Vulcan Project Overview

- Emily Rodriguez (MITRE)
- Will Dower (MITRE)
- Ryan Lakey (VMWare)
- Lincoln Porter (VMWare)

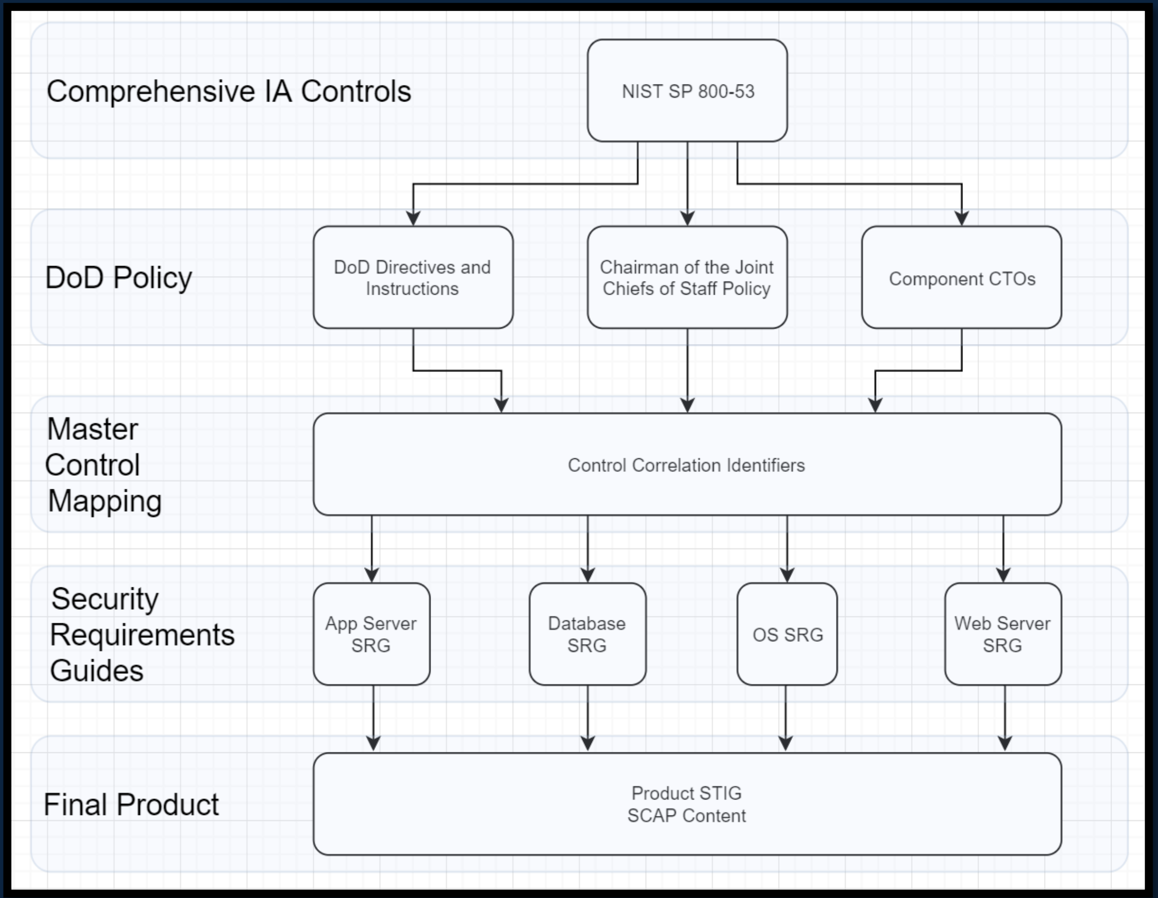
VMware & MITRE Open Collaboration

Vulcan Project History

- Conceptualized by MITRE and DISA's CTO in 2018-2019 to fill a gap in security automation workflows
- Hardening and testing security occurred at the speed of automation -- *writing security guidance became the bottleneck*
- Creating security guidance is a manual process

- Needed a tool for security guidance creation
- Created the first alpha build of Vulcan presented to DISA
- VMware became our corporate partner in Vulcan development
- VMware and MITRE have collaborated on Vulcan development ever since – the project is open-sourced and ready for use by the security community.

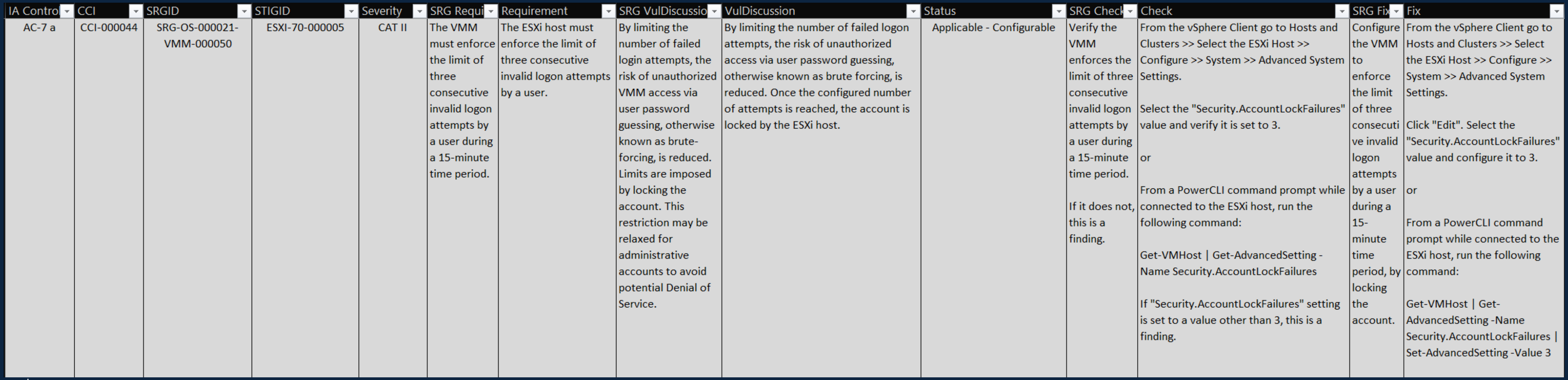
What is a STIG & how is it traditionally created?



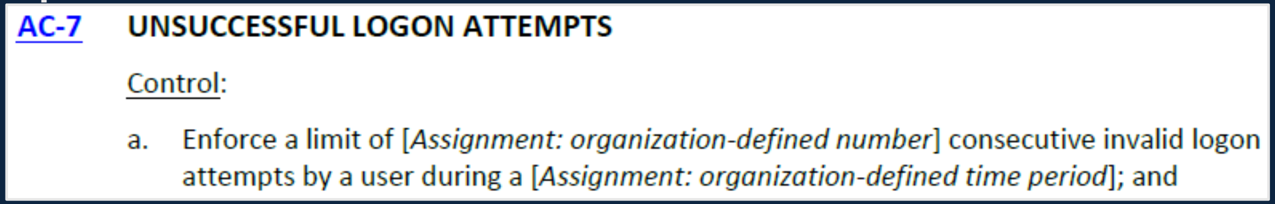
Comprehensive IA Controls
NIST SP 800-53
DoD Policy
DoD Directives and Instructions
Chairman of the Joint Chiefs of Staff Policy
Component CTOs
Master Control Mapping
Control Correlation Identifiers
Security Requirements Guides
App Server SRG
Database SRG
OS SRG
Web Server SRG
Final Product
Product STIG
SCAP Content

Security Technical Implementation Guide (STIG)

Traditional Process for STIGs



IA Contro	CCI	SRGID	STIGID	Severity	SRG Requi	Requirement	SRG VulDiscussio	VulDiscussion	Status	SRG Check	Check	SRG Fi	Fix
AC-7 a	CCI-000044	SRG-OS-000021-VMM-000050	ESXI-70-000005	CAT II	The VMM must enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period.	The ESXi host must enforce the limit of three consecutive invalid logon attempts by a user.	By limiting the number of failed login attempts, the risk of unauthorized VMM access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account. This restriction may be relaxed for administrative accounts to avoid potential Denial of Service.	By limiting the number of failed logon attempts, the risk of unauthorized access via user password guessing, otherwise known as brute forcing, is reduced. Once the configured number of attempts is reached, the account is locked by the ESXi host.	Applicable - Configurable	Verify the VMM enforces the limit of three consecutive invalid logon attempts by a user during a 15-minute time period. If it does not, this is a finding.	From the vSphere Client go to Hosts and Clusters >> Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Security.AccountLockFailures" value and verify it is set to 3. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures If "Security.AccountLockFailures" setting is set to a value other than 3, this is a finding.	Configure the VMM to enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period, by locking the account.	From the vSphere Client go to Hosts and Clusters >> Select the ESXi Host >> Configure >> System >> Advanced System Settings. Click "Edit". Select the "Security.AccountLockFailures" value and configure it to 3. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures | Set-AdvancedSetting -Value 3



AC-7 **UNSUCCESSFUL LOGON ATTEMPTS**

Control:

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

Manual development of the STIG from a spreadsheet of the SRG.

Traditional Process for STIGs the Challenges

Logistics

Collaborating and maintaining excel spreadsheets

Collaboration

Enabling STIG development between people and teams

Updates

New content revisions, what changed in the product?

Automation

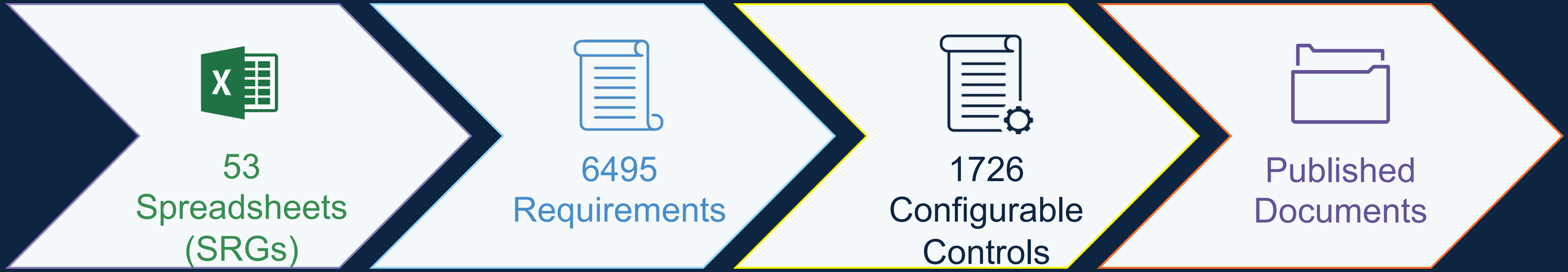
Writing tests, functional testing, staying in sync with content

Artifacts

Generating documents, transforming data to other formats

STIG Lifecycle Challenges VCF 4.x Example

VMware Cloud Foundation 4.x + vRealize Suite



53 Spreadsheets (SRGs)

6495 Requirements

1726 Configurable Controls

Published Documents

9+ products

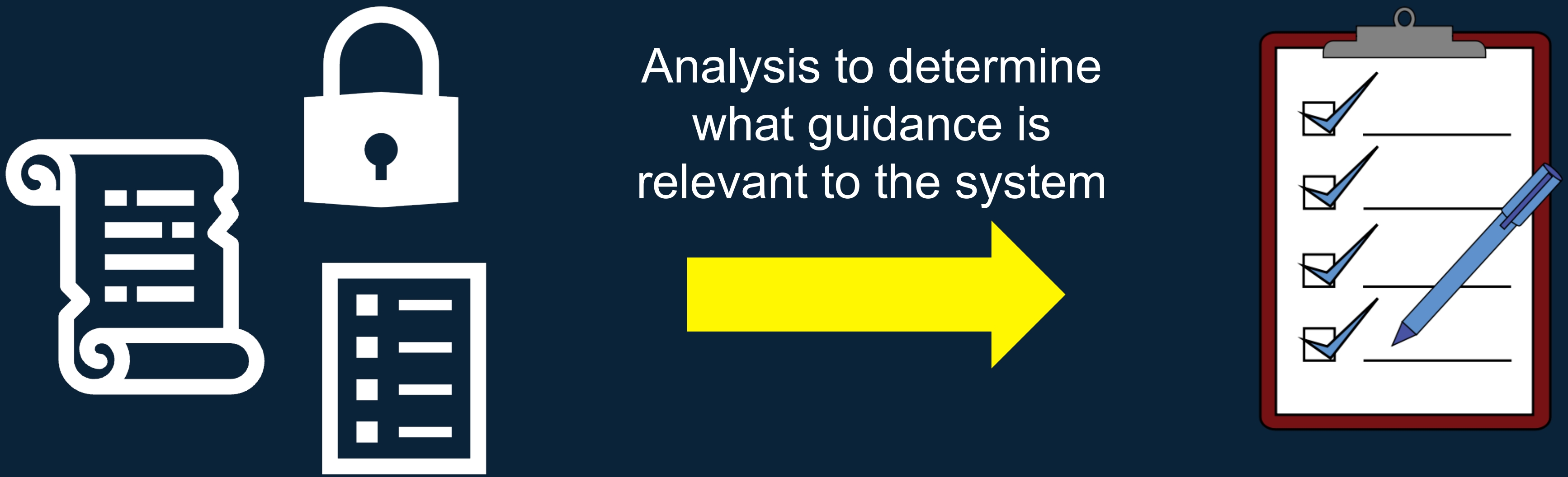
26 Technologies

Months of testing

Security Guidance: Building STIG-Ready Content

Develop STIG Ready Content from SRGs with Vulcan

Avoiding repeated manual assessment for programs and capturing the value of collaboration



Analysis to determine what guidance is relevant to the system

General Guidance (e.g. SRG)

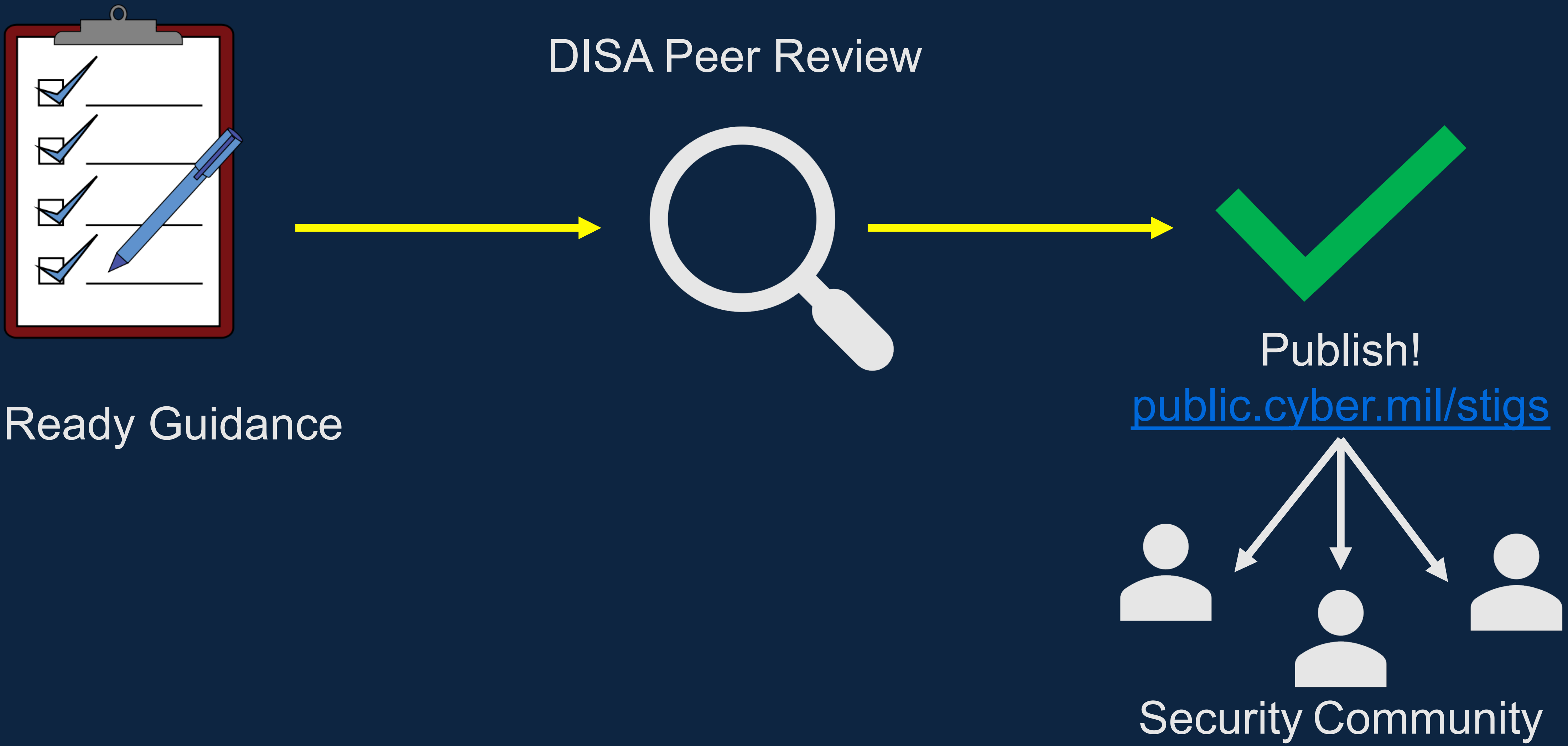
SRG-aligned STIG Ready Guidance

High-Level Security Requirements, Best Practices, Standards

Government and Industry Sources

Specific Instructions for Specific System Components

STIG-Ready Content



STIG Ready Guidance

DISA Peer Review

Publish!

public.cyber.mil/stigs

Security Community

“Security Guidance” vs “STIG-Ready Content” vs “STIGs”

- Security guidance is a general term – examples: CIS Benchmarks, STIGs, PCI benchmarks, vendor guidance, etc.
  - Ex. AWS uses “Best Practices” documents for S3, RDS. . .
- A STIG is tailored security guidance derived from SRGs for a component category that *is formally reviewed and published by DISA Services Directorate (SD) as the DoD standard for a particular system*
- STIG-ready content is tailored security guidance derived from SRGs for a component category that *has not (yet) undergone DISA SD’s formal review and publication via the Vendor Intent process*
  - Vulcan can help you author all the pieces needed for this

Using Vulcan © for Streamlining STIG-Ready Content Development

Vulcan © Project Goals

COMPLIANCE AS CODE

- Automation is tied to the source control
- Content updates also update code
- Changes automatically generated between releases as a detailed diff view

EFFICIENCY

- Artifact generation automated (XCCDF, InSpec, XLS, Revision History)
- Content reuse of common components
- STIG ID generation
- Import existing content in spreadsheets
- Handle adding controls as needed
- Associate requirements met by other controls
- SRG revision updates

GOVERNANCE

- Scale content generation to stakeholders
- Approval process
- Track changes and revert
- Release process
- Permissions model to support multiple projects and roles

USER EXPERIENCE

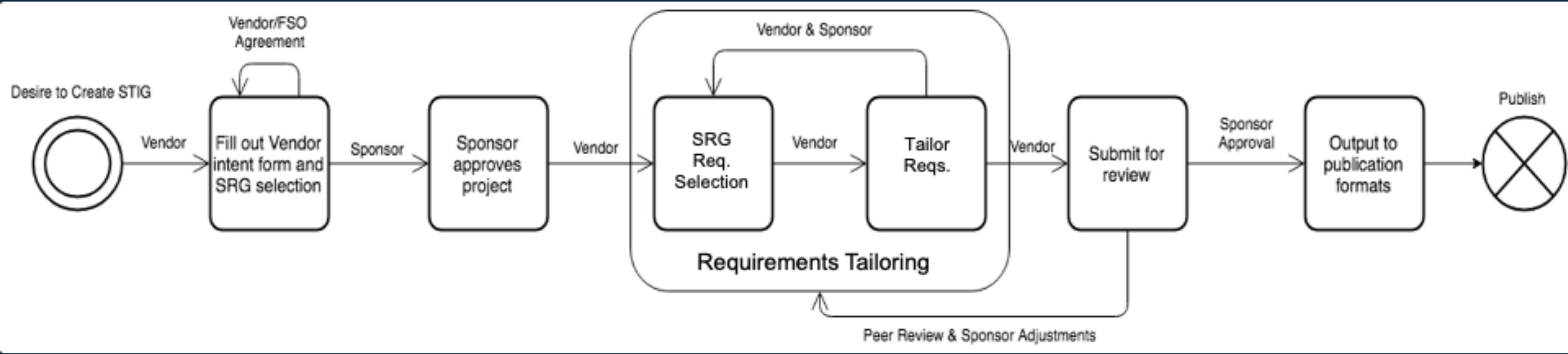
- Functional replacement for spreadsheets
- Sort and Filter controls by various fields
- Searchable
- Embedded guidance
- Spell check
- Comment History

STRATEGIC PRIORITIES

- Open Source Capability – https://github.com/mitre/vulcan
- Support STIG project engagement with DISA
- Enable other compliance needs (FedRAMP, IL4/5/6)

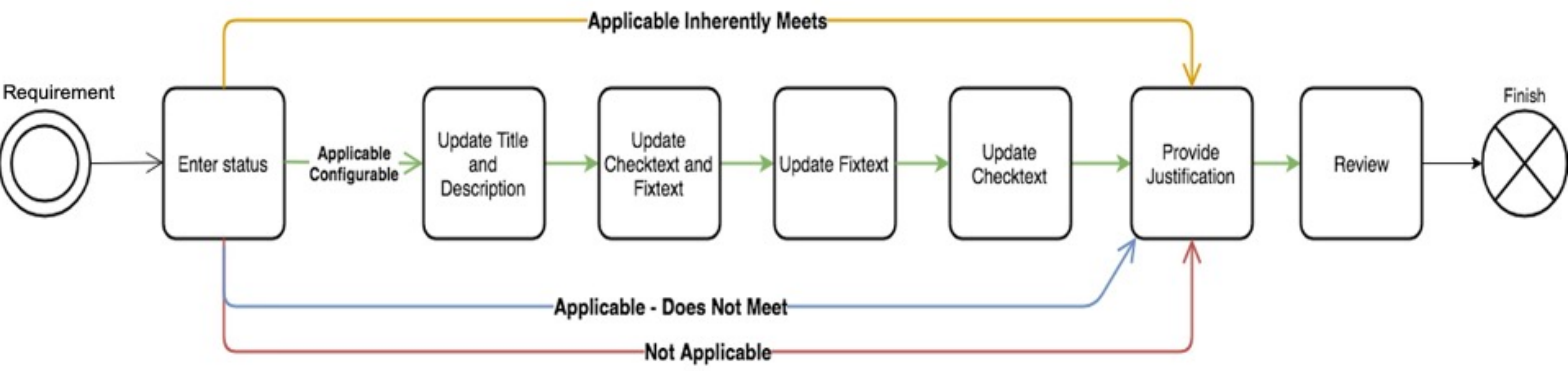
Core Vulcan © Workflow Process

- Import high-level security guidance
- Create new logical component from high-level guidance



Requirement Workflow Process

- SRGs are ultimately collections of security requirements for a system category
- Have SMEs review each requirement and determine applicability and how to implement it for the specific component



DEMO:
MITRE Vulcan © Deployment

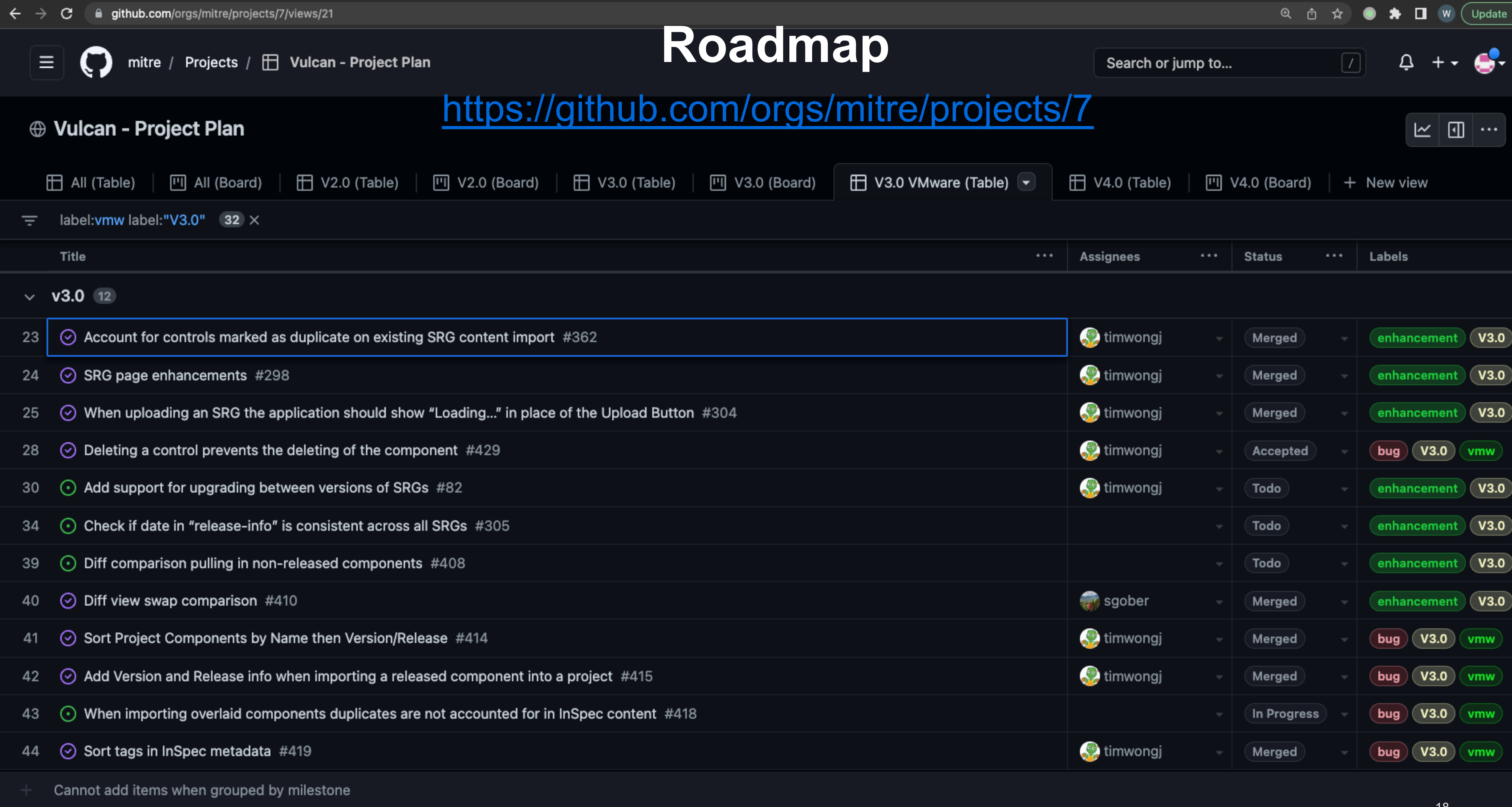
A web application to streamline security guidance development.
vulcan.mitre.org

Demo - Using Vulcan © in Production

Lincoln Porter & Ryan Lakey

Roadmap

https://github.com/orgs/mitre/projects/7



Vulcan - Project Plan

label:vmw label:"V3.0" 32

v3.0 12

	Title	Assignees	Status	Labels
23	Account for controls marked as duplicate on existing SRG content import #362	timwongj	Merged	enhancement V3.0
24	SRG page enhancements #298	timwongj	Merged	enhancement V3.0
25	When uploading an SRG the application should show "Loading..." in place of the Upload Button #304	timwongj	Merged	enhancement V3.0
28	Deleting a control prevents the deleting of the component #429	timwongj	Accepted	bug V3.0 vmw
30	Add support for upgrading between versions of SRGs #82	timwongj	Todo	enhancement V3.0
34	Check if date in "release-info" is consistent across all SRGs #305		Todo	enhancement V3.0
39	Diff comparison pulling in non-released components #408		Todo	enhancement V3.0
40	Diff view swap comparison #410	sgober	Merged	enhancement V3.0
41	Sort Project Components by Name then Version/Release #414	timwongj	Merged	bug V3.0 vmw
42	Add Version and Release info when importing a released component into a project #415	timwongj	Merged	bug V3.0 vmw
43	When importing overlaid components duplicates are not accounted for in InSpec content #418		In Progress	bug V3.0 vmw
44	Sort tags in InSpec metadata #419	timwongj	Merged	bug V3.0 vmw

Cannot add items when grouped by milestone

MITRE

Vulcan © - Phase III

- We want to grow the Vulcan © community to:
  - Define our next major set of features
  - Engage with more vendors and STIG content creators/maintainers
  - Create a coalition of support for ongoing development
- Engage with the Vulcan © open-source project – give us issues, PRs, suggestions
- Build STIG-ready content where none exists to help the security community work together to solve their cyber challenges
- Work with authors of other security benchmarks to see if the Vulcan © project can be expanded to support their workflows
  - FedRamp, PCI-DSS, GDPR

Vulcan	**https://mitre-vulcan-staging.herokuapp.com**
Vulcan Source Code	https://github.com/mitre/vulcan
MITRE SAF Info	https://saf.mitre.org/
MITRE GitHub	https://github.com/mitre/(*baseline or app)

Questions?

MITRE Security Automation Framework ©

saf@groups.mitre.org

Demo Sites and Source Code

Vulcan©	https://mitre-vulcan-staging.herokuapp.com
Vulcan© Source Code	https://github.com/mitre/vulcan
MITRE SAF© Info	https://saf.mitre.org/
MITRE GitHub	https://github.com/mitre/(*baseline or app)

MITRE

Next Step & Actions

- Department Level Support, Policy Updates and Clarification
  - Clarify policy support beyond just SCC, SCAP, etc.
  - Pushback, Challenges & Clarifications
- Supporting Engagement with DISA, Services & Vendors
  - STIG-Ready Trusted Vendor Program *
  - DCSA and DSCA Adoption
    - Diane Phan - Technical Director – Former DISA eMass PMO
- How can the SAF support DOD CIO's Container Security Workstream
- Thoughts & Suggestions