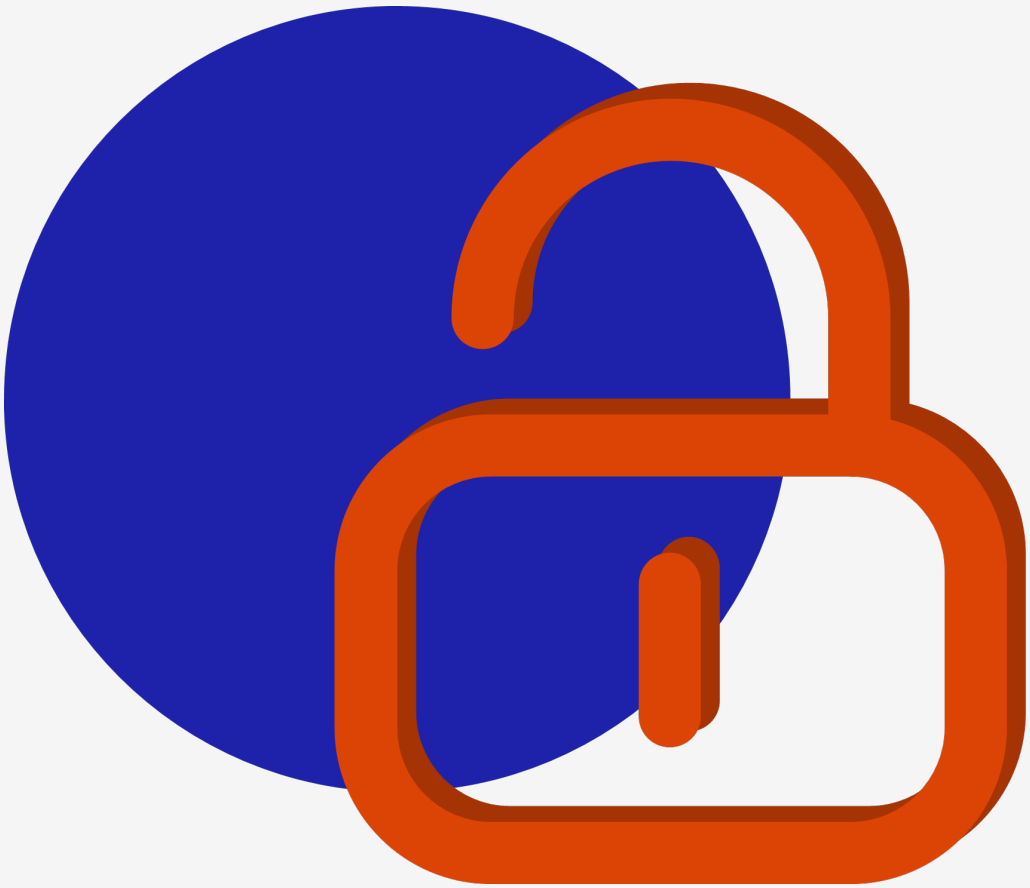
++

Secureworks Taegis NDR Device Security Assessment: Letter of Attestation

Sophos

3 March 2026



Document Control

Date	Change By	Change	Issue
2026–02–25	Christo Erasmus	Document created	0.1
2026–02–25	Johan van der Merwe	Document amended	0.1
2026–03–02	Connor du Plooy	Document QA	0.2
2026–03–02	Christo Erasmus	Document amended	0.3
2026–03–03	Christo Erasmus	Document published	1.0

Document Distribution

Date	Name	Company
2026–03–03	Sam Caise	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted a security assessment of the Secureworks Taegis NDR appliance for Sophos, between the 10th and the 27th of February, 2026. The assessment was performed against NDR virtual appliances deployed on MWR's own infrastructure, from two different testing perspectives:

- Unauthenticated penetration testing against the device from the local network
- Authenticated testing and security configuration review of the device's operating system via SSH, using a customised image provided by Sophos to allow shell access, which is not normally available to customers

2. Approach

The assessment followed a white-box approach, whereby MWR was provided with a customised device image allowing full shell access, as well as access to Sophos stakeholders familiar with the NDR device, to provide additional information and documentation where required. However, the assessment also included black-box testing of the NDR device from the perspective of an unauthenticated attacker on the network.

The following main focus areas were defined for the assessment:

- Penetration testing against any services exposed by the NDR appliance to the local network
  - This perspective focused on avenues for gaining a foothold on the appliance, causing interruptions to the services offered by the appliance, as well as attempts to bypass the controls it offers
- Attempting to compromise the user accounts running key services on the device from a black-box perspective
- Identifying local privilege escalation vectors from the perspective of user accounts running key services on the device
  - The purpose of this focus area was to determine whether an attacker would be able to escalate privileges, in the event that they managed to gain code execution on the device
- Denial-of-Service (DoS) testing to determine whether it is possible to disrupt the services that are exposed and utilised by the device

3. Results

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
NDR Device Security Assessment	0	0	1	3
Total	0	0	1	3

The Taegis NDR device exposed a minimal attack surface, due its architecture and the security controls that had already been put in place. Only a small number of vulnerabilities were identified, most of which were rated as informational. The one low risk vulnerability could only be exploited by an attacker that had already gained initial access to the device in a low-privileged context, which was considered unlikely given the minimal attack surface exposed by the device.

Risk Rating Scale

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 – Project Team

Assessment Team

Lead Consultant	Christo Erasmus
Additional Consultant	Johan van der Merwe

Quality Assurance

QA Consultant	Connor du Plooy

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC