April, 2025

fedramp.gov/20x

FedRAMP20X

Automating Assessment Working Group Townhall

Starting at 1:03pm until 2pm (1 hour today)


[REC ●]

Today's Agenda

- GitHub Discussion Recap
- How this is informing our work
- FedRAMP 20x Phase One Pilot
- Pete Waterman AMA
- RFCs, etc!
- Next steps

Workgroup Discussion Forum on GitHub:

https://github.com/FedRAMP/automating-assessment-cwg/discussions

Workgroup Video Recordings:

https://www.youtube.com/@FedRAMP/videos

How we'll work

The purpose of bi-weekly meetings is to recap discussions taking place in GitHub

For all of our Working Groups:

The Working Group GitHub Repo will be the source of work/truth. This includes:

- All discussions related to the working group
- Development/demonstration of proof of concepts
- Providing a venue for information sharing that may inform updates in guidance
- This is a part of our commitment to operating in public, transparently, in a way that fosters collaboration amongst the variety of stakeholders

Again– GitHub will be the primary hub for discussion and collaboration

Thank you for your participation so far!

	Last 2 Weeks	Total
Individual Discussions	5	18
Top Level Comments	18	104
Comment replies	42	179

Top 5 authors from the last two weeks:

- ★ **1. sunstonesecure-robert**
- ★ **2. jsantore-cgc**
- ★ **3. ProdSecCSP**
- ★ **4. ChanceofClouds**
- ★ **5. DragonHorse2019**

https://github.com/FedRAMP/automating-assessment-cwg/discussions

Ideas, themes, and code!

"[Can] we measure how many system changes are correctly monitored over total number of changes detected, internally or externally? If we go with this approach, we limit the need for very detailed classification about what is true and what is false."

1) Run each cloud connector to gather userId → methods list
2) Normalize combined data into a single list
3) Apply the rule: methods intersect {FIDO2, SECURITY_KEY, OATH_TOKEN} must be non-empty
4) Classify each user as Compliant or Non-Compliant

"In this case, support for phishing resistant MFA without an evaluation of other signals on its own is an incomplete assessment of an IdP. It's the aggregate of the tests (available in CISA ScubaGear) that would help us automate an audit."

"Push a new release and you have: {n-1,n-1, n-1,n}. Since everything is n-1 compatible the application functionality ran just fine. After you see things stable, you start cycling in more version n's: {n-1, n-1, n, n}. Then repeat again with version n+1. If you need to back out, you just remove that node from the load balancer."

How this is informing FedRAMP's work

- Folks are already coming up with creative, automatable assessment methods
  - Ways to use existing tools to apply to certain validations
  - Simple, platform-agnostic, programmatic ways to assess MFA
  - What distinguishes the "good" from the "bad" change management practices
    - How to assess that

- We want to incentivize more innovation and ideas from industry
  - In the spirit of "We set the standards and policies that enable private innovation to create the solution.

- Therefore, we released the **Key Security Indicators** & the **Phase One Pilot**
  - Come up with your own methods for addressing our Key Security Indicators
  - Wrap it up in a machine readable format
  - Submit to FedRAMP

FedRAMP 20x Phase One Pilot Goals

Understand effectiveness of Key Security Indicators for:

1. Automated technical assessment and validation of security decisions
2. Application of existing materials from SOC 2
3. 3PAO review and assessment
4. Creation and maintenance of machine-readable materials

Qualifying participants that successfully complete Phase One will:

1. Receive **FedRAMP Low** authorization (agency sponsor not required)
2. Be prioritized for **FedRAMP Moderate** in Phase Two

Pilot Participation Criteria

You are most likely to successfully complete the Phase One Pilot if you are…

Deployed on a FR Authorized Platform	Includes the use of cloud-native services from the host platform and the use of only FR Authorized external services
Service only over the public internet	Includes service via browser and API– does not include web or mobile applications or other clients/agents
Pre-existing certification or ATO	You have completed a SOC 2 Type 2 audit or federal agency ATO process within the last 12 months
3PAO	You have a 3PAO ready to conduct a pilot 20x assessment

20x Phase One Pilot Deliverables

We aren't looking for the same-old, narrative-driven, hundreds of pages of documents. We want to see:

- *Auto-generated evidence for the KSI Validations*
- *All KSI responses and evidence compiled into a machine-readable data format*
    - *Invent your own, but provide lightweight documentation or schema to help us orient to your format*
- *A 3PAO checks your work*
- A proposal or prototype for continuously reporting

This is the most flexible phase– Phase One submissions will serve as examples to the community and inform future standards for future phases

Community Working Groups

We have a new category of discussion in our working groups called “20x Phase One Pilot”. This category is present in:

Automating Assessment

Discuss auto-generated evidence and machine-readable data formats here

Applying Existing Frameworks

Discuss applying SOC 2 audits & other certs to the FedRAMP 20x KSIs here

Continuous Reporting

Discuss prototypes and proposals for reporting continuously here

fedramp.gov/20x/working-groups

FedRAMP 20x Phase One Example Workflow

CSP develops a process to generate a machine readable file including the KSI Validations and associated evidence. They also create a continuous reporting prototype/plan.

3PAO reviews the process used to generate the file and confirms the process used is generating accurate KSI Validation responses.

The CSP sends the deliverables to the FedRAMP PMO. The PMO will review the submission in the order it was received and provide feedback to the CSP.

If FedRAMP determines that the deliverables meet the FedRAMP 20x standards the CSP will be issued a 12 month FedRAMP Low Authorization and will be listed in the FedRAMP marketplace.

Q&A

Read more: **fedramp.gov/20x/phase-one**

Q&A will also continue in the working group discussion forums.

RFCs are out!

Give us feedback!

- ***Key Security Indicators***
  - You will need to review these in order to participate in the pilot, as the pilot is strongly linked to practical applications of the Key Security Indicators
- *Significant Change Notification Standard*
- *Minimum Boundary Scope Standard*

This week's discussion starters

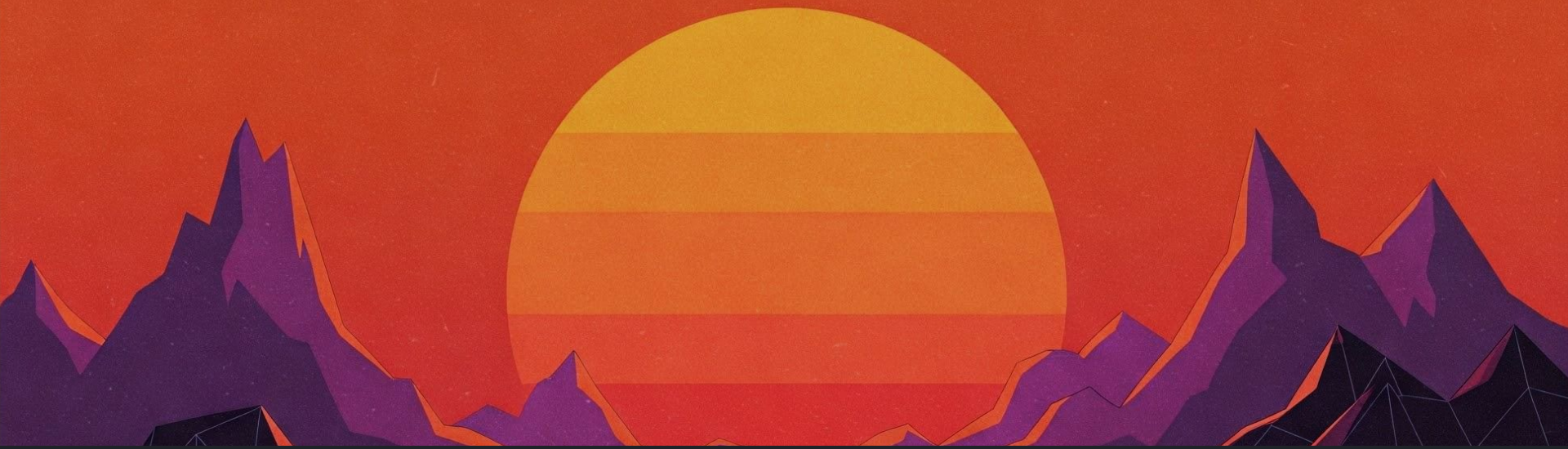
- Key Security Indicators are officially out! Week to week, we will focus on one security area and discuss automation ideas for the validations.
    - Which validations are conducive to automation, and which ones are not?
    - What auto-generated evidence can be applied to each validation?
    - How might 3PAOs assess these validations?
- We will start with Cloud Native Architecture:
    - **A secure cloud service offering will use cloud native architecture and design principles to enforce and enhance the Confidentiality, Integrity and Availability of the system.**

You can already find the discussion posts up on GitHub!

Working Group Next Steps

- Our next recap will be held on the **14th of May at 1 PM ET.**
- If you are interested in bringing forward a topic, prototype, or idea to this working group, post in the discussion forums
  - **This is NOT an opportunity for product pitches**

Close-out



Automating Assessment Working Group