

Letter of Attestation

Wednesday, 21st February 2024

To whom it may concern,

This letter is to confirm that MDSec was contracted by Sophos to perform a product assessment of their MDR/XDR/SOC.OS platform.

The engagement was undertaken between the 20th of November 2023 and 4th of January 2024. The Summary table below shows a summary of the results and their corresponding risk ratings:

Type of Test	Critical	High	Medium	Low	Informational
MDR Assessment	0	3	1	1	3
XDR Assessment	0	0	1	2	2
SOC.OS Assessment	0	0	1	1	1
Central MDR UI	0	0	2	0	2
MDR AWS Configuration Review	0	0	7	7	8
MDR Kubernetes Configuration Review	0	0	11	9	10

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

Approach:

- Tested for common attacks such as Client-side Access Controls, Logic flaws, session handling, replay attacks and other logic flaws, as well as using a combination of manual and automated techniques to assess the application for input-based vulnerabilities such as XSS, SQL Injection (client and server side), File path manipulation, and custom language injection
- Reviewed of the cloud service from design, architecture and deployment considerations, to practical security evaluation of the configuration, trusts, and weakly configured attributes that can be abused for privilege escalation or asset compromise.

The final report issued to Sophos 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