AV-Comparatives Introduces Enterprise-Class EDR TEST @ RSA 2020

AV-Comparatives has developed a comprehensive methodology for testing enterprise-class EDR systems, with tests commencing mid-Q2

INNSBRUCK, TYROL, AUSTRIA, February 24, 2020 /EINPresswire.com/ -- As the number and complexity of advanced persistent threats increase, so does the importance of endpoint detection and response systems. AV-Comparatives has developed a comprehensive methodology for testing enterprise-class EDR (endpoint detection and response) systems, with tests commencing mid-Q2 2020, and results being published around the end of Q3 2020. AV-Comparatives have been working closely with the IT security teams, security practitioners and security operation centre (SOC) personnel of typical enterprises that already employ EDR systems, or are planning to do so in the future.

AV-Comparatives Logo

EDR Test AV-Comparatives

The scenarios to be used in AVC's test of EDR products are based on this feedback. The test framework is flexible enough to allow for different scenarios in the future, as the technical nature of advanced threats (including APTs) evolves.

This will be the first time that such a comprehensive comparative test of EDR systems has been performed. It will allow participating vendors to showcase their respective products' features, functionality, and detection/response metrics, as well as illustrating the value provided by investing in these solutions.

The aim of the test will not be to determine whether the endpoints have been protected against compromise, but to evaluate the effectiveness of the tested systems in

detecting and monitoring the attacks, and providing reporting and remediation functions. We will require vendors to disable the protection (blocking) and prevention capabilities of their respective products during the entirety of the test timeframe. This will allow the attacks to run their full course, thus demonstrating the abilities of the EDR products to detect, record, analyse and respond to them.

The methodology considers the typical stages of an attack kill-chain, in order to find out how the tested EDR products identify, detect and collect data on them. These include initial access, execution, persistence, privilege escalation, credential access, data collection and exfiltration.

Various aspects of the tested EDR systems' functionality will be validated, including time to respond, threat classification, threat resolution options, threat timeline, endpoint and user data, and the ability to correlate and present data from multiple sources, including third-party.

AV-Comparatives' EDR testing methodology will include obfuscation techniques in the attacks, to determine the tested products' abilities to cope with detection-avoidance mechanisms in realistic enterprise-attack scenarios.

For more information please contact the AVC EDR team via mail: edr@av-comparatives.org

#avcomparatives #rsac2020 #cybersecurity #malwaredetection #antivirus #antimalware #EDR #EPP

Mediacontact
AV-Comparatives
+43 720 115542
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
