**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.

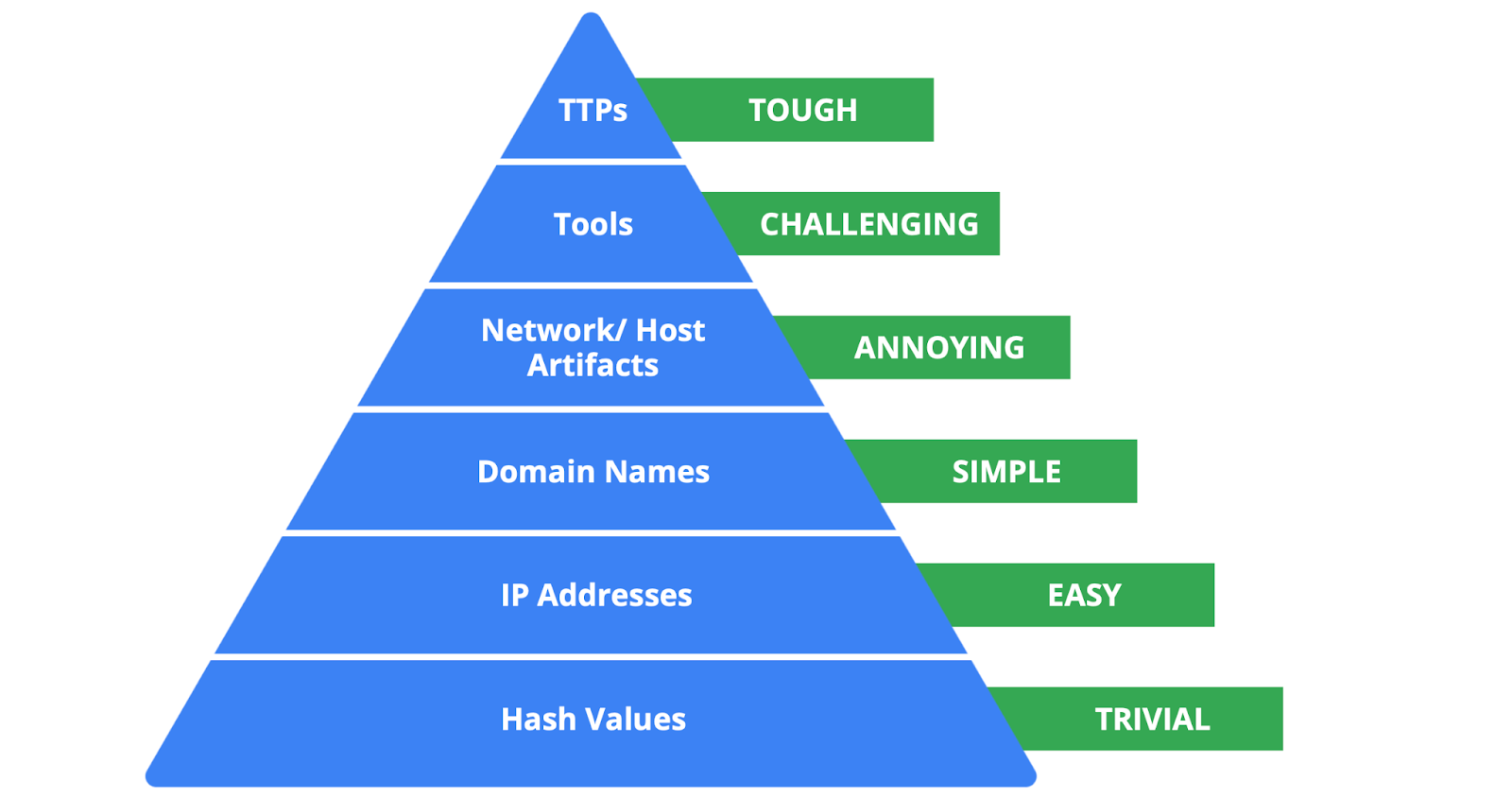
Essentially, IoCs help to identify the *who* and *what* of an attack after it's taken place, while IoAs focus on finding the *why* and *how* of an ongoing or unknown attack. For example, observing a process that makes a network connection is an example of an IoA. The filename of the process and the IP 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](http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html)

, 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.

**Analyze indicators of compromise with investigative tools**

So far, you've learned about the different types of detection methods that can be used to detect security incidents. This reading explores how investigative tools can be used during investigations to analyze suspicious **indicators of compromise (IoCs)** and build context around alerts. Remember, an IoC is observable evidence that suggests signs of a potential security incident.

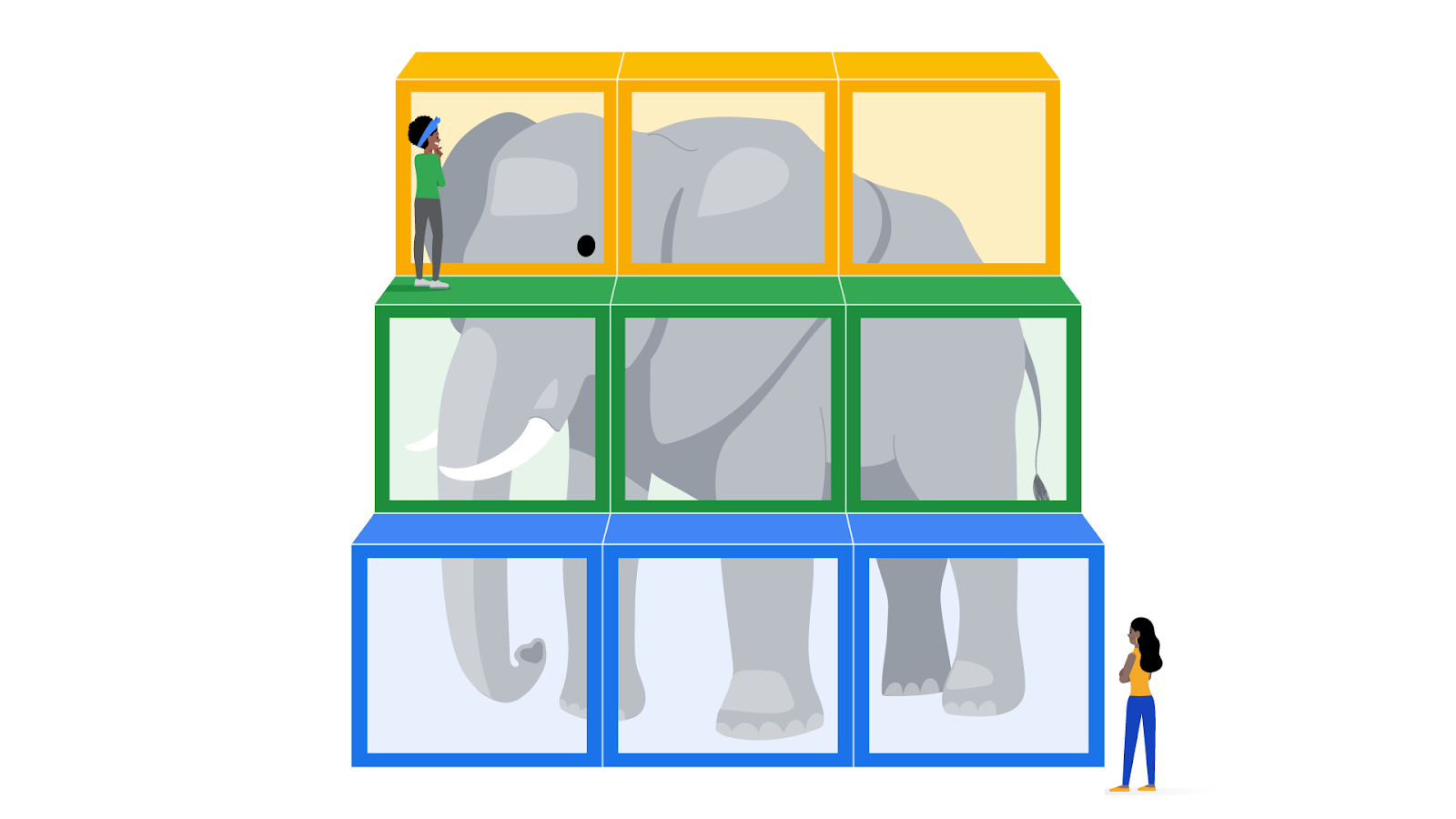
**Adding context to investigations**

You've learned about the Pyramid of Pain which describes the relationship between indicators of compromise and the level of difficulty that malicious actors experience when indicators of compromise are blocked by security teams. You also learned about different types of IoCs, but as you know, not all IoCs are equal. Malicious actors can manage to evade detection and continue compromising systems despite having their IoC-related activity blocked or limited.

For example, identifying and blocking a single IP address associated with malicious activity does not provide a broader insight on an attack, nor does it stop a malicious actor from continuing their activity. Focusing on a single piece of evidence is like fixating on a single section of a painting: You miss out on the bigger picture.



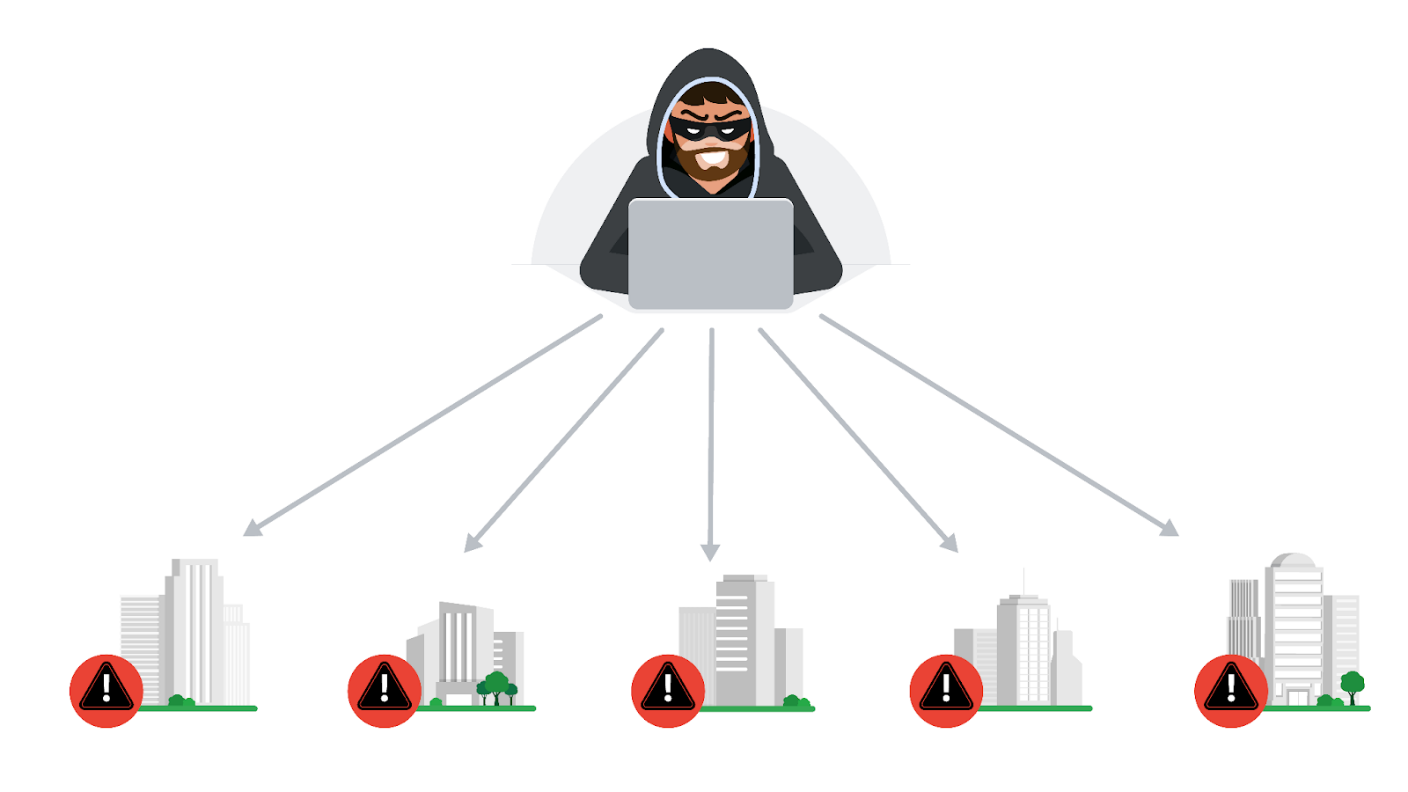
Security analysts need a way to expand the use of IoCs so that they can add context to alerts. **Threat intelligence** is evidence-based threat information that provides context about existing or emerging threats. By accessing additional information related to IoCs, security analysts can expand their viewpoint to observe the bigger picture and construct a narrative that helps inform their response actions.



By adding context to an IoC—for instance, identifying other artifacts related to the suspicious IP address, such as suspicious network communications or unusual processes—security teams can start to develop a detailed picture of a security incident. This context can help security teams detect security incidents faster and take a more informed approach in their response.

**The power of crowdsourcing**

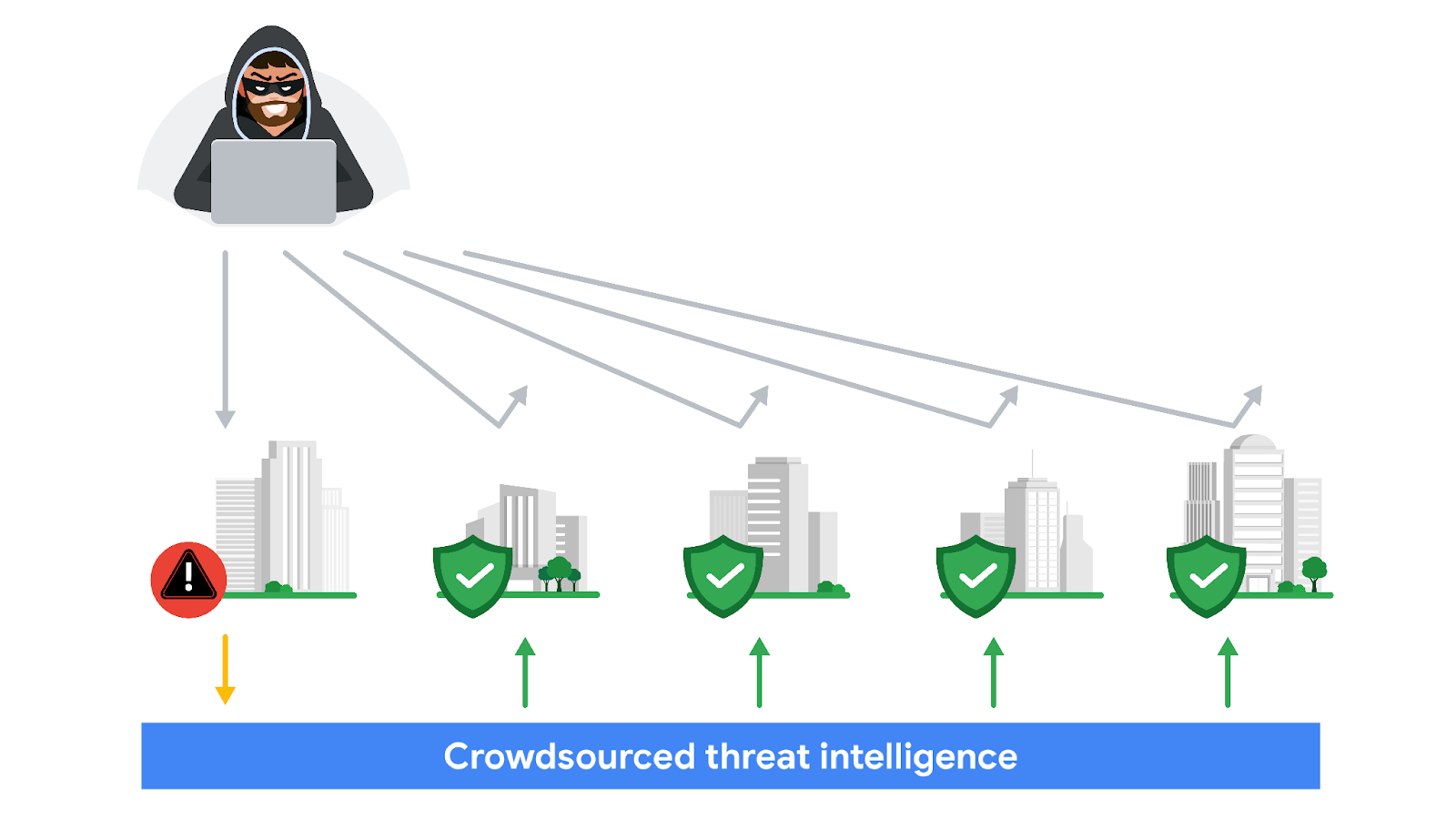
**Crowdsourcing** is the practice of gathering information using public input and collaboration. Threat intelligence platforms use crowdsourcing to collect information from the global cybersecurity community. Traditionally, an organization's response to incidents was performed in isolation. A security team would receive and analyze an alert, and then work to remediate it without additional insights on how to approach it. Without crowdsourcing, attackers can perform the same attacks against multiple organizations.



With crowdsourcing, organizations harness the knowledge of millions of other cybersecurity professionals, including cybersecurity product vendors, government agencies, cloud providers, and more. Crowdsourcing allows people and organizations from the global cybersecurity community to openly share and access a collection of threat intelligence data, which helps to continuously improve detection technologies and methodologies.

Examples of information-sharing organizations include Information Sharing and Analysis Centers (ISACs), which focus on collecting and sharing sector-specific threat intelligence to companies within specific industries like energy, healthcare, and others. **Open-source intelligence (OSINT)** is the collection and analysis of information from publicly available sources to generate usable intelligence. OSINT can also be used as a method to gather information related to threat actors, threats, vulnerabilities, and more.

This threat intelligence data is used to improve the detection methods and techniques of security products, like detection tools or anti-virus software. For example, attackers often perform the same attacks on multiple targets with the hope that one of them will be successful. Once an organization detects an attack, they can immediately publish the attack details, such as malicious files, IP addresses, or URLs, to tools like VirusTotal. This threat intelligence can then help other organizations defend against the same attack.

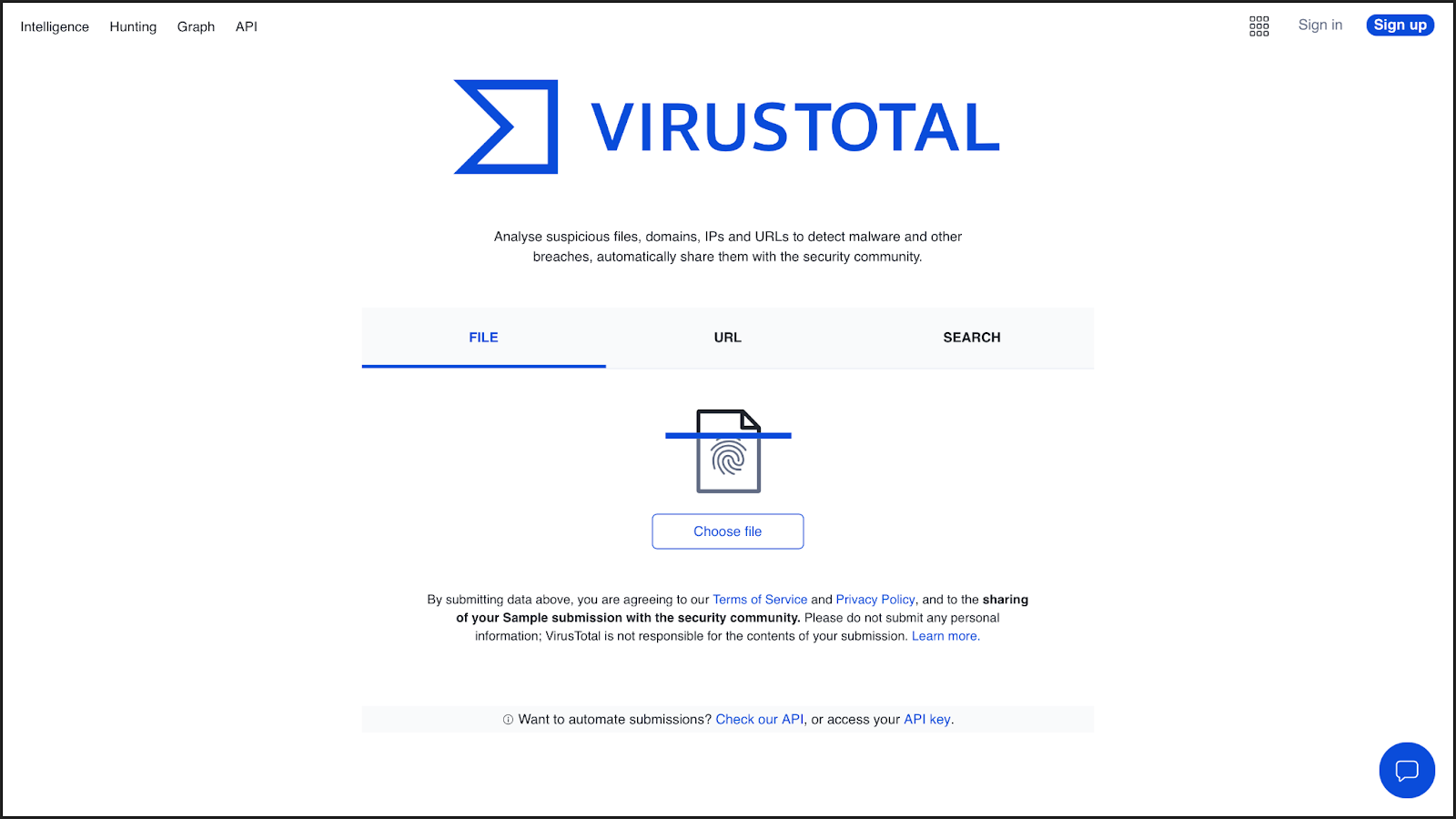


**VirusTotal**

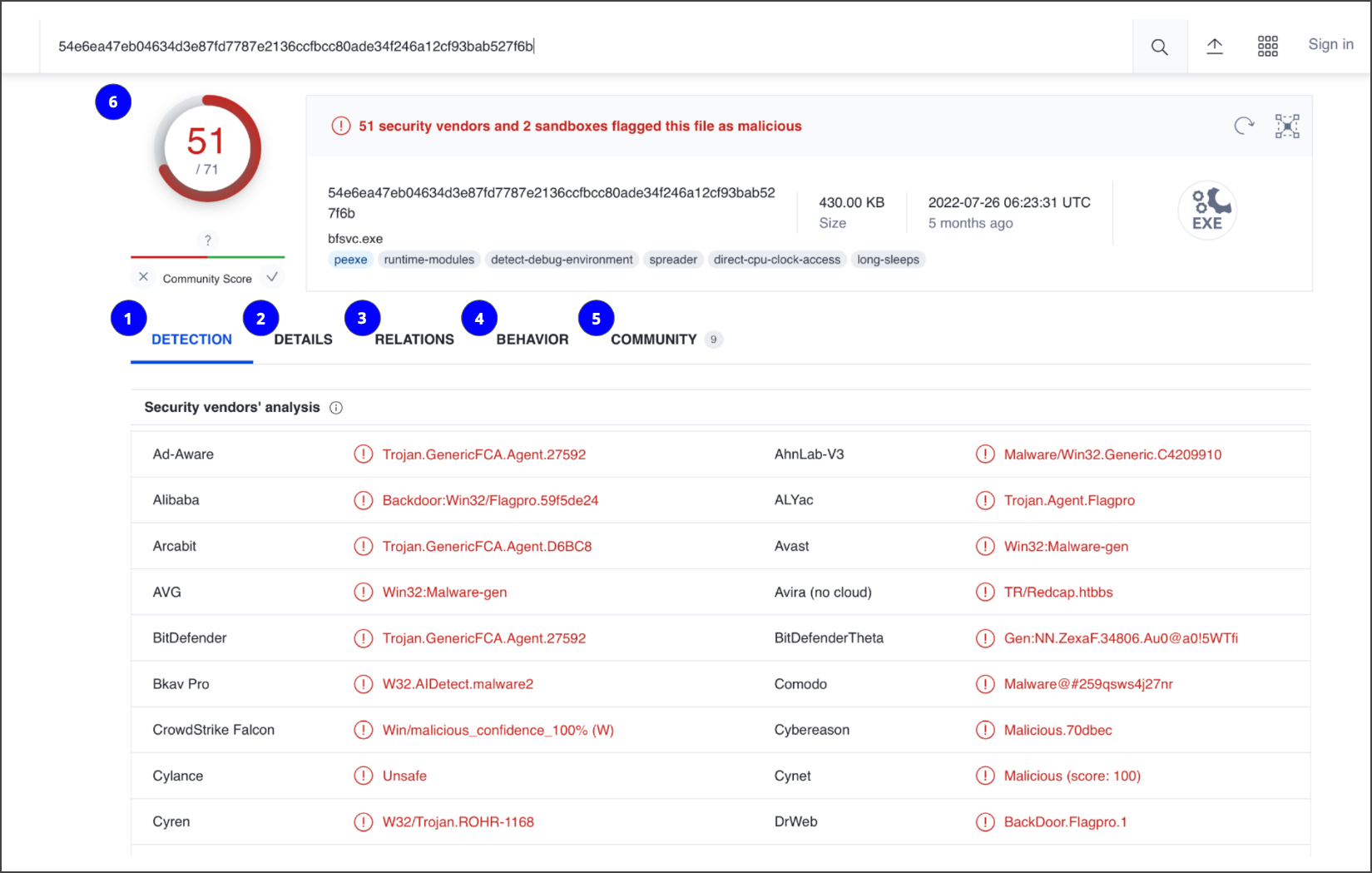
[**VirusTotal**](https://www.virustotal.com/gui/home)

is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. VirusTotal also offers additional services and tools for enterprise use. This reading focuses on the VirusTotal website, which is available for free and non-commercial use.

It can be used to analyze suspicious files, IP addresses, domains, and URLs to detect cybersecurity threats such as malware. Users can submit and check artifacts, like file hashes or IP addresses, to get VirusTotal reports, which provide additional information on whether an IoC is considered malicious or not, how that IoC is connected or related to other IoCs in the dataset, and more.



Here is a breakdown of the reports summary:



1. **Detection**: The Detection tab provides a list of third-party security vendors and their detection verdicts on an IoC. For example, vendors can list their detection verdict as malicious, suspicious, unsafe, and more.
2. **Details**: The Details tab provides additional information extracted from a static analysis of the IoC. Information such as different hashes, file types, file sizes, headers, creation time, and first and last submission information can all be found in this tab.
3. **Relations**: The Relations tab provides related IoCs that are somehow connected to an artifact, such as contacted URLs, domains, IP addresses, and dropped files if the artifact is an executable.
4. **Behavior**: The Behavior tab contains information related to the observed activity and behaviors of an artifact after executing it in a controlled or sandboxed environment. This information includes tactics and techniques detected, network communications, registry and file systems actions, processes, and more.
5. **Community:** The Community tab is where members of the VirusTotal community, such as security professionals or researchers, can leave comments and insights about the IoC.
6. **Vendors’ ratio and community score**: The score displayed at the top of the report is the vendors’ ratio. The vendors’ ratio shows how many security vendors have flagged the IoC as malicious overall. Below this score, there is also the community score, based on the inputs of the VirusTotal community. The more detections a file has and the higher its community score is, the more likely that the file is malicious.

**Note**: Data uploaded to VirusTotal will be publicly shared with the entire VirusTotal community. Be careful of what you submit, and make sure you do not upload personal information.

**Other tools**

There are other investigative tools that can be used to analyze IoCs. These tools can also share the data that's uploaded to them to the security community.

**Jotti malware scan**

[Jotti's malware scan](https://virusscan.jotti.org/)

is a free service that lets you scan suspicious files with several antivirus programs. There are some limitations to the number of files that you can submit.

**Urlscan.io**

[Urlscan.io](https://urlscan.io/)

is a free service that scans and analyzes URLs and provides a detailed report summarizing the URL information.

**MalwareBazaar**

[MalwareBazaar](https://bazaar.abuse.ch/browse/)

is a free repository for malware samples. Malware samples are a great source of threat intelligence that can be used for research purposes.

**Key takeaways**

As a security analyst, you'll analyze IoCs. It's important to understand how adding context to investigations can help improve detection capabilities and make informed and effective decisions.