THREATQUOTIENT™

# Service Organization Controls (SOC) 2 Type 2 Report

January 1, 2021 to June 30, 2021

Report on Management’s Description of ThreatQuotient’s Processes Relevant to Security, Availability, and Confidentiality

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

# Section I – Assertion of ThreatQuotient

# Assertion of ThreatQuotient

We have prepared the accompanying description of ThreatQuotient's testing services titled "Description of the System" throughout the period January 1, 2021 to June 30, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the testing services that may be useful when assessing the risks arising from interactions with ThreatQuotient's system, particularly information about system controls that ThreatQuotient has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

We confirm, to the best of our knowledge and belief, that:

a) The description presents ThreatQuotient's testing services that were designed and implemented throughout the period January 1, 2021 to June 30, 2021 in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that ThreatQuotient's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c) The controls stated in the description operated effectively throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that ThreatQuotient's service commitments and system requirements were achieved based on the applicable trust services criteria.

ThreatQuotient

8/17/2021

# Section II – Independent Service Auditor’s Report

# Independent Service Auditor's Report

To the Board of Directors of

ThreatQuotient

## Scope

We have examined ThreatQuotient's accompanying description of its testing services throughout the period January 1, 2021 to June 30, 2021 (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that ThreatQuotient's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust service criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

## ThreatQuotient's responsibilities

ThreatQuotient 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 ThreatQuotient's service commitments and system requirements were achieved. ThreatQuotient has provided the accompanying assertion, titled *Assertion of ThreatQuotient* (assertion), about the description and the suitability of design and operating effectiveness of controls stated therein. ThreatQuotient is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

## Service auditor's responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- 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 the description is presented in accordance with the description criteria

- 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
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

### Inherent limitations

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 individual users may consider important to meet their informational needs.

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 risks 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, in all material respects:

a. The description presents ThreatQuotient's testing services that was designed and implemented throughout the period January 1, 2021 to June 30, 2021 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that ThreatQuotient's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of ThreatQuotient's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that ThreatQuotient's service commitments and system requirements were achieved based on the applicable trust services criteria.

### Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section IV.

### Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of ThreatQuotient, user entities of ThreatQuotient's Testing services during some or all of the period January 1, 2021 to June 30, 2021, business partners of ThreatQuotient subject to risks arising from interactions with the Testing services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

a. The nature of the service provided by the service organization
b. How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties
c. Internal control and its limitations
d. User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services
e. The applicable trust services criteria
f. The risks that may threaten the achievement of the service organization’s service commitments and system requirements, and how controls address those risks

BD & Company, Inc.

BD & Company, Inc.

Owings Mills, MD

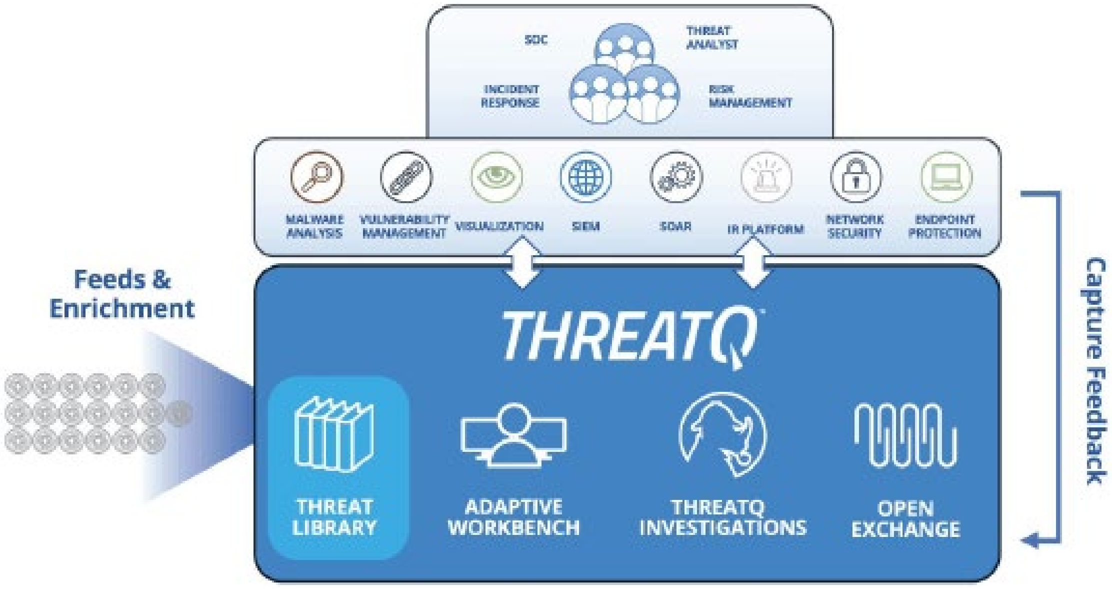
August 17, 2021

# Section III – Description of the System – ThreatQuotient's Processes Relevant to Security, Availability, and Confidentiality

# Description of System – ThreatQuotient’s Processes Relevant to Security, Availability, and Confidentiality

## Services Provided

ThreatQ™ is an open and extensible platform that accelerates and simplifies investigations and collaboration within and across teams and tools, supporting multiple use cases--including threat intelligence management, threat hunting, incident response, spear phishing, fraud, alert triage and vulnerability management.



<u>Key components of the ThreatQ platform include:</u>

### Threat Library ™

The Threat Library aggregates millions of threat-focused data points from both internal systems and external sources into a central repository, augmenting and enriching internal events and data with external threat data provides context for scoring and prioritization, based on parameters set by your organization. As more data and context is gathered, the library self-tunes—ensuring relevance and making the Threat Library increasingly more customized and valuable to your organization.

### Adaptive Workbench ™

The Adaptive Workbench streamlines the analysis of threat and event data for faster investigation and automates the intelligence lifecycle. By integrating with existing tools and fitting within your existing workflow and processes, it enables situational understanding, better decision making and automated actions that accelerate security operations across a wide variety of use cases.

## Open Exchange ™

The Open Exchange solves the organizational challenge of integrating existing security solutions within a single platform to increase value. ThreatQ supports an ecosystem of over 200 feed and product integrations out of the box, provides easy-to-use tools for creation of custom integrations, and streamlines security operations and management across an organization's existing infrastructure. With an SDK, easy-to-use APIs and a comprehensive set of industry-standard interfaces, the Open Exchange enables comprehensive integration with the equipment, tools, technologies, people, organizations and processes that protect the business.

## ThreatQ Investigations ™

The industry's first "cybersecurity situation room", ThreatQ investigations delivers collaborative threat analysis, shared understanding and coordinated response. Built on top of the ThreatQ platform, ThreatQ Investigations allows for capturing, learning and sharing of knowledge. This results in a single visual representation of a complete investigation—including "who did what and when," and creates a shared understanding across all components of the investigation: threat data, evidence and users.

### Managed Hosting

For customers that do not want the responsibility of administering an instance of ThreatQ in their own environment, a managed hosting option is available where the system is managed and monitored by ThreatQuotient Operations. Daily snapshots are created with a seven day retention period, and contractual service-level agreements (SLAs) are adhered to. Security Operations monitors each instance for malicious command and code execution, proactively scans for malware, and investigates anomalies when discovered.

Our mission is to improve the efficiency and effectiveness of security operations through ThreatQ, our threat-centric platform that saves organizations time and money. We achieve this by helping our customers:

### 1. Improve Detection and Accelerate Response

Organizations are bombarded with information from internal alerts, as well as from external threat data. This includes millions of threat-focused data points from multiple data feeds, including those from commercial sources, open source communities, industry associations and security vendors. Internal system data comes from sources including SIEM and advanced analytics platforms, log management repositories, endpoint detection and response, case management systems, vulnerability management solutions, and other security infrastructure. The ThreatQ Threat Library reduces noise and false positives by automatically aggregating and correlating external threat intelligence and internal threat and event data for context and relevance.

Inefficiencies in security operations and investigations commonly arise among team members acting independently with limited visibility into the tasks other teams are performing. Important commonalities are missed, so investigations take longer, hit a dead end, or key information falls through the cracks. ThreatQ provides increased collaboration, coordination and communication within and across teams—streamlining analysis by allowing teams to work from a common data set using existing tools and processes. ThreatQ Investigations, the industry's first cybersecurity situation room, delivers real-time visualization and collaboration within an investigation as it unfolds.

Fragmentation is the enemy of understanding and speed. Create a truly integrated security architecture with the ThreatQ platform that serves as the glue to bring together disparate data sources, enrichment and analysis tools, and layered security controls.

### 2. Make Better Decisions, Faster

Organizations need a deeper understanding of their threat landscape, which is where the threat landscape at large and their own infrastructure characteristics and configuration intersect. The ThreatQ platform acts as a central repository to define that intersection and ensure relevance to a specific organization.

Faster decision making requires the ability to quickly focus on the right intelligence. Customer-controlled prioritization, based on the organization's risk profile and their own set of scoring parameters, brings focus – not "global" risk scores published by some threat intelligence providers. With these parameters in place, ThreatQ automatically filters out what is "noise" and reveals the right priorities for action.

As new data and context become available and are added to the Threat Library and teams add observations and documentation from previous investigations, the self-tuning Threat Library learns and improves over time. Intelligence is automatically reevaluated and reprioritized so that teams continue to stay focused on what matters in a highly dynamic environment.

### 3. Get More from Existing Resources – Teams, Technologies and Processes

When teams are bogged down in mundane tasks and reacting to alerts, they don't have the time to combat real threats and conduct investigations quickly to mitigate risk, or to proactively strengthen defenses. Automate previously manual tasks from daily workflows, like aggregating, normalizing and prioritizing data via the Threat Library, and make advanced tasks like investigations more efficient and effective with the Adaptive Workbench and ThreatQ Investigations.

A truly integrated defense requires the sharing of intelligence across technologies to accelerate and improve security operations. As discussed previously, the ThreatQ platform aggregates data from external and internal sources and systems. It also enhances existing tools through bi-directional integration—sending curated threat intelligence to existing platforms within your environment, such as:

a. Case management and SIEM solutions, allowing these technologies to perform more efficiently and effectively – delivering fewer false positives
b. Enforcement technologies (firewalls, anti-virus, IPS/IDS, web and email security, endpoint detection and response, NetFlow, etc.) to generate and apply updated policies and rules proactively, strengthening security controls and mitigating risk.

Security teams are typically organized into silos and each use their own tools; sharing information across these teams to take advantage of potential synergies is complex. Using established workflows individual team members and different security teams can access the intelligence they need through the Adaptive Workbench, instantaneously share knowledge, and use their processes and tools of choice to improve security posture and reduce the window of exposure and breach.

### 4. Support Multiple Use Cases with a Single Platform

The ways in which people use technology continue to evolve, and threat actors are adapting. Organizations must be able to quickly adapt their defenses. An extensible platform with a flexible data model provides an efficient and effective approach. The ThreatQ platform was architected with a RESTful API and SDK, so customers have the freedom and capability to integrate with best-of-breed technologies and intelligence. The MITRE ATT&CK framework, for example, is leveraged to support threat intelligence management, threat hunting, incident response, spear phishing, fraud, alert triage and vulnerability management. A flexible data model allows teams to collect and work with data in a form that more accurately reflects their operational environment and workflows. They can then analyze and enrich that data with context so that they are able to more effectively hunt, investigate, triage and remediate.

For organizations that lack the breadth of expertise or depth of experience to adapt their defenses quickly enough, ThreatQuotient offers professional services and training to supplement in-house teams. The objective is to establish programs and processes, define best practices and transform the capabilities of enterprise security operations through knowledge transfer.

# Principal Service Commitments and System Requirements

## Service Commitments

ThreatQuotient designs its processes and procedures to meet the objectives defined for facilitating the best possible product experience for its customer base. Those objectives are based on the service commitments that ThreatQuotient makes to user entities, the laws and regulations that govern the provision of ThreatQuotient services, and the financial, operational, and compliance requirements that ThreatQuotient has established for the services. 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:

- Use of encryption technologies to protect customer data both at rest and in transit which implement valid modern cryptographic cipher requirements.
- Frequent security audits of the environment.
- Prevent malware from being introduced to production systems.
- Maintain production system uptime in accordance with ThreatQuotient's service-level agreements.
- Adhering to the principles of “least privilege” and “strict need to know” which are implemented in multiple facets of internal operations to compartmentalize information flow and access to achieve confidentiality.
- Maintaining a comprehensive Information Security Management System which defines an organization-wide approach to how systems and data are protected. These include policies around how the products are 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 all products by ThreatQuotient.
- Comprehensive logging of all system activities to identify anomalous behavior.
- Commitment to data security and privacy as defined in the General Data Protection Regulation (GDPR) and EU-U.S. Privacy Shield agreement.

ThreatQuotient utilizes Amazon Web Services, Inc. (AWS) to maintain its IT infrastructure and product offerings. As such, ThreatQuotient relies on AWS service commitments related to file backups, retention, business continuity and disaster recovery planning, and availability requirements. ThreatQuotient recognizes AWS as a critical vendor for business operations and reviews AWS service agreements and third-party assessments at least annually to ensure alignment of AWS commitments to ThreatQuotient's operational and business objectives.

### System Requirements

ThreatQuotient creates system requirements to achieve our service commitments and maintain compliance with applicable laws and regulations. The system requirements include access control standards, employee on-boarding and decommissioning, risk and vulnerability management, system monitoring, vendor management, incident response, periodic access reviews, and system change control standards. These requirements are communicated through ThreatQuotient's policies, procedures, and contractual arrangements.

The Information Security Management System (ISMS) defines an organization-wide approach for how systems and data are secured. These include policies around how the service is designed and developed, how the internal business systems and networks are managed, and how employees are hired and trained. Standard operating procedures have also been documented on how to carry out specific manual and automated processes required in the operation and development of the services.

## Components of the System Used to Provide the Services

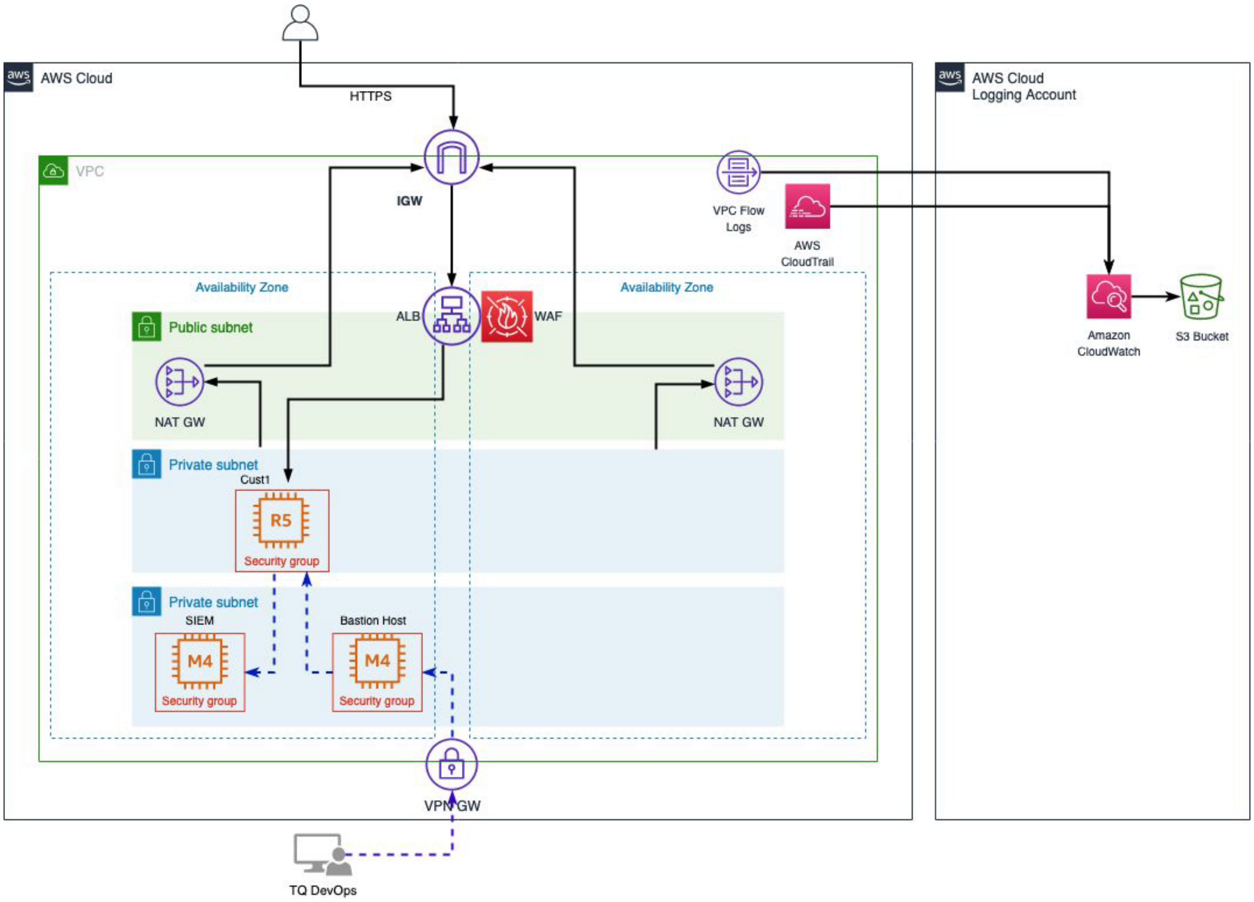
### Software

ThreatQuotient's ThreatQ platform is built on a software stack which consists of the following services: Apache, PHP, MariaDB, Python, and Solr. ThreatQuotient has a documented procedure for deploying a new instantiation of the ThreatQ hosted platform. The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

| Application or Service | Description | OS Components | Physical Location |
|---|---|---|---|
| ThreatQ | ThreatQuotient’s Security Operations Platform | CentOS, Docker-ce, Apache, PHP, Python, MariaDB, Solr | Multiple AWS Regions |
| AWS EC2 | Virtualized network and processing infrastructure to host ThreatQ | N/A | |
| AWS ELB | Virtualized network load balancer for directing traffic | N/A | |
| Ansible | Configuration management and deployment of ThreatQ | N/A | |
| OSSEC | Filesystem monitoring and alerting | N/A | |

## Infrastructure

ThreatQuotient leverages AWS for hosting instances of ThreatQ for customers in data centers located in geographically appropriate zones for the customer's specific needs. Instances are isolated from the internet on a private subnet with only an application load balancer (ALB) and web application firewall (WAF) allowing HTTPS access. Instances are also isolated from each other by VXLAN segmentation. A bastion host is used to relay temporary ssh connectivity as part of the zero-trust implementation used for system maintenance by the Operations team. Specific port allowances are made between the private subnets using security groups for security information event management (SIEM) logging. SEIM access is only available to specific Operations team individuals.



## People

### Operations: DevOps/IT and SecOps

The operations team consists of Development Operations (**DevOps**) , **IT** , and Security Operations (**SecOps**). Each portion of the team has a unique role to play in regards to supporting customers and general business operations.

**DevOps/IT** manages the full lifecycle of hosted environments including provisioning, disaster recovery plan execution, maintenance, and off-boarding. They are responsible for interfacing with engineering and/or support to address any issues that arise with the product. Additionally, they manage systems which facilitate business operations, monitoring hosted environments for performance and availability, and resolve any network or DNS related issues. All assets and inventory are managed by IT.

**SecOps** continually monitors the hosted environment for vulnerabilities, intrusions, indicators of compromise and the like. In addition to monitoring, they are responsible for auditing all platforms and vendors, vulnerability management and awareness, coordinating regular application and environmental penetration tests, and enforcing compliance throughout various facets of the company.

### Support

The support group provides technical assistance to verified ThreatQ customers to meet the terms and conditions defined in the ThreatQ Hosted Subscription Agreement.

### Finance / Human Resources

The Finance team in addition to handling all aspects of finance, processes agreements and interfaces with our legal council during negotiations. Human Resources reports to the CFO and is responsible for all aspects of employee management and well-being. HR is also responsible for coordinating employee reviews and mediating any fraud related incident.

## Data

ThreatQuotient believes that data privacy and security are the cornerstones for trusted relationships. We strive for conformity to the General Data Protection Regulation (GDPR) and are obliged to comply with verifiable requests pertaining to personal data handling. We have further committed to cooperate with EU Data Protection Authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) as set forth in the EU-U.S. Privacy Shield agreement. Additional information can be reviewed on our public privacy policy: https://www.threatq.com/privacy-policy/

Customer data residing on the hosted platform is stored on an encrypted EBS volume in AWS data centers (our third-party data processor), however, AWS does not have access to this data in an unencrypted format. A limited number of authorized users on the Operations team are able to temporarily access customer data strictly for maintenance purposes. When this access is granted, all actions are meticulously logged during the access period.

Customer instance volumes have snapshots taken daily at 2AM EST and are retained for a period of seven days. Should a customer make a valid request for deletion of any of the snapshots, we are obligated to comply per GDPR.

As defined in our Customer Off-Boarding policy, a Backup Artifact will be generated from the customer’s hosted ThreatQ Instance one day after the contractual completion date. After the artifact is generated, it will be stored for a period not exceeding three months. ThreatQuotient will deliver the artifact to the former customer without undue delay. The instance will be powered off two weeks after the contractual completion date, but kept in our account for the period of one month beginning after the power down. After one month has passed, the ThreatQ Instance will be deleted. After three months have passed since the contractual completion date, the Backup Artifact for the former environment will be deleted. These retention periods are in good faith and are still subject to GDPR's statute of "Right to Erasure". ThreatQuotient will comply immediately with verified data removal requests.

# Control Environment

The control environment is the basis for ThreatQuotient's internal operations and control. The objective of the control environment is to set the tone for the corporate mode of operation.

## Board of Directors and Assignment of Authority and Responsibility

ThreatQuotient's Board of Directors meet on a quarterly basis to review corporate governance, which defines their roles, responsibilities, meeting frequency, and other discussion topics. Meeting notes are recorded which include agenda, participants, and date the meeting occurred. The Board consists of a majority of independent members that also include principal investors and industry experts which apply their expertise in challenging the Executive team on their execution of business objectives.

The Executive team sets strategic operational objectives at least annually and reviews progress with the Board of Directors during these sessions. Each objective is disseminated to the functional business units for execution by the Management team. Progress toward the objectives are evaluated at least quarterly by the Executive and Management teams.

The structure of the company and its critical suppliers are reviewed routinely with the Board, through informal and formal quarterly meetings. Reporting lines are reviewed regularly by the CEO and Senior executives to ensure efficient management of the company's objectives. Designation of responsibilities and segregation of duties is under the direction of the CEO and Senior Executive team. This structure is reviewed as part of regular reviews with the Board of Directors. The Senior Executive team considers security, availability, processing integrity, confidentiality, and privacy when defining the authorities and responsibilities of the organization; The management team and the Board understand the need for the company to interact with external parties and apply the appropriate measures to monitor the authorities and responsibilities of the organization.

## Integrity and Ethical Values

Integrity and ethical values are fundamental components of the control environment being that they govern the design, administration, and monitoring of critical processes. ThreatQuotient's values and behavioral standards are communicated to personnel through policy statements, and by the examples set by executive management. These values are documented in the ThreatQuotient Code of Business Conduct, which employees and contractors are required to acknowledge on a periodic basis.

ThreatQuotient has four pillars of values, which are expected to be understood and followed:

- Respect For The Employee
- Respect For The Customers
- Respect For The Shareholders
- Assumption of Goodwill

## Management Philosophy and Operating Style

In addition to promoting the Code of Business Conduct, internal policies, laws, and regulations; ThreatQuotient management is expected to foster a culture of ethical and compliance-oriented behavior. Through mentoring, training, communication, and team building, ThreatQuotient is committed to developing a trust environment that makes ethical conduct the easiest and default option. ThreatQuotient believes that in addition to having an open door policy, holding regular one-on-one meetings between managers and subordinates is key to maintaining open channels of communication to provide quick feedback and remediate or reward any situation that arises.

Company-wide recognition for outstanding performance via a peer submitted nomination program provides an achievement objective and promotes integrity within the organization.

## Security Management

ThreatQuotient has a dedicated Security Operations (SecOps) team who is part of the operations team. This cross-functional group is responsible for executing security practice in all aspects of company operations, but the SecOps engineer is responsible for developing, maintaining, and enforcing the Information Security Management System (ISMS) of policies. The ISMS is reviewed annually by security operations, the Director of IT, and SVP of Engineering to ensure it aligns with the objectives of the organization.

Security awareness is a constant feature of communication to the organization since vulnerabilities can be discovered at any time. SecOps monitors the environment for known vulnerabilities and communicates the remediation steps to the company in a timely manner. Training exercises are performed regularly, as much as once per quarter, to keep employees sharp to current exploit techniques. Operations takes a special interest in employees that fail these tests to ensure they're receiving the proper education to protect company assets.

SecOps performs an annual review of all active vendors, and an ad-hoc review of prospective vendors. Verification of common certifications such as SOC2 / ISO 27001 / PCI DSS are acquired for each company, otherwise a security questionnaire is provided to the vendor during the review process to ensure compliance with standard secure operating practices.

## Security Policies

ThreatQuotient maintains a comprehensive Information Security Management System (ISMS) which addresses the following areas of concern:

- **Data Classification -** Data type definitions and proper handling procedure.
- **Encryption Standards -** Acceptable algorithms, cipher suites, and disk encryption methods.
- **Password Requirements -** Password complexity requirements.
- **Access Management -** Standards for access restriction and enforcement.
- **Change Control -** Standards and procedures for implementing change requests.
- **Asset Management -** Asset lifecycle management requirements.
- **Vendor Management -** Standards for vendor assurance.
- **Incident Response -** Incident response policy and procedure.
- **Human Resources Security -** Standards for employment verification and security training.

## Personnel Security

As part of the standard hiring process, all prospective employees are subject to a background check, reference check, and verification of employment eligibility. All new positions have clearly defined job descriptions and expectations for baseline access to resources. Since a policy of 'least privilege' is adhered to, role based access controls are implemented to restrict classes of employees from accessing specific information. All employees are subject to following the defined policies and procedures and will experience sanctions for violations of these processes. Employees are instructed to report all potential security incidents to the security@threatq.com alias.

ThreatQuotient implements a whistleblower policy which encourages employees to notify a supervisor or a representative from HR about concerns of fraudulent or illegal activity without fear of retaliation or confidentiality exposure.

## Physical Security and Environmental Controls

### Physical

ThreatQuotient leverages AWS for hosting instances of ThreatQ for customers in data centers located in geographically appropriate zones for the customer's specific needs. AWS data centers are housed in facilities that are not branded as AWS facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, their access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

### Environmental

#### Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

#### Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

#### Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

#### Management

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

## Change Management

ThreatQuotient has a formalized change control process implemented into the ISMS which requires that change requests be submitted through the official channels defined by IT to ensure record keeping compliance. When the requests are received, they are categorized and prioritized, then analyzed and subsequently justified if the request is warranted. After a request has passed the analysis of the receiver, it is approved and scheduled for implementation. The implementation phase follows the Plan-Do-Check-Act Cycle (PDCA) to ensure the change will have a positive outcome.

Finally, a post-implementation review is conducted to verify that the change did not have unintended consequences.

The SecOps team primarily focuses on monitoring existing systems for vulnerabilities and configuration issues and creating tickets to inform the proper group of administrators to remediate the problem. The SecOps team then continues to monitor the situation and will follow-up if necessary.

The DevOps team is solely responsible for managing software changes in hosted environments. Through regular upgrade intervals or specific change requests through the ticketing system, they ensure that customer environments are regularly patched and updated to mitigate vulnerabilities.

The IT team is responsible for managing software changes on internal infrastructure required for business operations. Through regular upgrade intervals or specific change requests through the ticketing system, they ensure that internal infrastructure is regularly updated to mitigate vulnerabilities.

## System Monitoring

The Operations teams use a variety of utilities to detect possible security threats and incidents. These utilities include, but are not limited to, system performance time series data, intrusion detection systems (IDS) or intrusion prevention system (IPS) alerts, vulnerability scanning reports, filesystem change alerts, and operating system event logs. Alerts with a high enough severity level are immediately brought to the attention of the security team via email and instant message notifications; Alerts below a specific severity level are not sent instantaneously and are reviewed daily by the SecOps team.

Security events of a sufficient severity that require incident response have a ticket created and are worked and monitored until a resolution is achieved. As part of the incident response policy, an executive summary is provided at the completion of the incident and retained for posterity.

## Problem Management

Customers typically report issues through the official ThreatQuotient Support means via their account login with Salesforce. There is a documented process for support engineers to escalate a request to either Engineering or Operations depending on the nature of the situation. Customers also have the option of discussing ongoing issues with their Customer Success representative to achieve greater visibility.

Internally reported problems are submitted through a preferred ticketing system directly to Operations. The operations engineer will make the determination of who to direct the request toward or will work on the issue until resolution.

## Data Backup and Recovery

ThreatQuotient takes data resiliency very seriously. It's our top priority to ensure our customers experience as little interruption in service as we’re able to achieve. Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) are defined in the Service-Level Agreement (SLA) that is part of the contract negotiation process, but as a general rule, snapshots are taken daily at 2AM EST and the RTO is approximately 15 minutes.

Snapshots are retained for 7 days and replicated to a different data center to ensure a single site failure at AWS will not impede our customers’ ability to operate. Access to backups / snapshots are restricted to specific authorized personnel on the Operations team. The Disaster Recovery (DR) Policy is tested twice a year by actual execution to ensure we can achieve our objectives. The DR policy is also reviewed at least once a year to make sure the process aligns with current goals, but is subject to change if the process needs to be refined midway through the year. All changes are analyzed for potential conflicts in contractual requirements.

## System Account Management

System access requests are directed toward authorized Operations personnel utilizing their preferred ticket management system. The request is verified independently for assurance of validity. If the request is validated, Operations grants access by adding the user to the appropriate group to conform with Role-Based Access Controls (RBAC). If group permissions are not a possibility, then individual user access will be granted. When users take on new roles and responsibilities within the company, a review of their permissions is required to identify any potential violation of 'least privilege' or 'need to know'. This is handled primarily through RBAC, however, exceptions will occur hence the need for review. A monthly Access Review meeting occurs between SecOps and IT to ensure the Access Control policy is being followed and that inappropriate accounts are not allowed to exist.

When a user exits the company or an authorized contractor is no longer under contract, then their permissions are revoked across all systems after the completion of their last day. With centralized user management and RBAC implemented, this is a simple process of deactivating the prime user account. Notification of this action is sent to all Operations administrators automatically.

To be absolutely clear: **In-scope system access is only provided to a handful of authorized users on the Operations team. All authentications are logged to an external system, privilege escalations also trigger an instant message alert to the Operations team.**

Our password policy dictates that all passwords must have the following characteristics:

- At least 16 characters
- Contain a combination of upper and lower case letters, numbers, and symbols
- Must not contain your username and/or legal name
- All system password changes must be logged and archived for auditing purposes
- Email notifications should be sent out whenever possible to notify of any potential or actual change in passwords
- User passwords must expire after 180 days
- New passwords cannot be the same as the previous 3 passwords in historical rotation

Customers' hosted instances maintain a separate authentication mechanism for accessing the web interface versus accessing the command line. Customers are able to either use local accounts or tie their internal authentication mechanisms to the ThreatQ web UI authentication to achieve Single-Sign-On (SSO) which ThreatQuotient does not have access to. We have temporary command line access granted to select individuals on the Operations team for maintenance purposes. We apply a Zero-Trust model when authenticating maintenance accounts on customer systems. With this model of time-restricted token issuance for user authentication, coupled with centralized identity management, we are able to leverage an implicit deny policy with temporary access grants, as well as block access to all systems and services with a single account deactivation.

## Risk Assessment Process

ThreatQuotient regularly reviews risks that may jeopardize the delivery of service commitments and system requirements. In all aspects of data handling and transference, careful consideration is made to ensure that we maintain confidentiality, integrity, and availability, and privacy.

The Security Operations team monitors systems, processes, and procedures for inherent risk on a consistent basis. System and Application risk is monitored through persistent vulnerability monitoring, alerting, and data mining of captured event logs. Penetration tests are coordinated multiple times per year for various aspects of our operations. Third-party application security assessments are performed once per year; Environmental security assessments are performed once per quarter.

Finance maintains a system of regulatory controls to ensure fraud is identified quickly. A segregation of duties is maintained with additional cross-checking for accuracy. A yearly audit is performed by an external public accounting firm to ensure compliance.

Security Operations coordinates with various stakeholders in each department to perform an annual security assessment of all vendors that ThreatQuotient utilizes. Current vendor certifications are verified, otherwise a security questionnaire is provided to the vendor to ensure they are compliant with secure operating procedures.

An annual review of all policies included in the Information Security Management System (ISMS) is performed by Security Operations and Senior Operations Executives to ensure it continues to align with the goals and objectives of our company. Changes in the security threat landscape will occasionally require a more frequent review of these policies.

## Information and Communication Systems

The Operations team coordinates with HR to disseminate security education and training during on-boarding of new staff. Regular training exercises are performed to keep the employee base aware of current exploitation tactics and prepare them for real world scenarios. Broad scope and targeted phishing campaigns are used on a quarterly basis to keep employees on the ready.

One of the primary communication goals for the Operations team is to inform employees of the impact that individuals have on company security. The mantra of employee accountability, responsibility, and diligence is repeated so the thought is embedded in all processes. We believe it’s better for staff to take their time and be cautious but confident about their actions rather than execute in a hurry and face regret. The individual is the front line of security in any company, it is everyone's responsibility to hold the line.

## Monitoring Controls

All changes to user accounts are logged and instant notifications are sent out to all authorized members of the Operations team. Authentication attempts are logged on each system individually in addition to being logged remotely with our identity management system. Full audit logs are recorded for every action.

Customer environments are monitored for all filesystem level changes. Any time a file changes, an authentication occurs, a privilege escalation occurs, the event is logged for later analysis. If the event is considered of higher significance, such as a privilege escalation, then the Operations team is notified immediately through instant message and email.

A monthly access review is performed within Operations to verify who currently has access, who has not used their access recently, and who is not supposed to have access. A record is maintained of when these meetings occur and what changes are made as a result of the meeting.

## Changes to the System During the Period

Though there will be bug fixes and features added to the ThreatQ system during the course of the audit, there will not be any fundamental changes in how the system functions between the evaluation period of January 4, 2021 to March 31, 2020.

# Section IV – Description of Criteria, Controls, Tests and Results of Tests

## Description of Criteria, Controls, Tests, and Results of Tests

The two tables comprising section IV describe the applicable Trust Services Criteria and the controls to meet the criteria that have been specified by, and are the responsibility of, ThreatQuotient. The testing performed and the results of the tests are the responsibility of the service auditor. Unless specifically noted in the columns "Conclusion of Testing" and "Resolution", no deviations resulted from testing. The first table displayed below under sub-section "Description of Criteria" outlines the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report and the associated Control Activities (CA). The second table displayed below under sub-section "Client Controls and Testing Performed" outlines the client controls, the related common criteria, and the results of service auditor's test and the testing performed.

### Description of Criteria

| ***TSP Ref #*** | ***Trust Services Criteria*** | ***Associated Control Activities*** |
|---|---|---|
| **CC1.0** | **Control Environment** | |
| CC1.1 | The entity demonstrates a commitment to integrity and ethical values. | TQ-01,TQ-08 |
| CC1.2 | The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | TQ-01 |
| CC1.3 | Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | TQ-02 |
| CC1.4 | The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | TQ-05, TQ-07, TQ-24 |
| CC1.5 | The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | TQ-05, TQ-07 |
| **CC2.0** | **Communication and Information** | |
| CC2.1 | The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | TQ-12, TQ-14, TQ-15 |
| CC2.2 | The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | TQ-06, TQ-24 |
| CC2.3 | The entity communicates with external parties regarding matters affecting the functioning of internal control. | TQ-15 |
| **CC3.0** | **Risk Assessment** | |
| CC3.1 | The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | TQ-22, TQ-23 |

| ***TSP Ref #*** | ***Trust Services Criteria*** | ***Associated Control Activities*** |
|---|---|---|
| CC3.2 | The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | TQ-04, TQ-23 |
| CC3.3 | The entity considers the potential for fraud in assessing risks to the achievement of objectives. | TQ-22 |
| CC3.4 | The entity identifies and assesses changes that could significantly impact the system of internal control. | TQ-04, TQ-06, TQ-23 |
| **CC4.0** | **Monitoring Activities** | |
| CC4.1 | The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | TQ-12, TQ-20 |
| CC4.2 | The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | TQ-14 |
| **CC5.0** | **Control Activities** | |
| CC5.1 | The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | TQ-06 |
| CC5.2 | The entity also selects and develops general control activities over technology to support the achievement of objectives. | TQ-06, TQ-18 |
| CC5.3 | The entity deploys control activities through policies that establish what is expected and in | TQ-06 |
| **CC6.0** | **Logical and Physical Access Controls** | |
| CC6.1 | The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | TQ-13, TQ-18, TQ-19, TQ-20, TQ-21 |
| CC6.2 | Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | TQ-19, TQ-20, TQ-21 |
| CC6.3 | The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity’s objectives. | TQ-19, TQ-20, TQ-21 |
| CC6.4 | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives. | TQ-09 |

| ***TSP Ref #*** | ***Trust Services Criteria*** | ***Associated Control Activities*** |
|---|---|---|
| CC6.5 | The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | TQ-09 |
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | TQ-11, TQ-26 |
| CC6.7 | The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | TQ-11 |
| CC6.8 | The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | TQ-13 |
| **CC7.0** | **System Operations** | |
| CC7.1 | To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | TQ-12 |
| CC7.2 | The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | TQ-12 |
| CC7.3 | The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | TQ-14 |
| CC7.4 | The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | TQ-14 |
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | TQ-14 |
| **CC8.0** | **Change Management** | |
| CC8.1 | The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | TQ-10 |
| **CC9.0** | **Risk Mitigation** | |
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | TQ-16, TQ-17, TQ-23 |
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | TQ-04, TQ-23 |

| ***TSP Ref #*** | ***Trust Services Criteria*** | ***Associated Control Activities*** |
|---|---|---|
| **A1.0** | **Availability** | |
| A1.1 | The entity maintains, monitors, and evaluates current processing capacity and use of system components. | TQ-25 |
| A1.2 | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | TQ-16, TQ-17 |
| A1.3 | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | TQ-16, TQ-17 |
| **C1.0** | **Confidentiality** | |
| C1.1 | The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality. | TQ-03, TQ-26, TQ-27 |
| C1.2 | The entity disposes of confidential information to meet the entity’s objectives related to confidentiality. | TQ-03, TQ-26, TQ-27 |

### Client Controls and Testing Performed

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| TQ-01 | Executive management including independent board members, representation from ThreatQuotient management, and investors participate in quarterly Board of Directors meetings. These meetings include updates from the heads of various functional areas (including sales, business development, finance, marketing, and engineering/support) and address company strategy and objectives. | Verified that the Board of Directors meetings address items that have a direct relationship to the operations of ThreatQuotient. | No Exceptions Noted | CC1.1, CC1.2 |
| TQ-02 | ThreatQuotient has a defined organizational structure which is documented in a formalized organization chart including direct reporting lines. Job descriptions are maintained to define the roles and responsibilities for each position. | Verified that lines of authority and supervision are clear within the organizational chart. | No Exceptions Noted | CC1.3 |
| TQ-03 | As defined in the Customer Off-Boarding Policy, a Backup Artifact will be generated from the customer's hosted ThreatQ instance one day after the contractual completion date. After the artifact is generated, it will be stored for a period not exceeding three months. ThreatQuotient will deliver the artifact to the former customer without undue delay. The instance will be powered off two weeks after the contractual completion date, but kept in our account for the period of one month beginning after the power down. After one month has passed, the ThreatQ Instance will be deleted. After three months have passed since the contractual completion date, the Backup Artifact for the former environment will be deleted. ThreatQuotient complies immediately with verified data removal requests. | Verified that the Hosted Customer Off-Boarding Policy outlines comprehensive details to assist with the processes of data handling when an evaluation period is complete or when a customer chooses not to renew their contract. Verified that no customers were off-boarded from the hosted platform during the audit period. | No Exceptions Noted | C1.1, C1.2 |
| TQ-04 | SecOps performs an annual review of all active vendors, and an ad-hoc review of prospective vendors. Verification of common certifications such as SOC2 / ISO 27001 / PCI DSS are acquired for each company, otherwise a security questionnaire is provided to the vendor during the review | Verified that reviews are performed at least annually for active vendors by assessing related security documentation. | No Exceptions Noted | CC3.2, CC3.4, CC9.2 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| | process to ensure compliance with standard secure operating practices. | | | |
| TQ-05 | The SecOps team undergoes training exercises regularly to keep employees sharp to current exploit techniques. Operations takes a special interest in employees that fail these tests to ensure they are receiving the proper education to protect company assets. | Verified that a process is in place to provide periodic industry training to the SecOps team. | No Exceptions Noted | CC1.4, CC1.5 |
| TQ-06 | ThreatQuotient maintains a comprehensive Information Security Management System (ISMS) which addresses the following areas of concern:<br>▪ Data Classification - Data type definitions and proper handling procedure.<br>▪ Encryption Standards - Acceptable algorithms, cipher suites, and disk encryption methods.<br>▪ Password Requirements - Password complexity requirements.<br>▪ Access Management - Standards for access restriction and enforcement.<br>▪ Change Control - Standards and procedures for implementing change requests.<br>▪ Asset Management - Asset lifecycle management requirements.<br>▪ Vendor Management - Standards for vendor assurance.<br>▪ Incident Response - Incident response policy and procedure.<br>▪ Human Resources Security - Standards for employment verification and security training.<br><br>The ISMS is reviewed annually by Security Operations, Director of IT, and SVP of Engineering to ensure it aligns with the objectives of the organization. | Verified that policies and procedures adequately lay out the responsibilities of employees in regard to security and confidentiality of the business.  Verified that policies and procedures are updated and reviewed at least annually. | No Exceptions Noted | CC2.2, CC3.4, CC5.1, CC5.2, CC5.3 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| TQ-07 | As part of the standard hiring process, all prospective employees are subject to a background check, reference check, and verification of employment eligibility. All new positions have clearly defined job descriptions and expectations for baseline access to resources. All employees are subject to following the defined policies and procedures and will experience sanctions for violations of these processes. | Verified that new hires are required to complete a successful background check before employment. | No Exceptions Noted | CC1.4, CC1.5 |
| TQ-08 | ThreatQuotient implements a Whistleblower Policy which encourages employees to notify a supervisor or a representative from HR about concerns of fraudulent or illegal activity without fear of retaliation or confidentiality exposure. | Verified that the Whistleblower Policy contains information for employees to reference in the scenario during which illegal or dishonest activities are identified. Verified that no whistleblower events occurred during the audit period. | No Exceptions Noted | CC1.1 |
| TQ-09 | Access to ThreatQuotient offices is managed by the Office Management team and key fobs are provisioned by the office administrator for each location. Only employees who will be in their respective office multiple times per week are provisioned a key fob to reduce the number of fobs in circulation. ThreatQuotient performs periodic fob inventories to ensure that fobs are only assigned to active and appropriate employees.<br>A small data center is located in the Mt. Airy office and access is controlled by a lock with a pin combination that is provided to limited members of the IT team and is changed when anyone with physical access to the Mt. Airy office is terminated. | Verified that adequate security measures are used to control access to the physical office and server room. | No Exceptions Noted | CC6.4, CC6.5 |
| TQ-10 | ThreatQuotient has a formalized change control process implemented into the ISMS which requires that change requests be submitted through the official channels defined by IT to ensure record keeping compliance. When the requests are received, they are categorized and prioritized, then analyzed and subsequently justified if the request is warranted. After a request has passed | Verified that change requests followed the appropriate change management workflow. | No Exceptions Noted | CC8.1 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| | the analysis of the receiver, it is approved and scheduled for implementation. The implementation phase follows the Plan-Do-Check-Act Cycle (PDCA) to ensure the change will have a positive outcome. Finally, a post-implementation review is conducted to verify that the change did not have unintended consequences. | | | |
| TQ-11 | Instances are isolated from the internet on a private subnet with only an application load balancer (ALB) and web application firewall (WAF) allowing HTTPS access. Instances are also isolated from each other by VXLAN segmentation. ThreatQuotient has firewalls in place for both the Development (FortiGate) and production environments (ASA) to protect against external threats. | Verified that the network diagram outlines mechanisms in place to protect the environment from external access by unauthorized actors. | No Exceptions Noted | CC6.6, CC6.7 |
| TQ-12 | IT management monitors the IT environment, including monitoring for changes to system configurations that could result in vulnerabilities. Vulnerability scans using Tenable.IO are performed on specific subnets as well as a weekly scan specifically on the VPN gateway to identify risks to the corporate IT security. The ThreatQuotient Security team reviews the results of all vulnerability scans. For each identified vulnerability, the Security team will either provide remediation via configuration changes/deploy security patches, implement other mitigating measures/controls, or document an exception to describe why a certain vulnerability is not being addressed. | Verified that vulnerability scan results are reviewed and then associated risks are tracked and managed. | No Exceptions Noted | CC2.1, CC4.1, CC7.1, CC7.2 |
| TQ-13 | Intrusion prevention and malware threat detection is performed by Wazuh and all code check-ins are scanned as part of ClamDB to ensure artifacts are free of malware. SELinux is enabled on all customer systems to prevent unauthorized file system changes. | Verified that Wazuh, ClamDB, and SELinux are in place to protect the environment from malicious code/malware. | No Exceptions Noted | CC6.1, CC6.8 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| TQ-14 | Per the Incident Management Policy, security events of a sufficient severity that require incident response have a ticket created and are worked and monitored until a resolution is achieved. As part of the Incident Response Policy, an executive summary is provided at the completion of the incident and retained for posterity. | Verified that security events requiring incident response are assessed and resolved through an investigative process using a Jira ticket and executive summary report. | No Exceptions Noted | CC2.1, CC4.2, CC7.3, CC7.4, CC7.5 |
| TQ-15 | Customers typically report issues through the official ThreatQuotient Support means via their account login with Salesforce. There is a documented process for support engineers to escalate a request to either Engineering or Operations depending on the nature of the situation. Customers also have the option of discussing ongoing issues with their Customer Success representative to achieve greater visibility. | Verify that mechanisms are in place for ThreatQuotient customers to report issues to ThreatQuotient management. | No Exceptions Noted | CC2.1, CC2.3 |
| TQ-16 | Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) are defined in the Service-Level Agreement (SLA) that is part of the contract negotiation process, but as a general rule, snapshots are taken daily and the RTO is approximately 15 minutes. Snapshots are retained for 7 days and replicated to a different data center. Access to backups / snapshots are restricted to specific authorized personnel on the Operations team. In order to ensure systems can be recovered back to a prior release, source code is deposited into escrow for each release and retained. | Verified that processes and standards are in place for the performance of backups related to both customer instances and internal IT systems. | No Exceptions Noted | CC9.1, A1.2, A1.3 |
| TQ-17 | The Disaster Recovery (DR) Policy is tested twice a year by actual execution to ensure we can achieve our objectives. The DR Policy is also reviewed at least once a year to make sure the process aligns with current goals, but is subject to change if the process needs to be refined midway through the year. All changes are analyzed for potential conflicts in contractual requirements. | Verified that the Disaster Recovery Policy adequately addresses all necessary disaster recovery areas. Verified that the Disaster Recovery Plan is reviewed and tested at least bi-annually. | No Exceptions Noted | CC9.1, A1.2, A1.3 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| TQ-18 | Our Password Policy dictates that all passwords must have the following characteristics:<br>▪ At least 16 characters<br>▪ Contain a combination of upper and lower case letters, numbers, and symbols<br>▪ Must not contain your username and/or legal name<br>▪ All system password changes must be logged and archived for auditing purposes<br>▪ Email notifications should be sent out whenever possible to notify of any potential or actual change in<br>passwords<br>▪ User passwords must expire after 180 days<br>▪ New passwords cannot be the same as the previous 3 passwords in historical rotation | Verified that the Password Policy contains adequate requirements related to password minimum length, password complexity, and password age. Verified that the Okta password configurations meet the requirements of the Password Policy. | No Exceptions Noted | CC5.2, CC6.1 |
| TQ-19 | System access requests are directed toward authorized Operations personnel utilizing their preferred ticket management system. The request is verified independently for assurance of validity. If the request is validated, Operations grants access by adding the user to the appropriate group to conform with Role-Based Access Controls (RBAC). If group permissions are not a possibility, then individual user access will be granted. When users take on new roles and responsibilities within the company, a review of their permissions is required to identify any potential violation of 'least privilege' or 'need to know'. | Verified that access requests were appropriately submitted to and processed by IT. | No Exceptions Noted | CC6.1, CC6.2, CC6.3 |
| TQ-20 | A monthly Access Review meeting occurs between SecOps and IT to ensure the Access Control Policy is being followed and that inappropriate accounts are not allowed to exist. | Verified that access modifications are appropriately monitored. | No Exceptions Noted | CC4.1, CC6.1, CC6.2, CC6.3 |
| TQ-21 | When a user exits the company or an authorized contractor is no longer under contract, then their permissions are revoked across all systems, by means of deactivating the prime user account, after the completion of their last day. Notification | Verified that user access is removed within a timely manner after termination. | No Exceptions Noted | CC6.1, CC6.2, CC6.3 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| | of this action is sent to all Operations administrators automatically. | | | |
| TQ-22 | Finance maintains a system of regulatory controls to ensure fraud is identified quickly. A segregation of duties is maintained with additional cross-checking for accuracy. A yearly audit is performed by an external public accounting firm to ensure compliance. | Verified that a system of regulatory controls is in place to identify fraud risk. | No Exceptions Noted | CC3.1, CC3.3 |
| TQ-23 | The Security Operations team monitors systems, processes, and procedures for inherent risk on a consistent basis. System and application risk is monitored through persistent vulnerability monitoring, alerting, and data mining of captured event logs. Penetration tests are coordinated multiple times per year for various aspects of our operations. Third-party application security assessments are performed once per year; environmental security assessments are performed once per quarter. | Verified that the results of risk assessments are properly documented and resolution items are tracked, as applicable. | No Exceptions Noted | CC3.1, CC3.2, CC3.4, CC9.1 |
| TQ-24 | The Operations team coordinates with HR to disseminate security education training during onboarding of new staff. Regular training exercises are performed to keep the employee base aware of current exploitation tactics and prepare them for real world scenarios. Broad scope and targeted phishing campaigns are used on a quarterly basis to keep employees on the ready. | Verified that new hires complete security education training during onboarding. Verified that phishing campaigns are administered on a recurring basis. | No Exceptions Noted | CC1.4, CC2.2 |
| TQ-25 | ThreatQuotient uses Prometheus Monitoring to monitor and alert on system performance for both their hosted and internal systems. Prometheus will alert IT management based on time series event logging to ensure system uptime is maintained. | Verified that system performance and capacity is monitored by Prometheus Monitoring and that alerts are enabled to inform IT management of issues. | No Exceptions Noted | A1.1 |
| TQ-26 | JAMF endpoint management and full-disk encryption are enabled for user devices. | Verified that endpoint protection and full-disk encryption are enabled for user devices. | No Exceptions Noted | CC6.6, C1.1, C1.2 |

| ***Control Activity Number*** | ***Client Control*** | ***Conclusion of Testing*** | ***Resolution*** | ***Associated Criteria*** |
|---|---|---|---|---|
| TQ-27 | The Data Classification Policy defines the types of data that are considered restricted and confidential. The policy includes descriptions for which information falls under each category controls around the management of the data. | Verified that the Data Classification Policy includes definitions and controls for management of data defined as restricted and confidential. | No Exceptions Noted | C1.1, C1.2 |