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

Relatori

Alessio L.R. Pennasilico

Andrea Muzzi

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

Information & Cyber Security Advisor @

Membro del Comitato Direttivo e del Comitato Tecnico Scientifico

Presidente dell'Associazione Informatici Professionisti

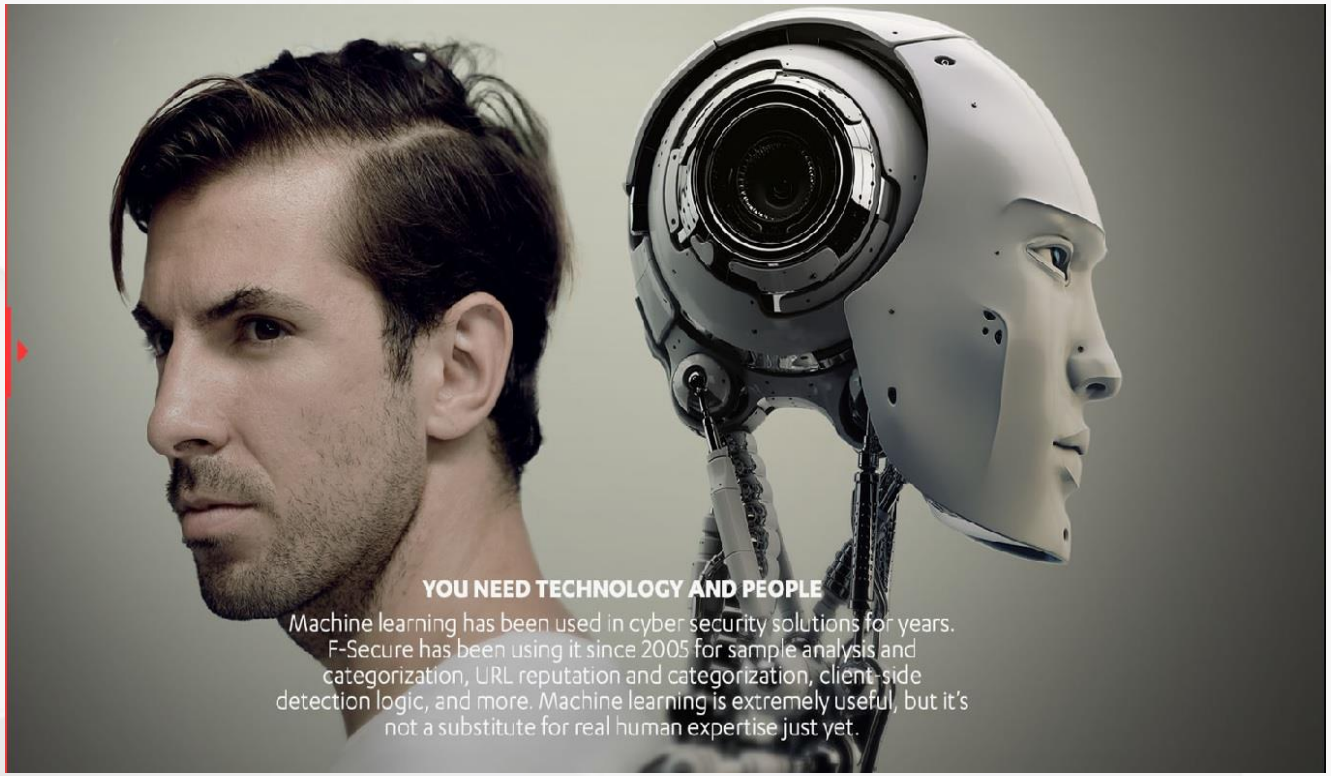
Vice Presidente del Comitato di Salvaguardia per l'Imparzialità

Membro del Comitato di schema

Andrea Muzzi

Sales Engineer F-Secure

A.I.
Artificial Intelligence



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

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

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**

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

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

Stupidità o presunzione ?

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

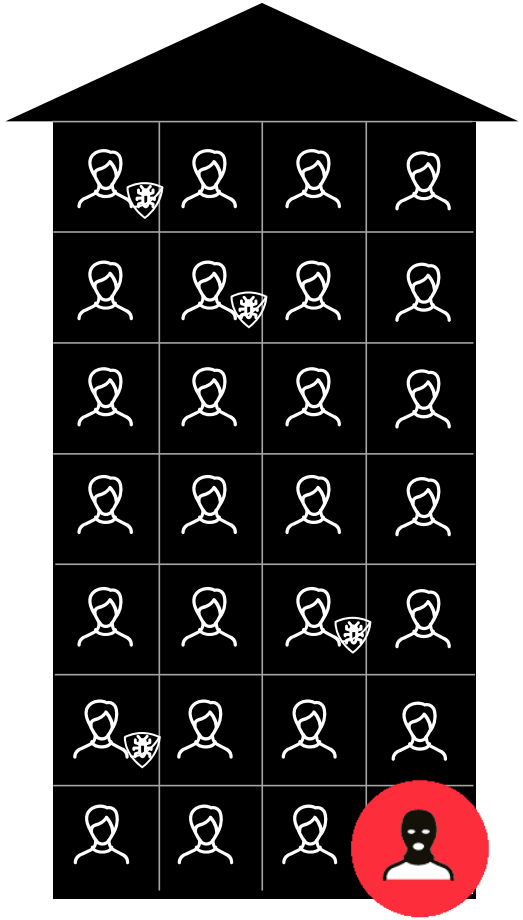
99,9 % DO LITTLE DAMAGE

0,1 % DO THE MOST DAMAGE

COMMODITY THREATS → TARGETED ATTACKS

Usually well covered

- Commodity threats
  - Machine conducted attacks
  - Malware, such as ransomware etc.
  - Spam and phishing campaign
  - >100 million new malware samples added each year (AV-TEST database)
- Addressed by preventive security:
  - Firewall
  - Email security
  - End-point protection
  - Other preventive solutions

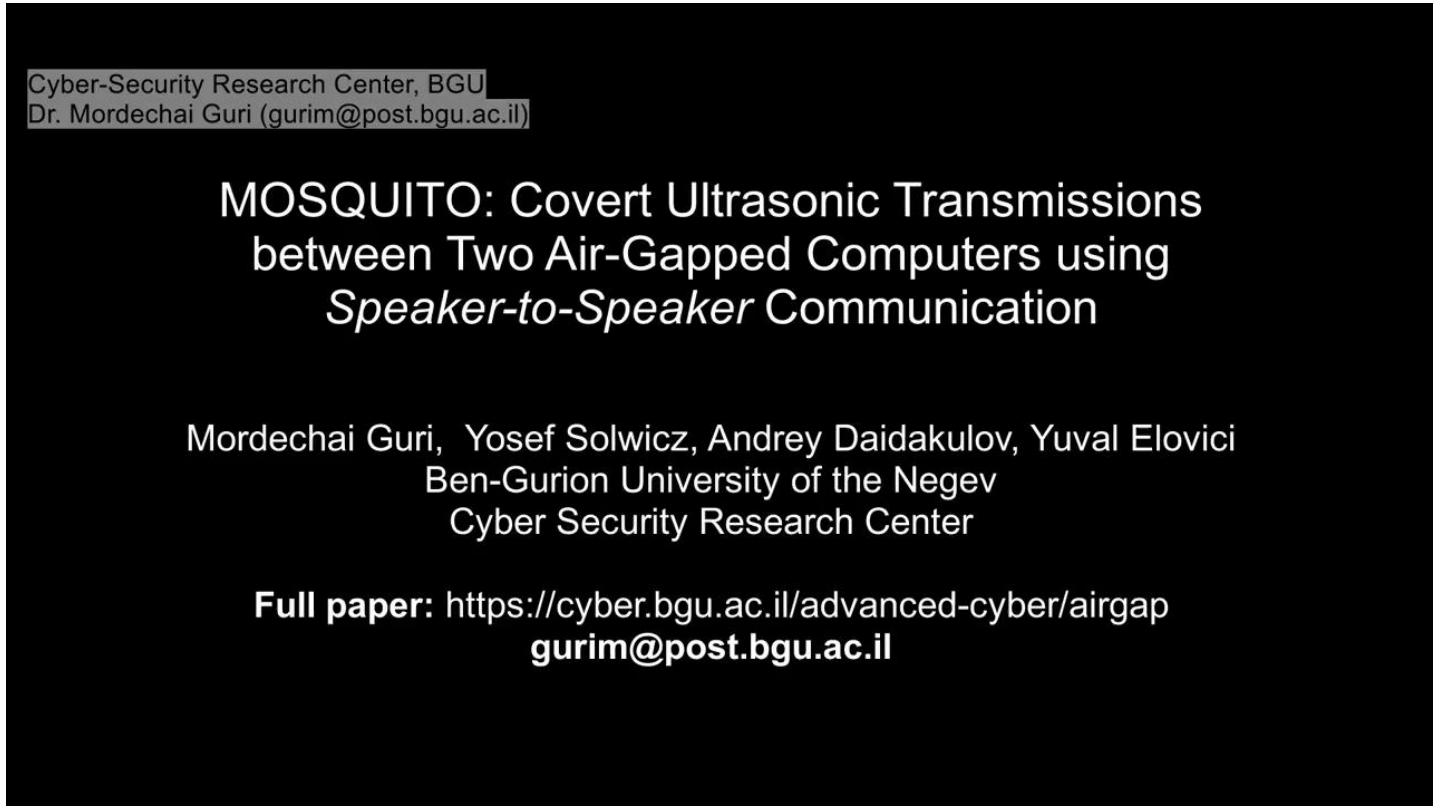


Usually not covered at all...

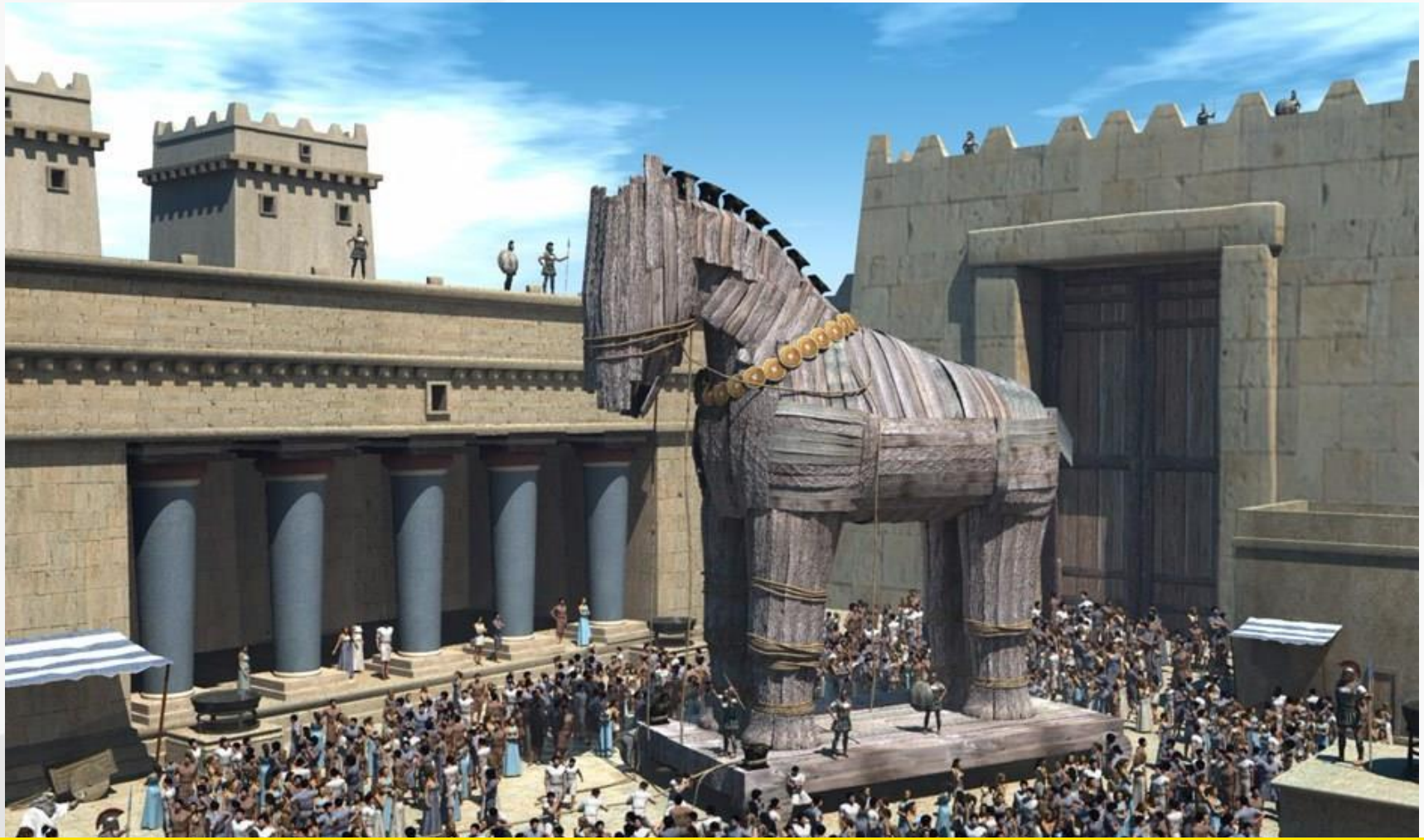
- Advanced and targeted cyber attacks
  - Human conducted phishing & exploit (email as vector)
  - Use of system internals (PowerShell, WMIC, Service Commands)
  - Use of remote admin tools (RAT) and hacking tools (Orcus, Litemanager, VNC, Mimikatz)
  - Hidden command & control traffic (Office365, GMail, HTTPS)

BREACHES HAPPEN:
BE PREPARED.

THE SECURITY LANDSCAPE IS CHANGING FASTER



The role of endpoint protection is still fundamental



CYBERSECURITY
IS A PROCESS

Preventive layer is crucial for mass attacks but it will not stop all advanced threats & targeted attacks

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

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.

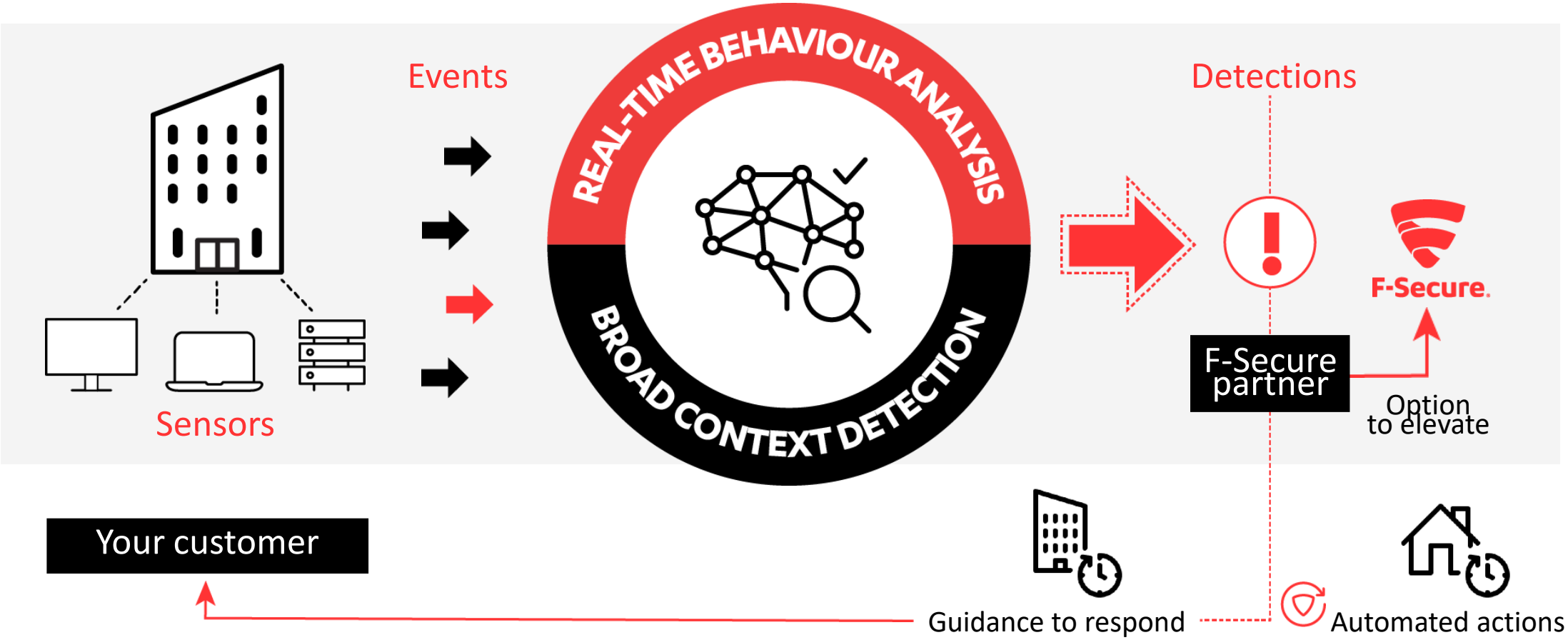
F-SECURE RDR/RDS

RAPID DETECTION & RESPONSE

RDR

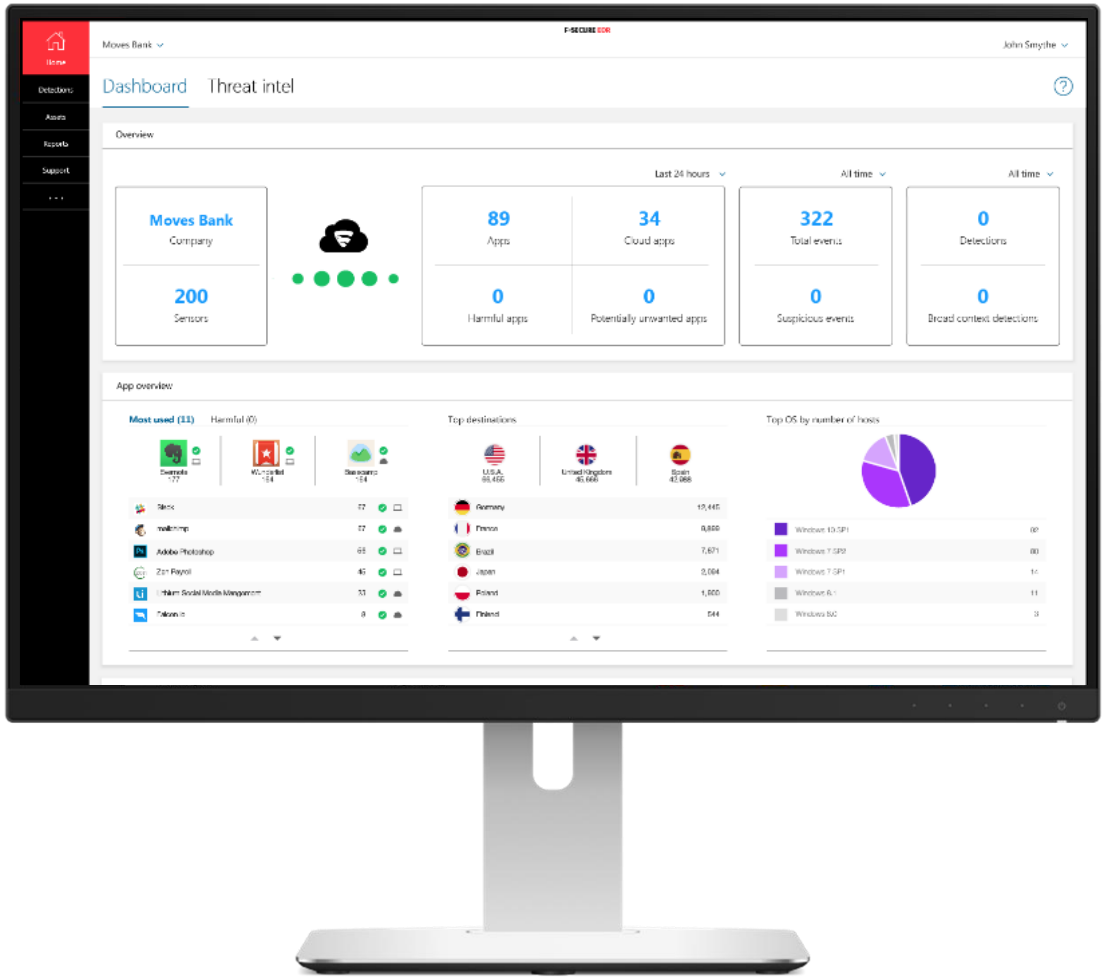
F-SECURE RAPID
DETECTION & RESPONSE

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



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*

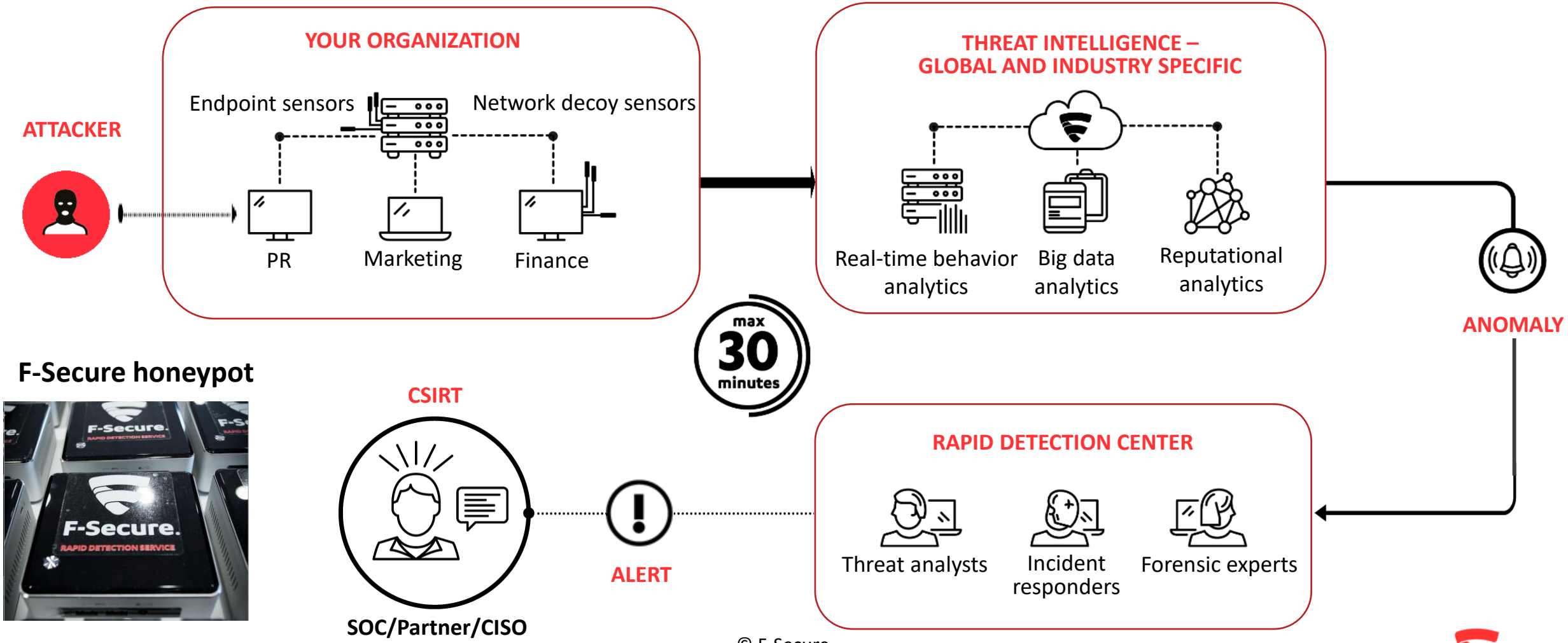
MANAGEMENT INTEGRATION*

*AVAILABLE AFTER THE CORE RELEASE

RAPID DETECTION SERVICE

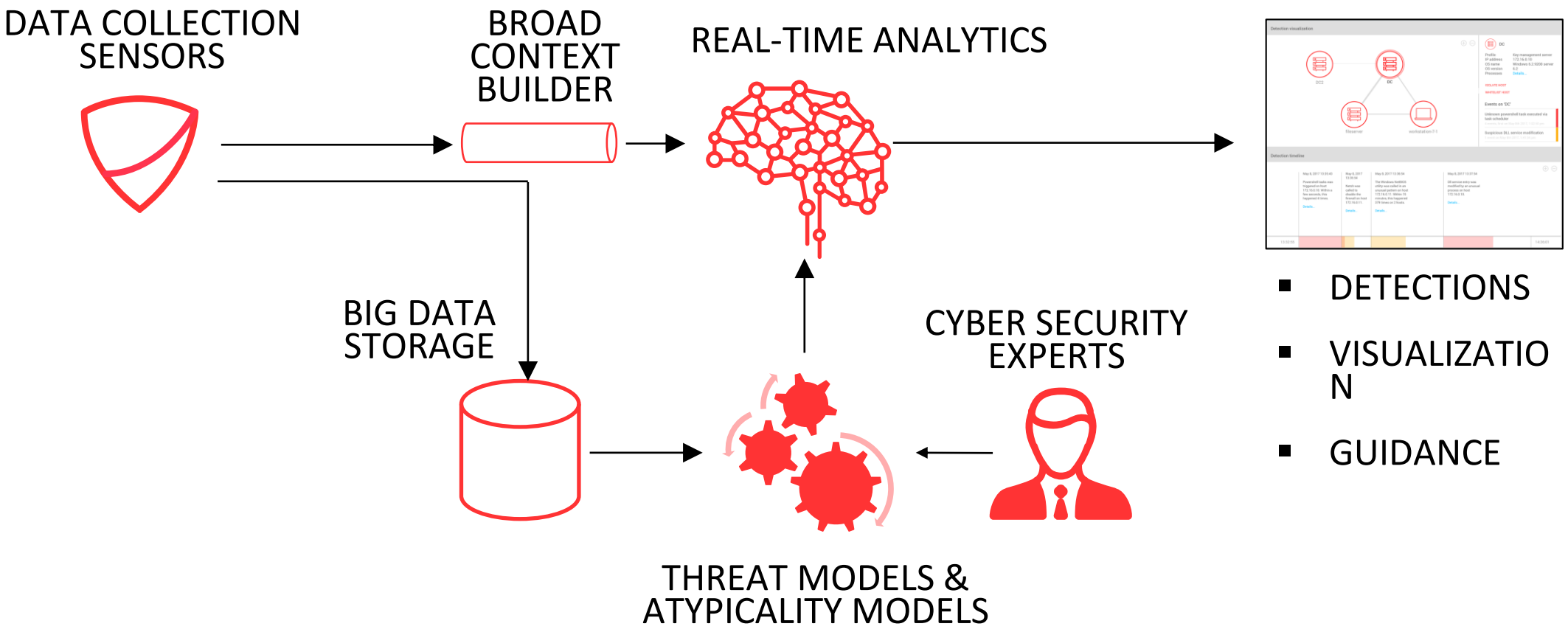
RDS

HOW RAPID DETECTION SERVICE WORKS
COMBINING MAN & MACHINE



F-Secure honeypot

AI AND MACHINE LEARNING AT THE HEART OF THE SOLUTION



PRACTICAL EXAMPLE FROM A REAL, MID-SIZE COMPANY

CAPTURING BEHAVIORAL EVENTS

500 mln
DATA EVENTS/MONTH

Collected by ~325 end-point sensors deployed across the organization

REAL-TIME BEHAVIORAL ANALYSIS

225,000
SUSPICIOUS EVENTS

After F-Secure's real-time behavior analysis of the raw data events

BROAD CONTEXT DETECTION™

6
DETECTIONS

After adding the broader context to the suspicious events

4
REAL THREATS

Confirmed as real threats

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


RAPID DETECTION
CENTER
F-Secure
WE SEE THINGS
OTHERS DON'T

PRIVACY & SECURITY

© 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

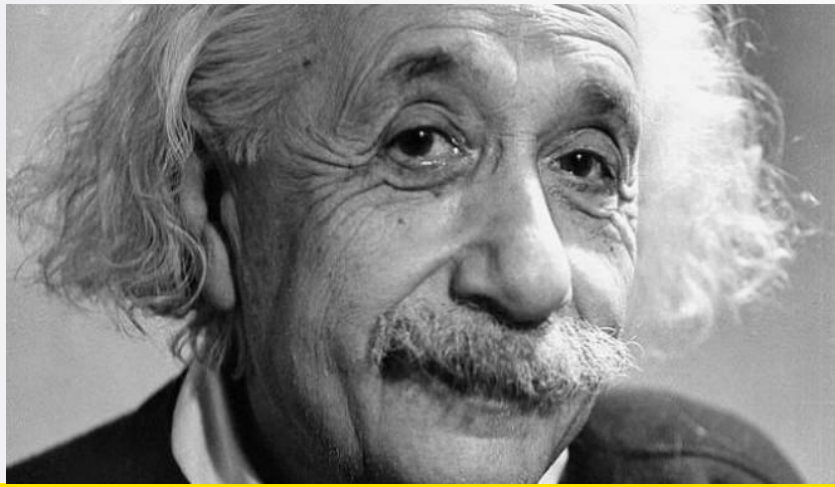
- The service is not intended for monitoring non-security related activities such as profiling employees' activities, interests, or interactions.
- The focus of data collection is not on individual employees or business documents.

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



F-Secure®

Grazie di aver partecipato !