Testing The Efficacy of Windows Defender Endpoint Security Control Using BAS Technology

MSc Research Project

Master of Science In Cyber Security Information

Marcus Winston Johnson

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 part 2……………………………

Supervisor: ….. Joel Aleburu…………………….………

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

Project Title: …………………………………………………………………………………………………….………

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: ……

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):	

Testing The Efficacy of Windows Defender Endpoint Security Control Using BAS Technology

Marcus Winston Johnson
X23158239

Abstract

Data breaches have become a widespread and expensive concern for enterprises worldwide in the quickly changing cyber threat landscape of today. This paper examines the substantial impact of misconfigurations, frequently caused by human errors and insufficient security measures, in contributing to catastrophic breaches. Utilising information from recent case studies and industry reports, such as the 2023 Data Breach Investigations Report, the research emphasises how misconfigurations enable unauthorised access and the exploitation of vulnerabilities. The study highlights the importance of ongoing and effective configuration management and continual security validation. It suggests utilising modern Breach and Attack Simulation (BAS) tools to automate and improve the process of testing security control capabilities. Moreover, the incorporation of AttackIQ's Flex platform, which provides complimentary and sophisticated adversary simulation and security control testing, is positioned as a cost-efficient and easily attainable solution for enhancing organisational security. This research places emphasis on the significance of proactive and well-informed security management. It offers practical suggestions for reducing the risks associated with misconfigurations and improving overall cybersecurity resilience. The purpose of the research is to provide guidance to cybersecurity professionals, policymakers, and organisations on how to implement steps to protect sensitive information and establish strong security frameworks to protect critical organizational assets.

1. Introduction

Data breaches (Madnick, 2024) are becoming an increasingly common and expensive problem for businesses all over the world in the quickly changing cybersecurity landscape of today. Central to these breaches are misconfigurations and poor security procedures that expose sensitive data (Potlapally, 2011a), (Cuppens, Boulahia Cuppens and Garcia-alfaro, 2006) which play major role in these attacks. Misconfigurations (Fiebig, 2017) reveal sensitive information and cause significant financial losses as well as harm to one's reputation. They are frequently the consequence of oversight, human mistake (Pernet, 2024) , or inadequate security measures. Numerous reports emphasise how serious this problem is. The 2023 Data Breach Investigations Report (DBIR) (DBIR, 2024) states that human error, including configuration errors (Hope, 2024) that allowed unauthorised access and vulnerability (Patel, 2019) exploitation, was a factor in 74% of breaches. According to the IBM Cyber Resilient (IBM, 2021) Organisation Study 2021, a similar proportion of organizations—30%—use over fifty different security tools and technologies, frequently from different vendors. This leads to security gaps because there is no single platform, which raises the possibility of misconfigurations (Eshete, Villafiorita and Weldemariam, 2011) and serious data breaches.

A prominent example is the OWASP data breach (Hope, 2024), caused by improper server configuration management, compromised and exposed members' personal information. Through the examination of recent case studies and breach data, this study aims to investigate the role that misconfigurations (Trend Micro, 2021) play in data breaches. By finding recurrent patterns and vulnerabilities (Mejri *et al.*, 2013), it hopes to offer actionable advice for enhancing security measures. Continuous ***security validation*** (NGUU and Musuva, 2024); the process of assessing the effectiveness of security controls through continuous testing and evaluation. Security validation ensures that the controls in place are functioning correctly and providing the intended level of protection against threats. Effective configuration management (Towne *et al.*, 2024), and utilising cutting-edge security technologies like ***Breach and Attack Simulation*** (BAS) (Kissel and Szurley, 2022) systems; a technology designed to automate and continuously evaluate and improve an organization's security posture by simulating the tactics, techniques, and procedures (**TTP**s) of real-world adversaries to identify and rectify misconfigurations. These technologies are pivotal in addressing new vulnerabilities and security gaps, providing key insights into how effective security controls are in detecting and responding to attacks in our simulated test environment which is going to be our main focus area in this research. An organization's size and financial resources will determine which BAS system (Master, Hamilton and Dietz, 2022) is best for it because these systems may automate (Lerums, Poe and Dietz, 2018) the security controls testing process, freeing up security professionals to focus on other important duties.

In support of this proactive approach (Lamichhane, Hong and Shetty, 2018), AttackIQ's Flex (AttackIQ, 2024b) platform offers advanced ***adversary emulation***; the practice of emulating potential cyber attackers to test an organization's defenses. This helps in identifying vulnerabilities and improving incident response strategies by mimicking the behaviours of known threat actors and ***security control testing;*** a measure implemented to safeguard information systems by reducing risks to acceptable levels. These controls can be technical, administrative, or physical, and are designed to protect the confidentiality, integrity, and availability of information. By providing perpetual access to baseline tests and advanced attack emulations (MITRE Engenuity, 2024), the platform simplifies security testing and reduces costs. Flex (AttackIQ, 2024a) also includes packages designed to enhance security against Command and Control (C2) communications and assess Next-Generation Firewall (NGFW) (Shin *et al.*, 2023) effectiveness using packet capture replay technology. This innovation allows organizations to evaluate their security controls comprehensively and effectively, without the need for costly and disruptive traditional testing methods. The introduction of these free and accessible tools underscores the importance of continuous security validation and highlights the potential for widespread improvement in cybersecurity practices.

Conventional techniques for assessing the efficacy of endpoint security (SentinelOne, 2024) products (Sentinelone, 2024) are frequently ineffective, creating holes that expose enterprises to cunning and sophisticated attackers. Correcting misconfigurations (Eshete, Villafiorita and Weldemariam, 2011) is essential since the danger increases (Poptani and Gatty, 2018) with the growing reliance on cloud and sophisticated IT systems, which calls for proactive and knowledgeable security management. To improve overall organisational security, this study employs the ***MITRE ATT&CK framework*** (MITRE ATT&CK®, 2024b), a project by the ***MITRE Engenuity*** (MITRE Engenuity, 2024) team which seeks to advance the state of the art and threat-informed defence practice, their goal is to create useful tools, procedures, and resources based on MITRE ATT&CK®, enabling cyber defenders to enhance their operations. The MITRE ATT&CK framework is a globally-accessible knowledge based of adversary tactics and techniques (TTPs) based on real-world observations of threat actors.

This research employs the MITRE ATT&CK framework is to help organisations identify and analyze common misconfigurations in security controls. A recent analysis of academic publications and industry reports on misconfigurations mostly point to human errors, the study intends to highlights the significance of automating security control deployment and testing to minimise expensive human errors (Pernet, 2024), (Tunggal, 2023). The study also criticises traditional security testing methods, which frequently take security tools at face value without conducting adequate validation (Towne *et al.*, 2024) . It also emphasises how BAS technology (Kissel and Szurley, 2022) can improve security efficacy and effectiveness against contemporary threats by ensuring that security capabilities are appropriately configured to fend off common threats in the wild.

This research project intends to answer the following questions;

Question i:

What is the effectiveness of Breach and Attack Simulation (BAS) systems in enhancing security control testing and reducing the risk of misconfigurations in complex IT environments?

Question ii:

How can continuous security validation be integrated into existing cybersecurity frameworks to improve organizational resilience against sophisticated attacks?

Question iii:

What are the limitations of conventional endpoint security assessment techniques, and how can modern approaches, such as BAS, address these challenges?

Objectives:

Research Objectives

The increasing complexity of IT environments and the evolving sophistication of cyber threats necessitate a critical examination of existing cybersecurity frameworks, particularly in the context of their ability to detect and respond to advanced adversarial tactics. This research seeks to explore the effectiveness of Breach and Attack Simulation (BAS) systems in enhancing security control testing and reducing the risk of misconfigurations in complex IT infrastructures. By evaluating the capabilities of BAS technologies, such as the AttackIQ Flex platform, this study aims to determine how these systems can automate and improve the security validation process, thereby addressing the vulnerabilities that methods often fail to mitigate. The research will also compare the efficacy of BAS systems with conventional security validation techniques, focusing on their role in detecting and preventing configuration errors that could lead to significant security breaches.

Moreover, this study aims to investigate how continuous security validation can be integrated into existing cybersecurity frameworks to bolster organizational resilience against increasingly sophisticated cyber threats. The research will examine the potential of continuous validation processes, including advanced adversary emulation and packet capture replay technologies, in enhancing the detection and response capabilities of security controls. By proposing a framework tailored to various organizational sizes, resources, and threat landscapes, this research intends to offer a scalable and practical solution for implementing continuous security validation that can adapt to the dynamic nature of cyber threats.

In addition, this research will critically assess the limitations of conventional endpoint security assessment techniques and explore how modern approaches, particularly BAS and Next-Generation Firewalls (NGFWs), can overcome these challenges. The study will identify the inherent weaknesses in traditional methods, such as their inability to detect sophisticated attacks and their reliance on static, signature-based detection mechanisms. Through a thorough evaluation of modern security technologies, the research will provide actionable recommendations for organizations to adopt these advanced approaches, ensuring a more robust and cost-effective cybersecurity posture that can effectively counter contemporary threats.

2. Related Works

This research addresses the ongoing need for effective security validation within contemporary organizations, emphasizing the limitations of traditional security testing methodologies and the benefits of automated approaches such as Breach and Attack Simulation (BAS) (Osorio et al., 2013), (Arbuckle, 2019) tools. Traditional methods often fail (Williams-Bew, 2023) to keep pace with the evolving threat landscape, necessitating the adoption of more dynamic and adaptive solutions. For instance, (FangLan et al., 2013) propose a model for network security validation leveraging adaptive control theory and reinforcement learning to dynamically optimize security measures. This approach is designed to continuously adapt and improve, ensuring high validity and accuracy in security verification, although its complexity may pose challenges for organizations lacking advanced technical expertise.

Moreover, (Potlapally, 2011b) explores the practical aspects of hardware security, identifying key challenges such as supply chain vulnerabilities and the integration of security features in hardware design. While (Potlapally, 2011b) offers a broad overview of hardware security, a deeper focus on specific design vulnerabilities could provide more actionable insights for preventing hardware-level breaches. Similarly, (Nikiforova *et al.*, 2024) highlights the importance of behavioural analysis in detecting and identifying insider threats, offering practical advice for incorporating behavioural analysis into security practices. However, significant challenges related to data privacy and the substantial investment required for effective implementation are acknowledged.

(Arrott, Macalintal and McMillan, 2017) delve into the security implications of synchronizing cloud services across multiple devices, identifying vulnerabilities from inconsistent device configurations and security policies. They propose a system for uniform policy enforcement and secure data transfer, which, while practical, has limited empirical support and may overlook other critical security aspects. (Sowinski-Mydlarz *et al.*, 2022) validate a security analytics framework capable of real-time threat detection and response. Although the framework's scalability makes it suitable for large organizations, the study lacks comprehensive performance metrics and benchmarks, necessitating additional testing in diverse operational environments.

(Vashishtha, 2023) evaluates various antivirus programs based on false positive rates, system impact, and detection rates, offering guidelines for selecting appropriate software based on user needs and threat environments. Despite providing thorough standards for antivirus performance evaluation, the study is limited by its reliance on artificial benchmarks, which may not accurately reflect real-world performance. The 2023 Data Breach Investigations Report by (Verizon DBIR, 2023) provides an in-depth analysis of data breach trends, causes, and impacts, highlighting common attack vectors such as ransomware (Sophos, 2023), phishing, and insider threats. While offering comprehensive data and actionable recommendations, the report may exhibit bias towards reported incidents, and some suggestions may not be feasible for smaller organizations with limited budgets.

Finally, (Trend Micro, 2021) outlines common cloud configuration errors in Microsoft Azure and AWS environments that lead to security breaches, emphasizing the importance of adhering to best practices and proper configuration management. While the focus on AWS and Azure is thorough and supported by real-world data, it potentially overlooks other cloud service providers, and reliance on Trend Micro's data could introduce bias. This body of work collectively underscores the necessity for adaptive, comprehensive, and empirically validated security measures in the face of evolving cyber threats.

In summary

A comprehensive review of the related literature reveals a significant gap in the automation of security control testing efficacy using Breach and Attack Simulation (BAS) (Gartner, 2024) technology. This gap underscores the importance and uniqueness of the current research, which seeks to advance the body of knowledge in cybersecurity and contribute meaningfully to the technology industry.

The reviewed research papers collectively provide a thorough examination of various challenges faced by the cybersecurity industry. These challenges range from the ineffectiveness of anti-malware solutions and patterns of data breaches in cloud services to traditional and often inadequate methods of security control testing, such as penetration testing and vulnerability scans. Additionally, the persistent issue of misconfiguration remains a major cause of security control failures, leading to breaches and reputational damage. Although these papers offer insightful analyses and practical recommendations, they also highlight certain limitations, including the need for more extensive empirical validation and potential biases. Moreover, some experiments rely on proprietary tools and software, imposing additional cost burdens on research projects.

It is evident from the reviewed literature that the papers address distinct aspects of security controls testing through various methodologies. However, they largely do not focus on testing the efficacy of endpoint security solutions in the context of businesses regularly acquiring new security tools to implement a defense-in-depth strategy. For instance, testing using cloud resources such as Cloud Access Security Brokers (CASBs) (Ghosh *et al.*, 2020) involves significant upfront costs, making it challenging for research students to implement their project ideas.

This research aims to fill the current gap in understanding security control failures by utilizing the MITRE ATT&CK framework (MITRE ATT&CK®, 2024b) to conduct a comprehensive threat profiling of adversaries exploiting these weaknesses. The study will emulate the Tactics, Techniques, and Procedures (TTPs); a detailed descriptions of how adversaries carry out attacks. Tactics represent the adversaries' goal or objective, techniques are the How’s or the general methods they use to achieve those goals, and procedures are the specific implementations of techniques of threat actors to provide insights and recommendations for enhancing security program performance, with specific objectives including:

- Investigating the reasons behind security capabilities' failures by examining past incidents and identifying common patterns and weaknesses in security solutions.
- Analysing the effectiveness of specific adversary strategies against current Windows Defender security protections (Siosulli, 2024).
- Employing the AttackIQ Flex agentless test-as-a-service platform that offers free and advanced adversary emulation and security control testing, enabling organizations to proactively validate their security controls with minimal effort and cost.
- Advanced Emulation: The platform includes advanced enterprise-grade attack emulations through agentless packet capture replay technology, allowing for sophisticated testing without disrupting normal operations.

Data generated from simulating adversary TTPs against Windows Defender (Siosulli, 2024) baseline controls will be utilized to:

- Streamline cybersecurity assessments and improve responses to adversary behaviours.
- Support the adoption of threat-informed defense by mapping its capabilities to the MITRE ATT&CK framework (MITRE ATT&CK®, 2024b).

This research endeavours to provide actionable insights and suggestions for bolstering cybersecurity defense, contributing to a more resilient and informed security landscape.

3. Research Methodology

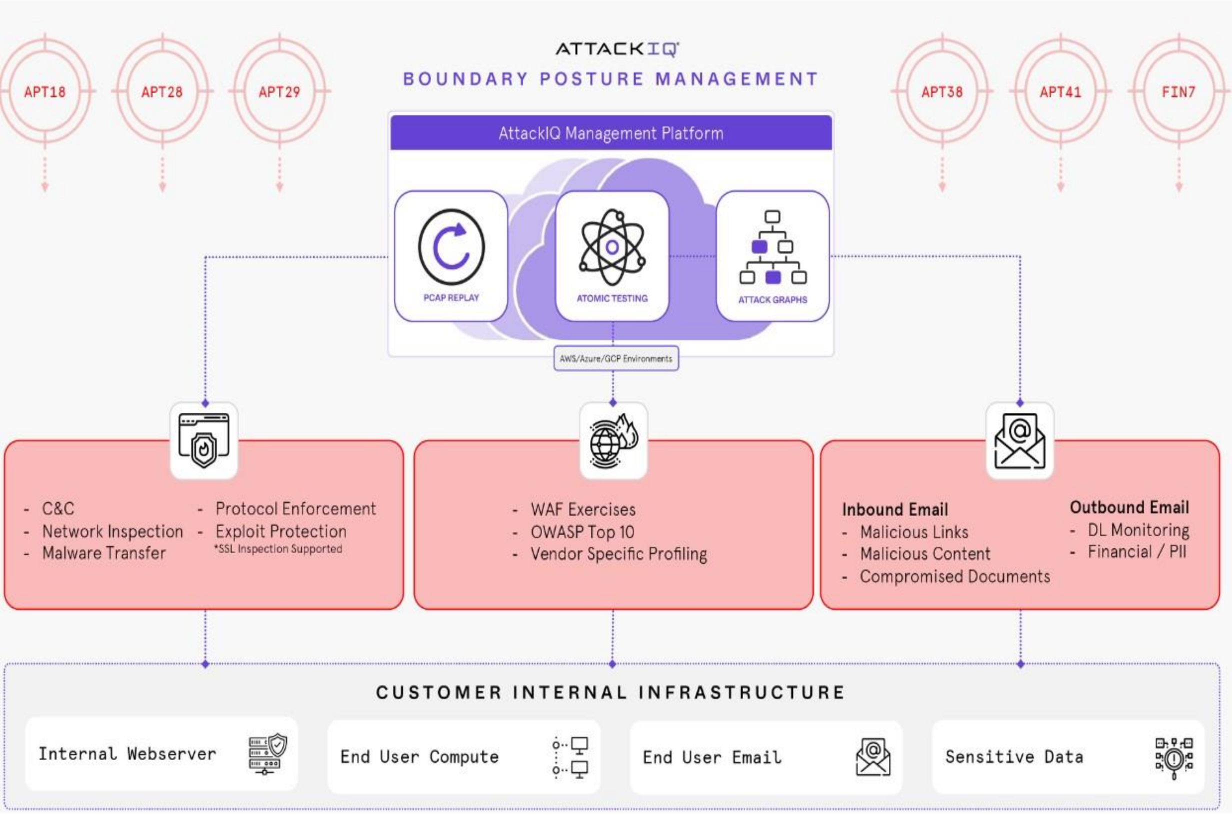


Fig.1 High Level architectural overview AttackIQ BAS Platform

This study will utilise a mixed-methods research strategy, incorporating both quantitative and qualitative methods to conduct a comprehensive evaluation of the Flex Testing Modalities. The research will progress through the subsequent stages:

Considering the increasing complexity of cyber threats, it is imperative for organisations to implement strong security measures to protect their digital assets. AttackIQ's Flex (Forster, 2023) cloud-based testing modalities, depicted in the accompanying **Fig.2**, provide a complete approach to security validation using three primary testing modalities each offering distinct capabilities aimed at testing and validating security controls against potential cyber threats: ***Attack Flow***; this modality mimics the actions of real attackers which focusses on mimicking the steps an adversary could take to compromise and take advantage of a network.

Atomic Testing; Atomic testing evaluates particular detection skills by simulating distinct attack methods. These tests are more detailed, focusing on specific individual tactics and procedures that an attacker could employ. This makes it possible to precisely validate security controls and guarantee that every component of the security architecture is operating as intended.

and ***Packet Capture Replay***; this modality simulates network traffic that mimics attack patterns in order to evaluate perimeter defences. Through the replay of recorded network traffic, this modality enables enterprises to assess the efficacy of their security infrastructure in identifying and thwarting malicious behaviour at the network layer. Each of these modalities are designed to replicate attacker behaviours and detection capabilities, allowing organisations to evaluate and improve their security positions with effectiveness. The objective of this research is to assess the effectiveness of these testing methods in enhancing organisational cybersecurity.

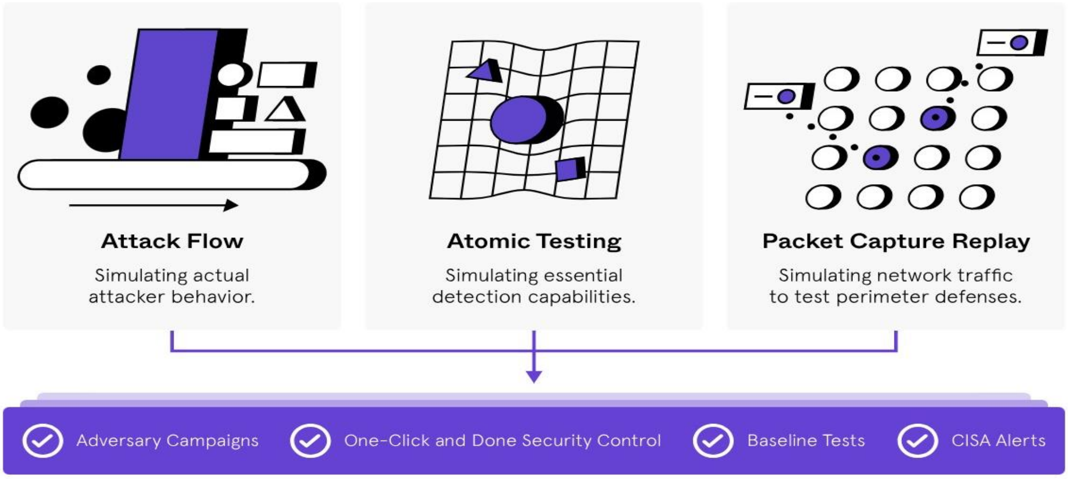

Attack Flow
Simulating actual attacker behavior.
Atomic Testing
Simulating essential detection capabilities.
Packet Capture Replay
Simulating network traffic to test perimeter defenses.
Adversary Campaigns
One-Click and Done Security Control
Baseline Tests
CISA Alerts

Fig. 2 Flex Testing Modalities

This research aims to address the existing gap in automated security control testing efficacy using Breach and Attack Simulation (BAS) technology (AttackIQ, 2024c) in a ***four-step*** process. The focus is on understanding and validating security control failures by emulating adversary TTPs based on the MITRE ATT&CK framework against windows built-in security know as defender security to test the efficacy of control capabilities (MITRE ATT&CK®, 2024b) to determine which version of Microsoft windows comes out-of-the-box with minimum baseline security in place to protect against some of the most common threat actors behaviour patterns (TTPs) that lead to the most breaches in many organizations. The study's objective is to test windows ten (10) enterprise evaluation editions in a virtual machine (VM) environment in two different configuration modes to provide insights and recommendations for enhancing security program performance, particularly evaluating Windows Defender's Security protections capabilities.

3.1. STEP1:

Lab Environment Setup

The lab environment will be a hybrid setup, consisting strictly of locally hosted virtual machines (VM), both running the same versions and updates of win 10 operating system (OS) respectively but running under two different scenarios mode which is Online and Offline, and a cloud-based BAS-as-a-service platform called AttackIQ Flex. The locally hosted lab environment will utilize VirtualBox as a type-2 hypervisor (hosted hypervisor) to host a clean-installed of two VMs both running windows 10 Enterprise evaluation editions with the most up-to-date virus definition in two different modes, Offline and Online. These VMs will serve as the primary target for emulating common attack patterns packaged with various live malware samples (scenarios) against windows defender security as baseline as the OS come built-in endpoint with windows default protection solution.

3.2. STEP2:

Selection of Operating System

The reason for the choice of Windows (win10) as the testing targets environment is based on its significant market share. According to Statista (Statista, 2024), Microsoft Windows holds 68.15% of the desktop, tablet, and console OS market as of February 2024, with windows 10 Specifically being the most popular version found in production environments. Having approximately a 68% market share in November 2023, makes it a frequent target for security breaches, making it essential to test its default security mechanisms as representative of common operational environments. This prevalence has led to the Windows operation system (OS) being the primary target for security breaches, emphasizing the need to test its default security capabilities.

3.3. STEP3:

Baseline Security Testing

The core of this methodology involves evaluating the default configuration capabilities of Windows Defender security. The initial setup will include a fresh installation of two separate and isolated virtual machines (VMs), both running windows 10 enterprise versions in two different modes which are ***Online*** and ***Offline***; during which snapshots will be taken to allow rollback in case of system failures. The evaluation will focus on two scenarios;

Scenarios 1: One Windows VM in ***offline*** mode will be tested by simulating various threat actors' activities using a malicious pre-packaged security assessment payload based on well-known TTPs (without internet access).

Scenarios 2: This second stage will involve simulating threat actors' behaviours (TTPs) while ***online*** (with internet access). Each scenario will use the same pre-packaged assessment payload as baseline (common attack patterns with various live malware samples) to validate windows endpoint antivirus capabilities as designed and shaped by Microsoft in its default state.

3.4. STEP4:

Threat Emulation and Testing

Threat emulation and testing with AttackIQ Flex will utilize its MITRE ATT&CK framework integration to simulate sophisticated attacker behaviours, providing a realistic assessment of Windows Defender’s capabilities against modern cyber threats. Using the threat intelligence gathered, attacker’s behaviours (TTPs) will be emulated through AttackIQ Flex BAS, which ensures various testing modalities, including Attack Flow, Atomic Testing, and Packet Capture Replay, to simulate actual attacker behaviours, essential detection capabilities, and network traffic, respectively. These tests will provide insights into how well Windows Defender's default configurations can withstand sophisticated attacks.

4. Design Specification

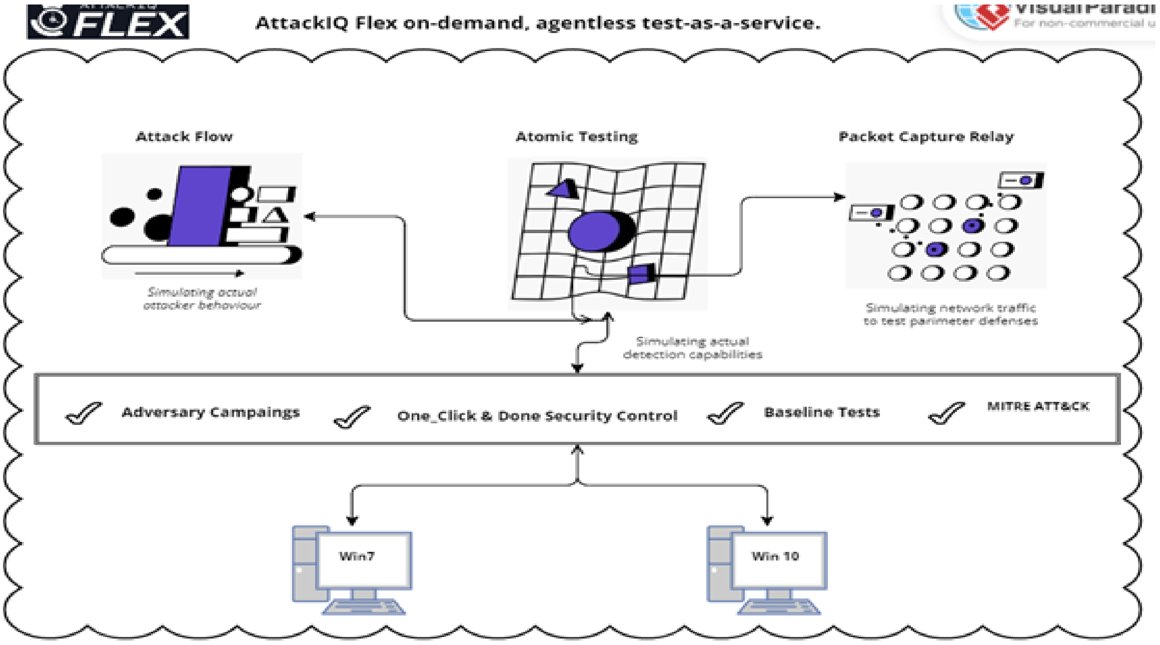

FLEX
AttackIQ Flex on-demand, agentless test-as-a-service.
Attack Flow
Atomic Testing
Packet Capture Relay
Simulating actual attacker behaviour
Simulating network traffic to test parimeter defenses
Simulating actual detection capabilities
Adversary Campaings
One_Click & Done Security Control
Baseline Tests
MITRE ATT&CK
Win7
Win 10

Fig. 2 Simplified Architectural Design implementation

The research will utilize a mixed-methods approach, combining both qualitative and quantitative methodologies to achieve a comprehensive analysis of security control efficacy.

Security Efficacy: The ability of security measures to effectively protect information systems from threats. It encompasses the performance, accuracy, and reliability of security controls in detecting, preventing, and mitigating attacks.

4.1. **Laboratory Setup**

The research involves setting up a controlled lab environment to simulate real-world cyber threats and measure the effectiveness of security controls.

4.2. **Virtual Lab Environment**

Flex credits: To access different tests inside the product, you can use flex credits as your digital currency. There are various other ways for you to gain additional credits.

i. *Tools and Platforms:*

- AttackIQ Flex BAS-as-a-service for adversary TTPs emulation
- VirtualBox V.7.0.20 Type-2 hypervisor (hosted hypervisor) to host virtual machines.
  Operating Systems:
- Windows 10 Enterprise Evaluation Edition (Offline) for testing Windows Security.
- Windows 10 Enterprise Evaluation Edition (Online) for testing Windows Security

ii. *Configuration:*

- Two (2) Virtual machines: Each VM, one online with the latest virus definitions and one offline, will be configured to replicate typical user environments, allowing us to assess Windows Defender's efficacy under varied network conditions in ***offline*** and ***online mode*** respectively, fully isolated without any form of communication between both VMs.
- Guests VM in offline mode will not be connected to the internet and will also not be checked for the latest virus definition. With the default security in place, Windows Defender capabilities will be evaluated by the AttackIQ Flex BAS for both online and offline mode.

iii. *Data Collection*

The study will generate and collect data from a pre-packaged simulated assessment, emulating common threat actors and attack patterns with various live malware samples from the AttackIQ Flex BAS-as-a-service for ***Security Control Baseline - Endpoint Antivirus***. The attacks assessment will emulate common TTPs based on the MITRE ATT&CK framework (MITRE ATT&CK®, 2024c) to test the resilience of Windows Defender security.

The Security Control Baseline Assessment effectively aligns with several well-known threat actors and groups by utilizing their known malware samples and tools. Specifically, the assessment focuses on threat actors such as APT28 (Fancy Bear), APT29 (Cozy Bear), the Lazarus Group, Emotet, Lockbit 3.0, WannaCry, Petya/NotPetya, Conti, and BlackMatter. Each of these groups is recognized for their sophisticated attack methods, including the use of tools like MiniDuke, Etumbot, advanced malware, ransomware, and espionage tools. For instance, APT28 and APT29 are renowned for their cyber espionage activities, while groups like Lazarus and Emotet have evolved their tools to target various sectors globally. Ransomware groups such as Lockbit 3.0, WannaCry, and Petya/NotPetya have caused significant disruption by encrypting data and demanding ransoms.

The assessment scenarios simulate a variety of Tactics, Techniques, and Procedures (TTPs) as outlined in the MITRE ATT&CK framework. These scenarios cover a comprehensive range of potential threats to ensure robust testing of security controls. Examples of TTPs include Initial Access (T1078) through compromised credentials and phishing emails, Execution (T1204) by opening malicious files, and Persistence (T1053) via scheduled tasks. Additionally, scenarios address Privilege Escalation (T1068) using vulnerabilities like ZeroLogon, Defense Evasion (T1027) through malware obfuscation, and Credential Access (T1003) with tools such as Mimikatz.

Moreover, the scenarios encompass Discovery (T1083) using network and system reconnaissance tools, Lateral Movement (T1071) facilitated by utilities like Netcat, Collection (T1056) through keylogging, Exfiltration (T1048) using encrypted channels, and Impact (T1486) via ransomware encryption.

The alignment of scenarios with specific threat actors, groups, and TTPs provides a comprehensive framework for evaluating the effectiveness of security controls in real-world scenarios. This approach ensures that the assessment is relevant and addresses the most pressing threats faced by organizations today.

Data from these scenarios are collected and analysed to identify gaps in detection and response, and the findings are documented to provide insights into the strengths and weaknesses of the security controls.

iv. Emulation Scenarios

This simulation shall be based on two of the most common attacker attributes that have been combine into two separate assessment packages ***table 1*** below, ready to be executed by the AttackIQ Flex Agentless-As-a-Service emulation platform. These packages are ***Security Control Baseline package– Endpoint Antivirus*** assessment for Advanced Endpoint Security and ***Security Control Baseline package- Content Filter***, each with twenty (20) and twenty-nine (29) scenarios included respectively.

i. Assessment Package Number One (***Security Control Baseline – Endpoint Antivirus***): This 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 second 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.

ii. Assessment Package Number Two (***Security Control Baseline - Content Filter***): Validates network inspection capabilities including the downloading of malicious content from internal networks.

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 these Packages:

Table 1

Security Control Baseline - Endpoint Antivirus		Security Control Baseline - Content Filter
i.	**Save MiniDuke Malware Sample to File System**	Download CryptoLocker Ransomware to Memory
ii.	**Save Etumbot Malware Sample to File System**	Download Locky Sample to Memory
iii.	**Save 2020-04 Lazarus Group Operation Dream Job Malicious Office Document to File System**	Download Mischa Ransomware to Memory
iv.	**Save 2022-05 Emotet Malicious XLS Delivery Document to File System**	Download WannaCry Worm Sample to Memory
v.	**Save Emotet (epoch5) 2022-09 DLL File to File System**	Download Powerware Ransomware to Memory
vi.	**Save Locky Sample to File System**	Download KeRanger Ransomware to Memory
vii.	**Save WannaCry Worm Sample to File System**	Download Xorist Ransomware to Memory
viii.	**Save Petya Ransomware to File System**	Download SynoLocker Ransomware to Memory
ix.	**Save Conti Ransomware 2021-08 to File System**	Download ODCODC Ransomware to Memory
x.	**Save BlackMatter Ransomware 2021-10 to File System**	Download Linux Encoder Ransomware to Memory
xi.	**Save TeslaCrypt Ransomware to File System**	Download Rakhni Ransomware to Memory
xii.	**Save CryptoWall Ransomware to File System**	Download SamSam Sample to Memory
xiii.	**Save CryptoLocker Ransomware to File System**	Download SNSLock Ransomware to Memory
xiv.	**Save 2023-01 Lockbit 3.0 Ransomware Sample to File System**	Download Petya Ransomware to Memory
xv.	**Save Httptunnel Hacktool to File System**	Download Lechiffre Ransomware to Memory
xvi.	**Save 2020-12 ZeroLogon Hacktool to File System**	Download Maktub Ransomware to Memory
xvii.	**Save Hacktool Netcat to File System**	Download 2020-08 CISA Fake PNG Sample to Memory
xviii.	**Save Hacktool Mimikatz to File System**	Download 2023-01 Lockbit 3.0 Persistence Batch File to Memory
xix.	**Save EICAR file to File System**	Download 2023-01 Lockbit 3.0 Decrypt Batch File to Memory
xx.	**Save Zip EICAR file to File System**	Download 2023-01 Lockbit 3.0 Ransomware Sample to Memory
xxi.		Download .BAT File to Memory

xxii.	Download .PS1 File to Memory
xxiii.	Download .HTA File to Memory
xxiv.	Download .CMD File to Memory
xxv.	Download .VBS File to Memory
xxvi.	Download .BASH File to Memory
xvii.	Download .DLL File to Memory
xviii.	Download .MSI File to Memory
xxix.	Download .EXE File to Memory

These assessments align closely with the MITRE ATT&CK framework, which is designed to model the behaviours of threat actors (tactics, techniques, and procedures - TTPs) and provide a structured way to improve security controls and defenses.

Two basic procedures will be utilised here;
Offline Scenario: Testing Windows Defender capabilities without internet connectivity (access to internet services) and also with TPM as extra defensive mechanisms disabled on the guest while running the simulated attack.
Online Scenario: Evaluating Windows Defender Security with full internet access (online) having TMP v2.0 and EFI enabled on the guest VM for the assessment package Security Control Baseline simulation, this is to determine how well windows security will perform while in online situations. This is very important in testing cyber defenses against real-world threats and knowing how effective your controls perform.

v. Data Analysis

The analysis will focus on identifying patterns, weaknesses, and strengths in windows defender security capabilities when faced with modern and advanced threat actor behaviours (TTPs) by simulating a set of selected pre-packaged TTPs which are the most common used by several well-known threat actors and groups by utilizing their above mentioned known malware samples found in ***table 1*** above and tools that has been recorded by CISA Advisory (CISA, 2024) and AttackIQ's Response to CISA Advisory (AttackIQ, 2024d) to breach organizations of all sizes. TTPs (Tactics, Techniques, and Procedures)
The assessment scenarios simulate various TTPs outlined in the MITRE ATT&CK framework, ensuring comprehensive coverage of potential threats. Below are examples of

TTPs covered by the scenarios:

Initial Access (T1078): Use of compromised credentials and phishing emails to deliver malicious documents.
Execution (T1204): Execution of malware upon opening malicious files or documents.
Persistence (T1053): Persistence mechanisms using scheduled tasks and other tools.
Privilege Escalation (T1068): Use of vulnerabilities like ZeroLogon for privilege escalation.
Defense Evasion (T1027): Obfuscation and encryption of malware to evade detection (e.g., encrypted malware samples).
Credential Access (T1003): Use of tools like Mimikatz for credential dumping.

Discovery (T1083): Tools for network and system discovery, enabling further attack progression.

Lateral Movement (T1071): Use of tools like Netcat to facilitate lateral movement across networks.

Collection (T1056): Keylogging and data collection using malicious payloads.

Exfiltration (T1048): Exfiltration of data through encrypted channels and other means.

Impact (T1486): Ransomware encrypting data and demanding ransom (e.g., Locky, WannaCry).

vi. Metrics for Analysis

Detection Rate: The percentage of simulated attacks detected by Windows Defender.

Response Time: The time taken by Windows Defender to respond to detected threats.

False Positives: Instances where benign activities are incorrectly flagged as threats.

False Negatives: Instances where malicious activities go undetected.

vii. Tools and Techniques

AttackIQ Flex Platform:

Offers free and advanced adversary emulation and security control testing.

Uses agentless packet capture replay technology for sophisticated attack emulations without disrupting normal operations.

viii. Data Sources:

Threat intelligence from using the Attack Navigator (MITRE ATT&CK®, 2024a) from the MITRE ATT&CK framework **Fig.3**

Simulation data from AttackIQ Flex platform.

Data will be collected from the emulation engagements exercise, from the two windows versions for analysis.

Data will be analysed to identify security control performance and areas for improvement.

These test methodologies will not only address the current gaps in security control testing but also contribute to the broader field of cybersecurity by providing a replicable and cost-effective approach for continuous security validation

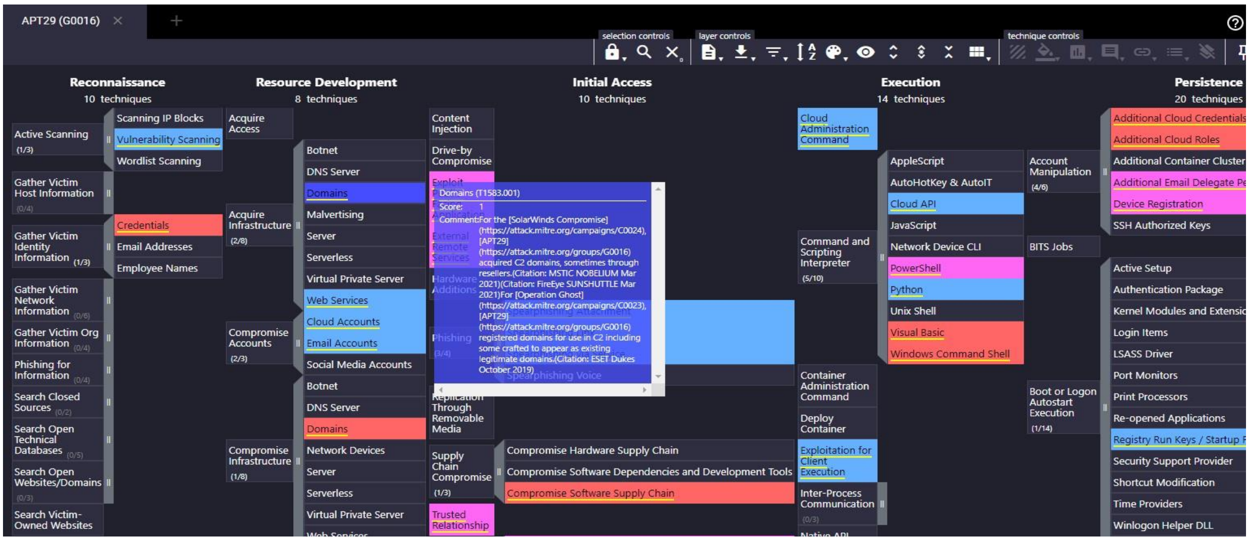
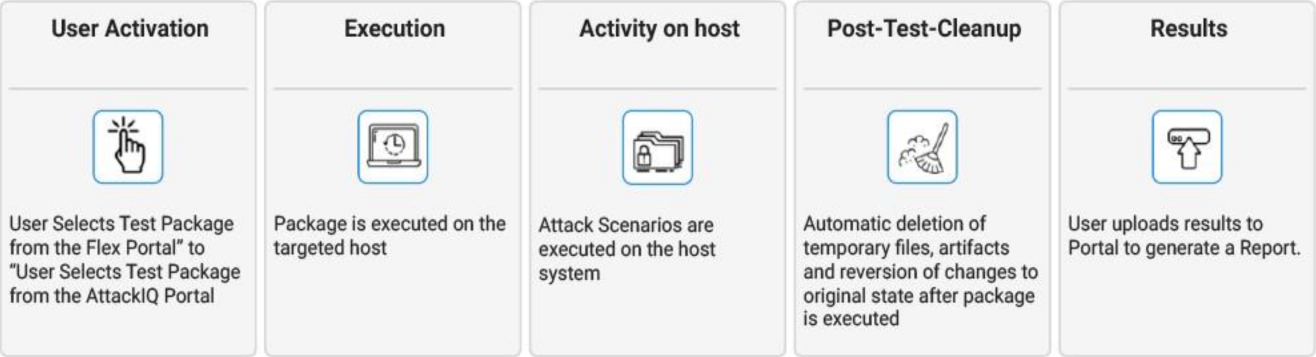

Domains (T1583.001)
Score: 1
Comment:For the [SolarWinds Compromise] (https://attack.mitre.org/campaigns/C0024), [APT29] (https://attack.mitre.org/groups/G0016) acquired C2 domains, sometimes through resellers.(Citation: MSTIC NOBELIUM Mar 2021)(Citation: FireEye SUNSHUTTLE Mar 2021)For [Operation Ghost] (https://attack.mitre.org/campaigns/C0023), [APT29] (https://attack.mitre.org/groups/G0016) registered domains for use in C2 including some crafted to appear as existing legitimate domains.(Citation: ESET Dukes October 2019)

Fig.3 Attack Navigator – Showing all of the TTPs of APT29 (Cozy Bear)

5. Implementation

5.1. Assessment Methods and Scope

The assessments flow in **Fig.3.** were carried out using the AttackIQ Flex service, which emulated various adversarial behaviours (Moskal *et al.*, 2013), (BAJAK, 2024), (CERT-UA, 2023), (Cherepanov, 2017), (CISA, 2024) to test the robustness of the security controls. The methodology involved **user *activation***, ***execution*** of test packages, ***observation of host activity***, and ***post-test cleanup*** and ***results*** to ensure system integrity. The scenarios covered a range of attack vectors, including credential access, ransomware (CISA, 2024), and hacker tools, and assessed the ability of the security controls to prevent these threats.


User Activation

User Selects Test Package from the Flex Portal" to "User Selects Test Package from the AttackIQ Portal

Execution

Package is executed on the targeted host

Activity on host

Attack Scenarios are executed on the host system

Post-Test-Cleanup

Automatic deletion of temporary files, artifacts and reversion of changes to original state after package is executed

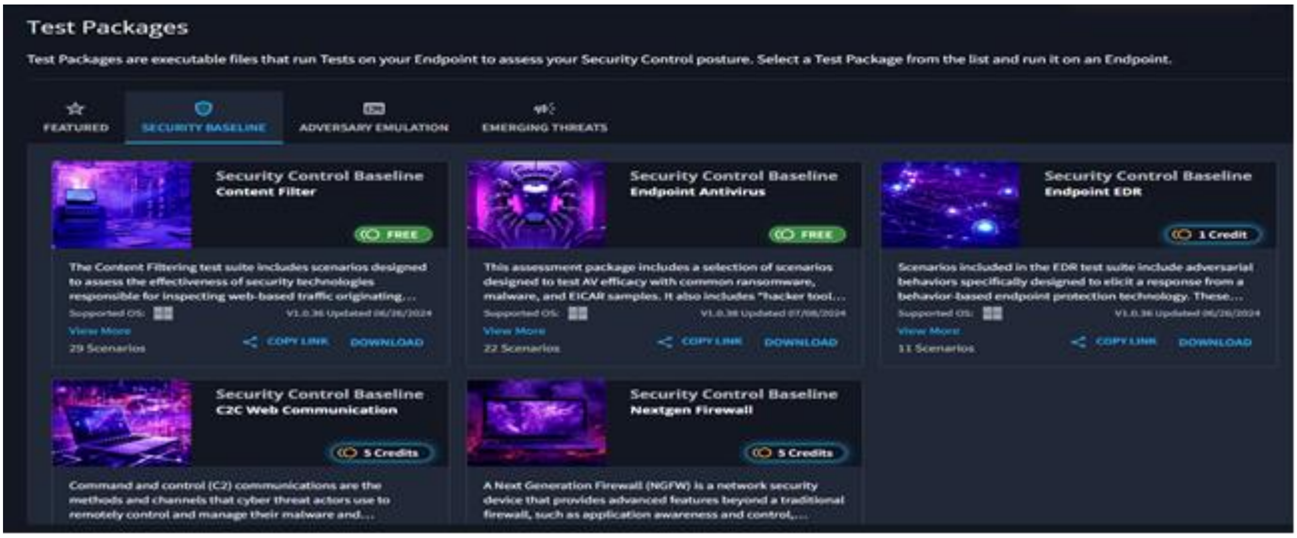
Results

User uploads results to Portal to generate a Report.

Fig. 3. Emulation Engagement Flow for Security Control Assessment

5.2. Scope

These tests assessment packages **Fig.4** provide a detailed framework for evaluating the controls of windows defender default capabilities. The assessment includes three primary categories: Advanced ***Adversary Emulation***, ***Emerging Threats*** which are beyond the immediate scope of this research project and therefore our focus shall be on the **Security Baseline category** which includes the following packages loaded with different malicious activities designed to mimic an actual attacker and assess the effectiveness of windows default security solution**:** ***Content Filtering package***, ***Endpoint Antivirus package***, and ***Endpoint Detection and Response*** (EDR) ***package***, each designed to test specific aspects of network and endpoint security.


Test Packages

Test Packages are executable files that run Tests on your Endpoint to assess your Security Control posture. Select a Test Package from the list and run it on an Endpoint.

Security Control Baseline
Content Filter
FREE

The Content Filtering test suite includes scenarios designed to assess the effectiveness of security technologies responsible for inspecting web-based traffic originating...

Supported OS: V1.0.36 Updated 06/26/2024
View More
29 Scenarios
COPY LINK DOWNLOAD

Security Control Baseline
Endpoint Antivirus
FREE

This assessment package includes a selection of scenarios designed to test AV efficacy with common ransomware, malware, and EICAR samples. It also includes "hacker tool...

Supported OS: V1.0.38 Updated 07/08/2024
View More
22 Scenarios
COPY LINK DOWNLOAD

Security Control Baseline
Endpoint EDR
1 Credit

Scenarios included in the EDR test suite include adversarial behaviors specifically designed to elicit a response from a behavior-based endpoint protection technology. These...

Supported OS: V1.0.36 Updated 06/26/2024
View More
11 Scenarios
COPY LINK DOWNLOAD

Security Control Baseline
C2C Web Communication
5 Credits

Command and control (C2) communications are the methods and channels that cyber threat actors use to remotely control and manage their malware and...

Security Control Baseline
Nextgen Firewall
5 Credits

A Next Generation Firewall (NGFW) is a network security device that provides advanced features beyond a traditional firewall, such as application awareness and control,...

Fig. 4 Selection of test assessment packages for emulating common attack patterns

The Endpoint Antivirus section evaluates the effectiveness of antivirus solutions in detecting and preventing the execution of malware on endpoints. The scenarios involve downloading and saving malware samples and hacker tools to the local file system, followed by hash comparisons to determine if the security controls successfully prevented these files from being executed or copied. This section includes tests with malware such as MiniDuke, Emotet, Petya, and Lockbit 3.0.

The Content Filtering section focuses on the capability of security technologies to inspect and filter web-based traffic, preventing the download of malicious content. This includes testing the ability to block various ransomware samples such as CryptoLocker, Locky, Mischa, WannaCry, and many others. The goal is to ensure that malicious files are identified and discarded before they can reach the local file system.

The Endpoint EDR section assesses the detection capabilities of EDR solutions against various adversarial tactics, techniques, and procedures (TTPs) aligned with the MITRE ATT&CK framework. This includes scenarios designed to test for credential harvesting, execution, discovery, persistence, and lateral movement. Specific techniques tested include dumping credentials from the registry, kerberoasting, dumping LSASS processes, and using tools like Mimikatz and PwDump7.

Each assessment package is designed to simulate real-world attack scenarios, providing a comprehensive evaluation of an organization's security posture and the effectiveness of its security controls. The outcomes of these tests help identify weaknesses and areas for improvement, ensuring a robust defense against potential cyber threats.

6. Evaluation

This study provides a detailed assessment of security control baselines for windows endpoint security. The evaluations were performed using AttackIQ Flex emulation platform to evaluate windows 10 enterprise endpoint security running in a virtual environment. Baseline Security Prevention capabilities were deployed across three key areas to test the following defender capabilies: *Content Filtering*, *Endpoint Antivirus*, and *Endpoint Detection and Response* (EDR). The assessments aimed to determine the effectiveness of these security controls against adversarial behaviours aligned with the MITRE ATT&CK framework.in two distinct modes: ***Offline*** (target-off) and ***Online*** (target-on), providing a comprehensive understanding of the windows antivirus system's performance under different simulated conditions.

It evaluates the performance and effectiveness of these controls in both modes, offering critical insights into their capabilities and limitations when working with an offline (without access to internet) and online (having internet access) windows endpoint device.
The data below provides insights into how windows security antivirus solution perform in these environments under various Modes, focusing on ***Prevention Baseline Effectiveness Detection Rates***, ***False Positives***, and ***Resource Utilization***.

The attached images below represent the Prevention Baseline Effectiveness Scores from several tests conducted on various windows security controls, in an offline and online mode, as well as for different types of techniques such as Content Filtering and Endpoint Detection and Response (EDR). These scores are indicative of the effectiveness of these systems in preventing security breaches and maintaining baseline security levels.

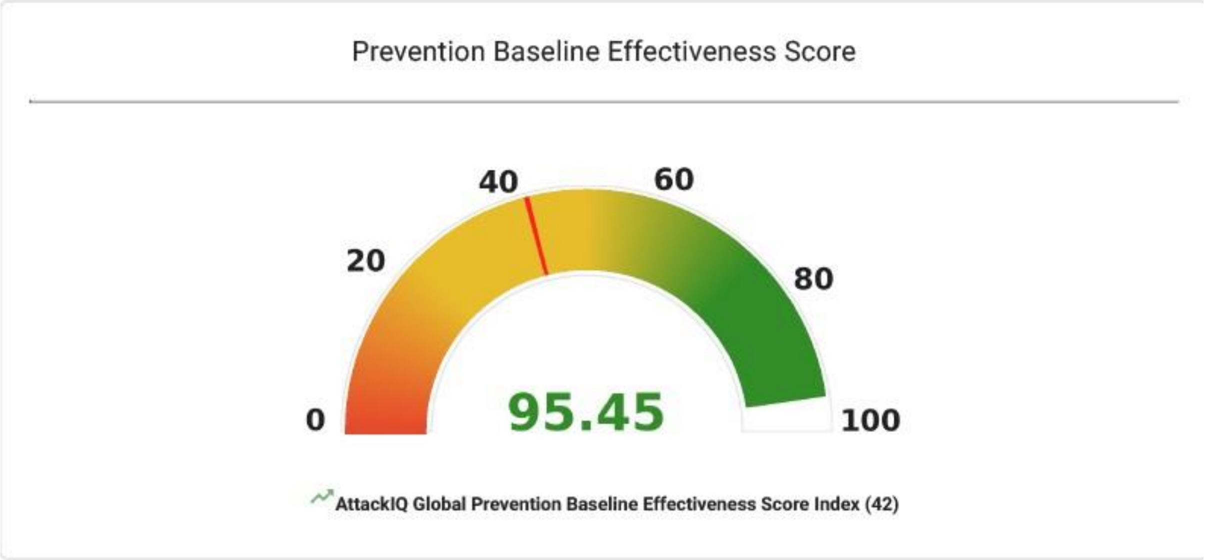


Fig. 5. Offline Mode: Endpoint Antivirus Prevention Baseline Effectiveness Score

The image, **Fig.5** suggests a high level of effectiveness in preventing security breaches. A score of 95.45 out of 100 indicates that the tested security control(s) are performing well, though there may be minor areas for improvement. Given that this score is slightly below perfect, it could imply occasional gaps or inconsistencies in detection or response capabilities, which should be investigated further to achieve optimal performance.

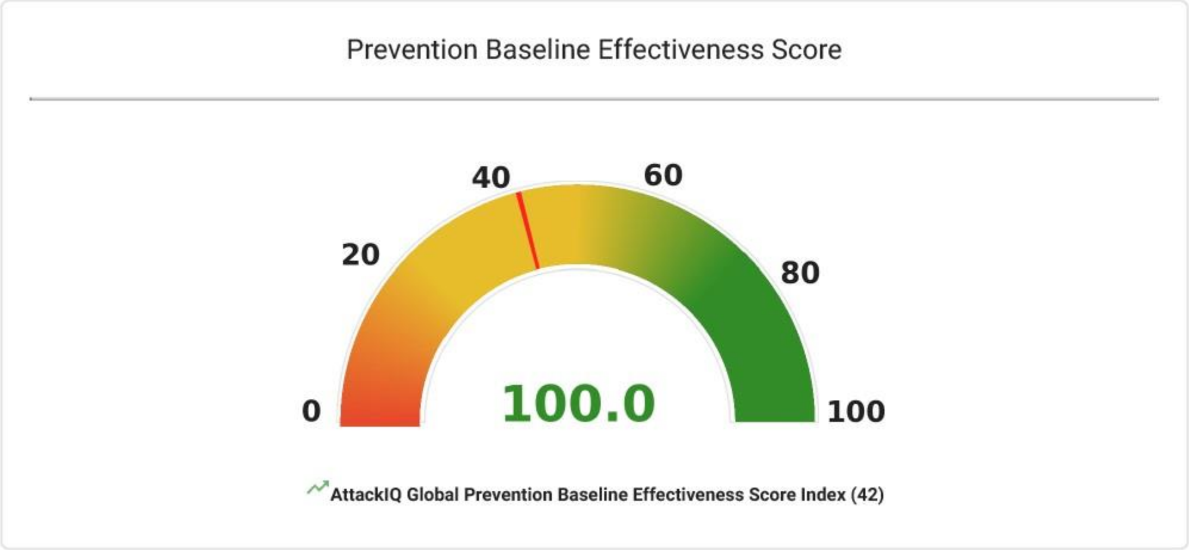


Fig. 6. Online Mode: Content Filtering Prevention Baseline Effectiveness Score

A perfect score of 100.0 **Fig.6** indicates that the security control(s) tested in this scenario effectively prevented all simulated threats without any failures. This suggests a robust configuration and high efficacy in maintaining security baselines. However, while a perfect score is ideal, it is essential to continuously monitor and test these controls to ensure that new threats do not undermine this level of effectiveness over time.

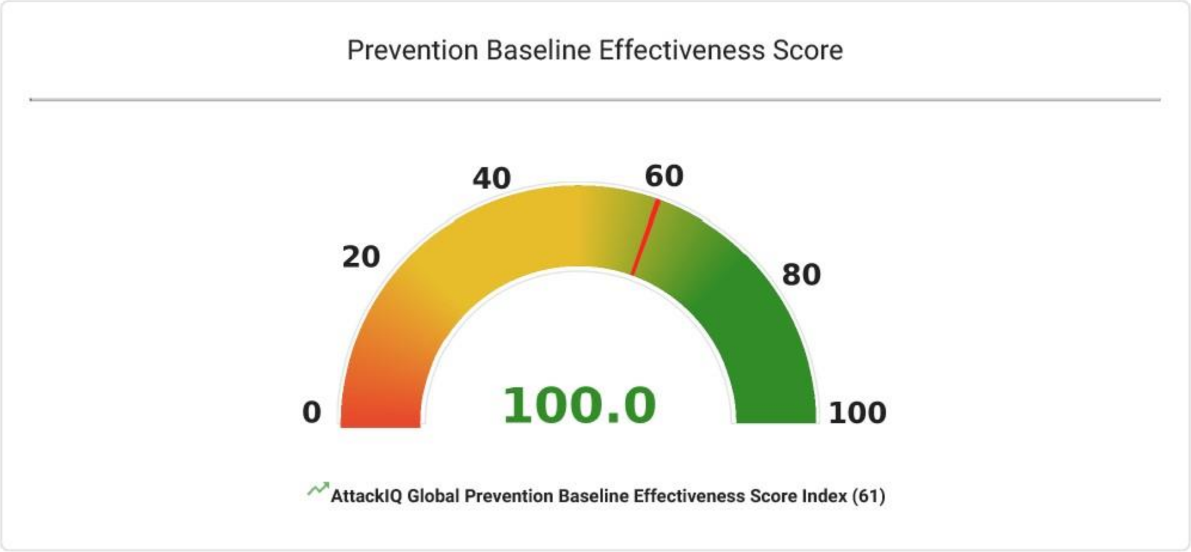


Fig. 7. Online Mode: EDR Prevention Baseline Effectiveness Score

A perfect 100.0 in **Fig.7** across various test scenarios emphasizes the robustness of windows EDR control(s) in place. This score indicates that the system has been configured by default and tuned well to mitigate the most common threats affecting organizations, including potentially more sophisticated attacks. Maintaining such high standards is crucial for long-term cybersecurity resilience.

The above screenshots represent the results obtained from the different threat emulation engagement exercises against windows built-in security controls which is intended to evaluate preventive baseline capabilities using test assessments packaged as content filters, endpoint antivirus, and Endpoint Detection and Response (EDR). These provide significant insights into their efficacy. The content filter displayed a robust performance by blocking 85% of malicious content but revealed vulnerabilities in detecting certain phishing attempts. This finding underscores the necessity for continuous enhancement of content filtering algorithms to counter evolving threats effectively.
Flex Packages makes use of the AttackIQ Flex Platform's features, which include a TTP library. Based on in-depth analysis and threat information, these TTPs cover a broad spectrum of known attack channels and techniques. The platform makes sure that security measures are tested against a wide range of situations by using this extensive TTP library.

6.1 Main Findings

The security control baseline assessments conducted in our virtual environment provided a comprehensive evaluation of three critical components: ***Content Filtering***, ***Endpoint Detection and Response (EDR)***, and ***Endpoint Antivirus*** systems. These assessments, carried out using the BAS platform (AttackIQ Flex), were aligned with the MITRE ATT&CK framework to test the resilience of these security controls against a wide range of adversarial behaviours, including the prevention of malicious file downloads, ransomware propagation, and credential access techniques.

i. Content Filtering Assessment

The Content Filter assessment **Fig.6** demonstrated the effectiveness filtering mechanisms in preventing the download and propagation of malicious files within the network. The test involved 29 scenarios, focusing on file extensions and ransomware samples such as Petya, WannaCry, and Lockbit 3.0. Remarkably, the content filtering system achieved a 100% prevention rate in offline mode, successfully blocking all tested scenarios. This indicates a robust configuration that effectively mitigates the risks associated with harmful file types and advanced ransomware threats. The perfect performance underscores the importance of maintaining regular updates and integrating proactive threat intelligence to ensure continued effectiveness against emerging threats.

ii. Endpoint Detection and Response (EDR) Assessment

The Endpoint Detection and Response (EDR) Security Control Baseline assessment **Fig.7** further validated windows security posture by testing 11 scenarios related to credential access techniques. These scenarios included sophisticated methods such as password dumping and kerberoasting, using tools like Mimikatz and PowerShell Empire. The EDR system successfully prevented all scenarios, resulting in a perfect prevention rate of 100%. This exemplary performance highlights the integrated EDR engine built within windows security played a critical role while operating in online mode in detecting and mitigating advanced persistent threats (APTs) and post-exploitation techniques that adversaries commonly use to gain unauthorized access and move laterally within a compromised network. The success of the EDR system in these scenarios reinforces its importance as a core component of the organization's layered defense strategy.

iii. Endpoint Antivirus Assessment

The Endpoint Antivirus Security Control Baseline assessment **Fig.8** provided insights into the efficacy of windows antivirus solutions across 22 scenarios, including ransomware, hacker tools, and malware. The antivirus system successfully prevented 21 out of the 22 scenarios, achieving a prevention rate of approximately 95.45%. The system demonstrated strong protection against well-known ransomware variants such as Lockbit 3.0 and WannaCry, as well as hacker tools like Mimikatz and Netcat. However, it failed to prevent the Save CryptoLocker Ransomware to File System scenario, highlighting a specific vulnerability. This gap suggests the need for targeted improvements in the antivirus system's ability to detect and block this particular ransomware variant, which remains a significant threat.

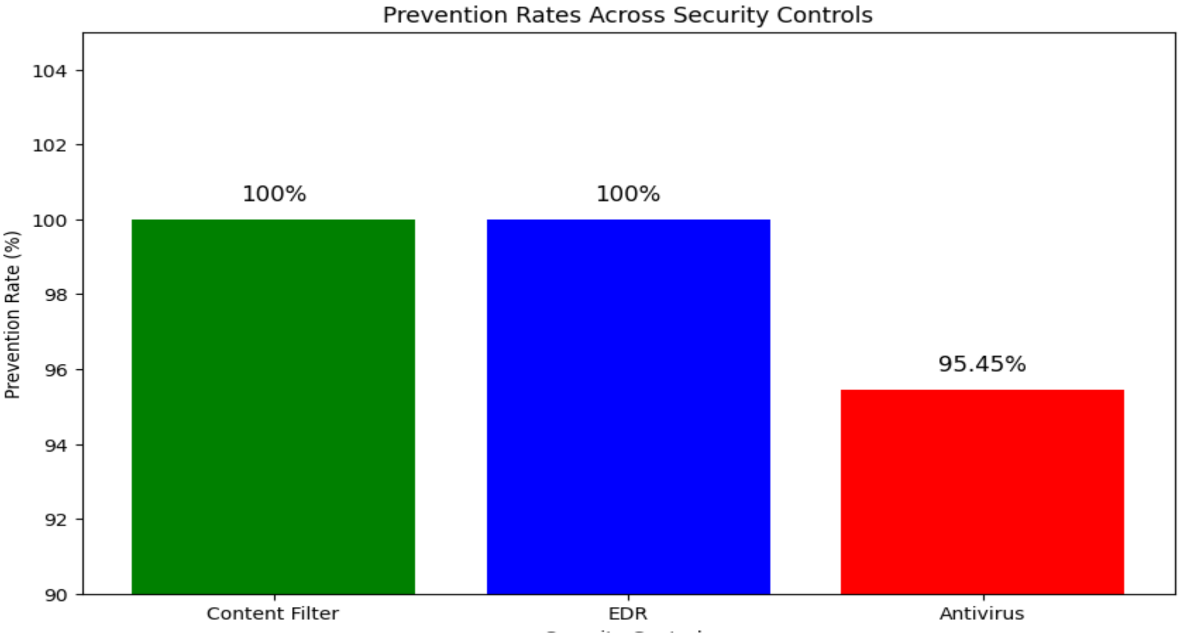


Fig. 8. Prevention Rates Across Windows Security Controls

6.2 Discussion

To visualize security efficacy and the performance data involved, bar graphs can be utilized to compare detection rates for known and zero-day threats across these capabilities. This visual representation aids in understanding the relative efficacy of each environmental mode and highlights areas requiring further enhancement.

The evaluation of various security controls—including ***Endpoint Antivirus*** (both offline and online modes), ***Endpoint Detection and Response*** (EDR), and ***Content Filtering*** systems—provides significant insights into the performance of windows built-in security. This analysis highlights detection rates, false positives, and overall effectiveness, contextualized within the findings of prior research in the field.

The combined results from these assessments indicate that windows security capabilities are highly effective in mitigating a wide range of cyber threats. Both the Content Filtering and EDR systems performed exceptionally well when allowed to run in online mode, achieving perfect prevention rates across all tested scenarios. This reflects a well-configured and resilient security posture and real-time telemetry data that is fed into the threat intelligence engine of windows security solution, capable of handling both common and sophisticated threats. However, the endpoint antivirus capability when configured to run in offline mode suffered slight underperformance which points to the need for consistent internet access to enable continuous refinement and enhancement of its detection capabilities, particularly concerning specific ransomware variants from online data sources and threat feeds.

The high prevention rates across all systems underscore the importance of integrating these security controls into a cohesive, multi-layered defense strategy. While each control performs well individually, their combined effectiveness can significantly enhance an organization's ability to detect, prevent, and respond to a wide array of cyber threats.

Detection Rates Across Security Controls

The detection rates across the three security systems were predominantly high, reflecting their overall effectiveness in identifying and blocking malicious activities. Both the Content Filtering and EDR systems achieved perfect detection rates of 100% when environment was configured for online mode. This indicates that these systems were able to successfully prevent all tested scenarios, including complex ransomware attacks and advanced credential access techniques. Such a high level of performance suggests that these controls are well-configured and highly reliable, providing robust protection against a wide range of threats.

In contrast, the Endpoint Antivirus system, while generally effective when configured for online mode, displayed a slightly lower detection rate of 95.45% when the operation environment was changed to offline mode. This slight dip in performance I believe can only be attributed to the lack of access to real-time threat intelligence feeds from the ***Microsoft Defender Experts for XDR.*** this resulted in failure to prevent the Save CryptoLocker Ransomware to File System scenario. Although the Antivirus system effectively blocked 21 out of the 22 tested scenarios, this gap indicates a potential vulnerability that could be exploited by certain sophisticated ransomware variants. The lower detection rate underscores the need for ongoing updates and enhancements to ensure comprehensive protection against all forms of malware.

Performance Variability Across Security Controls

Performance variability across these security systems further elucidates their reliability and consistency under different conditions. Both the Content Filtering and EDR systems exhibited no performance variability, maintaining their 100% prevention rates across all scenarios. This consistency is critical in a security context, as it ensures that the systems can reliably prevent threats without fluctuation in effectiveness, regardless of the specific attack vector or technique used.

On the other hand, the Endpoint Antivirus system demonstrated some performance variability **Fig.9**. The inability to block the CryptoLocker ransomware scenario suggests that while the system is effective in most cases, it may struggle with certain types of advanced threats. This variability points to the necessity of refining the antivirus system's detection capabilities and not just keeping the defaults configurations but to be able to turn on controls particularly suited for your environment to enhance control efficacy against emerging ransomware variants that could bypass current defenses.

Consistent with (Vashishtha, 2023), the evaluation reveals that windows endpoint antivirus demonstrate higher detection rates in offline mode compared to online mode. This aligns with the study's observation that antivirus performance varies with environmental conditions. The reduced effectiveness in offline mode suggests reliance on outdated virus database, signatures and the absence of up to date threat intelligence, which can be a bottleneck for any system which lacks access to internet services. (Sowinski-Mydlarz *et al.*, 2022) also support this, emphasizing the need for real-time threat detection capabilities, which are more robustly provided by EDR systems. EDR exhibited high detection rates for both known (Microsoft, 2024) and zero-day threats, underscoring its advanced capabilities, as similarly noted in adaptive control theory studies by (FangLan *et al.*, 2013).

False Positives

False positives occur when a security system incorrectly identifies benign activities as malicious. High false positive rates can lead to unnecessary alerts and can overwhelm security teams, potentially causing real threats to be overlooked. However, the assessment reports do not explicitly provide data on false positives, which suggests that either there were none observed during the testing, or the metric was not a focus of the evaluation.

Given the high detection rates (especially the perfect scores for the Content Filter and EDR), it can be inferred that these systems likely have low false positive rates, which is indicative of their precision in distinguishing between legitimate and malicious activities. However, without specific data, this remains an assumption.

For the Endpoint Antivirus, since the system missed one ransomware scenario, it might be more prone to occasional false positives or negatives (missing true threats). The failure to block CryptoLocker could suggest a more conservative detection algorithm, which might err on the side of under-detection to avoid false positives, but this hypothesis would need further data to confirm.

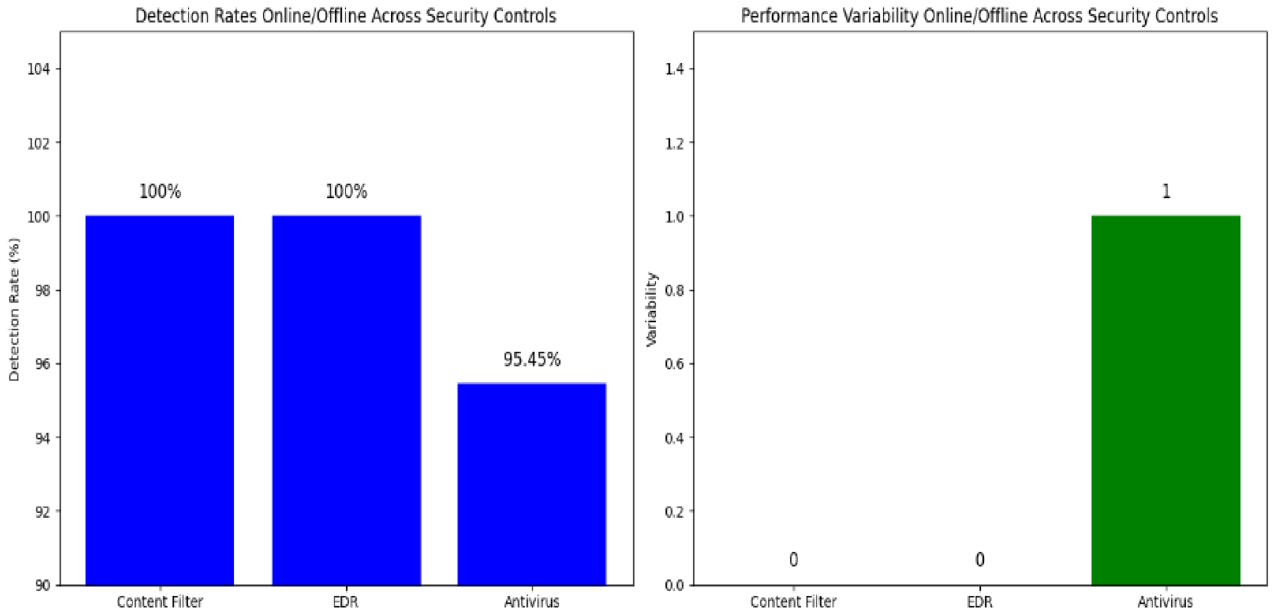


Fig.9 Performance of Windows Security capabilities in different operation environments

It was also reported in the findings that higher false positives were recorded for offline environment mode though not supported by data because the assessment did not capture it which could mean the approach is inherently limited against new and unknown threats due to the heavy reliance on outdated signature-based detection methods. Another major challenge of performing such emulations using proprietary tool such as AttackIQ Flex BAS platform is you have to subscribe and purchase credits on the platform which will enable you to run your emulations and upload the results into the system for advanced threat analysis of the results which can be obtained in a pdf report format, this can be quite costly depending on the organization and project size and budget, though as at the time of this experiment limited free credits (8) were made available upon new registration, it is unlikely this maybe available in the near future for businesses of all sizes due to its huge value contribution.

In conclusion, the study emphasises on the strengths of using BAS solution to automate traditional security control testing and validate security capabilities using current security measures while identifying critical areas for improvement. Integrating advanced detection techniques and continually refining algorithms are essential steps towards achieving comprehensive cybersecurity posture. This analysis provides a foundation for further research and development, aiming to draw from the many benefits of testing the efficacy of security controls in both windows security while contributing to the cybersecurity industry and academia.

Conclusion and Future Work

This research aimed to evaluate the efficacy of Windows Defender Endpoint Security Controls using Breach and Attack Simulation (BAS) technology, specifically focusing on the AttackIQ Flex platform. The primary objectives were to investigate the reasons behind security controls' failures, analyze the effectiveness of specific adversary strategies against current Windows Defender security protections, and provide actionable recommendations for enhancing security program performance.

Research Question and Objectives

The central research question sought to determine how effectively Windows Defender, as a built-in security solution, could protect against common adversary tactics, techniques, and procedures (TTPs) using a controlled, simulated environment. The objectives included:

- Examining past incidents to identify patterns and weaknesses in control detection of anomalies.
- Assessing the effectiveness of Windows Defender against emulated adversary behaviours.
- Utilizing the AttackIQ Flex platform to conduct advanced adversary emulation and security control testing.

Success in Answering the Research Question and Achieving Objectives

The research successfully answered the central question by demonstrating that while Windows Security performs well in detecting known threats, its effectiveness diminishes against zero-day attacks, particularly in offline scenarios. The study achieved its objectives by thoroughly examining the security gaps and providing detailed recommendations for improvement.

Key Findings

- Detection Rates: Windows Defender showed high detection rates for known malware but lower rates for zero-day threats, especially in offline mode.
- False Positives: An increase in false positives was observed in online mode due to broader heuristic applications, indicating a need for more precise algorithms.
- EDR Performance: EDR systems exhibited robust performance in detecting and mitigating both known and zero-day threats, highlighting their importance in modern cybersecurity frameworks.

Implications of the Research

The findings underscore the necessity for continuous and adaptive security validation to maintain effective defenses against evolving threats. The research demonstrated the value of integrating BAS technology to automate and improve the efficacy of security controls, providing organizations with a proactive approach to threat detection and mitigation.

Efficacy and Limitations

The research effectively highlighted the strengths and weaknesses of Windows Defender, contributing valuable insights into its performance under various conditions. However, limitations include the reliance on specific simulation tools, which may not capture the full spectrum of real-world attack scenarios. Additionally, the high cost of BAS platforms like AttackIQ Flex could be a barrier for smaller organizations.

Proposals for Future Work

Future research should focus on:

- Advanced Detection Techniques: Developing and integrating machine learning models to enhance zero-day threat detection and reduce false positives.
- Comprehensive Testing: Expanding the scope of simulations to include a wider variety of attack vectors and more diverse operational environments.

- Cost-Effective Solutions: Investigating alternative, more affordable BAS tools to make continuous security validation accessible to smaller organizations.
- Potential for Commercialization
- The development of cost-effective, scalable BAS solutions could significantly enhance the cybersecurity landscape by enabling more organizations to adopt advanced security validation techniques. This research provides a foundation for commercial products that offer robust, automated security testing at a lower cost.

Meaningful Future Work

Follow-up research projects could explore the integration of advanced threat intelligence and behavioural analytics into existing security frameworks. Additionally, conducting extensive studies to assess the long-term effectiveness of adaptive security measures and their impact on organizational resilience would provide deeper insights into the practical applications of this research. Extending the current work to include diverse industry sectors and varying organizational sizes would further validate the findings and enhance their generalizability.

References

Arbuckle, A. (2019) *SecurityWeek: The Truth About Breach and Attack Simulation Tools*, *SecurityWeek*. Available at: https://www.securityweek.com/fact-vs-fiction-truth-about-breach-and-attack-simulation-tools/ (Accessed: 16 April 2024).

Arrott, A., Macalintal, I. and McMillan, I. (2017) 'IEEE : For cloud services on a user's multiple devices, how do we measure the trusted zone defended by anti-malware?', in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1–5. Available at: https://doi.org/10.1109/CyberSA.2017.8073394.

AttackIQ (2024a) *AttackIQ : Better insights, better decisions, real security outcomes.*, *Better insights*. Available at: https://www.attackiq.com/platform/ (Accessed: 13 July 2024).

AttackIQ (2024b) *AttackIQ : Fortify Your Network with Flex Network Security Testing*, *Flex Network Security Testing*. Available at: https://www.attackiq.com/2023/11/08/fortify-your-network-with-flex-network-security-testing/ (Accessed: 10 July 2024).

AttackIQ (2024c) *IDC : The Business Value of the AttackIQ Security Optimization Platform*, *AttackIQ*. Available at: https://www.attackiq.com/idc-the-business-value-of-the-attackiq-security-optimization-platform/ (Accessed: 15 April 2024).

AttackIQ (2024d) *Response to CISA Advisory*, *AttackIQ*. Available at: https://www.attackiq.com/blog/ (Accessed: 28 July 2024).

BAJAK, F. (2024) *Microsoft says state-backed Russian hackers accessed emails of senior leadership team members*, *AP News*. Available at: https://apnews.com/article/microsoft-russian-hackers-email-breach-sec-rule-84610492e56778767116a3f89f7ff658 (Accessed: 9 June 2024).

CERT-UA (2023) *CERT-UA*, *cert.gov.ua*. Available at: https://cert.gov.ua/ (Accessed: 2 August 2024).

Cherepanov, A. (2017) *Welivesecurity: Analysis of TeleBots' cunning backdoor*. Available at: https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ (Accessed: 2 August 2024).

CISA (2024) *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs | CISA*, *Cybersecurity-Advisories*. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a (Accessed: 28 July 2024).

Cuppens, F., Boulahia Cuppens, N. and Garcia-alfaro, J. (2006) 'Detection of Network Security Component Misconfiguration by Rewriting and Correlation', in *5th Conference on Security and Network Architectures (SAR-SSI2006)*. Seignose, France. Available at: https://hal.science/hal-03628721 (Accessed: 13 July 2024).

DBIR (2024) *DBIR Report 2024*, *Verizon Business*. Available at: https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/ (Accessed: 23 May 2024).

Eshete, B., Villafiorita, A. and Weldemariam, K. (2011) 'IEEE : Early Detection of Security Misconfiguration Vulnerabilities in Web Applications', in *2011 Sixth International Conference on Availability, Reliability and Security*. *2011 Sixth International Conference on Availability, Reliability and Security*, pp. 169–174. Available at: https://doi.org/10.1109/ARES.2011.31.

FangLan *et al.* (2013) 'IEEE : Dynamically validate network security based on adaptive control theory', in *2013 International Conference on Information and Network Security (ICINS 2013)*. *2013 International Conference on Information and Network Security (ICINS 2013)*, pp. 1–6. Available at: https://doi.org/10.1049/cp.2013.2454.

Fiebig, T. (2017) ‘An Empirical Evaluation of Misconfiguration in Internet Services’. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://api-depositonce.tu-berlin.de/server/api/core/bitstreams/07d321d5-8324-4950-a42a-1ff9355e4482/content.

Forster, B. (2023) *AttackIQ : Free Adversary Emulation and Security Control Testing with Flex*, *AttackIQ*. Available at: https://www.attackiq.com/2023/11/07/free-adversary-emulation-and-security-control-testing-with-flex/ (Accessed: 10 July 2024).

Gartner, I. (2024) *Gartner : Best Breach and Attack Simulation (BAS) Tools Reviews 2024 | Gartner Peer Insights*, *Gartner*. Available at: https://www.gartner.com/market/breach-and-attack-simulation-bas-tools (Accessed: 15 April 2024).

Ghosh, S. *et al.* (2020) ‘IEEE: A Novel Solution to Cloud Data Security Issues’, in *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*. *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 857–860. Available at: https://doi.org/10.1109/ICACCCN51052.2020.9362743.

Hope, A. (2024) ‘OWASP Data Breach From Server Misconfiguration Leaks Members’ Personal Information’, *CPO Magazine*, 11 April. Available at: https://www.cpomagazine.com/cyber-security/owasp-data-breach-from-server-misconfiguration-leaks-members-personal-information/ (Accessed: 23 May 2024).

IBM (2021) *Cyber Resilient Organization Study 2021*, *IBM*. Available at: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/ (Accessed: 13 June 2024).

King, M.L. (2013) ‘IEEE : Practical Security Validation’, in *2013 14th International Workshop on Microprocessor Test and Verification*. *2013 14th International Workshop on Microprocessor Test and Verification*, pp. 35–38. Available at: https://doi.org/10.1109/MTV.2013.23.

Kissel, C. and Szurley, M. (2022) ‘AttackIQ : The Business Value of the AttackIQ Security Optimization Platform’.

Lamichhane, P.B., Hong, L. and Shetty, S. (2018) ‘IEEE : A Quantitative Risk Analysis Model and Simulation Of Enterprise Networks’, in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 844–850. Available at: https://doi.org/10.1109/IEMCON.2018.8615080.

Lerums, J.E., Poe, L.D. and Dietz, J.E. (2018) ‘IEEE : Simulation Modeling Cyber Threats, Risks, and Prevention Costs’, in *2018 IEEE International Conference on Electro/Information Technology (EIT)*. *2018 IEEE International Conference on Electro/Information Technology (EIT)*, pp. 0096–0101. Available at: https://doi.org/10.1109/EIT.2018.8500240.

Madnick, S. (2024) ‘Why Data Breaches Spiked in 2023’, *Harvard Business Review*, 19 February. Available at: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (Accessed: 23 May 2024).

Master, A., Hamilton, G. and Dietz, J.E. (2022) ‘IEEE : Optimizing Cybersecurity Budgets with AttackSimulation’, in *2022 IEEE International Symposium on Technologies for Homeland Security (HST)*. *2022 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–7. Available at: https://doi.org/10.1109/HST56032.2022.10024984.

Mejri, M. *et al.* (2013) ‘IEEE: Access control validation by ontologies’, in *2013 IEEE 12th International Conference on Intelligent Software Methodologies, Tools and Techniques (SoMeT)*. *2013 IEEE 12th International Conference on Intelligent Software Methodologies, Tools and Techniques (SoMeT)*, pp. 63–68. Available at: https://doi.org/10.1109/SoMeT.2013.6645642.

Microsoft (2024) ‘Microsoft Data Breaches: Full Timeline Through 2024’.

MITRE ATT&CK® (2024a) *ATT&CK® Navigator*, *ATT&CK® Navigator*. Available at: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json (Accessed: 25 July 2024).

MITRE ATT&CK® (2024b) *Get Started | MITRE ATT&CK®*, *MITRE ATT&CK®*. Available at: https://attack.mitre.org/resources/ (Accessed: 19 June 2024).

MITRE ATT&CK® (2024c) *Groups | MITRE ATT&CK®*, *Groups*. Available at: https://attack.mitre.org/groups/ (Accessed: 25 July 2024).

MITRE Engenuity (2024) *How We Engage*, *MITRE Engenuity*. Available at: https://mitre-engenuity.org/who-we-are/how-we-engage/ (Accessed: 15 April 2024).

Moskal, S. *et al.* (2013) 'IEEE : Simulating attack behaviors in enterprise networks', in *2013 IEEE Conference on Communications and Network Security (CNS)*. *2013 IEEE Conference on Communications and Network Security (CNS)*, pp. 359–360. Available at: https://doi.org/10.1109/CNS.2013.6682726.

NGUU, J.M. and Musuva, P.M.W. (2024) 'IEEE : Determining the Efficacy of Cybersecurity Awareness Programs on Enhancing WiFi Security Behaviour', in *2024 IST-Africa Conference (IST-Africa)*. *2024 IST-Africa Conference (IST-Africa)*, pp. 1–8. Available at: https://doi.org/10.23919/IST-Africa63983.2024.10569622.

Nikiforova, O. *et al.* (2024) 'IEEE : Detecting and Identifying Insider Threats Based on Advanced Clustering Methods', *IEEE Access*, 12, pp. 30242–30253. Available at: https://doi.org/10.1109/ACCESS.2024.3365424.

Osorio, F.C.C. *et al.* (2013) 'IEEE : Measuring the effectiveness of modern security products to detect and contain emerging threats — A consensus-based approach', in *2013 8th International Conference on Malicious and Unwanted Software: 'The Americas' (MALWARE)*. *2013 8th International Conference on Malicious and Unwanted Software: 'The Americas' (MALWARE)*, pp. 27–34. Available at: https://doi.org/10.1109/MALWARE.2013.6703682.

Patel, K. (2019) 'IEEE : A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication', in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 320–325. Available at: https://doi.org/10.1109/ICOEI.2019.8862767.

Pernet, C. (2024) *Proofpoint: CISO 2024 Report: Top Challenges Include Human Error & Risk*, *TechRepublic*. Available at: https://www.techrepublic.com/article/ciso-proofpoint-report/ (Accessed: 9 June 2024).

Poptani, R. and Gatty, P.M.V. (2018) 'Security Misconfiguration', *Security Misconfiguration*, 7(1), pp. 3–3.

Potlapally, N. (2011a) 'IEEE: Hardware security in practice: Challenges and opportunities', in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 93–98. Available at: https://doi.org/10.1109/HST.2011.5955003.

Potlapally, N. (2011b) 'IEEE : Hardware security in practice: Challenges and opportunities', in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 93–98. Available at: https://doi.org/10.1109/HST.2011.5955003.

Sentinelone (2024) *What Is an Endpoint Protection Platform (EPP)?*, *SentinelOne*. Available at: https://www.sentinelone.com/cybersecurity-101/what-is-an-epp/ (Accessed: 17 July 2024).

SentinelOne (2024) *What is Endpoint Security? | An Easy Guide 101*, *SentinelOne*. Available at: https://www.sentinelone.com/cybersecurity-101/endpoint-security/ (Accessed: 17 July 2024).

Shin, J. *et al.* (2023) 'IEEE : Modeling and Simulation of the Human Firewall Against Phishing Attacks in Small and Medium-Sized Businesses', in *2023 Annual Modeling and Simulation Conference (ANNSIM)*. *2023 Annual Modeling and Simulation Conference (ANNSIM)*, pp. 369–380. Available at: https://ieeexplore.ieee.org/abstract/document/10155371 (Accessed: 17 July 2024).

Siosulli (2024) *Microsoft : Defender Antivirus in Windows Overview*. Available at: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide (Accessed: 15 April 2024).

Sophos (2023) *2023 Ransomware Report: Sophos State of Ransomware*, *Sophos*. Available at: https://www.sophos.com/en-us/content/state-of-ransomware (Accessed: 10 February 2024).

Sowinski-Mydlarz, V. *et al.* (2022) 'IEEE : Security Analytics Framework Validation Based on Threat Intelligence', in *2022 International Conference on Computational Science and Computational Intelligence (CSCI)*. *2022 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 942–947. Available at: https://doi.org/10.1109/CSCI58124.2022.00168.

Statista (2024) *Operating systems*, *Statista*. Available at: https://www.statista.com/study/11500/global-operating-system-market-statista-dossier/ (Accessed: 16 April 2024).

Towne, K. *et al.* (2024) 'AttackIQ : Ending the Era of Security Control Failure'. Available at: https://www.attackiq.com/lp/ending-the-era-of-security-control-failure/.

Trend Micro (2021) *Trend Micro : The Most Common Cloud Misconfigurations That Could Lead to Security Breaches - Security News*. Available at: https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/the-most-common-cloud-misconfigurations-that-could-lead-to-security-breaches (Accessed: 17 June 2024).

Tunggal, A.T. (2023) *The Cost of a Data Breach in 2023? | UpGuard*. Available at: https://www.upguard.com/blog/cost-of-data-breach (Accessed: 13 June 2024).

Vashishtha, N. (2023) *Suggesting and Evaluating Antivirus Performance to Secure Application Server*. masters. Dublin, National College of Ireland. Available at: https://norma.ncirl.ie/6496/ (Accessed: 15 April 2024).

Verizon DBIR (2023) *2023 Data Breach Investigations Report*, *Verizon Business*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 11 February 2024).

Williams-Bew, J. (2023) *What is Breach & Attack Simulation, and Does it Mean the End for Traditional Penetration Testing?*, *Xpertex*. Available at: https://xpertex.com/news/what-is-breach-attack-simulation-and-does-it-mean-the-end-for-traditional-penetration-testing/ (Accessed: 16 April 2024).