Security Compass

SD ELEMENTS
Operational Security

SD Elements, the leading policy to procedure platform, now features operational security requirements in its robust knowledge library. Alongside its original AppSec track, the new extension allows engineering teams to use SD Elements as a holistic solution for managing software security requirements in a DevOps environment.

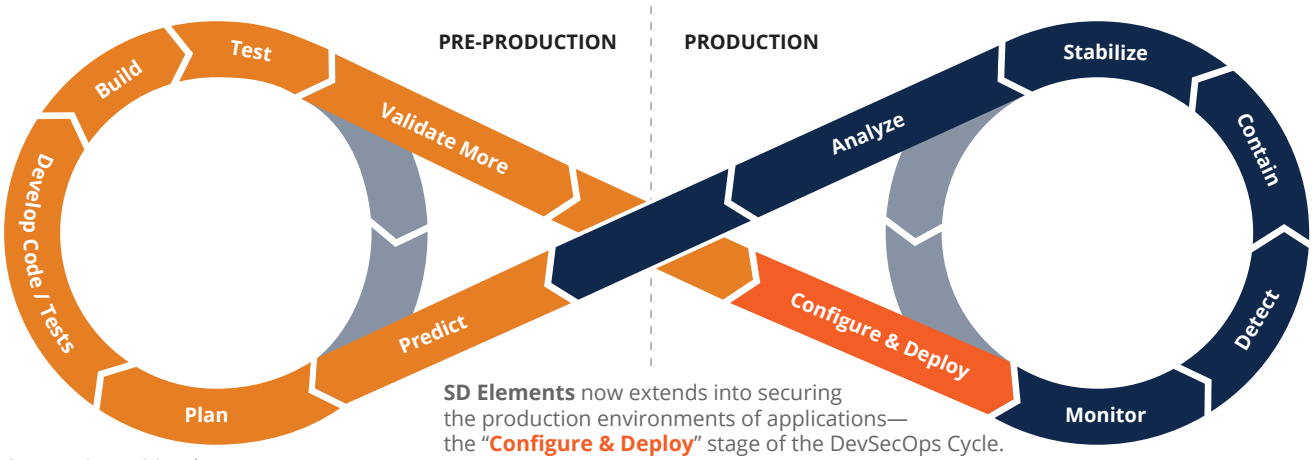
SD Elements makes it easy for DevOps teams to manage the security considerations of the entire technology stack–for both the software itself, as well as the operational security requirements of the web server, application server, database server, and application-hosting operating system. This includes both the traditional and cloud deployment environment.

- SD Elements now extends into securing the production environments of applications–the "Configure & Deploy" stage of the DevSecOps Cycle.
- SD Elements can be used to manage the security requirements of the deployment configuration settings, alongside the requirements for the application itself, to achieve DevSecOps.
- SD Elements' Operational Security content originates from the Center for Internet Security (R) (CIS) content, which we then applied our own standards to, so that it could integrate into our database and match our taxonomy.

CIS SecureSuite Membership

Cloud	Server
AWS Azure Google Cloud (coming soon)	**Web Server:** Apache HTTP, NGINX, IIS
	Application Server: Apache Tomcat
	Database Server: MySQL, Oracle, Microsoft SQL
CONTAINERS - Docker, Kubernetes	
OS LAYER - Redhat, Windows Server	

The DevSecOps Cycle



SD Elements now extends into securing the production environments of applications—the "**Configure & Deploy**" stage of the DevSecOps Cycle.

Source: Larry Maccherone

Examples of Automation Use Cases

In a DevOps environment, deployment and configuration are generally programmed into the software, rather than done manually by IT staff. In many cases, DevOps enablement technologies allow the core software to programmatically control its configuration and underlying server settings. Three notable groups of technologies in this area are:

Cloud-based infrastructure, such as AWS, where servers can be provisioned and managed programmatically.

Deployment management tools, such as Puppet, Chef, and Ansible, where a programmable interface is used for the configuration and deployment of the environment the software is operating in.

Container technologies, such as Docker and Kubernetes, where resource management is improved, as applications are isolated in the container environment that uses normal operating system (OS) calls, and where everything is pre-worked in an image, enabling individual services.

Contact us to learn more about using SD Elements for your company's DevSecOps needs
info@securitycompass.com

Security Compass