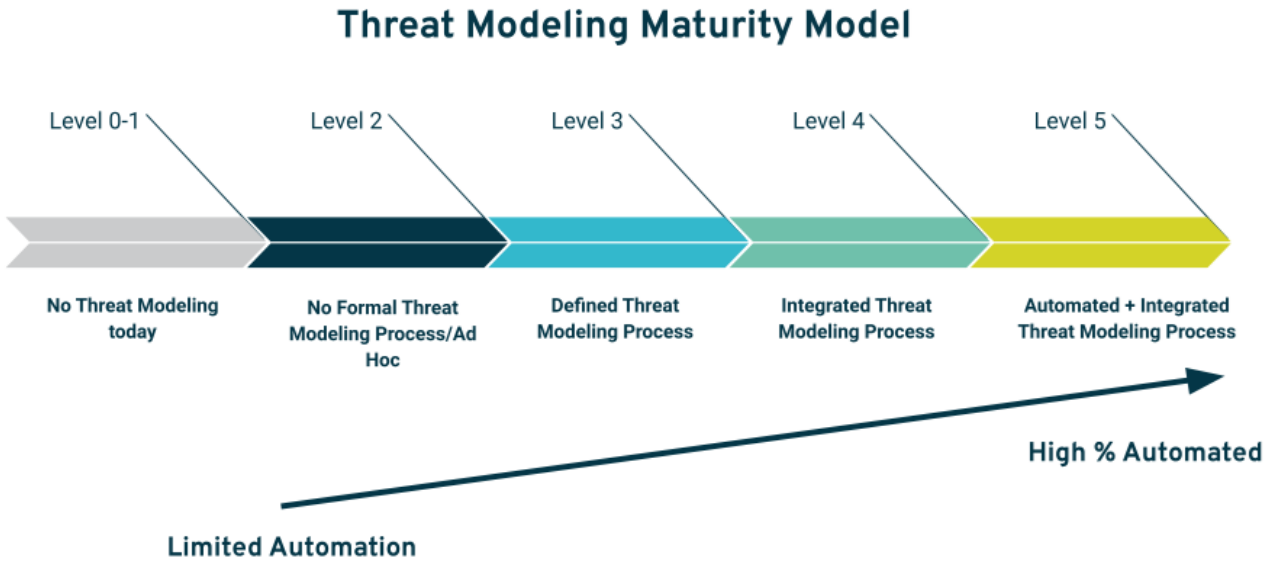
OKRs Unleashed: Supercharging Threat Modeling Effectiveness

Agenda

“An **Objective** is simply what is to be accomplished. It should be a crisp, one-line statement that is meaningful, action-oriented, and, ideally, inspirational.”

“**Key Results** should be specific and time-bound. They should be measurable and able to be assigned a grade at the end of the OKR cycle.”



Threat Modeling Program Maturity

Simple model that focuses on Process, Integration, and Automation

Threat Modeling Program Maturity

Level 1

No Threat Modeling is being done >>> Adhoc Threat Modeling

Objective

Start creating threat models for new systems prior to any code or systems changes

Key Results

Organization has provided 2 hours of threat modeling training to end users by end of March

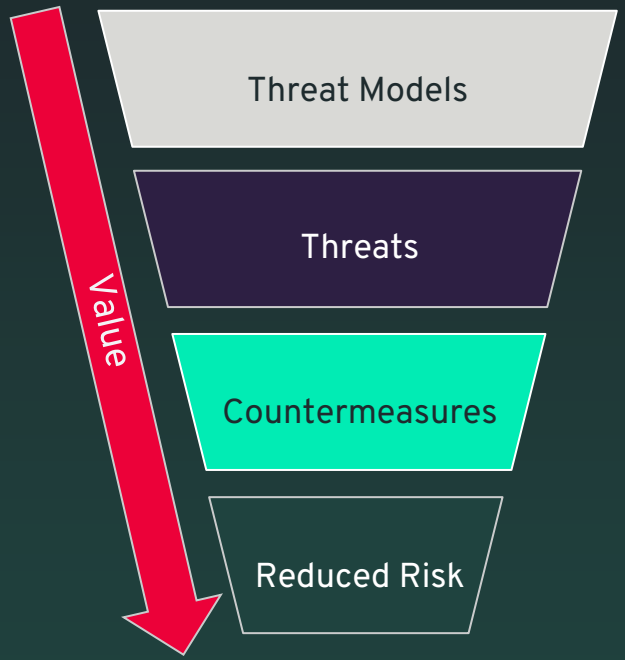
Organization has created a single bad threat model by end of March

KPIs - Threat Models Created, Trained Users (net)

Threat Model Value

What is the actual value of a threat model?

Value = Returns - Costs



HIGH ROI Threat Models

Relevant Scope

Prioritized Threats

Prioritized Countermeasures

Reduced Risk

Threat Modeling Program Maturity

Level 2

Adhoc Threat Modeling >>> Defined Threat Modeling Process

Objective

Create a systematic process that produces a consistently acceptable threat model.

Key Results

Threat Modeling process is defined, documented, and taught to relevant stakeholders

All v1 threat models are completed in 8 hours or less

KPIs - Avg Threat Model Time (in stages), Threat Model Qty, Threat models per SDLC stage

HIGH ROI Process

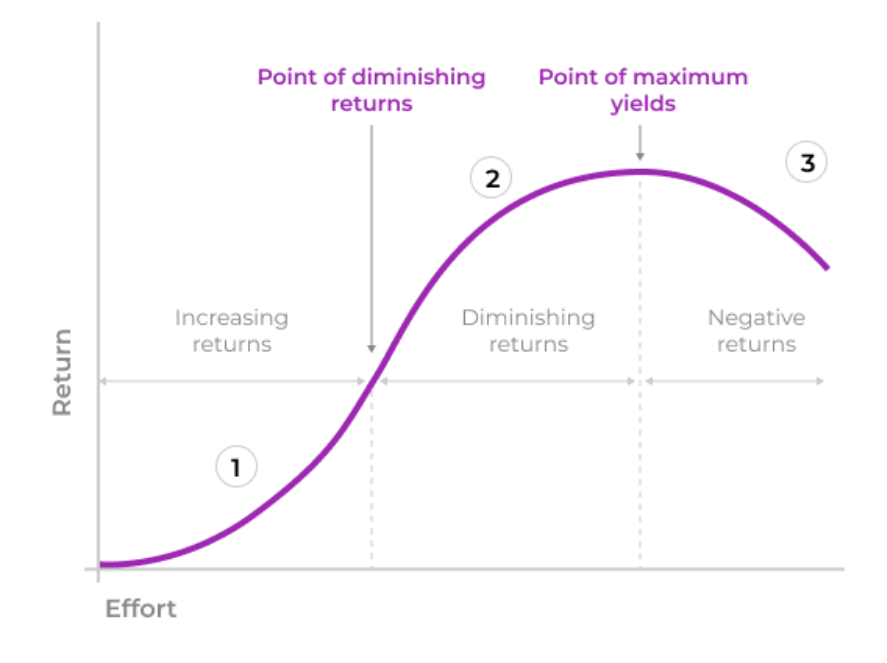
Shift Left

Secure by Default

Net Security Change vs perfect representation

Diminished Marginal Returns

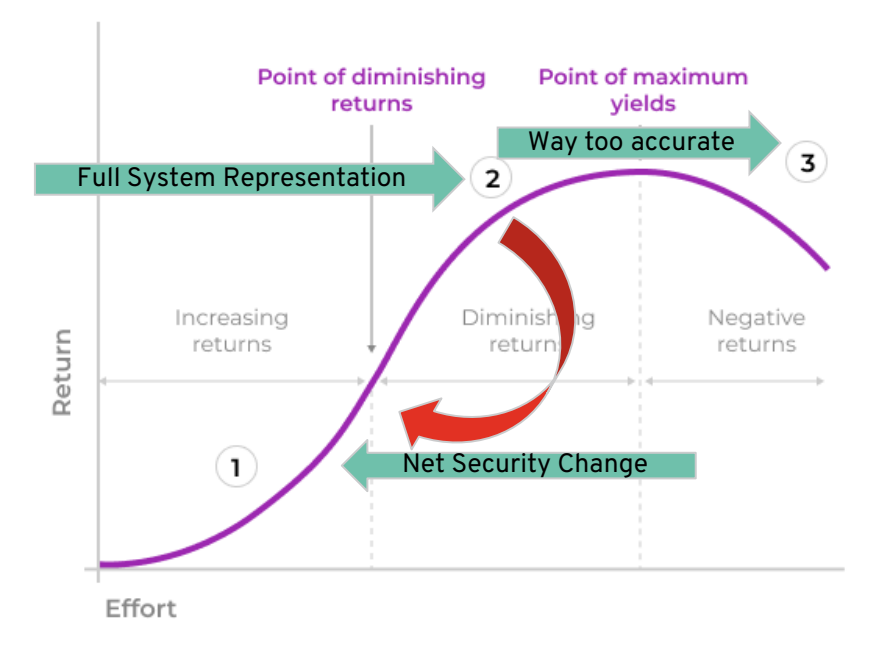
As the effort to create value (net return) increases the net value of the return is diminished over time.



Don't read the fine print - Image liberated from https://uxmag.com/articles/law-of-diminishing-returns-design-and-decision-making

Diminished Marginal Returns

As the effort to create value (net return) increases the net value of the return is diminished over time.



Don't read the fine print - Image liberated from https://uxmag.com/articles/law-of-diminishing-returns-design-and-decision-making

Threat Modeling Program Maturity

Level 3

Defined Threat Modeling Process >>> Integrated Threat Modeling Process

Objective

Defined process is integrated across the organization

Key Results

Integration points are documented and prioritized by end of Q1

Change management plan is documented and disseminated to all stakeholders by end of Q2

KPIs - Security Champions, Improvement Plan Existence

HIGH ROI Integrations

Governance Risk Management & Compliance

Architectural Review

Threat Modeling Program Maturity

Level 4

Integrated Threat Modeling Process >>> Automated Threat Modeling Process

Objective

Business integrated process is sustained and scaled through automation

Key Results

All net IaC changes are analyzed and threat modeled by end of Q3

Manual translation of information has been reduced by 50% by end of Q3

KPIs - Automated Threat Models, Issues created by automation, dashboards vs manual reporting

HIGH ROI Automation

Issue Tracker Integration

Standardized Threats

Automated Actioning

Template driven threat models

Questions?