SteelCloud

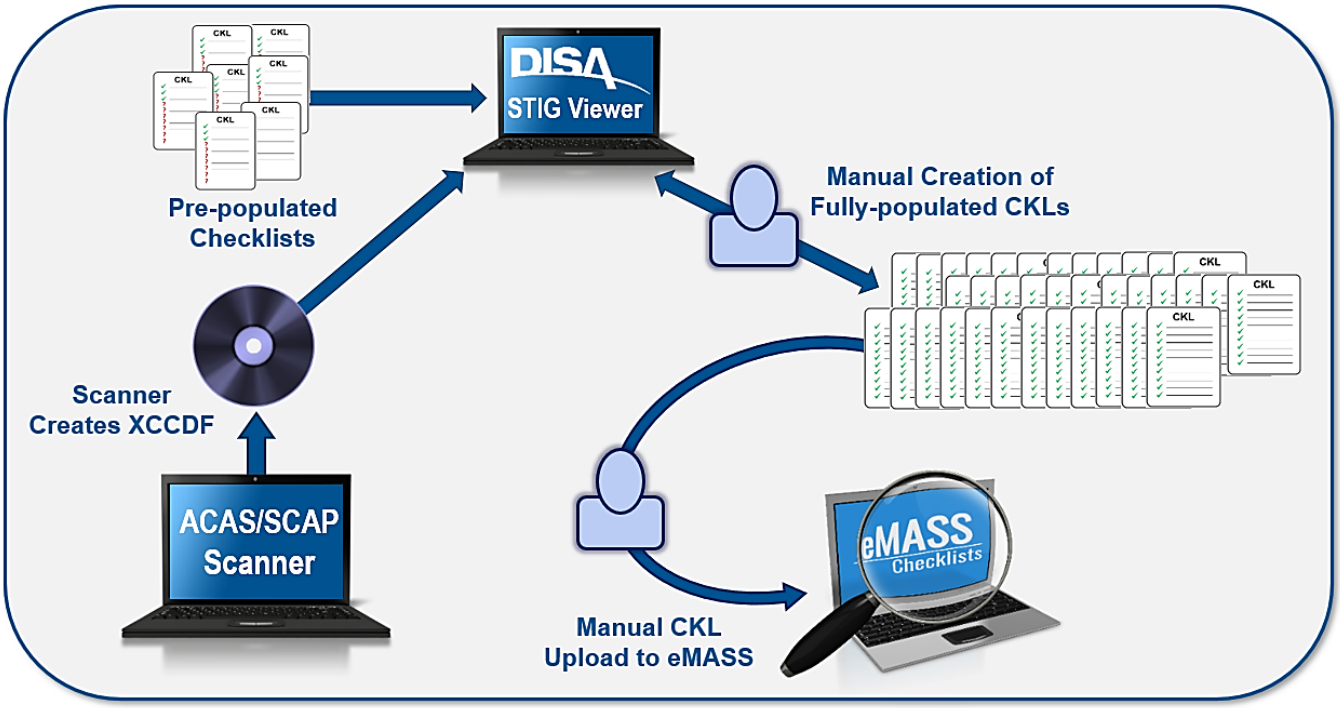
Automating Data for:

✓eMASS ✓Checklists ✓SIEM

eMASS Automation – The Search for a Solution to Unite and Automate Security Compliance Data

eMASS, or the Enterprise Mission Assurance Support Service, was developed by the DoD, in part, as a repository that unites technical/machine data generated from endpoint scans with the human/non-technical data documented by security/IA personnel. Traditionally the "uniting" process is accomplished by completing a STIG Viewer Checklist for each policy for each endpoint. So, as you can imagine, a 1,000 workstation environment could easily generate 10,000 individual checklist files or more.

January 2022

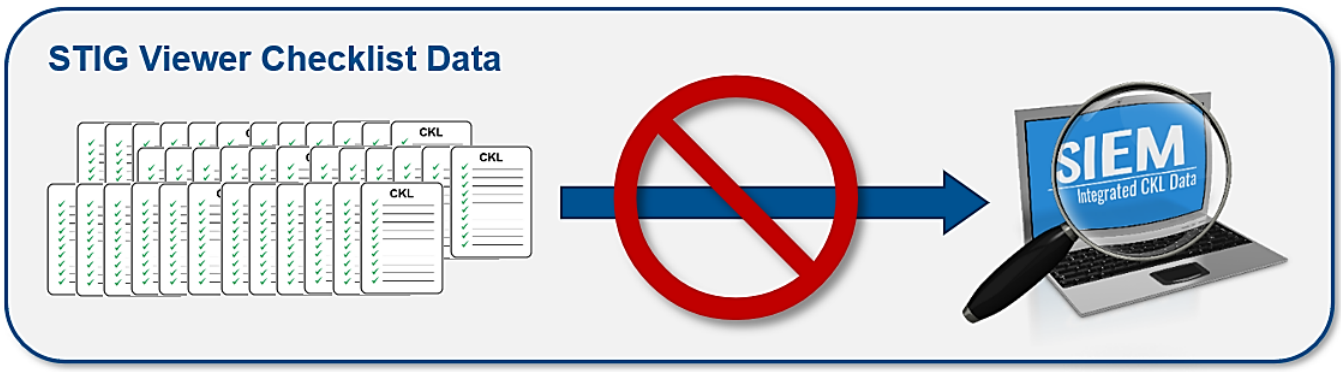


Navigating the Challenges of the STIG Viewer Checklist

These checklists are traditionally hand-created by pre-populating checklists for each policy with the appropriate non-technical data together with POAM/waiver information. Then security personnel combines the XCCDF output from the system scan (ACAS/SCAP) to create, name, and store the individual checklists for each endpoint. Once completed, the individual checklists that consolidate scan and human data are loaded into eMASS. Keeping eMASS current with the latest security information through this checklist creation and upload process is a challenge, both from a timeline and a personnel resource standpoint, since the process is inherently manual. As one can imagine, consistency, timeliness, and error handling are constant issues in such a human-dependent process.

Unifying eMASS and SIEM Data for a Unified View

eMASS currently supports more advanced ways to ingest information through API or ARF/ASR file interfaces. However, two challenges remain - how to access and integrate the human/non-technical data for eMASS and efficiently create fully-populated checklists required outside of eMASS. Beyond these two challenges, there is a great opportunity also to integrate the combined human/machine security compliance data to feed the organization's own dashboards. If this collective data feed could be combined, the organization's SIEM would represent the whole security compliance picture – not just the partial picture represented by only scan data.



Understanding It's TIME for Something New

Unfortunately, the processing architectures of scan-only products do not afford the DoD with any option to effectively address the requirement to combine security data and create fully-populated STIG Viewer Checklists. Therefore, a new solution will need to be invented . . .

Identifying Targets for AUTOMATION

There are four significant areas that automation can be applied to provide real advantage to the operationalization of cyber compliance within the DoD.

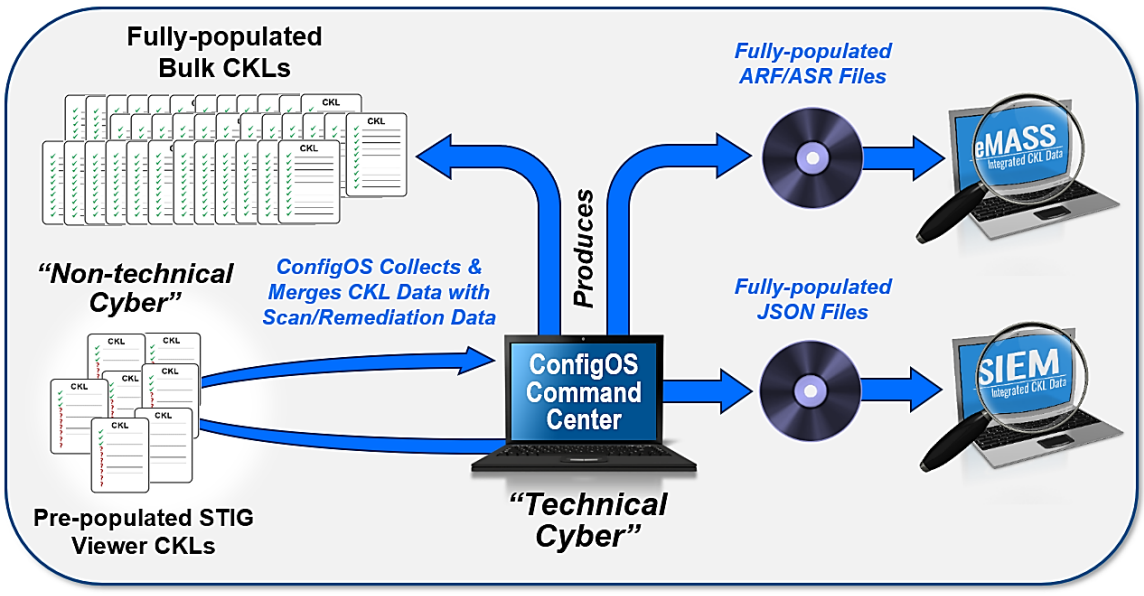
1. Automate and reduce the effort/errors in merging non-technical CKL data with machine-generated technical data.
2. Automate and simplify the production and input of compliance data into eMASS.
3. Automate and reduce the effort to produce, name, and store fully populated STIG Viewer Checklist in bulk (by the 1,000s).
4. Provide complete CKL data to SIEM data feeds so that complete compliance data is easily accessible through integrated enterprise dashboards.

Envisioning Something New – Integrating CKL, eMASS, and SIEM Data

In 2021, we participated in a SteelCloud-funded IRAD, sponsored out of one of the DoD component's CIO offices, to address the eMASS automation challenge. Because our existing STIG compliance software automates remediation, rather than just scanning, we started with a better foundation to address the four automation targets described above. From our IRAD that included multiple service components, SteelCloud developed and recently released a new version of its ConfigOS software that provides a simple integrated solution to address each of these automation challenges. We have provided this version of ConfigOS to all of our customers at no additional cost starting in December 2021.

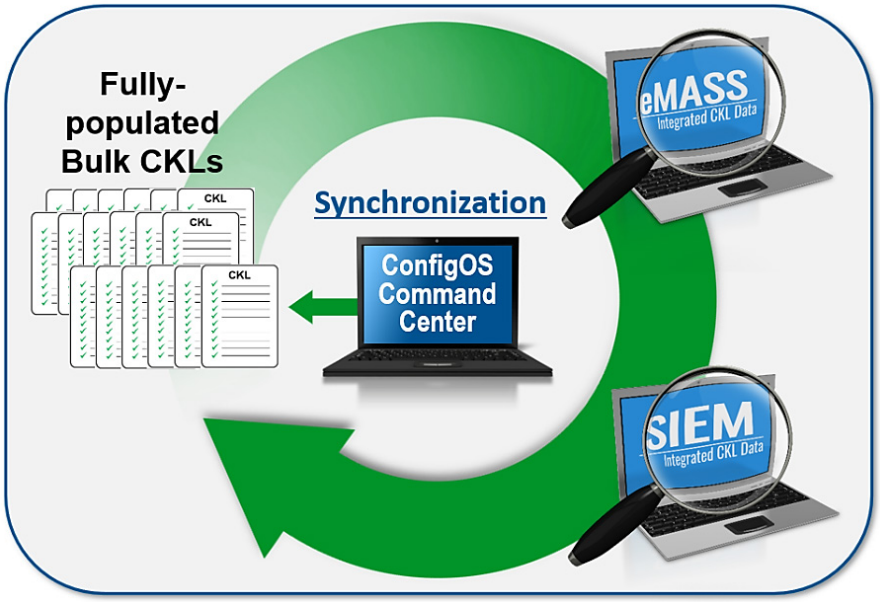
Discovering a Whole New Way to AUTOMATE DATA MERGING

We had already solved the problem of merging machine data with pre-populated STIG Viewer Checklist data several years ago. But it was a fairly manual one-at-a-time process. We enhanced ConfigOS to allow users to associate pre-populated checklists with policies for one or groups of computers. Therefore, at processing time, ConfigOS can merge the CKL and machine data to create bulk checklists, consolidated ARF/ASR eMASS files, and/or consolidated JSON files to populate our DashView Splunk dashboard or the customer's chosen SIEM.



To support real-world operations where non-production systems are excluded and/or information from individual systems need to be produced, ConfigOS allows the user to select individual/groups of computers to create bulk Checklists, eMASS files, and/or JSON output.

SteelCloud even enables the user the option of integrating CKL data into their normal production scan and remediation operations so that SIEM is always up to date with the complete security compliance picture.



SteelCloud's new software ensures the easy synchronization of massive numbers of checklist files, eMASS data, and SIEM dashboards – everything in synch, everything up to date.

SteelCloud
20110 Ashbrook Place
Ashburn, VA 20147
1.703.674.5500
info@steelcloud.com | **steelcloud.com**

www.steelcloud.com