EDR Test

Testing by AV-TEST

Date of the test report: August 2nd, 2024 (version 1.00)

ADVANCED EDR TEST 2023 Red Team Testing and Certification by the AV-TEST Institute

Seqrite XDR

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Executive Summary

AV-TEST conducted a comprehensive assessment of Seqrite XDR, focusing on its Endpoint Detection and Response (EDR) capabilities, from December 2023 to March 2024. The objective was to evaluate the product's effectiveness in detecting and mitigating threats typically associated with advanced persistent threats (APTs). The test scenarios simulated two distinct attack patterns, each highlighting a variety of tactics and techniques employed by sophisticated adversaries.

Scenario 1 - APT18-Style Cyber Espionage:
The first attack scenario evaluated Seqrite XDR against a detailed and methodically orchestrated cyber-attack, focusing on techniques frequently utilized in high-level cyber espionage. This scenario included spear-phishing, system reconnaissance, data exfiltration, and sophisticated evasion techniques, aiming to determine the product's ability to detect, respond, and mitigate complex attack vectors.

During Scenario 1, Seqrite XDR demonstrated robust detection capabilities, successfully identifying a comprehensive range of techniques deployed in the attack. The solution's detailed detections provided actionable insights at various stages, ensuring clear categorization of techniques and comprehensive visibility into the attack methods. This performance underscored Seqrite XDR's ability to handle complex cyber-espionage scenarios effectively.

Scenario 2 - Mixed Tactics Resembling TA577, Turla, and FIN6:
The second attack scenario involved mixed tactics resembling those utilized by multiple recognized threat groups, presenting a combination of phishing, data manipulation, and lateral movement techniques. The goal was to challenge Seqrite XDR's defence mechanisms against a variety of sophisticated threats attempting to extract sensitive data and establish a persistent network presence.

In Scenario 2, Seqrite XDR effectively identified all the tactics and techniques used during the attack. The product showed adaptability to various threat behaviours and overall demonstrated efficacy in countering a broad spectrum of advanced cyber threats.

Overall, Seqrite XDR displayed impressive performance across both simulated attack scenarios. Its consistent, high-quality detections affirm its potential to defend organizations against evolving and intricate cyber threats.

Based on these results, Seqrite XDR has been awarded the AV-TEST Approved Advanced Endpoint Detection and Response Certification, marking it as a reliable and effective solution in the cybersecurity domain.

Disclaimer

The information contained in this document is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of AV-TEST. The methodology is not finalized. During testing, we may decide to change some processes or remove certain aspects due to technical or other reasons.

Report Content

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

Overview of Seqrite XDR

Seqrite XDR is an advanced cybersecurity solution designed to enhance enterprise network security by providing comprehensive visibility and proactive threat responses. Unlike traditional solutions that focus on perimeter defences, Seqrite XDR secures the internal network against sophisticated threats that bypass initial measures.

At its core, Seqrite XDR integrates AI-enabled deep predictive malware-hunting technology with real-time threat intelligence. This powerful combination allows it to detect a wide range of threats, from initial access attempts to complex lateral movements within the network.

Seqrite XDR provides a unified dashboard for complete visibility, enabling efficient deployment, configuration, and monitoring of security measures across the network. It excels in advanced threat hunting, investigation, and remediation, offering real-time intelligence and proactive breach protection. The platform reduces complexity by simplifying data ingestion, alert correlation, and incident management, ensuring faster detection and response.

The solution leverages the MITRE ATT&CK® Framework for root cause analysis and utilizes automated playbooks for real-time response to critical incidents. Seqrite XDR supports both physical and virtual endpoints across various operating systems, making it adaptable to diverse enterprise environments.

By merging Endpoint Protection with Extended Detection and Response technologies, Seqrite XDR delivers total protection, remediation, and comprehensive visibility, helping enterprises defend against complex cyber threats effectively.

Test Scenarios

Scenario 1: APT18-Style Cyber Espionage

This scenario assesses the network's resilience against a simulated cyber threat modelled after APT18, a known advanced persistent threat group. The scenario leverages techniques commonly associated with APT18 to evaluate the network's defensive capabilities.

Scenario Description

- Initial Setup: Initiate the attack with a spear-phishing campaign, delivering a malicious Word document with an embedded macro to a user. Upon execution, this macro launches an agent that connects to a command and control server, simulating the sophisticated initial access tactics of APT18.
- Command and Control: Establish a command and control (C2) channel using HTTP requests to simulate external attacker communications and control. This includes downloading additional payloads and receiving commands directly from the attacker's infrastructure.
- Data Collection: Use PowerShell scripts to gather system information, scan for sensitive data within the network, and prepare this data for exfiltration, reflecting the espionage focus of APT18.
- Lateral Movement: Employ techniques such as exploiting service accounts and using remote execution tools to move laterally across the network, accessing multiple endpoints to simulate deep network penetration.
- Data Exfiltration: Simulate the extraction of gathered data, using HTTP for transmission to an external server, mimicking the typical data theft operations conducted by APT18.
- Persistence: Implement methods to maintain presence within the network, setting up backdoors and scheduled tasks, ensuring the attacker's long-term access to the network.

This scenario incorporates tactics such as spear phishing, user execution, PowerShell usage, and data exfiltration over HTTP, reflecting APT18's methods. It aims to test the network's detection mechanisms and incident response capabilities against such sophisticated threats.

Scenario 2: Mixed Threat Simulation Mimicking TA577, Turla, and FIN6

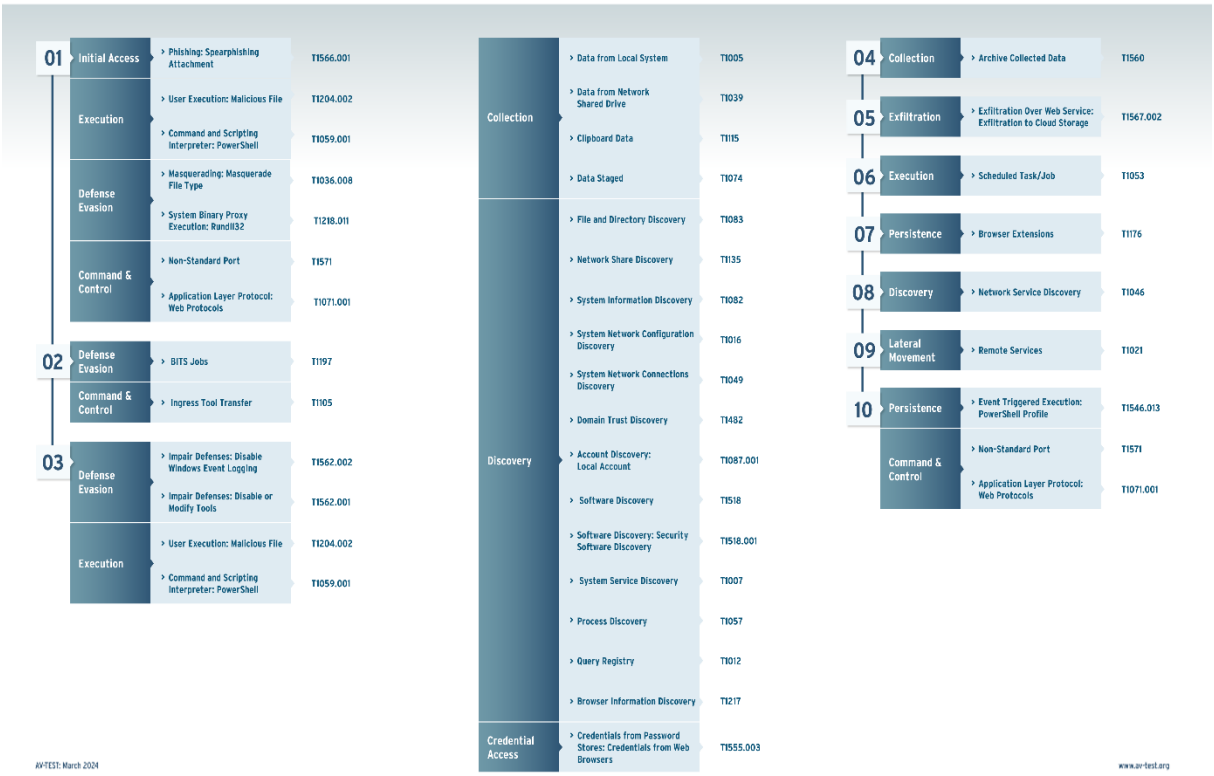
This scenario evaluates the system's defences against a blend of tactics and techniques used by cyber threat actor groups such as TA577, Turla, and FIN6, offering a robust test of the system's overall security posture.

Scenario Description

- Phishing Setup: Begin with a phishing email that delivers a malicious document designed to exploit specific system vulnerabilities.
- Credential Access: Use credential dumping techniques to gather user and admin credentials, mimicking internal data theft.
- Discovery and Collection: Execute scripts to discover network resources and collect sensitive data from multiple systems.
- Privilege Escalation and Persistence: Elevate privileges to gain deeper access and establish persistent threats within the network infrastructure.
- Lateral Movement and Data Exfiltration: Move laterally across systems and simulate exfiltration of large data sets to an external control server, employing encrypted channels to avoid detection.
- Impact: Execute commands that simulate the alteration or destruction of critical data to assess the network's resilience against such impacts, including commands that overwrite data or corrupt essential system files to cause operational disruptions.

This comprehensive scenario includes spear phishing, user execution, PowerShell scripting, the discovery of files and processes, credential access, privilege escalation, persistence mechanisms, lateral movement, data exfiltration, and impact assessment. It tests the system's capability to defend against and respond to complex and persistent cyber threats, reflecting the combined methodologies of the referenced threat actor groups.

Description:
Attack Scenario 02



Test Results

Introduction

The objective of this test was to comprehensively evaluate the effectiveness of the Seqrite XDR product in safeguarding against simulated cyber threats. In this evaluation, we conducted two scenarios inspired by real-world threat actors, APT18 and a combination of TA577, Turla, and FIN6, to assess the EDR's capabilities in detecting and responding to sophisticated attacks. Our assessment focused not only on the coverage, i.e., the extent to which the EDR detected any suspicious activities at each step, but also delved 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 Protection Assessment

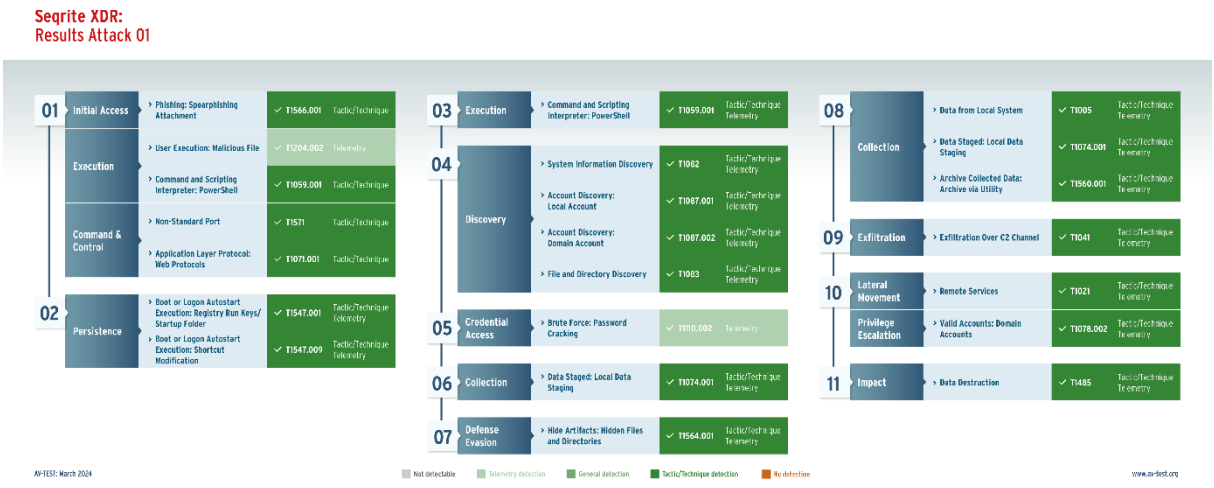
In addition to measuring coverage, we also assessed the quality of the EDR detections. It is imperative to differentiate between different types of detections, as not all are equally valuable in terms of threat mitigation. While telemetry-based detections provide valuable information about suspicious 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.

Results Analysis

The evaluation of Seqrite XDR assessed its efficiency in defending against advanced cyber threats through two distinct scenarios modelled after threat actors APT18, TA577, Turla, and FIN6. This analysis focuses on two main aspects: coverage and quality of detection.

Scenario 1: APT18-Style Cyber Espionage

The evaluation of Seqrite XDR assessed its efficiency in defending against advanced cyber threats through two distinct scenarios. This analysis focuses on two main aspects: coverage and quality of detection.



Coverage Assessment

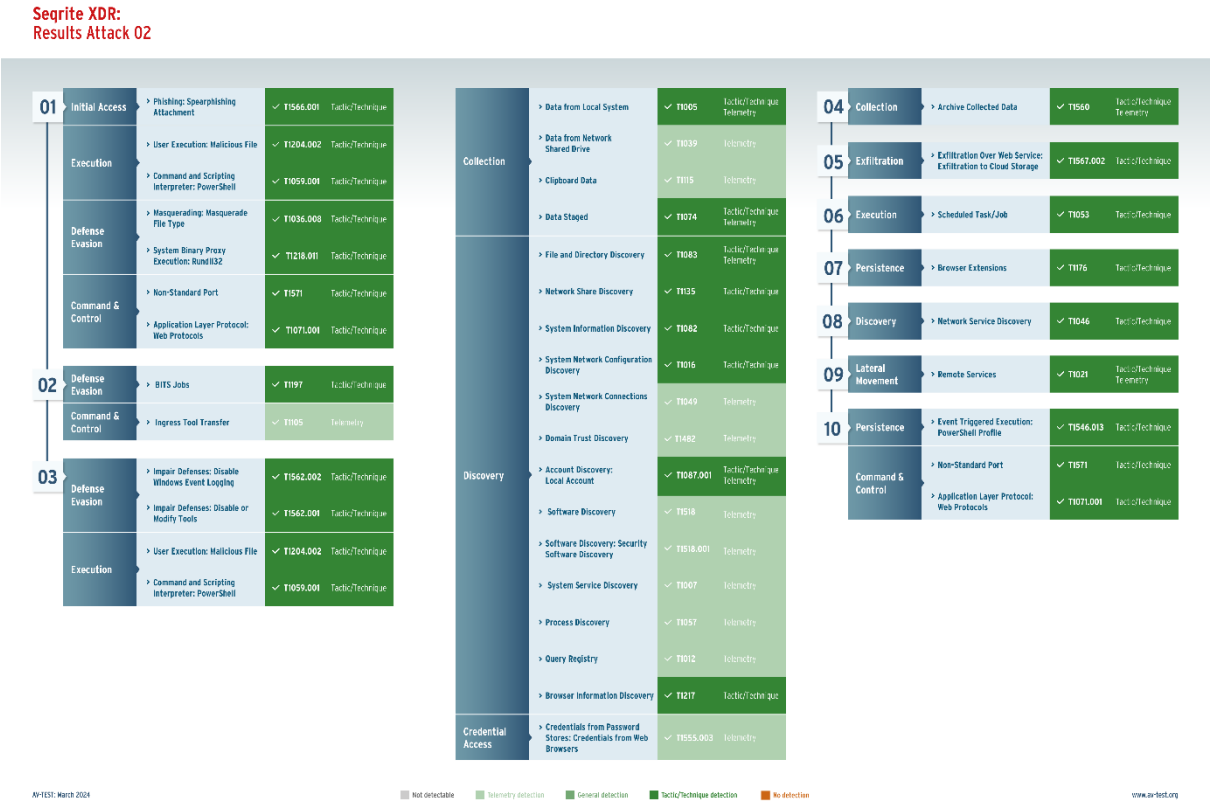
Seqrite XDR exhibited exceptional coverage in Scenario 1, successfully detecting all employed techniques. The product utilized various forms of detection, including both telemetry and tactic/technique-specific detections, to provide comprehensive monitoring of the attack. This extensive coverage underscores Seqrite XDR's capability to effectively track and identify complex threats.

Quality of Detection Assessment

Overall, Seqrite XDR displayed a strong performance in Scenario 1, with exceptional coverage and high-quality detections. The solution provided detailed insights and clear categorization of techniques, aiding in the identification and mitigation of sophisticated cyber-espionage threats. These results reinforce Seqrite XDR's role as a robust tool in the cybersecurity arsenal.

Scenario 2: Mixed Threat Simulation Mimicking TA577, Turla, and FIN6

This scenario tested Seqrite XDR against a combination of tactics typically used by TA577, Turla, and FIN6, focusing on the product's detection and response capabilities.



Coverage Assessment

Seqrite XDR showed effective coverage in Scenario 2, identifying all the key tactics and techniques utilized during the attack. The product leveraged extensive detection methods to provide visibility into various attack stages, including initial access, execution, and lateral movement, ensuring comprehensive coverage.

Quality of Detection Assessment

Seqrite XDR provided high-quality detections across multiple facets of Scenario 2, with detailed and actionable insights crucial for effective threat mitigation and incident response. The comprehensive detection approach helped identify a wide range of tactics, providing clarity and aiding in effective countermeasures. This underscores Seqrite XDR's capability to handle sophisticated and multifaceted cyber threats.

Overall, Seqrite XDR demonstrated robust detection capabilities and high-quality performance in evaluating its competency against intricate and evolving cyber threat landscapes. The consistent and comprehensive detections highlight Seqrite XDR's strength as a vital defence mechanism in modern cybersecurity.

Test Results Summary

The evaluation of Seqrite 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 simulated elaborate cyber-espionage techniques, Seqrite demonstrated comprehensive detection capabilities by successfully identifying all techniques used during the simulated attack. This high level of coverage underscores the product's robust monitoring and defensive features, ensuring that complex threats are effectively addressed.

Scenario 2 presented a mix of tactics from threat groups such as TA577, Turla, and FIN6. Seqrite displayed considerable proficiency in detecting these tactics, effectively identifying all the critical techniques employed. The product provided detailed and actionable detections for every employed tactic and technique, illustrating its overall effectiveness.

The impressive results from both scenarios highlight Seqrite XDR's utility in safeguarding against advanced cyber threats. The comprehensive detections and quality insights emphasize the tool's robustness, confirming its essential role in modern security infrastructures. This evaluation, conducted in a controlled environment, suggests that Seqrite is well-equipped to handle real-world cyber threats, cementing its position as a leading cybersecurity solution.