The EDR Test That Matters - AV-Comparatives to publish the first truly stealth-based EDR test

AV-Comparatives to publish the first truly stealth-based EDR test at the end of May, exposing how today's security tools fare against APT cyberattacks.

AV-Comparatives EDR 2025 Certificate

INNSBRUCK, TYROL, AUSTRIA, May 12, 2025 /EINPresswire.com/ -- AV-Comparatives, the world-renowned independent authority on cybersecurity product testing, is pleased to announce the forthcoming release of its EDR Detection Validation Report, the most realistic and comprehensive evaluation of endpoint detection and response capabilities in the cybersecurity industry.

The report, expected to be published in the coming months, is based on stealth-mode advanced persistent threat (APT) simulation using the Empire framework. This industry-first assessment evaluates how well EDR or XDR solutions detect complex attack sequences in real time, leveraging telemetry analysis, threat hunting, and management console alerting.

"While much of the industry talks about detection, we measure it," said Andreas Clementi, Founder and CEO of AV-Comparatives. "This report will give CISOs, SOC teams, and product vendors tangible insight into how well their tools perform in realistic, multi-stage attack scenarios."

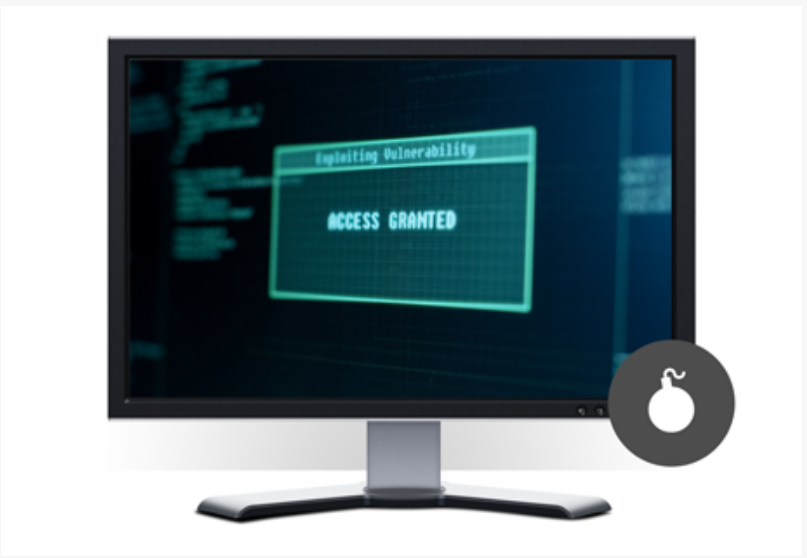
Unlike other evaluations that may rely on scripted, limited-scope scenarios or assume detection based on static indicators, AV-Comparatives' test replicates the entire adversarial kill chain, mirroring the most elusive real-world threats. The test does not simply measure whether indicators are present but validates if actionable alerts are triggered, and whether meaningful insights can be extracted by threat-hunting from telemetry alone.

Key differentiators of this test include:
Detection-Only Configuration: All products are tested with prevention features disabled, placing

the spotlight entirely on detection mechanisms—telemetry granularity, alert fidelity, and huntability.

Stealth-Oriented Execution: Attack scenarios unfold using real-world TTPs, pushing the tools' capabilities beyond detection of overt or batch-scripted threats.

Holistic Kill Chain Coverage: Each phase of the attack—initial access, execution, persistence, lateral movement, and data exfiltration—is exercised, offering a complete view of detection coverage across all attack stages.



Advanced Threat Protection Test 2020 - AV-Comparatives

Ground Truth Anchoring: Detection is validated by evidence-based methods, including visualised telemetry traces, console alerts, and the correlation of threat events.

> This is where detection is no longer theory—it's proven. Vendors who engage gain not only certification, but a true benchmark of their threat visibility."
>
> *Andreas Clementi, founder and ceo, AV-Comparatives*

Only products meeting the certification criteria will be published, ensuring the report's credibility. Solutions that fall short remain unpublished but receive internal feedback to support product improvement and responsible disclosure.

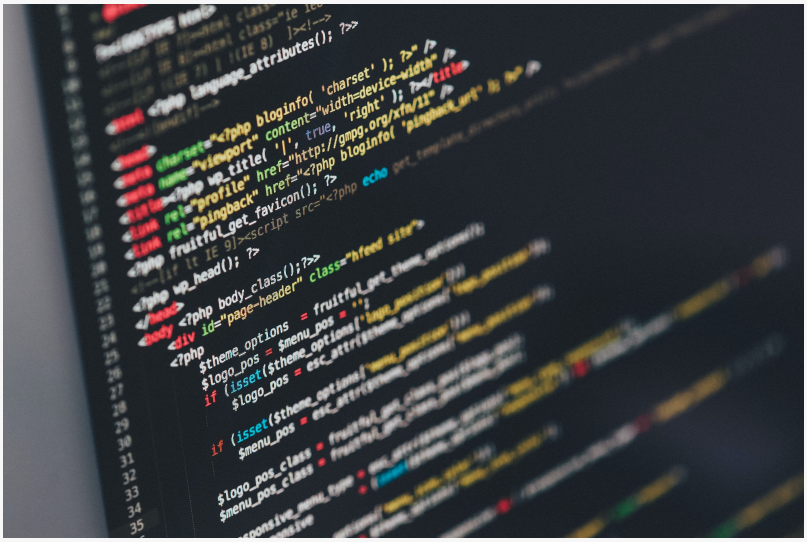
The methodology behind this landmark report was first introduced at the AV-Comparatives Cybersecurity Summit in Innsbruck in February 2025. With demand growing for vendor-neutral, evidence-backed assessments of EDR and XDR solutions, this initiative reaffirms AV-Comparatives' role as a trusted global benchmark in cybersecurity testing.

Key Highlights of the Report:

- APT-style testing using Empire and real-world TTPs
- Vendor configurations set to detection only (no prevention)
- Combined evaluation of alert visibility and telemetry depth
- Only certified results are published, maintaining rigour and credibility
- Cybersecurity-Vendor & CISO Engagement
- Vendors of EDR and XDR solutions, as well as CISOs and security decision-makers, are warmly

invited to contact AV-Comparatives to:

- Submit their product for individual evaluation under this rigorous detection validation framework.
- Request complimentary access to the report to gain insights into cutting-edge detection strategies and best practices.



Malware authors continue to write new malicious programs

Participation is open to products capable of running in detect-only mode. Early engagement offers the opportunity to be among the first certified solutions in the 2025 series. To enquire about participation or to request the pilot-report, please reach out via our contact portal at www.av-comparatives.org/contact

Cybersecurity and Antivirus Test Results available at https://www.av-comparatives.org for the following vendors:

Avast
AVG
Avira
Bitdefender
Checkpoint
Cisco
CrowdStrike
Elastic
Fortinet
F-Secure
ESET
G DATA
Gen Digital
Google
Intego
K7
Kaspersky
Malwarebytes
ManageEngine
McAfee
Microsoft

NetSecurity
Nordsec
Norton
Palo Alto Networks
Rapid7
SenseOn
Sophos
Total Defense
TotalAV
Trellix
TrendMicro
VIPRE
WithSecure

and many more

Peter Stelzhammer
AV-Comparatives
+43 512 287788
email us here
Visit us on social media:
LinkedIn
Facebook
X
