



MALDIVES
INLAND REVENUE
AUTHORITY

މުވާދިއާ ސަބަބު

1. ބުނާ ގުޅުމުގެ ތަވާރު		
(IUL)220-AS/1/2022/93	ސަފުޅާ ސަބަބު	1.1. 1.1 އިދާރާތަކުން
13 ސެޕްޓެމްބަރު 2022	އިދާރާތަކުން ނުވަތަ ވިޔަފާރި	
މުވާދިއާ ލިބިގެންނުވާނީ ތަފާތު ވިޔަފާރިތަކުން (މުވާދިއާ ލިބިދާރުކުރުމުގެ ނިންމުމުގެ ތެރޭގައި)	ވިޔަފާރި	1.2. 1.2 އިދާރާތަކުންނާއި ވިޔަފާރިތަކުން
އިދާރާތަކުން، 20379 ގަޑި ސެކަންޑް	ފަލާ ބަލާ	
20 ސެޕްޓެމްބަރު 2022	ވިޔަފާރި	ވިޔަފާރި
15:00	މުވާދިއާ	
ހުޅުވާ ފަންވަތް 1 ގެ ފުރުޞަތު ހުޅުވާން ވާނެ އިދާރާތަކުން		1.3 1.3 ފަލާ ބަލާ ކުޅިވަރު
13 ސެޕްޓެމްބަރު 2022		ވިޔަފާރި

2. ހުޅުވާން ވާނެ ފަންވަތް	
މުވާދިއާ ލިބިދާރުކުރުމުގެ ނިންމުމުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 1 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ.	2.1
ބުނާ ގުޅުމުގެ ތަވާރު ހުޅުވާން ވާނެ ފަންވަތުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 1 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ. procurement@mira.gov.mv އަށް ފޮނުއްވާ ފުރުޞަތު ހުޅުވާން ވާނެ ފަންވަތުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 3020478 / 3339513 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ.	2.2
ވިޔަފާރިތަކުން ވިޔަފާރިތަކުން ހުޅުވާ ފަންވަތުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 1 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ.	2.3
ވިޔަފާރިތަކުން ވިޔަފާރިތަކުން ހުޅުވާ ފަންވަތުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 1 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ.	2.4
ވިޔަފާރިތަކުން ވިޔަފާރިތަކުން ހުޅުވާ ފަންވަތުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 1 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ. 01 (އެއް) ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ.	2.5
ވިޔަފާރިތަކުން ވިޔަފާރިތަކުން ހުޅުވާ ފަންވަތުގެ ތެރޭގައި ބައިވެރިވާން ޖެހޭ ފުރުޞަތު ހުޅުވާ ގޮތަށް ހުޅުވާނީ 1 ގެ ފަންވަތުގެ ތެރޭގައި ބަޔާންކޮށްފައިވާ ގޮތެކެވެ.	2.6



Required item: [XDR Solution](#)

Requirements		Comply/Does not Comply
Agent Coverage	Solution must be compatible with the following operating systems: Windows (32-bit & 64-bit) 8, 8.1, 10 and 11, Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022	
Attack Surface Discovery & Detection	Solution should have the ability to discover communicating applications.	
	Solution should have the ability to detect IOT devices on the same network where the installed agents are located.	
	Solution should have the ability to display detailed information about detected devices such as: IP address, Name, MAC Addresses, Model, Location.	
	Solution should have the ability to detect workstations and servers in the organizational network that are not protected with an EDR agent.	
	Solution should provide off-network detection to detect potentially malicious activity when not connected to the corporate network.	
	Solution should Detect running processes, process starts, process stops, and cross process interaction.	
	Solution should provide command line visibility.	
	Solution should detect malicious registry changes	
	Solution should Detect suspicious activity associated with DLLs.	
	Solution should Incorporate MITRE ATT&CK technique into detection scheme.	
	Solution should detect known malicious activity.	
	Solution should detect connections established on the network from the protected device.	
	Solution should detect Suspicious user and workstation behavior	



Prevention	Solution should detect changes made by malicious processes in the registry keys of the workstation.	
	Solution should Prevent execution of malicious files, DLLs, or applications utilizing both Machine Learning (ML) and signature-based detection.	
	Solution should have the ability to load the indicators of Compromise (IOC) such as bad IP address, domain, file name, file hash, etc. for threat search.	
	Solution should identify known malicious activity.	
	Solution should have the ability to prevent malicious file execution.	
	Solution should have the ability to block/allow USB devices and Bluetooth devices.	
	Solution should block malicious traffic from data exfiltration (data leakage).	
	Solution should prevent from ransomware and modification of files or device records.	
	Solution should have the ability to receive daily threat detection intelligence updates	
	Solution should have the ability to whitelist/blacklist based on hash files.	
	Solution should support deployment in simulation mode in such a way that no blocking is performed but that all malicious activity is recorded.	
	The solution should support the False Positives reclassification ability to flag activity as false positives and prevent similar detections from re-occurring.	
	Solution should provide the real time containment.	
	Solution should provide isolation of endpoints from the network.	
Solution should allow periodic tracking of the files contained in the device with the agent installed.		
Diffusion	Solution should allow the automatic blocking of a device where malware-caused activity has been found.	
	Solution should allow the blocking of activities carried out by malicious files.	
	Solution should have the ability to create Whitelist/Blacklist for applications based on their name, version, and provider.	
	Solution should Allow to defuse malicious network activity to Prevent internal or external malicious connection establishment.	
	Solution should Allow to defuse malicious file activity to Prevent malicious file tampering (create, delete, or modify).	



Investigations	Solution should have the full process data collection at all times to collect any process/thread/library/driver related activities (creation, termination, start or load)	
	Solution should be able to collect full file data all the time which includes ability to collect any file related activities (creation, read, write, rename or delete)	
	Solution should be able to collect any network related activities such as socket accept/close etc.	
	Solution should be able to have ability to collect any registry related activities (key value, create, delete or rename)	
	Solution should have the ability to create custom classified rules based on threat hunting collected data.	
	Solution should allow to detect known techniques over raw normalized data such as lateral movement, extended privilege escalation, log deletion, scheduled tasks, startup tampering, memory violations, commands and arguments spoofing etc.	
	Solution should have the Data available for endpoints for a minimum of 10 days.	
	Solution should have Syslog available for SIEM integration.	
	Solution should have the ability to terminate processes remotely.	
	Solution should provide ransomware prevention policy and behavioral analysis offer real-time automated prevention of ransomware encryption.	
Incident Response	Solution should have the ability to kill process based on predefined activity classification.	
	Solution should have the ability to terminate a process based on its classification.	
	Solution should have the ability to delete a file based on the classification of the same	
	Solution should have ability to remove file based on predefined activity classification.	
	Solution should have the ability to restrict device accessibility based on predefined activity classification.	
	Solution should provide complete visibility into the chain of attacks and malicious modifications	
	Solution should allow automatic cleaning of devices and reverse malicious modifications while maintaining the availability of the affected device.	
	Solution should provide Orchestrated and Automated response in Real time	



XDR Functionality	Solution should have a set of AI based rules to support the Extended detection functionality.	
	Solution should provide automated playbook investigation.	
	Solution should provide automated remediation.	
Vulnerability Assessment and Patching	Solution should have the ability to create policies to prevent communication over the network based on application.	
	Solution should detect and identify all applications on devices that communicate over the network Including vulnerable applications.	
Management and Integration	Solution should comply with common security requirements (PCI DSS, HIPAA etc)	
	Solution should allow integration with Active Directory to ensure compliance with the requirements of your organization's password policies.	
	The solution administration console should allow integration with an external SMTP service for sending alerts via electronic mail.	
	The solution administration console should allow the use of access roles in a granular manner, with different access levels for administrators	
	The solution must support standardized and customizable reports.	
	The solution administration console should allow auditing of changes made by administrators/operators.	
Global Support & Service Offerings	Technical support by phone, web, and email	
	In-product resource center / Support portal access	
	Include an onboarding service for monitoring and fine-tuning of critical assets/resources.	
	Standard 8x5 Technical Support	
Implementation	Setup and Implementation of XDR Solution	
No. of Users	400	

- Must include vender authorization letter
- Must include 1-year license (if any)
- Must provide vendor certified overseas training x3
- Must provide the initial configuration and setup
- Must **clearly provide yearly subscription price separately**
- Must fill the comply/does not comply column when submitting the bid
- Solution must be a leader in the most recent Gartner report for Endpoint Protection Category

Evaluation Criteria

Price 100%
Delivery 30 Day



2: ދަފުޅުތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން

ދަފުހެތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން		
6.1	ދަފުހެތަކުގެ މަޢުލޫމާތު (އަޢުލާކުރުން) ގައި ބަޔާންކޮށްފައިވާ ފަޢަލުތަކުގެ ސަބަބުން ލިބިގެންވާ ކަންކަން ބަޔާންކުރުން	1
6.2	ކަނޑުވަނުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު / ޓަކުކުރުމުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން	2
6.3	ކަނޑުވަނުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން	3
6.5	ކަނޑުވަނުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން (އަޢުލާކުރުން) ގައި ބަޔާންކޮށްފައިވާ ކަންކަން ބަޔާންކުރުން	5
6.6	ކަނޑުވަނުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން (މިއަހަރުގެ 3 ވަނަ ދަފުހެ).	6
6.7	ކަނޑުވަނުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު ވިދާޅުކުރުން (މިއަހަރުގެ ދަފުހެތަކުގެ މަޢުލޫމާތު).	7



ދިވެހިރާއްޖޭގެ ބޭނުންކުރާ ސަރުކާރުގެ ގެޒެޓް (ބޭނުންކުރާ ސަރުކާރުގެ ގެޒެޓް) ގައި 2023

WHEREAS,[name of Bidder] (hereinafter called “the Bidder”) has submitted his Bid for the Project no.....issued by the Maldives Inland Revenue Authority onfor construction of[name of Contract] (hereinafter called “the Bid”).

KNOW ALL PEOPLE by these presents that We [name of Bank] of [name of country] having our registered office at (hereinafter called “the Bank”) are bound unto[name of Purchaser] (hereinafter called “the Purchaser”) in the sum of *..... for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents.

SEALED with the Common Seal of the said Bank thisday of20.....

THE CONDITIONS of this obligation are:

- (1) If, after Bid opening, the Bidder withdraws his Bid during the period of Bid validity specified in the Form of Bid; or
- (2) If the Bidder having been notified of the acceptance of his Bid by the Purchaser during the period of Bid validity:
 - (a) fails or refuses to execute the Form of Agreement in accordance with the Instructions to Bidders, if required; or
 - (b) fails or refuses to furnish the Performance Security, in accordance with the Instruction to Bidders; or
 - (c) does not accept the correction of the Bid Price pursuant to Clause 27,

* The Bidder should insert the amount of the Guarantee in words and figures denominated in Maldivian Rufiyaa. This figure should be the same as shown in Clause 16.1 of the Instructions to Bidders.

we undertake to pay to the Purchaser up to the above amount upon receipt of his first written demand, without the Purchaser’s having to substantiate his demand, provided that in his demand the Purchaser will note that the amount claimed by him is due to him owing to the occurrence of one or any of the three conditions, specifying the occurred condition or conditions.

This Guarantee will remain in force up to and including the date days after the deadline for submission of bids as such deadline is stated in the Instructions to Bidders or as it may be extended by the Purchaser, notice of which extension(s) to the Bank is hereby waived. Any demand in respect of this Guarantee should reach the Bank not later than the above date.

DATE..... SIGNATURE OF THE BANK
 WITNESS SEAL
 [signature, name, and address]