RingCentral

TECH BRIEF: RingCentral Threat Modeling

Applicability: Threat Modeling within the RingCentral Security Development Lifecycle

Why:

Customers want to understand how RingCentral conducts threat modeling as part of the Security Development Lifecycle (SDL).

What:

RingCentral validates the security design of products and services based on OWASP guidelines and NIST standards. These guidelines and standards help ensure the confidentiality, integrity, and availability of information and information systems.

Threat modeling is a structured process of reviewing product architecture to identify and quantify threats and potential vulnerabilities by criticality. Additionally, threat modeling enables the determination of security requirements. Examining both security and functionality in the product architecture avoids redesign, recoding, and retesting security issues later in product development.

How:

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 the 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.

When:

Threat modeling is not the same as the use of vulnerability scanning tools, which looks 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 based on successful 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.