A-LIGN

Human Security Inc.

Type 2 SOC 3

2024

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

August 1, 2023 to July 31, 2024

Table of Contents

SECTION 1

ASSERTION OF HUMAN SECURITY INC. MANAGEMENT

ASSERTION OF HUMAN SECURITY INC. MANAGEMENT

August 16, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Human Security Inc.'s ('HUMAN' or 'the Company') Human Defense Platform System throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HUMAN's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Human Security Inc.'s Description of Its Human Defense Platform System throughout the period August 1, 2023 to July 31, 2024" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HUMAN's service commitments and system requirements were achieved based on the trust services criteria. HUMAN'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 "Human Security Inc.'s Description of Its Human Defense Platform System throughout the period August 1, 2023 to July 31, 2024".

HUMAN uses Snowflake Inc. (Snowflake), Google Cloud Platform (GCP), Equinix, and Amazon Web Services, Inc. (AWS) to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HUMAN, to achieve HUMAN's service commitments and system requirements based on the applicable trust services criteria. The description presents HUMAN's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HUMAN's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve HUMAN's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of HUMAN's controls.

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 August 1, 2023 to July 31, 2024 to provide reasonable assurance that HUMAN's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of HUMAN's controls operated effectively throughout that period.

Gavin Reid
Chief Information Security Officer
Human Security Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Human Security Inc.

Scope

We have examined HUMAN's accompanying assertion titled "Assertion of Human Security Inc. Management" (assertion) that the controls within HUMAN's Human Defense Platform System were effective throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HUMAN's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*.

HUMAN uses Snowflake, GCP, Equinix, and AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HUMAN, to achieve HUMAN's service commitments and system requirements based on the applicable trust services criteria. The description presents HUMAN's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HUMAN's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at HUMAN, to achieve HUMAN's service commitments and system requirements based on the applicable trust services criteria. The description presents HUMAN's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HUMAN's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

HUMAN 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 HUMAN's service commitments and system requirements were achieved. HUMAN has also provided the accompanying assertion (HUMAN assertion) about the effectiveness of controls within the system. When preparing its assertion, HUMAN is responsible for selecting, and identifying in its assertion, the applicable trust services 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 AICPA. 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.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

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

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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

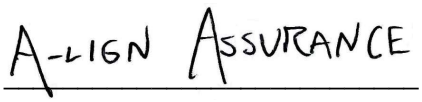
In our opinion, management's assertion that the controls within HUMAN's Human Defense Platform System were suitably designed and operating effectively throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HUMAN's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of HUMAN's controls operated effectively throughout that period.

The SOC logo for Service Organizations on HUMAN's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of HUMAN, user entities of HUMAN's Human Defense Platform during some or all of the period August 1, 2023 to July 31, 2024, business partners of HUMAN subject to risks arising from interactions with the Human Defense Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
August 16, 2024

SECTION 3

HUMAN SECURITY INC.'S DESCRIPTION OF ITS HUMAN DEFENSE PLATFORM SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2023 TO JULY 31, 2024

OVERVIEW OF OPERATIONS

Company Background

HUMAN was founded in 2012 in Brooklyn, New York with the objective of providing bot mitigation strategies through the creation of the Human Defense platform, the backbone of all their products that protect enterprises from sophisticated bot attacks, fraud and account abuse.

The organization headquarters is based in New York, NY with another global site in Tel Aviv, Israel. HUMAN was recognized by the TIME 100 Most Influential Companies of 2023 as a disruptor for stopping bot attacks, digital fraud and abuse. HUMAN's Bot Defender was recognized as a leader in the G2 Grid® for Bot Detection and Mitigation.

Industries served by HUMAN include but are not limited to Marketing firms, Advertising, Retail, and Government agencies.

Description of Services Provided

HUMAN supports cyber-security and fraud prevention with their products explained below:

- Bot Defender is a behavior-based bot management solution that protects websites, mobile applications and Application Programming Interfaces (APIs) from automated attacks.
- MediaGuard protects against disruptive ad fraud to improve quality and trust in the ecosystem.
- CleanAD detects and protects against malicious behavior in ads and landing pages.
- Account Defender safeguards app and website accounts by detecting and neutralizing compromised and fake accounts.
- Code Defender is a client-side web application security solution that provides comprehensive real-time visibility and control into the modern website's client-side supply chain attack surface, to identify vulnerabilities and anomalous behavior and proactively mitigate compliance risk.
- Credential Intelligence detects and stops the use of compromised credentials on websites and mobile apps in real-time.

Principal Service Commitments and System Requirements

HUMAN designs its processes and procedures related to bot mitigation to meet its objectives for MediaGuard, BotGuard for Growth Marketing, and Defender suite services.

Those objectives are based on the service commitments that HUMAN makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that HUMAN has established for the services.

The services provided by HUMAN are subject to the requirements of the American Institute of Certified Public Accountants (AICPA) 2017 Trust Service Principles, including relevant regulations as well as security laws and regulations in the jurisdictions in which HUMAN operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security concepts within the fundamental configurations to HUMAN services are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

HUMAN establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in HUMAN's 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, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development towards HUMAN products and services.

Components of the System

Infrastructure

Primary infrastructure used to provide HUMAN's Human Defense Platform System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Cloud infrastructure	GCP, AWS, Equinix Packet	All product operations
Wi-Fi Access Point	Meraki MX75 / MS350	Office Wi-Fi
AWS Elastic Cloud Compute (EC2)	Rocky Linux	Virtual machines support product infrastructure
GCP Google Compute Engine (GCE)	Flatcar	Virtual machines support product infrastructure
AWS Simple Storage Solution (S3)	Not Applicable	Object storage for Media product data
GCP Google Cloud Storage (GCS)	Not Applicable	Object storage for Enterprise product data

Software

Primary software used to provide HUMAN's Human Defense Platform System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Account Defender	Flatcar	Product offering
BotGuard for Growth Marketing	Rocky Linux	Product offering
Bot Defender	Flatcar	Product offering
Code Defender	Flatcar	Product offering
Credential Intelligence	Flatcar	Product offering
MediaGuard	Rocky Linux	Product offering
BigQuery	Not Applicable - Software as a Service (SaaS)	Data lake
Snowflake	Not Applicable - SaaS	Data lake
Okta	Not Applicable - SaaS	Employee and customer authentication
Datadog	Not Applicable - SaaS	Monitoring
NS1	Not Applicable - SaaS	Authoritative Domain Name Service (DNS)
Redash	Not Applicable - SaaS	Dashboards & visualization
Looker	Not Applicable - SaaS	Visualization
HubSpot	Not Applicable - SaaS	Web hosting, marketing
Salesforce	Not Applicable - SaaS	Customer relationship management
Sumo Logic	Not Applicable - SaaS	Security Incident & Event Management (SIEM) and Security Orchestration & Automated Response (SOAR)
Wiz	Not Applicable - SaaS	Cloud security posture management
Atlassian	Not Applicable - SaaS	Confluence document management, JIRA ticketing, and Opsgenie notifications
Netlify	Not Applicable - SaaS	Product documentation
Doc360	Not Applicable - SaaS	Product documentation
CrowdStrike	Not Applicable - SaaS	Endpoint Detection and Response (EDR)
Slack	Not Applicable - SaaS	Customer support
Fastly	Not Applicable - SaaS	Content delivery network (CDN)
Cloudflare	Not Applicable - SaaS	CDN
Akamai	Not Applicable - SaaS	CDN
Google Workspace	Not Applicable - SaaS	Productivity tools

People

Human Security has a headcount of 286 employees in the below functional areas:

Responsibility for HUMAN Information Security resides with the Chief Information Security Officer (CISO).

In addition to the overall governance provided by the executive leadership team, the following teams play key roles in the execution of controls:

- Executive Leadership - Aligns the company's business objectives to their vision and mission through strategic initiatives and approves capital expenditures for the organization.
- Security Team - Responsible for maintaining policies and the security of the systems.
- Information Technology (IT) Team - Responsible for maintaining IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support.
- Research and Development - Responsible for software development, signal detection, change management and infrastructure management.
- People Ops/Human Resources (HR) - Responsible for employee hiring, onboarding, offboarding and employee reviews.
- Finance - Responsible for maintaining accounting books & records, the company's capital funds, the budget of the company and vendor management.
- Legal - Supports the organization by delivering objective, relevant and creative solutions and advice to legal issues and problems.

Data

HUMAN provides data collection capabilities to their customers, who integrate their services into their web and mobile applications.

Customers access an online web portal, also called the dashboard or console, to configure their systems to interoperate with the customer's web and/or mobile software. Customer account and application integration details are stored in HUMAN's cloud.

During onboarding, customers integrate HUMAN components, including a Sensor component that runs in web or mobile code that executes on the customers' users' systems. The Sensor component transmits data to HUMAN either directly or indirectly through the customer's application, depending on the customer's integration preferences.

HUMAN code collects technical information about the use of customers' systems (ad delivery and user-oriented systems, typically e-commerce), such as browser user-agent string, Internet Protocol (IP) address, and short-lived cookies, as well as request/response metadata including Uniform Resource Locator (URL) and response code.

Customers may, at the customer's discretion, transmit additional enrichment data to HUMAN that HUMAN may use to increase the accuracy of analysis and classification.

User and application behavior is captured in HUMAN's cloud systems, where data is staged for real-time, near-real-time, and batch analysis by automated systems, including expert rules, machine learning systems, as well as manual processes for tuning and research. During this phase, HUMAN also evaluates any custom rules that customers have configured.

For eligible products, user requests to customer web and mobile systems are classified in real-time, and classification is delivered to customer systems for enforcement. Depending on customer configuration, customers may block or alter customer application behavior, such as showing alternate content or a captcha.

For each system, the operational record of system usage is captured in an online, configurable, near-real-time dashboard which shows the classification of customer applications' user traffic.

Customer personnel may self-configure, enroll, or remove additional applications throughout the account life cycle.

HUMAN offers customers ad-hoc reports as well as near-real-time data exports from their cloud systems to customer systems, typically through batch jobs self-managed by customers in the portal. Similarly, customers self-manage user access to their accounts using the portal. HUMAN offers Single Sign On (SSO) integration to customer authentication systems using Security Assertion Markup Language (SAML). Regarding customer employees, HUMAN may store Personal Identifiable Information (PII) for contact and business relationship purposes, such as username, e-mail address, and IP address for customer employees.

Portal access is protected by Transport Layer Security (TLS), as are outbound data flows from their systems to customer systems. HUMAN recommends TLS for each customer deployment, but also supports non-encrypted connections for customers who offer non-encrypted online services.

Processes, Policies and Procedures

HUMAN maintains physical and environmental policies established to protect the global HUMAN premises and equipment from environmental threats.

Physical Security

The in-scope system and supporting infrastructure are hosted by Snowflake, GCP, Equinix, and AWS. As such, Snowflake, GCP, Equinix, and AWS are responsible for the physical security controls for the in-scope system.

Logical Access

Logical access includes several components:

- IT and administrative controls over HUMAN corporate systems
- Product (engineering and research) system access
- Customer access

Corporate and IT Systems

Corporate and IT systems are administered by a centralized IT team which retains administrative to corporate systems along with business owners. Employees are provisioned end user devices which are centrally managed by IT using mobile device management systems.

Users request access through IT, and IT obtains approval from system owners before provisioning users.

IT administers employee Identity and Access Management (IAM) systems, which contain enterprise employee identity and access groups. These are used as IAM sources for employee access to corporate IT and product systems.

New users are communicated to IT from HR after offer acceptance. IT maintains access templates for departments and pre-provisions access based on the access template. New hires may then request additional access using the access request process after their start.

Users must set complex passwords in accordance with a password policy. Human uses threat intelligence services to manage risks associated to password authentication such as credential leakage and password reuse. Access to core business systems including privileged level access users requires multi-factor authentication.

IT obtains lists of separated employees from HR and removes underlying identity from IAM systems within 24 hours, which effectively prevents user access, as well as removing access entitlements associated to the separated employees.

Security leads annual user access reviews for corporate systems, and quarterly reviews for privileged access.

Product Systems

Product systems are administered by a centralized DevOps team, which retains administrative (privileged) access to product Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) infrastructure as well as Continuous Integration (CI) and Continuous Delivery (CD) systems.

Product source code is maintained in source code management systems, and access is granted to engineering teams. Product build logic is maintained by engineering teams; deployment and integration logic is maintained in IaaS repositories maintained by DevOps.

DevOps teams develop and maintain production solution architecture based on system requirements developed by engineering, product, and research teams. Users, including engineers and engineering leaders, request access to production systems by placing access requests to the DevOps team, which review access requests with product and infosec teams as needed.

Dashboard access (i.e., manual processing by Service Delivery functions) is maintained by IT. Infosec conducts annual user access reviews for product systems. DevOps performs quarterly reviews for privileged access.

Customer Access

During onboarding, customers are provisioned with a company-level account to the portal and an initial company administrator with the ability to configure the company-level account and create additional company account users. Customers thereafter self-manage access to their accounts on the portal.

Customer-facing teams maintain access to customer accounts in the portal. Customer-facing teams may use administrative functions in the portal to enter and configure customer accounts. Customer-facing teams may access customer accounts to configure and tune customer integrated apps, or in support of customer support requests for account maintenance or assistance with onboarding or account sustainment.

Computer Operations - Backups

Most business data is held in SaaS platforms, including data lakes Snowflake and BigQuery, that provide redundancy and high availability.

The main exception to this is customer account data, which is maintained in application databases. Application database instances are replicated for high availability and performance and are backed up nightly (Media systems) or hourly (Enterprise systems).

The overall backup procedure is incorporated into disaster recovery plans which are maintained on Confluence.

Restore jobs are tested on an ongoing basis, including annual manual validation (Media systems) or daily automated restoration (Enterprise systems).

Backup data is copied to access-restricted buckets and / or systems in the associated cloud platform.

Computer Operations - Availability

HUMAN has extensive monitoring controls in place as their systems are performance sensitive.

Hard and soft SLAs are incorporated variously into customer contracts based on product and customer requirements.

Media product systems are provisioned geographically in close proximity to customer systems using “bare metal” and static provisioned virtual machines in order to meet tight latency objectives.

Enterprise product systems are provisioned in central cloud providers with autoscaling based on GCP instance groups in order to meet soft SLAs and in proportion to widely fluctuating demand based on customer activity volume. Customers are encouraged to notify Enterprise account teams of high volume events, including Hype Sales (e.g., product releases or sales events) for which HUMAN may pre-scale infrastructure.

HUMAN product systems are configured for redundancy and high availability.

Monitoring systems are configured with thresholds of acceptable performance, including availability, and alert operations personnel through slack as well as pages. Operations personnel maintain written procedures for analyzing and responding to alerts.

Security logs are transmitted to a centralized Security Information and Event Management (SIEM). Infrastructure logs are first analyzed by an external SOC provider before escalating to Infosec. A cloud security posture management (CSPM) solution is used for automated configuration and security operational review, with configured alerting to the Security team. Security operates a staffed security operations function with defined cyber security information response (CSIRT) processes.

Change Control

HUMAN maintains cyber security policies, including secure coding standards, which require the use of change controls for changes that may impact system security. A Change Control policy defines requirements for change management practices across the HUMAN portfolio.

In general HUMAN practices agile technology development. Engineers and technology personnel are encouraged to rapidly develop and iterate solutions and capabilities, and this is critical to HUMAN’s business model, which includes adapting and responding in real-time to adaptive and dynamic threat behaviors by intelligent threat actors.

Change control policy is organized around sustaining velocity while managing enterprise risk. Engineers must identify and describe planned changes in the issue management system, Jira. Engineers submit source code changes to online source code management systems as pull requests, where changes are subject to peer review. Major changes require manager approval as well as approval of asset or process owners affected by the change.

Approved changes that pass build checks may be deployed automatically (see below) or may be deployed manually as per the discretion of the DevOps team and the associated build and deployment configuration.

Emergency changes may be made at any time, however upon the conclusion of the emergency, engineers are required to go back and complete any change management steps that may have been omitted to correct the emergency.

Technically, changes are controlled administratively through resource allocation (roadmaps, Kanban boards, and sprint plans), through technical controls in CI/CD systems, and access controls over and within production cloud infrastructure and applications. A centralized DevOps team manages deployment configuration in alignment with engineers, who provide build and integration logic within architecture frameworks established by the DevOps team.

HUMAN has implemented vulnerability management practices including vulnerability scanning, which is integrated in the SDLC, as well as external and internal penetration testing, attack surface management, and bug bounties. Pen-testing, bug bounties, and vulnerability reporting are managed by Security.

Critical and high vulnerabilities identified during scanners may break builds. Otherwise, validated vulnerabilities are handled as defects and handled as other engineering items in sprint planning and engineering.

Data Communications

Customer-deployed systems integrate HUMAN sensors into customer applications so that their users may transmit telemetry data to HUMAN. Receiver and collector systems use defined ports and protocols through high-volume-low-latency and / or highly elastic autoscaling capabilities.

A Sensor component is delivered directly or indirectly to the customers' users through customer-facing systems.
Upon the user interacting with customer application systems, customer-side integrated Enforcer components additionally provide telemetry to and may receive and act on classification results returned from HUMAN Security systems.

Analysis systems are substantially closed to remote access - internally within HUMAN private cloud networks only administrative and maintenance traffic is possible beyond application flows configured by engineering teams. Updates especially to machine learning systems may be processed dynamically in proportion to threat and research activity.

Administrative and remote access to cloud systems is protected through Virtual Private Networks (VPNs) linked to internal identity and access control management systems. Data and systems are organized by product offering, which generally defines the information classes, sensitivity, and performance characteristics required for the services provided. Cross-functional information flows are controlled by security groups based on engineering and product requirements.

Data exports are performed from dedicated egress systems.

Vulnerability Management

HUMAN conducts annual penetration testing of its internet footprint, including cloud as well as branded SaaS offerings i.e., documentation and marketing sites. HUMAN also operates a bug bounty program and practices continuous attack surface management using an external Attack Surface Management (ASM) provider.

Vulnerabilities identified through any external source are triaged according to HUMAN's Vulnerability Management Standard and defined processes for validation, analysis, and remediation planning. The Vulnerability Management Standard outlines a risk-based approach to analysis and prioritization of security defects. Defects that are validated are assigned a remediation timeline based on risk and communicated to engineering teams.

Defects that are not remediated during the remediation timeline are noted to the enterprise risk register and brought to the Security Committee, comprising executive leaders across technology and business areas, for review.

Boundaries of the System

The scope of this report includes the Human Defense Platform System performed in the New York City, New York facilities and Tel Aviv, Israel office.

This report does not include the cloud hosting services provided by Snowflake, GCP, Equinix, and AWS at various locations.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security criteria were applicable to HUMAN's Human Defense Platform System.

Subservice Organizations

This report does not include the cloud hosting services provided by Snowflake, GCP, Equinix, and AWS at various facilities.

Subservice Description of Services

The in-scope system and supporting infrastructure are hosted by Snowflake, GCP, and AWS. As such, Snowflake, GCP, Equinix, and AWS are responsible for the physical security controls for the in-scope system.

Complementary Subservice Organization Controls

HUMAN'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 HUMAN's services to be solely achieved by HUMAN control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of HUMAN.

The following subservice organization controls are implemented by Snowflake to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Snowflake		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to any office location requires an electronic badge.
		Camera/surveillance systems are located at critical internal and external entry points.
		CCTV collected data is retained and available for review unless otherwise restricted by law.

Subservice Organization - Snowflake		
Category	**Criteria**	**Control**
		Security personnel monitor video surveillance 24x7 and security personnel are on-site to control physical access to the site.
		Unauthorized access attempts are logged and monitored, and any suspicious activity is investigated.
		Access points such as delivery and loading areas are controlled and isolated from information processing facilities.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.
		Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
		Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.

The following subservice organization controls should be implemented by Equinix to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Equinix		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4, CC7.2	An ID card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.
		ID cards that include an employee picture must be worn when accessing or leaving the facility.
		Administrative access to the ID card system is restricted to appropriate personnel.
		Visitors must be signed in by an employee before a single-day visitor badge, which identifies them as an authorized visitor, can be issued.
		Visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.
		Visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

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

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

HUMAN'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 of the Trust Services Criteria related to HUMAN's services to be solely achieved by HUMAN control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of HUMAN'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 HUMAN.
2. User entities are responsible for notifying HUMAN of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of HUMAN 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 HUMAN services.
6. User entities are responsible for providing HUMAN with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying HUMAN of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for completeness and accuracy of data submitted to Human Security that is used for providing the services.
9. User entities are responsible for selecting and sanitizing data transmitted to Human Security in accordance with user entity data security requirements.
10. User entities are responsible to ensure that the data collected and processed by Human, as described in the Human Security Privacy Policy, on behalf of the user entity is under proper authorization, including transparency and (if applicable) opt-out according to applicable laws, rules, and regulations, including with respect to the user entity and its relationship with end users.
11. User entities are responsible for communicating lawful subject data request, and data retention and deletion beyond that which is provided by the service.
12. User entities are responsible for integrating applicable Human Security components securely, such as Enforcers, SDKs, tags, scripts.
13. User entities are responsible for any modifications or custom implementations of customer-managed system components, such as SDKs, tags, or scripts, which interoperate with Human Security systems.
14. User entities are responsible for managing system identifiers and associated authenticators, such as cookie encryption keys and server access tokens, including using the associated system facilities.
15. User entities are responsible for designing and implementing their tenant-level access, including SSO configuration as well as personnel invites and removals, role assignments, custom role definitions as applicable.
16. User entities are responsible for service parameters, including rule sets, reports, dashboard configurations, policy settings, and application definitions introduced by the user entity.

17. User entities are responsible for establishing and providing network (internet) connectivity between user entity-premises components and the Human Security cloud components.
18. User entities are responsible for securely implementing and operating cloud or service platforms upon which Human Security customer-side components are deployed by the user entity.
19. User entities are responsible for configuring and managing the look and feel of user-interface components, including the Human Challenge screen, and integrating accordingly into system and user interfaces and associated workflows.
20. User entities are responsible for selecting and implementing data protection controls (e.g., TLS) in transit, including encryption type and levels used to protect data, including in-scope services and associated components served to end users.
21. User entities are responsible for training and maintaining skill sets sufficient for user entity personnel to understand and accurately use the systems, components, and the associated customer platforms.
22. User entities are responsible for adhering to open-source licenses, as applicable, for any open-source components used in conjunction with the service.
23. User entities are responsible for communicating performance requirements, including regional factors, for system deployments, and notifying Human Security of changes to performance requirements including regions.