EDR Test

Testing by AV-TEST

Date of the test report: February 26th, 2026

ADVANCED EDR TEST 2025 Red Team Testing and Certification by the AV-TEST Institute

Padvish XDR

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Executive Summary

AV-TEST performed an extensive evaluation of Padvish XDR, concentrating on its Endpoint Detection and Response (EDR) capabilities, in November 2025. The goal was to measure the product's effectiveness in identifying and counteracting threats typically associated with advanced persistent threats (APTs). The assessment included comprehensive testing scenarios that emulated three different attack patterns based on the Kematian-Stealer, Bizfum-Stealer, and Helldown-Ransomware, each showcasing a variety of tactics and techniques used by sophisticated attackers.

Scenario 1 - Kematian-Stealer:
The first scenario involves a complex cyber espionage attack utilising PowerShell and extensive defence evasion. Progressing from an initial spearphishing attachment to comprehensive data collection and exfiltration, Padvish XDR demonstrated outstanding visibility. The product accurately detected critical stages like malicious file execution, command obfuscation, and privilege escalation via UAC bypass. Although explicit technique-level alerts were primarily replaced by telemetry for the final data archiving and exfiltration steps, high-quality detections for the preceding access and evasion phases provided the context needed to successfully track this evasive, multi-stage attack.

Scenario 2 – Bizfum Stealer:
This scenario replicates a targeted ransomware attack utilising phishing, defence evasion, and destructive payloads. Padvish XDR performed exceptionally well, detecting malicious executions, command obfuscation, and suspicious network communications. Critical impacts like data encryption, internal defacement, and attempts to inhibit system recovery were successfully flagged. The initial spearphishing attachment and complex sandbox evasions triggered comprehensive technique-level alerts. Although some final steps produced broader tactic-level warnings, the product maintained outstanding visibility into the primary attack vectors throughout.

Scenario 3 – Helldown Ransomware Emulation:
The final scenario emulates an advanced persistent threat, a modular attack using extensive system discovery, complex persistence, and evasion techniques to bypass standard detection. Padvish XDR successfully captured the initial spearphishing attachment and identified key subsequent phases, including malicious file execution, providing deep visibility into the later stages of lateral movement via RDP across the network. By explicitly flagging advanced manoeuvres such as OS credential dumping, privilege escalation, and COM hijacking, alongside monitoring automated system discovery activities and the impairment of security tools, the solution demonstrates a high degree of resilience.

Based on the findings across the simulated scenarios, including the cyber espionage, targeted ransomware, and advanced persistent threat emulations, Padvish XDR has demonstrated outstanding detection and visibility. The solution consistently identified critical attack vectors, from malicious file executions to sophisticated lateral movement and system impact activities. Consequently, the product has earned the prestigious AV-TEST Approved Advanced Endpoint Detection and Response (A2EDR) certification, signifying it as a trustworthy and effective solution in the field of cybersecurity.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Report Content

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

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 organisations the capability to continuously scrutinise the behaviour 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 organisations with critical intelligence on the modus operandi of attackers, thus enabling them to fortify their overall security infrastructure.

Overview Padvish XDR

Padvish XDR is a comprehensive Endpoint Detection and Response (EDR) solution designed to strengthen enterprise security by delivering continuous visibility, advanced behavioral detection, and proactive control across endpoints. The platform is engineered to address sophisticated and targeted cyber threats that increasingly bypass traditional perimeter-focused defenses.

At the core of Padvish XDR is its advanced protection engine, evaluated against zero-day malware and targeted attack simulations. By leveraging behavioral analysis and multi-layered detection mechanisms, the solution is capable of identifying complex attack techniques, including phishing-based initial access, privilege escalation, lateral movement, credential theft, and data exfiltration activities.

Padvish XDR provides centralized management capabilities that enable security teams to deploy, configure, investigate, and respond to threats efficiently across distributed enterprise environments. Its detection and response functions allow organizations to trace full attack chains—from initial execution and persistence mechanisms to final impact such as ransomware encryption—offering clear visibility into adversary behavior.

The solution is designed to support modern enterprise infrastructures, including endpoints running Windows 11, and delivers actionable insights that assist security teams in enforcing policies and mitigating advanced threats in real time. Through its comprehensive monitoring and response capabilities, Padvish XDR serves as a robust platform for organizations seeking to enhance resilience against complex and targeted cyber attacks.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Test Scenarios

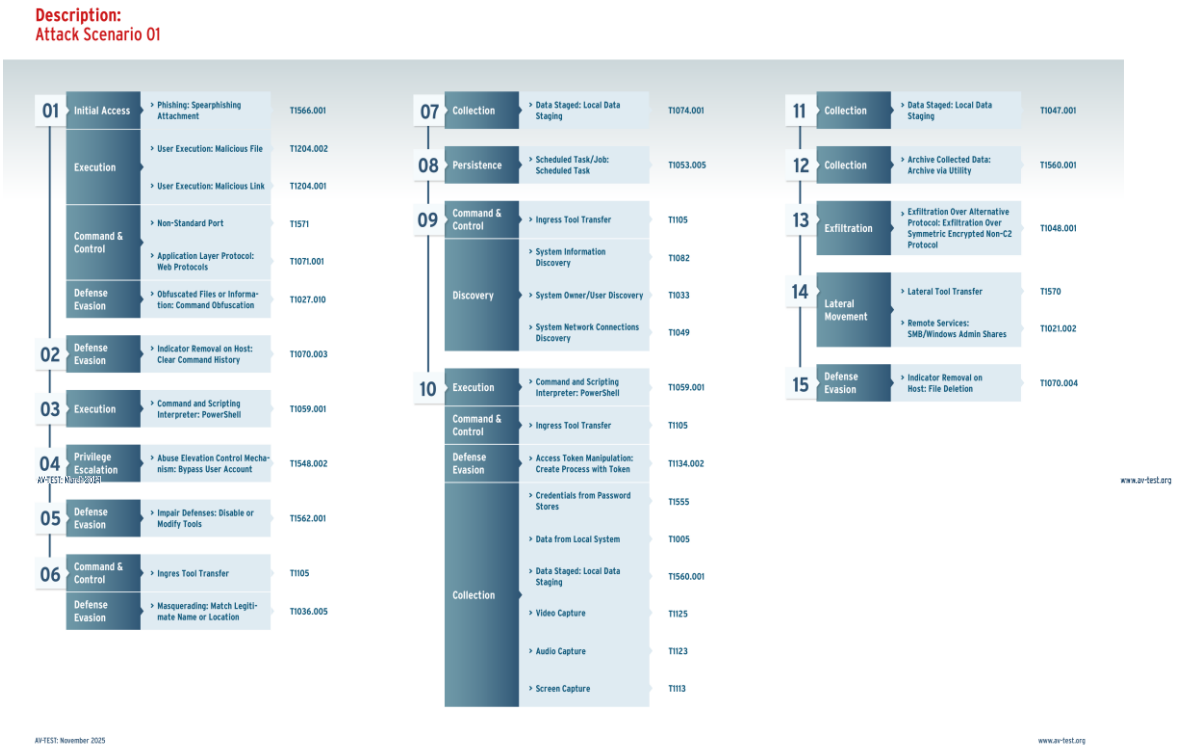
Scenario 1: Kematian-Stealer Emulation

This scenario assesses the network's resilience against a simulated cyber threat modelled after the "Kematian-Stealer," a sophisticated information stealer. The scenario leverages in-memory execution techniques and advanced evasion tactics to evaluate the defensive capabilities of the security solution.

Scenario Description

- Initial Setup: Initiate the attack with a spear-phishing campaign, delivering a malicious document with an embedded link. Upon execution, the victim downloads a malicious agent disguised as a setup file, simulating sophisticated initial access tactics.
- Defence Evasion & Privilege Escalation: The agent clears PowerShell history to avoid logging and modifies Windows registry values to bypass User Account Control (UAC), ensuring the adversary gains higher privileges while excluding directories from security scanning.
- Command and Control: Establish a C2 channel to receive commands and manage payloads, utilising a disguised agent ("svchost.exe") placed within the application data directories.
- Data Collection & Persistence: Use PowerShell scripts to gather detailed system information and construct JSON-based reports. Persistence is maintained by creating scheduled tasks to ensure long-term access to the victim's machine.
- Lateral Movement & Exfiltration: Employ SMB to move the agent across the network via administrative shares. Collected data is compressed and exfiltrated to an internal web server using standard web protocols.

This scenario incorporates tactics such as spear phishing, UAC bypassing, PowerShell usage, and lateral movement over SMB. It aims to test the network's detection mechanisms and incident response capabilities against such sophisticated, evolving threats.



Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Scenario 2: Bizfum Stealer Emulation

This scenario evaluates the system's defences against a simulated threat modelled after the "Bizfum Stealer," an advanced malware designed to collect browser credentials and private information. The scenario uses PowerShell to replicate the malware's original C-based logic and encryption methods to test the network's overall security posture.

Scenario Description

- Initial Setup: Begin with a spear-phishing campaign that delivers a malicious document with an embedded link. Upon execution, the victim downloads a malicious agent disguised as a setup file, simulating sophisticated initial access tactics.
- Staging and Collection: Create a dedicated staging directory within the system's temporary folders to aggregate collected private data, including login credentials, cookies, browsing history, and desktop screenshots.
- Data Manipulation: Execute scripts to discover sensitive browser files across multiple platforms (Chrome, Firefox, Edge). Instead of RSA, this emulation uses standard PowerShell functions and AES encryption to prepare the gathered data for exfiltration.
- Command and Control: Establish a C2 channel to manage the malicious agent, utilising non-standard ports and web protocols to simulate external attacker communications.
- Data Exfiltration: Simulate the extraction of the encrypted archive by uploading it to an external file-sharing server (Gofile), mimicking the typical data theft operations of modern information stealers.
- Clean-up: Execute commands to delete staging directories and temporary files, assessing the system's ability to track and log post-exploitation activities and anti-forensic measures.

This comprehensive scenario includes spear phishing, user execution, PowerShell scripting, the discovery of sensitive files, data encryption, and exfiltration. It tests the system's capability to defend against and respond to complex information-stealing threats, reflecting the methodologies of evolving malware variants.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

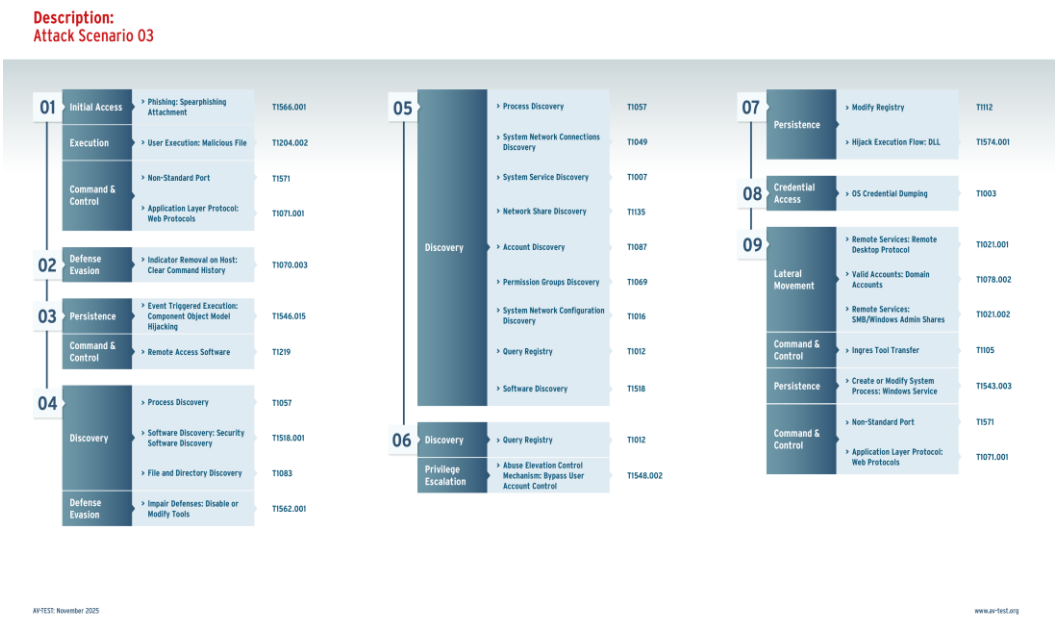
Scenario 3: Helldown Ransomware Emulation

This scenario evaluates the system's resilience against a simulated cyber threat modelled after "Helldown Ransomware," a modular and evolving threat known for its cross-platform capabilities. The scenario utilises advanced encryption payloads and evasion techniques to evaluate the network's defensive posture against modern ransomware.

Scenario Description

- Initial Setup: Initiate the attack via a spear-phishing campaign delivering a malicious attachment. Upon user execution, a command-and-control (C2) agent is launched through PowerShell via Caldera to establish an initial foothold.
- Defence Evasion: Employ sophisticated evasion techniques, including the use of indirect system calls (SysWhispers3) to bypass EDR hooks in ntdll.dll. The agent also clears command history and modifies system settings to avoid detection.
- Discovery: Execute automated scripts to perform a comprehensive scan of the environment, including process discovery, account discovery, and network configuration discovery to identify high-value targets.
- Persistence and Escalation: Implement methods to maintain a long-term presence, such as COM hijacking and the creation of new Windows services, while attempting to bypass User Account Control (UAC) to gain administrative privileges.
- Lateral Movement: Use remote execution tools and protocols such as RDP and SMB admin shares to move across the network, simulating deep penetration and the spread of ransomware to multiple endpoints.
- Encryption and Impact: Execute a C-based encryption payload to simulate the locking of critical files and the disruption of system operations, reflecting the primary goal of Helldown Ransomware.

This comprehensive simulation incorporates tactics such as spear phishing, advanced syscall evasion, network discovery, and lateral movement. It aims to evaluate the network's detection mechanisms and incident response capabilities against sophisticated ransomware patterns that intend to encrypt critical data and cause significant operational disruptions.



Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Test Results

Introduction

The objective of this test was to comprehensively evaluate the effectiveness of Padvish XDR in safeguarding against simulated cyber threats. In this evaluation, we conducted three scenarios inspired by real-world threat actors—Kematian-Stealer, Bizfum-Stealer, and Helldown-Ransomware—to assess the solution's capabilities in detecting and responding to sophisticated attacks. Our assessment focused not only on the coverage, i.e., the extent to which Padvish XDR detected any suspicious activities at each step, but also delved into the quality of these detections by measuring the reporting of specific tactics and techniques.

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 Protection 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. 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.

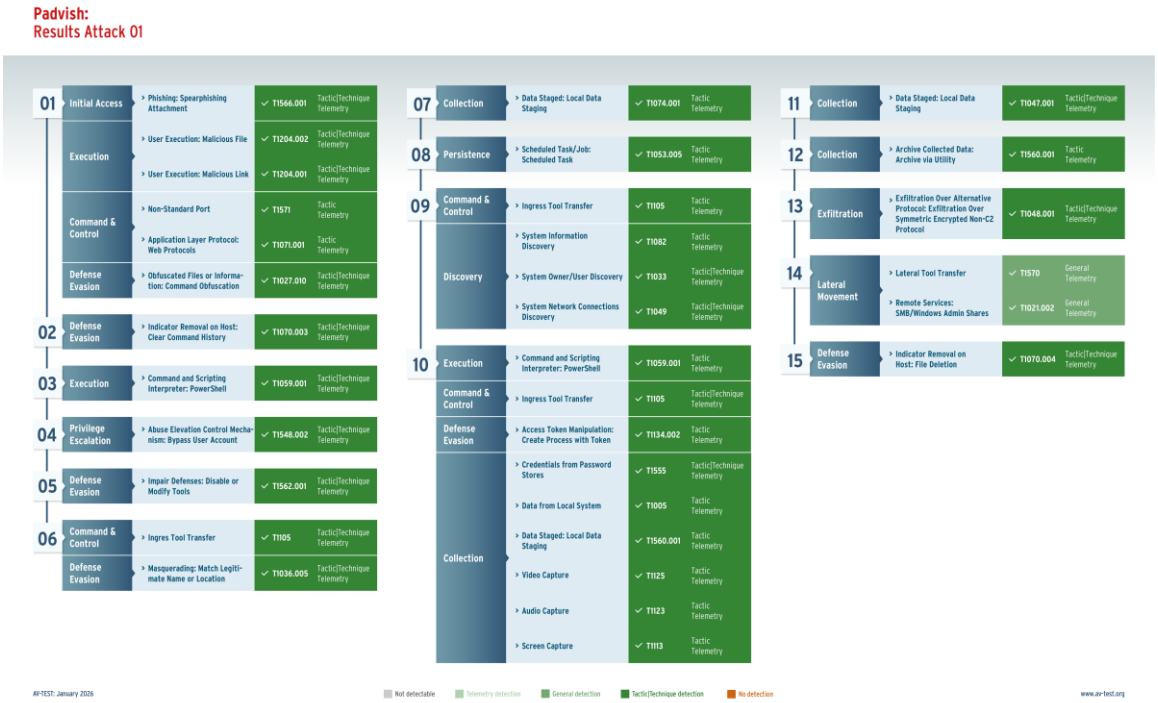
Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Results Analysis

The evaluation of Padvish XDR assessed its efficiency in defending against advanced cyber threats through three distinct scenarios. Based on the provided test data, these scenarios emulate real-world tactics including data exfiltration, service disruption, and ransomware deployment. This analysis focuses on two main aspects: coverage and detection quality.

Scenario 1: APT18-Style Cyber Espionage

This scenario simulated an attack by a PowerShell-based information stealer. The test examined Padvish XDR's ability to detect the entire chain, from the initial phishing attachment to data collection and exfiltration via an alternative protocol. The product reliably identified critical steps, including command obfuscation, User Account Control (UAC) bypass, and the local staging of stolen data.



Coverage Assessment

Padvish XDR demonstrated outstanding coverage in Scenario 1, successfully tracking the attack across its critical stages. The solution provided high visibility into the attack vectors, utilizing a combination of "Tactic", "Technique", and "Telemetry" alerts. This comprehensive visibility ensured that key activities—from malicious file execution and command obfuscation to privilege escalation—were continuously monitored, underscoring the tool's capability to flawlessly follow a complex attack lifecycle. Notably, the product provided telemetry and technique-level detail for the initial spearphishing attachment and subsequent execution steps right from the start.

Quality of Detection Assessment

The quality of detection was exceptionally high. Padvish XDR identified critical maneuvers like Command Obfuscation (T1027.010) and Impair Defenses (T1562.001) with precise, granular alerts. The product provided actionable intelligence throughout the attack, explicitly warning about UAC Bypass (T1548.002) and Credential Access (T1555). Although final steps like data exfiltration were captured primarily via telemetry, the strong "Technique" level alerts during the early phases provided excellent context, empowering security teams to intercept the threat in time.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Scenario 2: Bizfum Stealer Emulation

In this second scenario, the assessment shifted to Padvish XDR's capacity to defend against a complex attack involving service disruption and data encryption. The analysis examines how the system managed the simulated threat's activities, tracing the progression from initial access and defence evasion through to targeted service stops, sandbox evasion, data encryption, system defacement, and the inhibition of system recovery.

Coverage Assessment

Padvish XDR demonstrated strong coverage in Scenario 2, effectively monitoring the attack from the initial access to the final encryption and system impact phases. The solution provided high visibility into the primary attack vectors, utilizing a combination of "Tactic", "Technique", and "Telemetry" alerts. By successfully tracking the initial spearphishing attachment, the execution of malicious files and links, as well as the subsequent command obfuscation, the product ensured that the most critical stages of the ransomware operation were fully documented within the security console from the very beginning.

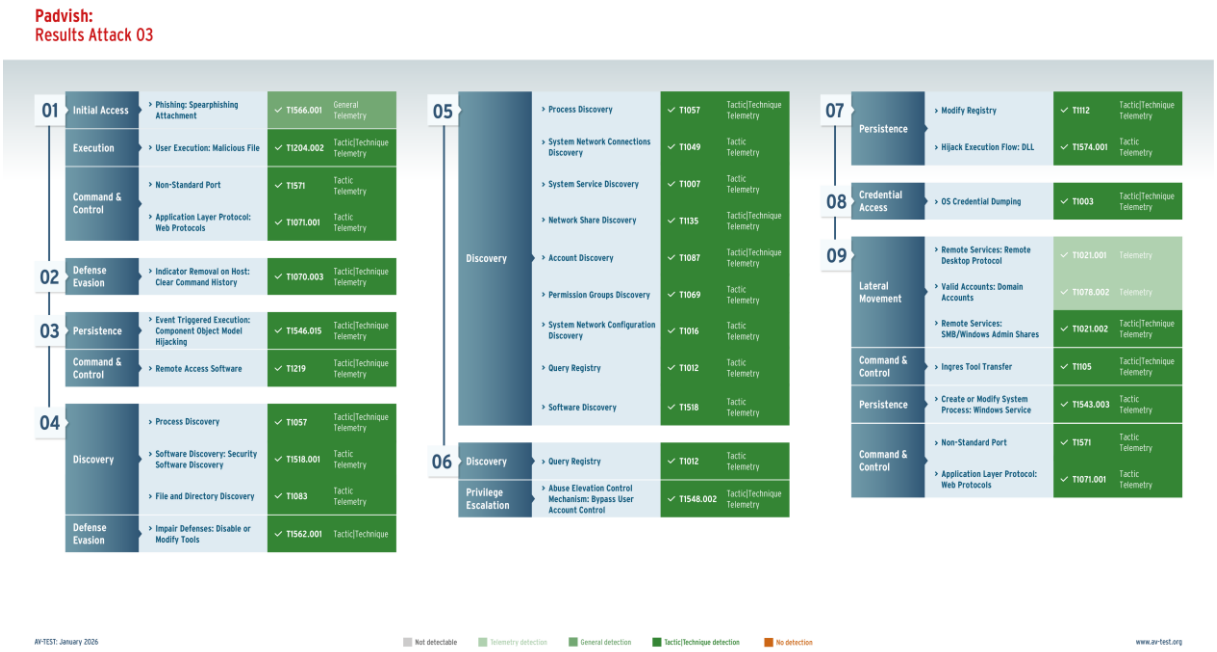
Quality of Detection Assessment

The quality of detection in Scenario 2 was exceptionally high, with Padvish XDR accurately identifying complex maneuvers such as Command Obfuscation (T1027.010) and Inhibit System Recovery (T1490) with comprehensive, granular alerts. The product provided actionable intelligence for nearly the entire lifecycle, effectively tracking User Execution (T1204.002) and communication over Non-Standard Ports (T1571). Furthermore, anti-analysis behaviors such as Virtualization/Sandbox Evasion (T1497.001) and Debugger Evasion (T1622) were successfully flagged with detailed "Technique" level alerts. While core impact actions like Data Encrypted for Impact (T1486) and Internal Defacement (T1491.001) were captured primarily at the "Tactic" level rather than with full technique granularity, the explicit detection of the initial Spearphishing Attachment (T1566.001) and subsequent evasive steps provided outstanding context. This gives security teams the necessary means to flawlessly identify the threat and understand its intent to disrupt operations and encrypt sensitive information.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Scenario 3: Helldown Ransomware Emulation

In this third simulation, the focus shifted to the product's resilience against the modular and adaptive nature of an advanced persistent threat. The analysis examines how Padvish XDR countered extensive system discovery, complex evasion techniques, and the lateral movement typical of modern targeted attacks.



Coverage Assessment

The test results for Scenario 3 revealed a high level of visibility as the solution tracked the threat's progression from the very beginning, capturing the initial Spearphishing Attachment (T1566.001) via "General" and telemetry events. Padvish XDR proved particularly effective at monitoring the subsequent automated reconnaissance, successfully logging a wide array of activities such as Process Discovery (T1057) and System Network Configuration Discovery (T1016). This consistent tracking across the broader attack chain ensured that the threat's behaviour remained entirely visible as it attempted to map the environment and identify high-value targets within the network.

Quality of Detection Assessment

Regarding alert precision, Padvish XDR delivered exceptional, high-fidelity warnings for critical phases of the attack. Crucial steps that often define an advanced breach, such as Privilege Escalation via UAC Bypass (T1548.002) and OS Credential Dumping (T1003), were explicitly flagged with comprehensive "Technique" level alerts. The product also accurately identified complex persistence methods, including Component Object Model (COM) Hijacking (T1546.015). While the final Lateral Movement via RDP (T1021.001) and specific execution flows like DLL Hijacking (T1574.001) were captured primarily via telemetry and "Tactic" alerts rather than with full technique granularity, the outstanding detections during the credential and privilege escalation phases provided abundant context to identify the advanced persistent threat pattern. This demonstrates that the platform effectively bridges the gap between raw telemetry and actionable intelligence, ensuring robust protection against multi-stage, targeted attacks.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Test Results Summary

The evaluation of Padvish XDR revealed its strong performance across multiple testing scenarios. Inspired by real-world threat actors, the evaluation examined the product's capability to detect and respond to a variety of sophisticated attack techniques.

In Scenario 1, which emulated the tactics of a complex cyber espionage and data exfiltration campaign via the Kematian-Stealer, Padvish XDR demonstrated outstanding detection capabilities. The product successfully identified the critical trajectory of the simulated attack, generating precise alerts for key steps such as command obfuscation, privilege escalation, and credential access. This level of coverage underscores the product's robust monitoring capabilities, ensuring that primary information-stealing threats are effectively tracked right from their initial execution.

Scenario 2 presented a mix of tactics modelled after the Bizfum-Stealer, involving service disruption, defense evasion, and data encryption. Padvish XDR displayed exceptionally high proficiency in detecting these tactics, successfully identifying critical elements like Command Obfuscation, Virtualisation/Sandbox Evasion, and attempts to Inhibit System Recovery with granular alerts. The product provided detailed and actionable detections throughout the attack's lifecycle, illustrating its effectiveness against destructive malware methodologies.

In Scenario 3, which simulated an advanced persistent threat inspired by the Helldown-Ransomware, the solution proved its resilience against extensive system discovery and complex persistence mechanisms. By successfully explicitly flagging critical steps such as OS Credential Dumping, Privilege Escalation via UAC Bypass, and automated reconnaissance activities, alongside capturing subsequent lateral movement, the product demonstrated its ability to maintain high-fidelity visibility even when faced with sophisticated, multi-stage attack patterns.

The impressive results highlight Padvish XDR's utility in safeguarding against advanced cyber threats. The exceptional detections and actionable insights across all three scenarios emphasise the tool's robustness, confirming its essential role in modern security infrastructures.

This evaluation demonstrates that Padvish XDR is well-equipped to handle real-world cyber threats, cementing its position as a highly capable cybersecurity solution. The product's ability to provide critical context against varied and complex attack patterns underscores its versatility and reliability.

Copyright © 2026 SITS Deutschland GmbH, Konrad-Adenauer-Ring 33, 65187 Wiesbaden, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org