COALFIRE CONTROLS

Report on Recorded Future, Inc.'s Recorded Future Intelligence Platform Relevant to Security, Availability, Confidentiality, and Privacy Throughout the Period June 1, 2022 to May 31, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Recorded Future®

Table of Contents

Section 1

Section 2

Attachment A

Attachment B

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Recorded Future, Inc. ("Recorded Future")

Scope

We have examined Recorded Future's accompanying assertion titled "Assertion of Recorded Future, Inc. Management" (assertion) that the controls within the Recorded Future Intelligence Platform (system) were effective throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Recorded Future uses a subservice organization to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Recorded Future, to achieve Recorded Future's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Recorded Future's controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Recorded Future is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved. Recorded Future has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Recorded Future is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Recorded Future's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Recorded Future's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Recorded Future Intelligence Platform were effective throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Recorded Future's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
August 10, 2023

Section 2

Assertion of Recorded Future, Inc. Management

Recorded Future®

Assertion of Recorded Future, Inc. (“Recorded Future”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Recorded Future Intelligence Platform (system) throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Recorded Future’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Recorded Future uses a subservice organization for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Recorded Future, to achieve Recorded Future’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Recorded Future’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Recorded Future’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Recorded Future’s controls operated effectively throughout that period. Recorded Future’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2022 to May 31, 2023 to provide reasonable assurance that Recorded Future’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Recorded Future, Inc.

Attachment A

Recorded Future, Inc.’s Description of the Boundaries of Its Recorded Future Intelligence Platform

Type of Services Provided

Recorded Future, Inc. (“Recorded Future” or “the Company”) delivers security intelligence to amplify the effectiveness of security and IT teams in reducing risk by uncovering unknown threats to inform decision making. Headquartered in Somerville, Massachusetts, USA, with an additional hub in Gothenburg, Sweden, and additional offices in Virginia, London, the United Kingdom, Singapore, Dubai, and Tokyo, Recorded Future works with clients from all sectors, both private and government. Direct clients typically fall in the Fortune 2000 sector. Recorded Future also works with partners or Managed Security Service Providers (MSSPs) who in turn work with smaller clients not hosting their own threat analysis teams or security operations centers (SOCs).

Working to provide a singular view of digital, brand, third-party, geopolitical, and other associated risks, the Recorded Future Intelligence Platform (“the Platform”) system provides proactive and predictive intelligence, analyzing data from open, proprietary, and aggregated customer-provided sources. Recorded Future provides threat analysts, vulnerability management teams, SOCs, and incident responders with context-rich, actionable intelligence in real time that is ready for integration across the security ecosystem. This approach empowers organizations to prioritize workflows based on risk, make confident decisions using external context, alert proactively on relevant threats, implement targeted blocking at security controls, and maximize value of existing security investments.

Platform Overview

Recorded Future provides offerings built on its all-in-one Intelligence Platform, which consists of processes ranging from source collection and processing to analysis and reporting. The Platform leverages many technologies as building blocks, including text search, data visualization, natural language processing, and entity extraction.

At the core of the Platform’s technology is Recorded Future’s patented Intelligence Engine, which innovatively mines data to enable the Platform to understand what events have been reported on and to place them in time and space. The Intelligence Engine works by separating collected, analyzed online media and documents and their content from their subject – the “canonical” entities and events. Documents contain references to these entities and events, and these references are used to rank entities and events based on: 1) the number of references to them, 2) the credibility of the documents or document sources containing these references, and 3) several additional factors, such as co-occurrence of different events and entities in the same or in related documents.

Recorded Future also conducts analysis on the “time and space” dimension of documents, i.e., references to when and where an event has taken place, or even when and where it will take place, since many documents refer to events expected to take place in the future.

The combination of automatic event, entity, time, and location extraction; implicit link analysis for novel ranking algorithms; and statistical prediction models forms the basis for the Platform and is Recorded Future’s core expertise. Figure 1 is a pictorial description of the process.

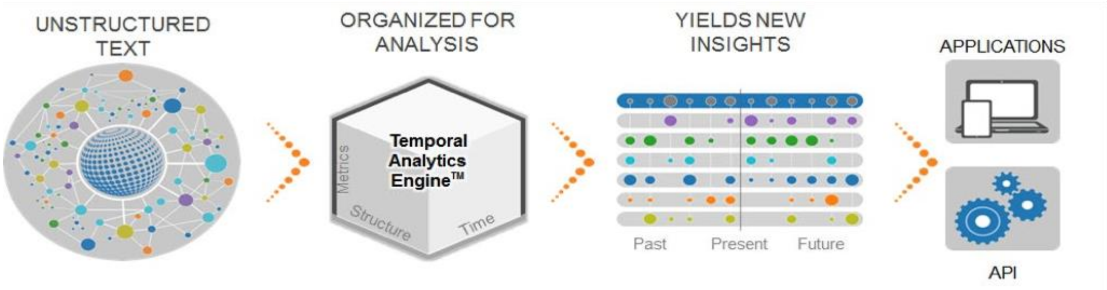


Figure 1: Intelligence Platform's Intelligence Engine Data Collection and Analyzation Process

The Platform can be used as either a standalone product or integrated into security information and event management (SIEM); security orchestration, automation and response (SOAR); governance, risk, and compliance (GRC), or other information technology (IT) and security systems, as shown in Figure 2 below.

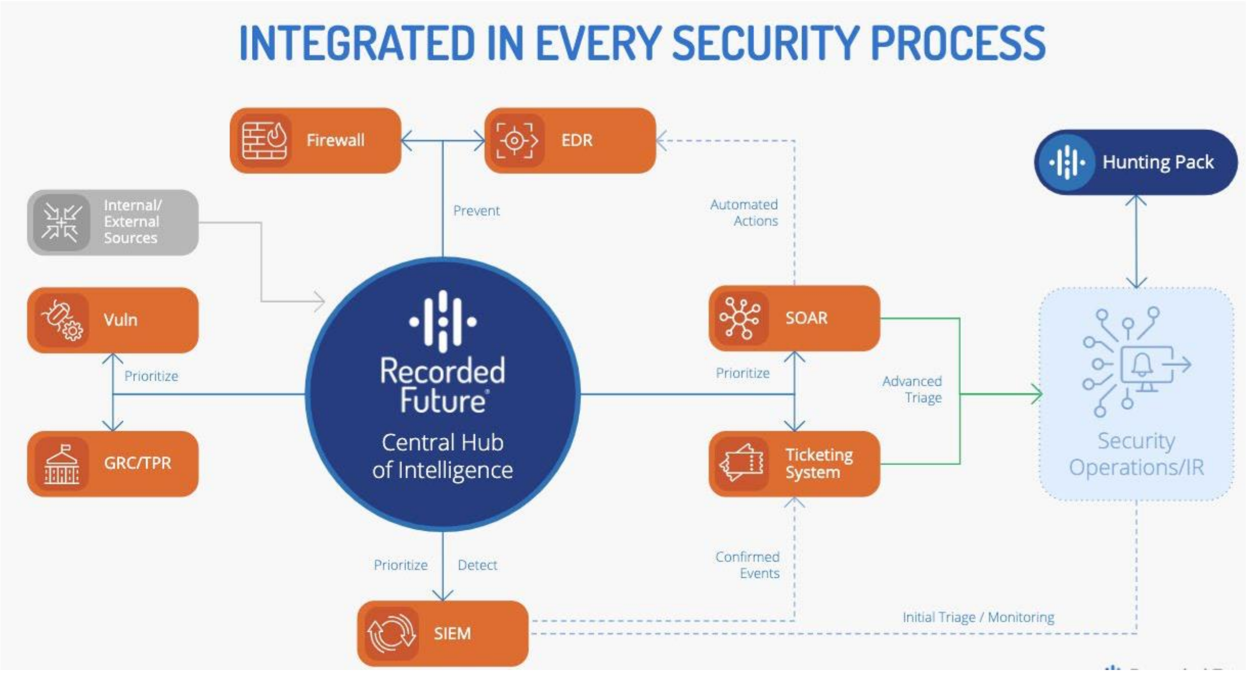


Figure 2: Intelligence Platform Security System Integrations

The Components of the System Used to Provide the Services

The boundaries of the 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 Platform.

As shown in Figure 3, the Platform is a universal security intelligence solution that centralizes information from across proprietary data sources, including research from the Company's threat research division Insikt Group, to enable its clients to use intelligence-driven security to proactively defend against cyberattacks.

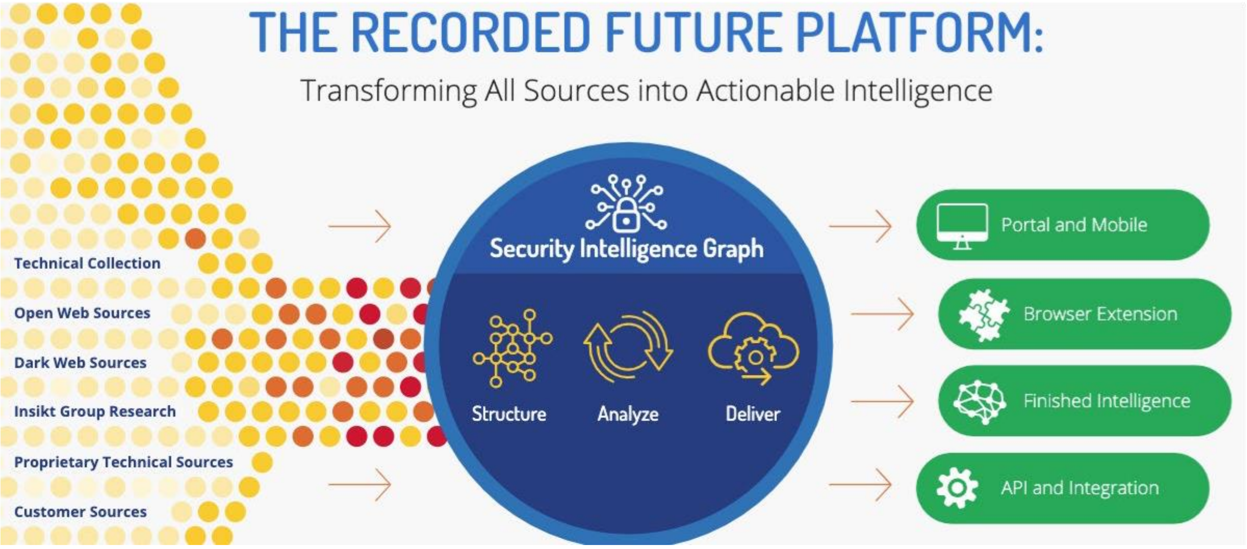


Figure 3: Intelligence Platform Workflow

The Company provides analysts deep visibility into client's threat landscape by analyzing and visualizing cyber threats, even across numerous foreign languages (partly by its natural language processing [NLP] and artificial intelligence [AI] capabilities), leveraging its open-source intelligence (OSINT) and proprietary data repository. Analysts receive real-time alerts when relevant cyber threats to their organization are identified.

The Company believes that machine learning combined with human expertise is a superior approach to create real-time, relevant security intelligence to effectively reduce risk at scale. The Company sources data from across the open, deep, and dark web to produce insightful and actionable intelligence data and reduce the manual collection and processing of intelligence data. This frees up security analyst and engineering manpower, allowing them to be making decisions where they are most needed instead of curating data.

The Company's use cases include:

- Security operations and incident response: Broad source coverage, real-time risk scores and context, block-grade indicators, and multiple SIEM and SOAR integrations allow for alert triage, threat detection, and threat prevention.
- Threat intelligence: Real-time search and alerting, high-confidence threat hunting and detection, risk scores, and transparent source evidence organized into over two billion Intelligence Cards allow for threat research and reporting, incident detection and validation, and dark web monitoring.
- Brand protection: Broad source coverage, closed forum dark web monitoring, real-time alerting, and takedown services allow for typosquat detection, data leakage monitoring, brand attack mitigation, and executive cyber protection.
- Vulnerability management: Vulnerability risk scores based on exploitation, real-time alerting before vulnerability publication, integrations with vulnerability management solutions, and browser extension for Common Vulnerabilities and Exposures (CVE) enrichment allow for vulnerability prioritization and for monitoring vulnerabilities in an organization's technology stack.

- Third-party risk: Continuous monitoring of over 150,000 organizations, real-time alerting on risk indicators, transparent sourcing and evidence, and Insikt Group research for in-depth analysis allows for continuous third-party risk management and procurement assessment.
- Business continuity and geopolitical risk: Real-time geopolitical monitoring, location-based Intelligence Cards, and broad source coverage in every language allow for executive monitoring and physical security analysis.

The Platform is delivered via:

1. Recorded Future Portal: A graphical user-interface that is accessible via any supported internet browser (including Google Chrome, Mozilla Firefox, Edge, and Safari.) The web interface gives organizations direct access to all Company data, including over 2 billion Intelligence Cards.
2. Recorded Future Browser Extension: The browser extension works by scanning the current webpage for CVEs, hashes, domains, and IP addresses and listing them in the extension popup when the user clicks the browser extension icon (located towards the top in the browser menu bar).
3. Recorded Future Connect Technology: Connect technology leverages the Recorded Future application programming interface (API) to integrate with a client's existing security technologies and provide intelligence within these services.
4. The Recorded Future Mobile App: The mobile app provides access to the Home Screen (including research from Insikt Group, cyber news, malware trends, and alerts), access to the Company's Intelligence Cards (covering threat actor profiles, IP addresses, hashes, CVEs, domains, and more), and allows searching for entities with risk scores.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure and Software

The Platform is a web application that has its entire Platform infrastructure hosted in a virtual private cloud. The network is divided into several subnets, and is replicated across multiple availability zones. Only the nodes in the public subnet can be directly accessed from the Internet. All outgoing traffic must pass through NAT-gateways which are placed in the public subnets.

There are two different ways to log in to the Platform. In most cases, users are sent to the Recorded Future identity provider (IdP) where they log in. Users can also use single-sign on (SSO) from their own IdP, and, in such cases, the login request goes over Auth0 before it goes to the user IdP.

The user browser includes the session cookie in the web request. If needed, the web application contacts the user service to check which access rights the user has. The web application queries the database, index, and, in some cases, a third-party database to fetch the required data. The web application may also set up a listener on RabbitMQ to listen for new references and other changes.

All configured alerts are stored in an alert collection in the MongoDB databases. The alert definition contains an encrypted reference to the user. The alert detector receives all new references via a RabbitMQ queue and checks them against the configured alerts. If it detects a matching reference, it sends a message via RabbitMQ to the alert creator. The alert creator sends the encrypted user reference to the user service in order to get the email addresses the alert should be sent to. The email is generated and sent via SendGrid, an external email sending service.

People

The Company has a staff of approximately 850 employees organized in the functional areas described below. The background of all employees varies, but most have a higher education within the technology field. Job descriptions are available for all roles. Depending on the job description, certifications may be required. The Company obtains references for candidates.

All new hires and current employees are required by law or internal policy to complete several checks before they are eligible to begin employment. Depending on location and role, these checks may include identity verification, verifying eligibility to work, and background checks.

Currently, the Company conducts background checks on all employees unless prohibited by local law or in cases where the legal department has granted an exemption. The Company retains a third-party agency to conduct the screening process and maintain the corresponding records. The types of screens that may be conducted include, but are not limited to, education verification, employment verification for as many as seven years, identity verification, criminal record searches, and a sex offender registry search. Additionally, as appropriate for a position, credit, professional license, or state motor vehicle checks may also be conducted.

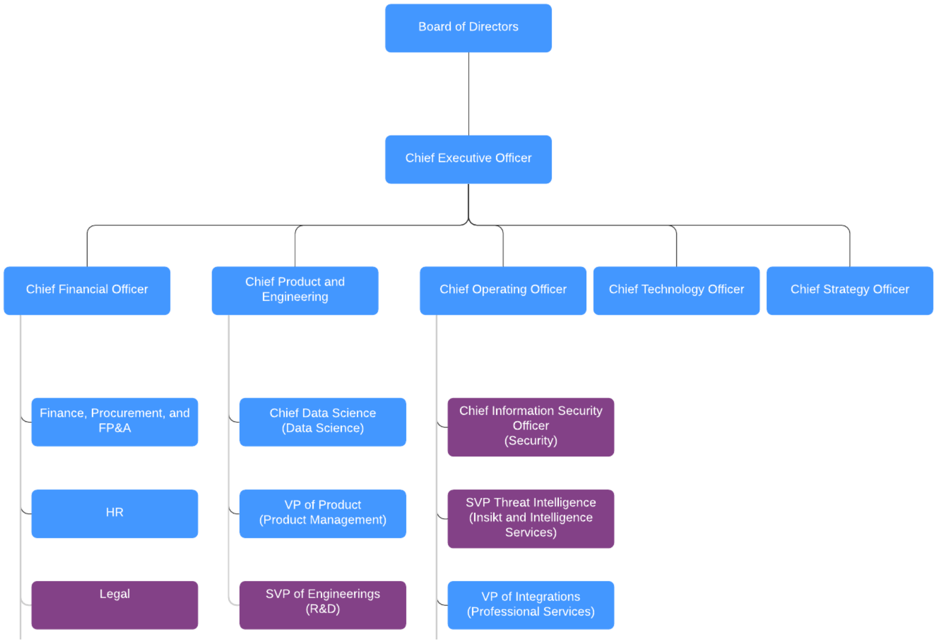
At a minimum, the Company applies a three-tier interview process, which includes prequalification for the job, assessment of the candidates' skills, including potential tests when applicable, and interviews with the candidates' direct colleagues.

The Company develops, manages, and secures the Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Chief Executive Officer (CEO)	Responsible for the Company's strategic direction, finances, key relationships, and operations with a focus on growing the business.
Research and Development (R&D)/Engineering	Responsible for all aspects of building and maintaining the Platform, including architecting the application, developing new functionality, fixing bugs, testing all releases, release deployment, and monitoring of the live systems. The primary goal of the R&D/Engineering group is to rapidly develop new innovative functionality while ensuring that the application performs to the highest levels.
Operations Team	Responsible for monitoring and deploying the system, creating and maintaining the Platform on which it is built, and covering third line support for any critical issues, as well as for focusing on internal security.
Platform Team	Responsible for building the underlying framework for the Platform (including databases), indexing operations, and optimization, as well as for API support.
Product Design Team	Responsible for breaking down the bigger product goals to actual R&D deliverables and designs.
Applications Team	Responsible for the development and maintenance of the end user interface.
Analytics Team	Responsible for linguistics and data quality, as well as for the framework for harvesting sources and breaking down text to the Company's patent-protected data model.

People	
Group/Role Name	**Function**
Integrations Team	Responsible for the development, quality assurance, and availability of the Platform’s integrations.
Quality Assurance Team	Responsible for assuring the quality of the offerings and solutions.
Delivery Management Team	Responsible for managing new releases, coordinating with internal stakeholders to ensure successful delivery of the Company’s offering, and overseeing the planning and resource allocation necessary for new development.
Professional Services	Responsible for offering customized services to customers, including integration support and API solutions.
Data Science Team	Responsible for ensuring good data quality for end customers through data cleaning, as well as for internal and external tools for data management.
Chief of Data Science	Responsible for the Data Science Team and for driving key analysis projects, both internal and external.
Intelligence Services	Responsible for customer success (including ensuring that customers can successfully deploy and use the product within their organization), responding to customer issues, training customers on using the product, providing analysis services, and collecting customer feedback that is used for product management to shape future releases
Product Management	Responsible for managing customer, partner, and internal requirements and feedback used to shape future product releases, as well as for sending notifications on new features and releases and setting the product roadmap
Threat Intelligence	Responsible for defining the Company threat Intelligence strategy influencing both business and product directions, this department includes Intelligence Services and the Insikt Group, the Company’s in-house research team that can provide subject-matter expertise to respond to Company and customer incidents upon request.
Sales	Responsible for business development, direct sales, inside sales, pre-sales, partners, account management, and sales management.
General & Administrative teams	Responsible for the Finance, Legal, and Human Resources (HR) functions, including the planning, organizing, auditing, accounting for, and controlling of finances, as well as for maintaining contracts and producing financial statements.
Marketing	Responsible for driving customer subscriptions to the Company, with a primary focus on new customer acquisition and subscription expansion by refining and communicating the Company’s unique value proposition.

The following organization chart reflects the Company’s internal structure related to the groups discussed above:


Board of Directors
Chief Executive Officer
Chief Financial Officer
Chief Product and Engineering
Chief Operating Officer
Chief Technology Officer
Chief Strategy Officer
Finance, Procurement, and FP&A
HR
Legal
Chief Data Science (Data Science)
VP of Product (Product Management)
SVP of Engineerings (R&D)
Chief Information Security Officer (Security)
SVP Threat Intelligence (Insikt and Intelligence Services)
VP of Integrations (Professional Services)

Procedures

The Company has developed and documented formal policies and procedures. These policies and procedures have been developed to segregate duties, where possible, and enforce responsibilities based on job functionality. They also serve as guidelines and directions for day-to-day work. Policies and procedures are reviewed periodically, but no less than annually, and are updated as necessary.

These procedures and policies are all found either on the Company intranet, called Lyra, or are included in the Recorded Future Employee Handbook. New employees are trained on these procedures and policies. If any material changes are made to the policies and procedures, these changes are communicated to all employees. Training for changes occurs when necessary.

To maintain the operation of the service, the Company continuously (24/7) provides the following main services:

1. Systems deployment and maintenance
2. Security administration and auditing
3. Intrusion detection and incident response
4. Operations and performance monitoring
5. Change controls
6. Business recovery planning

Data

The Company implements and maintains backup, security, and business continuity measures that are designed to maintain the security and integrity of Customer Data. Beyond financial information that is securely kept for billing purposes and user passwords to allow access to the service (for those organizations that are not using SSO), the Company stores the following Customer Data:

- Saved Queries and Alerts
- User-generated Analyst Notes
- Sandbox Submissions
- Observed Correlations and Notes
- Reports
- Lists, including Watch Lists
- Information collected via the Company's free browser extension (Recorded Future Express)

The Company encrypts and stores this data securely. The Company also logs certain user actions. Logs that contain user-provided query data are automatically deleted, or rendered unattributable, after 14 days, and all other customer provided data (including Analyst Notes) are deleted or rendered unattributable, as applicable, after the subscription is terminated.

The Company also stores error and event logs and documents from open-source data.

Subservice Organization

The Company uses a subservice organization for data center colocation services. The Company's controls related to the Platform cover only a portion of the overall internal control for each user entity of the Platform. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Controls are expected to be in place at the subservice organization related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organization's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organization's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the subservice organization's SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to management of the subservice organization.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Platform. Commitments are communicated in the Master Services Agreement (MSA), Service-Level Agreements (SLAs), and other customer agreements.

System requirements are specifications regarding how the Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Platform include the following:

- Recorded Future will implement and maintain commercially reasonable security measures to protect against unauthorized access, alteration, disclosure or destruction of data provided by customers.
- Recorded Future processes personal information only for the purposes for which it was collected and in accordance with the Privacy Policy.
- Recorded Future has robust back-up procedures to protect against accidental destruction or loss of system information.

The Company has established operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Company system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of these system requirements as they relate to the Platform.