



Kaspersky Industrial
Cybersecurity
Conference 2019

September 18-20, 2019, Sochi, Russia

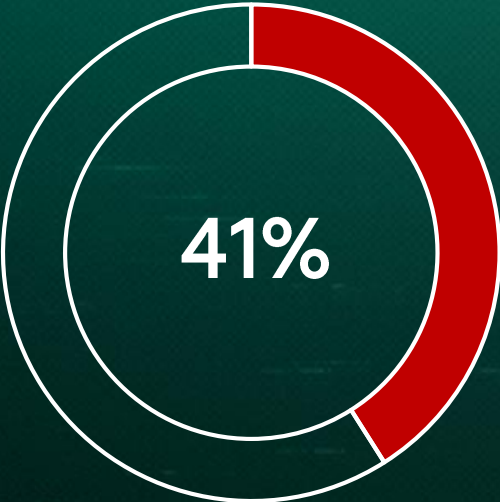
kaspersky

Kaspersky Industrial CyberSecurity Business Evolution

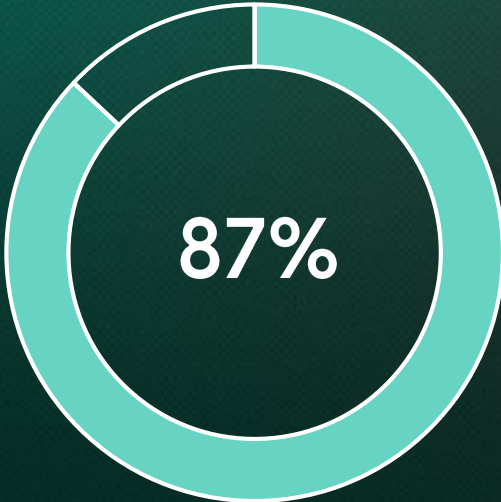
Georgy Shebuldaev, Head of Kaspersky Industrial Cybersecurity Business Development



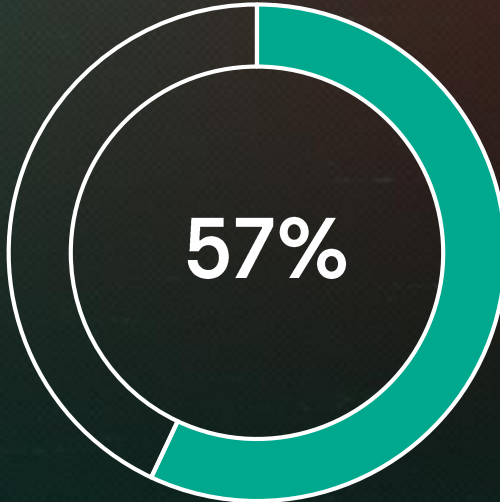
OT/ICS cybersecurity is no longer a 'unicorn'



Industrial endpoints on which malicious objects were blocked in H1 2019



Prioritize OT/ICS cybersecurity

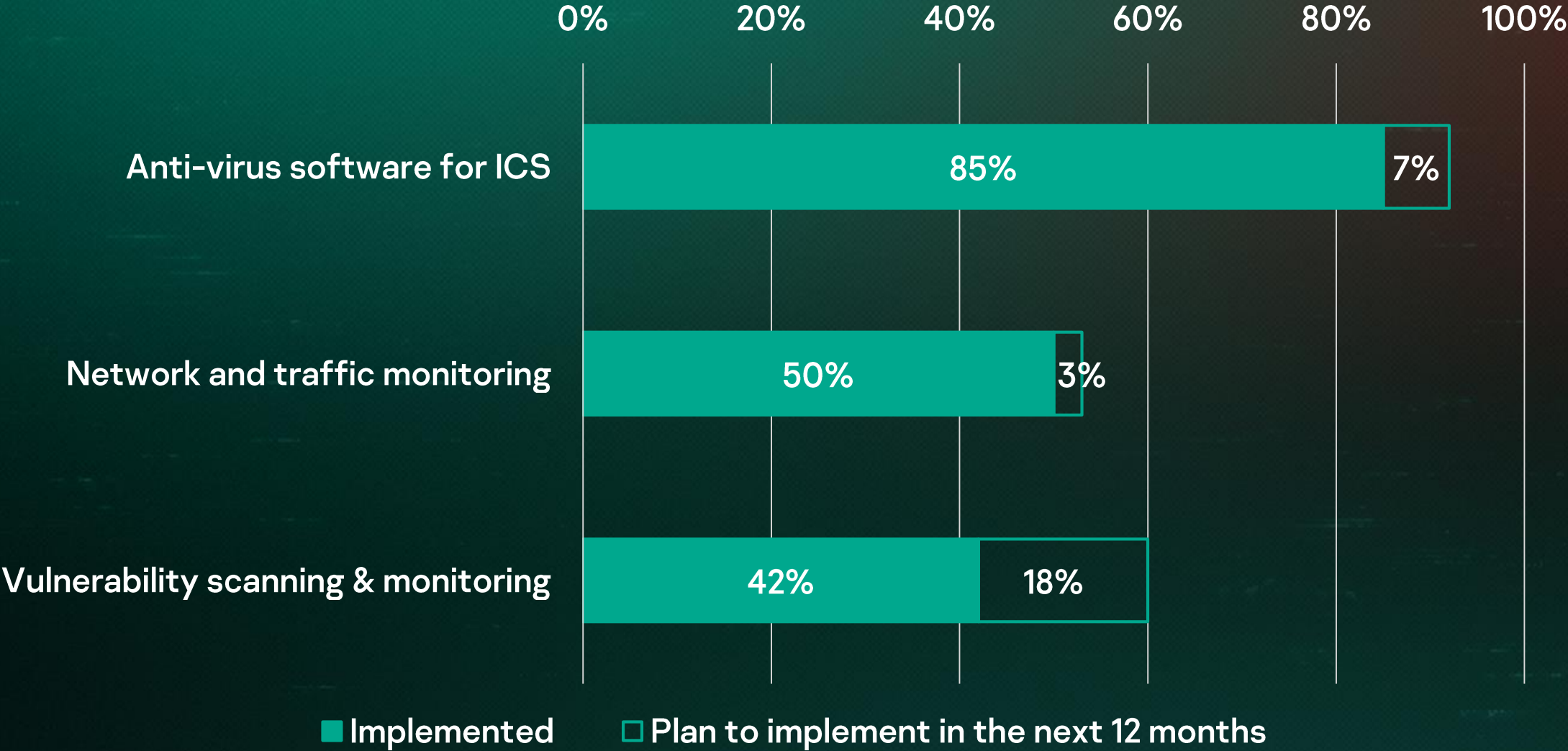


Have dedicated cybersecurity budget for ICS

Source: Kaspersky ICS CERT report 'Threat landscape for industrial automation systems H119'

Source: Kaspersky 'State of Industrial Cybersecurity 2019' report is based on a survey conducted by ARC Advisory Group in spring 2019 across 282 industrial organizations across the globe.

Essential cybersecurity measures already in place





Kaspersky Industrial CyberSecurity

PRODUCTS

SERVICES

Industrial
Endpoint Protection



KICS
for Nodes

Industrial
Anomaly and
Breach Detection



KICS
for Networks

Centralized Security
Management



Kaspersky
Security
Center

Training
and Awareness



Kaspersky®
Security
Awareness



Kaspersky®
Security
Trainings

Expert Services
and Intelligence



Kaspersky®
Security
Assessment



Kaspersky®
Incident
Response



Kaspersky®
Threat
Intelligence

Market Feedback



100+ projects
21 countries

Market Feedback: Products



KICS
for Nodes

Industrial
Endpoint
Protection



KICS
for Networks

Industrial
Anomaly and
Breach Detection



Kaspersky
Security
Center

Centralized
Security
Management

①

Win XP / Win 7 support became an issue globally

②

Customers start to use full Endpoint Protection tool stack

- Antivirus
- Device Control
- Application Whitelisting
- Log inspection
- File integrity control

③

Network anomaly detection rate is being challenged

④

Market slowly approach Response capabilities

Kaspersky Evolution: Products



KICS
for Nodes

Industrial
Endpoint
Protection

Win XP support confirmed in KICS for Nodes till 12/2024

Advanced Threat Detection Capabilities (Exp 2020)

Basic Response Capabilities (Exp 2020)



KICS
for Networks

Industrial
Anomaly and
Breach Detection

Integration Scenarios with:

-Industrial Network Equipment (Advanced Detection and cost effectiveness)

-Firewalls (Response)



Kaspersky
Security
Center

Centralized
Security
Management

Advanced Centralized Management Capabilities (Exp 2020)

Vulnerability Detection and Management Capabilities (Exp 2020)

Market Feedback: Services



How to approach vulnerability and patch management processes?



How to use a current detection and response tool stack efficiently?



How to develop internal expertise?

Kaspersky Evolution: Services

ICS Vulnerabilities Database



Kaspersky®
Threat Intelligence

Available EoY 2019

- Most critical vulnerabilities
- Most popular OT devices and software
- Expert criticality evaluation
- Actionable mitigation advisory
- Network attack signatures and IoCs
- Human and machine readable format

Kaspersky Evolution: Services

Kaspersky Incident Response



IR Handbook



Kaspersky team on hand to:

- Investigate the incident
- Provide recommendations on how to avoid it in future
- Assess current customer team and tool stack
- Analyze and improve existing IR business processes
- Simulate, test and train customer team

Conclusion





**Kaspersky Industrial
Cybersecurity
Conference 2019**

September 18-20, 2019, Sochi, Russia

kaspersky

Thank you!

