Detecting the Intent, Not just the Technique

Changing the Mindset of Cyber Defense

Vadim Pogulievsky
Director of Cyber Research, Verint

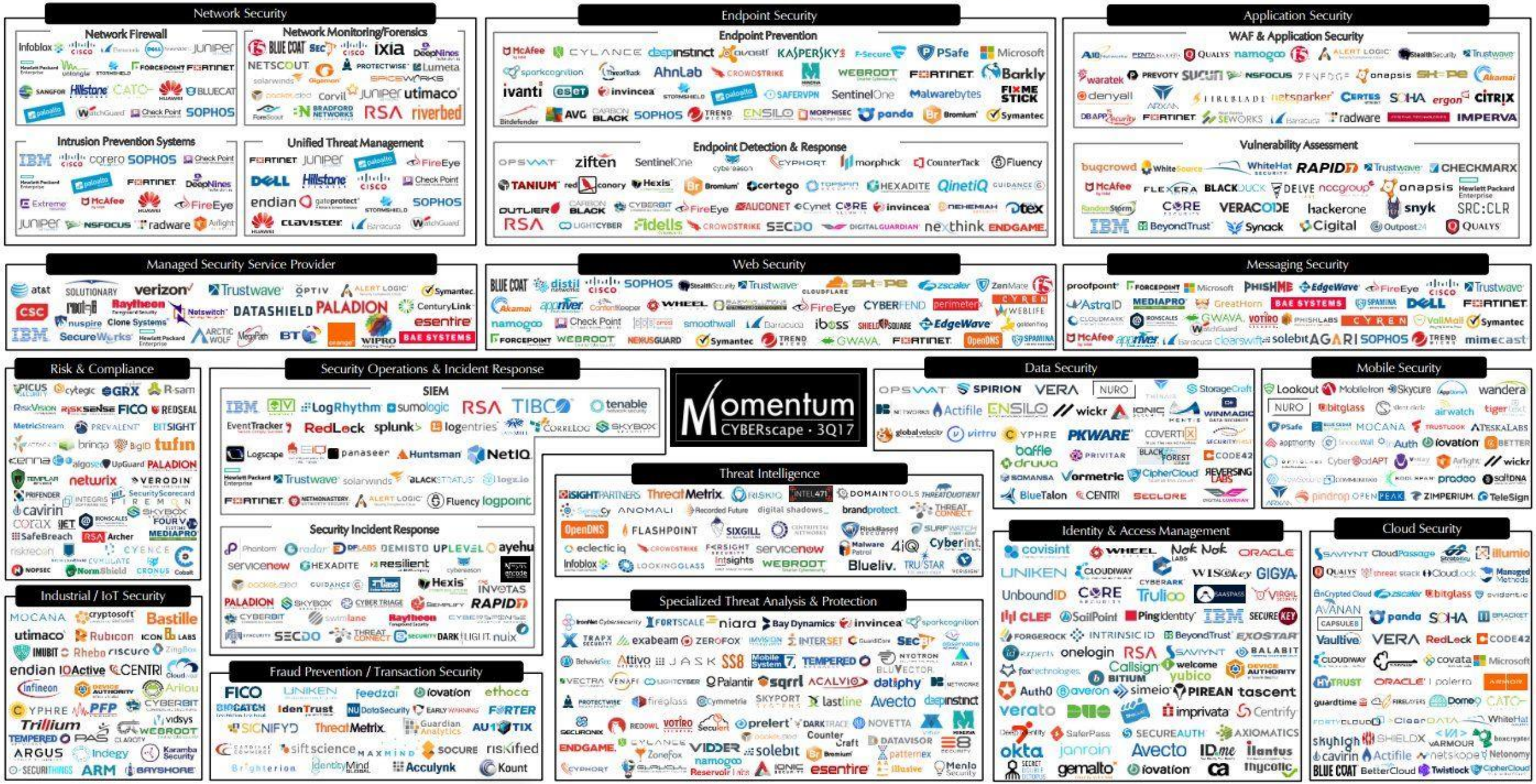
About me

- Vadim Pogulievsky
- Director of Cyber Research at Verint
- Building Cyber Security products for last 15 years
- Previously led Cyber Security Research teams for Finjan, M86 Security and McAfee

Agenda

- Current industry state
- Seeing a big picture
- Can it be better?
- What we should do as an industry to improve it?

CYBERscape: The Cybersecurity Landscape



Source: Momentum Partners

On the other hand..

"Hackers Attack Every 39 Seconds"

"One in Three Americans Hacked in the Past Year "

"Cyber crime damage costs to hit $6 trillion annually by 2021"

"Around one billion accounts and records were compromised worldwide in 2016 "

"Cyber crime will more than triple the number of unfilled cybersecurity jobs, which is predicted to reach 3.5 million by 2021"

So, why that's the situation?

+ Because we compare instead of cooperate

+ Because every single security product is built in a way it's the only product installed in customer's network

+ Because customer has to build a cyber defense ecosystem from products that weren't built to be a part of an ecosystem

High FP rate – Why it happens?

According to Cisco 2017 Security Capabilities Benchmark Study:

"Organizations can investigate only 56 percent of the security alerts they receive on a given day"

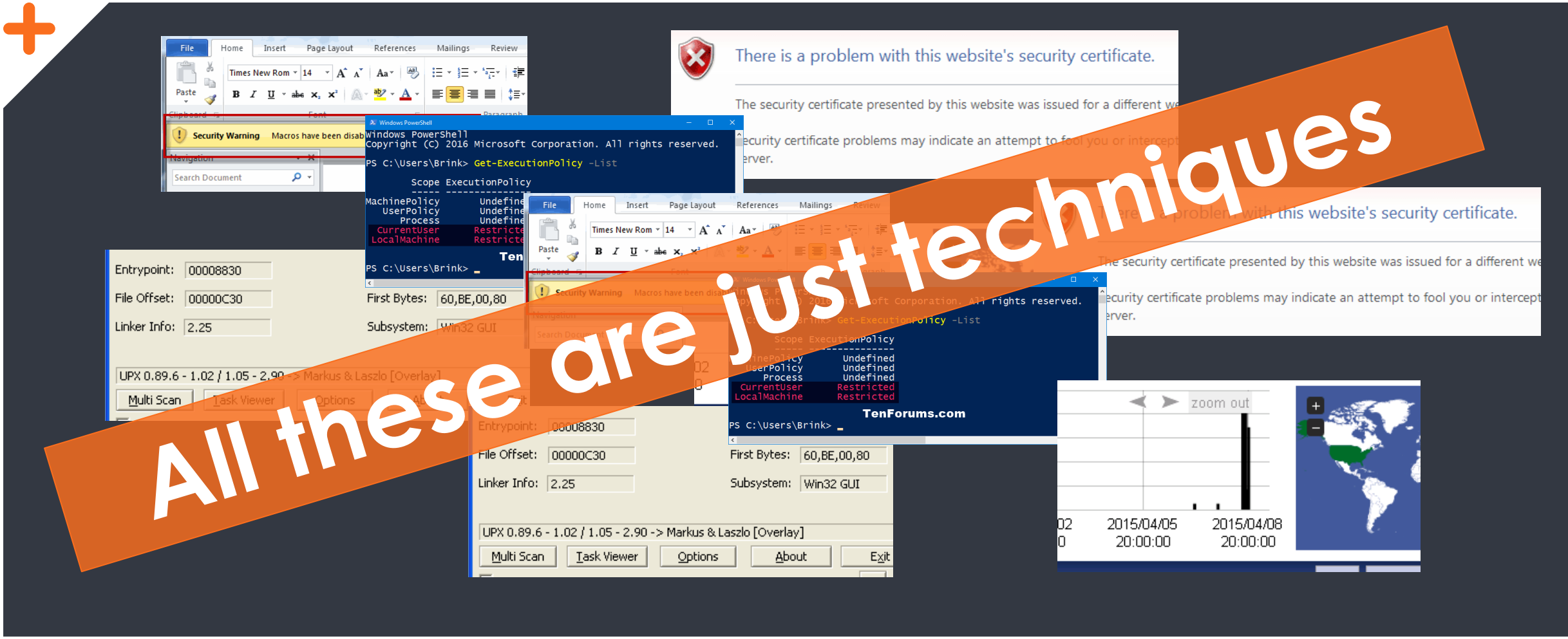
To Alert or Not to Alert?

I see a suspicious JS, but can't analyze it properly..
So, will I miss a possible attack
or
Create possible false positive?

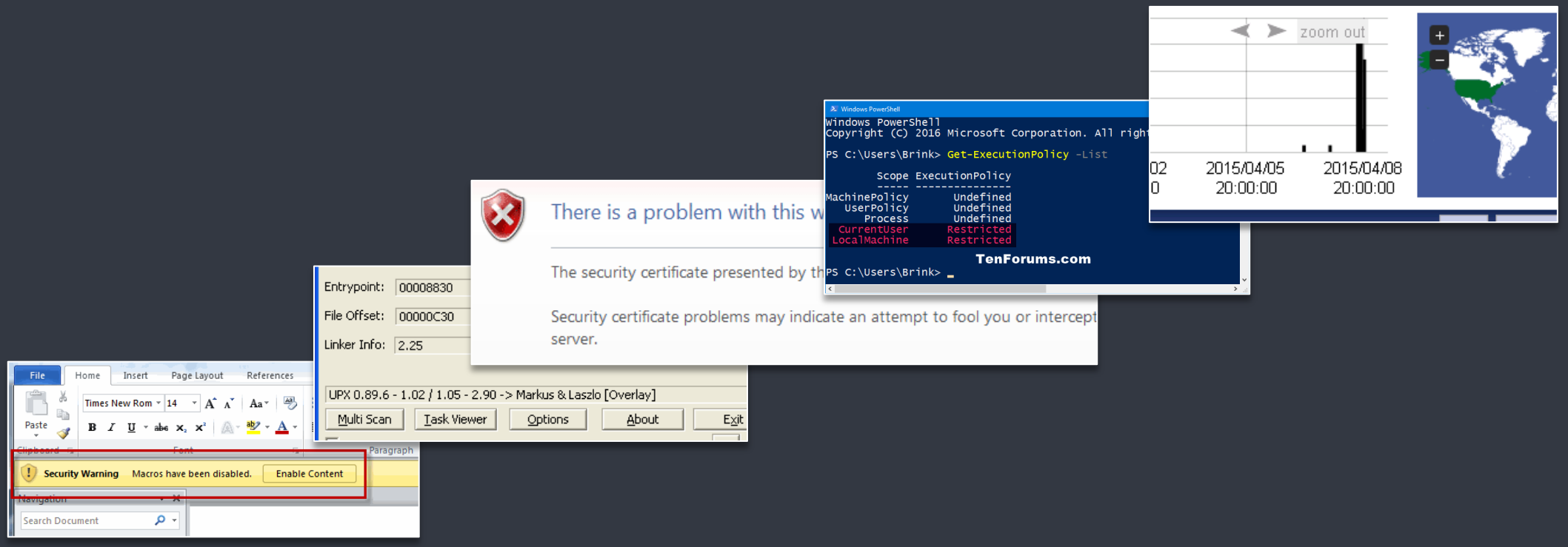
Dilemma…

PDF with Obfuscated JS

Detecting malicious technique is not enough



Seeing the entire picture – Is a Must!



Only this way you can understand the intent!

What if it would work this way..

Seeing all together is an utopia?

+ Interactive Conversation instead on One way Street
  - Ability to answer questions vs triggering alerts

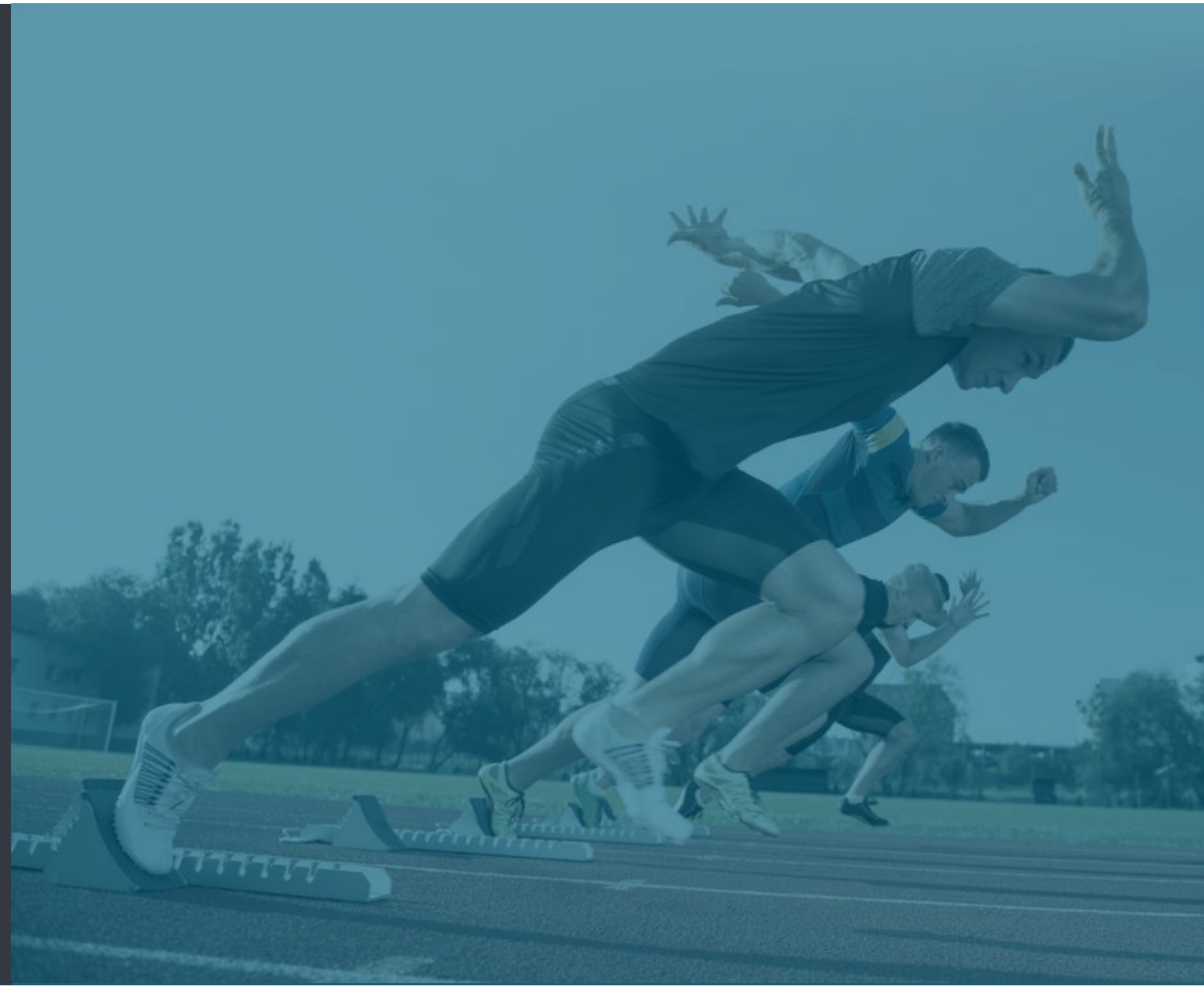
+ Automatic Investigation
  - Investigation of every single lead is too much for human

First Steps to this direction

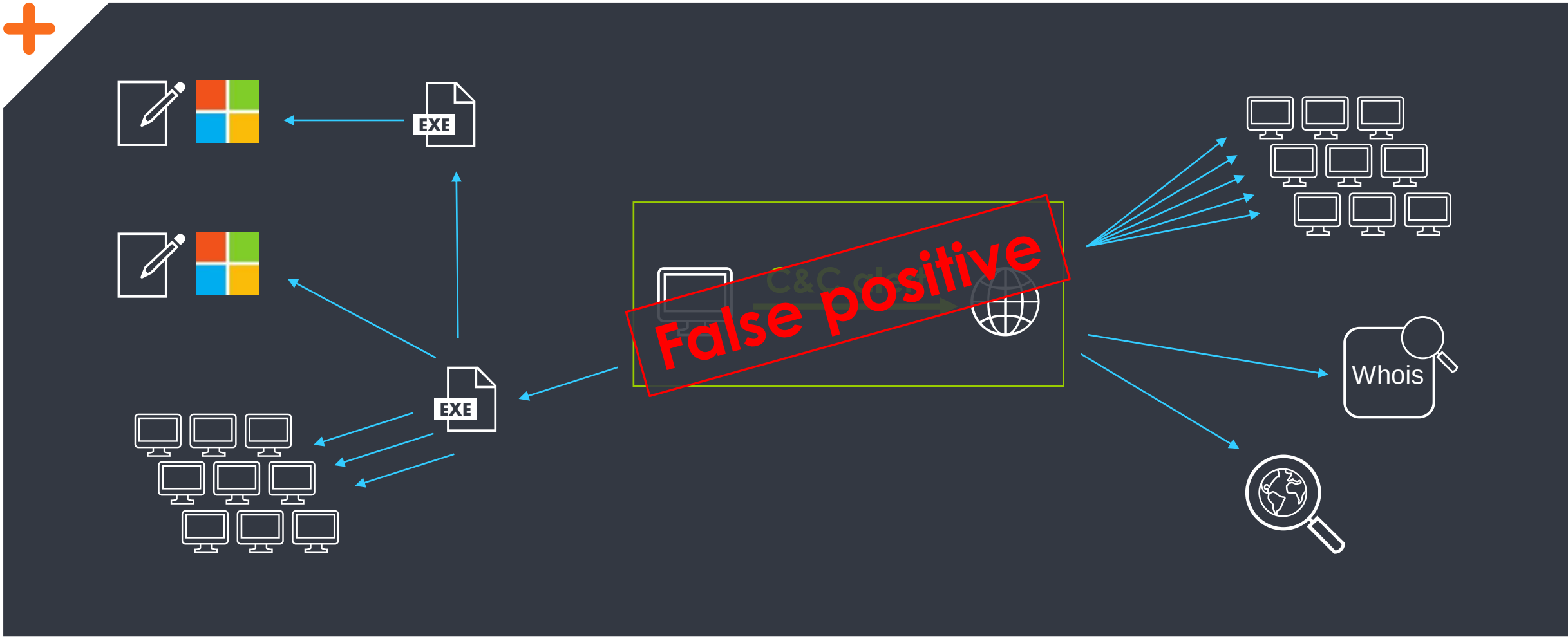
Security Automation and Orchestration

- Automating some time and effort consuming tasks
- Enriching data with internal and external sources

Good start, but not enough!
Let's look further !



False Positive investigation



True Positive investigation

Building an integrated cyber security ecosystem

Detection
One lead for an attack should be enough

Forensics data
Collecting in advance for future investigations

Investigation Engine
Run the investigation process and make decisions

Response
Response in a best appropriate way

Summary

- Ecosystem instead of silo products
- Automation as a central investigation platform
- Every alert is investigated
- Relevant forensics data is available for investigations


VERINT
Thank You!