AGILE SECURITY
BY EXAMPLE

MATT KONDA
@MKONDA
JEMURAI.COM
SECURE 360 conference

Security For Software Developers
BACKGROUND ON ME

- Developer (~16 years)
- Used Agile a lot (~9 years)
- Appsec focused (~5 years)
- Speaking around dev & sec (~2+ years)

jemurai.com
@mkonnda
DEVELOPER (~16 YEARS)

BACKGROUND ON

ME

JEDI

SAMURAI

Security For Software Developers

Jemurai
BACKGROUND ON YOU

- **Management Role?**
- **Technical Role?**
- **CISSP?**
- **How many people “know” Agile?**
- **Like Agile?**
- **Use Agile?**
Agile Hurts Security
HOW THIS IS GOING TO WORK

- IDENTIFY STAKEHOLDERS
- RUN THE TALK WITH AGILE
- DO 5 MINUTE SPRINTS
- START WITH 4 EPICS
INITIAL EPICS

• EXPLAIN AGILE
• A FICTIONAL CASE STUDY
• AGILE SECURITY METRICS
• AGILE ANTI-PATTERNS
AGILE VALUES

INDIVIDUALS AND INTERACTIONS OVER PROCESSES AND TOOLS
AGILE VALUES

WORKING SOFTWARE OVER COMPREHENSIVE DOCUMENTATION
AGILE VALUES

CUSTOMER COLLABORATION OVER CONTRACT NEGOTIATION
AGILE VALUES

RESPONDING TO CHANGE
OVER
FOLLOWING A PLAN
Traditional Plan
AGILE CONCEPTS

STORY

A NARRATIVE DESCRIPTION OF A FEATURE OR TASK.

OFTEN IN THE FORM OF: AS A <STAKEHOLDER> I NEED TO <ACTION> IN ORDER TO <ACTUAL BUSINESS OBJECTIVE>. 
AGILE CONCEPTS

STAKEHOLDER

THE PEOPLE WHO WILL BE IMPACTED BY A STORY.

OFTEN PRODUCT MANAGERS AND CUSTOMERS IN ADDITION TO DEVELOPMENT, QUALITY ASSURANCE, OPERATIONS, SECURITY AND IT.
AGILE CONCEPTS

SPRINT

AN ARBITRARY UNIT OF TIME IN WHICH WORK WILL BE MEASURED.

OFTEN ONE OR TWO WEEKS.
ALSO AN “ITERATION”.

AGILE CONCEPTS

BACKLOG

THE QUEUE OF WORK TO BE DONE.

SOMETIMES DIFFERENT BACKLOGS FOR DIFFERENT TYPES OF THINGS — SAY FEATURES, ISSUES, DOCUMENTATION, TECHNICAL CONTROLS.
AGILE CONCEPTS

RELEASE

The point where work is made available to a broader audience.

Often after several sprints. M stories per sprint, N sprints per release.
AGILE CONCEPTS

STORY BOARD

The place where work for the current sprint is easy to see and track.

Could be on the wall like we are doing, or in a tool like Trello, AgileZen, JIRA/GreenHopper, etc.
Trello Example

**To Do**
- Build backlog
- Build a security team.
- Bring Manufacturing into discussion.
- Bring Software Engineering into discussion.
- Bring R+D into discussion.
- Get HR involved with policies.
- Update IT / Password policies.
- Add security to employee training.
- Add a card...

**Doing**
- Immediately hire a small ops team to start with hands on security measures.
- Define milestones
- Add a card...

**Done**
- Run DLP on File Servers
- Run Vulnerability Scan on External Net
- Add a card...

Security For Software Developers
Agilezen Example
AGILE CONCEPTS

STANDUP

A PERIODIC CHECKPOINT MEETING ATTENDED BY STAKEHOLDERS DURING WHICH ISSUES AND PROGRESS ARE REVIEWED.

BEST IF DAILY, VERY SHORT, REVIEW ANY ISSUES.
AGILE CONCEPTS

VISIBILITY

STAKEHOLDERS CAN SEE STATUS ON STORY BOARD.

BUILT IN AT A FINE GRAINED LEVEL OF DETAIL.
AGILE CONCEPTS

PARKING LOT

A process for managing issues as they arise.

Usually says that new issues will be added to a list of items to be discussed and triaged by the team (including business stakeholders) at the next standup.
AGILE CONCEPTS

SPRINT PLANNING

The process by which a team chooses and estimates what work to do in a given Sprint.

Stakeholders must prioritize and know what is in the Sprint. Team discusses & estimates tasks assigned.
AGILE CONCEPTS

VELOCITY

HOW MANY TASKS GET DONE PER SPRINT.

MEASURED IN STORIES, STORY POINTS OR ESTIMATED STORY HOURS PER SPRINT.
AGILE CONCEPTS

RETROSPECTIVE

BUILT IN MECHANISM FOR CONTINUOUS IMPROVEMENT.

AT THE END OF EVERY SPRINT, THE TEAM TALKS ABOUT WAYS THE PROCESSES/PROJECT CAN BE IMPROVED.
AGILE CONCEPTS

TECHNICAL DEBT

A MEASURE OF WORK THAT SHOULD BE DONE BECAUSE CORNERS HAVE BEEN CUT IN ONE WAY OR ANOTHER.

OFTEN MANIFESTED AS LACK OF DOCUMENTATION, LACK OF TESTING, LACK OF OPERATIONAL PROCESS.
AGILE CONCEPTS

GROOMING

THE PROCESS OF MANAGING THE BACKLOG.

LET LONGER TERM GOALS STAY BIG AND BROADLY ESTIMATED, LET SHORTER TERM UPCOMING WORK BE ESTIMATED AT A FINER LEVEL OF DETAIL.
Break down stories as they move up the backlog

- Ready for iteration planning
- Mid-range (4-10 iterations out)
- Long-term (10+ iterations out)

Increasing detail
Increasing priority

Credit: RallyDev.com
Notice that traditional presentations are not especially conducive to Agile collaboration.
Traditional Plan

Original goal
CASE STUDY

The following slides illustrate how Agile could be applied to different types of security projects.
CASE STUDY: POLICY FRAMEWORK

- A MASTER POLICY COULD BE A STORY.
- EACH POLICY COULD BE A STORY.
- STAKEHOLDERS ARE POLICY APPROVERS AND IMPLEMENTERS.
- ADDITIONAL STORIES FOR MAPPING POLICY TO COMPLIANCE/STANDARD.
CASE STUDY: PEN TEST

• EACH PART OF A PENETRATION TEST COULD BE A STORY
• SCOPE & APPROVAL
• RECON
• EXPLOITATION
• PIVOT & EXPLOIT
• REPORT
CASE STUDY: DLP IMPLEMENTATION

• REQUIREMENTS (EMAIL, FILE, DB, NETWORK)
• TOOL/PARTNER SELECTION
• IMPLEMENTATION PHASES
  RULE TUNING
  SERVER PREP
• TESTING
Case Study: Remediation

- Issue remediation demands tracking and visibility
- Consolidate issues
- Each sprint assign and track issues
- Maintain backlog of issues that haven’t been addressed.
CASE STUDY: ALL TOGETHER NOW

- A combined story board will show issues across the previous four areas.
- By managing at the detailed level, you can choose what tasks are next and easily communicate to management what is and what is not being done.
Agile Security Metrics

The following slides illustrate how Agile security metrics can work.
WHAT IS HARD ABOUT METRICS?

MEASURES.

TIME.
Agile security metrics

• Agile is great for metrics.

• Check the case study.

• Check out progress so far in the talk.
AGILE SECURITY METRICS

• **USING STANDARD AGILE METRICS, YOU CAN TRACK PROGRESS TOWARD ANY LONG TERM PROJECT GOAL, INCLUDING:**
  
  - Policy Development
  - Pen Test
  - Product Implementation
  - Issue Remediation
AGILE METRICS

CREDIT: RALLYDEV.COM
AGILE SECURITY METRICS

- BURNDOWN
- VELOCITY
- EASY TO FILTER
Use metrics to show your organization what you are doing and the impact of their prioritization.
AGILE ANTI-PATTERNS

HOW DO YOU KNOW YOU ARE DOING IT WRONG?
AGILE SECURITY ANTI-PATTERNS

• STAKEHOLDERS ARE NOT INCLUDED

• STAKEHOLDERS OR TEAM DO NOT PARTICIPATE IN PROCESS

• AFTER A SPRINT, SUBSTANTIAL WORK DONE DURING THE SPRINT IS NOT WHAT WAS PLANNED
AGILE SECURITY ANTI-PATTERNS

• Stories are estimated at bigger than a sprint

• Stories get stuck as work in progress and never move without raising a red flag

• Backlog is disorganized
AGILE SECURITY ANTI-PATTERNS

• TEAM NOT INVOLVED IN ESTIMATION
• STANDUP TAKES AN HOUR