VOTIRO

Securing Your Data

An In-Depth Look at Hidden Threats in Files

Data is the lifeblood of most organizations. Whether it's used to generate insights, drive decision-making, or fuel innovation. The security and protection of this valuable data is paramount to ensuring the continuity and success of businesses large and small. After all, safeguarding sensitive information from unauthorized access, theft, or tampering is crucial in maintaining the trust of customers, clients, and stakeholders.

The ever-present threat of cybercriminals and their constantly evolving tactics to steal this valuable data is making this harder by the day, especially with the sudden rise of generative AI. One of the top tools in their arsenal is malware and ransomware, which, according to Verizon research, are present in 40% and 30% of breaches, respectively. Cybercriminals have gotten so creative with their delivery of malware and ransomware that they have learned how to embed it within normal data, setting a trap for unknowing users.

In this guide, we investigate the growing use of hidden threats in files, dissecting the way attackers use them, and provide guidance on how they can be eliminated from your organization.

Securing Your Data

Hidden threats in files encompass malicious content or malware concealed within files that appear harmless at first glance, such as documents, images, or executables. These threats pose a significant risk as they can exploit vulnerabilities present in software or employ deceptive techniques to evade detection. Once accessed or executed, these files can compromise systems, infect them with malware, or even steal sensitive information without the user's knowledge. The hidden nature of these threats allows them to infiltrate systems undetected, making it crucial for individuals and organizations to adopt robust security measures and stay vigilant to protect against such risks.

Common Threats and Vulnerabilities

Hidden Excel Macros

Malicious code embedded within macros in Excel files that execute upon opening the document.

Drive-by Downloads

When visiting a website, malware is automatically downloaded and executed without the user's knowledge or consent.

Fileless Malware

Malware resides in memory rather than on the file system, making it difficult to detect and remove.

Document Exploits

Exploiting vulnerabilities in document formats like PDF or Word to inject and execute malicious code.

Trojan Horse Files

Files that appear harmless but contain hidden malware that is activated when the file is executed.

Script-based Attacks

Using scripting languages like JavaScript to embed malicious code in files or websites.

Zero-day Exploits

Exploiting vulnerabilities that are unknown to the software vendor, making it difficult for security measures to detect or prevent the attack.

Steganography

Hiding malicious code or files within seemingly innocent images or other media files.

Malicious File Attachments

Email attachments or downloads that contain malware disguised as harmless files, such as documents, images, or executables.

Watering Hole Attacks

Compromising a trusted website frequently visited by the target audience to distribute malware, often through exploit kits or compromised files.

How do threats reach endpoints?

Attackers employ various techniques to infiltrate systems with malicious code. One method involves sending email attachments or providing innocuous downloads, such as documents or images. However, these seemingly harmless files contain embedded malware, which can be activated once the file is opened or executed. Another approach leverages vulnerabilities present in file formats and applications. By exploiting these weaknesses, hackers can inject malicious code or scripts into files, enabling the malware to execute upon opening.

Additionally, hackers frequently utilize macros found in office documents, like Word or Excel files. By exploiting users' trust in these file types, they embed malicious code within macros, which is executed when the document is opened, leading to the activation of the malware. These techniques allow attackers to covertly introduce and execute malicious code, posing a significant threat to the security of systems and sensitive data.

Hidden threats in files can have far-reaching consequences for businesses, affecting not only the infected endpoints but the entire organization. One significant impact is data theft, which can result in compliance failures and compromise sensitive information. These threats can also grant unauthorized access to attackers through rootkits and remote tunneling, enabling them to infiltrate systems and gain control over critical resources.

System disruption, beyond that which is a result of data theft, is another consequence, as attackers may destroy essential files, rendering them unusable and causing operational disruptions. Ransomware is a prevalent threat that locks files and demands a ransom for their recovery, potentially leading to financial losses and reputational damage. This is often paired with an exfiltration step, where data is sent off-site to attackers while rendered locally useless.

Hidden threats may also have the capability for keylogging, enabling attackers to collect valuable data, including passwords, and transmit it back to malicious actors. Additionally, these threats can self-propagate, spreading to other visible endpoints on the network and multiplying the impact.

Hidden threats are not restricted to a single type of malicious action and often incorporate multiple ones simultaneously to maximize the impact.

How does malware spread?

Hidden threats in files have various means of spreading, extending beyond the commonly assumed email vector. While email remains a standard method, it merely scratches the surface of how these threats infiltrate organizations. Any place where data crosses a control boundary, there is an opportunity for cybercriminals to spread hidden threats.

Collaboration tools make it easy for users to collaborate and share information in real-time. However, the ease of sharing makes it a prime vector for spreading hidden threats. As many hidden dangers do not immediately display their malicious actions, users share files they believe are safe, further distributing the toxic code.

File portals are a necessity for many organizations, allowing vendors, customers, and other external parties to submit important files. These may include seemingly harmless documents like invoices from contractors, income evidence from loan applicants, or manifests from shipping companies. As they originate from uncontrolled sources, these files may contain hidden threats, which pass into mass storage, such as the cloud or data lakes, lying in wait for staff to open them and execute the dangerous content.

Even activity as commonplace as web browsing can be a source of hidden threats. The web is teeming with innocuous files such as PDFs posted on legitimate websites that harbor malicious content. In fact, 66% of malware is delivered via PDF. Cybercriminals specifically target these sites as their users are less likely to scrutinize the content they discover there.

How to stop threats

With so many varieties of threats and ways that they can make their way into an organization, there is no single step that can be taken to eliminate everything. Instead, organizations must consider a multi-faceted approach to defend their business from evolving cyber threats.

Level One
Detect

Level Two
Disarm

Level Three
Analyze

Level One

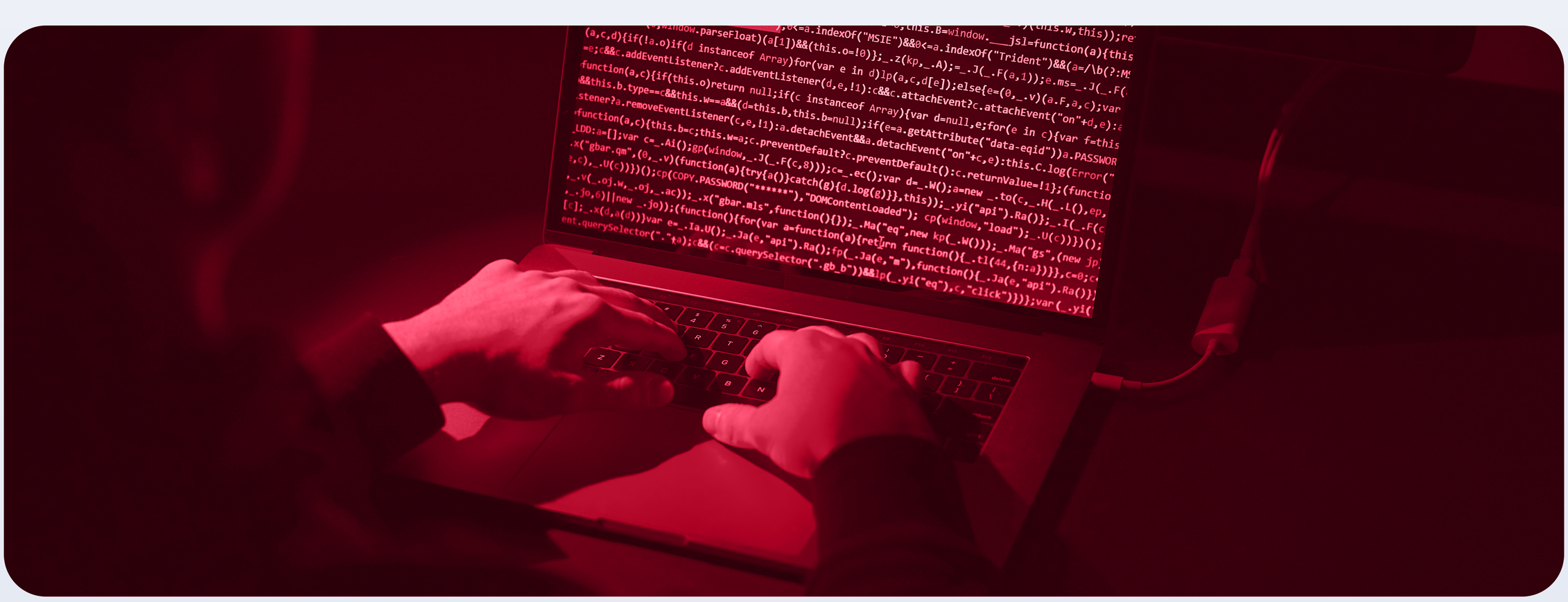
Detect

Detection plays a crucial role in the overall security framework, serving as the first line of defense against a wide range of threats that can infiltrate files and systems. Particularly, antivirus software plays a crucial role in detecting and identifying known malicious entities, such as viruses, worms, trojans, and other malware. By continuously scanning files and monitoring incoming data, antivirus programs help organizations stay informed about the potential threats attempting to breach their boundaries.

Rapid detection is essential as it allows for swift action, minimizing the potential damage caused by these threats. With the ability to recognize known threats, antivirus software enables organizations to promptly remove or quarantine infected files, preventing further spread and reducing the risk of data loss or system compromise.

Catching what is known

Antivirus programs play a critical role in catching known threats by leveraging both signature-based and behavior-based detection techniques. Signature-based detection relies on a database of known malware signatures to identify and block malicious files that have been encountered before. This method is effective in quickly recognizing and neutralizing well-established threats. On the other hand, behavior-based detection focuses on monitoring the actions and activities of files or processes to identify suspicious behaviors indicative of malicious intent. By analyzing the execution of files in real-time, behavior-based detection can detect and halt threats that may not have a known signature.



Level One

Detect

The benefits

Detection-based solutions offer several notable benefits that make them vital to comprehensive protection strategies. One key advantage is their speed and efficiency in identifying and mitigating malicious files. These solutions can swiftly recognize known threats and suspicious activities by leveraging signature-based and behavior-based detection methods, enabling prompt action. The ability to quickly eliminate malicious files helps prevent further damage to systems, data, and networks, minimizing potential disruptions and financial losses for organizations.

Moreover, detection-based solutions create a valuable documentation trail that records the actions taken in response to identified threats. This documentation is an audit trail and provides a valuable resource for incident response, forensic analysis, and compliance. Organizations can demonstrate their commitment to security and ensure accountability for their security measures by maintaining a clear record of the detected and eliminated threats.

Level Two

Disarm

In the ongoing battle against hidden threats, disarmament takes the protection of organizations to the next level. Unlike traditional approaches that involve deleting or quarantining identified threats, the disarming method focuses on extracting dangerous code from files while preserving their functionality. This process, commonly known as Content Disarm and Reconstruction (CDR), goes beyond identifying and neutralizing known threats. It meticulously analyzes files to identify and remove potentially malicious elements, rendering them safe for use without impacting their intended purpose.

The disarm approach offers a proactive and comprehensive solution by sanitizing files rather than discarding them. It eliminates existing threats and prevents new and emerging threats from infiltrating organizations' systems and networks. This method reduces the risk of zero-day attacks and other advanced threats that may exploit vulnerabilities in traditional detection methods.

Stopping the unknown

One of the inherent challenges with traditional detection-based tools lies in their limited ability to identify and stop new or novel threats. The landscape of threats is constantly evolving, with cybercriminals utilizing techniques such as permutation kits to create variations of known malware that can evade detection. This constant adaptation makes it increasingly tricky for detection-based tools to keep up and effectively identify emerging threats.

Furthermore, there is often a lag between when a new threat is detected and when it is analyzed and incorporated into detection algorithms. This time gap creates a window of opportunity for attackers to exploit vulnerabilities before security measures catch up. As a result, organizations need to adopt a proactive and adaptive approach that goes beyond relying solely on detection-based tools. Implementing complementary security measures such as behavioral analysis, sandboxing, and threat intelligence sharing can help bridge this gap, allowing organizations to proactively detect and respond to unknown threats and reduce the likelihood of successful attacks.

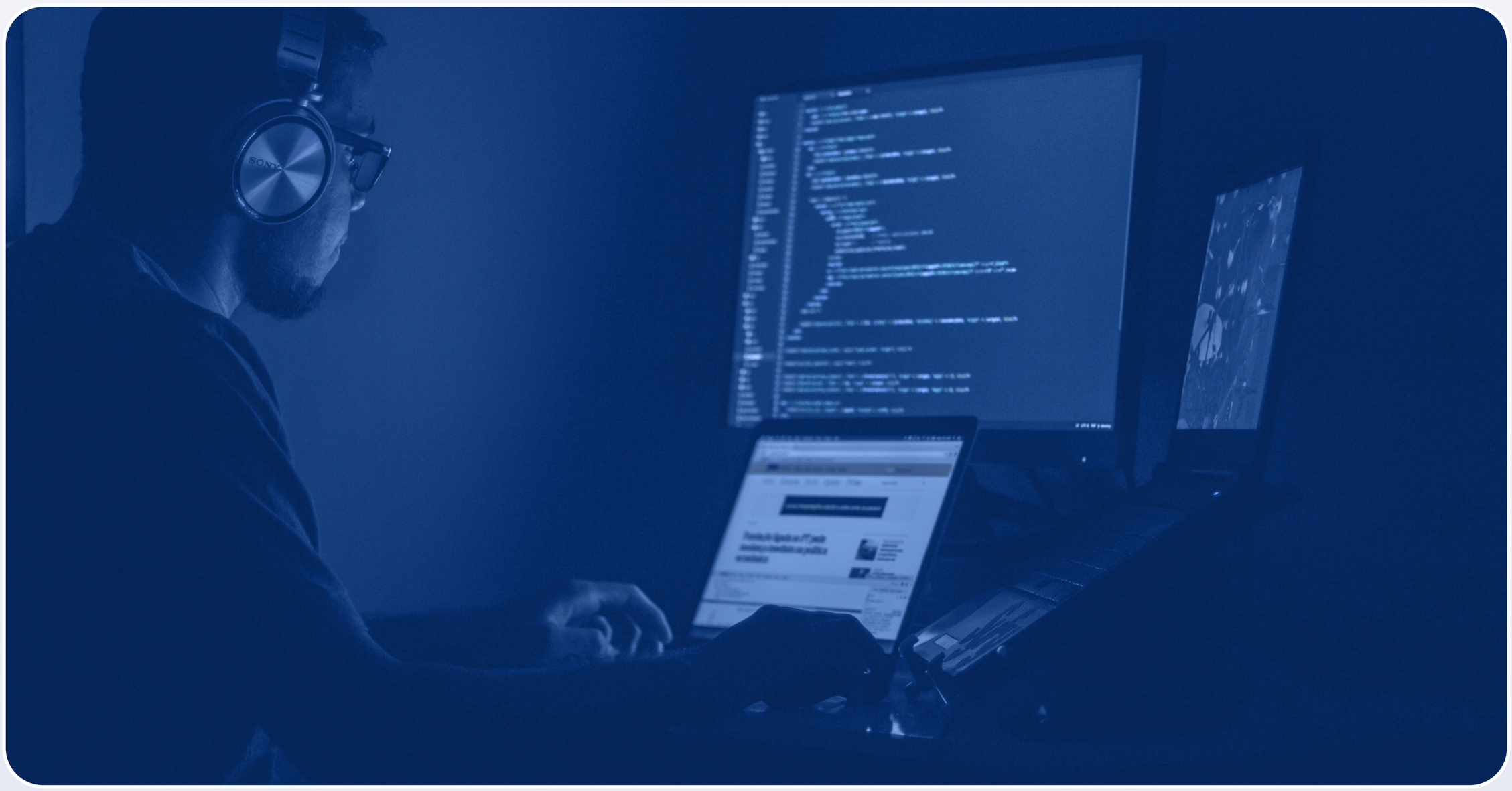
Level Two

Disarm

What are the benefits of CDR?

CDR is an advanced security technique designed to catch zero-day and previously unseen threats that may bypass traditional detection methods. CDR works by carefully analyzing files and stripping out potentially malicious code while retaining the file's original functionality. This approach is essential in industries such as finance, where macros and other file elements are commonly used. By preserving the functionality of files, organizations can ensure business continuity and prevent disruptions while eliminating potential threats. Additionally, CDR considers the importance of maintaining file formatting and layout, as valuable information can be conveyed through these elements.

It is worth noting that CDR solutions can vary in terms of quality and maturity, with more advanced systems offering higher accuracy and minimizing false positives. In a zero-trust approach, every file is automatically sanitized, regardless of source or perceived security level, ensuring a consistent and robust defense against threats. The implementation of CDR enhances the overall security posture by effectively neutralizing threats while preserving the usability and integrity of files, thus safeguarding organizations against emerging and unknown threats.



Level Three

Analyze

Analyzing files is a critical step in the security process, especially when using Disarm-based tools. While these tools excel at eliminating threats without the need for explicit detection, there is a trade-off when identifying and analyzing specific threats. By sanitizing everything that comes through, Disarm-based tools proactively eliminate potential new threats that may have evaded traditional detection methods. However, the drawback is that these tools don't always provide specific visibility into the nature of the threats being eliminated. This lack of analysis, especially when it comes to zero-days, can make it challenging to gain insights into the characteristics and behavior of emerging threats.

Data analysis is also crucial to the privacy and compliance regulations within certain organizations - especially those in finance and government sectors handling highly sensitive information and client data. Leveraging a robust threat analytics platform will help IT and SOCs get a better understanding of incoming data in order to stay compliant, mitigate future threats, and allow leadership to make the best decisions available when it comes to budgetary concerns and the makeup of their security architecture.

All in all, the advantage lies in the proactive nature of the process. To achieve a comprehensive security posture, organizations should combine Disarm-based tools with complementary detection mechanisms and analytics to obtain a more detailed understanding of threats and enhance their overall defense capabilities. With these pillars in place, organizations can better protect their systems, networks, and valuable assets from known and emerging threats.

Hindsight is 20-20

Hindsight analysis plays a crucial role in assessing the effectiveness of sanitization tools and understanding the threats that have targeted an organization. By retrospectively analyzing files and data that have undergone the sanitization process, organizations can gain valuable insights into the types of threats encountered. This information is essential for evaluating the security posture, identifying potential vulnerabilities, and informing future defense strategies.

However, it's important to note that hindsight analysis can be time-consuming, especially if organizations don't have tools in place to automate this process. As mentioned earlier, detection can take significant time, during which threats may already have been neutralized through the sanitization process.

Nonetheless, hindsight analysis provides highly accurate data, helping organizations understand the time gap between sanitization eliminating a threat and detection-based tools being able to identify it. This information helps organizations quantify the effectiveness of their security measures.

Level Three

Analyze

Showing value through analytics

The information from analytics helps to drive a collective defense against file-based threats. It is not only about knowing what was sanitized but detectable later, but also about determining the effectiveness of layers. Knowing the subsequently sanitized files highlights the threats that managed to slip through one layer but were caught and neutralized by subsequent defenses.

This holistic story gives organizations a deeper understanding of the evolving threat landscape they face - as well as the effectiveness of the security tools in their tech stack. The insights gained from this analysis can enhance overall threat detection and elimination strategies, including feeding the information back into security tools such as a Security Information and Event Management (SIEM) system. By incorporating accurate and filtered data from the analysis, false positives in SIEM detection can be reduced, improving efficiency and effectiveness in identifying and mitigating threats.

How Votiro prevents file-borne threats

Votiro takes an every-level approach by providing detection, disarmament, and data analysis. Surpassing the capabilities of traditional CDR, Votiro offers additional features such as optional antivirus integration and RetroScan. RetroScan enables auditable tracking of threats eliminated by Votiro, aligning with the detection capabilities of antivirus software as they become detectable. By leveraging Votiro's advanced CDR solution with Retroscan, organizations can achieve a demonstrable return on investment. This ensures their performance requirements are met while also protecting staff and customers from concealed threats. Votiro's comprehensive approach enhances security measures and gives companies the confidence to mitigate risks effectively.

Contact us today to learn how Votiro leads the way in proactive prevention of file-borne threats, known and unknown, while securing organizations and maintaining business productivity. And if you're ready to see Votiro in action, you can **start today with a free 30-day trial.**