MDSec Consulting Limited
1st Floor
32 Park Green
Macclesfield
SK11 7NA

Letter of Attestation

3rd April 2024

To whom it may concern,

This letter is to confirm that MDSec was contracted by Sophos Ltd to perform a product assessment of their Factory Platform.

The engagement was undertaken between the 5th of February 2024 and 15th of February 2024. The Summary table below shows a summary of the results and their corresponding risk ratings:

Type of Test	Critical	High	Medium	Low	Informational
Web App & API Assessment	0	0	1	3	2
AWS Assessment	0	0	5	5	7
Kubernetes Assessment	0	0	4	2	1

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, etc.
- Tested the API endpoints for known API-specific issues such as input validation, authorisation checks, server-side request forgery, etc.
- Tested for the presence of Anti-Virus scanning on file uploads.
- Assessed the TLS configuration of the web server.
- Tested Kubernetes environment for common attacks such as privilege escalation, RBAC misconfiguration, Network and Namespace Isolation, etc.
- Scanned the container images for security vulnerabilities.
- Assessed encryption of data in rest and transit, permission of IAM roles/Users, logging and monitoring of data, etc. in the AWS environment.

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,

MDSec Consulting Limited
1st Floor
32 Park Green
Macclesfield
SK11 7NA

Sincerely

S.Chell

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