System Description (Section 3)

Company Background

Teramot is a technology company headquartered in Rosario, Argentina, with legal presence in the United States (Delaware). The company specializes in building AI agents that autonomously perform data-driven tasks across multiple channels and enterprise environments. Teramot operates with a distributed, cloud-native architecture. Its primary products include Auto ETL agents built on top of AWS Lambda, DynamoDB, and LLM-based assistants.

Description of services overview or services provided

The Teramot AI Agent Platform enables the deployment of intelligent agents designed to automate real-time conversations and back-office processes. The platform provides a fully serverless stack to configure agents that interact with users over web, WhatsApp, and other channels, using a dynamic memory-driven architecture. The system includes message ingestion, use case management, orchestration of expert agents, and interaction storage. All services are delivered through our infrastructure hosted in AWS, and only the Teramot AI Agent Platform is in scope for this SOC 2 report.

Orchestration of LLM-based Main and Secondary Agents, pIipeline to create AI agents from structured customer input, State machine to control interaction lifecycle and authorization, Integration with messaging channels (WhatsApp, WebApp, Telegram, others), Real-time memory and context management with DynamoDB and S3, Modular bot CLI interface with configurable actions and system queries, AutoETL module to generate data transformation pipelines from customer sources, CI/CD pipelines to deploy agents and monitor usage via GitHub and AWS

Principal service commitments and system requirements

Teramot designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Teramot makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Teramot has established for the services. The system services are subject to the Security commitments established internally for its services.

Teramot communicates its commitments via its Service Level Agreements (SLAs), Privacy Policy, Terms of Service, and client onboarding materials. Additional commitments are detailed in security documentation shared with customers during onboarding.

Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

Components of the system

The System description is comprised of the following components:

- The System description is comprised of the following components:
- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Teramot maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Hardware	Type	Purpose (optional)
AWS Elastic Compute Cloud (EC2)	AWS	
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

Software

Teramot is responsible for managing the development and operation of the Teramot AI Agent Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Teramot infrastructure and software components are shown in the table provided below:

System/ Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Datadog	Datadog	Monitoring application used to provide monitoring, alter, and notification services for Teramot platform
Amazon Web Services	<table-input>	<table-input>
GitHub	<table-input>	<table-input>
Google Workspace	<table-input>	<table-input>
Slack	<table-input>	<table-input>
Vanta	<table-input>	<table-input>

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Teramot has a staff of approximately 1 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
This includes:

- CEO -
- CFO -
- CTO -
- CRO -

Operations: Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data as defined by Teramot, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Teramot

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Teramot.	● Press releases ● Public website
Internal	Access to internal information is approved by management and is protected from external access.	● Internal memos ● Design documents ● Product specifications ● Correspondences
Customer data	Information received from customers for processing or storage by Teramot. Teramot must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Customer operating data ● Customer PII ● Customers' customers' PII ● Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Teramot to operate the business. Teramot must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Legal documents ● Contractual agreements ● Employee PII ● Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Teramot has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical security

Teramot's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Teramot reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical access

Teramot provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems are split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

Management and Cybersecurity Team is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Teramot's policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Management and Cybersecurity Team is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

Computer operations - backups

Customer data is backed up and monitored by the CTO, Infrastructure and Cybersecurity Team for completion and exceptions. If there is an exception, CTO, Infrastructure and Cybersecurity Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer operations - availability

Teramot maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Teramot internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Teramot utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change management

Teramot maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data communications

Teramot has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Teramot application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

We run automated vulnerability scans on a quarterly basis using integrated AWS and GitHub tools. In addition, we contract annual penetration tests with external vendors. All vulnerabilities are triaged and managed through our Cerberus security board in Jira, following Teramot's incident response workflow.

Boundaries of the system

The boundaries of the Teramot AI Agent Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Teramot AI Agent Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Integrity and ethical values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Teramot's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Teramot's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to competence

Teramot's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's philosophy and operating style

The Teramot management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Teramot can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Teramot to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational structure and assignment of authority and responsibility

Teramot's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Teramot's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

HR policies and practices

Teramot's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Teramot's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk assessment process

Teramot's risk assessment process identifies and manages risks that could potentially affect Teramot's ability to provide reliable and secure services to our customers. As part of this process, Teramot maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Teramot product development process so they can be dealt with predictably and iteratively.

Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Teramot's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Teramot addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Teramot's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and communication systems

Information and communication are an integral component of Teramot's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Teramot uses several information and communication channels internally to share information with management, employees, contractors, and customers. Teramot uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Teramot uses in-person and video “all hands” meetings to communicate company priorities and goals from management to all employees.

Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Teramot’s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Teramot’s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in Teramot’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Teramot’s personnel.

Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the system (Type 1)

No significant changes have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

Changes to the system (Type 2)

No significant changes have occurred to the services provided to user entities during the review period or since the organization's last review.

Incidents (Type 1)

No significant security incidents have occurred in the past 3 months.

Incidents (Type 2)

No significant security incidents have occurred during the audit observation period.

Criteria not applicable to the system

All Common Criteria/Security, Security criteria were applicable to the Teramot's Teramot AI Agent Platform system.

Subservice organizations

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Subservice description of services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services.

Complementary Subservice Organization Controls

Teramot's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Teramot's services to be solely achieved by Teramot control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Teramot.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.

Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Availability	A 1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
Availability	A 1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.
Availability	A 1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
Availability	A 1.2	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Availability	A 1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Availability	A 1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Availability	A 1.2	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.

Teramot management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Teramot performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary user entity controls

Teramot's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Teramot's services to be solely achieved by Teramot control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Teramot's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Teramot.
2. User entities are responsible for notifying Teramot of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Teramot services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Teramot services.
6. User entities are responsible for providing Teramot with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Teramot of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.