Attestation of Secure Coding Practices

Archer's Product and Application Security organization has established a security program that applies across all Archer products and applications. This framework addresses all aspects of product security: Policy, People, Process and Technology.

Standardized Product and Application Security

Archer's internal Secure Development Lifecycle Standard is a common reference for the Archer product organizations to benchmark product and application secure development activities against market expectations and industry practices.

Security-Awareness Community

Archer offers a security training curriculum to educate new and existing Archer employees on job-specific security best practices and how to use relevant resources. Archer strives to create a security-aware culture across its entire community.

Repeatable, Secure Development Process

Archer's Secure Development Lifecycle (SDL) defines security controls that Archer product teams should adopt while developing new features and functionality. Archer's SDL includes both analysis activities, as well as, prescriptive proactive controls around key risk areas. The analysis activities, such as threat modeling, static code analysis, scanning and security testing, are intended to discover and address security defects throughout the development lifecycle. The prescriptive controls are intended to ensure that development teams code defensively to prevent specific prevalent security issues including those found in the OWASP Top 10 or SANS Top 25.

External Penetration Testing

Archer at a minimum annually engages the services of an external penetration company to assess the product applications ahead of our SOC2 audit. There are Letters of Attestation available for our product application PEN tests. They are available to our customers upon request.

We cannot share the scanner results, per the following company policy: Under Archer corporate policy we cannot provide more than the Letter of Attestation. In order to avoid potentially putting customers in our shared multihost environments at risk, Archer does not share the findings from internal security testing or other types of security activities with external entities. We provide customers copies of letters of attestation from independent third-party testing as a good faith act to demonstrate that we have undertaken the effort, time, and expense to have an external entity verify that Archer has properly secured its systems and software.

Vulnerability Response

Archer strives to help its customers minimize risks associated with security vulnerabilities in its products by providing them with timely information, guidance, and mitigation(s) to address threats from vulnerabilities. Archer employs a rigorous process to continually evaluate and improve its vulnerability response practices. See Archer's Vulnerability Response Policy for more information.