**Kubernetes static code analysis**

Unique rules to find Security Hotspots in your KUBERNETES code

### [Mounting sensitive file system paths is security-sensitive](https://rules.sonarsource.com/kubernetes/RSPEC-6433)

[Security Hotspot](https://rules.sonarsource.com/kubernetes/RSPEC-6433)

### [Using host operating system namespaces is security-sensitive](https://rules.sonarsource.com/kubernetes/RSPEC-6431)

[Security Hotspot](https://rules.sonarsource.com/kubernetes/RSPEC-6431)

### [Allowing process privilege escalations is security-sensitive](https://rules.sonarsource.com/kubernetes/RSPEC-6430)

[Security Hotspot](https://rules.sonarsource.com/kubernetes/RSPEC-6430)

### [Exposing Docker sockets is security-sensitive](https://rules.sonarsource.com/kubernetes/RSPEC-6429)

[Security Hotspot](https://rules.sonarsource.com/kubernetes/RSPEC-6429)

### [Running containers in privileged mode is security-sensitive](https://rules.sonarsource.com/kubernetes/RSPEC-6428)

[Security Hotspot](https://rules.sonarsource.com/kubernetes/RSPEC-6428)

### [Setting capabilities is security-sensitive](https://rules.sonarsource.com/kubernetes/RSPEC-5849)

[Security Hotspot](https://rules.sonarsource.com/kubernetes/RSPEC-5849)

### [Kubernetes parsing failure](https://rules.sonarsource.com/kubernetes/RSPEC-2260)

[Code Smell](https://rules.sonarsource.com/kubernetes/RSPEC-2260)