Security FAQ

1. **What kind of security model/compliance frameworks does your organization use?**

   XTM International is ISO 27001 certified. As part of the ISO 27001 requirements, XTM is audited annually by a third-party ISO-27001-certification company. XTM benefits from the NIST security recommendations, CIS Benchmarks, OWASP Top 10 Vulnerabilities list, and MITRE ATT&CK framework.

2. **Do you have a Security Management Program implemented?**

   The XTM Security Program and Policy is the main document containing all high-level policies including data, human resources, physical and environmental security, Disaster Recovery Plan, and Business Continuity Policy. The Risk Assessment Committee meets once a month to discuss incidents, apply or update proper procedures based on reported incidents, and proactively act to identify and mitigate possible risks.

3. **Do you have a Business Continuity / Disaster Recovery Plan in place?**

   XTM has a formally defined DRP which is tested on a regular basis. It includes restoring the whole instance, validation of backup, and recovery processes.

4. **Do you have an incident-response plan in place?**

   XTM International has an information security incident management program that addresses the management of information security incidents and system weaknesses. Incidents include, without limitation: any loss, theft, misuse of or unauthorized access, disclosure, or destruction of any Customer Confidential Information, and any violations or potential violations of federal or state law. XTM has a dedicated channel of communication to report any incidents: incidents@xtm.cloud.

5. **Do you have a data-classification matrix defined?**

   All Customer information is treated as highly confidential regardless of receipt, creation, processing, in-transit, in-storage, and backup media.

6. **Does your company do periodic risk-assessment reviews of the company? How are these performed and with what frequency?**

   XTM has a formal Risk Assessment Committee (RAC). The RAC meets once a month to discuss incidents, apply or update proper procedures based on reported incidents, and proactively act to identify and mitigate possible risks.

7. **How often are information security policies reviewed by your company?**

   XTM reviews policies and procedures at least annually.

8. **Do you conduct penetration tests of your application prior to being delivered?**

   Independent third-party penetration testing of the XTM application is carried out annually by an independent third-party penetration testing specialist company. Penetration testing includes but is not limited to OWASP Top 10 Vulnerabilities. Each new version of XTM undergoes internal penetration testing as part of each new release.

9. **How do you identify vulnerabilities in your environments?**

   XTM uses industry-leading solutions to automatically scan operating systems, networks, and software against vulnerabilities that are evaluated according to severity, and appropriate patches are implemented. The XTM software development team, Systems Admin team, and Security team are tasked with constantly monitoring for information regarding any vulnerabilities of the operating systems and utility software used.

10. **What is your change management process?**

    All change requests must be approved by development management. No new software releases and patches are implemented without a ticket issue being raised. All source code is checked into the software repository and a clean build of the system is produced for testing through the continuous build process. All new software releases are tested by the test department. Once tested and approved, no software can be released to the live servers without the express permission of the development management. All software patches are only implemented by a duly authorized systems administrator. No updates/upgrades are deployed without prior notification (excluding major security updates that require immediate action).

11. **How do you protect your networks?**

    All networks/subnetworks are segmented to be used as production/test/development networks. Firewalls are used and configured to drop needless traffic. All firewall rules are reviewed on a regular basis. XTM follows the least-privilege principle. Access and permissions are applied to particular roles with minimum operational privileges. All services/processes are allowed to communicate within strictly defined traffic rules. Checks are applied to monitor ports and to validate if they meet firewall policies. All device administrative interfaces are configured to apply encryption and authentication methods, are accessible for strictly defined roles, and are hidden behind the VPN. Access to the administrative elements of the devices is possible through a strictly defined separated VLAN.

12. **How do you protect workstations/end users? (e.g.: disk encryption, etc.)**

    All workstations are configured with the baseline security recommendations. Antimalware software is installed and updated on a daily basis. Software installation is strictly managed and monitored. All removable media ports are blocked by default. All disks on workstations are encrypted.

13. **How do you protect access to your systems?**

    XTM implements a Segregation of Duties (SOD) approach to sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Using the SOD approach in key processes, fraud and error risks are far more manageable. To ensure that only authorized individuals are allowed to gain access to business applications, information systems, networks, and computing devices, individual accountability is assured, and authorized users are provided with access privileges that are sufficient to enable them to perform their duties without exceeding their authority.

14. **Do you use 2FA?**

    Yes. XTM uses 2-factor authentication whenever it is supported.

15. **Do you perform security-awareness training?**

    XTM conducts security-awareness training regarding XTM's security requirements for all workers who handle Customer-confidential information, including simulated phishing attacks. XTM also routinely reviews and updates its security awareness training annually.

16. **I have discovered a vulnerability in your system. Who should I contact?**

    Please send a report to **bugbounty@xtm.cloud**. Our team will evaluate it and subsequently give a reward to the person who found it based on its severity and criticality.

17. **What are the locations where XTM data will be processed?**

    In regard to hosted and fully managed servers, XTM allows customers to choose between the main XTM Cloud, which is located in Northern France; XTM US Cloud, which is located in theUnited States;, XTM SOC2 US Cloud, also located in the United States;, or XTM Private Cloud, which can be in any AWS or OVH, or other data centre. The Private Cloud option is single-tenant.

18. **How is physical security managed at your location(s)?**

    All workers in high-risk security zones are trained in the physical security controls designed and applied to their work environment. While in high-risk security zones, all visitors are escorted. The high-risk zones are equipped with intruder alarms and CCTV cameras at all entrances. Access to the high-risk zones is secured by the RFID cards namely assigned to the employees with time scope access restrictions. All entries are logged in the system.

19. **Do you encrypt data in transit?**

    We use TLS 1.2/1.3. No data is transmitted across external networks unencrypted.

20. **Do you encrypt data at rest?**

    We use AWS EBS encryption (AES-256 algorithm) to encrypt data at rest.

21. **Do you perform phishing tests?**

    XTM performs simulated phishing attacks on a regular basis to ensure all of our employees are aware of how to identify spoofed and dangerous messages.