UNCLASS

SCAP
&
AF Mission Planning

Mr. Dave Bricker, Leidos Inc., IVV&E
David.bricker.2.ctr@us.af.mil
850-217-1682

Version 1 - As of 9 Apr 2019

SCAP Workshop

McLean VA – 29 Apr 2019

UNCLASS

UNCLASS

Thinking Out Loud

- Am I overlooking tools that are already out there?
- Do I making creating content harder than it should be?
- Is this the right venue for this discussion?

UNCLASS

UNCLASS

Overview

- AF Mission Planning Systems
- How we use SCAP
- Our Challenges

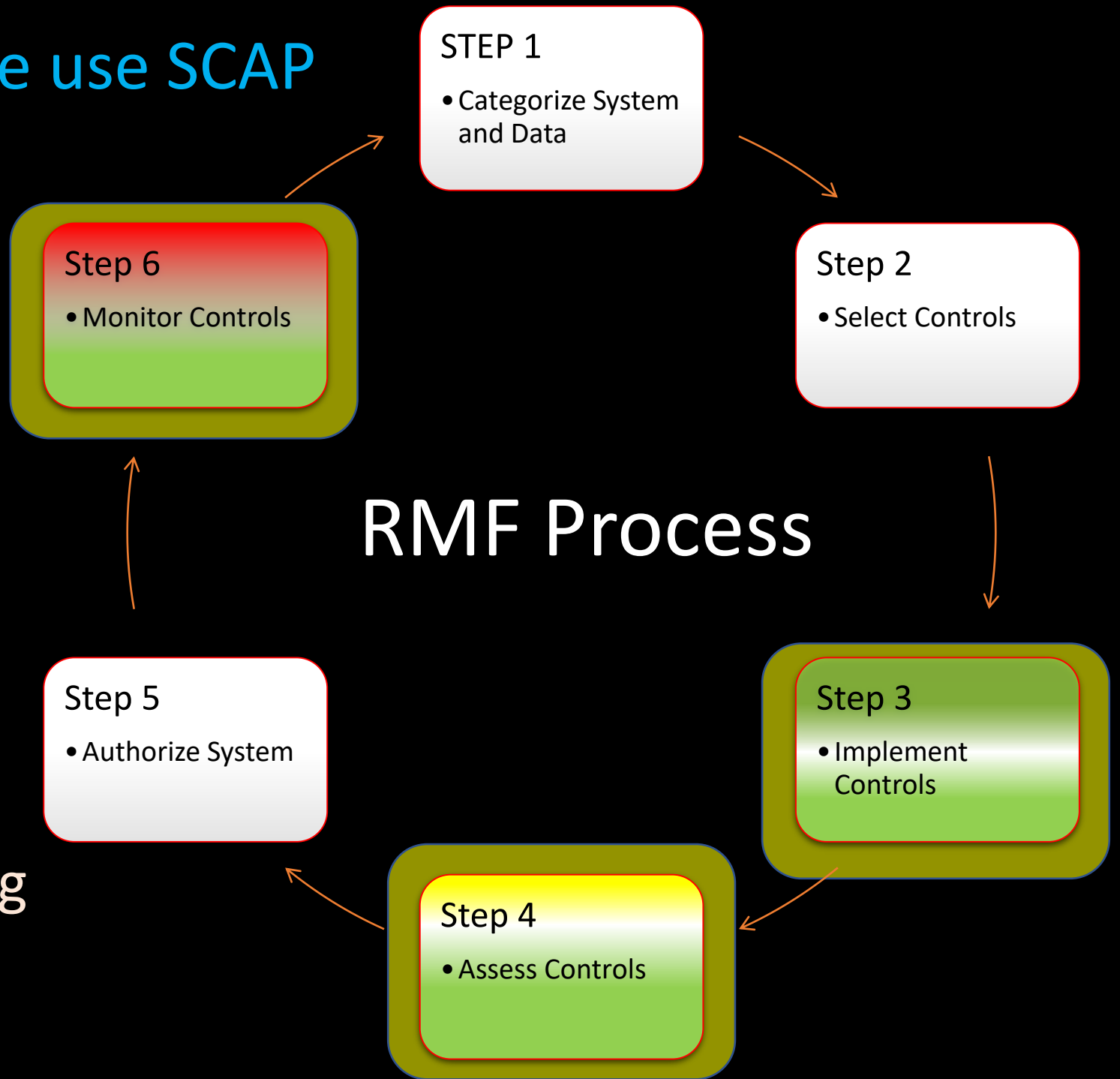
UNCLASS

AF Mission Planning Systems

- Based on AF SDC Client (all the good and bad)
  - 100+ Applications added to baseline SDC
  - Includes GPO's and Monthly Patching
- Windows 7 and Windows 10
- NIPRNET and SIPRNET
- Ad hoc Networks
- Standalone
- HBSS, Tanium, ACAS, and other tools not always in play and they don't focus on Mission Planning Needs!

UNCLASS

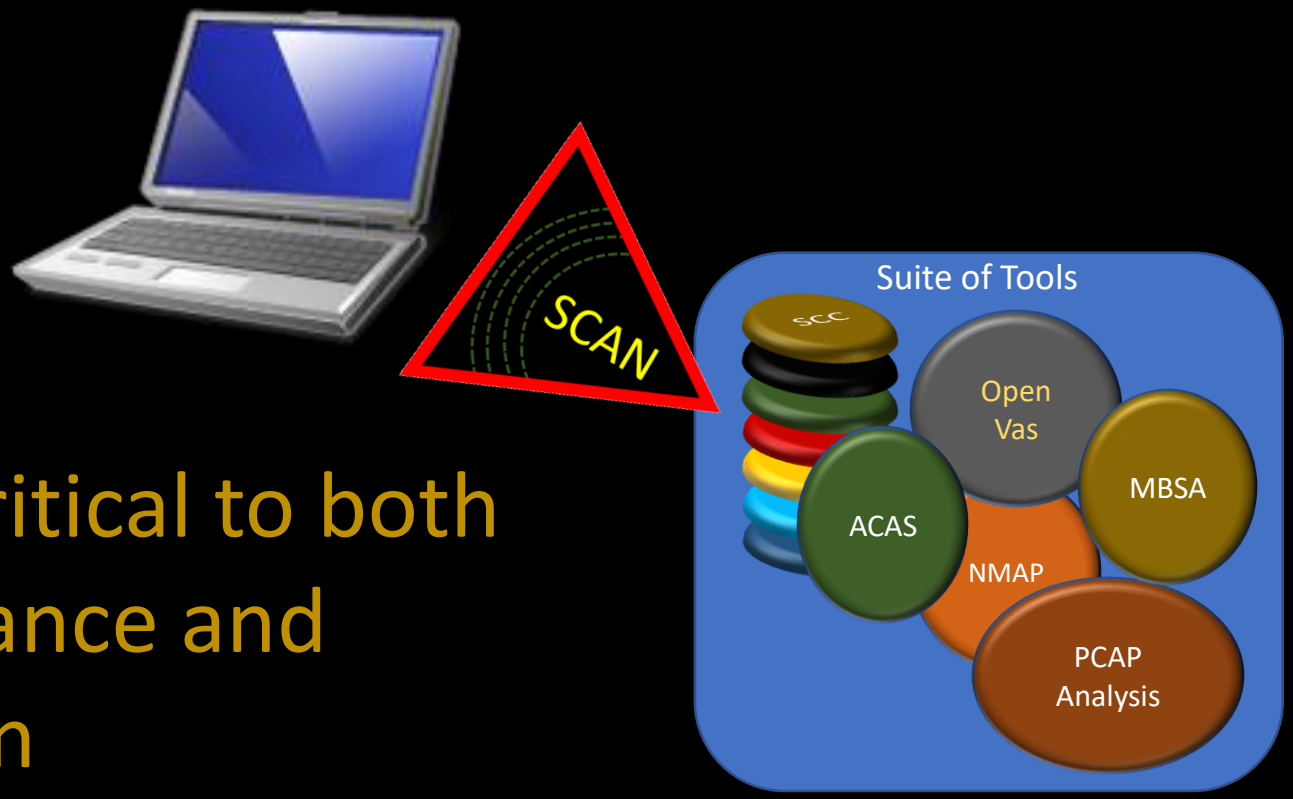
How we use SCAP



SCAP is critical to Measuring Controls during RMF Process

UNCLASS

Many Tools used for Compliance Checking and Continuous Monitoring



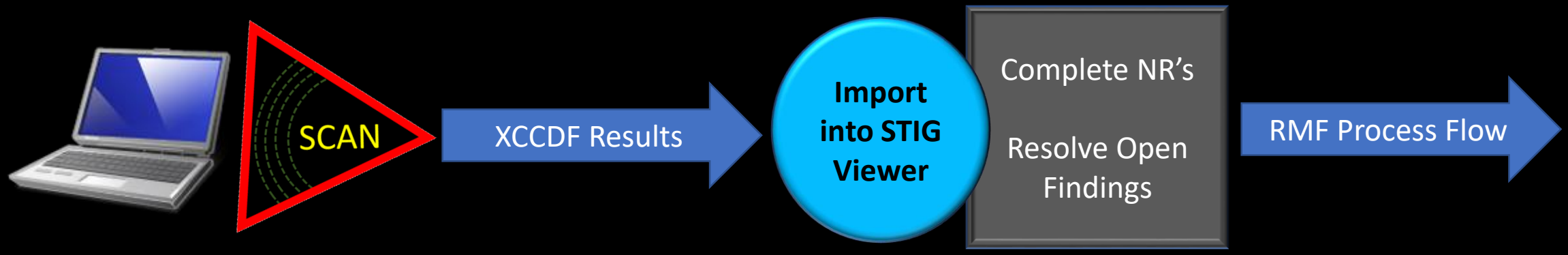
SCAP Critical to both Compliance and ConMon

SCAP content is one part of the suite of tools.

SCAP is a critical part that provides automated compliance checking!!

How we use SCAP

- Navy's Security Compliance Checker (SCC Tool)
- Uses DISA's SCAP content



1) SCAN system with SCAP Content; 2) Import results; 3) Resolve NR's and Open; 4) Report; 5) Monitor

Our Challenges

- ***Where is the Content?*** Missing Automated DISA Content:
  - McAfee (*We created OVAL and SCAP → way too complicated*) 
  - MS Edge Browser (no content or limited OVAL)
  - Java 8 (We created OVAL; transitioned to C# → outputs directly to CKL file.) 
  - Java 7 (We created OVAL; transitioned to C# → outputs directly to CKL file.) 
  - IIS (created our own with C# → Soon to output to CKL)
  - RabbitMQ (No content)
  - Apache2 (Oval, STIG alignment TBD)
  - SQL Server (2012, 2014, or 2016) (Oval, STIG alignment TBD)
  - MySQL anything (Oval, STIG alignment TBD)
  - MS Windows 10 – Only ~75% automated (all other via manual checks)
  - DoTNet - ~75% automated (all other via manual checks)

UNCLASS

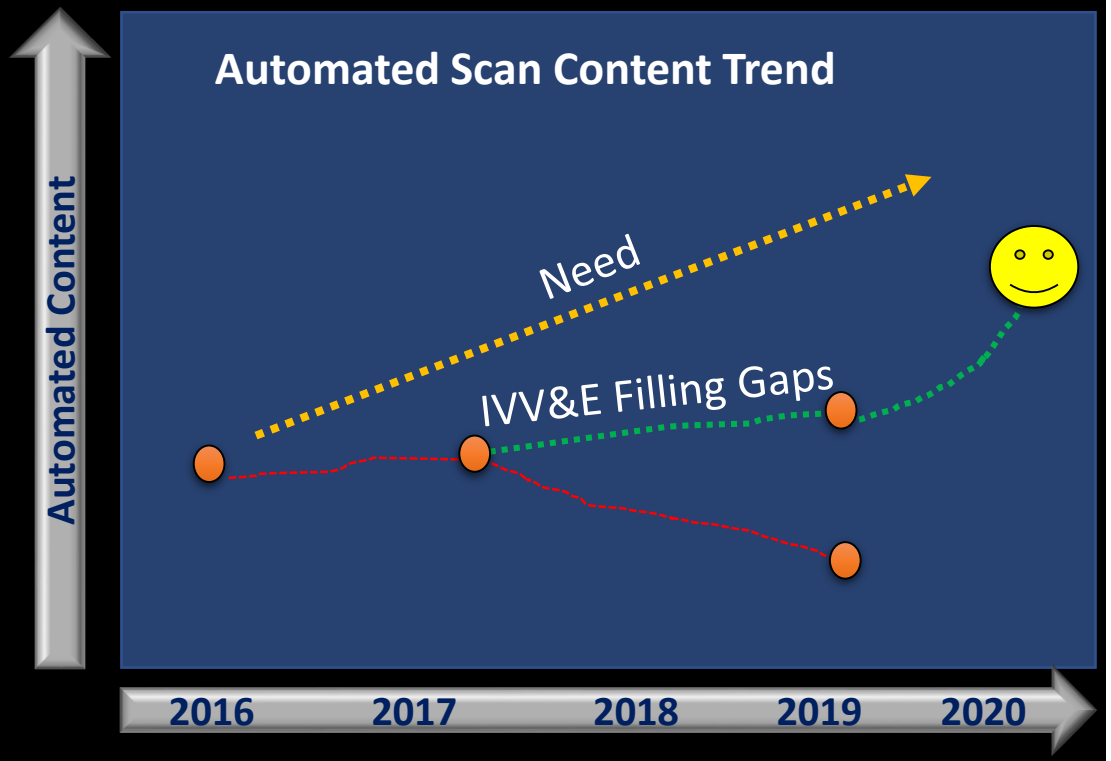
Our Challenges

DISA SCAP

Not keeping pace

*Missing office products

*Windows 7 is sunset



SCAP 1.2 Content

Download	Date	Size	Format
Adobe Acrobat Reader Document Cloud (DC) Classic Track STIG Benchmark - Ver 1, Rel 5	10/24/2018	12 KB	ZIP
Adobe Acrobat Reader Document Cloud (DC) Continuous Track STIG Benchmark - Ver 1, Rel 4	10/24/2018	12 KB	ZIP
Google Chrome for Windows STIG Benchmark - Ver 1, Rel 11	1/18/2019	24 KB	ZIP
Microsoft .Net Framework 4 STIG Benchmark - Ver 1, Rel 5	10/24/2018	9 KB	ZIP
Microsoft Internet Explorer 11 STIG Benchmark - Ver 1, Rel 12	7/20/2018	62 KB	ZIP
Microsoft Windows 10 STIG Benchmark - Ver 1, Rel 13	11/27/2018	97 KB	ZIP
Microsoft Windows 2008 DC STIG Benchmark - Ver 6, Rel 42	7/20/2018	98 KB	ZIP
Microsoft Windows 2008 MS STIG Benchmark - Ver 6, Rel 42	7/20/2018	98 KB	ZIP
Microsoft Windows 2008 R2 DC STIG Benchmark - Ver 1, Rel 30	10/24/2018	113 KB	ZIP
Microsoft Windows 2008 R2 MS STIG Benchmark - Ver 1, Rel 31	10/24/2018	109 KB	ZIP
Microsoft Windows 2012 and 2012 R2 DC STIG Benchmark - Ver 2, Rel 15	1/25/2019	130 KB	ZIP
Microsoft Windows 2012 and 2012 R2 MS STIG Benchmark - Ver 2, Rel 14	11/27/2018	127 KB	ZIP
Microsoft Windows Defender Antivirus STIG Benchmark - Ver 1, Rel 1	4/27/2018	21 KB	ZIP
Microsoft Windows Firewall STIG Benchmark - Ver 1, Rel 7	7/20/2018	13 KB	ZIP
Microsoft Windows Server MS DC 2016 STIG Benchmark - Ver 1, Rel 8	1/25/2019	91 KB	ZIP
Red Hat 6 STIG Benchmark - Ver 1, Rel 22	1/18/2019	90 KB	ZIP
Red Hat Enterprise Linux 7 STIG Benchmark - Ver 2, Rel 2	1/18/2019	96 KB	ZIP
Solaris 10 SPARC STIG Benchmark - Ver 1, Rel 21	1/18/2019	80 KB	ZIP
Solaris 10 x86 STIG Benchmark - Ver 1, Rel 22	1/18/2019	81 KB	ZIP
Solaris 11 SPARC STIG Benchmark - Ver 1, Rel 10	10/24/2018	44 KB	ZIP
Solaris 11 x86 STIG Benchmark - Ver 1, Rel 10			

Office missing for 2+ months
As of 9 Apr 2019

SCAP 1.1 Content

Download			
AIX 6.1 STIG-Benchmark - Ver 1, Rel 9	10/28/2016	70 KB	ZIP
Microsoft Internet Explorer 10 STIG Benchmark - Ver 1, Rel 9	4/28/2017	67 KB	ZIP
Microsoft Windows 7 Audit Benchmark has been moved to the Sunset list.			

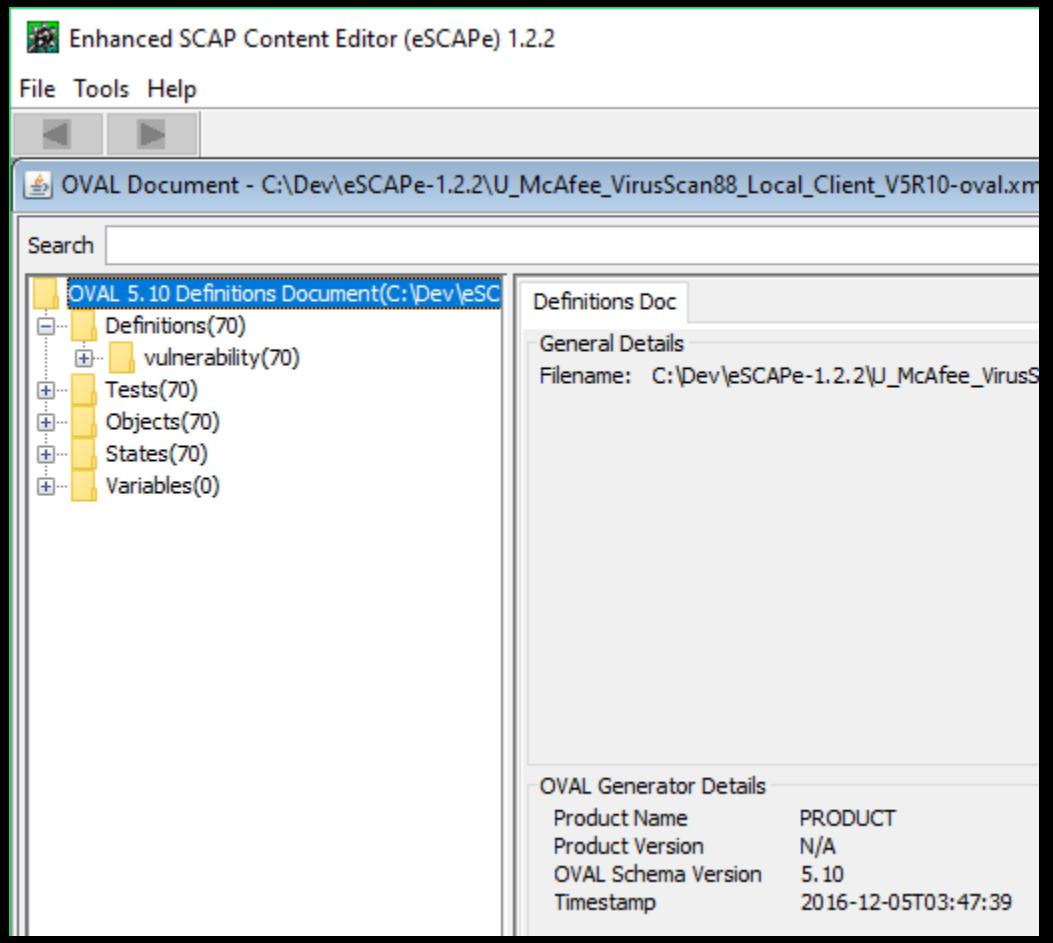
Why Challenges Exists\Persist?

- Lack of content/Content building is complex
  - No readily available tools to create content
  - Don't need to hear "all you need is notepad"

- eSCAPe 1.2.2
  - Created from a SIBR → is there a completed/up-to-date application?
  - Can make oval (must build intermediate tools to automate results)
  - No success in making SCAP Benchmarks from the generated OVALs

VMWARE released an updated product; same issues with OVAL to SCAP.

IVV&E Created this McAfee



UNCLASS

Advancing SCAP

- AF Mission Planning needs to be able to build content for unique applications
- The process of creating content should flow from STIG to SCAP
- Where STIG does not exist, we need to be able to create SCAP out of best practices and other derived policies
- Creating SCAP should be easy, intuitive, and easy to keep up-to-date as STIGs change.

UNCLASS

UNCLASS

Our Goal

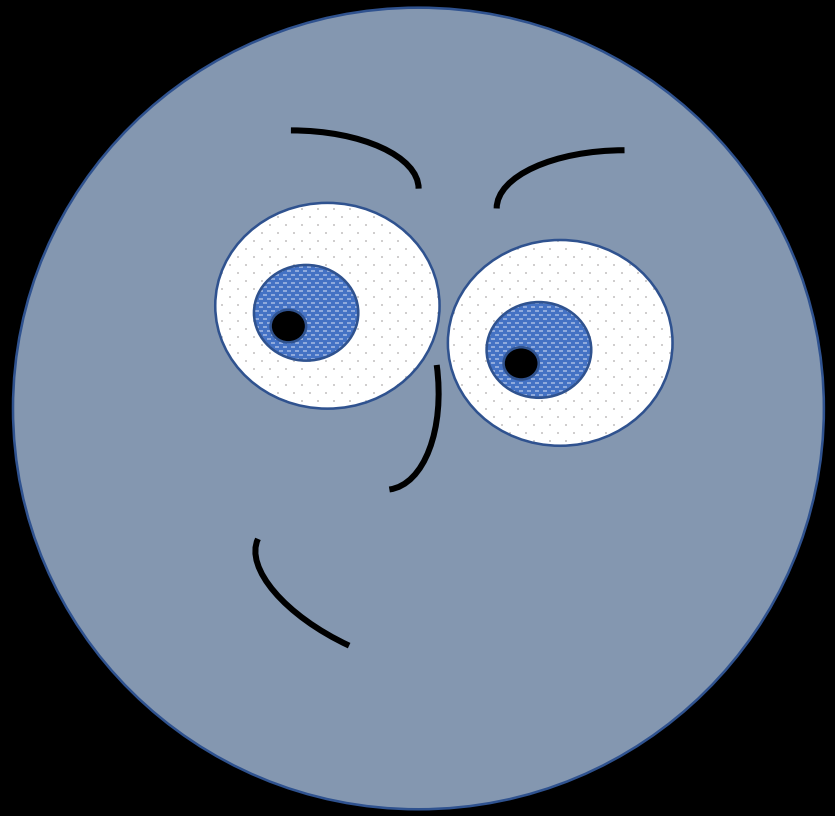
- Improve scanning/automation of compliance checking and ConMON

- Can we get there by:
  - Participating in the community effort to improve SCAP and SCAP availability?

UNCLASS

UNCLASS

?



UNCLASS