MOSAICS

MOSAICS Protection Requirements and Scheme

5 November 2020

Harley Parkes (JHU APL)

Automation and SOAR Security

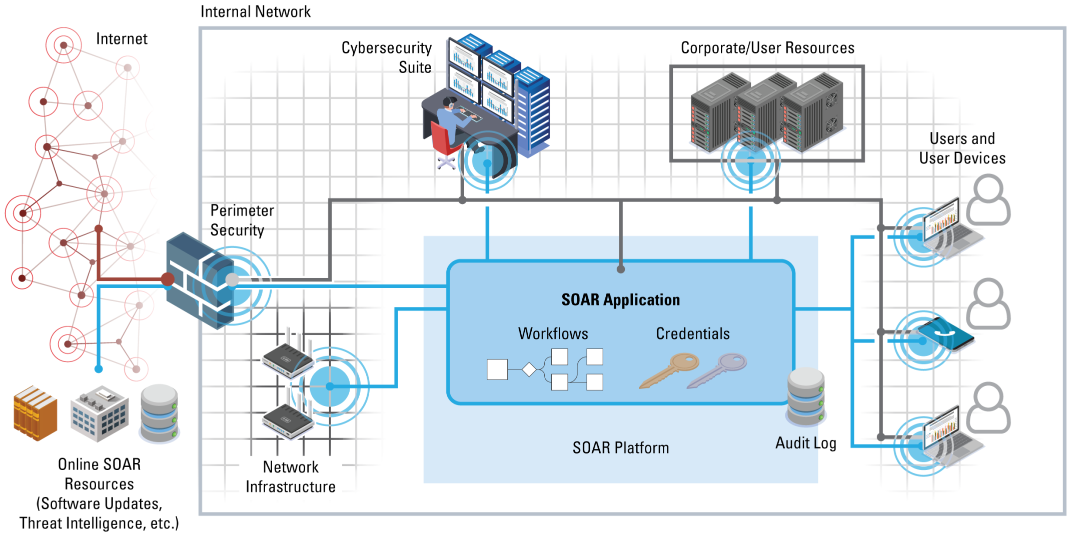
1. Security practices codified into workflows
   a. Improper execution can lead to security vulnerabilities

2. Workflows are software and need to be protected accordingly

3. Privileged access to potentially everything on network

4. Access to plaintext credentials
   a. Logins require access credentials

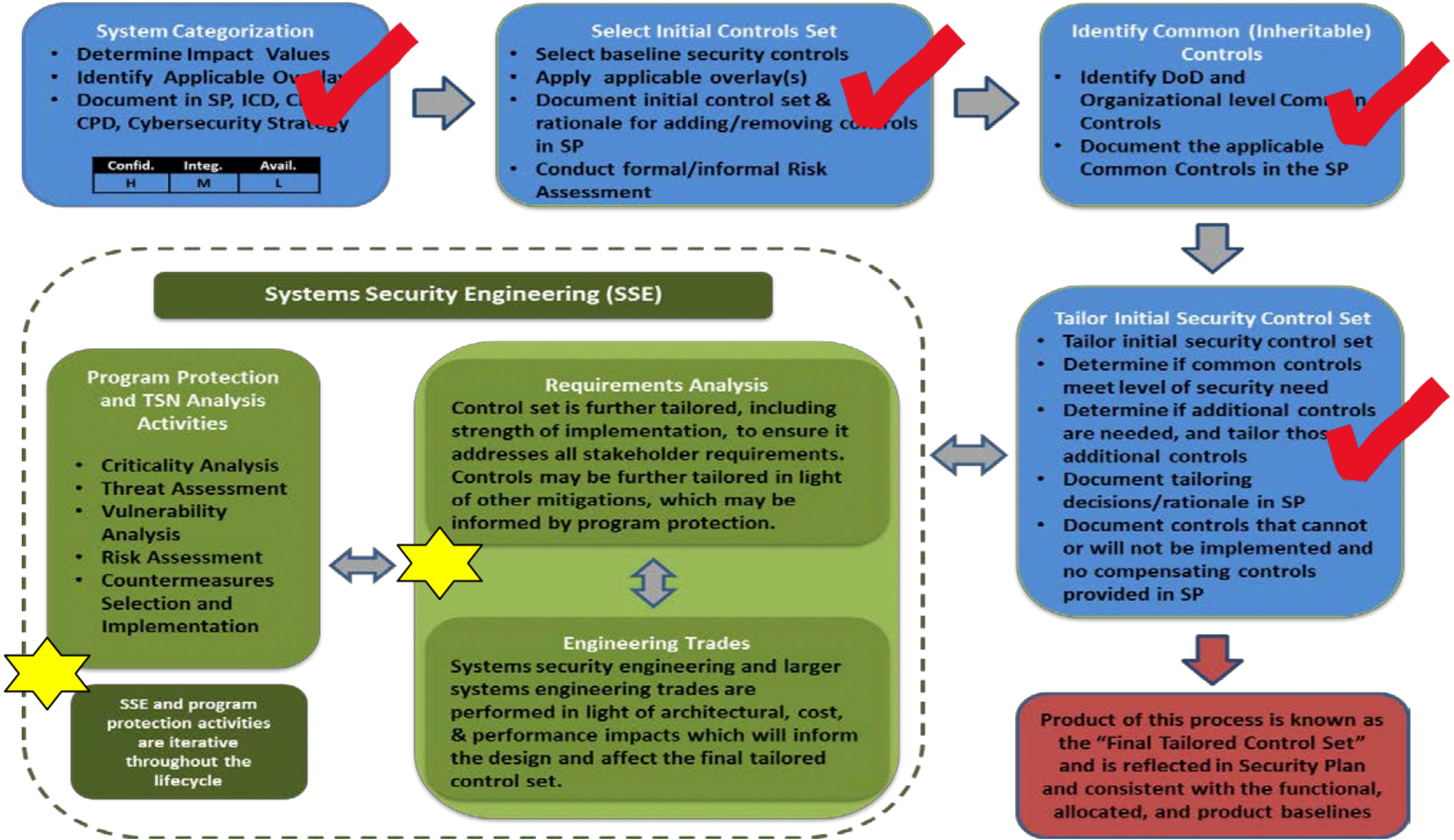
5. Need to support SW best practices
   a. Approval policies for operations
   b. Integrity protections
   c. Robust error handling and logging



MOSAICS
2020
INDUSTRY
DAY

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

MOSAICS Application of RMF



System Categorization
- Determine Impact Values
- Identify Applicable Overlays
- Document in SP, ICD, CDD, CPD, Cybersecurity Strategy

Confid.	Integ.	Avail.
H	M	L

Select Initial Controls Set
- Select baseline security controls
- Apply applicable overlay(s)
- Document initial control set & rationale for adding/removing controls in SP
- Conduct formal/informal Risk Assessment

Identify Common (Inheritable) Controls
- Identify DoD and Organizational level Common Controls
- Document the applicable Common Controls in the SP

Tailor Initial Security Control Set
- Tailor initial security control set
- Determine if common controls meet level of security need
- Determine if additional controls are needed, and tailor those additional controls
- Document tailoring decisions/rationale in SP
- Document controls that cannot or will not be implemented and no compensating controls provided in SP

Product of this process is known as the "Final Tailored Control Set" and is reflected in Security Plan and consistent with the functional, allocated, and product baselines

Systems Security Engineering (SSE)

Program Protection and TSN Analysis Activities
- Criticality Analysis
- Threat Assessment
- Vulnerability Analysis
- Risk Assessment
- Countermeasures Selection and Implementation

SSE and program protection activities are iterative throughout the lifecycle

Requirements Analysis
Control set is further tailored, including strength of implementation, to ensure it addresses all stakeholder requirements. Controls may be further tailored in light of other mitigations, which may be informed by program protection.

Engineering Trades
Systems security engineering and larger systems engineering trades are performed in light of architectural, cost, & performance impacts which will inform the design and affect the final tailored control set.

SOAR Best Practices

Prevent the execution of unknown binaries and the execution of non-SOAR applications on systems hosting SOAR. ✓

Enable continuous monitoring of automation to record security sensitive events. ✓

Establish SOAR backup and restore procedures to ensure rapid recovery. ✓

Safeguard SOAR workflows by ensuring a fail-safe path is achievable ✓

- Errors encountered during workflow execution promptly reported to operators.

Establish and manage a **SOAR-specific identification and authentication service** ✓

Use **multi-factor authentication** for users.

Protect SOAR network connections by using secure cryptographic protocols and requiring the use of certificate-based mutual authentication. ✓

SOAR Protection Profile

Select a SOAR product that meets NIAP certification standards. ✗

1. Orchestration Protection Profile” – Task from NSA
   a. Partnership with NIAP
   b. Robust participation from industry
      a. (SOAR vendors, test labs)
   c. Bi-weekly Technical Community meetings

2. Currently in the public review process

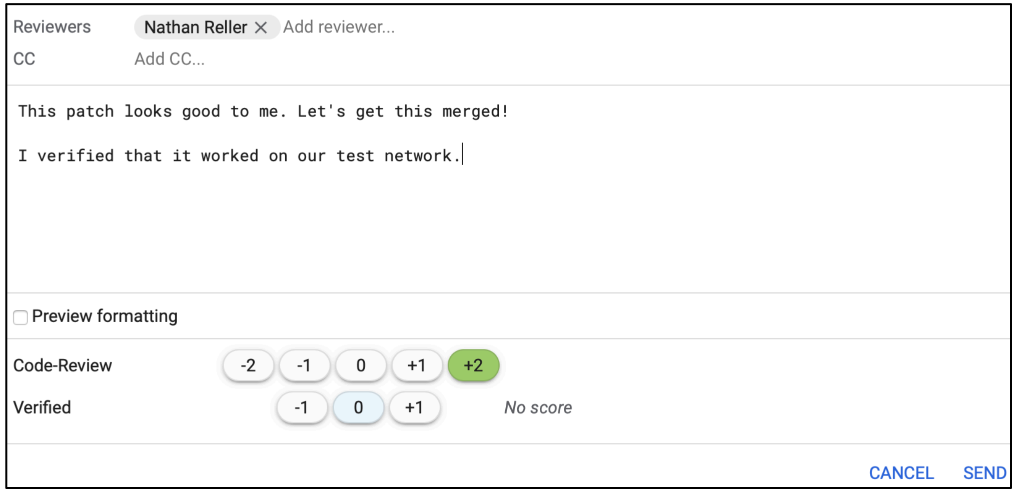
MOSAICS
2020
INDUSTRY
DAY

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Workflow Approval Process

1. Intent
   a. Integrate coding best practices
   b. Multi-party consent

2. Most SOAR applications do not support workflow approval processes



Reviewers: Nathan Reller × Add reviewer...

CC: Add CC...

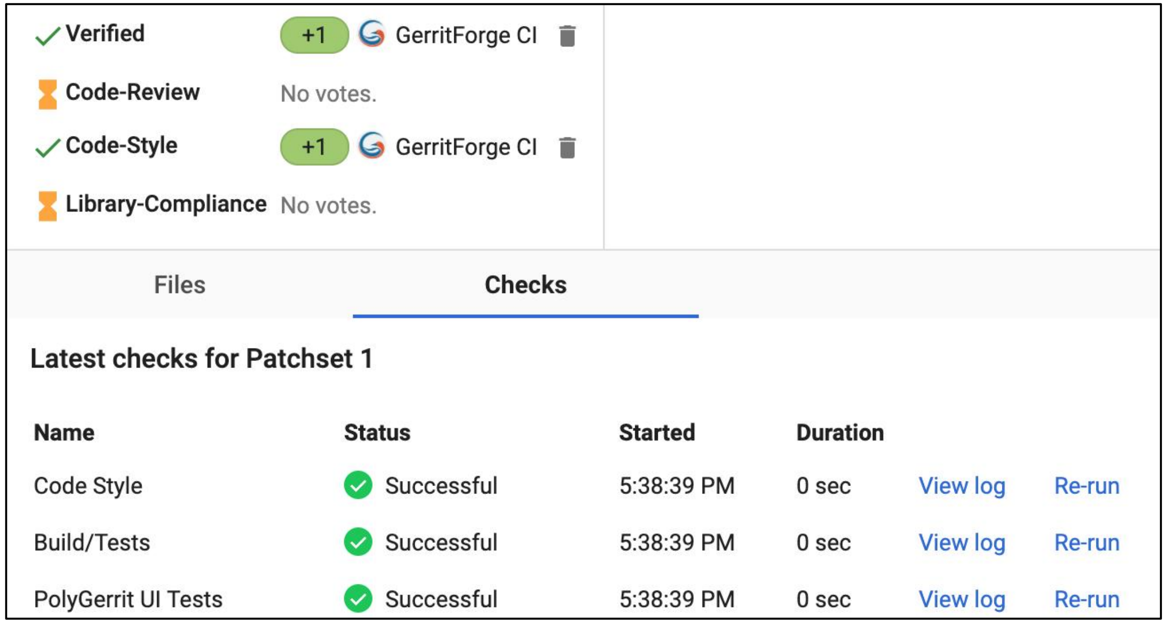
```
This patch looks good to me. Let's get this merged!

I verified that it worked on our test network.
```

□ Preview formatting

Code-Review: -2 -1 0 +1 [✓ +2]

Verified: -1 [✓ 0] +1 *No score*



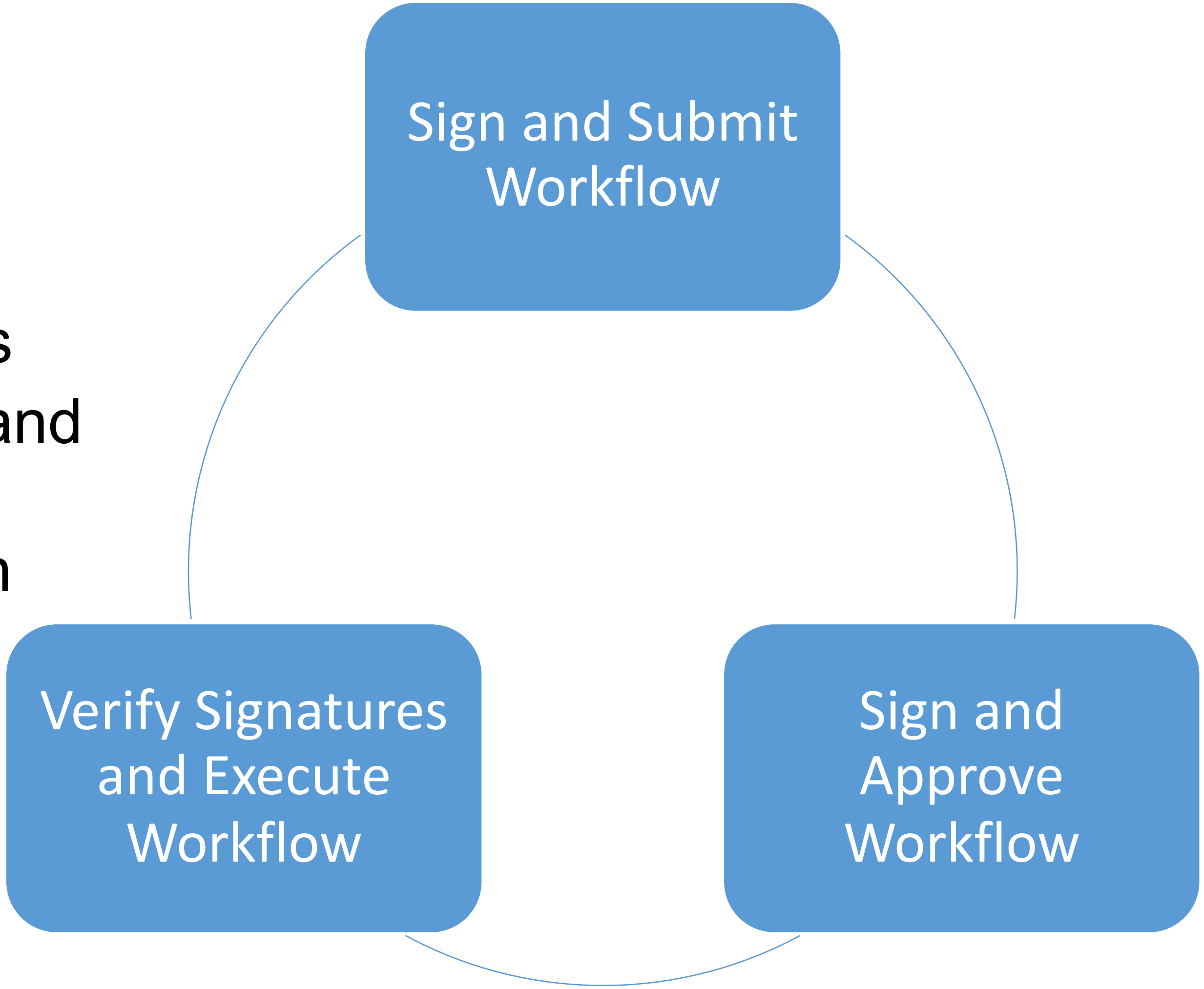
✓ Verified	+1	GerritForge CI
Code-Review	No votes.	
✓ Code-Style	+1	GerritForge CI
Library-Compliance	No votes.	

Latest checks for Patchset 1

Name	Status	Started	Duration		
Code Style	✓ Successful	5:38:39 PM	0 sec	View log	Re-run
Build/Tests	✓ Successful	5:38:39 PM	0 sec	View log	Re-run
PolyGerrit UI Tests	✓ Successful	5:38:39 PM	0 sec	View log	Re-run

Workflow Integrity Protections

1. Intent
   a. Prevent tampering of workflows
   b. Provide provenance of author and approver
   c. Validate prior to each execution



Sign and Submit Workflow

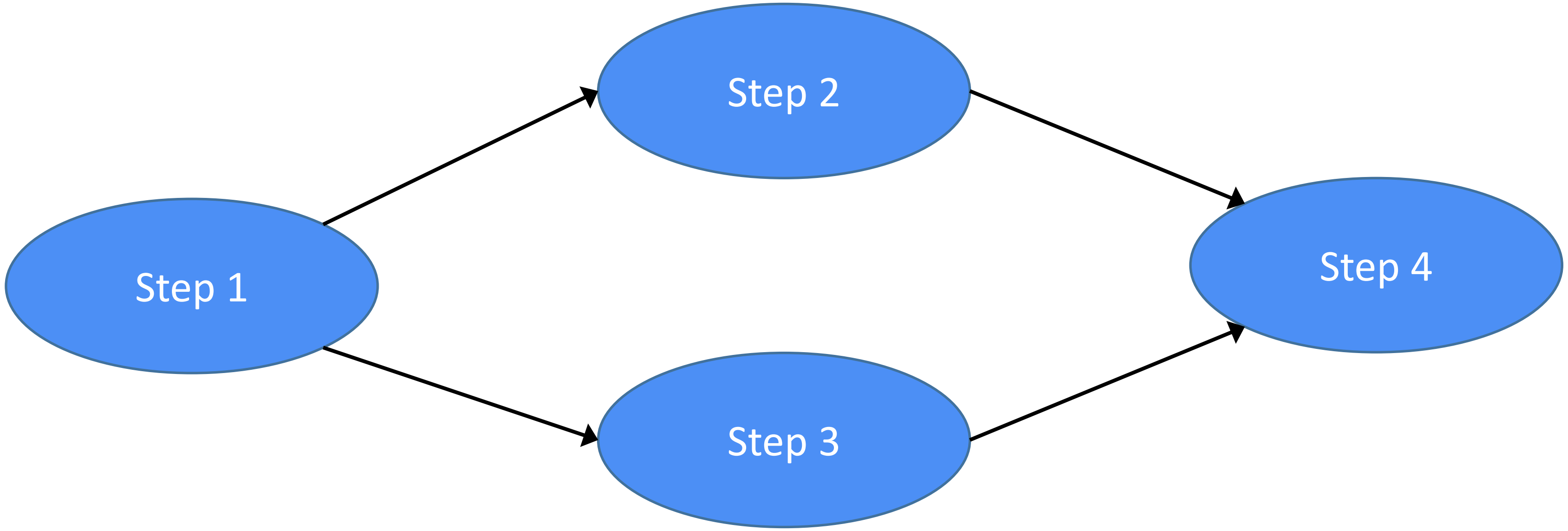
Sign and Approve Workflow

Verify Signatures and Execute Workflow

Workflow Success

- Intent of requirements
  - Notify users when workflows do not execute successfully

- Problem
  - Success is not defined consistently amongst SOAR vendors



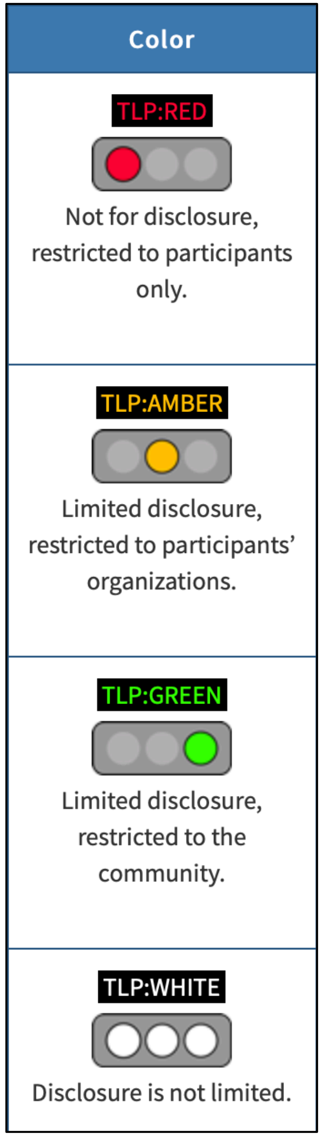
MOSAICS

2020 INDUSTRY DAY

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Access Control

- Intent
  - Define policy support but not policy
  - Label resources with sensitivity levels
  - Support attribute-based access control (ABAC)
  - Support role-based access control (RBAC) and ABAC
- Resources that should have sensitivity levels
  - Workflow artifacts/threat intelligence
  - Workflows
- Possible sensitivity level schemes for resources:
  - Traffic Light Protocol (TLP)
  - Government classifications



Color
TLP:RED ●○○ Not for disclosure, restricted to participants only.
TLP:AMBER ○●○ Limited disclosure, restricted to participants' organizations.
TLP:GREEN ○○● Limited disclosure, restricted to the community.
TLP:WHITE ○○○ Disclosure is not limited.

MOSAICS
2020
INDUSTRY
DAY

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Needs from Industry

1. Focus on workflow and credential protections!
2. Consider ABAC for SOAR
   a. Tagging for subjects and objects
3. Participate in PP public review process
4. Obtain NIAP certification for SOAR!

Questions??