SE Labs

On-Demand Malware Detection Certification

On-Demand Malware Detection Certification

Product: CrowdStrike Falcon (ML)

Certification date: 28 July 2016

CrowdStrike Falcon (ML)
28 July 2016

SE Labs certifies the ability of CrowdStrike Falcon (ML) to detect malware.

The product identified in this certificate has been evaluated by SE Labs Ltd using the On-Demand Malware Detection methodology and found to meet the certification criteria.

Test date: 25 July 2016
Malware detection rate (known samples): 100 per cent
Malware detection rate (unknown samples): 100 per cent
False positive rate: 0 per cent

Certificate number: 20160728001

This certificate is valid until 28 July 2017

SE LABS LTD
24 Ripon Street, Aylesbury, Buckinghamshire, HP20 2JP, United Kingdom.
Registered in England: 9688006.
Tel: +44(0)20 3875 5000; Email: aux@selabs.uk

SE Labs

On-Demand Malware Detection Certification

Test Details: 20160728001

Methodology: On-Demand Malware Detection 1.0 (https://selabs.uk/download/on-demand-malware-detection-1.0.pdf)

This data was acquired through the Real Time Threat List provided by the Anti-Malware Testing Standards Organization, Inc. (AMTSO), at www.amtso.org.

RTTL query: {"resultsLimit": "500", "lastSeen": "2016-07-25", "firstSeen": "2016-07-24"}

Product build: 20160725

Number of test runs to achieve certification: one

SE LABS LTD
24 Ripon Street, Aylesbury, Buckinghamshire, HP20 2JP, United Kingdom.
Registered in England: 9688006.
Tel: +44(0)20 3875 5000; Email: aux@selabs.uk

Methodology: On-Demand Malware Detection

This methodology is designed to test the ability of anti-malware products to detect malicious code without error. To pass this certification test a product must classify all malicious code used in the test as being unwanted, using unambiguous terms including, but not exclusively restricted to, 'malware', 'virus', 'exploit', 'threat' and 'Trojan'. It must also not misclassify legitimate software as being malicious.

In an effort to use recent and prevalent threats the malicious code used in the test is obtained from the Anti-Malware Testing Standards Organization (AMTSO), through its Real-Time Threat List (RTTL) system. The sample selection comprises the 250 most recent, prevalent and verified threats.

Threat selection is made automatically via a query to the RTTL system, which is submitted without any intended bias towards or against any vendor involved in any test conducted by SE Labs Ltd. The details of this query are available in each test's Test Details document.

The test includes checks for false positives, using 1,000 standard Microsoft files commonly found on Windows systems.

In order to detect significant reliance on third-party multi-scanner engines each piece of malicious code is altered in such a way as to preserve its nature but to change its appearance. The new code is scanned. Products must detect all such files as being malicious. Hashes of the new code are submitted to VirusTotal, which should not detect them as being malicious.

SE LABS LTD
24 Ripon Street, Aylesbury, Buckinghamshire, HP20 2JP, United Kingdom.
Registered in England: 9688006.
Tel: +44(0)20 3875 5000; Email: aux@selabs.uk