**Edumanichukwu Nwachukwu**

**CYBR 445 - Advanced Incident Detection and Response  
Module 6 Lab – MITRE Framework and Tools**

**List the generated Top 10 Techniques Below**

**T1059 – Command and Scripting Interpreter**

**T1047 – Windows Management Instrumentation**

**T1053 – Scheduled Task/Job**

**T1574 - Hijack Execution Flow**

**T1543 – Create or Modify System Process**

**T1562 – Impair Defenses**

**T1055 – Process Injection**

**T1036 – Masquerading**

**T1021 – Remote Services**

**T1003 – OS Credential Dumping**

**List the MITRE 15 Most Observed Techniques from the Report Below**

**1. Scheduled Task/Job [T1053]**

**2. Command and Scripting Interpreter [T1059]**

**3. Hijack Execution Flow [T1574]**

**4. Proxy [T1090]**

**5. Masquerading [T1036]**

**6. System Binary/Proxy Execution [T1218]**

**7. Create or Modify System Process [T1543]**

**8. Process Injection [T1055]**

**9. Impair Defenses [T1562]**

**10. Obfuscated Files or Information [T1027]**

**11. Remote Services[T1021]**

**12. Non-Application Layer Protocol [T1095]**

**13. Windows Management Instrumentation [T1047]**

**14. Modify Registry [T1112]**

**15. Ingress Tool Transfer [T1105]**

**DeTT&CK YAML File Results**

version: 1.1

file\_type: data-source-administration

name: Bellevue Bank and Trust DeTT&CK Analysis

domain: enterprise-attack

systems:

- applicable\_to: 'Bellevue Bank and Trust Systems '

platform:

- Windows

- Linux

- macOS

- Office 365

- Network

- SaaS

data\_sources:

- data\_source\_name: Active Directory Credential Request

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Active Directory Object Access

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 5

timeliness: 3

consistency: 5

retention: 3

- data\_source\_name: Active Directory Object Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 5

timeliness: 3

consistency: 5

retention: 3

- data\_source\_name: Active Directory Object Deletion

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 5

timeliness: 3

consistency: 5

retention: 3

- data\_source\_name: Active Directory Object Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 5

timeliness: 3

consistency: 5

retention: 3

- data\_source\_name: Application Log Content

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 2

data\_field\_completeness: 2

timeliness: 2

consistency: 2

retention: 3

- data\_source\_name: Command Execution

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Drive Access

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Drive Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Drive Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Driver Load

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Driver Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: File Access

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: File Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 4

retention: 5

- data\_source\_name: File Deletion

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: File Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: File Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Firewall Disable

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Firewall Enumeration

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 3

timeliness: 3

consistency: 5

retention: 3

- data\_source\_name: Firewall Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 3

timeliness: 3

consistency: 5

retention: 3

- data\_source\_name: Firewall Rule Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Group Enumeration

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Group Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Group Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Host Status

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Logon Session Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Logon Session Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Module Load

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Named Pipe Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Network Connection Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Network Share Access

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Network Traffic Content

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 2

data\_field\_completeness: 2

timeliness: 2

consistency: 3

retention: 1

- data\_source\_name: Network Traffic Flow

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: OS API Execution

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Process Access

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Process Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 4

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Process Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Process Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Process Termination

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Scheduled Job Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Scheduled Job Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Scheduled Job Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Script Execution

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Service Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Service Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: false

comment: ''

data\_quality:

device\_completeness: 0

data\_field\_completeness: 0

timeliness: 0

consistency: 0

retention: 0

- data\_source\_name: User Account Authentication

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: User Account Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: User Account Deletion

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: User Account Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: User Account Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Volume Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Volume Deletion

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Volume Enumeration

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Volume Metadata

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Volume Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: WMI Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Web Credential Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 2

data\_field\_completeness: 2

timeliness: 2

consistency: 3

retention: 3

- data\_source\_name: Web Credential Usage

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 3

data\_field\_completeness: 3

timeliness: 3

consistency: 3

retention: 3

- data\_source\_name: Windows Registry Key Access

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Windows Registry Key Creation

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Windows Registry Key Deletion

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Windows Registry Key Modification

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

- data\_source\_name: Web [DeTT&CT data source]

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 2

data\_field\_completeness: 2

timeliness: 2

consistency: 3

retention: 3

- data\_source\_name: DHCP [DeTT&CT data source]

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Internal DNS [DeTT&CT data source]

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 3

- data\_source\_name: Email [DeTT&CT data source]

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 4

data\_field\_completeness: 5

timeliness: 4

consistency: 5

retention: 3

- data\_source\_name: Kernel Module Load

data\_source:

- applicable\_to:

- all

date\_registered: null

date\_connected: null

products: []

available\_for\_data\_analytics: true

comment: ''

data\_quality:

device\_completeness: 5

data\_field\_completeness: 5

timeliness: 5

consistency: 5

retention: 5

notes: Bellevue Bank and Trust DeTT&CK Analysis

**List any techniques that aren’t solid green below:**

**White: Active scanning, gather victim host information, Garda victim identity information, gather victim network information, gather victim Org Information, search open technical databases, acquire access, acquire infrastructure, compromise accounts, compromise infrastructure, develop capabilities, establish accounts, obtain capabilities, stage capabilities, boot or logon auto start execution, boot or logon initialization scripts, compromise client software binary, event triggered execution, direct volume access, execution guardrails, hide artifacts, indirect command execution, Plist File modification come on reflective code loading, rogue domain controller, system script proxy execution, system script proxy execution, trusted developer utilities proxy execution, weakened encryption, input capture, cloud service discovery, device driver discovery, group policy discovery, system location discovery, internal spearfishing, audio capture, data from network shared drive, automated exfiltration, account access removal, data manipulation.**

**Light Green: N/A**

**Yellow: Search closed sources, search victim owned websites, shared modules, debugger evasion, deobfuscate/decode files of information, indicator removal, modify registry, root kit, visualization/sandbox evasion, XSL Script Processing, File and Directory Discovery, peripheral device discovery, permission groups discovery, process discovery, query registry, remote system discovery, software discovery, system information discovery, system network configuration discovery, system network connections discovery, system owner/user discovery, system service discovery, system time discovery, automated collection, clipboard data, data staged, screen capture, video capture, data encrypted for impact, resource hijacking, system shutdown/reboot.**

**Orange: N/A**

**Red: N/A**