

kaspersky

Jak vzdělávat své zaměstnance na kybernetickou bezpečnost

**Petr Kuboš | Enterprise Sales Manager CZ a SK;
petr.kubos@kaspersky.com**

Fakta o Kaspersky

> 22

let historie

> 4,000

vysoce kvalifikovaných zaměstnanců

> 400,000,000

uživatelů celosvětově je chráněno našimi
technologemi

> 270,000

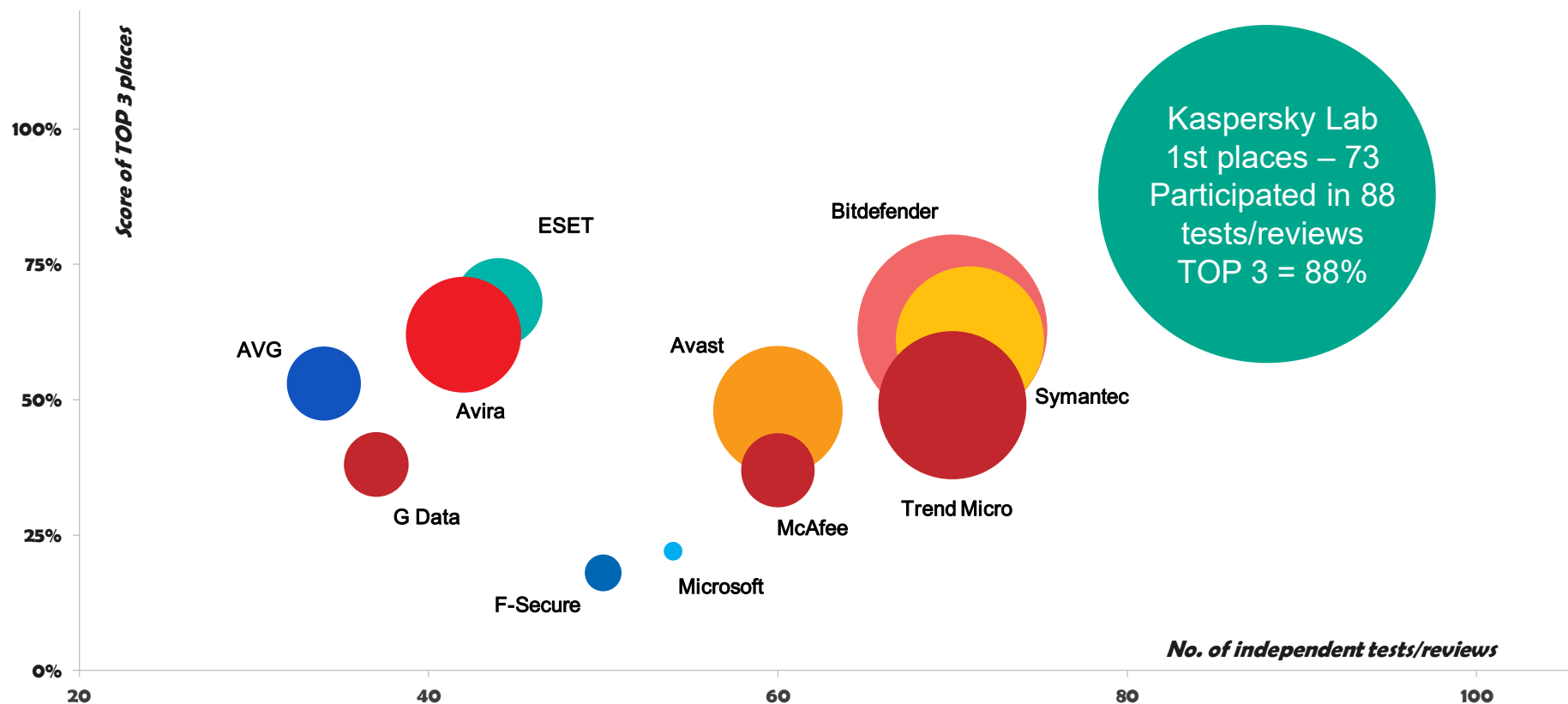
firemních zákazníků celosvětově

> Celosvětově největší, soukromě
vlastněná bezpečnostní společnost



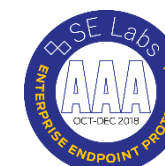
Kaspersky ochrana – nejvíce testována, nejlépe oceňována.

V roce 2018 se produkty Kaspersky Lab zúčastnily 88 nezávislých testů a recenzí. V 73 případech obsadily první místo a v 88% skončily v první trojce.



**MOST TESTED*
MOST AWARDED*
KASPERSKY LAB
PROTECTION**

*kaspersky.com/top3

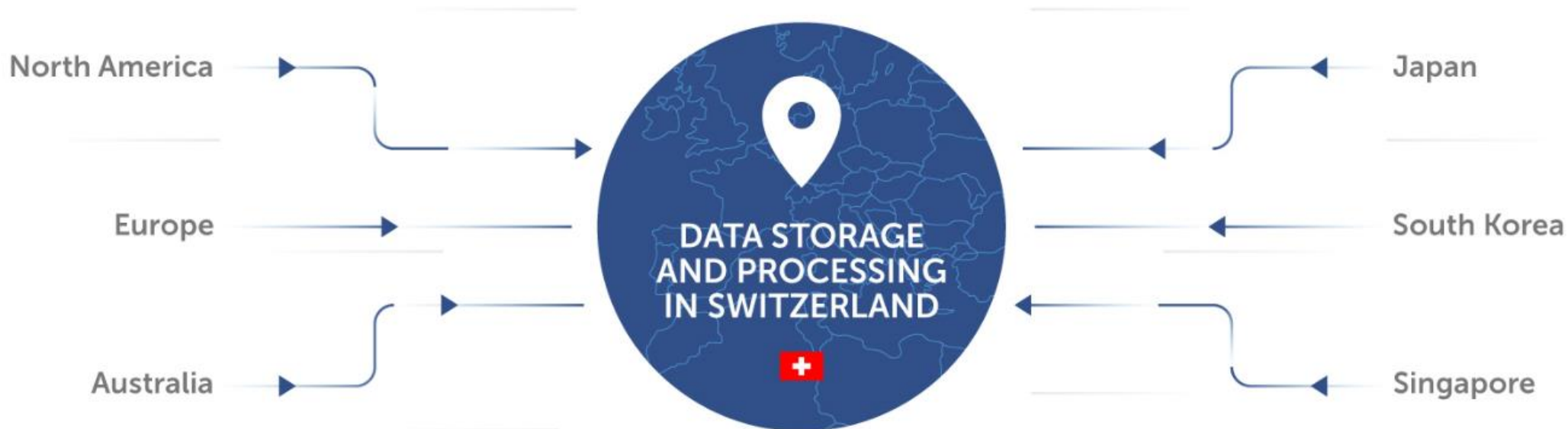


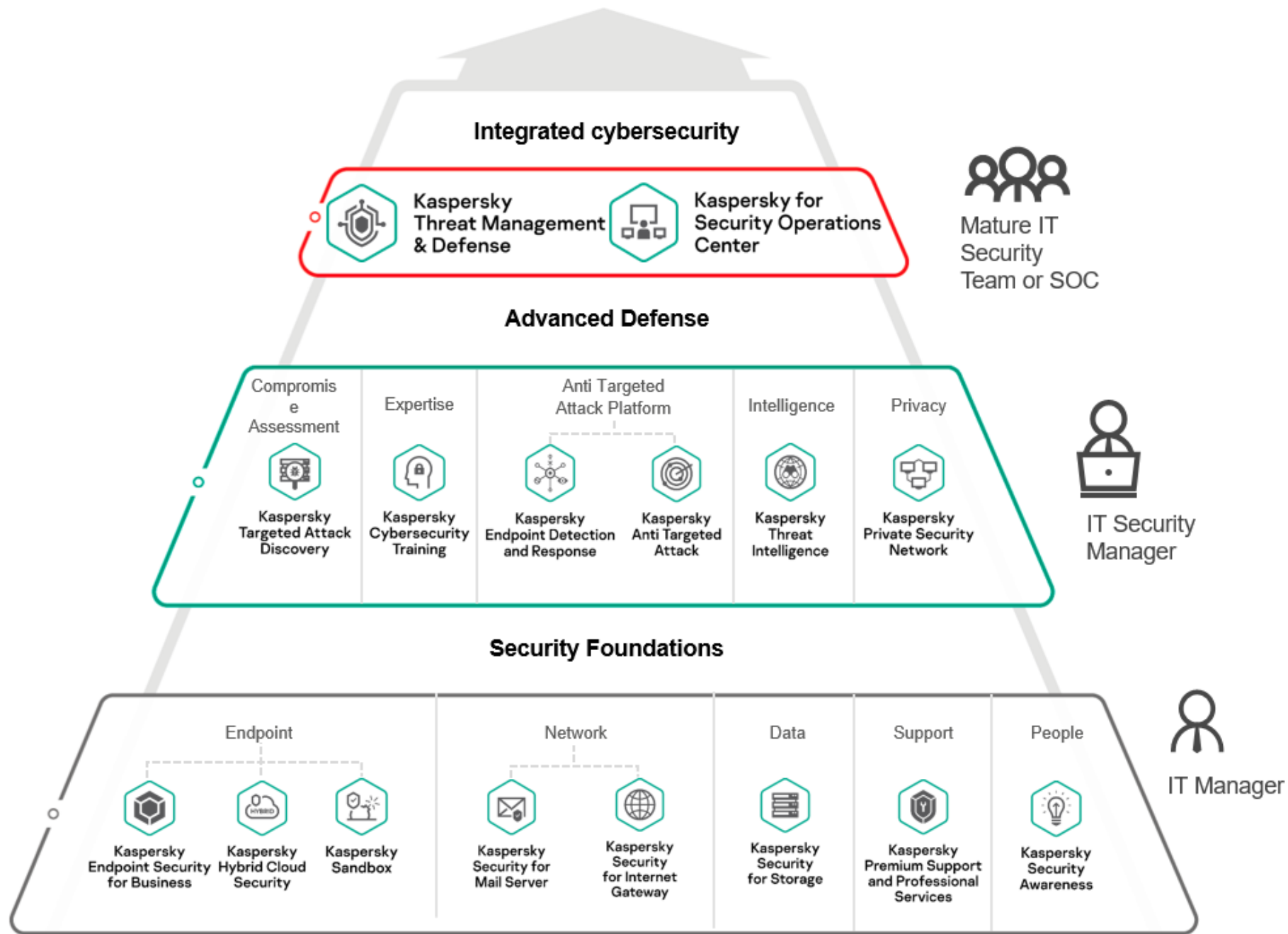
* Notes:

- According to summary results of independent tests in 2018 for corporate, consumer and mobile products.
- Summary includes independent tests conducted by: AV-Comparatives, AV-Test, SE Labs, MRG-Effitas, Virus Bulletin, ICESA Labs, PCSL, NSS Labs.
- Tests performed in these programs assess all protection technologies against known, unknown and advanced threats.
- The size of the bubble reflects the number of 1st places achieved.

Global Transparency Initiative: Kaspersky Lab moves data processing to Switzerland

Kaspersky Lab opens a data center in Switzerland for the secure storage and processing of information received from users in many regions – with more countries to follow.





Vývoj malwaru

(Škodlivých nežádoucích programů)

STUPNICE NÁRUSTU HROZEB

1994

1

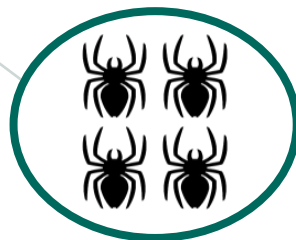
NOVÝ VIRUS
KAŽDOU
HODINU



2006

1

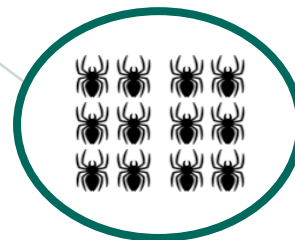
NOVÝ VIRUS
KAŽDOU
MINUTU



2011

1

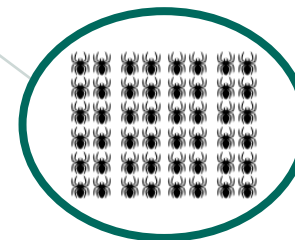
NOVÝ VIRUS
KAŽDOU
SEKUNDU



2014 - 2019

+300,000

NOVÝCH
VZORKŮ
KAŽDÝ DEN



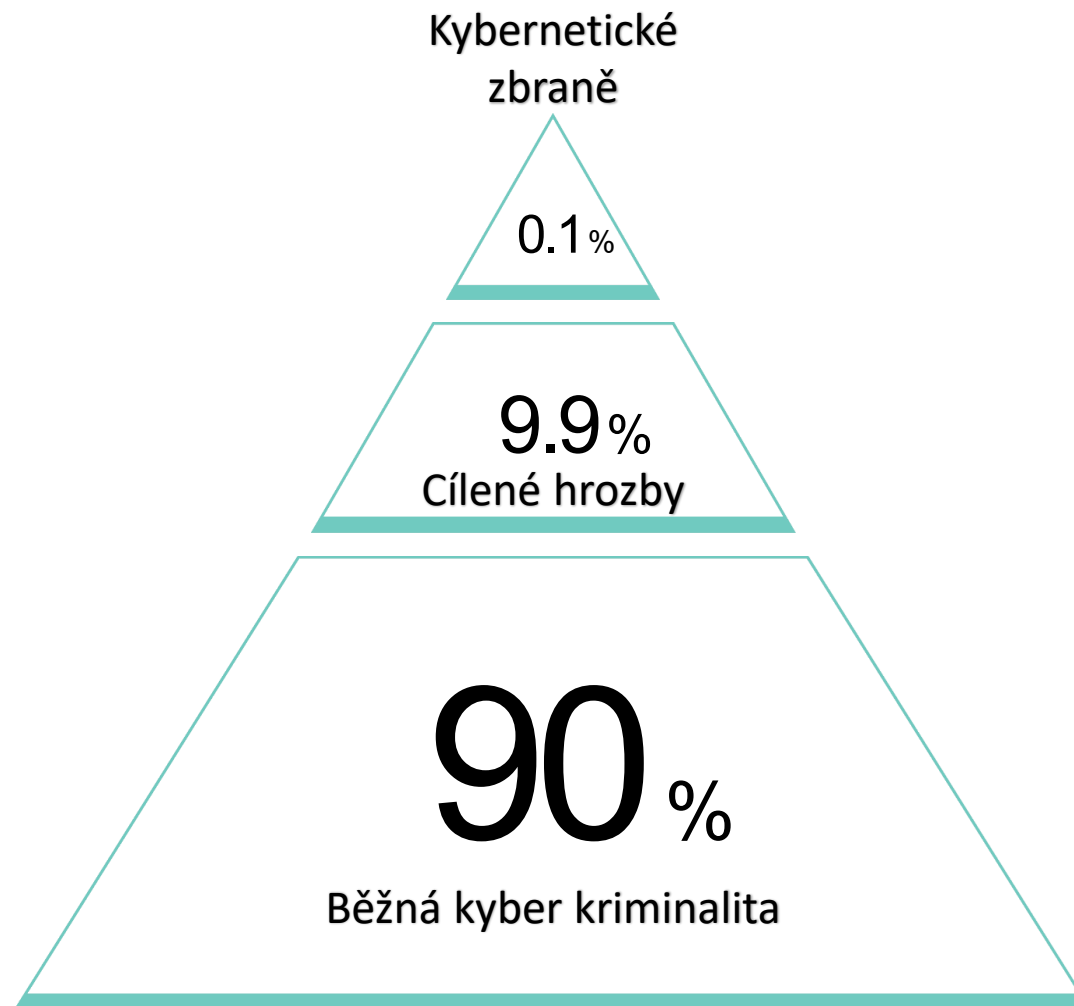
+360,000

Kaspersky detekuje více než 360,000 nových
unikátních

škodlivých souborů denně.

Skladba kybernetických hrozeb

kaspersky



APT – pokročilé persistentní hrozby a útoky,

Cílené útoky a pokročilý malware

„běžné“ hrozby



Profi IT Security Team or SOC



IT Security Manager



IT Manager

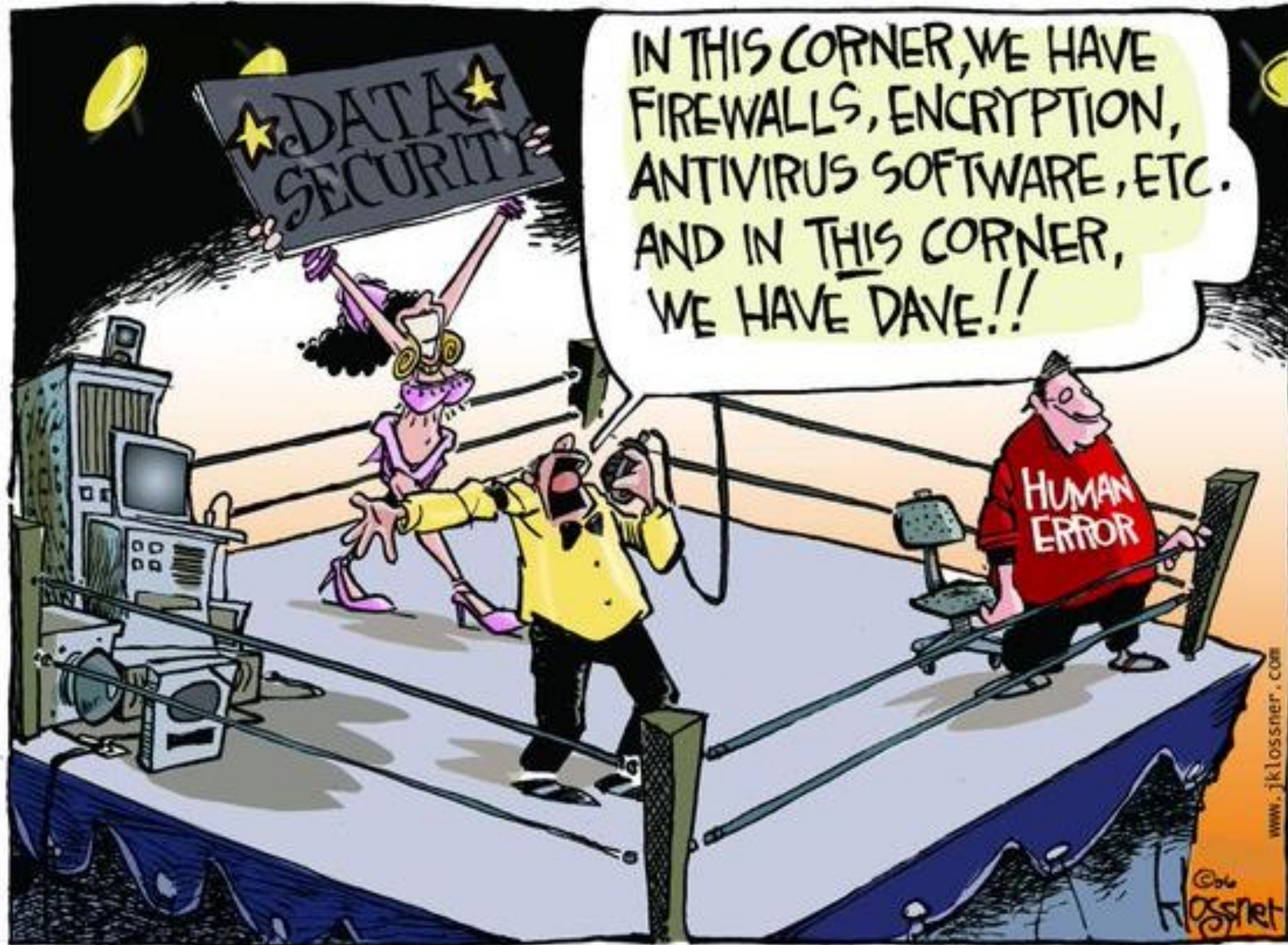
Kybernetické hrozby

jsou realitou dnešních dnů.

Hlavní rizika obchodních společností v roce 2018



2018



IN THIS CORNER, WE HAVE
FIREWALLS, ENCRYPTION,
ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER,
WE HAVE DAVE!!

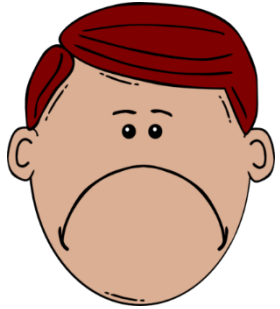
www.jklossner.com

copyright 2006 john klossner, www.jklossner.com

© 06
Klossner

kaspersky

UŽIVATELÉ JSOU TEN NEJSLABŠÍ ČLÁNEK



Až **80%** všech kybernetických incidentů jsou způsobeny lidskými chybami.
Společnosti utrácejí miliony za jejich nápravu.

Lidský faktor jako významná bezpečnostní hrozba

Chování zaměstnanců je pro organizace významná IT bezpečnostní hrozba, navzdory tomu, že jsou využívány tradiční způsoby školení zaměstnanců.



\$1,057,000

v Enterprise organizaci

Průměrný finanční dopad způsobený únikem dat a kybernetickými incidenty zaměstnanců či nedostatečnými IT zdroji



\$98,000

v SMB

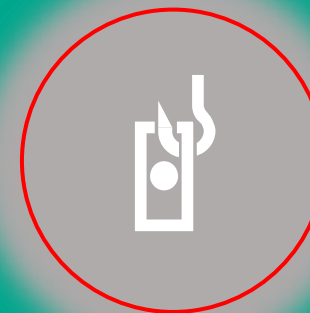
Průměrný finanční dopad způsobený únikem dat a kybernetickými incidenty zaměstnanců či nedostatečnými IT zdroji



\$101,000

v SMB

Finanční dopad útoků způsobených phishingem. *



up to **\$400**

na zaměstnance a rok

Průměrné náklady na řešení phishingového útoku

Proč je důležité vybrat si ten správný vzdělávací program?

Nezajímavé a neefektivní pro zaměstnance:



Považován za obtížné, nudné, nedůležité.



Většinou je to o : „co nesmíte“ než „jak na to“



Účastníci si po školení nic nepamatují



Čtení a poslouchání není efektivní



Přítěž pro administrátory:

Jak vytvořit vzdělávací program a nastavit cíle školení?



Jak zvládnout proces vzdělávání?



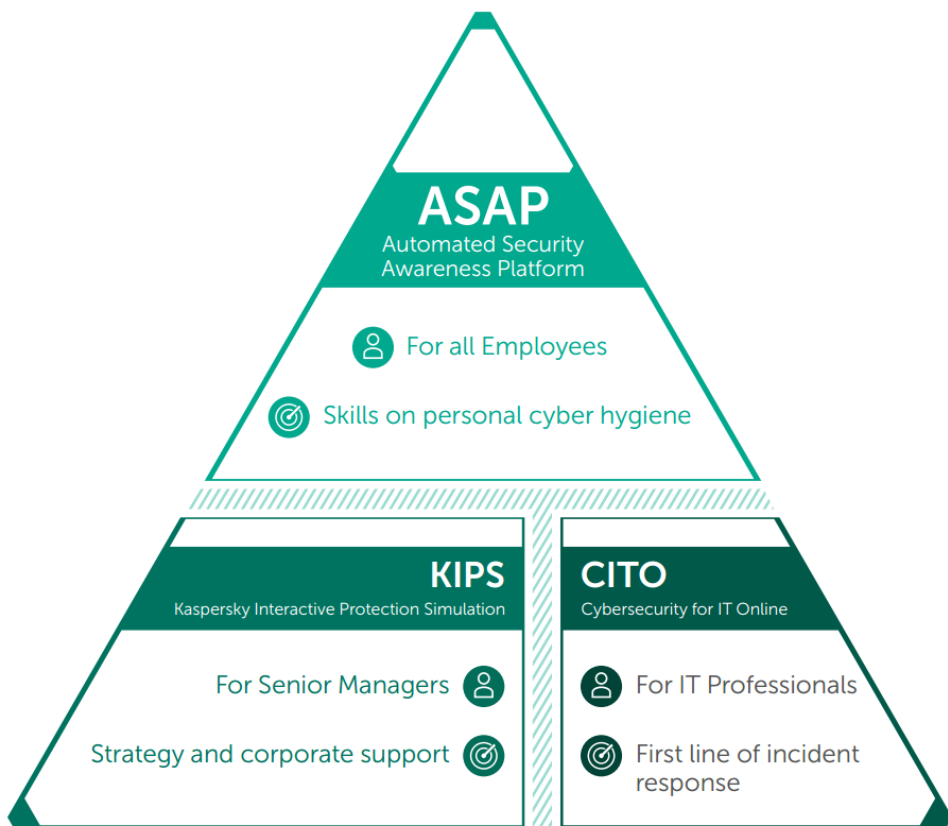
Jak kontrolovat průběžné výsledky?



Jak oslovit zaměstnance aby se zapojili do školení



Kaspersky vzdělávací programy kybernetické bezpečnosti



Praktické dovednosti místo jen znalostí

PC orientované, jednoduché na správu a doručení, skvělý reporting.

Příklady z reálného světa & praktické cvičení – zaměstnanci jsou motivováni a zapojeni do vzdělávacího programu

Jednoduchá správa pro administrátory a efektivní pro organizaci

Redukuje počet lidských chyb a selhání až o

80%

kaspersky

Kaspersky Automated Security Awareness Platform (ASAP)

k-asap.com

Automated cybersecurity skills development platform:

Effective training for employees

01

Kaspersky Automated Security Awareness Training

02

An easy-to-manage online tool which builds employee's cybersecurity skills level by level

03

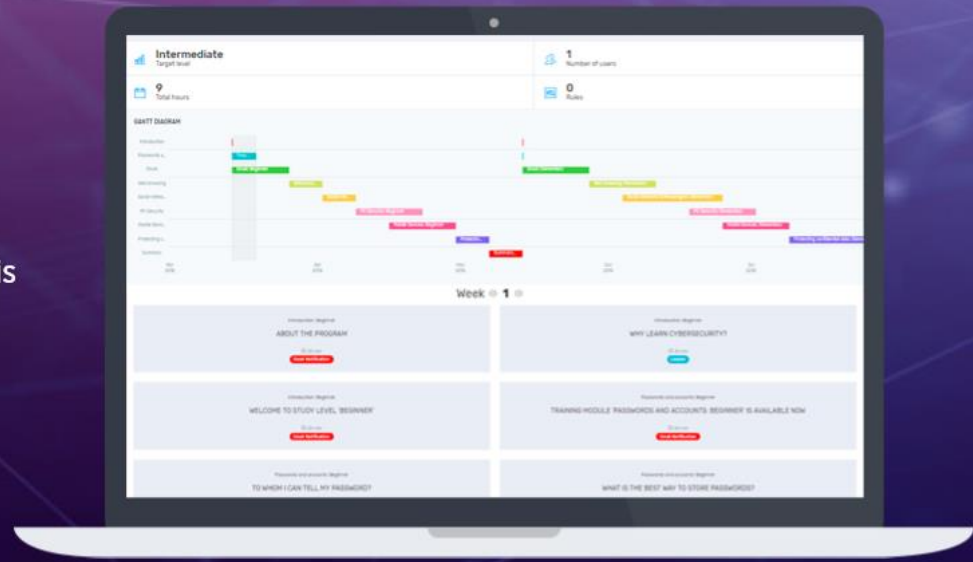
Kaspersky Automated Security Awareness Platform (ASAP) is created by leading cybersecurity experts to protect your business

04

Launch your awareness program online in just a few steps

05

TRY NOW >

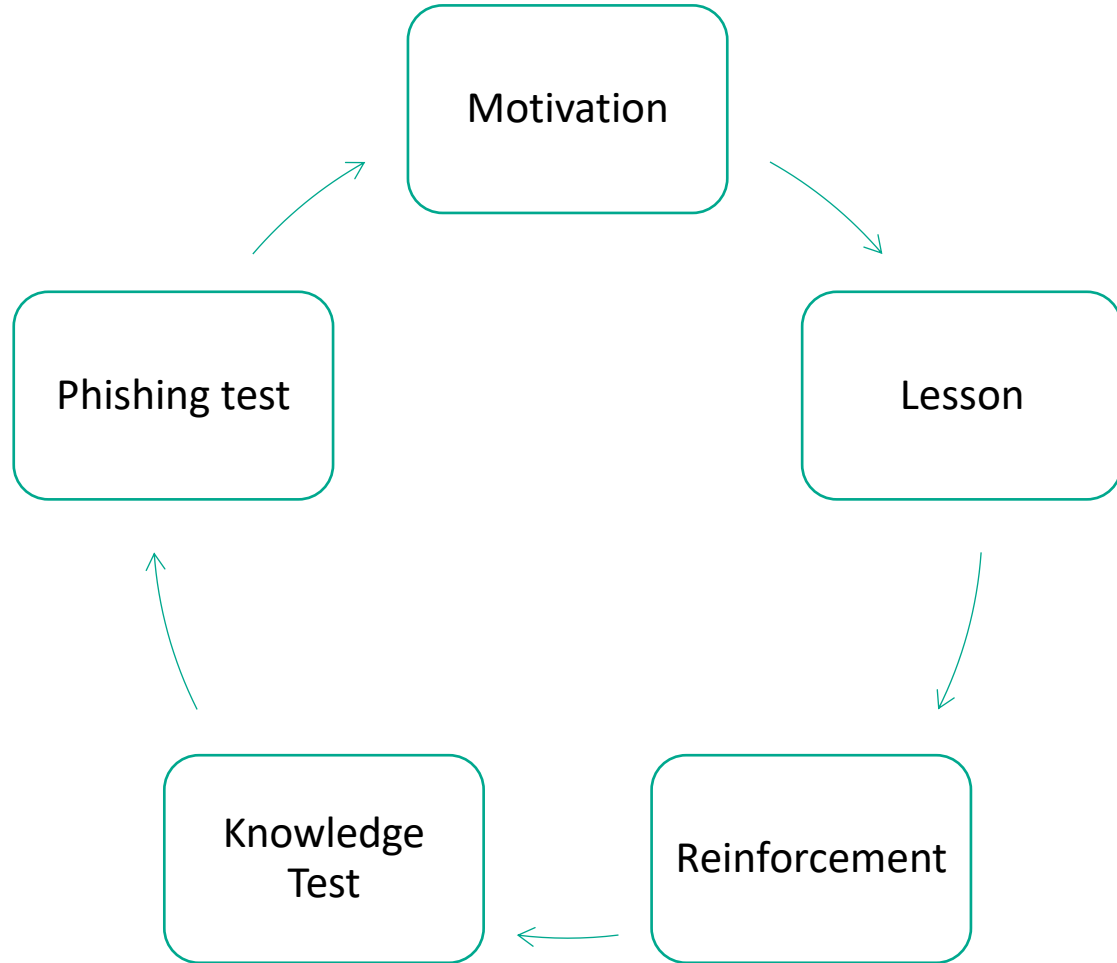


View Demo



View Datasheet

Automated Awareness Platform



- All types of training elements are auto-scheduled and assigned automatically
- Aligned around developing the same skills at the time
- Logical and based on the specifics of human memory

ASAP provides full training management automation

What you need to start training on ASAP?



All the rest:

- individual scheduling
- appointments and individual weekly training reports for employees
- regular reports for the administrator

Will be done automatically by the platform without a manager intervention.

Clear actionable all-in-one dashboard...

Everything you need in one page

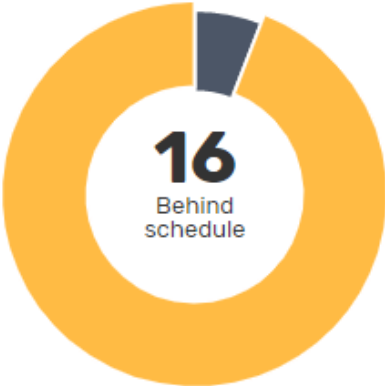
ROUTINE TASKS

MY ACTIONS ?

- Add new users
- Import Users
- Start Group Training
- Add to training
- Pause Training
- Resume Training
- Download report

STUDENTS NEED ATTENTION ?

WHO NEEDS MY ATTENTION? ?



16
Behind schedule

Can not finish on time	1
Significantly behind schedule	0
Behind schedule	16
Going well	0
Ahead of schedule	0

LICENSE CONTROL ?

USERS & LICENSES ?

Studying	14
Completed	0
Unassigned	130
Paused	3
Total users	147

10 Total number of available licenses	30 Total number of licenses
---	---------------------------------------

Report just in 1 click

You can download report anytime from the admin's main page just in 1 click

USERS' PERFORMANCE REPORT EXAMPLE

Total users	1500		
Study status for each one:			
Unassigned	17		
Studying	1483		
Paused	0		
Completed	0		
Archived	0		
Licenses in Use	1483		
Who needs my attention?			
Study Speed	Number of Users	Reasons For Falling Behind	Number of Users
Total Studying	1483		
Ahead of schedule	31		
Going well	1386		
Behind schedule	58	Do not take tests	3
		Fail tests	55
		Never entered the platform	0
Significantly behind schedule	8	Do not take tests	6
		Fail tests	2
		Never entered the platform	0
Can not finish on time	0	Do not take tests	0
		Fail tests	0

PLATFORM INTERFACE EXAMPLE

MY ACTIONS ?

Add new users

Import Users

Start Group Training

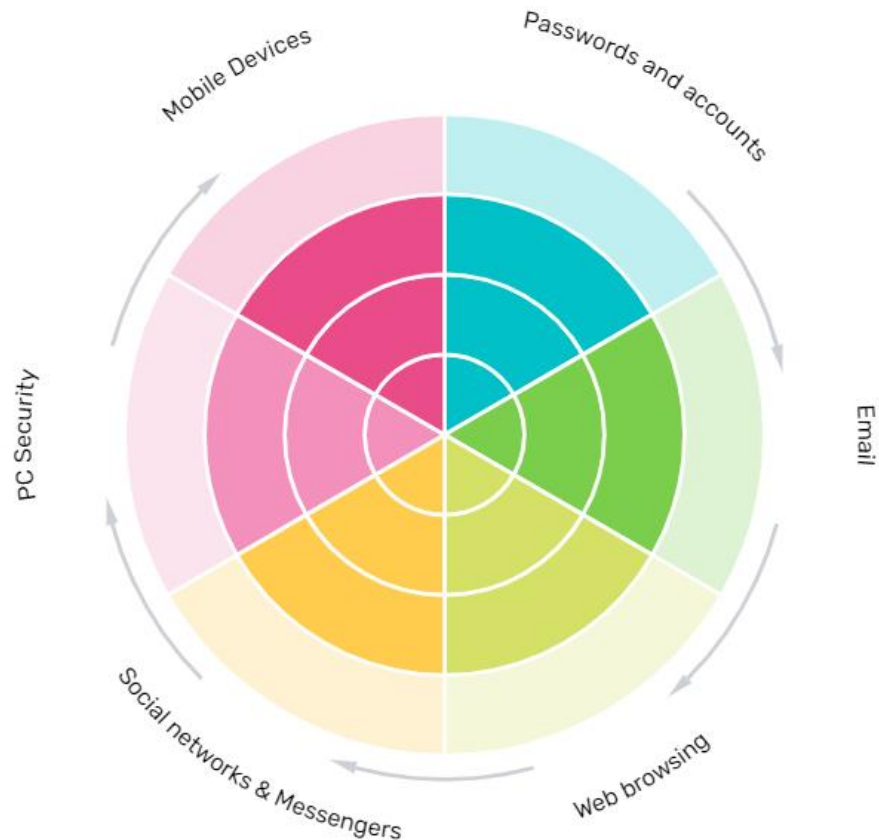
Add to training

Pause Training

Resume Training

Download report

Kaspersky Automated Security Awareness Platform (ASAP)



As 350 lessons structured by 3 levels of complexity and 6 topics:

- Passwords and accounts
- Email
- Web browsing
- Social networks & messengers
- PC Security
- Mobile devices

Various phishing templates

Available in 9 languages

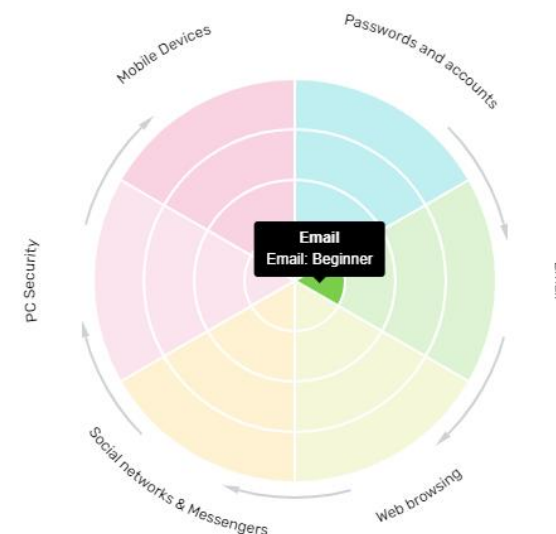
350* specific skills

Kaspersky Lab's expertise and experience in cybersecurity are at the heart of creating a **cybersafe behavior model** - skills an employee must have so that, through ignorance or negligence does not harm the company

Hundreds of lessons covering 1 or more skills, 350 skills total*

** By the end of 2019; 300 at the moment*

LESSON'S INDEX EXAMPLE



● Lesson

- What endangers my email?
- Whom can you tell your email password?
- What should I do if my email is hacked?
- What kinds of passwords should I use for my email accounts?
- Why is it important to use different passwords for your personal and work email accounts?
- What kinds of information should not be sent over email?
- What should you look out for if you're asked to enter your email password?
- Can I open any link from email?
- Are all attachments good to open?
- What should I do about my email accounts today?

Relevant for everyday employees' job

- Learn what you need to know, based on the role and risk profile
- Practical skills in every lesson that can be put in immediate use

LESSON'S CONTENT EXAMPLE

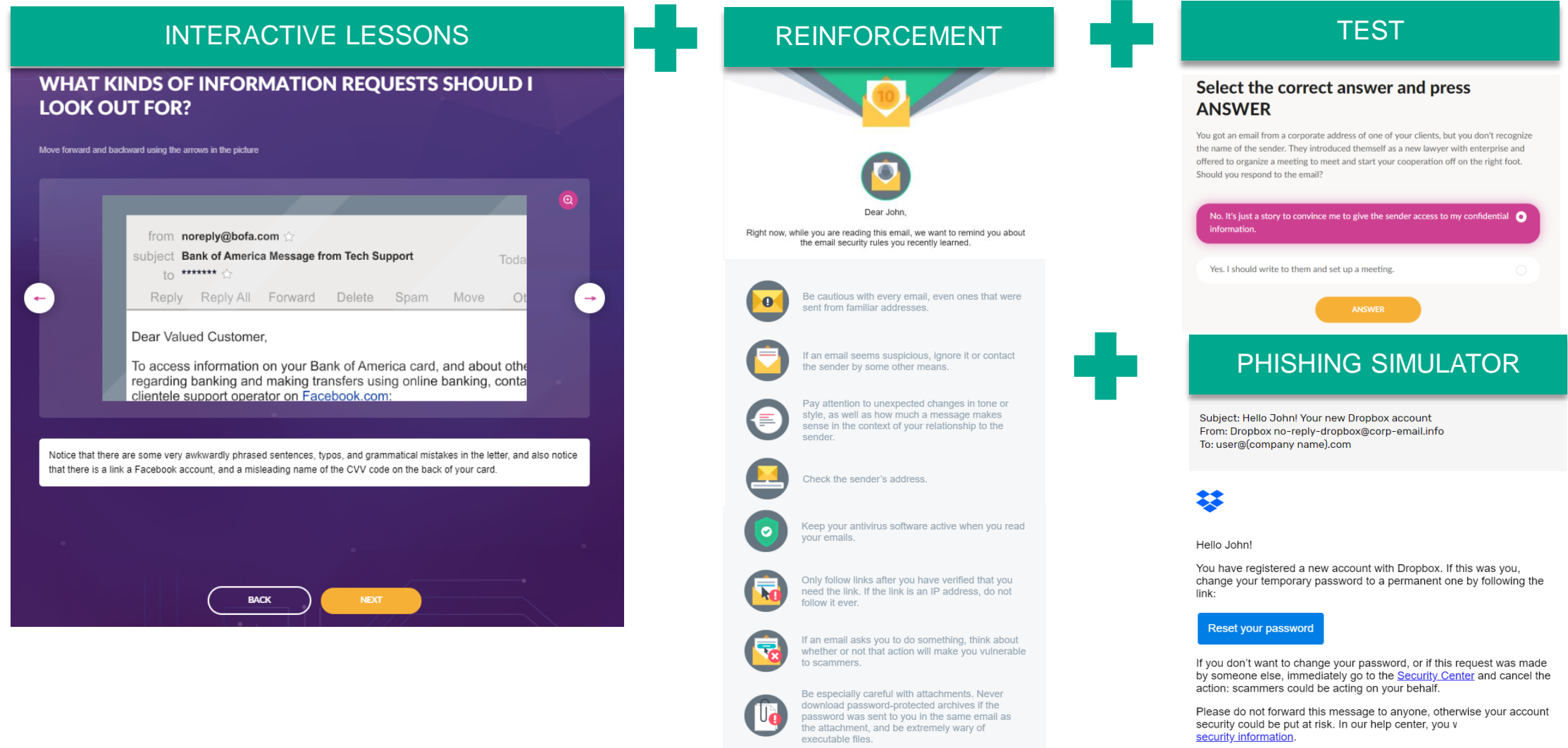
● Lesson

- Can viewing a webpage be dangerous?
- Do I need to update OS and browser?
- What is the right way to update my software?
- Which downloads to accept?
- What kind of browser extensions to install?
- Which sites deserve leaving immediately?
- How to respond to security warnings?
- Why and how to check files you are downloading
- How can I be safer when surfing the web?



Continuous training process

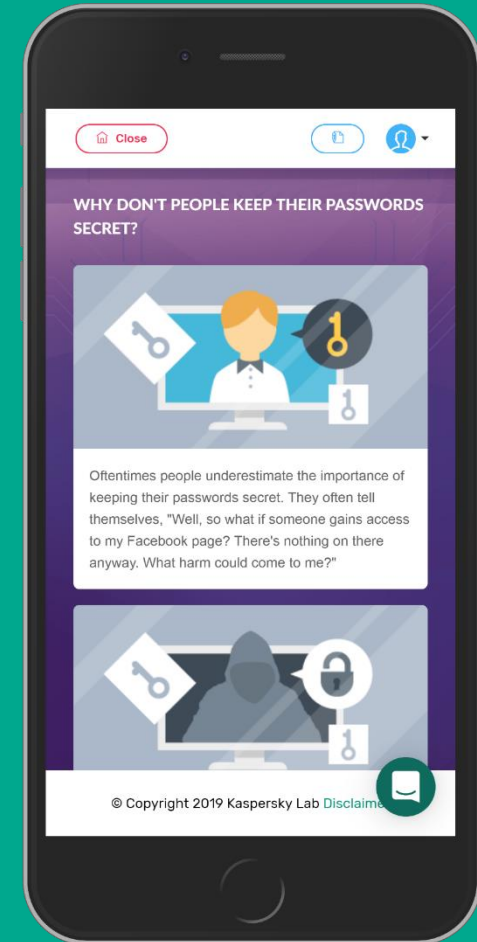
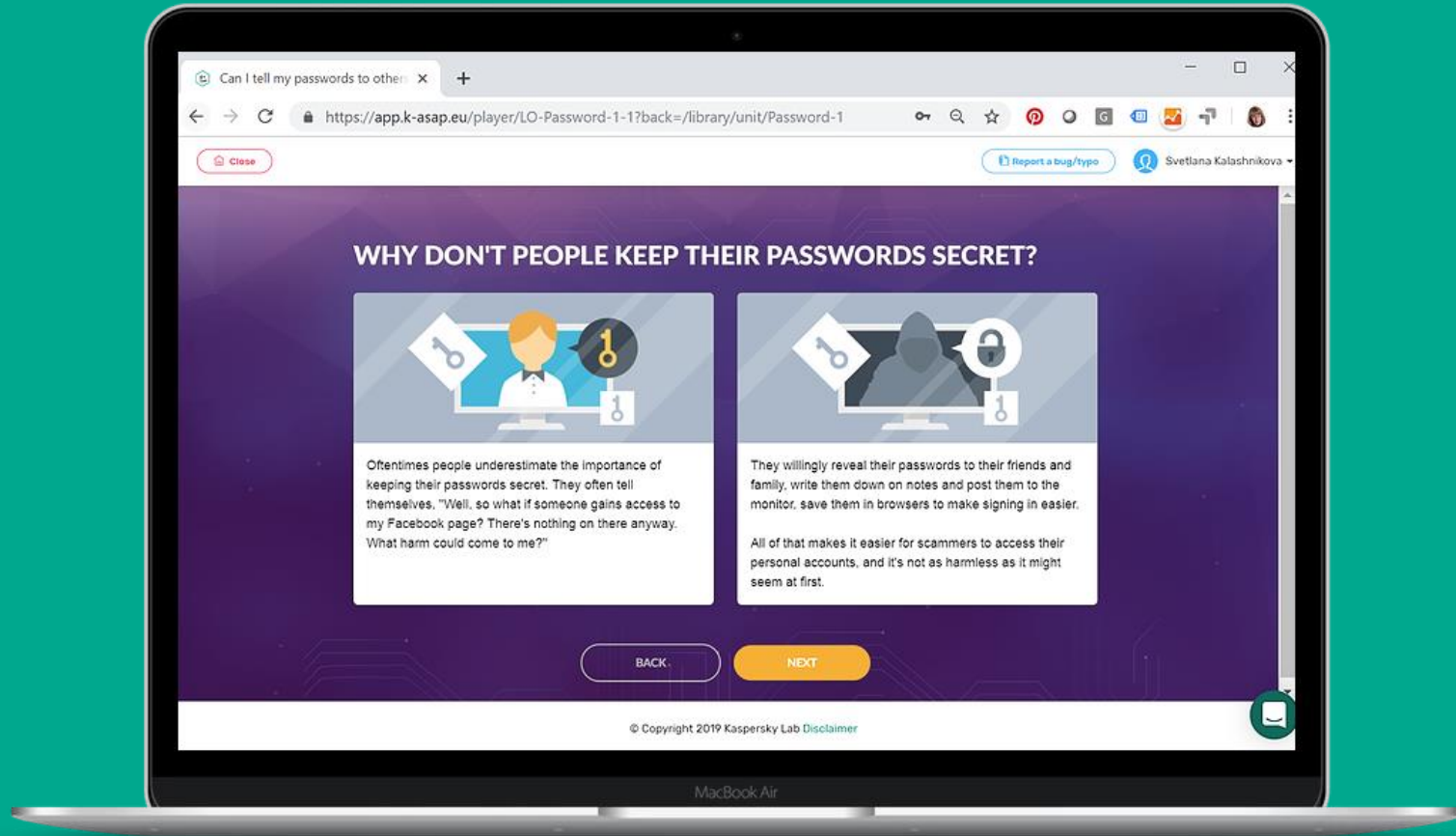
Different training elements complement each other developing the skill



kaspersky

ASAP additional benefits

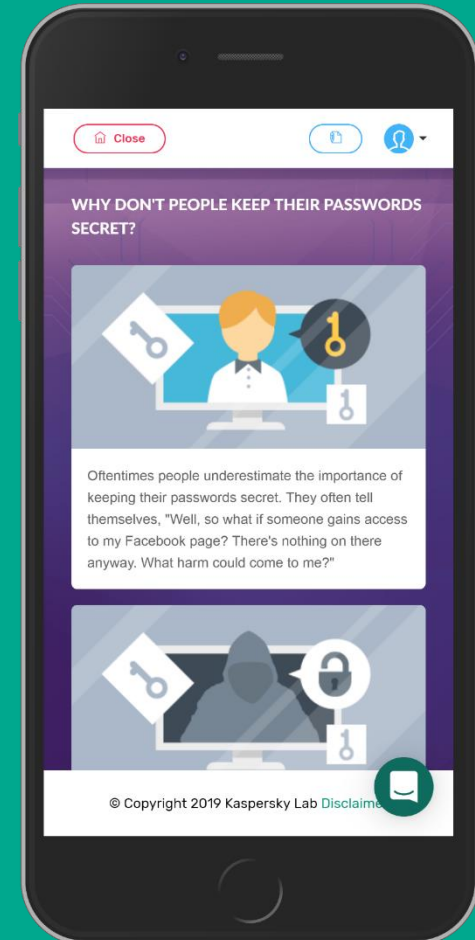
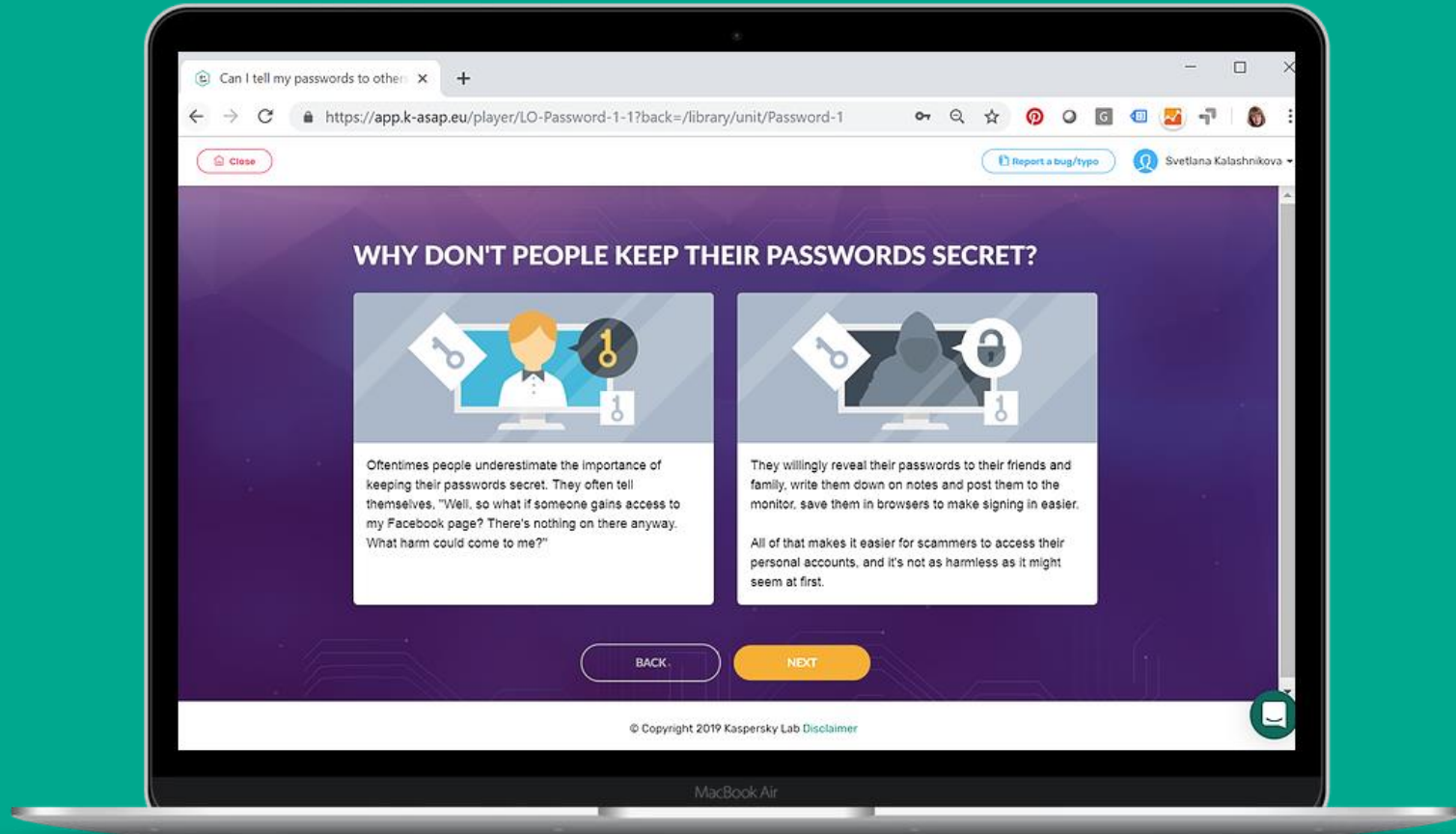
Training materials are adaptive / mobile ready: study from any device



ASAP supports MSP model

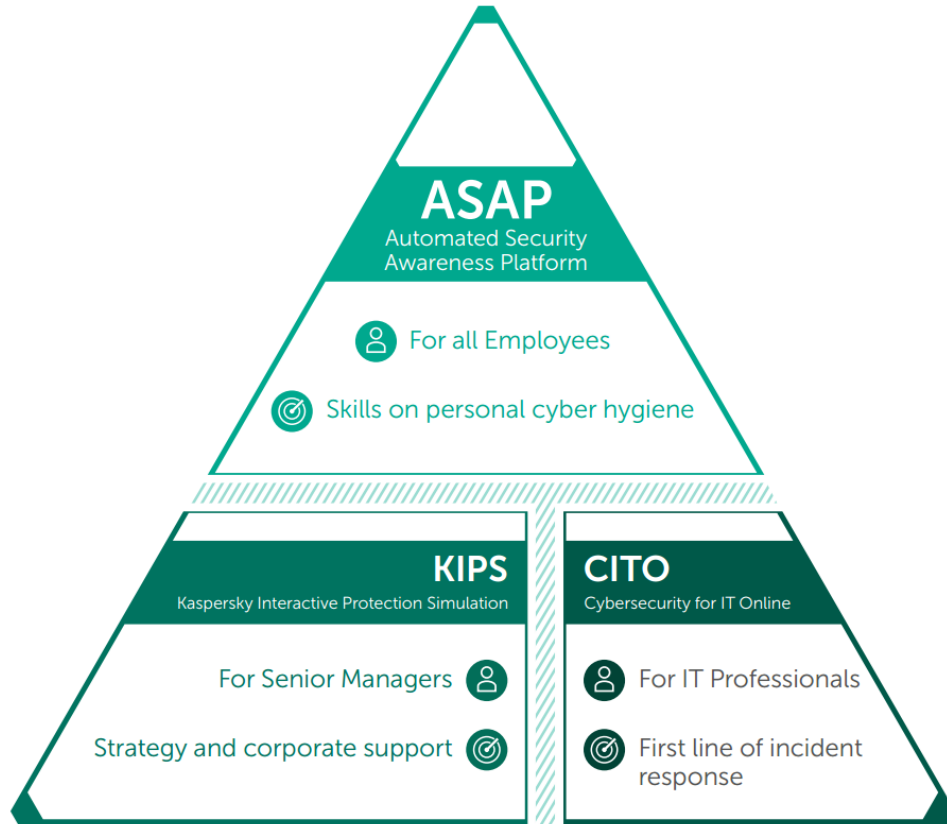
- **License starting from 5 users**
- **Manage multiple companies under one account**
- **Shared license pool**
- **Monthly payments based on the cumulative license number**
 - ✓ Flexible — no need to credit your customers
 - ✓ Scalable — you can easily add or reduce the number of licenses your customers need
 - ✓ Pay-as-you-go — customers are invoiced at the end of a month, based on the number of ordered licenses
- **Multiple administrators with rights management (*)**

Try it on: k-asap.com





Kaspersky Security Awareness - CITO



**Efficient training for general
IT specialists**

<https://cito.cloudapp.net/>

Reduces
the number of human
errors by up to

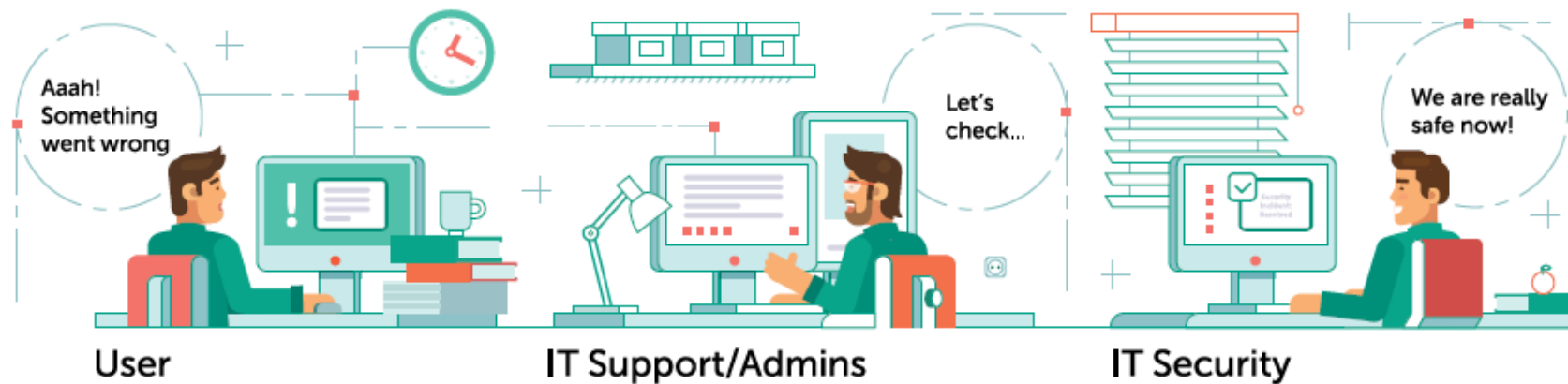
80%

IT Specialists – new role and responsibilities – Now and then

Now



Should be



Cybersecurity For IT Online

Training outcome

- Critical thinking on IT Security
- Knowledge of hacker's tools and techniques
- Basic skills of threat analysis
- Knowledge how to help Security department during incident response

Training audience

- Service desks
- IT/ network professionals
- IT Security
- Local administrators and other technically advanced staff

4 modules, ~ 30 practical exercises

Malicious Software

Verification of existence or absence of incident related to malware

#Processhacker, #Autoruns, #Fiddler,
#GMER

Potential unwanted Programs

Working with event monitors of the systems and sandboxes. Using statistical engines (virustotal). Removing PuPs

#ProcessMonitor, #Cuckoo, #VirusTotal

Phishing Incident Response

Phishing emails lookup. Verification of the incident related to phishing. OSINT

#ExchangeComplianceSearch , #Robtex,
#Whois, #GoogleDorks

Investigation Basics

Incident localization, data collection, collecting digital evidence, log and timeline analysis

#EventLogExplorer, #Autopsy, #FTK-Imager

Cybersecurity For IT Online

Awareness => incident response training

Target audience: IT generalists (IT support, service desks, etc)

The screenshot shows a training interface for 'Malware Hunting'. On the left, there is a sidebar with instructions for a 'BASIC HEURISTICS' exercise. The main area displays a remote administration session for IP 192.168.152.2, with a 'Process Hacker 2' window open. The window shows a list of processes with columns for Name, PID, CPU, I/O T..., Privat..., User..., Description, Verified Signer, and Verificat... The process 'task...' (PID 1792) is highlighted in blue.

Name	PID	CPU	I/O T...	Privat...	User ...	Description	Verified Signer	Verificat...
winlogon.exe	468			19.9 KB	NT AU...	Windows Logon Ap...	Microsoft Windows	Trusted
wininit.exe	404			41.9 KB	NT AU...	Windows Start-Up ...	Microsoft Windows	Trusted
services.exe	504			200.2 ...	NT AU...	Services and Contro...	Microsoft Windows	Trusted
svchost...	628			34.2 KB	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
task...	1792			52.5 KB	WIN-6...	Task Scheduler Engi...	Microsoft Windows	Trusted
Wmi...	3580			282.6 ...	NT AU...	WMI Provider Host	Microsoft Windows	Trusted
lsmon.exe	692			42.7 KB	NT AU...	Local Session Mana...	Microsoft Windows	Trusted
sppsvc...	724			220.3 ...	NT AU...	Microsoft Software ...	Microsoft Windows	Trusted
dllhost...	772			114.5 ...	NT AU...	COM Surrogate	Microsoft Windows	Trusted
svchost...	864			1.2 MB	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
dllho...	1544			39.9 KB	WIN-6...	COM Surrogate	Microsoft Windows	Trusted
svchost...	904	0.1		322.4 ...	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
svchost...	1008	0.1		94.6 KB	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
svchost...	1076			508.4 ...	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
spoolsv...	1224			225.7 ...	NT AU...	Spooler SubSystem...	Microsoft Windows	Trusted

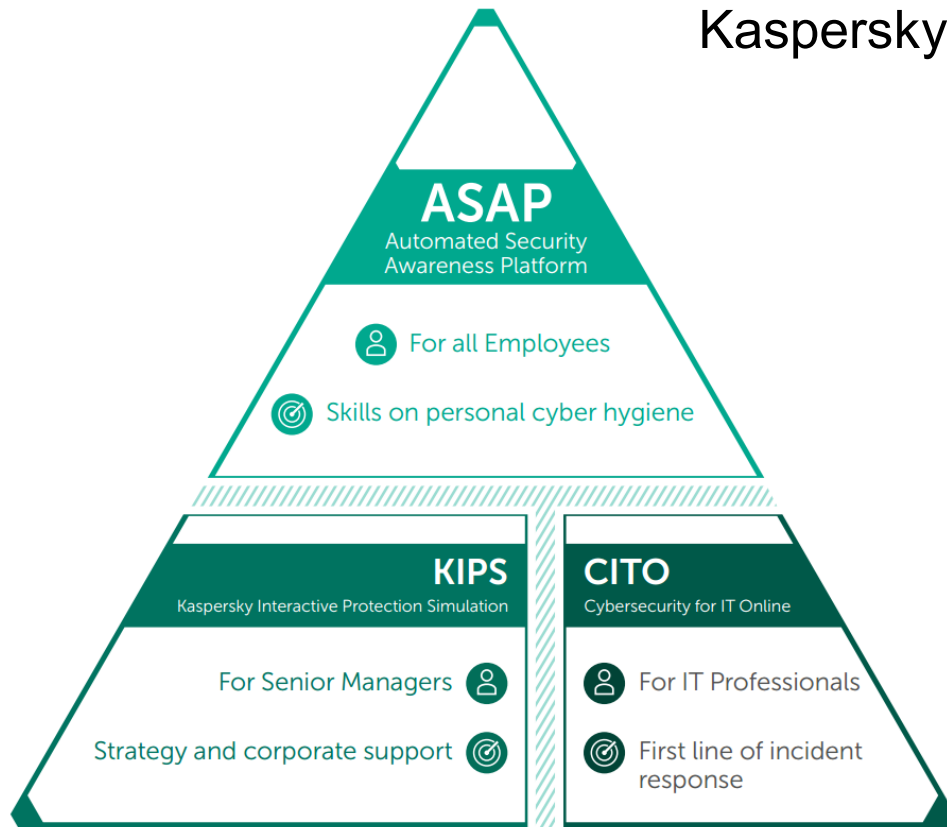
Security Awareness Online Training for IT people

- Empower “first line of defense” in the cyber incident response
- Decrease the number of incidents caused by misconfiguration mistakes
- Develop the critical thinking for IT teams on cybersecurity



Kaspersky Security Awareness - KIPS

Kaspersky Interactive Protection Simulation



Reduces
the number of human
errors by up to

80%

Cybersecurity today – lost in a ‘corporate bermuda triangle’



CEO

Does not see how cybersecurity spendings relate to Revenues



SECURITY

Focus on protecting the confidential information
Many security controls are under IT management



IT & BUSINESS MANAGERS

Focused on business efficiency, automation, new technologies

Mutual understanding and daily attention to cyberthreats between these 3 are crucial to successful cybersecurity in the modern business

KASPERSKY INTERACTIVE PROTECTION SIMULATION

- Senior managers

For IT, Business and Security – strategy simulation for cybersecurity decision-makers.

● Fun, engaging and fast (2 hours)

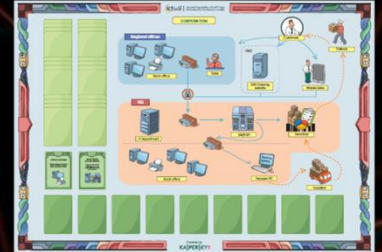
● Team-work builds cross-divisional co-operation

● Competition fosters initiative & analysis skills

● Gameplay develops an understanding of cybersecurity measures and strategy

● Teams compete at running a simulated enterprise and earning money

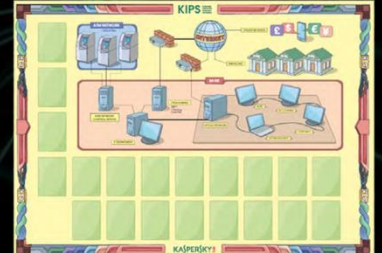
Corporate



Industrial



Financial



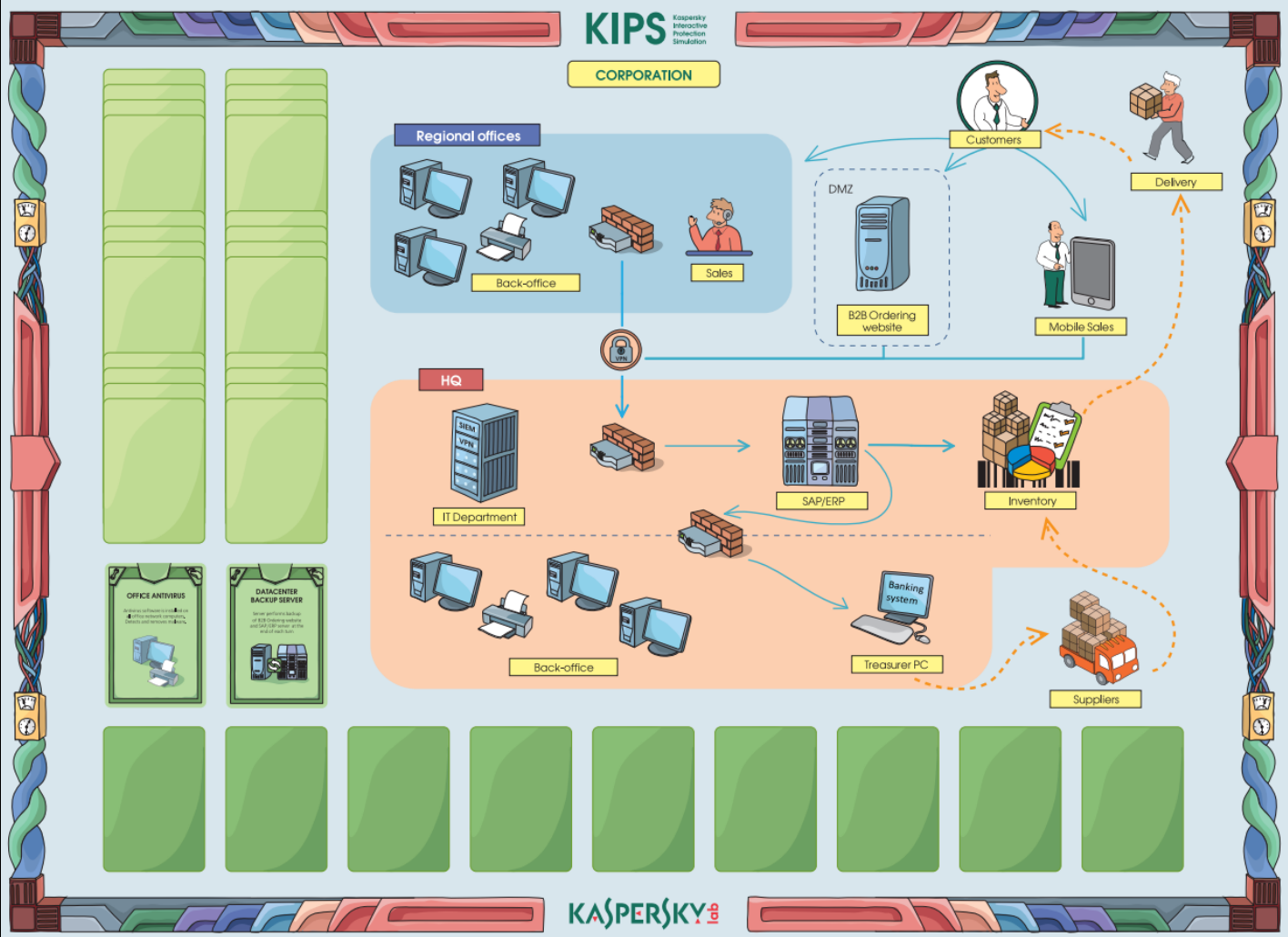
Government



KIPS Kaspersky
Interactive
Protection
Simulation

KASPERSKY

KASPERSKY INTERACTIVE PROTECTION SIMULATION



Game Board



Web Console



Action Cards

Training process overview

Game rules and housekeeping explained

Trainer tells about the game and its rules, trainees listen and follow slides on a big screen or via WebEx.

20 minutes

KIPS is played by teams

Players read news and decide on actions by choosing cards according to their strategy and budget and time limitations.

After each turn a rating is updated.

Trainer facilitates, encourages and controls timing.

40 - 50 minutes

Ideal scenario unveiled and lessons learned

Trainer tells about threats met by players, unveils the ideal scenario and draw participants to conclusions and practical takeaways.

20 - 30 minutes

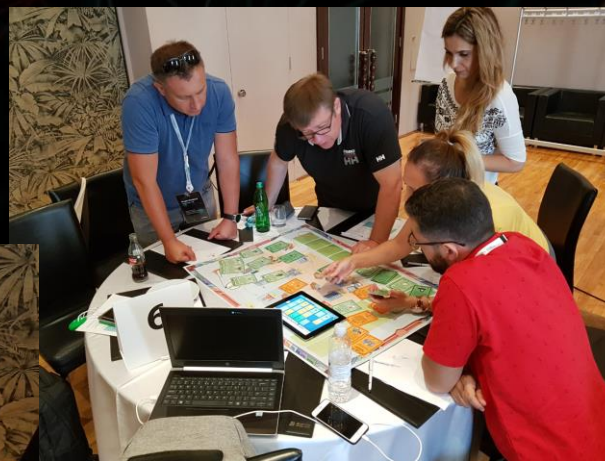
Results announced – congratulations to winners!

Participants can be invited to share results and photos on social media.

10 - 20 minutes

Overall 1,5 – 2 hours

VYZKOUŠEJTE TO S NÁMI....



ComputerWeekly

"The Kaspersky Interactive Protection Simulation was a real eyeopener and should be made mandatory for all security professionals."

www.computerweekly.com/feature/Interactive-cyber-attack-a-dangerous-game



KASPERSKY

A na závěr...

Kybernetické hrozby jsou **všude okolo nás..**

Nemusíte být cílem útoku, aby jste se stali jeho obětí..
Chraňte sebe i svou organizaci.



kaspersky

Děkuji Vám !