

Security and Privacy Assessment Report



**Beaconer Inc.** (Vendor Name)

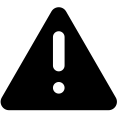
Niagara Falls, Canada Contact Industry - Cyber Security

## Scope of Service

For ABC Enterprise (Client), Beaconer Inc. will provide an AI-powered Machine learning platform that automates the Vendor Risk assessment. Beaconer will provide the service based on the subscription taken by ABC Enterprise (Client). Beaconer will be responsible for conducting the Vendor risk assessment for any new vendor working with ABC Enterprise (Client) and periodic.

## Rating Summary

Yes No

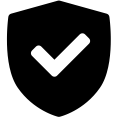


**Data Elements**

PII Data

Cardholder Data

Data outside USA



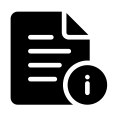
Penetration Testing

**Security Testing**

Defined Remediation Process

Tested Within Last 12

Months

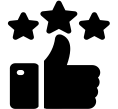


Data is Encrypted

**Information Security**

Server/Network Security

Password Policies

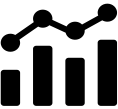


SOC Provided

**Third-Party Reviews**

SOC Unqualified

Other Third-Party Audit Provided

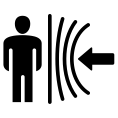


Privacy Policy

**Data Privacy**

Exempt Individual Data

Breach Notification

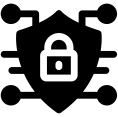


**Resiliency**

Infrastructure

Monitoring/ Maintenance

Backup Practices

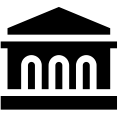


Electronic Access Control

**Physical Security**

Access Reviews

Security Cameras

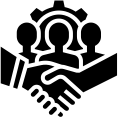


Info Security Policy

**Information Security Governance**

Asset Management

Employee Security



Vendor Maintains a BCP

**Business Continuity**

BCP Tested Annually

RTO and RPO



# MITRE ATT&CK coverage score

The chart below identifies high level tactic vulnerabilities and inspects assessment results in view of attack post-mortems. The shaded area indicates the degree to which your third party has controls in place to prevent, detect, or respond to these tactics. The higher the percentage, the better the coverage.

Discovery 92.29%

Execution 84.71%

Exfiltratio n

94.27%

Defense Evasion 87.46%

Control Coverage

Credential Access 92.66%

Command and Control 97.62%

Collection 83.34%

Impact 83.97%

Initial Access 89.09%

Lateral Movement 91.32%

Privilege Escalation 89.46%

Persistence 89.83%

**Beaconer Matching Report**

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Question** | **Response** | **Risk** |
|  |  |  |  |
| **Risk Management** | Is there a formalized risk governance plan in place? |  |  |
| Is there a formalized Risk Assessment process in place? |  |  |
| Is there a process to identify and manage the risk response and treatment of risks? |  |  |
| Is there a formal Risk Exception process for the Risk Business decided to accept? |  |  |
| **Information security Policies** | Is there a set of information security policies in place? |  |  |
| Have all policies been assigned to an owner responsible for review and approved periodically? |  |  |
| Have all information security policies and standards been reviewed in the last 12 months? |  |  |
| Is there a process to approve exceptions to the established security policies? |  |  |
| **Organization of Information Security** | Is there a respondent information security function responsible for security initiatives? |  |  |
| **Human Resource Security** | Are Human Resource policies in place? |  |  |
| Do HR policies include background checks on employees including criminal screening? |  |  |
| Does security awareness training program including new hire in place? |  |  |
| Does the HR policy includes a disciplinary process for Non-compliance? |  |  |
| **Asset Management** | Is there an Asset management program or policy in place? |  |  |
| Do all projects involving Scoped Systems and Data go through some form of information security assessment? |  |  |
| Is there an asset Inventory list or configuration management Database (CMDB) in place? |  |  |
| Do you have a process to remove the client information prior to decomissionning or reuse of equipment with client information? |  |  |
| **Access Control** | Is there an access control program or policy in place? |  |  |
| Are unique IDs required for authentication to applications, operating systems, databases and network devices? |  |  |
| Is access to applications, operating systems, databases, and network devices provisioned according to the principle of least privilege? |  |  |
| Is there segregation of duties for granting access and approving access to Scoped Systems and Data? |  |  |
| Does the password policy define specific length and complexity requirements for passwords? |  |  |
| **Physical and Environmental Security** | Is there a physical security program in place? |  |  |
| Are there physical security controls in place for all secured facilities e.g., data centers, office buildings? |  |  |
| Do the physical security controls include electronic controlled access system (key card, token, fob, biometric reader, etc.)? |  |  |
| Are there environmental controls in secured facilities to protect computers and other physical assets e.g., Fire detection and suppression? |  |  |
| Are visitors permitted in the facility? If yes, are they escorted all the time? |  |  |
| **Communication and Operations Management** | Are management approved operating procedures utilized? |  |  |
| Is there an operational change management/change control policy in place? |  |  |
| Does the change control process to ensure clients are notified prior to changes being made which may impact their service? |  |  |
| Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced? |  |  |
| **System Acquisition, Development,**  **and Maintenance** | Is there a formal Software Development Life Cycle (SDLC) process in place? |  |  |
| Is there a formal Secure software development lifecycle policy in place? |  |  |
| Are Applications used to transmit, process or store Scoped Data? |  |  |
| Are Outside development resources utilized? |  |  |
| Are Web applications configured to follow best practices or security guidelines e.g., OWASP? |  |  |
| Is there a documented change management /change control process for applications with Scoped Data? |  |  |
| **Third-Party** | Is there a documented third party risk management program in place? |  |  |
| Do Subcontractors have access to scoped systems and data or processing facilities? |  |  |
| Does the TPRM program require Confidentiality and/or Non-Disclosure Agreements & Data Breach Notification from Subcontractors? |  |  |
| Are background checks performed for Service Provider Contractors and Subcontractors? |  |  |
| **Information Security Incident Management** | Is there an established incident management program in place? |  |  |
| Is there a formal Incident Response Plan in place? |  |  |
| Does the Incident Response Plan include guidance for escalation procedure & actions to be taken in the event of an information security event? |  |  |
| Does regular security monitoring include malware activity alerts such as uncleaned infections and suspicious activity? |  |  |
| **Business Continuity Management** | Is there an established business resiliency program in place? |  |  |
| Is there a periodic (at least annual) review of your Business Resiliency procedures? |  |  |
| Are formal business continuity procedures developed and documented? |  |  |
| Is there a formal, documented Information TechNology Disaster Recovery exercise and testing program in place? |  |  |
| Was RTO & RPOs achieved during the last DR test? |  |  |
| **Compliance** | Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements? |  |  |
| Is there a records retention policy covering paper and electronic records, including email in support of applicable regulation, standards and contractual requirements? |  |  |
| Is there a documented process to identify and assess regulatory changes that could significantly affect the delivery of products and services? |  |  |
| Are policies and procedures in place to restrict activities or transactions for sanctioned countries e.g., country blocking? |  |  |
| Are audits performed to ensure compliance with applicable statutory, regulatory, contractual or industry requirements? |  |  |
| **Privacy** | Is there a documented privacy policy and are procedures maintained for the protection of client information? |  |  |
| Are you collect, access, process, disclosure of, or retention of client scoped data that includes any classification of personal information or personal data of individuals? |  |  |
| Is there a designated organizational structure or function responsible for data privacy or data protection as it relates to client scoped data? |  |  |
| Is documentation of data flows and/or data inventories maintained for client scoped data based on data or information classification? |  |  |
| Are regular privacy impact risk assessments conducted? |  |  |
| **Cloud** | Are you providing the cloud Services? If yes, what service model is provided? (SAAS, PAAS, IAAS). |  |  |
| Is there a management approved process to ensure that backup image snapshots containing Scoped Data are authorized by Outsourcer prior to being snapped? |  |  |
| Are backup image snapshots containing Scoped Data stored in an environment where the security controls protecting them are commensurate with the production environment? |  |  |
| Is data segmentation and separation capability between clients provided? If yes, how is this implemented? |  |  |
| Is Scoped Data encrypted? If yes, In which states it is encrypted. |  |  |
| Is there a cloud audit program to address client audit and assessment requirements? |  |  |

# Security Testing HIGH

Penetration tests are performed by internal staff

NO

Penetration tests are performed by a third party

YES

Date of the most recent test

7/5/2020

Scope of penetration testing

Externally-facing networks.

Frequency of penetration testing

Annually

If other:

Medium and higher findings are remediated timely

NO

Planned remediation date from last test  Results were reviewed by Senior management

-

YES

Social engineering or phishing performed

NO

Frequency of social engineering testing

Application security tests are performed by internal staff

Application security tests are performed by a third party

Medium and higher findings are remediated timely

No Testing Performed

If other:

YES

NO

Planned remediation date from last test  Results were reviewed by senior management

NO

-

NO



## Gap Analysis



**Domain Name**

**Gap Analysis**

|  |  |
| --- | --- |
| Risk Management |  |
| Information Security Policies |  |
| Organization of Information Security |  |
| Human Resource Security |  |
| Asset Management |  |
| Access Control |  |
| Physical and Environmental Security |  |
| Operations Security |  |
| Communications Security |  |
| System Acquisition, Development, and Maintenance |  |
| Third Party Risk |  |
| Information Security Incident Management |  |
| Business Continuity Management |  |
| Compliance |  |
| Privacy |  |
| Cloud |  |

[www.beaconer.io](http://www.beaconer.io/) Confidential |12