BISHOP FOX

contact@bishopfox.com
P 480 621 8967
F 480 383 6401

www.bishopfox.com

Threat Modeling is the practice of conceptualizing your organization's worst security fears–and how to mitigate against them

THREAT MODELING
You are already doing it.

You are doing it.

We all do threat modeling daily. Whether it is buckling your seatbelt when you get in your car or turning on your alarm system before you leave your house, you're already engaging in some form of threat modeling.

Why Threat Model?

Every organization is a target. Threat modeling is a way of realistically viewing a high-risk situation and how you would circumvent it.

So, if the situation should ever manifest, your organization knows the next steps to take and isn't left helpless or scrambling to act as the smoke clears.

BISHOP FOX

contact@bishopfox.com
P 480 621 8967
F 480 383 6401

www.bishopfox.com

How Do I Start?

Begin with a diagram that includes data flows, internal and external processes, and identified trust boundaries. You'll need to balance the level of detail with enough information to understand a system's purpose (but without going too deep into specifics of port numbers or variable names).

You can search for applicable threats whether by identifying potential threat actors, building attack threes, creating attack scenarios, or playing the card game, "Elevation of Privilege" (EOP).

From there, evaluate the model across separate teams (design, engineering, operations, support). You need to ask the critical questions: "What did we miss? Are the responses valid? Did we file a ticket/bug/action item for each mitigation? What is our highest priority?" Be objective.

What else should I know?

Your first few attempts at threat modeling might be rough, but with time, you will improve at thinking of the threat to your security holistically and considering every aspect of the equation. You will eventually become aware of threats you never previously considered and become adept at addressing threats before they escalate into security events or incidents.

To learn more ...

Escalation of Privilege (EOP) Card Game (created by Microsoft):

www.microsoft.com/en-us/SDL/adopt/eop.aspx

STRIDE Threat Model:

https://msdn.microsoft.com/enus/library/ee823878(v=cs.20).aspx

Dread Risk Assessment Model:

http://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/

The OCTAVE Method:

www.cert.org/resilience/products-services/octave/

Subscribe to our blog:
https://www.bishopfox.com/blog/2017/12/your-worst-case-scenario-an-introduction-to-threat-modeling/

Discuss threat modeling with an expert:

contact@bishopfox.com | 480 621 8967