Q1 2017

Advanced Threat Defense

Certification Testing Report

Cyphort, Inc.
Cyphort Anti-SIEM

ICSA Labs Advanced Threat Defense Criteria v.1.0

April 5, 2017

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

ATD-CYPHORTX-2017-0405-01

ICSA Labs Advanced Threat Defense – Report-at-a-Glance

Cyphort, Inc.

Cyphort Anti-SIEM

ANTI SIEM

Everything you want in a SIEM. And less.

www.cyphort.com

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

ICSA Labs Advanced Threat Defense

Certified

Test Period: Q1 2017

Certified Since: 04 / 2017

Executive Summary

During 40 days of testing during the first quarter of 2017, ICSA Labs tested the advanced threat detection components of Cyphort's Anti-SIEM platform with a mix of over 900 test runs. The mix was primarily composed of new and little-known malicious threats – i.e., recently harvested threats not detected by traditional security products. Please note that the Anti-SIEM platform also includes security analytics and automated mitigation, but these components were not included in testing by ICSA Labs.

Periodically, ICSA Labs launched innocuous applications and activities to additionally test Cyphort's ATD Solution in terms of false positives. Throughout testing ICSA Labs observed product logs to ensure not only that the Cyphort Anti-SIEM indicated the existence of a malicious threat but also that logged threats were distinguishable from other logged traffic and events.

The Cyphort Anti-SIEM passed, having met all criteria requirements. As seen in Figure 1 below, Cyphort's ATD Solution did very well during this test cycle - detecting previously unknown threats while having minimal false positives. Figures 2 and 3 below further break down the product's detection effectiveness and false positives.

Test Length	40 days	**Malicious Samples**	445	**Innocuous Apps**	490
Test Runs	935	**% Detected**	**99.6%**	**% False Positives**	**1.0%**

Fig. 1 – High Detection Effectiveness & Few False Positives

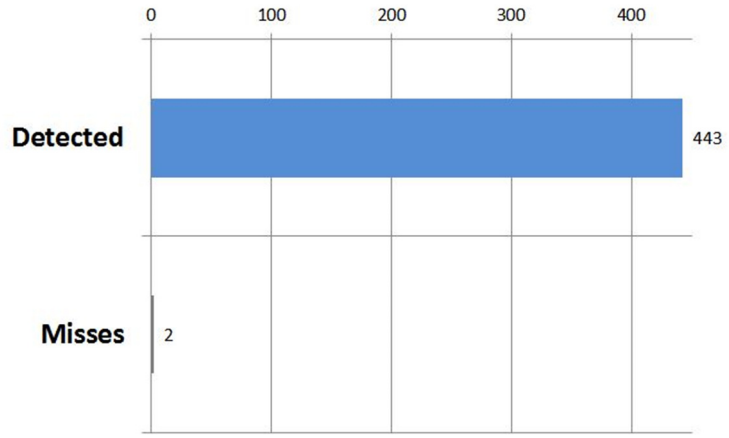


Fig. 2 – Detected 443 of 445 *New & Little-Known* Malicious Samples

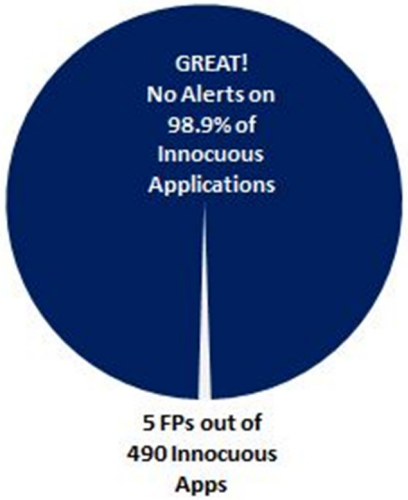


Fig. 3 – Few Alerts on Innocuous Applications

Introduction

This is Cyphort's first ICSA Labs Advanced Threat Defense Certification testing report for the Cyphort Anti-SIEM.

Standard ICSA Labs Advanced Threat Defense (ATD) testing is aimed at vendor solutions designed to detect new threats that other traditional security products miss. Thus the focus is on how effectively vendor ATD solutions detect these unknown and little-known threats while minimizing false positives.

The remainder of the report presents a more detailed look at how Cyphort's ATD solution performed during this cycle of standard ICSA Labs Advanced Threat Defense Certification Testing. To better understand how to interpret the results, this report documents not just the testing results themselves but the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against the Cyphort Anti-SIEM.

Test Cycle Information

This report reflects the results of one test cycle at ICSA Labs. Standard ATD and ATD-Email test cycles are performed by ICSA Labs each calendar quarter and typically range from three to five weeks in duration. To be eligible for certification, security vendor solutions must be tested for at least 3 weeks. Because testing is performed quarterly, ICSA Labs tests ATD solutions four times during a calendar year.

During each test cycle ICSA Labs subjects advanced threat defense solutions to hundreds of test runs. The test set is comprised of a mix of new threats, little-known threats and innocuous applications and activities – delivered and launched one after another continuously for the length of testing. Below in Figure 4 is information about the test cycle from which this findings report is based. Note that this test cycle extended beyond the usual 5 weeks:

Start Date	Jan. 17, 2017	**Days of Testing**	40
End Date	Feb. 25, 2017	**Test Runs**	935

Fig. 4 – This Test Cycle

ATD Solution Tested

ICSA Labs tested the Cyphort Anti-SIEM platform. The Cyphort advanced threat defense solution tested was comprised of the single component described below.

- Cyphort Anti-SIEM (version 4.0.1.19) (Content Version 4.0.1.3)

  Cyphort's platform is built on strong advanced threat detection capabilities. Lightweight virtual collectors in the network continually ingest web, email, and lateral spread traffic to provide greater visibility into the vectors most often used for advanced targeted attacks. In addition, the Anti-SIEM also offers automated "one-touch" mitigation capabilities to create new rules and policies for inline devices, strengthening them against future attacks. Built with an open architecture, there is no need to "rip and replace" anything. Instead, the Cyphort platform can ingest log and event data from other network and endpoint security tools already deployed, thus providing security teams with even greater network visibility. The data ingested from Cyphort collectors and other devices in your network are continuously fed into the SmartCore analytics engine, which consolidates and correlates all data and applies machine learning and behavioral analysis technologies to identify advanced threats within 15 seconds.

For more information about the Cyphort Anti-SIEM advanced threat defense solution, please visit:

http://www.cyphort.com

Detection Effectiveness

To meet the criteria requirements and attain (or retain) certification through ICSA Labs testing, advanced threat defense solutions must be at least 75% effective at detecting new malicious threats. As shown in Figure 5 the Cyphort Anti-SIEM ATD solution detected 99.6% of the threats it encountered during this test cycle, considerably better than the percentage required for certification.

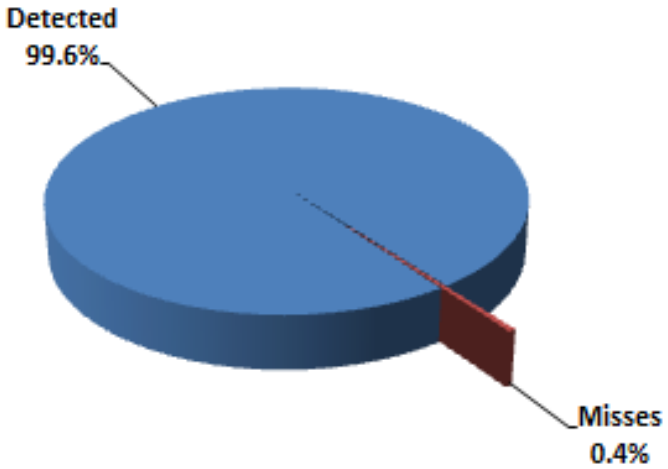


Fig. 5 – Cyphort ATD Solution Detection Effectiveness

A second plot depicting the detection effectiveness of the Cyphort Anti-SIEM ATD Solution appears in Figure 6. For the Cyphort solution the chart sheds light on whether or not Cyphort Anti-SIEM did better or worse – the newer the malicious sample. In terms of threats one hour old or less, Cyphort Anti-SIEM detected 100% of them. The Cyphort Anti-SIEM also detected 100% of threats less than two hours old. In fact, regardless of how new or how old the threat, Cyphort Anti-SIEM platform did a very good job detecting new and little-known malicious threats. Cyphort's ATD solution provided this excellent detection effectiveness while having just five false positives during this test cycle.

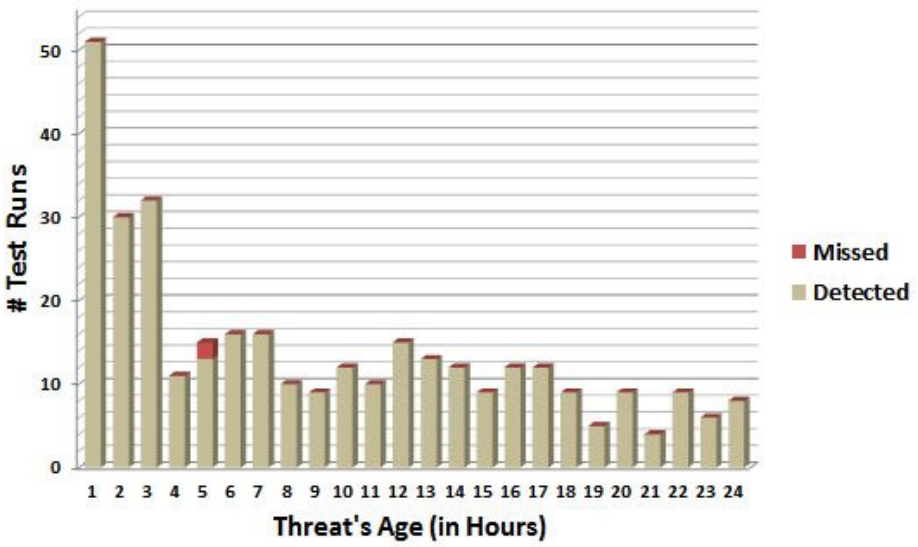


Fig. 6 – Detection Effectiveness by Age of Threat (Threats < 24 Hours Old)

A final effectiveness-related plot to consider for Cyphort Anti-SIEM ATD solution during this test cycle is Figure 7 below. Plotted in the figure are the 40 days during the test cycle along with how effective the ATD Solution was on each of those days. The Cyphort Anti-SIEM was 100% effective against new and little-known threats on all but two days during the Q1 2017 ATD test cycle.

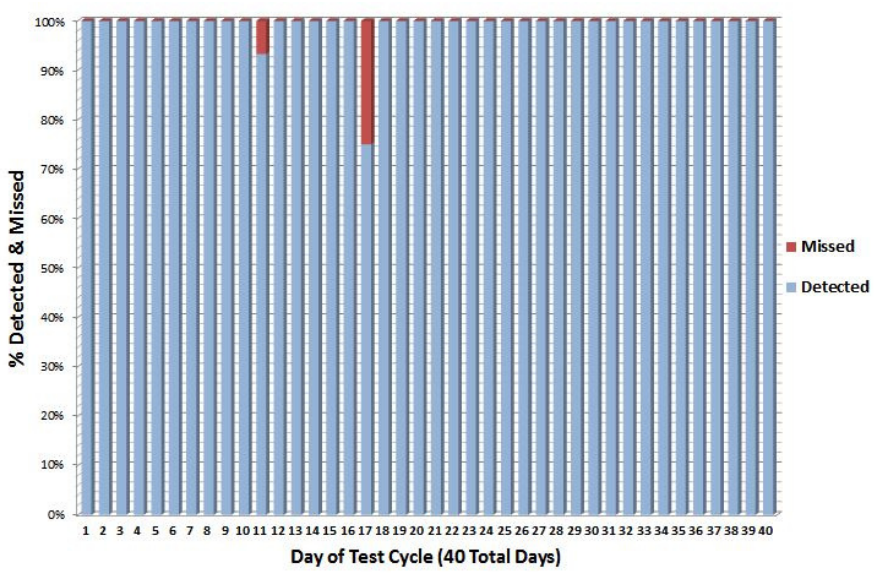


Fig. 7 – Detected & Missed Threats by Day of Test Cycle

Threat Vectors

In testing, ICSA Labs delivers new and little-known malicious threats to security vendor solutions using many of the top threat vectors that have led to enterprise cybersecurity incidents and breaches as reported in the latest Verizon Data Breach Investigation Report (DBIR).

DBIR data indicates that malware has been a key factor in thousands of security events where an information asset had its integrity, confidentiality, and/or availability compromised. Figure 9 on the following page depicts the threat vectors involved in these malware-related security incidents throughout the over ten year history of Verizon's DBIR. Figure 8 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2015 alone (2016 DBIR).

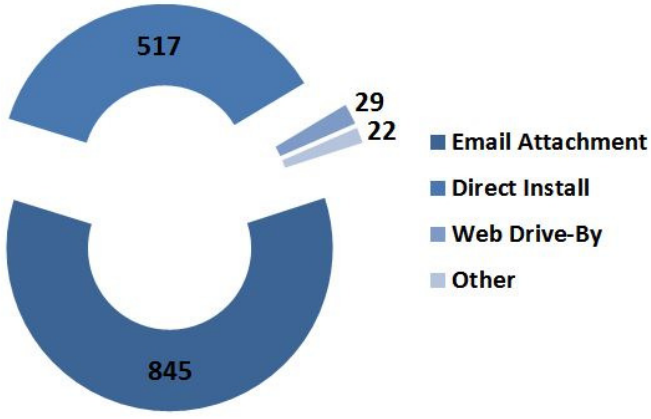


Fig. 8 – Top Threat Vectors Leading to Breaches in 2015 (2016 DBIR)

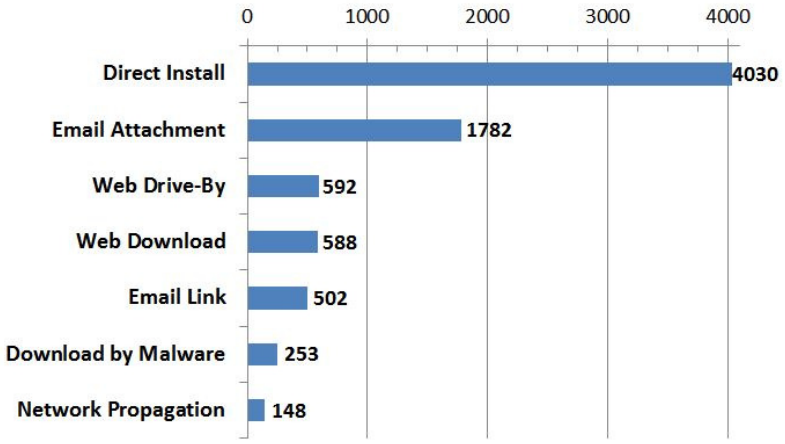


Fig. 9 – Malware-Related Threat Vectors Involved in Incidents (DBIR All-Time)

Standard ICSA Labs ATD testing includes the threat vector that is by far the most prevalent over time, "Direct Install". In addition, standard ATD testing includes the threat vectors labeled "Web Download", "Web Drive-By", and "Download by Malware". In the separate but related, ICSA Labs ATD-Email testing, ICSA Labs delivers new and little-known malware in URLs and attachments, corresponding to DBIR threat vectors "Email Link" and "Email Attachment", the latter being the single most common threat vector leading to enterprise breaches according to the 2016 DBIR (refer to Figure 8 above).

Source of Samples

A number of sample sources feed ICSA Labs' ATD testing.

One source is the spam ICSA Labs collects. The labs' spam honeypots receive approximately 250,000-300,000 spam email messages/day. For ICSA Labs ATD testing, the team harvests attachments in that spam, making use of the ones that are malicious.

Samples may also come from malicious URLs. Some of these come from the spam mentioned above. From feeds like this ICSA Labs filters and checks the URLs to see if there is a malicious file on the other end of that URL -- either as a direct file link or a series of steps (e.g. a drive-by attack with a multi-stage download process) leading to it. If so, ICSA Labs collects the sample for potential use in testing.

ICSA Labs additionally uses other tools and techniques to create unique malicious files as an attacker or penetration tester might do. In some cases these are trojanized versions of clean executables. In other cases they may be original executables that are malicious.

Still another source of samples is the samples themselves. Any dropped files resulting from running another malicious sample are also evaluated and potentially used in testing.

Finally – and importantly to test for false positives – ICSA Labs also launches legitimate executables. Running innocuous applications helps ensure that vendor solutions aren't just identifying everything as malicious.

Ransomware Less Hot This Test Cycle

While Ransomware levels were off the charts throughout most of 2016, they were down significantly in the Q1 2017 test cycle. Figure 10 below indicates that there were just 133 messages per day on average with Ransomware archives attached. Thus, the average number of spam emails with ransomware received during the Q1 2017 ATD daily test cycle was over 68,000 fewer than the daily average the previous quarter.

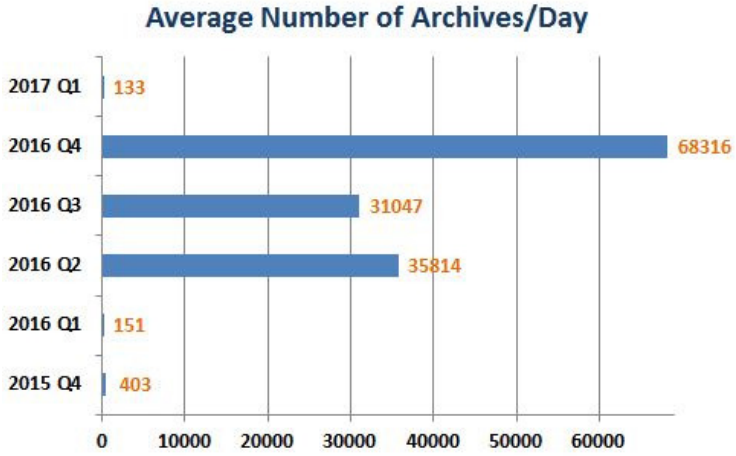


Fig. 10 – Ransomware Per Day Averages During Recent ATD Test Cycles

Regarding The Samples From This Test Cycle

Samples harvested for use in ATD testing are often unmodified and used as is. That is the case if ICSA Labs determines that the sample is new enough and/or not being detected by traditional security products. In many cases malicious samples require modification before they can avoid detection by traditional security products.

Of the 445 malicious samples, Figure 11 shows that there were many more original samples used and far fewer samples that required some kind of modification before use in testing. As there were many more unmodified samples, Figure 12 reveals the source of the 349 malicious samples used in testing that were both unmodified and non-dropped (i.e., not left behind by other malware).

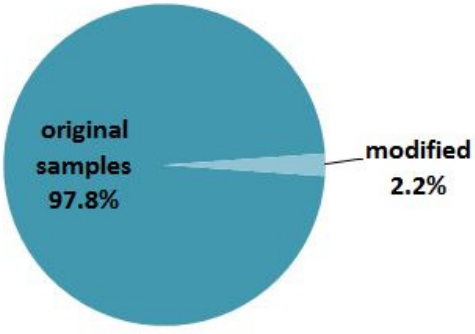


Fig. 11 –Malicious Samples – Original vs. Modified

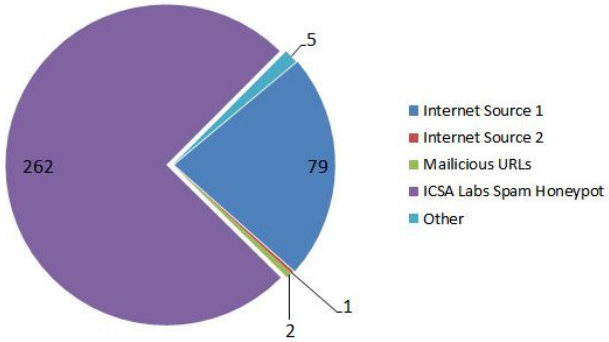


Fig. 12 – Unmodified/Non-Dropped Sample Sources

Prior ATD Reports

With this report, the Cyphort Anti-SIEM passed all the test cases to earn ICSA Labs Advanced Threat Defense Certification. Thus there are no earlier ICSA Labs Advanced Threat Defense Certification testing reports for the Cyphort Anti-SIEM advanced threat defense solution.

Significance of the Test & Results

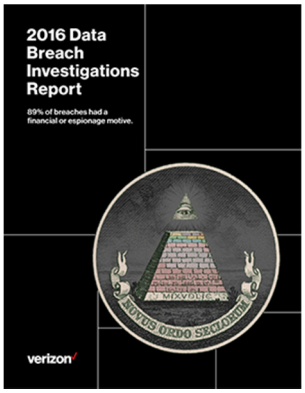
Readers of certification testing reports often wonder what the testing and results really mean. They ask, "In what way is this report significant?" The four statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested the Cyphort Anti-SIEM platform using the primary threat vectors leading to enterprise breaches according to Verizon's Data Breach Investigations Report (DBIR).

2. ICSA Labs tests with malicious threats that other security products typically miss.

3. The Cyphort Anti-SIEM demonstrated excellent threat detection effectiveness against nearly 450 *new and little-known* threats.

4. The Cyphort Anti-SIEM had few false positives during testing.



Authority

Report Date: April 5, 2017

This report is issued by the authority of the Managing Director, ICSA Labs. Tests are done under normal operating conditions.

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 20 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Cyphort, Inc.

Cyphort, Inc. is a network security company providing mid- and large-size enterprise customers with the innovative Adaptive Detection Fabric, a scalable software solution designed to integrate with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011, is privately-held, and distributes its software through direct sales and channel partners across North America and international markets. Learn more at www.cyphort.com.

Cyphort, Inc.
5451 Great America Pkwy
Suite 225
Santa Clara, CA 95054