

# Awake Security Platform

## Evaluating the Evolution of Network Traffic Analysis:

### Awake Security Platform vs. Darktrace Enterprise Immune System

#### EXECUTIVE SUMMARY

Threats to enterprise network security have evolved in complexity and sophistication. Protecting your network by catching virus fingerprints is a thing of the past. Today, threats are multi-faceted and often try to camouflage themselves within normal traffic flows. Network detection and response (NDR) solutions focus on ferreting out such attacks.

Awake Security, Inc. commissioned Tolly to evaluate the Awake Security Platform and compare it to the Darktrace Enterprise Immune System. Awake provided test scenarios that its customers have identified as relevant. Testing was performed in a live, high-tech company's production environment and was comprised of five different scenarios that exercised different methods of data theft, exfiltration and credential theft that ran over common protocols and programs such as browsers, DNS and SMB file protocols.

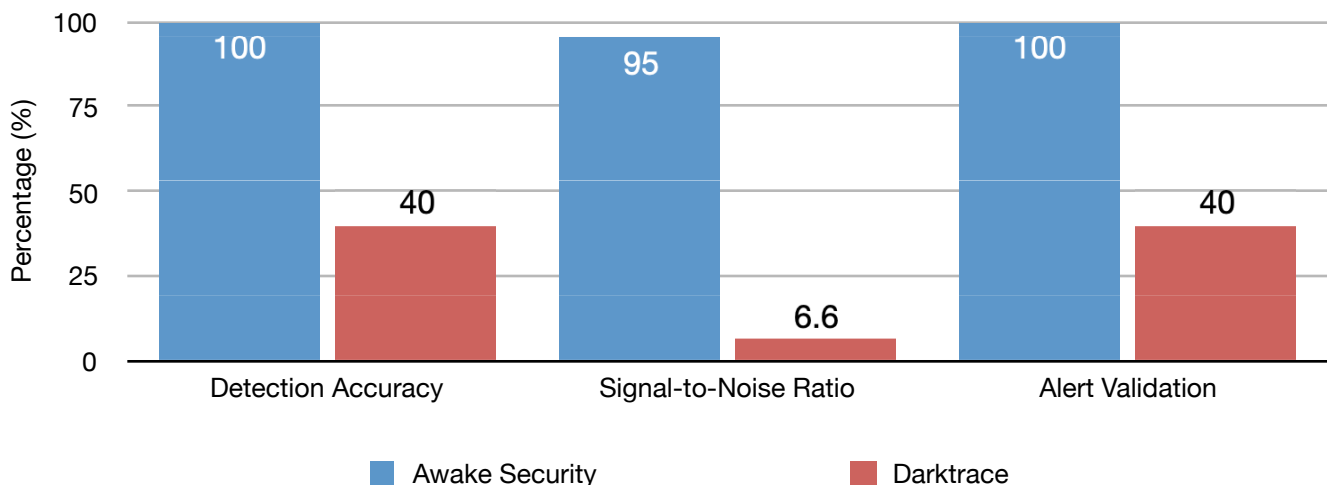
Tests showed that the Awake Security solution detected significantly more threats across the full suite of malicious behavior detection tests. See Figure 1.

#### THE BOTTOM LINE

The Awake Security Platform delivered:

- 1 2.5X greater accuracy (100% vs 40%)
- 2 Better signal-to-noise ratio (95% vs 13.5%)
- 3 Better validation of attacks (100% vs 40%)
- 4 Intuitive, powerful user interface
- 5 Advanced architecture with multiple detection engines and rich security-focused search capabilities

**Awake Security Platform vs. Darktrace Enterprise Immune System**  
**Threat Detection: Five Scenarios - Overall Summary**



Notes: Higher numbers are better. Signal-to-noise ratio (SNR) represents the percentage of accurate and relevant alerts vs. all alerts generated.

Source: Tolly, August 2019

Figure 1

# Background & Overview

Network traffic analysis technology is rapidly evolving from simple anomaly-based reporting to a more advanced, multi-faceted system that monitors, correlates and integrates a broad range of data points to deliver higher fidelity, actionable intelligence.

For this test, five attack scenarios were used to evaluate the responses of the two network detection and response (NDR) systems under test. (See sidebar.) Testing was conducted at a current Darktrace customer site that was evaluating the Awake Security Platform. See Figure 2.

# Test Results

## Summary

Awake recognized all five attack scenarios, Darktrace recognized two of the five. See Figure 1 and Table 2.

Quantitatively, Tolly engineers determined that Awake generated only one non-actionable, "noisy" alert compared to over 50 for Darktrace. Excessive irrelevant alerts can lead to "alert fatigue" where an operator tends to ignore alerts. This could cause an actual problem or threat to be masked or overlooked. Qualitatively, Tolly engineers noted that the Awake system was easier to use and more intuitive than Darktrace. It was easy to note alerts and follow through

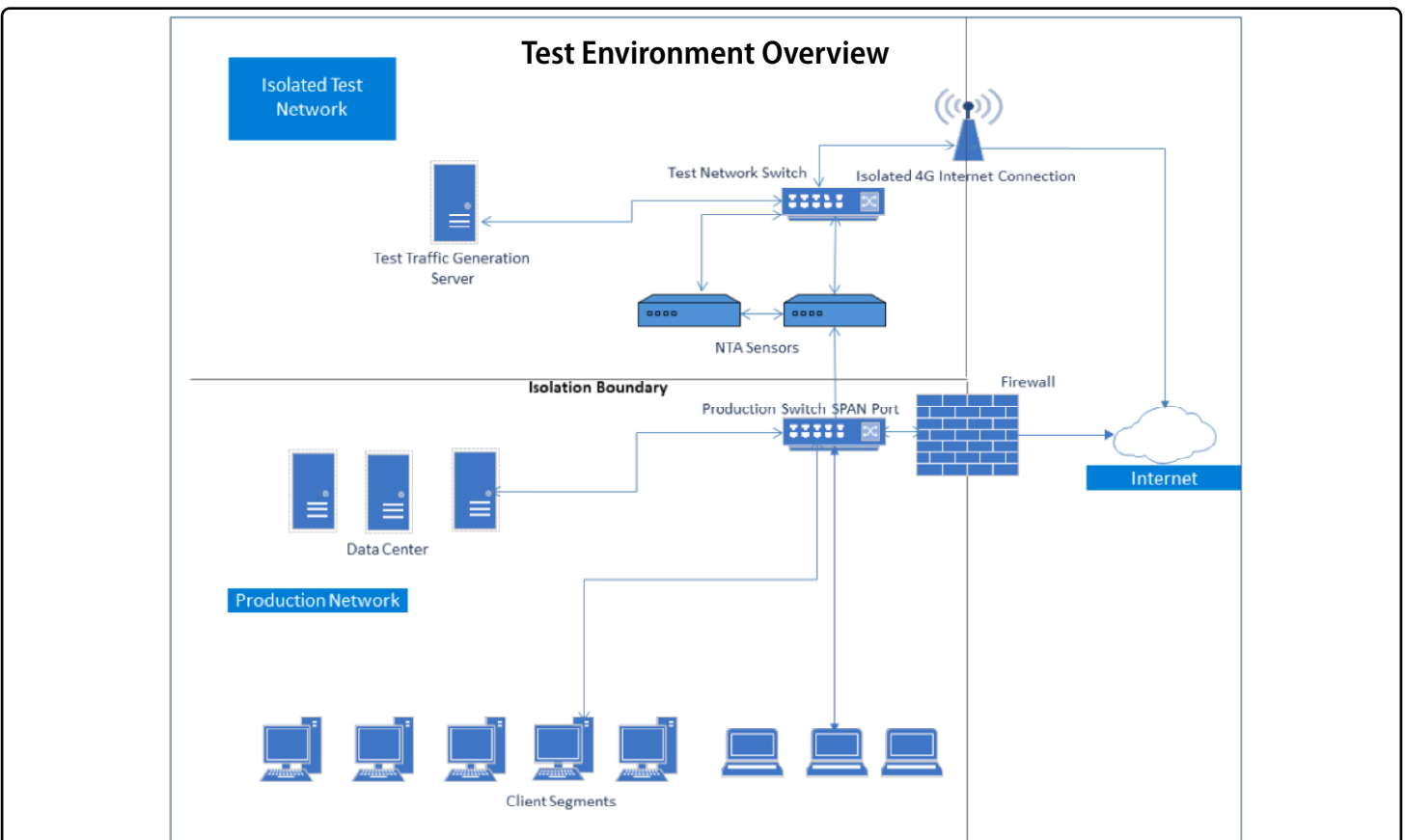
## Testing Network Detection & Response

At present, commercial security testing products do not provide tools for evaluating NDR.

For this test, Awake Security identified five attack scenarios relevant to its customers and built scripted traffic streams to generate the threat scenarios. The test cases were based on techniques identified by MITRE Corp's ATT&CK™ framework. [attack.mitre.org](http://attack.mitre.org)

Both systems tested use profiles of "normal" traffic which is difficult to duplicate in a lab setting. This test included "live" customer production traffic to provide the real-world behavior needed to ensure that accurate profiles could be built by the units under test.

to validation and investigations when needed.



Source: Tolly, August 2019

Figure 2



### Solutions Under Test

| Vendor         | Product Name             | Version | Build                         |
|----------------|--------------------------|---------|-------------------------------|
| Awake Security | Awake Security Platform  | 3.0     | 2019-07-11                    |
| Darktrace      | Enterprise Immune System | 3.1.0   | 3.1.899-20190426 bundle 31107 |

Source: Tolly, August 2019

Table 1

Awake Security, Inc.

Awake Security Platform

Network Traffic Analysis



Tested August 2019

### Awake Security Platform vs. Darktrace Enterprise Immune System Threat Detection Scenario Detailed Results

| Scenario                            | Attack Detection   |  | Noisy Alerts       |                                  | Alert Validated   |   |
|-------------------------------------|--|--|--------------------|----------------------------------|---|---|
|                                     | Awake Security   | Darktrace  | Awake Security     | Darktrace                        | Awake Security  | Darktrace   |
| #1 IoT Exfiltration                 | 1 for exfiltration, 2 for command and control              | No (zero)  | No                 | No                               | Yes (upload to external site detected)  | No (threat undetected)  |
| #2 Data Theft via Browser           | 3 command and control, 1 exfiltration, 1 credential access | No (zero)  | No                 | Yes (18 Dropbox activity alerts) | Yes (cookie log captured on upload)   | No (threat undetected)  |
| #3 Exfiltration via DNSCAT          | 1 DNS tunneling alert                                      | No (zero)  | No                 | Yes (14 Dropbox activity alerts) | Yes (file captured with DNSCAT header)  | No (threat undetected)  |
| #4 Insider Threat via SMB           | 2 exfiltration, 2 lateral movement, 1 command & control    | 2 suspicious domain  | No                 | Yes (12 Dropbox activity alerts) | Yes (user connecting to admin\$ shares and downloading files)                                 | Yes (large volume of unsuccessful logins recorded)                  |
| #5 Credential Theft via Brute Force | 2 credential access, 2 lateral movement, 1 exfiltration    | 1 large volume of Kerberos failures, 1 Kerberos password brute force | Yes (1 compliance) | Yes (12 Dropbox activity alerts) | Yes (record of numerous failed login attempts followed by a successful login and rdp capture) | Yes (record of numerous failed login attempts in short time period) |

Notes: "Yes" is the desired result for "alerts validated" and "accurate alerts." "No" is the desired outcome for noisy alerts.

Source: Tolly, August 2019

Table 2

# #1. IoT Exfiltration

## Threat Overview

In this test case three similar Raspberry Pi IOT devices perform standard video surveillance tasks. One of the three devices (raspberryp3) is set up to perform a “low and slow” exfiltration of data to an attacker-controlled site hosted on a common cloud provider. The challenge is to identify these signs of malicious activity from a device that is behaving differently from similar single function devices on the network.

## MITRE ATT&CK Reference

This attack scenario uses techniques as described in ID: [T1020](#) - Tactic: Exfiltration.



### Awake Security Detail: Test #1

**This Device**

56 raspberryp3

**Threat Behaviors**

80 Exfiltration: Persistent non-browser TLS upload

57 C2: Weekly check-in for commands to cloud stor

53 C2: Multiple check-ins for commands to cloud s

## Expected Results

An alert indicating that a device is exfiltrating data. Validation of this alert should show that of the three identical devices only one exhibits exfiltration and remote control behavior confirming that the unit may be compromised.

## Awake Results

Awake correctly identified the single IOT device among the 3

deployed which was under an attacker’s control.

## Darktrace Results

Darktrace did not identify the malicious behavior or generate alerts of any kind on the Raspberry Pi devices.

## Comments

Correlation of multiple types of behavior into a single overall event makes it much easier and quicker to determine if a real security breach has occurred.

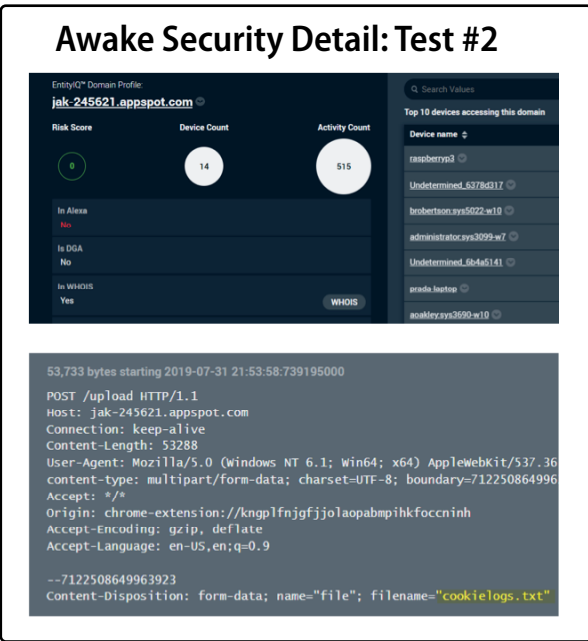
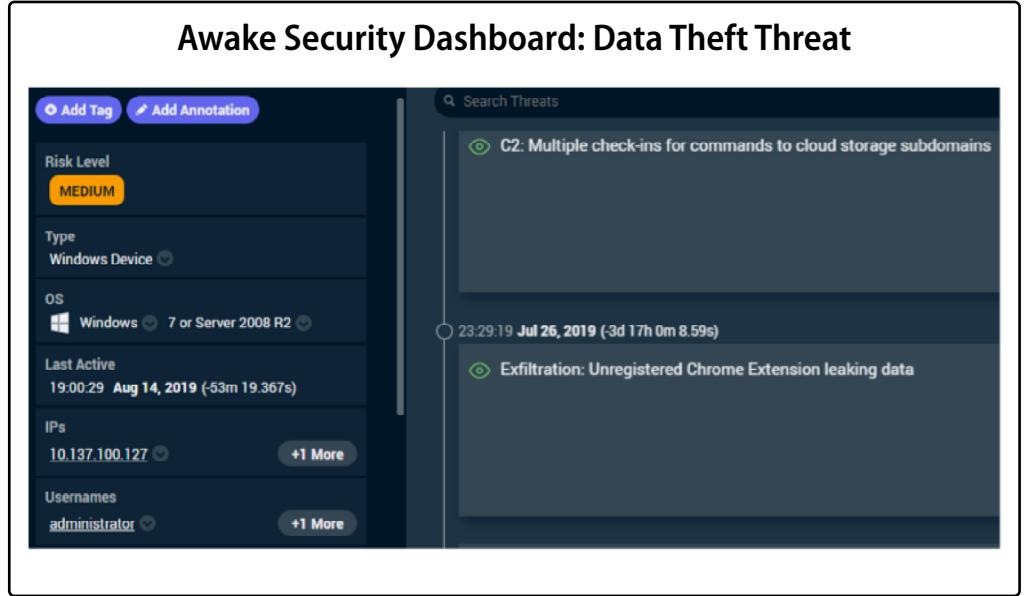
| Scorecard: Test Case #1 IoT |   |           |   |
|-----------------------------|---|-----------|---|
| Category                    | Awake Security                          | Darktrace | Comment   |
| Accurate Detections         | 1 exfiltration, 2 command and control   | 0         | An alert detailing malicious activity from the system generating the test case traffic  |
| Noisy Alerts                | 0                                       | 0         | Any alert associated with the system generating the test case traffic not specifically identified as malicious or high priority |
| Attack Validated            | Yes, upload to external site documented | 0         | Ability to validate the attack using tools provided. I.E. links to details on malicious domains, data capture etc.              |

Source: Tolly, August 2019 Table 3

## #2. Data Theft

### Threat Overview

In this test an unregistered Google Chrome browser extension has been configured to gather information on the endpoints browsing history and cookies and communicate these to an attacker-controlled site hosted on a common cloud provider for both command and control and data exfiltration.



### MITRE ATT&CK Reference

This attack scenario uses techniques as described in ID: [T1041](#) -Exfiltration Over C&C Channel.

### Expected Results

An alert indicating data exfiltration and/or use of a suspicious application or command and control activity.

### Awake Results

Awake identified five different malicious activities for this event across the kill chain. A sample of the stolen data was

captured for validation of the activity as malicious.

### Darktrace Results

Darktrace did not identify any malicious behavior, but did record the that the system in question showed Dropbox activity. Dropbox was not used as the destination of the stolen data.

### Comments

Validating the accuracy of an alert generated by a behavioral based system can be a time consuming process. Packet captures (provided by both systems) are useful, but the more data points provided the better.

### Scorecard: Test Case #2 Data Theft

| Category            | Awake Security                                   | Darktrace            | Comment   |
|---------------------|--|----------------------|---|
| Accurate Detections | 3 C2 events, 1 exfiltration, 1 credential access | 0                    | An alert detailing malicious activity from the system generating the test case traffic  |
| Noisy Alerts        | 0  | 18 Dropbox activity  | Any alert associated with the system generating the test case traffic not specifically identified as malicious or high priority |
| Attack Validated    | Yes, cookie logs captured                        | No alert to validate | Ability to validate the attack using tools provided. I.E. links to details on malicious domains, data capture etc.              |

Source: Tolly, August 2019

Table 4

### #3. Data Exfiltration

#### Threat Overview

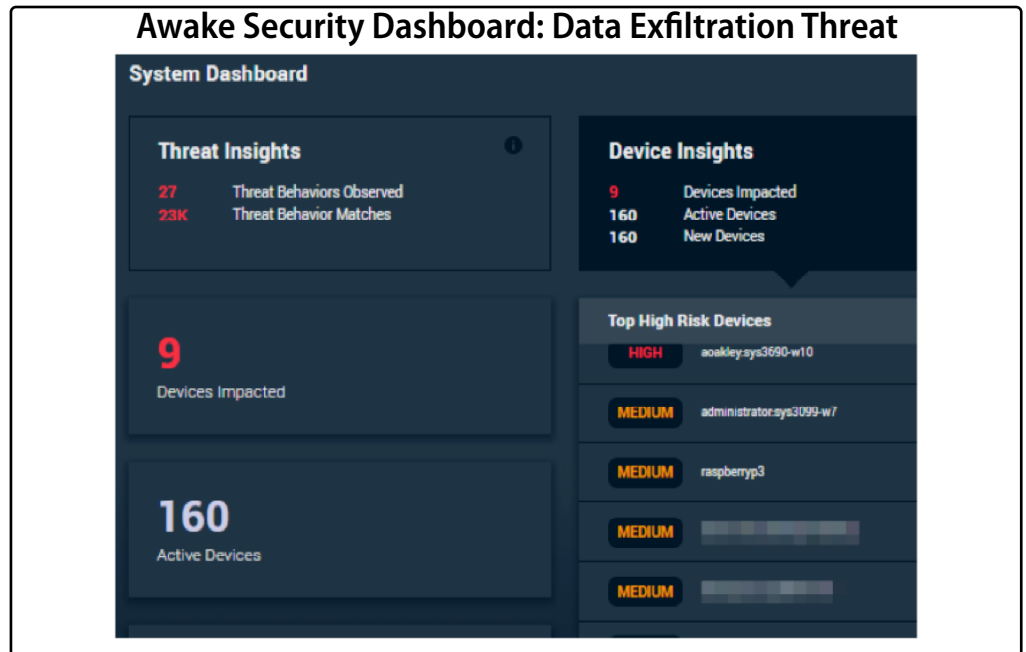
This test uses a common DNS tunneling tool (dnscat2) to perform tunneling to an external network entity to perform a “low and slow” transfer of sensitive files outside the organization.

#### MITRE ATT&CK Reference

This attack scenario uses techniques as described in ID: [T1048](#) - Exfiltration Over Alternative Protocol.

#### Expected Results

An alert indicating data exfiltration via a DNS tunnel. Validation of this alert includes the ability to view PCAPs of DNS Tunnel



packet sequence to confirm the DNSCAT label is embedded in the packets. DNSCAT

is a well-known “penetration testing” tool often used by attackers.

#### Awake Results

Awake raised a “DNS Tunneling Suspected” alert for this attack. Data captured shows packet headers containing “dnscat” label.

#### Darktrace Results

Darktrace did not identify any malicious behavior, but did record that the system in question showed dropbox activity. Dropbox was not used as the destination of the exfiltrated data.



#### Scorecard: Test Case #3 Data Exfiltration

| Category            | Awake Security                          | Darktrace              | Comment   |
|---------------------|---|------------------------|---|
| Accurate Detections | 1 DNS Tunneling alert                   | No malicious alerts    | An alert detailing malicious activity from the system generating the test case traffic  |
| Noisy Alerts        | 0                                       | 14 drop box activities | Any alert associated with the system generating the test case traffic not specifically identified as malicious or high priority |
| Attack Validated    | Yes, packet captured with DNSCAT header | 0                      | Ability to validate the attack using tools provided. I.E. links to details on malicious domains, data capture etc.              |

Source: Tolly, August 2019

Table 5



## #4. Insider Threat

### Threat Overview

A legitimate but malicious insider uses "built-in" operating system tools to gather sensitive files from other network devices. The insider connects directly to the IP addresses of other systems using Windows SMB to connect to sensitive administrative shares. The files are then exfiltrated to an attacker-controlled site on a common cloud provider.

### MITRE ATT&CK Reference

This attack scenario uses techniques as described in ID: [T1077](#) - Lateral Movement – Windows Admin Shares.

### Expected Results

An alert indicating data exfiltration, and/or lateral movement or command and control activity.

### Awake Results

Five malicious activities identified across the kill chain. Access to sensitive windows shares (admin\$) recorded.

### Darktrace Results

Two alerts on Suspicious Domain access. Model identifies any domain ending in .RU as being suspicious.

### Comments

Identifying this complex attack by a legitimate user without the use of any

malicious code is a very challenging use case.

### Awake Security Detail: Test #4

#### This Device

**54** brobertson:sys5022-w10

#### Threat Behaviors

**80** Exfiltration: Persistent non-browser TLS upload

**76** Exfiltration: Internal download closely followed

**53** C2: Weekly requests from C2 server hosted on c

**28** Discovery: Direct-to-IP SMB C drive access

**28** Download: User collecting files from multiple se

### Scorecard: Test Case #4 Insider Threat

| Category            | Awake Security  | Darktrace                                      | Comment   |
|---------------------|---|--|---|
| Accurate Detections | 2 Exfiltration, 2 lateral movement, 1 command & control | 2 suspicious domain                            | An alert detailing malicious activity from the system generating the test case traffic  |
| Noisy Alerts        | 0   | 12 dropbox activity                            | Any alert associated with the system generating the test case traffic not specifically identified as malicious or high priority |
| Attack Validated    | Yes, PCAP showing download of file "Netsetup.log".      | Yes, Domain is suspicious due to .RU extension | Ability to validate the attack using tools provided. I.E. links to details on malicious domains, data capture etc.              |

Source: Tolly, August 2019

Table 6



## #5. Credential Theft

### Threat Overview

A vulnerable admin account is compromised via a Kerberos brute force attack. Lateral movement is then initiated by an authenticated RDP session to transfer files back to the malicious system where the data is then exfiltrated to an attacker-controlled site on a common cloud provider.

### MITRE ATT&CK Reference

This attack scenario uses techniques as described in ID: [T1110](#) - Credential Access – Brute Force.

### Expected Results

An alert indicating a brute force password attack followed by lateral movement and a download via RDP protocol.

### Awake Results

Five malicious activities identified across the kill chain. Access to sensitive windows shares (admin\$) recorded.

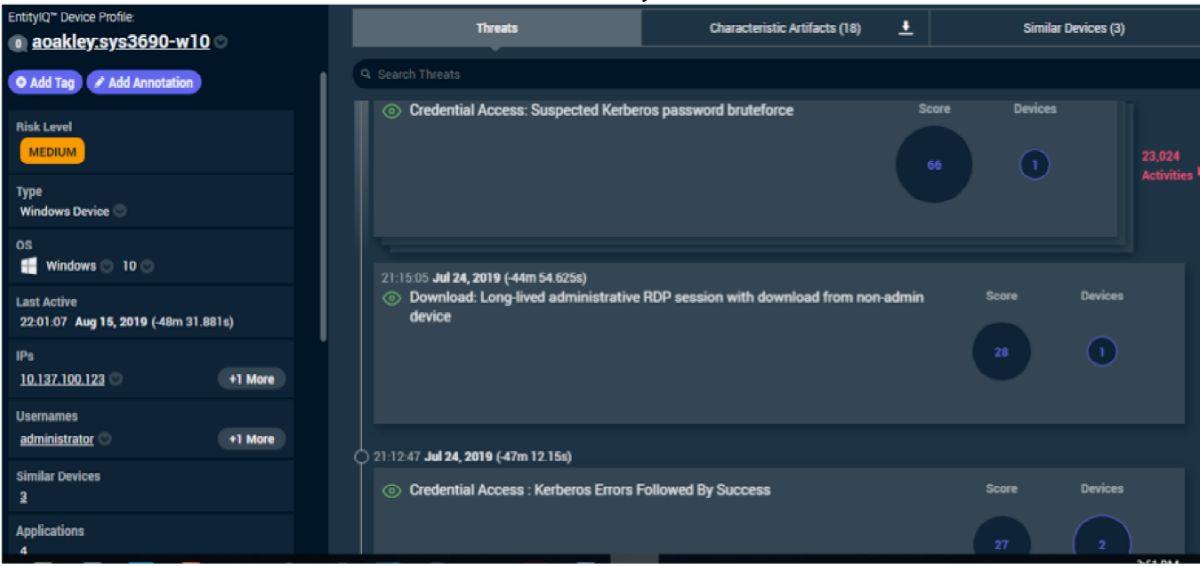
### Darktrace Results

Two user/Kerberos password brute force alerts were generated. A high volume of failed Kerberos login attempts was recorded.

### Comments

This is another complex attack chain, however the use of a brute force password attack to initiate the breach should allow the attack to be detected early.

### Awake Security Detail: Test #5



### Scorecard: Test Case #5 Credential Theft

| Category            | Awake Security   | Darktrace  | Comment   |
|---------------------|--|--|---|
| Accurate Detections | 2 credential access, 2 lateral movement, 1 exfiltration                                      | Large volume of Kerberos failures, Kerberos password brute force   | An alert detailing malicious activity from the system generating the test case traffic  |
| Noisy Alerts        | 1 compliance, traffic to paste site alert  | 12 dropbox activities  | Any alert associated with the system generating the test case traffic not specifically identified as malicious or high priority |
| Attack Validated    | Yes, record of numerous failed login attempts followed by a successful login and rdp capture | Yes, record of numerous failed login attempts in short time period | Ability to validate the attack using tools provided. I.E. links to details on malicious domains, data capture etc.              |

Source: Tolly, August 2019

Table 7





# Test Setup & Methodology

## Overview and requirements

NDR solutions offer a wide range of capabilities and functionality. Fully testing all the capabilities of these solutions is beyond the scope of this test. Instead, this methodology focuses on examining five key use cases an NDR solution must address and its ability to deliver the key requirements outlined above.

NDR solutions are different than most other security solutions as they focus on delivering tools, workflows and context for use by a human operator rather than solely relying on the automatic blocking or prevention of an arbitrary action like a firewall or an endpoint protection system. This methodology will test for “detection effectiveness” and solution “efficiency and usability” which will provide a measurement of both of the key requirements of these systems with both objective and subjective scoring.

NDR systems incorporate behavioral analysis elements and are dependent on monitoring “real-world traffic” vs artificially generated load traffic used for stress testing network gear for the best functionality. Therefore this test will include the use of “live” production network traffic rather than artificially generated load traffic which is commonly used to test network device throughput.

NDR solutions are designed to detect post compromise, malicious events rather than traditional malware or exploit payloads. For this test malware detection will not be performed, with the focus being on

malicious events which will be generated using a suite of penetration tools similar to what can be found in an advanced “Red Team” tester’s toolbox.

## Key Test Cases

**IOT Threat Detection:** Identifying unique or pre-existing compromises that don’t trigger an alert is one of the greatest current challenges for the security professional. This test will examine the systems capabilities for finding a previously undetected compromise from an IOT device exfiltrating data.

**Data Theft Detection:** The theft of data via an undetected breach or compromise (often referred to as North-South traffic) is a key area of concern for organizations. In this test we will determine the solution’s ability to detect and validate an active “Man in the Browser” using an un-registered Chrome extension that results in compromise and the exfiltration of data to an external destination.

**Data Exfiltration Detection:** This test looks at the ability to detect the use of common penetration testing tools for illegitimate purposes. The well-known tool DNSCAT2 is used to exfiltrate sensitive password files to an AWS instance.

**Insider Threat Detection:** This test case examines a legitimate user using their valid credentials and standard tools to harvest sensitive data from internal systems and exfiltrate the data using a “low and slow” technique to an external domain with a good reputation.

**Credential Theft Detection:** Many damaging breaches include an attacker’s theft of legitimate credentials at some stage of the attack chain. This scenario tests the ability of the system to detect a credential attack in progress, lateral

movement using the compromised credentials and finally exfiltration of the data to an external, legitimate domain controlled by the attacker.

## Test Execution Protocol

As NDR systems are used in the “real world” by “real operators”, each use case scenario is designed to test how a production user would experience these use cases in their production environment. For each of the use cases tested the following protocol will be followed.

**Training Baseline:** Both systems are trained side by side on a mix of production and event generation traffic to establish baselines of behavior. Some of the event generation traffic will represent the existence of malicious actors on the network.

**Event Generation:** Systems exhibiting subtle traces of malicious behavior that has been recently observed “in the wild” will be included which use common tools and techniques to perform malicious activities.

## Test Case Scoring Protocol

**Alert Validated.** Determine whether NDR accurately detected the threat scenario.

**Alert Accuracy.** Determine accuracy of alerts. Note number and content of alerts. A higher number of accurate alerts is better.

**Noisy Alerts.** Note number and content of alerts deemed irrelevant to the threat. These alerts could distract or possibly mask the actual problem. A lower number of noisy alerts is better.

**Signal-to-Noise Ratio (SNR).** This number is calculated by comparing the number of accurate alerts to the number of noisy alerts. A higher SNR is better.



## Testing Environment

This test methodology incorporates real time monitoring of an actual "production network" to ensure that the units under test are provided a fully realistic environment for evaluation. An "Event Generation" network is used to host the "Test Case" systems which perform activities that mirror current Tactics, Techniques and Procedures used by attackers. Using a dedicated network to generate these behaviors ensures that results are directly attributable to the events generated during the test. See Figure 1 and Table 2.

## Event Generation Tools

Event generation is performed using a number of virtual machines executing Python scripts that perform the behaviors desired for each test case. A total of eight client systems and one server are hosted using VMware ESXi 6.7 running on an industry standard server. Six of the test generation systems perform activities indicative of a post breach attack with the remaining two systems performing a range of standard business user activities to serve as a bench mark. Each benchmark system is scripted to perform over 50 activities across a five day period representative of a standard work week. Activities include:

### User-like interactive behavior:

- Browse Google for job-specific terms hourly
- Checking email and clicking on links
- Checking social media (FB, Twitter, LinkedIn)
- Reading the news (various sites)

### Starting up apps:

- Cisco WebEx, TeamViewer, Slack (including clicking on links)

### Getting work done:

- Accessing, uploading, downloading files between similar users (SMB)
- Opening Dropbox and interacting with it

The events incorporated into each test case are executed based on pre-defined timelines to accurately represent both "smash and grab" and "low and slow" attacks that are seen "in the wild. These test generation systems are able to demonstrate complex, multi-stage/multi-day attacks in exactly the way a human operator would perform an attack.

## Signal-to-Noise Ratio

Signal-to-noise ratio (SNR) represents the percentage of accurate and relevant alerts vs. all alerts generated. Testing done with default settings for alerts.

To calculate the SNR, engineers counted the total number of alerts generated by each system as documented in the scorecards and the summary table.

Awake: 20 total alerts with 1 "noisy" alert. 95% of the total alerts were accurate or represented "signal". the remaining 5% was noise.

Darktrace: 60 total alerts, with 4 accurate. This represents 6.6% accurate alerts or "signal" and 93.4% noise.



### About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at [sales@tolly.com](mailto:sales@tolly.com), or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at: <http://www.tolly.com>

### Contact Awake Security



For more information about Awake Security solutions, go to:

<https://awakesecurity.com>

### Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.