PERCONA Database Security Assessment

What if you could...

- Identify vulnerabilities and weaknesses in your database systems?
- Meet compliance requirements?
- Strengthen security measures?
- Protect sensitive data and enhance customer trust?

A Percona Database Security Assessment may include, but is not limited, to the following:

- Password management
- User access control
- Patch management
- Network security
- Kernel security modules
- intrusion detection installed
- Hosts vulnerable to meltdown / SPECTRE
- Data backup and disaster recovery
- Antivirus and anti-malware
- Physical security
- Incident response
- Vendor security
- Monitoring and logging
- Encryption at rest

A Percona Database Security Assessment enables you to reduce risks and improve the overall security of your database systems.

The Percona team will assess your environment, evaluating overall security as well as your adherence to identified security requirements and/or compliance regulations. The analysis involves a thorough vetting of your database environment, configuration, policies, and procedures to identify potential vulnerabilities, weaknesses, and risks.

Once complete, our team will provide you with recommendations for improvement. You can opt to implement these measures on your own, or if needed, our team is readily available to offer support.

Key benefits of a Percona Database Security Assessment

Identify vulnerabilities: Identify vulnerabilities and weaknesses in your database system that could potentially be exploited by malicious actors. A Percona Database Security Assessment examines:

- Database configuration
- Access controls
- Authentication mechanisms
- Encryption
- Patch levels, and other security settings.

Prioritize risk mitigation: Discover high-risk areas so you can focus your resources on mitigating the most critical risks first.

Enhance security posture: Get tailored recommendations for proactive measures you can take to strengthen your security posture, such as:

- Implementing additional security controls
- Improving access controls
- Encrypting sensitive data
- Applying patches and updates
- Establishing robust security policies and procedures.

Protect sensitive data: Mitigate the risk of data breaches, data leaks, or data loss, and better protect sensitive data such as customer information, intellectual property, financial records, and more.

Improve customer trust: Demonstrate a strong commitment to database security and ensure customers, partners, and stakeholders that their data is protected and their information is handled confidentiality and with integrity.

Save costs: Prevent security incidents and associated costs, such as legal liabilities, financial losses, and reputational damage.

073123

For more information, contact us at +1-888-316-9775 (USA), +44 203 608 6727 (Europe) or via email at sales@percona.com.