



# 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

## Network Security

**Network Firewall**  
Infoblox, Cisco, Palo Alto, Juniper, Fortinet, Check Point, Sophos, WatchGuard, SANGFOR, Hillstone, CATO, Huawei, BlueCat, WatchGuard, Check Point, SOPHOS

**Network Monitoring/Forensics**  
Blue Coat, Sec, Ixia, DeepNines, Netscout, Solarwinds, Protectwise, Lumeta, Spiceworks, Checkmate, Corvil, Juniper, Utimaco, ForeScout, Bradford Networks, RSA, Riverbed

**Intrusion Prevention Systems**  
IBM, Cisco, Corero, Sophos, Check Point, Fortinet, DeepNines, McAfee, Huawei, FireEye, Juniper, NSFOCUS, Radware, Avlight

**Unified Threat Management**  
Fortinet, Juniper, Palo Alto, FireEye, Dell, Hillstone, Cisco, Check Point, Endian, Gateprotect, Stormshield, Sophos, Huawei, Clavister, Barracuda, WatchGuard

## Endpoint Security

**Endpoint Prevention**  
McAfee, Cylance, DeepInstinct, Avast, Kaspersky, F-Secure, P-Safe, Microsoft, SparkCognition, ThreatStack, AhnLab, CrowdStrike, Webroot, Fortinet, Barkly, Ivanti, Eset, Invincea, Stormshield, Palo Alto, SafeVpn, SentinelOne, Malwarebytes, Fixme Stick, BitDefender, AVG, Carbon Black, Sophos, Trend Micro, Emsisoft, Morphisec, Panda, Bromium, Symantec

**Endpoint Detection & Response**  
Opswat, Ziften, SentinelOne, Cybereason, Cyphort, Morphick, CounterTack, Fluency, Tanium, Red Canary, Hexis, Bromium, Certego, Topspin, Hexadite, Qinetiq, Guidance, Outlier, Carbon Black, Cyberbit, FireEye, Audonnet, Cynet, Core, Invincea, Nessmah, Dtex, RSA, LightCyber, Fidells, CrowdStrike, Secdo, Digital Guardian, Nextthink, Endgame

## Application Security

**WAF & Application Security**  
AIO, Qualys, Namogoo, Alert Logic, HealthSecurity, Trustwave, Waratek, Prevoty, Sucuri, NSFOCUS, ZENEDGE, Onapsis, SH-PE, Akamai, Denyall, Fireblade, Netsparker, Certes, SOHA, Ergon, Citrix, DBApp, Fortinet, Secworks, Barracuda, Radware, Imperva

**Vulnerability Assessment**  
Bugcrowd, WhiteSource, WhiteHat, Rapid7, Trustwave, Checkmarx, McAfee, Flexera, BlackDuck, Delve, Nocgroup, Onapsis, Hewlett Packard Enterprise, BeyondTrust, Synack, Cigital, Outpost24, Qualys

## Managed Security Service Provider

At&T, Solutionary, Verizon, Trustwave, Optiv, Alert Logic, Symantec, CSC, Raytheon, Notswitch, Datashield, Paladion, CenturyLink, IBM, Nuspire, Clone Systems, Arctic Wolf, BT, Wipro, BAE Systems, ESentire

## Web Security

Blue Coat, Distil, Cisco, Sophos, HealthSecurity, Trustwave, Cloudflare, SH-PE, Zscaler, ZenMate, Akamai, Apprivo, ContentKeeper, Wheel, FireEye, Cyberfend, Perimeter, Cyren, Namogoo, Check Point, Smoothwall, Barracuda, Iboss, ShieldSquare, EdgeWave, GoldenFog, Forcepoint, Webroot, NewsGuard, Symantec, Trend Micro, Gwava, Fortinet, OpenDNS, Spanix

## Messaging Security

Proofpoint, Forcepoint, Microsoft, PhishME, EdgeWave, FireEye, Cisco, Trustwave, AstralID, Mediapro, GreatHorn, BAE Systems, Spanix, Dell, Fortinet, Cloudmark, Bomscals, Gwava, Votiro, PhishLabs, Cyren, VailMail, Symantec, McAfee, Apprivo, Barracuda, Clearswift, Solebit, Agari, Sophos, Trend Micro, Mimecast

## Risk & Compliance

Vpicus, Cyteck, GRX, R-sam, RiskVision, RiskSense, FICO, RedSeal, MetricStream, Prevalent, BitSight, Cenna, Algosix, UpGuard, Paladion, Netwrix, Verodin, RiskFender, Integrals, SecurityScorecard, Remon, Cavirin, Corax, JET, Bomscals, Skybox, SafeBreach, RSA, Archer, Mediapro, Riskrecon, Cyvulate, Cyence, Nopsec, NormShield, Cronus, Cobalt

## Security Operations & Incident Response

**SIEM**  
IBM, LogRhythm, Sumologic, RSA, TIBCO, Tenable, EventTracker, RedLock, Splunk, Logentrics, Correlog, Skybox, Logscape, Panaseen, Huntsman, NetIQ, Hewlett Packard Enterprise, Trustwave, Solarwinds, BlackStatus, Logzila, Fortinet, Netmonitory, Alert Logic, Fluency, Logpoint

**Security Incident Response**  
Phantom, Radar, Opslabs, Demisto, Uplevel, Ayehu, Servicenow, Hexadite, Resilient, Invotas, Paladion, Skybox, CyberTriage, Demury, Rapid7, Cyberbit, Swimlane, Raytheon, CyberSense, Infoblox, Secdo, Threat Connect, SecurityDark, Ligitt, Nuix

**Momentum**  
CYBERScape · 3Q17

## Data Security

Opswat, Spion, Vera, Nuro, StorageCraft, Actifile, ENSILO, Wickr, IONIC, Winagic, GlobalVelocity, Vitru, CYPHRE, PKWARE, COVERTIX, Baffle, Druva, Privitar, BlackForest, CODE42, SOMANSA, Vormetric, CipherCloud, REVERSING LABS, BlueTalon, CENTRI, SECLORE

## Mobile Security

Lookout, MobileIron, SkyCure, Wandera, Nuro, Bitglass, AirWatch, TigerConnect, P-Safe, MOCANA, Trustlook, Ateskalabs, Appointy, Auth, Iovation, Better, CyberAdapt, Aflights, Wickr, Pradeo, SaltDNA, Pindrop, OpenPeak, Zimperium, TeleSign

## Industrial / IoT Security

Mocana, Cryptosoft, Bastille, Utimaco, Rubicon, Icon Labs, Inubit, Rheba, Riscuro, ZingBox, Endian, IOActive, CENTRI, InFINEON, ADVISORY, Arivio, Cyberbit, YPHRE, PFP, Vidys, Trillium, PAS, Webroot, ARGUS, Indegy, Karamba Security, Securithings, ARM, Grayshore

**Threat Intelligence**  
ISIGHT PARTNERS, ThreatMetrix, RISIKIO, INTEL471, DOMAINTOOLS, THREATQUOTIENT, ANOMALI, Recorded Future, Digital Shadows, BrandProtect, OpenDNS, FLASHPOINT, SIXGILL, CENTRI, SURFPOST, EclecticIQ, CrowdStrike, FERSIGHT, Servicenow, Malware Patrol, 4iQ, Cyberint, Infoblox, LookingGlass, IntSights, Webroot, Blueliv, TRU STAR

## Identity & Access Management

Covisint, Wheel, Nok Nok, Oracle, UnboundID, Core, Trulioo, SaaSPASS, VIRGIL, CLEF, SailPoint, PingIdentity, IBM, SecureKey, Forgerock, Intrinsic ID, BeyondTrust, EXOSTAR, Experts, Onelogin, RSA, SAVINT, BALABIT, Fxtechnologies, CallSign, welcome, DEVISE AUTHORITY, Auth0, Avera, Simeio, PIREAN, tascant, Verato, Duo, Impriata, Centrify, DeepFinity, SaferPass, SECUREAUTH, AXIOMATICS, Okta, Janrain, Avecto, ID.me, Iantus, Gemalto, Iovation, CA, mycoic

## Cloud Security

SavvyNT, CloudPassage, Illumio, Qualys, Threat Stack, CloudLock, Managed Methods, Encrypted Cloud, Zscaler, Bitglass, EvidentIQ, AVANIR, Panda, SOHA, BRACKET, Vaultive, VERA, RedLock, CODE42, Cloudway, Covata, Microsoft, TRUST, ORACLE, Polerra, ABBOR, Guardtime, FIRELAYERS, Dome, CATO, FortifyCloud, ClearDATA, WhiteHat, Skyhigh, SHIELDX, VARMOUR, CAVIRIN, Actifile, netskope, Netonomy, Blue Coat, BetterCloud, Twistlock, CipherCloud

## Fraud Prevention / Transaction Security

FICO, UNIKEN, feedzai, Iovation, ethoca, Biogatch, IdenTrust, NU DataSecurity, EARLY WARNING, FORTER, SICNIFYD, ThreatMetrix, Guardian Analytics, AU1TIX, Brighterion, IdentityMind, Acculynk, Kount

## Specialized Threat Analysis & Protection

Innovative Cybersecurity, FORTSCALE, niara, Bay Dynamics, Invincea, SparkCognition, TRAPX SECURITY, exabeam, ZEROFOX, IMVISION, INTERSET, GuardDns, SEC, Vectra, Venafi, LightCyber, Palantir, sqrrl, ACALYIO, datiphy, Network, Behavior, Attivo, JASK, SSB, Mobile System, TEMPERED, NYOTRON, AREA 1, PROTECTWISE, Fireglass, Cymmetria, SKYPORT, lastline, Avecto, DeepInstinct, Securonix, Redowl, Votiro, Securix, preler, DARKTRAC, NOVETTA, ENDGAME, Cylance, ZoneFax, VIDDER, namogoo, Solebit, Craft, Patternex, Cyphort, Reservoir, IONIC, esentire, Illusive, Menlo Security

# 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

```
12 0 obj
<</JS 11 0 R /S /JavaScript>>
endobj
13 0 obj
<</Length 521 /Filter [/FlateDecode]>>
stream
x<9c>]<92>0sq@^PÄÛ^V^<97>^He6â^ZMÛr=h<8c>^XwñÏVBÖK<97>^F^P" <84>Ä%iüi<99>é<99>^
^ [=W%«Pà!^A^·<99>\&I'<93>$f^G0ó<93>ë<8d>Cg«<8d>c; iµ<8b>iDCø.<88><8e>8ÇÉAC:á#<84>
^?úá<83>éäY=A<8e>]<96>^] Ä^K<96>qvx`9±^C=WXX¹»XävN3,Y^[^FkmY^?E;(P ê9!1<85>U0E0^
endstream
endobj
14 0 obj
<</JS 13 0 R /S /JavaScript>>
endobj
15 0 obj
<</Length 185 /Filter [/FlateDecode]>>
stream
x<9c>M<8f>K^K<82>@^Ä¿ÉviW^Ho<9d>ÄC^=v<90>^TB½^LzEx!^V=DøY[^_ [P~3iïi¿I<9e>ä0^Föä
endstream
endobj
16 0 obj
<</JS 15 0 R /S /JavaScript>>
endobj
17 0 obj
```



# Detecting malicious technique is not enough



File Home Insert Page Layout References Mailings Review

Times New Rom 14 A Aa B I U abc x, x' Aa

Clipboard Font Paragraph

Security Warning Macros have been disabled

Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
PS C:\Users\Brink> Get-ExecutionPolicy -List

```
Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Restricted
LocalMachine Restricted
```

File Home Insert Page Layout References Mailings Review

Times New Rom 14 A Aa B I U abc x, x' Aa

Clipboard Font Paragraph

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website than the one that you are trying to visit.

Security certificate problems may indicate an attempt to fool you or intercept your data. To help protect your privacy, Outlook prevented automatic download of this picture.

Entry point: 00008830  
File Offset: 00000C30  
Linker Info: 2.25

First Bytes: 60,BE,00,80  
Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo [Overlay]

Multi Scan Task Viewer Options

File Home Insert Page Layout References Mailings Review

Times New Rom 14 A Aa B I U abc x, x' Aa

Clipboard Font Paragraph

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website than the one that you are trying to visit.

Security certificate problems may indicate an attempt to fool you or intercept your data. To help protect your privacy, Outlook prevented automatic download of this picture.

Entry point: 00008830  
File Offset: 00000C30  
Linker Info: 2.25

First Bytes: 60,BE,00,80  
Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo [Overlay]

Multi Scan Task Viewer Options About Exit

TenForums.com

PS C:\Users\Brink> \_

zoom out

2015/04/05 20:00:00 2015/04/08 20:00:00

World map showing a green highlighted region in South America.

**All these are just techniques**

# Seeing the entire picture – Is a Must!



The collage consists of several overlapping windows:

- Microsoft Word:** Shows a document with a "Security Warning" that says "Macros have been disabled." and an "Enable Content" button.
- Windows PowerShell:** Displays the command `Get-ExecutionPolicy -List` and its output:

Scope	ExecutionPolicy
MachinePolicy	Undefined
UserPolicy	Undefined
Process	Undefined
CurrentUser	Restricted
LocalMachine	Restricted
- Security Warning:** A white dialog box with a red shield icon containing a white 'X'. The text reads: "There is a problem with this website's security certificate. The security certificate presented by this website may indicate an attempt to fool you or intercept the data you are sending to the server."
- Bar Chart:** A chart with a y-axis from 0 to 02 and an x-axis with dates 2015/04/05 and 2015/04/08. A single bar is visible at 2015/04/05. A "zoom out" button is present.
- World Map:** A small globe showing North and South America, with a green highlight over the United States.

Only this way you can understand the intent!

# What if it would work this way..



“Hey folks, found a fishy file sending some traffic to suspicious domain. Anyone can take a look?”



“Hi there, scanned it. Don't worry, it's benign, on my whitelist”



# 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



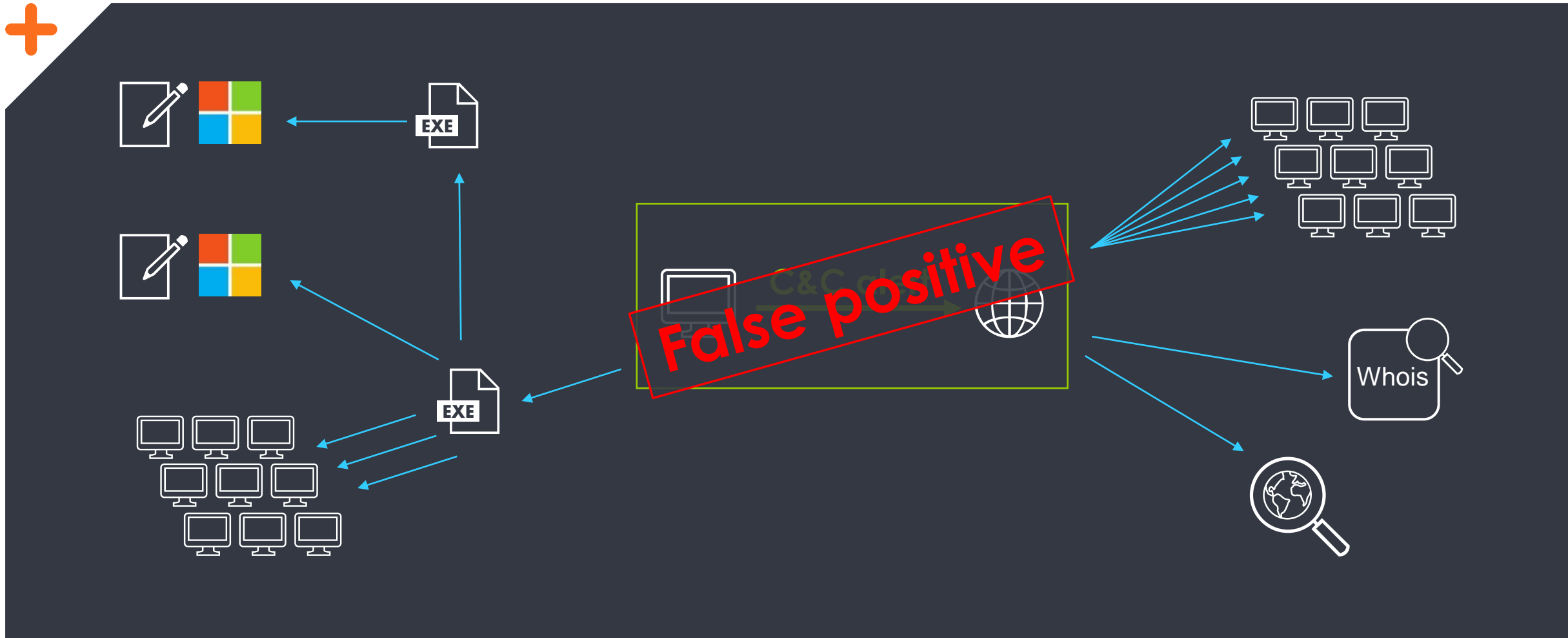
## Security Automation and Orchestration

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

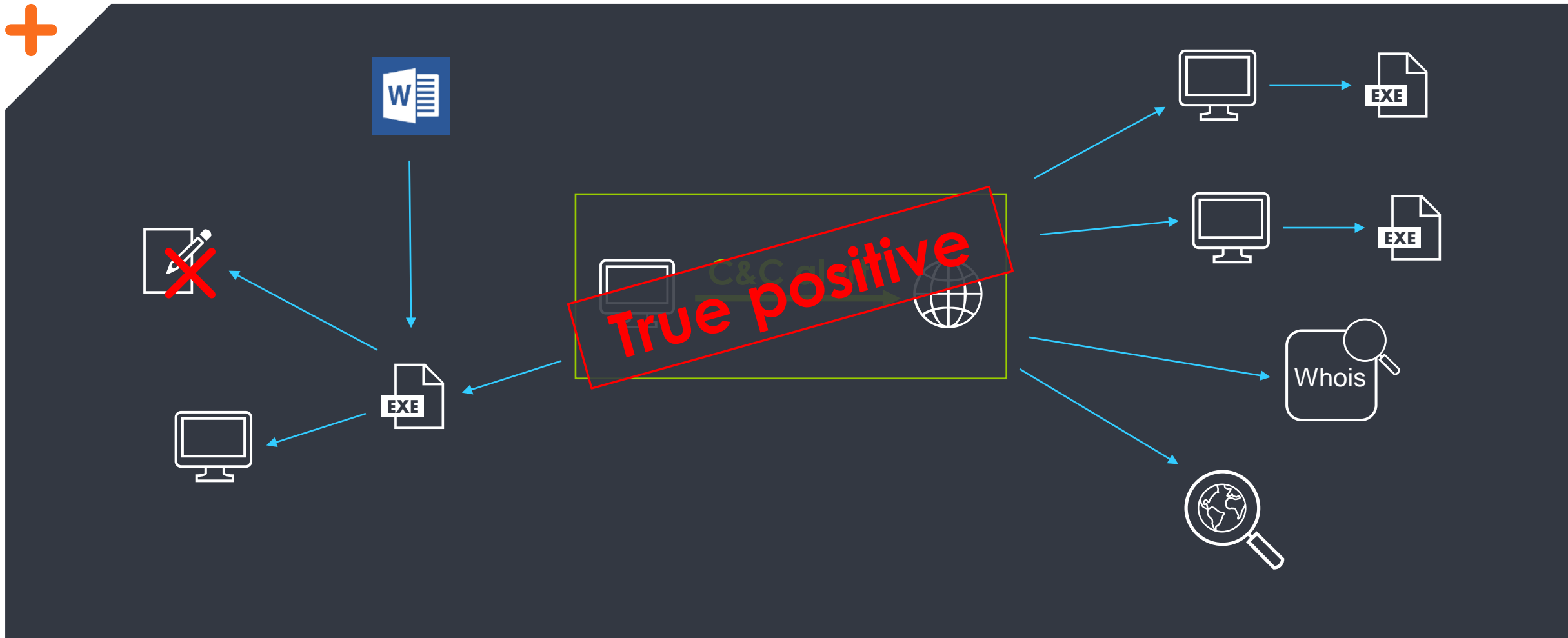
Good start, but not enough!  
Let's look further !



# False Positive investigation



# True Positive investigation



# Building an integrated cyber security ecosystem







## Summary



Ecosystem  
instead of silo  
products



Automation as a  
central  
investigation  
platform



Every alert is  
investigated



Relevant  
forensics data is  
available for  
investigations



Thank You!