riskrecon by

This report was created on **01 Oct 2024** by RiskRecon

Last Assessment Date: **27 Sep 2024**

Risk Summary Report For

Argos Risk, LLC

Issued By

Argos Risk

If you have any questions concerning your report, or want to get an updated report, please feel free to contact us at support@riskrecon.com.

Learn more at riskrecon.com.

Introduction

Argos Risk, LLC
Summary Report

RiskRecon monitors the cybersecurity performance of Argos Risk, LLC using open-source intelligence. RiskRecon employs passive, non-invasive techniques to discover the organization's public systems and to analyze the cybersecurity risk posture of those systems. Given the open-source intelligence assessment methodology, the analysis is centered on publicly-accessible systems that can be observed from the Internet. RiskRecon assessments are risk-based, where every issue is contextualized based on the severity of the issue and the value of the system in which the issue exists.

This report provides the results of the RiskRecon assessment and is intended to enable simple understanding and action on cybersecurity risk. To that end, RiskRecon distilled the results into a RiskRecon Rating, which serves to provide rapid orientation of the organization's cybersecurity performance. The summary section of the report highlights areas of strength and weakness, supported by the underlying detail necessary to understand and act. In addition to this PDF report, RiskRecon provides the assessment online, where additional information, knowledge bases, and tools are available. To obtain online access to your RiskRecon assessment, email RiskRecon at support@riskrecon.com.

Methodology

RiskRecon continuously monitors the cybersecurity risk of companies through open-source intelligence techniques. Being based on open-source intelligence, all system discovery and security analytics are passive, based on collection and analytics of publicly available data. RiskRecon discovers systems through sophisticated analytics of a variety of data sources, including network registration records, domain registration records, Internet DNS resolution logs, and search engine data sets, among others. RiskRecon assesses cybersecurity risk of systems through analysis of public system content such as headers, cookies, code and content. RiskRecon also monitors and analyzes a variety of security-related network communications, including commercial and open-source data feeds.

RiskRecon Does...

- Deep mining of domain registration databases
- Deep mining of network registration databases
- Analysis of Internet DNS IP to hostname resolution logs
- DNS queries
- Lightly browse web sites, obeying robots.txt instructions
- Analytics of publicly accessible code, content, configurations
- Monitoring and analysis of commercial and open-source IP reputation feeds
- Mining the internet for relevant information such as indicators of data loss events
- Analyze Internet port scan data sourced from a commercial provider

RiskRecon Does Not...

- Tamper with parameters
- Inject code
- Conduct cross-site scripting
- Conduct SQL injection
- Attempt to bypass authentication
- Execute memory overflow tests
- Fill out form fields
- Guess credentials
- Execute vulnerability exploits
- Attempt to bypass security controls

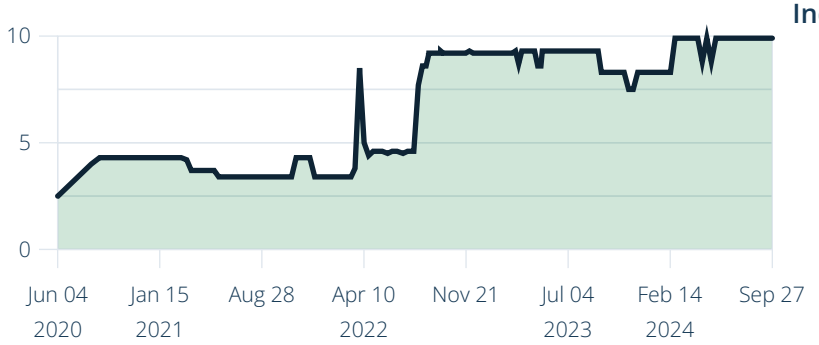
RiskRecon Portal

The RiskRecon portal provides additional information, beyond that provided in the printed report. In the portal, RiskRecon provides detailed finding information, additional risk context, rich knowledge bases, and readily-accessible customer support. The RiskRecon portal is available to all RiskRecon licensed customers and can be accessed at https://www.riskrecon.com. Vendors may also gain access to their RiskRecon cybersecurity rating profile by contacting RiskRecon support by emailing support@riskrecon.com.

Risk Priority Report

Argos Risk, LLC
Summary Report

Recon Rating



Industry Metrics

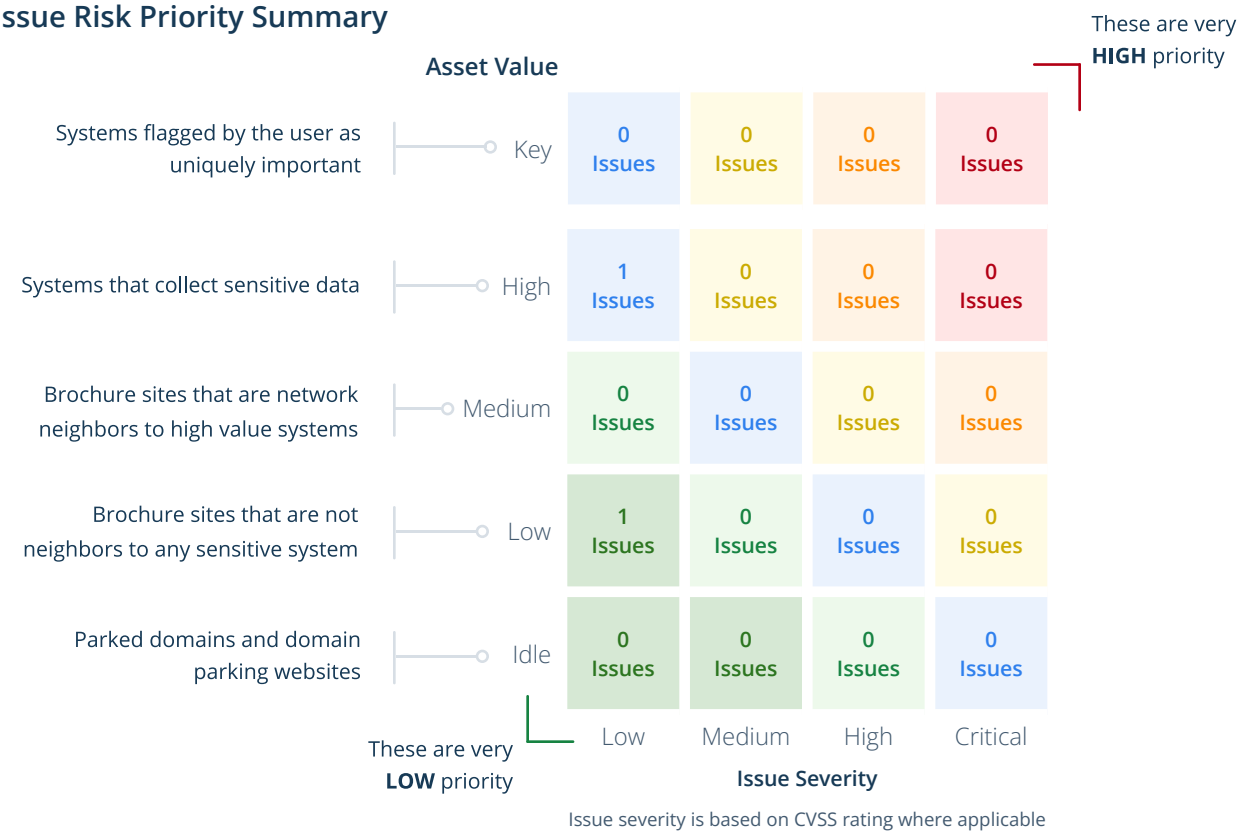
Industry Average
7.7
Percentile Rank
90th
Industry
Software Services

Domain Ratings

Domain	Rating	Issues	Trend
Software Patching	A 10	0	0.0→
Application Security	A 9.9	2	0.0→
Web Encryption	A 10	0	0.0→
Network Filtering	A 10	0	0.0→
Breach Events	A 10	0	0.0→

Domain	Rating	Issues	Trend
System Reputation	A 10	0	0.0→
Email Security	A 10	0	0.0→
DNS Security	A 10	0	0.0→
System Hosting	A 10	0	0.0→

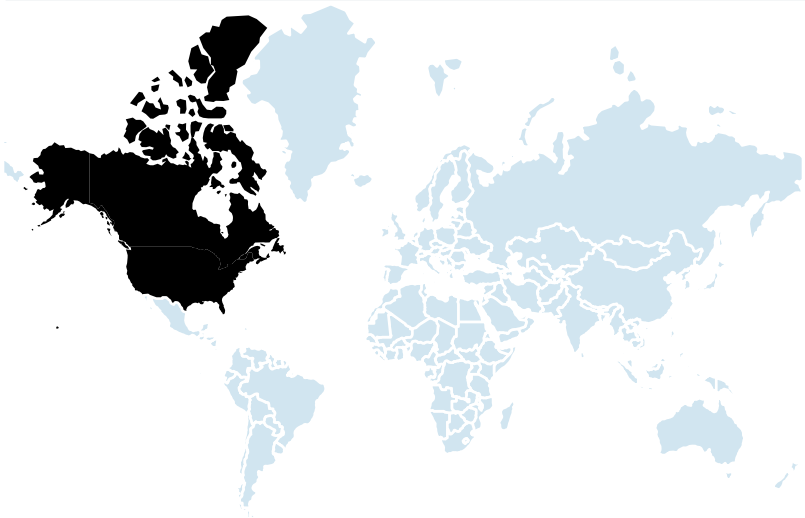
Issue Risk Priority Summary



Issue severity is based on CVSS rating where applicable

Company Overview

Argos Risk, LLC
Summary Report



Web

Web Servers	5
Web Hosting Providers	2

Email

Email Servers	2
Email Providers	1

DNS

Registered Domains	1
DNS Servers	2
DNS Hosting Providers	1

Owned Networks

Netblocks	0

Active Systems

Active Hostnames	6

2

Hosting Countries

Country	Systems
United States	5
Canada	1

1

Domains

Domain	Systems
argosrisk.com	6

2

Hosting Providers

Provider	Systems
Rackspace Inc.	5
Google, Inc.	1

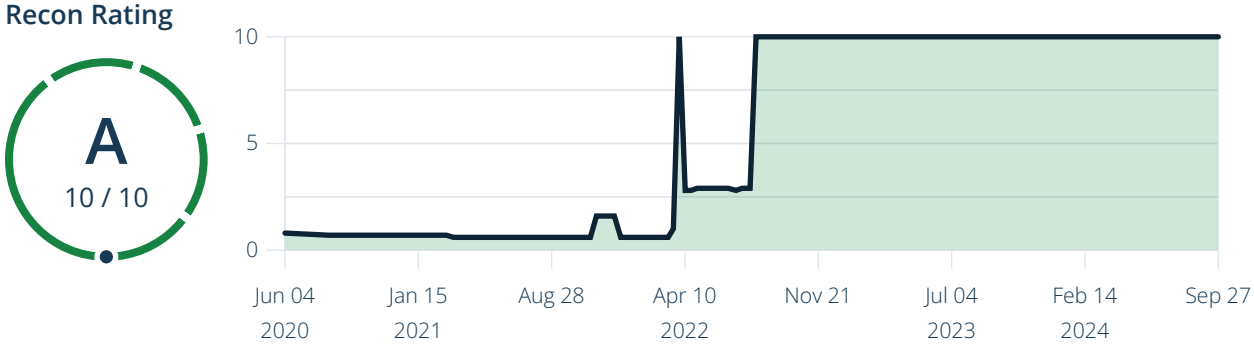
Software Patching

Argos Risk, LLC
Summary Report

Overview

RiskRecon used passive analysis to identify systems running end of support software that have security vulnerabilities. Operating unpatched software increases the likelihood of unauthorized access or degradation of system performance. From the issues identified, Argos Risk selected the software patching issues detailed in this section as important to address due to the issue severity and the sensitivity of the system in which the issue exists.

Recon Rating



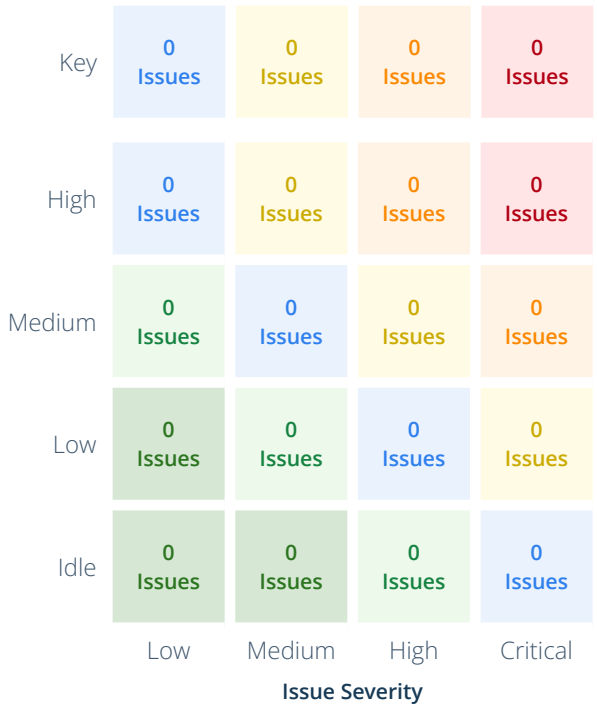
Summary Metrics

6	0	0%
Observations	Issue Count	Issue Rate

Industry Rating

100th	9.4
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Application Server Patching	0
OpenSSL Patching	0
CMS Patching	0
Web Server Patching	0

Application Security

Argos Risk, LLC
Summary Report

Overview

RiskRecon used passive techniques to analyze web applications for the presence of common application security controls. From the issues identified, Argos Risk selected those detailed in this section as important to address due to the issue severity and the sensitivity of the system in which the issue exists.

Recon Rating

Summary Metrics

9	3	33%
Observations	Issue Count	Issue Rate

Industry Rating

85th	6.1
Percentile Rank	Industry Avg.

Risk Priority Summary

Asset Value

	Low	Medium	High	Critical
Key	0 Issues	0 Issues	0 Issues	0 Issues
High	1 Issues	0 Issues	0 Issues	0 Issues
Medium	0 Issues	0 Issues	0 Issues	0 Issues
Low	1 Issues	0 Issues	0 Issues	0 Issues
Idle	0 Issues	0 Issues	0 Issues	0 Issues

Issue Severity

Security Criteria	Finding Count
CMS Authentication	0
HTTP Security Headers	2
High Value System Encryption	0
Malicious Code	0

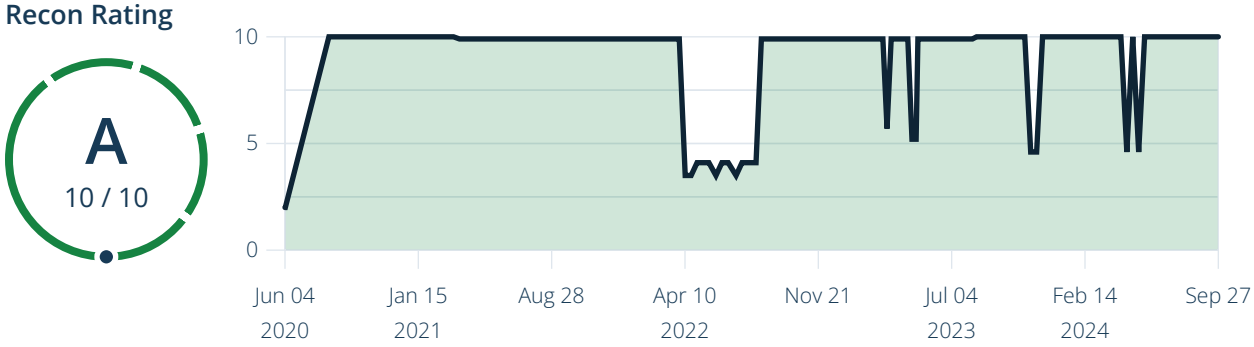
Web Encryption

Argos Risk, LLC
Summary Report

Overview

RiskRecon used passive techniques to analyze web encryption security configurations. Correctly configured web encryption is essential to ensuring that communications are protected from eavesdropping and that people can verify the authenticity of the system. From the issues identified, Argos Risk selected those detailed in this section as important to address due to the issue severity and the sensitivity of the system in which the issue exists.

Recon Rating



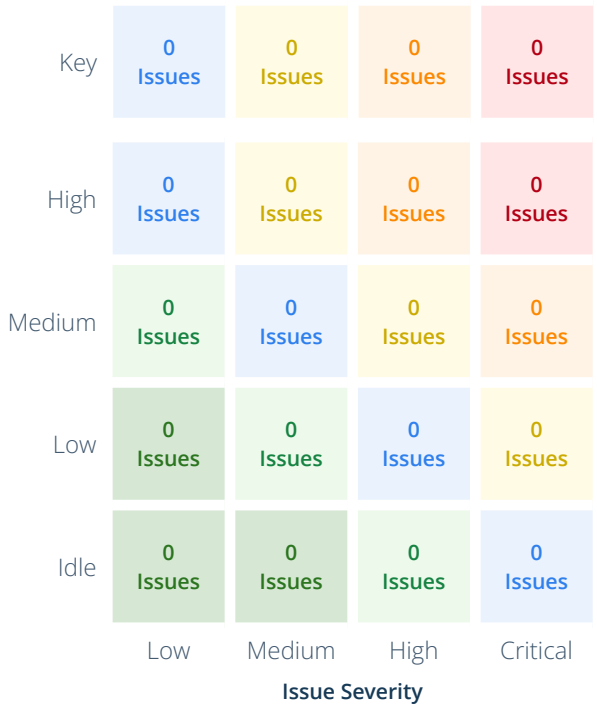
Summary Metrics

36	0	0%
Observations	Issue Count	Issue Rate

Industry Rating

100th	8.8
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Certificate Expiration Date	0
Certificate Valid Date	0
Encryption Hash Algorithm	0
Encryption Key Length	0
Encryption Protocols	0
Certificate Subject	0

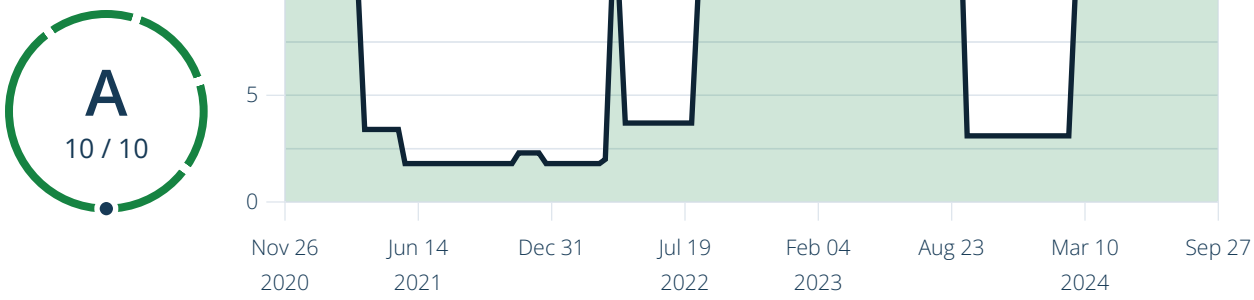
Network Filtering

Argos Risk, LLC
Summary Report

Overview

The Network Filtering domain enumerates unsafe network services and Internet of Things (IoT) devices the organization has exposed to the Internet. Enterprises should limit Internet-accessible network services and systems to those that are safe and necessary. Unsafe network services and IoT devices are very susceptible to compromise through various methods such as credential guessing, communications intercept, and vulnerability exploitation. RiskRecon analyzes Internet-facing systems and networks for the following services: MS SQL Server, MySQL, PostgreSQL, MongoDB, Elastic, DB2, Redis, Memcached, CouchDB, Cassandra, Remote Desktop Protocol, VNC, Telnet, FTP, Samba, Finger, netBIOS, BGP, PPTP, X11, Oracle TNS, Apple Airport, Webmin. RiskRecon analyzes systems and networks to discover Internet of Things (IoT) devices, such as printers, elevator control systems, HVAC interfaces, cameras, and network storage devices.

Recon Rating



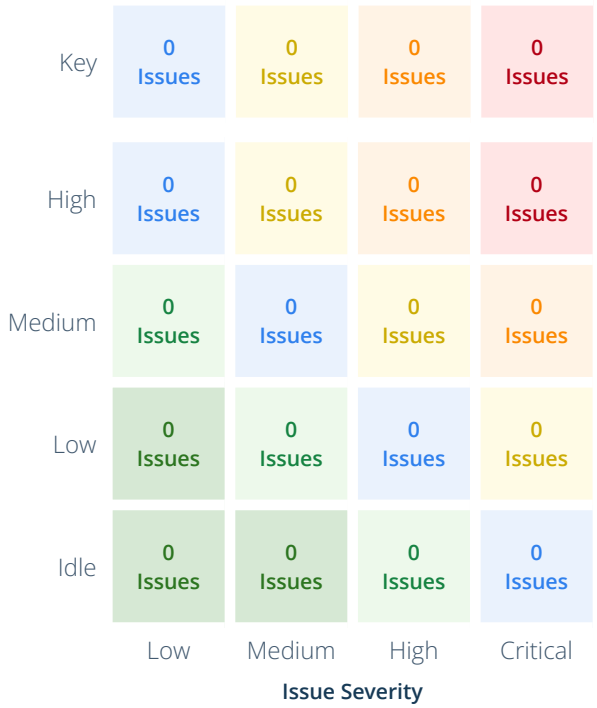
Summary Metrics

N/A	0	N/A
Observations	Issue Count	Issue Rate

Industry Rating

100th	9.0
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Unsafe Network Services	0
IOT Devices	0

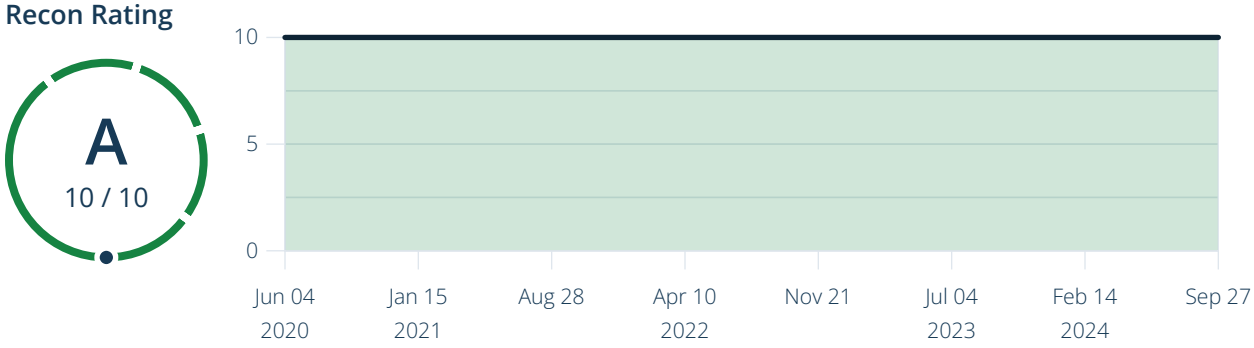
Breach Events

Argos Risk, LLC
Summary Report

Overview

The Breach Event domain summarizes the breach events the organization has experienced. Recent breach events indicate gaps in the breach protection program. Organizations with breach events occurring consistently over time very likely have ineffective breach prevention programs and material gaps in their information security program. Organizations with recent and also repeated breach events over time should be examined closely to ensure that controls are operating effectively to prevent future breaches and loss of data.

Recon Rating



Summary Metrics

N/A	0	N/A
Observations	Issue Count	Issue Rate

Industry Rating

100th	10
Percentile Rank	Industry Avg.

Security Criteria	Finding Count
Breach Events: 0-6 Months	0
Breach Events: 6-12 Months	0
Breach Events: 12-24 Months	0
Breach Events: 24-36 Months	0
Breach Events: > 36 Months	0

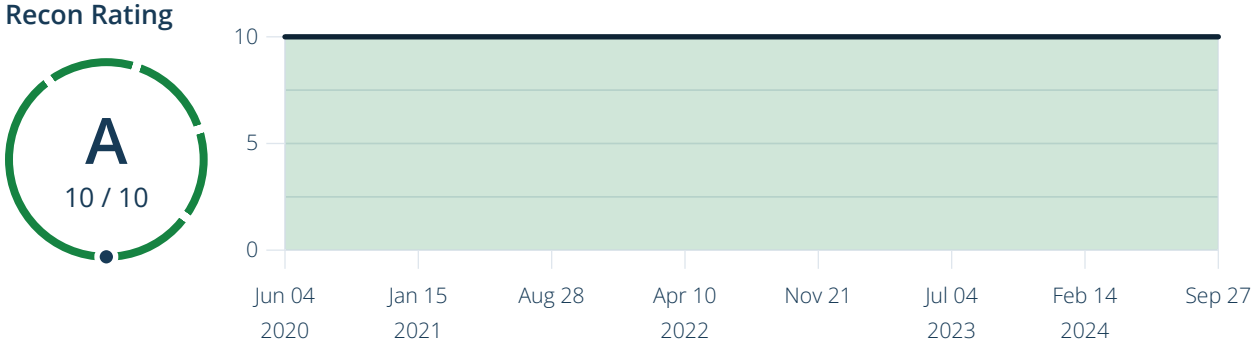
System Reputation

Argos Risk, LLC
Summary Report

Overview

RiskRecon analyzed IP reputation and threat intelligence databases to identify suspicious system activity. Observed malicious activity may indicate the system is compromised or is being used for unauthorized purposes. Of the issues identified, Argos Risk selected those detailed in this section as important to investigate and address due to the issue severity and the sensitivity of the system in which the issue exists.

Recon Rating



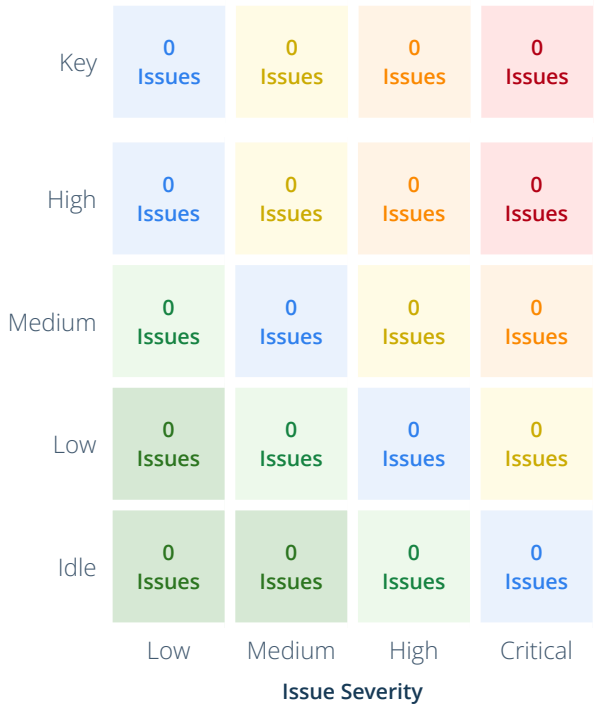
Summary Metrics

9	0	N/A
Observations	Issue Count	Issue Rate

Industry Rating

100th	10
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Command and Control Servers	0
Botnet Hosts	0
Hostile-Hosts: Hacking	0
Hostile-Hosts: Scanning	0
Phishing Sites	0
Other Blacklisted Hosts	0
Spamming Hosts	0

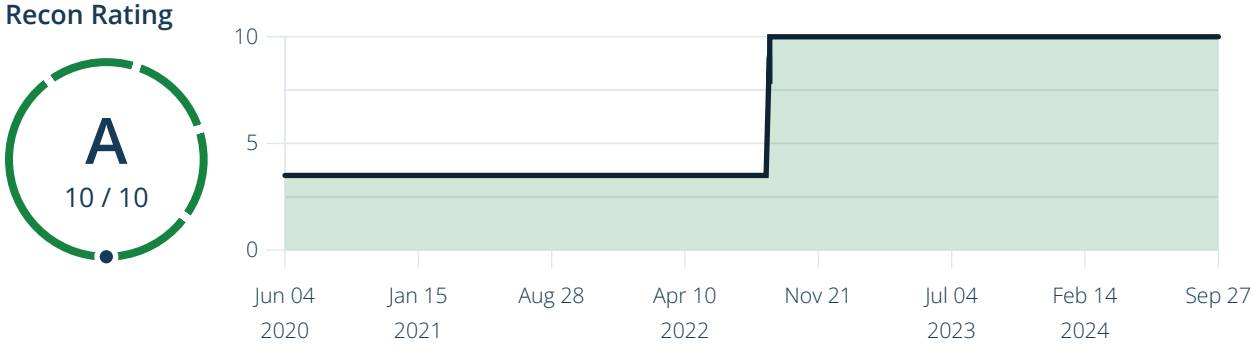
Email Security

Argos Risk, LLC
Summary Report

Overview

RiskRecon used passive techniques to analyze the security configuration of email services. Email servers should be configured to encrypt email communications to protect email messages from unauthorized access. Domains should be configured to prove the authenticity of email messages to prevent spoofing. Of the issues identified, Argos Risk selected those listed in this section as important to address due to the issue severity and sensitivity of the system in which the issue exists.

Recon Rating



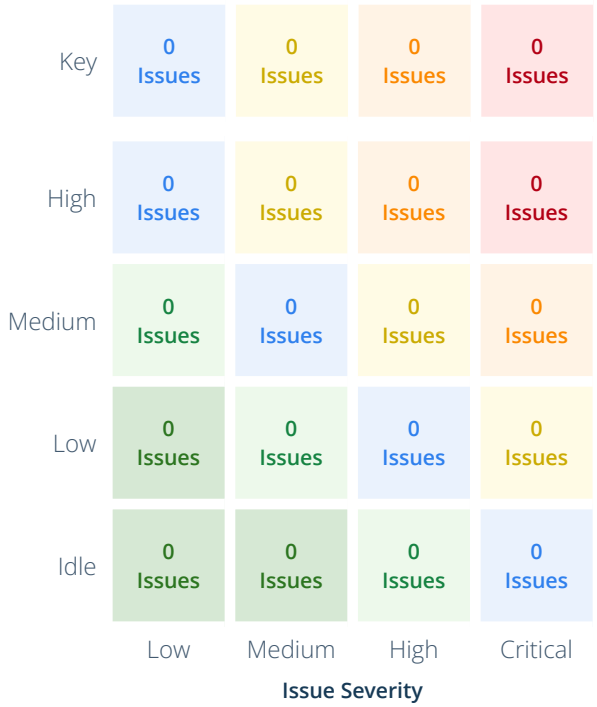
Summary Metrics

3	0	0%
Observations	Issue Count	Issue Rate

Industry Rating

100th	9.3
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Email Authentication (SPF or DKIM)	0
Email Encryption (STARTTLS)	0

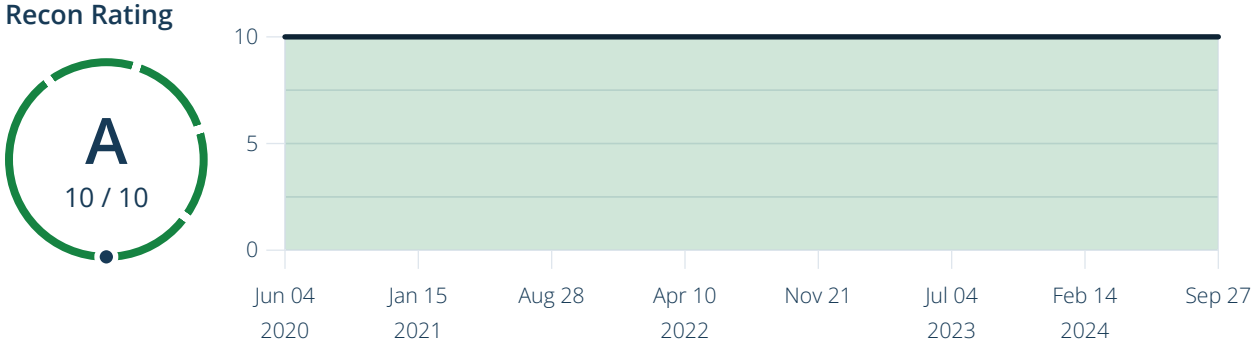
DNS Security

Argos Risk, LLC
Summary Report

Overview

RiskRecon used passive techniques to analyze the security configuration of domain name services. Proper DNS security configuration helps ensure the availability and control of domains. Of the issues identified, Argos Risk selected those listed in this section as important to address due to the issue severity and sensitivity of the domain in which the issue exists.

Recon Rating



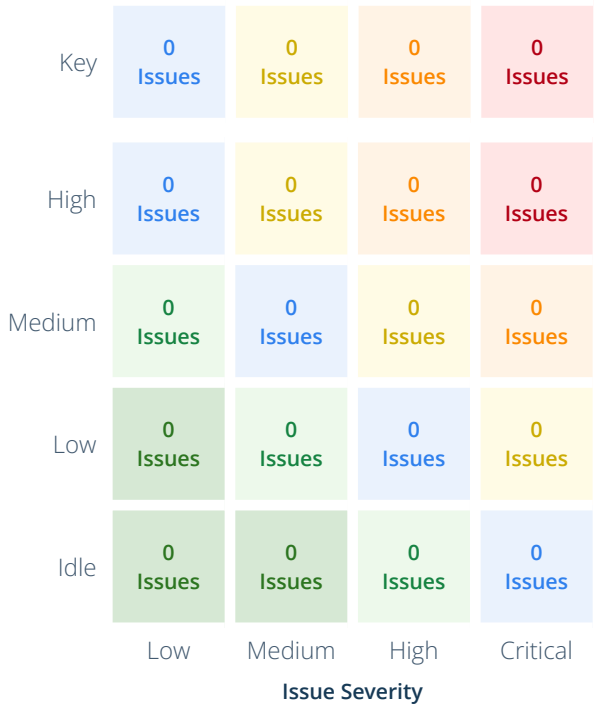
Summary Metrics

1	0	0%
Observations	Issue Count	Issue Rate

Industry Rating

100th	9.0
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Domain Hijacking Protection	0

System Hosting

Argos Risk, LLC
Summary Report

Overview

RiskRecon used passive techniques to analyze the defensibility of the system hosting configuration. In doing so, RiskRecon specifically sought to identify any systems using IP addresses shared with other companies. Where possible, companies should host systems using IP addresses that are dedicated to their use only. Systems that use a shared IP address are more difficult to defend because network layer control options are limited, such as IP address filtering and intrusion monitoring. Systems using shared IP addresses are also often blacklisted due to malicious activity of other tenants using the same IP address. Of the issues identified, Argos Risk selected those detailed in this section as important to address due to the sensitivity of the system in which the issue exists.

Recon Rating

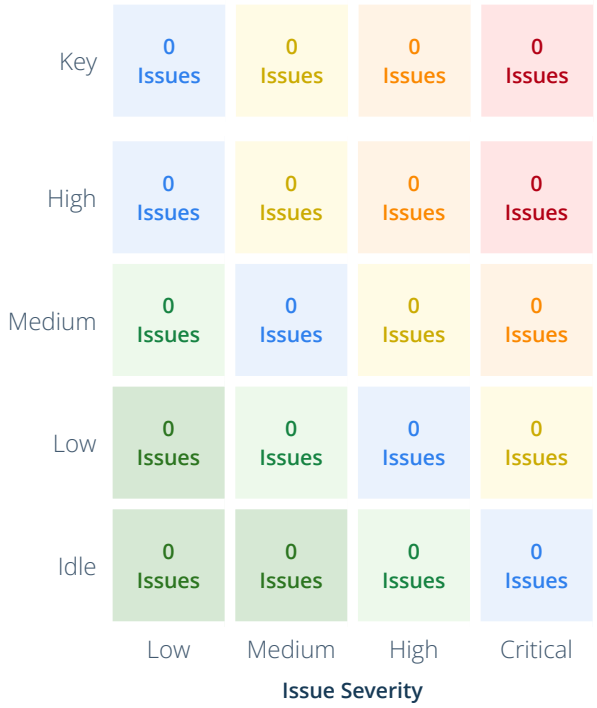
Summary Metrics

N/A	N/A	N/A
Observations	Issue Count	Issue Rate

Industry Rating

100th	8.3
Percentile Rank	Industry Avg.

Risk Priority Summary



Security Criteria	Finding Count
Cotenant IP Hosting	0

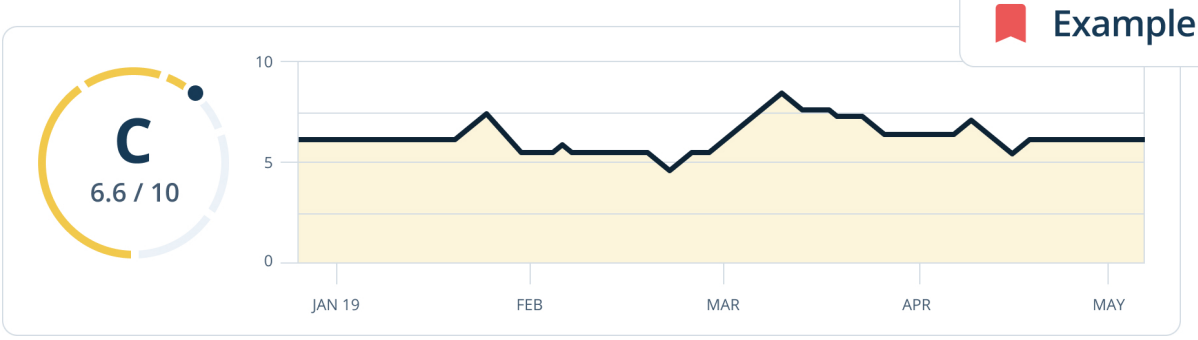
Appendix: Reading the Report

Argos Risk, LLC
Summary Report

Ratings

Using sophisticated analytics, RiskRecon distills the issues discovered into a single numerical rating on a scale from 0 - 10, where 10 is the highest possible rating. This rating is provided for the overall organization, as well as for each security domain. This rating provides directional signal intended to provide rapid point-in-time assessment and to easily monitor performance trend over time.

Example



Data

The ratings information naturally directs attention towards detailed data, which enables understanding and action that reduces risk. For each issue, RiskRecon provides the information necessary to pinpoint the source of the issue, in addition to issue severity, the value at risk, and a suggested risk priority. The RiskRecon portal provides additional information, beyond that provided in the printed report, where RiskRecon provides robust knowledge bases, detailed finding information, additional risk context, and readily-accessible customer support. Contact RiskRecon at support@riskrecon.com to obtain online access to your assessment.

Example

The Issue

RiskRecon identified one or more web encryption implementations that support use of insecure protocols such as SSLv2, SSLv3, and TLS 1.0. Insecure protocols have fundemental flaws that allow miscreants to break the encryption process, exposing the authorized paties to risk of communications intercept and fraud.

Recommendation

From the total set of issues discovered, RiskRecon identified the issues listed in this section as important to address based on the sensitivity of the system in which the issue exists. Correct the issue by disabling support for insecure protocols such as SSLv2, SSLv3, TLS 1.0, and TLS 1.1.

Finding	Hostname	Asset Value	Severity	Priority
PHP 5.2x	fakehostname.foobar	High	Critical	1
PHP 5.2x	fakehostname.foobar	Medium	Medium	4

The RiskRecon Portal

The RiskRecon portal provides additional information, beyond that provided in the printed report. In the portal, RiskRecon provides detailed finding information, additional risk context, rich knowledge bases, and readily-accessible customer support. The RiskRecon portal is available to all RiskRecon licensed customers and can be accessed at https://www.riskrecon.com. Vendors may also gain access to their RiskRecon cybersecurity rating profile by contacting RiskRecon support by emailing support@riskrecon.com.