ODYSSEY™
Impossible Challenges, Possible Solutions

Detecting suspicious/malicious activity using Security Analytics

Dr. Pantelis Georgiades | Data Scientist | Research & Development

April 2018

Agenda

1. Who we are
2. Cyber-threats landscape
3. Our approach to cybersecurity
4. Summary

ODYSSEY™

Company Overview

Who We Are

Founded in 2002

Odyssey was founded in 2002 with the main objective to provide High-Quality, Cutting-Edge, Cybersecurity, Managed Security and Risk Management Services to organizations that value their information assets.

Regional Leader

In the provision of **Information Security Solutions, Services and Products**, helping organizations in effectively and efficiently manage Information Risk.

Offices

Headquarters Nicosia-Cyprus, Athens-Greece, and **New York-USA** as well as an extensive international network of **Value Added Resellers and Distributors** of the ClearSkies™ NG SIEM and Managed Security Services.

Certifications

Certified with **ISO 27001** and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a **Qualified Security Assessor (QSA**) and an **Approved Scanning Vendor (ASV).**

Cyber-threats landscape

The Threat landscape is constantly *changing*……

Cyber-threats are increasing in…

Volume

Complexity

Impact

ODYSSEY™

The Threat landscape is constantly *changing*……

Cybercrime is now a “lucrative” industry….

Cybercriminals are…

ODYSSEY™

The Threat landscape is constantly *changing*……

Cybercrime is now a “lucrative” industry….

Cybercriminals are…

ODYSSEY™

Dark Web - Market Value of “Valuable” information

Valuable Information Categories	$$$$$$$$
Credit Card # (with CVV or without)	$5 - $15
Identity (SSN, Bank Account, …)	$20 - $30
Online banking account with $5,000 balance	$500
Compromised Computer	$5 - $25
Phishing Web site hosting – per site	$3 - $5
Verified PayPal account with balance	$50 - $1000
Skype Account	$10
World of Warcraft Account	$10
Medical Health Record	$150-1300
Personal Information (Loan, Property……)	Name your price

Source: Dark Web 2017-2018

Traditional approaches are failing… Why?

- Traditional protections like antivirus software, firewalls or HIPS and Sandboxing are failing to identify or block “Sophisticated” threats.

Traditional approaches are failing… Why?

- Traditional protections like antivirus software, firewalls or HIPS and Sandboxing are failing to identify or block “Sophisticated” threats.
- The investment needed in Human Intelligence and Expertise to defend against these threats is proving to be economically inefficient and ineffective.

Traditional approaches are failing… Why?

Machine Learning in cybersecurity

We need to

- Create a profile for users' and entities' behavior and detect deviations from it
- Create adaptive correlation rules
- Complement traditional threat detection systems

Machine Learning in cybersecurity

We need to

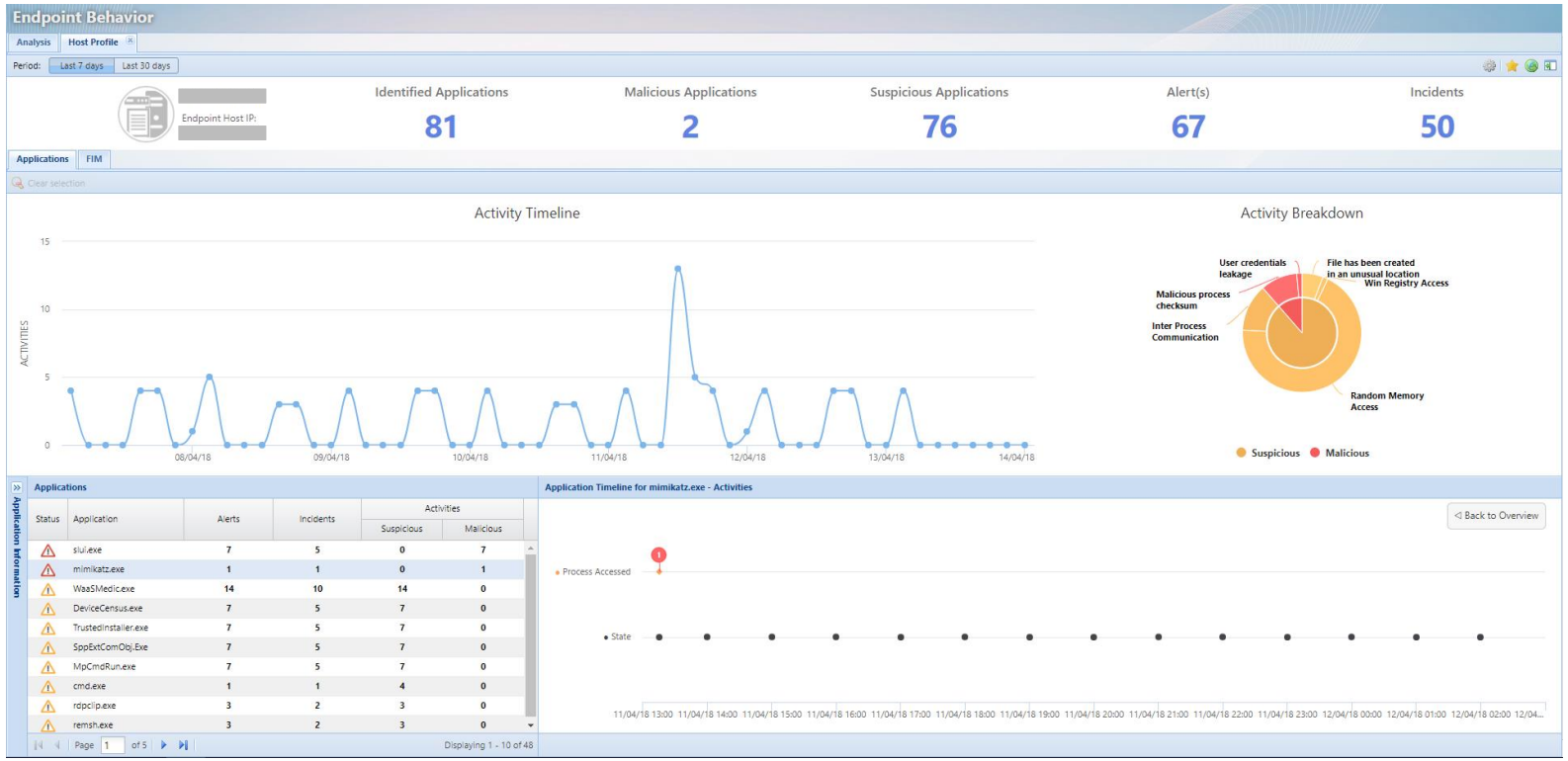
- Create a profile for users' and entities behavior and detect deviations from it
- Create adaptive correlation rules
- Complement traditional threat detection systems

The use of Machine Learning has enabled us to create advanced analytics to satisfy these needs

Machine Learning in Cybersecurity

Machine Learning has enabled us to:

- Create advanced anomaly detection algorithms for detecting:
  - ✓ Malware, zero-day exploits and Advanced Persistent Threats

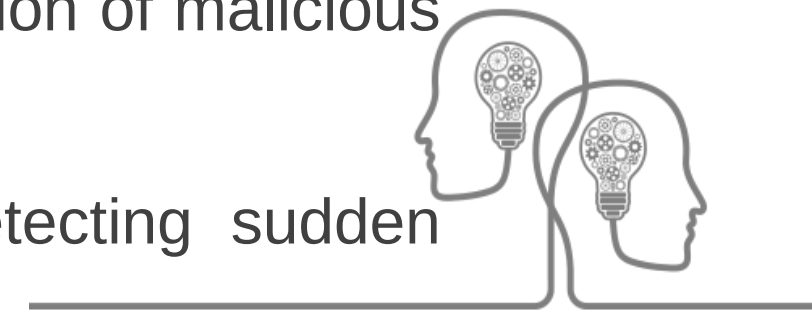


ODYSSEY™

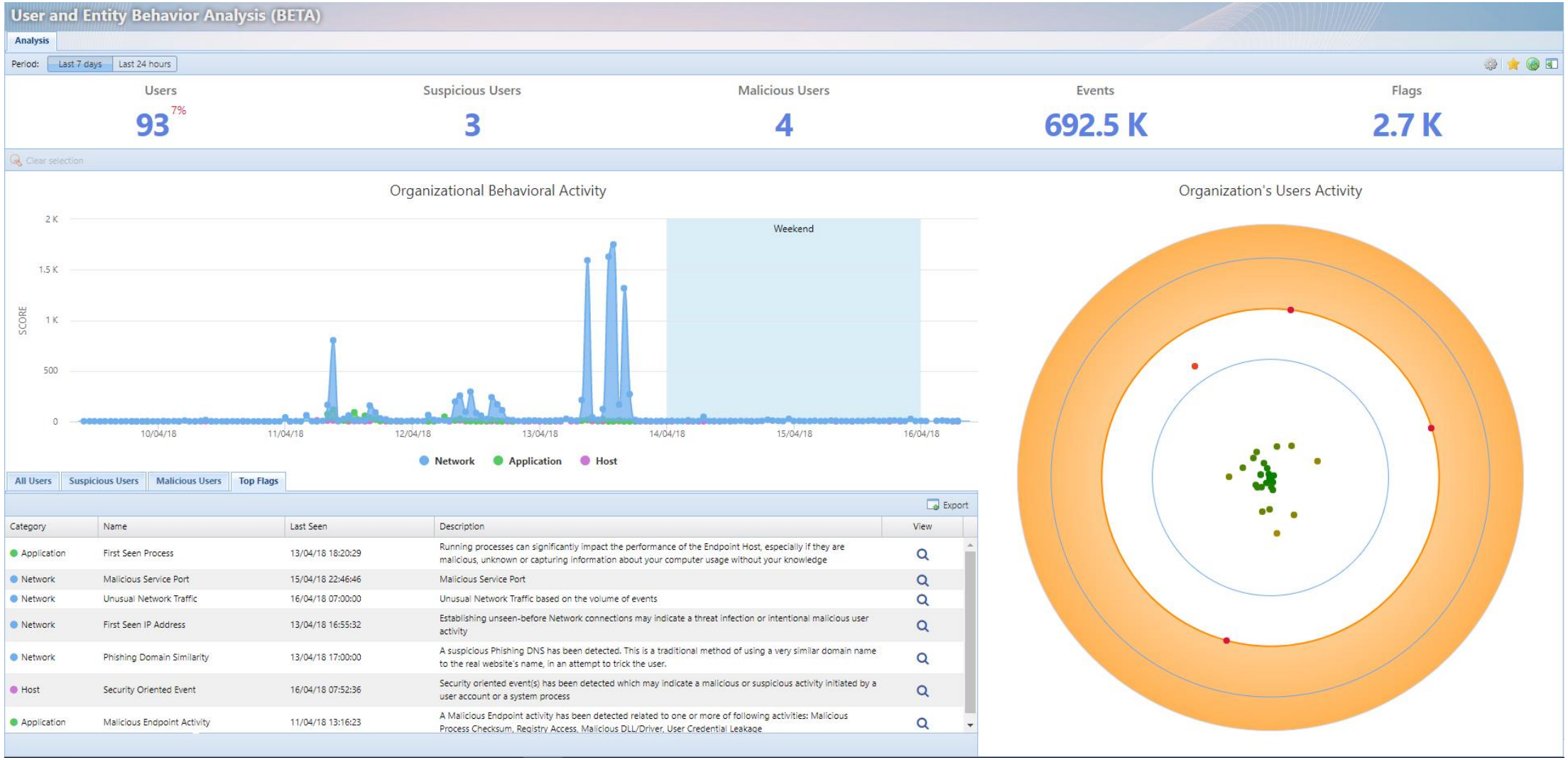
Machine Learning in Cybersecurity

Machine Learning has enabled us to:

- Create advanced anomaly detection algorithms for detecting:
  - ✓ Malware, zero-day exploits and Advanced Persistent Threats
- Use Artificial Neural Networks for generic detection of malicious threats, such as Phishing Attacks
- Develop behavioral forecasting models for detecting sudden change in behavior
- Develop User & Entity Behavior Analytics (UEBA) for detecting suspicious and malicious users' and entities' activities



Machine Learning in Cybersecurity



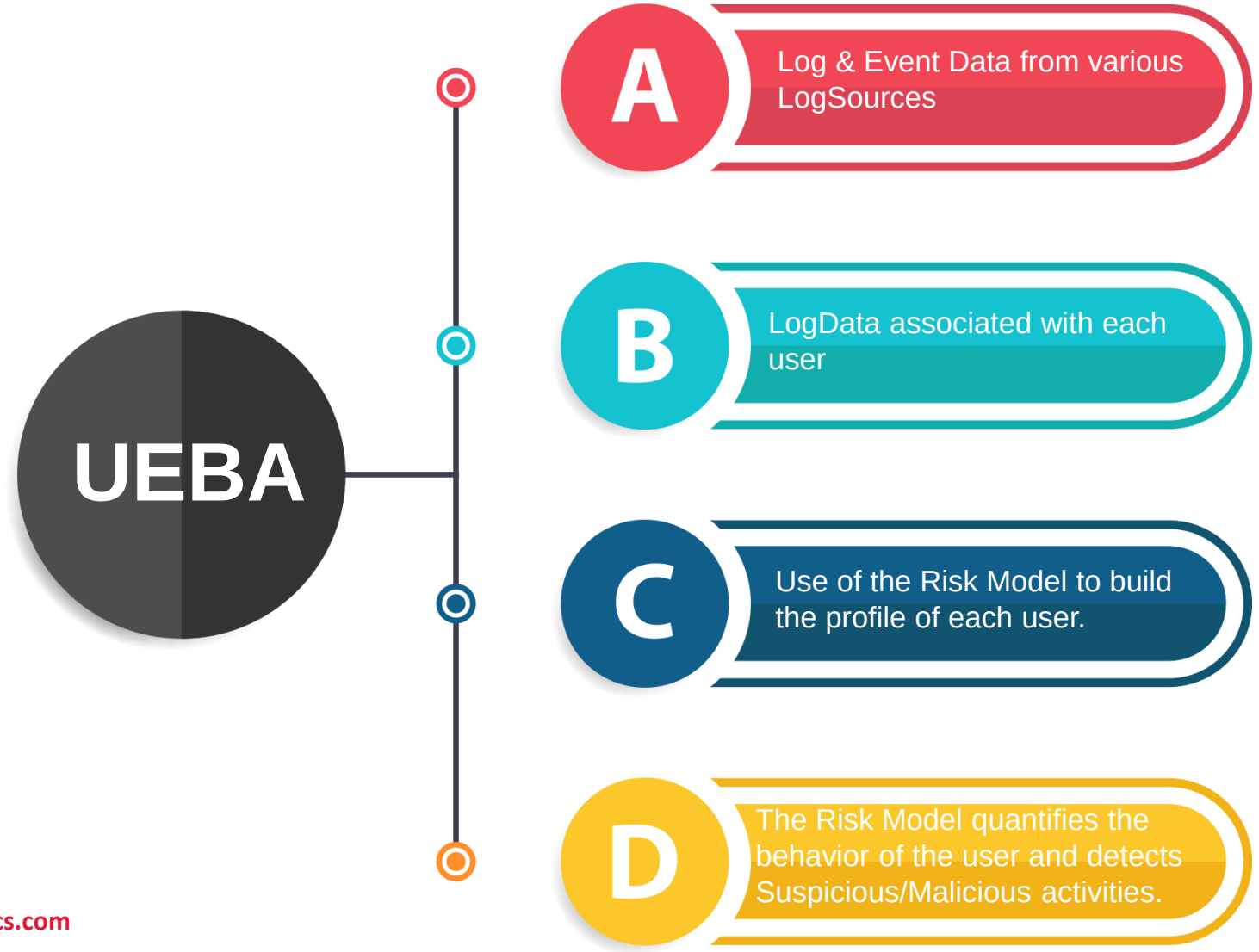
ODYSSEY™

User and Entity Behavior Analytics

The UEBA framework:

- Creates a holistic view of users' behavior over time
- Detects targeted attacks (Malicious)
- Identifies anomalies which could potentially pose threats (Suspicious)
- Creates a forensic audit trail for investigation

User and Entity Behavior Analytics



ODYSSEY™

Summary

Summary

- Cyber-threat landscape is ***Evolving***
- Traditional threat detection/prevention methods are proving inadequate
- **What got us here, won't get us there.** So we need to adapt our approach to counter the ever-evolving cybersecurity landscape

For a live demonstration of our platform and the use of advanced analytics in Cybersecurity please **join us at 12.30pm today in our workshop**

Why Security Analytics

“In order to find the needle in the haystack, we need the whole haystack”

Gartner 2005

ODYSSEY™

ODYSSEY™
Impossible Challenges, Possible Solutions

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades Str.,
2012 Strovolos, Nicosia
Tel.: +357 22463600
Fax: +357 22463563
Email: info@odysseycs.com
www.odysseycs.com

OFFICES

CYPRUS | GREECE | USA

Contact details
Dr Pantelis Georgiades
pgeorgiades@odysseycs.com