Indicators of compromise

In this reading, you'll be introduced to the concept of the Pyramid of Pain and you'll explore examples of the different types of indicators of compromise. Understanding and applying this concept helps organizations improve their defense and reduces the damage an incident can cause.

Indicators of compromise

Indicators of compromise (**IoCs**) are observable evidence that suggests signs of a potential security incident. IoCs chart specific pieces of evidence that are associated with an attack, like a file name associated with a type of malware. You can think of an IoC as evidence that points to something that's already happened, like noticing that a valuable has been stolen from inside of a car.

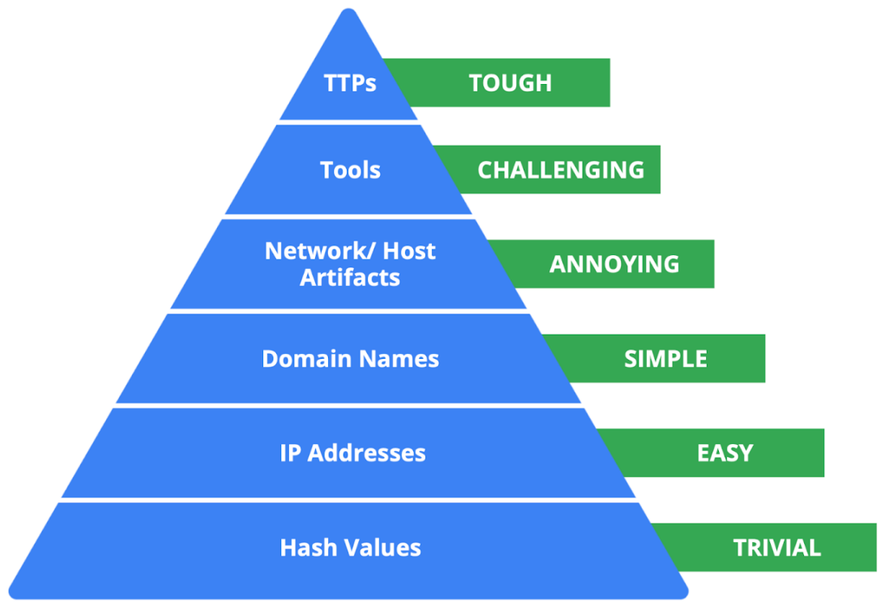
Indicators of attack (**IoA**) are the series of observed events that indicate a real-time incident. IoAs focus on identifying the behavioral evidence of an attacker, including their methods and intentions.

Essentially, IoCs help to identify the *who* and *what* of an attack after it's taken place, while IoAs focus on finding the *why* and *how* of an ongoing or unknown attack. For example, observing a process that makes a network connection is an example of an IoA. The filename of the process and the IP address that the process contacted are examples of the related IoCs.

Note: Indicators of compromise are not always a confirmation that a security incident has happened. IoCs may be the result of human error, system malfunctions, and other reasons not related to security.

Pyramid of Pain

Not all indicators of compromise are equal in the value they provide to security teams. It's important for security professionals to understand the different types of indicators of compromise so that they can quickly and effectively detect and respond to them. This is why security researcher David J. Bianco created the concept of the Pyramid of Pain, with the goal of improving how indicators of compromise are used in incident detection.



The Pyramid of Pain captures the relationship between indicators of compromise and the level of difficulty that malicious actors experience when indicators of compromise are blocked by security teams. It lists the different types of indicators of compromise that security professionals use to identify malicious activity.

Each type of indicator of compromise is separated into levels of difficulty. These levels represent the "pain" levels that an attacker faces when security teams block the activity associated with the indicator of compromise. For example, blocking an IP address associated with a malicious actor is labeled as easy because malicious actors can easily use different IP addresses to work around this and continue with their malicious efforts. If security teams are able to block the IoCs located at the top of the pyramid, the more difficult it becomes for attackers to continue their attacks. Here's a breakdown of the different types of indicators of compromise found in the Pyramid of Pain.

1. **Hash values**: Hashes that correspond to known malicious files. These are often used to provide unique references to specific samples of malware or to files involved in an intrusion.
2. **IP addresses**: An internet protocol address like 192.168.1.1
3. **Domain names**: A web address such as www.google.com
4. **Network artifacts**: Observable evidence created by malicious actors on a network. For example, information found in network protocols such as User-Agent strings.
5. **Host artifacts:** Observable evidence created by malicious actors on a host. A host is any device that's connected on a network. For example, the name of a file created by malware.
6. **Tools**: Software that's used by a malicious actor to achieve their goal. For example, attackers can use password cracking tools like John the Ripper to perform password attacks to gain access into an account.
7. **Tactics, techniques, and procedures (TTPs)**: This is the behavior of a malicious actor. Tactics refer to the high-level overview of the behavior. Techniques provide detailed descriptions of the behavior relating to the tactic. Procedures are highly detailed descriptions of the technique. TTPs are the hardest to detect.

Key takeaways

Indicators of compromise and indicators of attack are valuable sources of information for security professionals when it comes to detecting incidents. The Pyramid of Pain is a concept that can be used to understand the different types of indicators of compromise and the value they have in detecting and stopping malicious activity.

Mark as completed