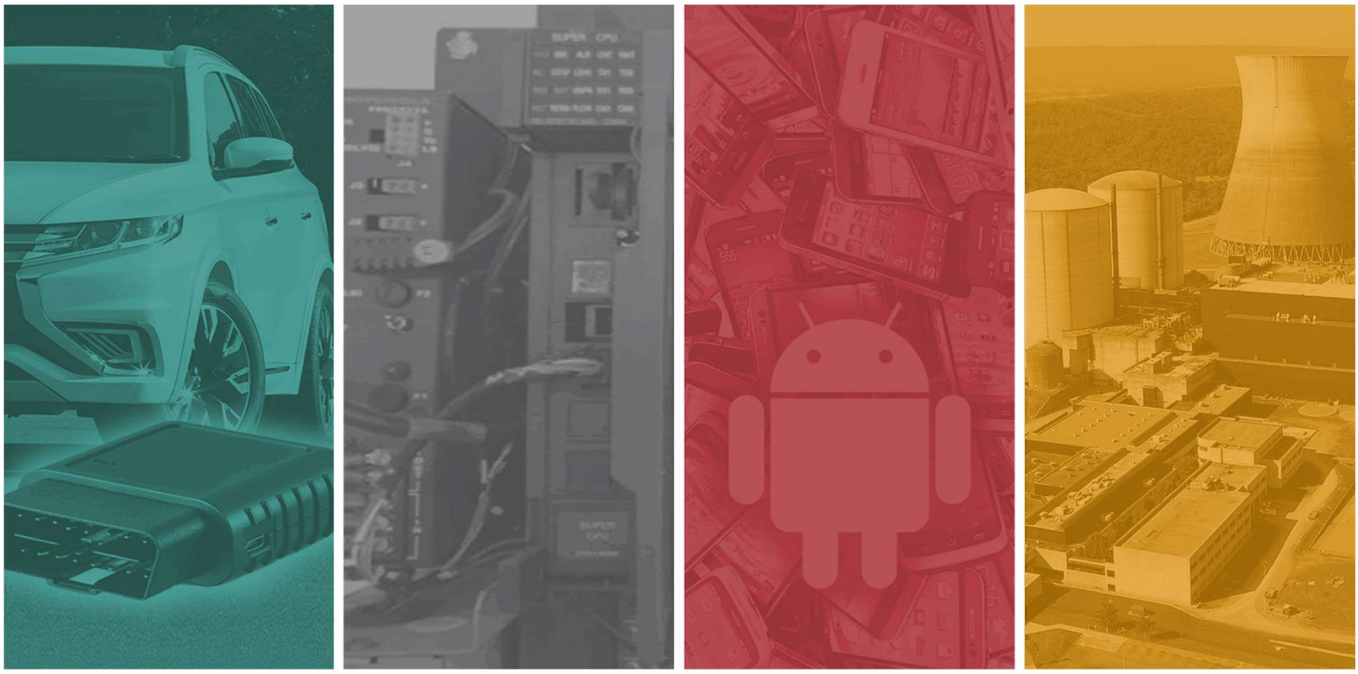
PEN TEST PARTNERS

Attestation of Penetration Testing of ZTNA Solution Security Review

for

Sophos Ltd



PTP Job ID: 16942
Version 1.0
13th March 2025

Technical Consultants: Joe Durbin, Gabriel Garcia Teran
Account Manager: Ben Ruffell

CREST

THE CYBER SCHEME CERTIFIED TESTERS

1. Attestation of Penetration Testing

1.1. Introduction

Pen Test Partners conducted a penetration test of the ZTNA Solution. This included their Amazon Web Services (AWS) environment, their Elastic Kubernetes Service (EKS), and their publicly facing web application. The purpose of the engagement was to provide visibility of security risks of the solution and to understand how to remediate any findings identified to improve resilience against attempted compromise. Testing was carried out from 17th February to 27th February 2025.

1.2. Scope and methodology

The scope of the assessment covered the following elements of work:

- ZTNA Networking Review
- ZTNA Web Application Testing
- ZTNA AWS Security Review
- ZTNA Kubernetes Security Review

The ZTNA networking review and the ZTNA web application testing were conducted replicating the solution in a lab environment and through the ZTNA section of the Sophos Central web application, alongside with the solution hosted on AWS and Kubernetes. Industry standards, alongside with PTP's methodologies were followed to ensure adherence to security best practice.

The AWS account's configuration was assessed against CIS benchmarks and Amazon security best practices, using a hybrid approach of automated tooling and manual checks.

Finally, the Kubernetes Cluster was assessed against Kubernetes CIS benchmarks and several automatised Kubernetes security audit tools, alongside with manual checks calling directly the Kubernetes API via `kubectl` were used to ensure full coverage was achieved when assessing the security posture of the cluster.

No Denial-of-Service (DoS) attacks were performed.

1.3. Conclusion

Penetration testing the mentioned scope resulted in discovering the vulnerabilities rated in the risk categories listed below:

Table 1: Number of vulnerabilities discovered for each phase and risk class

		Risk rating			
		Critical	High	Medium	Low
Phase	ZTNA Networking and Web	0	0	0	0
	ZTNA AWS account	0	0	3	3
	ZTNA Kubernetes cluster	0	1	1	3

No security issues were found on the Networking and Web phases, making the solution appropriately secured. The AWS environment and Kubernetes cluster were found slightly misconfigured; however, despite the high-risk finding on the Kubernetes cluster, no vulnerabilities were found that could be promptly exploited from the perspective of an outside attacker.

Pen Test Partners can only confirm these statements and attest to the security assessment of the phases carried out during the security review at the time of testing and delivery of the last report as dated above.

This document does not serve as a full executive summary report of the penetration test.

1.4. Industry standards

Pen Test Partners is an ISO 27001, Cyber Essentials, PCI QSA, NCSC CHECK, UK CAA Assure, CREST and CREST STAR certified independent information security consultancy.