Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Develop Your ICS Security Product Mix With The Future In Mind

Dale Peterson, Founder of S4 Events

https://dale-peterson.com/ics-detection-market-analysis/

Set Expectations

Whatever you deploy will likely be replaced in 2 years

Play with, Pilot, Test

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Develop Your ICS Security Product Mix With The Future In Mind

Dale Peterson, Founder of S4 Events

Promises Made

Asset Inventory

Vulnerability Management

Cyber Incident Detection & Response

Passive
- Listen only

Not sufficient for asset inventory

(not to mention CMDB, change control, ...)

OT Asset Inventory Choices

Active Query: Langner OT Base, Verve, Indegy plus some passive solutions are adding active

Project Files: PAS, MDT, Honeywell

Manual Entry (which can be combined with the other methods)

This Is The Single Source of Truth


New
Passive
Solution
Asset
Mgmt
Detailed
Asset Inventory


New
“Passive”
Solution
New Assets
& Detail
PLC Project
Integrity Check
Asset
Mgmt

Dashboard
Asset Hierarchy
Asset Discovery
Inventory
Policies
Workflows
Changes
Patches
Vulnerabilities
Reports
Queries
Baselines
Search

View/Edit Assets

	Source	Location	Last Update	Vendor	Device Descrip...	Mac Address	IP Address	Status	Inventory Item	Case
	Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	XEROX CORPORATION	Printer in Copy room	00:00:01:00:00:12	10.10.1.14	Missing		17121105
	Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	ROCKWELL AUTOMATION		00:00:BC:00:00:10	10.10.1.12	Added	AB_CONTROLOGIX500...	17121105
	Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	ROCKWELL AUTOMATION		00:00:BC:00:00:11	10.10.1.13	Existing	AB_CONTROLOGIX500...	17121105
	Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	HEWLETT PACKARD		00:01:E6:29:8D:16		Transient		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	IDIS CO., LTD.		00:03:22:14:39:16		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	POLYCOM		00:04:F2:4C:D0:9D		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	ICP ELECTRONICS INC.		00:08:9B:EF:47:7A		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:0A:F7:4E:27:08		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:0A:F7:86:90:B2		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	VMWARE, INC.		00:0C:29:1A:2F:82		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	VMWARE, INC.		00:0C:29:D3:6D:C8		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	CISCO SYSTEMS, INC		00:0C:85:33:23:C0	192.168.1.4	Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:6C		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:8C		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:8E		Added		17121101
	A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:90		Added		17121101
	A_Network Devices	Company » Plant A » Unit	2017-10-17	SYNOLOGY		00:11:32:35:2C:ED		Added		17121101

Dashboard
Asset Hierarchy
Asset Discovery
Inventory
Policies
Workflows
Changes
Patches
Vulnerabilities
Reports
Queries
Baselines
Search

View/Edit Assets

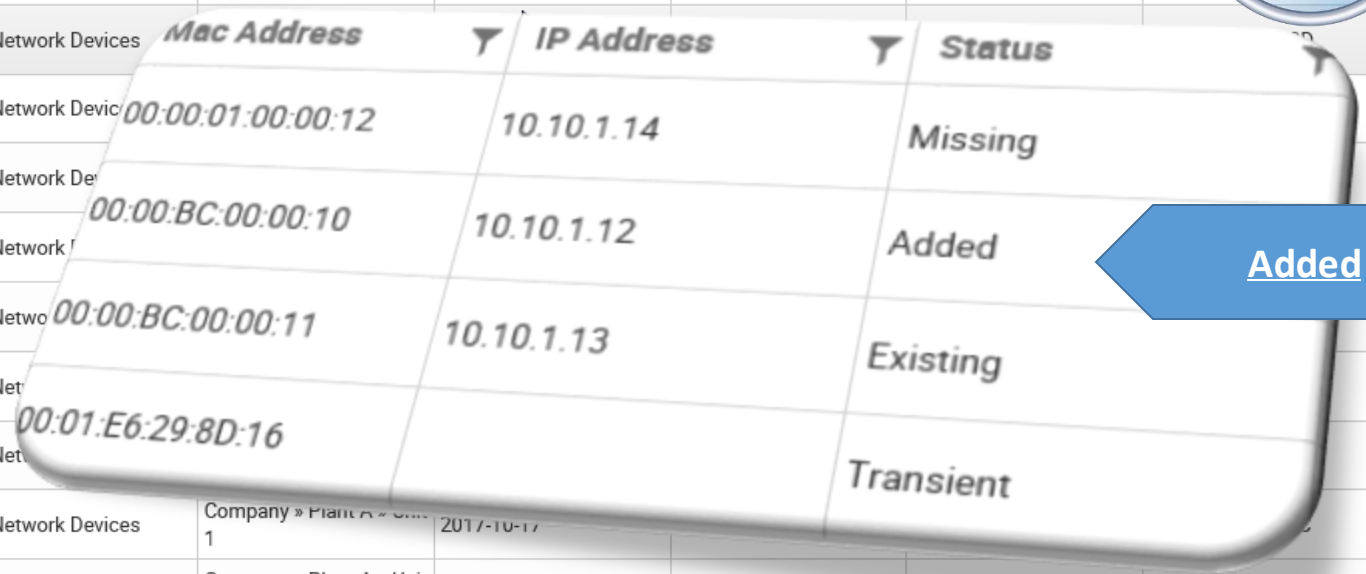
Source	Location	Last Update	Vendor	Device Descrip...	Mac Address	IP Address	Status	Inventory Item	Case
Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	XEROX CORPORATION	Printer in Copy room	00:00:01:00:00:12	10.10.1.14	Missing		17121105
Passive Network Detection	Company » Plant A » Unit 1				00:00:10	10.10.1.12	Added	AB_CONTROLOGIX500...	17121105
Passive Network Detection	Company » Plant A » Unit 1				:11	10.10.1.13	Existing	AB_CONTROLOGIX500...	17121105
Passive Network Detection	Company » Plant A » Unit 1				0:16		Transient		17121101
Passive Network Detection	Company » Plant A » Unit 1				9:16		Added		17121101
A_Network Devices					D0:9D		Added		17121101
A_Network Devices					:47:7A		Added		17121101
A_Network Devic					E:27:08		Added		17121101
A_Network De					86:90:B2		Added		17121101
A_Network De					:1A:2F:82		Added		17121101
A_Network Devices	1				29:D3:6D:C8		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	CISCO SYSTEMS, INC		00:0C:85:33:23:C0	192.168.1.4	Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:6C		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:8C		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:8E		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:90		Added		17121101
A_Network Devices	Company » Plant A » Unit	2017-10-17	SYNOLOGY		00:11:32:35:2C:ED		Added		17121101

Source | Location
Passive Network Detection | Company » Plant A » Unit 1
Passive Network Detection | Company » Plant A » Unit 1
Passive Network Detection | Company » Plant A » Unit 1
Passive Network Detection | Company » Plant A » Unit 1

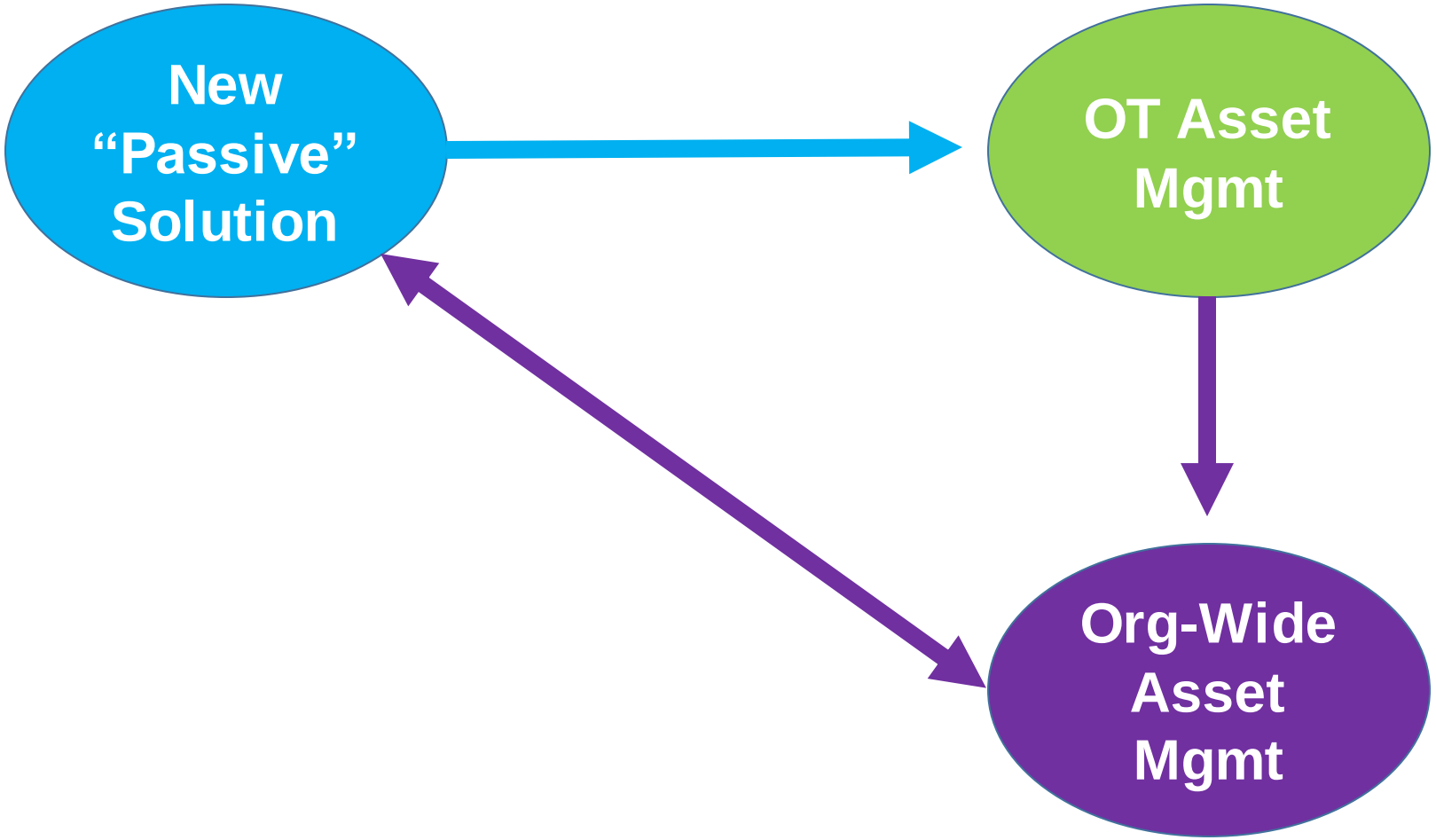
Dashboard
Asset Hierarchy
Asset Discovery
Inventory
Policies
Workflows
Changes
Patches
Vulnerabilities
Reports
Queries
Baselines
Search

View/Edit Assets

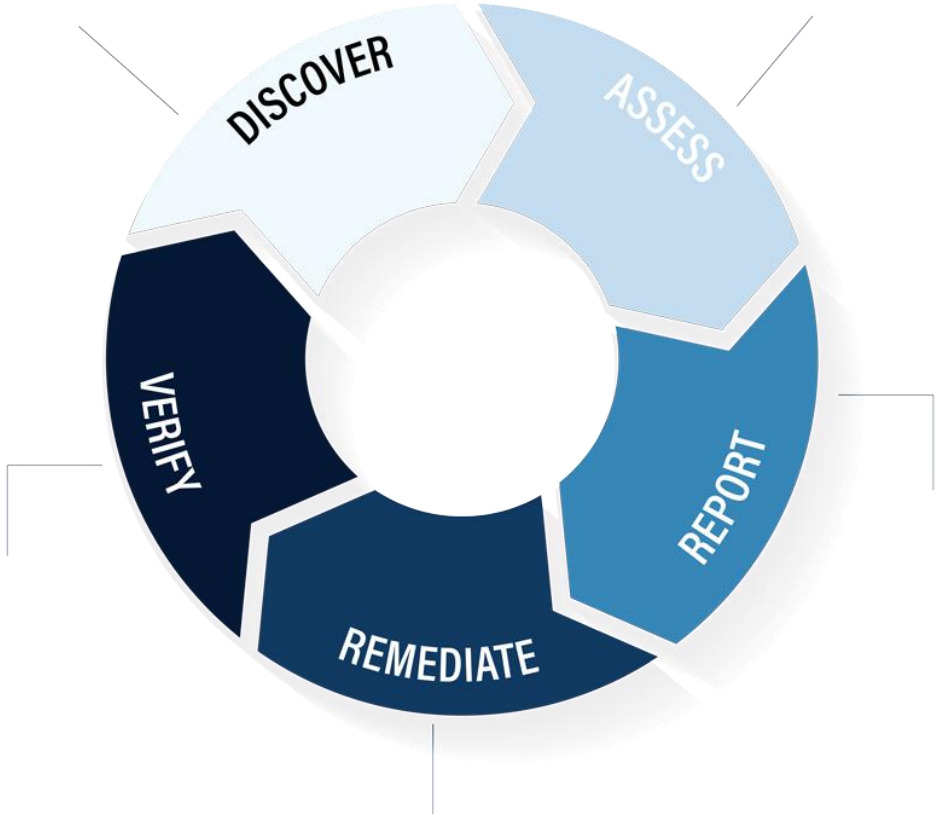
Source	Location	Last Update	Vendor	Device Descrip...	Mac Address	IP Address	Status	Inventory Item	Case
Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	XEROX CORPORATION	Printer in Copy room	00:00:01:00:00:12	10.10.1.14	Missing		17121105
Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	ROCKWELL AUTOMATION		00:00:BC:00:00:10	10.10.1.12	Added	AB_CONTROLOGIX500...	17121105
Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	ROCKWELL AUTOMATION		00:00:BC:00:00:11	10.10.1.13	Existing	AB_CONTROLOGIX500...	17121105
Passive Network Detection	Company » Plant A » Unit 1	2017-10-17	HEWLETT PACKARD		00:01:E6:29:8D:16		Transient		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	IDIS CO., LTD.		00:03:2[illegible]:14:39:16		Added		17121101
A_Network Devices							Added		17121101
A_Network Devic							Added		17121101
A_Network De							Added		17121101
A_Network									17121101
A_Netwo									17121101
A_Net							Added		17121101
A_Net						192.168.1.4	Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17					Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:8C		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:8E		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	BROADCOM		00:10:18:B8:18:90		Added		17121101
A_Network Devices	Company » Plant A » Unit 1	2017-10-17	SYNOLOGY		00:11:32:35:2C:ED		Added		17121101



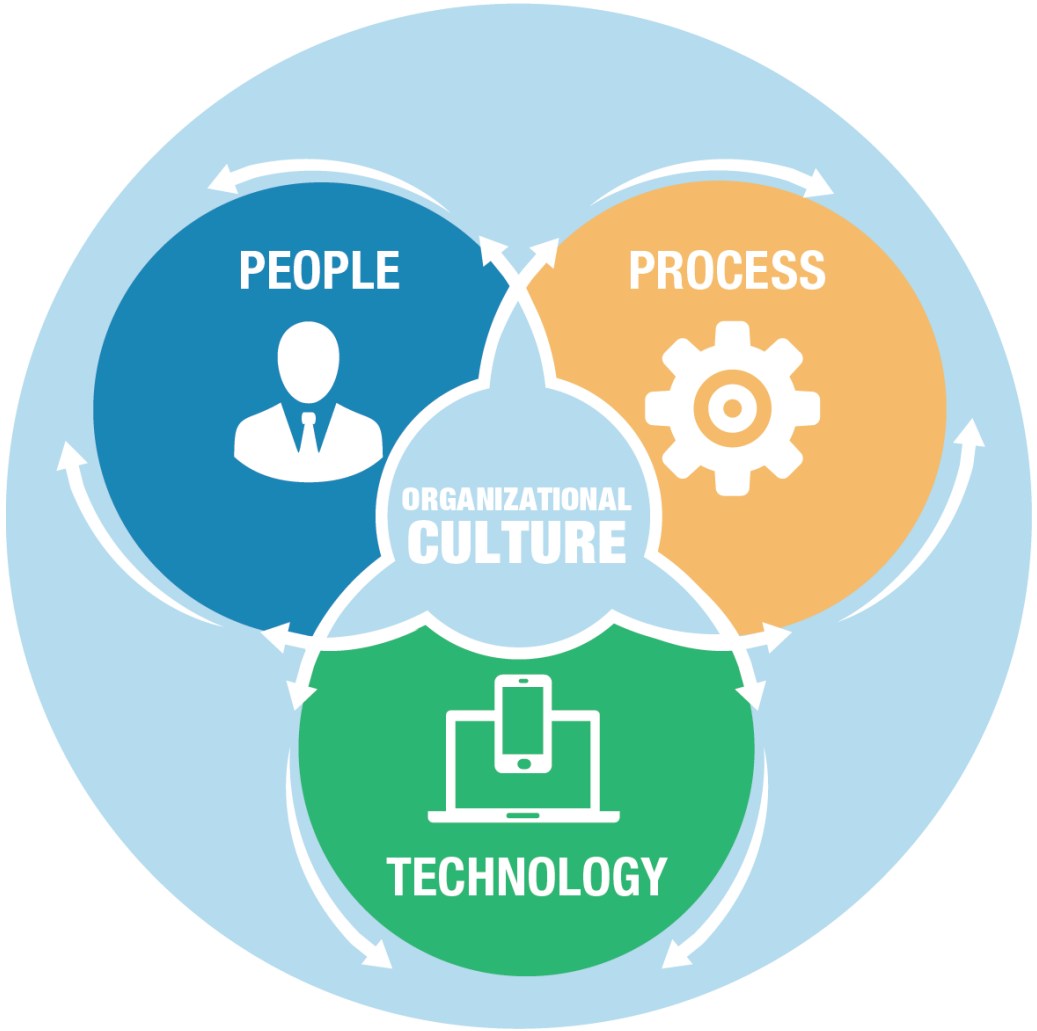
Added : Detected Device Added To Network


New
“Passive”
Solution
OT Asset
Mgmt
Org-Wide
Asset
Mgmt
ServiceNow

Vulnerability Management



Detection / Incident Response




12:53:58
T22 COUNTDOWN

“

Passive network monitoring is one of many data sources for detection AND it does not score highly in efficiency or effectiveness.

OT Detection Sources

Passive Network Monitoring

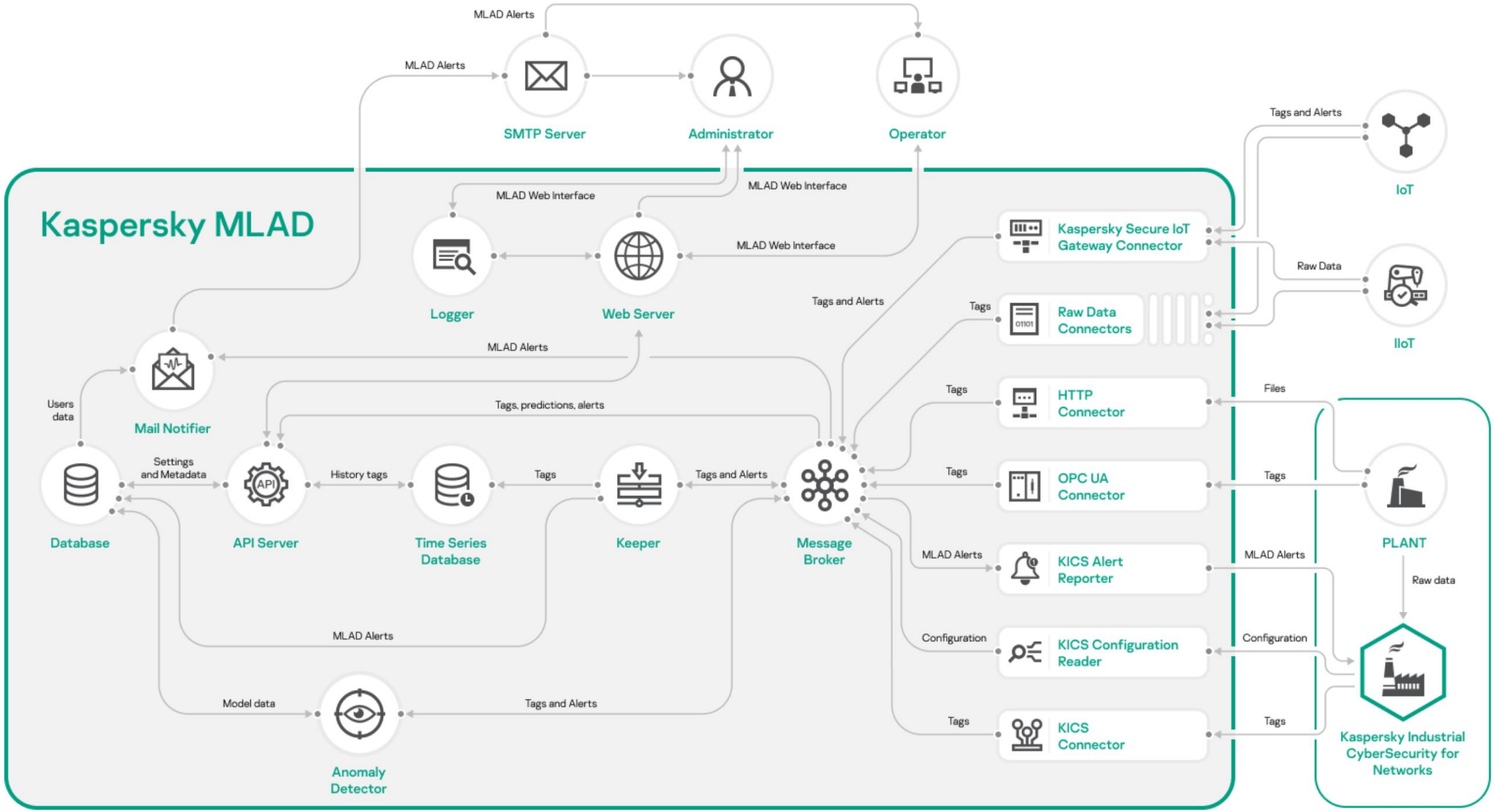
Endpoint Protection Activity

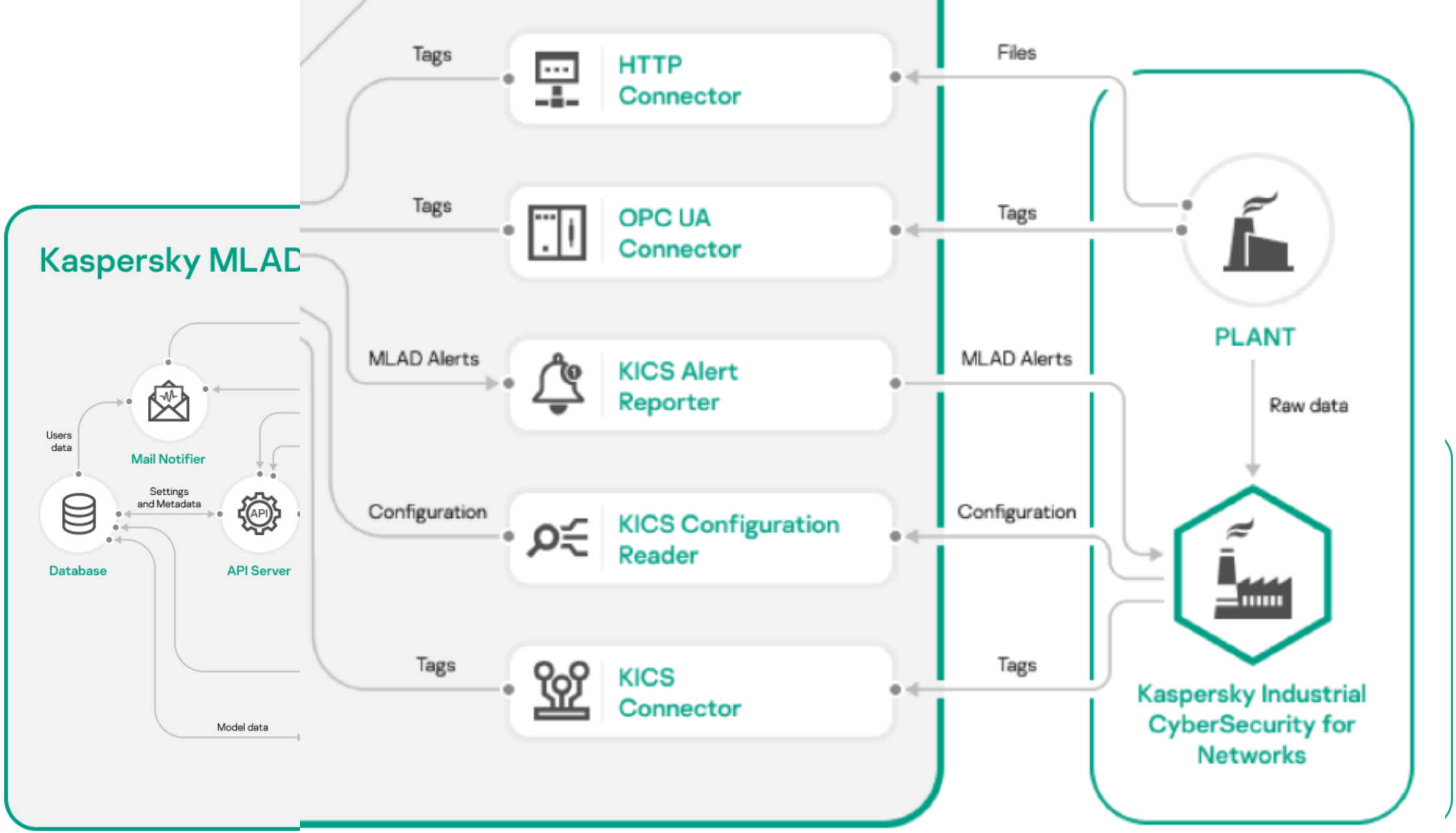
Firewall / Security Perimeter Logs

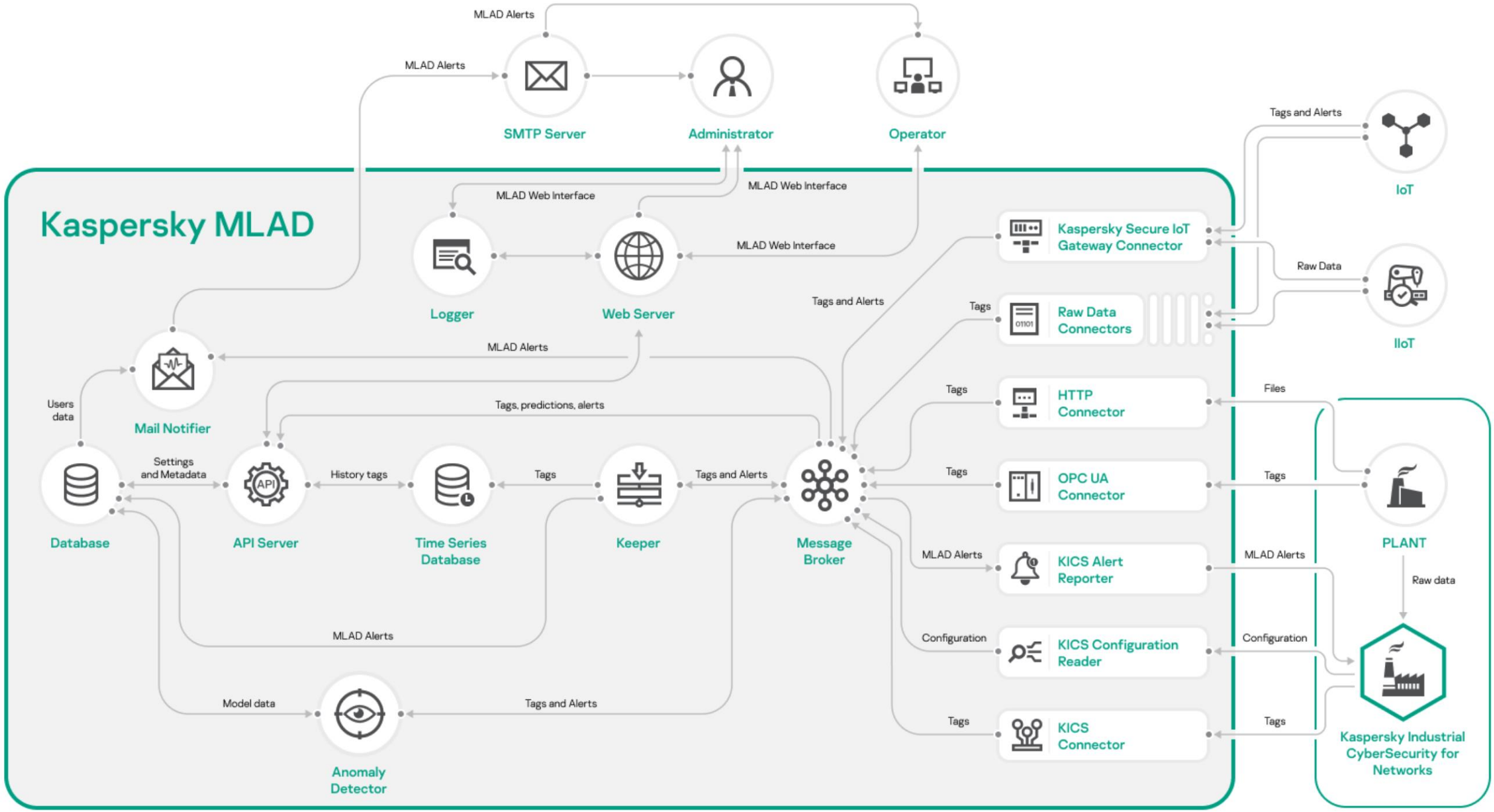
Active Directory User Management

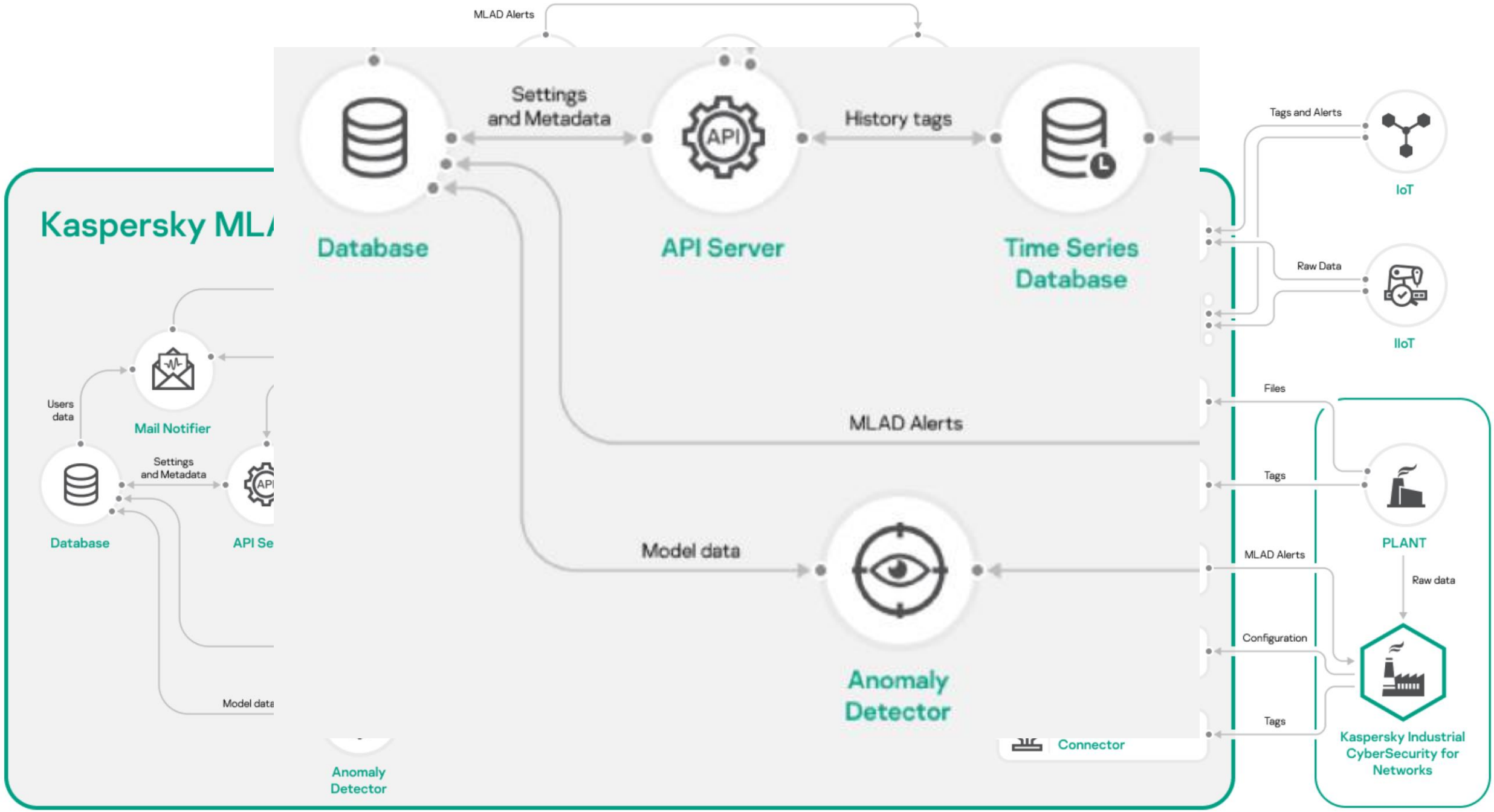
ICS Application Alerts & Events

Historical Data


MLAD Alerts
MLAD Alerts
SMTP Server
Administrator
Operator
Kaspersky MLAD
MLAD Web Interface
MLAD Web Interface
MLAD Web Interface
Logger
Web Server
Tags and Alerts
IoT
Kaspersky Secure IoT Gateway Connector
Raw Data
Tags
Raw Data Connectors
IIoT
MLAD Alerts
Users data
Mail Notifier
Tags, predictions, alerts
Tags
HTTP Connector
Files
Settings and Metadata
History tags
Tags
Tags and Alerts
Tags
OPC UA Connector
Tags
PLANT
Database
API Server
Time Series Database
Keeper
Message Broker
MLAD Alerts
KICS Alert Reporter
MLAD Alerts
Raw data
MLAD Alerts
Configuration
KICS Configuration Reader
Configuration
Model data
Tags and Alerts
Tags
KICS Connector
Tags
Anomaly Detector
Kaspersky Industrial CyberSecurity for Networks


Kaspersky MLAD
Users data
Mail Notifier
Settings and Metadata
API
Database
API Server
Model data
Tags
HTTP Connector
Files
Tags
OPC UA Connector
Tags
PLANT
MLAD Alerts
KICS Alert Reporter
MLAD Alerts
Raw data
Configuration
KICS Configuration Reader
Configuration
Tags
KICS Connector
Tags
Kaspersky Industrial CyberSecurity for Networks


MLAD Alerts
MLAD Alerts
SMTP Server
Administrator
Operator
Kaspersky MLAD
MLAD Web Interface
MLAD Web Interface
MLAD Web Interface
Logger
Web Server
Tags and Alerts
IoT
Kaspersky Secure IoT Gateway Connector
Raw Data
Tags
Raw Data Connectors
IIoT
MLAD Alerts
Users data
Mail Notifier
Tags, predictions, alerts
Tags
HTTP Connector
Files
Settings and Metadata
History tags
Tags
Tags and Alerts
Tags
OPC UA Connector
Tags
PLANT
Database
API Server
Time Series Database
Keeper
Message Broker
MLAD Alerts
KICS Alert Reporter
MLAD Alerts
Raw data
MLAD Alerts
Configuration
KICS Configuration Reader
Configuration
Model data
Tags and Alerts
Tags
KICS Connector
Tags
Anomaly Detector
Kaspersky Industrial CyberSecurity for Networks


MLAD Alerts
Settings and Metadata
History tags
Database
API Server
Time Series Database
Tags and Alerts
IoT
Raw Data
IIoT
Files
MLAD Alerts
Tags
PLANT
Model data
MLAD Alerts
Raw data
Configuration
Anomaly Detector
Tags
Kaspersky Industrial CyberSecurity for Networks
Connector
Kaspersky MLA
Users data
Mail Notifier
Settings and Metadata
Database
API Se
Model data
Anomaly Detector

Enterprise Detection and Incident Response

Enterprise SOC, SIEM or SOAR

Do you already have one?

Do you want to run and staff and OT and Enterprise SOC?

Most attacks on the ICS come through the Enterprise

Enterprise wide, including ICS / OT, is required

SIEM / OT detection integration is minimal today. Large users will cause this to progress

Set Expectations

Whatever you deploy will likely be replaced in 2 years

Play with, Pilot, Test

Be Proactive

Develop and present a strategy to Executive Management

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Thank you!

peterson@digitalbond.com, dale-peterson.com, @digitalbond

S4x20: Jan 21 – 23 in Miami South Beach, see s4xevents.com

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky