anchore

CASE STUDY

US Navy achieves ATO in days with continuous compliance and OSS risk management

PEO Digital's DevSecOps Platform "Black Pearl" enables US Navy programs to build and deploy software rapidly while maintaining the most stringent government security and compliance requirements. Compliance reporting and maintenance are time intensive and so are managing vulnerabilities and risks through open-source software.

PEO Digital
Washington, DC

INDUSTRY
IT Infrastructure

SEGMENT
DevSecOps Platform

Challenges

- Achieve RMF security and compliance requirements
- Maintaining continuous compliance
- Managing the risk of open-source software
- Vulnerability overload for developers

Solutions

Anchore automates security and compliance to reduce risks in the software supply chain:

- Policy packs to meet RMF security controls
- Automated and continuous ATO compliance
- Managing OSS risks with continuous monitoring (ConMon)
- Automated prioritization of vulnerabilities

Results

Achieve authority to operate (ATO) for software under RMF framework:

- Deploy a ready to be assessed DSOP in 3-5 days
- Significantly reduced time spent on compliance reporting
- Proactive OSS risk management
- Reduced vulnerability overload with prioritized vulnerability reporting

Deploy assessment ready DSOP in

3-5 days

Introduction

Black Pearl is a PEO Digital Enterprise DevSecOps Platform comprised of two offerings, Party Barge and Lighthouse.
Lighthouse is a resilient, production-grade DevSecOps Platform, tailored to meet specific Mission Owner requirements whether it be on-prem or in a custom cloud deployment.

Party Barge is built from the Lighthouse baseline, designed as a Multi-tenant Development and Test environment (IL2/5) offering DevSecOps Tools as a Service using a simple per user licensing model, and is fully managed by the Black Pearl Party Barge Team.

Challenge

For any software to be built, deployed and used by the warfighter it has to achieve ATO. To achieve ATO, all software developed for a DoD mission has to be built on a software development platform that meets the DoD DevSecOps Enterprise Reference Design.

Sigma Defense, a technology company that specializes in networking, security and software engineering for the public sector, faced a number of challenges while architecting the Black Pearl platform such as securing the software supply chain, ATO-compliance, open-source software (OSS) risk management and vulnerability management.

» Achieving RMF security and compliance for both DSOP and customers

Not only does Black Pearl need to achieve ATO for itself, it has to help its customers achieve ATO for the applications that are built on it. In order to achieve both of these goals, they required a software supply chain security platform that could both scan the Black Pearl platform for compliance and all applications built by its customers.

» Maintaining continuous compliance

With the advent of the RAISE 2.0 memo jointly signed by the Senior Information Security Officers of the Navy and Marine Corps in November 2022, continuous ATO-compliance is now a priority for all DON missions. Given the amount of time and effort that goes into achieving an ATO in the first place, automating the bulk of the compliance tasks is crucial.

» Managing the risk of open-source software

The average application contains 500+ open-source components; this is a powerful source of leverage for developers when building applications but creates risk. Black Pearl has the dual problem of having to manage the risk of open-source dependencies in its own platform and provide tools to help its customers manage the OSS risk in their own applications. Finding a solution to manage this risk is not only a security prerogative for Black Pearl but a compliance requirement.

» Vulnerability overload for developers

Identifying vulnerabilities is the first step to ATO but given the number of vulnerabilities that exist in typical open-source components, triaging vulnerabilities can rapidly consume all of a developer's time and resources. This degrades the developer velocity gains that were achieved by adopting a DevSecOps practice. Being able to filter which vulnerabilities are priorities rather than noise is a key challenge to overcome in order to achieve compliance without sacrificing velocity.

Solution

To address these challenges, Sigma Defense chose Anchore to protect Black Pearl's software supply chain.

» Policy packs to meet RMF security controls

Sigma Defense chose Anchore to secure both Black Pearl's software supply chain and all DON applications that are built on Black Pearl. Anchore can identify, evaluate, prioritize, enforce and report on whether security controls meet the compliance requirements of the Risk Management Framework (RMF). Each software development platform must meet stringent security requirements such as RA-5 (Vulnerability Management), SI-3 (Malware Protection), and IA-5 (Credential Management). This process can be daunting and resource-intensive, requiring continuous attention to detail and expertise in compliance review. Anchore and Sigma Defense have demonstrated their expertise to help various DoD missions, including Platform One's Big Bang and PEO IWS The Forge, pass their authorizing official (AO) reviews and achieve ATO, mitigating this typically massive undertaking.

"By using the Anchore and the Black Pearl platform, applications inherit 80 percent of RMF security controls…You can avoid all of the boring stuff and just get down to what everyone does well, which is write code."

—Christopher Rennie, Black Pearl Product Growth Lead

» Automated and continuous ATO compliance

Achieving ATO is just the beginning; maintaining continuous compliance is an ongoing challenge. This involves managing security findings, tracking plan of action and milestones (POA&Ms), and ensuring that all necessary security controls are continuously met. Manual processes for maintaining compliance can be error-prone and resource-intensive.

Anchore offers automated ATO compliance, continuously managing findings and POA&Ms. This automation ensures that compliance is maintained with minimal manual intervention, reducing the risk of non-compliance and the associated penalties.

The DoD has four different layers of authorizing officials in order to achieve ATO. You have to figure out how to make all of them happy. We want to innovate by automating the compliance process. Anchore helps us achieve this, so that we can build a full ATO package in an afternoon rather than taking a month or more.

—Josiah Ritchie, DevSecOps Staff Engineer

» Managing OSS risks with continuous monitoring (ConMon)

Open-source software is widely used in modern software development, but it comes with inherent risks, including potential security vulnerabilities. Anchore mitigates this risk by integrating a vulnerability scanner, policy enforcer and reporting system to continuously monitor OSS vulnerabilities and risk in any software supply chain. This enables proactive management and active defense of OSS risk ensuring that vulnerabilities are detected and addressed promptly; reducing the risk of security breaches.

» Automated prioritization of vulnerabilities

Black Pearl integrates the Anchore Developer Bundle which automatically flags vulnerabilities that developers are able to address and move their application to ATO quicker. This shift-left security practice creates actionable feedback for developers to overcome compliance hurdles before the review process. The power of DevSecOps is developer velocity. By embedding security directly into the development process DON missions get access to rapid and secure deployments.

Results

» Platform ATO in 3-5 days

The main advantage of adopting the Black Pearl platform is the accelerated timeline of having a fully operational DSOP. While DIY builds can take up to 6 months or longer, Black Pearl users are able to access a fully operational DSOP within 3-5 days. With Anchore fully integrated into Black Pearl and its pre-built RMF policy pack running, all software built on Black Pearl will dramatically reduce the time to application ATO. Non-compliant software design decisions can be identified in development which prevents unnecessary engineering cycles from being wasted. Security is not the only practice that can benefit from a shift left approach to software development.

» Significantly reduced time spent on compliance reporting

Anchore automates compliance checks and compliance artifacts:

1. Reduces hours spent manually reviewing vulnerability reports and creating the compliance artifacts that will then be delivered to the authorizing officials (AOs).
2. Ensures that all of the data exists in the reports and is formatted in the way expected by the reviewer. This prevents delays due to the inconsistencies that inevitably occur as part of any manual process.

Working alongside Anchore, we have customized the compliance artifacts that come from the Anchore API to look exactly how the AOs are expecting them to. This has created a good foundation for us to start building the POA&Ms that they're expecting.

—Josiah Ritchie, DevSecOps Staff Engineer

» Proactive OSS risk management

By shifting security and compliance left, Black Pearl enables its customers to identify and remediate open-source vulnerabilities that would block an ATO as early as the development phase of the software development lifecycle (SDLC). This proactive approach to security and compliance ensures that OSS risk is mitigated, compliance is smooth and the benefits of composable software are available to the developers of the US Navy. The downstream benefit is that time to ATO is reduced.

» Reduced vulnerability overload with prioritized vulnerability reporting

The less time developer's spend remediating vulnerabilities that have no tangible security value, the more time they can spend writing software to help the warfighter. Anchore automatically prioritizes actionable vulnerabilities and alerts developers. This prevents vulnerability overload and accelerates the time to delivery of critical software and features.

Request a demo

Watch Now

sales@anchore.com
anchore.com