Qualia

How Qualia Protects Against & Responds to Security Threats

Cybersecurity is constantly evolving. New threats emerge every day as cybercriminals continue to develop new methods of exploiting vulnerabilities in information technology (IT). This document provides an overview of how Qualia proactively protects against and responds to evolving security threats.

Inventory Management

It's incredibly hard to defend what you don't know you have, which is why the first step of any security program is to take an inventory of the company's IT assets. An IT asset can be anything owned or managed by Qualia that has value to Qualia or its customers—some piece of data shared by a customer, an employee laptop, a service provided to our customers, or intellectual property.

Qualia maintains an inventory of every asset. With that inventory, Qualia groups asset types together into asset classifications based on their relative value and level of importance, allowing us to understand which assets may be more likely to be targeted by attackers.

Understanding the Threat Landscape

Business email compromise (BEC)—and by extension, wire fraud—is particularly prevalent in the real estate industry, as is the rising trend of ransomware. BEC, wire fraud and ransomware are examples of a threat: something that could have an adverse effect on Qualia's assets. Threats are not necessarily human-driven. For example, a natural disaster can negatively impact the assets of a business just as much as a cybercriminal's attack.

The threat landscape can vary from industry to industry. Therefore, it is extremely important to study threats that are impactful to the real estate industry, especially as they continue to evolve. Qualia leverages a variety of resources to understand the real estate threat landscape, including government agencies such as US-CERT, communities of industry security researchers, and the breach disclosures of other companies both within and outside the real estate sector.

Understanding the threat landscape allows Qualia to gain insight into what threats might target or impact specific assets. Knowing this information allows Qualia to implement controls and test systems to determine where these threats are most likely to target so that our team can proactively prevent successful attacks and system failures.

Security Testing and Vulnerability Management

By understanding our assets and threats, Qualia can test for vulnerabilities. A vulnerability is any kind of weakness that can make a threat more likely to negatively impact an asset. Examples include a software bug or a business process that doesn't properly safeguard data.

Qualia has a range of tools to test for vulnerabilities. For example, with software bugs, Static Analysis Security Testing (SAST) is used to audit source code for flaws, and Dynamic Analysis Security Testing (DAST) to send malicious input to applications and ensure it is handled safely. Similarly, Business Continuity and Disaster Recovery (BCDR) tests help identify any vulnerabilities that may impact business availability or delay recovery in the event of a disaster.

As an industry best practice, Qualia regularly commissions external penetration tests. In an external penetration test, Qualia engages with a company reputable at doing these specific types of tests, to attempt breaking into its systems. If successful, Qualia can immediately identify the vulnerability and act swiftly to correct it.

Based on the impact a vulnerability would have on an asset and the likelihood it would be exploited by a threat, each vulnerability is given a service level agreement (SLA), measured in days, by which it must be fixed. This process ensures accountability and prioritizes vulnerability remediation.

Monitoring & Incident Response

Our holistic view of assets and periodic testing helps Qualia understand "normal" baseline behavior and "abnormal" behavior. (We also set up a variety of alerts and notifications to stay apprised of the well-being of our assets and their use.) If an alert or notification indicates abnormal behavior, it is promptly investigated by Qualia's dedicated security team. An investigation may include (as appropriate) a review of system logs, network traffic, access history, and more to determine whether a threat may have had, or is likely to have a negative impact on an asset.

If an event is determined to have a material adverse impact on our systems or customer data, the incident response process is initiated, bringing all hands on deck to respond to the situation. This process is methodically defined and includes processes around mitigating the threat, reporting the situation to customers, regulators, and/or government bodies, and identifying mechanisms to ensure a similar incident never happens again. This process is regularly tested in "dry run" scenarios to ensure that all stakeholders are trained in how to execute the process effectively, should the need arise.

Conclusion

Qualia has a multifaceted approach to proactively protect against and respond to security threats across products and the platform. Our monitoring and testing program is not static. The approach and tools used to monitor and respond are constantly evolving to stay ahead of security threats.