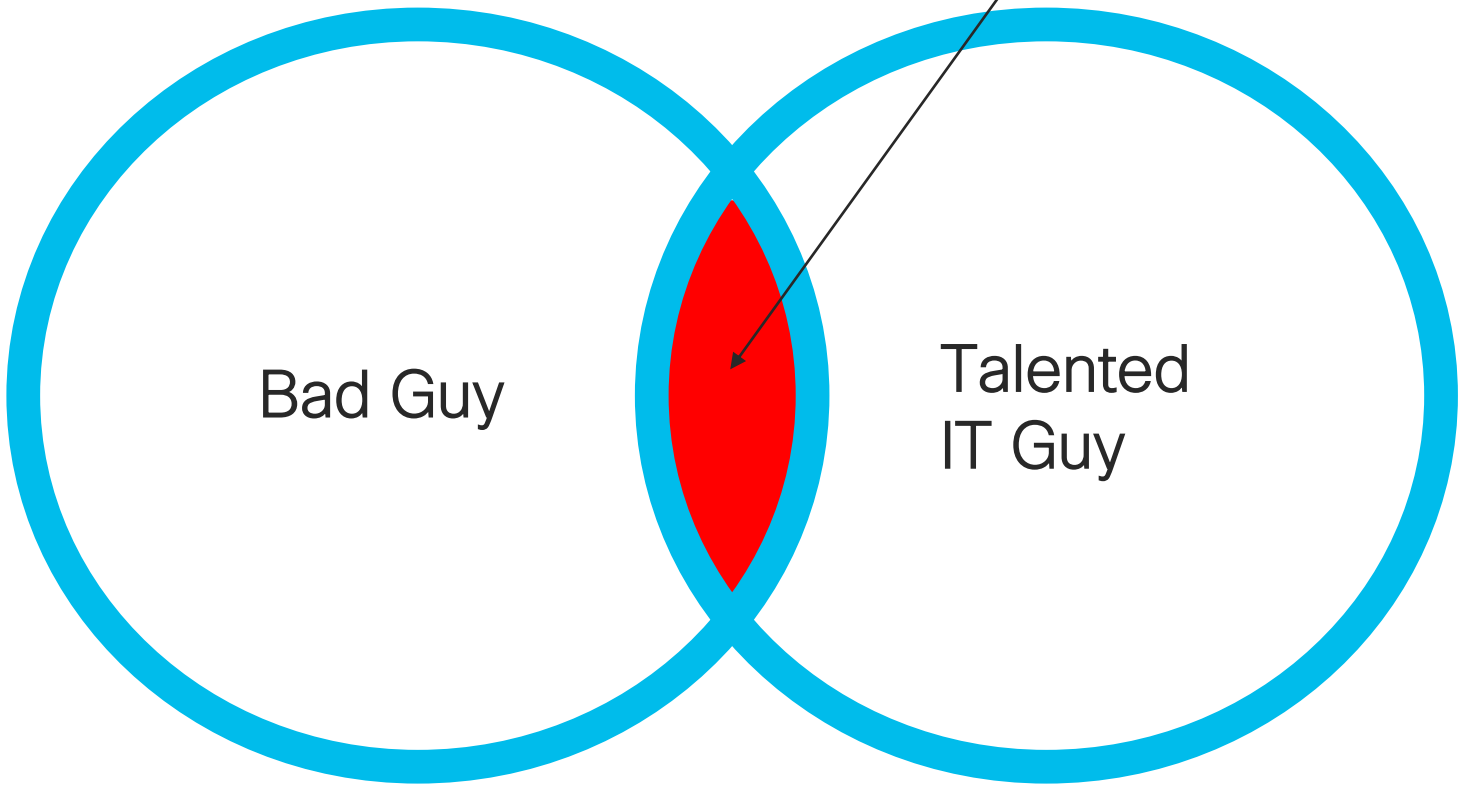
How to make the invisible threats visible

AMP Everywhere

Andreas Schober – AMP Cyber Security Team
Volodymyr Ilibman – Cyber Security Ukraine

Who can be a Hacker?
(in the past)



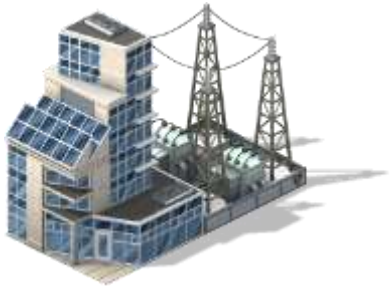
Who can be a Hacker?
(Today)

HaaS

Hacking as a Service

Every „Bad Guy“ can be a Hacker
and
State-owned Actors

Известные атаки



Май 2014

Атака на предприятия Укрзалізниці

Август 2014

Blackenergy 0-Day атака на широкий спектр органов госвласти в Украине

Октябрь 2015

Blackenergy атака на медиакомпании. Уничтожение видеоматериалов, вывод из строя рабочих мест операторов

Декабрь 2015

Blackenergy атака на ряд облэнерго. Вывод из строя АСУТП электроподстанций, обесточена значительная территория на несколько часов

Декабрь 2015

Атака на АП Борисполь при помощи BlackEnergy

Time

Известные атаки

Декабрь 2016

Атака на финансовые и транспортные организации

Декабрь 2016

Атака на энергосистемы с помощью malware Industroyer

Май 2017

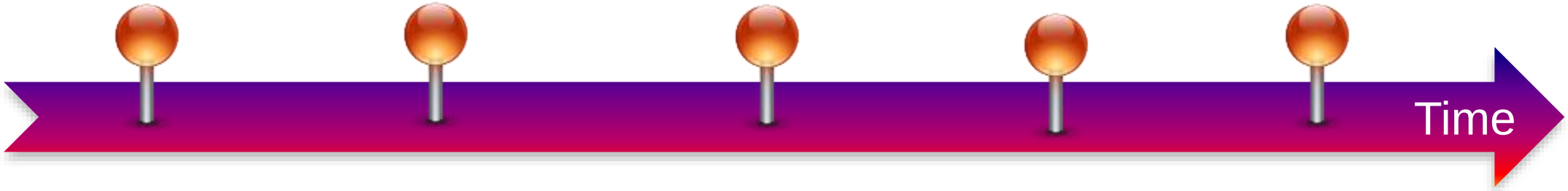
Атака WannaCry

Июнь 2017

Атака Nyetya/Notpetya, которая затронула большинство предприятий Украины

Октябрь 2017

Атака badrabbit, пострадали организации в Украине, Болгарии, Турции, России



И на закуску…VPNFilter

https://blog.talosintelligence.com/2018/05/VPNFilter.html

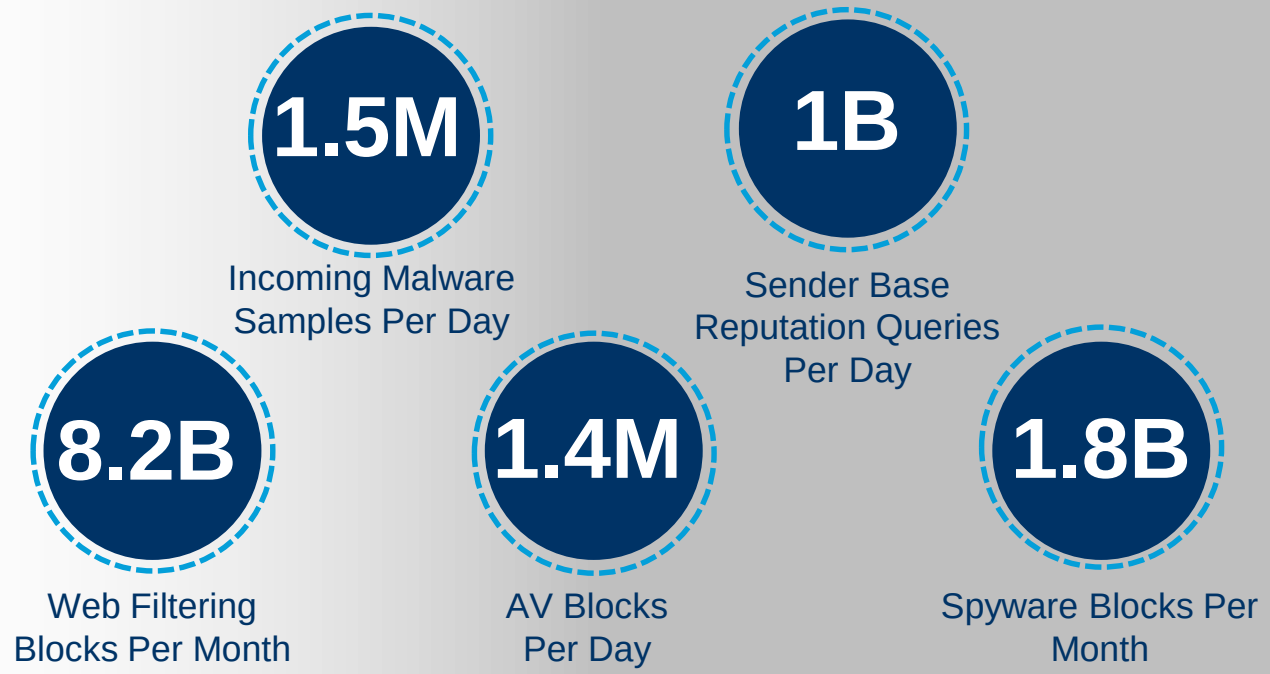
Cisco активно развивает аналитику и обмен информацией о киберугрозах

TALOS

300+
Исследователей угроз

100TB
Аналитической информации

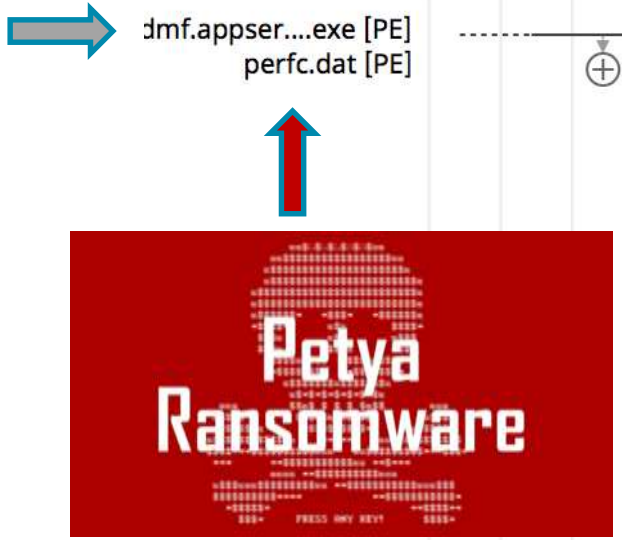
19.7M
Угроз в день

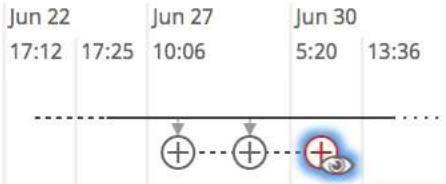


https://www.talosintelligence.com

AMP в расследовании и защите от Neytya/ Non-Petya

M.E.Doc





2017-06-30 08:20:34 EEST

Detected W32.Malwaregen:Petya.20h3.1201 as **perfc.dat** (027cc45..d3a745)[PE_Executable] .

Created by an unknown process. Could **not** get a handle on the process's executable.

The file was **not quarantined.** In audit only mode.

File full path: C:\Windows\perfc.dat

File SHA-1: 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d.

File MD5: 71b6a493388e7d0b40c83ce903bc6b04.

File size: 362360 bytes.

File signed by Microsoft Corporation with certificiate serial 6101cf3e00000000000f from Microsoft Code Signing PCA. Expired 22:40:29, Mon Mar 7 2011 UTC. the certificate was **Cloud Recall**.

Many endpoint solutions claim to block

99% of threats

But what about the 1% of threats they're missing?

How does that 1% get through?

Advanced evasion techniques:

- Fileless malware
- Environmentally-aware malware
- Polymorphism
- Exploit legitimate processes

Uncover the 1% with Cisco AMP for Endpoints

Stop Malware

Using multiple detection and protection mechanisms

Eliminate Blind Spots

The network and endpoint, working together across all operating systems

Discover Unknown Threats

With proactive threat hunting

Stop Malware

Using multiple detection and protection mechanisms

How we…

Prevent

- Antivirus
- Fileless malware detection
- Cloud lookups (1:1, 1:many)
- Client Indicators of Compromise

Detect

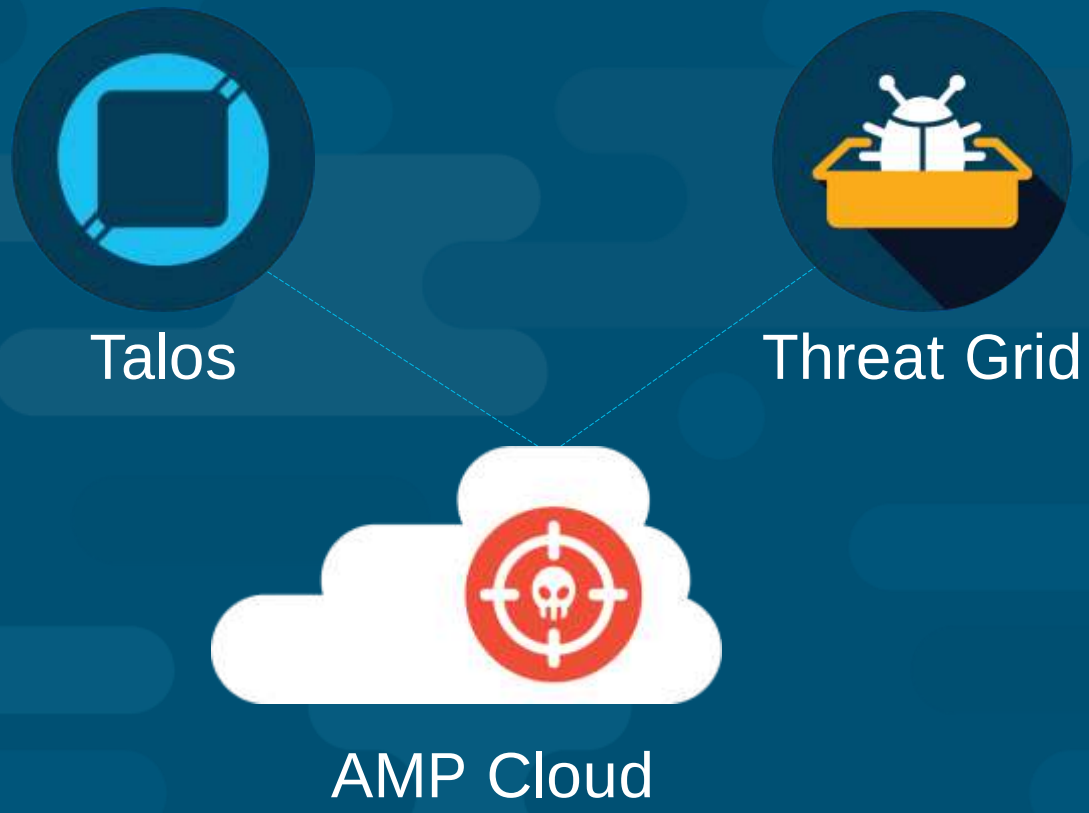
- Static analysis
- Sandboxing
- Malicious Activity Protection
- Machine learning
- Device flow correlation
- Cloud Indicators of Compromise

Reduce Risk

- Vulnerable software
- Low prevalence
- Proxy log analysis

Cloud-based analysis

AMP cloud constantly updated with the latest threat intelligence and research to protect against advanced threats.



Eliminate Blind Spots

The network, web, email and endpoints, working together across all operating systems

See once, block everywhere

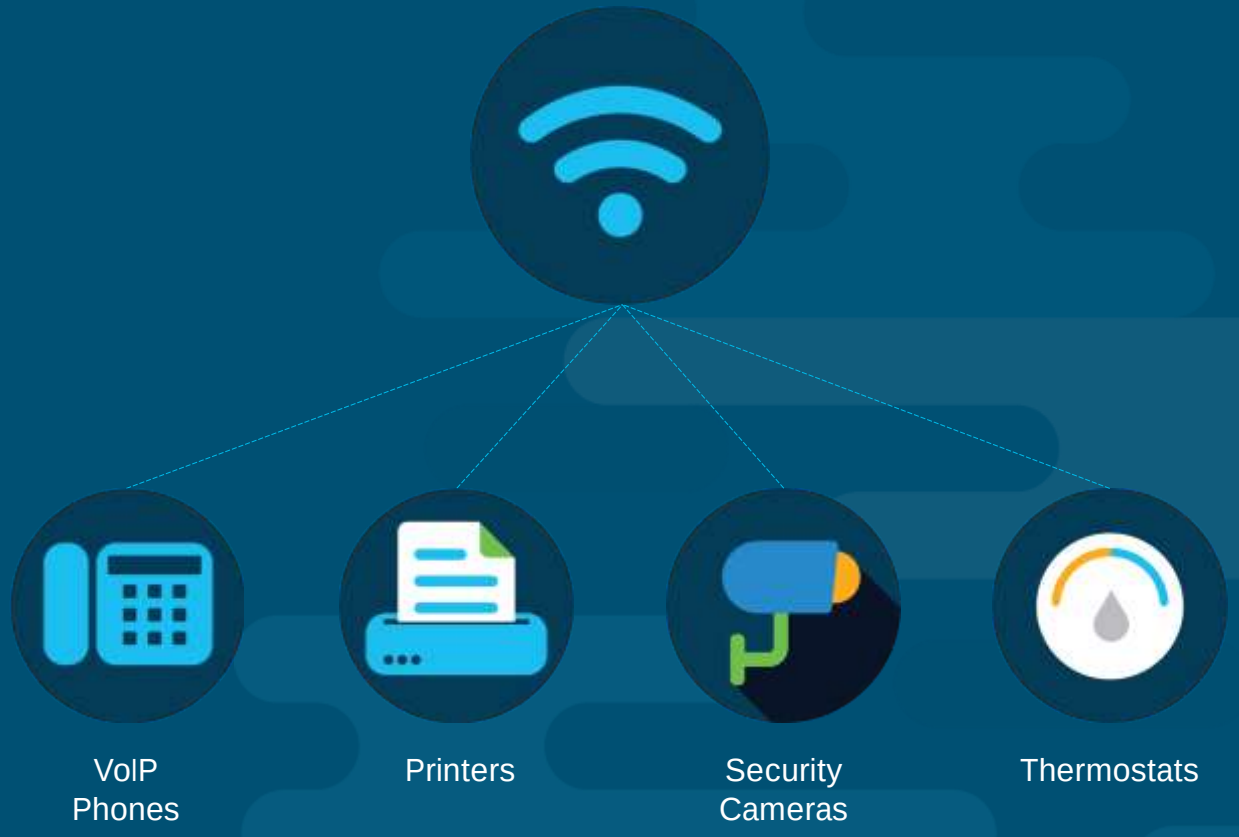
Share intelligence across network, web, email, and endpoints to see once, block everywhere.

Holistic view of endpoints

Regardless of operating system – from servers to desktop to mobile devices

Agentless detection with proxy analysis

Identify anomalous traffic occurring within your network



Discover Unknown Threats

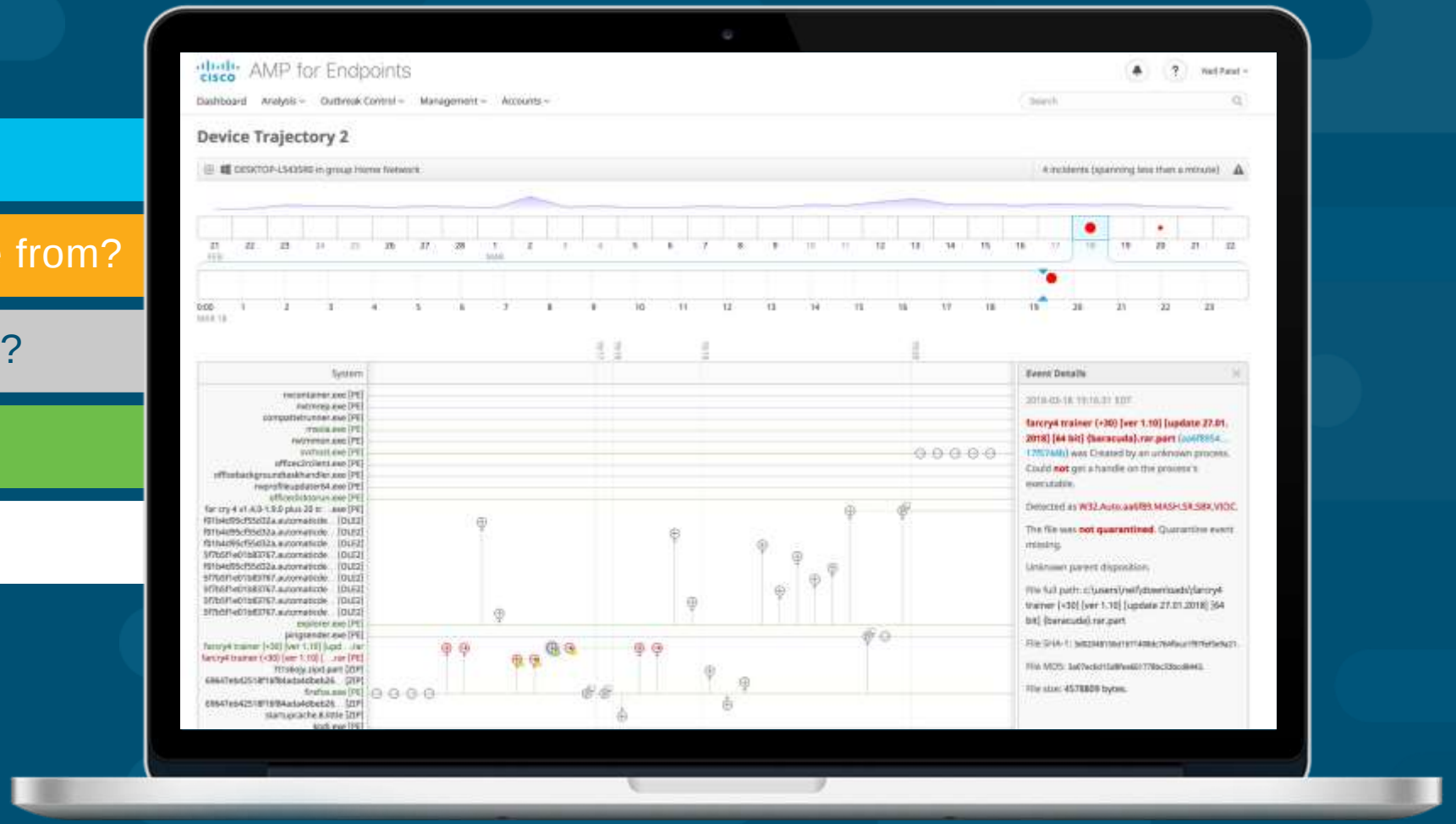
With proactive threat hunting

Dynamic analysis and sandboxing

Execute, analyze, and test malware behavior in order to discover previously unknown zero-day threats

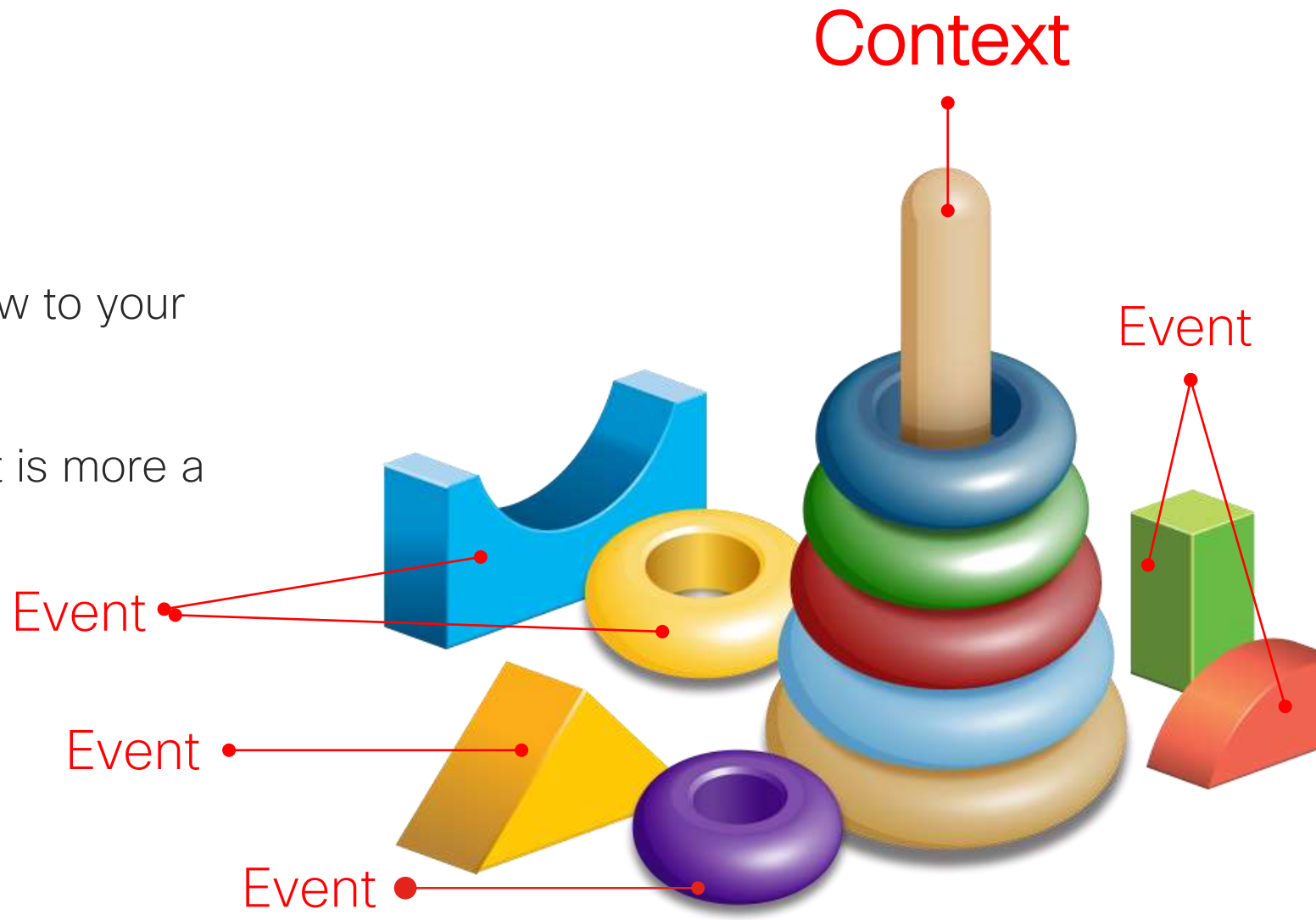
Continuous monitoring – Retrospective Security

- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is it doing?
- How do we stop it?



From Event to Context

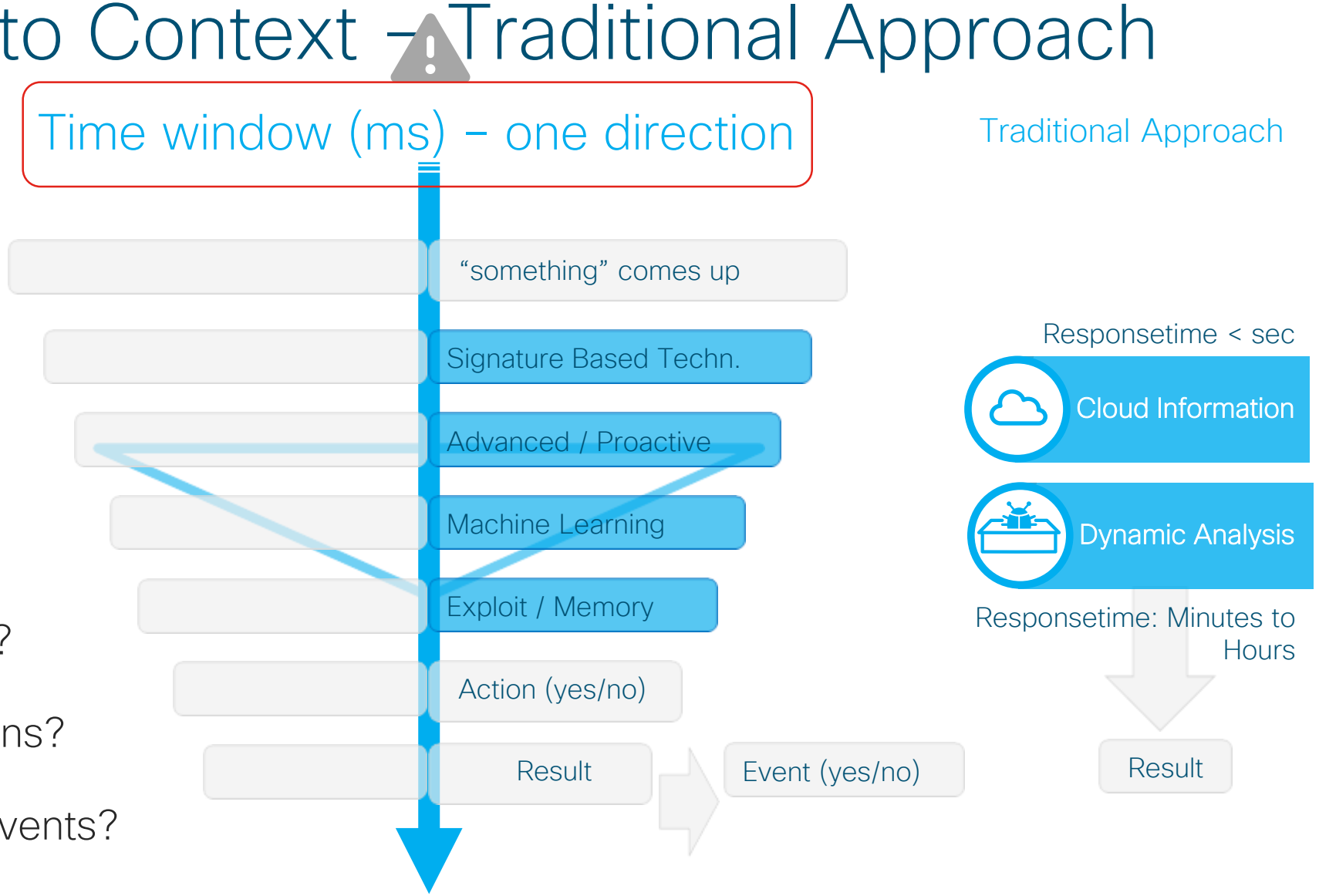
- Context simplifies complexity
- Provides a complete different view to your insight threatlandscape
- Context aware is not a product, it is more a capability and approach
- Context is Relationship between Events



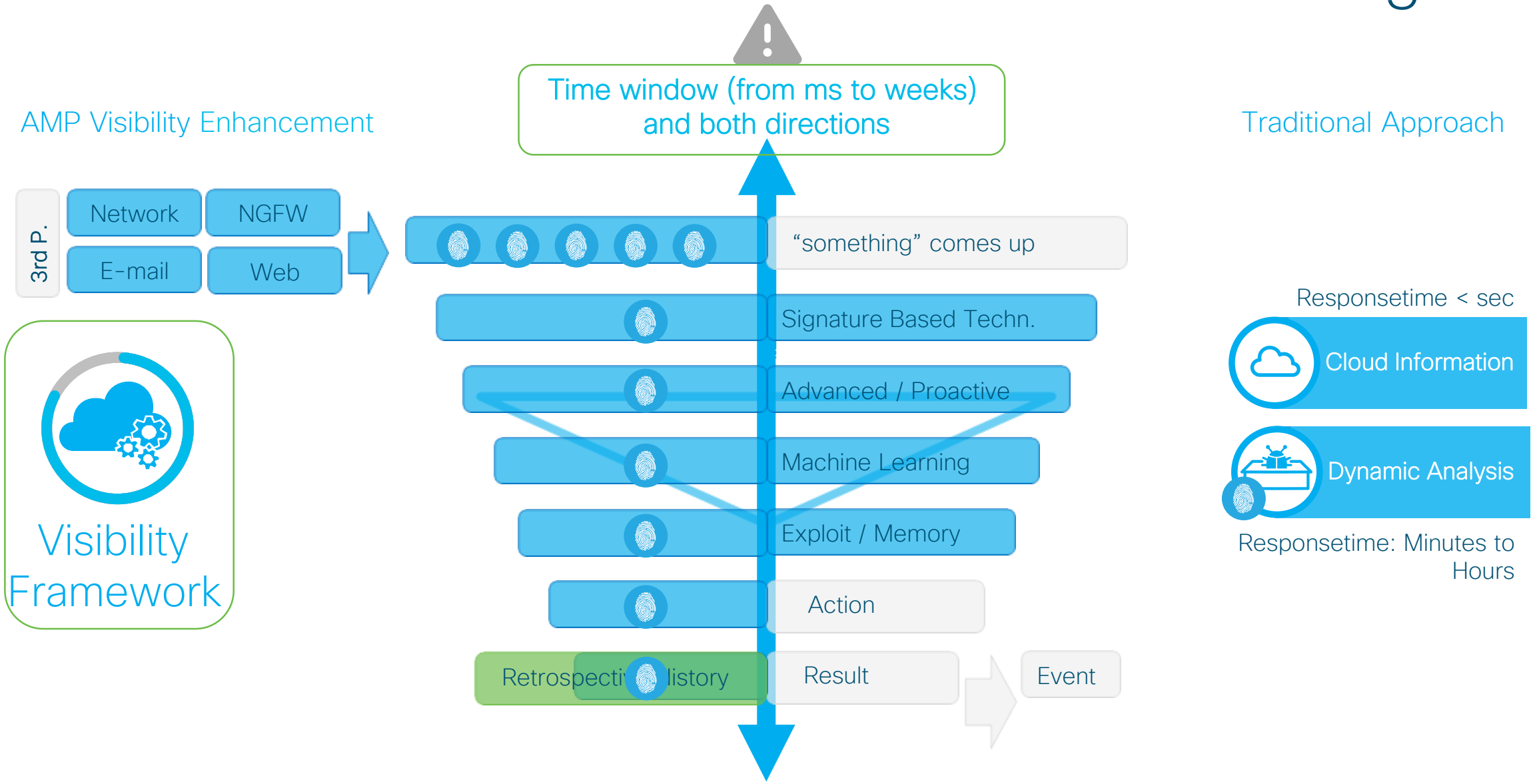
From Event to Context – Traditional Approach

Challenges

- All systems protected?
- Cloudservice available?
- When asking cloud?
- Dynamic Analysis – What / When
- Proper endpoint config?
- Monitoring normal actions?
- Monitoring non threat events?
- How Dynamic Analysis Results are handeled?

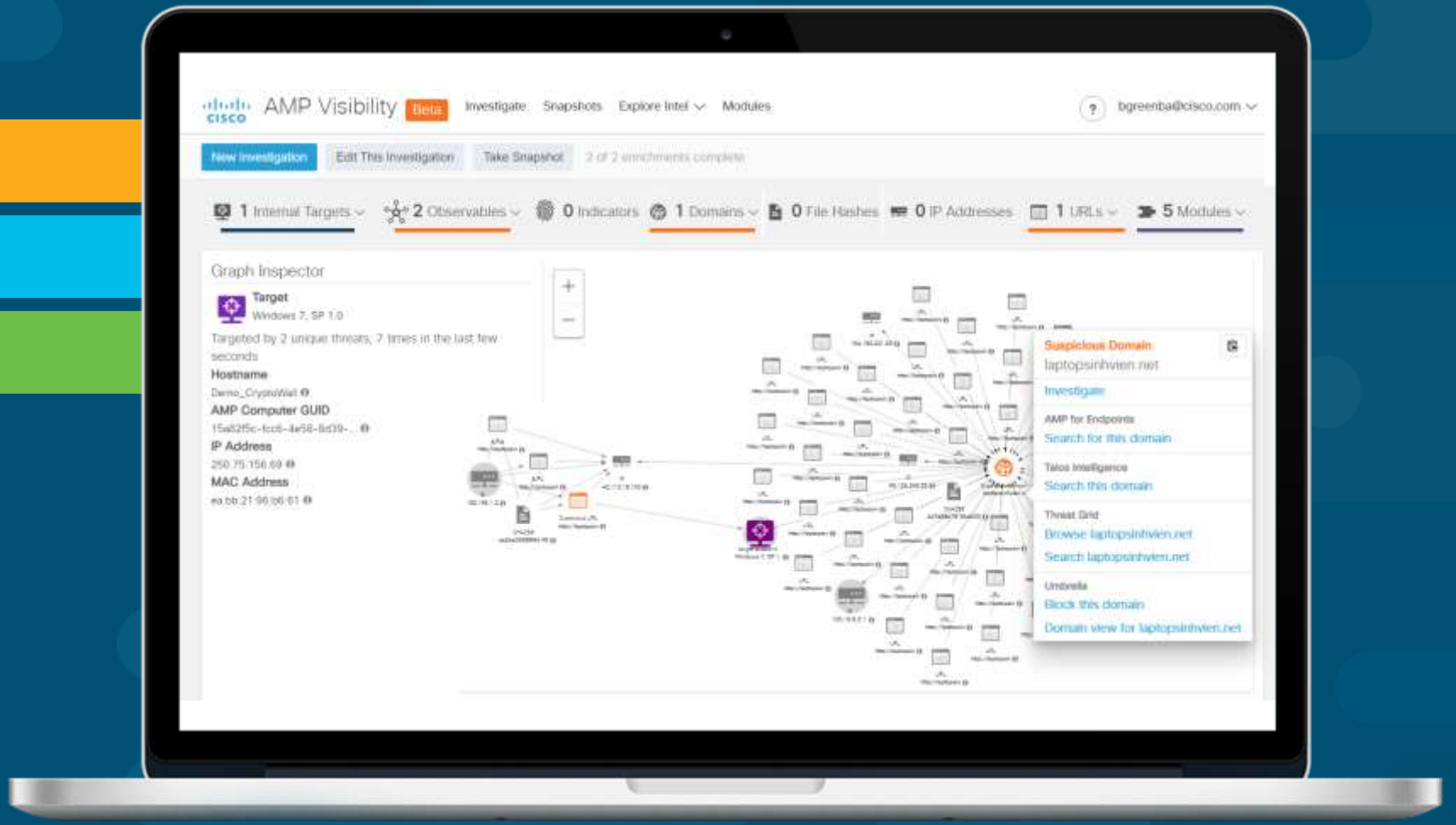


From Event to Context – Continous Monitoring



Perform in-depth investigations

- Threat hunting
- One click remediation
- Intelligence correlation



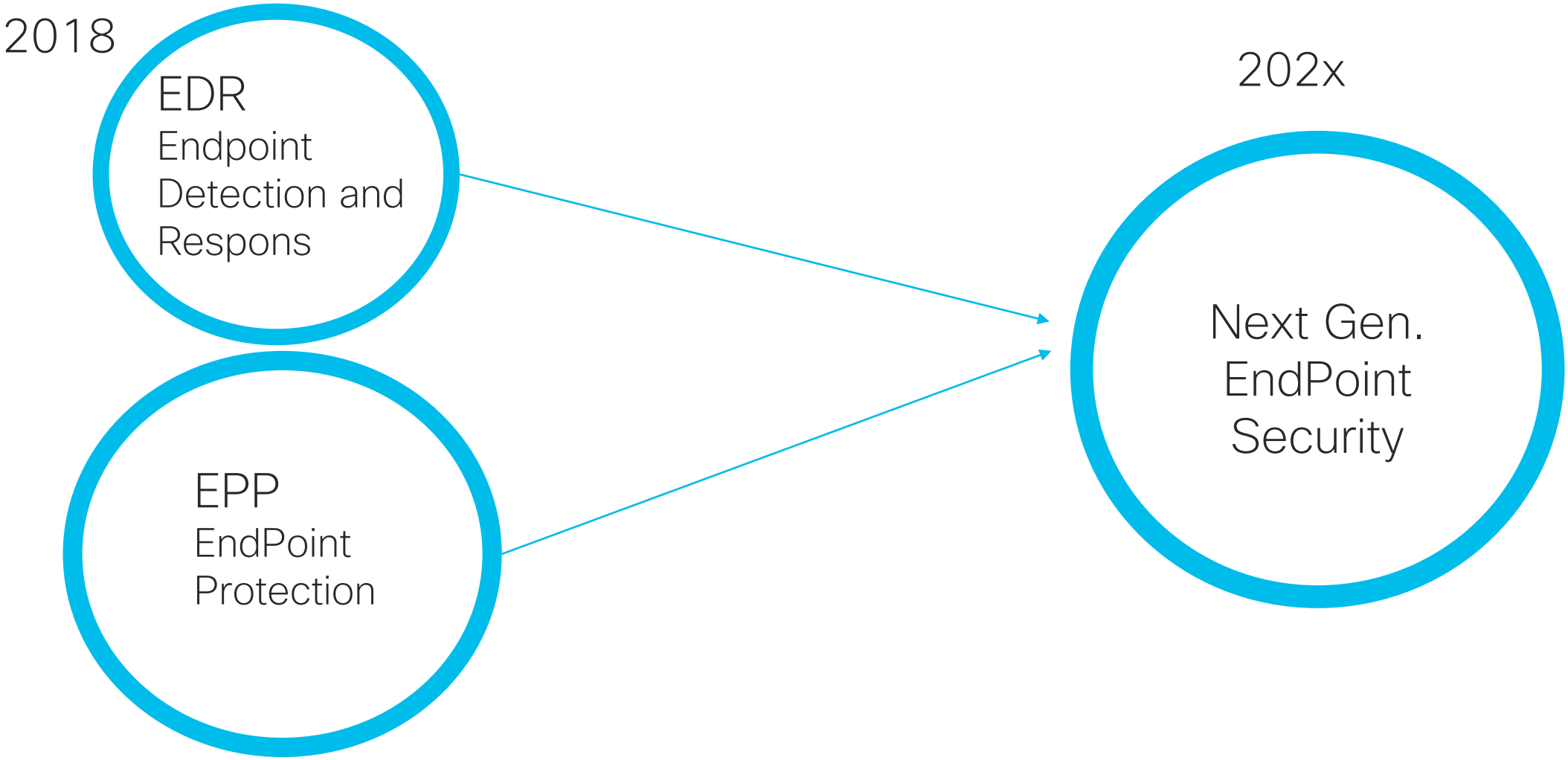
DEMO TIME

Case Study

“AMP нашел то, что другие продукты безопасности не заметили. При это показал отличную эффективность защиты при минимуме потребляемых ресурсов”

ПАО КБ Приватбанк

EPP/EDR Install Base

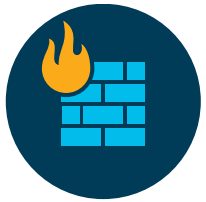


Cisco AMP Install Base

- 10+ millions AMP for Endpoints (32.000 Customers)

- 32+ millions Mailboxes secured with AMP

- 17+ millions Network Devices with AMP enabled



Overall 60+ millions of AMP agents

Current results

- Cisco named a ‘Visionary’ in 2018 Magic Quadrant for Endpoint Protection Platforms

- NSS Labs provides ‘Recommended’ rating in 2018 Advanced Endpoint Protection test
- NSS Labs finds AMP has fastest time to detection 3 years in a row, Breach Detection Test

- IDC names AMP for Endpoints a Leader in Endpoint Specialized Threat Analysis and Protection, 2017 vendor assessment