Top 10 Salesforce DevOps Cybersecurity Best Practices

autorabit

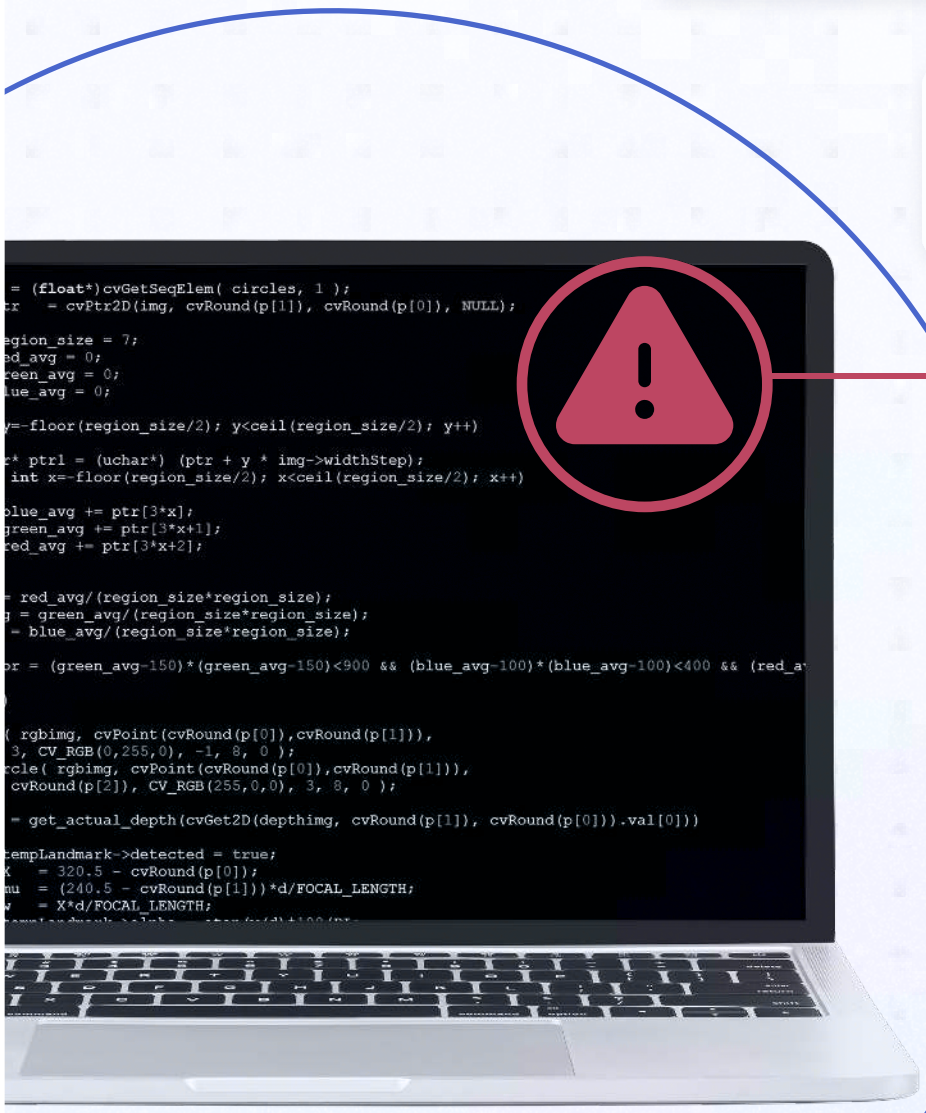
These intentional practices will boost the security of your Salesforce environment while streamlining DevOps processes.

Verify Proper Permissions:

Avoid overexposing data by ensuring team members are only able to access the data they need to perform their duties.

Implement Two-Factor Authentication:

This additional layer of security continues to protect your platform even if a password is compromised.



Eliminate Coding Errors:

Static code analysis ensures all coding errors are immediately found and addressed before they can become data security vulnerabilities.

Automate Whenever Possible:

Deployment automation, code integrations, and data loading are examples of automated processes that reduce errors and streamline DevOps processes.

Source Complementary Tools:

DevOps tools need to work together seamlessly to provide the best possible results—now and in the future.

Run Frequent Audits:

Policy scanners and automated release management tools can be used to run risk assessments, compliance audits, vulnerability assessments, and more.

Offer Continuous Training:

Enhancing the skills and knowledge of your team members will increase the value they provide to your organization through more secure practices and stronger responses to issues.

Scan for Technical Debt:

Automated scans can be leveraged to seek data security vulnerabilities that exist within a live environment so they can be fixed.

Encourage Proper Usage:

Strong passwords, avoiding public networks when accessing company platforms, and other mindful habits will protect the security of your environment.

Backup Everything:

A recent data backup and the ability to quickly recover it will save your organization massive amounts of time and money should an outage occur.