1

Active Directory Auditing for CMMC Compliance

CHRISTOPHER KYRIACOU | JAMIE SUTTON | NATHAN CHONG | SAFEE GHAFOORI | DAVE FULLER

Alpha 4

Development Roles:

Team Leader | Lead Developer:

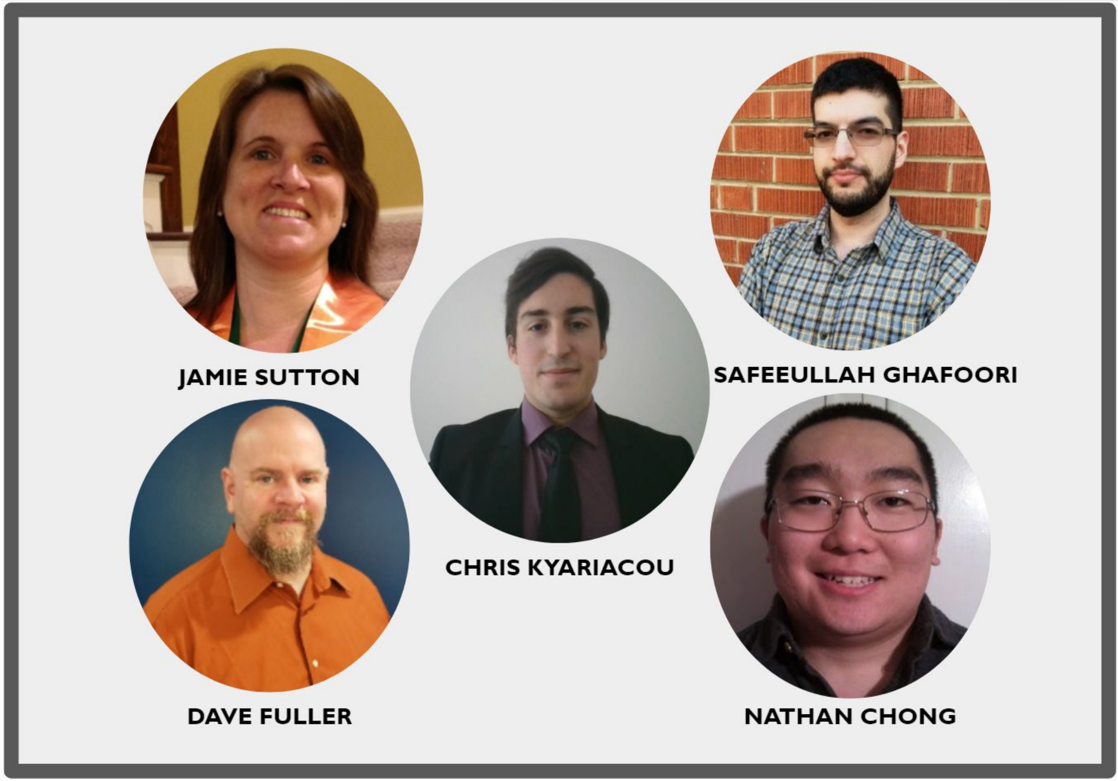
- Christopher Kyriacou

Deputy Team Leader | Developer:

- Safeeullah Ghafoori

Researcher | Developer | Documentation Specialist:

- Nathan Chong
- Jamie Sutton
- Dave Fuller



Project Presentation Roles

Role	Contributor(s)
Original Business Process	Nathan Chong
IT Solution	Christopher Kyriacou
Changed Business Process	Jamie Sutton
Solution Implementation	Safeeullah Ghafoori | Dave Fuller
Demonstration	Christopher Kyriacou

4

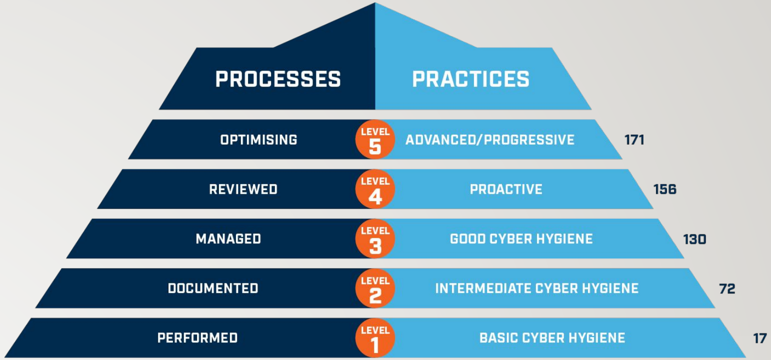
CMMC Compliance

Cybersecurity Maturity Model Compliance

Primary Goal: **Safeguard controlled unclassified information (CUI) across the DoD supply chain.**

CUI: **Any information or data created or possessed by the government or another entity on the government's behalf.**

CMMC Compliance Levels



PROCESSES		PRACTICES	
OPTIMISING	LEVEL 5	ADVANCED/PROGRESSIVE	171
REVIEWED	LEVEL 4	PROACTIVE	156
MANAGED	LEVEL 3	GOOD CYBER HYGIENE	130
DOCUMENTED	LEVEL 2	INTERMEDIATE CYBER HYGIENE	72
PERFORMED	LEVEL 1	BASIC CYBER HYGIENE	17

Level 1: Addressing FAR 52.204-21 cybersecurity principles.

Level 2: Build on CMMC Level 1 and addresses a little over half on NIST 800-171 controls.

Level 3: Build on CMMC Level 2 and addresses all NIST 800-171 controls.

Level 4 & 5: Build off CMMC Level 3 and include controls from a range of frameworks:

- **CERT RMM v1.2**
- **NIST SP 800-53**
- **NIST SP 800-172**
- **ISO 27002**
- **CIS CSC 7.1**
- **Unattributed "CMMC" references that are not attributed to existing frameworks.**

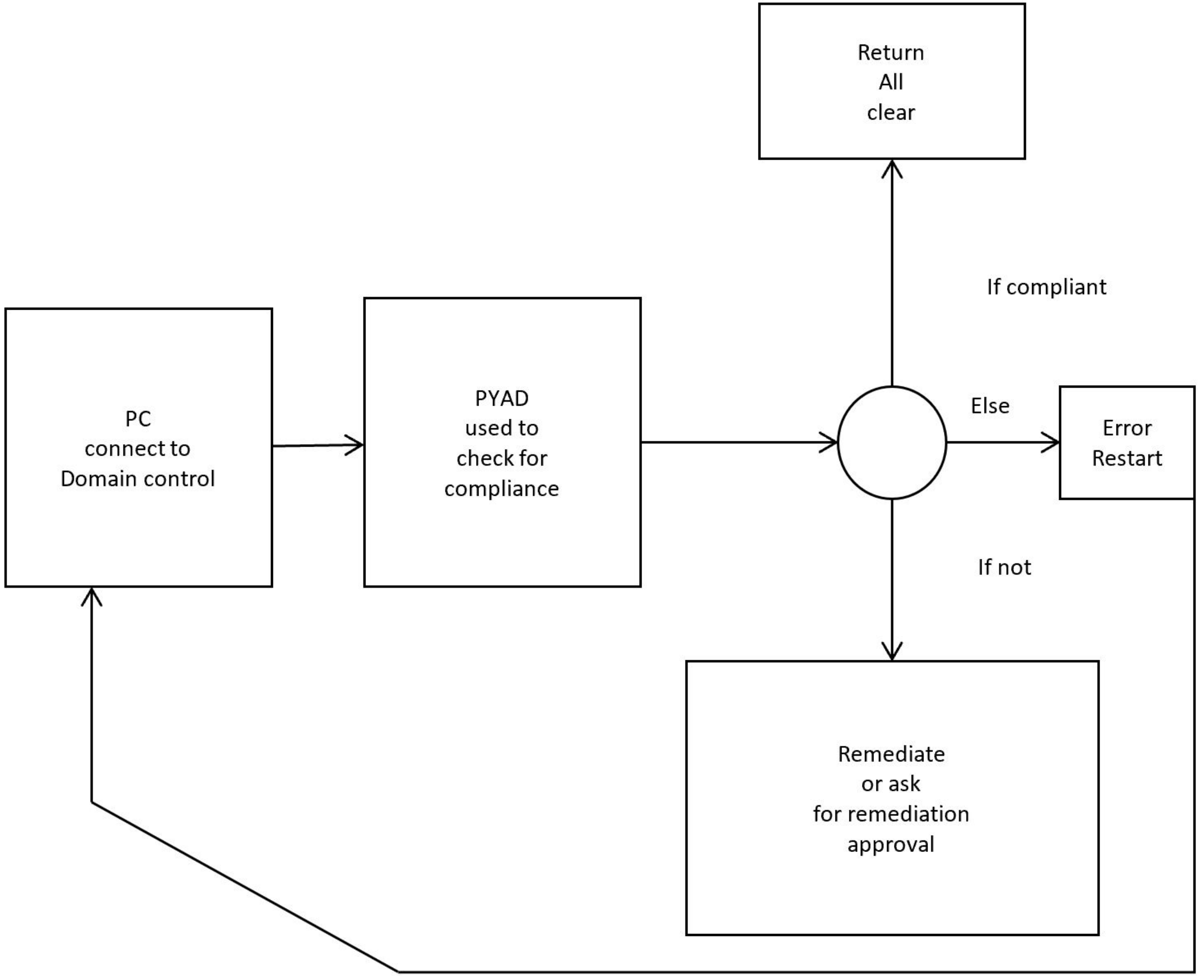
Auditing Active Directory for CMMC Level 3

Main Objective: Create an auditing system that can audit AD servers to ensure **CMMC Level 3 Compliance.**

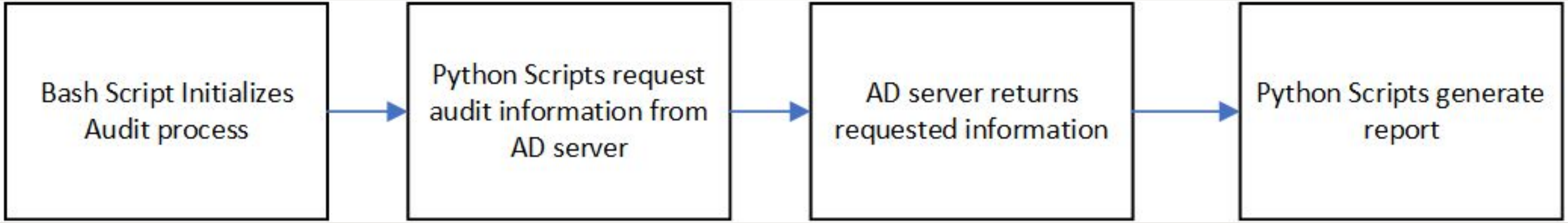
- **Must be open source and not rely on proprietary software**
- **Must be automatable (Using Ansible, etc.)**
- **Must be reliable & efficient**
- **Must be easily maintained**
- **Must be scalable (To include other functions in the future for Level 4 & 5)**

7 Desired Result

- pyad 0.6.0 to query for info
- Info passed to check if Remediation is necessary
- Take appropriate action based on findings or issues that occurred



Current Prototype



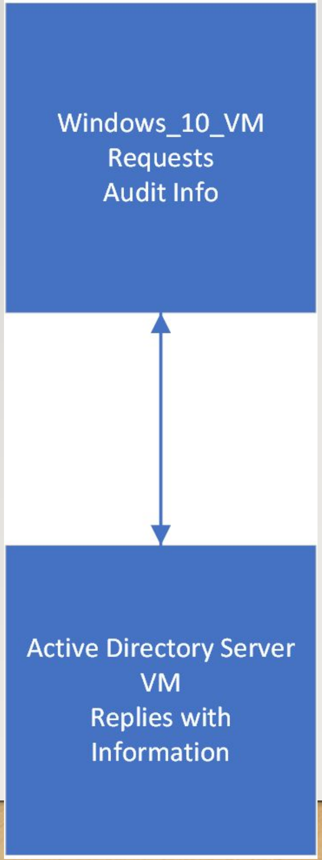
Bash Script Initializes Audit process

Python Scripts request audit information from AD server

AD server returns requested information

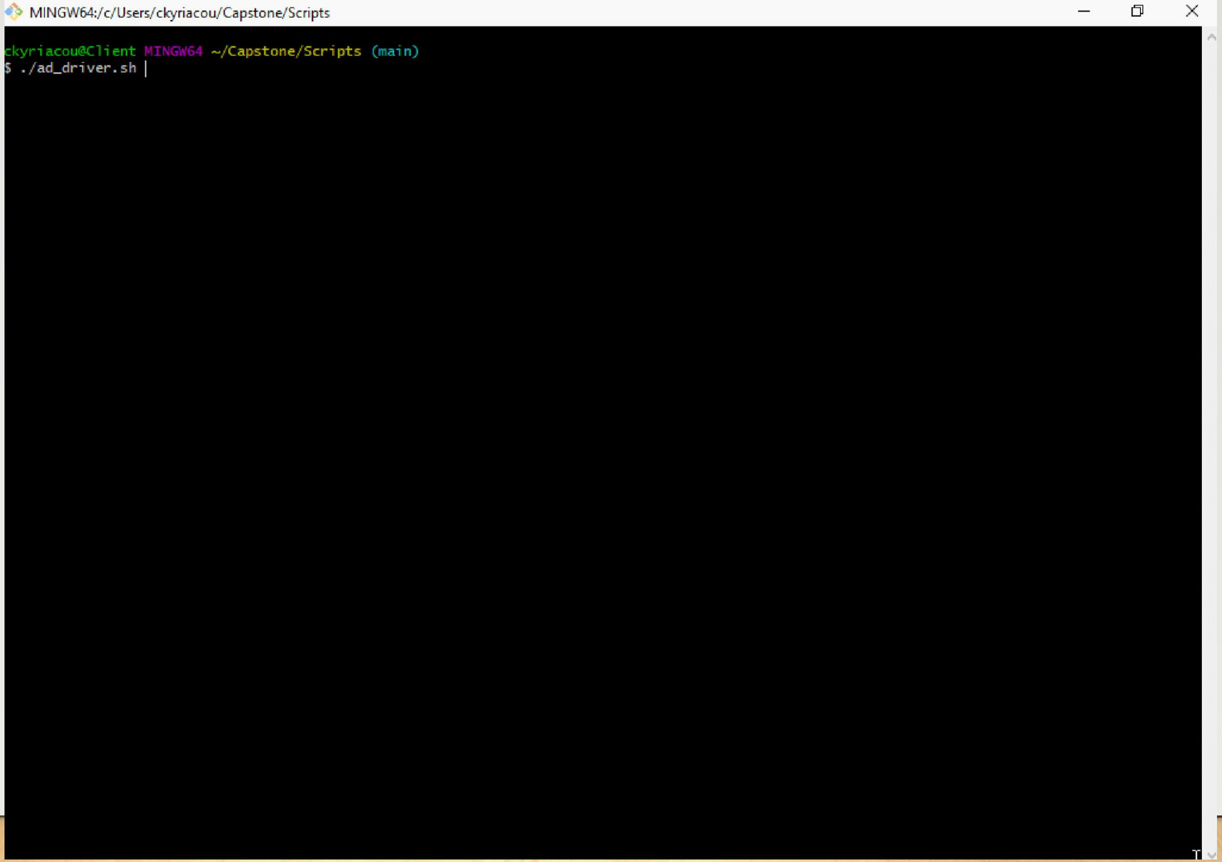
Python Scripts generate report

Prototype 1 - (Client/Server communication w/ Python)



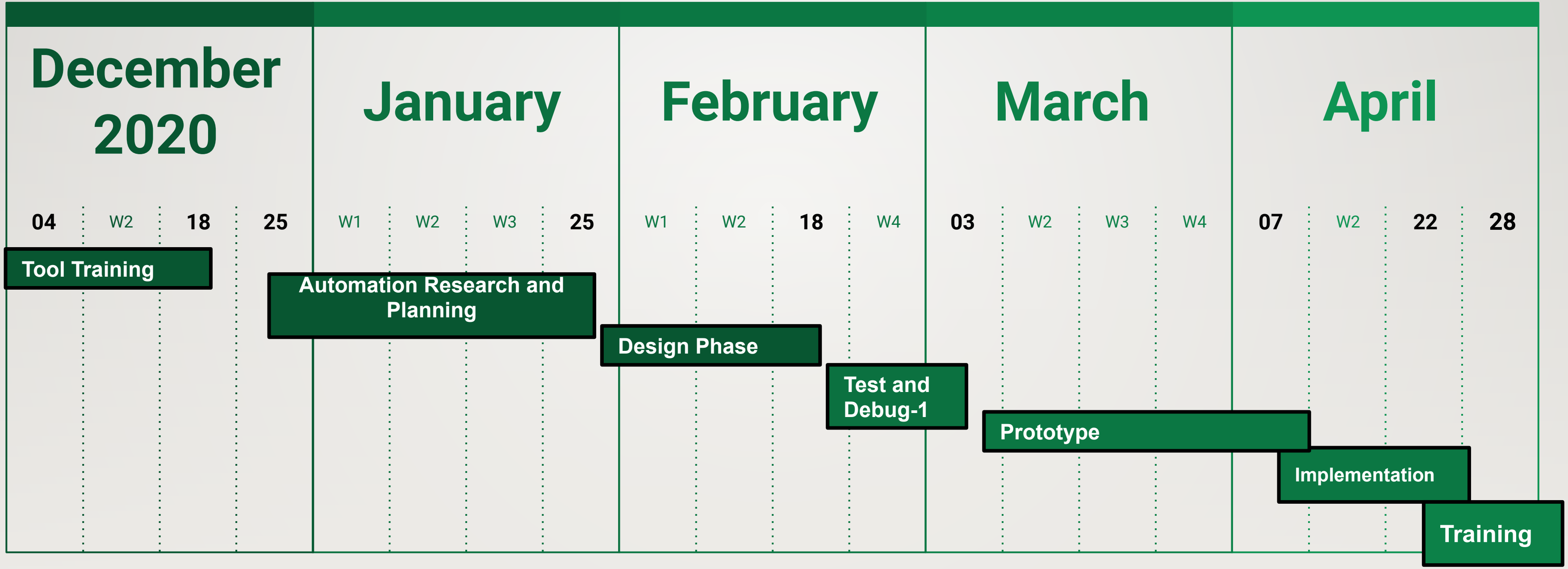
Windows_10_VM
Requests
Audit Info

Active Directory Server
VM
Replies with
Information



```
ckyriacou@Client MINGW64 ~/Capstone/Scripts (main)
$ ./ad_driver.sh
```

IT-493 Spring 2021 Project Schedule



11

Questions?