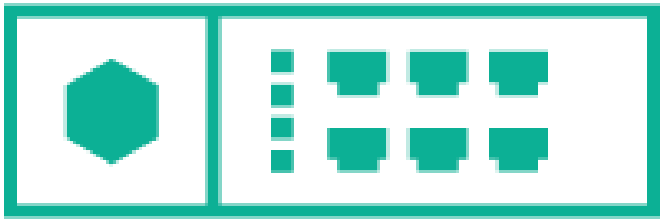
KICS EVOLUTION 2018-2020

Dmitry Lukiyan, product manager

KASPERSKY

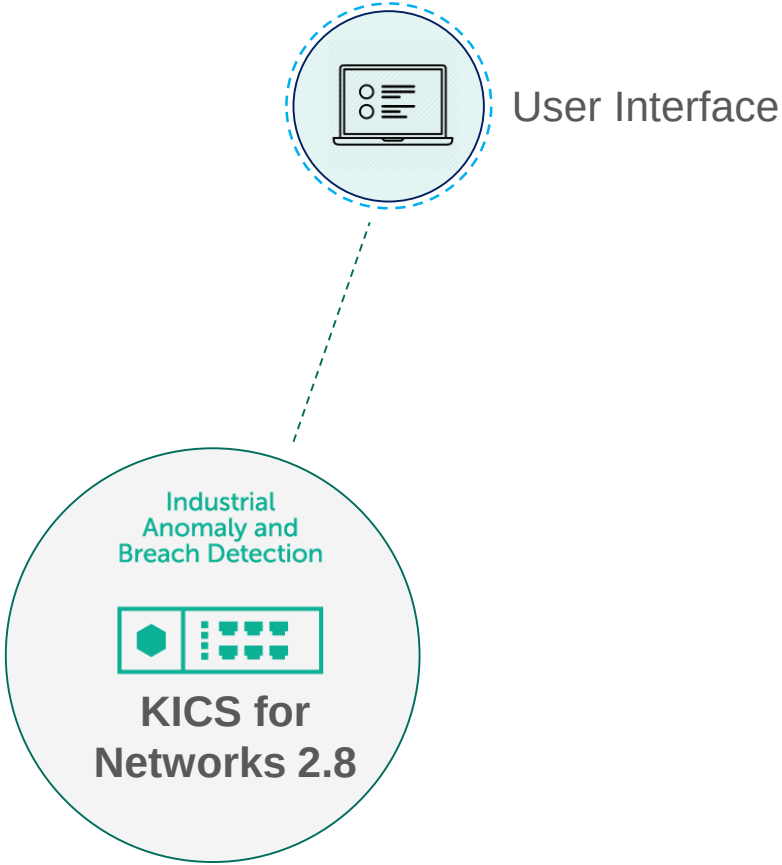
Industrial Anomaly and Breach Detection

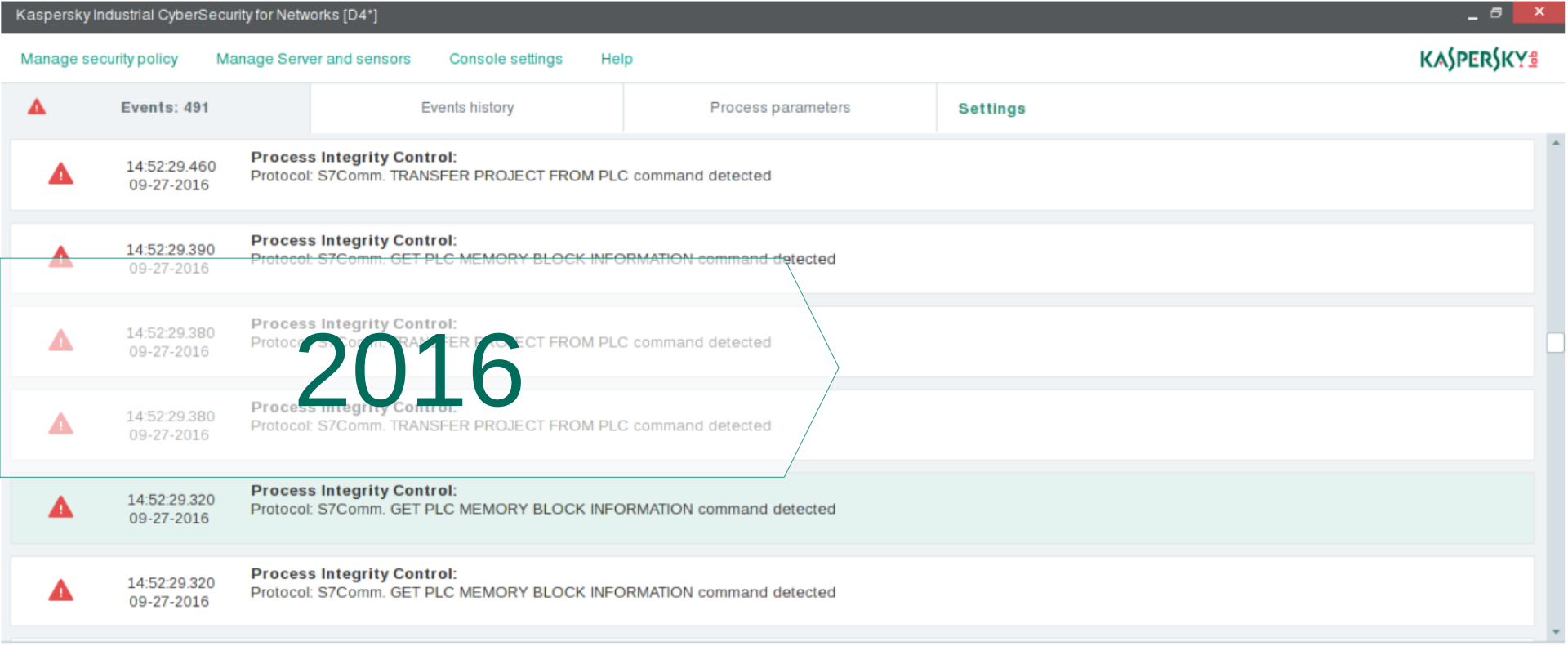


KICS for Networks

2.8

Technical Preview


User Interface
Industrial
Anomaly and
Breach Detection
KICS for
Networks 2.8


Kaspersky Industrial CyberSecurity for Networks [D4*]
Manage security policy
Manage Server and sensors
Console settings
Help
KASPERSKY
Events: 491
Events history
Process parameters
Settings
14:52:29.460
09-27-2016
Process Integrity Control:
Protocol: S7Comm. TRANSFER PROJECT FROM PLC command detected
14:52:29.390
09-27-2016
Process Integrity Control:
Protocol: S7Comm. GET PLC MEMORY BLOCK INFORMATION command detected
14:52:29.380
09-27-2016
Process Integrity Control:
14:52:29.380
09-27-2016
Protocol: S7Comm. TRANSFER PROJECT FROM PLC command detected
2016
14:52:29.320
09-27-2016
Process Integrity Control:
Protocol: S7Comm. GET PLC MEMORY BLOCK INFORMATION command detected
14:52:29.320
09-27-2016
Process Integrity Control:
Protocol: S7Comm. GET PLC MEMORY BLOCK INFORMATION command detected

Kaspersky
Industrial CyberSecurity for Networks

user_name

Events | Process parameters

Update table
enabled

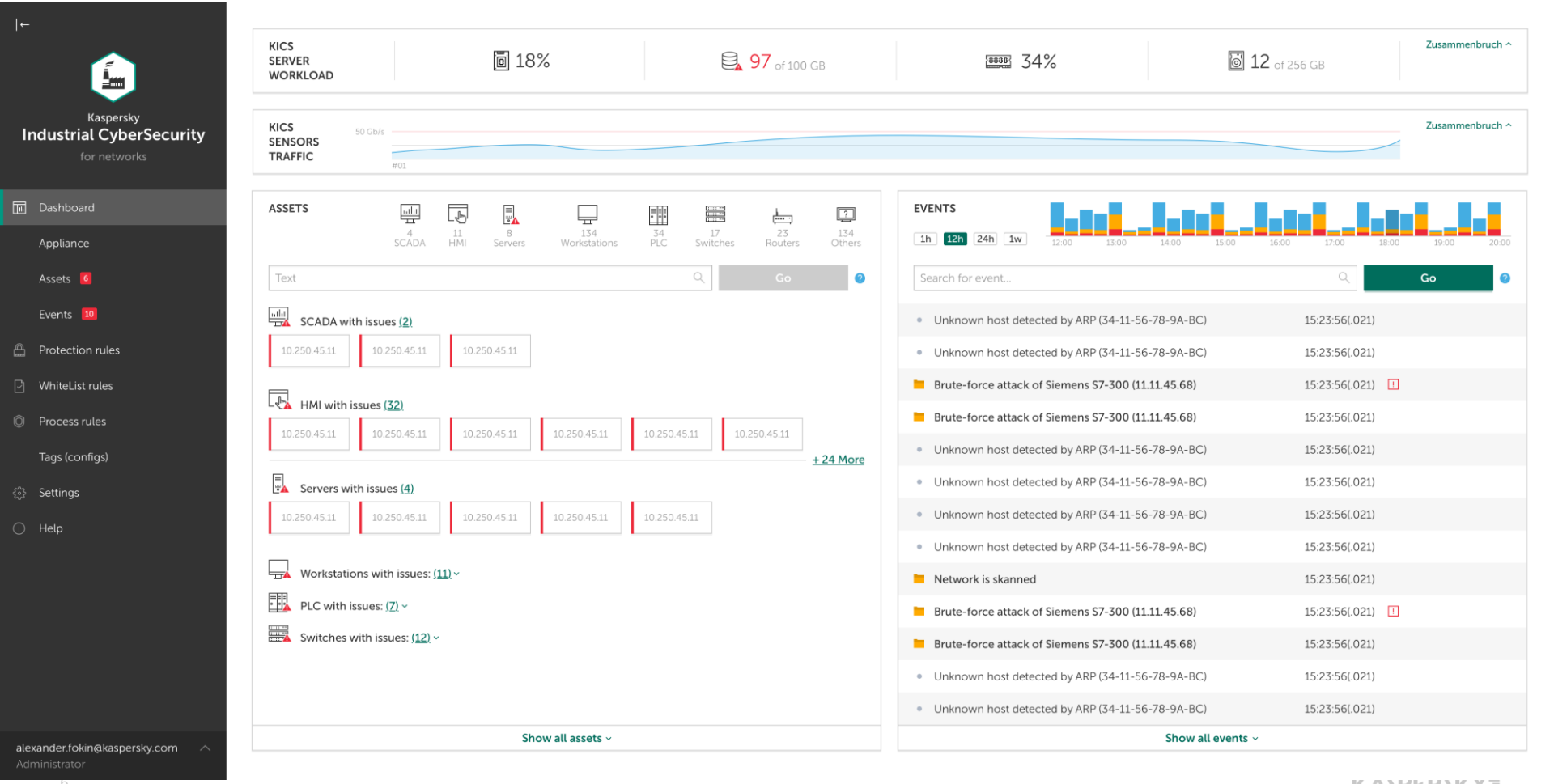
Period:
Last 24 hours

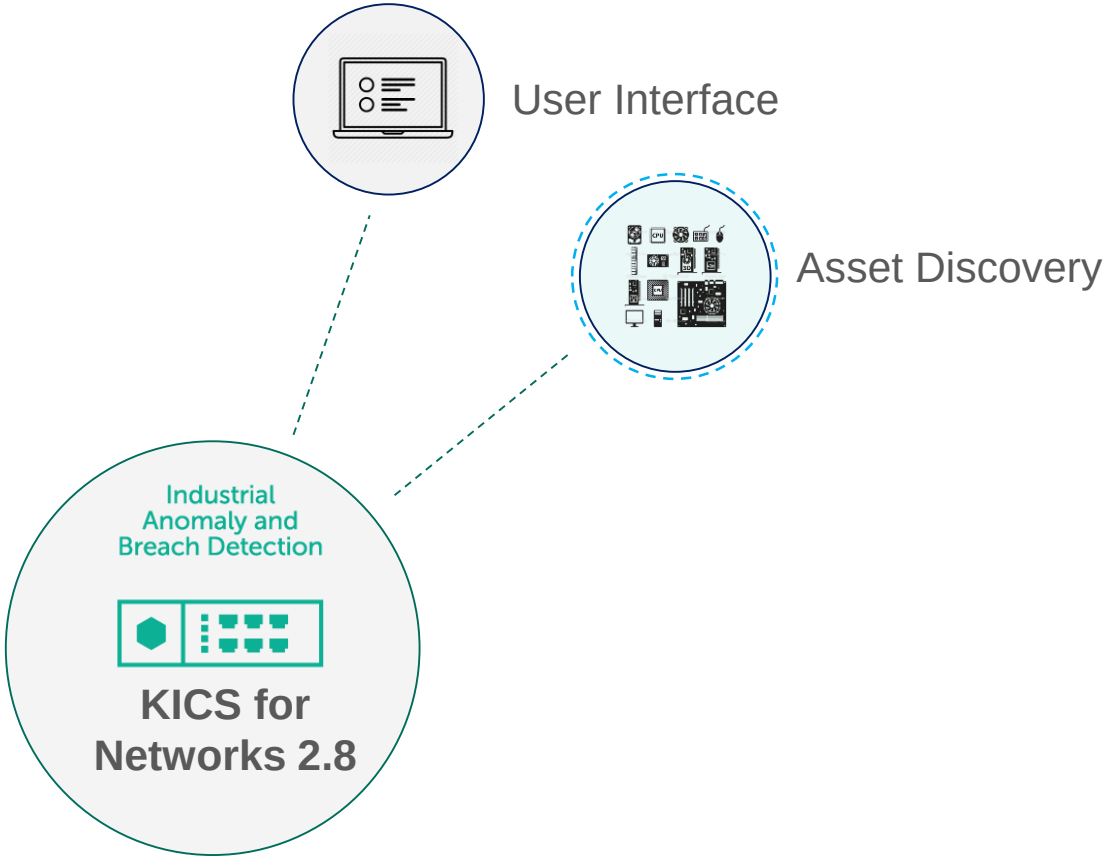
Table templates

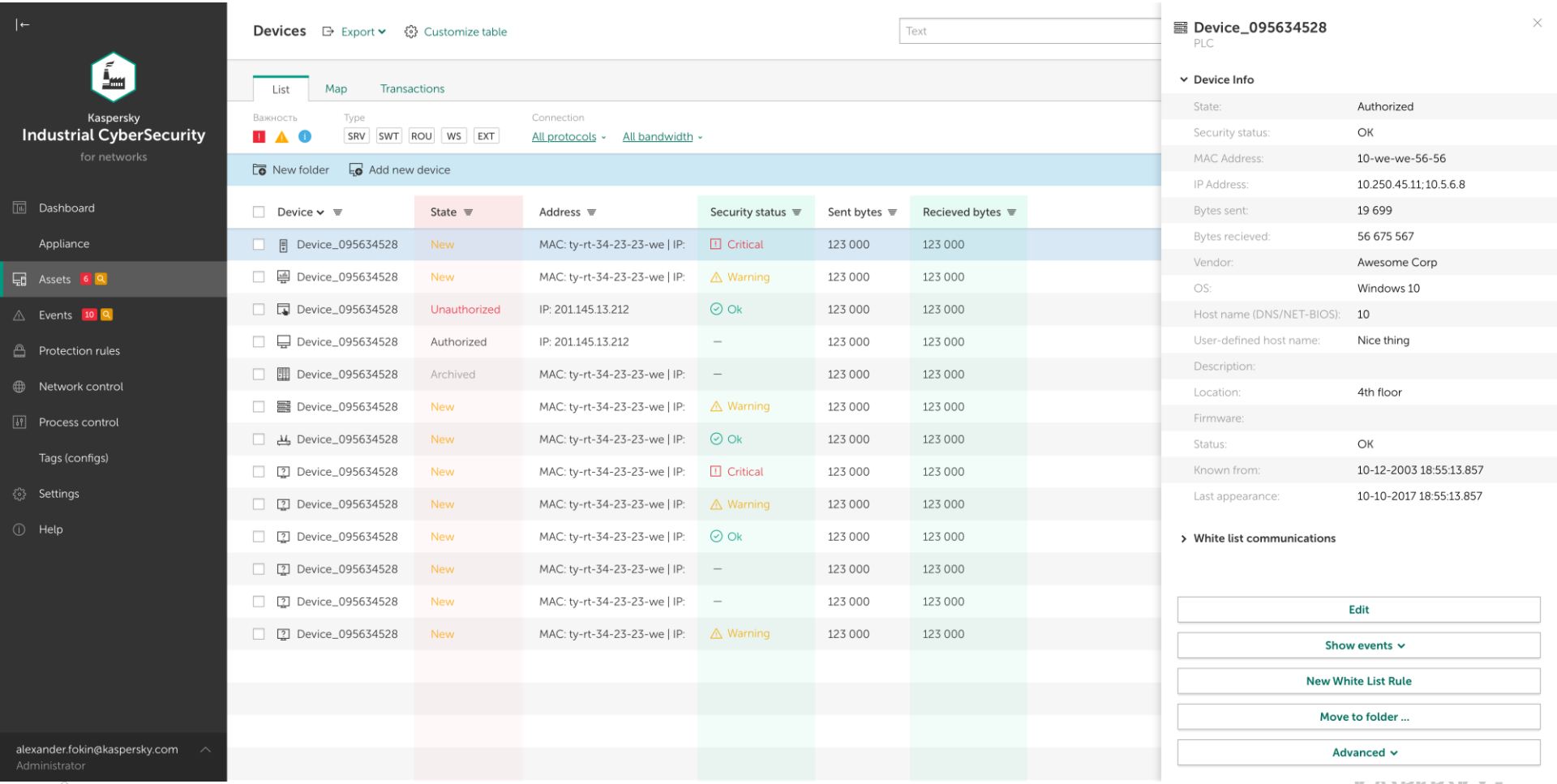
2017

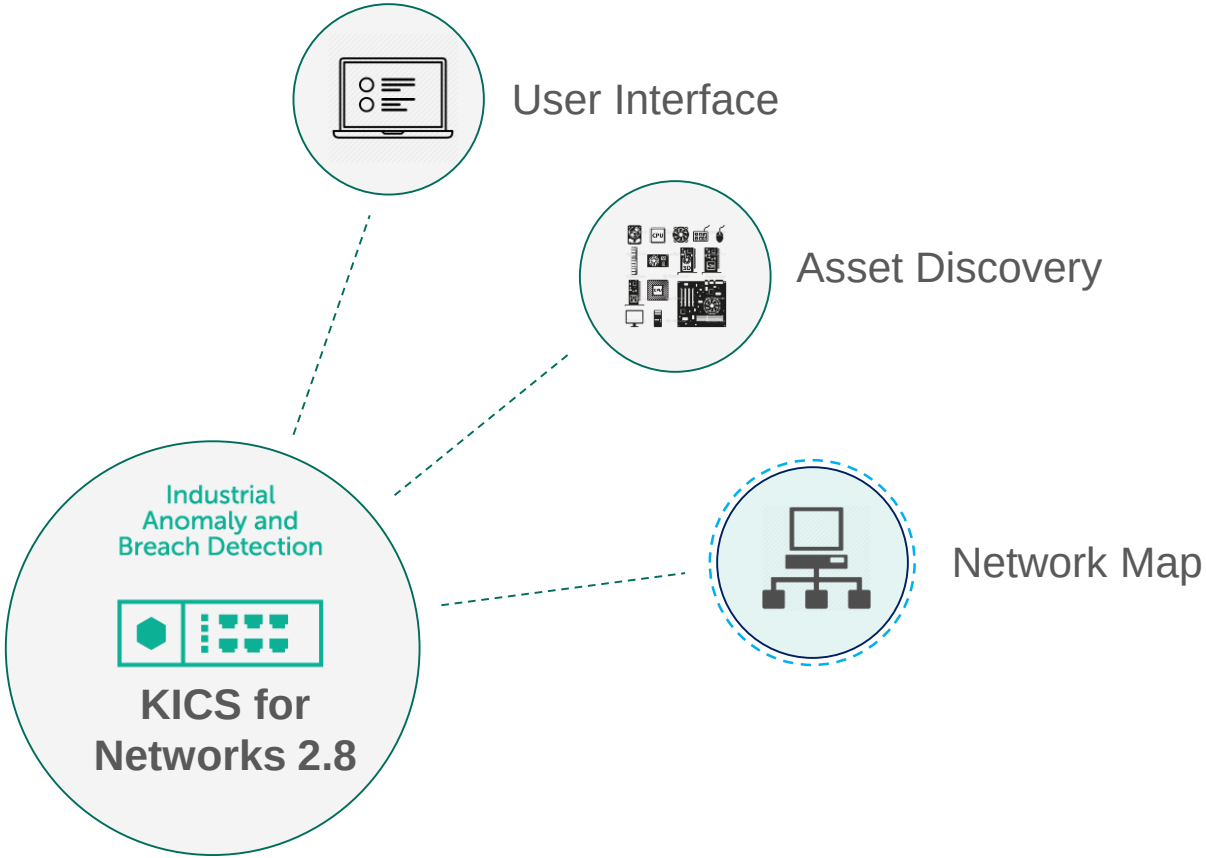
	ID	Date/time	Severity	Title	Technology	Protocol	Source	Destination
	44427	2017-11-24 11:46:02.774		FileDirectory - SUCCESS command has be...	CC	IEC 61850: MMS	192.168.2.20...	192.168.2.4:59855
	44426	2017-11-24 11:46:02.587		FileDirectory - SUCCESS command has be...	CC	IEC 61850: MMS	192.168.2.20...	192.168.2.4:59854
	44425	2017-11-24 11:46:02.287	⚠	Unauthorized network interaction detected....	NIC	BOOTP or DHC...	0.0.0.0:68	255.255.255.255:67
	44424	2017-11-24 11:46:00.263	⚠	Unauthorized network interaction detected....	NIC	BOOTP or DHC...	0.0.0.0:68	255.255.255.255:67
	44423	2017-11-24 11:45:59.722	⚠	Unauthorized network interaction detected....	NIC	IPv6		
	44422	2017-11-24 11:45:55.981	⚠	Unauthorized network interaction detected....	NIC	IPv6		
	44421	2017-11-24 11:45:55.329	⚠	Unauthorized network interaction detected....	NIC	IPv6		
	44420	2017-11-24 11:45:54.888	⚠	Unauthorized network interaction detected....	NIC	BOOTP or DHC...	0.0.0.0:68	255.255.255.255:67
	44419	2017-11-24 11:45:52.374	⚠	Unauthorized network interaction detected....	NIC	ARP		
	44418	2017-11-24 11:45:52.360	⚠	Unauthorized network interaction detected....	NIC	NetBIOS (netwo...	192.168.2.21...	192.168.2.255:138
	44417	2017-11-24 11:45:51.536	⚠	Unauthorized network interaction detected....	NIC	ARP		

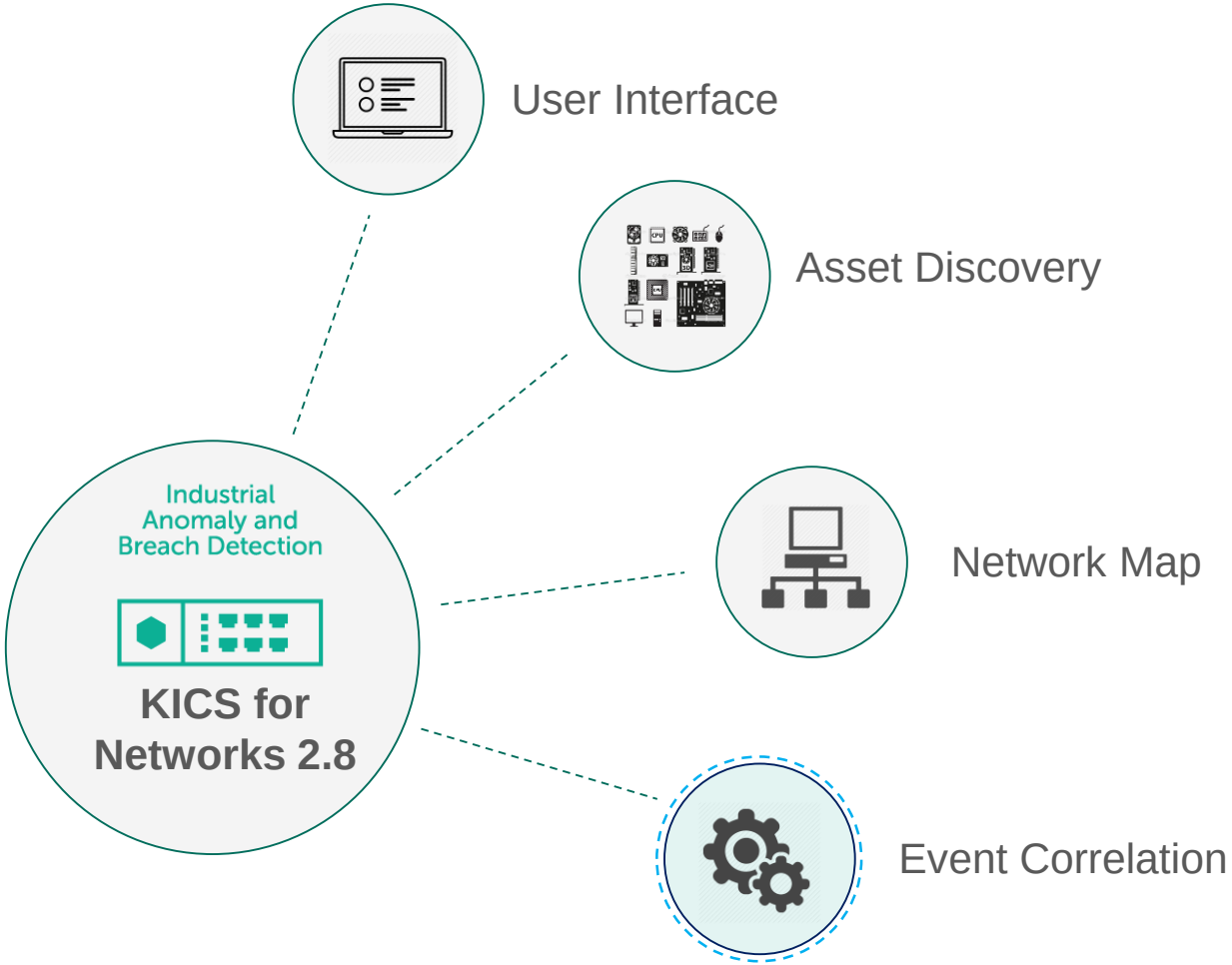
KASPERSKY lab


Kaspersky
Industrial CyberSecurity
for networks
Dashboard
Appliance
Assets 6
Events 10
Protection rules
WhiteList rules
Process rules
Tags (configs)
Settings
Help
alexander.fokin@kaspersky.com
Administrator
KICS SERVER WORKLOAD
18%
97 of 100 GB
34%
12 of 256 GB
Zusammenbruch
KICS SENSORS TRAFFIC
50 Gb/s
#01
Zusammenbruch
ASSETS
4 SCADA
11 HMI
8 Servers
134 Workstations
34 PLC
17 Switches
23 Routers
134 Others
Text
Go
SCADA with issues (2)
10.250.45.11
10.250.45.11
10.250.45.11
HMI with issues (32)
10.250.45.11
10.250.45.11
10.250.45.11
10.250.45.11
10.250.45.11
10.250.45.11
+ 24 More
Servers with issues (4)
10.250.45.11
10.250.45.11
10.250.45.11
10.250.45.11
10.250.45.11
Workstations with issues: (11)
PLC with issues: (7)
Switches with issues: (12)
Show all assets
EVENTS
1h
12h
24h
1w
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
Search for event...
Go
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Brute-force attack of Siemens S7-300 (11.11.45.68) 15:23:56(.021)
Brute-force attack of Siemens S7-300 (11.11.45.68) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Network is skanned 15:23:56(.021)
Brute-force attack of Siemens S7-300 (11.11.45.68) 15:23:56(.021)
Brute-force attack of Siemens S7-300 (11.11.45.68) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Unknown host detected by ARP (34-11-56-78-9A-BC) 15:23:56(.021)
Show all events


User Interface
Asset Discovery
Industrial
Anomaly and
Breach Detection
KICS for
Networks 2.8


Kaspersky
Industrial CyberSecurity
for networks
Dashboard
Appliance
Assets 6
Events 10
Protection rules
Network control
Process control
Tags (configs)
Settings
Help
alexander.fokin@kaspersky.com
Administrator
Devices
Export
Customize table
Text
List
Map
Transactions
Важность
Type
SRV SWT ROU WS EXT
Connection
All protocols
All bandwidth
New folder
Add new device
Device
State
Address
Security status
Sent bytes
Recieved bytes
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Critical 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Warning 123 000 123 000
Device_095634528 Unauthorized IP: 201.145.13.212 Ok 123 000 123 000
Device_095634528 Authorized IP: 201.145.13.212 – 123 000 123 000
Device_095634528 Archived MAC: ty-rt-34-23-23-we | IP: – 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Warning 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Ok 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Critical 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Warning 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Ok 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: – 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: – 123 000 123 000
Device_095634528 New MAC: ty-rt-34-23-23-we | IP: Warning 123 000 123 000
Device_095634528
PLC
Device Info
State: Authorized
Security status: OK
MAC Address: 10-we-we-56-56
IP Address: 10.250.45.11;10.5.6.8
Bytes sent: 19 699
Bytes recieved: 56 675 567
Vendor: Awesome Corp
OS: Windows 10
Host name (DNS/NET-BIOS): 10
User-defined host name: Nice thing
Description:
Location: 4th floor
Firmware:
Status: OK
Known from: 10-12-2003 18:55:13.857
Last appearance: 10-10-2017 18:55:13.857
White list communications
Edit
Show events
New White List Rule
Move to folder ...
Advanced


User Interface
Asset Discovery
Network Map
Industrial
Anomaly and
Breach Detection
KICS for
Networks 2.8

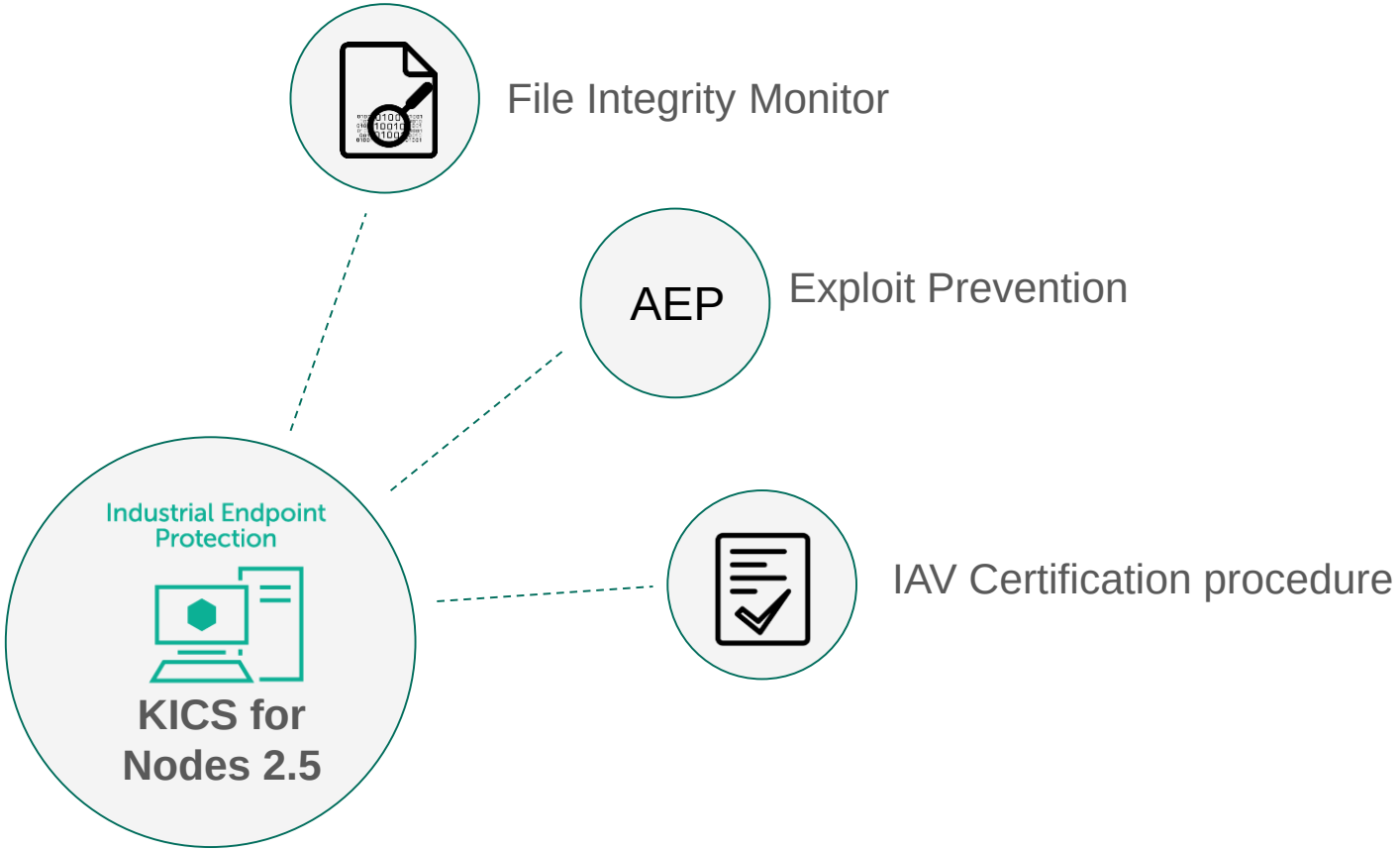

User Interface
Asset Discovery
Industrial
Anomaly and
Breach Detection
KICS for
Networks 2.8
Network Map
Event Correlation

Industrial Endpoint Protection

KICS for Nodes

2.5

Already at the Market


File Integrity Monitor
AEP
Exploit Prevention
Industrial Endpoint Protection
KICS for Nodes 2.5
IAV Certification procedure

Let’s talk!!!

Waiting for you in the Exhibition area…

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab