



# Security and Privacy Assessment Report




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

**Security Testing**

✓ Penetration Testing

✗ Defined Remediation Process


✗ Tested Within Last 12 Months

**Information Security**

✓ Data is Encrypted

✗ Server/Network Security


✓ Password Policies

**Third-Party Reviews**

✓ SOC Provided

✓ SOC Unqualified


✓ Other Third-Party Audit Provided

**Data Privacy**

✓ Privacy Policy

✓ Exempt Individual Data


✓ Breach Notification

**Resiliency**

✗ Infrastructure

✗ Monitoring/Maintenance


✗ Backup Practices

**Physical Security**

✓ Electronic Access Control

✓ Access Reviews


✗ Security Cameras

**Information Security Governance**

✓ Info Security Policy

✗ Asset Management

✓ Employee Security

**Business Continuity**

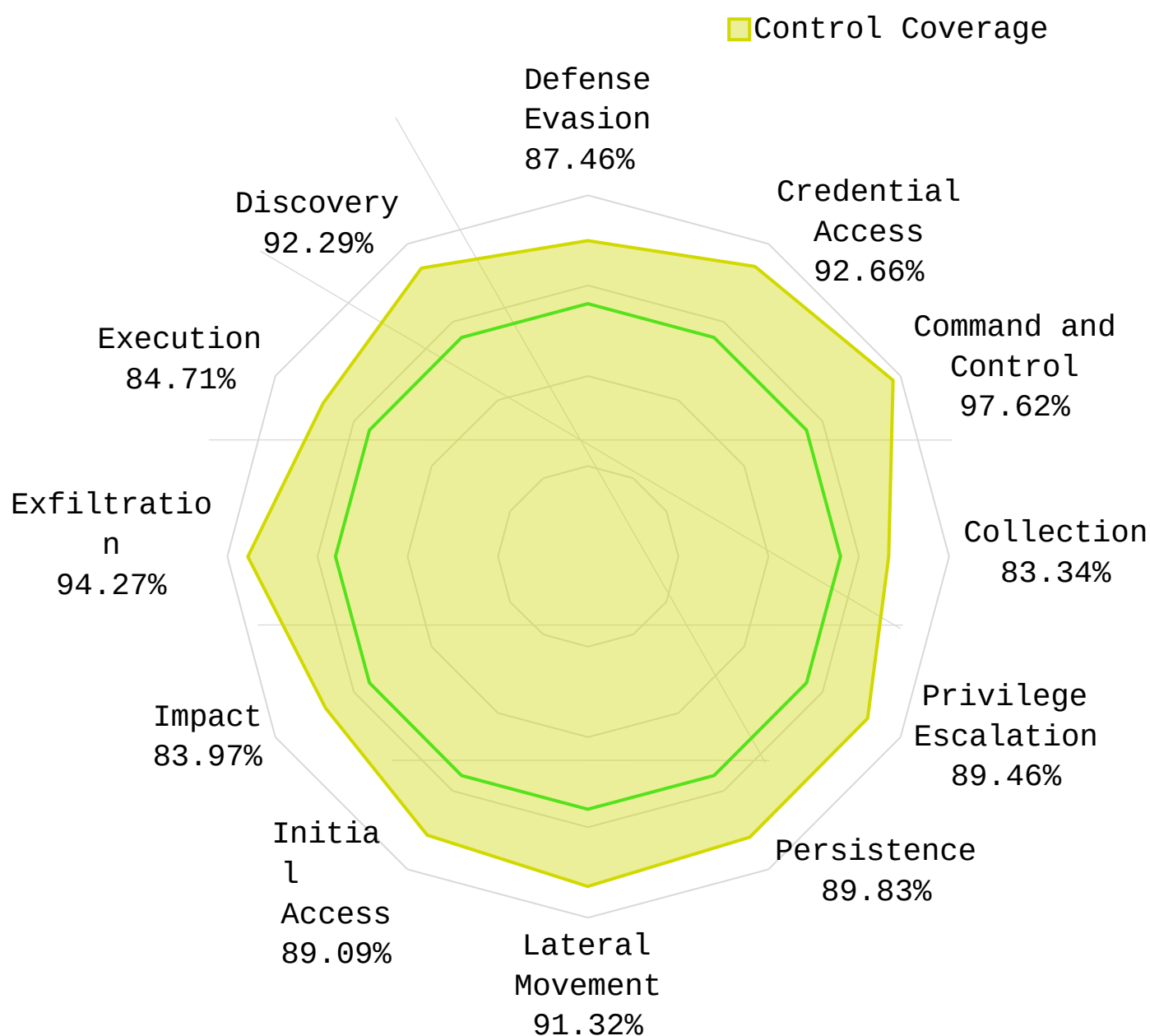
✓ Vendor Maintains a BCP

✓ 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.



# Beaconer Matching Report

Domain	Question	Response	Risk
<b>Risk Management</b>	Is there a formalized risk governance plan in place?	Yes	
	Is there a formalized Risk Assessment process in place?	Yes	
	Is there a process to identify and manage the risk response and treatment of risks?	Yes	
	Is there a formal Risk Exception process for the Risk Business decided to accept?	Yes	

Domain	Question	Response	Risk
<b>Information security Policies</b>	Is there a set of information security policies in place?	No	
	Have all policies been assigned to an owner responsible for review and approved periodically?	Yes	
	Have all information security policies and standards been reviewed in the last 12 months?	Yes	
	Is there a process to approve exceptions to the established security policies?	Yes	

Domain	Question	Response	Risk
<b>Organization of Information Security</b>	Is there a respondent information security function responsible for security initiatives?	Yes	

Domain	Question	Response	Risk
<b>Human Resource Security</b>	Are Human Resource policies in place?	Yes	
	Do HR policies include background checks on employees including criminal screening?	No	
	Does security awareness training program including new hire in place?	Yes	
	Does the HR policy includes a disciplinary process for Non-compliance?	Yes	

Domain	Question	Response	Risk
<b>Asset Management</b>	Is there an Asset management program or policy in place?	No	
	Do all projects involving Scoped Systems and Data go through some form of information security assessment?	Yes	
	Is there an asset Inventory list or configuration management Database (CMDB) in place?	Yes	
	Do you have a process to remove the client information prior to decommissioning or reuse of equipment with client information?	No	

Domain	Question	Response	Risk
<b>Access Control</b>	Is there an access control program or policy in place?	No	
	Are unique IDs required for authentication to applications, operating systems, databases and network devices?	Yes	
	Is access to applications, operating systems, databases, and network devices provisioned according to the principle of least privilege?	Yes	
	Is there segregation of duties for granting access and approving access to Scoped Systems and Data?	No	
	Does the password policy define specific length and complexity requirements for passwords?	Yes	

Domain	Question	Response	Risk
<b>Physical and Environmental</b>	Is there a physical security program in place?	No	
	Are there physical security controls in place for all secured facilities e.g., data centers, office buildings?	Yes	

<b>Security</b>	Do the physical security controls include electronic controlled access system (key card, token, fob, biometric reader, etc.)?	Yes	
	Are there environmental controls in secured facilities to protect computers and other physical assets e.g., Fire detection and suppression?	Yes	
	Are visitors permitted in the facility? If yes, are they escorted all the time?	Yes	

Domain	Question	Response	Risk
<b>Communication and Operations Management</b>	Are management approved operating procedures utilized?	Yes	
	Is there an operational change management/change control policy in place?	Yes	
	Does the change control process to ensure clients are notified prior to changes being made which may impact their service?	Yes	
	Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?	No	

Domain	Question	Response	Risk
<b>System Acquisition, Development, and Maintenance</b>	Is there a formal Software Development Life Cycle (SDLC) process in place?	Yes	
	Is there a formal Secure software development lifecycle policy in place?	Yes	
	Are Applications used to transmit, process or store Scoped Data?	Yes	
	Are Outside development resources utilized?	Yes	
	Are Web applications configured to follow best practices or security guidelines e.g., OWASP?	Not Available	
	Is there a documented change management /change control process for applications with Scoped Data?	Yes	

Domain	Question	Response	Risk
--------	----------	----------	------

<b>Third-Party</b>	Is there a documented third party risk management program in place?	Yes	
	Do Subcontractors have access to scoped systems and data or processing facilities?	No	
	Does the TPRM program require Confidentiality and/or Non-Disclosure Agreements & Data Breach Notification from Subcontractors?	Yes	
	Are background checks performed for Service Provider Contractors and Subcontractors?	No	

Domain	Question	Response	Risk
<b>Information Security Incident Management</b>	Is there an established incident management program in place?	No	
	Is there a formal Incident Response Plan in place?	Yes	
	Does the Incident Response Plan include guidance for escalation procedure & actions to be taken in the event of an information security event?	Yes	
	Does regular security monitoring include malware activity alerts such as uncleaned infections and suspicious activity?	Not Available	

Domain	Question	Response	Risk
<b>Business Continuity Management</b>	Is there an established business resiliency program in place?	Yes	
	Is there a periodic (at least annual) review of your Business Resiliency procedures?	No	
	Are formal business continuity procedures developed and documented?	Yes	
	Is there a formal, documented Information Technology Disaster Recovery exercise and testing program in place?	No	
	Was RTO & RPOs achieved during the last DR test?	Yes	

Domain	Question	Response	Risk
<b>Compliance</b>	Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements?	Yes	
	Is there a records retention policy covering paper and electronic records, including email in support of applicable regulation, standards and contractual requirements?	Yes	
	Is there a documented process to identify and assess regulatory changes that could	No	





	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?	Not Available	
	Are audits performed to ensure compliance with applicable statutory, regulatory, contractual or industry requirements?	Yes	

Domain	Question	Response	Risk
Privacy	Is there a documented privacy policy and are procedures maintained for the protection of client information?	Not Answered	
	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?	No	
	Is there a designated organizational structure or function responsible for data privacy or data protection as it relates to client scoped data?	Yes	
	Is documentation of data flows and/or data inventories maintained for client scoped data based on data or information classification?	Yes	
	Are regular privacy impact risk assessments conducted?	Yes	



Domain	Question	Response	Risk
Cloud	Are you providing the cloud Services? If yes, what service model is provided? (SAAS, PAAS, IAAS).	Yes	
	Is there a management approved process to ensure that backup image snapshots containing Scoped Data are authorized by Outsourcer prior to being snapped?	No	
	Are backup image snapshots containing Scoped Data stored in an environment where the security controls protecting them are commensurate with the production environment?	No	
	Is data segmentation and separation capability between clients provided? If yes, how is this implemented?	Yes	
	Is Scoped Data encrypted? If yes, In which states it is encrypted.	Yes	
	Is there a cloud audit program to address client audit and assessment requirements?	No	

## Security Testing

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	Medium and higher findings are remediated timely No Testing Performed
Application security tests are performed by internal staff	If other:
Application security tests are performed by a third party	NO
Planned remediation date from last test	 -
Results were reviewed by senior management	NO YES



# Gap Analysis

Domain Name	Gap Analysis
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	