ROAR Third-Party Vendor Assessment Report

Vendor: Qualys
Assessor: Adam Richie-Halford, ROAR Information Security Officer

Overview

Qualys is a leading provider of cloud-based security and compliance solutions, offering a comprehensive platform for vulnerability management, continuous monitoring, and web application security. ROAR leverages Qualys Web Application Scanning (WAS) to ensure continuous web application security, vulnerability detection, and compliance monitoring. This assessment evaluates Qualys' compliance with recognized industry standards and its suitability as a third-party vendor for ensuring ROAR's web application security.

Certifications and Compliance

- **ISO 27001**: Qualys complies with ISO 27001, the international standard for information security management systems (ISMS). This certification ensures that Qualys implements rigorous security controls to protect sensitive information and maintain the confidentiality, integrity, and availability of customer data.
- **FedRAMP Authorized**: Qualys has been authorized under the Federal Risk and Authorization Management Program (FedRAMP) for moderate impact level systems, which certifies that it meets the stringent security requirements for federal information systems. This makes Qualys suitable for government and regulatory-sensitive environments.

Qualys' compliance certifications can be accessed via their Trust and Compliance.

Security Practices

- **Data Encryption**: Qualys employs AES-256 encryption for data at rest and HTTPS/TLS encryption for data in transit, ensuring that sensitive information is safeguarded during transmission and storage.
- **Access Control**: Role-based access control (RBAC) and multi-factor authentication (MFA) are used to secure user access to the Qualys platform. These measures ensure that only authorized personnel can access critical security data and management interfaces. Authorized ROAR employees authenticate into Qualys using Stanford SSO with MFA.

- **Incident Response and Monitoring**: Qualys follows a structured incident response process, which includes real-time monitoring, automated alerts, and a detailed plan for responding to and mitigating security incidents. ISO 27001 audits confirm that Qualys adheres to industry-standard incident detection and response practices.

Conclusion

Qualys meets the security and compliance requirements necessary to support ROAR's continuous monitoring and vulnerability management needs. With its ISO 27001 certification and FedRAMP authorization, Qualys upholds rigorous security standards for its cloud-based services.