Domination Thru Automation

"Deliver effective tools for continuous Cyber compliance and fuel the most efficient Cyber Professional imaginable"

Topics

- Contact Information
- Introduction
- A Little Math
- DTA Toolset Objectives
- Cyber Kill Cycle (CKC)
- Automated Compliance Evaluator (ACE)
- Continuous Cybersecurity Compliance Targeting System (C3TS)
- Documentation Automation Program (DAP)
- Monitoring Tools
- Future Capabilities

Contact Information

Frank Unpingco III

Phone: 801-888-4319

Email Address: Frank.Unpingco@dta.solutions

**SAM UEI**: M695D83HZQM5

SAM CAGE: TBD

Introduction

- Retired Air Force Master Sergeants and one DB Mad Scientist
  - Over 50 years as Cyber System Operators
  - Over 30 CCRIs
    - 2 Outstanding/Outstanding's
    - Passed a no notice CCRI
    - 6 DISA Best practices
- 5 years as a Hill Enterprise Data Center Engineer
  - 500 Microsoft servers
  - 700 Linux Servers

DTA Toolset Objectives

- Improve compliance assessment rates throughout the DoD enterprise

- Standardize the analyzation process throughout the DoD enterprise

- Improve the time it takes to identify High Value Targets (HVTs)

- Empower leadership at all levels

- Introduce a certification process

- Enhance cyberspace capabilities

- **Help organizations save time and manpower**

Cyber Kill Cycle (CKC)
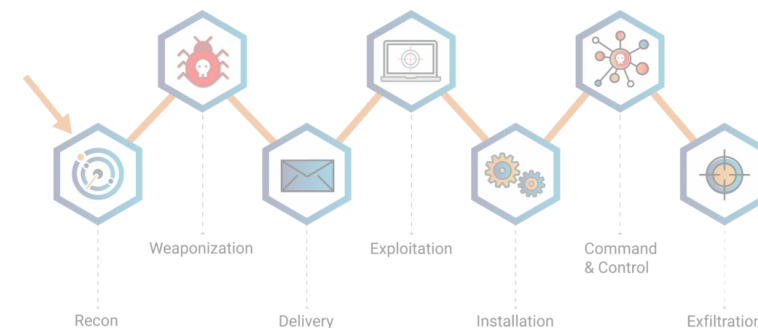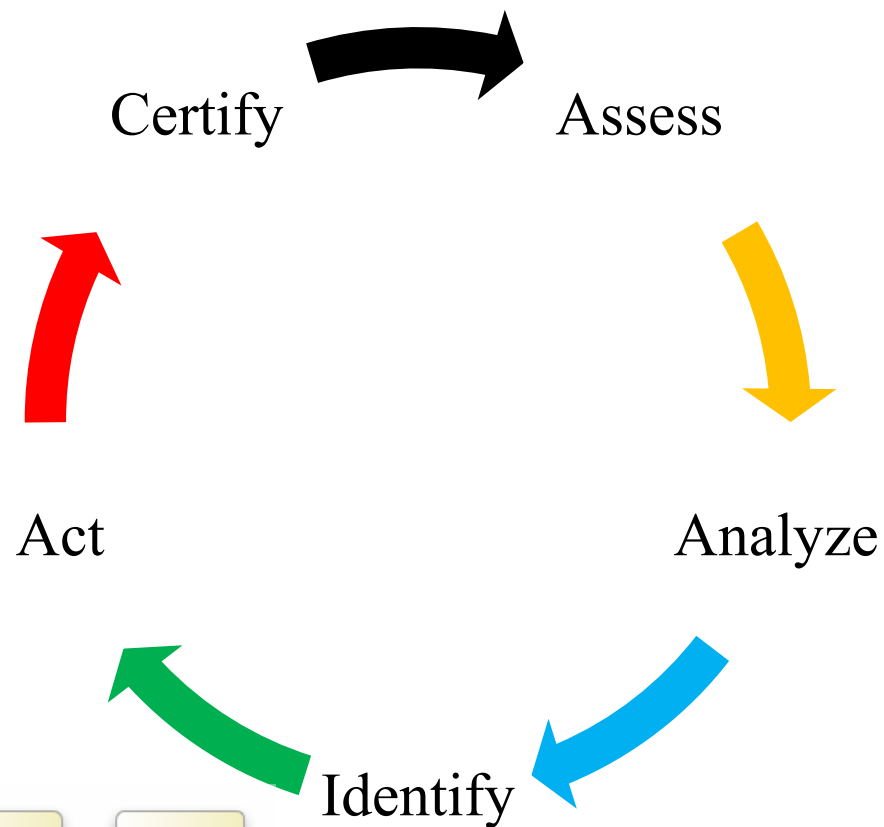
Certify → Assess → Analyze → Identify → Act → Certify

Automated Compliance Evaluator (ACE)

- Optimizes STIG Assessments
  - Endeavors to account for 100% of the DISA checklist

- Outputs checking and finding details for each check
  - Including GPO information

- Reduces the amount of manual intervention required
  - One person can run hundreds of thousands of checks

- Introduces Comparison 2 Baseline (C2B)
  - Analytics quickly provided and baseline drift
  - Incorporates into Configuration/Change Management programs
  - Facilitates risk management

- Locally empowered, remotely unified, centralized credibility
  - Multiple ways to execute the program
  - Artifacts stored locally and automatically uploaded to C3TS

- Useful Output
  - Required .ckl files
  - Logs for effective and efficient use
  - Immediate verification/reporting

Saves time and manpower

Continuous Cyber Compliance Targeting System (C3TS)

- Centralized CKC targeting system
  - Unified Intelligence
  - Incorporates CCRI scoring
    - Updates automatically as new results are introduced

- Cyber Readiness governance
  - Historical data
  - Vetting processes
  - Missing ACAS/STIG scan data

- Unit management
  - ACAS scores
  - STIG scores

Workforce Multiplier

C3TS cont'd

- PMO management
  - ACAS scores
  - STIG scores
- PoA&M lifecycle management
- Not only available to a few
- Integrates with existing DoD toolsets
  - Minimal/No data manipulation required for ingest
- Detailed system information
- Malleable framework ready for additional datasets

Documentation Automation Program (DAP)

- Documentation is the number one reason STIG reviews go bad
  - "Takes too much time"
  - "This is an unrealistic expectation"

- One template to rule them all!
  - Create accurate, DISA approved, ready to sign documentation on a "Per system" at scale

- Gather documentation when you need it
  - Be ready for a STIG review in minutes

Monitoring Tools

- Security Group Monitoring (SGM)
  - Selective email alerts
  - Baseline control
  - Based on Active Directory
- Software Certificate Monitoring (.pfx/.p12)
  - Identify existing files
  - Provides vetting process

Future Capabilities

- C3TS
  - Vendor collaboration
  - Role Based Access Control (RBAC)
  - Directive/TASKORD/NOTAM tracking
  - Multisite reporting
  - DAP Integration
  - Integrate Monitoring tools into C3TS
    - 8570 tracking
    - Security Groups
    - Service Account Monitoring
    - Software Certificate Monitoring (.pfx/.p12)
  - Predictive analysis for STIGs

Future Capabilities cont'd

- More ACE automation
  - Vendor collaboration
- More integration
  - CMMC, NIST Controls
- Comply 2 Connect
- Asset Monitoring
- Software License tracking
- Targeted Patching

Questions