Leveraging Machine Learning & Al in Cyber Defense

Effective Security Strategy: between open space and the bunker

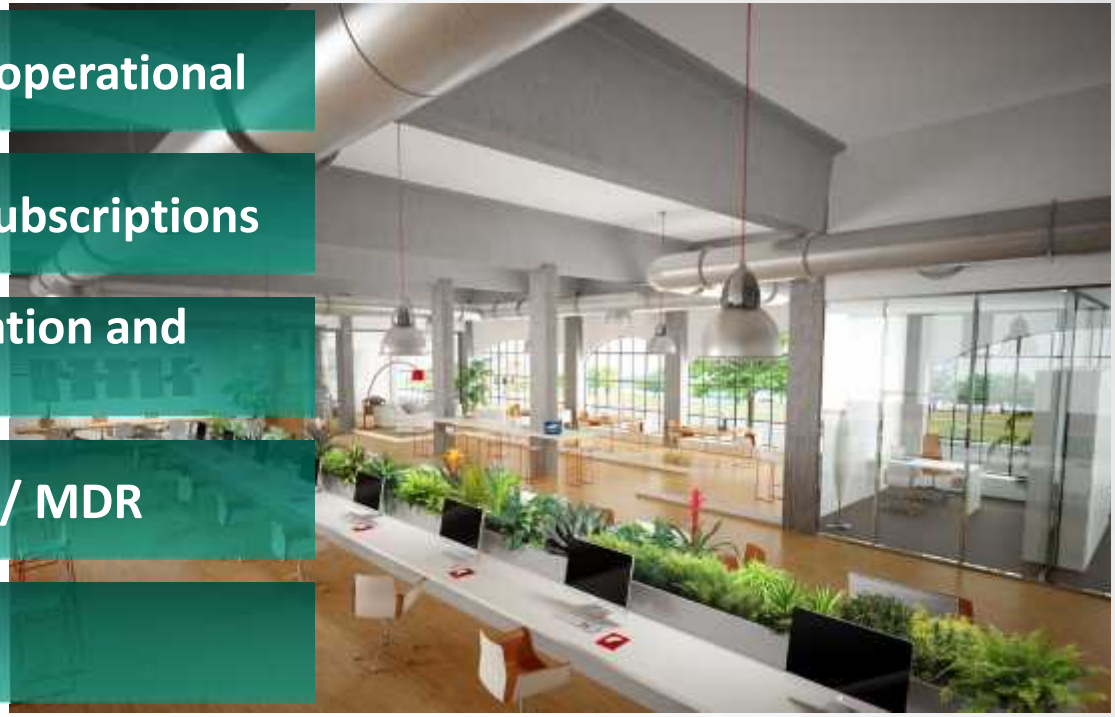
Veniamin Levtsov
Vice President Corporate Business
Kaspersky Lab

MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

Cyber security becomes more open

- CISO role: rather strategic than operational
- Passion to OPEX: services and subscriptions
- Risk management: from elimination and mitigation to transfer
- Manager services: MSP / MSSP / MDR
- Cyber Insurance



MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

Cyber insurance as easy way to cover incident response cost

Kaspersky Lab to Provide Insurance Policy Holders of Allianz Global Corporate & Specialty SE with IT Forensics in Cyber Incidents

Next-Gen incident response in the event of security incidents for AGCS customers in Germany, Austria and Switzerland

Kaspersky Lab will provide IT forensics and incident response services to Allianz Global Corporate & Specialty SE (AGCS) cyber insurance customers in Germany, Austria and Switzerland. In a cyber crisis, businesses can now benefit from Kaspersky Lab's expertise, helping them to limit the damage of security incidents through fast access to Next-Gen services and the ability to initiate a highly professional investigation into the incident. As one of the selected IT forensics partners of AGCS, Kaspersky Lab´s services will be available in Germany, Austria and Switzerland.

Trusted service providers' pool attested and approved by Insurance company

MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

Balkanization

Balkanization, by Wiki, is a geopolitical term used to describe the process of **fragmentation or division** of a region or state into smaller regions or states that are often **hostile or uncooperative with one another**.

Research Reports on the states-sponsored actors' activity

APT1

- According to Mandiant* the group may be government-sponsored and its origins lie in China
- There have been 141 victim organizations spanning 20 major industries
- Targets reflect industries that China identifies as strategic to economic growth

Sofacy ** (Fancy Bear ***)

- Probably affiliated with Russian military intelligence, according to CrowdStrike's assessments
- X-Agent spyware implanted in Android app used by Ukrainian artillery forces to target howitzers
- X-Agent was able to obtain location details of artillery forces
- According to open source data, Ukrainian forces lost over 80% of their howitzers in 2 years

Equation ****

- 500+ victims worldwide according to Kaspersky Lab research
- Access to zero-day exploits in advance of other groups
- When a computer boots, the malware hijacks OS loading by injecting its code into boot record
- This enables the malware to control the Windows launch

* http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-083.pdf
* * https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset
* * * https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf
* * * * https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

KASPERSKY lab

Suspicious activity of mobile firmware

Mobile phone firmware supposedly transmits personal information (Nov 15th, 2016)*

- Kryptowire** has identified several models of Android mobile devices that contained firmware that collected and transmitted sensitive personal data to third-party servers without disclosure or the users' consent
- Information included full-body of messages, contact lists, call history, unique device IDs
- It also transmitted information about the apps installed, bypassing the Android permission model
- It was able to execute remote commands and remotely reprogram the devices
- The information was encrypted and then transmitted over secure web protocols to a server located in Shanghai

*https://www.prnewswire.com/news-releases/kryptowire-discovered-mobile-phone-firmware-that-transmitted-personally-identifiable-information-pii-without-user-consent-or-disclosure-300362844.html

** Kryptowire was founded in 2011 by the Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security (DHS). For more information, visit www.kryptowire.com

Mishandling of top-secret NSA documents

- A former employee of the U.S. National Security Agency's elite hacking team (Tailored Access Operations) has pleaded guilty in connection with mishandling top-secret documents
- Nghia Pho worked for the division, which designs efforts to compromise computer systems to gather information about terrorism, national security threats and foreign government intentions
- From 2010 through 2015, Pro **brought home** both hard copies and digital versions of sensitive documents containing closely held secrets

*https://www.politico.com/story/2018/09/20/national-security-agency-hacking-833587, By JOSH GERSTEIN | 09/20/2018
*https://www.washingtontimes.com/news/2017/dec/2/nghia-hoang-pho-former-nsa-employee-pleads-guilty/

Once the government loses positive control over classified material, the government must often treat the material as compromised and take remedial actions as dictated by the particular circumstances.

Adm. Michael S. Rogers, head of the National Security Agency and commander of the U.S. Cyber Command

MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

Balkanization of Internet and Cybersecurity

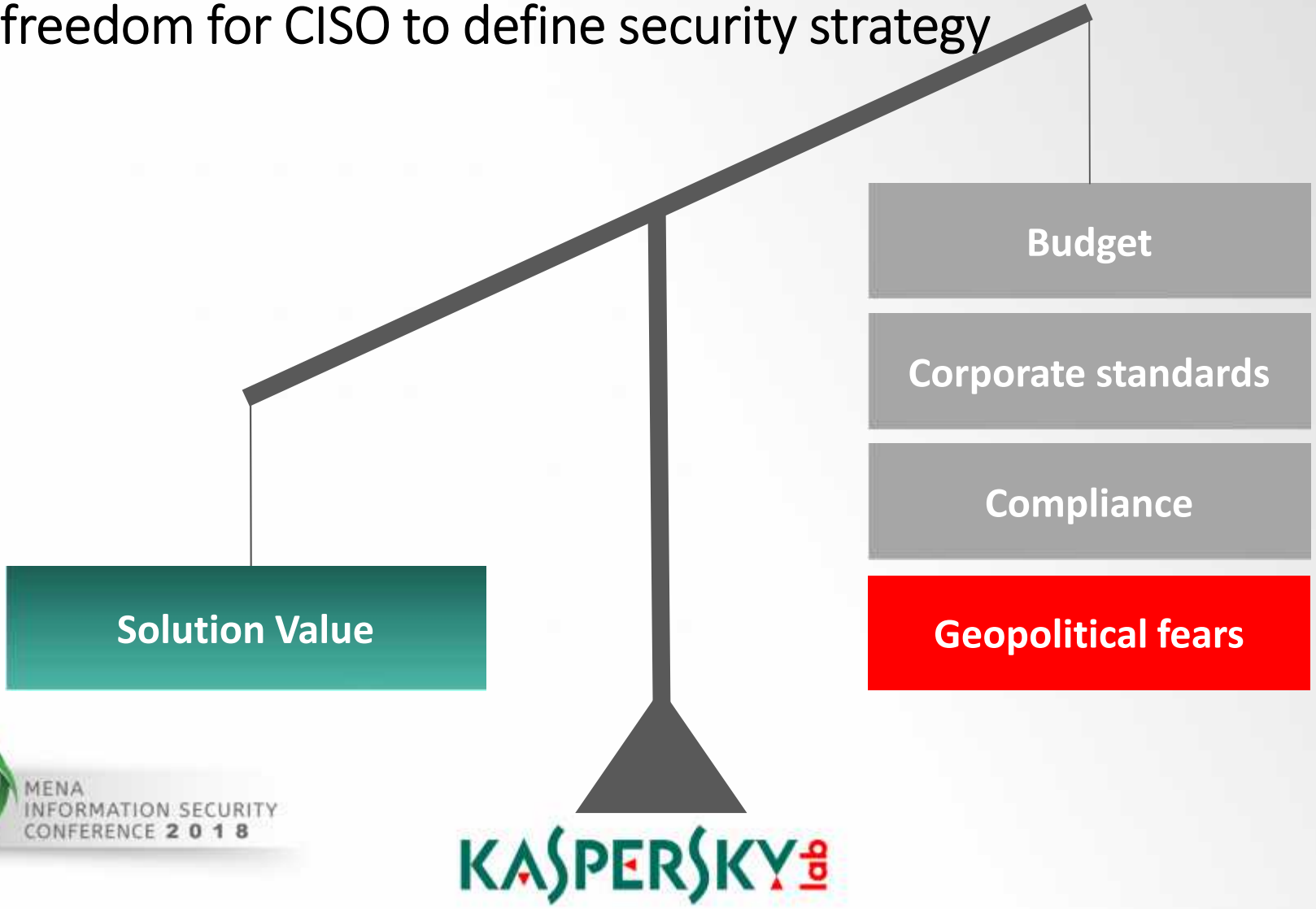
"Balkanization" of the Internet, "splinternet", fragmentation of the Internet - the national segments of Internet become **walled off** from the rest of the Web

- NSA surveillance program
- The Golden Shield of China
- Blocking LinkedIn and Telegram in Russia
- Ban on Huawei and ZTE in the US
- Limitations for Public Clouds

It results in

- rising influence of national cyber authorities
- domestic security technologies growing
- restriction of using of some security products

Less freedom for CISO to define security strategy



MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

What causes concerns in cyber security tools

- Non-declared features and built-in ZERO days in products
- Restriction on some products to use
- Involving of external experts in incident response
- Communications of products with the vendor’s cloud

MENA INFORMATION SECURITY CONFERENCE 2018

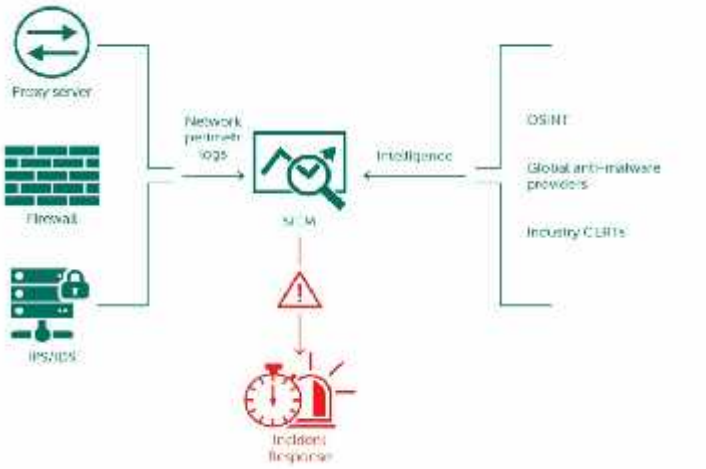
KASPERSKY lab

How informational services can benefit

Restriction or ban of products using in IT infrastructure

- APT research reports
- Actionable Threat Intelligence:
  - Threat Data Feeds
  - IoCs
- Cloud Threat Look-up system
- In-lab tools (sandbox)
- Malware hunting prof trainings

Hash Lookup	URLs/Domain Lookup	IP Lookup	Sandbox	Threat Name Lookup
MD5, SHA1, SHA256	URL Name	IP Address	Virtual machine, used for Sandboxing	Threat Name
Popularity	Host Name	Threat Score	Loaded / run DLLs	Threat Name Description
Threat Name	Web site category	Category	Registry Keys created	Distribution - GEO (graph)
Timestamps (first&last seen)	Popularity	Popularity	Registry Values modified	Timestamps (first&last seen)
File Size	Files Count	MD5 related	External connections	Known MD5s, SHA1, SHA256
File Format	Resolved IPs	Detected URLs	HTTP requests (URI + Data)	Related Host Names
Packer	MD5 related	Geo Map	DNS Queries	Related IP address
Signer	Referred to URLs	ASN	Drop Zones	Affected users GEO (graph)



MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

Trust but verify

Non-declared features and built-in ZERO days in products

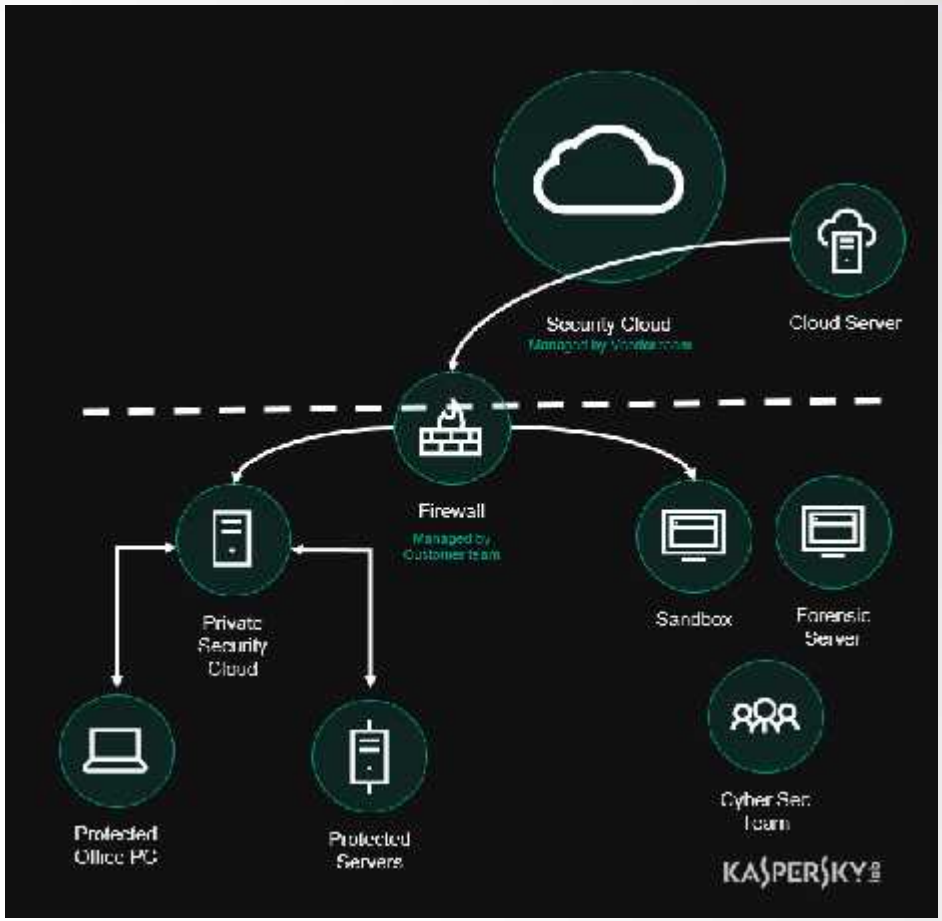
- **Source code revision by national cyber authorities and private Labs**
- **Using of layered security system in addition to OS built-in tools**
- **Virtual patching**

On-premise solutions for critical systems

Communications of products with the vendor's cloud

Use on premise solutions for

- **Vendor's reputation base: hash, IP/URL, behavioral patterns**
- **Sandboxing**
- **Security events data depositary (EDR)**
- **Forensic data-in-rest**



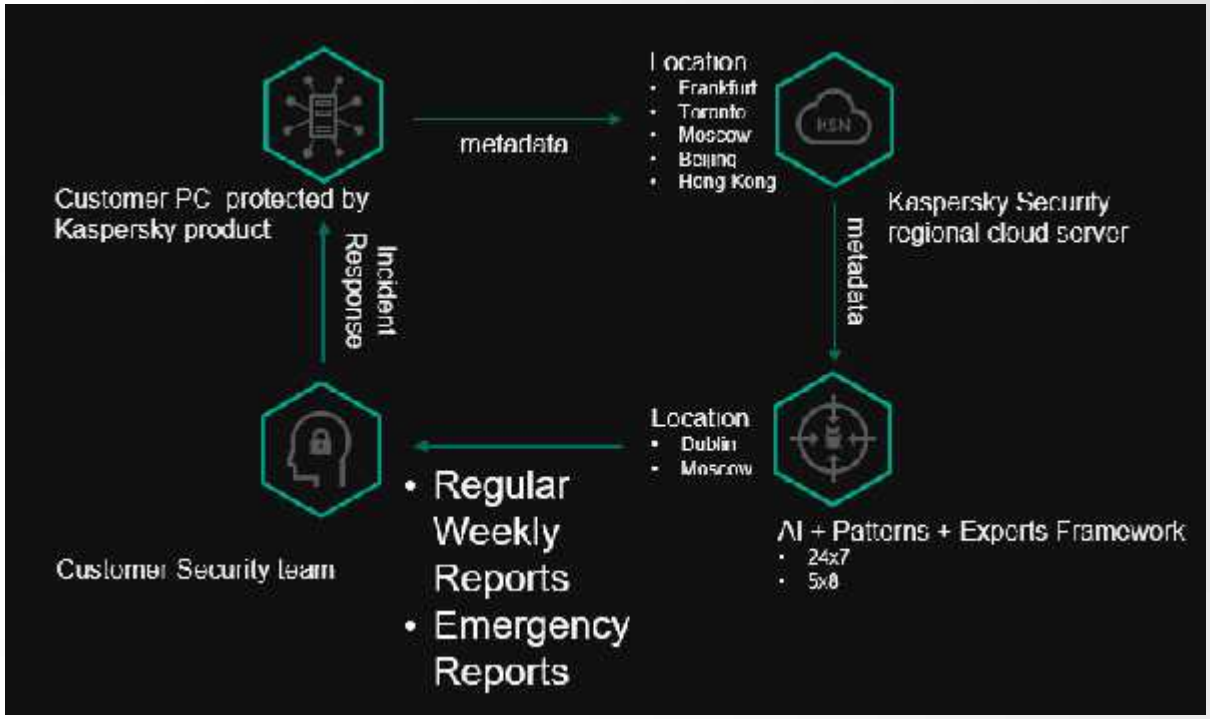
MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

Acquiring knowledge and frameworks

Involving of external experts in incident response and using vendor's infrastructure

Run your own Threat Hunting Center and Threat Lab based on framework provided by the vendor



MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab

«The only fence against the world is a thorough knowledge of it»

John Locke, English philosopher

- 1632-1704

Veniamin Levtsov
Veniamin.Levtsov@Kaspersky.com
Skype: V.Levtsov
https://www.linkedin.com/in/veniaminlevtsov/

MENA INFORMATION SECURITY CONFERENCE 2018

KASPERSKY lab