Kaspersky Industrial
Cybersecurity
Conference 2024

NG SOAR: Maximum automation from detection to response

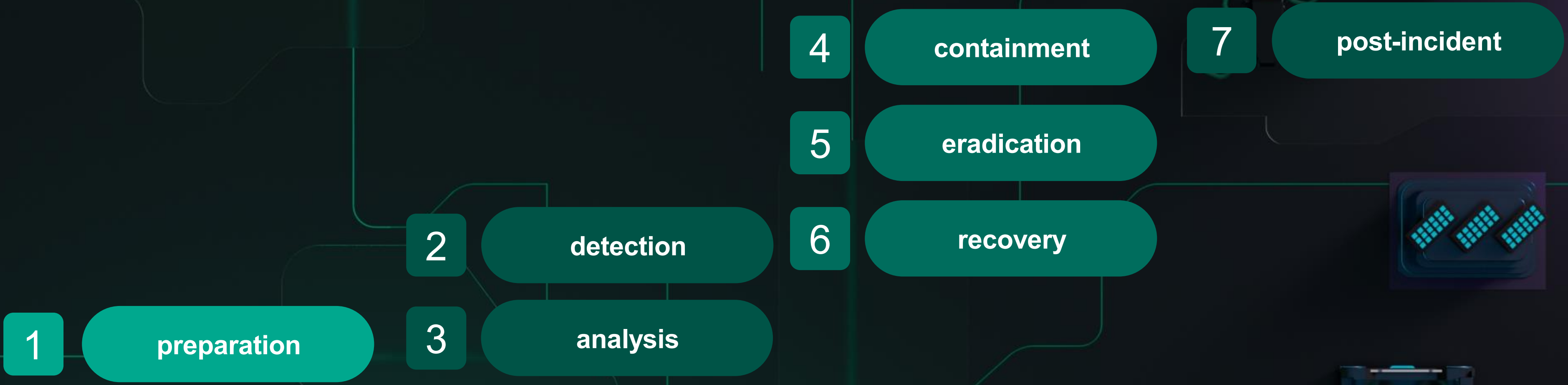
Eve Belyaeva,
Security Vision

kaspersky

Complete coverage of the phases of incident handling: from preparation, event collection and detection to investigation and response.

- Processes
- Detection as code
- TDIR
- Threat Intelligence
- Behavioral analysis
- Unified platform

NIST & SANS incident response process



1 preparation

2 detection

3 analysis

4 containment

5 eradication

6 recovery

7 post-incident

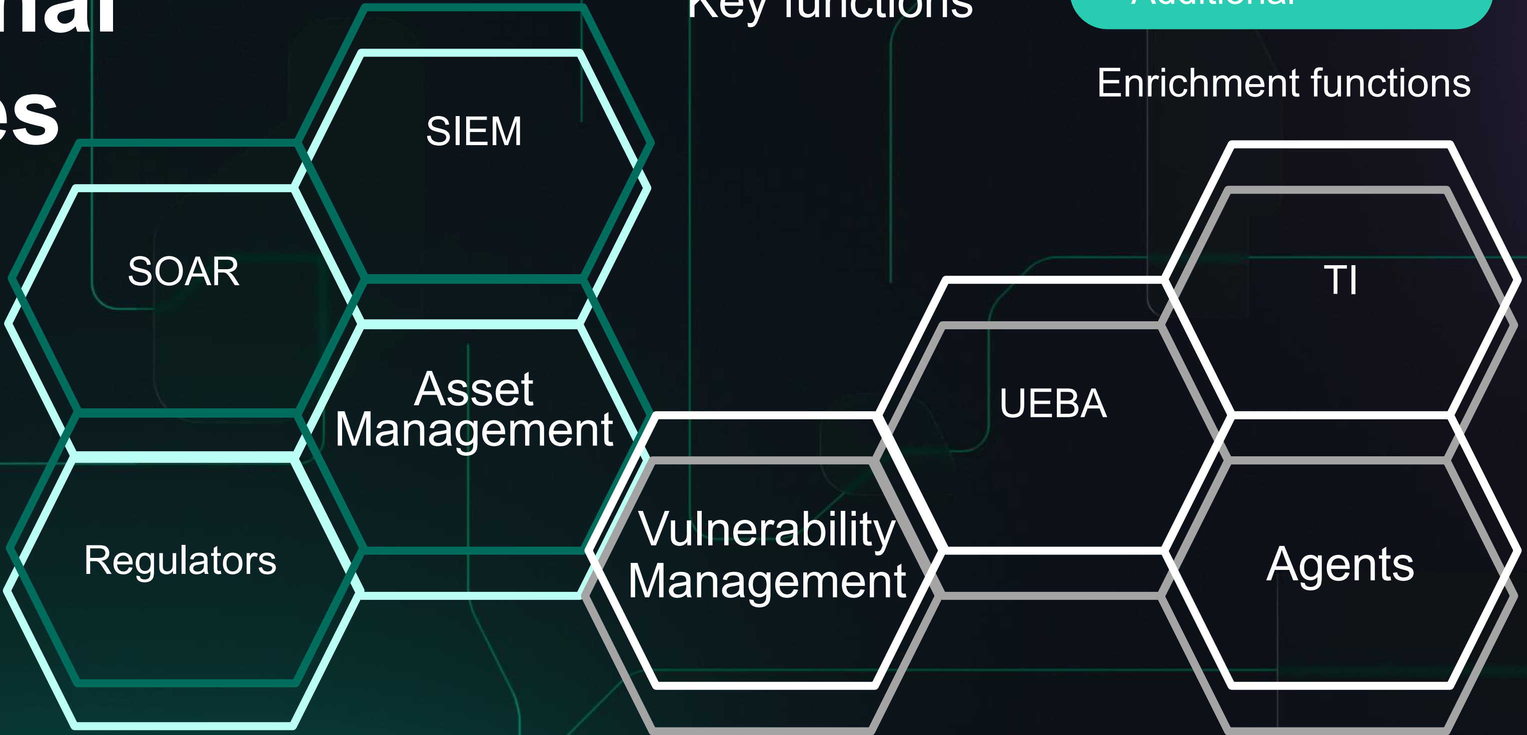
Optional and additional modules

Obligatory

Key functions

Additional

Enrichment functions



Key features of the system

In order to have an understanding of what happened at every stage of the investigation process, a number of new features are being applied

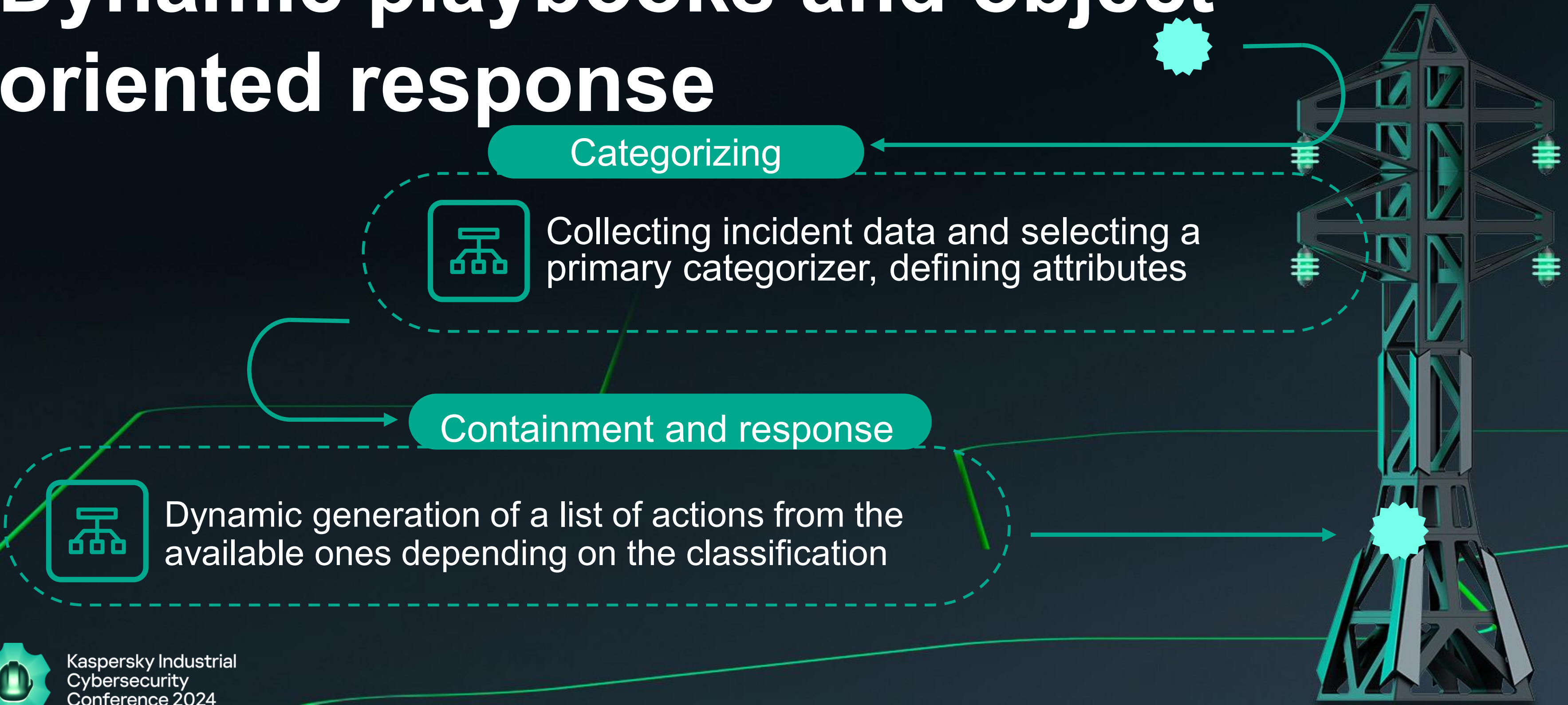
Ability to work with a customer's volatile infrastructure

Object-oriented response allows the analyst's actions to be atomized

System automatically builds incidents into a complete attack chain to reconstruct the full picture of what happened

Assistance for the analyst with selection of the most effective incident response strategies

Dynamic playbooks and object-oriented response



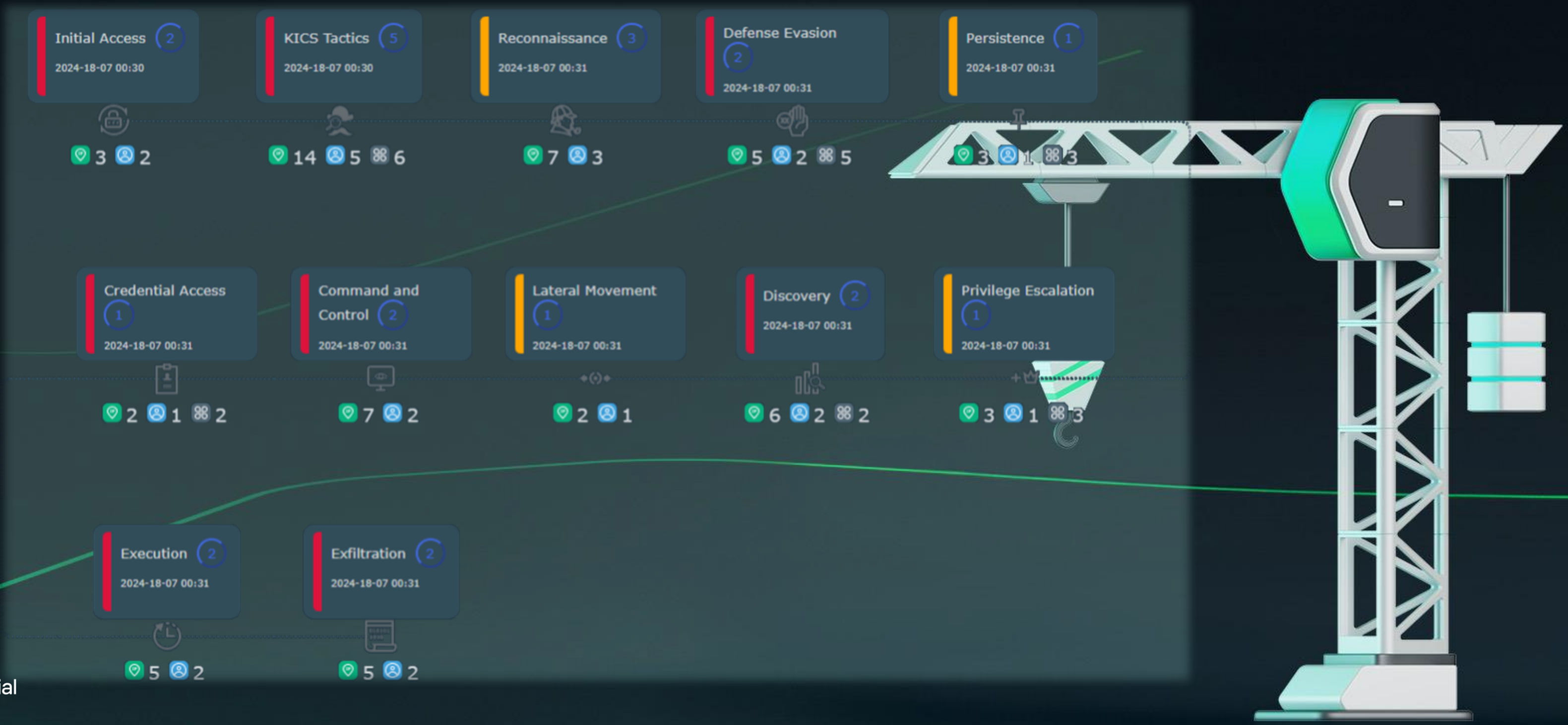
Categorizing

Collecting incident data and selecting a primary categorizer, defining attributes

Containment and response

Dynamic generation of a list of actions from the available ones depending on the classification

Real-time Kill Chain



Initial Access 2
2024-18-07 00:30
3 2

KICS Tactics 5
2024-18-07 00:30
14 5 6

Reconnaissance 3
2024-18-07 00:31
7 3

Defense Evasion 2
2024-18-07 00:31
5 2 5

Persistence 1
2024-18-07 00:31
3 1 3

Credential Access 1
2024-18-07 00:31
2 1 2

Command and Control 2
2024-18-07 00:31
7 2

Lateral Movement 1
2024-18-07 00:31
2 1

Discovery 2
2024-18-07 00:31
6 2 2

Privilege Escalation 1
2024-18-07 00:31
3 1 3

Execution 2
2024-18-07 00:31
5 2

Exfiltration 2
2024-18-07 00:31
5 2

MITRE-based recommendations

- Initial and full analysis of the incident
- Universal and custom containment
- Mandatory and optional actions
- Post-incident: error correction and hardening

Key benefits for investigation and response

- Optimization of resources (finances, assets, time), high speed of implementation
- Elimination of blind spots in the infrastructure by eliminating data transmission problems
- Customization to the customer's infrastructure
- Strengthening existing processes in the company and building new ones
- Combining investigative and response technologies in a single window
- Full post-analysis of investigation results
- Convenient no-code tools for the analyst

Thank you!

kaspersky