

**panda**

**Lampros Katsonis**  
Presales Manager



# Let me tell you a story ...



## **The main character**

CY Oil Tanker company

## **Situation**

Malware-less attacks to capture confidential information

## **Target**

Corporate customers' information and credentials

## **Challenge**

Detect attacks from apparently legitimate activity

## **Scenario**

Data leak and compliance investigation

# Let me tell you a story ...



## **The main character**

Hotel Chain Cyprus

## **Situation**

Access to the network through a compromised remote access tool.

## **Target**

Infect with a ransomware 500 endpoints + 60 servers

## **Challenge**

Detect the lateral movements and use of legitimate tools

## **Scenario**

External attack + lateral movements using administrator account



Fri 3/17/2017 6:35 AM

Panda Threats Intelligence Platform <ADThreatEmailAlert@pandasecurity.com>

[Adaptive Defense 360]

] malicious program Alert 3/17/2017 4:34:06 AM UTC

To paps@pandasecurity.com.cy

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear administrator,

Adaptive Defense 360 has detected activity by the malicious program **"Trj/Genetic.gen"** on computer "**-MAILSERVER**", on 3/17/2017 4:34:06 AM UTC.

Please contact our Technical Support team if you have any questions.

#### malicious program details

Computer: -MAILSERVER  
 malicious program name: Trj/Genetic.gen  
 malicious program path: SYSTEMDRIVE|\MAILSERVER.exe  
 malicious program hash: 24481E81232380C97CEC890F5FA31B19

#### malicious program life cycle

Date	Action	Path/URL/Registry/Key	File/Hash/Registry Value	Trusted
3/17/2017 4:32:32 AM UTC	Is run by	WINDOWS \PSEXESVC.EXE	a283e768fa12ef33087f07b01f82d6dd	Yes

#### Occurrences on the network

Computer	First seen	File path
-MATERIAL-C	3/17/2017 3:55:59 AM UTC	3 SYSTEMDRIVE \-MATERIAL-C.exe
-SERVER	3/17/2017 3:56:37 AM UTC	3 SYSTEMDRIVE \-SERVER.exe
MGR1	3/17/2017 4:01:42 AM UTC	3 SYSTEMDRIVE \-CR-MGR1.exe
-REC2	3/17/2017 3:54:40 AM UTC	3 SYSTEMDRIVE \-REC2.exe
-MGR2	3/17/2017 3:55:32 AM UTC	3 SYSTEMDRIVE \-MGR2.exe
-DIRECTOR-2	3/17/2017 3:55:41 AM UTC	3 SYSTEMDRIVE \-DIRECTOR-2.exe
-MAILSERVER	3/17/2017 3:55:57 AM UTC	3 SYSTEMDRIVE \-MAILSERVER.exe
PIO-CHEF	3/17/2017 4:01:40 AM UTC	3 SYSTEMDRIVE \-CHEF.exe
-FRASS	3/17/2017 3:54:47 AM UTC	3 SYSTEMDRIVE \-FRASS.exe

# The purpose of this malware

At first sight the malware seems that it did not perform any malicious activities on the machine.

But the malware managed to configure a Registry entry that will load malware in the startup of the machine

This malware will encrypt the machine in the next startup.

Adaptive Defense 360 has detected activity by the malicious program "Trj/Genetic.gen" on computer " ", on 3/17/2017 12:09:51 PM UTC.

Please contact our Technical Support team if you have any questions.

**malicious program details**

Computer: .  
 malicious program name: Trj/Genetic.gen  
 malicious program path: APPDATA | \usercache\svchost.exe  
 malicious program hash: 24481E81232380C97CEC890F5FA31B19

**malicious program life cycle**

Date	Action	Path/URL/Registry/Key	File/Hash/Registry Value	Trusted
3/17/2017 11:59:33 AM UTC	Modifies registry key to point to an exe file	\REGISTRY\USER\S-1-5-21-2073749359-4067451734-257756863-500\Software\Microsoft\Windows\CurrentVersion\Run?svchost	3   APPDATA   \usercache\svchost.exe	Null
3/17/2017 11:59:36 AM UTC	Has a thread injected by	SYSTEM   \rundll32.exe	dd81d91ff3b0763c392422865c9ac12e	Yes
3/17/2017 11:59:54 AM UTC	Communicates with	190.97.166.61:80	TCP-Download	Null
3/17/2017 12:00:02 PM UTC	Modifies registry key to point to an exe file	\REGISTRY\USER\S-1-5-21-2073749359-4067451734-257756863-500\Software\Microsoft\Windows\CurrentVersion\Run?svchost	3   APPDATA   \usercache\svchost.exe	Null

# Let me tell you a story ...



## **The main character**

Supermarket chains in Cyprus.

## **Situation**

Compromised Remote desktop that was exposed on the internet.

## **Target**

Encrypt customer data and request ransom

## **Challenge**

Detect the origin of the attack

## **Scenario**

Incident investigation + Threat Hunting

**Every organization, regardless of size,  
has the same security aspirations.**

# “Attackers can’t be stopped”

Dedicated nation-state attacks are persistent

Adversaries and malware can be stopped

Using basic defensive steps that are already available



# “All attackers are geniuses”

Attackers are average  
(Electricians, not Einstein)

Use tools passed on  
from others

Brilliant hackers are  
few and far between

# “IT Security knows what to do”

IT Security teams  
are full of intelligent,  
hardworking people

Lacking real data  
to back up beliefs  
about problems

Individuals driven by  
preference, not  
organizational priority

# “Patching is under control”

100,000s of programs with undiscovered bugs

10 to 20 unpatched programs represent the majority of risk

Hardware, firmware, and drivers are frequently missed

**In most cases, “successful” attacks are on the endpoint or user.**

**BUT - It is no longer just about  
“bad file” v “good file” decisions.**

# Infections are Dwindling



- Only hackers represent a challenge
- When they are on the network with admin credentials

## Hackers are the new problem

- Trained by governments, security companies, and criminal organizations
- Create targeted attacks with proprietary malware
- Using applications and goodware to fly under the radar
- An equivalent response to this is needed

**Aside from using EPP, EDR to detect the known knowns or unknown we need to change our way of thinking ...**



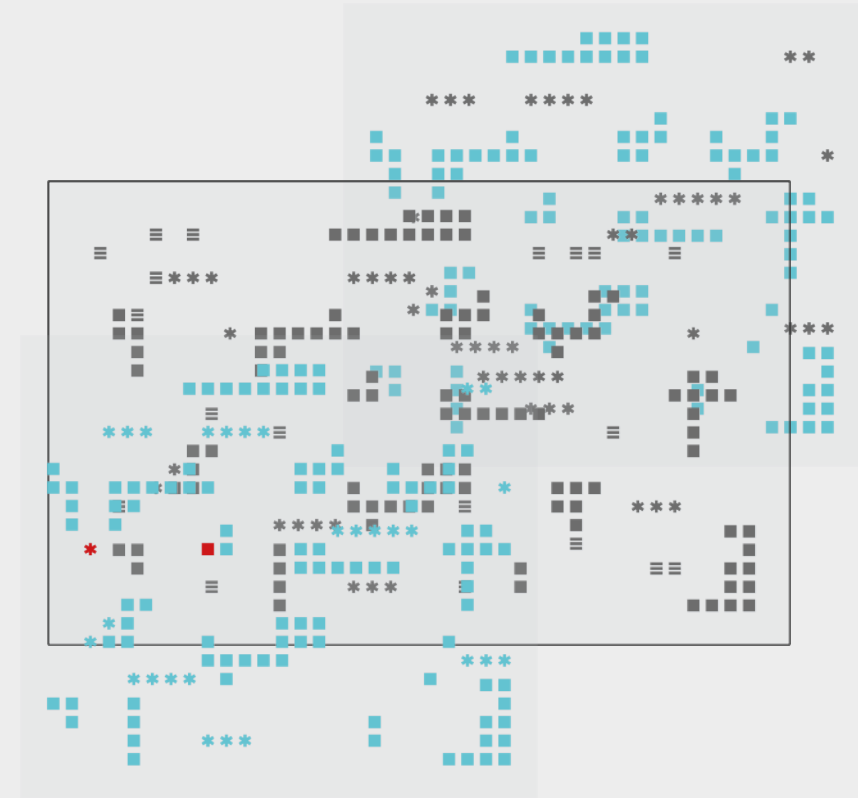


# What is Threat Hunting

“...the process of **proactively** and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.”

This is in contrast to traditional threat management measures, such as firewalls, intrusion detection systems (IDS), malware sandbox (computer security) and SIEM systems, which typically involve an investigation

**After** there has been a warning of a potential threat or an incident has occurred.”

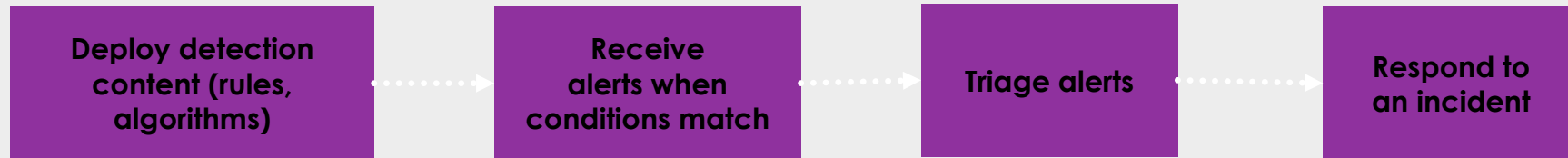


# What Is NOT Threat Hunting

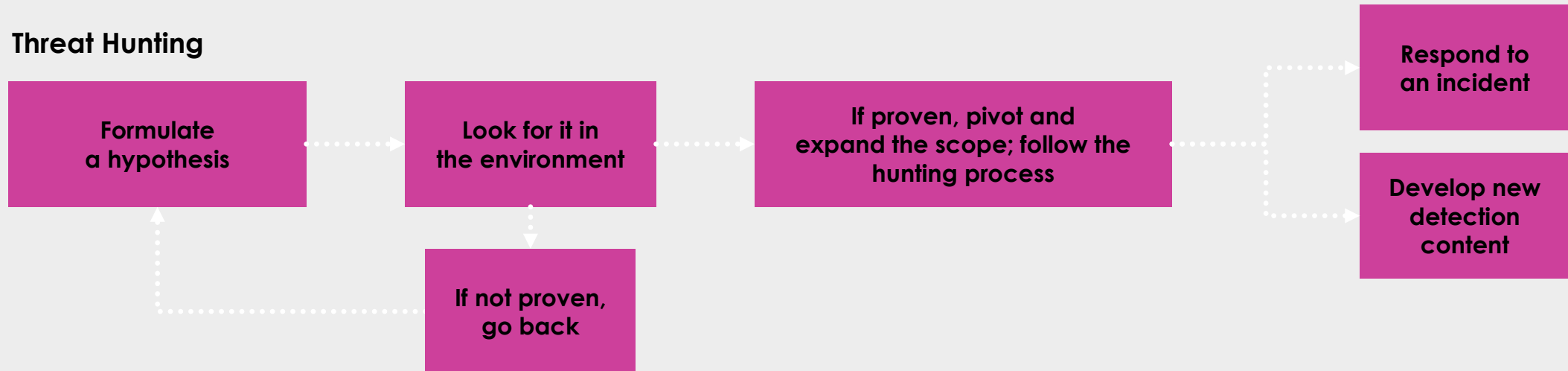
- **It is not better alert triage (very much still "gathering!"):**
  - ... and neither is "much better/faster alert triage"
- **It is not using endpoint detection and response (EDR) to match threat intel/indicators in your systems:**
  - This may form part of the hunt, this is loC search and should be automated.
- **It is not searching for things in a security data lake:**
  - Again, you may search data during the hunt, but this is still loC searching.
- **It is not a replacement for threat detection.**

# Threat Detection vs. Threat Hunting

## Threat Detection



## Threat Hunting



# Threat Hunting Prerequisites

**People** — since Threat Hunting is analyst-centric, need strong threat analysts and "tribal" knowledge

**Process** — Threat Hunting is ad hoc, but there is a method to this madness

**Technology** — naturally, you need the [data] "pond" to hunt with; visibility tools are essential!

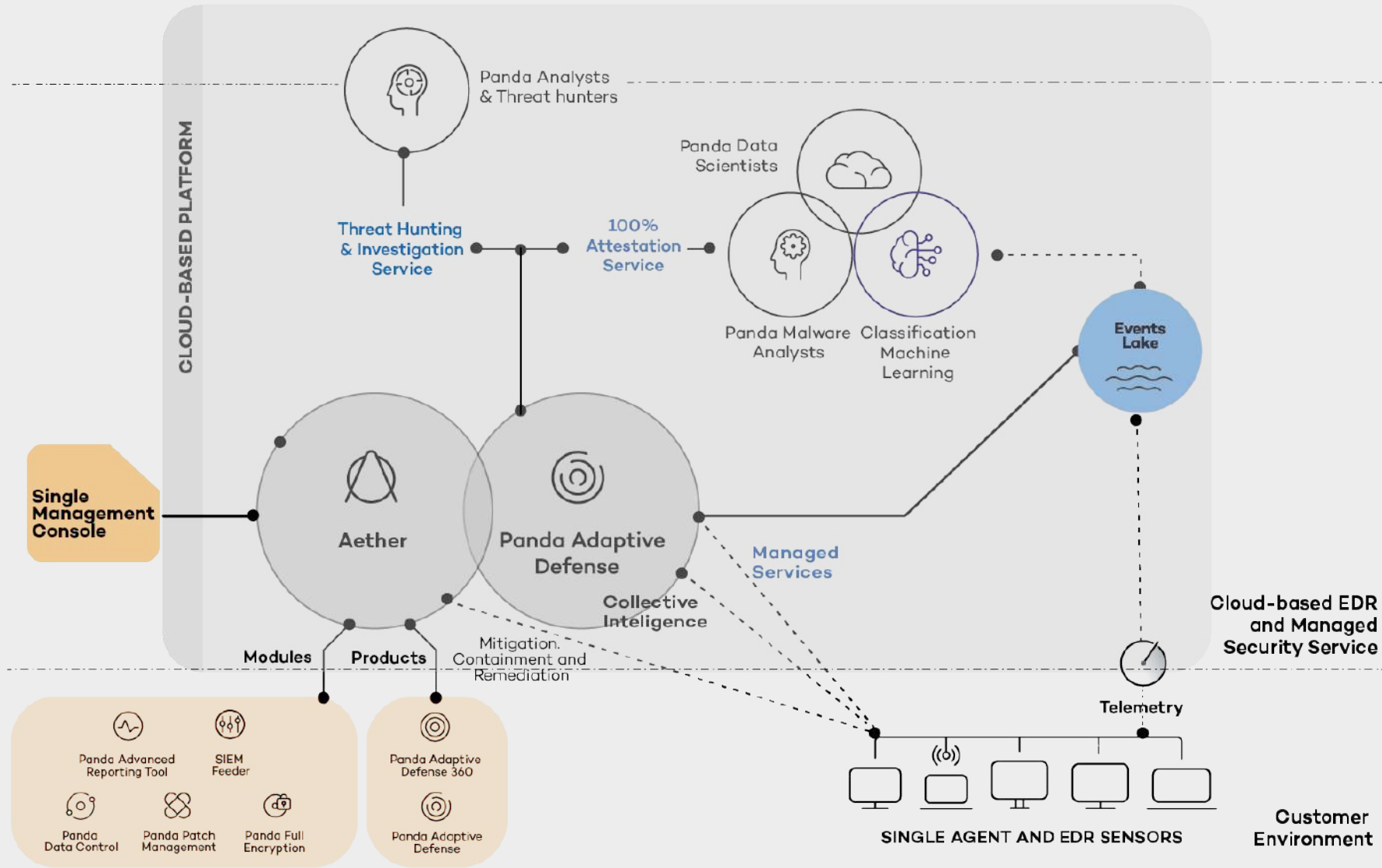
**Limited staffing, limited expertise, and the number of threats, attacks and breaches continue to grow...**

**So what can we do?**

**Mainstream organizations start to look for these Features-as-a-Service to address threat detection and response.**

**.. AND ...**

**Mainstream organizations start to streamline their security and IT operations workflow.**



Visit our booth, to see live what is Threat Hunting and why it's essential for all the companies!

# Thank You !

[lampros.katsonis@cy.pandasecurity.com](mailto:lampros.katsonis@cy.pandasecurity.com)

**Lampros Katsonis**  
Presales Manager

