SecureIQlab®

REPORT

2024 Content Disarm and Reconstruction (CDR) Validation Report – OPSWAT Deep CDR

Product Version: OPSWAT MetaDefender Core

Report Contents

1. Executive Summary

In today's dynamic digital environment, the exchange of digital files has become integral to organizational operations and collaborative endeavors. However, the rapid pace of digital transformation has also ushered in a surge of cyber threats, presenting substantial challenges to the security and integrity of digital assets. SecureIQlab's Content Disarm and Reconstruction (CDR) validation test underscores the pivotal role of CDR technology in fortifying cybersecurity defenses and safeguarding the integrity of digital assets shared among stakeholders. CDR technology effectively addresses file-borne cyber threats by meticulously deconstructing, disarming potential threats, and reconstructing productivity files to eradicate potential threats while preserving functionality.

SecureIQlab is an innovative independent security testing lab established in 2019. As a leading cloud validation provider, SecureIQLab remains dedicated to its core values and the cybersecurity industry's commitment to enhancing security for organizations. In a groundbreaking initiative, SecureIQLab has successfully conducted the testing for CDR solutions, evaluating the OPSWAT Deep CDR technology, which is a core module of the OPSWAT MetaDefender Core product. SecureIQlab CDR validation test aims to validate the efficacy of OPSWAT's leading CDR solution.

2. Introduction

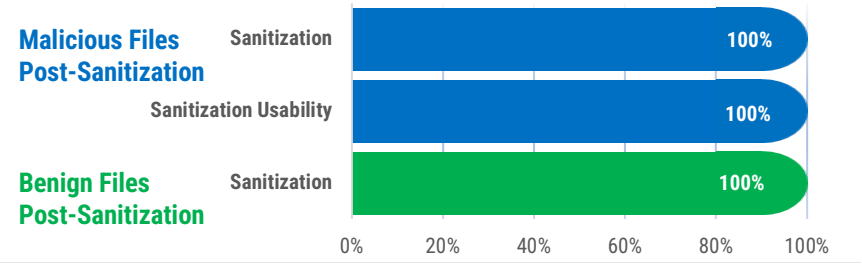

Figure 1. Summary of Security Validation for OPSWAT Deep CDR

The convergence of digital transformation and the evolving landscape of cyber threats highlights the indispensable necessity for resilient cybersecurity measures across all sectors. With the accelerating adoption of remote workforces and migration to cloud-based systems, enterprises face heightened risks, threats, and vulnerabilities, particularly from file-borne malware. The consequences of malware attacks are far-reaching, resulting in service disruption, tarnished brand reputation, and substantial losses in both data and revenue. According to the IBM Cost of Data Breach report for 2023, the average cost of a data breach is a staggering $4.45 million [1]. Organizations can effectively prevent breaches from file-borne threats by adding a security control like OPSWAT Deep CDR, renowned for its exceptional effectiveness in countering zero-day attacks and ensuring business continuity.

[1] https://www.ibm.com/reports/data-breach

Since its inception, the value of CDR has been increasingly appreciated. The CDR market has exhibited robust growth: "The size of global and Content Disarm and Reconstruction Market is anticipated to increase at a CAGR of 15.7% throughout the forecast period, from USD 0.2 billion in 2021 to USD 0.5 billion in 2026."[2].

CDR is a pivotal cybersecurity technique designed to prevent cyber threats by regenerating safe-to-consume files. It operates by disarming and rebuilding files, eliminating potentially malicious elements while preserving their functionality and usability. CDR is crucial in mitigating risks associated with file-based attacks and exploits, including malware, viruses, and other concealed cyber threats within files or HTML codes.

Both traditional and so-called next-generation antimalware solutions rely on detection methods, whether through signatures or heuristics, which now often include advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), extensive data analysis, and sandboxing. While these solutions excel in blocking known threats, they may fall short against newer, unidentified malware. In contrast, CDR operates as a prevention technology using techniques that effectively combat hard-to-catch threats. CDR removes any potentially harmful content, irrespective of whether it is malicious or benign. Elements, that are out-of-policy or deemed suspicious, such as macros, OLE files, and scripts are promptly eliminated, effectively disarming the file before undergoing reconstruction. Its capacity to sanitize files while preserving functionality proves valuable in countering zero-day attacks and emerging threats, showcasing its relevance in scenarios where file-sharing and collaboration are paramount.

The adage that security is risk management holds; however, managing risk requires alignment with risk tolerance. As such, OPSWAT's implementation of CDR within their flagship MetaDefender offering is highly robust and has the configuration granularity required to allow even those most adverse to risk to get a better night's sleep. "OPSWAT Deep CDR regenerates safe, usable files and supports hundreds of file types, including PDFs, archives, and file formats that support archives."[3]

To begin with, a proper implementation of CDR is tough to break. A failure can only be determined within the context of policy. If the policy is set to remove macros, then some documents will not work as intended, per policy; however, if the macros are signed, and the configured policy allows signed macros, then functionality will remain intact while also managing risk.

CDR finds primary use in preventing malicious files delivered via email, file-sharing platforms, and files uploaded to web applications and portals. An examination of over 100 Advanced Persistent Threat (APT) groups documented at MITRE ATT&CK reveals that nearly every APT group employs phishing attacks, often utilizing weaponized PDFs and Office documents to introduce further malware into organizations, extracting sensitive data afterward. Given that, virtual email services, including corporate email servers, block executables, and weaponized documents, entice users to visit malicious websites or exploit vulnerabilities in PDFs and other productivity files. It's important to note that, due to the ability to perpetrate attacks using steganography in files, CDR solutions must be able to sanitize media files. Sanitization, therefore, means that all potentially harmful content is removed. The term "potentially" is crucial here, as CDR is not a detection technology. Since an image can contain steganography, all image files are sanitized regardless of their nature. Similarly, files containing OLE objects are eliminated to mitigate their potential harm, whereas the entire file itself remains unaffected. Only the OLE objects contained within the files are removed. A significant majority of compromises originate from emails and file uploads containing

[2] https://www.marketsandmarkets.com/Market-Reports/content-disarm-reconstruction-market-89335390.html

[3] https://www.opswat.com/technologies/deep-content-disarm-and-reconstruction

malicious attachments, with PDFs and Microsoft Office documents being the preferred choices for numerous attackers and APT groups, including Aoqin Dragon, The Ajax Security Team, APT groups 28 and 29, Poseiden Group, the Lazarus Group, and many others among the 160 APT groups listed by Mitre Att@ck.

3. Sanitization Efficacy by File Type

In cybersecurity, particularly concerning productivity files, the accurate identification of file types is paramount. Different file types inherently possess unique structures, vulnerabilities, and modes of exploitation. It's essential to recognize that file extensions can be changed, leading to uncertainty if, for example, a bitmap is processed as an Excel file. Therefore, file types must be identified by content, including magic bytes. CDR plays a crucial role in this process, as it accurately identifies file types for processing. With a robust configuration capability, such as OPSWAT Deep CDR security experts can apply more nuanced and tailored defensive strategies, allowing granular decisions about handling different file types. With the ability to accurately determine file types, files with mismatched extensions (accidentally or intentionally) can be blocked. Incorrect file extensions have been used to bypass defenses that fail to choose the file type, highlighting the importance of accurate file identification. Evasion through misidentified file types is why polyglots exist, aiming to fool cybersecurity products. Understanding these distinctions enables more effective neutralization of potential threats.

Moreover, the value of CDR solutions becomes even more apparent when considering their capability to handle various file formats, including archives and nested layers of embedded files and objects. This capability ensures comprehensive inspection and subsequent removal of Russian doll-style nested layers of files and objects, even those hidden within multiple layers of nested files, various types of compression, or concealed through steganographic methods.

Because CDR is designed to prevent potential threats embedded in files from entering an environment, it disarms the payload and reconstructs before the file reaches the end user. SecureIQlab focused on and tested a variety of file formats, and OPSWAT Deep CDR performed exceptionally well, with the results depicted in Figure 2.

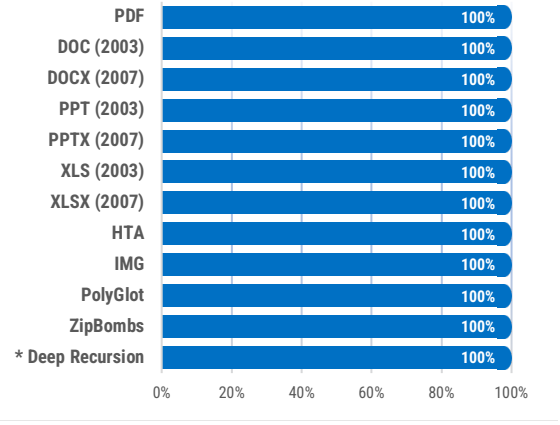

Figure 2. OPSWAT Deep CDR Security Validation Results by File Type

*** *Note*:** Deep recursion refers to the ability of a CDR solution to open a file that has embedded objects that, in turn, have more embedded objects. These embedding can continue for several layers. A CDR solution capable of deep recursion must sanitize every object down to the last layer and then reconstruct the entire file to a safe, functional file, with each nested object having been sanitized and reconstructed as well.

4. Sanitization Efficacy by Attack Type

Besides validating the solution's efficacy in sanitizing various file types, it's essential to include harmful content that employs different attack angles. Malicious content often utilizes exploits capable of delivering a broad range of payloads, including macros and OLE objects that can execute various attacks. The litmus test lies in whether a sanitized file remains capable of causing harm.

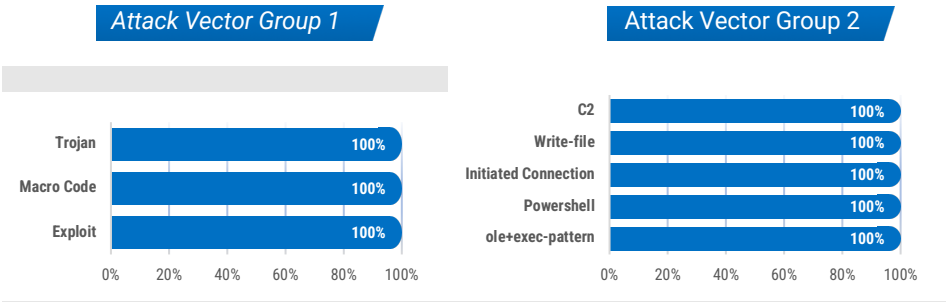

Figure 3. OPSWAT Deep CDR Security Results by Attack Type

As illustrated in Figure 3, the OPSWAT Deep CDR adeptly handled the gamut of attack types that can be launched by active content.

5. Sanitization by File Type and Attack Type

An attack vector exists, and the assessment in this section states which attack vector was used by file-borne threats. This delineation signifies a breakdown in coverage. It's important to understand that "N/A" doesn't necessarily imply that CDR is incapable of addressing the attack vector but instead that the attack vector does not apply to this particular scenario. It's essential to distinguish this distinction clearly. This breakdown in coverage offers valuable insights into the scope of how OPSWAT Deep CDR handled different attack vectors, as depicted in Figures 4 and 5.

File types	Attack Vector Group 1		
	Exploit	Macro Code	Trojan
PDF	100%	NA	NA
DOC (2003)	100%	100%	100%
DOCX (2007)	100%	100%	100%
PPT (2003)	100%	100%	100%
PPTX (2007)	100%	100%	100%
XLS (2003)	NA	100%	100%
XLSX (2007)	NA	100%	100%
HTA	NA	NA	100%
IMG	100%	NA	100%
PolyGlot	NA	NA	100%
ZipBombs	NA	NA	100%
Deep Recursion	NA	NA	100%

Figure 4. OPSWAT Deep CDR Security Results by Attack File Type and Vector Group 1

File types	Attack Vector Group 2				
	ole+exec-pattern	Powershell	Initiated Connection	Write-file	C2
PDF	100%	100%	100%	100%	100%
DOC (2003)	100%	100%	100%	100%	100%
DOCX (2007)	100%	100%	100%	100%	100%
PPT (2003)	NA	100%	100%	100%	100%
PPTX (2007)	NA	100%	100%	100%	100%
XLS (2003)	NA	100%	100%	100%	100%
XLSX (2007)	NA	100%	100%	100%	100%
HTA	NA	100%	100%	100%	100%
IMG	NA	NA	NA	100%	NA
PolyGlot	NA	NA	NA	NA	NA
ZipBombs	NA	NA	NA	NA	NA
Deep Recursion	NA	NA	NA	NA	NA

Figure 5. OPSWAT Deep CDR Security Results by Attack File Type and Vector Group 2

6. Fidelity of Sanitized Files Analysis

CDR solutions are primarily designed to effectively sanitize files by removing potentially malicious content rather than analyzing the integrity or usability of the file. CDR operates as a prevention-based and policy-driven technology, with policies dictating what content remains, what is removed, or what gets transformed. Evaluating the fidelity of sanitized files post-CDR is crucial to ensuring that security measures do not compromise usability and functionality. Through meticulous analysis of file integrity and usability, coupled with the flexible granularity of CDR policies, organizations can strike a delicate balance between robust cybersecurity and seamless user experience, optimizing CDR implementation's effectiveness. In this assessment, SecureIQlab evaluated both benign and malicious file integrity and usability post-sanitization, showcasing the efficacy of OPSWAT Deep CDR with results depicted in Figures 6 and 7.

File Type	Benign
PDF	100%
DOC (2003)	100%
DOCX (2007)	100%
XLSX (2007)	100%
Deep Recursion	100%

Figure 6. Usability of Benign File Type Post Sanitization

File Type	Malicious
PDF	100%
DOC (2003)	100%
DOCX (2007)	100%
PPT (2003)	100%
PPTX (2007)	100%
XLS (2003)	100%
XLSX (2007)	100%
HTA	100%
IMG	100%
PolyGlot	100%
ZipBombs	100%
Deep Recursion	100%

Figure 7. Usability of Malicious File Type Post Sanitization

7. SecureIQlab CDR Test Methodology

In our relentless pursuit of cybersecurity excellence, SecureIQLab embarked on a journey to meticulously assess and validate the OPSWAT Deep CDR technology, a leading offering in the CDR market. With an unwavering commitment to fortifying digital defenses, SecureIQlab spared no effort in conducting extensive research to vet malware samples spanning a diverse spectrum of file types, archives, and nested. Our rigorous testing methodology encompassed every conceivable threat vector related to productivity file attacks, from standard office documents to complex PDF files and stealthy steganography techniques to nefarious VBS/Macro embedded scripts.

Not stopping there, we delved into the realm of polyglot and HTML Applications (.hta) extensions, recognizing their potential as vectors for remote code execution and exploitation. Our dedication to comprehensively evaluating OPSWAT's CDR technology led us to scrutinize these files with precision, pushing the boundaries of our testing framework. Through this exhaustive process, we sought to validate the efficacy of OPSWAT Deep CDR technology under the most demanding circumstances, ensuring its readiness to combat emerging threats with unparalleled resilience. This approach exemplifies our unwavering dedication to advancing cybersecurity defenses and underscores our commitment to delivering solutions that stand the test of time.

8. Summary

OPSWAT Deep CDR performed exceptionally well in the SecureIQlab CDR validation test as shown in Figure 1. With its robust configurable policy capability, security experts can apply more nuanced and tailored defensive strategies, allowing for granular decisions about handling different file types, including archives and nested layers of files and objects. Organizations, therefore, can strike a delicate balance between robust security and a seamless user experience.

9. Contact Information

SecureIQLab, LLC.

9600 Great Hills Trail Suite 150W

Austin, TX 78759 USA

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

10. Copyright and Disclaimer

For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (January 2024)