"INTELLIGENZA ARTIFICIALE E STUPIDITÀ NATURALE: È DAVVERO POSSIBLE PROTEGGERE GLI ENDPOINT?"

ALESSIO L.R. PENNASILICO AKA -=MAYHEM=-

Information & Cyber Security Advisor @ P4I

Membro del Comitato Direttivo e del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Presidente dell'Associazione Informatici Professionisti AIP Associazione Informatici Professionisti ITCS Italian Computer Society

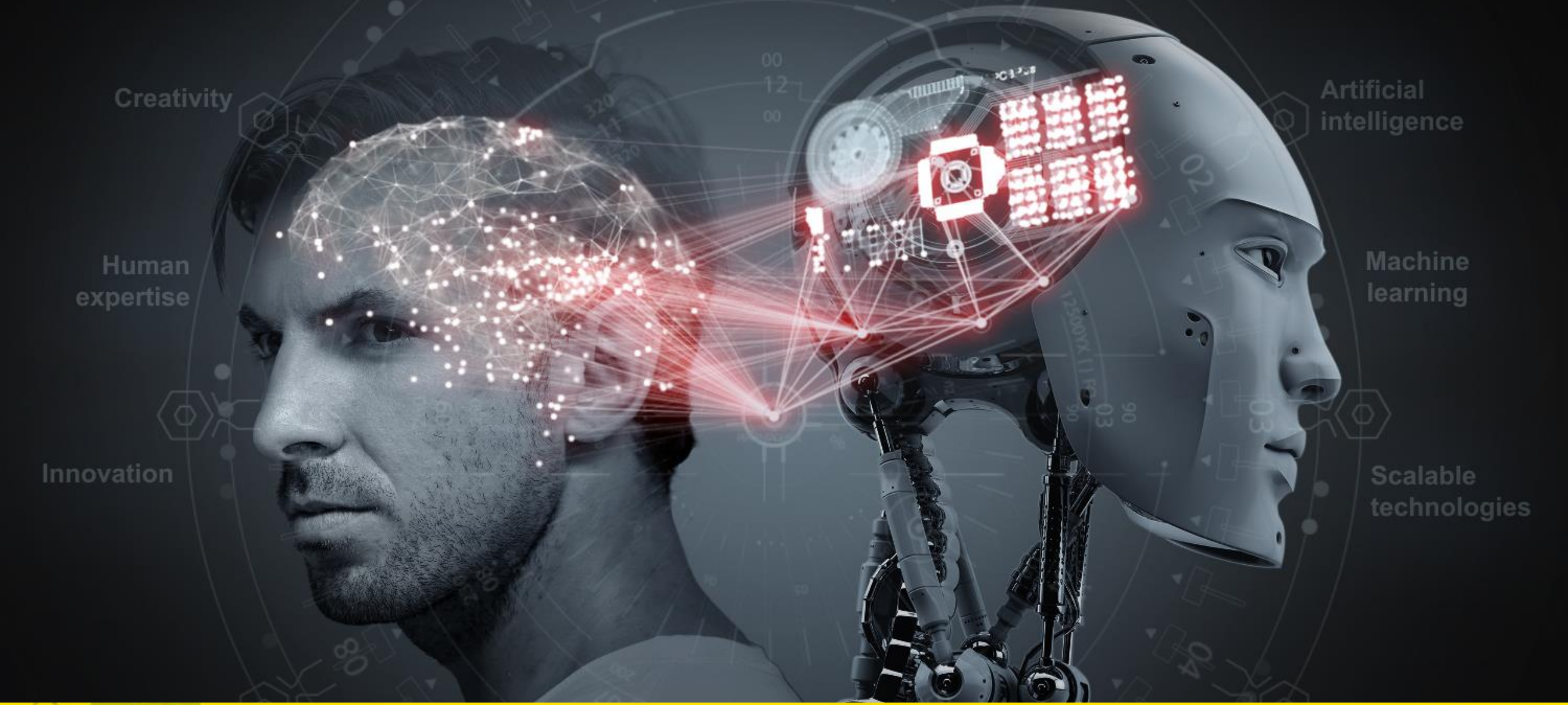
Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Andrea Muzzi

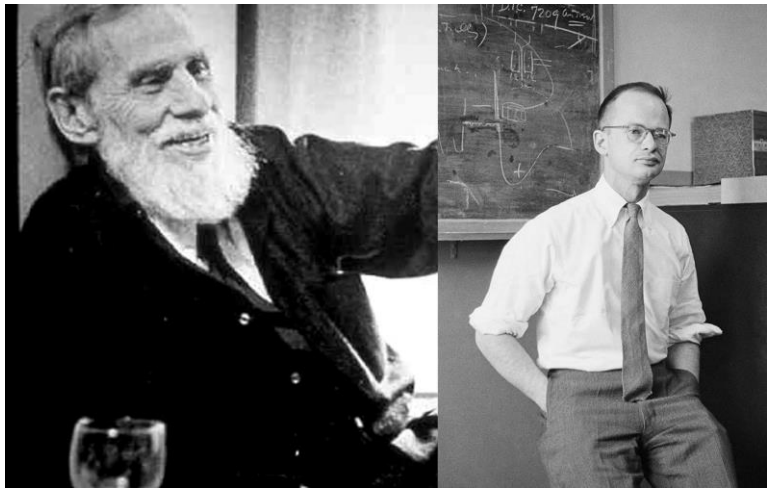
Sales Engineer
13 anni
in
F-Secure

A.I. Artificial Intelligence



A.I. first steps

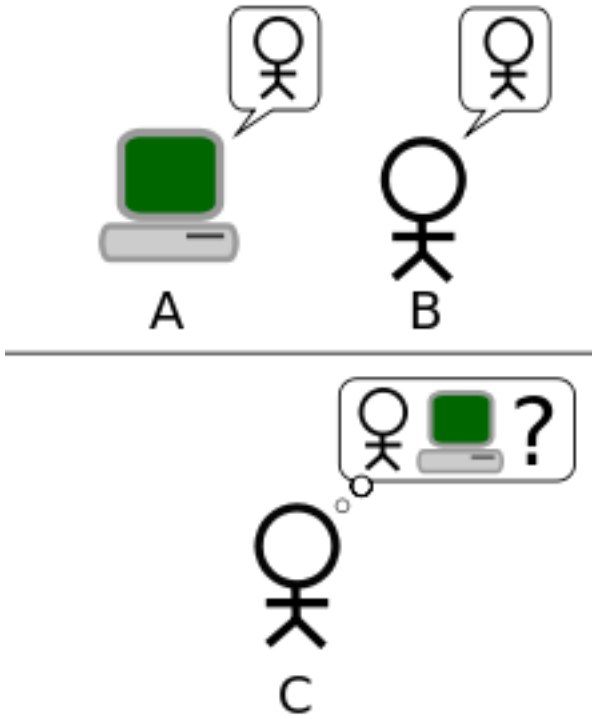
The first real A.I. project dates back to **1943** when two researchers **Warren McCulloch** and **Walter Pitt proposed** to the scientific world **the first artificial neuron**

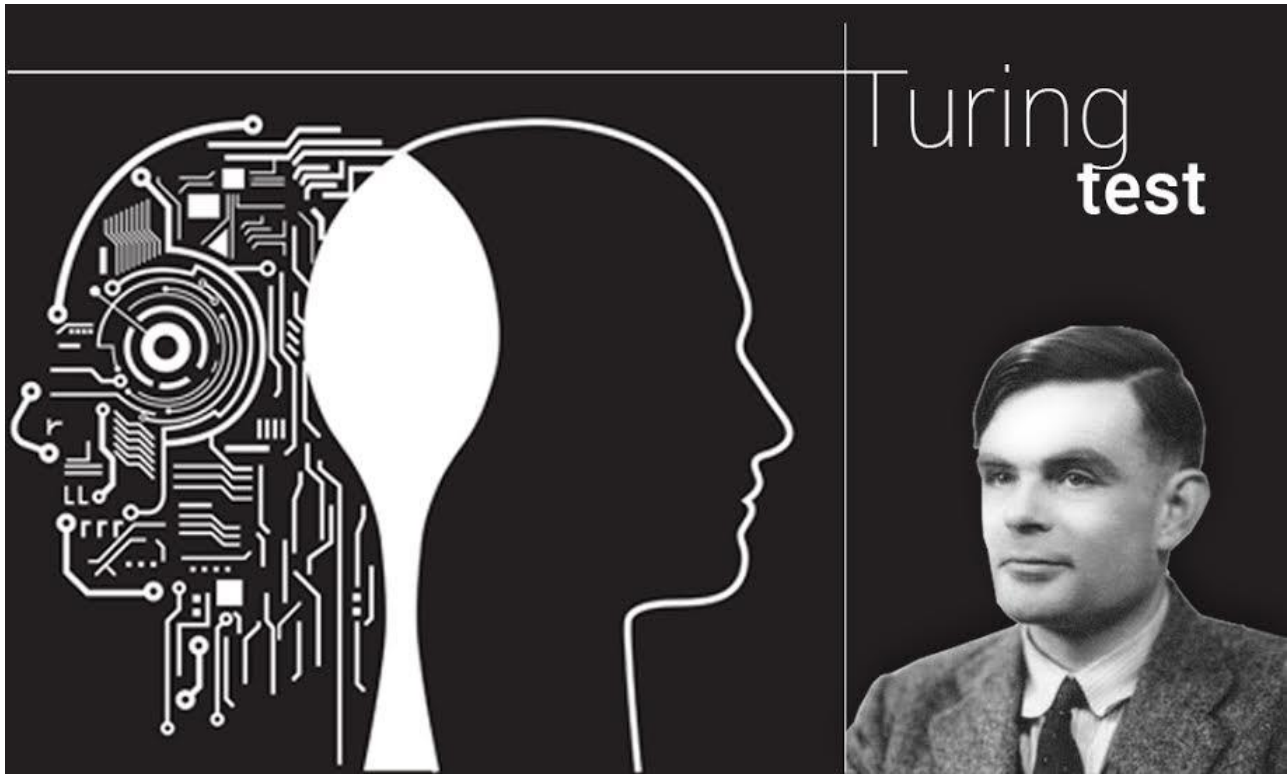


1949 Donald Olding Hebb, Canadian psychologist **publish a book** where **the links between artificial neurons and** the complex models of **the human brain were analyzed in detail**

A.I. first steps

1950 Alan Turing considered A.I. father tried to explain how a computer can behave like a human being. **He invented a test** that could give a **measure of** the ability of a **thinking machine**.





A.I. first steps

1958 Thanks to **Frank Rosenblatt** the **first neural network model** is born **«Percettone»**

A.I. is based on artificial neural networks,
also used in Machine Learning

today **they are able to classify data faster** and more accurately than **any human being**

A.I. around us

- **Video Games** – A.I. algorithms allow characters, environments, stories to evolve according to the behavior of the player, creating situations that are always new and unpredictable.

- **Security Camera's images** - the images are examined in real time through powerful software that can recognize patterns of behavior that can be an alarm signal

- **Fraud.net** - leading platform in the prevention of fraudulent activities based on crowdsourcing

- **Tinder** - the most popular app to meet new people Behind every single swipe in search of the perfect match there is in fact a system that manages millions of requests per minute, billions of swips a day, in more than 190 countries in the world

How was it possible ?

THE DEVELOPMENT OF NEURAL NETWORKS #1

At the end of the 2000s, then, **three** almost **simultaneous events made large-scale neural networks possible**,

these three factors allowed the neural networks **to keep their promises**

How was it possible ?

THE DEVELOPMENT OF NEURAL NETWORKS #2

- **Large data** sets become widely available. Texts, images, films, music: all of a sudden, everything is digitized and can therefore be used to form neural networks

- Researchers are able to exploit the **extraordinary power of parallel processing of graphics processors (GPUs)** to form large neural networks

- **The cloud has provided resiliency and flexibility to developers and researchers**, allowing them to use all the necessary training infrastructure without having to build, manage or pay for long-term use.

Algorithms that may conceal hidden biases are already routinely used to make vital financial and legal decisions. Proprietary algorithms are used to decide, for instance, who gets a job interview, who gets granted parole, and who gets a loan.

https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/?set=608263

Self-driving cars with no in-vehicle backup driver get OK for California public roads from April 2nd 2018

MIT Technology Review

Log in / Register Se

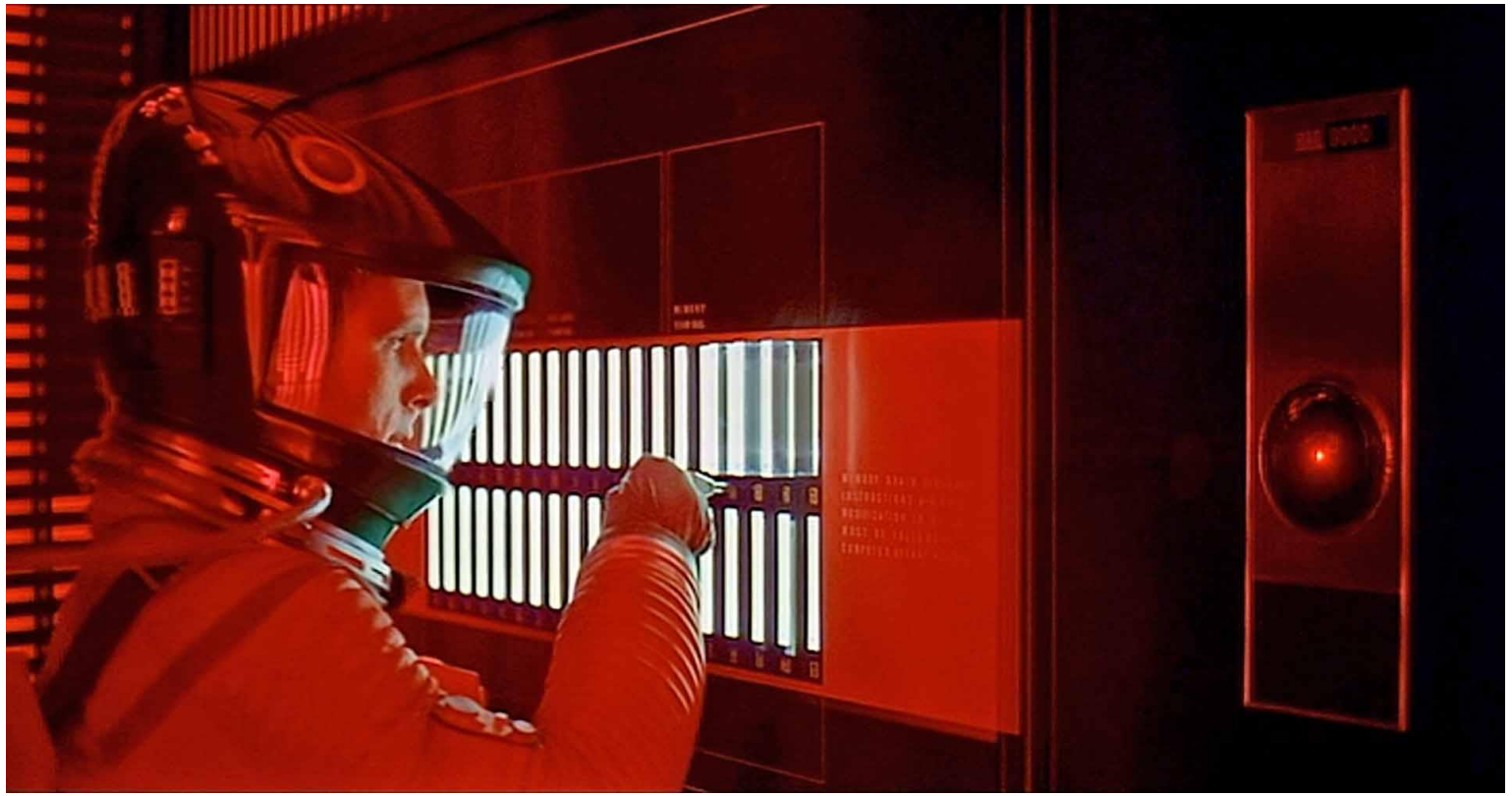
Topics+ The Download Magazine Events

COURTESY OF OTTO

Intelligent Machines

Hackers Are the Real Obstacle for Self-Driving Vehicles

Il Pericolo della Singolarità



OVVERO IL PUNTO NEL QUALE LE MACCHINE DIVENTERANNO PIÙ INTELLIGENTI DEGLI UMANI, MA È GIÀ ARRIVATO…?

Il Pericolo della Singolarità

- Una traguardo possibile potrebbe essere entro il 2050

Facebook ha improvvisamente fermato un esperimento di intelligenza artificiale (https://www.forbes.com/sites/tonybradley/2017/07 /31/facebook-ai-creates-its-own-language-in-creepy-preview- of-our-potential-future/#4ffad49d292c) **dopo aver scoperto che le macchine avevano autonomamente sviluppato un linguaggio tutto nuovo, incomprensibile all'uomo. I ricercatori** del Facebook AI Research Lab (https://research.fb.com/category /facebook-ai-research-fair/) **si sono** infatti **accorti che i robot stavano comunicando in maniera totalmente inaspettata**

È un avvertimento che persone del calibro di Stephen Hawking, Elon Musk, Steve Wozniak, Bill Gates…. stanno riproponendo nel corso degli ultimi anni.

THE SECURITY LANDSCAPE IS CHANGING ! (AND FAST)

WHY THE SECURITY LANDSCAPE IS CHANGING?

EVERY COMPANY IS A TARGET

All companies are targeted as criminals go for the easiest victims

RANSOMWARE WITH BITCOINS

With Bitcoins criminals can easily receive money without getting caught

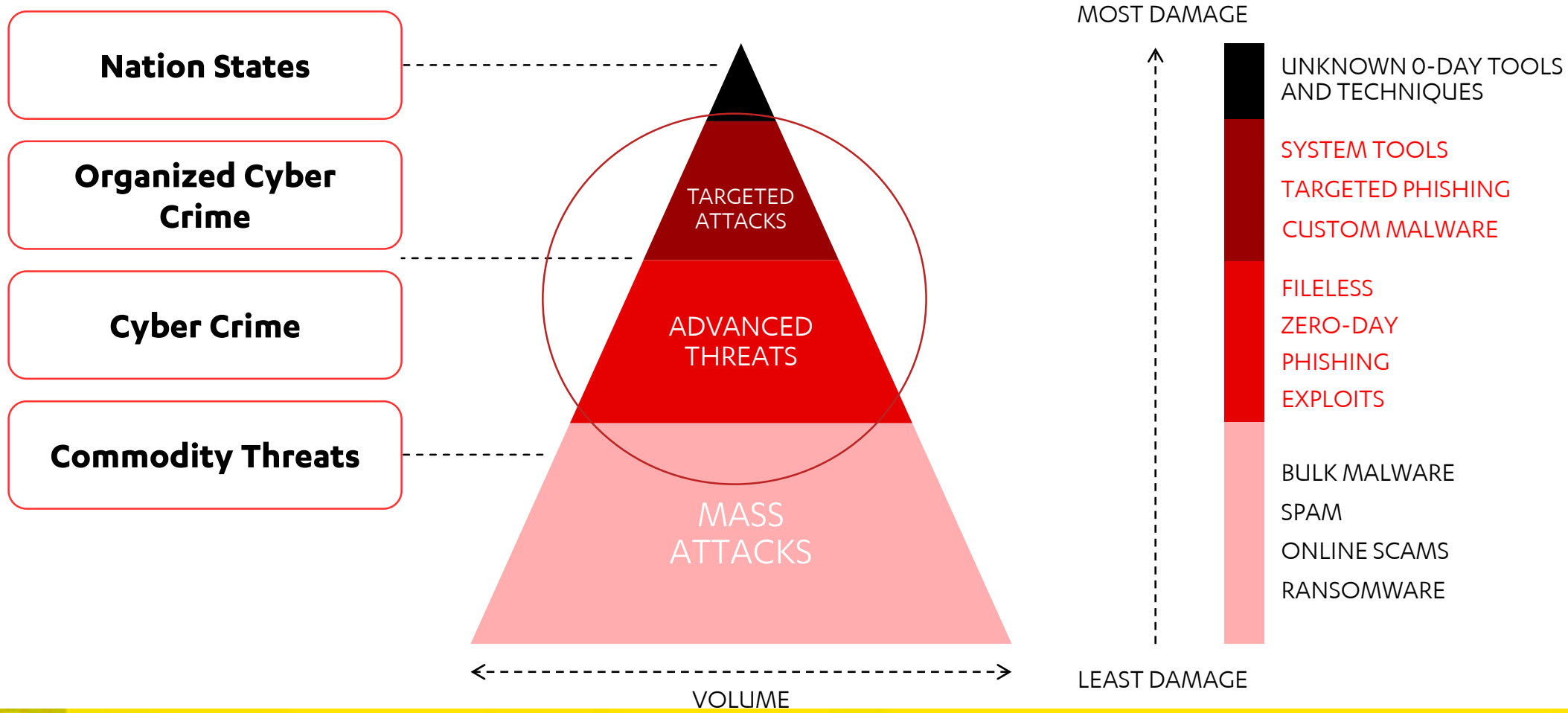
NO MORE EASILY DETECTED METHODS

Criminals move to using fileless attacks and normal operating system tools

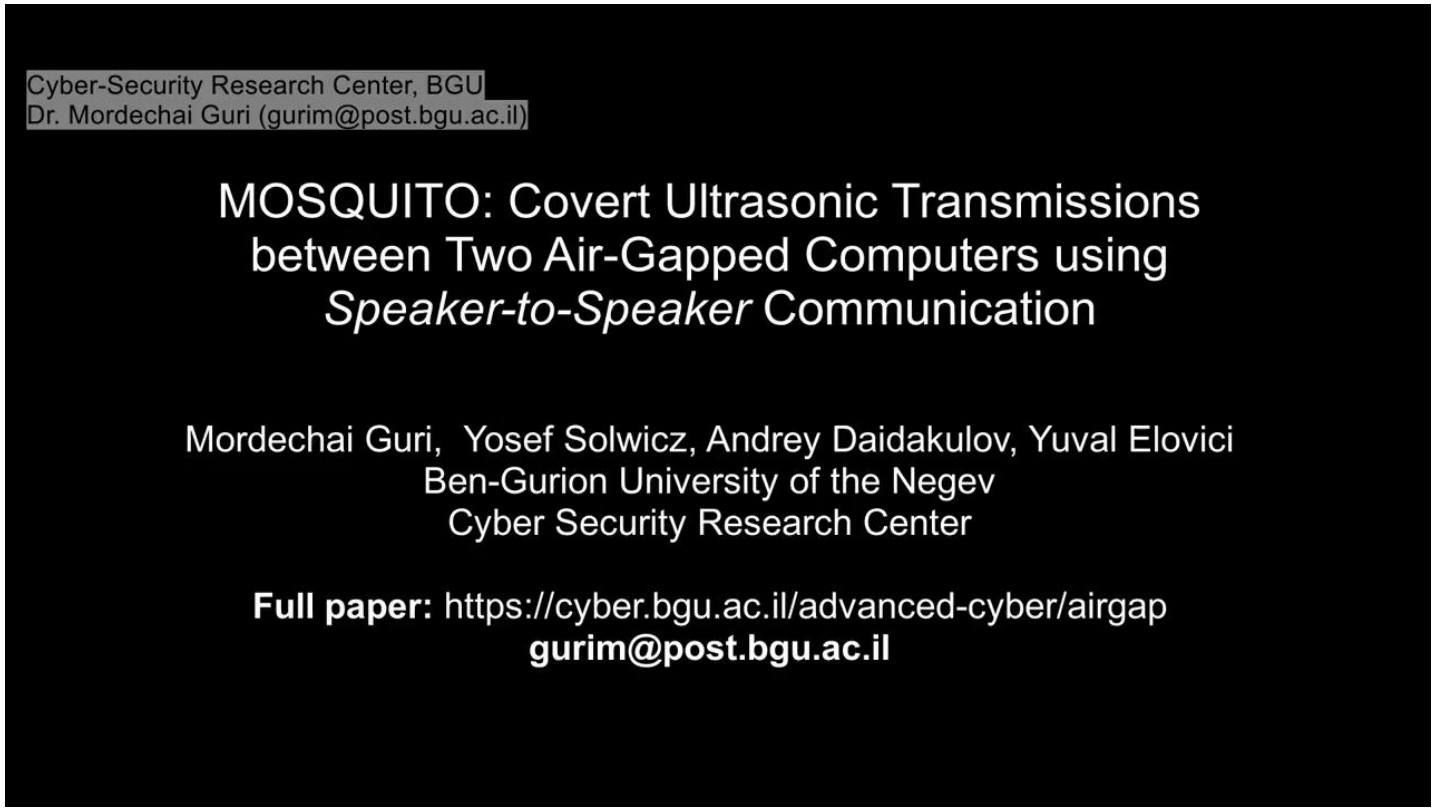
Still endpoint protection is the foundation you must use as basis for security

ecure

UNDERSTANDING
THE THREAT LANDSCAPE



THE SECURITY LANDSCAPE IS CHANGING FASTER



BREACHES HAPPEN:
BE PREPARED.

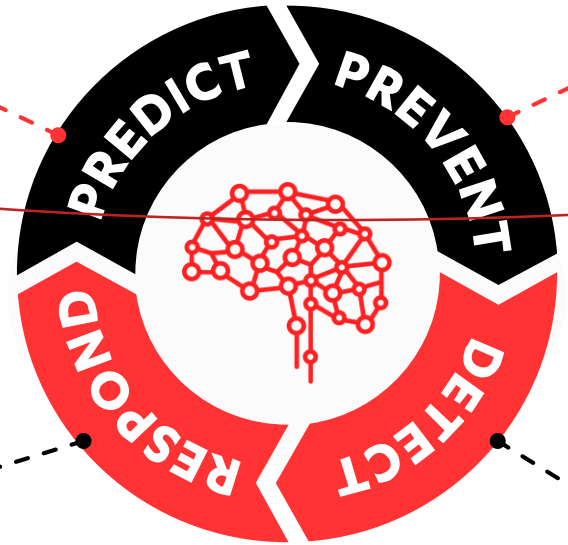
CYBERSECURITY IS A PROCESS

PREDICT
Vulnerability Management

Understand your risk, know your attack surface, uncover weak spots

PREVENT
Endpoint Protection, Service Protection

Minimize attack surface, patch vulnerabilities and prevent incidents



Pre-Compromise

Post-Compromise

React to breaches, mitigate the damage, analyze and learn

Recognize incidents and threats, isolate and contain them

ON AVERAGE IT TAKES

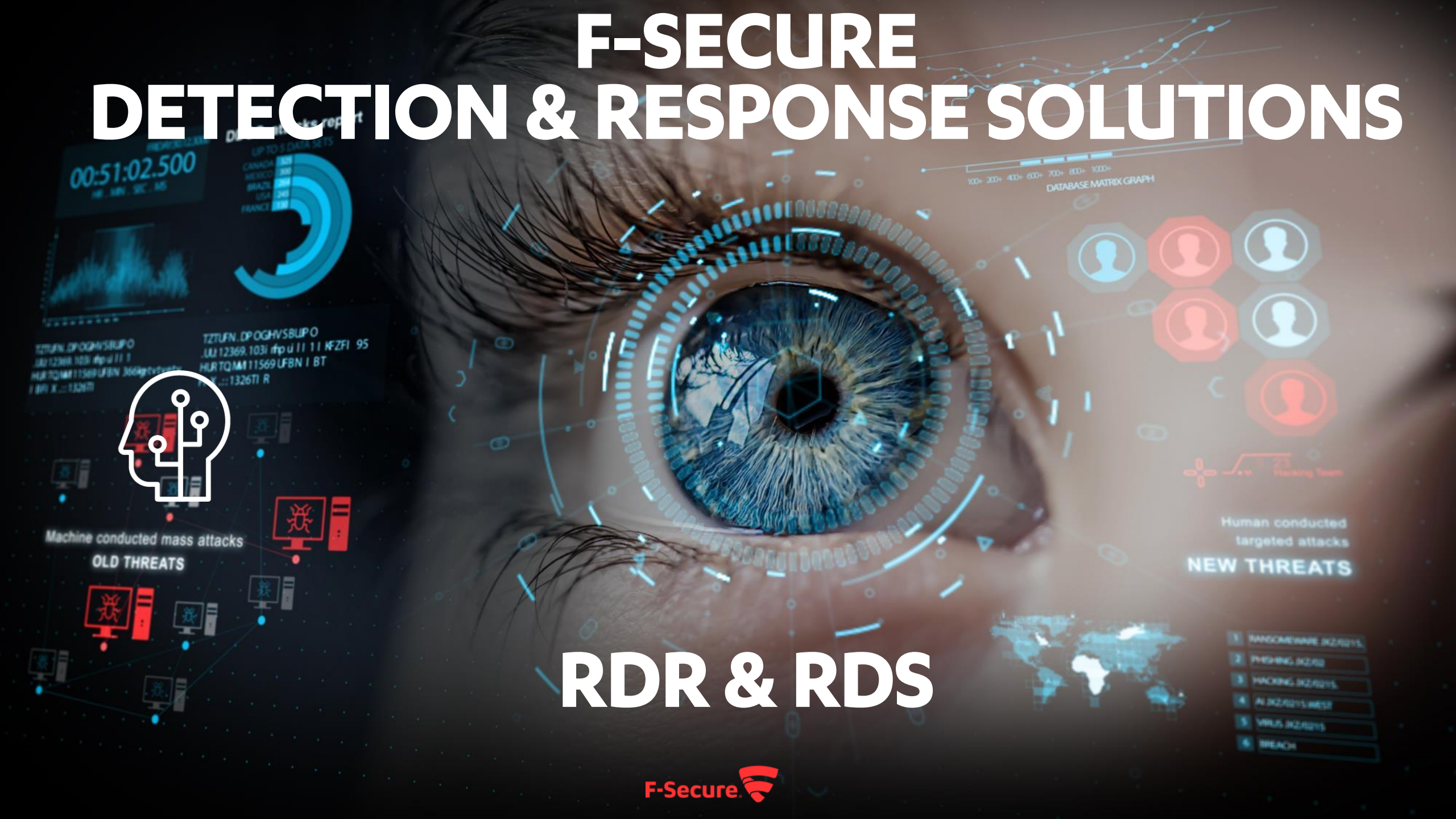
100 DAYS

TO DETECT A BREACH

Source: Gartner 2017

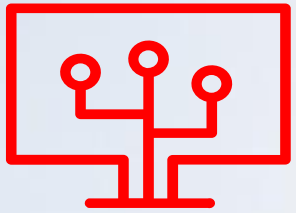
All statements in this report attributable to Gartner represent F-Secure's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

F-SECURE
DETECTION & RESPONSE SOLUTIONS



RDR & RDS

F-Secure



F-SECURE RDR
RAPID DETECTION & RESPONSE

Introducing F-Secure's Endpoint Detection and Response solution

F-Secure.

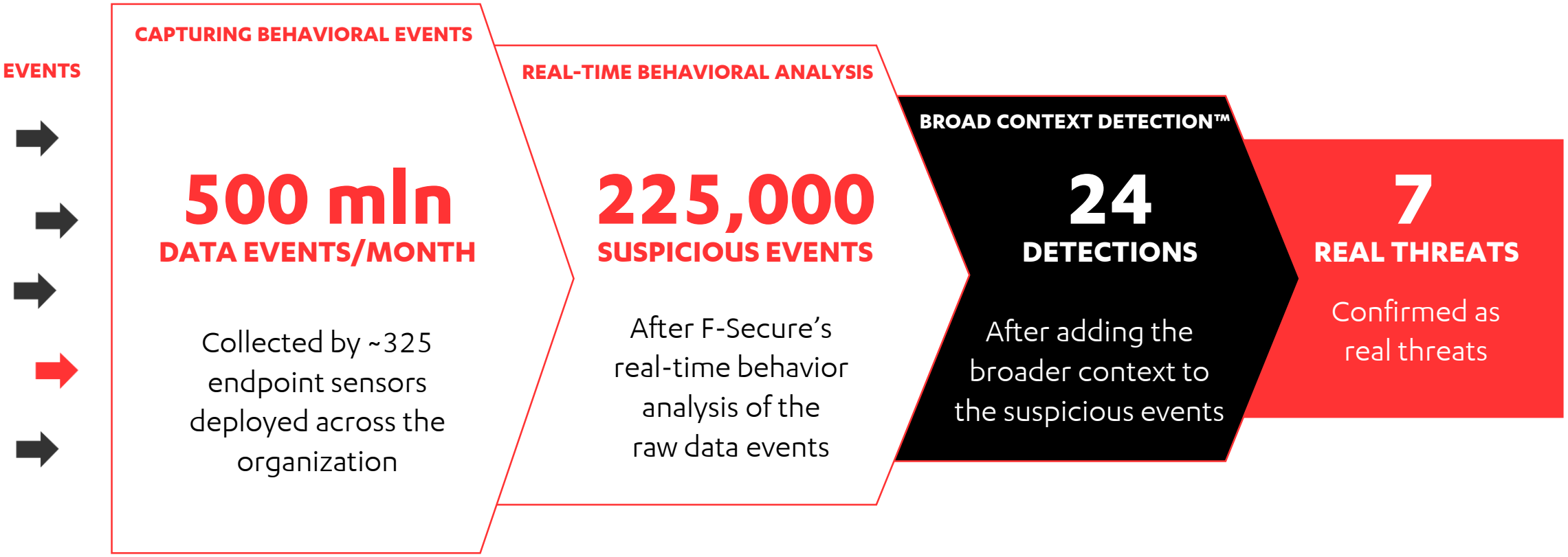
F-SECURE RAPID DETECTION & RESPONSE

100% partner driven detection and response service against targeted cyber attacks

F-Secure.

AI AND MACHINE LEARNING AT THE HEART OF THE SOLUTION

BROAD CONTEXT DETECTION™ IN ACTION



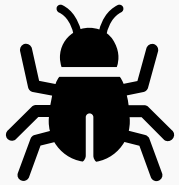
F-Secure

DETECTION ?

t event.data_.category	NewProcess
? event.data_.context.baselinerScore	⚠ 62
t event.data_.context.command_line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noprofile -windowstyle hidden -executio Cj').mFpOieBO)));
t event.data_.context.parent_file_full_path	%systemroot%\explorer.exe
t event.data_.description	powershell.exe with parameters that are typical for post exploit payload

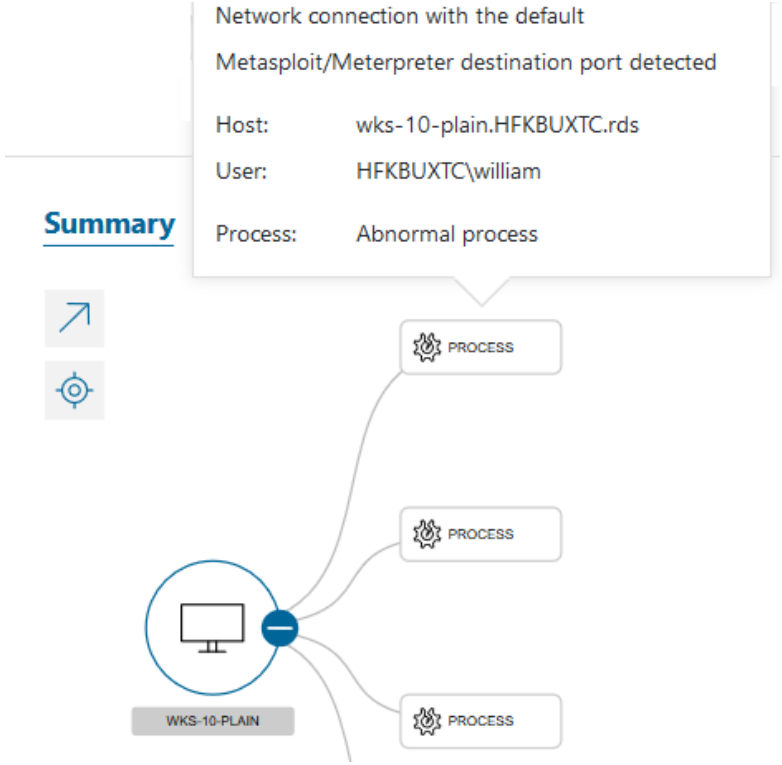
event.data_.process_details.cmdl **"C:\Windows\system32\rundll32.exe" \----_____-------_____----__-----_________---**
-__________.----_____-------_____----__-----_________---_______,UYcgueYcWQKOSWky

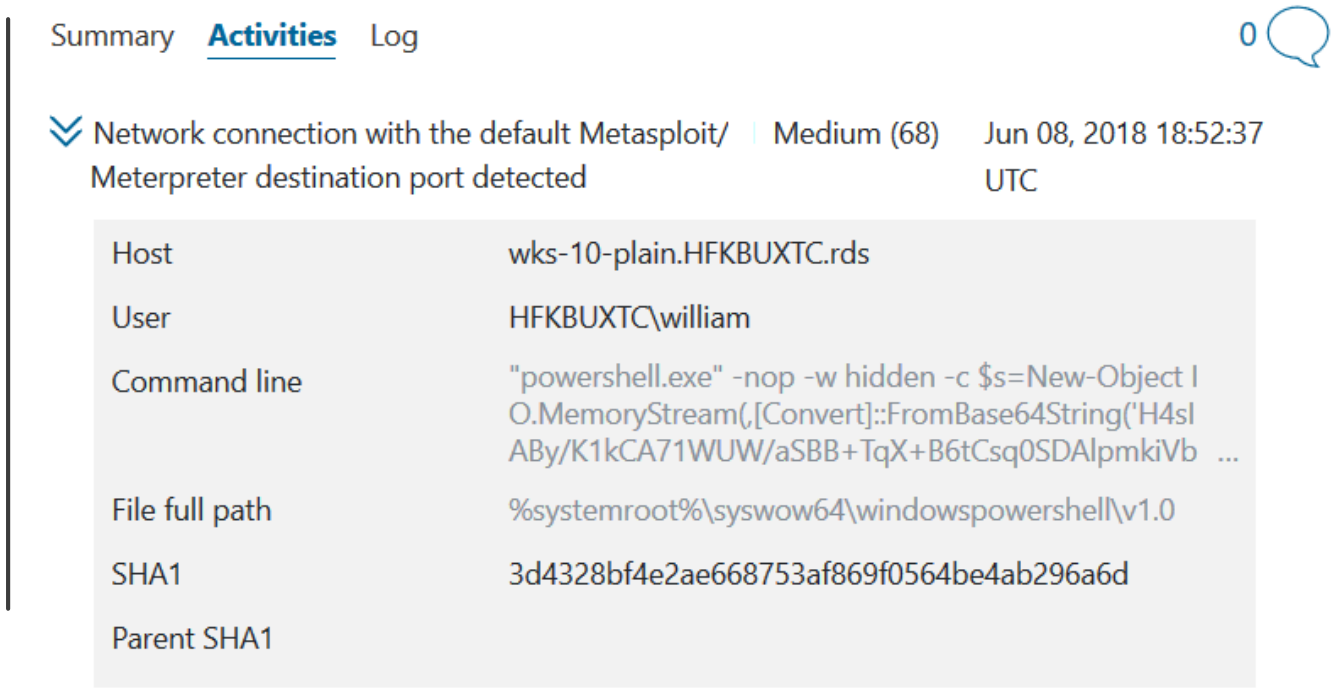
Wauchos / Trojan.Inject.BCX



F-Secure

FEATURE HIGHLIGHTS:
BROAD CONTEXT DETECTION™

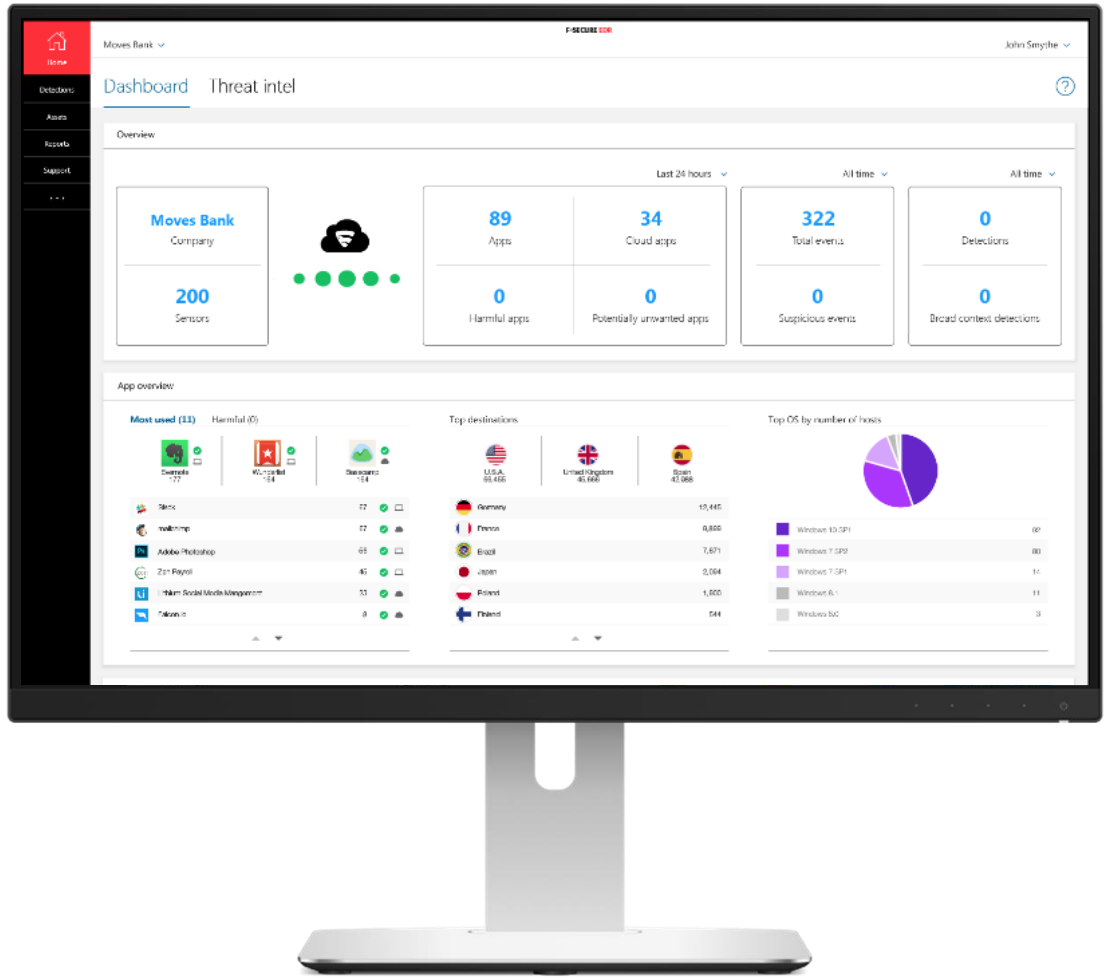




F-Secure

KEY FEATURES

F-SECURE RAPID DETECTION & RESPONSE



BEHAVIORAL ANALYSIS

BROAD CONTEXT DETECTION

WINDOWS SENSOR

APPLICATION INVENTORY

INCIDENT MANAGEMENT

CENTRAL MANAGEMENT

EXPERT GUIDANCE*

MAC SENSOR*

THREAT INTELLIGENCE

HOST ISOLATION*

AUTOMATED RESPONSE*

API MANAGEMENT INTEGRATION*

*AVAILABLE AFTER THE CORE RELEASE

F-SECURE RDS
RAPID DETECTION & RESPONSE MANAGE SERVICE

F-Secure.

HOW RAPID DETECTION SERVICE WORKS
COMBINING MAN & MACHINE

ATTACKER

YOUR ORGANIZATION

Endpoint sensors

Network decoy sensors

PR

Marketing

Finance

THREAT INTELLIGENCE – GLOBAL AND INDUSTRY SPECIFIC

Real-time behavior analytics

Big data analytics

Reputational analytics

ANOMALY

max 30 minutes

CSIRT

SOC/Partner/CISO

ALERT

RAPID DETECTION CENTER

Threat analysts

Incident responders

Forensic experts

F-Secure

© F-Secure

DATA COLLECTION

Endpoint sensors collect following kinds of event based data:

- file accesses
- process creations
- network connections
- registry writes
- system log entries relevant to detecting security breaches
- extracts of scripts derived from run-time execution

PRIVACY & SECURITY

- All communications are encrypted.
- All data is physically stored in Europe, on secure and controlled servers.
- Access only by authorized users and for authorized purposes.
- More detailed information can be found in the RDR privacy policy (GDPR applicable https://business.f-secure.com/10-myths-european-gdpr/).

PRIVACY & SECURITY #2

- The service is not intended for monitoring non-security related activities such as profiling employees' activities, interests, or interactions.
- The focus of data collection is not on individual employees or business documents.

I computer sono incredibilmente veloci,accurati e stupidi.

Gli uomini sono incredibilmente lenti, innacurati e intelligenti.

L'insieme dei due costituisce una forza incalcolabile

Albert Einstein