

CYBERSECURITY PROJECT

PROJECT TITLE: ASSESSMENT DESIGN FOR SECURITY CONTROLS

TEST: SIGNATURE-BASED VALIDATION TESTING WITH ATTACKIQ BREACH AND ATTACK SIMULATION FRAMEWORK

TEST PLAN SCENARIO:

So I joined the company (LinQ Technologies) team as a Security Validation Analyst and I've been tasked with testing the company's existing security controls to validate that they are working as expected.

TEST SCHEDULE PLANNING

The schedule of when assessments are executed may seem like a minor consideration. However, when an assessment is scheduled to run can ultimately impact results. Here are some things to think about when determining when and how often to run an assessment:

- Are the assets to be tested remote or local? Always available? Business-critical?
- Will the scenarios have any impact on local users?
- How often could my test results change?
- How does this testing fit in with the overall IT/Security Operations schedule?

ANTI-VIRUS SIGNATURE-BASED TESTING

TEST SCHEDULE

Test Statement	Does the anti-virus in place stop Malware? Hypothesis: The Security Team believes everything is working as they should
Assets:	System 1(acad6969): A Microsoft Windows 10 Pro, Protected with CB -EDR by Carbon Black. System 2(acad2815): A Microsoft Windows 10 Pro, Unprotected
Scenarios	<ol style="list-style-type: none">1. Download EICAR files to Memory2. Download Zip EICAR file to memory3. Download txt EICAR file to memory4. Download double Zipped EICAR file to memory
Schedule:	At least 2 times in a week, None Business days/hours.

Ref: The EICAR Anti-Virus Test File or EICAR test file is a computer file developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO) to test the response of computer antivirus (AV) programs










Test Statement	Does the anti-virus in place stop Malware? Hypothesis: The Security Team believes everything is working as they should
Assets:	System 1(acad6969): A Microsoft Windows 10 Pro, Protected with CB -EDR by Carbon Black. System 2(acad2815): A Microsoft Windows 10 Pro, Unprotected
Scenarios	<ol style="list-style-type: none"> 1. Download <i>MAZE Ransomware Sample to Memory</i> 2. Download Zip Robinh to memory 3. Download txt EICAR file to memory 4. Download double Zipped EICAR file to memory
Schedule:	At least 2 times in a week, None Business days/hours.

Requirements:

1. ATTC&CKIQ Breach and Simulation Platform

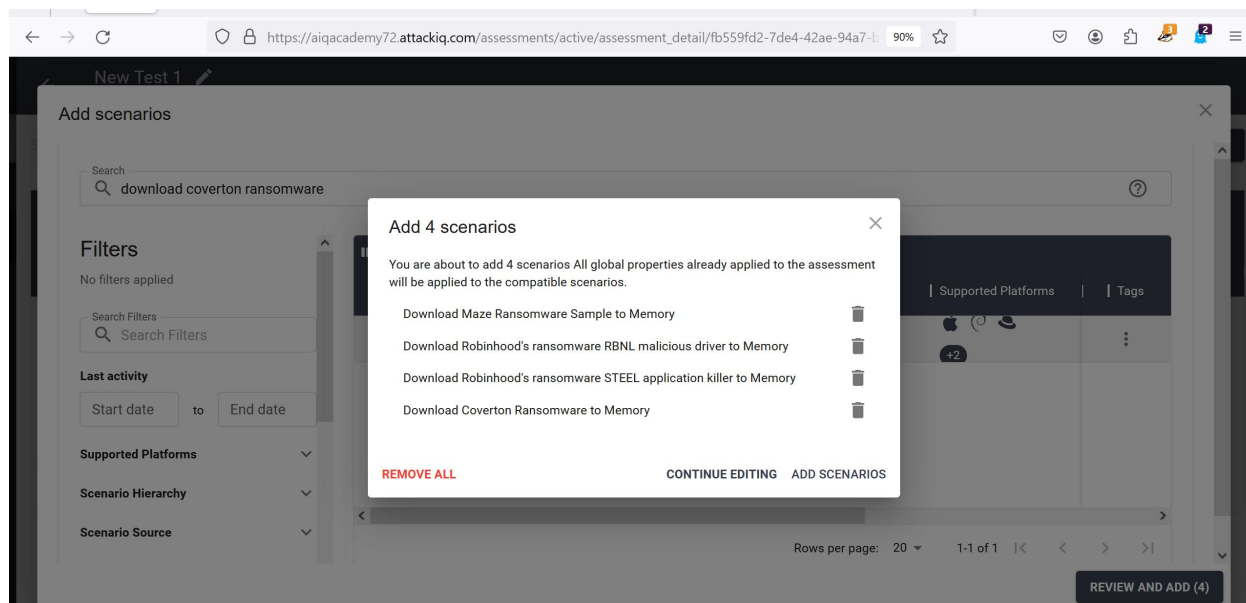
2. EICAR Anti-Virus Test Files

- a. EICAR File
- b. Zipped EICAR File
- c. TXT EICAR File
- d. Double Zipped EICAR File

EICAR 						
Showing 4 of 4 scenarios						
Scenario Name						ADD SCENARIOS
Scenarios						
Scenario name	Compatible Technologies	Forced via SIEM	Capabilities Tested	Global Properties	Status	
Download Zip EICAR file to Memory			NGFW +2	N/A	✓	⋮
Download EICAR file to Memory			NGFW +2	N/A	✓	⋮
Download TXT EICAR file to Memory			NGFW +2	N/A	✓	⋮
Download Double Zipped EICAR file to Memory			NGFW +2	N/A	✓	⋮

3. RANSOMWARE TEST FILES

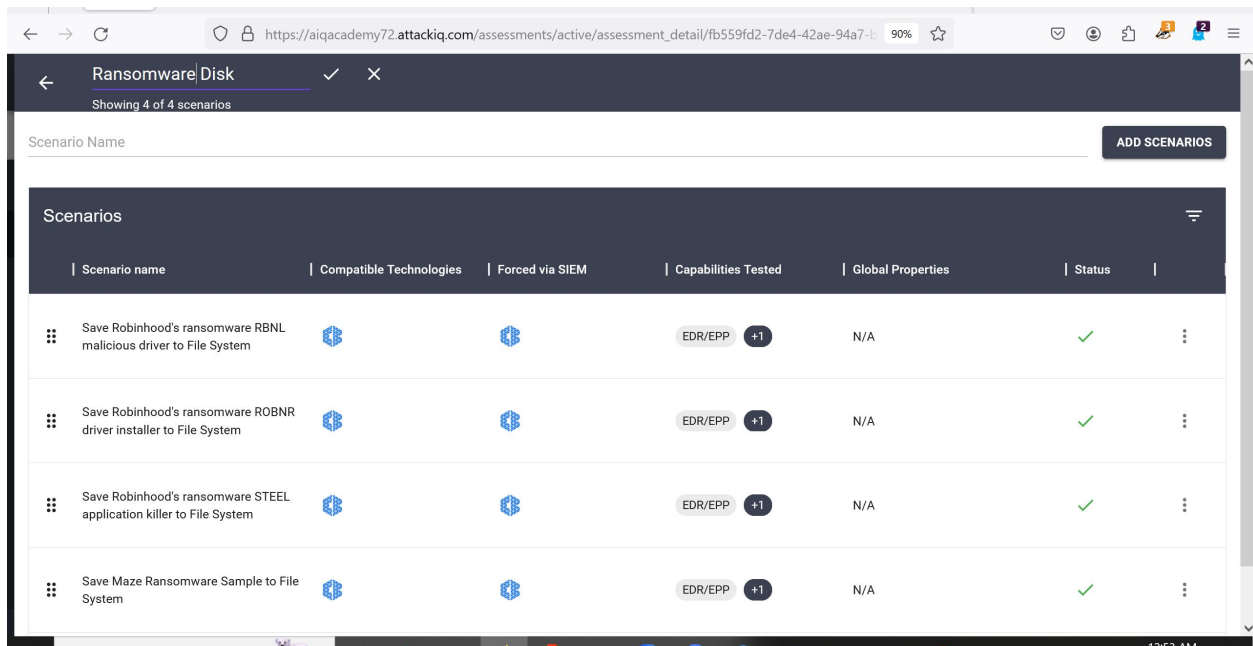
- MAZE Ransomware Sample
- Robinhood Ransomware RBNL Test Script
- Robinhood Ransomware STEEL Application Stealer Test Script
- Covertor Ransomware Test Script



1. RANSOMWARE TEST FILES

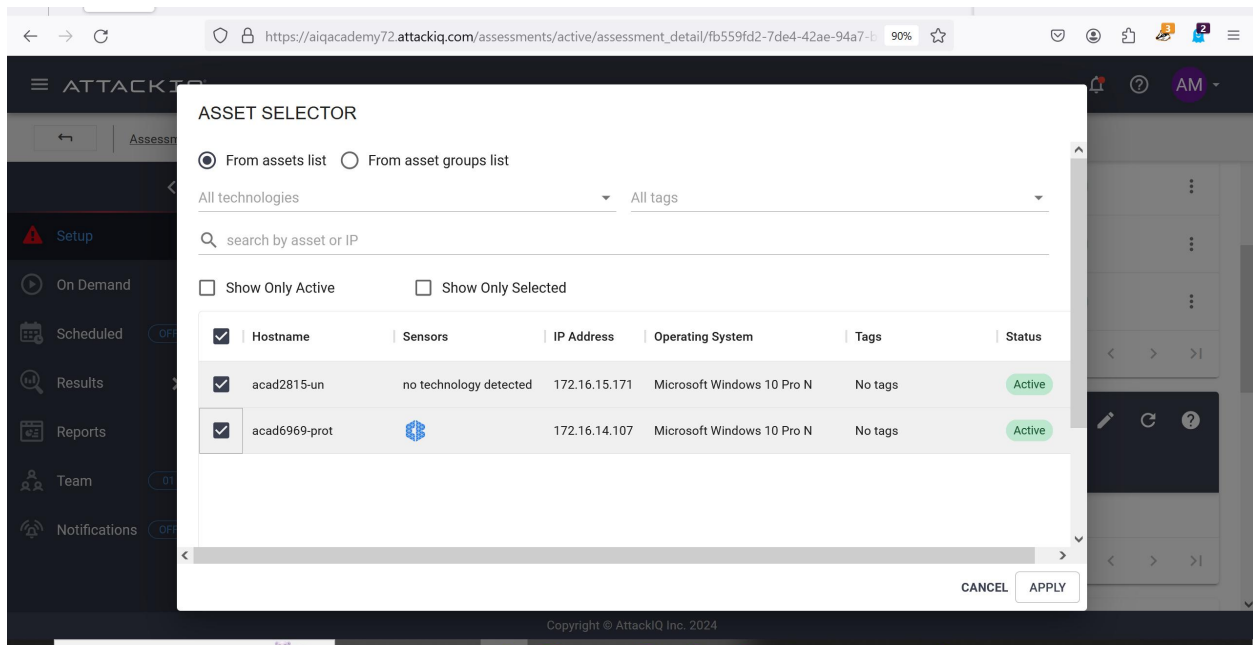
- MAZE Ransomware Sample
- Robinhood Ransomware RBNL Test Script
- Robinhood Ransomware STEEL Application Stealer Test Script
- Covertor Ransomware Test Script

Ransomware Memory						
Showing 4 of 4 scenarios						
Scenario Name						
ADD SCENARIOS						
Scenarios						
Scenario name	Compatible Technologies	Forced via SIEM	Capabilities Tested	Global Properties	Status	
Download Maze Ransomware Sample to Memory			NGFW +2	N/A	✓	⋮
Download Covertor Ransomware to Memory			NGFW +2	N/A	✓	⋮
Download Robinhood's ransomware STEEL application killer to Memory			NGFW +2	N/A	✓	⋮
Download Robinhood's ransomware RBNL malicious driver to Memory			NGFW +2	N/A	✓	⋮



SELECTED ASSET (Target-PCs):

- ACAD6969-prot is the CB EDR by Carbon Black the while second asset is unprotected
- ACAD2815-un is unprotected



Now our scenarios are set and ready to be tested:

ATTACKIQ

Assessments > Anti-Virus Test (Setup)

Setup

On Demand

Scheduled OFF

Results

Reports

Team 01

Notifications OFF

Hostname	Sensors	IP Address	Operating System	Status
acad2815-un	no technology detected	172.16.15.171	Microsoft Windows 10 Pro N	Active
acad6969-prot		172.16.14.107	Microsoft Windows 10 Pro N	Active

Selected Assets

Rows per page: 51-3 of 3

EICAR	2	-	4	SYSTEM	Ready (4)
Ransomware Memory	2	-	4	SYSTEM	Ready (4)
Ransomware Disk	2	-	4	SYSTEM	Ready (4)

Copyright © AttackIQ Inc. 2024

ATTACKIQ

Assessments > Anti-Virus Test (On Demand)

Setup

On Demand

Scheduled OFF

Results

Reports

Team 01

Notifications OFF

Anti-Virus Test

RUN NOW

Assets

Integration Manager Status: ACTIVE

2Total

2Active

Assessment in Progress

Date	Status	Created by	Prevention	Scenarios	Assets	Detection
No assessments on demand run in progress						

Copyright © AttackIQ Inc. 2024

Pre-assessment Verification:

pre_assessment_notification(1) - Microsoft Excel							
Asset IP							
Asset IP	Asset Hostname	OS Version	Agent Version	Test Name	Scenario Name	Scenario Tags	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download Zip EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download TXT EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download Double Zipped EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Maze Ransomware Sample to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Covertion Ransomware to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Robinhood's ransomware STEEL application killer to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Robinhood's ransomware RBNL malicious driver to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Robinhood's ransomware RBNL malicious driver to File System	EDR/EPP;Endpoint Antivirus	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Robinhood's ransomware ROBNR driver installer to File System	EDR/EPP;Endpoint Antivirus	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Robinhood's ransomware STEEL application killer to File System	EDR/EPP;Endpoint Antivirus	
172.16.15.171	acad2815-un	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Maze Ransomware Sample to File System	EDR/EPP;Endpoint Antivirus	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download Zip EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download TXT EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	EICAR	Download Double Zipped EICAR file to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Maze Ransomware Sample to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Covertion Ransomware to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Robinhood's ransomware STEEL application killer to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Memory	Download Robinhood's ransomware RBNL malicious driver to Memory	Network Antivirus;Network Content Filtering;NGFW	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Robinhood's ransomware RBNL malicious driver to File System	EDR/EPP;Endpoint Antivirus	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Robinhood's ransomware ROBNR driver installer to File System	EDR/EPP;Endpoint Antivirus	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Robinhood's ransomware STEEL application killer to File System	EDR/EPP;Endpoint Antivirus	
172.16.14.107	acad6969-prot	Microsoft Windows 10 Pro N	3.8.18	Ransomware Disk	Save Maze Ransomware Sample to File System	EDR/EPP;Endpoint Antivirus	

Test is now running:

ATTACKIQ

Assessments > Anti-Virus Test (On Demand)

Setup

On Demand

Scheduled

Results

Reports

Team

Notifications

Anti-Virus Test

CANCEL

Assessment run in progress.

Assets

Integration Manager Status: ACTIVE

2

Total

2

Active

Assessment progress

Scenarios

In progress

Integrations

In progress

Scenarios

12

Assets

2

Integrations

No integration jobs available yet

Assessment in Progress

Date	Status	Created by	Prevention	Scenarios	Assets	Detection
02/28/2024 01:08 am	In progress	mohammad.abdulazeez@virtuallytestingfoundation.org		12	2	

Copyright © AttackIQ Inc. 2024

REPORTING

ATTACKIQ

AM

Assessments > Anti-Virus Test (Results)

On Demand

Scheduled ON

Results

Summary

History

MITRE ATT&CK

Mitigations

Reports

Team 01

Notifications OFF

Select a run
02/28/2024 - 01:08 am

Selected Run Results

Overall Results

4 out of 24 Scenario Runs were Prevented or Detected

Tests Results

EICAR 0/8

Ransomware Memory 0/8

ATTACKIQ

AM

Assessments > Anti-Virus Test (Results)

On Demand

Scheduled ON

Results

Summary

History

MITRE ATT&CK

Mitigations

Reports

Team 01

Notifications OFF

Select a run
02/28/2024 - 01:08 am

EICAR 0/8

Ransomware Memory 0/8

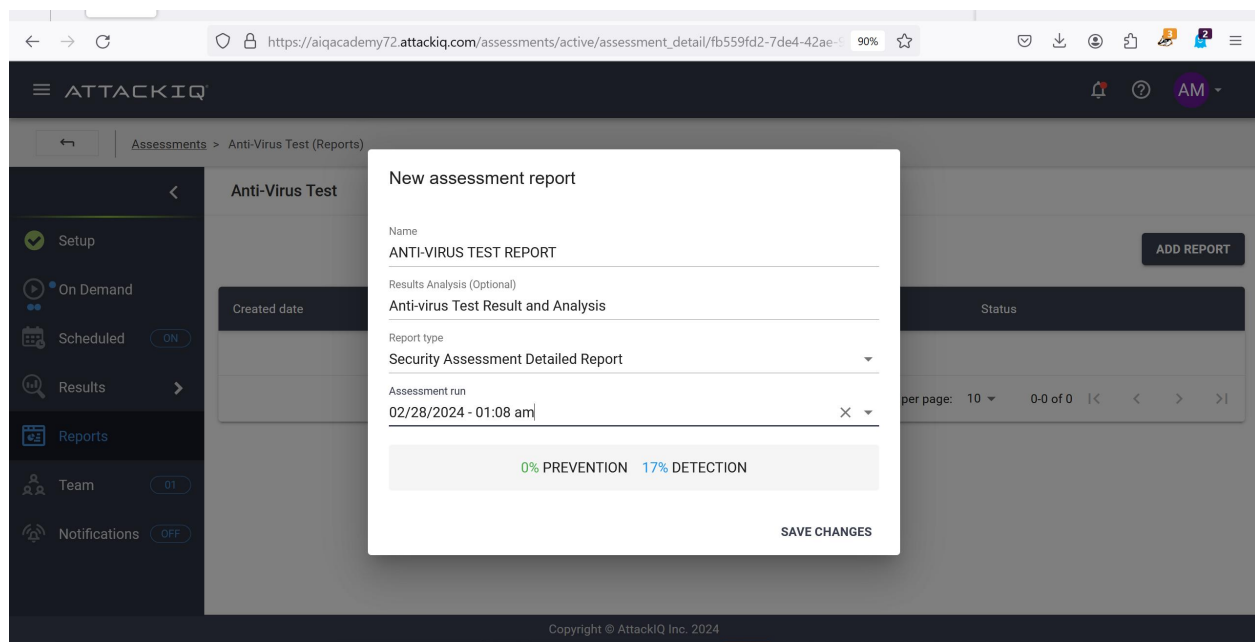
Ransomware Disk 4/8

Next Steps

Mitigations

1 recommendation

VIEW MITIGATION PLAN



IN CONCLUSION

A comprehensive assessment Report containing results, starting at an executive Summary level with overall scenario pass rates and then progresses to increasingly detailed information about individual scenarios, assets, and mitigation recommendations was prepared and sent to the Board of Executives.