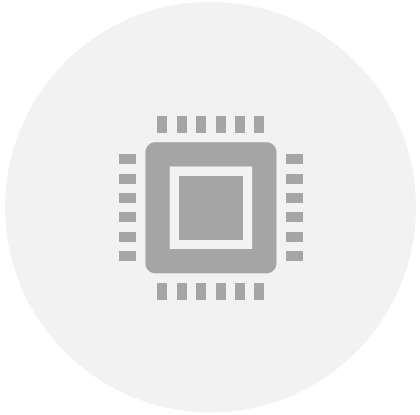
Security Life Cycle Management of Connected Devices

Recent Attacks & Best Practices

Sivani Peesapati

Introduction

Overview of Connected Devices

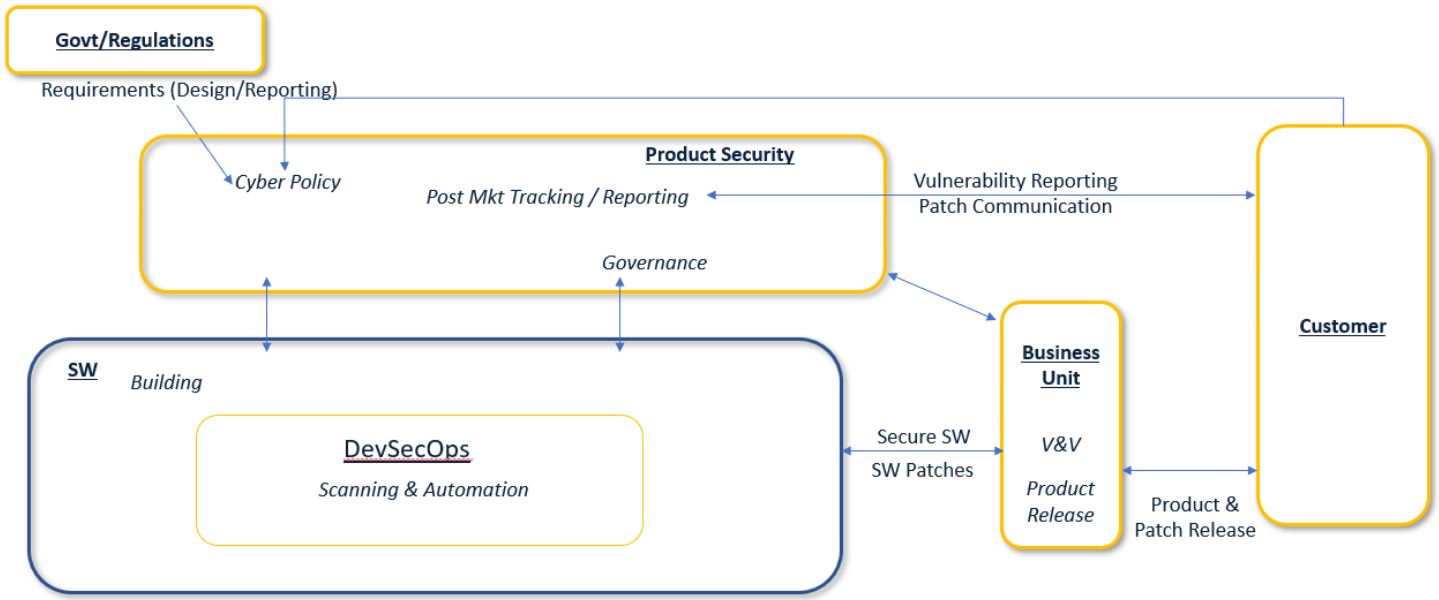


Definition & Examples (IoT Devices, Healthcare Devices, etc.)

Importance of Security in Connected Devices

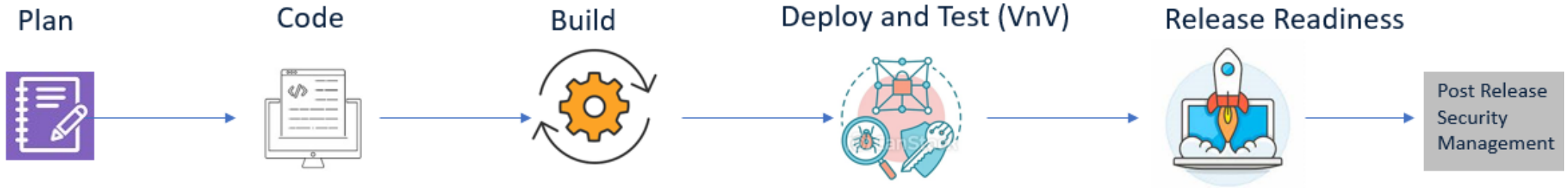
Security Lifecycle Overview

- High-level process of managing security in connected devices.
- Includes phases:
  - Design
  - Implementation
  - Deployment
  - Monitoring
  - Maintenance
  - End-of-life



Pre-Release Stages

- Design and Development
- Security Testing
- Compliance Checks
- User Training



	Process & Governance				
Cyber Activity Performed	Threat Analysis Cyber Security Trainings	SAST (Static application security testing) Code Review Security Logging	SAST (Static application security testing) Secure Pipeline SCA (Software Composition Analysis)	Penetration test Vulnerability scans (Nessus, Twistlock etc.) DAST (Dynamic application security testing)	Code Signing Anti Virus Scan Compliance Checks

Post-Release Stages

- Continuous Monitoring
- Incident Response
- Regular Updates
- End-of-Life Management

	Process & Governance		
Cyber Activity Performed	**AV Scans** **Configuration Checks** **Penetration Test**	**Periodic Vulnerability Scans** **Security Monitoring & Incident Response**	**On demand vulnerability report submission to customers** **Security Patches** **Vulnerability Patch/Fix Communication**

Industry Best Practices

Comprehensive Inventory Management

Regular Updates and Patch Management

Robust Authentication Mechanisms

Network Segmentation

Recent Attack Examples

Change Healthcare Ransomware Attack (2024):	• Disruption in processing claims due to inadequate security management.
2. Ascension Health System Ransomware Attack (2024):	• Forced diversion of emergency care.
3. Aliquippa Water Plant Attack (2023):	• Targeted operational technology systems.

Conclusion

- Summary of Key Points
- Call to action for organizations to adopt best practices.
- Q&A: Open the floor for questions and discussions.