



CYBERSECURITY AND PRIVACY PROFESSIONALS CONFERENCE

AN **[EDUCAUSE]** EVENT



#CybersecPrivacy24

CONTAINING SECURITY

Integrating Security (DevSecOps) into Container Ecosystems

Gabriel Tocci

HOUSEKEEPING

- Moving Quickly
- Q&A Time at End
- Eye Test

Can you read this code font?

- Deck Available
 - www.gabrieltocci.com/talks

> whoami

Gabriel Tocci

Senior Consultant / Cloud Architect

- **Cloud and Container Technologies**
 - Cloud Migration
 - Cloud Optimization
 - Containerization
- **Certified Cloud Solutions Architect**
 - Amazon Web Services (AWS)
 - Oracle Cloud Infrastructure (OCI)
- **Industry Innovations**
 - 2016: ERP Implementation in AWS
 - 2016: ERP Implementation on Docker (AWS ECS)
 - 2020: ERP Implementation on Kubernetes
- **Diverse IT Background**
 - DevOps Engineer / SRE
 - Oracle DBA / Linux Sysadmin
 - Senior Software Engineer
 - BS and MS in Computer Science





HIGHER EDUCATION
TECHNOLOGY CONSULTANTS

Our mission is simple:
SIG solves problems.

- 37+ Years in Business
- Focused on HigherEd Exclusively
- 200+ Consultants
- 700+ Satisfied Clients
- Technology Agnostic

What We Do



Strategic

Process Improvement
Assessments
Digital Transformation
Project Management
Technology Procurement



Functional

Implementation
Training
Operational Performance
CRM Systems
ERP Systems



Technical

Integration
System Upgrades
BI
Reporting
Cybersecurity



Support

Staff Augmentation
Post-Implementation Support
Remote DBA (Cloud & OnPrem)

Strategic Partnerships

SIG is committed to partnering with industry leaders. And while each partnership is unique, our goal is to deliver a broad range of solutions, expert guidance, and quality services to our mutual client base. Our strategic partners include:



DISCUSSION TOPICS



Containers in HigherEd



Building / Packaging Images



Container Configuration Patterns



Container Orchestration Security



Common Issues



Monitoring / Observability

THEMES

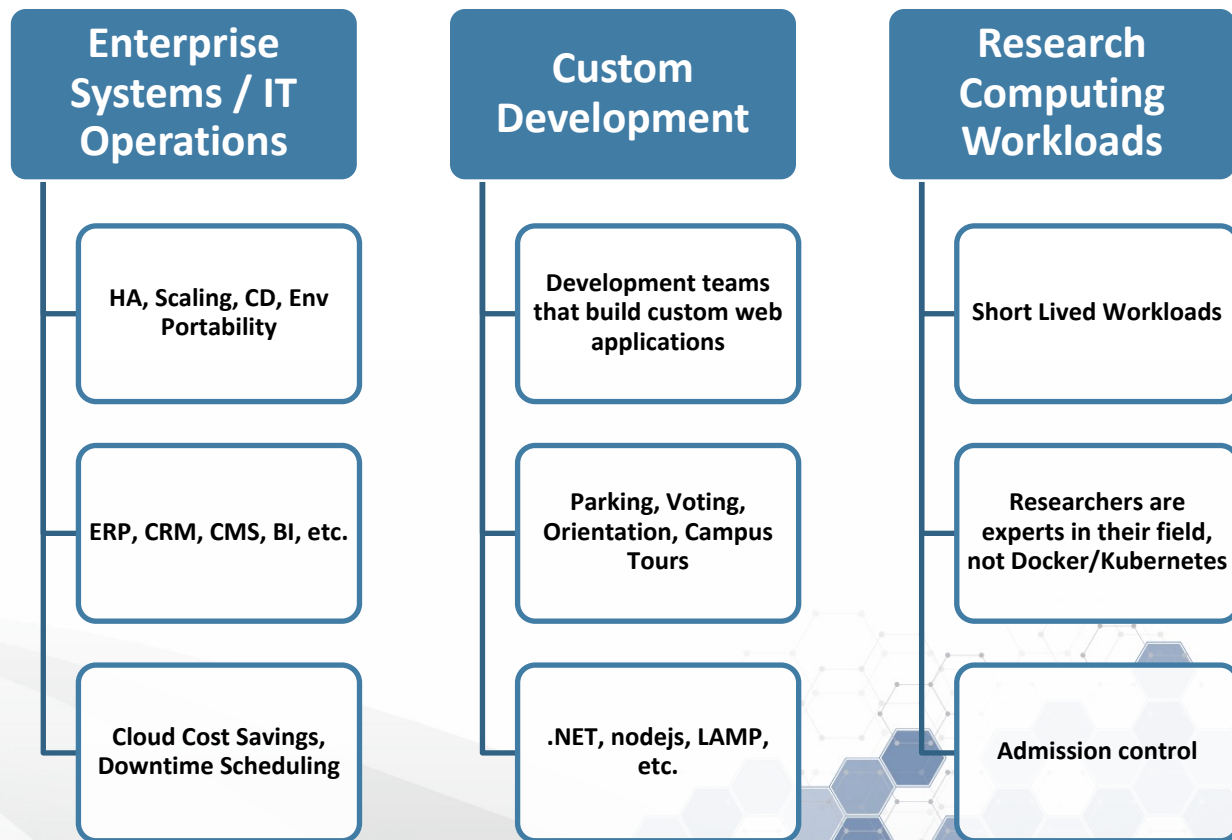


DEFAULTS

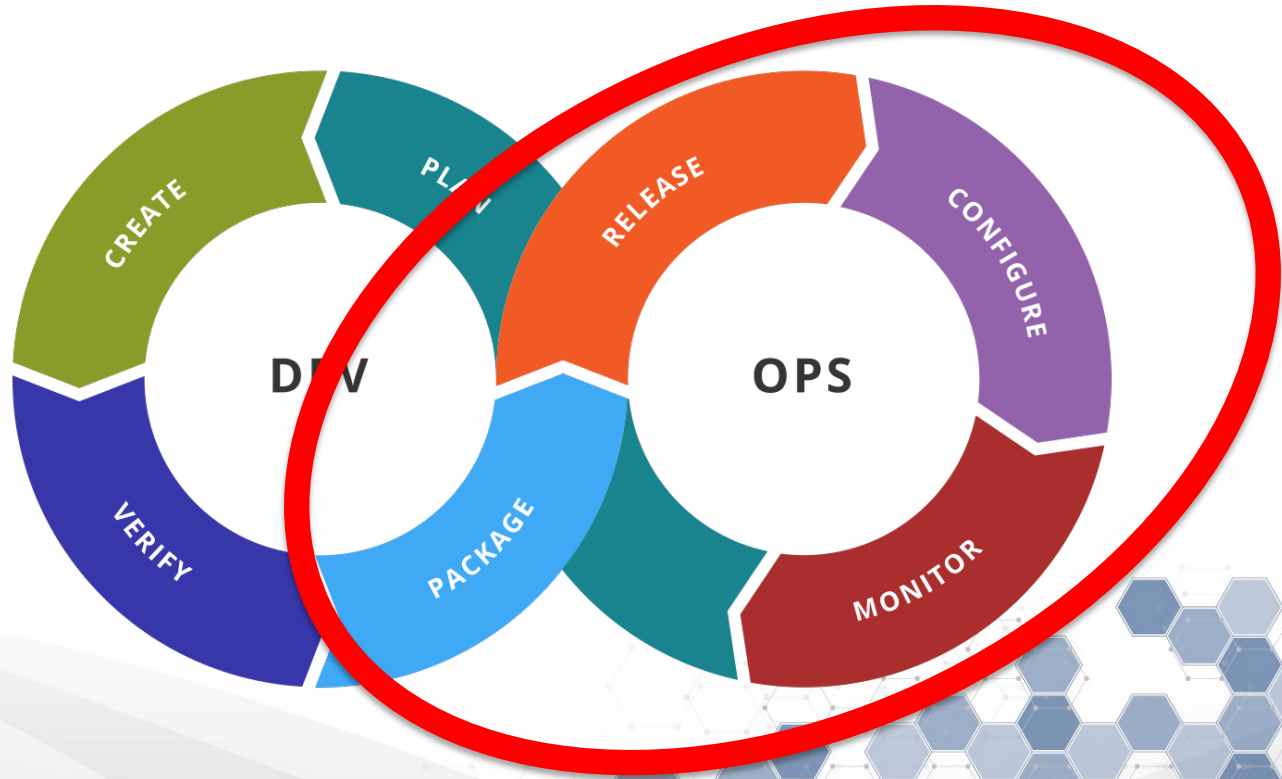
AUTOMATION

OBSERVABILITY

CONTAINERS IN HIGERED

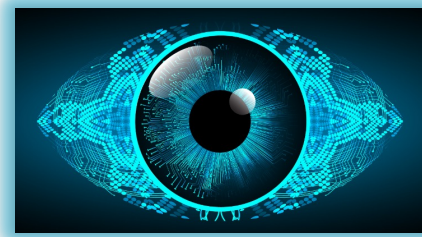


DEVOPS CYCLE



DEVOPS TOOLS

Monitoring





Packaging


Deployment




 **Jenkins**


 **CI/CD**



GitHub Actions



AWS CodeBuild



 **dockerhub**

 **RED HAT[®] Quay.io**


GitHub Packages

 **amazon ECR**




 **Amazon ECS**

 **minikube**

 **Azure Kubernetes Service (AKS)**

 **Google Kubernetes Engine**

 **Amazon EKS**


 **RED HAT[®] OPENSIFT**

 **okd**




 **docker** +  **kubernetes**

MINIOHIFT

 **K3S**

 **MicroK8s**

 **The Cloud Native Computing Foundation**

The Central Distribution of Kubernetes

PACKAGING

COMMON ISSUE: Root User

- DEFAULT Configuration Pattern for Popular Base Images
- Grants ROOT on Cluster Node!

```
# setup tomcat user
RUN groupadd -r tomcat \
  && useradd -g tomcat -d ${CATALINA_HOME} -s
/bin/bash tomcat \
  && mkdir -p /home/tomcat/bin \
  && chown -R tomcat:tomcat $CATALINA_HOME \
  && chmod +x $CATALINA_HOME/run.sh
USER tomcat
```

- K8s Admission Control

SUDO HAS A VULNERABILITY?

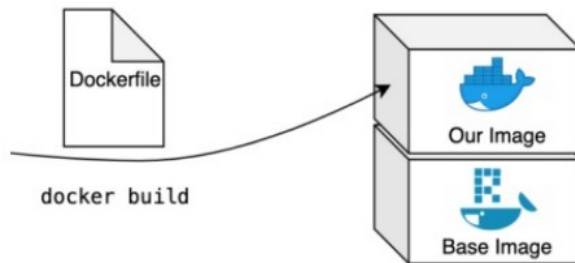
OH NO!

**WAIT, ALL MY
CONTAINERS RUN AS ROOT**

ANYWAY

PACKAGING: \$ (docker build)

- Signed Official Images
- Multilayer Images
 - Base Images
 - Common Configurations
 - Libraries
 - Create User
 - Hardening
 - Optional Layers
 - Enabled Email
 - Database Connections
 - Release Images



COMMON ISSUE: Keeping up to date

■ Automation: GitOps

- `git push(merge)`
- `image build, tag, push, rollout`

■ Upgrades: Minor / Patch

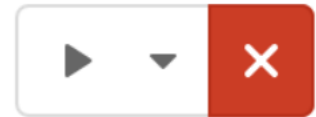
- `FROM tomcat:9.0.88-jre11`
- ✓ `FROM tomcat:9.0-jre11`
- `FROM tomcat:9-jre11`

■ Package updates

- `RUN apt-get update -y`



Run Pipeline



Start build

CONFIGURATION: \$(entrypoint.sh)

- Twelve Factor App
 - Environment Agnostic
 - No Static Values/Files
- Build time Configurations
 - Non-Secret
 - [server.conf]
 - JDBC_STRING
 - SSO_URL
 - DOMAIN
 - Secrets
 - To Be Continued...
- Runtime Configurations
 - ENV Injected into container at runtime
 - [deployment.yml]
 - [aws ssm:GetParameter]
 - ENV Examples
 - \${JDBC_STRING}
 - \${SSO_URL}
 - \${DOMAIN}

```
[entrypoint.sh]
$ envsubst < server.conf
$ sed -i -e "s|JDBC_STRING|${JDBC_STRING}|g" server.conf
$ sed -i -e "s|SSO_URL|${SSO_URL}|g" server.conf
$ sed -i -e "s|DOMAIN|${DOMAIN}|g" server.conf
```

COMMON ISSUE: Static Secrets



■ Static Secrets

- API Keys / Service Tokens
- DEFAULT Configuration Pattern for Popular Frameworks
- .env files

```
{  
  dev: "devPASS123",  
  test: "testPASS456",  
  prod: "prodPASS789"  
}
```

- Runtime identity / assumable role
- K8s Secrets vs. External Secrets
 - K8s Secrets are Stored Unencrypted
 - K8s External Secrets Operator
- Injected into container ENV at runtime
 - [deployment.yml]
 - [aws secretsmanager:GetSecret]
 - \${JDBC_PW}



```
[entrypoint.sh]  
$ envsubst < server.conf  
$ sed -i -e "s|JDBC_PW|${JDBC_PW}|g" server.conf
```

COMMON ISSUE: Static Secrets

```
$ docker run -it --rm --entrypoint /bin/bash  
<registry/image:tag> -c "<some-command>"
```

```
1  $ docker run -it --rm --entrypoint /bin/bash <registry/image:tag> -c "find / -name *env*"
2  /etc/environment
3  /etc/security/pam_env.conf
4  /etc/environment.d
5  /run/.containerenv
6  /opt/laravel/app/.env
7  /usr/bin/env
8  $ docker run -it --rm --entrypoint /bin/bash <registry/image:tag> -c "grep DB /opt/laravel/app/.env"
9  DB_CONNECTION=mysql
10 DB_HOST=127.0.0.1
11 DB_PORT=3306
12 DB_DATABASE=laravel
13 DB_USERNAME=root
14 DB_PASSWORD=<thepassword>
15 $
```


COMMON ISSUE: Static Secrets

- NSA/CISA Hardening Guidance
 - [Kubernetes](#)
 - [DevOps](#)
- Security Research
 - ACM CCS 2023:
 - [Secrets Revealed in Container Images: An Internet-wide Study on Occurrence and Impact](#)
 - DC31: Ian Dillon
 - [Hunting Sensitive Docker Images in Google Container Registry Leaks](#)



COMMON ISSUE: Build Context Leaks

```
docker.com/blog/getting-started-with-docker-using-node-jspart-i/

FROM node:12.18.1

WORKDIR /app

COPY package.json package.json
COPY package-lock.json package-lock.json

RUN npm install

COPY . .

CMD [ "node", "serve"
```

github.com/search?q=org%3Adockersamples+"COPY+.".&type=code

org:dockersamples "COPY . ." repo:

Filter by

- Code 52
- Repositories 0
- Issues 14
- Pull requests 22
- Discussions 0
- Users 0
- More

52 files (89 ms) in dockersamples

dockersamples/example-voting-app · vote/Dockerfile

```
24 FROM base AS final
25
26 # Copy our code from the current folder to the working directory inside the container
27 COPY . .
28
29 # Make port 80 available for links and/or publish
30 EXPOSE 80
```

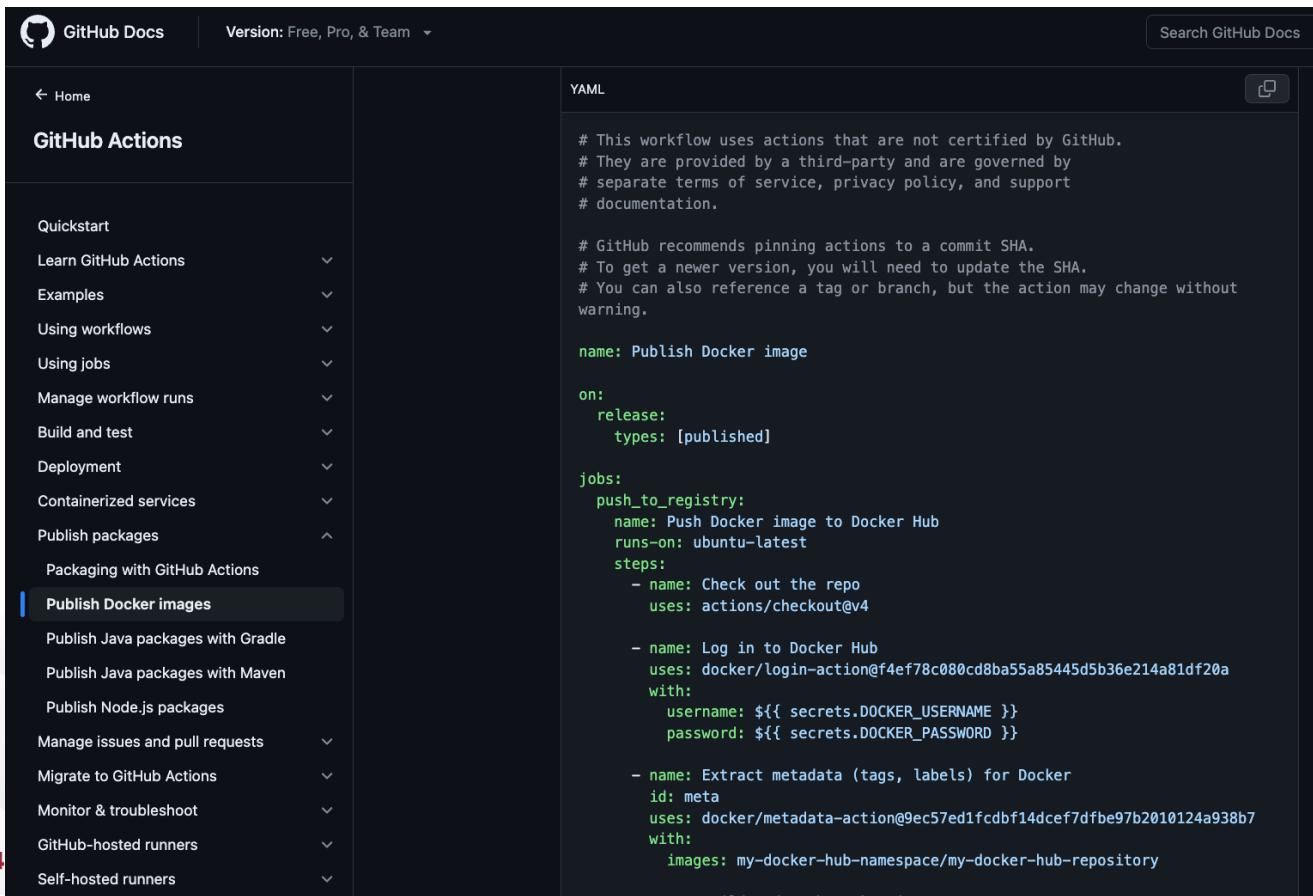
COMMON ISSUE: Build Context Leaks

- What Just Happened?
 - COPY . .
 - Implicit COPY ALL
 - Better:
 - Explicit COPY
 - COPY /app /app
 - COPY /bin /bin
 - .dockerignore
 - Explicit DENY
 - Better
 - Implicit DENY
 - Explicit COPY
- How To Defend This?
 - Dockerfile Static Analysis
 - Image Scanning
 - Education

COMMON ISSUE: Registry Misconfiguration

- Privacy is often Public by DEFAULT
- UI Confusion
- `$ docker push`
- Public/Private Images
- Add registry audit log to SIEM
 - Alert on privacy changes

COMMON ISSUE: CICD Context Leaks



The screenshot shows the GitHub Docs interface. The left sidebar contains a navigation menu for 'GitHub Actions', with 'Publish Docker images' selected. The main content area displays a YAML workflow for publishing Docker images to a registry. The workflow includes comments about action certification and pinning, and defines a job named 'push_to_registry' with steps for checking out the repository, logging into Docker Hub, and extracting metadata.

```
YAML

# This workflow uses actions that are not certified by GitHub.
# They are provided by a third-party and are governed by
# separate terms of service, privacy policy, and support
# documentation.

# GitHub recommends pinning actions to a commit SHA.
# To get a newer version, you will need to update the SHA.
# You can also reference a tag or branch, but the action may change without
warning.

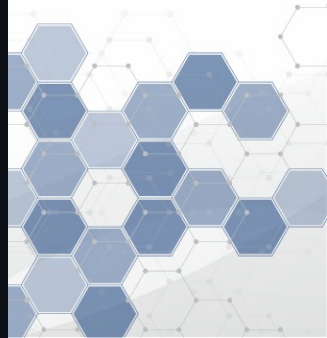
name: Publish Docker image

on:
  release:
    types: [published]

jobs:
  push_to_registry:
    name: Push Docker image to Docker Hub
    runs-on: ubuntu-latest
    steps:
      - name: Check out the repo
        uses: actions/checkout@v4

      - name: Log in to Docker Hub
        uses: docker/login-action@f4ef78c080cd8ba55a85445d5b36e214a81df20a
        with:
          username: ${ secrets.DOCKER_USERNAME }
          password: ${ secrets.DOCKER_PASSWORD }

      - name: Extract metadata (tags, labels) for Docker
        id: meta
        uses: docker/metadata-action@9ec57ed1fcd8bf14dcef7dfbe97b2010124a938b7
        with:
          images: my-docker-hub-namespace/my-docker-hub-repository
```



COMMON ISSUE: CICD Context Leaks

- **Gitlab Pipelines Logfiles**
 - Secrets are stripped from logs via regex
 - Careful with structured data
 - Audit User Access
- **Protect main Branch**
 - Monitor and Audit changes to CICD scripts
 - Scope secrets from environment to branch
 - Prod Secrets = main
 - Dev Secrets = develop

```
build-and-deploy
succeeded 2 minutes ago in 2m 21s

> ✓ Set up job
> ✓ Build sonarsource/sonarcloud-github-action@master
> ✓ Build wei/curl@v1
✓ ✓ Demo secret
  1 ▶ Run echo ***
  6 ***
  7 m y - s e c r e t - v a l u e
> ✓ Run actions/checkout@v1
```

CICD CONCERNS

- GitHub Actions
 - Open-source modules executed by Runner
 - Audit the Source Code
 - [Pin the commit SHA](#)
- Runner Security
 - Node Security

```
on: push

name: Continuous Integration

jobs:
  harden_security:
    name: Harden Security
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@5a4ac9002d0be2fb38bd78e4b4dbde5606d7042f
      - name: Ensure SHA pinned actions
```

DEPLOYMENT

COMMON ISSUE: Keeping up to date

- Automation and Scheduling
 - Node Updates and Patches
 - Cloud/Serverless Runtimes
 - K8s API Updates
 - Manual-ish In the Cloud
 - Manual On-Prem
 - Ansible, etc.

■ Image Builds

- Scheduled Pipeline Execution
 - ✓ FROM tomcat:9.0-jre11
- RUN apt-get update -y

```
▼ Dockerfile
1 - FROM public.ecr.aws/docker/library/tomcat:8.5-jdk8-temurin-focal
2 + FROM public.ecr.aws/docker/library/tomcat:9.0-jdk11-temurin-focal
2 2
```

ORCHESTRATION: \$ (kubect1 rollout)

- Network Topology
 - Private Subnets
 - Control Plane and Workers
 - Network Security Policies
 - Disabled by DEFAULT
- Data Encryption
 - TLS
 - ETCD
- RBAC: Roles and Privileges
 - Disabled by DEFAULT
- Mounted Volumes (ro/rw)
- Admission Control...



ORCHESTRATION: Admission Control

- Gatekeeper
 - [42 Public Policies](#)
- Kyverno
 - [328 Public Policies](#)
- Example Polices
 - Disable root execution
 - Disable creation of nodeport service
 - All Traffic via Ingress
 - Require Default deny network policy for all namespaces
 - Force resource limits on pods/quotas
- Whitelist image registries
- Whitelist base images
- Block specific known CVEs
- Require hostname in ingress routes
 - No */* routes
- Force encryption of etcd



MONITORING

COMMON ISSUES: Flying Blind

- Nothing is Monitored by DEFAULT
 - Blocked API Requests
 - Scan Results
 - Images
 - Registry Privacy
 - Infrastructure
 - System Response Time
- Alerts
 - Multi-Channel
 - Priorities
 - Thresholds



MONITORING: SIEM, SOAR

- **Image Build Pipelines**
 - Return codes
- **Image Scanning**
 - SBOM
 - Static (registry)
 - Build Time && Runtime
- **Image Registry Auditing**
 - Privacy Changes
 - Push/Pull Activity
- **Infrastructure Scanning**
 - Cloud Infrastructure
 - Vulnerabilities
 - Penetration Tests
- **Centralized Logging**
 - Network/WAF/LB Logs
 - Orchestration
 - Users
 - Deployments
 - Cluster Nodes
 - Application Logs
- **Analysis**
 - Anomaly Detection
 - Alerting
- **Single Pane of Glass**
 - Avoid Fragmentation

QUESTIONS?

RESOURCES

■ Resources

- NSA/CISA Hardening Guidance
 - [Kubernetes](#)
 - [DevOps](#)
- DC31: Ian Dillon
 - [Hunting Sensitive Docker Images in Google Container Registry Leaks](#)
- ACM CCS 2023:
 - [Secrets Revealed in Container Images: An Internet-wide Study on Occurrence and Impact](#)
- [12 Factor Methodology](#)

■ Contacts

- www.gabrieltocci.com
 - linkedin/gabrieltocci
- www.sigcorp.com
 - linkedin/strata-information-group

■ Rate My Professor

