1

Active Directory Auditing for Cybersecurity Maturity Model Certification (CMMC) Compliance

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

2

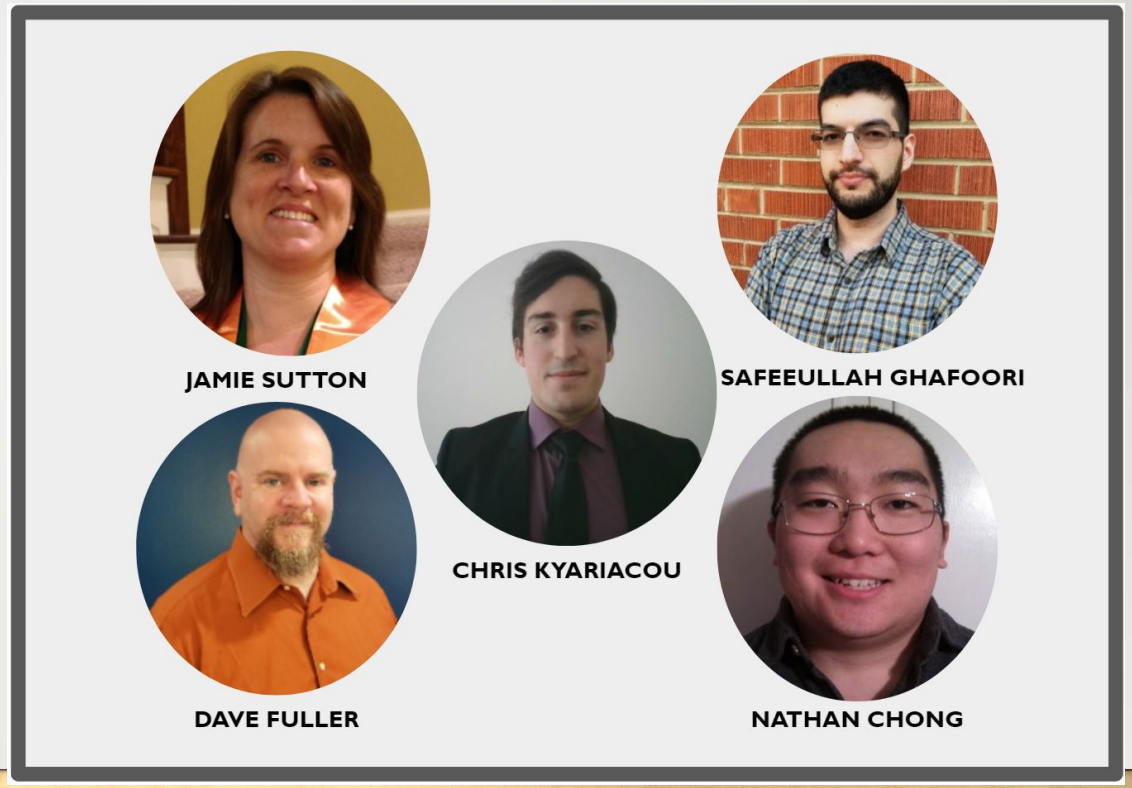
Alpha 4

Roles:

Team Leader | Lead Developer:
- Christopher Kyriacou

Deputy Team Leader | Developer:
- Safeeullah Ghafoori

Researcher | Developer | Documentation Specialist:
- Nathan Chong
- Jamie Sutton
- Dave Fuller



3

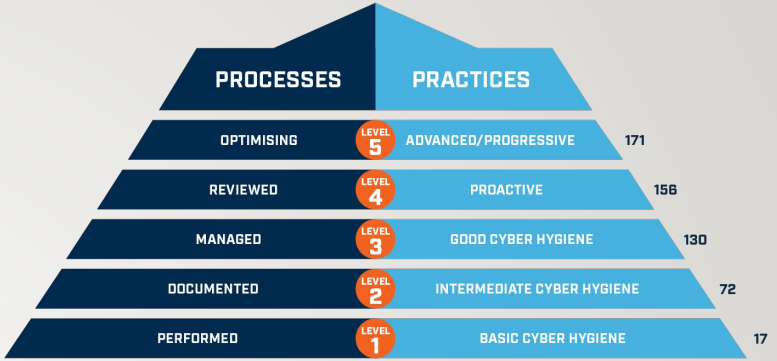
CMMC Compliance

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



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.**

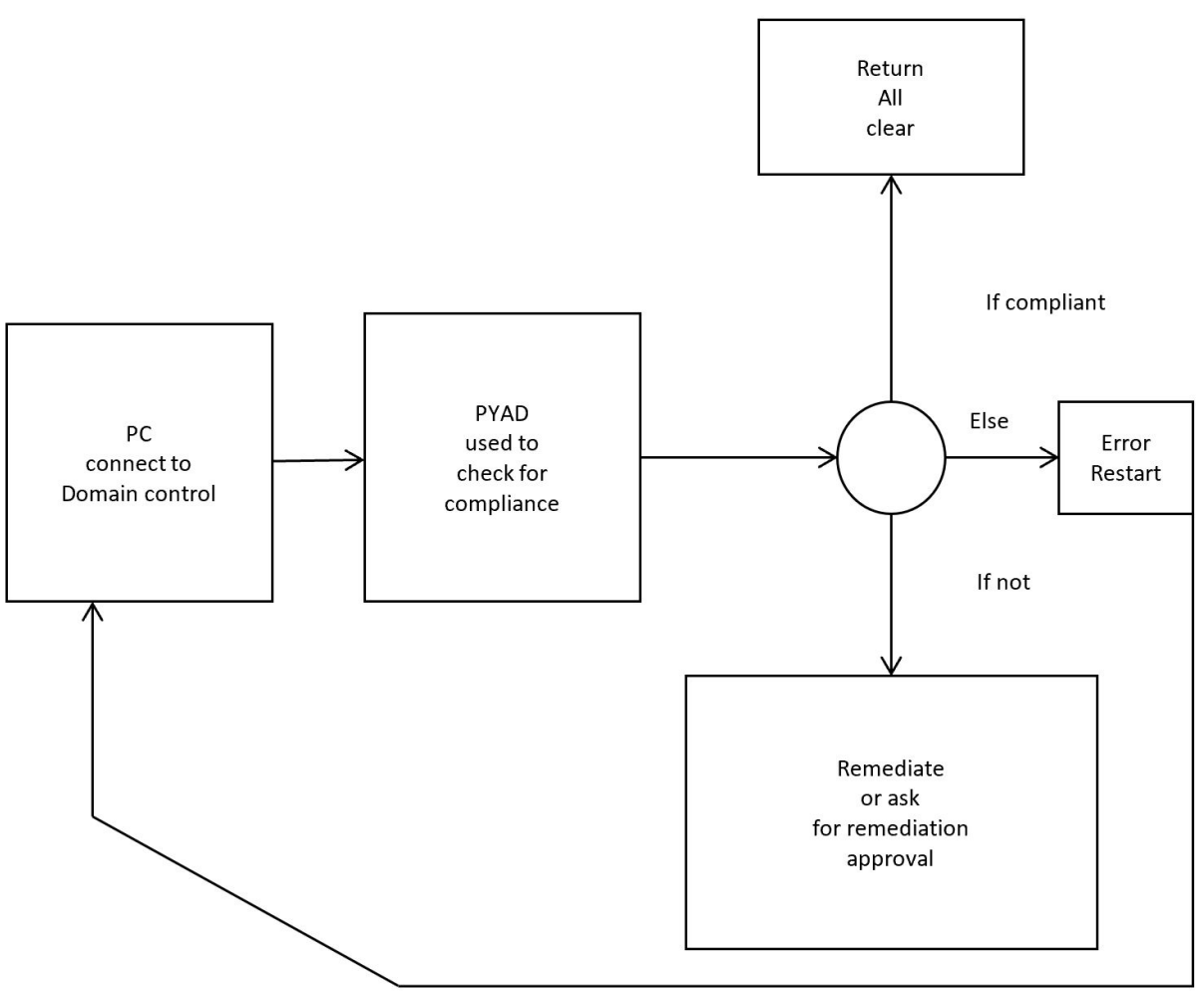
5 Auditing Active Directory for CMMC Level 3

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)**

6 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

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

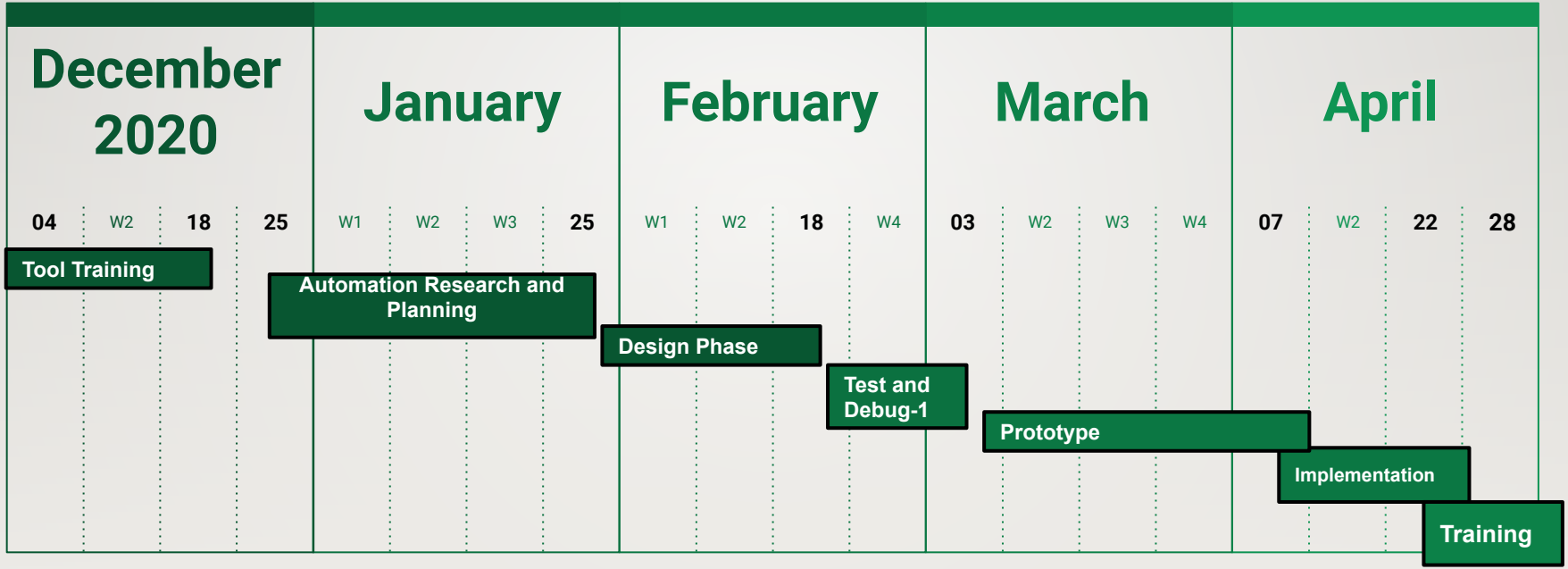
Windows_10_VM
Requests
Audit Info

Active Directory Server
VM
Replies with
Information

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


Unused Users:
Administrator Days Unused: 12
Christopher Kyriacou Days Unused: 12
Unused User Count: 2

Unused Computers:
CLIENT Days Unused: 19
DESKTOP-A67GOP2 Days Unused: 20
Unused Computer Count: 2

Users with passwords unchanged past the day limit:
Administrator, Christopher Kyriacou, Guest, krbtgt,

Admin Report:
Domain Admins: CN=Christopher Kyriacou,CN=Users,DC=KTG,DC=local,CN=Administrator
,CN=Users,DC=KTG,DC=local,
Enterprise Admins: CN=Administrator,CN=Users,DC=KTG,DC=local,
Key Admins:
Schema Admins: CN=Administrator,CN=Users,DC=KTG,DC=local,


Service Accounts without manager set:
Updates,

Port Status:

KTG.local -> IPv4: 192.168.1.101

53 is open
Port: 53 => service name: domain

80 is open
Port: 80 => service name: http

88 is open
Port: 88 => service name: kerberos

135 is open
Port: 135 => service name: epmap

139 is open
Port: 139 => service name: netbios-ssn

389 is open
Port: 389 => service name: ldap
```

IT-493 Spring 2021 Project Schedule

9



10

Questions?