Google Cloud

IT automation tools for security configuration management

So far, you've learned that the features and benefits of internet technology (IT) automation tools include flexibility, efficiency, and consistency. Automation tools, like Ansible and Puppet, help streamline the process of resource provisioning and configuration management and improve the detection and remediation of vulnerabilities. As a cloud security professional, you can use automation tools to manage complex IT infrastructure and ensure security compliance.

In this reading, you'll dive deeper into how you can implement secure by default IT automation tools in a cloud environment to help with security and compliance. Then, you'll explore how you can use IT automation tools as part of a secure configuration management (SCM) process for scalability and consistency.

Secure by default tools

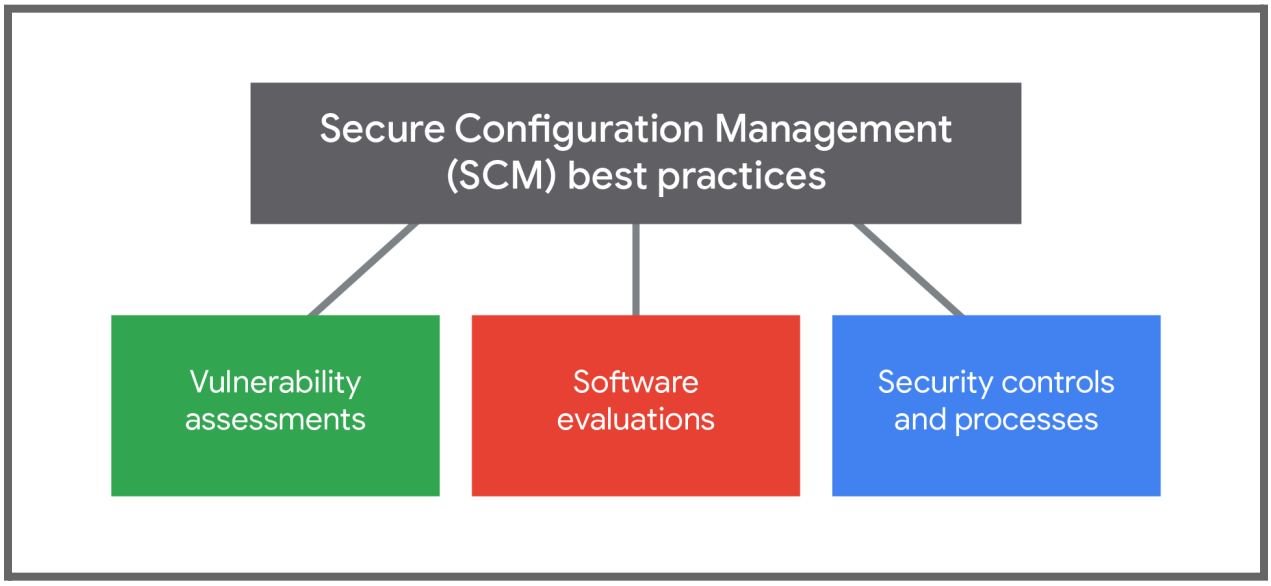
According to the U.S. Cybersecurity and Infrastructure Agency, secure by default tools are secure to use out-of-the-box, with little to no configuration changes. A cloud security team can implement secure by default tools to provide security and demonstrate compliance to internal and external standards and governances. Secure by default examples include multi-factor authentication (MFA), logging evidence of potential intrusions, and controlling access to sensitive information. Many configuration processes and tools support secure by default.

Secure configuration management (SCM) process

According to the U.S. National Institute of Standards and Technology, implementing a secure configuration management (SCM) process means to enable security and facilitate the management of risk. SCM is a foundational control to manage tool configurations for scalability and consistency. With SCM, a cloud security team can implement these best practices:

- Conduct vulnerability assessments to mitigate some known weaknesses in security.
- Evaluate software configurations and authorized hardware.
- Automate remediation by using security controls and processes.

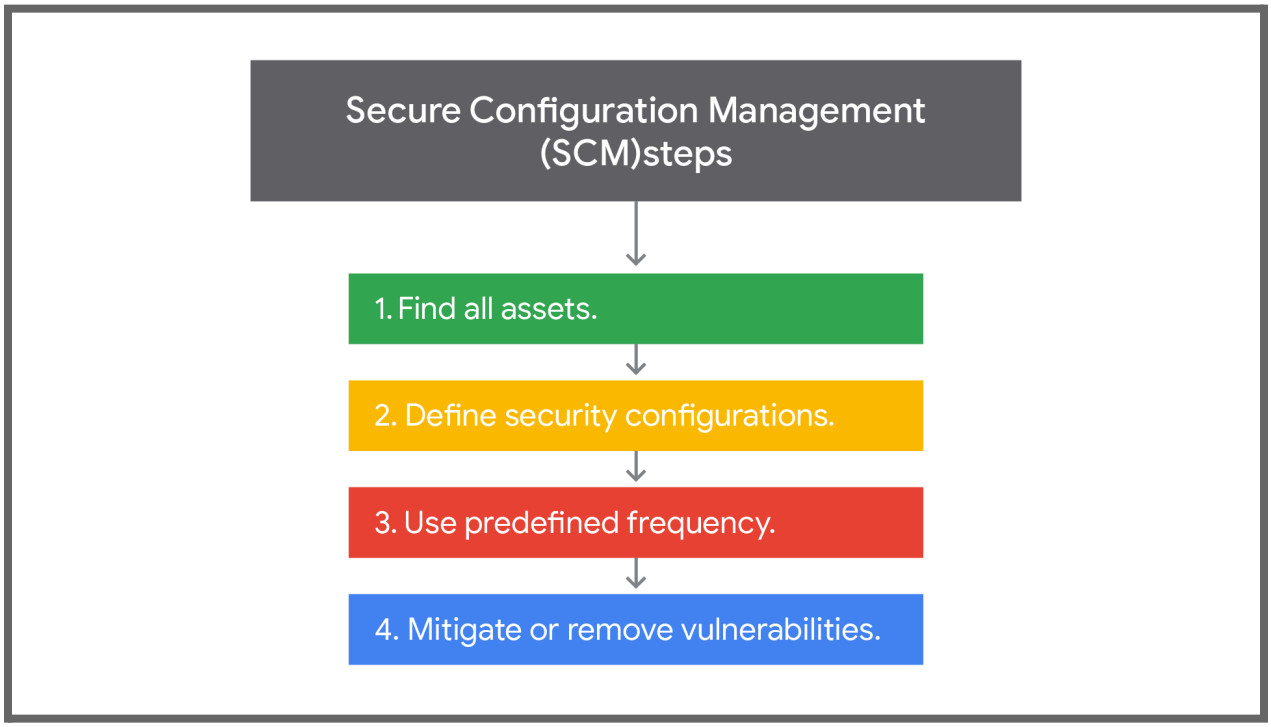
This graphic details a breakdown of these best practices:



Security configuration management has four steps:

1. Find all assets, including all connected software and hardware.
2. Define security configurations to use as baselines for each managed device type.
3. Use a predefined frequency the security policy specifies to alert for any deviations.
4. Mitigate or remove vulnerabilities by remediating configuration deviations.

This graphic provides a breakdown of these four steps:



Pro tip: Be sure organization members you are working with know how resources interact to reduce the chances of a misconfiguration of resources.

Key takeaways

You can use IT Automation management tools and processes to help you implement and manage your security configurations in a cloud environment. Be sure to use tools that are secure by default and provide you with tool configurations that are scalable and consistent across all devices in your organization. You'll also need to follow processes that will help ensure you meet internal and external compliance standards and governances. The benefits to this type of security management include reducing time spent on manual tasks that could cause errors and freeing up your cloud security team for other important work.