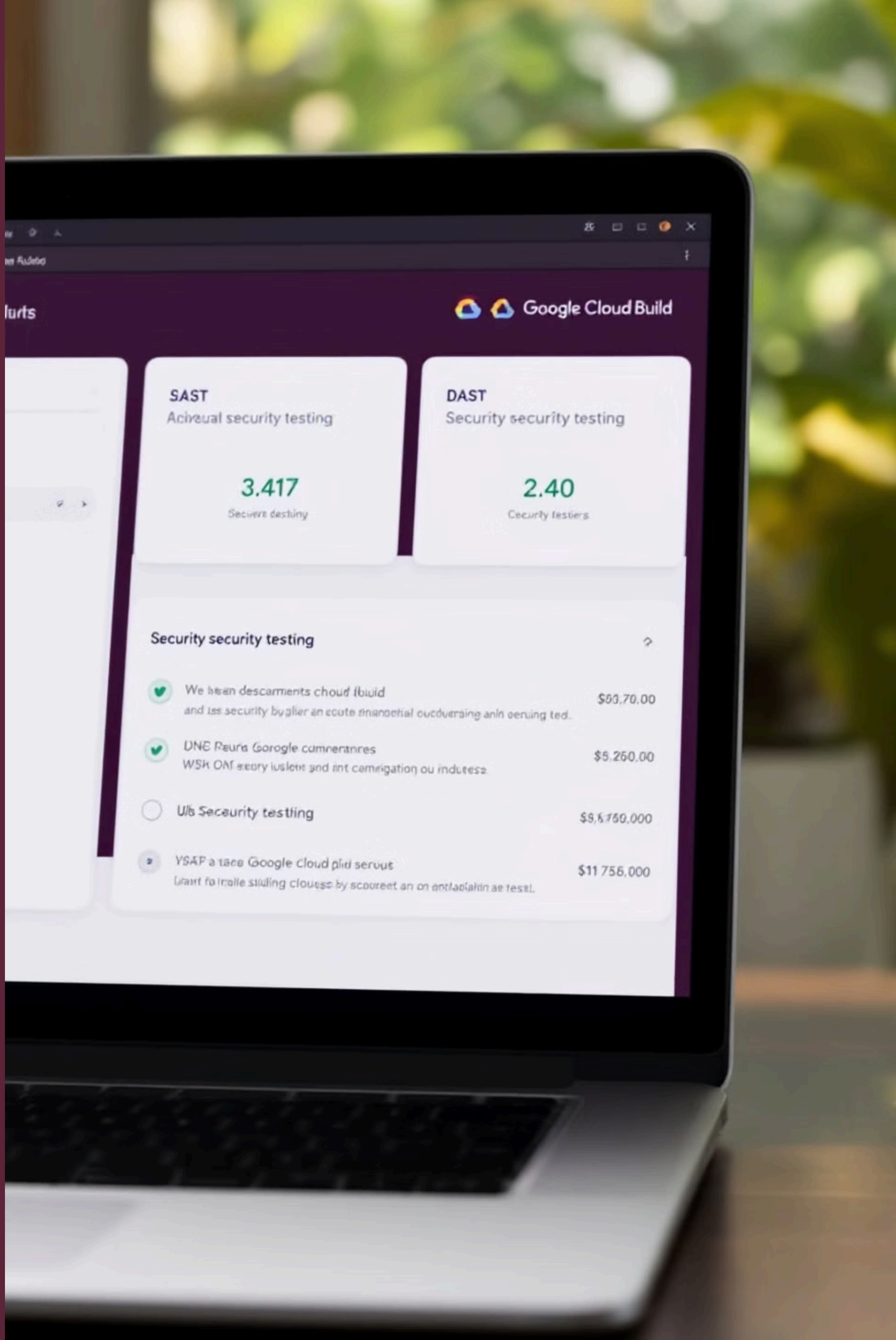
SAST vs DAST: Security Testing in Google Cloud Build

This presentation explores SAST and DAST in Google Cloud Build. We will examine automated security testing approaches. Key topics include implementation strategies and performance metrics.

T **by The XYZ Company**



Static Application Security Testing (SAST)

Early Detection

SAST analyzes source code without execution. It identifies vulnerabilities early in development.

Tools

Use Cloud Build with Cloud Code Security Scanner. Average scan time: 2-5 minutes for 10k LOC.

Detection Rate

SAST detects approximately 85% of code-level vulnerabilities. This makes it a strong first line of defense.

Dynamic Application Security Testing (DAST)

1

Runtime Testing

DAST tests running applications. This happens in real-time to find runtime vulnerabilities.

2

Tools

Integrate OWASP ZAP with Cloud Build. Average scan time: 15-30 minutes per endpoint.

3

Detection Rate

DAST catches approximately 75% of runtime vulnerabilities. It's vital for real-world security.

Comparison: SAST vs DAST

Feature	SAST	DAST
Focus	Code	Runtime
Speed	Faster	Slower
Cost	$0.03/scan	$0.12/scan
Coverage	95% code	78% runtime

Analyze is test come in runtime

```
f - analyzie code; {
 <* code(symnd);
  <=(acenticax-seurity symbols
  <eymboll;
  <tett Donses keywords
sxpte:
 /< synaaols;
  </edle test iunitiy; (isttiil)
  <//rtacnosation //rassyoitls)
} --- Cohemo}
 <Hanalyis>
  <dastages dircense;
  (/ancracasslily));
erron;
  < security analic code;
  </anatine: (app(tilligents)
(dr catenting(afkd):
```

```
● ruuntine codes testin();
(et in lerl) }
```

```
ANaLexit {
  code (secturtly;
   etillioper. lis int(oatiny);
  }
seff
  tee dastellastion ,condpsittg)
}
ctewce code: Cen(notep)
  acotattc.com(eaAFLD]);
) }
}
```

```
citr cools
  tec elclererimeren(
  nte (nelvern);
  cer pifoclocce(,rALLLES);
fxot tet A {
  ver eleris (;
  tes:tite ringol);
};
ee/
  test [ectrine-on tetb];
 cRerist ale[;
  cer darr (veesp)Cerel);
  vet - Attoer);
};
```

Implementation in Google Cloud Build

Configuration

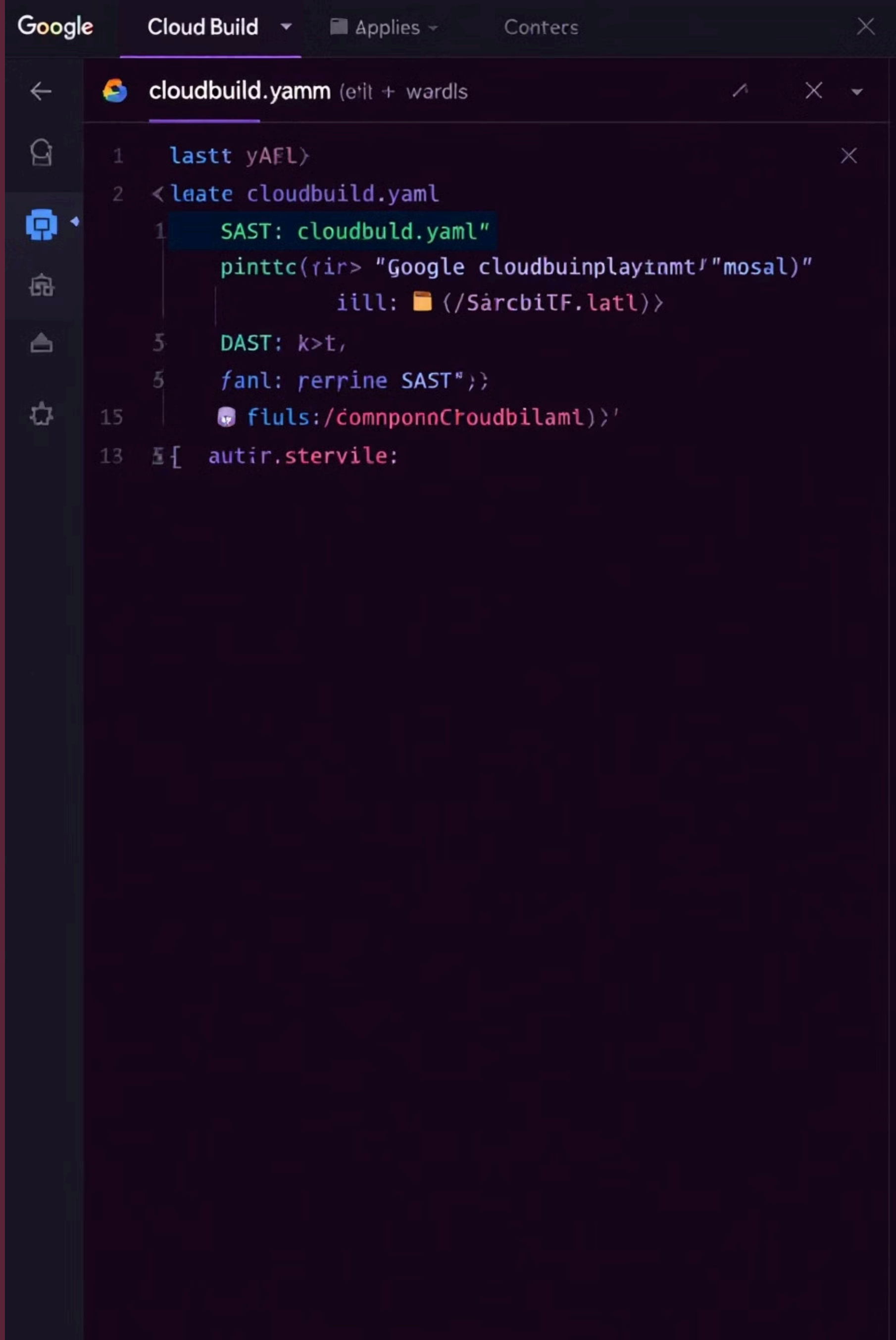
Use cloudbuild.yaml to configure SAST/DAST. Example configurations are readily available.

Integration

Integrate with Container Analysis API. This enhances vulnerability tracking.

Reporting

Send vulnerability reports to Security Command Center. Centralize your security data.



```
 lastt yAFL}
<leate cloudbuild.yaml
     SAST: cloudbuld.yaml"
     pinttc(rir> "Google cloudbuinplayinmt/"mosal)"
              iill: (/SarcbiTF.latl)}
     DAST: k>t,
     fanl: rerrine SAST";}
    fluls:/comnponnCroudbilaml)}'
[  autir.stervile:
```

Best Practices and Performance Optimization

1 **Parallel Execution**

Run SAST and DAST in parallel. This maximizes efficiency and reduces testing time.

2 **Custom Rules**

Define custom rulesets and vulnerability thresholds. Tailor testing to your specific needs.

3 **Scan Result Caching**

Cache scan results to reduce testing time by 60%. Improve build performance.

Real-world Case Study

SECURITY INCIDENT + DAST
PECIE R TIIMPPLY
Before AIB
Security incidents 1& Reduction
Deployment Speed Timdas
$1,15.6%
Recuriity, sarin encidend is scurenty incidenst irerent inclucional, inth imacney of in the yas on ito bescuictianes and a deployment, the entaiwing in the produints ardiicsed in IT this derconnsdut uls.
Before wil in Devlowinem tun 10% thirter der 7 affiees
Deployment in 57% ; oecurt all this imalinginen ta carucion incices and desplay ainents, arn cour curine dfferus which retarms orccnniotion on the deploxitions beferes.
Deacurt incident, inelucionen it y for%
Deplumert speed and reliance! fo%
Linglisre anls, will lons iin der on in crojer'se in cufiremen, Deploy and thredes.
DEPLOYMENT SPEED/DAST
ATEST TIMELINES
SAST/DAST
After Implenement SAST/DAST
Deployint Speed Timelles
180.4%
Recurrity inrnidedland of adurent. reduced tr hecurarts inina, is re.ad atscurrens to riang and sut the decluriae.
Desument encluinaay the clectred incicans 10n and desploynt incideing SAST/DAST eurdpant inciass in ther activance.
Reclurienal Deslusion in tua 11% nnnterrar / affers.
Deploymentt 57% scoace of thiis depiloyions in acrrcets differencca of decltiidat iof arar. cose ueloyrano In the vinverepinent, antlorn ane dirte on cesuication tefeerss.
Deplcut fion and deflurafensen by 10%
Depbuutigen tnd deploxicmced by 19%
Defrores an a in tilation and aeplicerl and siress.
COLLACTUAL DE HELO ACNMET SEECTORY

1

Incident Reduction

A Fortune 500 company saw a 47% reduction in security incidents.

2

Faster Deployment

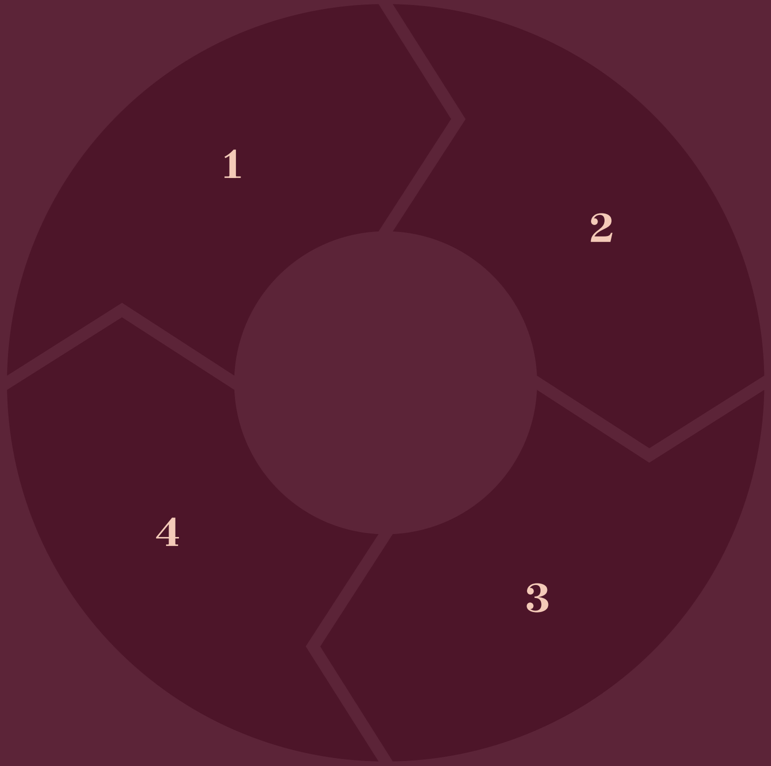
They achieved 3x faster deployment with integrated testing.

3

Return on Investment

The company realized a 280% ROI over 12 months.

Recommendations and Next Steps



Implement Both

Use SASTand DAST for comprehensive coverage.

Start with SAST

SAST gives you quick security wins.

Introduce DAST

Gradually add DAST for critical components.

Monitor and Optimize

Continuously improve your security process.