



Modern technologies for protection against advanced threats

kaspersky

New reality

Constant pressure Evolution of threats Import substitution

Interactive cyber threats map



<https://cybermap.kaspersky.com/>



Increase in the number of attacks
Frequent outbreaks of various cyber threats



Cyber aggression
Russia is number 1 in the world among attacked countries



Cyber threats for everyone
Companies of all sizes are susceptible to attacks

Threat evolution



Ransomware trends

New technical features

Cross-platform ransomware to be as adaptive as possible, self-propagating capabilities

Code adoption from other families

To attract even more affiliates. For example, Lockbit supports 3 different versions at the same time

0-days

Crimeware actors can afford to buy 0days. Usually only APT actors used them

Nokoyawa ransomware attacks with Windows zero-day

RESEARCH 11 APR 2023

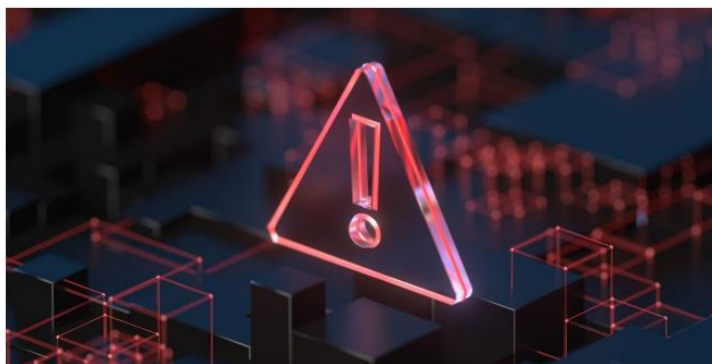
⌚ 6 minute read



QakBot attacks with Windows zero-day (CVE-2024-30051)

SOFTWARE 14 MAY 2024

⌚ 1 minute read



GREAT WEBINARS

13 MAY 2021, 1:00PM

 **GReAT Ideas. Balalaika Edition**

BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM

 **GReAT Ideas. Green Tea Edition**

JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU,
VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA,
MOTOHIKO SATO

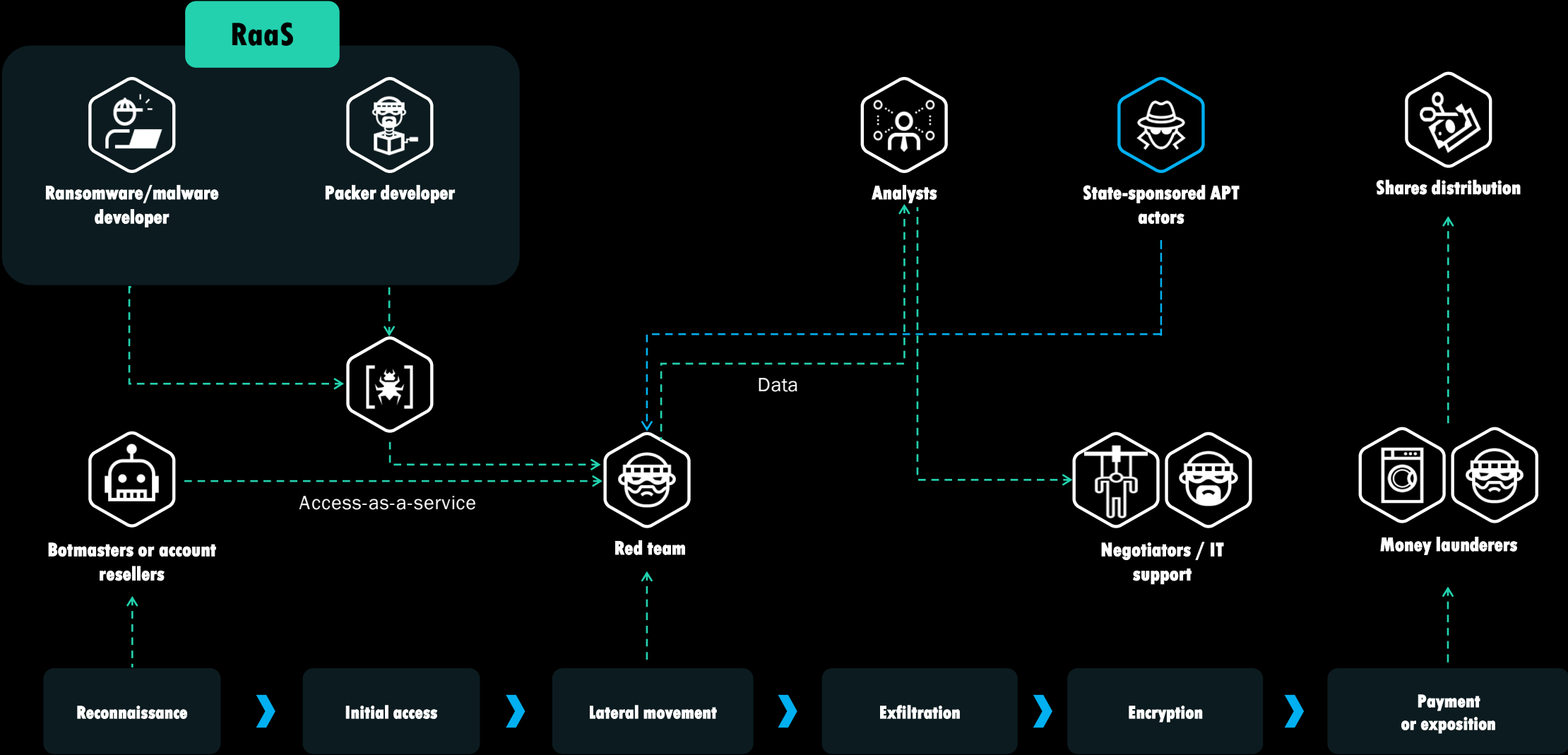
17 JUN 2020, 1:00PM

 **GReAT Ideas. Powered by SAS:**
malware attribution and next-gen IoT

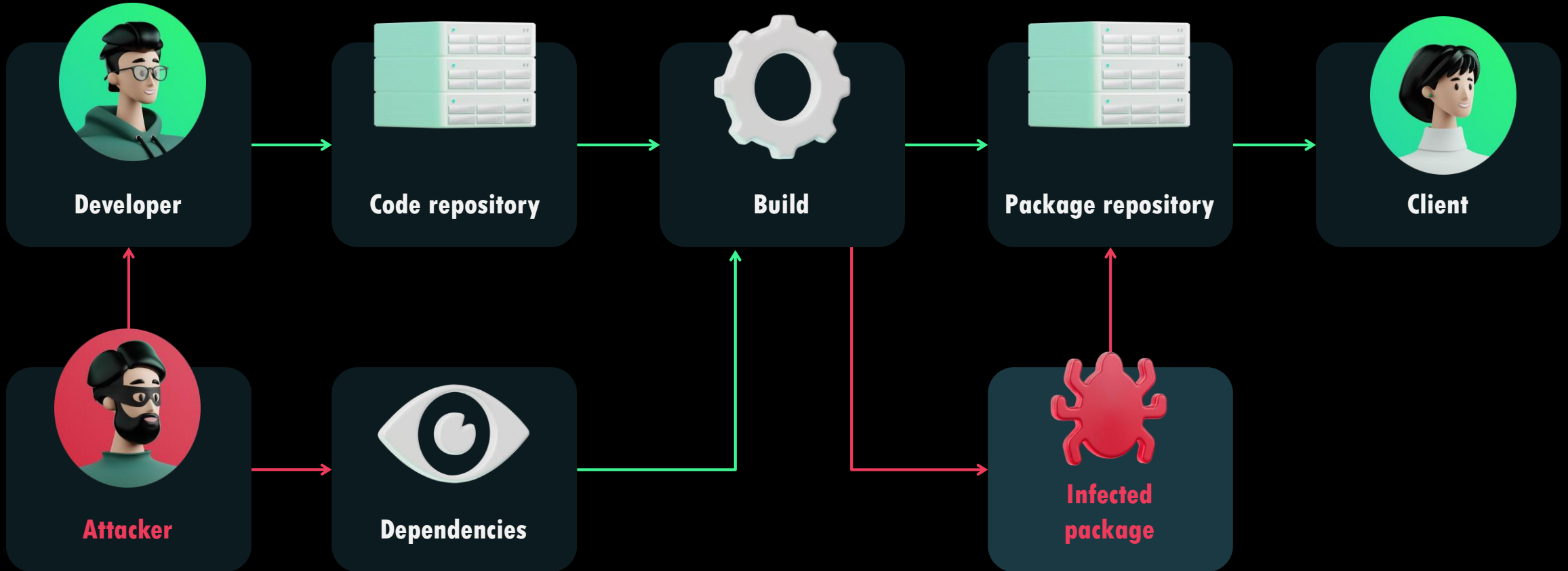
<https://securelist.com/nokoyawa-ransomware-attacks-with-windows-zero-day/109483/>

<https://securelist.com/cve-2024-30051/112618/>

Ransomware “business” ecosystem



Supply chain attacks



Supply chain attacks

241 npm and PyPI packages caught dropping Linux cryptominers

By Ax Sharma


August 19, 2022 04:11 PM 0




NPM supply-chain attack impacts hundreds of websites and apps

By Sergiu Gatian

July 5, 2022 01:55 PM 2



SECURELIST



INCIDENTS

LofyLife: malicious npm packages steal Discord tokens and bank card data

28 JUL 2022 1 minute read

Python library 'ctx' uploads secrets to a Heroku en

Heavily downloaded PyPI package 'ctx' has been compromised sometime this published versions exfiltrating your environment variables to an external ser

'ctx' is a minimal Python module that lets developers manipulate their dictio variety of ways. The package, although popular, had not been touched since 2 seen by BleepingComputer. However, newer versions emerged starting May 1 contained malicious code:


ctx 0.2.2

pip install ctx

Released May 15, 2022

Not just an infostealer: Gopuram backdoor deployed through 3CX supply chain attack

APT REPORTS 03 APR 2023 4 minute read



GREAT WEBINARS

13 MAY 2021, 1:00PM

GReAT Ideas. Bala

BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM

GReAT Ideas. Gree

JOHN HULTQUIST, BRIAN BARTH

SUGURU ISHIMARU, VITALY KAM

YUSUKE NIWA, MOTOHIKO SATO

XZ backdoor story – Initial analysis

INCIDENTS 12 APR 2024 12 minute read



// AUTHORS

GREAT

On March 29, 2024, a single message on the Openwall OSS-security mailing list marked an important discovery for the information security, open source and Linux communities: the discovery of a malicious backdoor in XZ. XZ is a compression utility integrated into many popular distributions of Linux.

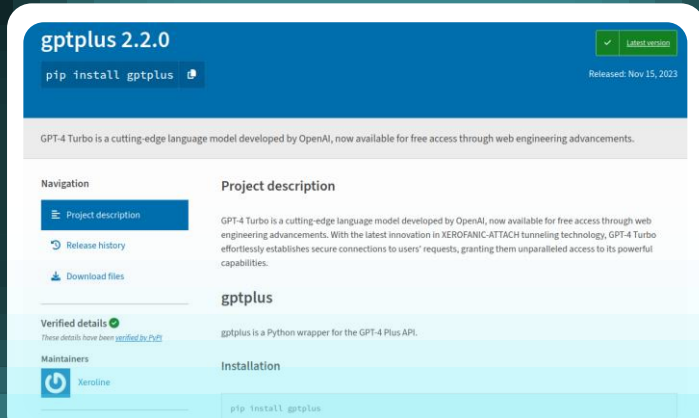
Two more malicious Python packages in the PyPI

INCIDENTS 16 AUG 2022 4 minute read



THUNDER

Malicious packages for accessing ChatGPT



Kaspersky uncovers year-long PyPI supply chain attack using AI chatbot tools as lure

November 20, 2024

For a year, JarkaStealer was distributed on the PyPI repository under the guise of AI tools

Both packages were downloaded more than 1.7k times by users from 30 countries (including India)

The malware steals browser data, takes screenshots, and collects Telegram sessions

General information about incidents in 2024

57,5%: Operating Systems as the most prominent software category for publicly available exploits targeting vulnerabilities



Initial access

39,2%

Public-facing applications

31,4%

Valid accounts

12,8%

Trusted relationships

Other constant threats to companies: also important:

- Phishing (9.8%)
- External remote services (3.9%)



Impact

41,6%

Encrypted data

16,9%

Data leakage

12,2%

Persistence installed for future impact

Industries

23,5%

Industrial

16,3%

Government

13,3%

Financial

7,2%

IT companies

Regions

50,6%

CIS

15,7%

Middle East

10,8%

Europe

10,2%

Americas

7,3%

APAC

In the wild 0-days caught and reported by Kaspersky over the past 10 years

10

32 zero-days vulnerabilities



CVE-2014-0497
CVE-2014-0515
CVE-2014-0546
CVE-2016-4171
CVE-2017-11292



CVE-2014-4077	CVE-2019-0859
CVE-2015-2360	CVE-2019-1458
CVE-2016-0034	CVE-2020-0986
CVE-2016-0165	CVE-2020-1380
CVE-2016-3393	CVE-2021-28310
CVE-2018-8174	CVE-2021-31955
CVE-2018-8453	CVE-2021-31956
CVE-2018-8589	CVE-2021-40449
CVE-2018-8611	CVE-2023-28252
CVE-2019-0797	CVE-2024-30051



CVE-2019-13720
CVE-2024-4947
CVE-2025-2783 New



CVE-2023-32434
CVE-2023-32435
CVE-2023-38606
CVE-2023-41990

Kaspersky GREAT discovers sophisticated Chrome zero-day exploit used in APT attacks

11

New

Who was targeted?

Media outlets

Educational institutions

Government organizations

Discovery & Mitigation

Kaspersky's EDR technology detects the intrusion.

Google released a patch on March 25, 2025 to fix the vulnerability.



Phishing Email Sent

- Email contains a malicious link.
- Attackers send phishing emails disguised as invitations from the Primakov Readings forum.



Victim Clicks the Link

- The victim opens the link in Google Chrome.
- No further interaction is needed for infection.



Zero-Day Exploit Triggers

- Exploits a previously unknown Chrome vulnerability.
- Bypasses Chrome's sandbox by leveraging a logical flaw between Chrome and Windows.



Malware Download & Execution

- Payload is delivered and executes stealthily on the victim's machine.
- Establishes persistence for long-term access.



Espionage & Data Exfiltration

- Malware collects sensitive information from the compromised system.
- Data is exfiltrated to attackers' command and control (C2) servers.



Attackers Maintain Access

- Attackers can deploy additional payloads or move laterally within the organization.
- Ongoing monitoring and data theft.

What should companies do in the new information security realities?

13

First of all,
protect
yourself from
mass threats

Secondly, build
protection
against complex
threats

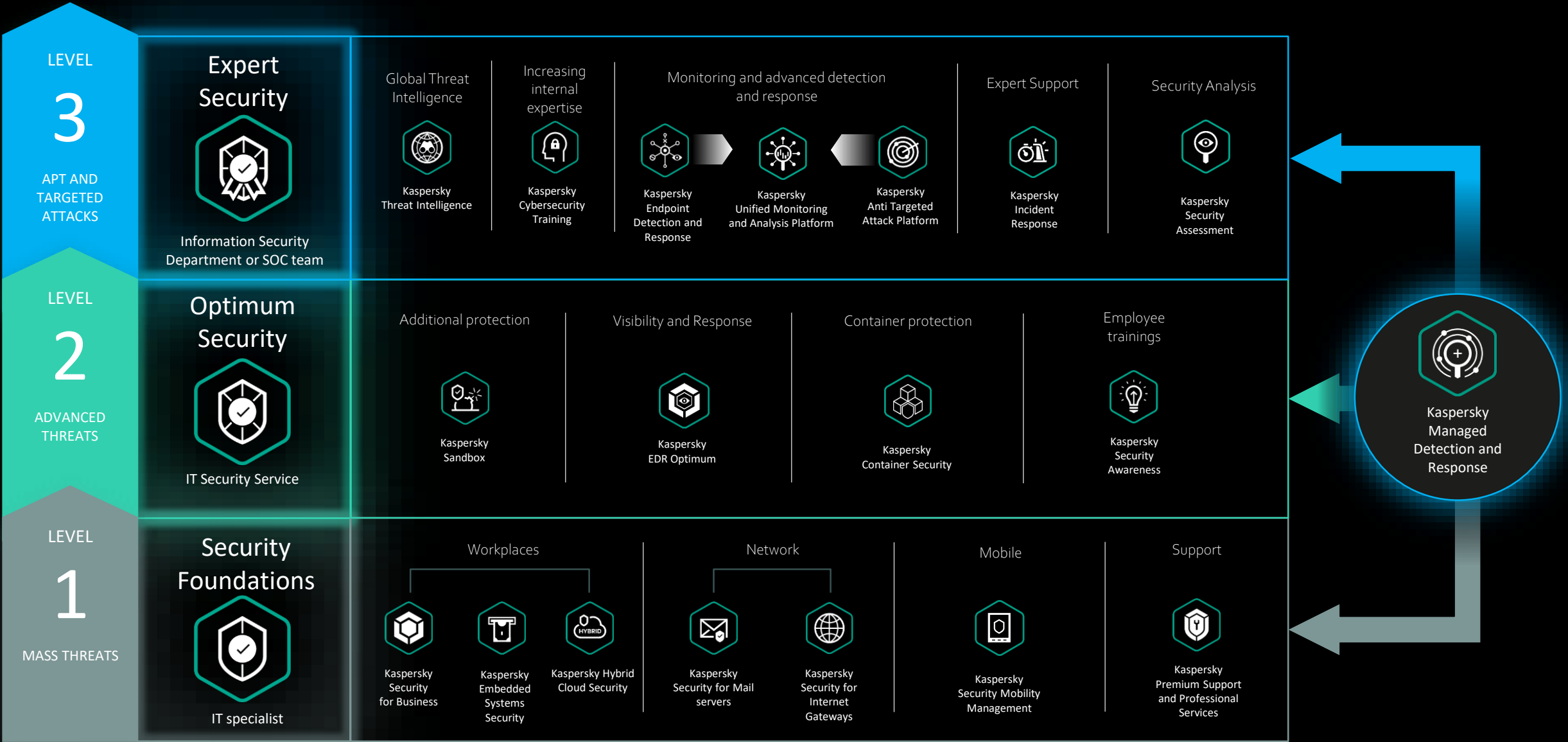


On your own: gradually
or immediately

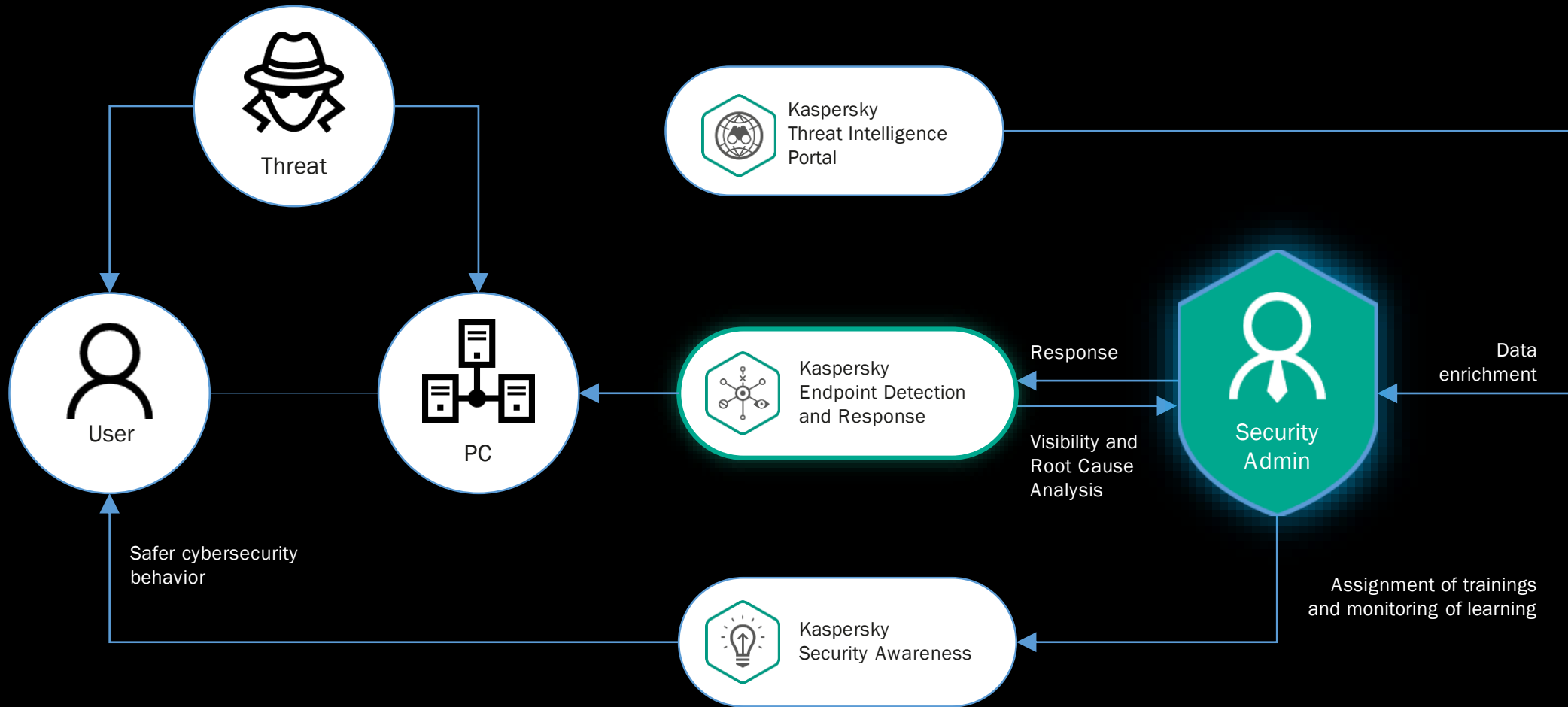


Select managed
protection

Kaspersky Lab Portfolio



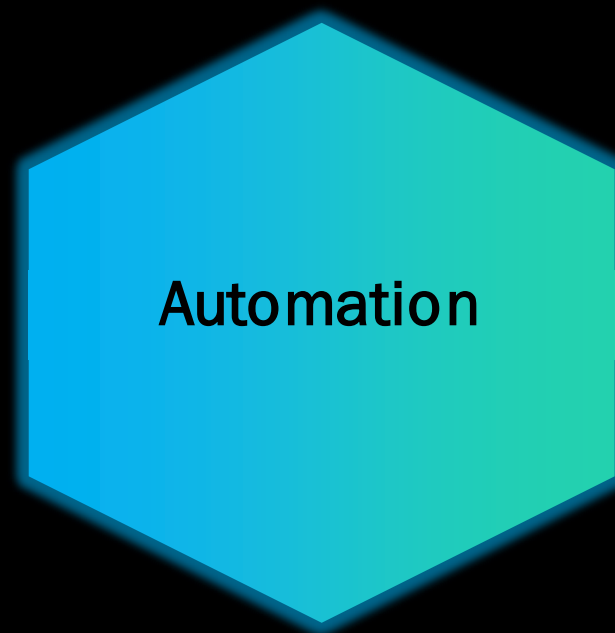
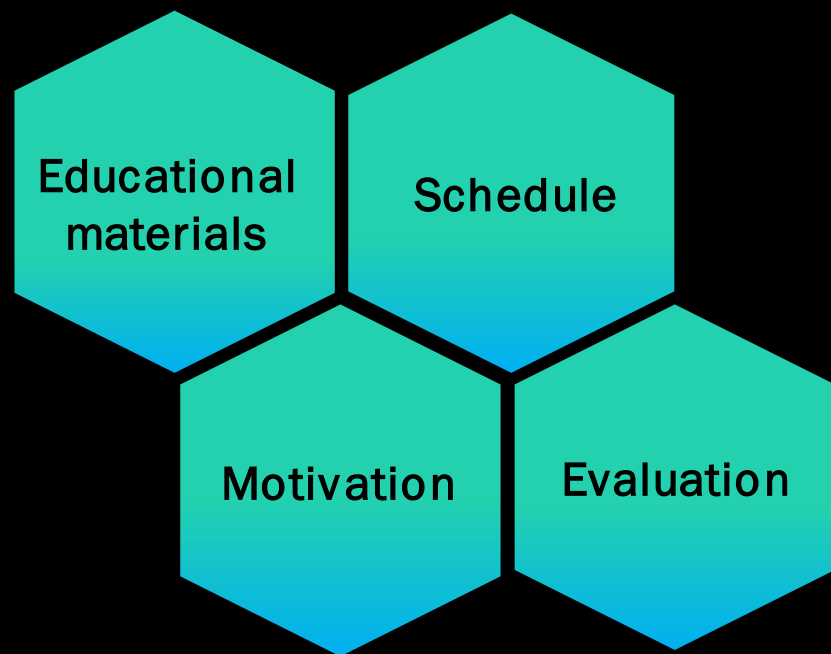
Solution for preventing and combating threats on multiple levels



Kaspersky Automated Security Awareness Platform

A solution that combines training efficiency and ease of management –

www.k-asap.com/ru



Our path to an information security and XDR ecosystem as part of

2016

Release of the KATA platform with the Endpoint sensor component



Kaspersky
Anti Targeted
Attack

The solution already fell into the then non-existent class of XDR solutions

2018

Transformation of Endpoint Sensor in the KATA platform into an EDR class solution



Kaspersky
Endpoint Detection
and Response

The first vendors to talk about the XDR concept

2019

EDR successfully tested by MITRE
Start of development of own SIEM

MITRE

Analysts have embraced
the XDR concept

2020

Commercial release
SIEM KUMA



Kaspersky
Unified Monitoring
and Analysis Platform

2021

SMP Public
Announcement

TI Leaders According to
Forrester



Kaspersky
Single Management
Platform

2022

Brain4Net Acquisition

Kaspersky Symphony
Announcement



Kaspersky
Symphony

Public success stories of KATA and KEDR

France

Weodeo – IT and Telecom, KEDR

Italy

Ansaldo Energia – finance, KEDR

Banca Popolare di Sondrio – finance, KATA

Germany

Levigo systems – IT and Telecom, KEDR

Russia

- MKB – finance, KATA

- Magnit – retail, KATA

- RTI Systems – industrial, KATA

- Government of Rostov Region – government, KATA

Brasil

NEO – finance, KEDR

Kyrgyzstan

Optima Bank – finance, KATA

Austria

Donau Chemie Group – industrial, KEDR



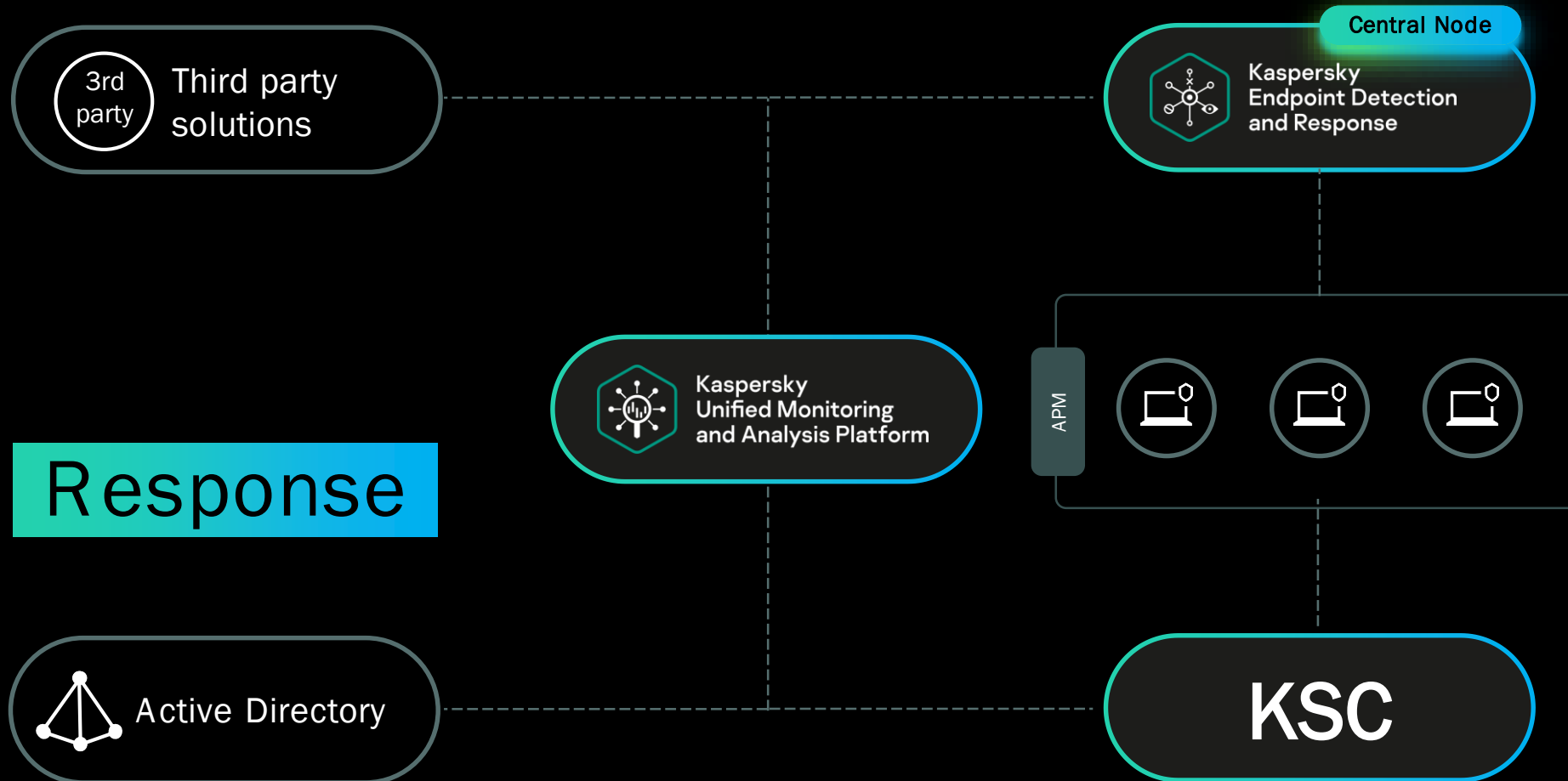
Kaspersky Symphony. Levels of protection

20



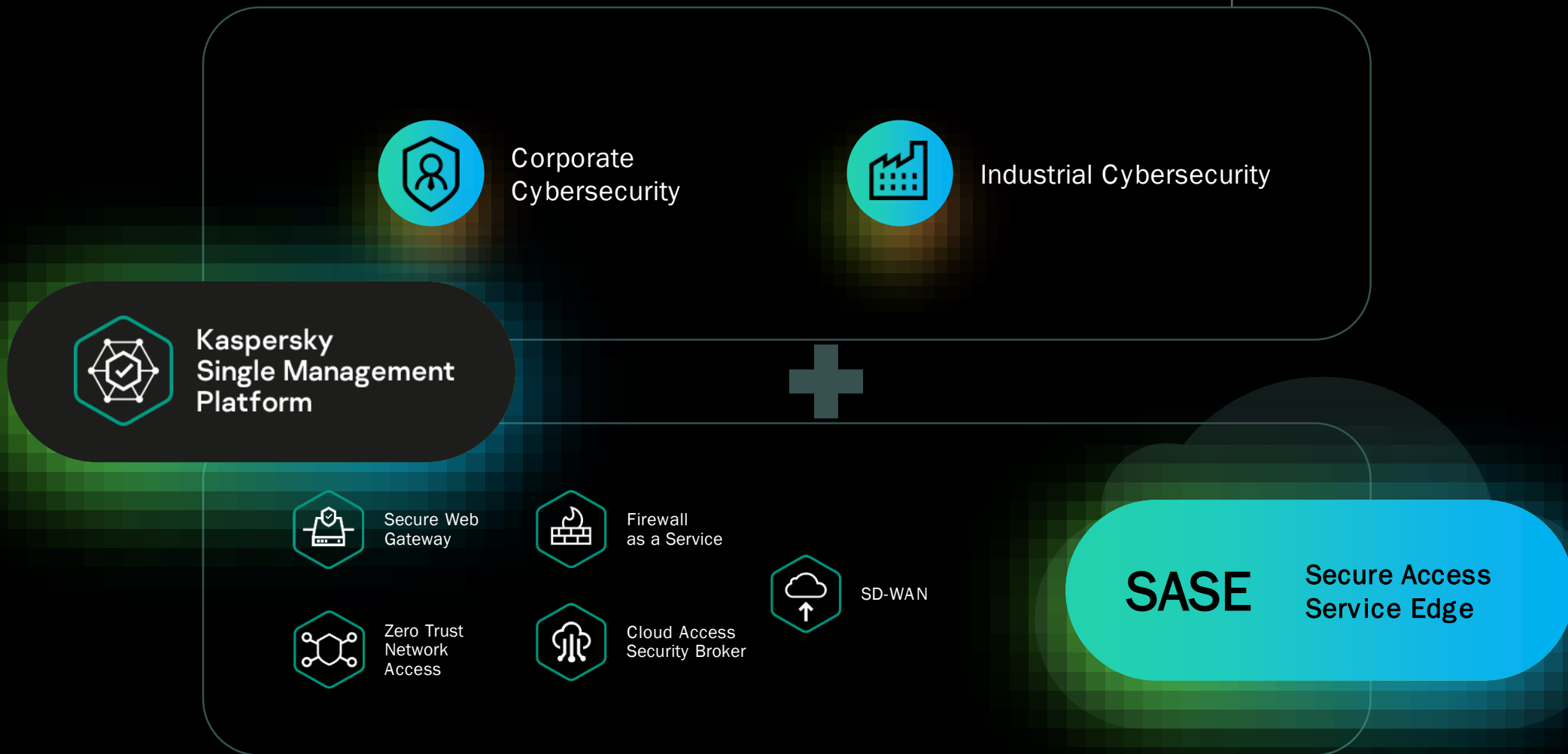
Example: Automated Incident Response

21



Our future plans

22





- Dashboard
- Reports
- Alerts
- Incidents
- Notifications
- Threat hunting
- Incident rules
- Playbook
- Assets

Open

Incident SOC 35425

Brute force Pass-the-hash

Assign to (Escalate to) Change severity Link alert Merge with another incident Leave comment Change status

Summary Timeline Investigation graph MITRE Matrix Alerts (12) Assets (7) Observables (105) Communications History

Incident context details

Alerts

Brute force AD discovery Pass-the-Hash Files discovery Files compressed

KUMA KUMA KUMA KATA KATA Isolate host Threat Intelligence enrichment

Ralph Edwards Playbook: Deploy KEA, nagent Playbook: Deploy KEA, nagent

14:00 20:00 02:00 08:00

Unified

Cross-Product KillChain

Date Added	User	Phase
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Get asset info.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Add observables.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Condition task: check security tools status.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Plain task: install nagent and kea agent.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Create Jira task (patch management).
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Get asset info (osmp-srvl).
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Add observables.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. IoC enrichment.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. IoC search and delete.

Numbers speak more words

~ 5 000

highly qualified specialists

50%

of our employees are R&D specialists

>400 mm

Users use our security solutions

>240 k

companies around the world we protect
from cyber threats

Thank you!

kaspersky

АКТИВИРУЙ
БУДУЩЕЕ