HDO Customer Needs

Dan Lyon
Principal Consultant
dlyon@synopsys.com
Current State - Cybersecurity

• 1 M unfilled positions – 2016
  – Dice.com: 32,000

• Average Spend:
  – Healthcare IT 6%
  – Other sectors 12-16%

• Ponemon Medical Device Security Report
  – 40% of orgs take no steps to secure medical devices
Cause of Adverse Event or Harm

Source: Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend
Trends from Medical Device customers

• HDOs increasingly requesting more security information

• Purchasing decisions now including security

• Mayo Clinic
  – Purchasing process requires security information
  – Specific forms, reporting requirements
  – Security Risk profile used as input in procurement
  – Example: Windows XP devices
  – Contract requires support
Customer Needs

• FDA
  – Understand risk profile
  – Evidence of security risk management
  – Equal stakeholder with safety, effectiveness,
• If not met, no approval

• HDOs must **efficiently control** medical device risks

• Starting to Assess
  – Development Process
  – Security Architecture
  – Penetration Testing
  – Long term, rapid patch support
• If not met, no sale
How to Meet Customer Needs

• MDS2 forms
• Secure Development Lifecycle
• Evidence of risk exposure
• Information for Use
  – Responsibility handoff
• Commitment of support for expected lifecycle
  – Monitor and respond to the threat landscape
  – Routine, timely updates for security patches
  – Expected lifecycle

• Requires “Secure by Design”
Secure by Design

• All about risk
• Identify and reduce through risk assessments throughout lifecycle
  – AAMI TIR57, NIST 800-30, CWE/CVSS, OCTAVE Allegro

• Pick a methodology
• Cover the entire lifecycle