Kaspersky Industrial
Cybersecurity
Conference

Kaspersky ICS MDR

Anton Ivanov,
CTO, Kaspersky

kaspersky

Agenda

Challenges

Our expertise

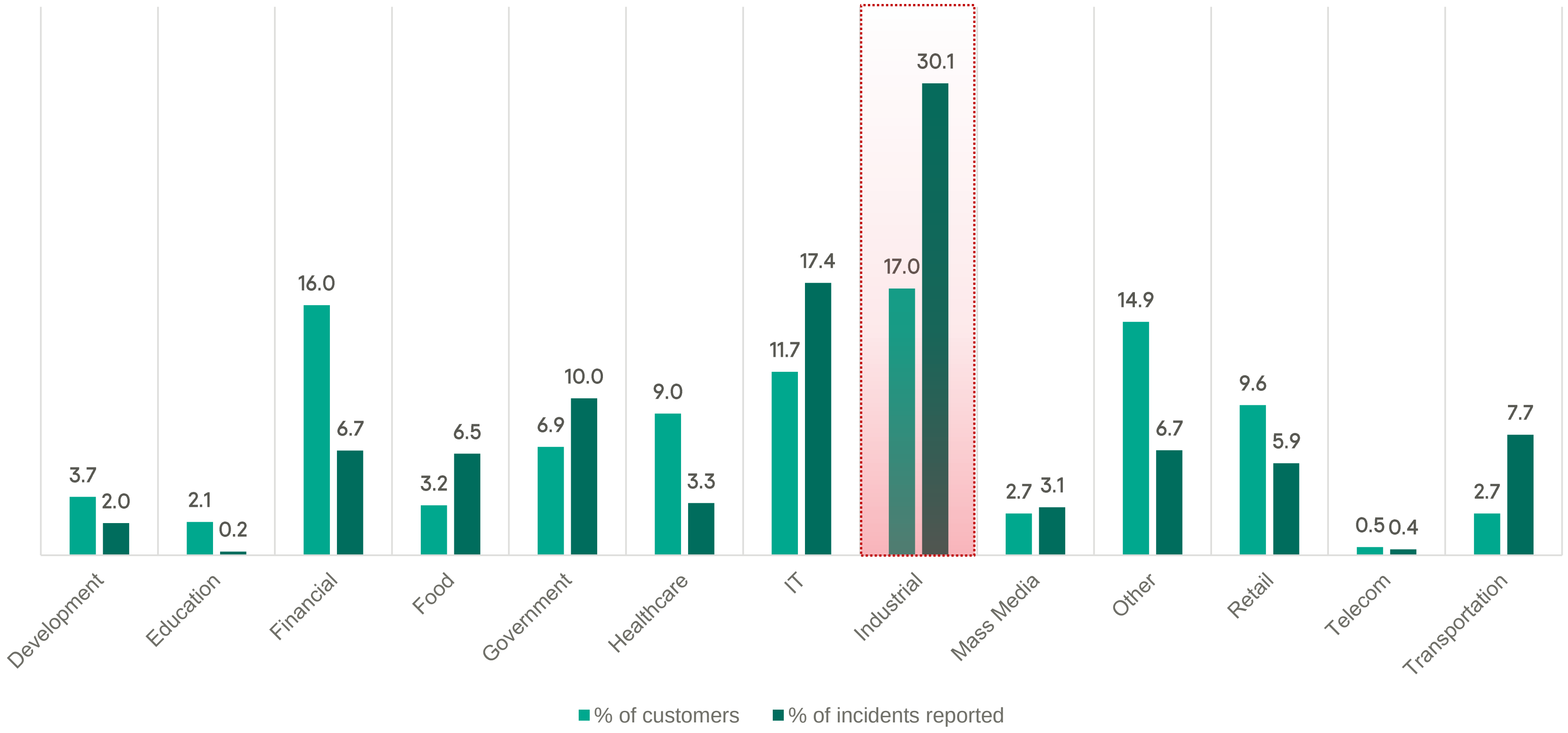
New service

How it works

Summary

Challenges

Industrial is one of the primary targets for cybercrime and APT



Based on Kaspersky MDR service data (2021)

ICS statistics (H1 2022)

- **31.8%** of industrial hosts encountered malware at least once
- **16.5%** of threats was from the internet sources
- on **7%** of industrial hosts malware was blocked in emails or web traffic

See https://ics-cert.kaspersky.com/publications/reports/2022/09/08/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2022/ for details

Key security elements

Expertise

The effectiveness of modern complex security solutions directly correlates with the expertise level of IT security / SOC teams. Organizations should invest in education of their local experts, or use external Managed Detection & Response services from a proven, trusted provider.

Reliable security solutions

IT security / SOC experts need solutions that monitor all security-related events within their organization's IT infrastructure, with timely and accurate detection of cyberthreats – plus a high level of automation for fast, effective containment and eradication. Such solutions must be specifically designed to address today's evolving challenges.

Threat Intelligence

Without relevant, actionable information about which threat actors pose the highest threat to an organization, and what their tactics, techniques and procedures are, it's impossible to protect against modern, sophisticated cyberthreats. The use of Threat Intelligence data should be an integral part of any business's cybersecurity strategy.

Our expertise

Our expertise

700+ Threat groups and campaigns

380K new malicious files are detected by Kaspersky every day

200+ world-leading security researchers

Threat Research and Global Research and Analysis Teams are strategically located all around the globe, providing unparalleled depth of analysis and understanding of all kinds of threats

Targeted attack research

2016

- ProjectSauron
- StrongPity
- Lazarus
- Fruity Armor
- ScarCruft
- Poseidon
- Danti
- Dropping Elephant

2017

- WannaCry
- Shamoon 2.0
- StoneDrill
- BlueNoroff
- ExPetr/NotPetya
- Moonlight Maze
- ShadowPad
- BlackOasis
- Silence
- WhiteBear

2018

- Zebrocy
- DarkTequila
- MuddyWater
- Skygofree
- Olympic Destroyer
- ZooPark
- Hades
- Octopus
- AppleJeus

2019

- Topinambour
- ShadowHammer
- SneakyPastes
- FinSpy
- DarkUniverse
- COMpfun
- Titanium

2020

- Cycldek
- SixLittleMonkeys (aka Microcin)
- CactusPete
- DeathStalker
- MATA
- TransparentT ribe
- WellMess
- TwoSail Junk
- MontysThree
- MosaicRegressor
- VHD Ransomware
- WildPressure
- PhantomLance

2021

- GhostEmperor
- ExCone
- BlackShadow
- BountyGlad
- EdwardsPhesant
- HotCousin
- GoldenJackal
- FerociousKitten
- ReconHellcat
- CoughingDown
- MysterySnail
- CraneLand

ICS specific threat intelligence

ICS Reporting

Subscription-based access via a web portal to regular TI reports with ICS-specific information on attacks, threats and vulnerabilities

ICS malware data feed

Feed contains Indicators of Compromise (IOCs) and metadata for integration with third-party SIEM systems

Tailored reports

Highly customized threat intelligence reports with either a tactical or strategic focus for the period (quarter / year) and specified geography / industry

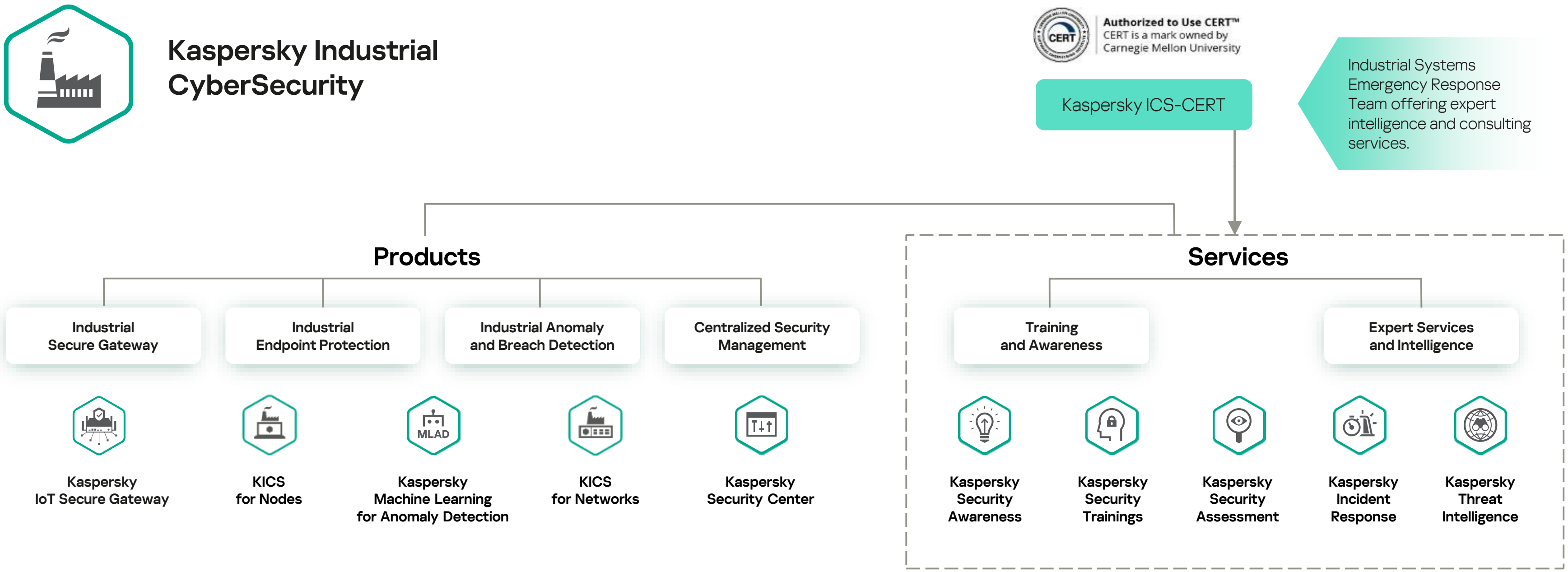
ICS vulnerability data feed

Feed contains accurate and up-to-date information to identify vulnerabilities in the ICS network

ICS related threat intelligence research is conducted by a dedicated team — Kaspersky ICS CERT

- Established in 2016
- The first CERT team created by a commercial organization
- Around 20 highly qualified experts in ICS threat and vulnerability research, incident response and security analysis

Kaspersky Industrial Cybersecurity Solution



Kaspersky Industrial CyberSecurity

Authorized to Use CERT™
CERT is a mark owned by Carnegie Mellon University

Kaspersky ICS-CERT

Industrial Systems Emergency Response Team offering expert intelligence and consulting services.

Products

- Industrial Secure Gateway
  - Kaspersky IoT Secure Gateway
- Industrial Endpoint Protection
  - KICS for Nodes
- Industrial Anomaly and Breach Detection
  - Kaspersky Machine Learning for Anomaly Detection
  - KICS for Networks
- Centralized Security Management
  - Kaspersky Security Center

Services

- Training and Awareness
  - Kaspersky Security Awareness
  - Kaspersky Security Trainings
- Expert Services and Intelligence
  - Kaspersky Security Assessment
  - Kaspersky Incident Response
  - Kaspersky Threat Intelligence

Some of the supported devices & protocols

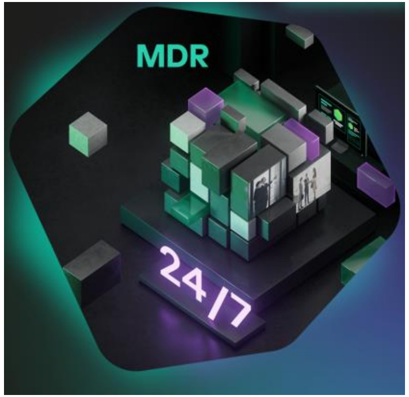
ABB · CODESYS · EMERSON. · MITSUBISHI ELECTRIC · OMRON · Rockwell Automation · Schneider Electric · SIEMENS · YOKOGAWA

New service

ICS Managed Detection and Response

ICS Managed Detection and Response

- **Continuous incident detection** service on top of KES, KATA and KICS with easy setup and no additional infra costs
- **Threat detection** and **Cyber threat hunting**:
  - New malware detection
  - Non-malware attack detection (Living-off the land)
  - APT and targeted attack detection (any sort of human-driven)
- Covers both OT and IT networks
- Unified console for product configuration, incidents and response management
- API support
- Direct access to SOC analysts



Service value for customers

Advanced Threat Detection

Kaspersky SOC experts detect even sophisticated targeted attacks with hundreds of threat hunting rules based on our Threat Intelligence and 20+ years of experience in cybersecurity.

Efficiency

Kaspersky SOC experts monitor events from your organization on **24x7** basis.

We analyze all suspicious actions and report only real incidents avoiding false positives.

Response and Remediation

All incidents are reported with the recommendations how to respond to detected threats.

Remote controlled pre-approved and approved response is also supported.

Who is the service for

Customer Profile	MDR Value
No security operations at all	Baseline security operations: - Monitoring, threat detection, investigation
Mature security operations (Enterprise SOC)	Additional detection capabilities: - Detect threats with Kaspersky products - Reported incidents can be pulled to corporate Incident management system (API)
Managed Security Service Provider	Augment existing threat detection capabilities: - Detect threats with Kaspersky products - Enrich Provider's reports

Service SLAs

Priority level	Reaction time	Target value
High (example: targeted attack)	1 hour	90%
Medium (example: common malware)	4 hours	90%
Low (example: adware, riskware, etc.)	24 hours	90%

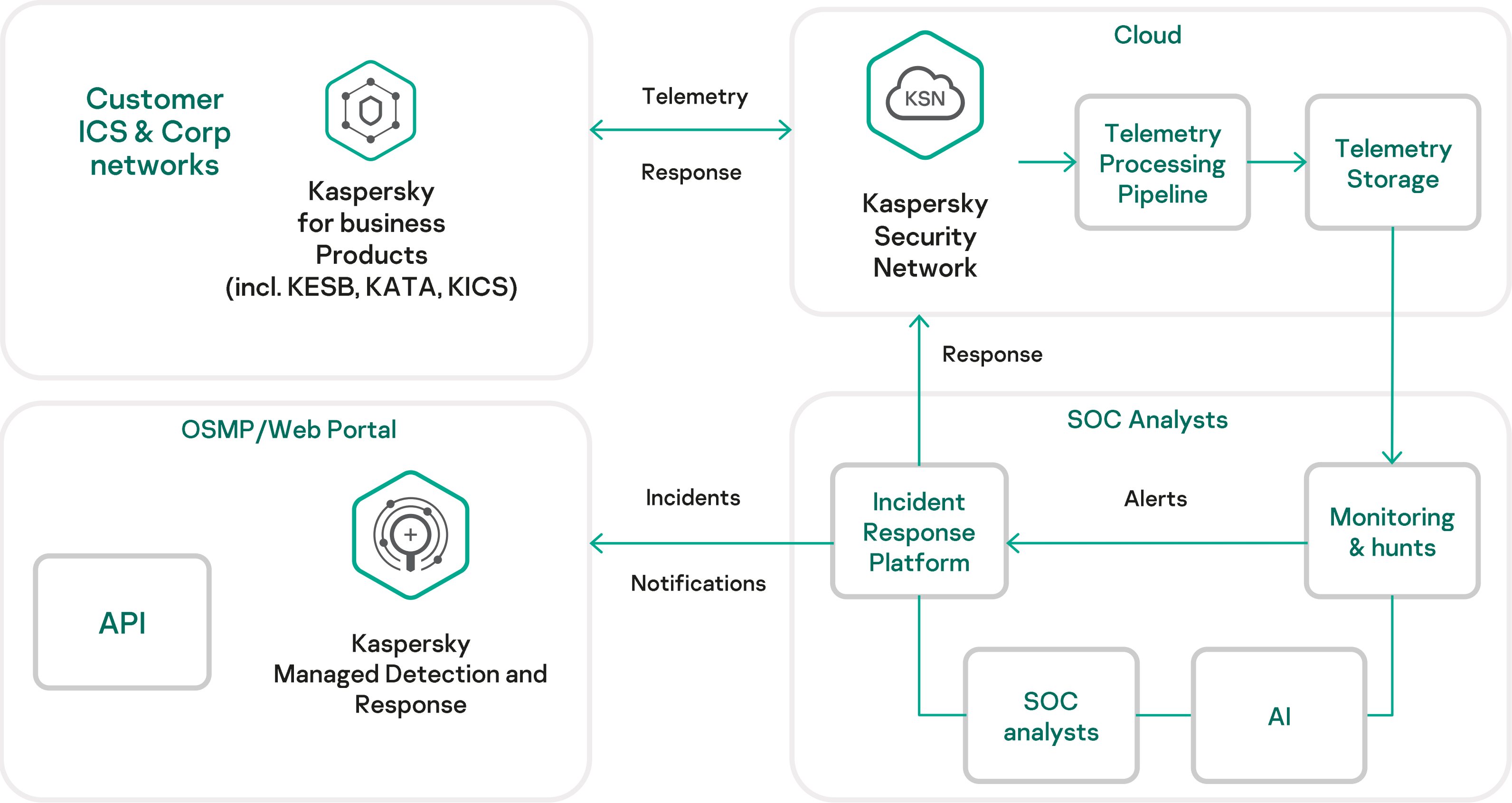
- **Reaction time** – the time from detection of incident (Created time) to publishing it to MDR portal (Updated time)
- **Target Value** – percent of the number of incidents with Reaction time and Response time met Target value objective

More information including incident criteria can be found in Terms and Conditions

How it works

ICS Managed Detection and Response

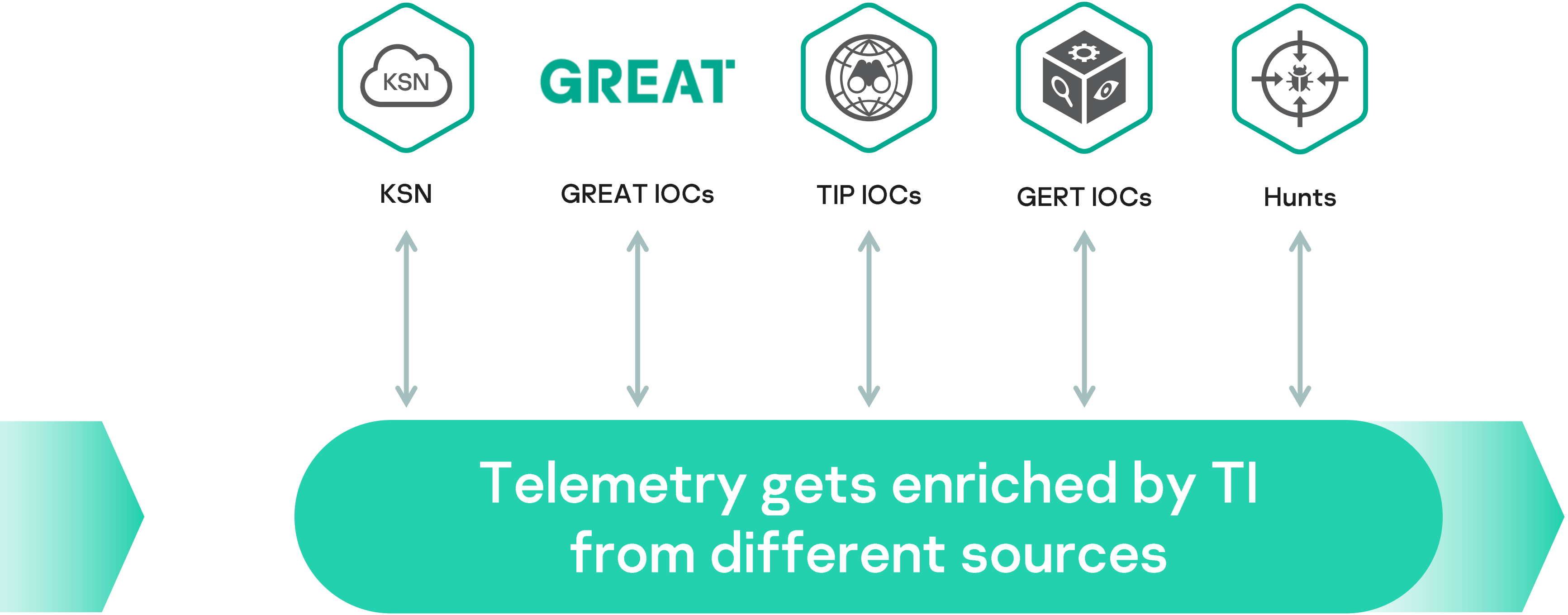
High-level service architecture



Telemetry

- Filesystem events (file creation, modification)
- Process events (process start, process injection, etc.)
- Network events (connection, DNS query, file downloading, email, etc.)
- System events (registry, event logs, WMI, autorun, etc.)
- Endpoint security events (AV/KICS detect, etc.)
- Network security events (KICS detect, KATA, etc.)
- Service events

Telemetry processing pipeline – enrichment (examples)



KSN

GREAT IOCs

TIP IOCs

GERT IOCs

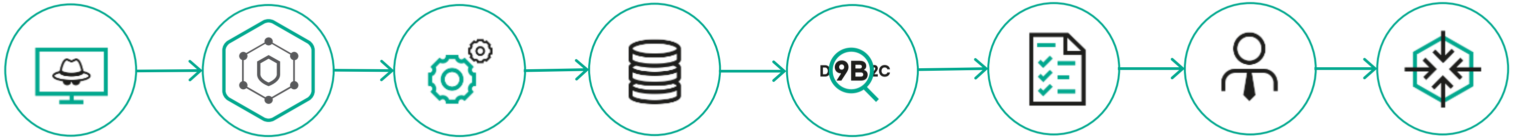
Hunts

Telemetry gets enriched by TI
from different sources

Threat hunting rules or “hunts”

- 1100+ active threat hunting rules including ICS-specific
- Each rule created by our experts
- Rules are based on our Threat Intelligence and MITRE ATT&CK Framework
- Rules are regularly updated with information from our Threat Intelligence services

So how it works



Suspicious activity

Telemetry Collection

Telemetry Processing

Telemetry Storage

Analysis
Threat Hunting Rules Applied

Alerts
Created

SOC Analyst
Alerts analyzed

Response
Incident is published and response recommendations are given

Summary

- 24x7 incident detection service
- Run by Kaspersky SOC analysts with years of experience and 500K+ protected nodes of 200+ customers
- Covers both IT and OT networks
- Works on top of Kaspersky security products (no additional software required)
- Can be integrated with existing IRP/SOAR systems (through API)
- Easy setup and no additional infrastructure costs
- **Free trial period**

Thank you

Try ICS MDR now for free!

Anton Ivanov

Chief Technology Officer

kaspersky