About Document

This document describes the baseline of the requirements for the successful deployment of the AI-Agent to remote environments and describes the list of hardware and software prerequisites.

1. AI Agent Description

The EdgeLabs Agent is the agent that continuously verifies network connectivity on the Edge Host/IoT Gateway performance and configuration.

AI-Agent - is a container-based application that holds inside threat detection logic on board and can be deployed to Linux-based operating systems through runtimes like Docker, Kubernetes, or similar solutions. The container is implemented in Rust and Python programming language and holds compressed AI-models on board.

2. Prerequisites

In order to successfully deploy EdgeLabs.AI cyber-security solution here is a list of requirements that should be fulfilled in the table below:

No.	Requirement	Description
1.	Connectivity to EdgeLabs API on Cloud	Cloud-Based API coordinates AI-Agent deployments, provides reporting about threats, and allows to expose results on Dashboard
2.	Access to Edge host network (default network interface - in/out)	It's important to understand that AI-Agent verifies traffic by sniffing edge nodes. So to guarantee protection and firewalling, the Agent requires sniffing capability.
3.	Access to Edge processes and installations	For malware detection and protection it's important to have access to OS-wide processes on the Edge Host.
4.	Access to Filesystem	Access to the filesystem is required for quarantining capabilities and for periodic

		malware verification of the software installed on the host.
5.	Linux Kernel	Linux Kernels 4.14 or higher, different variations of OS (e.g. Ubuntu, Debian, SUSE, CentOS). Agent supports deployments to older Kernel versions than 4.14 however the functionality for EDR and IPS might be not guaranteed.
6.	Docker runtime	Any flavors of Docker runtime e.g. Kubernetes, Docker Swarm, and others
7.	x86_64 or ARM_64 platforms	Container supports both architectures and based on requirements required registry URL should be selected. Also, multiplatform containers are supported too.
8.	Host minimal requirements: 512Mb RAM, and 1 CPU with base frequency 1.0GHz	These requirements are mostly based on runtime traffic volume and network data processing capability.
9.	700Mb on disk space and total bandwidth for installation	These requirements exclude Docker installation. Please note: this actually includes network bandwidth consumption.

3. PoC process and pre-validation phase

The requirements above do not give 100% guarantee that all cybersecurity capabilities will be preserved after deployment Agent to a custom Linux environment or modified version of Kernel. For example Edge Orchestrators often use restricted and customized image distrubutions, that would cause some exceptional situations or missing kernel modules.

Stages for the integration phase:

1. Requirements document evaluation and verbal communication with client ;
2. Provide dry-run Agent on the same Linux environments to understand limitations of kernels. It can be remote SSH access to the host with assistance from the AI EdgeLabs team.
3. Deployment to all client hosts if previous step showed now issues;

Deployment Example:

A E-Commerce company orchestrates Edge hosts with deployed AI apps with the K3S (Kubernetes for resource-constrained devices). The edge hosts have both Raspberry Pi (ARM) and Celeron (x86) architectures with Linux on board. These boxes are located inside shops in multiple regions across the US.

EdgeLabs.AI Agent could be easily installed in this case with the Kubernetes-based installer and helm chart by using a multiplatform (ARM + x86) build. So installation would take a few minutes with the ‘helm install’ command on the Kubernetes Cluster.
With this installation, the AI-Agent will be installed as a DaemonSet (one instance per node), and would protect all the in/out network traffic. Malware Detection capability will verify and check all the software that is running on the node.