Appendix 2
SUBSCRIPTION SUPPORT AND SERVICE LEVEL POLICY

I. SUPPORT.

Support is available for the Service indicated on an applicable Order Schedule (the "Service") for the Subscription Term set forth therein. Requests for Support should be submitted to COMPANY Support through COMPANY's email address support@threatmate.com. Upon request a Slack channel will be created for the CUSTOMER which will allow for live chat with the COMPANY support group.

CUSTOMER will designate up to three (3) key contacts for the reporting and coordination of support requests (the "Business Administrators"). CUSTOMER may change the Business Administrators upon days prior written notice to COMPANY.

Support is available 9 a.m. through 6 p.m. ET, Monday-Friday, excluding COMPANY holidays, except as noted in the Support Response Times table below.

Support includes the following:

- Knowledgebase
- Email support
- Messaging service live chat support
- Upgrades, Updates, Patches generally made available to COMPANY's other support customers
- Hotfixes
- Performance Troubleshooting

Support is provided in the English language only.

II. SEVERITY LEVELS AND INCIDENT RESPONSE.

When starting a Support email or messaging live chat request, CUSTOMER must 1) provide COMPANY with all information necessary for COMPANY to process the request and 2) respond promptly to COMPANY with any information reasonably requested to clarify the support request and 3) provide COMPANY the necessary internal access to servers in order to troubleshoot the reported issue.

Upon starting a Support email or live chat request within operating hours, the next available COMPANY Support Engineer will respond.

If the support issue cannot be resolved via email or live chat, COMPANY will create an internal support ticket and provide continued communication based on the resolution progress. Additional video conference meetings can be scheduled in order to assist the COMPANY with resolving the support request. The severity of all Support tickets is based on the definitions provided below.

Incidents are escalated as necessary through the COMPANY Support organization, ending, if necessary, with COMPANY's Chief Technology Officer.

Support Severity Definitions

Severity	Definition
Urgent (Severity 1)	Production / Mission Critical functionality is down with no obvious or immediate workaround.

High (Severity 2)	Major loss of functionality, but can still continue in a degraded or restricted capacity. Not viable long term.
Normal (Severity 3)	Production issue where minor functionality is impacted, a development issue, or non-production outage.
Low (Severity 4)	Non-critical loss of functionality. Request for information or other non-production requests.

Support Ticket Response Times

	Urgent (Severity 1)	High (Severity 2)	Normal (Severity 3)	Low (Severity 4)
Initial Response 24 x 7	8 hours (email)	8 hours (email)	next business day (email)	Next business day (email)
Status Updates	every business day	every business day	every 5 business days	every 7 business days
COMPANY Responsibility	Resources available Monday Friday during local business hours until a workaround or resolution is achieved. Senior management immediately notified.	Resources available Monday Friday during local business hours until a workaround or resolution is achieved.	Resources available Monday Friday during local business hours until a workaround or resolution is achieved.	Resources available Monday Friday during local business hours until a workaround or resolution is achieved.
CUSTOMER Responsibility	Resource available Monday-Friday during local business hours to provide diagnostics to COMPANY as needed.	Resource available Monday-Friday during local business hours to provide diagnostics to COMPANY as needed.	Resource available Monday-Friday during local business hours to provide diagnostics to COMPANY as needed.	Resource available Monday-Friday during local business hours to provide diagnostics to COMPANY as needed.

III. SUPPORT EXCEPTIONS.

COMPANY has no obligation to address a Service issue if

(i) caused by CUSTOMER's negligence;

(ii) caused by unauthorized modifications or enhancements to the Service made by CUSTOMER;

(iii) CUSTOMER fails to utilize a patch, correction or an update which addresses the issue;

(iv) arising from a CUSTOMER's or a third party's system or environment or a third party product or service.

(v) identified by a CUSTOMER's vulnerability scanning, penetration testing or other security tool.

Issues outside the scope of this Support Policy may be addressed upon the request of CUSTOMER at COMPANY's professional services rates then in effect.

IV. MAINTENANCE.

COMPANY may perform maintenance to the equipment, software, hardware and infrastructure comprising the hosting environment for the Service as COMPANY deems necessary. During maintenance, CUSTOMER may not be able to access the Service. COMPANY will maintain at least one page that informs CUSTOMER that maintenance is underway along with an estimate of when the Service will be available for use. For scheduled maintenance, COMPANY will use commercially reasonable efforts to provide reasonable prior notice, conduct maintenance on weekends and between midnight and 6 AM, and keep the frequency and duration of impeded access during the maintenance period to a minimum. Emergency maintenance may be performed without notice to CUSTOMER, though COMPANY will endeavor to provide as much notice as possible.

V. AVAILABILITY.

COMPANY will use commercially reasonable efforts to make the Service available to CUSTOMER twenty four (24) hours a day, seven (7) days per week, three hundred sixty five (365) days per year and attain a Service level availability of 95%, with the exception of service maintenance or in the event of emergencies and circumstances beyond COMPANY's control, including without limitation events of force majeure.

VI. SECURITY MEASURES

COMPANY shall utilize industry standard security measures to protect against the loss, misuse and/or alteration of data located on systems. COMPANY shall conduct vulnerability monitoring in accordance with formally documented vulnerability management processes and procedures.

During the term of the Agreement, COMPANY will utilize code scanning tools to conduct vulnerability assessments. All identified vulnerabilities shall be addressed based upon Common Vulnerabilities and Exposures (CVE) level. COMPANY will make commercially reasonable efforts to prioritize Critical and High vulnerabilities for remediation, when identified by internal scanning tools. Each reported vulnerability shall be verified by COMPANY Data to be valid and applicable, or a false positive.

Medium, Low and Informational criticality vulnerabilities shall be reviewed by the COMPANY Security Team and considered for future remediation, if legitimate, exploitable risk is identified.

COMPANY reserves the right to accept the risk on any identified CVE, at any time and for any reason. Risk acceptance relieves COMPANY Data of vulnerability remediation for that specific CVE.