Panda Security

Corporate Presentation

Luca Settino
Presales Manager

panda

pandasecurity.com

Great minds and Global Presence

From 1990, Panda Security has become the leading European multinational developing **advanced cybersecurity** solutions, management, and monitoring tools.

We protect
+200M
devices

We care for
+30M
users

We are
+600
employees

Innovating for
27
years

Distribution in
+180
countries

Offices in
55
countries

We have
16
subsidiaries

We speak
23
different languages

The very best put their trust in us

Panda Security named a Visionary in Gartner's Magic Quadrant for EPP

Figure 1. Magic Quadrant for Endpoint Protection Platforms

[1] Gartner 2018 Magic Quadrant for Endpoint Protection Platforms, Ian McShane Eric Ouellet Avivah Litan, Prateek Bhajanka, 24 January 2018

- Gartner[1] describes **EPP Visionaries** to those that:

"… ***deliver in the leading-edge features —*** *such as cloud management, managed features and services, enhanced detection or protection capabilities…* ***— that will be significant in the next generation of products, and will give buyers early access to improved security and management.***"

"Panda Security's ***unique value proposition*** *is the classification or attestation of every single executable file and process on a protected endpoint device,* ***and it is the only vendor to include a managed threat hunting service in the base purchase of its EPP****. Adaptive Defense 360 is fully cloud managed, and combines EPP and EDR into a single offering and single agent. "*

Panda Adaptive Defense 360 provides both managed services, at no extra cost:

100% Attestation Service

Threat Hunting & Investigation Service

. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Panda Security. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[2] Gartner, "Redefining Endpoint Protection for 2017 and 2018", Ian McShane, Peter Firstbrook, Eric Ouellet, 29 September 2017

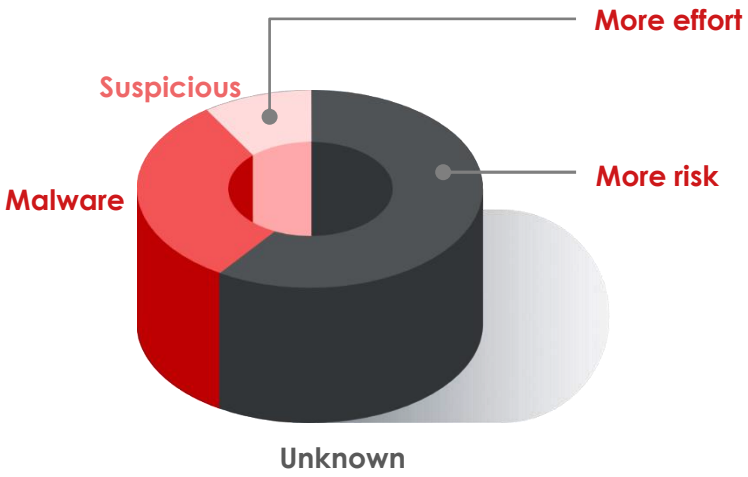
A New Approach to Endpoint Security

The Ability to Anticipate: A Secret Weapon for Intelligent Cybersecurity.

The Prevailing Paradigm…

… is based on **punctual detection** only of **known malicious processes**, this means that:

- All **suspicious activity** has to be **investigated case by case**.
- **All unknown malicious processes are allowed**. That's why attackers skirt around these systems so easily, and their **attacks' success rate is so high**.

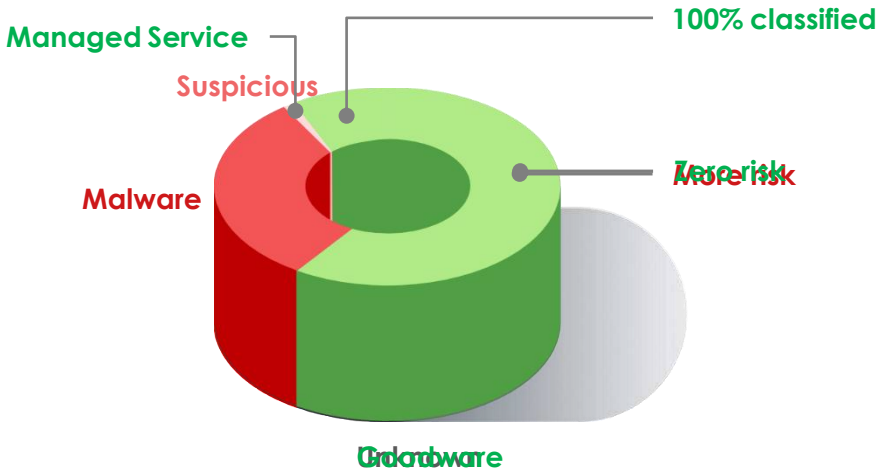


- The result is a higher success rate in attacks, a detection gap.

The Prevailing Paradigm…

It is based on the **classification of absolutely all running processes** on your network.

- All **activity of all programs is monitored and analyzed in real-time**.
- All **behaviors are verified by a managed service**, the admins don't have to investigate anything.
- **Higher level of protection with fewer effort.**



- No application, process, DLL, or script can run unless it is trusted
- The result is a higher protection rate with minimum effort

Mission: Allow to run only binaries Certified by us

All binaries are classified (MW/GW)

Cloud-based Collective Intelligence

Live repository of MW&GW

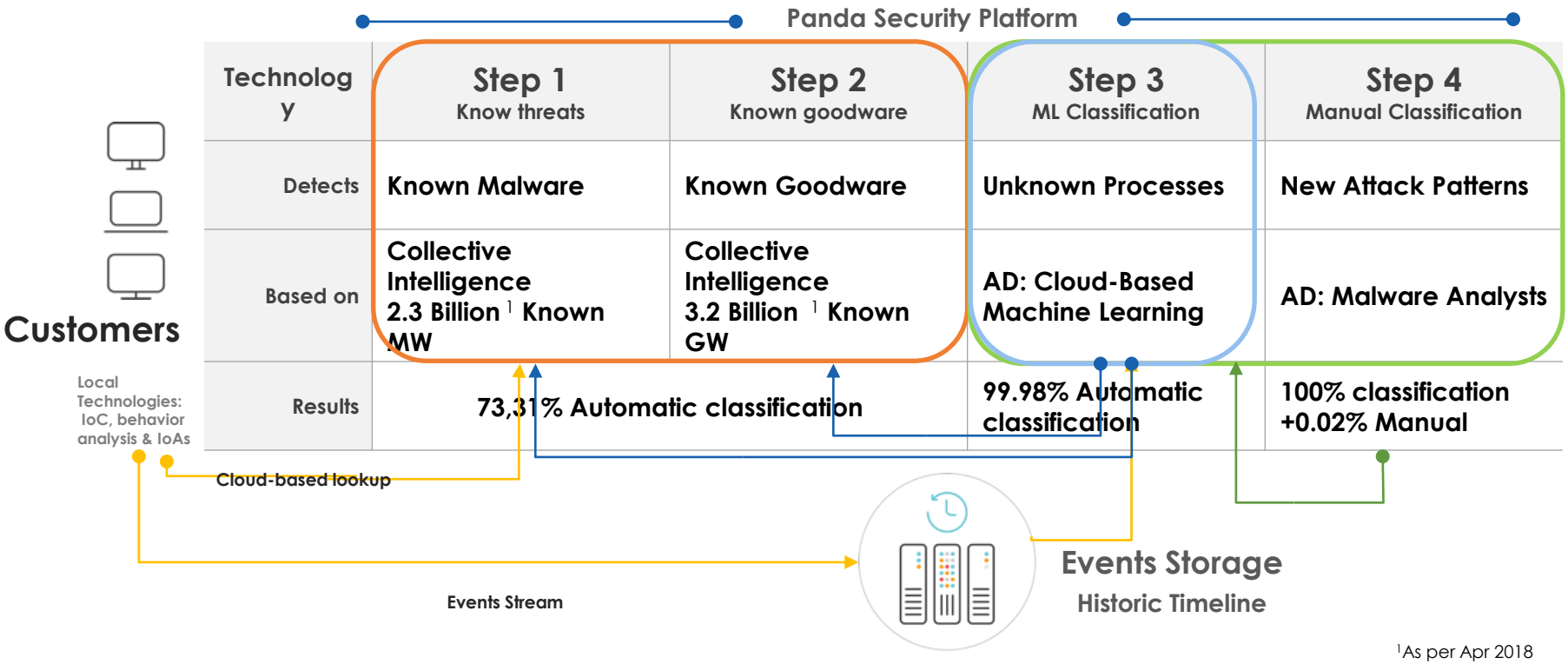
Behavioral, Static and context Cloud-based ML determines all binaries nature in real-time

For each binary: 10,000 attributes

The Service classifies the 100% of them

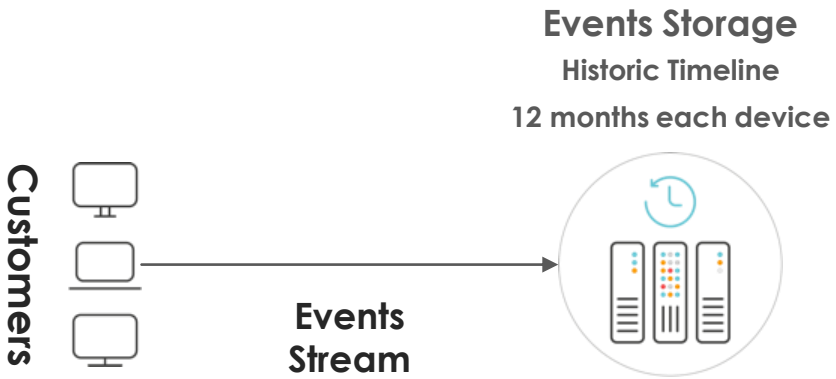
That is why endpoint are not infected by malware

How the 100% Attestation Service works



[1] As per Apr 2018

Event Telemetry



Main events gathered:

Process
- Creation
- Injections

Files
- Creation
- Modification
- Open

Communications
- IPs Origin and Destiny
- Downloads (URLs)

Registry
- Creation
- Modification

Administrative
- Installation
- Turn on/off

The Platform

Global Numbers

~4,000 Events per machine daily

~4 Billions Events processed Daily by Big Data

~500 Billions Events stored (last 12 months)

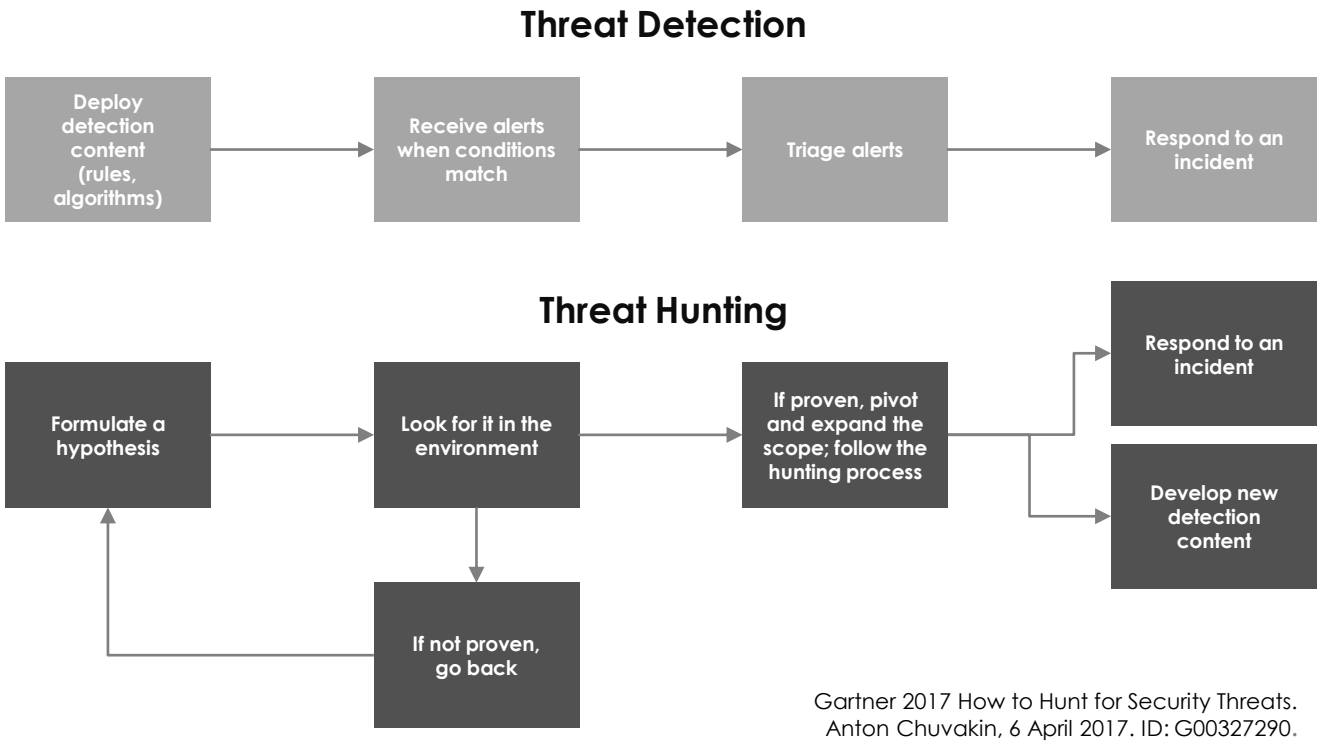
~5,5 Billions Classified processes by Attestation Service

~2,3 Millions New undiscovered Malware &PUP found

99,98% 0,02% 99,98% by Machine Learning 0,02% by Analysts

Threat Hunting

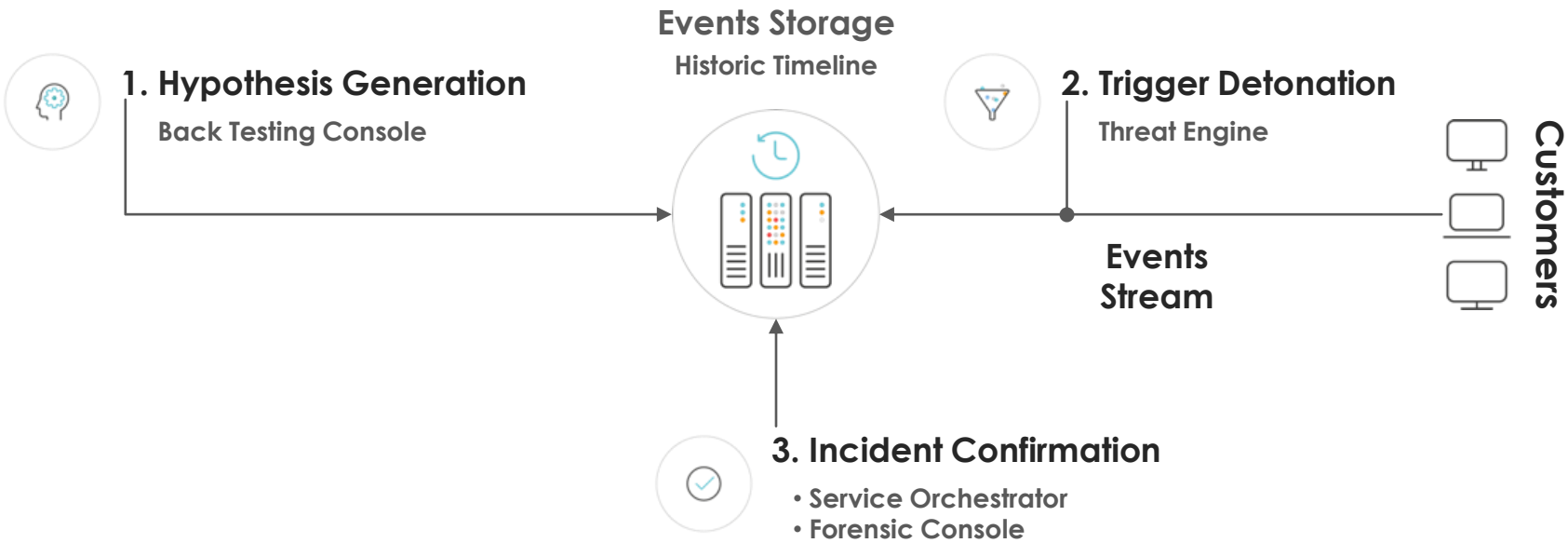
Gartner's Definition: Threat Hunting vs More Traditional Methods of Threat Detection



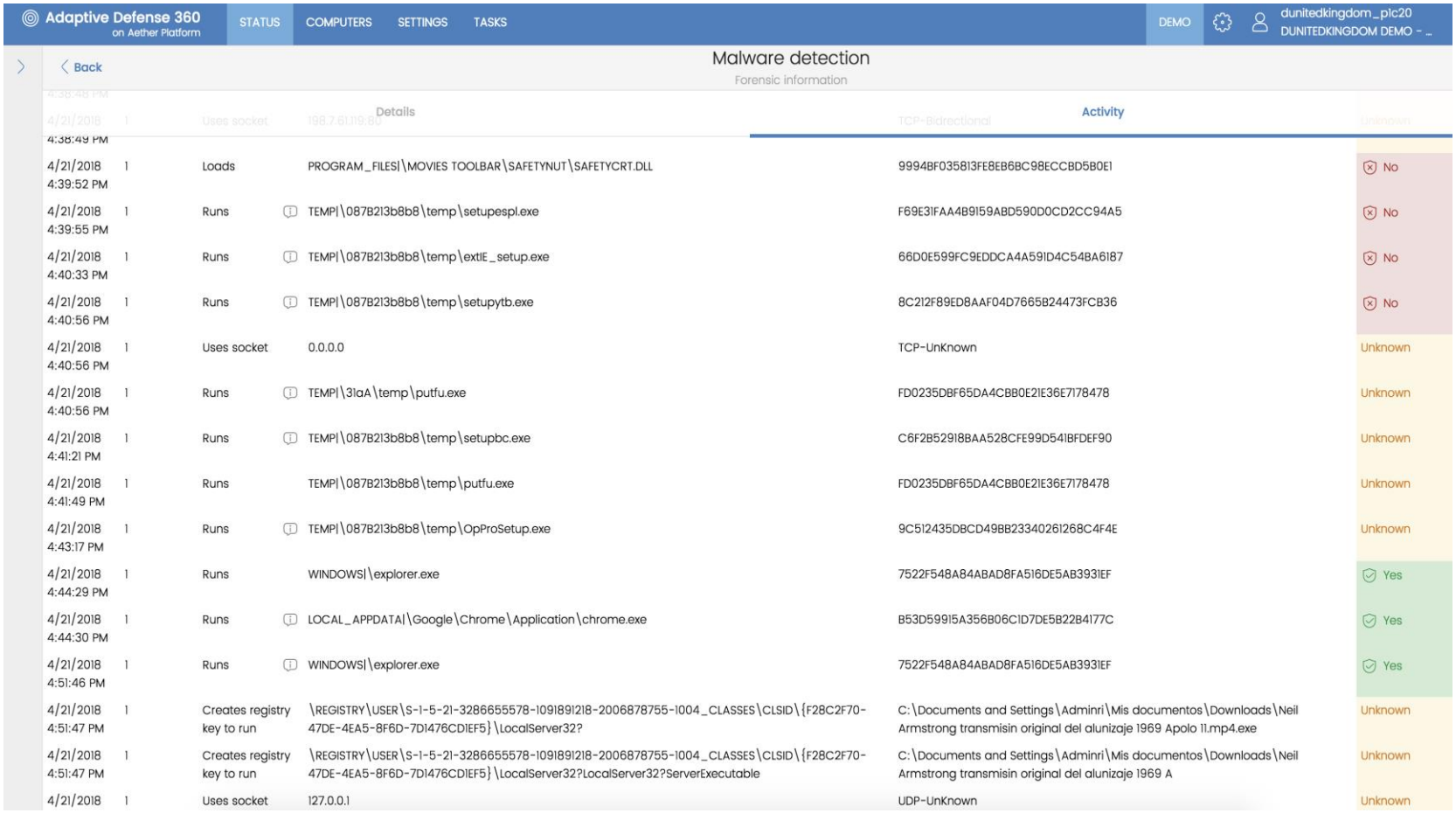
Gartner 2017 How to Hunt for Security Threats. Anton Chuvakin, 6 April 2017. ID: G00327290.

The Threat Hunting Process

Where could we find the attack?

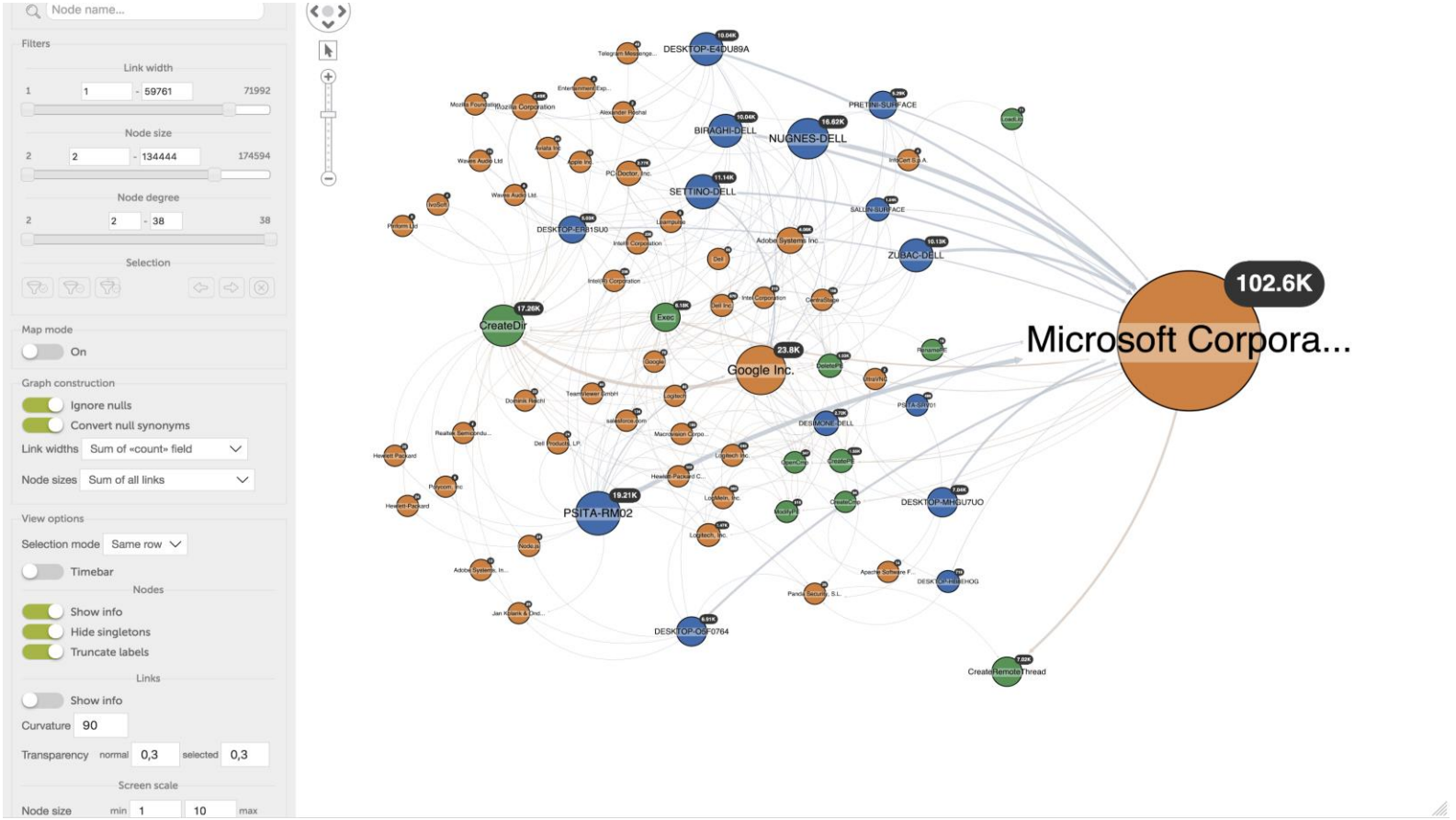


Visibility and Correlation

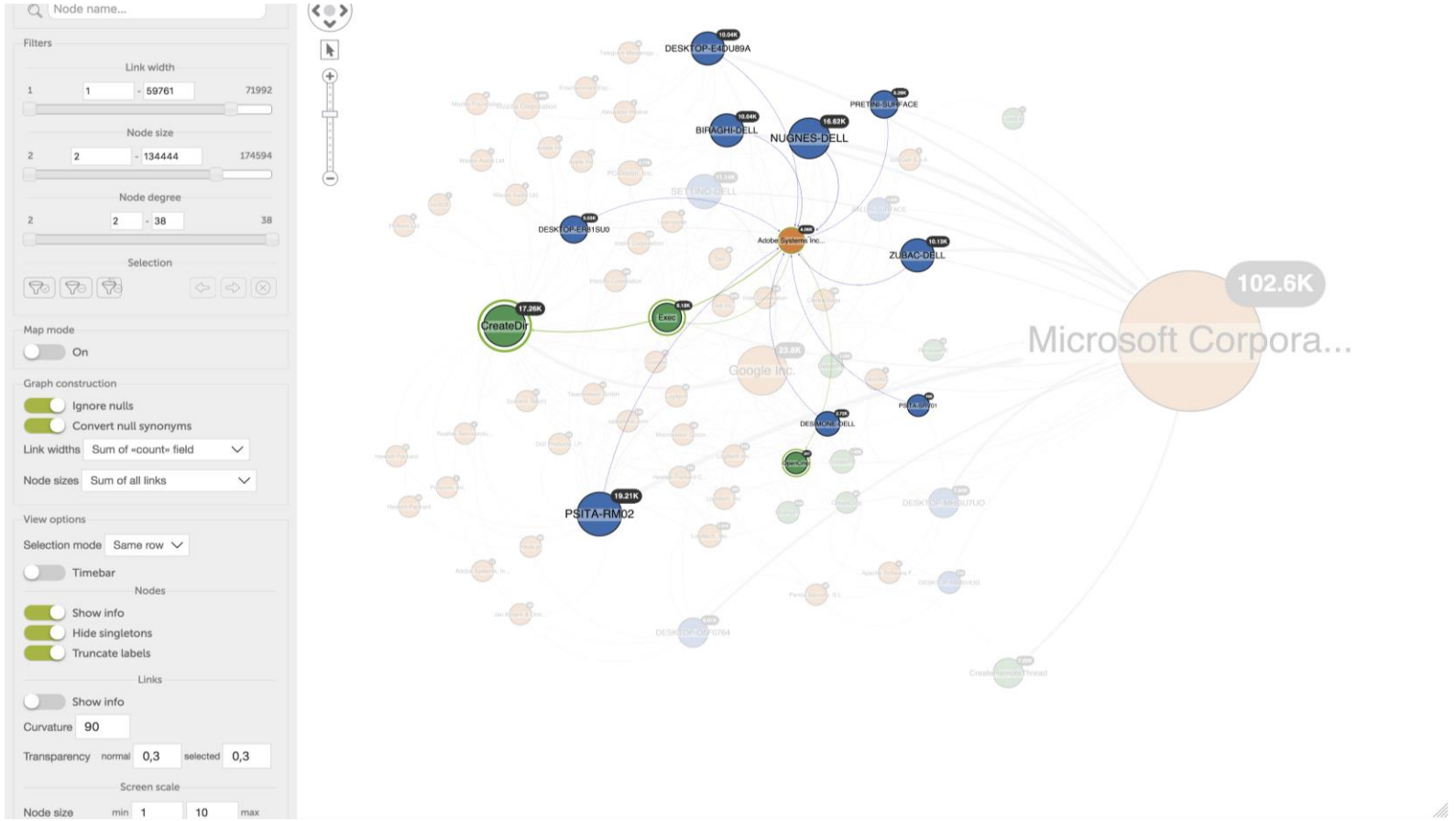


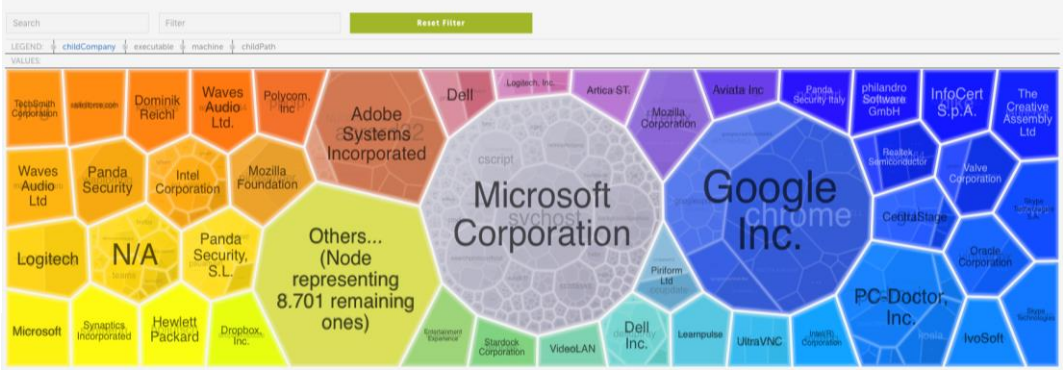
4/21/2018 4:39:52 PM	1	Loads	PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL	9994BF035813FE8EB6BC98ECCBD5B0E1	No
4/21/2018 4:39:55 PM	1	Runs	TEMP|\087B213b8b8\temp\setupespl.exe	F69E31FAA4B9159ABD590D0CD2CC94A5	No
4/21/2018 4:40:33 PM	1	Runs	TEMP|\087B213b8b8\temp\extIE_setup.exe	66D0E599FC9EDDCA4A591D4C54BA6187	No
4/21/2018 4:40:56 PM	1	Runs	TEMP|\087B213b8b8\temp\setupytb.exe	8C212F89ED8AAF04D7665B24473FCB36	No
4/21/2018 4:40:56 PM	1	Uses socket	0.0.0.0	TCP-UnKnown	Unknown
4/21/2018 4:40:56 PM	1	Runs	TEMP|\31aA\temp\putfu.exe	FD0235DBF65DA4CBB0E21E36E7178478	Unknown
4/21/2018 4:41:21 PM	1	Runs	TEMP|\087B213b8b8\temp\setupbc.exe	C6F2B52918BAA528CFE99D541BFDEF90	Unknown
4/21/2018 4:41:49 PM	1	Runs	TEMP|\087B213b8b8\temp\putfu.exe	FD0235DBF65DA4CBB0E21E36E7178478	Unknown
4/21/2018 4:43:17 PM	1	Runs	TEMP|\087B213b8b8\temp\OpProSetup.exe	9C512435DBCD49BB23340261268C4F4E	Unknown
4/21/2018 4:44:29 PM	1	Runs	WINDOWS|\explorer.exe	7522F548A84ABAD8FA516DE5AB3931EF	Yes
4/21/2018 4:44:30 PM	1	Runs	LOCAL_APPDATA|\Google\Chrome\Application\chrome.exe	B53D59915A356B06C1D7DE5B22B4177C	Yes
4/21/2018 4:51:46 PM	1	Runs	WINDOWS|\explorer.exe	7522F548A84ABAD8FA516DE5AB3931EF	Yes
4/21/2018 4:51:47 PM	1	Creates registry key to run	\REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CD1EF5}\LocalServer32?	C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmisin original del alunizaje 1969 Apolo 11.mp4.exe	Unknown
4/21/2018 4:51:47 PM	1	Creates registry key to run	\REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CD1EF5}\LocalServer32?LocalServer32?ServerExecutable	C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmisin original del alunizaje 1969 A	Unknown
4/21/2018	1	Uses socket	127.0.0.1	UDP-UnKnown	Unknown

Visibility and Correlation



Visibility and Correlation



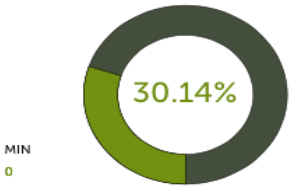


Priority	Alert	Detailed Information	When
●	Executions of Vulnerable apps per endpoint today	The number of vulnerable application executed today in endpoint DESKTOP-E4DU89A is 2	10 hours ago

Real time stats

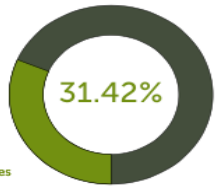
Now 0 EPS - 10.73 Byte/s

Updated 10s ago Average of 5m compared with the max of 6h



MIN 0 MAX 5

2 EPS



MIN 231.96 Bytes MAX 2.17 KB

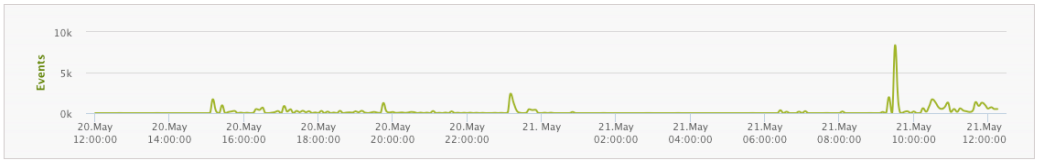
856.32 Bytes/s

Favorite Queries

Alias	Last access date
mycustom.analisys	04-13-2018 11:39
oem.panda.paps.processnetbytes	03-05-2018 22:59
oem.panda.paps.socket	03-05-2018 19:59
oem.panda.paps.processnetbytes	01-23-2018 09:51

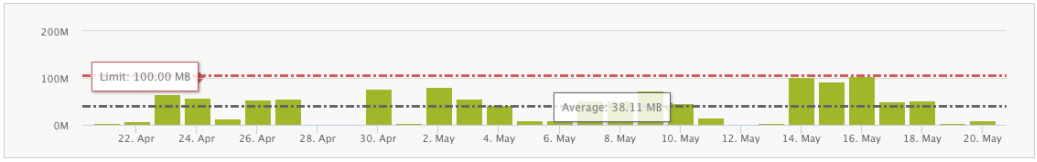
Events Sent

Time Range: 1 day Period: 5 minutes



Size Events Sent

Time Range: 1 month Period: 1 day



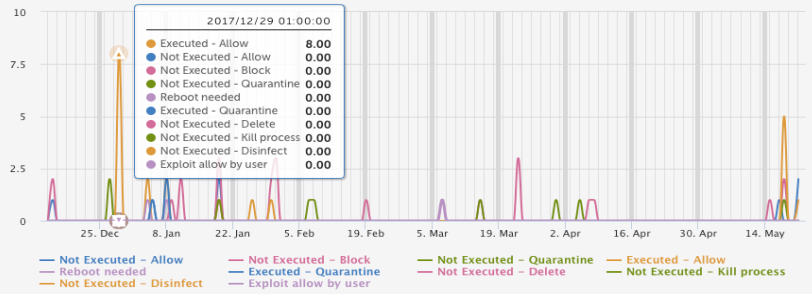
Map

Destinations of outbound network traffic

User operations by device type on PII files

USER	DEVICE TYPE	OPERATION	COUNT	%
AzureAD\CH-LaraZubac	Fixed	Open	64599	87.13%
NT AUTHORITY\SYSTEM	Fixed	Open	2606	3.51%
AzureAD\CH-LaraZubac	No_Root_Dir	Open	1533	2.07%
AzureAD\IT-GianlucaBuscoArre	Fixed	Open	1119	1.51%
AzureAD\CH-SelineMeixner	Fixed	Open	800	1.08%
AzureAD\IT-GiuseppeRizzoPinn	Fixed	Open	441	0.59%
AzureAD\CH-GeorgesSallin	Fixed	Open	422	0.57%
AzureAD\IT-LucaSettino	Fixed	Open	349	0.47%
AzureAD\IT-LauraBiraghi	Fixed	Open	313	0.42%
NT AUTHORITY\SYSTEM	No_Root_Dir	Open	266	0.36%

Incidents Execution status




Reinventing
Cybersecurity.
Thank you.
panda
pandasecurity.com