Accelerating the Authority to Operate Process with DevOps

Highlights from a Government Roundtable, hosted by ATARC in partnership with CloudBees, March 2023

For Federal agencies, Continuous Authority to Operate (cATO) is a challenging, but necessary, approach to reduce cyber risk and accelerate innovation. To achieve cATO, agencies must produce real-time security data through continuous monitoring of risk management framework (RMF) controls that are embedded in the DevSecOps process.

At a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with CloudBees, participants from various federal agencies shared their experiences with the ATO process, the role of an Authorizing Official (AO), as well as the challenges of transitioning to a continuous ATO model.

> **“Cybersecurity is everyone's job. It should be budgeted with security in mind, procured from secure supply chains, designed with all controls considered, coded securely, tested to assure the mechanisms are working to the standards and then operated with security on all of these elements for the full lifecycle.”**

The ATO process

Several agencies on the panel are attempting to focus their efforts on maturing the cATO process, but are met with resistance and confusion from team members. One participant describes cATO as a maturation of the ATO process to a point where there is a certain level of risk, but with robust monitoring in place to mitigate that risk. In other words, it’s an agency’s ability to understand its entire ecosystem.

The role of an AO is to monitor a cumulative set of security controls in order to make real-time risk decisions for the agency. From their perspective, AOs are looking for monitoring plans, how agencies respond to issues, and if these procedures are embedded into the DevSecOps process.

In reality, many developers do not have access to the operations environment, which can hinder their ability to diagnose system issues accurately. The goal for many agencies is to tighten the loop between the DevSecOps teams through a continuous ATO process.

Challenges with ATO

- **Automating Cyber Assessments and Authorization in the Delivery Pipeline-** Several agencies bolt cyber assessments onto the end of the delivery process, rather than integrating cyber assessments or authorization approvals directly into the delivery pipeline. Other agencies struggle to align the security process with the acquisition process. Generally, automating these processes is challenging for agencies.

- **Streamlining ATO Efforts-** Some agencies are challenged by the duplication of ATO efforts within a single department, resulting in security personnel being spread too thin. Agencies should consider creating an enterprise approach to streamline ATO for some platforms and software tools.

- **Moving from Compliance-Based Security to a Risk-Based Model-** Transitioning from compliance-based security to a risk-based model is challenging for many agencies. Some AOs are more tolerant of risk than others, which can hinder progress towards cATO. As one participant noted, being prepared from a compliance standpoint is not going to protect agencies from a zero day event. Being prepared to handle risk when it appears is the most important thing agencies can do.

- **Building a Culture of Automation and Change-** Changing agency culture is a challenge. As agencies work to deploy new solutions, automating processes flies in the face of how agencies have conducted business for decades. If the workforce does not acknowledge and embrace the idea that these processes must be automated, then agencies do not stand a chance at success.

- **Mitigating Risk with AI and ML in Unreliable Security Documentation-** When accrediting a new release of a software application, AOs and CIOs try to leverage as many inherited controls as possible, so the new release only contains elements with a significant security impact. Unfortunately, agencies often encounter unreliable security risk documentation or they inherit systems that were transferred without paperwork. These scenarios usually result in the agency scrapping the system due to the amount of unknown risk. Advancements in AI and ML may automate this documentation in the future.

- **Risk Evaluation-** Many agencies need adequate tools to accurately define an issue by continuously monitoring the entire ecosystem. Instead of reviewing the same vulnerabilities multiple times in different scanners, agencies would benefit from an aggregate view of all the scanners in order to identify the vulnerability once.

- **System Vulnerabilities-** Understanding whether a system is exploitable is a challenge the market is still working through. SBOMs can inform an agency of a software component that may contain vulnerabilities, but cannot tell whether the component is being used in a way that makes it exploitable.

The effectiveness of software factories to accelerate the ATO process depends on whether the specific design pattern of the software factory is compatible with an agency's existing software stack. Not all software factories are functioning at an enterprise level, nor are they able to refactor and modify legacy systems.

Role of the AO or Security Assessor

Roundtable participants concur that some AOs are more comfortable with risk-focused models and have a higher tolerance for risk than others. Likewise, some AOs prefer to take a verification approach. These different approaches to ATO likely stem from their diverse backgrounds. For instance, some AOs may have an easier time understanding system engineering based on their background, whereas others may have a higher proficiency in cybersecurity.

The challenge comes with determining how a security assessor should be trained or what qualifying credentials they should have. Some participants argue that security assessors should have some sort of engineering background due to the increasing amount of coding required. While coding is certainly a strong skill to possess, this would require an assessor to attend SCRUM ceremonies while monitoring numerous systems, essentially tripling their workload.

The learning curve for an assessor can be significant, depending on how the product is engineered. One system might use a CRM, whereas another might use SOLR. One participant noted that it’s unfortunate that assessors need to be highly specialized, but the role is usually an entry-level position. Many agencies lack training and cross-training among this group of important personnel.

Currently, many security assessors are trained to conduct security assessments for traditional, on-premise legacy systems. Agencies are now at a point with cloud and software development where more fluidity is needed. Skilling the workforce is paramount to enabling a continuous ATO model. If a security assessor is uncomfortable with this model or comes in with no prior knowledge of new technology, there is quite a lot of risk of not being able to deliver value. Some smaller agencies outsource assessors and don’t have an assessor on staff. With an increased speed of development for cloud products, agencies are burdened on the back end to conduct assessments on short notice.

Ultimately, trust and integrity are necessary components of cATO. Not only does the process need to be designed with integrity, but the people executing the process need to have high integrity themselves.