SD Elements in the U.S. Federal Government

Obtain ATO Faster, Deliver Secure Software at Scale

Organizations that develop or modify software for U.S. federal government agencies and the Department of Defense (DoD) must ensure compliance with Federal Information Security Management Act (FISMA) security requirements in order to receive Authority to Operate (ATO).

SD Elements is a secure application development platform for U.S. federal government agencies that are using agile DevSecOps methodologies to develop trustworthy, reliable software at the speed of mission while reducing the time, effort, and cost to obtain ATO.

U.S. Air Force Kessel Run

Kessel Run is the operational name for Air Force Life Cycle Management Center's (AFLCMC) Detachment 12. Kessel Run builds, tests, delivers, operates, and maintains cloud-based infrastructure and warfighting software applications for use by Air Force personnel worldwide.

At Kessel Run, disconnected software development tools, vulnerability scanning processes, and manual assessment practices made obtaining Authority to Operate (ATO) a manual, time-consuming process. To achieve their mission of rapidly delivering best-in-class software with combat capabilities to warfighters, Kessel Run needed a way to streamline their ATO process in order to obtain not just ATO, but continuous ATO (cATO).

Kessel Run deployed SD Elements within its software factory to deliver tailored, task-based guidance and embedded, just-in-time training designed to help developers write secure code faster. With SD Elements, they can automatically track completed tasks as well as generate the reports and other audit artifacts required to demonstrate compliance with NIST 800-53, the OWASP Application Security Verification Standard (ASVS), and other applicable compliance requirements. The extensive customization capabilities SD Elements provides also helped Kessel Run automate previously manual ATO processes, which in turn dramatically reduced the amount of time required to achieve cATO.

U.S. Department of Defense Platform One

Platform One, an official U.S. Department of Defense (DoD) DevSecOps Enterprise Services team, manages Air Force software factories and provides DevSecOps managed services. Platform One is the go-to team for programs in the Defense Department who want to adopt commercial best practices to develop software, enable continuous upgrades, and release new features with baked-in cybersecurity testing on a much faster timeline and at a lower cost than the traditional "waterfall" cycle.

Platform One is focused on rapidly delivering secure, innovative software to warfighters at the speed of mission while meeting cATO requirements. In order to demonstrate compliance with the NIST Cybersecurity Framework and NIST 800-53, Platform One uses SD Elements to simplify secure software delivery. Initially, demonstrating compliance with the NIST Cyber Security Framework and NIST 800-53 controls, a key requirement for cATO, was a very manual, labor-intensive process. However, once Platform One development teams began using SD Elements to automatically identify and translate software security requirements into easy-to-follow tasks for developers and track the implementation of security controls to completion, SD Elements helped reduce the time required to meet ATO requirements from months or years down to days or weeks.

SD Elements is also now available in the Platform One Iron Bank repository, which means it has been certified and pre-approved for use by developers creating applications for the U.S. federal government who need to release applications quickly in a secure, efficient, and agile manner.

U.S. Air Force Space and Missile Systems Center

The U.S. Air Force Space and Missile Systems Center (SMC) is the U.S. Space Force (USSF) center of excellence for acquiring and developing military space systems. It provides the technologies used to defend the interests of America and its allies in space.

At the SMC, tracking compliance with NIST 800-53 security controls was a manual process. Obtaining authority to operate, or ATO, for applications developed by SMC DevOps teams was also a long, challenging — yet critical — process.

The DevOps team at SMC used SD Elements to streamline and automate the generation and tracking of NIST 800-53 requirements. SD Elements now enables application security teams to deliver detailed requirements, code samples, and short, relevant training modules related to 800-53 security standards to DevSecOps teams right within their issue trackers. They can also track and monitor security control status, validate security activities by importing results from code scanners, and create compliance artifacts. These capabilities help the SMC team to dramatically reduce the amount of time required to obtain and maintain cATO for their applications.

U.S. Air Force Business and Enterprise Systems Product Innovation

Business and Enterprise Systems Product Innovation (BESPIN) is one of USAF's newest agile development labs. BESPIN creates mobile and desktop apps for maintenance crew chiefs, aircrew readiness, and ammunition crews.

Within the U.S. Air Force, application teams in software factories are adopting agile methodologies to release software faster than ever before. To keep pace, the BESPIN DevOps team needed a solution to automate security requirements generation and compliance traceability early in the development cycle in order to streamline the amount of time required to obtain and maintain cATO for its web and mobile applications.

With SD Elements, BESPIN is able to streamline and automate the generation of web and mobile application security requirements, then deliver requirements directly to the issue tracking systems used by developers. BESPIN security architects use SD Elements threat modeling capabilities to identify and remediate security issues earlier in the software development lifecycle. BESPIN also leverages Security Compass experts to ensure security champions within the organization are trained in secure software development principles and best practices.

U.S. Security and Exchange Commission

The Securities and Exchange Commission (SEC) is a U.S. government oversight agency responsible for regulating the securities markets and protecting investors.

Application developers within the SEC are responsible for delivering software applications on time and within budget without missing application security targets. They also must efficiently and effectively obtain and maintain ATO, as well as ensure their DevOps teams are fully trained on application security best practices.

DevOps teams within the SEC use SD Elements to shift security left, meet NIST 800-53 compliance requirements, and maintain ATO assessment readiness. SD Elements enables the SEC to efficiently automate, simplify, and scale application security modeling and requirements delivery. SD Elements' out-of-the-box content library also helps internal security SMEs to improve developer security expertise and instill a security culture.