

Letter of Attestation

Monday, 17th March 2025

To whom it may concern,

This letter is to confirm that MDSec was contracted by Sophos Ltd to perform a product assessment of their MDR, SOC.OS and XDR Applications.

The engagement was undertaken between the 6th January 2025 and 5th February 2025. The Summary table below shows a summary of the results and their corresponding risk ratings:

Type of Test	Critical	High	Medium	Low	Informational
MDR Application Assessment	0	2	3	3	1
SOC.OS Application Assessment	0	0	1	3	2
XDR Application Assessment	0	0	2	5	1

During this period, MDSec assessed the implemented security measures with the aim of identifying and exploiting possible vulnerabilities within the product.

Approach:

MDSec uses a full, rigorous web application assessment methodology, as described in Chapter 21 of their Web Application Hacker's Handbook, which is taught and accepted throughout the security industry. A modified version of this methodology is used when assessing API security. MDSec also tests for vulnerabilities described by the Open Web Application Security Project's (OWASP) Top Ten.

MDSec uses PortSwigger's Burp Suite Professional tool; the de facto standard for web application and API security testing, alongside custom extensions and open-source tools where appropriate.

MDSec combines automated tools with manual testing to achieve the best possible outcome in terms of the number and severity of vulnerabilities identified, whilst eliminating false positives.

Where desktop client applications were part of the assessed product, these were analysed to obtain knowledge of their inter-process communications, network traffic, file operations and sensitive data handling. A combination of static and dynamic analysis, as well as OS-

level tracing and function hooking was employed for this purpose. Their security measures were then probed for vulnerabilities that could affect both the application's client and the remote servers, as well as third party users of the same application.

The final report issued to Sophos Ltd contained technical details and remediation steps that should be followed to ensure the ongoing security and integrity of the in-scope product,

Sincerely

S.Chell

Sharon Chell
Business Development Manager
sharon.chell@mdsec.co.uk
(44) 7944 678750