

kontron

The Power of IoT

Explore the Kontron Group

We are a fast-moving multinational technology leader.

Kontron Cybersecurity

Portfolio



KontronOS

CRA / NIS 2 ready minimalistic
Linux OS with deep Hardware
integration

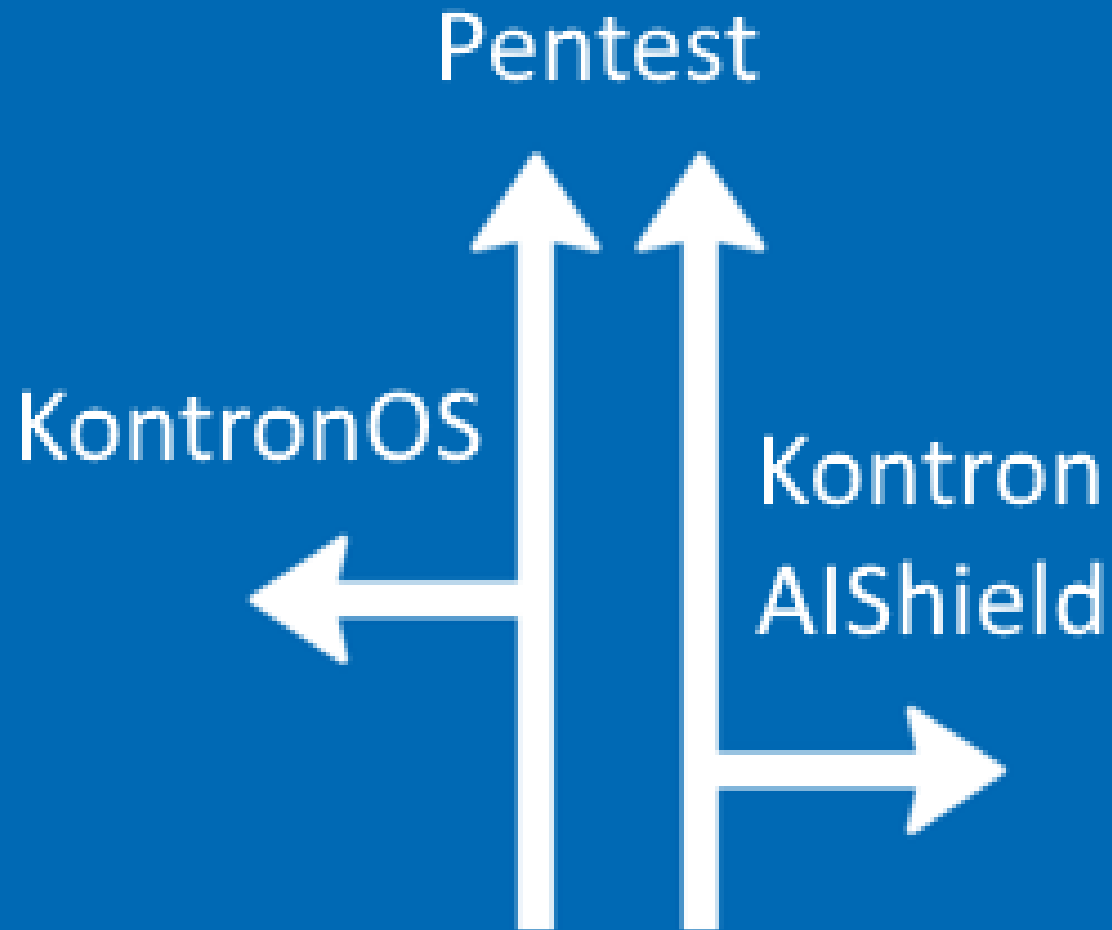
Pentests

Regular pentests designed for
embedded devices

KontronAIShield

- Appliance based
- KontronOS App based
- Security Operations Center

The signpost in the security landscape



Pentest:

- Shows which systems have problems
- Describes solutions
- Focus on embedded hardware
- Focus on recurring tests

Kontron OS:

- For new designs and Greenfield
- Fulfills most of the security requirements

KontronAIShield:

- For existing setups that need to be retrofitted
- Secure not only individual systems but entire networks



KontronOS – Key features

The Secure Long Term Supported Platform for your application
combining Hardware and Software

- › KontronOS is – CRA/NIS 2 Ready for IEC 62443-4-2 and IEC 62443-4-1
- › Possibility to rollback to the last working version
- › Same manageability regardless it On or Off line (Service technician friendly interface)
- › Possibility to rollback to the last working version
- › Support of firmware updates (e.g. uboot)
- › Hardened uBoot, Hardened read-only OS
- › Encrypted delta (saving bandwidth) updates for OS + Applications
- › Customer specific set of signing keys.
- › Release and Development build pipelines
- › Binding of application to device (in case of Docker e.g.: bundling a well tested set of Docker and images)
- › Samples for application bundles like: QT, Docker(Compose), NodeRed ...
- › Local management UI
- › Remote Web interface (over Server or USB OTG)
- › Remoting (Remote access of Server with ssh or xRDP)
- › Support of encrypted USB update sticks in the field

KontronOS - Chain of trust

on iMX8

iMX8 SoM with eMMC

actual hardware fuses having the checksum of 4 public keys burned (read only)

Bootloader 1

- uBoot fit image with 4 Keys checked by CPU at boottime (signed with private Key 2)
- Image contains the public OS key for the read only OS partition and Linux fit image

Bootloader 2

.
. .
. .

Partition 1

- Containing Kernel Fit Image (signed with private OS key)
- Is only booted from uBoot if hash/signature are valid
- Checks hash of RootFS partition (Read only)


Partition 2

.
. .
. .

Application Bundles are also signed with the OS key, Rauc is checking this hashes/signatures during installation, while still allowing delta updates.

Pentest

Our Solution

- 
- › We offer a comprehensive security check with various elements:
 - › Pentest: Identification and analysis of vulnerabilities of individual and specially developed components in accordance with regulatory requirements such as CRA/NIS2.
 - › Phishing: Testing employee security awareness through phishing and vishing attacks.
 - › Regular security tests: Optional subscription model for continuous security monitoring.

KontronAIShield

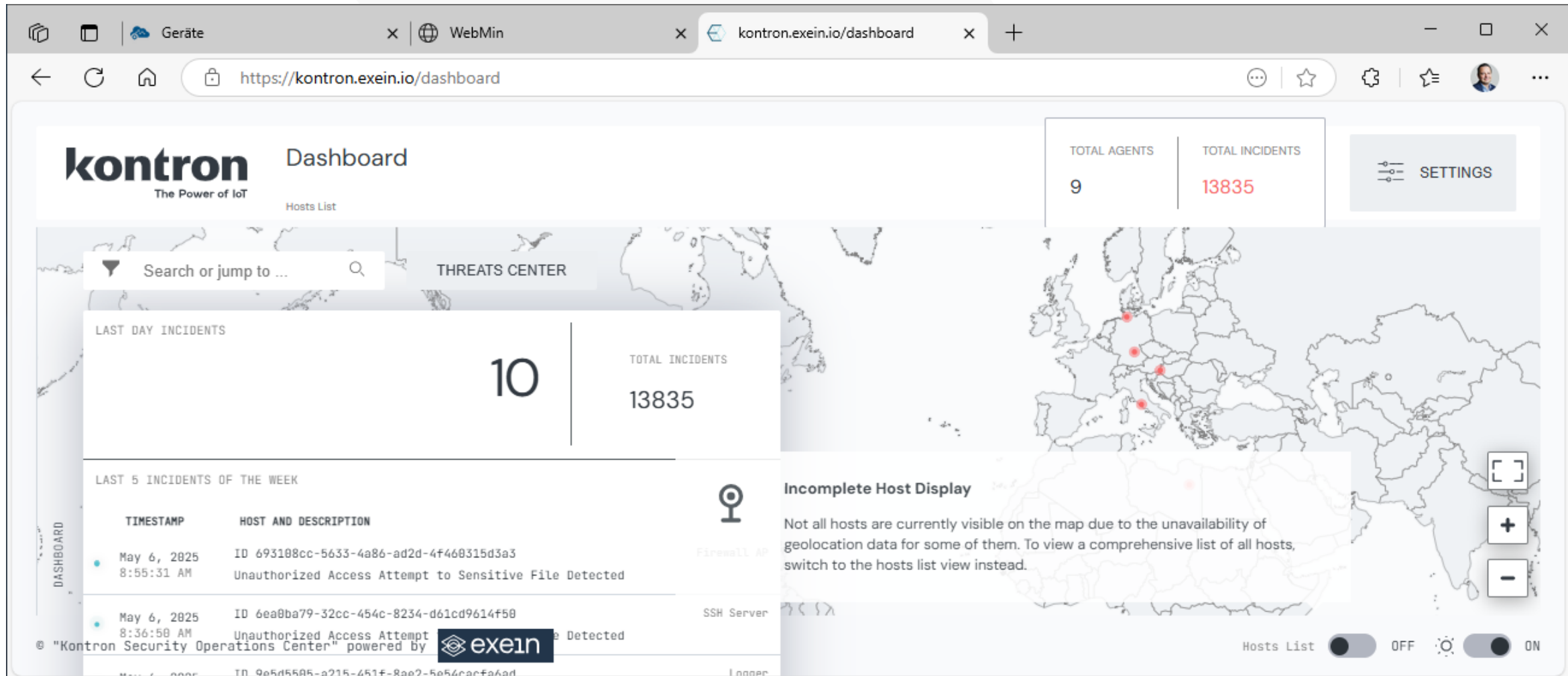
Is an **AI-based firewall/IDS/threat** prevention application **with zero-touch provisioning**.

It consists of four mostly optional components::

- Our **KontronAIShield Appliance**: an embedded system with 2 Ethernet ports that can simply be ‘plugged’ into an Ethernet cable without having to reconfigure the existing network - easy to handle.
 - It also acts as a gatekeeper per end device, which is particularly useful for IDS capabilities.
 - AI makes it possible to monitor encrypted data traffic and recognise threats.
 - Our system can block the attack so that the IT department has time to react. The artificial intelligence in AI-IDS not only makes it possible to detect and combat known threats, but also to detect unknown, new threats by evaluating the behaviour of the potential threat.



- Our KontronAIShield Security Operations Centre, which enables incidents to be reported in accordance with



- Our **KontronAIShield App** for KontronOS, which makes it possible, for example, to securely manage containerised solutions and extend them with an IDS system.
 - AI is used here to monitor application resource access from the perspective of the kernel and to intervene if necessary.
 - IDS messages are forwarded to the backend as with the appliance
- Our **KontronGrid**, with which AI-IDS fleets can be managed and supplied with new trained AI networks.