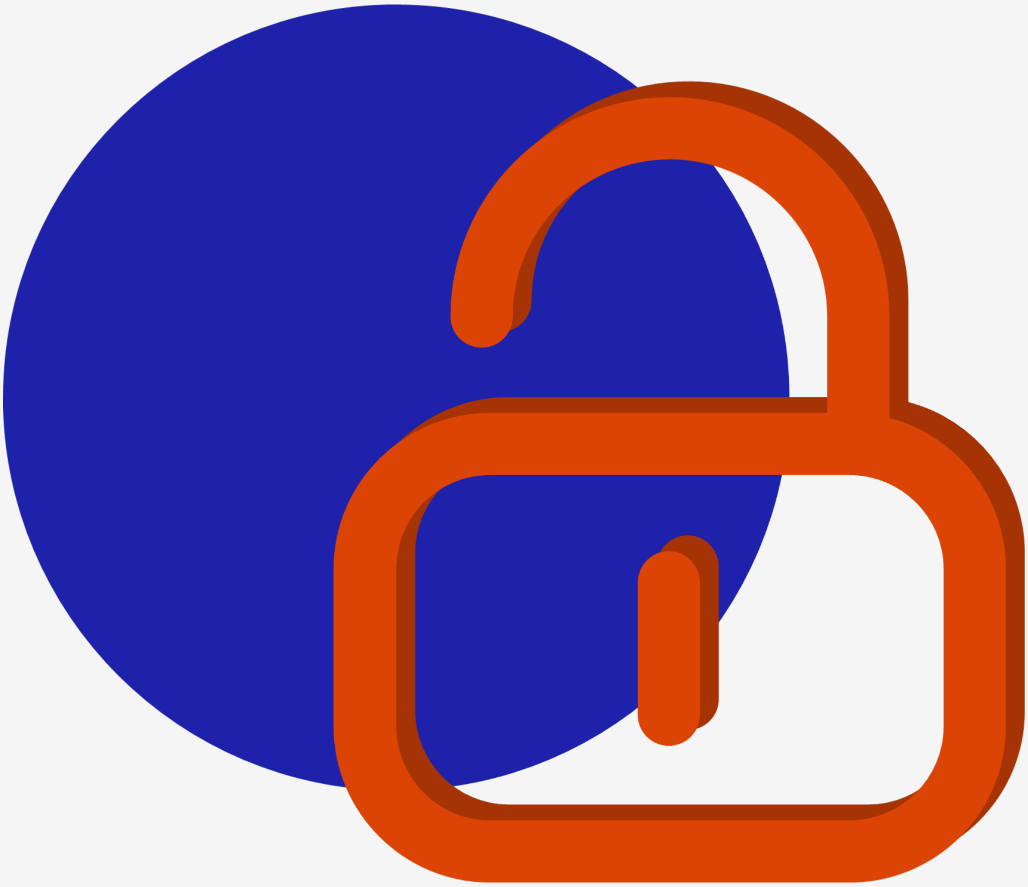
++

Sophos Central Phase 2 Security Assessment - Attestation Letter

Sophos

19 January 2024



MWR CYBERSEC

Document Control

Date	Change By	Change	Issue
2024–01–15	Muhummud Deedat	Document created	0.1
2024–01–19	Stephen Munro	Document QA	0.2
2024–01–19	Muhummud Deedat	Document published	1.0

Document Distribution

Date	Name	Company
2024–01–19	Steven Hedworth	Sophos

Contents

1. Overview

MWR CyberSec (MWR) was commissioned by Sophos to conduct an in-depth security assessment of their Central application. The application provides a software as a service (SaaS) solution to allow Sophos customers to manage all of their Sophos products from a central location. The assessment was performed remotely from the 22nd of November 2023 to the 16th of January 2024.

The assessment comprised of multiple separate testing components, namely:

- SiSense Custom Authentication Protocol Security Review
- SiSense Web Application Security Assessment
- High Risk Central Web Services Assessment
- Central Application UI Assessment
- SiSense AWS and Kubernetes Security Review

MWR's consultancy team has built a strong reputation as a research-driven IT security consultancy firm. The team has a proven track record of collaborating with organisations that are industry leaders in information security. This is evident in the number of advisories and security-related publications available on MWR's Intel web page[1] and corporate insight webpages[2].

Beyond the technical competency of consultants, MWR prides itself in providing a unique set of client engagement services that put security management at the core of clients' business processes. Consultants are experienced in analysing the security architecture of solutions and providing catered security design recommendations.

2. Approach

The primary aim for the assessment was to determine whether or not any of the deployed resources were exposed in a way that could be exploited from the public internet. In addition, testing aimed to determine whether or not any potential security-related enhancements could be made to improve the overall security posture of the Central application and the environment it resided in.

2.1. SiSense Custom Authentication Protocol Security Review

Testing of the JDBC driver was performed primarily by inspecting the application source code and building sections of the driver for isolated test cases.

2.2. SiSense Web Application Security Assessment

The testing approach involved navigating the Central UI web application's functionality to identify which SiSense API endpoints were used by the application. The endpoints that were identified were then tested for any vulnerabilities or misconfigurations that could pose a security risk to Sophos.

[1] https://www.mwrcybersec.com/technical-research

[2] https://www.mwrcybersec.com/corporate-insights

The API endpoints identified and tested were deemed to have a strong security posture overall, with no identified vulnerabilities posing a significant risk to Sophos. Among the endpoints, only three vulnerabilities were discovered, all of which carried minimal risk to Sophos.

2.3. High Risk Central Web Services Assessment and Central Application UI Assessment

The security assessments performed against the Sophos Web Service and the Central application, was conducted in line with MWR's standard testing methodology which is in line with the CREST application testing methodology, covering aspects including information gathering, content discovery, injection attacks, session management, and authentication and authorisation bypass attacks.

In addition to testing for common vulnerabilities, focus was placed on assessing the authorisation controls for both vertical and horizontal authorisation bypasses for the in-scope components. Vertical authorisation checks were performed to ensure that low-privileged users could not access functionality reserved for higher-privileged user roles, such as functionality available to internal Sophos user roles. Horizontal authorisation checks were performed to ensure that users belonging to a particular customer could not access data belonging to another customer.

2.4. SiSense AWS and Kubernetes Security Review

The Sophos SiSense web application solution was hosted in an AWS environment. MWR assessed the resources within the AWS environment pertaining to phase 2 to identify any security misconfigurations and possible hardening controls that could be enforced within the environment to ensure that the associated configurations deployed within Sophos' environments were secure.

MWR's methodology for assessing such environments combines best practice guidance issued by AWS and other industry organisations (such as NIST, NCSC and CIS) with MWR's own experience performing offensive security assessments of cloud environments.

MWR's methodology focuses on the following areas:

- Administration and patch management
- Network/Boundary Security Controls (VPCs, subnet layouts, Security Groups, etc):
  - This includes a port scan of any externally exposed assets, and basic vulnerability scanning for vulnerabilities in any of the exposed services
- Data Security and Encryption:
  - Encryption at rest
  - Encryption in transit (TLS)
- Identify Management and Access Controls:
  - IAM policies, roles, groups, and users
  - Any federated access control mechanisms
  - Resource-specific access policies
- Certificate, key and secrets management
- Detection controls, such as CloudTrail and CloudWatch
- Incident readiness
- The deployed AWS Organisations' SCPs and other access controls

The assessment also included an in-depth security review of the Kubernetes cluster within the AWS environment.

3. Results

3.1. SiSense Custom Authentication Protocol Security Review

The results of this component identified two low risk vulnerabilities. Although neither of these vulnerabilities posed any significant risk to Sophos, remediation of these vulnerabilities would aid in ensuring that the JDBC implementation adheres to security best practise and reduces the overall attack surface.

3.2. SiSense Web Application Security Assessment

The SiSense Web Application Security Assessment identified two low risk vulnerabilities and one informational risk vulnerability which presented minimal risk to Sophos. These vulnerabilities related to defence-in-depth measures that could be applied to further improve the overall security posture of the Sophos SiSense solution.

3.3. High Risk Central Web Services Assessment and Central Application UI Assessment

The findings identified in Central Web Services and Central Application UI Assessment consisted of four low risk vulnerabilities and two informational risk vulnerabilities.

Both the web services and application were resilient towards the majority of the attack techniques attempted and consistently incorporated security best practices and effective security controls. Only a small number of vulnerabilities were identified, which if remediated by Sophos, will further harden the solution against attacks.

3.4. SiSense AWS and Kubernetes Security Review

The results of the AWS and Kubernetes Configuration review identified three medium risk, eight low risk and two informational risk vulnerabilities within the configuration of resources in the Sophos AWS environment. These vulnerabilities were not exploitable from an external perspective, and related to security hardening controls which should be implemented.

3.5. Vulnerabilities Summary

The assessments identified three medium risk, fifteen low risk and six informational risk vulnerabilities. In total, 24 vulnerabilities were found; the table below shows a count breakdown of these vulnerabilities per component and risk rating.

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
JDBC Custom Authentication Security Assessment	0	0	2	0
SiSense Web Application Security Assessment	0	0	2	1

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Central High Risk Web Services Security Assessment	0	0	2	0
Central Application UI Assessment	0	0	2	2
SiSense AWS Security Assessment	0	3	7	3
Total	0	3	15	6

The vulnerabilities identified were a result of defense-in-depth measures and inconsistencies with the implementation of security best practices. Although the overall security of each component was already of a high standard, by remediating these vulnerabilities the security posture of Sophos Central solution would be improved.

The following risk profiles were used as guidelines to classify the vulnerabilities:

HIGH	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Sophos's electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
MEDIUM	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Sophos's electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
LOW	A vulnerability will be assessed to represent a low risk if the likelihood or impact of exploitation is extremely low. For example, this could be an HTTPS configuration that allows weak ciphers or outdated protocols, or a CAPTCHA that can be solved programmatically.
INFORMATIONAL	A vulnerability will be assigned the informational classification when it cannot be exploited directly but is not in line with security best practice. Such a vulnerability could provide information that would facilitate research into an attack against the target system. For example, disclosure of the server type in an HTTP response.

APPENDIX I – Disclaimer and Non-Disclosure Agreement

Non-Disclosure Statement

This report is the sole property of Sophos. All information obtained during the testing process is deemed privileged information and not for public dissemination. MWR CyberSec pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of Sophos. MWR CyberSec strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

MWR CyberSec and Sophos have signed an NDA.

Disclaimer

This report is not meant as an exhaustive analysis of the level of security now present on the tested hosts, and the data shown here should not be used alone to judge security of any computer system. Some scans were performed automatically and may not reveal all the possible security holes present in the system. Some vulnerabilities that were found may be 'false positives', although reasonable attempts have been made to minimise that possibility. In accordance with the terms and conditions of the original quotation, in no event shall MWR CyberSec or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss or other damages.

APPENDIX II – Project Team

Assessment Team

Lead Consultant	Muhummud Deedat
Additional Consultants	Logan Kroeger Momelezi Mchunu Connor Du Plooy Justin Moorcroft

Quality Assurance

QA Consultant	Stephen Munro

Project Management

Delivery Manager	Cath de Wet
Account Director	Gaylen Postiglioni

MWR
CYBERSEC