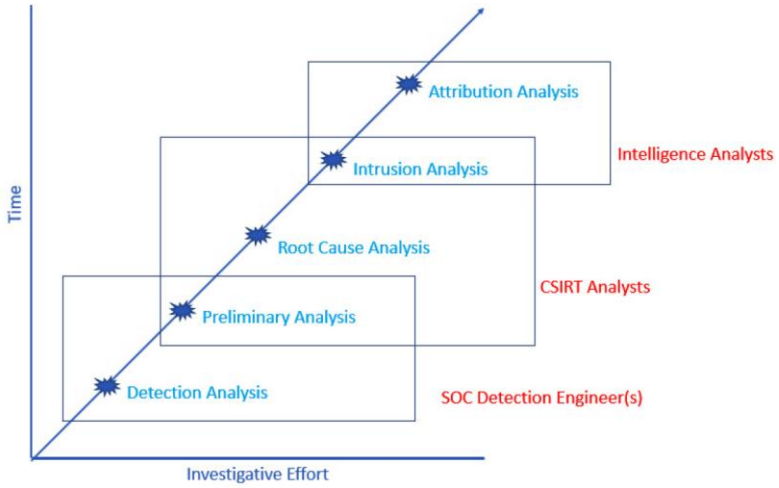
Digital Forensics and Incident Response: Investigation Methodology

An incident investigation is a methodology and process through which analysts form a hypothesis and test that hypothesis to answer questions regarding digital events. There are several different types of incident investigations conducted by various individuals within an organization. The figure below shows the five layers and the personnel involved, along with the corresponding time and the necessary investigative resources:



Detection analysis : This is the basic analysis that is often conducted at the first signs of a security event's detection. A quick check of the dashboard may indicate a localized event or potentially a wider incident. The detection analysis is often limited to telemetry and a secondary source, such as an external threat intelligence feed. The goal of this analysis is to determine whether the event is an incident that needs to be escalated to the CSIRT or not.

Preliminary analysis: The preliminary analysis utilizes tools that rapidly acquire selected evidence and analysis to determine the scope of an incident and provide information to the leadership, which can be used to contain an incident and gain time to decide on the next steps in investigation and response.

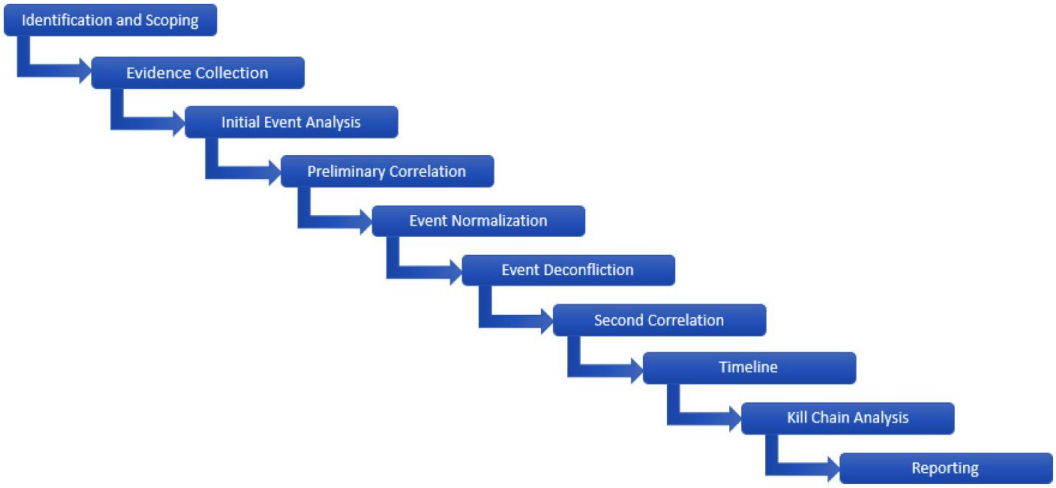
Root-cause analysis : This type of investigation is usually executed in conjunction with containment steps. The main goal here is to acquire and analyze evidence to determine how the adversary was able to gain access to the network, what steps they took and what they were, and what the potential impact on the organization was.

Intrusion analysis : Organizations can glean a good deal of insight into the TTPs of an adversary through a root-cause analysis. An intrusion analysis goes into greater detail to present a comprehensive picture of how an adversary operated during the network intrusion.

Attribution analysis: At the top end in terms of time and investigative effort is attribution. Attribution, simply put, ties an intrusion to a threat actor.

The evidence available will largely dictate how far analysis can go. Without a good deal of evidence sources across the network, the ability to conduct a full intrusion analysis will be limited, or even impossible.

The following methodology utilizes 10 distinct phases of an incident investigation to ensure that the data acquired is analyzed properly and that the conclusion supports or refutes the hypothesis created.



Identification and scoping. This is the first stage of an incident investigation, which begins once a detection is made and is declared an incident. The initial identification should be augmented with an initial examination of telemetry to identify any other systems that may be part of the incident. This sets the scope or the limits of the investigation.

Collecting evidence. Once an incident has been identified and scoped, the next stage is to begin gathering evidence. Evidence that is short-lived should be prioritized, working down the list of volatility.

The initial event analysis. After the evidence has been acquired, the next stage of the investigative process is to organize and begin to examine the individual events. This first stage is looking for obvious IOCs. An IOC can be defined as a data point that indicates that a system or systems is or was under adversarial control . IOCs can be divided into three main categories:

- **Atomic indicators** : These are data points that are indicators in and of themselves that cannot be further broken down into smaller parts, for example, an IP address.

- **Computational indicators** : These are data points that are processed through some computational means, for example, the SHA256 file hash of a suspected malware binary.

- **Behavioral indicators** are a combination of both atomic and computational indicators that form a profile of adversary activity.

The key at this stage of the investigation is to determine what looks suspicious and include it in the investigation. There will be plenty of opportunities to remove false positives. A good rule to follow is if you have any doubt about an IOC, include it until such a time that you can positively prove it is either malicious or benign.

The preliminary correlation. At this point in the investigation, the analysts should start to detect some patterns, or at least see relationships in the IOCs. Simply put, the preliminary correlation phase takes the individual events and correlates them into a chain of events .

Event normalization. Adversary actions on a system may have multiple sources of data. One challenge that has been an issue in the past with event normalization is the formulation of a global syntax of adversary behaviors. MITRE ATT&CK framework is a knowledge base that provides a standard syntax to describe adversary actions and normalize various pieces of evidence.

Event deconfliction. There are also times when there are multiple events related to an adversary's activity. A brute-force attempt that records 10,000 failures should be counted as a single event. Instead of listing all of them, the analyst can simply record the failures during a defined time. In this way, the overall intent and the adversary action are known without having to include all the raw data.

The second correlation. Now that the data has gone through an initial correlation and subsequent normalization and deconfliction processes, the analysts have a set of data that is then fed through a second correlation. This second correlation should produce a much more refined set of data points that can then be fed into the next phase.

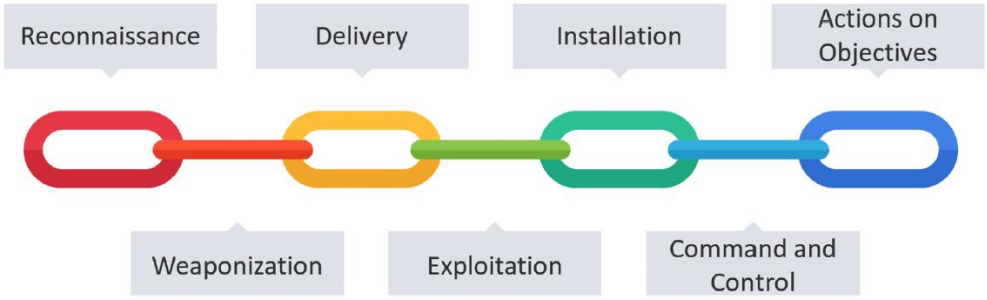
The timeline. The one output of an incident investigation is a timeline of events. Now that the analysts have the incident events normalized, deconflicted, and correlated, they should place the events in order.

Kill chain analysis. The next phase is to place the IOCs and other evidence into a construct that guides the analyst through an understanding of the relationship of the events to the overall intrusion, along with the interaction between the adversary and the victim organization.

Reporting. Incident reporting is often divided into three sections and each one of these addresses the concerns and questions of a specific audience. The first section is often the executive summary. The second section of the report is the technical details. In this section, the incident response analysts will cover the findings of the investigation, the timeline of the events, the IOC, and the TTPs of the adversary. The final section of the report is the recommendations. Detailed strategic and tactical recommendations assist the organization in prioritizing changes to the environment to strengthen its security.

The Cyber Kill Chain.

The timeline that was created as part of the incident investigation provides a view into the sequence of events that the adversary took. This view is useful but does not have the benefit of context for the events. One construct that provides context is placing the events into a kill chain that describes the sequence of events the adversary took to achieve their goal.



Reconnaissance can be broken into two major categories. The first is a technical focus where the threat actor will leverage software tools to footprint the target's infrastructure, including IP address spaces, domains, and software visible to the internet. A second focus will often be the organization and

employees. One common way that threat actors will gain access to the internal network is through phishing attacks.

The next stage of the kill chain is the **Weaponization** phase. During this phase, the adversary configures their malware or another exploit.

The third phase of the kill chain is the **Delivery** of the exploit or malware into the defender's environment. Delivery methods vary from the tried-and-true phishing emails to drive-by downloads and even the use of physical devices such as USBs.

The fourth phase of the kill chain is **Exploitation** . At this stage, the adversary exploits a vulnerability in the software, the human, or a combination of both.

The next stage is to maintain some sort of persistence. This is where the next stage of the kill chain, **Installation**, comes into play. In the Installation phase, the adversary installs files on the system, makes changes to the registry to survive a reboot, or sets up more persistent mechanisms, such as a backdoor.

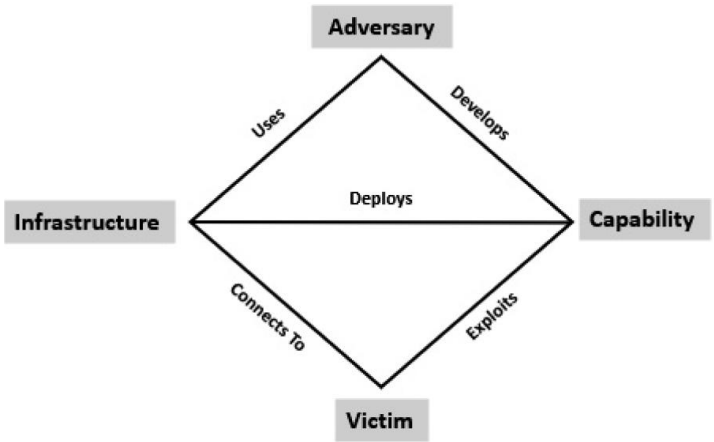
Once the adversary can establish their persistence, they need to be able to interact with the compromised systems. This is where phase six, **Command and Control**, comes into play. In this stage, the adversary establishes and maintains network connectivity with the compromised systems.

The final stage, **Actions on Objectives**, is where the adversary executes actions after they have effective control of the system. These actions can vary from sniffing network data for credit cards to the theft of intellectual property.

The Diamond Model.

The diamond model of intrusion analysis provides an approach that considers much more detail than the cyber kill chain's phases. What this model does is uncover the relationship between the adversary and the victim and attempt to determine the tools and techniques used to accomplish the adversary's goal.

The figure below visualizes the basic structure of the diamond model with the following four vertices: Adversary, Capability, Victim, and Infrastructure. In addition to the four vertices, there are also five relationships: Uses, Develops, Exploits, Connects To, and Deploys. Coupled together, these provide the foundation for describing the relationship of the four vertices.



The Four Vertices:

- The *Adversary* vertex describes any information or data concerning the perpetrators of the intrusion activity.

- *Capability* describes what tools and tradecraft the adversary can leverage.

- *Infrastructure* refers to a physical or logical mechanism that the adversary uses to deploy their tools or tradecraft.

- The *Victim* vertex can be broken down into either an individual or an organization.

The diamond model serves as a good construct to show the relationship between the adversary, their capabilities and infrastructure, and the victim. The diamond model's utility is derived from how it defines the relationship with each vertex. This provides a context to the overall event.

Diamond model axioms:

Axiom 1: For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result .

Axiom 2: There exists a set of adversaries (insiders, outsiders, individuals, groups, and organizations) that seek to compromise computer systems or networks to further their intent and satisfy their needs .

Axiom 3: Every system, and by extension every victim asset, has vulnerabilities and exposures .

Axiom 4: Every malicious activity contains two or more phases that must be successfully executed in succession to achieve the desired result .

Axiom 5: Every intrusion event requires one or more external resources to be satisfied prior to success. In an intrusion, the adversary has to configure a C2 infrastructure, aggregate their tools, register domains, and host malware delivery platforms. These are all data points that should be incorporated into any intrusion analysis to gain as complete a picture of the adversary as possible.

Axiom 6: A relationship always exists between the Adversary and their Victim(s) even if distant, fleeting, or indirect . A concept that is often used in the investigation of criminal activity is victimology or the study of the victim. Specifically, investigators look at the aspects of the victim, their personality, habits, and lifestyle to determine why they were selected for victimization. The same thought process can be applied to intrusion analysis.

Axiom 7: There exists a sub-set of the set of adversaries that have the motivation, resources, and capabilities to sustain malicious effects for a significant length of time against one or more victims while resisting mitigation efforts .

Integrating a diamond model into each phase of the kill chain provides a much more structured and comprehensive approach to intrusion analysis. What the diamond model / cyber kill chain methodology does is provide a construct to both guide the analysis and place the evidence items within an appropriate relationship to each other, so that a more comprehensive analysis of the adversary is conducted.