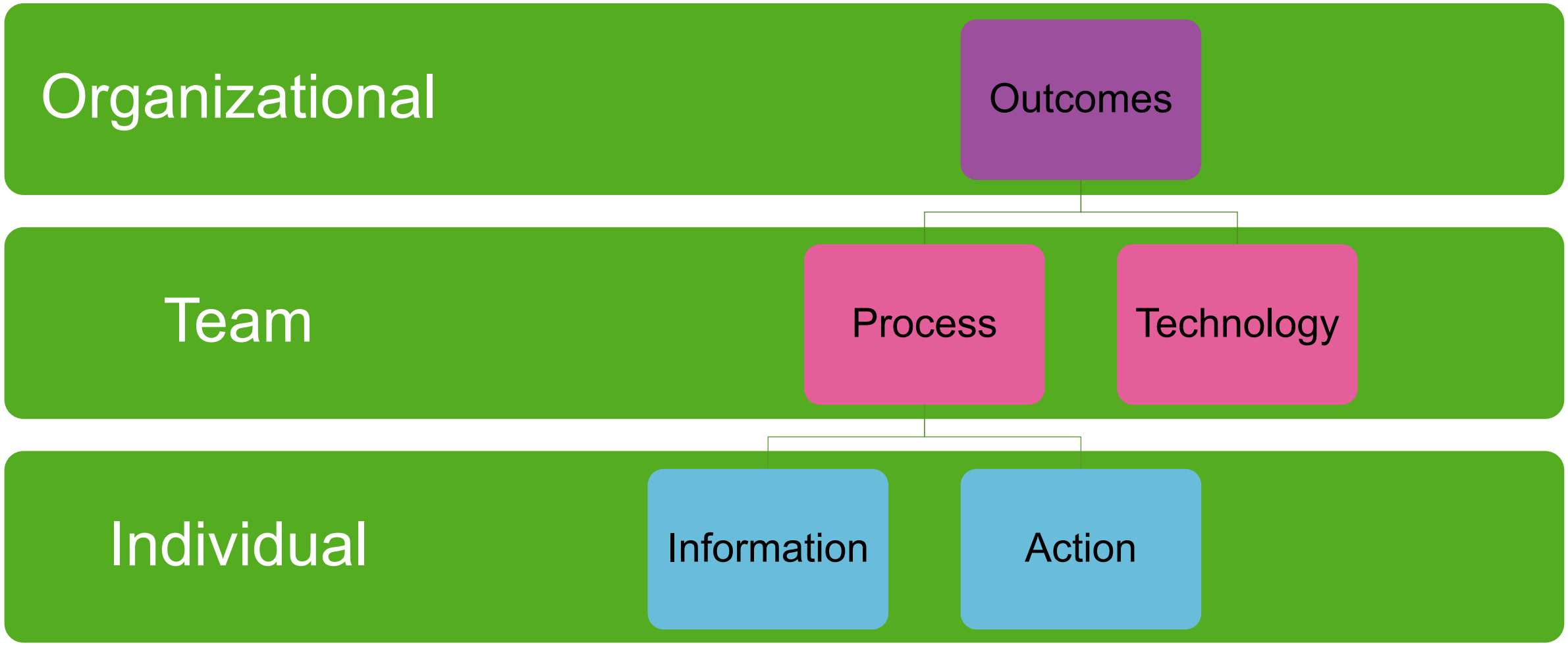
The Agile Security Program

Maximizing efficacy in a world of fast-changing threats

Craig Vincent | Regional Security SME, Higher Education

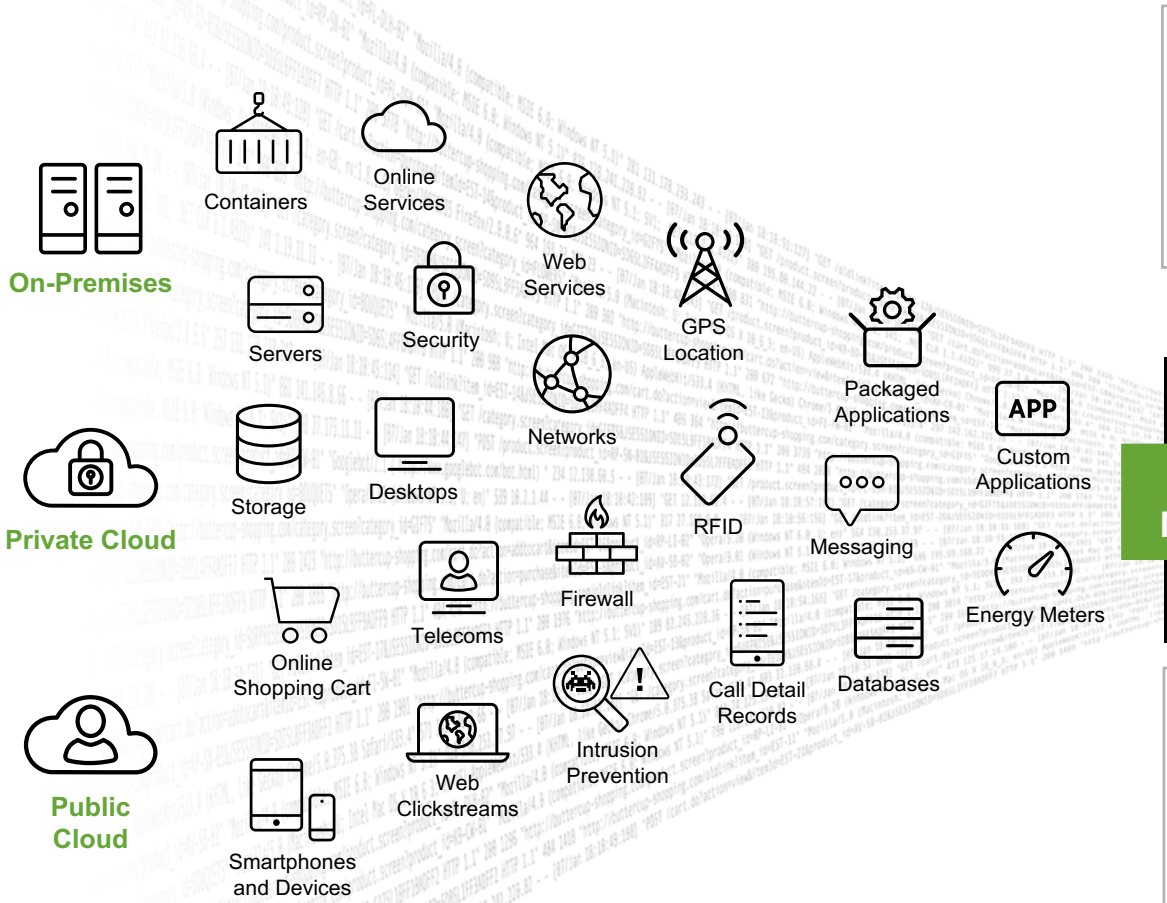
August 2017

Outcomes Breakdown



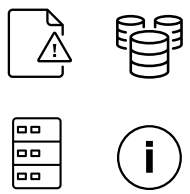
The Checkbox.

The Living, Breathing Security Program



Real-Time Machine Data

SIEM



- **References** – Coded fields, mappings, aliases
- **Dynamic information** – Stored in non-traditional formats
- **Environmental context** – Human maintained files, documents
- **System/application** – Available only using application request
- **Intelligence/analytics** – Indicators, anomaly, research, white/blacklist

splunk> listen to your data®

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> listen to your data®

Objectives

Origins of Checkbox Culture

Principles of Agile and Lean Philosophies

Common Challenges

Framework

About Me

Craig Vincent

- Solution Engineer & Regional Security Subject Matter Expert

splunk> MANDIANT ncta
THE INTERNET & TELEVISION ASSOCIATION

Universities & Colleges

State & Local Governments

Medical Centers

History

Where did this culture come from?

splunk> listen to your data®

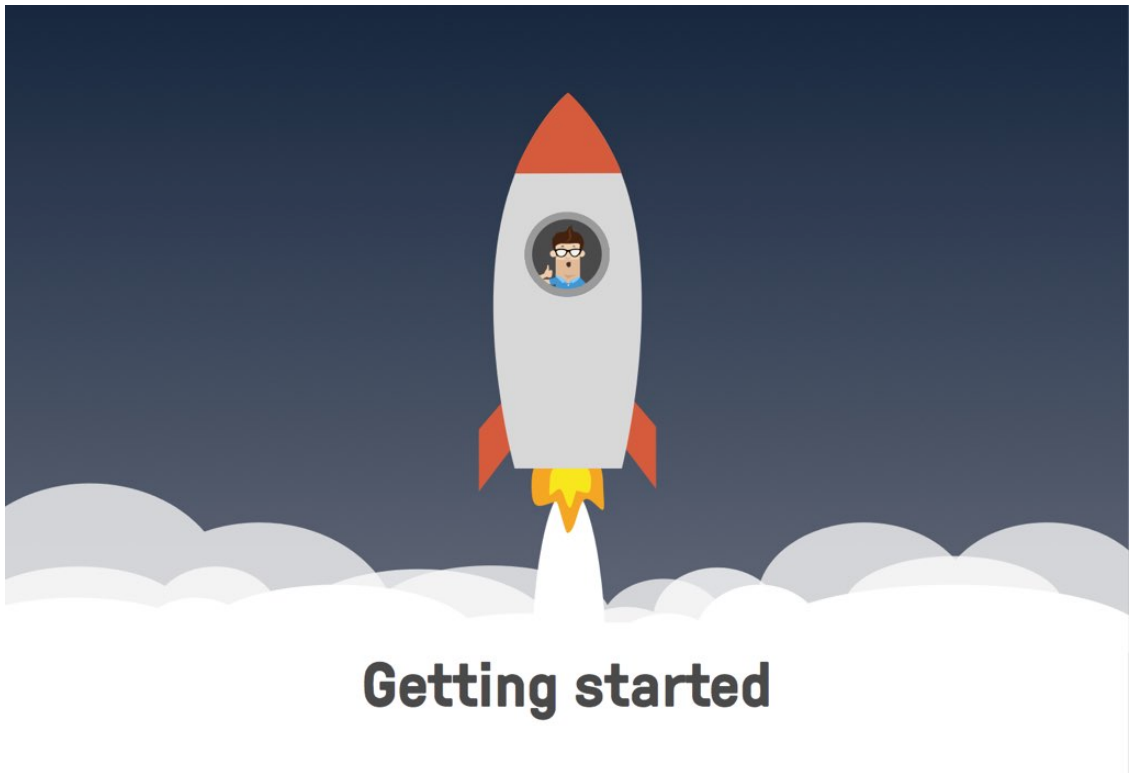

© 2017 SPLUNK INC.
splunk> listen to your data

splunk> listen to your data

Challenges

Getting Started

- Invest once mentality
- Projects seem difficult to completely define
- Hard to manage operational risks



Challenges

Keeping up with the security landscape

Cyber Criminals

Malicious Insiders

Nation States

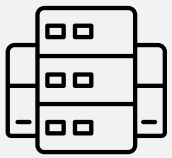
Advanced Threats are Hard to Find

Cyber Criminals

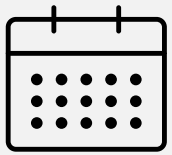
Nation States

Insider Threats

100%
Valid credentials were used



40
Average # of systems accessed



143
Median # of days before detection

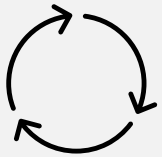
67%
Of victims were notified by external entity

Source: Mandiant M-Trends Report 2012/2013/2014/2015/2016

Advanced Threats are Hard to Find

Threat

People



Process

Technology

Attack Approach

- Human directed
- Goal-oriented
- Dynamic (adjust to changes)
- Coordinated
- Multiple tools & activities
- New evasion techniques

Security Approach

- Fusion of people, process, & technology
- Contextual and behavioral
- Rapid learning and response
- Share info & collaborate
- Analyze all data for relevance
- Leverage IOC & Threat Intel

splunk> listen to your data

NIST Special Publication 800-137

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

National Institute of Standards and Technology

U.S. Department of Commerce

Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

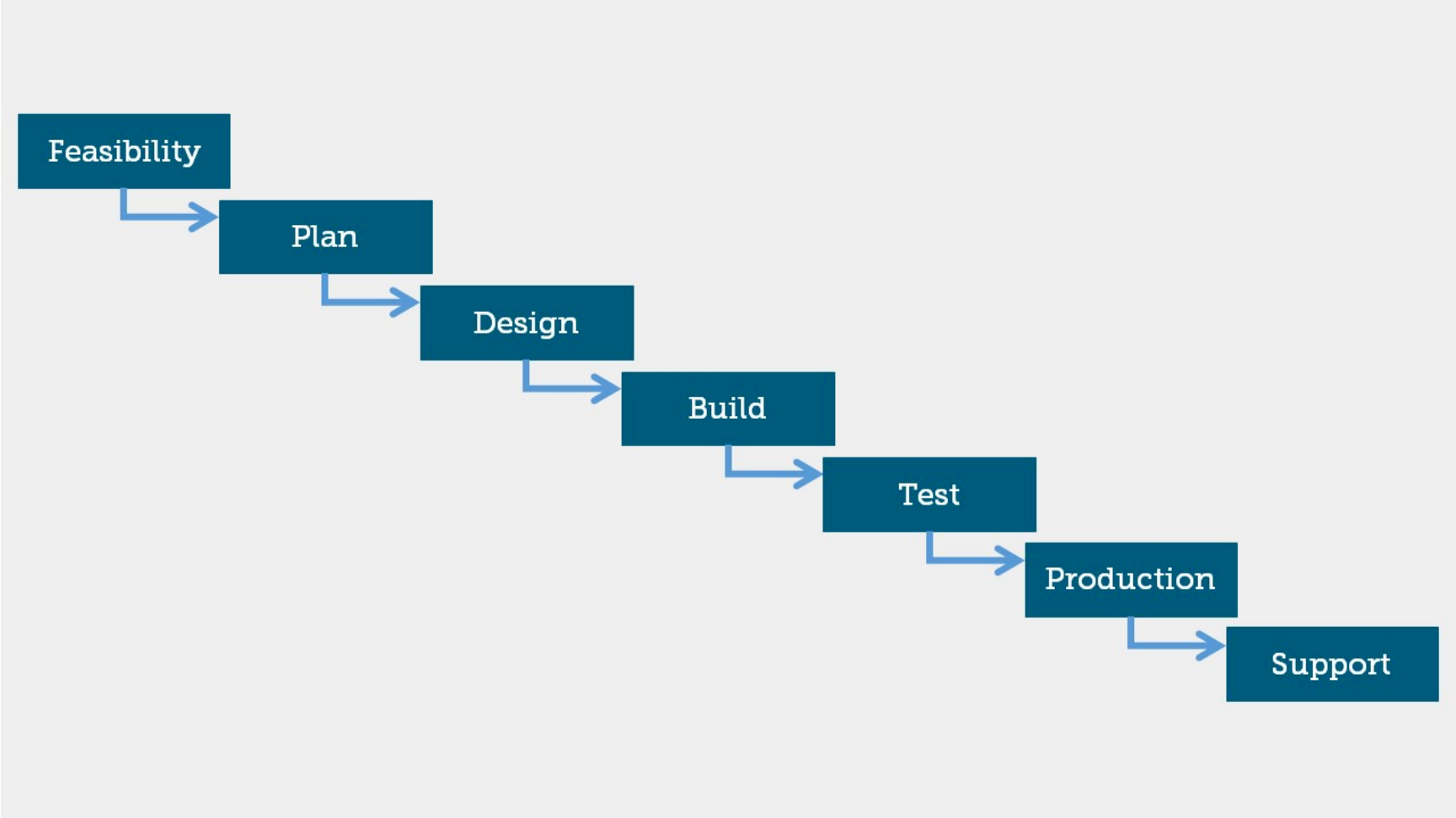
Federal Government is changing

INFORMATION SECURITY

Introduction to Agile & Lean

Project Management

Project Management

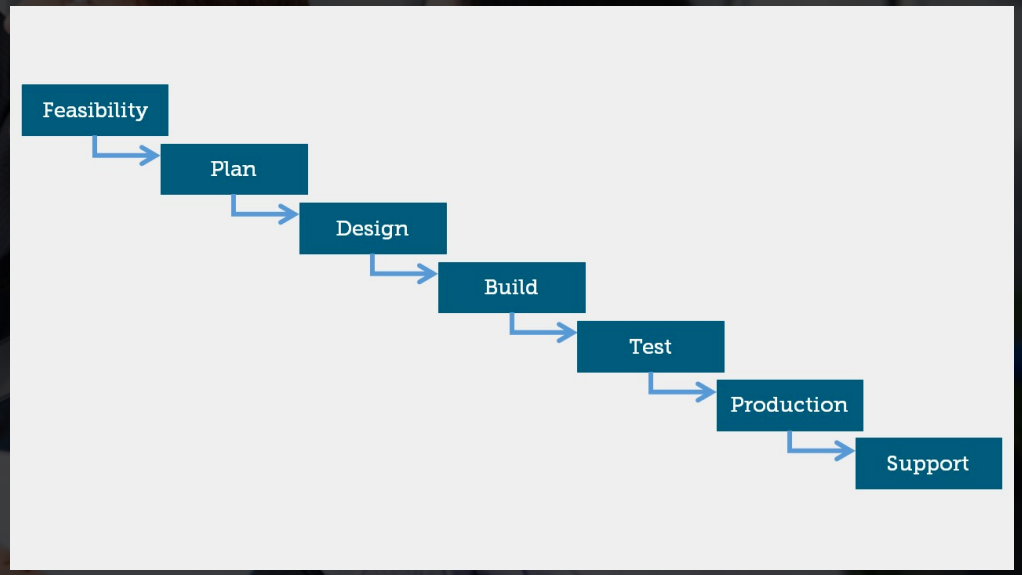


Traditional Project Management Challenges

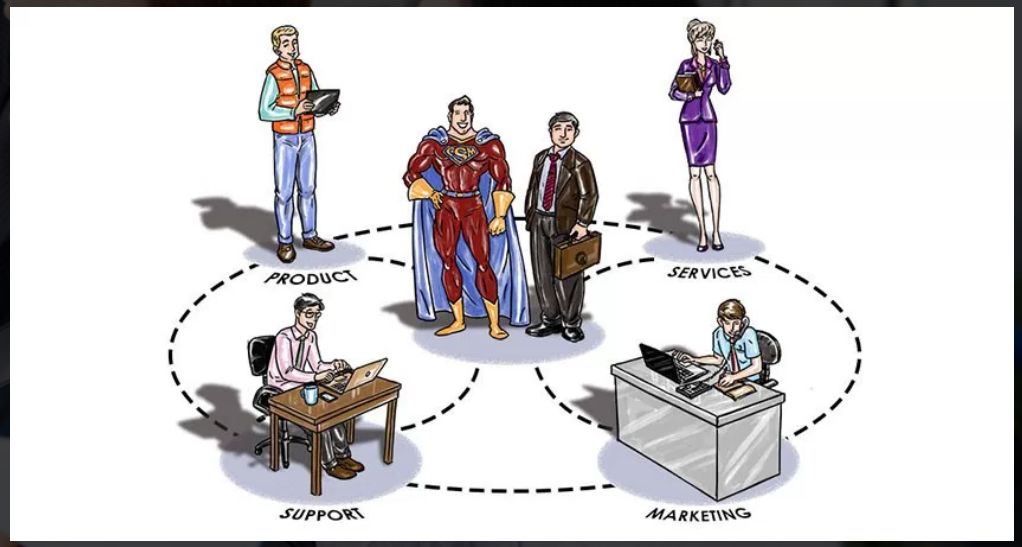
- Doesn't handle in-flight change
- Extended time to value/ revenue
- Little communication across groups
- Limited focus on customer needs

In-flight Change

Time to Value/ Revenue

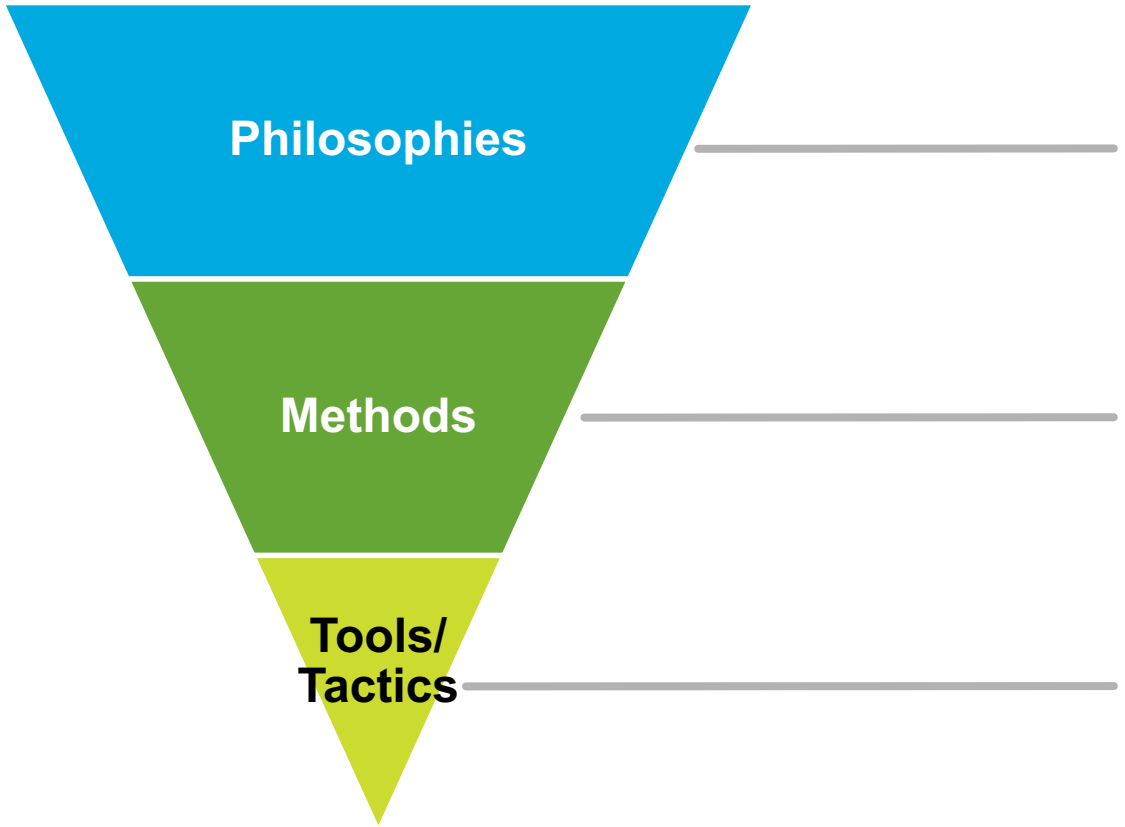


Cross-functional Communication



Customer Needs

Understanding the Terminology



		Examples
Philosophies	Ideas & Beliefs	• Traditional • Agile • Lean
Methods	Decisions	• Waterfall • Scrum • Kaizen • Kanban
Tools/ Tactics	Details	• [redacted] • [redacted] • Stand-ups • Technology Integration

5 Principles of Lean

1. Specify value from the standpoint of the end customer by product family.
2. Identify all the steps in the value stream for each product family, eliminating whenever possible those steps that do not create value.
3. Make the value-creating steps occur in tight sequence so the product will flow smoothly toward the customer.
4. As flow is introduced, let customers pull value from the next upstream activity.
5. As value is specified, value streams are identified, wasted steps are removed, and flow and pull are introduced, begin the process again and continue it until a state of perfection is reached in which perfect value is created with no waste.

12 Principles of Agile

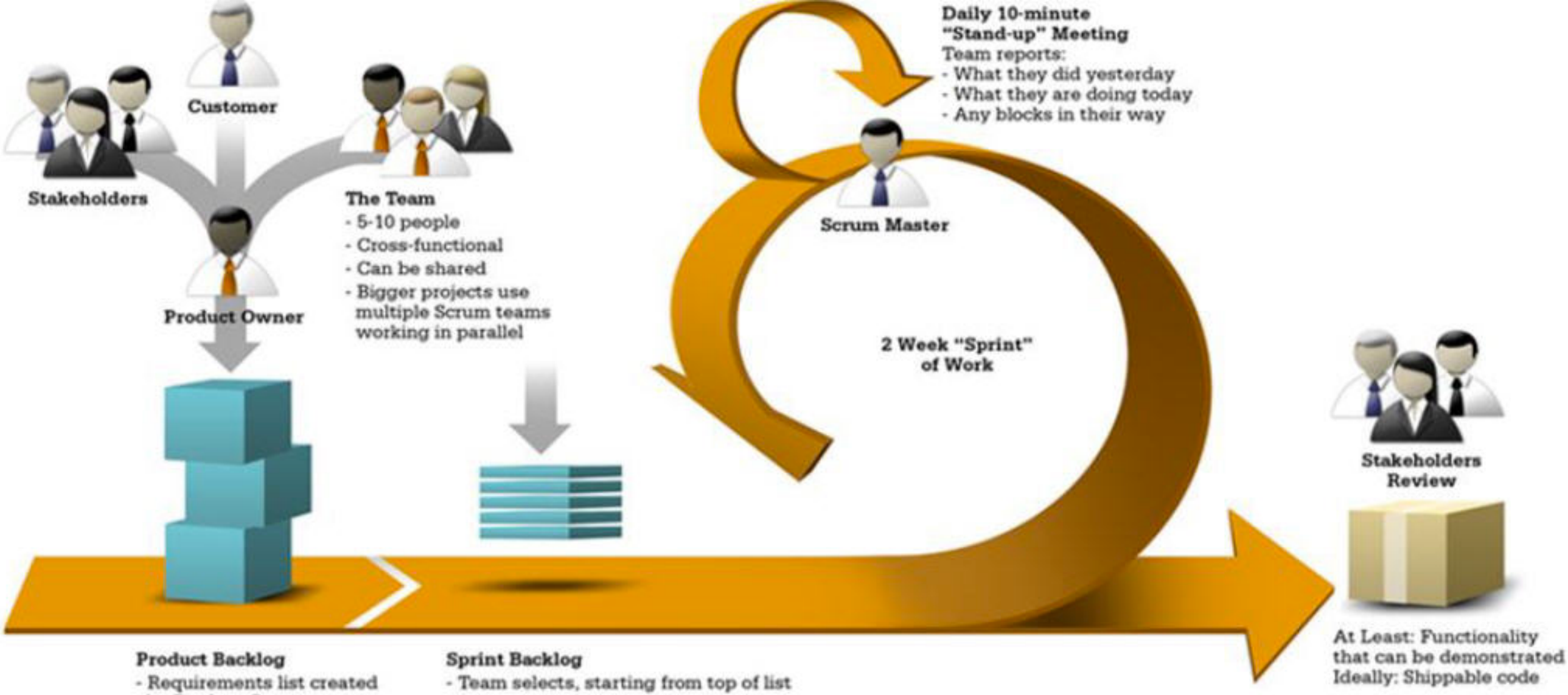
1. Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
2. Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
3. Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
4. Business people and developers must work together daily throughout the project.
5. Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
6. The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
7. Working software is the primary measure of progress.
8. Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
9. Continuous attention to technical excellence and good design enhances agility.
10. Simplicity--the art of maximizing the amount of work not done--is essential.
11. The best architectures, requirements, and designs emerge from self-organizing teams.
12. At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

www.agile.org

splunk> listen to your data

Relevant Principles

1. Continuous Delivery
2. Change-agility
3. Short Dev Cycle/ Minimum Viable Product
4. Cross-Functional Communication
5. Self-Improvement



Poll

splunk.com/poll

How many of you have a SIEM?

Answer at splunk.com/poll

How many of you have a SIEM that you use?

Answer at splunk.com/poll

Are your security technologies static?

Answer at splunk.com/poll

Did it take a long time for you to start using your security technology?

Answer at splunk.com/poll

Think of the last major security threat, did you adapt your security technologies to address that threat?

Answer at splunk.com/poll

Do all your security teams communicate regularly?

Answer at splunk.com/poll

Do you regularly review your security processes to identify areas of improvement?

Answer at splunk.com/poll

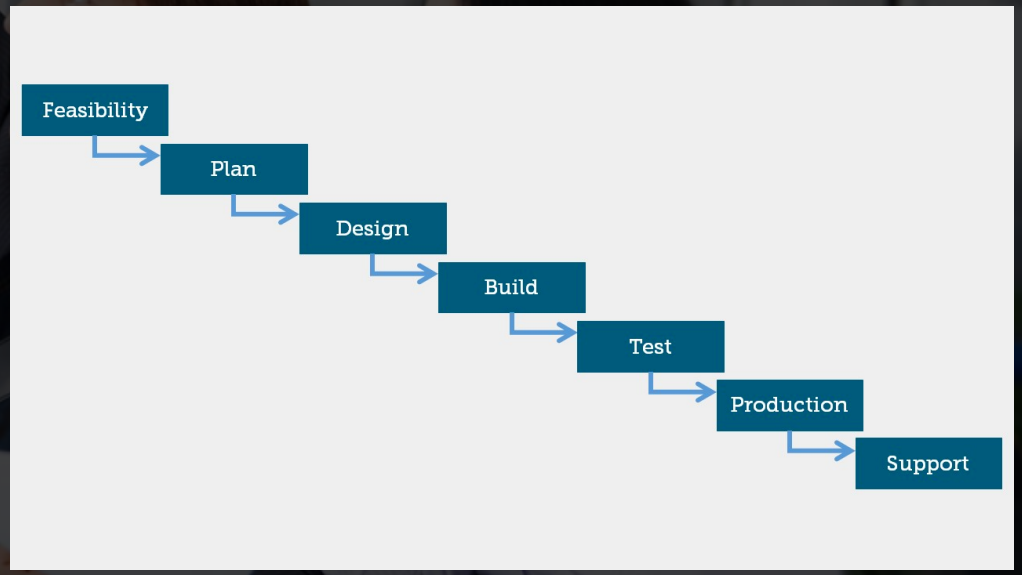
Security Takeaways

Security Project Management Challenges

- Doesn’t handle in-flight change
- Extended time to value/ revenue
- Little communication across groups
- Limited focus on customer needs

In-flight Change

Time to Value/ Use



Cross-functional Communication

Operational Risks

Agile Security Operations Framework

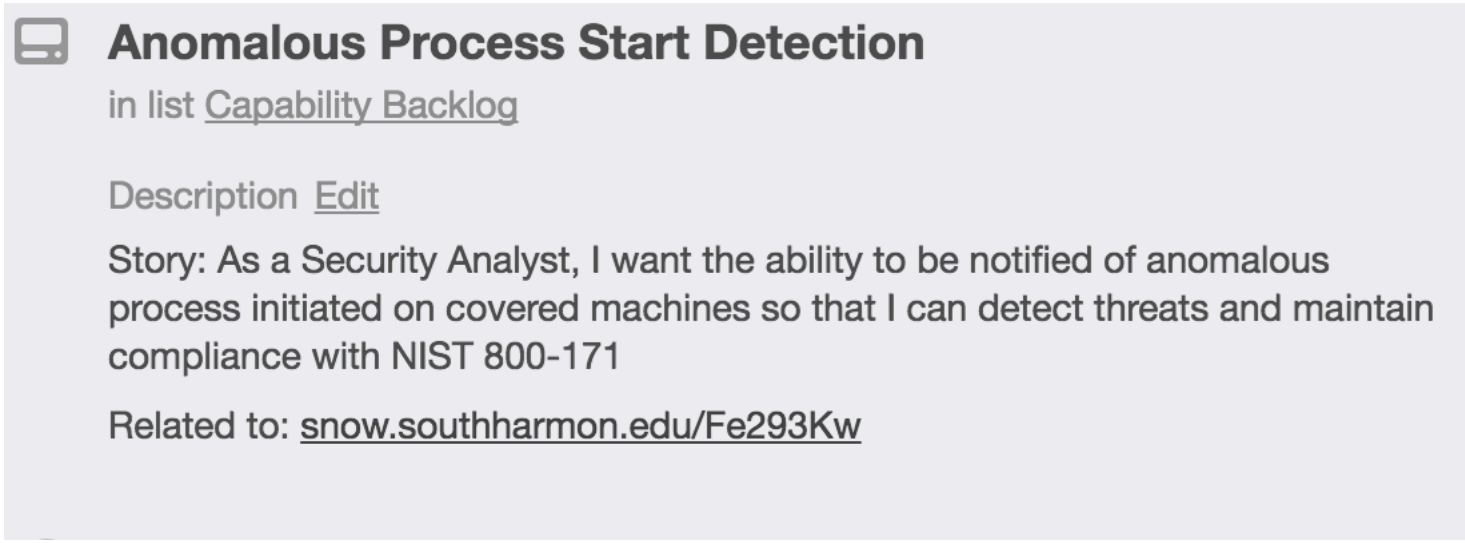
Incident
Response

Incident Response

Capability Backlog

Incident responders/manager write ’User Stories’ or short blurbs specifying a capability that they lack

Example User Story



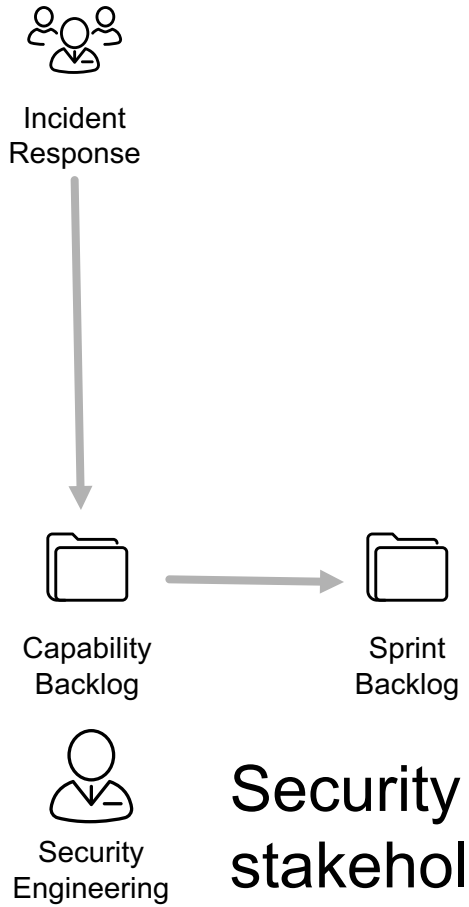
Anomalous Process Start Detection

in list Capability Backlog

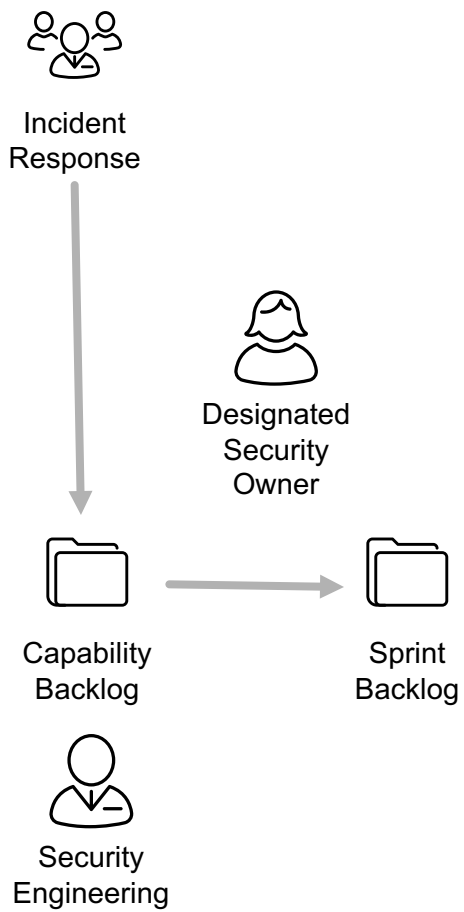
Description Edit

Story: As a Security Analyst, I want the ability to be notified of anomalous process initiated on covered machines so that I can detect threats and maintain compliance with NIST 800-171

Related to: snow.southharmon.edu/Fe293Kw



Security Engineering and other appropriate stakeholders annotate the ’user story’ with the technical requirements and dependencies. If a task is too broad, it can be divided into smaller stories.



Designated Security Owner prioritizes a set number of capabilities to be developed in the next sprint by considering threat landscape and organizational priorities and initiatives

Annotation by Security Engineering

Determining the ‘how’

Anomalous Process Start Detection

in list Capability Backlog

Due Date

Dec 31 at 12:00 PM

Description Edit

Story: As a Security Analyst, I want the ability to be notified of anomalous process initiated on covered machines so that I can detect threats and maintain compliance with NIST 800-171

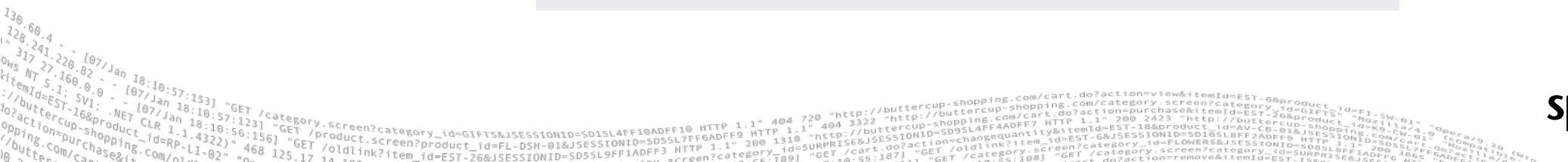
Related to: snow.southharmon.edu/Fe293Kw

Dependencies Delete…

0%

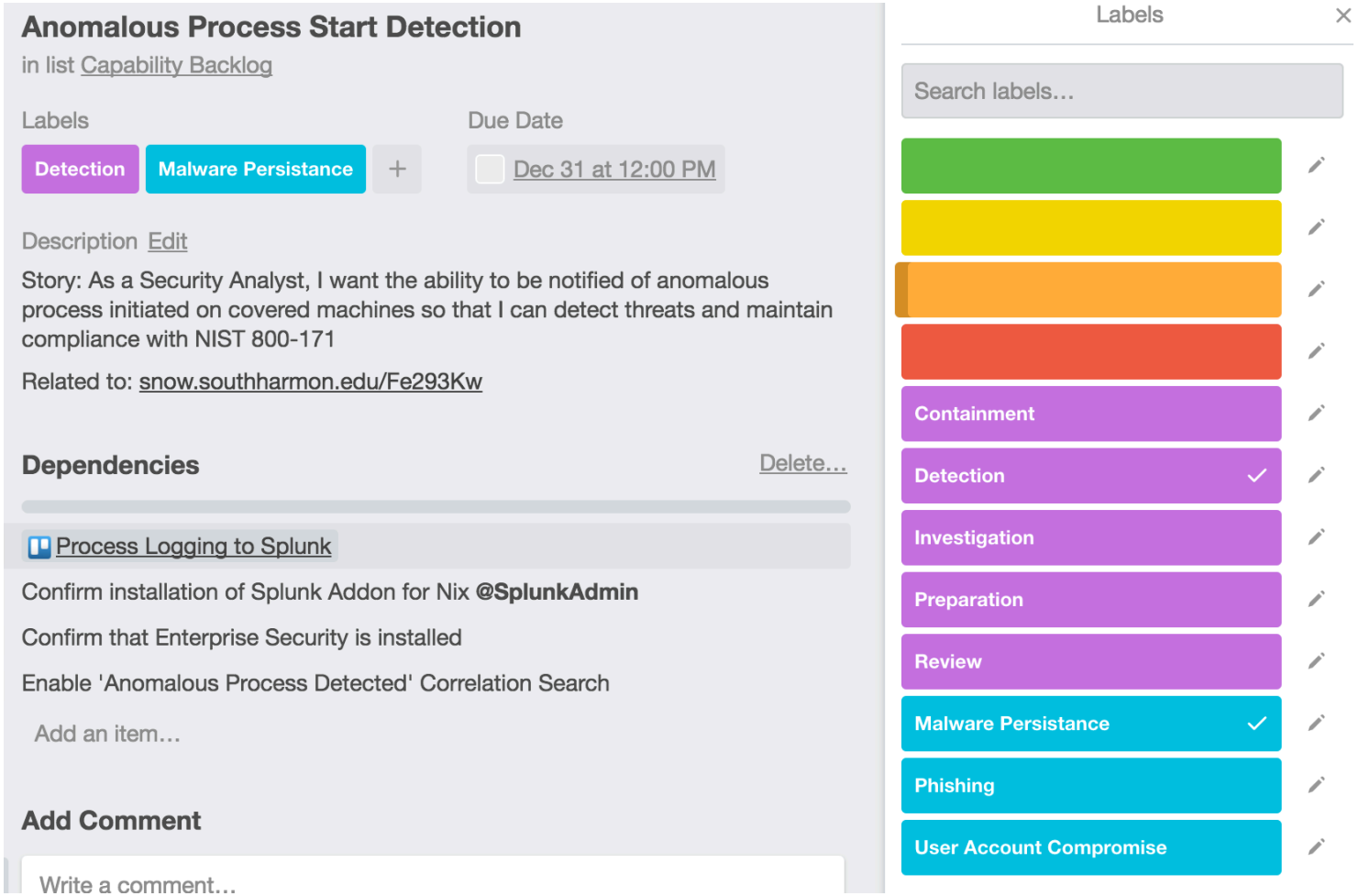
- [ ] Process Logging to Splunk
- [ ] Confirm installation of Splunk Addon for Nix **@SplunkAdmin**
- [ ] Confirm that Enterprise Security is installed
- [ ] Enable 'Anomalous Process Detected' Correlation Search

Add an item…



Annotation by Security Engineering

Classify



Building a Sprint

Identify threat priorities and place story on incident response lifecycle

	Preparation	Detection	Investigation	Containment	Recovery	Review
Phishing						
User Account Compromise						
Persistent Malware		X				

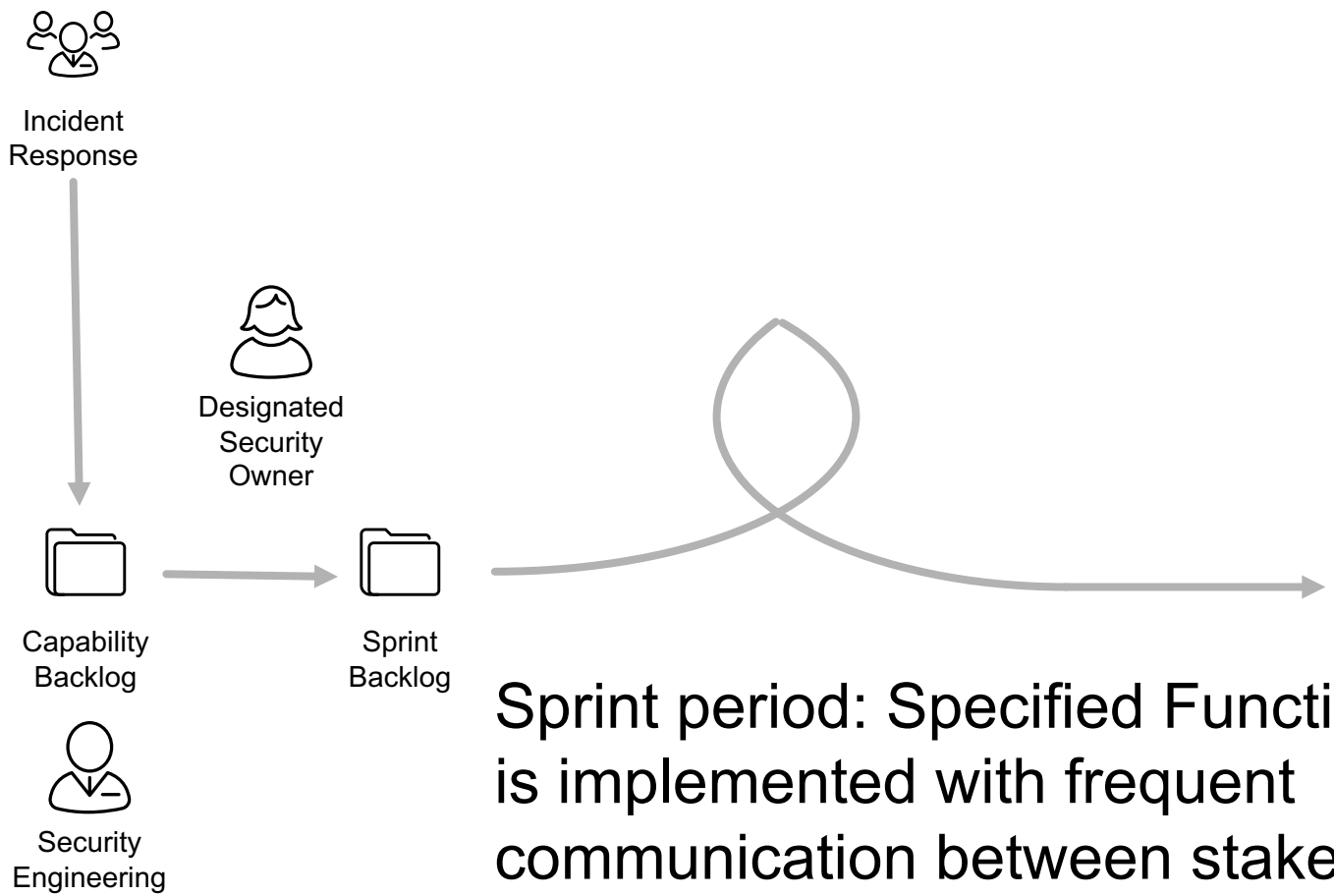
Anomalous Process Start Detection

in list Capability Backlog

Description Edit

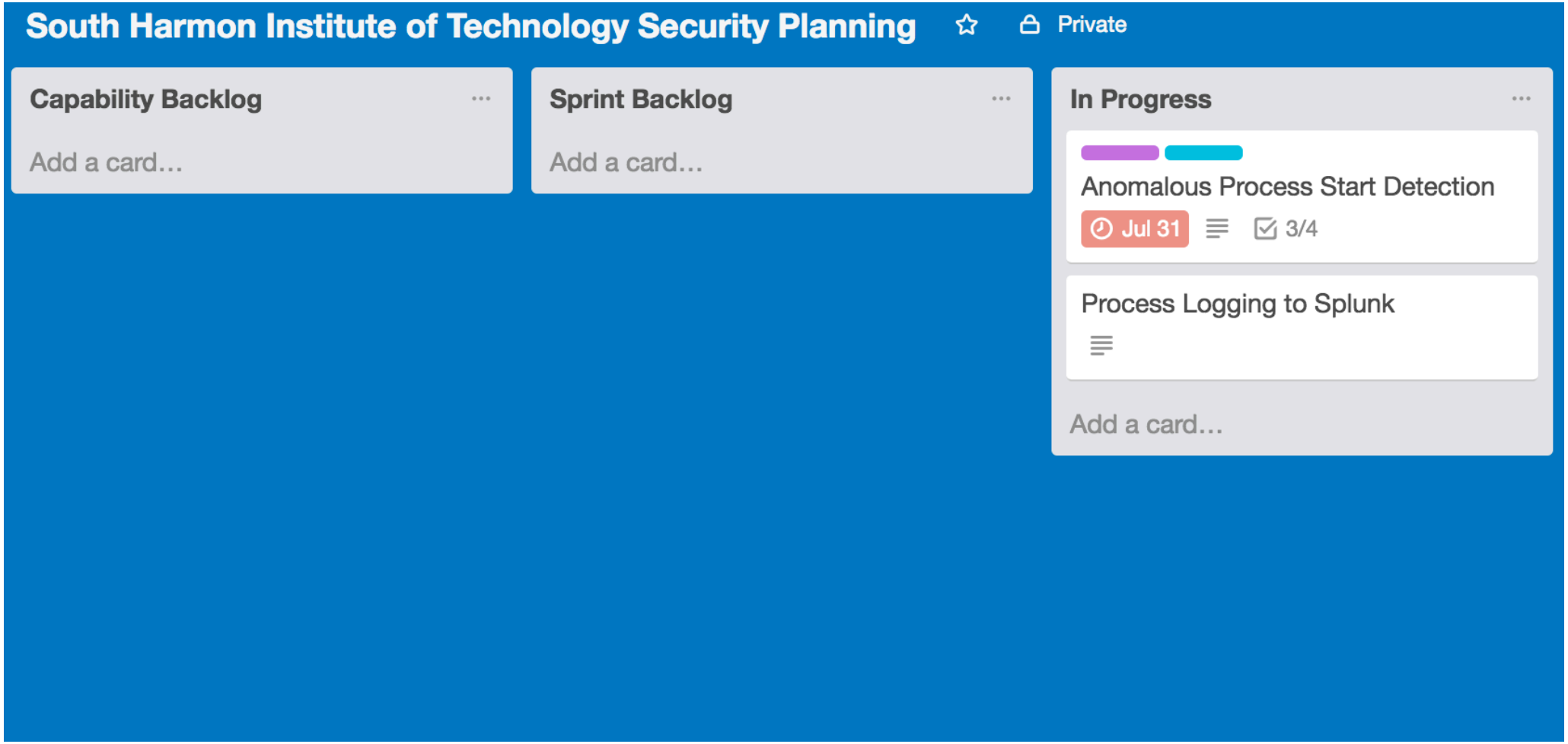
Story: As a Security Analyst, I want the ability to be notified of anomalous process initiated on covered machines so that I can detect threats and maintain compliance with NIST 800-171

Related to: snow.southharmon.edu/Fe293Kw

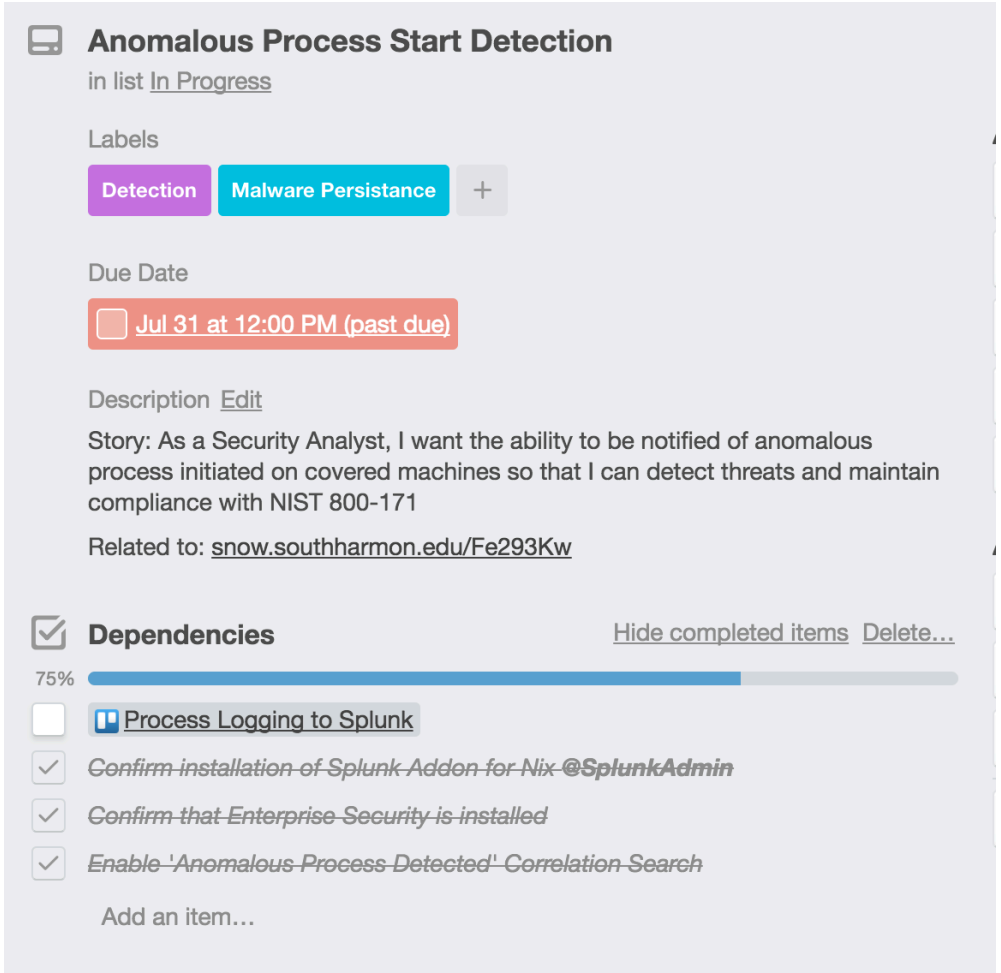


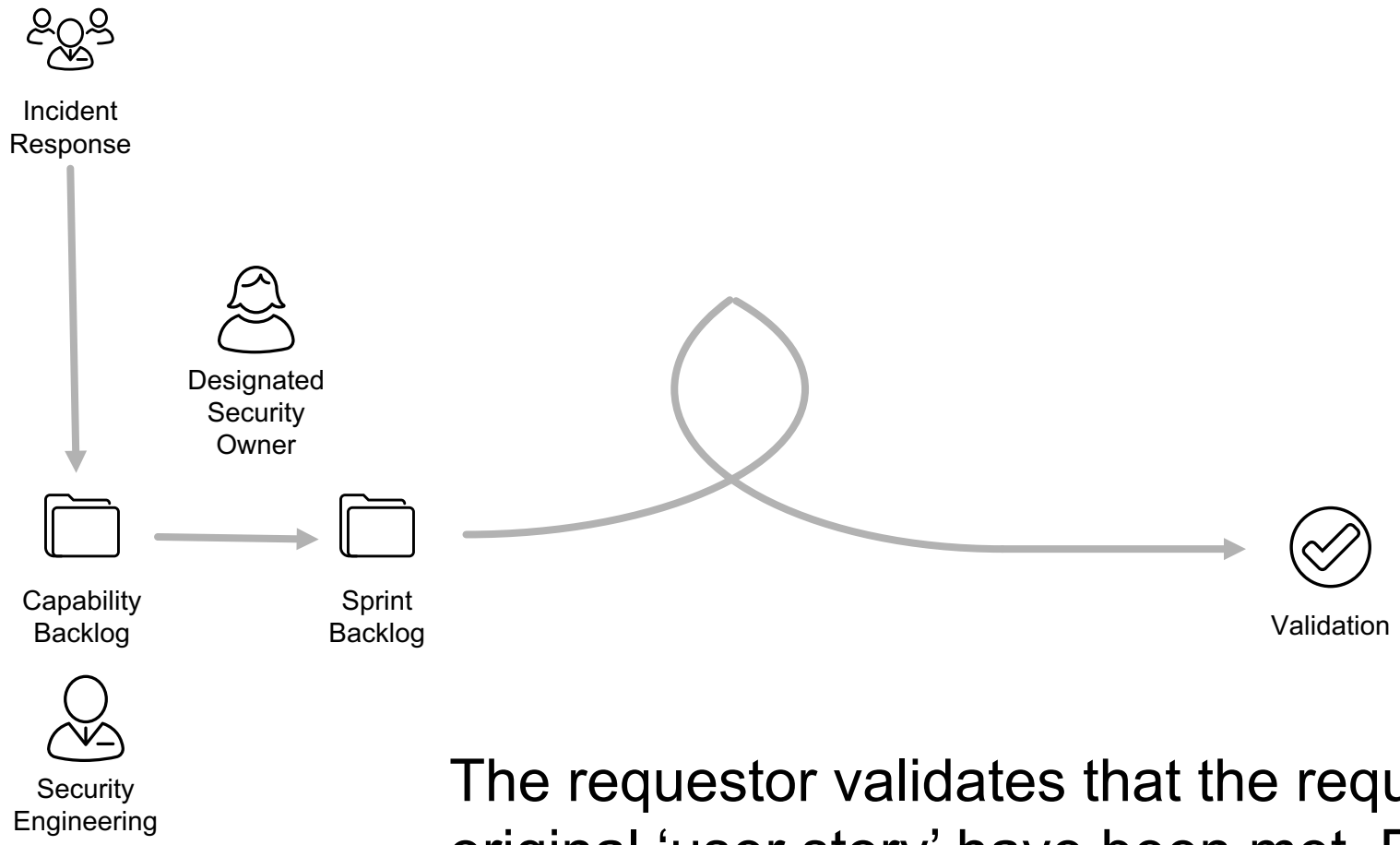
Sprint period: Specified Functionality is implemented with frequent communication between stakeholders and with the incident responders

In Progress



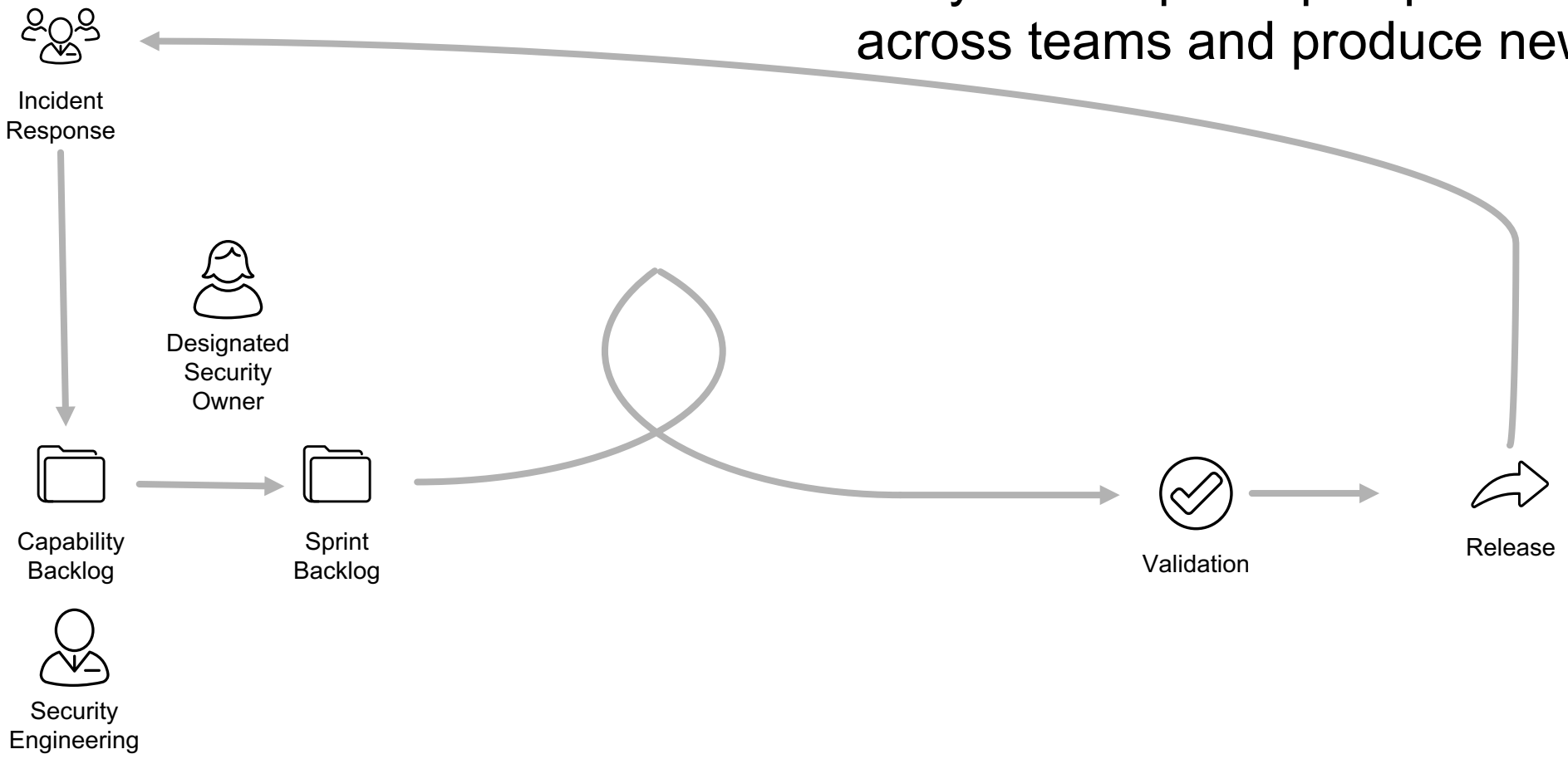
Information is openly available



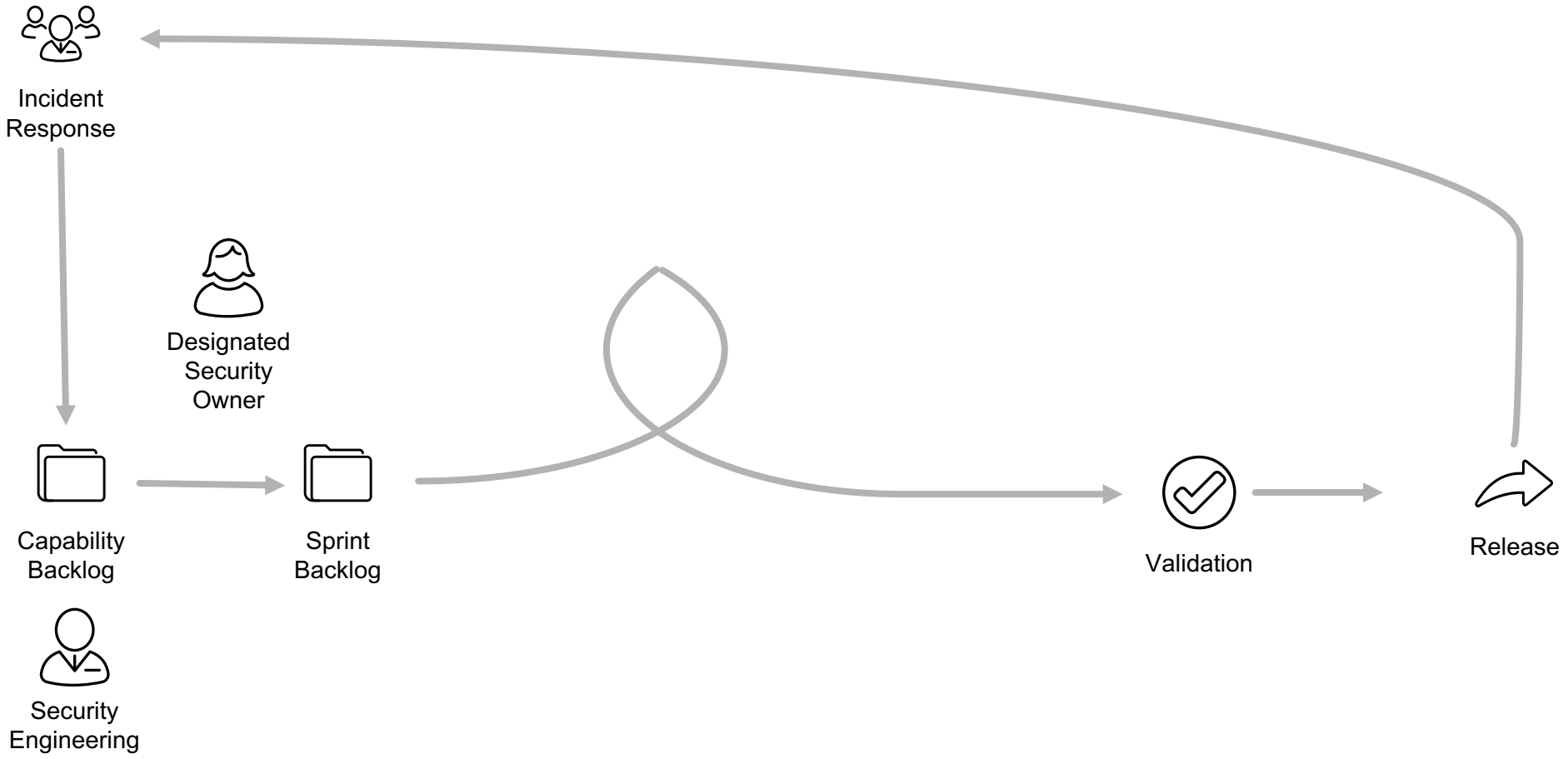


The requestor validates that the requirements of the original ‘user story’ have been met. Deviations are permitted at the sub-story level. If there are any deviations or changes, a new user story can be authored and prioritized

Daily Standups help to promote sharing across teams and produce new stories



Capture metrics to improve the process



Early Results

- Certain customers have started incorporating this framework into their operations
- Challenges involved buy in with other groups and process purity
- Surprising benefit was increased motivation

Security Takeaways

The Benefits

- Faster time to value
- Save Money
- Higher Motivation
- Greater Collaboration
- Focus limited resources

Related Works

- NIST 800-137 Information Security Continuous Monitoring
- Agile Cybersecurity Action Plan (ACAP)
- Agile Manifesto

Key Takeaways

1. Security is a Program, not a project
2. Outcomes-driven decision making
3. Focus on the ‘quick wins’
4. Foster cross-functional communication
5.

Thank You