ACTIVITY-9

IDENTIFY DIFFERENT DEVOPS TOOLS AND LIST THEIR FEATURES.

**List of DevOps Tools**

DevOps tools play a pivotal role in addressing challenges associated with the implementation of DevOps practices. It's crucial to recognize that a "one-size-fits-all" solution is not feasible due to the diverse nature of DevOps requirements. Consequently, the market offers a broad spectrum of DevOps tools, each tailored to specific needs and scenarios.

#### Version Control tools

* **GitHub**
* **Bitbucket**
* **GitLab**

**Study and report owasp coding guidelines :-**

OWASP Code Review Guide is a technical book written for those responsible for code reviews (management, developers, security professionals). The primary focus of this book has been divided into two main sections. Section one is the “why and how of code reviews” and section two focuses on the “types of vulnerabilities and how to identify throughout the review”. While security scanners are improving every day the need for manual security code reviews still needs to have a prominent place in organizations’ SDLC (Secure Development Life Cycle) that desires good secure code in production.

Chapters in the second section are mostly based on the popular OWASP 2013 top 10. Here you will find most of the code examples for both on “what not to do” and on “what to do”. A word of caution on code examples; Perl is famous for its saying that there are 10,000 ways to do one thing. The same is true for C#, PHP, and Java or any other computer language. Now add in “Object-Oriented Programming” and if we are using design patterns or even what designs patterns are being used and sample code becomes very “iffy” in what to write. We tried to keep the sample code so code reviewers can see red flags and not “do it my way or else”.

The last section is the appendix. Here we have content like code reviewer check list, etc. of items that really don’t flow in book form but needed to be included to make the code review guide complete.

## Licensing

OWASP Code Review Guide is free to use. It is licensed under the [Creative Commons Attribution-ShareAlike 4.0 license](http://creativecommons.org/licenses/by-sa/4.0/), so you can copy, distribute and transmit the work, and you can adapt it, and use it commercially, but all provided that you attribute the work and if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

**Learn and report twelve factor app methodology :-**

The twelve-factor app methodology was originally conceived to define the patterns for applications targeting PaaS offerings such as Heroku and Engine Yard. Given the resemblance between PaaS and container platforms, these principles are applicable for modern, cloud-native applications.

**Below is a list of the patterns and practices advocated by this methodology.**

#### 1. Codebase

The very first principle of the methodology is related to versioning and tracking the code. The entire code base that belongs to the application must be stored in one repository such as Git or SVN.

#### 2. Dependencies

An application must explicitly declare all the dependencies. It cannot make assumptions about the availability of dependencies

#### 3. Configuration

This principle emphasizes on the clean separation of configuration and code.

#### 4. Backing Services

The fourth factor deals with the backing services management. Backing services are external services, which an app depends on over a network connection.

#### 5. Build, Release, Run

This principle emphasizes clean separation of the stages in the software lifecycle.

#### 6. Processes

The application is expected to run in an execution environment as one or more processes. Processes are completely stateless and share-nothing.

#### 7. Port Binding

Cloud-native applications are exposed through a URL but cannot assume the port binding through which they are exposed to the external network.

#### 8. Concurrency

Processes in twelve-factor apps are treated as first-class citizens.

#### 9. Disposability

The ninth factor emphasizes the robustness of an application through faster startup and shutdown methods

#### 10. Dev/Prod Parity

Twelve-factor apps are designed for continuous deployment by keeping the gap between development and production small.

#### 11. Logs

Logging plays an important role in debugging and maintaining the overall health of an application.

#### 12. Admin Processes

Applications often deal with one-off administrative processes such as initializing a database, cleaning up the database, and migration of servers. These processes should be run in an identical environment as the regular long-running processes of the app.

**identify different version control and configuration management tools and report their market :-**

Version control and configuration management are closely related, but they are not the same. Version control focuses on the individual files or artifacts that are part of a software project, while configuration management focuses on the whole system or project that consists of multiple artifacts.

# 11 BEST Software Configuration Management Tools (SCM Tools In 2024)

[](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2018/08/1.CONFIGURATION-MANAGEMENT.png)

### 1  [Auvik](https://try.auvik.com/er1f6)

Auvik is the provider of cloud-based network management tools. These tools offer true network visibility and control.

### 2 [ManageEngine Endpoint Central](https://softwaretesthelp.com/DC-Top5SoftConfManT)

Endpoint Central is a tool one can employ to keep sensitive business data secure on managed endpoints from all sorts of cyber-attacks.

### 3 [ManageEngine Network Configuration Manager](https://softwaretesthelp.com/NCM-Top5SoftConfManT)

With Network Configuration Manager, you get a tool that can schedule device configuration backups, track user activity, and compare configuration versions to identify changes.

### 4 [SolarWinds Server Configuration Monitor](https://solarwinds.sjv.io/c/1399142/1679074/17790)

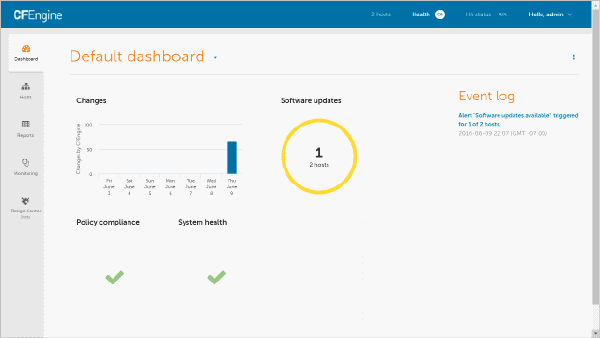
SolarWinds provides a Server Configuration Monitor to detect unauthorized configuration changes to your servers and applications.

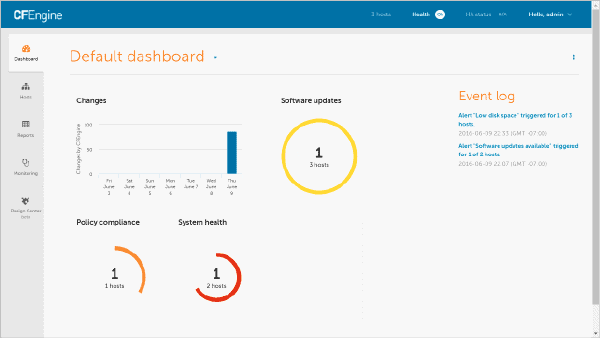
### 5 [Tripwire Enterprise](https://softwaretesthelp.com/Fortra-SftConf-MgmtT)

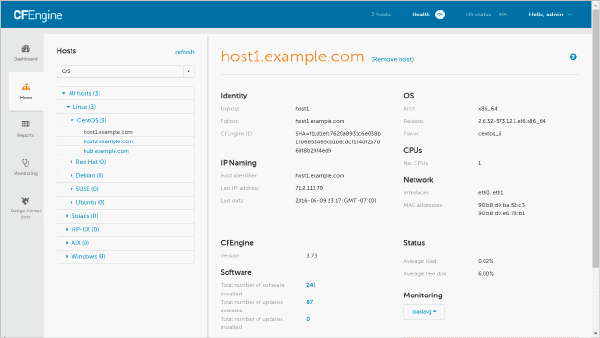
Tripwire® Enterprise is a fully integrated suite of solutions for policy compliance, system integrity, and remediation management that reaches far beyond simple compliance.

### 6 [SysAid](https://appwiki.nl/link/brand/ZwsfH4MWefknw7OgP3kD1u5udyvHDT9Q)

With SysAid, you are basically getting a complete ITIL package that can be customized as per the specific requirements of your organization.

[](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2018/08/2.-CFEngine-Configuration.png)

[](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2018/08/2.2.-CFEngine-Configuration.png)

[](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2018/08/4Refer-CFEngine-Tool-images.png)