Key Elements in Secure by Design

Todd Carpenter, Chief Engineer, Adventium Labs
Secure by Design Process

(You saw this from Dan a few minutes ago)

This is where we’ll focus our attention
Examples Seen in the Field

“Spaghetti” Architectures

- Untrustworthy subcomponents
  - Software and Firmware
  - Processor microcode
  - Chipsets

- Untrustworthy data input protocols

- Hardcoded passwords

- Plaintext communications

- Weak input validation

- Unnecessary services

In theory, the process should prevent these things
Example Interfaces in the Field

Libraries

EHR

ICE

Marketing often overrides safe and secure decisions
Three Essential Architecture Properties

• Separation
• Determinism
• Non-bypassability

These properties will help you future-proof your designs