



Kaspersky Industrial
Cybersecurity
Conference 2024

Cyber Range

Automating risk assessment
and testing business
continuity plans



kaspersky

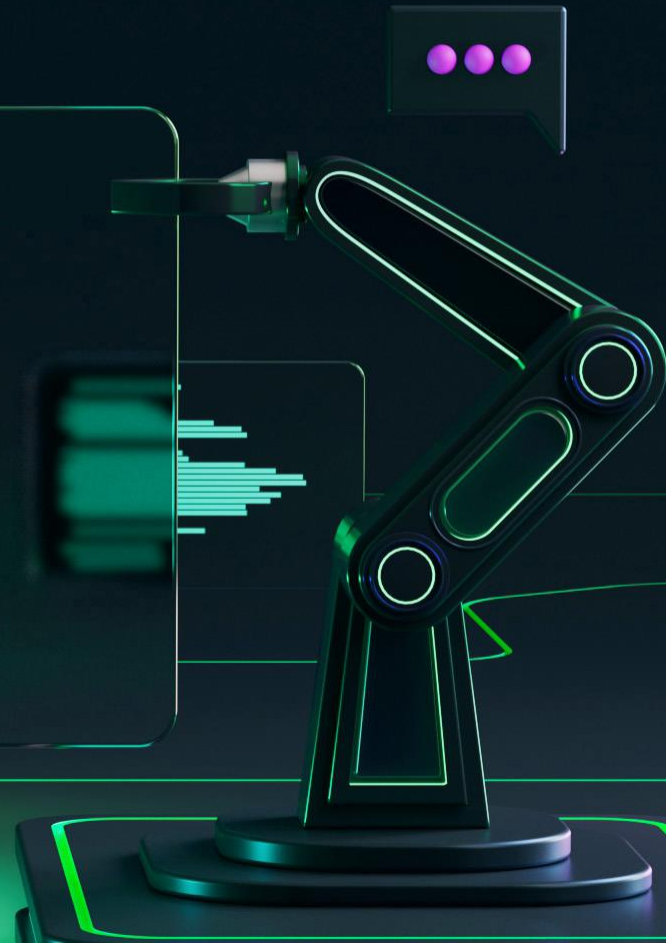


Kaspersky Industrial
Cybersecurity
Conference 2024

Andrey Abashev

Head of cybersecurity methodology
and innovations

kaspersky



Cyber Range

Is a specialized software and hardware complex designed for conducting cybersecurity training and exercises



How Cyber Range can help

in risk assessment:

- Likelihood of cybersecurity threat
- Probability of success of various cyber attack scenarios
- Estimation of downtime and possible damage

and cyber resilience:

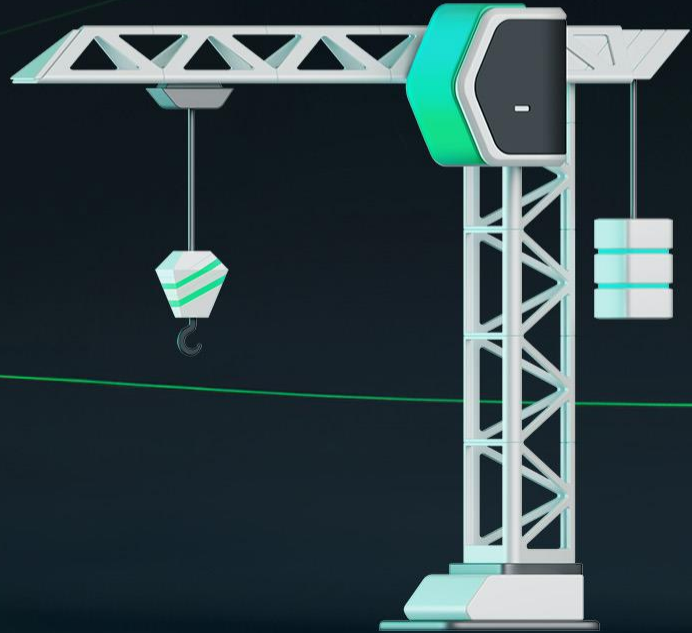
- Assessment of Disaster recovery plans
Practicing actions in the event of an incident and post-Incident analysis
- Identification of weaknesses and understanding vulnerabilities that can be exploited by an attacker



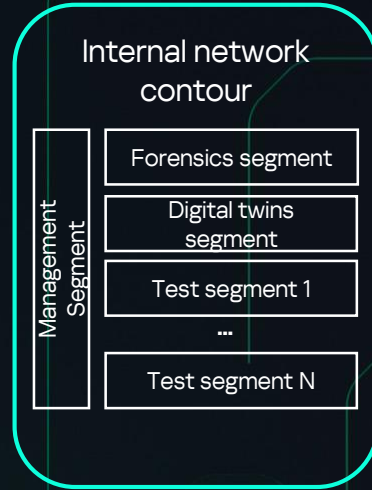
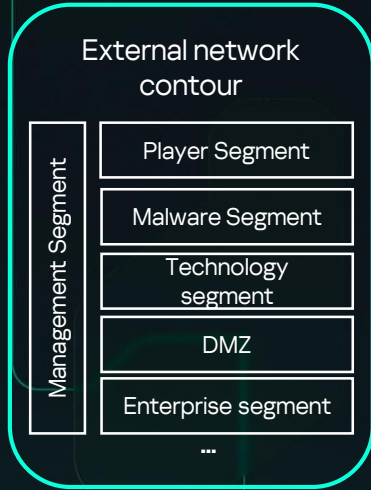
2023
Creating a concept
Design and Development

2023-2024
The first cyber training

2024-2030
Development of additional
cyber training scenarios
and research activities



Scenarios of complex attacks on the infrastructure of an industrial enterprise
Cyber training of blue teams

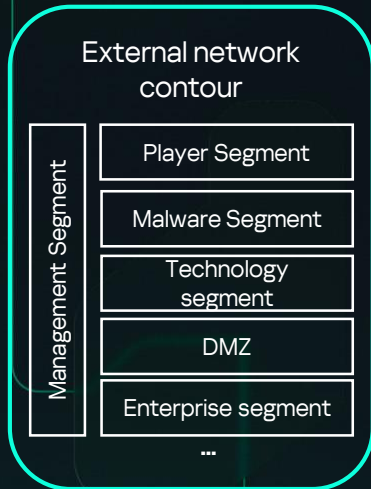


DRP testing

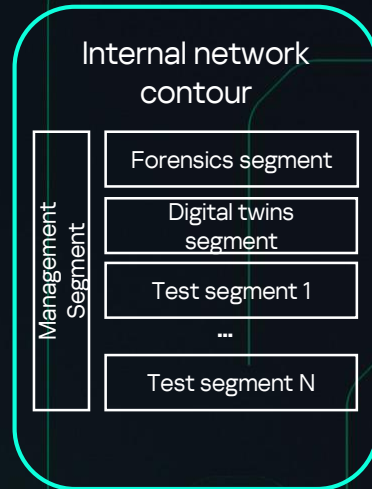
System security research



Scenarios of complex attacks on the infrastructure of an industrial enterprise
Cyber training of blue teams



- Research of new threats
- Cyber exercises (including for external parties)
- Malware research



- Prototypes of real segments
- Testing of corporate information security systems
- Cyber training for employees
- Digital twins

DRP testing

System security research

Attack scenarios on our infrastructure

Automation of cyber training process management and personalized assessment of results

Automated scripts for attack scenarios

Corporate information security systems connected to SIEM-system

Modeling Attacker Behavior with AI



Problems we faced



Complexity of production processes and their specificity



A large number of possible cyber attack scenarios



Lack of standard objects and processes in the company



Import substitution in terms of IT systems and security tools



Need to develop a scoring model to assess the success of test results, participant ratings, etc.



Uniqueness of the architectural landscape of the technological and IT infrastructure



Lack of operational technology (OT) systems, including SCADA systems and Industrial Control Systems (ICS) to perform Cyber Range tasks



How did we do it?

- ✓ Special architectural solutions have been developed for the placement of resources and connections to the Cyber Range
- ✓ Strict prioritization and consistent implementation of new functionality

- ✓ Creating your own digital twins lab
- ✓ Virtual PLCs used
- ✓ Lean Agile Mindset was used to deploy Cyber Range functionality

Tips for those who want to walk this path on their own:

10

Define goals and objectives

Determine the volume

Decide on the resources

Choose a platform

Don't try to cover everything at once

Develop attack scenarios

Weigh the pros and cons



If you decide to create your own Cyber Range

11

Use modern technology

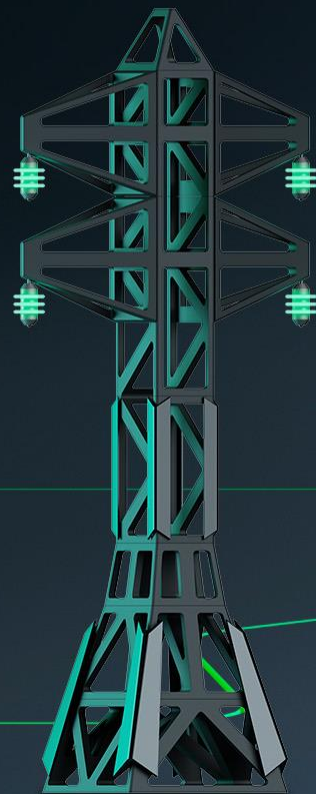
Test and improve

Ensure safety

Grant access

Create a community

Implement a monitoring and analysis system



Kaspersky Industrial
Cybersecurity
Conference 2024



Kaspersky Industrial
Cybersecurity
Conference 2024

Enhancing Business Continuity by Integrating and Automating Business and IT Processes



kaspersky

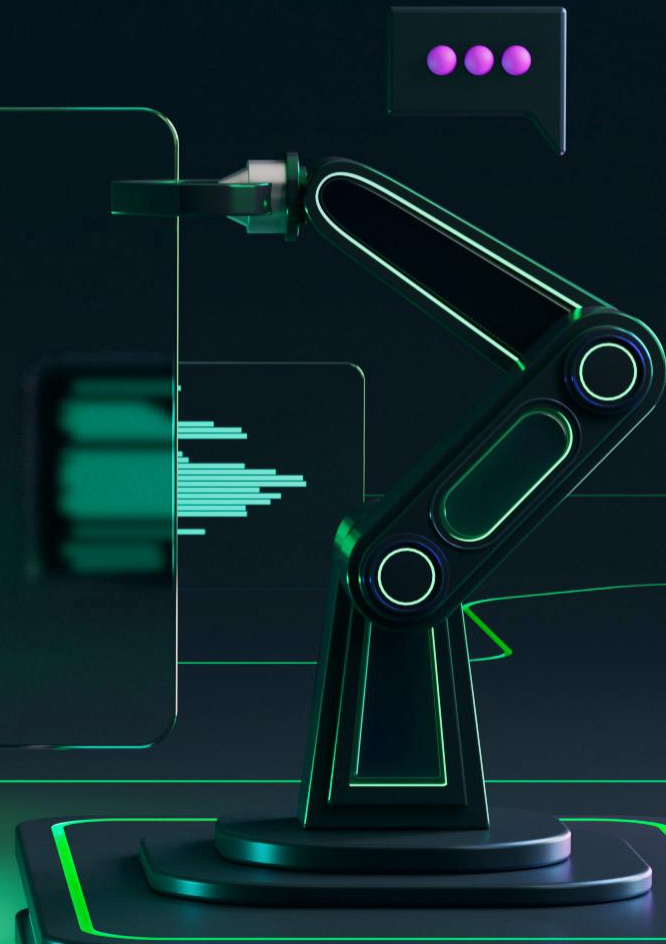


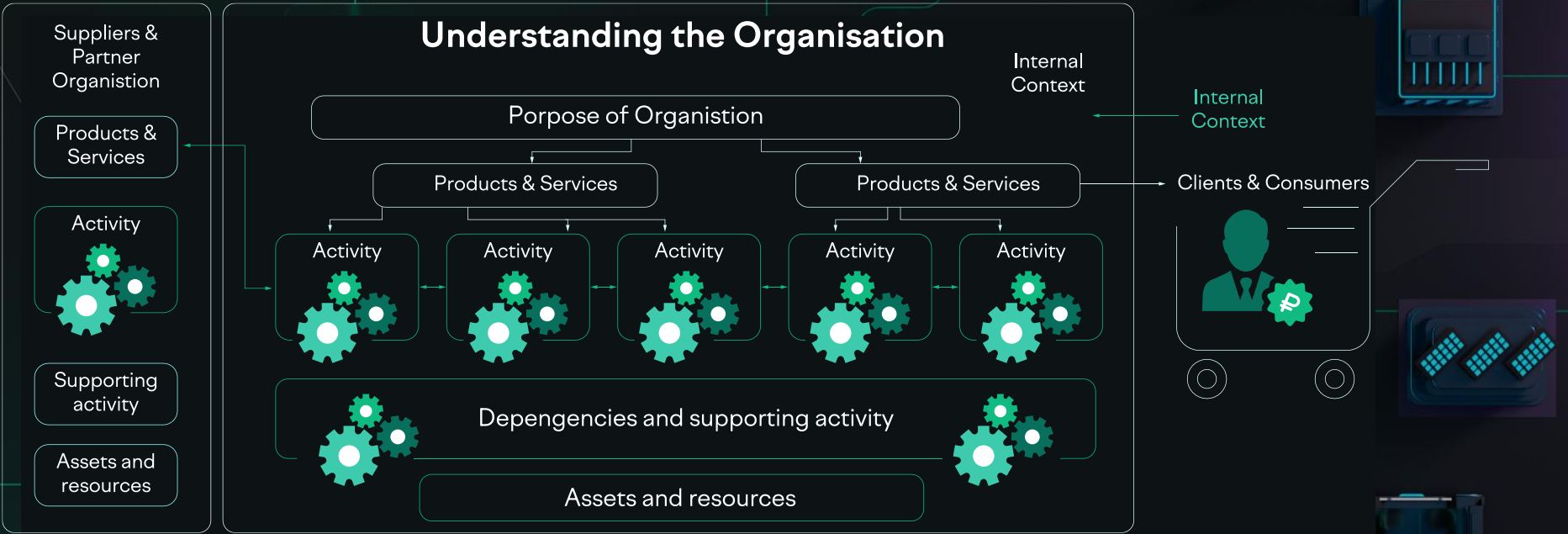
Kaspersky Industrial
Cybersecurity
Conference 2024

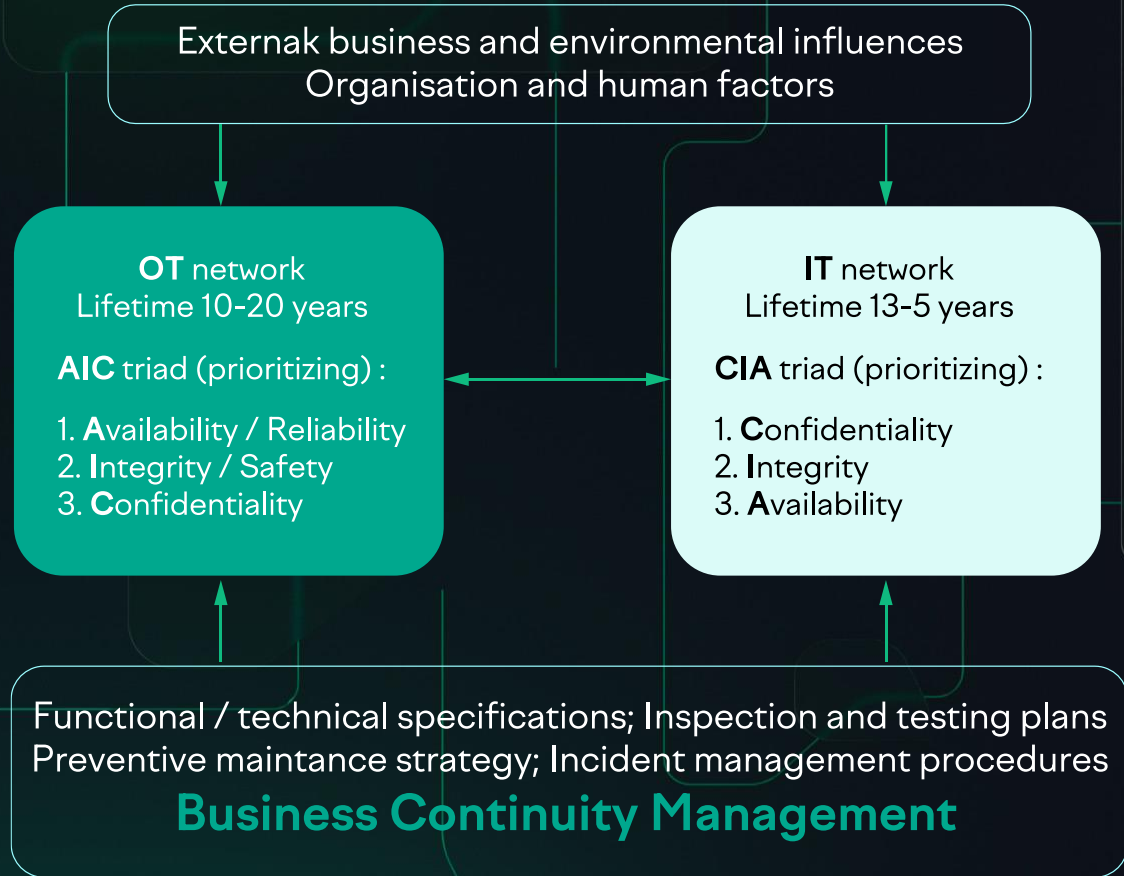
Maxim Annenkov

Expert, Security Vision

kaspersky







Rich capabilities for storing, enriching, inventorying, and managing enterprise assets.


Information system

General Relations History

CRM Active

Number IS: 017-ACY
 IS purpose: Customer Relationship Management
 Date of commissioning: 01.09.2023
 Date start support: 01.09.2023
 End date support: 01.09.2023

Customer Relationship Management (CRM) system — application software for organizations designed to automate customer interaction strategies, particularly to increase sales, optimize marketing, and improve customer service by storing information about customers and their interaction history, establishing and improving business processes, and subsequently analyzing results.



Id: 867
 Created: 10.10.2023 17:04:46 (Михаил Пименов)
 Updated: 19.09.2024 17:20:29 (Геннадий ИС Овнер)
 Owner: Ясеньков Ярослав
 Organization: ООО "Вектор-Плюс"
 Department: Бизнес-отдел

Severity level: Medium
 Recovery Time Objective 0 days 02 hours 00 minutes (RTO):
 Required Point Objective 0 days 03 hours 00 minutes (RPO):
 Alternative IS: Email system

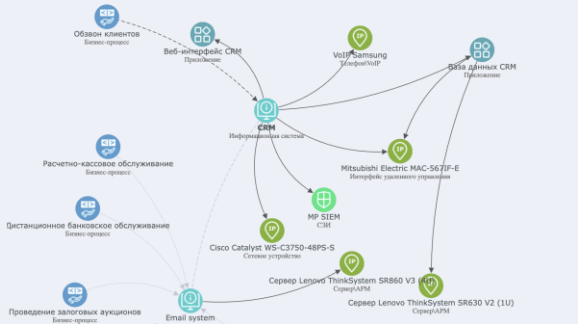
Information system

General Relations History

Alternative IS: Email system

Name	Dependency
VoIP Samsung	Partial
Cisco Catalyst WS-C3750-48PS-S	Full
Веб-интерфейс: CRM	Full
База данных CRM	Full
MP SIEM	Partial
Mitsubishi Electric MAC-567IF-E	Partial

Total: 6



Get host information from service directories

States: 5, Transitions: 5

Actions:

Host enrichment in CMDB

States: 9, Transitions: 9

Actions:

Host enrichment from scanning systems

States: 3, Transitions: 3

Actions:

Request information by IP

States: 11, Transitions: 11

Actions:

Enrichment for the host from VPM

States: 6, Transitions: 8

Actions:

Collecting host data from AV

States: 3, Transitions: 3

Actions:

Host enrichment from monitoring systems

States: 3, Transitions: 3

Actions:

nslookup

Type: LocalExecution

Enrichment: host

Group: Enrichment

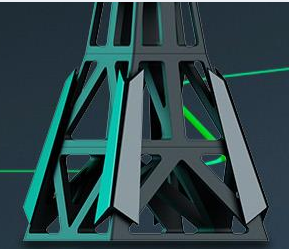
Entity types: Account, Application, Asset inventory, Attack, Business process, Components, Database, Data sources, Email, Equipment, External host, Groups, ILO/DRAC, Implement, Incident, Information system, ISS, Malware, Mitigations, NAS, Network device, Network scan, Objects action policy, Other device, Phone/VoIP, Post incident task, Printer/Scanner, Process, Product, References, Room, Server/PC, Software, Subtechnics, Tactics, Techniques, Ticket, Unknown device, URL, Vendor, Vulnerability, Whitelist

Version: 1 - 12.08.2024 09:50:54

nslookup

Type: LocalExecution

Save Save and close Cancel



01

Define
Assessment
scope

- Assessment object
- Responsible
- Experts

02

Gather
information

- Relations
- Dependencies
- Severity of assets
- Impact range
- Likelihood of events

03

Assessment
& **Analysis**

- Compile a single report
- Conduct GAP analysis
- Identify potential damage
- Model the effect of implementing security measures



Creating disaster recovery plans based on a Resource-Service Model



Reaction to an event



Ensuring Continuity



Recovery

Continuity group

Initiation and organization of necessary procedures

Coordination of work of departments in a crisis situation

Methodological support for participants in recovery processes

Recovery Team Leader

Making decisions on how to restore operations

Timely and effective communication with recovery team members

Managing the return of processes to normal operation

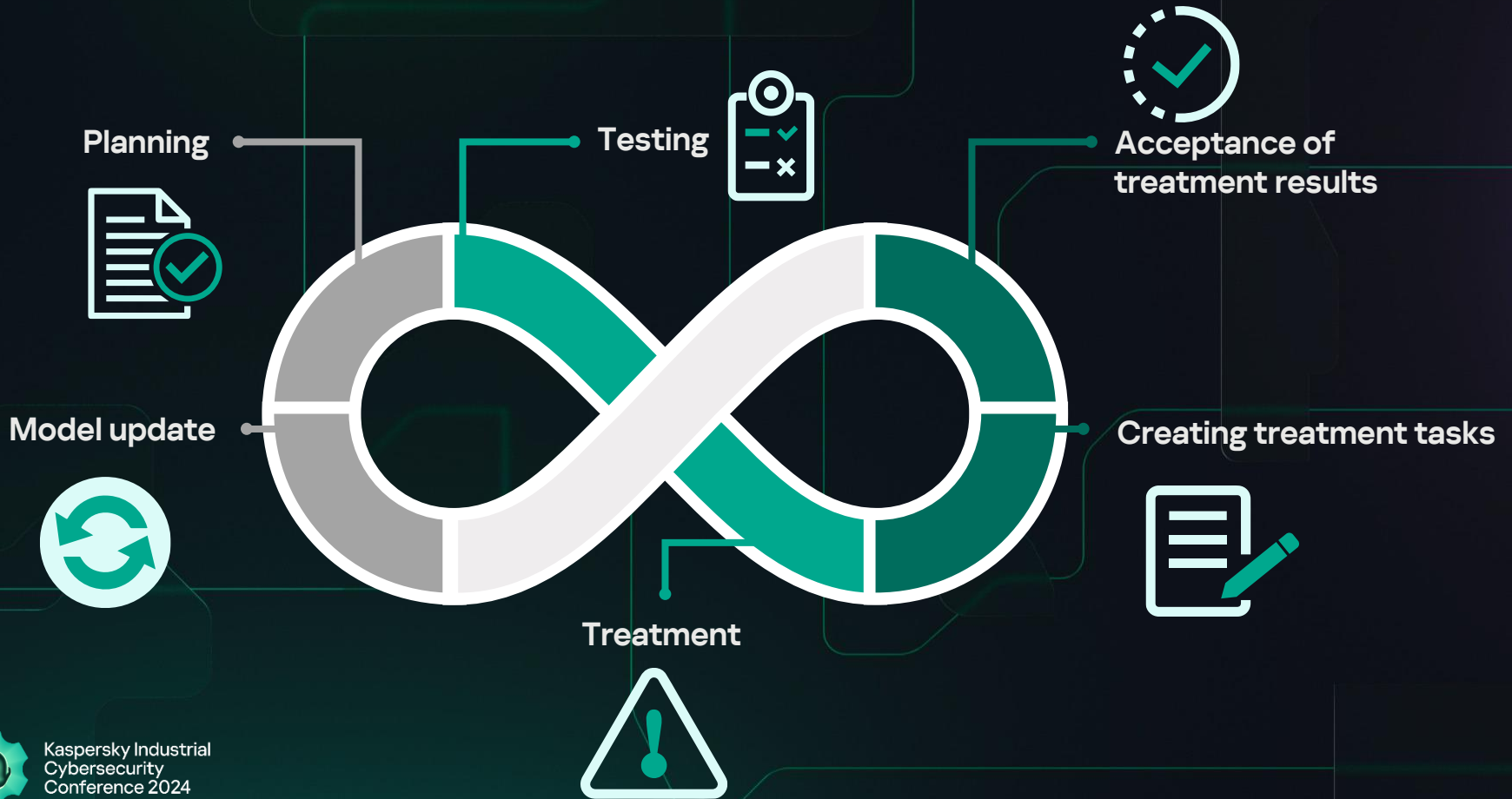
Recovery Team

Timely communication with your recovery team leader

Completing tasks according to plan

Carrying out the orders of the Recovery Team Leader





Thank you!



Andrey Abashev

Head of cybersecurity
methodology and innovations



Maxim Annenkov

Product manager
Security Vision

kaspersky