ADVANCED EDR TEST 2023

Red Team Testing and Certification by AV-TEST

Date of the test report: December 07, 2023 (version 1.00)

Bitdefender's Endpoint Security Tools

Phone +49 391 6075460 * E-Mail info@av-test.com * Web https://www.av-test.org

Executive Summary

AV-TEST conducted a rigorous assessment of Bitdefender's Endpoint Security Tools with its Endpoint Detection and Response (EDR) capabilities between November 2022 and January 2023. The evaluation was designed to measure the effectiveness of Bitdefender's EDR in identifying and thwarting malicious activities typically associated with advanced persistent threats (APTs). The study involved a series of red-team attacks simulated in two distinct detection scenarios, each encompassing various tactics and techniques that an attacker may employ.

Scenario 1 - Hafnium-Style Unauthorized Data Exfiltration: Assess your network's readiness against a simulated cyber threat inspired by Hafnium, a notorious state-sponsored actor. This scenario replicates Hafnium's tactics, involving spear-phishing, lateral movement, data exfiltration, and evasion techniques. It aims to evaluate your organization's ability to detect, respond to, and mitigate sophisticated attacks, providing valuable insights into your cybersecurity resilience.

Scenario 2 - Lazarus-Style Unauthorized Data Access and Lateral Movement: Evaluate your system's defenses against a simulated cyber threat reminiscent of the Lazarus group, a nation-state-sponsored threat actor known for advanced attacks. This scenario involves phishing, data collection, payload execution, privilege escalation, data exfiltration, mirroring Lazarus's tactics. It assesses your system's security posture and incident response capabilities against sophisticated threats, helping you identify vulnerabilities and enhance your defenses.

In Scenario 1, designed to emulate Hafnium's tactics, Bitdefender demonstrated exceptional coverage by successfully detecting all 29 techniques across 14 steps. The product excelled in identifying techniques through a variety of detection types, including telemetry, general detections, and tactic/technique detections. This flawless coverage highlighted Bitdefender's robust monitoring and detection capabilities, solidifying its effectiveness against complex cyber threats.

Bitdefender further distinguished itself in the quality of detection assessment, achieving the highest level of detection quality. The product consistently identified all 29 techniques using tactic or technique detections, offering detailed and actionable insights into the attacker's tactics and techniques. This outstanding performance underscored Bitdefender's ability to recognize and respond effectively to sophisticated cyber threats.

In Scenario 2, inspired by the Lazarus group, Bitdefender demonstrated commendable coverage by successfully detecting 29 out of 30 techniques across 5 steps. The single missed detection related to "Exfiltration over the C2 Channel (T1041)" in step 2. This strong coverage highlighted Bitdefender's capacity to monitor and detect a significant majority of techniques used during the scenario, reaffirming its robust defense against a wide range of cyber threats.

Bitdefender's quality of detection in Scenario 2 was exceptional. It successfully identified 29 out of 30 techniques with tactic or technique detections, indicating a high level of precision and depth. Although there was a single missed detection related to exfiltration over a C2 channel, the remaining 29 detections provided detailed and actionable information about the attacker's tactics and techniques.

In conclusion, Bitdefender's EDR solution demonstrated impressive coverage and consistently delivered high-quality detections in both scenarios. These results highlight Bitdefender's capability to effectively safeguard organizations against complex and evolving cyber threats, underscoring its value as a robust security solution.

With the remarkable results obtained, the product is now eligible for the prestigious AV-TEST Approved Endpoint Detection and Response Certification, a testament to its exceptional capabilities and commitment to advanced cybersecurity.

Introduction to EDR products

Endpoint Detection and Response

Endpoint Detection and Response (EDR) solutions are a category of security software specifically engineered to monitor endpoint devices like laptops, workstations, and mobile devices for indications of malicious activities and security threats. These solutions are essential for detecting and countering cyber threats such as malware, ransomware, and phishing attacks that are aimed at exploiting vulnerabilities in endpoint devices. EDR solutions offer organizations the capability to continuously scrutinize the behavior and state of endpoint devices, thereby sending alerts to IT personnel for suspicious activities that warrant investigation. These tools not only facilitate immediate threat detection but also provide a comprehensive analysis of the nature and extent of the threat, aiding in the formulation of robust response and recovery strategies. Additionally, EDR solutions equip organizations with critical intelligence on the modus operandi of attackers, thus enabling them to fortify their overall security infrastructure.

Overview of Bitdefender Endpoint Security Tools

Bitdefender Endpoint Security Tools is an Endpoint Detection and Response (EDR) solution designed to enhance the security posture of enterprise networks by providing granular visibility and control over endpoints. Unlike traditional cybersecurity solutions that focus solely on perimeter defense, Bitdefender's EDR aims to secure the internal landscape of an organization, making it particularly effective against advanced persistent threats (APTs) that often bypass initial security layers.

At the core of Bitdefender's EDR capabilities is its multi-layered analytics engine, which combines Artificial Intelligence/Machine Learning (AI/ML) algorithms with real-time threat intelligence feeds. This fusion of technologies enables the solution to accurately identify a wide range of threat tactics and techniques, from initial access attempts to complex lateral movements within the network.

The system is especially beneficial for threat hunters and IT security teams who require a dynamic and responsive toolset to sift through suspicious activities and isolate advanced threats. Bitdefender's EDR provides automated playbooks and customizable response actions, allowing for immediate disruption and denial of unauthorized activities. These features make it a comprehensive and powerful tool for organizations looking to bolster their internal security measures and protect against sophisticated cyber threats.

Test Scenarios

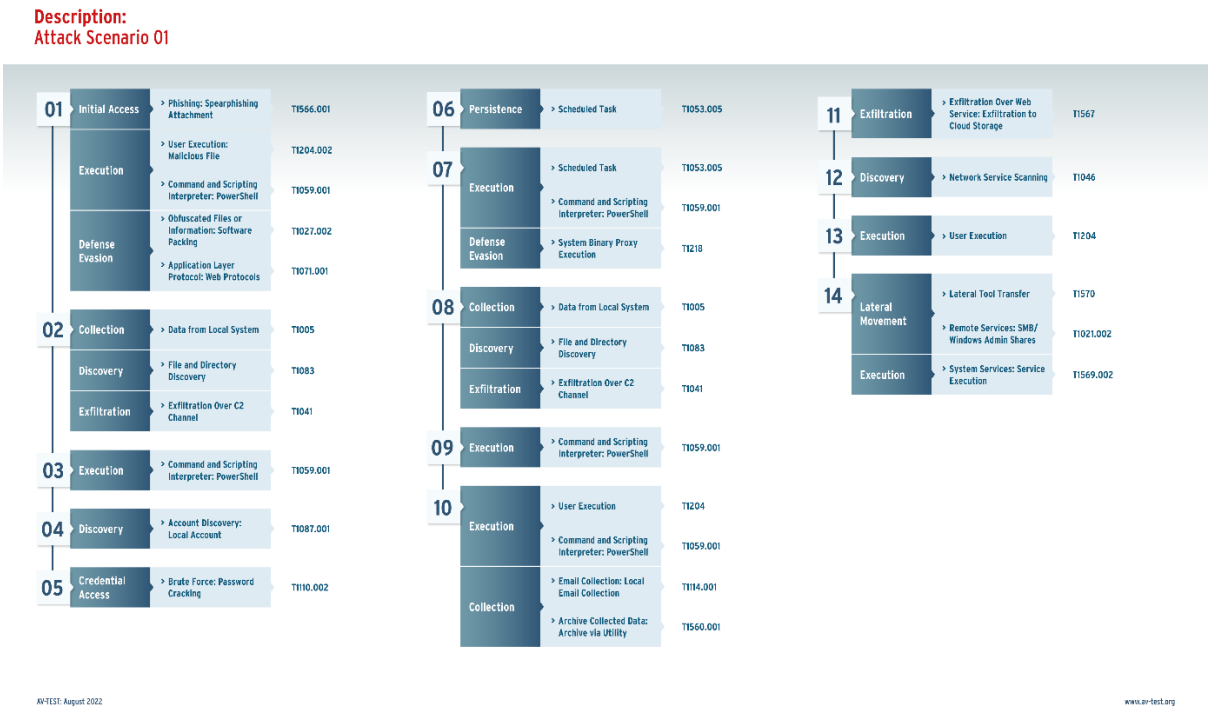
Scenario 1: Hafnium-Style Unauthorized Data Exfiltration - Assess the network's resilience against a simulated cyber threat inspired by Hafnium's tactics

Hafnium, a state-sponsored cyber threat group, gained infamy for exploiting Microsoft Exchange vulnerabilities in 2021 to infiltrate organizations worldwide. This scenario mirrors their tactics to evaluate your network's preparedness.

Scenario Description

- Initial Setup: Launch a spear-phishing campaign, sending a malicious Word document to a user on VM1, initiating the attack. Covenant Listener and Grunt are employed for further operations.
- Data Collection: Covenant's Grunt is used to gather system information via commands like WhoAmI and Seatbelt.
- Reverse Shell Setup: A second Covenant session on the host sets up a reverse shell for attacker access.
- Admin Privilege Escalation: The attacker leverages Brute Force techniques to crack admin passwords.
- Data Exfiltration: Sensitive data is exfiltrated to Dropbox.
- Lateral Movement: PsExec is employed to move laterally to VM2.

This scenario incorporates tactics such as spear phishing, user execution, PowerShell, system binary proxy execution, brute force, and data exfiltration over a web service, mirroring Hafnium's methods. It aims to assess your network's defense capabilities and incident response readiness against similar advanced threats.



Scenario 2: Lazarus-Style Unauthorized Data Access and Lateral Movement - Evaluate the system's resilience against a simulated cyber threat inspired by the Lazarus group

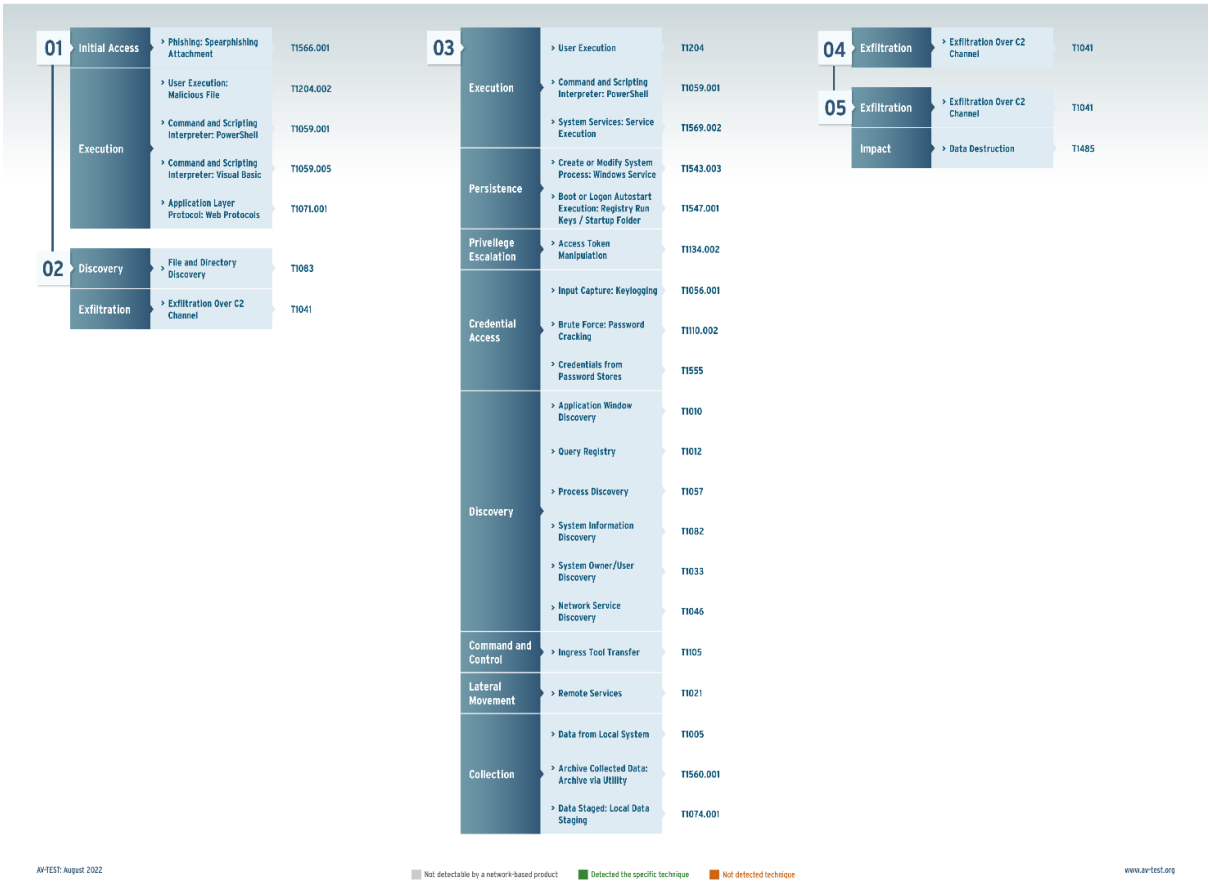
Lazarus is a prominent threat group associated with nation-state-sponsored cyberattacks, known for sophisticated and persistent campaigns. This scenario replicates their techniques to assess your system's security posture.

Scenario Description

- Phishing Setup: Initiate the attack by sending a phishing email containing a malicious Word document to a user on VM1.
- Initial Data Collection: Use Covenant's Grunt to perform initial data collection with commands like WhoAmI, ListDirectory, and Screenshot.
- Payload Execution: Execute a PowerShell command to download and run a script, enabling various tasks, including keylogging, on the compromised system.
- Admin Credentials: Set up a new Grunt session to uncover the admin username and password.
- User Interaction: Interact with VM1 to generate data for the keylog file.
- Data Exfiltration: Download a data archive from both VMs (Virtual Machine), simulating unauthorized data access.
- Data Destruction: Execute a script to destroy specific data types on VM1, mimicking the impact of an advanced threat.

This scenario encompasses a range of tactics and techniques, including spear phishing attachments, user execution, PowerShell and Visual Basic scripting, discovery of files and processes, keylogging, password cracking, privilege escalation, persistence through Windows services and registry run keys, lateral movement, exfiltration over a command and control channel, and data destruction. It assesses your system's ability to defend against and respond to complex threats, mirroring the Lazarus group's tactics and objectives.

Description:
Attack Scenario 02



Test Results

Introduction

The objective of this test is to comprehensively evaluate the effectiveness of the EDR (Endpoint Detection and Response) product in safeguarding against simulated cyber threats. In this evaluation, we conducted two scenarios inspired by real-world threat actors, Hafnium and Lazarus, to assess the EDR's capabilities in detecting and responding to sophisticated attacks. Our assessment not only focuses on coverage, i.e., the extent to which the EDR detected any suspicious activities at each step but also delves into the quality of these detections.

Coverage Assessment

For each step executed in the test scenarios, we diligently assessed whether the EDR product registered any form of detection, ranging from basic telemetry notifications to more advanced tactic or technique detections. This meticulous evaluation provides valuable insights into the EDR's ability to monitor and respond to various stages of an attack. The coverage metric highlights how effectively the EDR tracks an attacker's actions throughout the attack lifecycle.

Quality of Detection Assessment

In addition to measuring coverage, we also assessed the quality of the EDR detections. It is imperative to differentiate between different types of detections, as not all are equally valuable in terms of threat mitigation. For instance, while telemetry-based detections provide valuable information about suspicious activities, detecting the specific technique used by the attacker is far more actionable. Therefore, our evaluation delves into the granularity and context provided by each detection. We assess whether the EDR identifies and reports on the tactics and techniques employed by the attacker, enabling security teams to make informed decisions regarding threat containment and response.

By combining these two dimensions, coverage and quality of detection, our analysis provides a comprehensive view of the EDR product's overall effectiveness in defending against advanced threats. This information empowers organizations to make informed decisions about their cybersecurity posture and make improvements where necessary to enhance their security resilience.

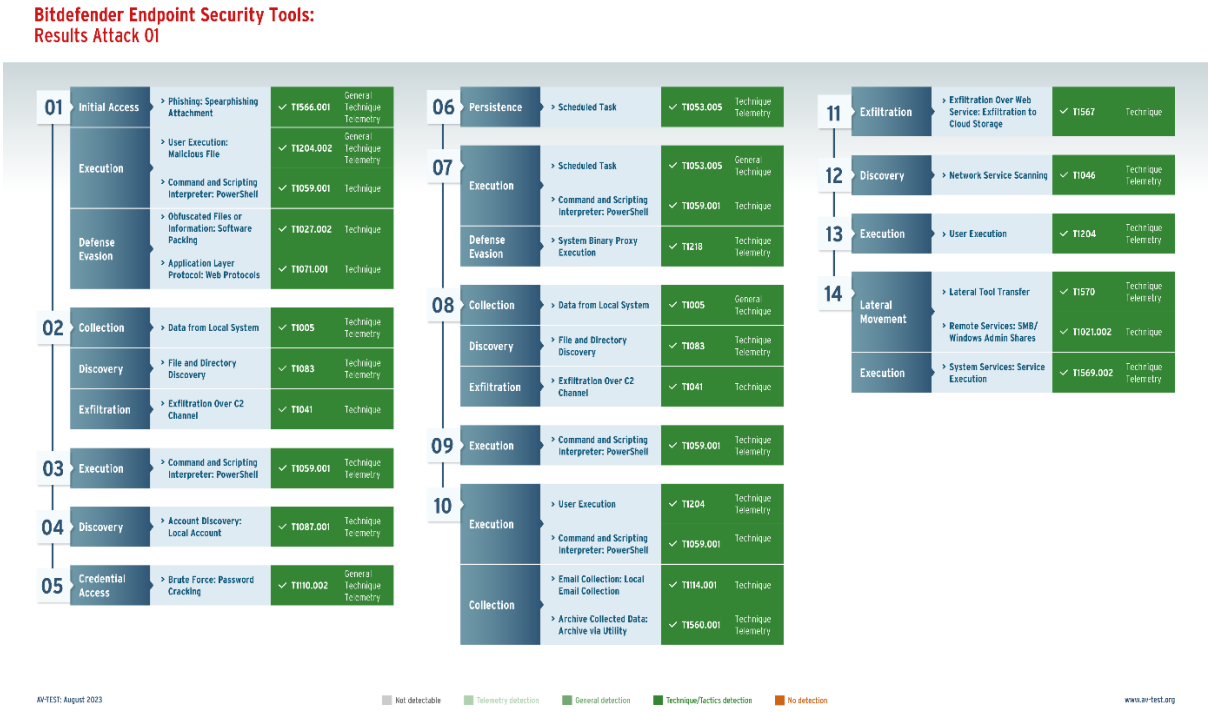
Test Results Analysis

In our rigorous evaluation of Bitdefender's Endpoint Detection and Response (EDR) solution, we explored its effectiveness in safeguarding organizations against sophisticated cyber threats. The test encompassed two distinct scenarios inspired by real-world threat actors, Hafnium and Lazarus. Our assessment focused on two critical dimensions: coverage and the quality of detection.

In this section, we present a comprehensive analysis of the test results for both Scenario 1 and Scenario 2. These findings shed light on Bitdefender's performance, strengths, and areas for improvement in defending against advanced cyber threats, providing valuable insights for organizations seeking robust cybersecurity solutions.

Scenario 1: Hafnium-Style Unauthorized Data Exfiltration - Assess the network's resilience against a simulated cyber threat inspired by Hafnium's tactics

The following graphic illustrates Bitdefender's results for each step and technique, including the type of detection employed by Bitdefender in each case.



Coverage Assessment

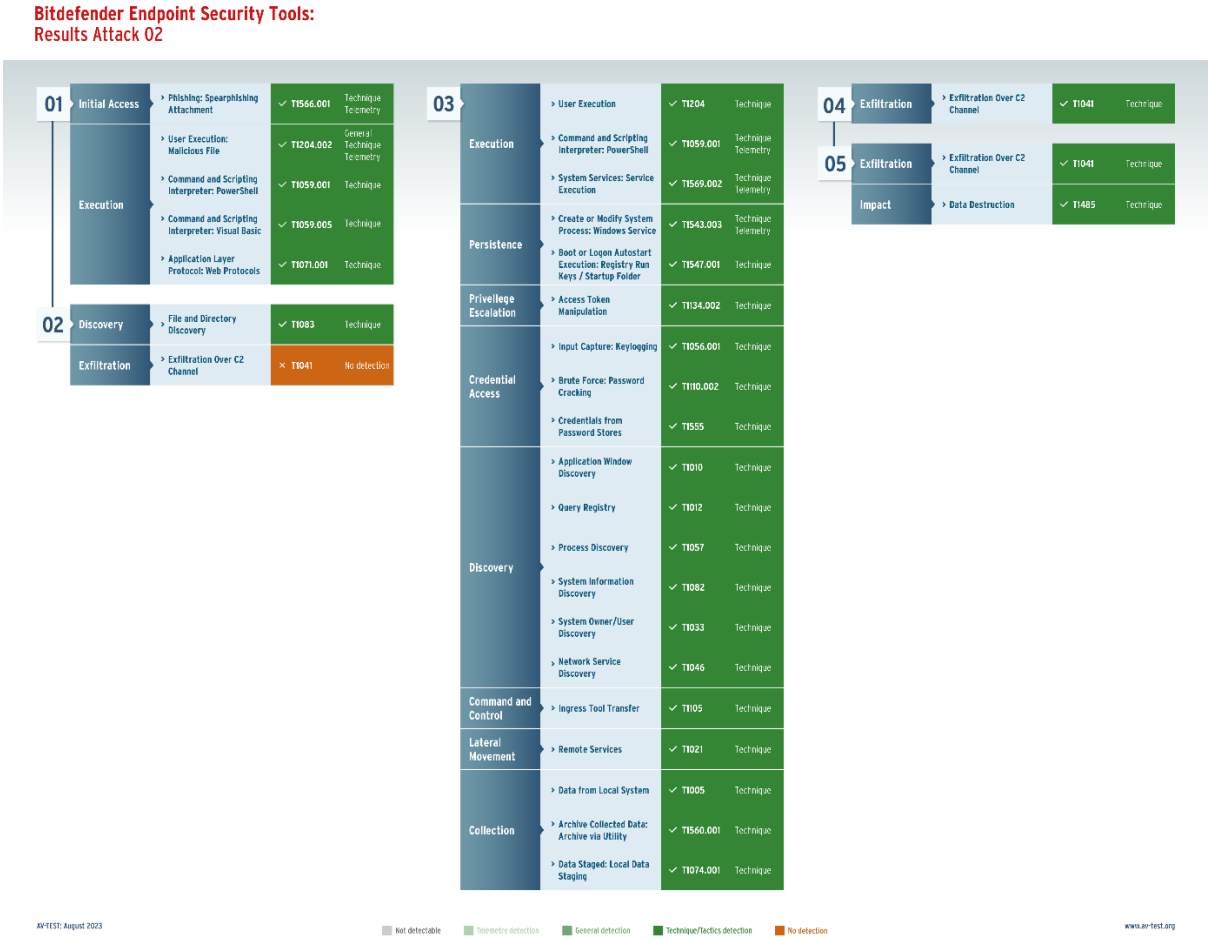
In Scenario 1, which encompasses 14 steps involving a total of 29 techniques, Bitdefender achieved exceptional coverage by successfully detecting all 29 techniques. The product demonstrated its ability to identify these techniques through various types of detections, including telemetry, general detections, and tactic/technique detections. This perfect coverage underscores Bitdefender's comprehensive monitoring and detection capabilities in safeguarding against complex cyber threats.

Quality of Detection Assessment

Bitdefender achieved the highest level of detection quality in Scenario 1, successfully identifying all 29 techniques with tactic or technique detections. This exceptional performance signifies Bitdefender's capacity to not only provide comprehensive coverage but also to deliver detailed and actionable information about the specific tactics and techniques employed by the attacker. Bitdefender's ability to consistently detect and report on these techniques demonstrates its effectiveness in recognizing and responding to sophisticated cyber threats.

Scenario 2: Lazarus-Style Unauthorized Data Access and Lateral Movement - Evaluate the system's resilience against a simulated cyber threat inspired by the Lazarus group

The following graphic illustrates Bitdefender's results for each step and technique, including the type of detection employed by Bitdefender in each case.



Coverage Assessment

In Scenario 2, which includes 5 steps and a total of 30 techniques, Bitdefender exhibited a commendable level of coverage by detecting 29 out of the 30 techniques. The single missed detection was related to "Exfiltration Over C2 Channel (T1041)" in step 6. This strong coverage highlights Bitdefender's capability to effectively monitor and detect a significant majority of the techniques employed during the scenario, demonstrating its robust defense against a wide array of cyber threats.

Quality of Detection Assessment

Bitdefender demonstrated exceptional quality of detection in Scenario 2, successfully identifying 29 out of 30 techniques with Tactic or Technique detections. These detections, while nearly perfect, indicated a single missed detection in step 2, specifically related to "Exfiltration over the C2 Channel (T1041)." Nonetheless, the 29 detections achieved in this scenario were all of the highest quality, highlighting Bitdefender's capacity to provide detailed and actionable information about the majority of tactics and techniques employed by the attacker. This performance underscores Bitdefender's effectiveness in recognizing and responding to complex cyber threats throughout the scenario.

Test Results Summary

Bitdefender's Endpoint Detection and Response (EDR) solution exhibited exceptional performance in our comprehensive evaluation. Across two challenging scenarios inspired by real-world threat actors, Bitdefender demonstrated outstanding coverage, detecting a vast majority of techniques, and maintained consistently high-quality detections, offering actionable insights. These results underscore Bitdefender's effectiveness in protecting organizations against advanced cyber threats and affirm its value as a robust security solution.