online

SecurityScorecard Summary Validation Assessment Report

PREPARED BY:

ONLINE BUSINESS SYSTEMS
8500 NORMANDALE LAKE BLVD, SUITE 350
BLOOMINGTON MN, USA 55437

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

TABLE OF CONTENTS

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information that is confidential and proprietary to the subject of the testing for SecurityScorecard. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the validation testing and SecurityScorecard for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

Date: April 24, 2020
Change Description: Initial Report

William Bechtel
Online Director
wbechtel@obsglobal.com

Ben Kettlewell
Online Pentester
bkettlewell@obsglobal.com

EXECUTIVE SUMMARY

Small, local utilities have the same threat profile as large domains. Each validation assessment consisted of the following activities:

- Independent reconnaissance of the client's external domain footprint
- Comparison and validation of Online's results with the data provided by SecurityScorecard
- Manual investigation and documentation of all discrepancies
- Reporting of all results including details for any records deemed as invalid

To conduct each assessment, Online evaluated the external footprints of each domain using a variety of open-source intelligence databases, externally exposed services, and non-invasive information gathering tools. The first of the 13 assessments began on December 09, 2019 and the final assessment concluded on March 16, 2020.

SUMMARY OF FINDINGS

Online found SecurityScorecard's footprinting to be very accurate. Over the course of testing Online evaluated SecurityScorecard's data for a total of 13 unique, unrelated, and randomly selected domains and found SecurityScorecard's attribution process to have an accuracy of 95%. The accuracy for positively attributing IP Addresses was found to be **94%** while for DNS Records it was found to be 100%.

SUMMARY OF VALIDATION ASSESSMENT ACTIVITIES

Assessment	Minimum	Maximum	Mean	Average	Total	Accuracy
IP Addresses	36	277	98	114	1480	94%
DNS Records	6	96	20	29	377	100%
Combined	48	286	130	143	1857	95%

SELECTION PROCESS

In order to ensure the results of the 13 tested domains are an accurate representative sample of SecurityScorecard's overall attribution process, the criteria for selecting the domains to be tested was defined and performed entirely by Online.

A list of fifty thousand unique but similarly sized domains were provided to Online by SecurityScorecard. This list was processed using a random number generator to select the domains to be evaluated. Statistically, the vast number of domains provided ended in ".com". To ensure potential outlier data was captured in the relatively small sample size, Online ensured an appropriate percentage of uncommon domain endings were included in the random sample set. These randomly selected endings included ".org", ".co.nz", ".jp", ".bz", ".gr" and ".com".

VALIDATION PROCESS

To ensure the integrity of these validation results, SecurityScorecard provided no instructions or guidance on either the methodology or tools which should or could be used to validate any records, whether IP Addresses or DNS Records. The methodology used by Online is built upon the same procedures used in the reconnaissance phase of a blind Red Team engagement.

This phase closely aligns with SecurityScorecard's goal of enumerating a domain's entire external boundary and subsequently all potential attack vectors the domain is responsible for securing. The various techniques and tools used by Online collect ownership information from a wide variety of locations, ranging from publicly available service information to 3rd party databases. The details of these methods and tools have not been revealed to SecurityScorecard and, depending on the domain being tested, may vary as needed to obtain the most accurate information possible.

The results from Online's independent reconnaissance are then compared to SecurityScorecard's results and any discrepancies are investigated. For Online to make the determination any record provided by SecurityScorecard is valid, the following criteria must be met:

- Online must be able to independently obtain, at absolute minimum, one positive indicator the record can be attributed to the domain
- In the course of all Online's reconnaissance activities, there must be no strong indication the record can be attributed to any other entity
- There must be no indication the record is being operated OR maintained on behalf on the

domain by a 3rd party or vendor

- The indicators observed for each record must be sufficiently strong as to be judged by Online as both owned AND controlled by the domain

It is Online's professional opinion that, only when all of these criteria are met is it reasonable to claim the domain has both the right and the responsibility to assess and maintain the security of said record. In the few cases where any one of these criteria are not met, Online determined the record to be invalid and provided SecurityScorecard with an explanation as to why. No information as to the tools or techniques used, nor recommendations as to how to adjust SecurityScorecard's process, were provided to ensure the integrity of future testing is not negatively impacted.

Note: *As the practice of penetration testing requires written legal permission from the device owner, Online relied entirely on third party data and passive or non-intrusive reconnaissance activities. At no point did Online perform any targeted scanning or exploitation of any device being evaluated.*

DOMAINS EVALUATED

The following is a list of all top level domains which received validation testing.

- milestonepowered.com
- cuwest.org
- baycity.co.nz
- ricondo.com
- hostmetro.com
- i2i.jp
- joinreal.com
- engage.bz
- comoretel.com
- ameriflight.com
- txpchat.com
- alpinemetalfinishing.com
- kone.gr

SecurityScorecard

ABOUT SECURITYSCORECARD

SecurityScorecard helps enterprises gain operational command of their security posture and the security posture of their third-parties through continuous, non-intrusive monitoring. The company's approach to security focuses on identifying vulnerabilities from an outside perspective, the same way a hacker would. SecurityScorecard's proprietary SaaS platform offers an unmatched breadth and depth of critical data points including a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering, and Leaked Information.

When to receive an email with your company's current score, please visit instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017