System and Organization Controls 3 (SOC) 3 Report

Management's Report of Its Assertions on Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System Based on the Trust Services Criteria for Security and Privacy

For the Period August 1, 2019 to July 31, 2020

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Critical Start, Inc.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System based on the Trust Services Criteria for Security and Privacy" (Assertion) that Critical Start, Inc.'s controls over the Professional Services and Managed Detection and Response (MDR) System (System) were effective throughout the period August 1, 2019 to July 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to security 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*).

The Assertion also indicates that Critical Start, Inc's ("Critical Start" or "Service Organization") controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Critical Start's infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Critical Start uses a subservice organization to provide cloud hosting 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 Critical Start, to achieve Critical Start's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitably designed or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Critical Start management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Professional Services and Managed Detection and Response (MDR) System and describing the boundaries of the System;

- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Professional Services and Managed Detection and Response (MDR) System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of Critical Start's Professional Services and Managed Detection and Response (MDR) System relevant to security and privacy policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Critical Start's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

In our opinion, management's assertion that the controls within Critical Start's Professional Services and Managed Detection and Response (MDR) System were effective throughout the period August 1, 2019 to July 31, 2020 to provide reasonable assurance that Critical Start's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP
October 5, 2020
Orange, California

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER CRITICAL START, INC.'S PROFESSIONAL SERVICES AND MANAGED DETECTION AND RESPONSE (MDR) SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY AND PRIVACY

October 5, 2020

Scope

We, as management of Critical Start, Inc., are responsible for:

- Identifying the Critical Start, Inc. Professional Services and Managed Detection and Response (MDR) System (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled "Description of Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System" (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment A) "Description of Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System";
- Identifying, designing, implementing, operating, and monitoring effective controls over Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period August 1, 2019 to July 31, 2020.

Critical Start uses a subservice organization to provide cloud hosting 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 Critical Start, to achieve Critical Start's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We assert that the controls within the system were effective throughout the period August 1, 2019 to July 31, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and privacy set forth in the AICPA's TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice organizations and user entities applied the complementary controls assumed in the design of Critical Start, Inc.'s Professional Services and Managed Detection and Response (MDR) System controls throughout the period August 1, 2019 to July 31, 2020.

Critical Start, Inc.

SECTION THREE:

ATTACHMENT A: DESCRIPTION OF CRITICAL START, INC.'S PROFESSIONAL SERVICES AND MANAGED DETECTION AND RESPONSE (MDR) SYSTEM

Overview of Critical Start, Inc.'s Operations

Critical Start, founded in 2011, is a cybersecurity partner to clients. The Critical Start team has cybersecurity experts that help clients navigate the ever-evolving security landscape. Critical Start strives to improve the security capabilities of customers through a strategy-based approach called the Defendable Network. Through this common-sense approach to complex security standards, Critical Start has identified and achieved security goals based on Security Readiness Condition (SecCon) levels.

SecCon levels range from 5 (highest risk with lowest resources) to 1 (lowest risk and most resources). The progression from 5 to 1 is exponential, with headcount and cost doubling each step along the way. This is not a maturity model, but rather a desired outcome for an organization to match risk tolerance, budget, and threats of concern. The methodology is not to determine which products (if any) should be purchased, but to define a set of capabilities to accomplish specific security goals. The effectiveness of those capabilities relies heavily on another aspect of security that drives the approach: the people aspect. Good governance and processes, as well as secure architecture and configuration, all play a crucial role in any security program.

Critical Start's professional and managed services and the related controls include a zero-trust policy, which are key differentiators in providing a high availability, 24/7 access for customers.

Critical Start, Inc. is divided into three different departments: development, professional services and managed security service provider.

Critical Start offers three categories of service within Professional Services:

- **Advise** – Critical Start offers compliance guidance, cloud security architecture design and incident response. Moving to the cloud presents both new challenges and new opportunities from a security perspective. The Critical Start team can help an organization integrate security best practices and translate existing security requirements into cloud security controls. The company provides clients with a highly skilled CyberSOC team that works to identify the scope of breaches and acts quickly to reduce exposure and minimize the threat. Detailed reports are produced afterwards to aid in preventing future compromise.

- **Assess** – Critical Start offers Penetration testing, Red Team Assessments, Risk Assessments and a Tools Assessment. The Penetration Team evaluates an organization's security posture and determines how exposed the systems, services and data are to malicious actors. Risk Assessments are used to evaluate an organization's defenses, threats, and methods of mitigating associated risks. Through an inventory and understanding of deployed security controls and tools, Critical Start can provide an organization with a tools map to reach security goals and identify functionality gaps.

- **Implement** – Critical Start implements an experience of deep product knowledge to integrate technical solutions into a client's environment efficiently and effectively. The certified engineers can provide installations for endpoint security, next generation firewalls and SIEMs to maximize the effectiveness of log collection, analysis and reporting.

Critical Start also serves as a Managed Detection and Response Security Service Provider. Within the managed services, the company offers security event management, security orchestration through the Zero Trust Analytical Platform (ZTAP), incident response and workflow, Service Organization Control reporting and fully operationalized and automated security controls. The cloud-based, fully managed security operations center (SOC) was designed to leverage the most advanced capabilities to maximize threat detection and prevention. Through the services offered, clients receive fewer escalated alerts, more comprehensive monitoring and a convenient mobile interaction model. Critical Start is able to ingest 100% of potential alerts capable by a client's technical environment, review and resolve every alert, escalate alerts where necessary, and provide a quick response to prevent an unauthorized behavior by an environment. Our ability to scale effectively and efficiently is through our ZTAP application which can determine the difference between authorized and unauthorized behavior.

Overview of the System and Applications

System Overview

The System is comprised of the following components:

- ***Infrastructure***: The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software***: The programs and operating software of a system (systems, applications, and utilities)
- ***Data***: The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People***: The personnel involved in the operation and use of a system (developers, operators, users, and managers)

- ***Procedures***: The automated and manual procedures involved in the operation of a system.

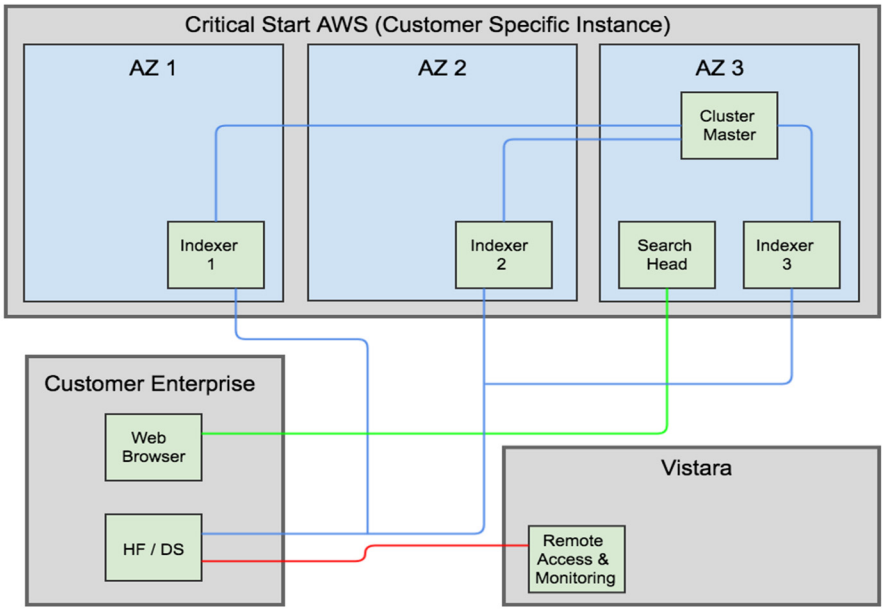
The IT environment has been stable throughout the period and there have been no significant changes to the system. The description does not omit or distort information relevant to the Critical Start's system. Critical Start acknowledges the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

Infrastructure

Critical Start MDR (Manage, Detect, and Respond) service provides a Security Operations Center function to customers to detect, investigate, and respond to cybersecurity threats. It combines people, processes and technologies to provide situational awareness through the detection, containment, and remediation of IT threats.

The specific MDR services to be provided to a customer determine the infrastructure deployed. Critical Start's Splunk architecture is hosted by Amazon Web Services (AWS Cloud). Other vendor products, such as Cylance and Duo, are hosted and managed in AWS by the respective vendor.

The Critical Start Splunk Server(s) deployment is a single tenant instance of VPCs within AWS. Each customer has its own segment and security group, and there is no resource or data sharing between customer Splunk instances. All segments are isolated via Zero-Trust Firewall Policies, allowing no visibility or access to any resources not implicitly whitelisted in the firewall configuration. The figure below shows a typical Splunk architecture for a customer.



The typical deployment includes:

- 2 or more Splunk Indexers running Linux in AWS
- 1 or more Splunk Search Heads running Linux in AWS
- 1 or more Splunk Forwarders/Deployment Servers at the customer premise
- Salt Enterprise
- Amazon SSM (Systems Manager)

Software

For Splunk, Critical Start collects data via on-site co-managed Heavy Forwarder / Deployment Server (HFDS) systems. These HFDS systems are remotely managed via a locally installed agent (Salt Enterprise / Amazon SSM), which allows configuration changes to Splunk configuration and tuning files. The agent allows Critical Start to remotely monitor and manage the local Splunk systems.

Additional data collection may be done from remote networks or sites via child Universal Forwarders (UF), which act as slaves to the master HFDS system for the environment. This allows tuning changes to be made remotely without direct access to UF systems.

The production elements deployed on site at a customer for Splunk include:

- The UF contains only the components that are necessary to forward data. The UF gets data from a variety of inputs and forwards the data to a Splunk deployment for indexing and searching. It can also forward data to another forwarder as an intermediate step before sending the data onward to an indexer.
- A heavy forwarder is a full Splunk Enterprise instance that can index, search, and change data as well as forward it. The heavy forwarder has some features disabled to reduce system resource usage.

Forwarders can transmit three types of data:

- Raw
- Unparsed
- Parsed

The type of data a forwarder can send depends on the type of forwarder it is, as well as how it is configured. UFs can send raw or unparsed data. Heavy forwarders can send raw or parsed data.

With raw data, the forwarder collects the data and sends it unaltered over a TCP stream; it does not convert the data into the Splunk communications format. This is particularly useful for sending data to a non-Splunk system.

With unparsed data, a UF performs minimal processing. It does not examine the data stream, but it tags the stream with metadata to identify source, source type, and host. It also divides the data stream into 64-kilobyte blocks and performs rudimentary timestamping on the stream that the receiving indexer can use in case the events themselves have no discernible timestamps. The UF does not identify, examine, or tag individual events, except when it is configured to parse files with structure data (such as comma-separated value files).

With parsed data, a heavy forwarder breaks the data into individual events, which it tags and then forwards to a Splunk indexer. It can also examine the events and perform conditional routing based on event data, such as field values.

Multiple indexers are used to ensure no single point of failure can result in lost data. Having multiple indexers is important, but it does increase the hosting costs in AWS.

For vendor products, such as Cylance and Duo, the customer installs endpoint software on various mobile devices, Windows machines, Linux servers, and OSX machines.

Data

- Critical Start collects event and log data via secure Internet connection from clients;
- Critical Start stores all data in the AWS data center, which is backed-up in accordance with an applicable MDR Agreement;
- Critical Start uses event and log data for incident analysis and investigation to determine if alerts or security events warrant incident classification. If an event is classified as an incident by Critical Start MDR staff, the company tracks the incident with the customer through final resolution; and
- Critical Start destroys all data once the service contract is cancelled or terminated per the MDR Agreement with clients.

People

The overall organization supports the framework for an effective control environment. The organization is comprised of the following functional areas:

Executive Management provides strategic direction and leadership for Critical Start and all of its domestic and international subsidiaries and affiliates. Executive Management oversees and is ultimately responsible for all aspects of service delivery (including business development, marketing, and quality assurance), and all corporate services functions including but not limited to finance, information technology, human resources, legal, real estate and facilities, and corporate development.

The MDR CISO leads the SOC mission through the coordination and management of SOC Analysts. This person ensures that analysts, processes and technology are meeting the SOC security monitoring, analysis and escalation objectives, organizational service level agreements and objectives, and metrics. In addition, they ensure daily operational processes effectively support SOC operations objectives:

- Execute continuous process improvement
- Interface with outside teams and customers
- Manage the process improvement program for SOC process
- Ensure that all SOC personnel issues are being addressed
- Make sure senior management is aware of any issues of problems
- Ensure all SOC staff receive development guidance in accordance with the practices and standards of the SOC

Critical Start is committed to equal opportunity of employment and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. Critical Start endorses a work environment free from discrimination and harassment.

Procedures

Critical Start provides monitoring services through ZTAP. This system is online and provides document management, statistical information and reports.

Critical Start establishes a new client account(s) and individual users from the documented service agreement contract. Those names listed as authorized individuals can provide name, e-mail and phone numbers for the purpose of having a new client account created in OneLogin.

Once new client accounts and individual users from the client account have been established within the system, the following activities occur to ensure that services are performed accurately, completely and timely:

- Open tickets to the CyberSOC team
- Perform Quality Assurance review
- Pull data for client review
- Upload/distribute information based on clients' requirements
- Host information for clients in Critical Start web-based system

Critical Start also has other logical security policies, procedures, and controls in place that are described in more detail in the following pages.

Scope

The scope of the review is limited to the Critical Start's Professional Services and Managed Detection and Response Services.

Control Environment

Key facets of the Company's control environment relating to processing and staffing for all processes performed by the Company are summarized below. These areas include:

- Integrity and Ethical Values
- Commitment to Competence
- Board of Directors Participation
- Management's Philosophy and Operating Style
- Human Resources Policies and Practices
- Organizational Structure and Assignment of Authority and Responsibility

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 Critical Start's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Critical Start's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices.

Commitment to Competence

Critical Start's management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Critical Start has focused on hiring experienced employees for the various positions required for the business.

Board of Directors Participation

Critical Start's control consciousness is influenced significantly by its board of directors and audit committee. A board of directors oversees management activities.

Management's Philosophy and Operating Style

Critical Start's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. Management monthly meetings are held to discuss operational issues.

Human Resources Policies and Practices

Critical Start's Human Resources policies and procedures relate to employee hiring, orientation, training, evaluating, promoting, compensating, and remedial actions.

Organizational Structure and Assignment of Authority and Responsibility

Critical Start's organizational structure provides the framework within which its activities for achieving entity- wide objectives are planned, executed, controlled, and monitored. Critical Start's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Critical Start has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Risk Assessment

Critical Start recognizes the importance of risk management in properly managing Critical Start and customer transactions and providing high-quality, cost effective services to its customers. The SVP of Managed Security Operations oversees an annual assessment of risk with respect to the industry, competition, IT processing environment and related application systems and services provided to users of the company's application systems. The annual assessment findings are communicated to the Board of Directors and risks are prioritized and managed to appropriate resolution.

Monitoring

The SVP of Managed Security Operations and MDR CISO monitor the quality of internal control performance as a normal part of the activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to (i) determine if objectives are achieved, (ii) identify any new risks that develop, and (iii) implement appropriate measures to address those risks. Critical Start adopts a proactive approach to the monitoring of application security to ensure that any issues or risks are addressed before becoming significant problems.

Monitoring of the Subservice Organization

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 Critical Start, to achieve Critical Start's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

Information and Communication

Description of Computerized Information Systems

The Critical Start production network is cloud-based and is segmented. Critical Start has a defendable network that is influenced by popular frameworks like PCI, NIST, SANS, ISO and ASD35. Industry standard network operating and database systems from major vendors are used to construct its network architecture, support database, and application systems. Critical Start has workstations throughout the company that have connectivity to the network or are stand-alone. In addition, ZTAP is a web-based system which resides on a secure server. Users access ZTAP through the Internet and data communication with clients is via VPN or HTTPS.

The operations and corporate facilities are located in Plano, TX. Critical Start, Inc. utilizes a combination local area network (“LAN”) / wide area network ("WAN") to share data among its employees. The corporate IT data center is located in the headquarters facility, contains no production/customer systems or data, and is accessible 24 hours a day, 7 days a week, and 365 days a year to authorized Critical Start personnel. Critical Start uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

Communication

Critical Start has established policies and procedures that are formally documented and clearly communicated to all employees.

Description of Complementary User Entity Controls

Critical Start Infrastructure controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of Critical Start Infrastructure’s controls are suitably designed and operating effectively, along with related controls at Critical Start Infrastructure.

SECTION FOUR:

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Critical Start, Inc. ("Critical Start") designs its processes and procedures related to our MDR Platform to meet its objectives for protecting organizations from a highly diverse, multi-faceted threat environment . Those objectives are based on our service commitments that Critical Start makes to our customers, the laws and regulations that govern MSSP / MDR services and the financial, operational and compliance requirements that Critical Start has established for the services.

Our compliance and security commitments to our customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of our service offering provided online. These commitments are standardized and include, but are not limited to, the following:

- Privacy principles within the fundamental designs of our MDR Platform that are designed to protect the privacy of customer data.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Access controls to ensure only authorized users access customer data and protect against unauthorized activity.
- Additional security and privacy principles documented through security frameworks such as SOC 2 and PCI.

Critical Start establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Critical Start'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 of our MDR Platform.