XM Cyber | See All Ways™

Technical Support Program ("TSP")

1. Introduction

This XM Technical Support Program ("**Technical Support Program**" or "**TSP**") contains all the necessary information detailing the support services provided by XM Cyber Ltd ("**XM**" or "**XM Cyber**") to the customer for the XM Solution as of the commencement date of the customer's paid-up subscription for the XM Solution. Customers that purchased a subscription license for the XM Cyber products as a SaaS solution, are covered under this Technical Support Program for as long as their subscription of the XM solution is in force and is fully paid. Customers that elect to purchase Premium/Elite Services will enjoy superior support services, as described in Table 3A. XM's customer support program is intended to assist customers with any software issues arising from the use of the XM solution. XM's representatives follow comprehensive quality management procedures and continuous training to resolve any software issues promptly.

XM's Technical Support Program relates only to XM's software products installed in a production environment. Third parties' software products are not included in this TSP.

2. Plan Essentials

The support services require customers to grant XM Cyber remote or local access to its network and systems. Giving such access is under the customer's sole control, and the customer acknowledges that XM Cyber will not provide support services if the customer chooses not to grant such access. Any support services and response time shall commence upon giving such access.

3. Support Plans

Customers that license XM Cyber products are covered under this TSP. Customers that elect to purchase Premium/Elite Services will enjoy superior support services, as described below in Table 3A:

3A. **Customer Service Tier:**

Customer Service Tier		Standard	Premium	Elite
Support and Response Time	Fixes, Updates, and Maintainance	V	V	V
	Online Support	9 to 5 Business Service Hours	9 to 5 Business Service Hours	24x7
	SLA - Response Time	Critical - 4 hours High - 8 hours Medium/Low - Next day	Critical - 4 hours High - 8 hours Medium/Low - Next day	Critical - 2 hours High - 4 hours Medium/Low - Next day
	Telephone Support			V
Product Adoption & Enablement	Guided Onboarding	V	V	V
	Access to Customers Portal and XM Academy	V	V	V
	Access to Exposure Room - Live Customer Webinar	V	V	V
	In-depth Training Sessions	V	V	V
Value Realization	Designated Customer Success Manager	V	V	V
	Status Meetings: Periodic Value Delivery calls to review New Features, Security Findings, Trends and Reports	V	V	V
	Cadence Executive Business Reviews	V	V	V
	Roadmap Session with Product Management	Webinar only	V	V
	Annual Value Report		V	V
	XM Executive Sponsor		V	V
	Advisory Workshops		V	V
	Assistance with strategic security projects		V	V
Fully Managed and Operationalized Solution	Designated Exposure Management Analyst		V	V
	EMS Initiate and Track Remediation Process, including Direct Engagement with Remediation Teams (IT/Infra/DevOps etc.)		V	V
	Remediation Validation		V	V
	Monthly Executive Report		V	V

4. Reporting an Error

XM Cyber's representatives shall receive customers' support requests via a dedicated web support portal, detailed with the services' Errors ("**Support Request**"). An "Error" means any verifiable and reproducible material failure of the software to perform the functions described in the software documentation. XM Cyber will respond to such Support Requests based on the severity levels set out in Table 7A below. XM Cyber will use its best efforts to resolve the Error or provide a workaround for the Error.

5. Customer Support Requests Submission

Customers may reach XM Cyber's support center by submitting a Support Request using one of the following ways:

a. Through our Customer Portal at https://customers.xmcyber.com/
b. For Elite customers only – you may call XM Cyber's support line at +1 972 703 2153.

All support cases are logged into the Customer Portal and assigned to the appropriate representatives. After that, your support case will go through the following service flow:

a. Collecting information to help troubleshoot the issue
b. Troubleshooting by XM's support engineer
c. Finding a solution (including workarounds, fixes and patches)
d. Closing the support case.

6. Required information

This section defines the types of information needed for XM Cyber to diagnose the issues and resolve your Support Request quickly. Please

make sure to have the below information readily available before contacting XM Cyber's customer support team.

a. Account Name
b. XM Cyber's module that is relevant to the Support Request
c. The XM Cyber's version you are using
d. Provide the exact wording of the Error messages and relevant screenshots
e. Listing of any output
f. Setup information
g. Any other data that XM Cyber may reasonably request to reproduce operating conditions like those present when the Error occurred
h. Single point of contact for severity 1 Error.

7. Initial Response Time per Service Tier

A case severity level measures the impact of the technical issue on your systems. Accurately defining the problem and its severity ensures a timely and effective response by your XM Cyber's customer support team. The following severity will assist XM Cyber's customer support engineers in assigning the right resources to resolve all technical issues as efficiently as possible. Support response times for all Service Tiers are based on the incident severity and are addressed per the table below.

Table 7A – Technical Support Initial Response Times

Severity Level	Description	Standard / Premium Service Tier	Elite Service Tier
1- Critical	Severe impact to the production environment, such as system downtime or other major technical issues that prevent the customer from using the product.	Up to 4 business hours	Up to 2 business hours
2- High	Software is functioning, but its uses in a production environment are severely reduced.	8 business hours	4 business hours
3- Medium/Low	Partial, non-critical loss of software used in a production environment, but you can continue using it with a workaround.	Next business day	Next business day

8. Escalations:

8.1. The escalation of support matters serves as a critical mechanism to enhance awareness, focus attention, and expedite the resolution of specific issues. It is imperative to emphasize that escalation procedures are exclusively applicable to currently active cases under consideration by XM.

8.2. The designated methodologies for initiating a support escalation procedure are as follows:

8.2.1. Direct Escalation Process:

Escalating an issue by the Customer should be initiated through the Customer Portal by accessing the relevant case, selecting the appropriate reason for the escalation in accordance with the guidelines outlined in Table 8.2 below, and submitting the escalation request.

8.2.2. Email Correspondence to Technical Support:

Should an escalation initiated through the Customer Portal fail to yield a satisfactory resolution, customer should transmit a comprehensive email detailing the escalated case along with all pertinent information to sup-ops@xmcyber.com. Following XM's acknowledgment of the escalation communication, the Technical Support team of XM will engage as soon as reasonably possible without delay to delineate the subsequent steps or strategic plan aimed at promptly resolving the identified issue.

8.3. The escalation reasons are described as follows:

Table 8.2 – Escalation Reasons

Escalation Reason	Description
Communication	• Indicate dissatisfaction with XM Cyber's response or communication frequency concerning the specific issue. • Express concerns regarding the quality of XM Cyber's support services.

Lack of Progress	Highlight prolonged case resolution duration or instances of unmet expectations.
Urgent Issue	Identify issues of substantial business impact necessitating immediate attention for the customer or the affected platform.

9. Exclusions

The support services described in Table 3A will only be provided for the then-current release of the XM solution and shall exclude Errors resulting from the following events (without limitation):

9.1. Failure of the customer to promptly implement software updates and/or upgrades released by XM Cyber.

9.2. Written instructions from XM Cyber that the customer did not implement.

10. Maintenance, Continuity and Resilience Measures

Relevant for SaaS customers only:

10.1. Updates, upgrades, and other system maintenance tasks necessary to secure the proper operation of the XM solution, will be scheduled by XM as needed. Normally, system maintenance will be carried out on Sundays between 12:00 to 13:00 CET. To the extent that system maintenance is carried out at other times, it will be done with minimal disruption to the operation of the system. To the extent possible, XM Cyber will inform the Customer of such system maintenance as early as possible.

10.2. Backup of the data in the XM solution shall be according to the following matrix:

10.2.1. Recovery Time Objective (RTO) - 12 hours (3 days for STACKIT)

Indicating the duration of “real-time” that can pass before the disruption begins to impede regular business operations significantly.

10.2.2. Recovery Point Objective (RPO) - 24 hours

Indicating the variable amount of data (within and up to 24 hours) that may be lost or may require the re-entry during network downtime.

11. Customer Responsibilities

11.1. Customer agrees to receive from XM Cyber communications via email, telephone, and other formats. (e.g., Slack)

11.2. Collaboration of the customer with XM Cyber’s engineers during the provision of Support Request.

11.3. The customer shall report to XM Cyber all problems with the software and shall implement the corrective procedures provided by XM Cyber promptly after receiving such procedures.

12. Exposure Management Services (EMS)

Customers can purchase the EMS add-on (Premium/Elite service tiers) at additional cost. The terms and conditions for the EMS service are attached as Addendum 1 to this TSP.

13. Others

XM Cyber reserves the right to modify this TSP at any time by posting the revised version on XM Cyber's website.

14. Limitation Of Liability

Except as specifically provided for in this TSP, XM extends no warranty, express or implied, including any warranty of merchantability or fitness for a particular purpose, to customer for the services or any other maintenance or

support.

Notwithstanding any other provision of this TSP, under no circumstances shall XM or any of its subcontractors be liable to customer or any third party , for any special, incidental, punitive, indirect or consequential damages as a result of the provision of the TSP.

15. Miscellaneous

15.1. Time Limitation for Action

Any action for breach or to enforce any provision of this TSP shall be brought within two years after the cause of action accrues or it will be deemed waived and barred.

15.2. Non-Cancellable

This TSP is non-cancellable, for SaaS any ongoing program which customer is entitled to for support ends whenever the customer's SaaS subscription ends and for premium services under this TSP, these are purchased for a year in advance, any amount paid by the customer due to this TSP is nonrefundable and non-cancellable.

15.3. Renegotiation of Unenforceable Provisions

If any provision of this TSP is held to be unenforceable or invalid, the remaining provisions shall be given full effect, and the parties shall negotiate, in good faith, a substitute valid provision which most nearly approximates the parties' intent of the unenforceable or invalid provision.

15.4. Severability of Provisions

The provisions of this TSP are severable, and if any provision hereof is held invalid or unenforceable, the remaining provisions of this TSP shall not be affected thereby. Furthermore, failure by either party at any time to require the other party to perform any obligation under this TSP shall not affect the

party's right subsequently to require the other party to perform that obligation.

15.5. Assignment

Customer may not assign its rights to receive XM's support services under this TSP or any of its obligations hereunder without the prior written consent of XM. XM may assign any obligation or order placed under this TSP to an affiliate, subcontractor, or other third party, provided that a comparable quality of service is provided to the customer.

ADDENDUM 1 - EXPOSURE MANAGEMENT SERVICE (EMS)

Customers purchasing Premium/Elite services are entitled to fully managed exposure management services. XM Cyber's Exposure Management Service (EMS) is designed to help organizations worldwide eradicate cyber risk. With the growing threat of cyber-attacks, our team of experts works tirelessly to identify and eliminate attack vectors, ensuring the customer's business is protected from cyber threats. Exposure Management Service (EMS) is available to customers who have purchased XM Cyber's Attack Path Management Platform.

1. What is the XM EMS Service?

The EMS Provides a fully managed and operationalized solution, which includes:

1.1. Designated Exposure Management Analyst (EMA): XM Cyber assigns a designated remediation expert to the customer to ensure that they have a single point of contact for questions or concerns.

1.2. Onboarding: The EMA works closely with the customer's IT and security teams ("fixers" - customer's teams that needs to apply fixes) to understand the customer's processes, infrastructure, applications and systems.

1.3. Assessment: Using the XM Cyber Attack Path Management platform, the EMA will create scenarios and conduct assessment to understand the current security posture of the customer's IT infrastructure and identify existing risk exposures and potential threats.

1.4. Tailored and Practical Remediation Plan: Based on the findings of the initial assessment, the EMA develops a practical and tailored step-by-step

remediation plan that outlines the steps required to address the identified exposures and potential threats.

1.5. Remediation Initiation and Guidance: the EMA will initiate the remediation directly with the "fixers", and will provide step-by-step guidance to implement the remediation plan in a timely and efficient manner.

1.6. Remediation Follow-up and Validation: the EMA provides ongoing monitoring and follow-up the remediation activities until closure. Once remediation is defined closed, the EMA will validate the risk has been mitigated.

1.7. Reporting and Communication: the EMA will provide monthly reports and communication to the customer to keep them informed of the status of their IT security, including exposures or threats that have been identified and remediated, as well as ongoing risks that need to be addressed.

* Stages and processes may vary depending on XM Cyber and the client's needs. Additionally, the remediation plan may need to be updated and modified as new vulnerabilities, exposures, and threats emerge over time.

2. Communication Methods

At our core, effective and ongoing communication is critical to the success of our Exposure Management Service. The process and service mentioned above will be based on the following communication methods:

2.1. Direct communication with non-security teams ('Fixers') performing remediation tasks: Communication with the Fixers will be conducted via a service request using the customer's ticketing system.

2.2. Ticketing System Integration:

2.2.1. Integration with the customer's ticketing system and communicating directly with the relevant fixer's team, i.e. IT/DevOps, etc., to ensure that all communication is monitored, assigning the relevant priority, thus extending the arm of the customer's SecOps/IT team to push remediation tasks.

2.2.2. The integration process will be implemented with the assistance of EMS security experts, as part of the Onboarding. A prerequisite for the integration is installing an XM Cyber Add-On app from the customer's ticketing system (e.g., JIRA).

2.3. Bi-Weekly Calls: XM Cyber EMA will have a video conference (i.e. Zoom, Google Meet etc.) meeting with the customer to review the status of our service, discuss any issues or concerns, and identify areas for improvement.

2.4. Status Updates and Monthly Reports: XM Cyber EMA provides monthly status updates and reports to keep the customer informed of the progress of the security issues that the EMS has identified during that month, thus ensuring the customer has visibility to its security posture and remediation status.

2.5. The following table clarifies the frequency of the provided EMS services:

Service	Description	Frequency
Initial Assessment	XM Cyber EMA will review the findings, assess and prioritize the most pressing security findings	Daily (during Customer's normal business days)
Tailored and Practical Remediation Plan	XM Cyber EMA assign a tailored remediation to findings. XM Cyber EMA will open a corresponding ticket to the relevant handling team (Fixer)	Daily (during Customer's normal business days)
Remediation Assistance	XM Cyber EMA will follow up on each open remediation and will assist in handling the entire remediation process with the Fixers	To be individually agreed on with the customer's Fixers
Service Calls	XM Cyber EMA will have scheduled sessions with the customer (eg. its security team) in case any adjustments in the remediation process are needed	Bi-weekly service calls
Reporting	The customer will be provided with the past calendar month's progress status report	Monthly Executive Report (By the end of the first business week of the next calendar month)
Mitigation Validation	XM Cyber EMA will confirm and validate the risk was indeed mitigated using the XM Cyber	Upon ticket closure/resolution and based on

	Platform	the scenario(s) run and security report

3. Customer Responsibilities

To ensure a successful service, the customer is also responsible and committed to ensuring the success of the Exposure Management Service.

The customer's responsibility and commitment include (without limitation), in particular:

3.1. Providing access to the necessary IT infrastructure, systems, and applications that are required for the XM Cyber security expert to conduct the initial assessment and implement the remediation plan, such as Ticketing System (e.g., JIRA/SNOW, etc.)

3.2. Working closely with the XM Cyber security expert throughout the process, providing timely and accurate information and feedback to ensure the remediation plan is implemented effectively and efficiently.

3.3. Adhering to security policies and procedures established by the customer or the customer's service provider and following best practices for IT security to minimize the risk of potential threats or vulnerabilities.

4. Applicability of EMS service and Exclusions

4.1. The EMS service described in this document will only be provided for XM Cyber Continuous Exposure Management (CEM) Platform which is part of the EMS service. The service is available for CEM and VM customers only.

4.2. The EMS service covers up to 10 remediation teams ("fixers") at a time.