ThreatModeler

CASE STUDY

Charles Schwab transforms threat modeling with AUTOMATION

Architects and developers drive threat modeling at scale, with security baked into every release.

OVERVIEW

A client-first approach to security

Investment services leader Charles Schwab Corporation offers brokerage, banking, and financial advisory services. The firm is dedicated to a client-centric approach, prioritizing the security of client information by continuously updating its technology, training its people, and refining protocols against emerging threats. Schwab chose ThreatModeler®, an automated threat modeling platform, to roll out a scalable, comprehensive practice that raises the security posture of its applications, platforms, and infrastructure, with architects and developers independently driving the work.

INITIAL CHALLENGES

A manual process that could not scale

Schwab followed a manual threat modeling process that was slow, repetitive, and heavily dependent on the security team, so it did not fit the firm's agile development practices.

- **Manual process:** Resource-intensive, repetitive threat modeling done by hand.
- **Security-team dependency:** Solution architects relied on security experts to identify threats and requirements.
- **Agile integration:** Threat modeling was cumbersome to fold into the agile development cycle.
- **Shift-left limits:** The process could not scale to keep up with a shift-left approach.

SOLUTION

Threat modeling the architects own

ThreatModeler made threat modeling painless for solution architects and drove widespread adoption across the architect community. The platform provides an extensive component library and lets teams codify custom threats and security requirements in a shared framework. Schwab integrated modeling into the development lifecycle, scaled it to architects with first-hand knowledge of each solution, and added an approval workflow tied to its governance processes.

> **Now, all our solution architects can use the drag-and-drop interface to threat model and automatically get the same benefits of having a security architect by their side to point out solution-specific threats and security requirements.**
>
> **Johnson Michael**
> Director of Enterprise Security Architecture, Charles Schwab

IMPACT & RESULTS

Faster models, lower cost, stronger compliance

A risk-based approach let Schwab prioritize higher-risk applications, while automation gave architects and security engineers time back for other priorities. Treating threats at the design phase reduced rework and remediation costs, and uniform security requirements strengthened adherence to standards across projects.

50%

reduction in threat-modeling effort

10X

improvement in model production

- **Shift-left security:** Threat modeling integrated into the lifecycle; solution-specific requirements added to the backlog.
- **Uniform practice:** Consistent threat modeling across applications and platforms, performed by the architects closest to each solution.