

Tender Fee: Rs. 5,000/-  
(Non-Refundable)

## TENDER FORM

### Tender # IT/29/23-24 Provide and Supply Network Anti-APT Solution

Date of Issue : April 17, 2024  
Last Date of Submission : May 10, 2024 (3:00 PM)  
Date of Opening of Tender : May 10, 2024 (3:30 PM)

Company Name: Securic Systems

NTN: 7547400-0, SRB Registration Number: 57547400-0

GST Registration Number: 4240197559687

Pay Order / Demand Draft # 00006320, Dated: 09-May-2024

Amount of Rs. 1,70,000/-, Drawn on Bank: Bank Alfalah





**8. Bill of Quantity**

Quoted Brand: Trend Micro  
 Quoted Model: XDR for Networks + XDR

Sr #	Description	Qty	Amount
1	<p><b>Network Anti-APT Solution &amp; NDR</b>                      Network Sensor for XDR 500                      500 Mbps Virtual Appliance                      Features:</p> <ul style="list-style-type: none"> <li>• Leader in Forrester Wave Network Analytics report</li> <li>• Integration with existing implemented solution of Trend Micro XDR platform.</li> <li>• Behaviour detection capabilities, traffic and object analyses.</li> <li>• Inspect up to 500 Mbps of traffic irrespective of users involved.</li> <li>• Support 90+ protocols including SMB for lateral movement detection (must share list of all protocols)</li> <li>• Sandbox solution must not be detectable by malware to avoid evasion</li> <li>• Network and Document exploit detections</li> <li>• Feature to analyse scripts</li> <li>• Remain completely invisible to both the end user as well as the attacking website.</li> <li>• Detect rootkits.</li> <li>• Handle DLL injections.</li> <li>• Accurately identify malware and maintain a very low false-positive rate.</li> <li>• Utilize XFF headers to identify the client machine generating the alerts when deployed in front of a proxy server.</li> <li>• Display the geo-location of the remote command and control server(s) when possible.</li> <li>• Report the Source, Destination, Detection Name, Detection Severity and Protocol.</li> <li>• Detect potential malicious network traffic, such as DNS queries to Botnet C&amp;Cs.</li> <li>• Monitor SMTP Traffic.</li> <li>• Integrate with the investigation platform to perform threat hunting and investigation.</li> <li>• Signature-based and advanced detection technologies Machine Learning, AI and behavior monitoring.</li> <li>• Cloud offering to monitor all users.</li> <li>• Support for Zero Trust model</li> </ul>	1 Job	2,521,566.92

MIRZA MUDASSIR BAIG  
 Member PC-B  
 Sr. Exec Finance, IBA Karachi

MANSOOR ALI  
 Member PC-B  
 Manager IT, IBA Karachi



Stamp and Signature


SHAH AB UDDIN KHAN  
 Member PC-B  
 Manager Admin, IBA Karachi

MUHAMMAD HANIF  
 Member PC-B  
 Sr. Exec Purchase, IBA Karachi

MUHAMMAD NAVEED AKHYAR  
 External Member PC-B  
 Chief Accounts Officer,  
 KIBGE, University Of Karachi

OSAMA A. QAYOOM  
 External Member PC-B  
 Head of Biomedical Engineering  
 Department, Dow University

MUHAMMAD ANWAR  
 Chairperson PC-B  
 Chief Librarian, Karachi

<ul style="list-style-type: none"> <li>• Threat intelligence platform</li> <li>• Run security playbooks on particular alerts to isolate compromised endpoints or block suspicious hash, IP, URL and domain.</li> <li>• Automatically discover exploitable vulnerabilities for both internal assets and assets exposed to the Internet.</li> <li>• Discover public assets, and identify available services and open ports.</li> <li>• Discover service accounts mapped with their risk scores.</li> <li>• Integration with Sangfor NGAF and third-party tools.</li> <li>• Integrate with MISP for both ingesting intelligence feeds and sharing suspicious objects like hash, IP, URL and domain..</li> <li>• Zero Trust capability to block access to specific internal applications or specific Internet resources based on user and device risk</li> <li>• Perform the following response action with XDR:             <ul style="list-style-type: none"> <li>• Disable/Enable user account</li> <li>• Force password reset</li> <li>• Collect file Dump process memory</li> <li>• Run remote custom script</li> <li>• Take remote shell of Linux and Windows systems.</li> </ul> </li> <li>• Port scan and detecting reconnaissance scan using Firewall feature.</li> <li>• Device-based risk visibility.</li> <li>• User-based risk visibility.</li> <li>• Disable and enable user accounts remotely.</li> <li>• Force user account password reset.</li> <li>• Gather hardware and OS information of the managed system.</li> <li>• Collect Windows Event Log, including RDP, Security, System etc.</li> <li>• Collect auto-start entries, scheduled tasks, services etc.</li> <li>• Showcase information resources for active threats and threat actors.</li> <li>• Showcase leveraging valuable indicators of potential threats from both custom and curated intelligence reports for auto and manual sweeping.</li> <li>• Integration with TAXII feeds.</li> <li>• Create incidents to group related workbench alerts</li> <li>• Analyse the URL in the sandbox</li> <li>• Collect the file and send it to the sandbox for analysis</li> <li>• Detect exploitable vulnerabilities in the managed systems</li> <li>• Detect weak authentication in Azure / AD</li> <li>• Detect stale accounts in Azure / AD</li> <li>• Detect extra admin accounts in Azure / AD</li> <li>• Dashboard and reporting</li> <li>• Integration with SIEM</li> </ul>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------


  
**MIRZA MUDASSIR BAIG**  
 Member PC-B  
 Sr Exec Finance, IBA Karachi

  
**MANSOOR ALI**  
 Member PC-B  
 Manager IT, IBA Karachi

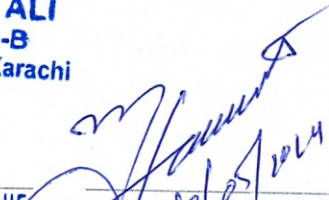





Stamp and Signature

  
**SHAH AB UDDIN KHAN**  
 Member PC-B  
 Manager Admin, IBA Karachi

  
**MUHAMMAD HANIF**  
 Member PC-B  
 Sr. Exec Purchase, IBA Karachi

  
**MUHAMMAD NAVEED AKHTAR**  
 External Member PC-B  
 Chief Accounts Officer,  
 KIBGE, University Of Karachi

  
**OSAMA A. QAYOOM**  
 External Member PC-B  
 Head of Biomedical Engineering  
 Department, Dow University

  
**MUHAMMAD ANWAR**  
 Chairperson PC-B  
 Chief Librarian, Karachi

Sr #	Description	Qty	Amount
2.	<p><b>Network Managed Services &amp; Response</b></p> <p>Managed XDR for Networks</p> <p><u>Features:</u></p> <ul style="list-style-type: none"> <li>• MDR services for 500 Mbps</li> <li>• 24x7x365 Alert Investigator, Incident Responder, Threat Hunter/Forensic, Analyst and SOC Manager at their local/regional/ international locations to ensure Purchase services are monitored and remotely managed vigorously.</li> <li>• Advanced threat assessment and intelligence:                             <ul style="list-style-type: none"> <li>a) Identify, isolate, and investigate indicators of compromise (IOCs) before damage can occur</li> <li>b) Correlate security events with Threat Intelligence to prioritize response efforts</li> <li>c) Gain essential insight into attackers' intent as well as techniques</li> <li>d) Respond to emerging threats through a detailed incident management approach.</li> </ul> </li> <li>• Uses Machine and Human Elements to Analyse Millions of Events in Real-Time.</li> <li>• Continuous threat hunting of in-scope assets.</li> <li>• Creation of Incident Playbooks.</li> <li>• Complete security to the organization network, and its systems against All/any threat, including but not limited to (cyber-attacks, hacking, data lost due to viruses, ransomware attacks, bugs, security breaches, gaining unauthorized access to the organization network etc).</li> <li>• Monthly and quarterly reporting demonstrating the summarized view of catered alerts/offences/incidents detected in each month from the Management Perspective.</li> <li>• Investigation and response proactive outreach including IoC sweeping.</li> <li>• Round-the-clock managed protection against modern evasive threats.</li> <li>• Visibility across your entire network, analysing network traffic and hunting for threats.</li> <li>• Include IOA hunting</li> <li>• Full picture of the attack across the entire enterprise</li> <li>• Root cause analysis, attack vector, dwell time, spread, and impact.</li> <li>• Include impact analysis and response guidance.</li> </ul>	1 Job	₹ 8,79,194.91
<b>Total</b>			₹ 200,762.83
<b>13% SST (if applicable)</b>			936,099.04
<b>18% GST (if applicable)</b>			—
<b>Grand Total</b>			8,136,860.87

**Grand Total Amount (Rupees in words)** Eight Million One Hundred Thirty Six Thousand Eight Hundred Sixty and Eighty-seven Hundredths.

MIRZA MUDASSIR BAIG  
Member PC-B  
Sr. Exec Finance, IBA Karachi

*(Signature)*  
MANSCOR ALI  
Member PC-B  
Manager IT, IBA Karachi



SHAH ABUDDIN KHAN  
Member PC-B  
Manager Admin, IBA Karachi

*(Signature)*  
MUHAMMAD HANIF  
Member PC-B  
External Member PC-B  
Chief Accounts Officer,  
KIBGE, University Of Karachi

*(Signature)*  
Stamp and Signature

MUHAMMAD ANWAR  
Chairperson PC-B  
Chief Librarian, Karachi

OSAMA A. QAYOUM  
Member PC-B  
Department of Engineering  
University of Sindh