

Continuous Security Intelligence Proof of Concept

Why DeployHub

With an obfuscated software supply chain, IT teams struggle to know all the pieces of software they deliver to their end-users. Without insights, its hard to confirm that the software delivered is safe for consumption. The software supply chain includes thousands of open-source packages, consumed across hundreds of containers that make up the software applications delivered to end-users.

DeployHub's Continuous Security Intelligence unifies supply chain forensics to expose all the pieces of software, making it easy to respond to threats and vulnerabilities within hours not months. DeployHub collects supply chain and DevOps intelligence generated by the DevOps Pipeline. DeployHub clarifies 'logical' application composition, aggregates SBOM and CVE reports from lower-level dependencies, and tracks opensource inventory across all environments.



Table of Contents

DeployHub POC Success Criteria 3

The DeployHub SaaS or On-Premise Installation Options 4

Installing the CI/CD CLI for Pipeline Automation 5

Ortelius CLI Data Gathering using the .toml File 5

Steps for Running the Proof of Concept 6

Expected Results 11

Next Steps 13

Get Help 13



DeployHub POC Success Criteria

Implementing DeployHub's Continuous Security Intelligence will ensure that IT teams can deliver secure, high-quality software at scale by exposing the following:

Versioning and Component to Application Dependency Management

DeployHub will track updates and create new versions of components (containers, DB objects, File based objects) that are being continuously pushed across the supply chain.

DeployHub will automatically create new logical application versions based on changes occurring at the lower component dependency level.

DeployHub will show the 'many-to-many' relationships between components and the logical applications that consume them.

Supply Chain Security

DeployHub will integrate into the DevOps pipeline consuming component-level SBOMs and producing CVE reports for each new version of a component.

DeployHub will produce application-level SBOMs and CVE reports for all logical applications impacted by a lower-level component change.

Service Ownership and Organization

DeployHub will track component ownership and provide a simple method of knowing whom to call when a lower-level object has an issue that impacts multiple teams.

(4)

Component and Open-Source Usage and Inventory

DeployHub will provide the ability to search for open-source packages across all logical applications.

The DeployHub SaaS or On-Premise Installation Options

DeployHub offers a SaaS model provding you operational management and a cost effective way to implement your supply chain catalog. Alternatively you can install DeployHub on premise. Pricing is the same for both methods. For terms of use see: <u>https://www.deployhub.com/terms-of-use/</u>

SaaS Signup

Signup for the SaaS option at https://www.deployhub.com/deployhub-team

You will recieve an email that provides you instructions for accessing the SaaS portal at https://console.deployhub.com/

To access the SaaS portal you will be asked to enter a UserID/Password, Company and Project name. Your UserID/Password and Company name are unique. Once you login, your Project will be a found under your Company's high-level Domain.

On-Prem Installation

DeployHub can be installed into your own cloud environment, or onto a hosted cloud environment. DeplyHub uses Helm to manage and perform the installation. The process includes the installation of multiple containers. Note: You will not need the Reverse Proxy if you are installing into your own enviornment.

The DeployHub on-premise Helm chart and instructions can be found at <u>ArtifactHub</u>. This is the location for the most up to date instructions for downloading and running the DeployHub Helm chart. (<u>https://artifacthub.io/packages/helm/deployhub/deployhub</u>)

Installing the CI/CD CLI for Pipeline Automation

Regardless if you are running the SaaS version or an on-premise version, you will need to install the CI/CD Command Line Interface (CLI) to automate the gather of supply chain data from your pipeline workflows.

DeployHub integrates into your CI/CD process using the Ortelius Open-Source Command Line (CLI). The Ortelius CLI gathers supply chain data based on a single pipeline workflow at the build and deploy steps. The CLI will support any CI/CD engine, but does require Python. The build step gathers Swagger, SBOM, Readme, licenses, Git data, Docker image, and other build output. The deploy step records when a release occurs, what was sent and where the objects were sent to.

To complete your POC you will need to install the Ortelius CLI where your CI/CD server is running. Refer to the <u>Ortelius GitHub CLI Documentation (https://github.com/Ortelius/cli/blob/main/doc/dh.md)</u> for installation instructions.

The <u>Ortelius (https://Ortelius.io)</u> CLI is maintained by the Ortelius Open Source Community under the governance of the Linux Foundation's Continuous Delivery Foundation.

Ortelius CLI Data Gathering using the .toml File

The Ortelius CLI reads from a .toml file. The .toml file contains non-derived information for each artifact that you create at your build step. In DeployHub, an artifact is referred to as a Component. A Component is a Container, DB Object, or file object (.jar, Lamda Function, Apex file, etc.). The .toml file will provide the 'non-derived' data for the Component your are tracking in DeployHub which includes the Component name, owner, Component type, and owner contact details. The Ortelius CLI will read the .toml file from the Git Repository associated to your pipeline. If you are using a Mono Repository for your entire codebase, you will need a separate Component.toml file for each Component, managed in sub-directories.

In a cloud-native, microservice architecture there are many, if not hundreds, of Components. Organizing your Components within DeployHub is done in two ways. They are grouped based on a subject Domain and assigned to a logical Application. Not all Components need to be assigned to an Application, but they should be stored in a subject matter Domain so they can be easily found and reused.

A logical Application is a collection of Components that make up a complete software systems consumed by an end user. Applications are composed of shared Components and Application specific Components, and are a logical representation of what Components need to be deployed in order for the software system to run.

Note: Once created, your .toml file does not need to be updated unless the non-derived information changes, or



Steps for Running the Proof of Concept

To automate DeployHub, you will need to add it's data gathering to your CI/CD pipeline. The following steps will guide you through the process of implementing the Ortelius CLI to implement your Proof of Concept. Be sure you have installed the Ortelius CLI before you start.

Note: This POC does not include data gathering of the deployment for inventory tracking.

Step 1 - Define Your DeployHub Pipeline Variables

The following variables should be set at the beginning of your Pipeline.

DHURL - URL to DeployHub Login

DHUSER - The ID used to log into DeployHub

DHPASS - The password used to log into DeployHub. This can encrypted based on the CI/CD solution.

DOCKERREPO -Name of your Docker Repository .For Components that are Docker Images. Not needed for non-docker objects.

IMAGE_TAG - Tag for the Docker Image if used . For Components that are Docker Images. Not needed for non-docker objects.

Example:

export DHURL=https://console.deployhub.com export DHUSER=Stella99 export DHPASS=chasinghorses export DOCKERREPO=quay.io/DeployHub/hello-world export IMAGE_TAG=1.0.0

Step 2 - Create your Component.toml file

Cut and paste the following into a component.toml file, update 'your' information, and commit/push it to your Git Repository.

Application Name and Version - optional. If not used the Component will not be associated to an Application

Application = "GLOBAL.your Application Name" Application_Version = "your Application Version"

Define Component Name, Variant and Version - required Name = "GLOBAL.your Component Name" Variant = "\${GIT_BRANCH}" Version = "vyour Component Version.\${BUILD_NUM}-g\${SHORT_SHA}"

Key/Values to associate to the Component Version
[Attributes]
 DockerBuildDate = "\${BLDDATE}"
 DockerRepo = "\${DOCKERREPO}"
 DockerSha = "\${DIGEST}"
 DockerTag = "\${IMAGE_TAG}"
 DiscordChannel = "Your Discord Channel" or SlackChannel="Your Slack Channel"
 ServiceOwner= "\${DHUSER}"
 ServiceOwnerEmail = "Your Component Owner Email"

Example:

```
# Application Name and Version
Application = "GLOBAL.Santa Fe Software.Online Store Company.Hipster Store.Prod.helloworld app"
Application_Version = "1"
```

Define Component Name, Variant and Version
Name = "GLOBAL.Santa Fe Software.Online Store Company"
Variant = "\${GIT_BRANCH}"
Version = "v1.0.0.\${BUILD_NUM}-g\${SHORT_SHA}"

```
# Key/Values to associate to the Component Version
[Attributes]
DockerBuildDate = "${BLDDATE}"
DockerRepo = "${DOCKERREPO}"
DockerSha = "${DIGEST}"
DockerTag = "${IMAGE_TAG}"
DiscordChannel = "ttps://discord.gg/wM4b5yEFzS"
ServiceOwner= "${DHUSER}"
ServiceOwnerEmail = "stella@DeployHub.io"
```

Note: For SaaS users, you will have a second high-level qualifier that was created as part of your sign-up. This second high-level qualifier must be used as the start of your Application Name and Component Name. For example: GLOBAL.Santa Fe Software.Online Store.

Step 3 - Add a step in your pipeline to run Syft if you are not generating SBOMS (Optional)

DeployHub can consume any SPDX and CycloneDX formatted SBOM. If you are already generating SBOMs, you will pass the name of the SBOM results to DeployHub is step 4 below. If you are not generating SBOMs as part of your pipeline process, you will need to add SBOM generation to collect the lower dependency data. Following is how to add Syft to your workflow to include the collection of SBOM data.

<u>Syft SBOM tool</u> (https://github.com/anchore/syft) will generate Software Bill of Material Reports for popular coding languages and package managers, including Docker images.

The following code example scans a Docker Image to generate the SBOM. See <u>Syft Options (https://github.</u> com/anchore/syft#supported-sources) to scan other objects and coding languages.

install Syft curl -sSfL https://raw.githubusercontent.com/anchore/syft/main/install.sh | sh -s -- -b \$PWD

create the SBOM ../syft packages \$DOCKERREPO:\$IMAGE_TAG --scope all-layers -o cyclonedx-json > cyclonedx.json

display the SBOM cat cyclonedx.json

Step 4 - Run the Ortelius CLI to add Your Component and Create an Application

Execute the following calls to the Ortelius CLI as part of your workflow. It should be called after the build and SBOM generation:

With CycloneDX SBOM

dh updatecomp --rsp component.toml --deppkg "cyclonedx@name of your SBOM file"

Example: dh updatecomp --rsp component.toml --deppkg "cyclonedx@cyclonedx.json"

With SPDX SBOM

dh updatecomp --rsp component.toml --deppkg "spdx@name of your SBOM file. "

Example: dh updatecomp --rsp component.toml --deppkg "spdx@spdx.json"

Without SBOM

dh updatecomp --rsp component.toml



Expected Results

Bring up your DeployHub URL and login using the DHUSER and DHPASS from Step 1.

Application to Component Dependencies

Select Your Application from the 'Application View.' It should show you one Component as a dependency.

General Package Components Applica	ition Service Hierarchy Bundle		Application Version: helloworld a	pp:1
Details	🖉 Edit 🔯 Save 🛞 Cancel	Dependencies		
Foll Domain:	GLOBAL.Santa Fe Software.Online Store Company.Hipster Store.Prod	Component	Domain	
Name:	helloworld app;1	helio-world:master:v1_0_0_101_gsbdbbdd	GLOBAL Santa Re Software. Online Store Company	
Description:				
Change Request Data Source:				
Pre-Action:				
Post-Action:				
Custom Action:				
Successful Deployment Template:				
Failed Deployment Template:				

Application Level SBOM and CVE

Review the Application SBOM and vulnerabilities. *Note: CVE Results may vary depending on the time of the scan.*

Vulnerabilities	Software Bill of M	Materials (SBOM)		
Package 🔺 Version 🔺 ID 🕴 Summary 🕴 Component 🔶	Package	0 Version	License	Component 0
CVF-2013-6393 : Happ Based Buffer GLOBAL Santa Fe Software Online Store Ilibyami 0.1.7-5.el8 <u>GHSA-m7Xh-cpbp-clih5</u> Dowelline in Dowelline in Company hello-	hello-world	0.1.0	No License	GLOBAL.Santa Fe Software.Online Store Company.hello- world:master.v1_0_0_101_g3b3bbdd
Ure non al world:master.v1_0_0_101_g3b3bbdd libyarni	libyaml	0.1.7-5.el8	MIT	GLOBAL.Santa Fe Software.Online Store Company.hello- world;master;v1_0_0_101_g3b3bbdd
	json-c	0.13.1-3.el8	MIT	GLOBAL.Santa Fe Software.Online Store Company.hello- world;master;v1_0_0_101_g3b3bbdd
	elfutils-libelf	0.186-1.el8	No License	GLOBAL.Santa Fe Software.Online Store Company.hello- world:master.v1_0_0_101_g3b3bbdd
	librosi	0.20.2.6 cl8	MIT	GLOBAL.Santa Fe Software.Online Store Company.hello-

Component Ownership

Go to the 'Component View'. You should see your Component Ownership and Detail, including its SBOM and vulnerabilities.

General			Eamponent Version: hollo-work
Sendor Owner:	Stella Admin	Component Details	
Service Owner Emolt	stel kill DepkyHub.io	Build Date	Tue Ort 18 11:48-00 2022
Service Owner Phone:		Read of the	101
PagerDuty Business Service Urt:		multi con-	http://lienkins.myoroject.org
PagenDuty Service Unit		Centerburg Anniators	raww. jo/ar tel kuv/teello-evaria
Steph Channel		Contrainer Direct:	212/9296/310
Discord Channel:	https://discord.gg/wM4b5yEFz5	Container Tag	master.co.u.org
Mpchor channel:		Heiro Chart	
Component Overview		Hrine Chart Nomenador:	
Aul Domain:	GLOBAL Santa Re Software Online Store Company	Heiro Chart Repo:	
Norne:	hello-worldmasterov1.0.0.101_g3b3bbdd	Helito Chart Repo Unit	
Description		Helin Chart Version	
Component Type:	container	Dif Consent:	sbabbdd
Endpoler Type:	GLOBAL Rubernetes	Git Repor	dstar65/docker-helio-world-spring-boot
Change Request Data Source:		Git Tag	mester
Category:	General	GR URL:	https://github.com/dstar55/docker-hello-world-spring-boot
Always Deplay:	No		
Deploy Sequentially:	NO		
Custom Action:			

Supply Chain "Package" Search

Package Search

Go to the 'Application View.' Select 'Package Search' from the high-level menu. Enter a package name such as 'spring' to identify all locations where the package is used.

plications Refresh + Add Base + Add Version 🗇 Delete 🗄 Tasks 🕫 🗮 List 🛱 Map = Compare Package Search				
Parent: helloworld	app			
Version		A Domain 🕴 Parent 🔅 Env	rironment 🕴 Last Deployment to Environment 🕴 Completed	
O helloworld a	p.p;1	GLOBALSanta Fe Software.Online Store Company.Hipster Store.Prod helloworld app AWS	1705 2022-05-16 21:40:43.197	
w 25 🗸 entries		Showing 1 to 1 of 1 entries (filtered from 17 total en	tresi	
		Package Search		
		Package Name spring		
		Package Version		
		Ok Cancel		
	2.22.4	PLOBAL Parts To Enforce Astron Parts Concerns New Engine Processoriality Participants and A.S. 18, edited by 19	21 2011 Early S. S. Salaran Pathon Stein Programs Markov Stars July 34, 84 Sec. 5, 5, 4	
prings	2.22.1	TO DRAW States to Explore these state company state states to explore the states and the states of t	CLOCKE, Sama ne domane crime come company repair score, bay which are 1, 2, 2, 1	
an a	5340	CLOBAL Senie To Software Online Sone Company Senie Service Recommendation Service Recommendation and CLOBAL Senie To Software Online Sone Communicational maniferration 0, 0, 101 of 1/2/2/2/2	GLOBAL Same Participant Online Store Company Paper Store Date belowed and 1	
op	33.10	GLOSH, Sena Pe Schere Scher Sere Campergreen New Engine Processing States and A 5 18 (4)(7)(2)	CLORED Series To Series College Store Company reports Store Programmers and app 1	
op	A 3 2 RELEASE	CLOCK, Sama re portante offere state company state periods recommendation service, man yr _k_k_st_ po_portante	CLOUCK Same Processes Online Solice Company repairs solice (Large An Gale (Large 1	
op	A 1 2 RELEASE	TO DEAL WARD IN SOME PERSON THAN POPULATION SHOPPING SHOPPING SHOPPING SHOPPING THE DEAL SHOPPING THE DEAL SHOPPING SHOP	ALL CARL, SARRA THE DERIVATE CARRY STATE COMPANY PROFESSION, AND THE CARL AND THE CARRY AND THE CARL AND THE CARRY AND THE CARL AND THE CARRY	
aperta	A 3 2 DELEASE	CLOBAL Senie 1: Commission and Company State Services Decrementation Service and an A. S. W. governa.	GLOBAL Savia To Sedware Online Store Company Hapter Store July 30 Oct. (C. 2)	
opeca	5318	CLORED SAME TO SAME TO THE AND COMPARISHED AND AND ADDRESS AND THE ADDRESS AND THE ADDRESS AND THE ADDRESS AND THE ADDRESS AND	CLORED Same to Setting Come State State Company report and the Company of State Company of	
ears	4.1.7 BELEARE	CLOSE, Sama re somere came som companyamenter mane recommendate somere and vit 7, 7, 78, 2047027	CLUCKE, Sama ne tratacia nome come company report store into the store 1 at a	
	A 1 2 BD CARC	Of POAL States To Bothere Asian Conservation Based and Annual Recommendations dening recommendation and the state of the state The Poal Th	OLDERAL SERVICE ON MARK CHINE COME COMPANY PROFESSION AND THE COMPANY AND THE	
cont.	24.6	CLOSED STREET CONTRACTORY CARE CONTRACTORY AND CONTRACTORY AND CONTRACTORY AND CONTRACTORY AND CONTRACTORY AND CONTRACTORY	CLOBER SERVICE CONTRACTORS OF STATE OF STATE STATE STATE TO A STATE OF STATE	
out.	140 88 848	TO DRAW HARD TO RAW THE COMPANY AND REACHES RECOMPOSITION TO DRAW TO THE DATASET	CELEVEL MERCE & DEVENTS CHIER OVER COMPANY (Space Mark Pres (Second Company))	
oot	1 4 0 RELEASE	CLOCKE, Salta FE Extense Caller Rule Company State Service Recommendation Service Incommendationservice man v1 5 5 18 abJ7010	OLOGIAL Banks Fe Software College Store Company Apple Store July 46 Old, CCC, 1	
ool autocontina re	266	Ci OSAL Santa Fe Kohore Chine State Company Jellis and master v1 0 0 101 reference	GLOBAL Santa Fe Serbarate Online Store Company I spore Contracting for One, CCC,	
	140 851 5435	N CRAL Ratio for Software Chaine Ratio Company Name Resident Recommendation Resource state vol 2, 2, 38, operators	CLORAL RANGE RE-REFACE PARTIES OF STREET PARTIES FOR THE REFERENCE OF THE	
ool a tocortig re	140 80 6486	CLOCKE James - C. Weiner, Carline Brain, Company State Banders Decomposations States and C. C. C. C. C. States and C. S. States and States an	OLOBAL States College One Company report States in the College States	
oot immode investrok	25.6	GLOBAL Santa Fe Kohare Online State Company believed in activity 0.0.101 references	GLOBAL Santa - Contraine Control Company - spore Control of the Cate Control of the Ca	
pol-states	1.4.0 RELEASE	Ci OSN Santa En Software Caline Strain Company Stain Sandora Recommendation Santov roja vi. 2, 2, 36, ph/7b22	GLOBAL Switz Ex Software Online Store Company interfer Store July 4th Sale 1, 5, 6, 1	
oot starter	1.4.0.RELEARE	OLIOBAL Sasta Fe Boftware Online Base Company State Benvices Recommendation Benvice recommendationservice and vol 3 3 38 and/Tatio	GLOBAL Banta Fe Software Online Store Company Hipster Store July 4th Sale 1 2 5 1	
ool states and	140 BELEASE	OLORAL Santa Fe Kothore Online Store Company Store Services Recommendation Service role v1 2 2 38 ph/2007	GLOBAL Santa Fe Software Online Store Company Hinder Store July ath Sale 1, 2, 9, 1	
	to the second second			

🐼 Deploy Hub

Next Steps

After completing these initial POC steps, you can add additional Components to your Application, update them via your pipeline, and view how DeployHub creates new versions of both Components and Applications overtime. Each time a Component is updated, you will see that a new version of all impacted "logical" Applications have been captured, showing you what changed.

You can also add CLI integration to your deployments and begin tracking your service inventory across all clusters, controlling drift and proactively understanding your 'blast radius" caused by a single service update.

Thank you for your interest in DeployHub.

Get Help

Email us at: request-info@deployhub.com

Report an Issue: <u>github.com/DeployHubProject/DeployHub-Pro/issues</u>

Community Discord Channel: <u>https://discord.gg/wM4b5yEFzS</u>

DeployHub Documentation: https://docs.deployhub.com/userguide/

» Get Involved in Open-Source



Help us create the best, open source supply chain management catalog available at <u>ortelius.io</u>. We believe everyone has something to offer in solving the microservice management puzzle. We would love to have you on board.



About the Author:

Tracy Ragan, CEO and Co-Founder DeployHub

Tracy is a DevOps and Open-Source security evangelist with expertise in software configuration management, and supply chain security. She has served on Boards at the Open Source Security Foundation (OpenSSF) and the Continuous Delivery Foundation. She was a founding member of the Eclipse organization and served on the board for 5 years. She is a recognized leader in open-source and has been published in multiple industry publications as well as presenting to audiences at industry conferences. Tracy co-founded DeployHub in 2019 to improve security in a the software supply chain.

Visit us at:

DeployHub.com