Qodea

Google Cloud
Partner

Public Attack Surface Report (PASR)

EXAMPLE REPORT

Introduction

The Qodea Security Team conducts continual Attack Surface assessments' for existing and prospective customers as part of our ongoing commitment to improving Cloud Security. A Qodea PASR assesses online vulnerabilities using multiple sources of publicly available information to make a broad passive initial assessment of a customer's attack service through the eyes of a hostile actor. All of the information presented below is publicly available to any entity actively conducting a reconnaissance exercise on your organisation and the Attack Surface it presents to the Internet.

All report information was accurate when the report was created. Cloud resources are constantly changing, so as a result some minor discrepancies might appear in some findings. We have identified findings that may require attention and as such should be reviewed internally with remediation action agreed or mitigating controls configured.

General Findings

4 subdomains were detected. 6 hosts are running 25 services. The collected information was checked against a set of security rules. The configuration may not align to best security recommendation in 19 assessment (out of 25), HTTP service is enabled on 14 services, CAA isn't configured on 5 services.

Darkweb Findings

A total of 100 records found on the darkweb, that includes:

100 Account(s)
100 Email(s)
10 IP Addresses)
25 Username(s)
56 Cleartext Password(s)
37 Hashed Password(s)
3 Address(es)
15 Person Name(s)
12 Phone Number(s)

Domain Statistics

Hosts	10
Services	24
DNS Records	25
Darkweb Records	224
Subdomain count	8
Security Assessment Playbooks	25
Security Assessment Rules Failed	25
Security Assessment Rules Passed	6
Security Assessment Rules Checked	28