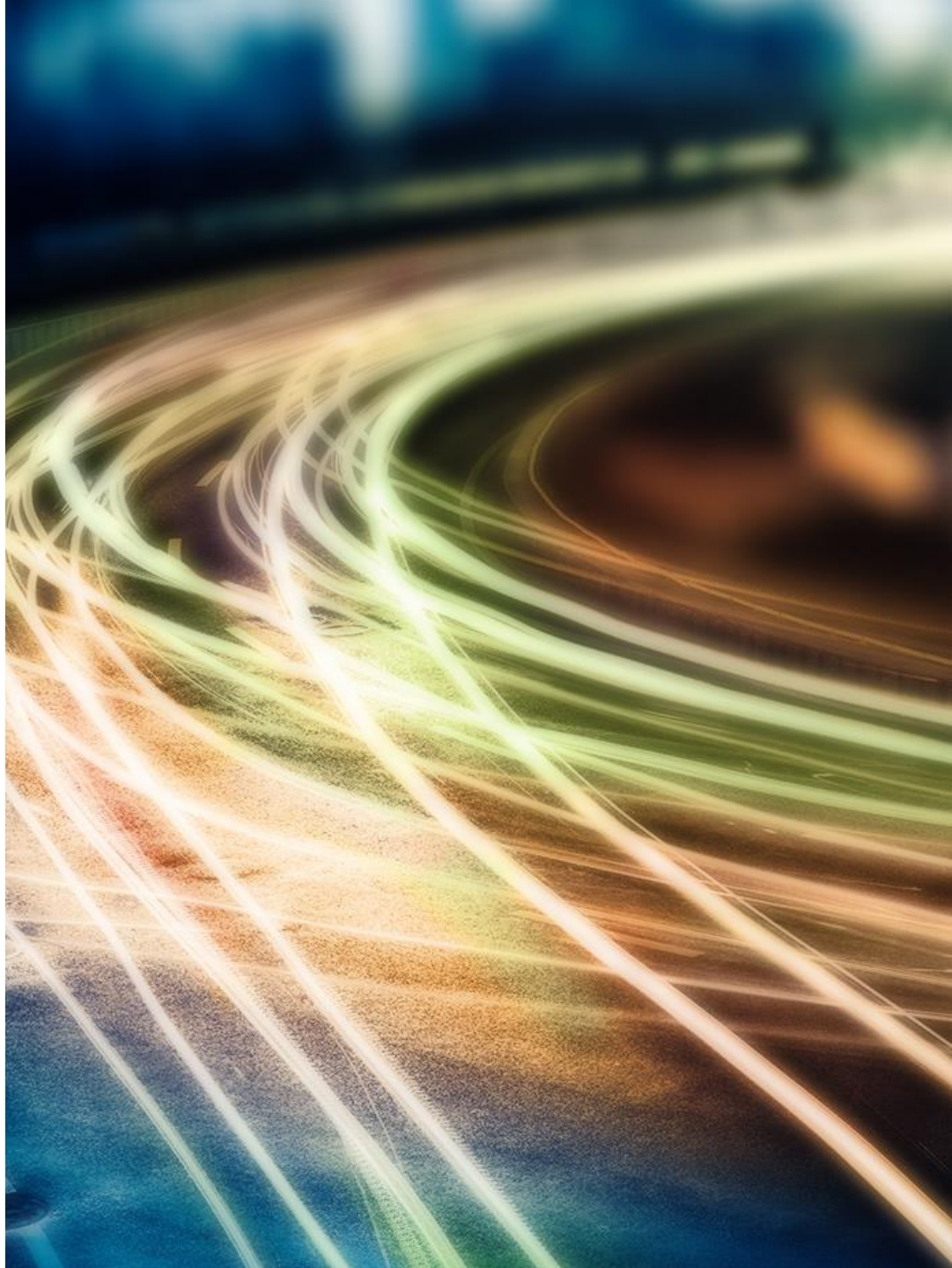
Proper Threat Modeling Techniques

Dexter Law



omnitracs
innovation. driven.

DevOps Principles

With the goal of closing the gap between IT operations and development to improve communication/collaboration and align objectives faster and more efficiently delivery

- Automation
  - Automate everything from workflows to testing new code
- Iteration
  - Write smalls chunks of code during a time-box sprint to support releases and rereleases that increase the speed and frequency of deployment
- Continuous Improvement
  - Continuously test, learn from failures, and act on feedback in order to optimize performance, cost and time to deployment
- Collaboration
  - Unite teams, foster communication and breakdown silos between deployment, IT operations, and quality assurance

omnitracs
innovation. driven.

What is Threat Modeling?

Threat Modeling a technique used to help you identify **Threats**, **Attacks**, **Vulnerabilities**, and **Countermeasures** that could affect your **applications,** software, systems, networks, and business processes, etc.

- It's about understanding your system in a risk-based way
- Offers a strategic practice by which you can think about system characteristics
- Provides visibility into weaknesses that may affect not only the application, but potentially the entire organization

omnitracs
innovation. driven.

The Purpose

Including threat modeling in the Software Development Lifecycle/DevOps toolchain can help

- Build a secure design
- Efficient investment of resources; appropriately prioritizing security, development, and other task
- Bringing security and development together to collaborate on shared understanding, informing development of the system
- Identify threats and compliance requirements, and evaluate their risk
- Define and build required controls

omnitracs
innovation. driven.

What to include

Your threat model should include the following:

- A description / design / model of what of the whatever you're building or worrying about
- A list of assumptions that can be checked / challenged I the sure as the threat landscape changes
- A list of potential threats to the system
- A list of actions to be taken for each threat
- A way of validating the model and threats, and verification o success of actions taken for each threat
- A way of validating the model and threats, and varication of sues of actions taken

omnitracs
innovation. driven.

The Purpose

Including threat modeling in the Software Development Lifecycle/DevOps toolchain can help

- Balance risk, controls, and usability
- Identify where building a control is unnecessary, based on acceptable risk
- Document threats and mitigation
- Ensure business goals are protected in the face of malicious actors, accidents, etc.
- Identification of security test cases / security test scenarios to test the security requirements

omnitracs
innovation. driven.

When to use Threat Modeling

The motto: “Threat modeling: the sooner the better, but never too late,”

At the earlier stages of the Software Development Lifecycle/DevOps toolchain, perform threat modeling:

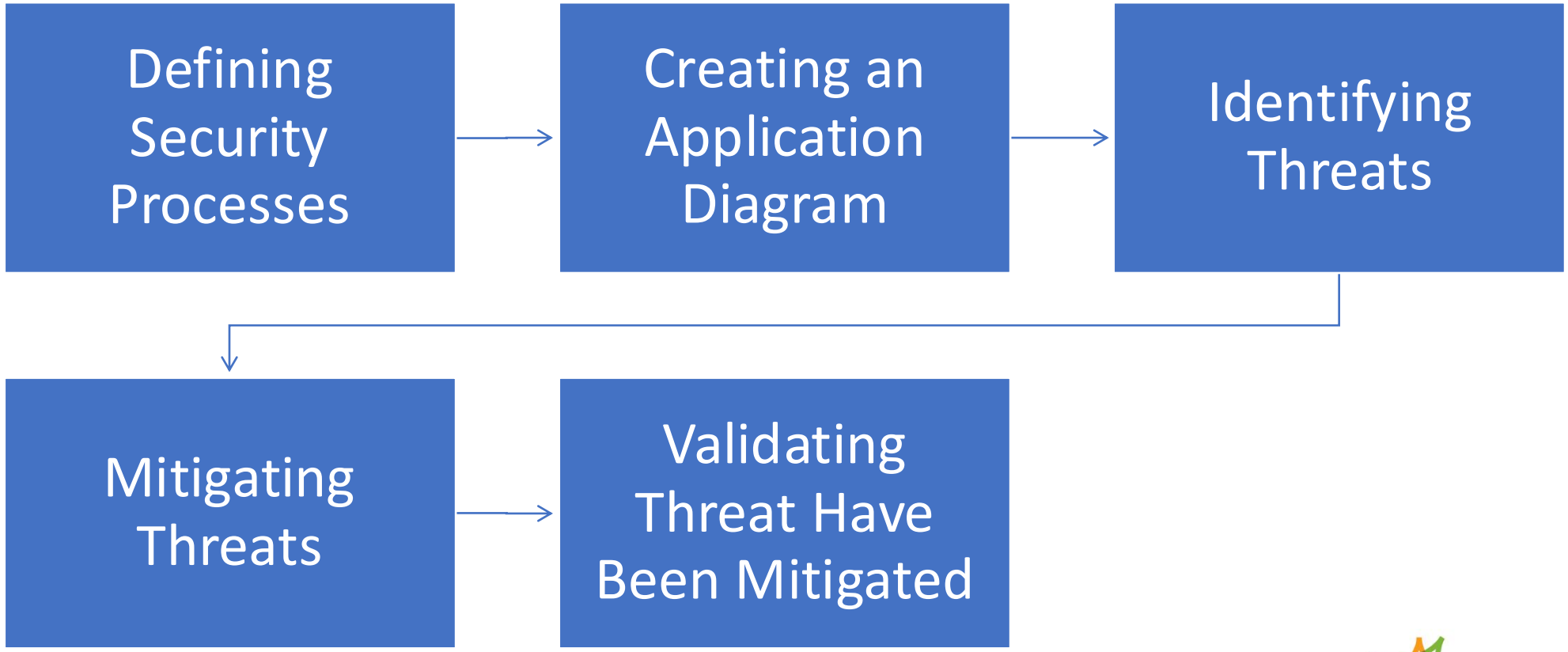
- Every time there is a change in system architecture
- After security incident has occurred or new vulnerabilities are introduced
- As soon as architecture is ready

The more the better!

omnitracs
innovation. driven.

Major steps in threat modeling

Threat modeling should be apart of your routine development lifecycle, enabling you to progressively refine your threat model



omnitracs
innovation. driven.

Attack Personas

- Attack Personas
- Evil User Stories
- Raindance
- Mozilla Rapid Risk Assessment
- OWASP ThreatDragon

omnitracs
innovation. driven.

The Prompt

Threat modeling
Teach us how good threat modeling looks like
Learn about the process, ways, how, and why?
Supposed to help people think like the bad guy