Configuration Manual

MSc Research Project
Master of Science In Cyber Security Information

Forename Surname
Student ID: x23158239

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Marcus Winston Johnson

Student ID: x23158239

Programme: … Master of Science In Cyber Security Information…… **Year:** ……2023/2024……..

Module: …… MSc Research Practicum/Internship part2…….

Lecturer: …… Rohit Verma…….

Submission Due Date: ……12 August,2024…….

Project Title: …… Testing The Efficacy of Windows Defender Endpoint Security Control Using BAS Technology

Word Count: …… **Page Count:** …….

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……

Date: ……11 August, 2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Marcus Winston Johnson
Student ID: x23158239

AttackIQ Flex Getting Started Guide

AttackIQ Flex is an automated Breach and Attack Simulation (BAS) technology which provides a secure and straightforward method for evaluating your security measures through simulated attacks. Select from our extensive library of pre-configured tests and receive your results within minutes. By using breach and attack simulation, you are able to continuously assess all of your security technology sensors, including event logs, network security controls, and the SIEM, to ensure that every alert is triggering correctly. The net result is a comprehensive understanding of your entire security pipeline performance.
Safety First: Flex prioritizes your safety by offering secure simulations of cyber-attack tactics, techniques, and procedures.

How it Works: Each test comes as a ready-to-run executable, packed with all the essential components. For instance, specific campaign tests are designed to mirror the top methods commonly used by attackers.

Where to Run It: Execute tests on the endpoints you wish to evaluate. Afterward, bring the results back to Flex for comprehensive analysis.

Starting Out: Kick off your experience with baseline assessments, an uncomplicated approach to gauging your core security controls.

1 Creating Account

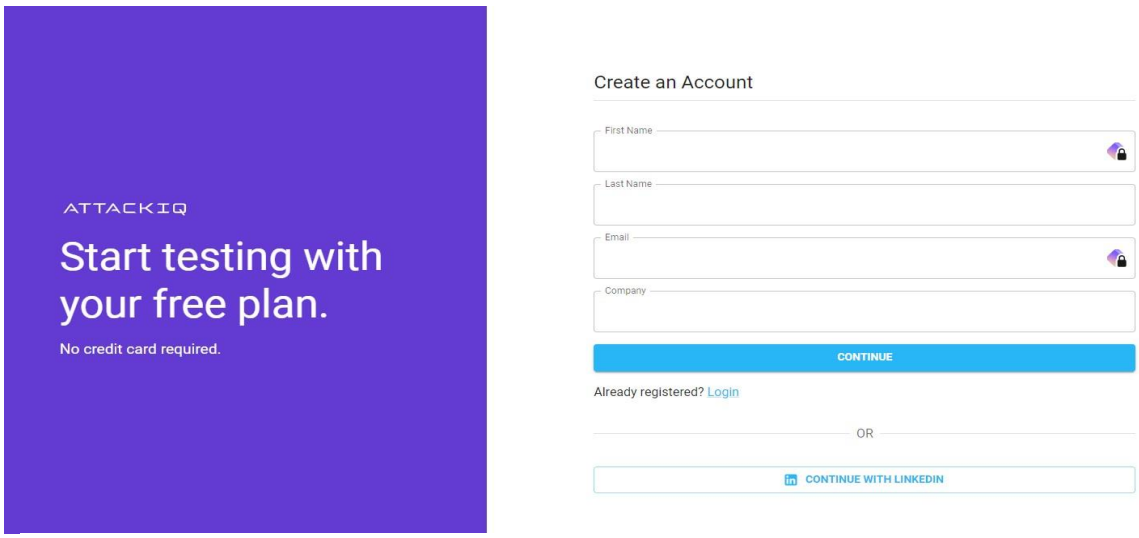

Fig. 1. ***https://portal.attackiqready.com/flex-signup***

Here you have the option to register for a new account or login with a LinkedIn account or use the *Try it for free* link

Complete the registration process and your account will be verified shortly with a link to login.

In your email you will receive a message ‘’ You have been invited to the AttackIQ Security Validation Platform’’

With 8 free credits to begin your assignment.

2 Login

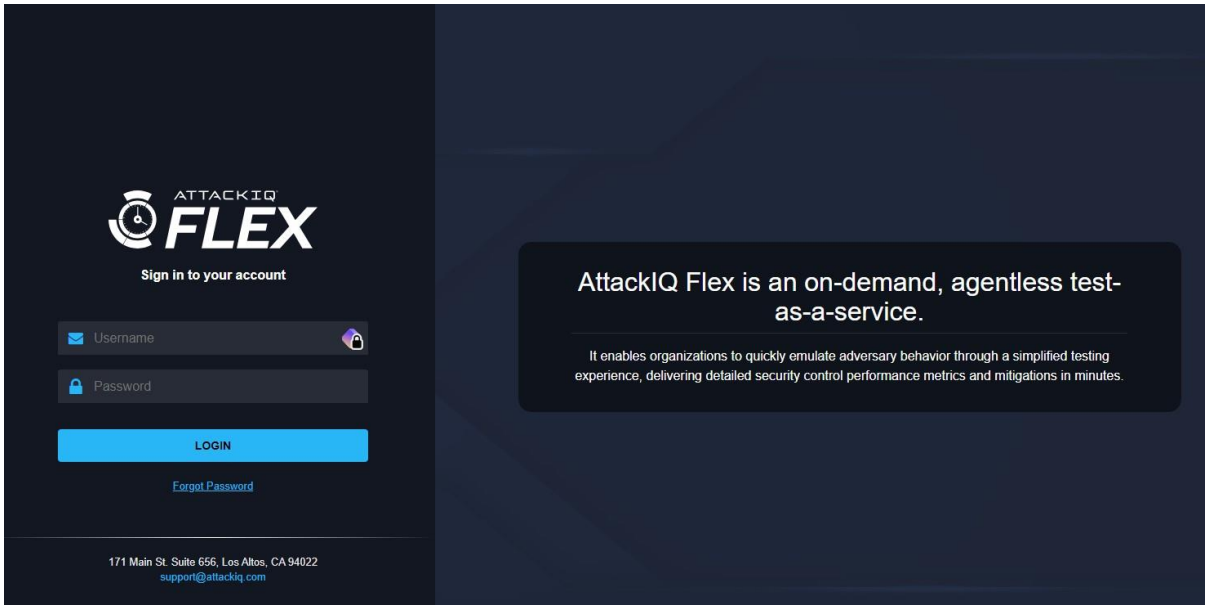

Figure 2. login screen

Login into your account and will be presented with the Home Dashboard screen.

3 Home Dashboard

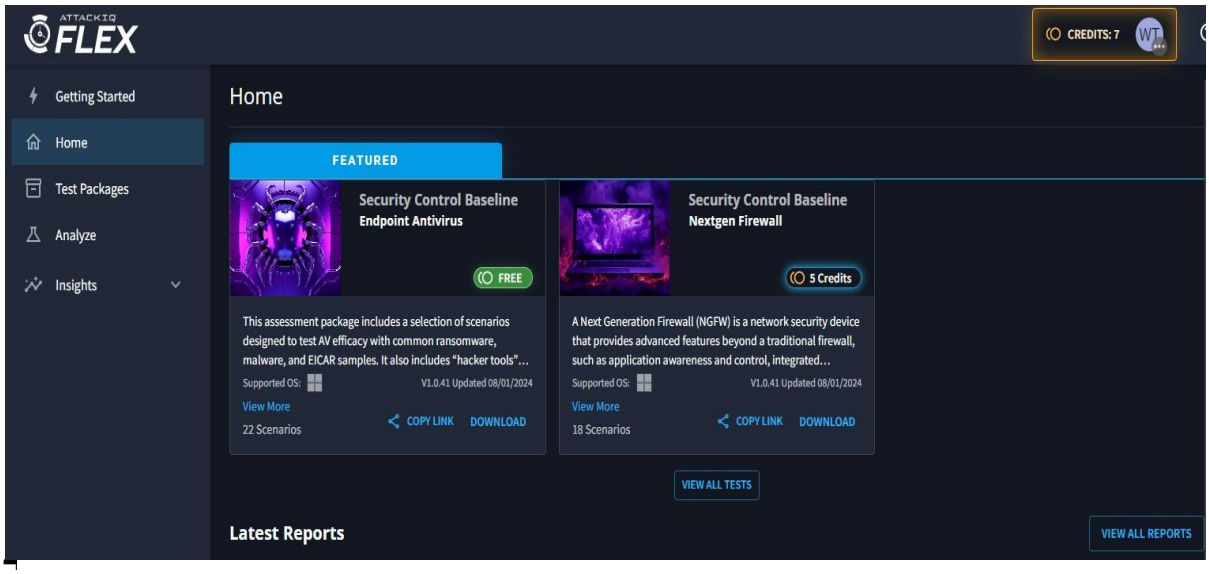

Figure 3. Home Dashboard screen

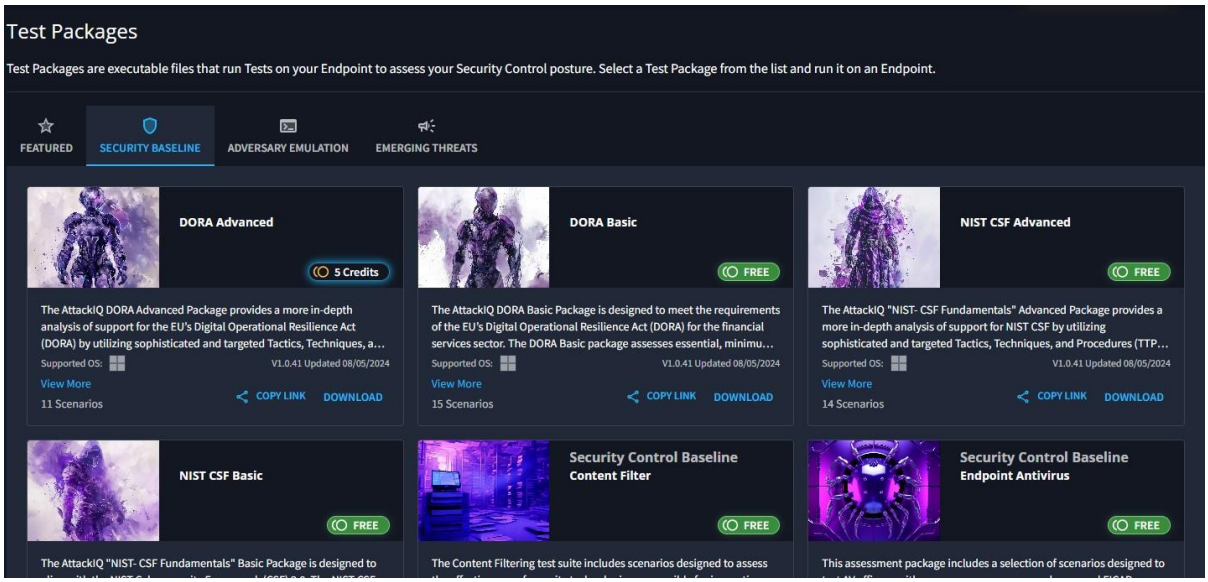

Figure 4. Library of Test Packages

This is the library where you find test packages for all scenarios that can be emulated in any given environment based on your red/blue team engagements.
New test packages are added regularly to test and validate your security controls to know how well they are performing against new and emerging threats.
Users can download a Flex test package and upload and execute on the endpoint of any supported OS.

5 Emulation Package Details

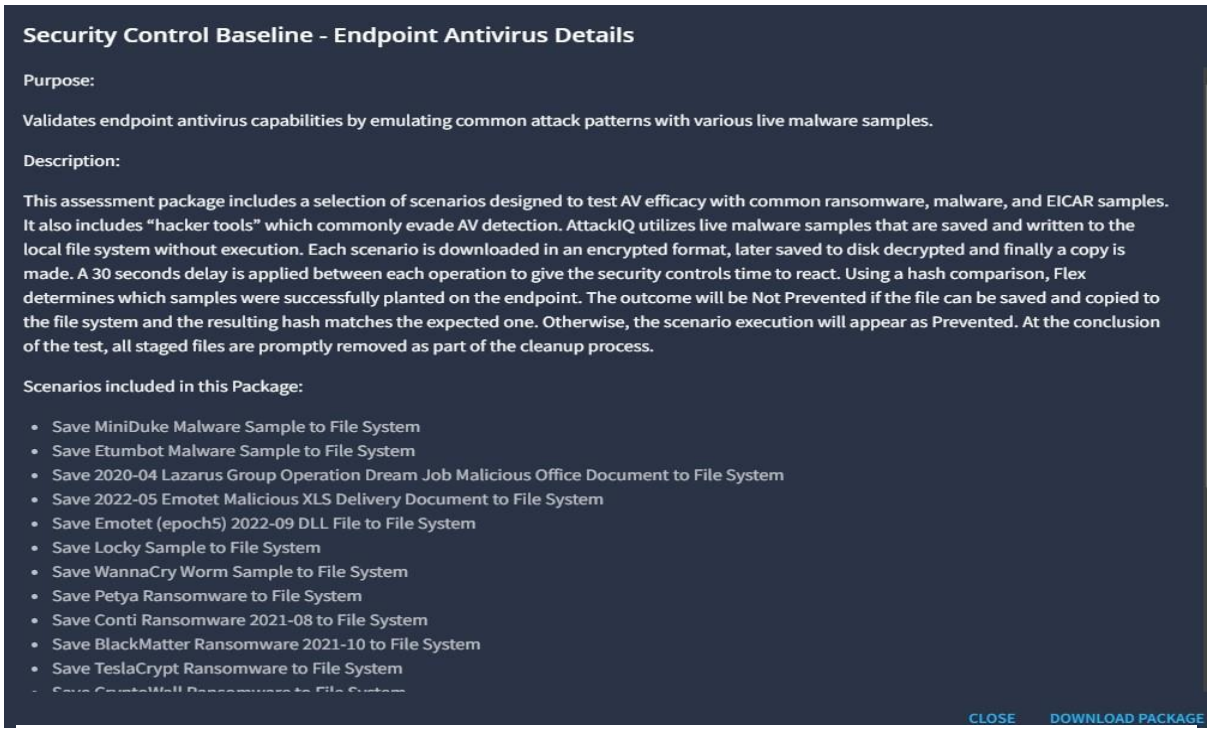

Figure 5. Endpoint Antivirus Package Details

Security Control Baseline - Content Filter Details

Purpose:

Validates network inspection capabilities including the downloading of malicious content from internal networks.

Description:

The Content Filtering test suite includes scenarios designed to assess the effectiveness of security technologies responsible for inspecting web-based traffic originating from the internal network. While some Next-Generation Firewalls (NGFWs) include this capability, it is often provided by a separate web proxy or web content filter. In the assessment scenarios, content will be utilized to attempt the download of malware samples from hosted infrastructure. If successful, they are immediately discarded, without being saved or written to the local file system. This suite of tests validates network inspection capabilities and does not test category blocks for inappropriate content.

Scenarios included in this Package:

- Download CryptoLocker Ransomware to Memory
- Download Locky Sample to Memory
- Download Mischa Ransomware to Memory
- Download WannaCry Worm Sample to Memory
- Download Powerware Ransomware to Memory
- Download KeRanger Ransomware to Memory
- Download Xorist Ransomware to Memory
- Download SynoLocker Ransomware to Memory
- Download ODCODC Ransomware to Memory
- Download Linux Encoder Ransomware to Memory
- Download Rakhni Ransomware to Memory
- Download SamSam Sample to Memory
- Download SNSLock Ransomware to Memory

Figure 6. Content Filter Package Details

Security Control Baseline - Endpoint Antivirus Details

Purpose:

Validates endpoint antivirus capabilities by emulating common attack patterns with various live malware samples.

Description:

This assessment package includes a selection of scenarios designed to test AV efficacy with common ransomware, malware, and EICAR samples. It also includes "hacker tools" which commonly evade AV detection. AttackIQ utilizes live malware samples that are saved and written to the local file system without execution. Each scenario is downloaded in an encrypted format, later saved to disk decrypted and finally a copy is made. A 30 seconds delay is applied between each operation to give the security controls time to react. Using a hash comparison, Flex determines which samples were successfully planted on the endpoint. The outcome will be Not Prevented if the file can be saved and copied to the file system and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented. At the conclusion of the test, all staged files are promptly removed as part of the cleanup process.

Scenarios included in this Package:

- Save MiniDuke Malware Sample to File System
- Save Etumbot Malware Sample to File System
- Save 2020-04 Lazarus Group Operation Dream Job Malicious Office Document to File System
- Save 2022-05 Emotet Malicious XLS Delivery Document to File System
- Save Emotet (epoch5) 2022-09 DLL File to File System
- Save Locky Sample to File System
- Save WannaCry Worm Sample to File System
- Save Petya Ransomware to File System
- Save Conti Ransomware 2021-08 to File System
- Save BlackMatter Ransomware 2021-10 to File System

Figure 7. Endpoint Antivirus Details

These emulation packages **Fig.5**, **Fig.6**, and **Fig.7** are downloaded from the AttackIQ Flex Library in a **.exe** file format which is then executed in the endpoint environment to test specific capabilities as outlined in the package details.

These packages utilize live malware samples that are saved and written to the local file system without execution. Using a hash comparison, Flex determines which samples were successfully planted on the endpoint. At the conclusion of the test, all staged files are promptly removed as part of the cleanup process.

6 Emulation in Virtual Environment

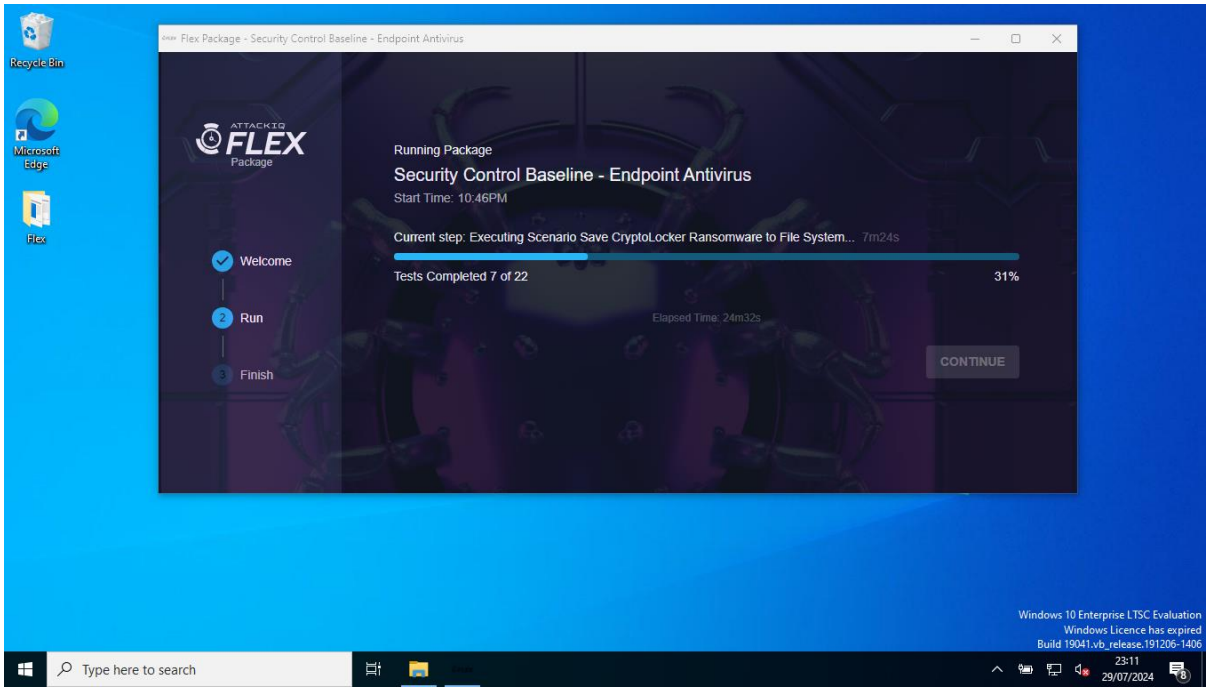

Figure 8. Emulation of the endpoint antivirus package on win10 (online mode)

Aligned with the MITRE ATT&CK framework, threat actors' behaviours (TTPs) are emulated to test defenses.

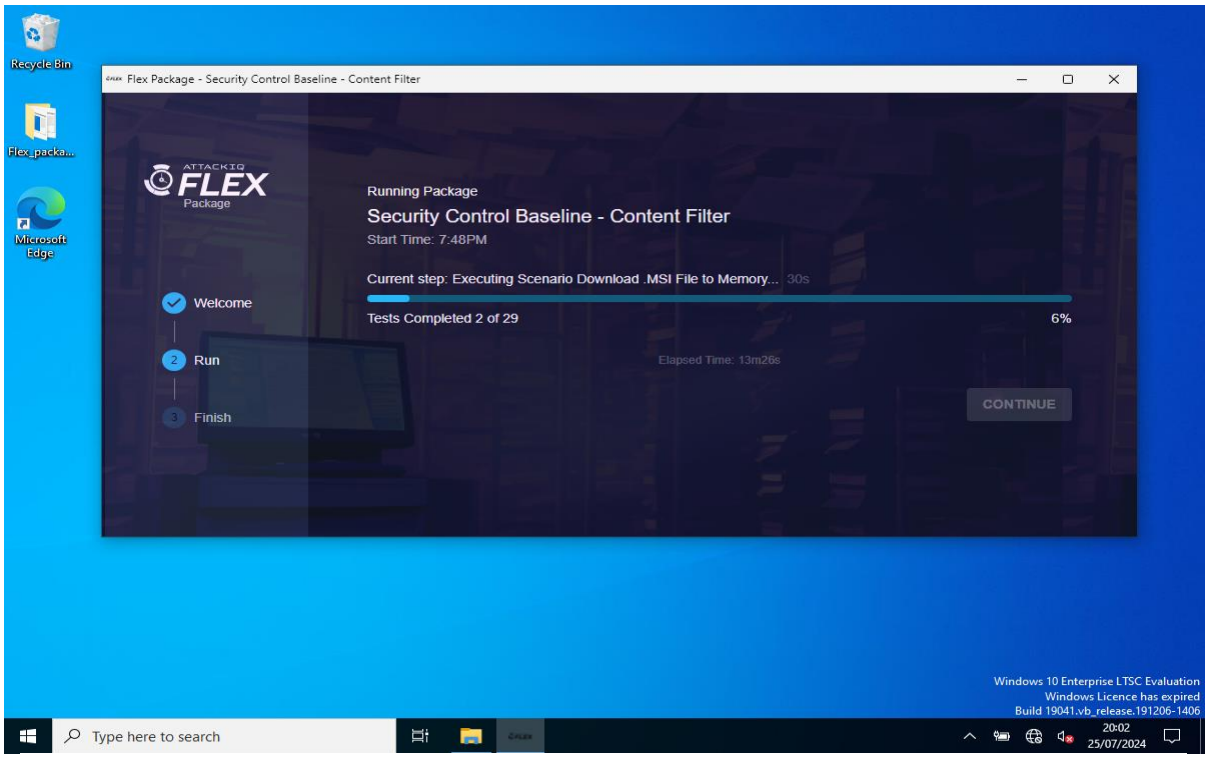

Figure 9. Content Filter Emulation in progress on win10 (offline Mode)

7 Analysing Package

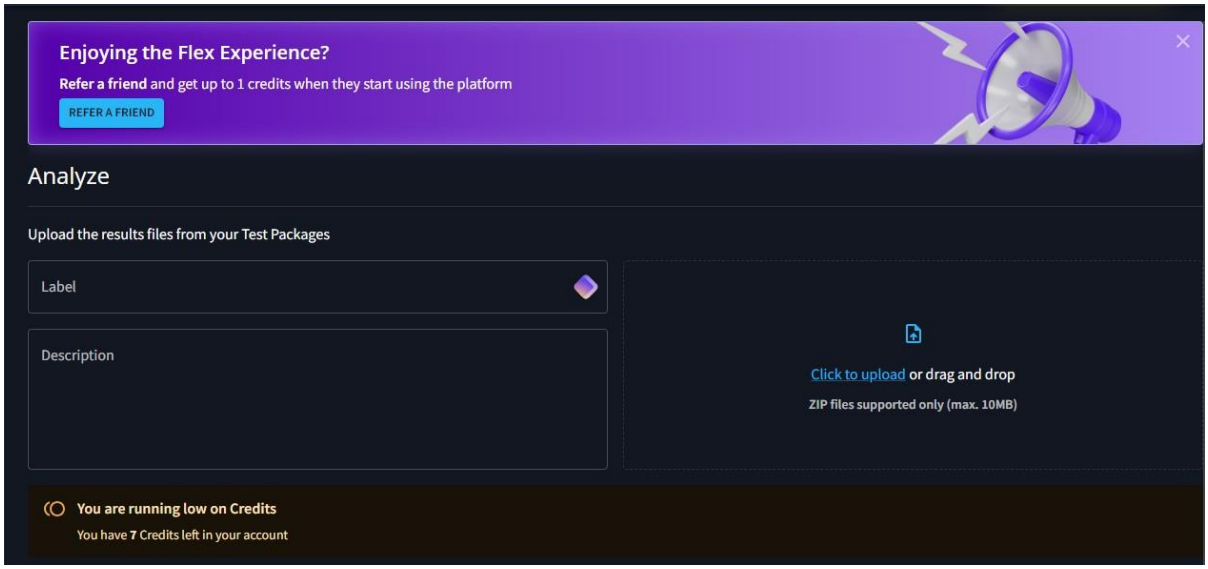

Figure 10. Results from the emulation is saved in a .Zip file format

These results from the emulation are saved automatically in a .zip file format in the same directory where the package is executed.
If successfully executed, without being blocked by your security tool, allow the emulation to run fully to completion.
Then upload results to the BAS platform for advanced analysis.

8 Reports

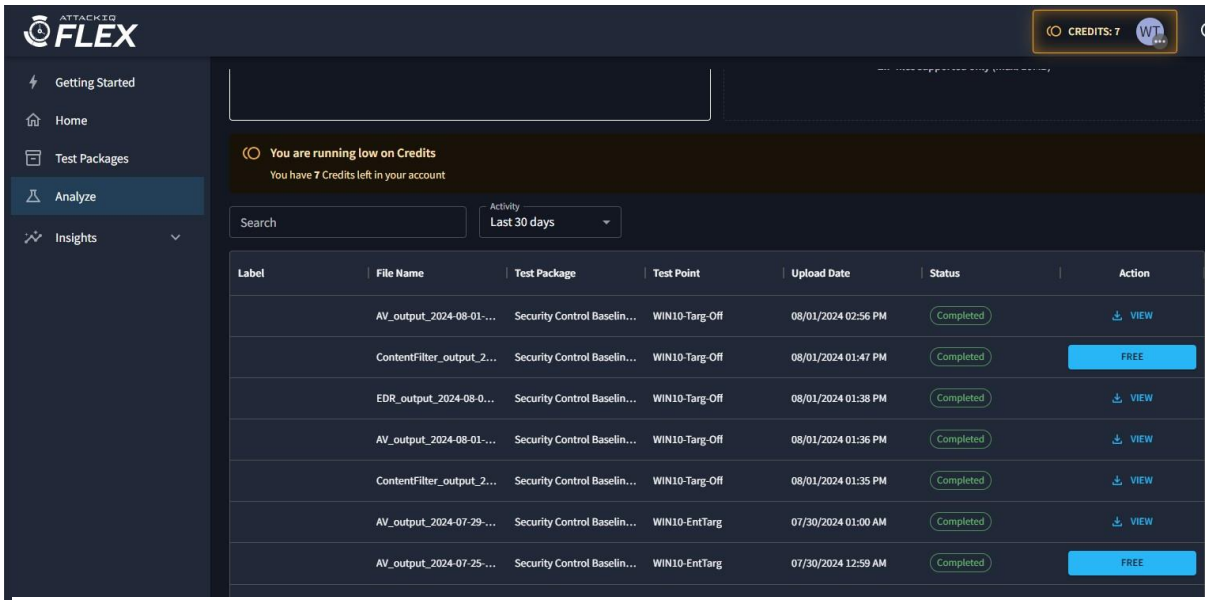

Figure 11. Completed result from analysis

Flex automatically generates a comprehensive report once the testing output is uploaded to the Flex portal. Specific report content varies depending on the report that is run.

9 Insights

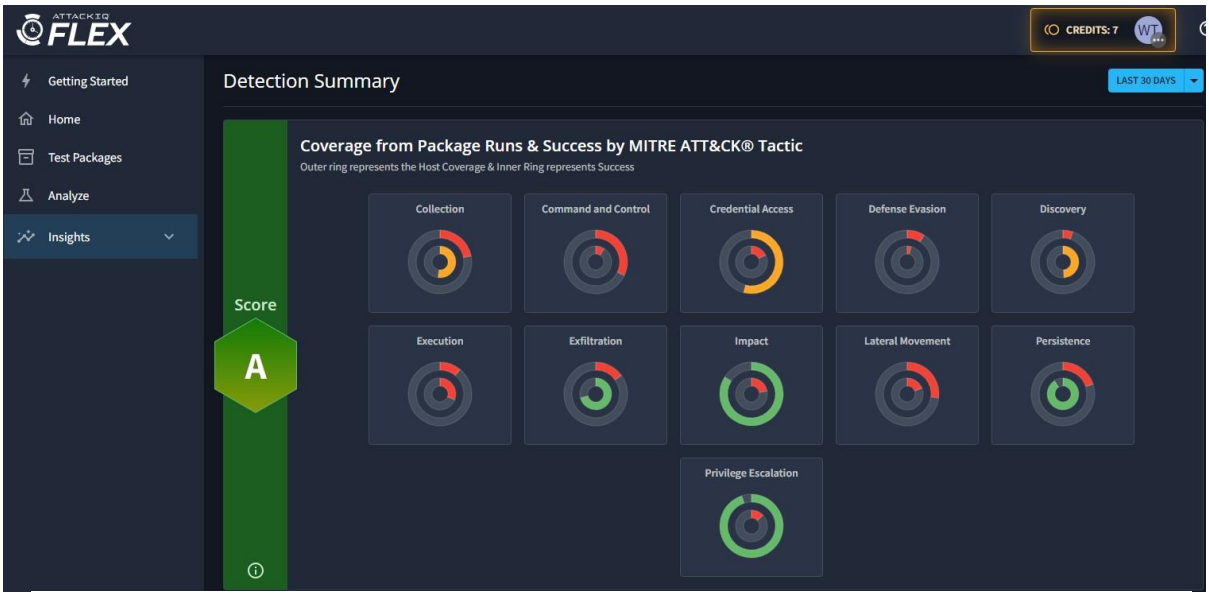

Figure 12. Results from emulation Detection

Figure 13. Passed/Failed Scenarios per Tactic

Figure 14. Package Success/Failure Rate

Simple, comprehensive, and MITRE ATT&ACK aligned test performance insights that are designed to drive action. Easily understand your security performance at-a-glance.