Tech Brief: Threat Modeling

Applicability

Threat modeling as part of the RingCentral Security Development Lifecycle.

Basis

RingCentral bases the security design of products and services on OWASP guidelines and NIST standards and validates this security design using threat modeling.

Process

Threat modeling is a structured process of reviewing product architecture to identify security vulnerabilities. Thus, threat modeling validates the application of security requirements in design. Examining both security and functionality in the product architecture avoids redesigning, recoding, and retesting against security issues later in product development.

RingCentral uses both tool-based threat modeling and traditional, manual mapping techniques. Using both allows the most coverage for a variety of risks. Traditional threat modeling methods require data flow diagramming and trust boundary analysis for potential threats. Tool-based methods automate the review of features and use cases to map remediation back to the security requirements. For instance, identifying attack surfaces and features such as authentication, use of cryptography, and file upload provides vital steps in threat modeling. This knowledge and the corresponding requirements provide information for remediation or mitigation.

Threat modeling is performed for new applications, new integrations, major redesigns, or new features with privacy or security implications.

Threat modeling is not the same as the use of vulnerability scanning tools, which look for vulnerabilities based on incorrect programming practices, that is, unsecure coding. In fact, vulnerability scanning is another activity in the Security Development Lifecycle (SDL) that is usually performed on code that has already undergone threat modeling. Completing SDL as a whole provides the best assurance of developing secure products than any one of its discrete activities such as threat modeling.