are through network alerting, which looks for signs of attacker intranetwork and extra-network communications, and system alerting, which looks for indications of attacker presence on the endpoint.

The activities we can identify by using network traffic include the following: • Reconnaissance • Delivery • Command and control, and lateral movement • Actions on target

The first concrete place to focus alerting on is the Delivery phase. In most cases, delivery means an email (for phishing), a website (for a watering hole attack), or web service compromise (accessing a web application, database, or other service).

- Attachments: The most common form of delivery in the last few years has been attachments, typically documents for commonly installed software containing exploits.

- Links: In some cases, malicious links in emails will lead users to a web page that is serving malware and will exploit the browser.

Eventually, the attacker needs to communicate with their systems. A lot happens between delivery and command and control, but those are all things most easily detected on the system level. Command and control (C2) refers to the attacker interacting with their malware to execute actions, which by necessity results in network communication.

You can look for a few common characteristics in C2 communication:

- Destination: The first and simplest of approaches. Hundreds of threat-intelligence products are dedicated to listing known bad locations, in terms of IPv4 addresses and domains. Many tools will let you blacklist and alert on known bad destinations.

- Content: many pieces of malware will misuse common protocols, such as sending encrypted HTTP traffic over port 80/TCP, which is usually not encrypted. These mismatches of content and protocol can be a big tip-off.

- Frequency: Most malware reaches from a host on an internal network out to a command-and-control server, which we call a beacon. These usually take place at regular intervals. It's often possible to identify patterns in the frequency of communication and search for that.

- Combinations: Often one characteristic isn't enough, but a combination of them may be. This takes time, recognition, and sometimes a bit of luck to develop a pattern and find a way to detect it.

System alerting can be similarly be divided into the following areas: • Exploitation • Installation • Actions over target.

Exploitation usually manifests itself in one of two key ways: • A new process begins running on a user's system, one that's created and controlled by the attacker. • A previous, user-controlled process is modified and co-opted to do something new and different.

Indicators of unexpected activity can indicate an intrusion. This includes modification of underlying binaries, applications running from unexpected or incorrect directories, or even brand-new processes with names meant to blend in at first glance.

After exploitation, the next step for most attackers is to make sure they can maintain access. In a single-system phishing-style compromise, this usually means installing a second stage that maintains persistence and adds capabilities the attackers can use to execute their objectives. These features are often bundled together into a modular tool, often called a remote-access Trojan (RAT), or a rootkit.

An attacker may need to access specific resources in order to carry out their objectives. In most cases, the actions over target follow the CRUD acronym:

- Create: Writing new files to disk from original material
- Read: Reading files currently on a system
- Update: Changing the content of files already on the system
- Delete: Removing files on a system, generally to keep them from being recovered later

Alerting on these actions is complicated because creating, reading, updating, and deleting files are common actions. Everything done on a computer does these. Much of it depends on understanding the actions an attacker may want to take.

Separating alerting and investigation workflows often requires walking a fine line because they often use the same tools, just in different ways. If alerting is about reduction (finding the smallest, most specific bit of data that will tip you off to malicious activity), then investigation is about gathering as much data as possible to get context and then reducing data again into a cogent analysis. This expansion (collection and processing) and then reduction (analysis and dissemination) workflow is common in both security analysis and intelligence analysis.

Traffic analysis involves identifying adversary activity based on metadata, the patterns of how the adversary communicates, rather than based on the content of the communication itself.

Analysts should look for the following activities:

- Connections to a known bad IP address can indicate command-and-control activity.
- Frequent, regular, short-duration, low-byte in/out connections can indicate malware beaconing, checking in for new instructions.
- A connection to a never-before-seen domain with a long duration and large bytes out/low bytes in could indicate data exfiltration.
- Port 445 connections from a known compromised host to other internal hosts could indicate data collection (445/TCP is Microsoft SMB file sharing).

While traffic analysis is purely focused on metadata around connections, signature-based analysis is monitoring for specific content. Intrusion detection systems (IDSs) combine network capture, a rules engine, and a logging method. The rules are applied to the network traffic, and when one matches, a log is generated.

Effectively applying intelligence to signature-based analysis requires not just creation of signatures, but also modification and removal. Having inaccurate or inactionable signatures slows incident response, forcing teams to waste time on fruitless investigations or analyses.

What signature analysis can do is key you into the patterns and content of past attacks, including bad sources and destinations, so when a signature triggers against a certain endpoint, that endpoint may be a good starting point for investigating.

Memory analysis focuses on collecting volatile system state in memory. Given that every process on a system requires memory to run, this technique provides an excellent vantage point to gather information, especially from tools that attempt to run stealthily with limited system footprint.

The power of an experienced forensic analyst is an understanding of exactly where to go looking, based on what's being hunted for. For instance, if you have a compromised machine, a forensic analyst should be able to look at common persistence mechanisms, identify any malware running, and then acquire any artifacts the malware dropped. Typically, the whole goal of disk analysis is to carve out useful artifacts to be analyzed by others.