KASPERSKY LAB METHODOLOGIES AND FRAMEWORKS FOR ENTERPRISE SECURITY

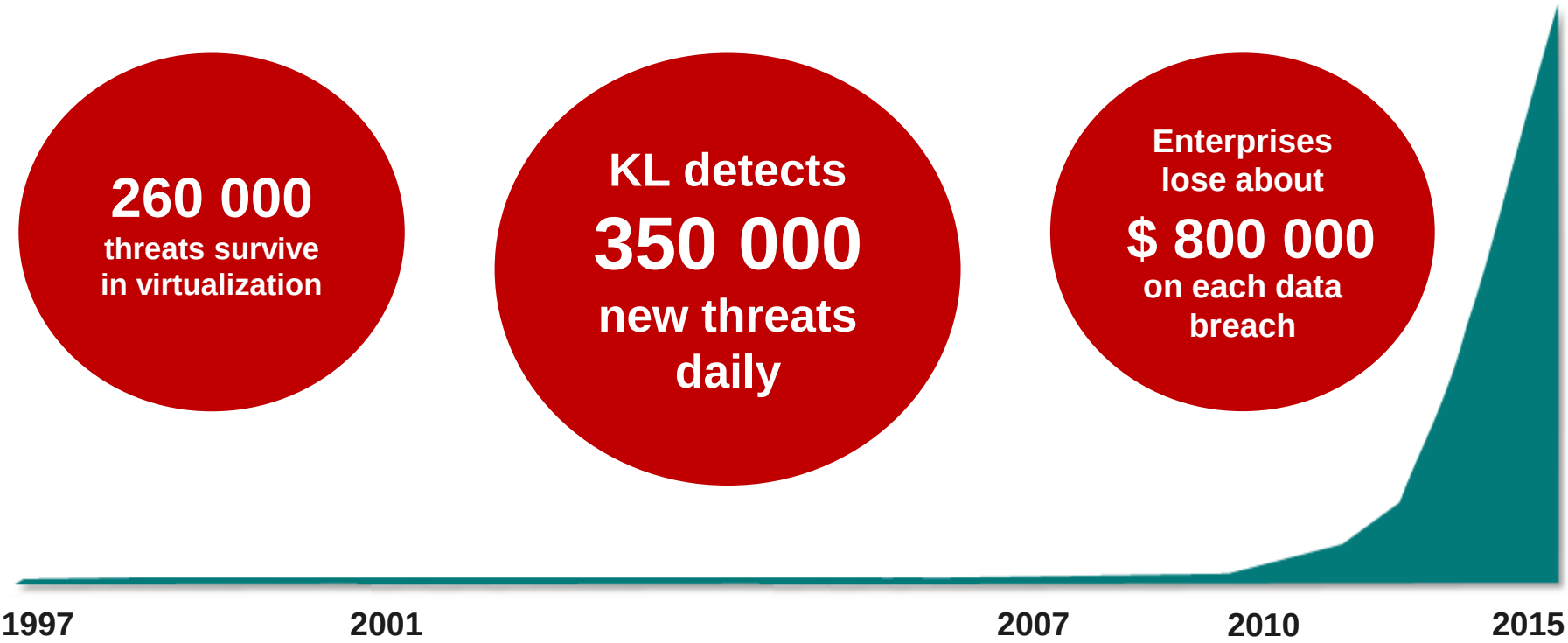
Ashraf Abdelazim
Director, Enterprise Business – Emerging Markets
Enterprise Security Division

Mikhail Nagorny
Head of Security Services
Enterprise Security Division

AGENDA

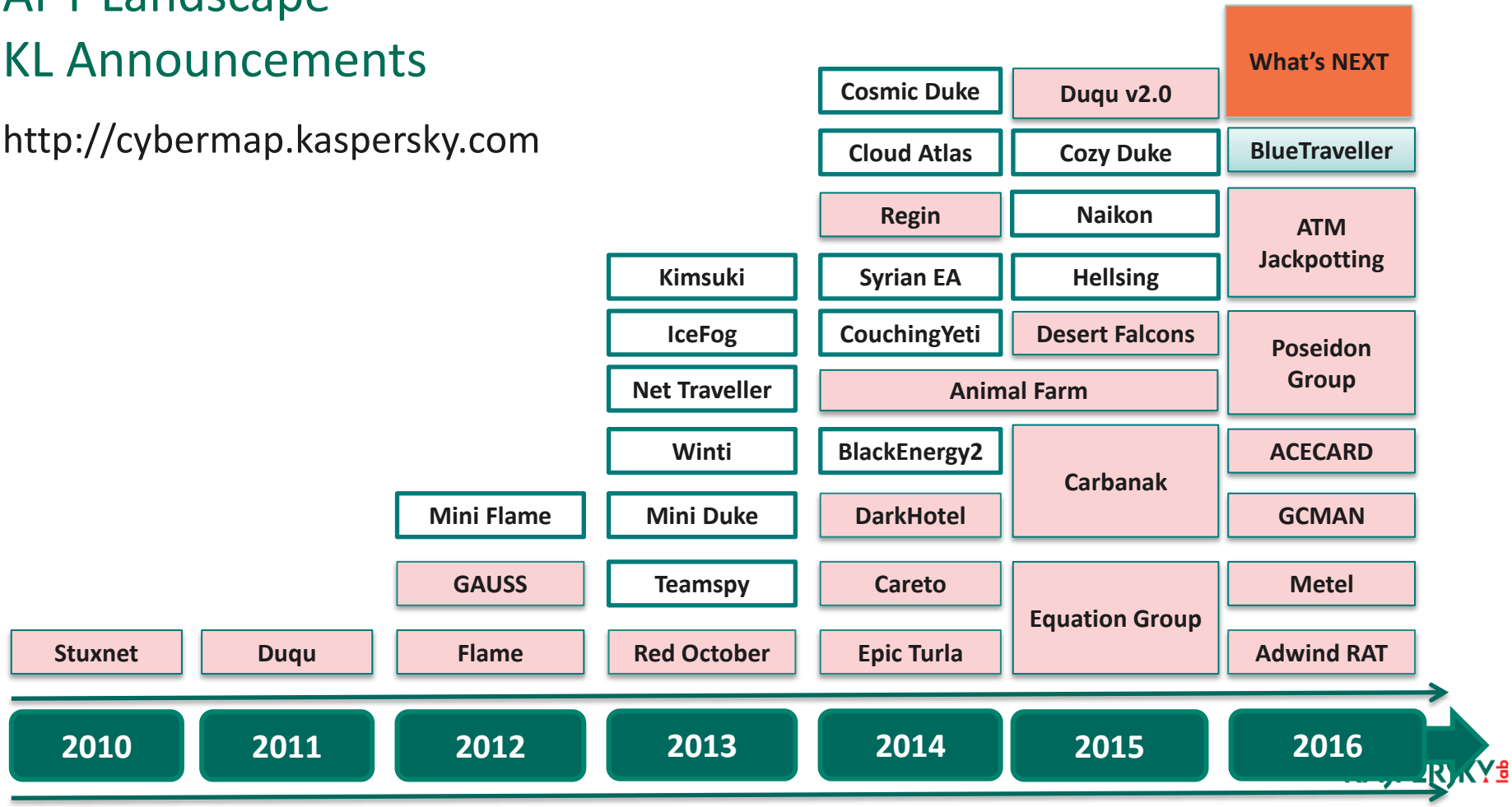
KASPERSKY lab

THREAT LANDSCAPE OVER 15+ YEARS

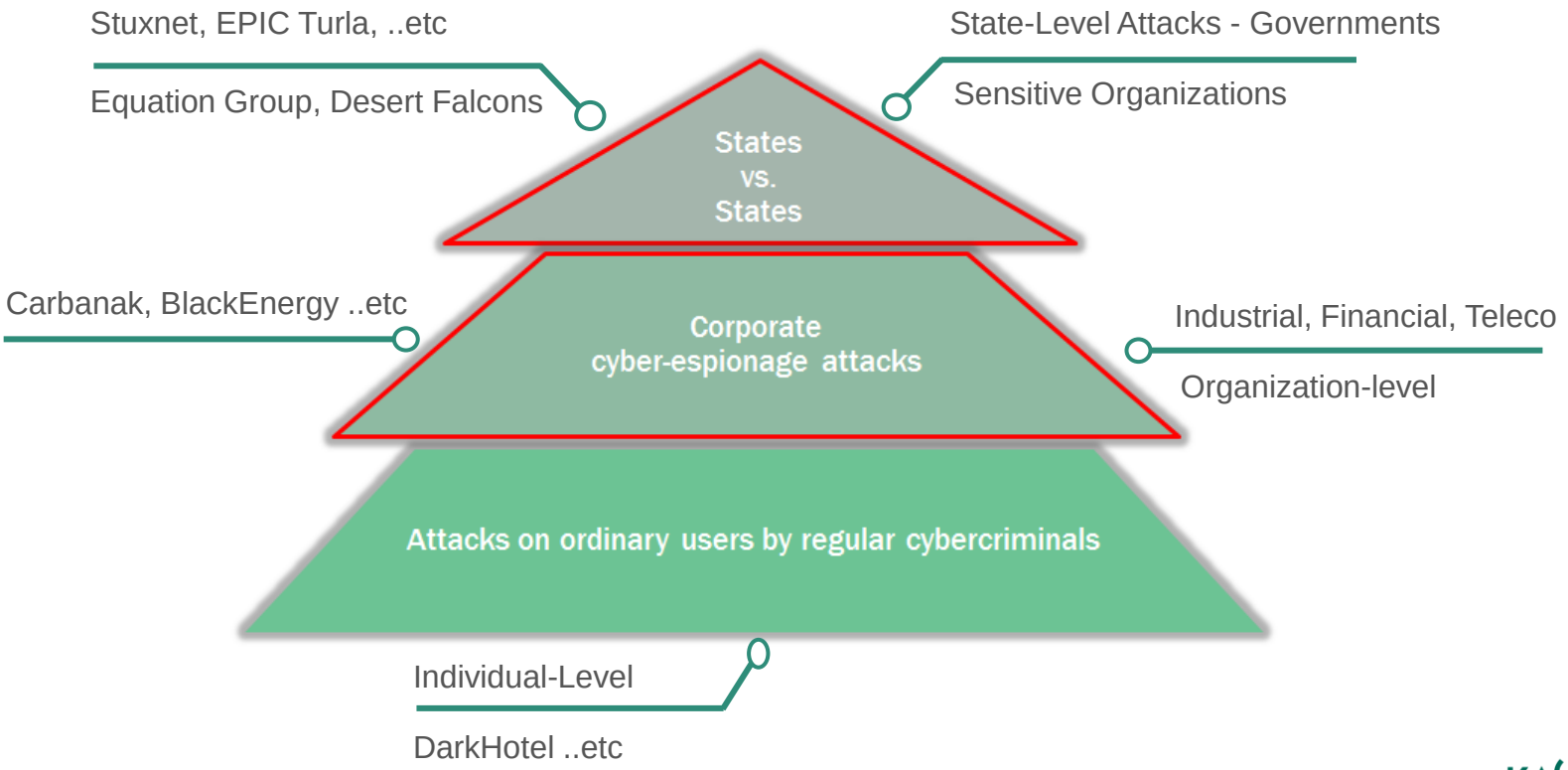


APT Landscape
KL Announcements

http://cybermap.kaspersky.com

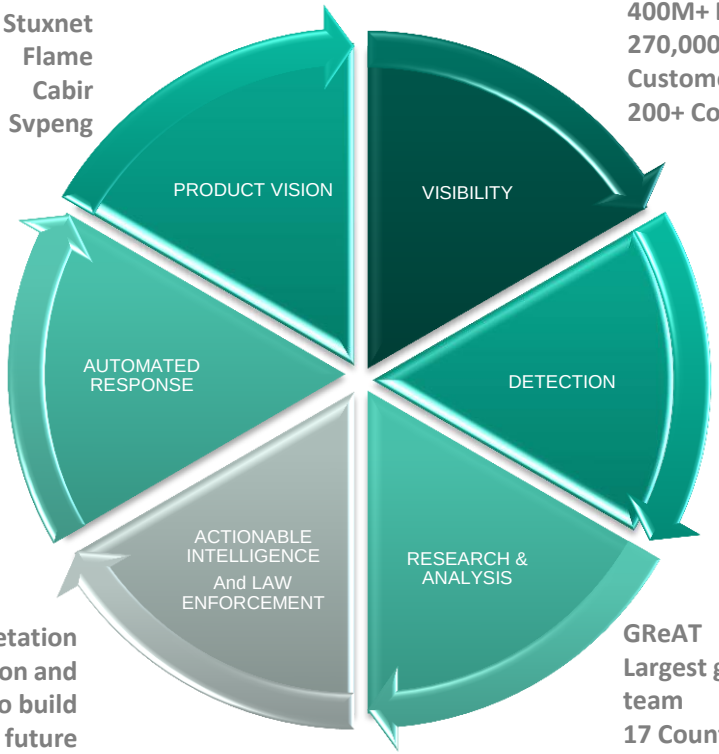


THREATS PYRAMID



THREAT INTELLIGENCE – THE ENDURING ADVANTAGE

One of The Most Advanced Global Threat Intelligence Ecosystem



Stuxnet
Flame
Cabir
Svpeng

400M+ Endpoint;
270,000 Corporate Customers
200+ Countries

Sophisticated threats require intelligent detection methodologies; 350,000+ Unique Samples Collected Daily

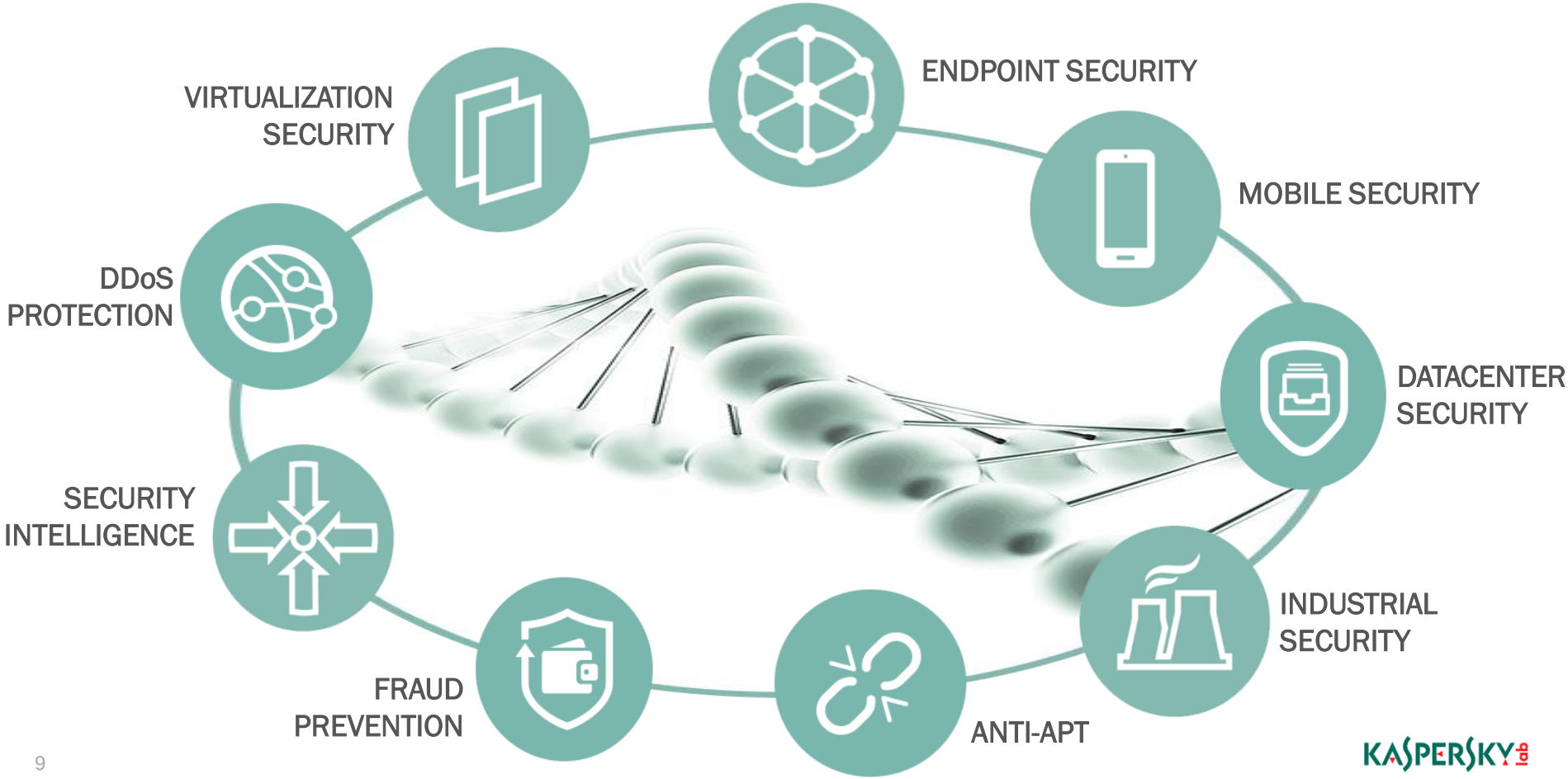
GReAT
Largest global threat research team
17 Countries

Intelligent interpretation of threat evolution and trends allows us to build protections for future threats

Updates are globally distributed silently less then a minute

GLOBAL RESEARCH AND ANALYSIS TEAM - GREAT

SECURITY INTELLIGENCE IS IN OUR DNA



INDUSTRIAL CYBER SECURITY

JANUARY 2016, UKRAINE

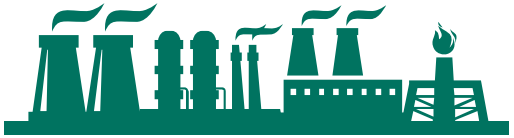
deliberate attack into 2 Ukrainian electricity distribution companies

- 23 Substations (35kV)
- 7 Substations (110kV)
- 80,000 customers affected

http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

INDUSTRIAL SECURITY APPROACH

Industrial Network



1. Availability
2. Integrity
3. Confidentiality

Corporate Network

1. Confidentiality
2. Integrity
3. Availability

- Corporate IT Security is about Data protection
- Industrial Security is about Process protection
- Process should be continuous and only then secure

INDUSTRIAL CYBER SECURITY METHODOLOGY

Continuous Risk Assessment

ICS-Specific Regular PenTesting and Security Assessment, Gap Assessment, IR and Managed Defense

Risk Assessment

Knowledge, Cyber Intelligence, Security Gap Assessment, Penetration Testing

Incident Response & Forensics, Managed Defense,

Consultancy for regulations & compliance

Consultancy, Incident Response & Forensics, Standards & Security Requirements

Risk and Threat Awareness

Awareness Training for ICS Operators, Engineers and Managers from Business, ICS and InfoSec

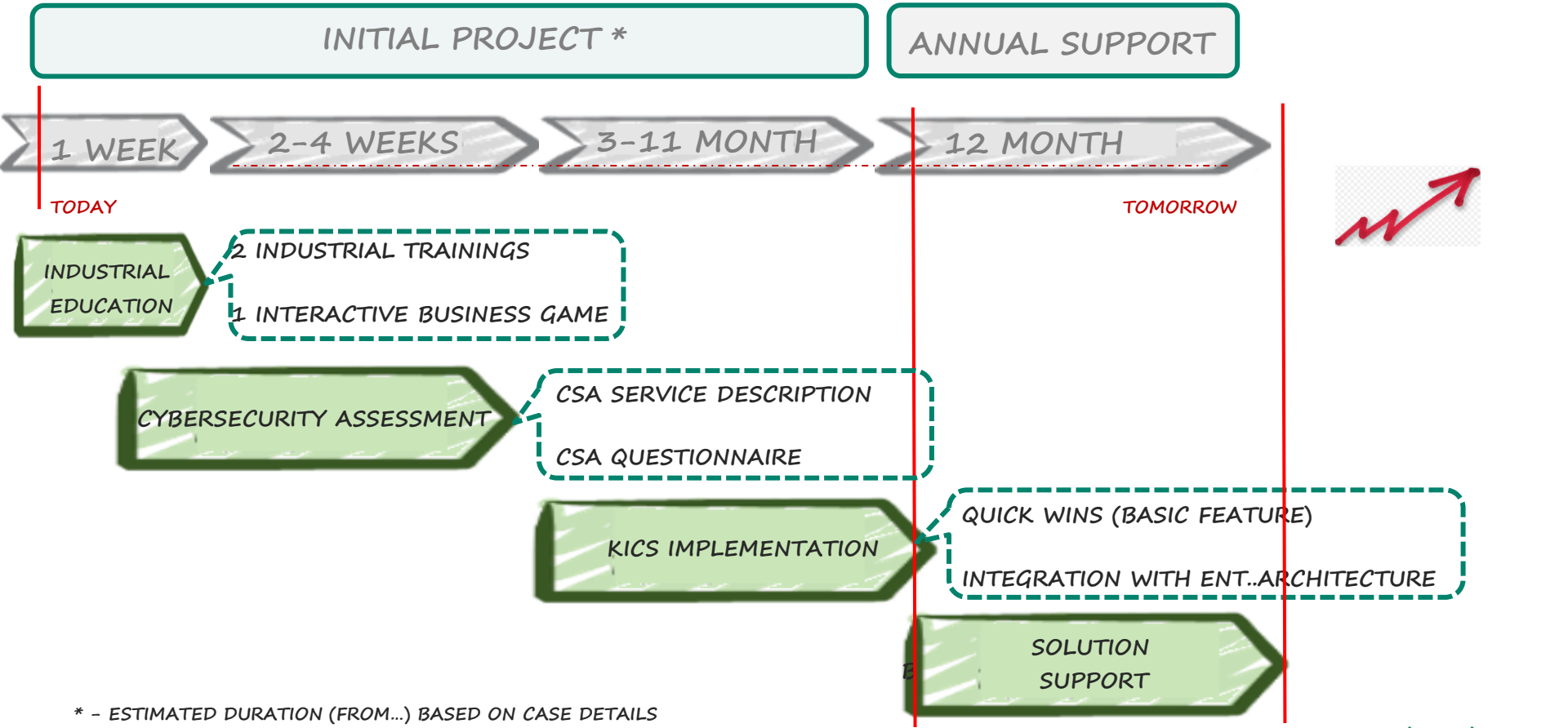
24x7 Support

Technical Support, Emergent Response, Regular Maintenance

Multi-layer Tailored ICS Security

Nodes Integrity Control,
Network Integrity Control,
Process Integrity Control,
Anti-Malware Protection

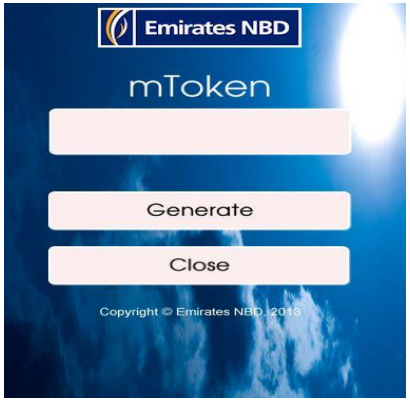
ICS SECURITY EXECUTION APPROACH AND TIMEFRAMES

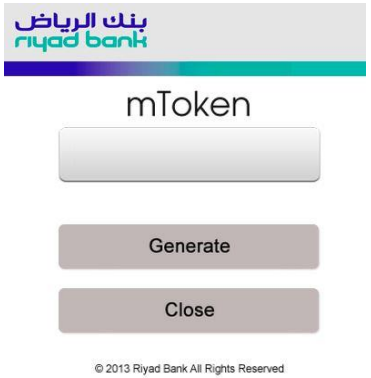


* – ESTIMATED DURATION (FROM…) BASED ON CASE DETAILS

ONLINE FINANCIAL SYSTEMS SECURITY

MOBILE BANKING THREATS





KASPERSKY lab

MATCHING 5 LEVELS OF WEB FRAUD (GARTNER)

Level 1: **Endpoint-centric**, and it involves technologies deployed in the context of users and the endpoints they use.

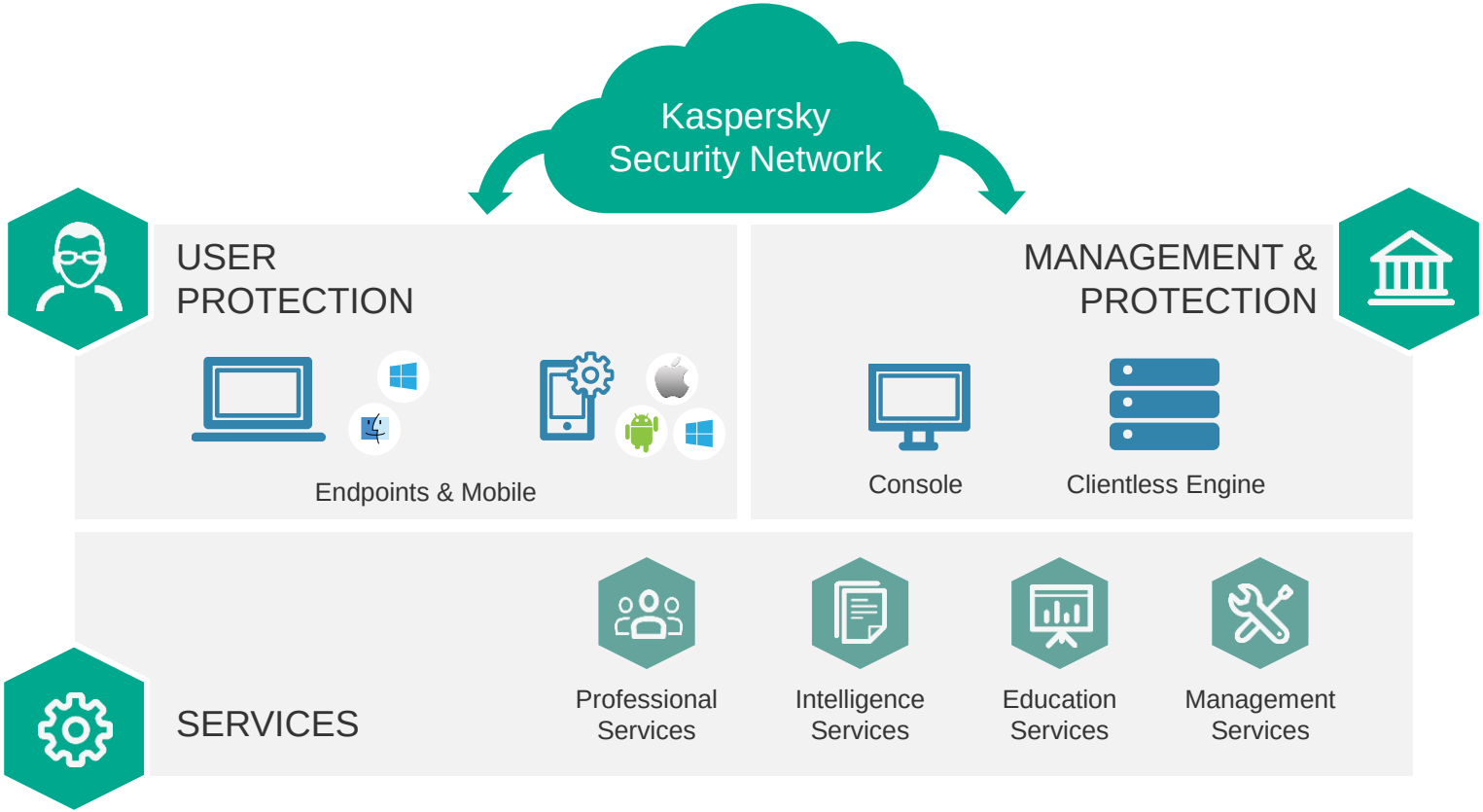
Level 2: **Navigation-centric**; monitors and analyzes session navigation behavior and verifies it with expected patterns

Level 3: **User- and account-centric for a specific channel** (e.g. online sales); it analyzes user behavior and transactions.

Level 4: **User- and account-centric across multiple channels and products** (e.g. online sales and in-store sales).

Level 5: It is entity link analysis. It enables the analysis of relationships among internal and/or external entities and their attributes to detect organized or collusive criminal activities or misuse.

KASPERSKY FRAUD PREVENTION PLATFORM



FINANCIAL SYSTEMS FRAUD DETECTION AND PREVENTION

Continuous Risk Assessment

Financial-Specific Regular PenTesting and Security Assessment, Gap Assessment, IR and Managed Defense

Risk Assessment

Knowledge, Cyber Intelligence, Security Gap Assessment, Penetration Testing

Incident Response & Forensics, Managed Defense,

24x7 Support

Technical Support, Emergent Response, Regular Maintenance

Risk and Threat Awareness

Awareness Training for Financial Systems Operators, Engineers and Managers from Business, Technical and InfoSec Depts.

Multi-layer Tailored Fraud Detection and Prevention

Secure Browsing for Internet Banking

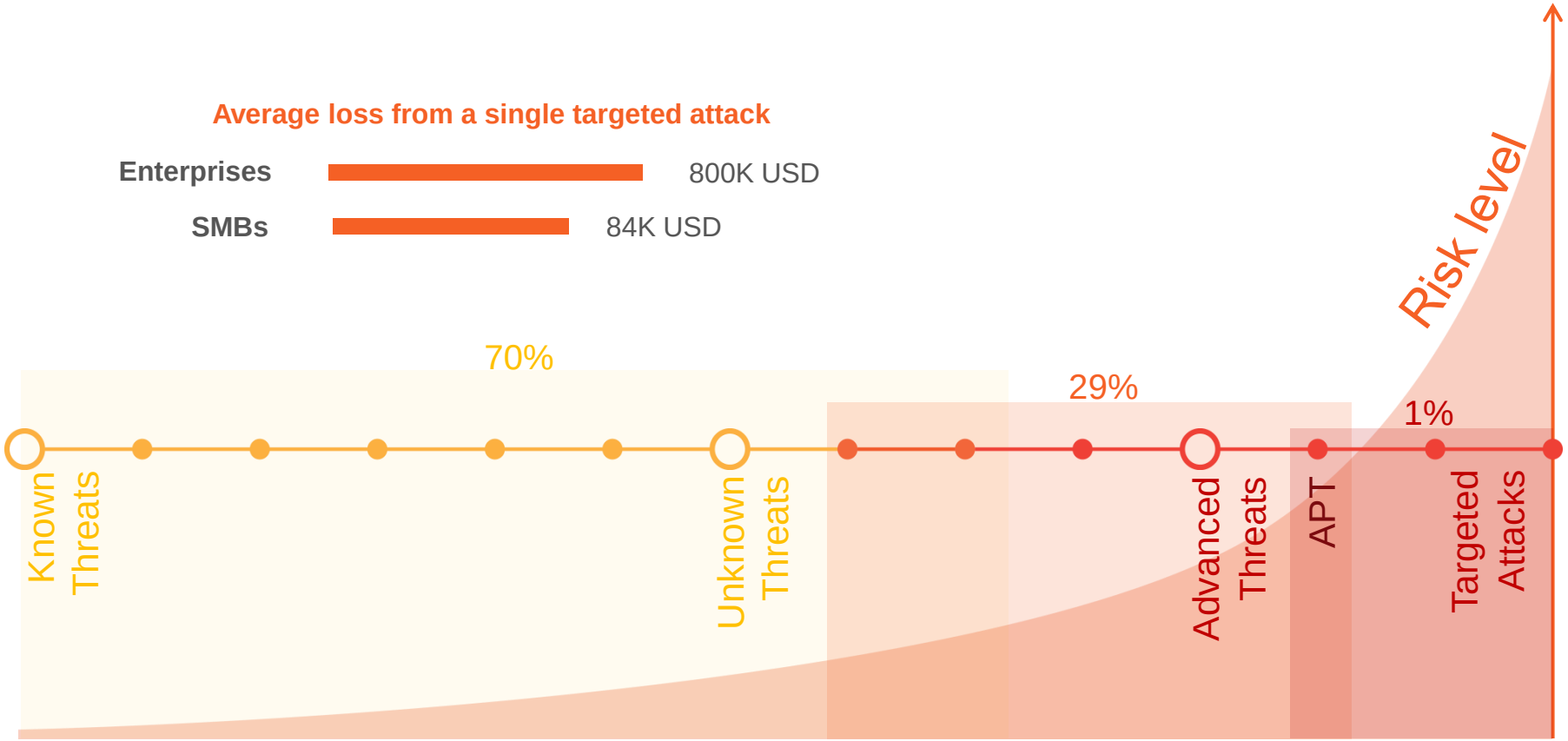
Mobile App Security,

ATM – POS Specific Security

Server-side Malware Detection, Account Takeover and Behavior Analysis

ANTI-TARGETED ATTACKS PLATFORM

1% BRINGS HIGH RISK AND HIGH LOSSES



* Based on Corporate IT Security Risks Survey, 2015, conducted by Kaspersky Lab and B2B International. Indicates an average loss from a single targeted attack, including direct losses and additional spend required to recover from an attack.

KASPERSKY lab

TARGETED ATTACK IS NOT A ‘ONE-OFF’ OFFENSIVE: IT’S AN ONGOING PROCESS

KASPERSKY lab

HOW TO ADDRESS THE ISSUE OF TARGETED ATTACKS

SMART PREDICT

- Analyze the potential security gaps
- Adjust countermeasures accordingly
- (if not already done) create a dedicated SOC

PREVENT MULTI-LAYERED

- Mitigate the risks
- Raise the threat awareness
- Implement the right approaches to mitigate potential risk with existing solutions

EFFECTIVE RESPOND

- Analyze the incident
- Take immediate steps to mitigate the consequences

DETECT VIGILANT

- Discover of the incident
- Track its immediate source
- Understand its nature

STAGES .. FOR EFFECTIVE PROCESS

Data Acquisition

- Sensors
  - Network
  - Web/Proxy
  - EMail
  - Endpoint

Analysis

- Processing engines
- Targeted Attack Analyzer
- Advanced Sandbox
- Threat Intelligence (KSN)

Verdict

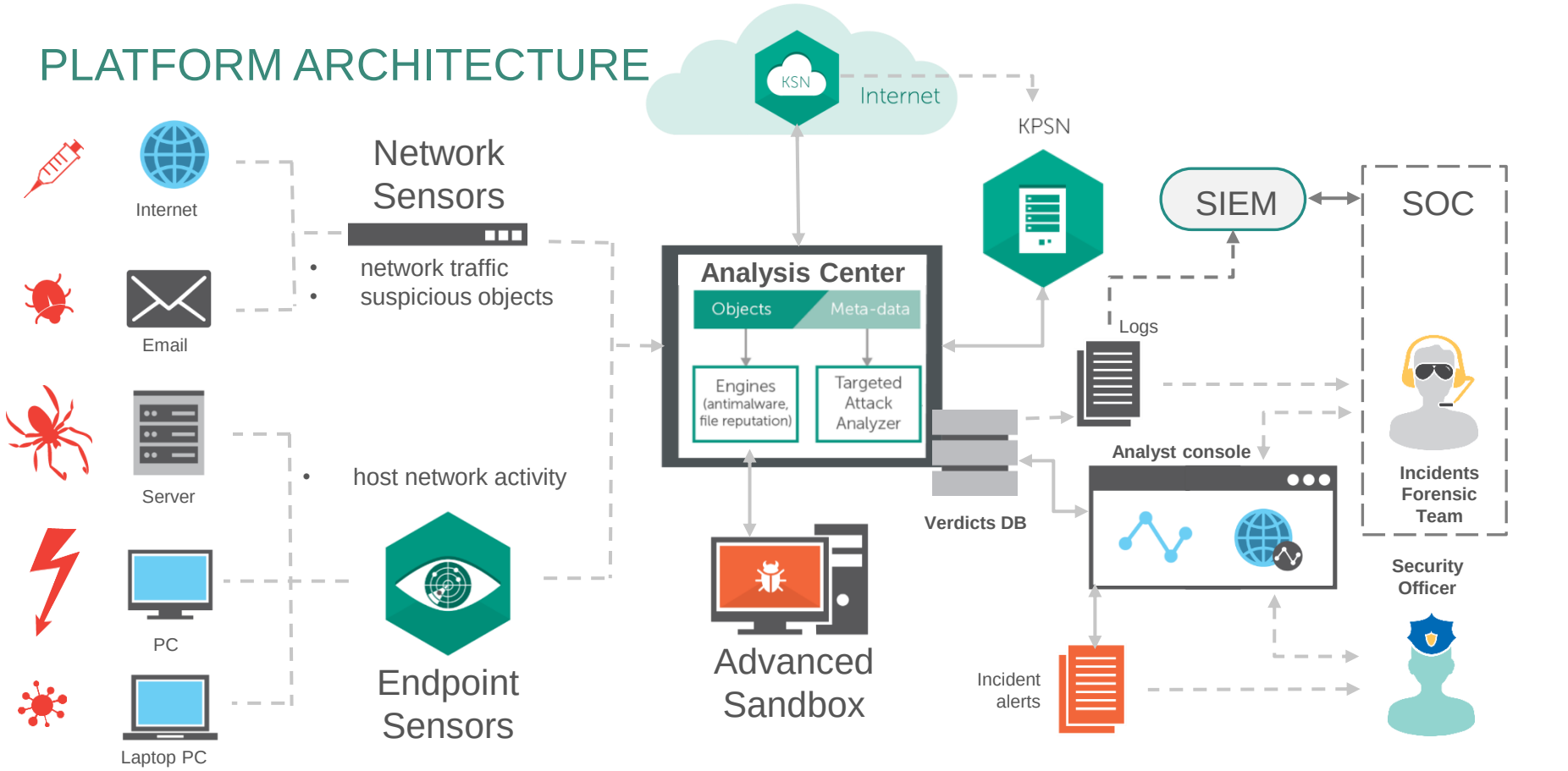
- Visualization Console
- SYSlog
- SB activity log
- Pcaps
- Detonated samples

Response

- Security Intelligence Services

KASPERSKY lab

PLATFORM ARCHITECTURE



Attack vectors | Data Acquisition | Data Analysis | Verdict prioritizing | Response

KASPERSKY lab

BUILDING AN ADAPTIVE ENTERPRISE SECURITY STRATEGY

PREDICT

KNOW YOURSELF:

- Penetration testing service
- Security assessment service
- **Targeted Attack Discovery Service**

PREVENT

TRAIN:

- Cybersecurity training

PROTECT:

- Kaspersky Lab Enterprise security solutions

EDUCATE:

- Cyber-safety Games
- Threat simulation

RESPOND

REACTION:

- **Incident response service**

INVESTIGATE:

- Malware analysis service
- Digital forensics services

DETECT

EXPERTISE:

- **Targeted Attack Investigation Training**

THREATS LANDSCAPE:

- APT reporting
- Botnet tracking
- Threat data feeds

SOLUTION:

- **Kaspersky Anti Targeted Attack Platform**

KASPERSKY lab

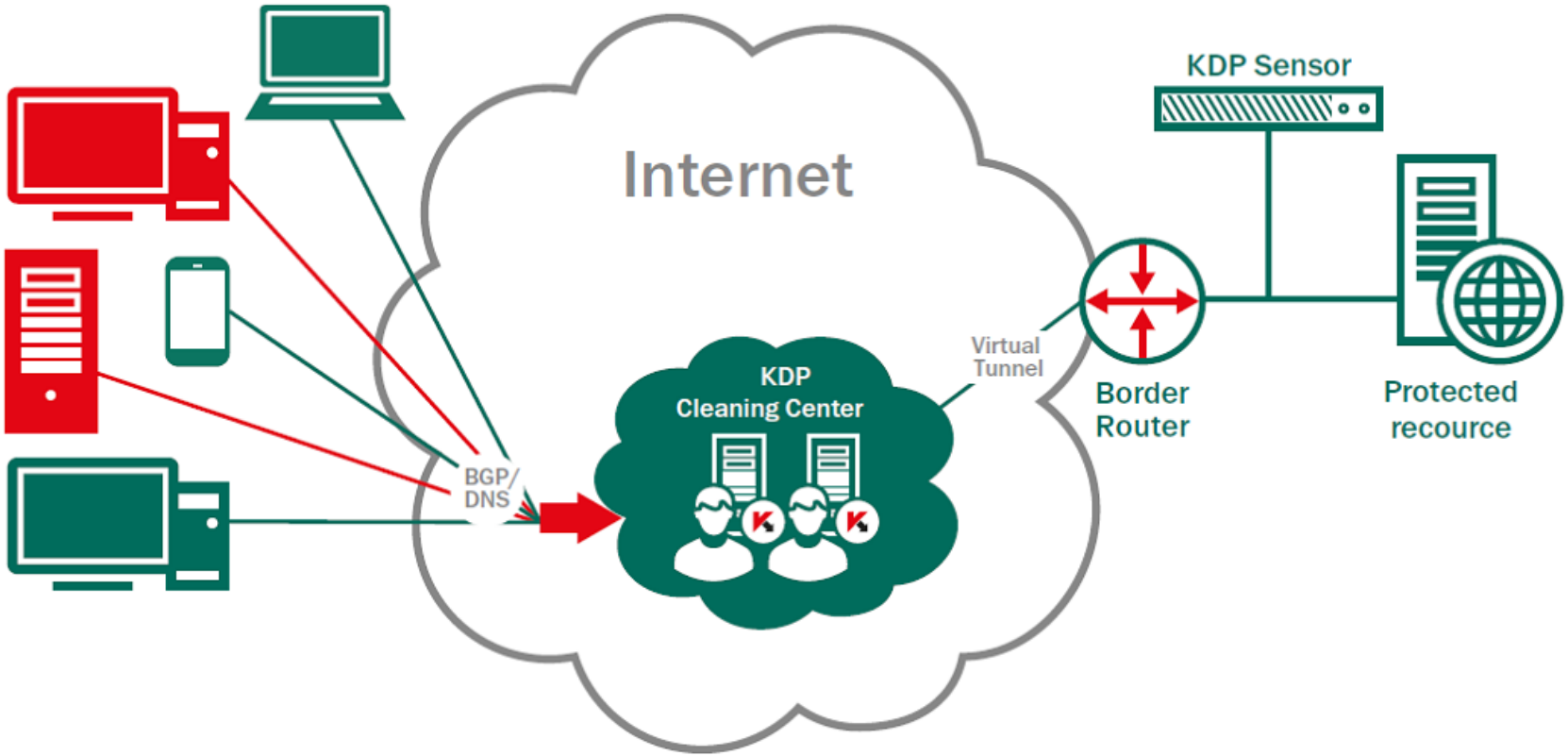
DDOS MITIGATION AND PROTECTION

NEXT GENERATION DDOS PROTECTION

DDOS ‘SERVICES’ ARE READILY AVAILABLE

- $200 – black market cost of a day-long DDoS attack.
- Specialized online marketplaces exist where you can buy and sell botnets or individual DDoS attacks.
- Would-be DDoS attackers simply pay by PayPal, Bitcoin or credit card and choose desired attack.
- If you don’t want to do the dirty yourself, you can hire someone to perform the service for you, known as a ‘booter.’

KASPERSKY DDOS PROTECTION



KDP ADVANTAGES

In-house developed Solution

The way the solution works can be changed flexibly and rapidly in response to changes

Emergency Response Team 24x7

Filter rules can be modified individually in real time depending on current situation

Protection of resources, not channels

Monitoring traffic more thoroughly and repelling even very big and/or sophisticated attacks

Technology partnership with ISP

Filtering most of the traffic on the provider's side and decreasing burden of attack

KL DDoS Intelligence

Our proven threat expertise helps to identify an attack at a very early stage

THREAT AND SECURITY INTELLIGENCE

BUILDING AN EARLY WARNING SYSTEM AGAINST ADVANCED THREATS

INTEGRATE THREAT INTELLINGENCE INTO YOUR INFOSEC FRAMEWORK

ALERTING

Notifications

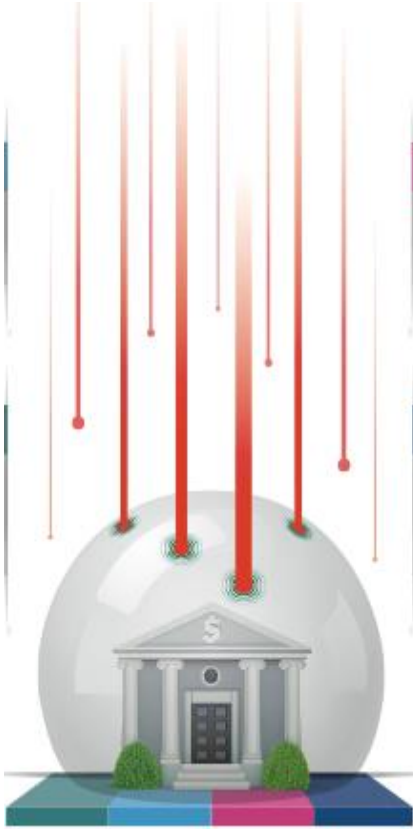
Botnet Tracking

Intelligence Reporting and Early IOC

Suspicious Activity

Analysis & Forensics

Malware Analysis, Digital Forensics, IR, PenTesting, Security Assessment.



External Intelligence

Feeds

Feed your internal systems with external trusted security &threat intelligence

Cyber-Threat

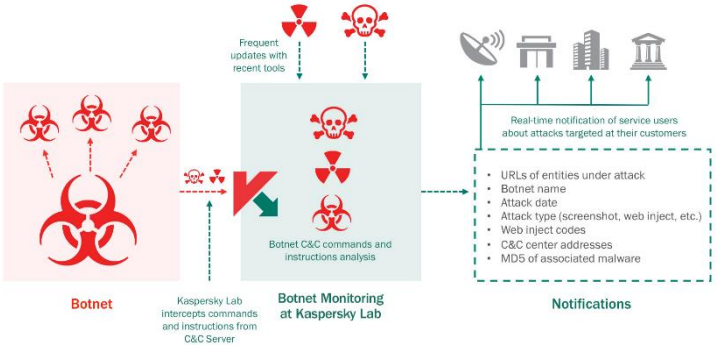
EDUCATION

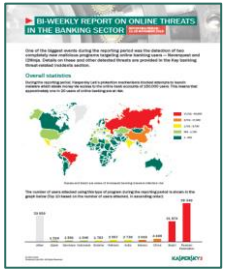
1) Malware Analysis and DF, Reverse Engineering

2) CyberSafety Games

37

1ST: ALERTING – THREAT INTELLIGENCE





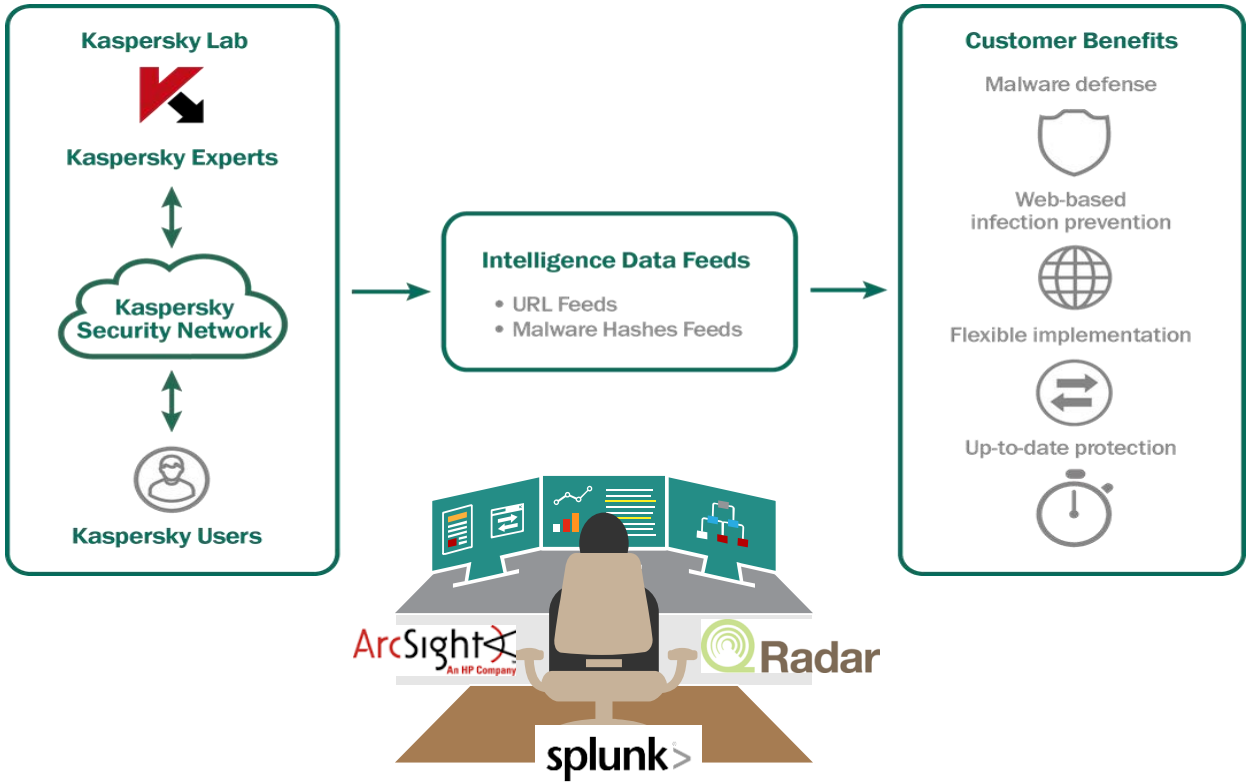
Real-time Notification for External Threats

- Monitor Mobile, Online and Payment Systems for threats targeting the entity or its consumers
- Real-time notification – within 20 minutes
- Notification Includes Target System, Attack Description, Attack Distribution, Malware Hash, Attack Rules, C&C …etc
- Two Level: Standard and Premium

APT Reporting & External Threat Reporting

- Identification of Threat Actors
- Malware and Cyber-Attacks Tracking Analysis
- Third-Party Attacks
- Information Leakage
- Current Attack Status and APT Private Reporting

2ND: EXTERNAL THREAT DATA FEEDS



Feed your existing security controls with external intelligence to add advanced layer of protection.

SIEM: Qradar, ArcSight, Splunk

Gateways: Firewalls, UTMS ..etc

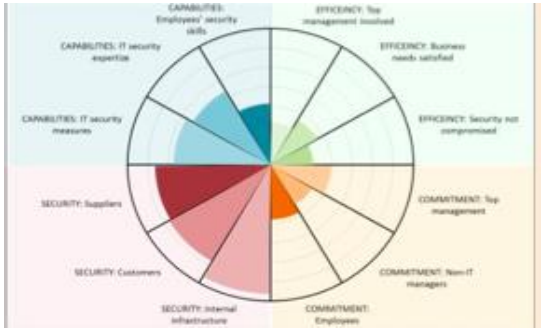
KASPERSKY lab

3RD: CYBER SAFETY TRAINING PROGRAM

Cyber Safety Games

- Interactive Games that cover 9 cyber security domains in teams' format.
- Impersonate Cybercriminals, Focus on Dos not Don'ts, Play in teams for maximum benefit.
- At least 10% of the organization staff

Cyber Safety Culture Assessment



- Assessment for 12 cyber security domains across the organization
- Help in understanding the gaps and areas of focus in the organization's culture
- At least 15% of the organization staff

Cyber Safety Online Training Platform

- Online Training modules to cover 11 different domains.
- Skills Assessment
- Analytics and Reporting
- Supporting security posters, email templates, screensaver images.

4TH: SUSPICIOUS ACTIVITY SERVICES

The Expert!

Proactive Response!

Analyze different threat sources and perform tool aided scanning

Is this single incident or part of a chain!

Continuous Process!

KASPERSKY lab

ENHANCING SOC OPERATIONS AND CAPABILITIES

SECURITY EDUCATION

Security Awareness & Fundamentals
Digital Forensics
Malware Analysis & Reverse Engineering
Cyber Safety Games

INVESTIGATION SERVICES

Malware Analysis
Digital Forensics
APT Discovery and Incident Response

THREAT INTELLIGENCE

Threat Data Feeds
Botnet Tracking
Intelligence Reporting
Threat Lookup

SECURITY ASSESSMENT

Pen Testing
Application Security Assessment
Telco-Specific Assessment
Financial-Specific Assessment

KASPERSKY lab

PRACTICAL EXAMPLES

SUCCESS STORIES

SUCCESS STORY — INTERPOL

INTERNATIONAL CRIMINAL POLICE ORGANIZATION
ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL

ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE
المنظمة الدولية للشرطة الجنائية

INTERPOL

Letter

To whom it may concern

Date 6 June 2014

Our Ref. 2014/244/L/EDIGCI/NN

Contact Mr Noboru Nakatani
Executive Director
INTERPOL Global Complex for Innovation

Subject **Reference letter**

INTERPOL has been working with Kaspersky Lab in the field of cybersecurity since April 2013 and have had a very positive experience in doing so.

The Internet security company has been actively assisting us in the run up to the launch of the INTERPOL Global Complex for Innovation (IGCI) in Singapore. It has provided training courses for our officers and one of the company's top researchers will stay in Singapore to support the launch of the IGCI's new Digital Forensics Laboratory. Kaspersky Lab has also been sharing its threat intelligence with INTERPOL and assisting in several investigations in cyber-incidents.

I believe that Kaspersky Lab has made a serious contribution to providing security on a global scale by actively helping INTERPOL's efforts to form a Global Alliance against Cybercrime. In doing so the company has demonstrated its continued commitment to making cyberspace a safer and more secure place, while respecting its openness.

Should you need any further information, please do not hesitate to contact me on the following email address: n.nakatani@interpol.int.

Yours faithfully,

Noboru Nakatani
Executive Director
INTERPOL Global Complex for Innovation

General Secretariat - Secrétariat général - Secretaría General - الأمانة العامة
200 Quai Charles de Gaulle | 69006 Lyon | France | T +33 4 72 44 70 00 | F +33 4 72 44 71 63 | www.interpol.int

KASPERSKY lab

SUCCESS STORY — TELEFONICA

http://www.kaspersky.com/about/news/business/2014/Kaspersky-Lab-and-Telefonica-join-forces-to-improve-cyber-protection-for-European-and-Latin-America-customers

http://www.eurocomms.com/industry-news/49-online-press/9898-telefonica-signs-cyber-security-deal-with-kaspersky-lab

LET'S TALK!

Ghareeb Saad
Senior Security Researcher
Global Research and Analysis Team
Ghareeb.Saad@kaspersky.com

Amr Ismail
Senior Security Consultant
Enterprise Business
Amr.Ismail@kaspersky.com

Ashraf Abdelazim
Director, Enterprise Business
Emerging Markets
Ashraf.Abdelazim@kaspersky.com

Mikhail Nagorny
Head of Security Services
Enterprise Business
Mikhail.Nagorny@kaspersky.com

KASPERSKY lab