# Security Service

Security for your Open Source infrastructure



**Survey and analysis for all Open Source components**

**Security audits**

**Taking inventory and software management**

**Active monitoring**

**Active security and patch management**

**24x7 support with guaranteed service level agreements**

**Configuration management**

**Software deployment**

**To ensure a smooth working environment, the extensive usage of Open Source software generally also needs concepts for taking inventory, software management, maintenance and software deployment.**

**We provide you with substantial services and solutions.**

- What Open Source projects and software components are being used in our company's infrastructure?
- Are we using old or outdated Open Source software, that is not getting patched or updated anymore?
- Where does Open Source software get utilized as the central component?
- What part of our business depends on these Open Source applications? Could there possible be risks and how can we get rid of them?
- Do we have a reliable and active security and patch management?
- How do we monitor and administrate our Open Source infrastructure?
- Are there business risks on the account of licence conflicts?
- How do we make sure that we get support for Open Source software, which has no applicable manufacturer support available?

**For our services we use data content provided by the Black Duck® KnowledgeBase™.**

The BlackDuck® KnowledgeBase™ is the world's most extensive database for Open Source software. It goes back more than 10 years ago and contains more than 2+ million Open Source projects out of 8500+ sources. Furthermore included are more than 2400 software licenses with security vulnerabilities, license texts, as well as dozens of attribute and license requests. New versions and the associated metadata is constantly being updated.