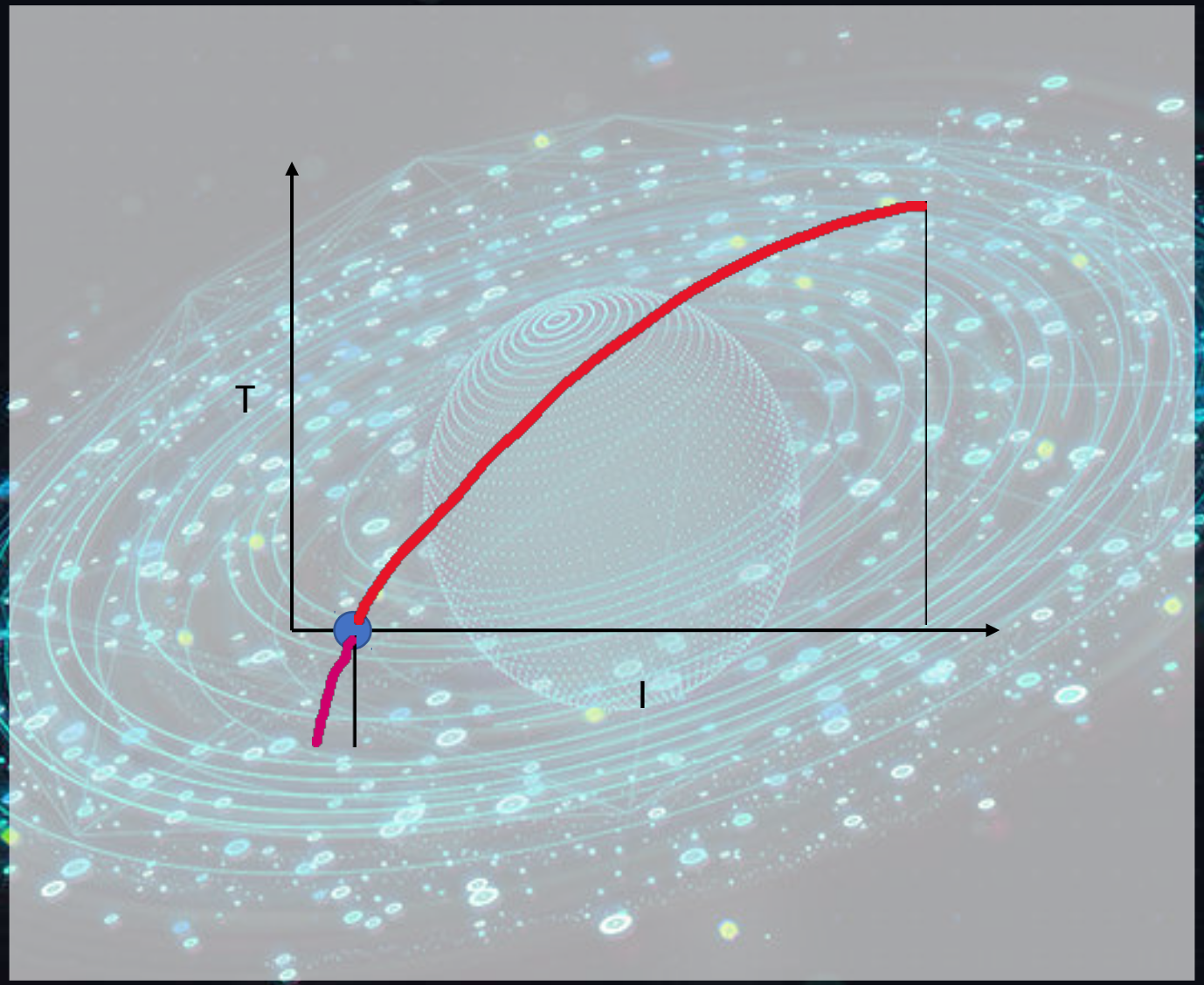
Microsoft

# Security Orchestration, Automation and Respons, czyli jak AI wspiera działy bezpieczeństwa.

Olga Budziszewska, CISM Cybersecurity Assurance Program Manager


T
I

| Crime | Annual Revenues* |
| --- | --- |
| Illicit, illegal online markets | $860 billion |
| Trade secret, IP theft | $500 billion |
| Data trading** | $160 billion |
| Crimeware, CaaS (Cybercrime-as-a-Service) | $1.6 billion |
| Ransomware*** | $1 billion |

*totals are approximate
**Revenues derived from trading in stolen data, such as: credit and debit card information banking log-in details, loyalty schemes and so on
***Revenues derived from extortions based on encrypting data and demanding payments

https://venturebeat.com/2018/04/21/the-web-of-profit-a-look-at-the-cybercrime-economy/

# 2018 Cyber Security Top 5 Predictions:
## Attacks, Regulations and Innovations


**01 Blockchain Maturity**
It's an encrypted leger where everyone on the leger has a private key whose code is randomly generated so that it changes with every message.

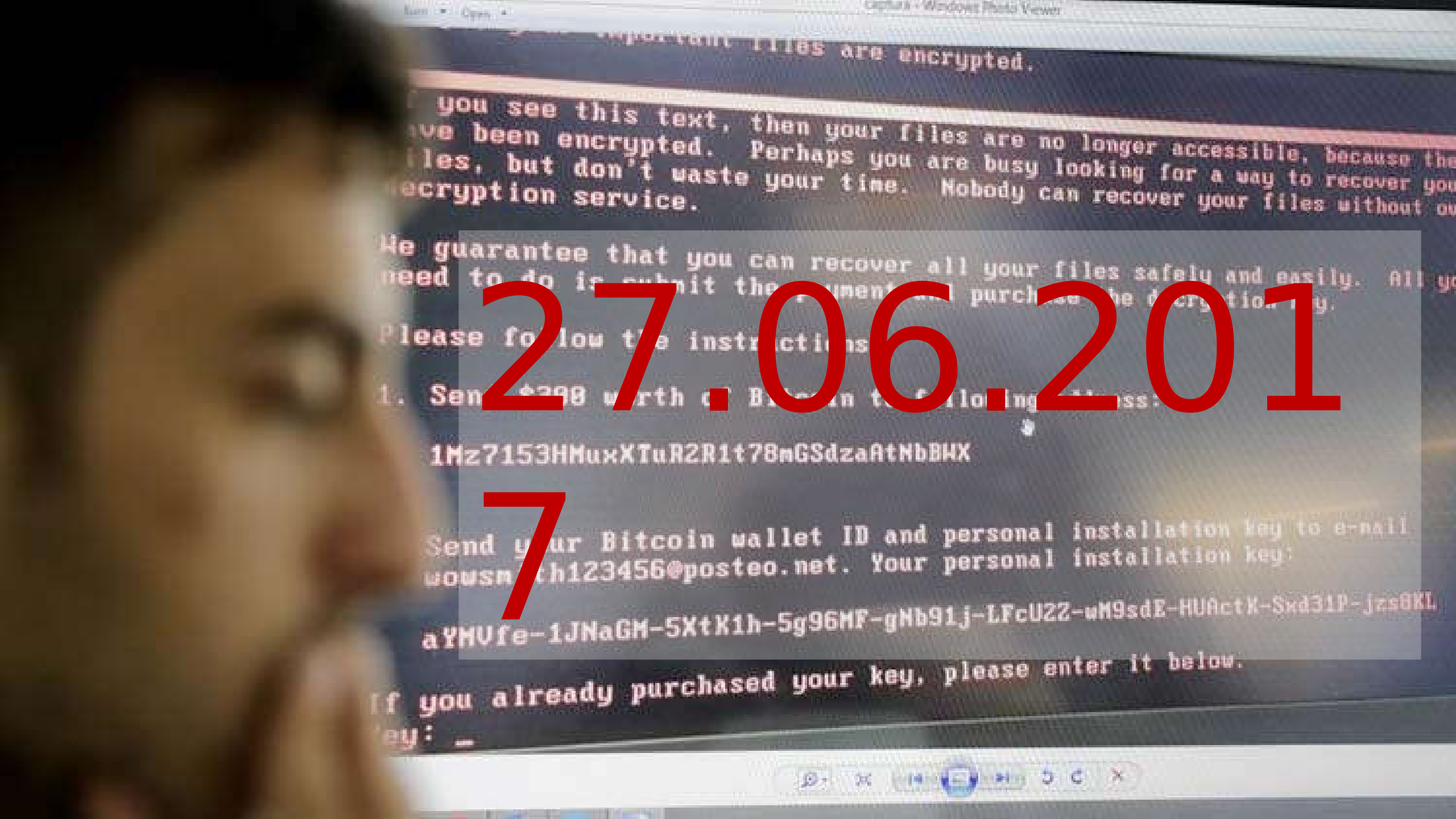
**02 IoT Attacks get more Aggressive**
Over the past few years, we've seen the potential of broad, massive damage the exploitation of IoT vulnerabilities can bring. 2018 will bring us more focused, aggressive and money-motivated attacks.

**03 The Scramble to GDPR Compliance**
GDPR stands for General Data Protection Regulation and will be mandating a set of data processing, handling and storing requirements that give EU resident consumers more control over the data companies collect from them.

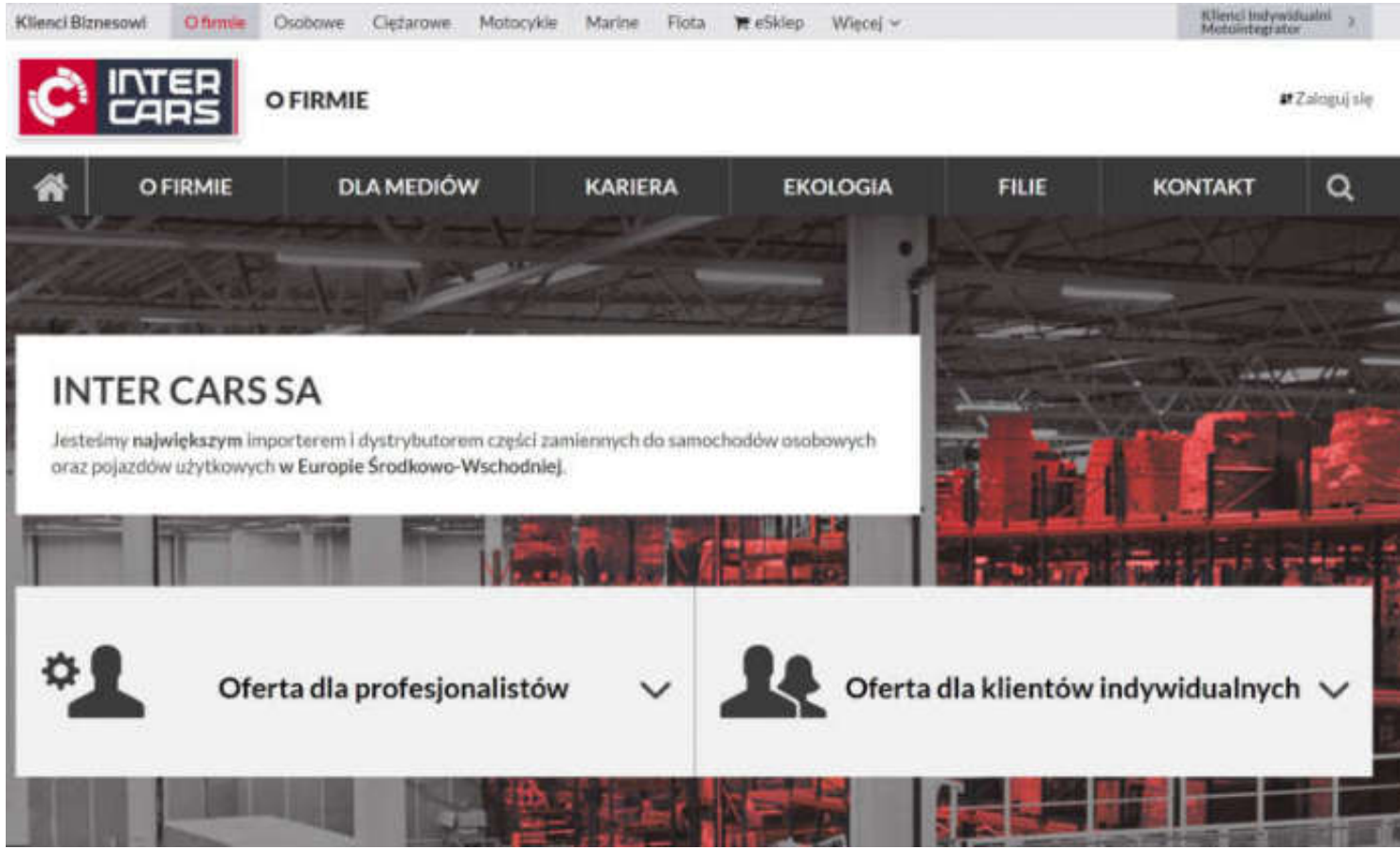
**04 Enterprise Hacks through Mobile Devices**
The possibilities for hacking mobile devices are endless and our smartphones' software is far from secure.

**05 More Adoption of Adaptive and Layered Security Approaches**
Automated systems can use machine learning determine which events are malicious attacks and artificial intelligence to carry out the functions necessary for mitigating said attacks.

http://blog.cybertraining365.com/2018/01/15/2018-cyber-security-top-5-predictions-attacks-regulations-innovation/2018-cyber-security-top-5-predictions-attacks-regulations-and-innovations-01/


files are encrypted.
you see this text, then your files are no longer accessible, because the
ve been encrypted. Perhaps you are busy looking for a way to recover you
les, but don't waste your time. Nobody can recover your files without ou
ecryption service.
We guarantee that you can recover all your files safely and easily. All yo
need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HHuxXTuR2R1t78mGSdzaAtNbBWX
Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:
aYHVfe-1JNaGM-5XtX1h-5g96MF-gNb91j-LFcU2Z-wM9sdE-HUActK-Sxd31P-jzs0KI
If you already purchased your key, please enter it below.
Key: _
27.06.2017

Inter Cars SA to największy dystrybutor części zamiennych do samochodów osobowych, dostawczych i ciężarowych w Europie Środkowo – Wschodniej. Oferta spółki obejmuje również wyposażenie warsztatowe, w szczególności urządzenia do obsługi i naprawy samochodów oraz części do motocykli i tuningu. Inter Cars oferuje najszerszy asortyment części



- 90% systemów firmy nie jest dostępnych,
- 800 serwerów wymaga przeinstalowania,
- Klienci i partnerzy nie są w stanie składać zamówień ani przeprowadzić żadnej transakcji,
- W ciągu 4 dni firma musi wygenerować sprawozdanie giełdowe

# Dalczego Petya jest tak zaskoczyła?

## INNOWACYJNY ATAK

**ŁAŃCUCH DOSTAW**
nietradycyjny wektor ataku – przez aplikacje biznesowe (nie phishing czy przeglądarkę)

**RÓŻNE TECHNIKI**
Automatyzacja różnych technik ataku

**PRĘDKOŚĆ**
Automatyzacja przeprowadzenia ataku nie pozostawiała zespołom bezpieczeństwa czasu na reakcję

## POTĘŻNE KONSEKWENCJE

**POZIOM ZNISZCZEŃ**

w porównaniu z tradycyjnymi atakami skala rażenia okazała się większa niż kiedykolwiek wcześniej. Dodatkowo proces odzyskania danych był bardzo utrudniony, ponieważ zostały zaatakowane pliki MFT.

*Po ataku w firmie nastąpiło wiele zmian i z pewnością będzie ich jeszcze więcej. Instalujemy ponownie uszkodzone systemy, kierujemy się restrykcyjnymi zasadami bezpieczeństwa.* ***Całkowicie zmieniliśmy podejście do kwestii ich administrowania****. Powołaliśmy wewnętrzną komórkę bezpieczeństwa informatycznego.* ***Wiemy, że nie jesteśmy w stanie zabezpieczyć się w stu procentach****.*

Maciej Oleksowicz
PREZES ZARZĄDU INTER CARS SA

# Petya – techniczne i biznesowe skutki ataku

## Example of Technical Impact (Anonymous)

| | |
|---|---|
| **GEOGRAPHIES** | All |
| **DURATION** | ~60 minutes |
| **IMPACTED COMPUTERS** | 62,000 computers<br>12,000 servers<br>50,000 workstations |

## Publicly Reported Losses (By Different Organizations)

**$200** Million

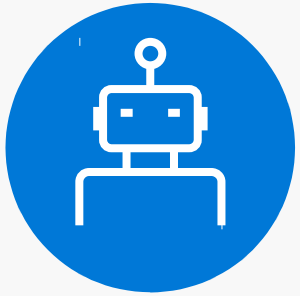
**$300** Million

**$310** Million

# odróżnia „szybkie cyberataki” od tradycyjnych meto

## SZYBKOŚĆ

Rozprzestrzeniają się w organizacji w kilka sekund/minut nie pozostawiając czasu na reakcję



## AUTOMATYZACJA

Gdy cykl ataku się rozpocznie, nie potrzeba dalszego zaangażowania

## ZNISZCZENIA

Celowe zakłócenie działania poprzez niszczenie / szyfrowanie danych / systemów

Nie pokonamy zagrożeń teraźniejszości bronią z przeszłości

Photo credit: Wikimedia Cannon from Galera Forte


Anomaly detection
Endpoint protection
Infrastructure security
Hybrid cloud security
Data & application security
Fraud prevention
Security management
Data loss prevention
Threat management
Rynek cyberbezpieczeństwa jest rozdrobniony i wymaga integracji
Data center security
Cloud Access Security Broker
Information rights management
Identity & access management
Compliance tools
Threat detection
IoT security
Email security

# CYBERscape: The Cybersecurity Landscape

# Model dojrzałości cyberbezpieczeństwa organizacji

| PIERWOTNY | ROZWOJOWY | ZDEFINIOWANY | ZARZĄDZANY | ZOPTYMALIZOWANY |
|---|---|---|---|---|
| Gaszenie pożarów<br>- nie ma żadnego formalnego systemu, działanie ad-hac | Wdrożone rozwiązania punktowe<br>Istnieje już baza doświadczeń jednak nie jest udokumentowana | Wdrożony system bezpieczeństwa (ISO, NIST...)<br>Procesy są udokumentowane, jednak wszystko odbywa się manualnie | Aktywne wsparcie kierownictwa<br>Wdrożone plany reagowania na incydenty i DR<br>Zakres całej organizacji | Wdrożone procesy doskonalące<br>Podejście proaktywne<br>Automatyzacja wykrywania i reakcji na incydenty |


https://www.gartner.com/doc/reprints?id=1-4O4VC17&ct=180109&st=sb


## Automatyzacja bezpieczeństwa

wykorzystanie technologii do automatycznego reagowania i zarzadzania incydentami bezpieczeństwa

## Orkiestracja bezpieczeństwa

integracja narzędzi i rozwiązań mająca na celu usprawnienie procesów i automatyzacji

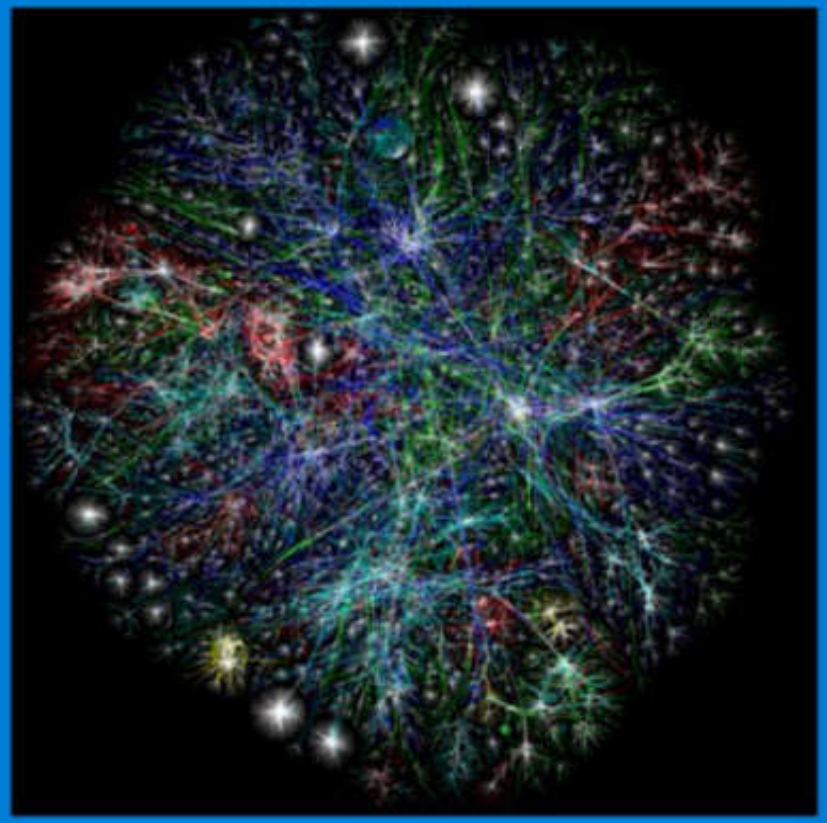
# Brak specjalistów na rynku

- szacuje się, że do 2021 r na świecie będzie brakowało ok 3,5 miliona specjalistów w zakresie cyberbezpieczeństwa

https://cybersecurityventures.com/jobs/

# Skala, szybkość i złożoność cyberataków

## Complexity



## Velocity

23% of recipients **opened phishing messages**

50% of those who open and click attachments do so **within the first hour**

**24 hours** from click to domain compromise

## Volume

**6,449 new** vulnerabilities in 2016

**16%** of new vulnerabilities rated as **critical**

**100Ks** of detections **per day**

*Sources include https://nvd.nist.gov, Verizon Data Breach Report & Microsoft Incident Response Data*

# Security Orchestration, Automation, Response

## CZAS

Szybsza reakcja na incydent bezpieczeństwa to podstawa skutecznej ochrony. Im dłużej problem nie zostanie rozwiązany, tym gorsze są jego konsekwencje

## EFEKTYWNOŚĆ

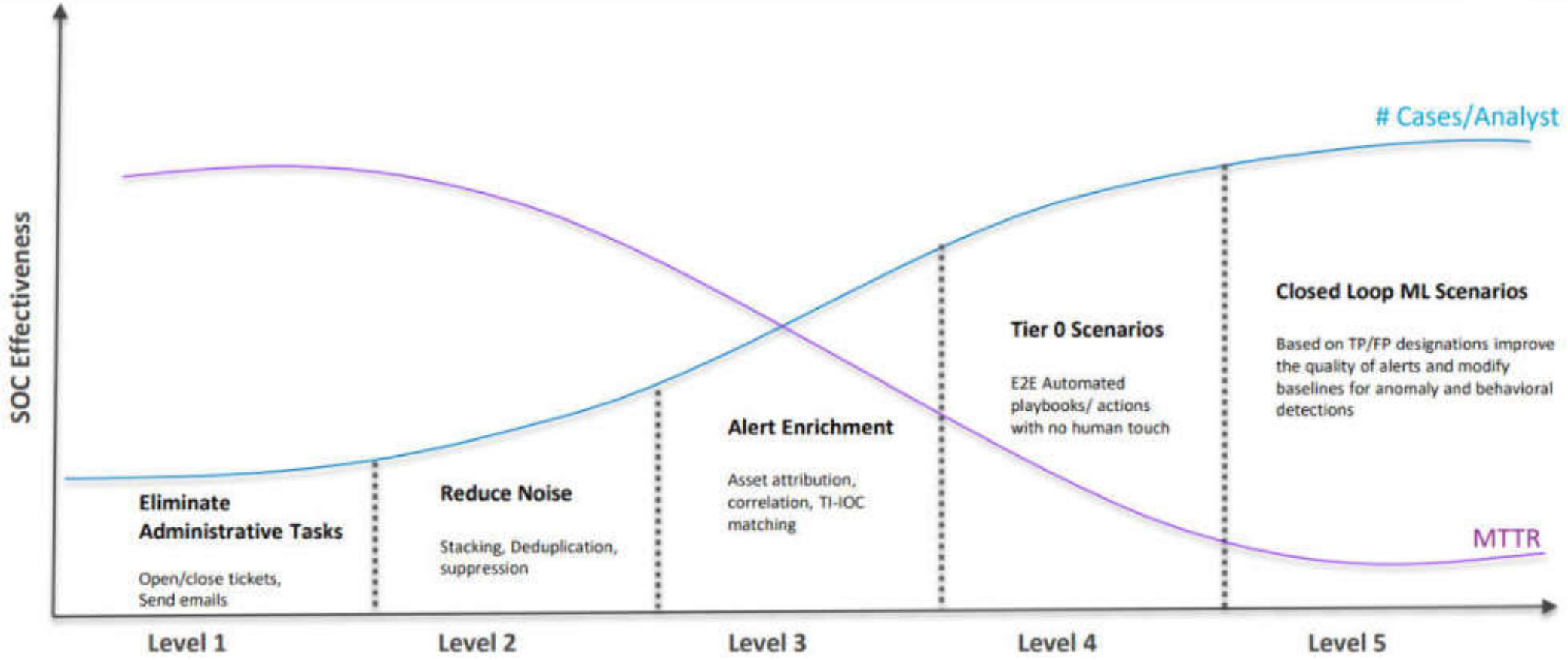
Niedobór kadr to krytyczny problem dla bezpieczeństwa. Dzięki SOAR analitycy bezpieczeństwa poświęcają mniej czasu na konkretny incydent

## INTEGRACJA

Automatyzacja i orkiestracja pozwalają integrować różne narzędzia – dzięki temu mogą one współpracować w rozwiązywaniu problemów.


PROTECT
DETECT
RESPOND

# Model dojrzałości SOC




*The automation maturity model and automation journey, Copyright Microsoft Corporation*


IDG CONTRIBUTOR NETWORK Want to Join?

**WINDOWS INTO THE FUTURE**

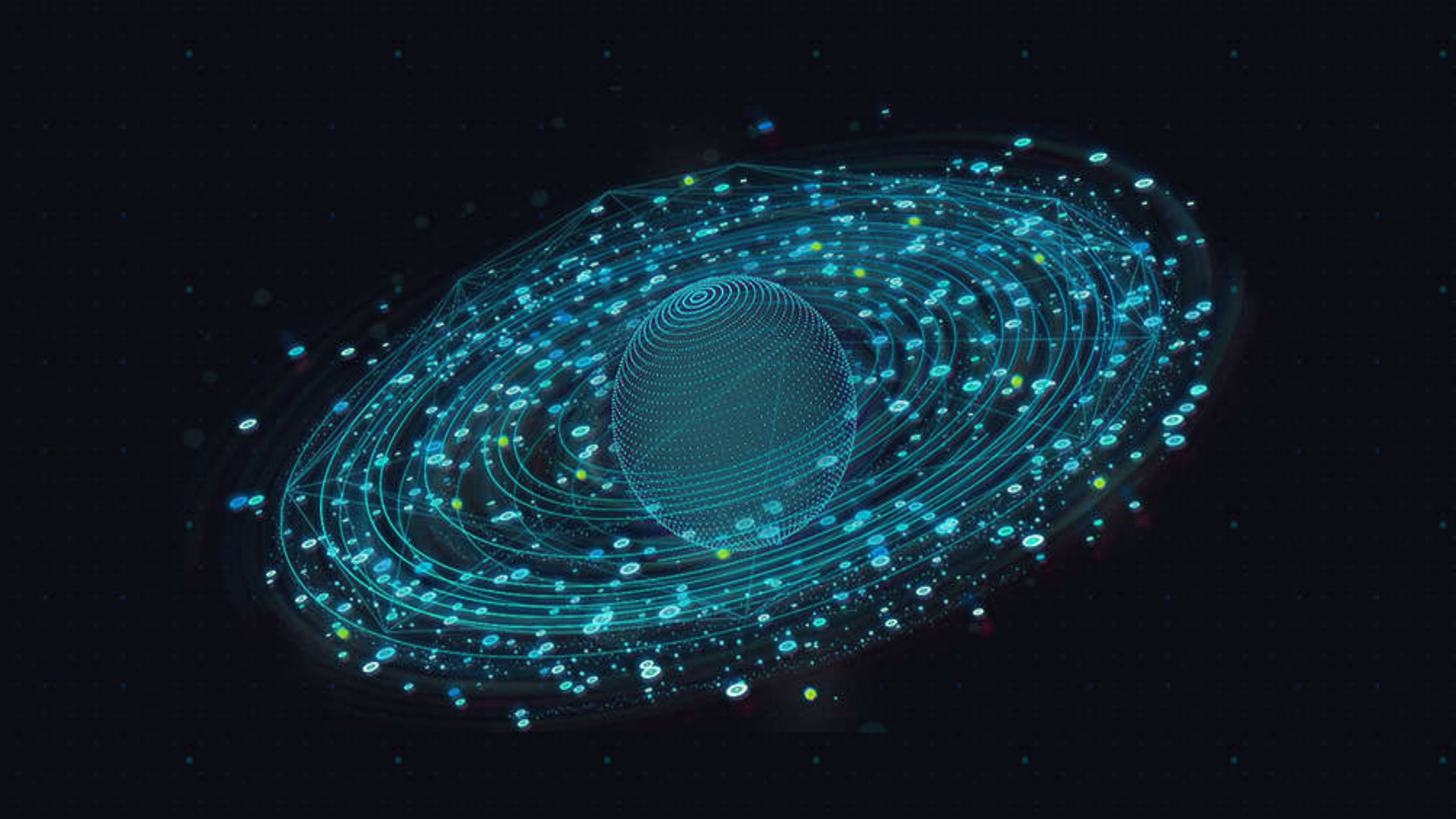
By Rob Enderle, Contributor, Computerworld | SEP 21, 2017 5:00 AM PT

Opinions expressed by ICN authors are their own.

OPINION

# Microsoft Security stopped being an oxymoron with the acquisition of Hexadite

How Microsoft shifted from thinking security was someone else's job to making it a strategic part of their Windows platform.



Microsoft


Olga Budziszewska
Cybersecurity Assurance
Program Manager at Microsoft
v-olbudz@Microsoft.com