metadata name: [policy name] Mandatory KubeArmorHostPolicy Spec Diagram — No Namespace in the case of KubeArmorHostPolicy severity: [1-10] Key Difference between KubeArmorPolicy and KubeArmorHostPolicy tags: ["tag1", "tag2", ...] Mandatory if these are not defined in each rule KubeArmorPolicy — action: {Allow | Audit | Block} message: "message here" KubeArmorHostPolicy — action: {Allow | Audit | Block} action: {Audit | Block} nodeSelector nodeSelector (not selector) In the case that 'fromSource' is defined, then 'Allow' is available. matchLabels Mandatory key=value capabilities network process severity: [1-10] severity: [1-10] severity: [1-10] tags: ["tag1", "tag2", ... tags: ["tag1", "tag2", ... tags: ["tag1", "tag2", ...] tags: ["tag1", "tag2", ...] Optional Optional Optional Optional message: "message here" message: "message here" action: {Audit | Block} action: {Audit | Block} action: {Audit | Block} matchPaths matchPaths matchProtocols matchCapabilities path: [absolute file path] path: [absolute executable path] protocol: { tcp | udp | icmp } capability: { net_raw } ownerOnly: [true|false] readOnly: [true|false] fromSource fromSource ownerOnly: [true|false] fromSource path: [absolute executable path] path: [absolute executable path] List fromSource List path: [absolute executable path] severity: [1-10] severity: [1-10] path: [absolute executable path] List tags: ["tag1", "tag2", ...] tags: ["tag1", "tag2", ...] severity: [1-10] Optional Optional message: "message here" message: "message here" tags: ["tag1", "tag2", ...] severity: [1-10] Optional action: {Audit | Block} action: {Audit | Block} tags: ["tag1", "tag2", ...] message: "message here" Optional action: {Audit | Block} message: "message here" action: {Audit | Block} matchDirectories matchDirectories dir: [absolute directory path] dir: [absolute directory path] recursive: [true|false] recursive: [true|false] ownerOnly: [true|false] readOnly: [true|false] ownerOnly: [true|false] fromSource fromSource List path: [absolute executable path] path: [absolute executable path] severity: [1-10] severity: [1-10] tags: ["tag1", "tag2", ...] Optional tags: ["tag1", "tag2", …] message: "message here" Optional i message: "message here" action: {Audit | Block} action: {Audit | Block} matchPatterns matchPatterns pattern: [regex pattern] pattern: [regex pattern] ownerOnly: [true|false] readOnly: [true|false] ownerOnly: [true|false] List severity: [1-10] tags: ["tag1", "tag2", ...] severity: [1-10] Optional tags: ["tag1", "tag2", ...] message: "message here" Optional action: {Audit | Block} ı message: "message here" action: {Audit | Block}