

Final Security Review (FSR)



Traditional Microsoft Software Product Development Lifecycle Tasks and Processes



Why is the FSR important?

- Ensure security is considered in the release process
- Manage remaining security issues at release
- Ensure risks are managed explicitly

Final Security Review (FSR)

- “From a security viewpoint, is this software ready?”
 - Software must be in a stable state with only minimal non-security changes expected prior to release
- If the FSR finds a pattern of remaining vulnerabilities:
 - Fix the vulnerabilities found AND
 - Revisit the earlier phases and address root causes (e.g., improve training, enhance tools)

Final Security Review (FSR)

- What is in the FSR?
 - Interview by a security team member assigned to the FSR
 - Review of bugs that were initially identified as security bugs, but on further analysis were determined not to have impact on security, to ensure that the analysis was done correctly
 - Analysis of any newly reported vulnerabilities affecting similar software to check for resiliency
 - Additional penetration testing, possibly by outside contractors to supplement security team

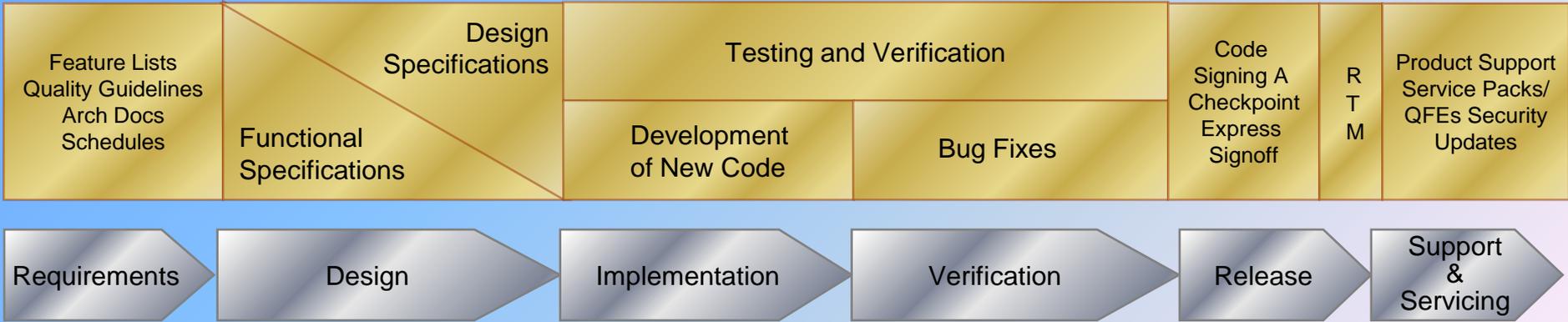
FSR - Calls to Action

- Ensure security is part of release criteria
- What outcomes do we have here?
 - Escalation of issues to management for attention
 - Feedback into development process to address ongoing issues
 - Delay release until issues are resolved

Security Response



Traditional Microsoft Software Product Development Lifecycle Tasks and Processes



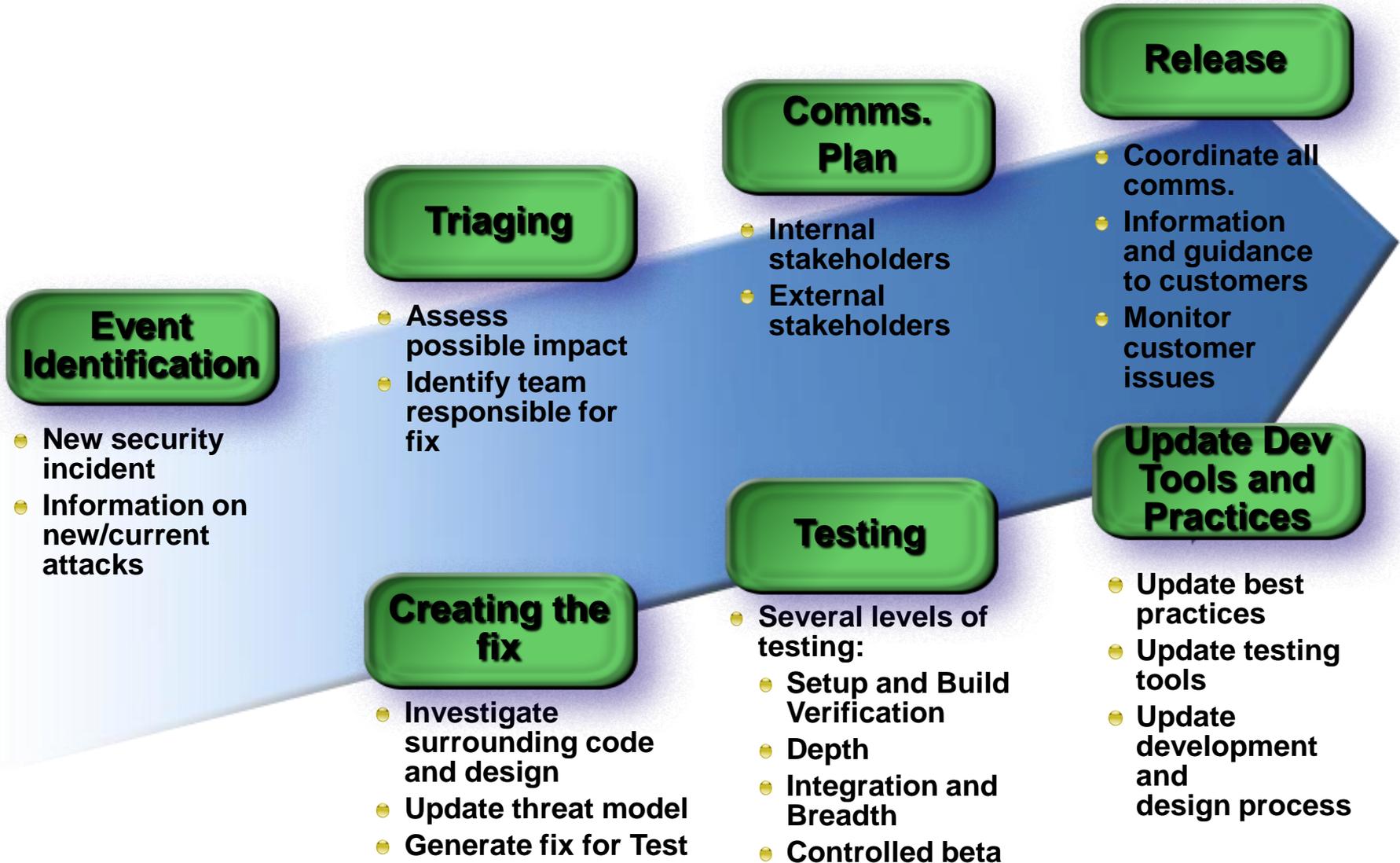
Why plan for security response?

- Testing addresses KNOWN vulnerabilities
- Security incidents are inevitable
- Security response is part of product support
- Identify process and resources proactively

Security Response Plan

- A response plan needs to cover:
 - The team supporting the application
 - Contact points for a security event
 - Application servicing in production
 - Integration with organizational response plan
- Specific to application:
 - Technology in use
 - Risk profile of the application

Responding to an Event (Based on MSRC process)



Response Planning - Calls to Action

- Plan for production security issues before the application is released
- Include the application security response within the overall security response process
- Feed lessons learned back into process

Summary



The Security Development Lifecycle



Traditional Microsoft Software Product Development Lifecycle Tasks and Processes



Goodbye

- That's it ...