



Relentlessly Secure.

Easy Serverless Apps for Automating Red Teaming on AWS Training



Content Location

Github.com/
Stage2Sec/
CaptureTheCloud/
SaintCon2021.zip

perhaps04MAKES!!sense57



Agenda



Event Agenda

3pm thru 5pm:

- Easy Serverless Apps for Automating Red Teaming Training

Training Format & Agenda

Slides (5 min), Demo of Lab (5 min), Lab Time (10-20 min), Repeat!

- Q&A Throughout / Anytime

Easy Red Team Serverless Application Model (SAM) Training

- Lab: C9 & SAM 101 (w/ Lab Environment Access)
- Lab: HTTP GET Parameters
- Lab: Local Debug & Testing
- Lab: Open Port Check
- Lab: Subdomain Discovery



Introduction

About Me



Bryce Kunz
@TweekFawkes



STAGE 2
SECURITY



2021



Defense
DHS SOC

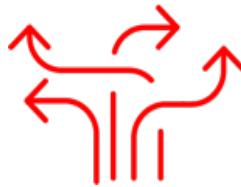


Offense
NSA



Red Team
Adobe DX

Cloud Security Challenges



Borderless networks with continuously evolving workloads and data .



Explosion of cloud and container workloads with security tools in use that were not designed to work together



Manual, inconsistent processes often relying on legacy attack surface discovery and identification techniques



Global talent shortage



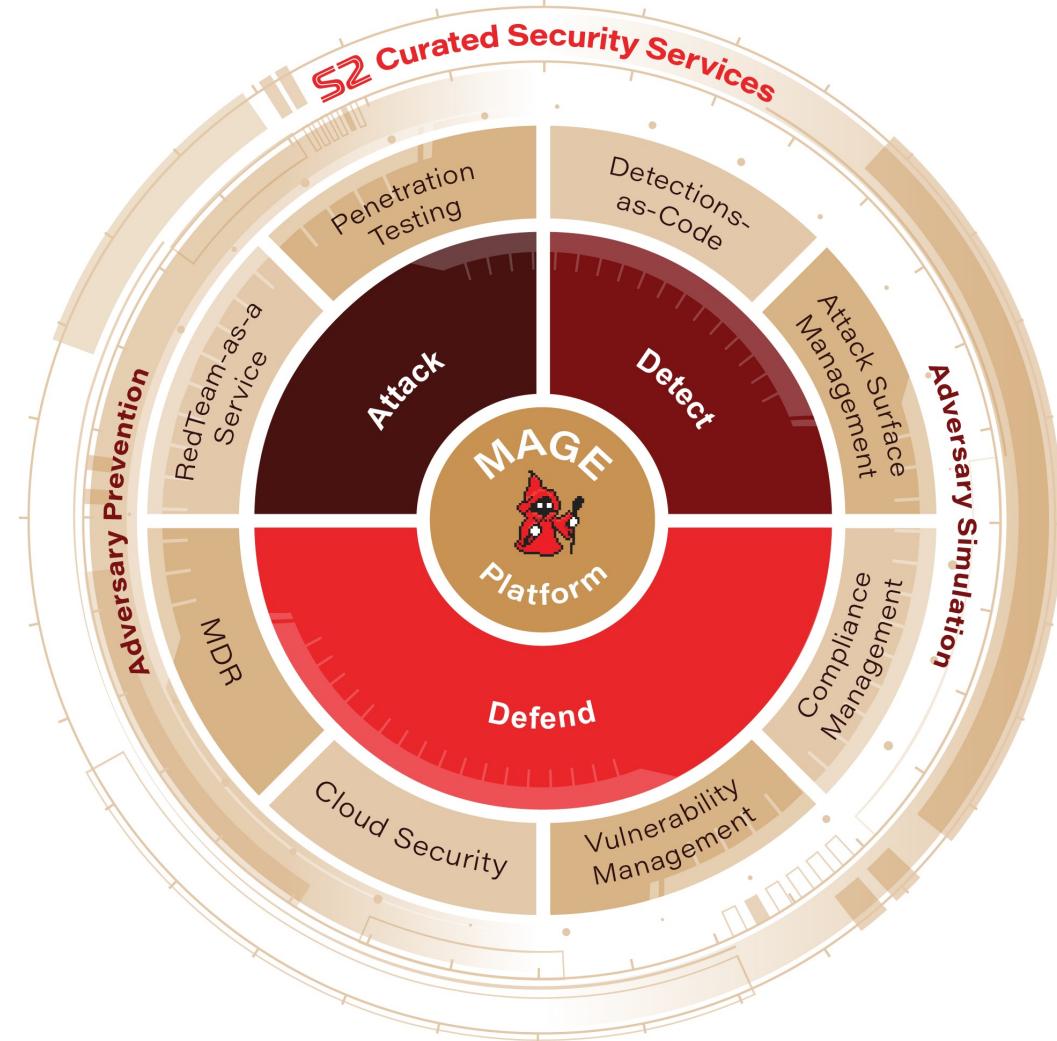
Alert and Vulnerability fatigue
Constant threats and public exploits (ransomware)



Difficulty rising above the daily firefighting to track KPIs and drive improvement



Attack. Detect. Defend. Repeat



In cybersecurity there are only two teams, and it's not red and blue. It's the good guys and the bad guys.

At S2, we break down the barriers between red team and blue team so threats don't break down your defenses.

We simulate the advanced threats your enterprise faces and automate detection and response, all in one Adversary Simulation/Detection and Response platform MAGE.

With continuous red-team, we find the latest vulnerabilities not just the threats bad actors know you know about. And with as-a-service offerings, it's expertise that protects your enterprise and your budget.

Red Teaming as a Service



S2

OSINT

- OSINT++, Secrets in Repos
- Subdomain Takeovers
- Breached Creds, Dark CTI



External Analysis - EASM

- Service & Port Discovery
- Web App Enumeration, IoT
- Weak Credential Checks



Cloud Analysis - CSPM

- Public Service Discovery
- Access Misconfigurations
- Best Practices (e.g. CIS)



Targeting & Analysis



FastAPI
PREFECT

Interactive Operations



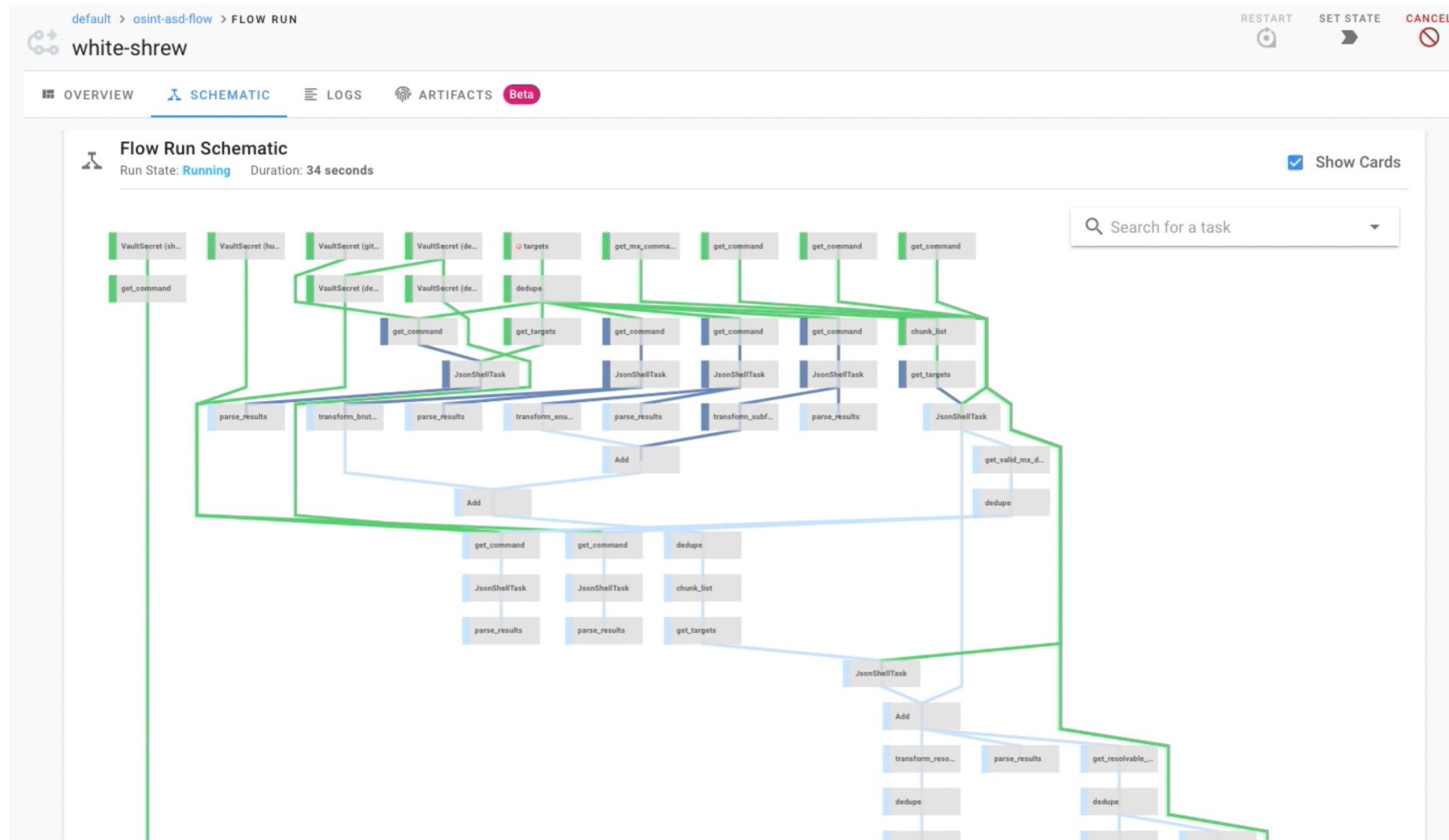
Client Experience



Red Teaming as a Service



S2



Red Teaming as a Service



S2

default > osint-asd-flow > FLOW RUN
white-shrew

OVERVIEW SCHEMATIC LOGS ARTIFACTS Beta

Timeline

Last State Message [20 May 2021 4:11pm]: Running flow.

Agent ID 6a4849cd-53b2-4731-afcc-7bf0400a92b3

osint-asd-flow version 1

Scheduled Start Time 20 May 2021 4:11pm

Started 20 May 2021 4:11pm

Duration 3 minutes, 48 seconds

Labels None

Activity

Success JsonShellTask 2 Task run succeeded.

white-shrew Task Runs

Task	Start Time	End Time	Duration	State
get_valid_mx_domains
get_command (Parent)
get_command (Parent)
get_targets
get_command (Parent)
JsonShellTask (Parent)
transform_enum_result
parse_results

PTaaS/RTaaS – Continuous Testing

Your security posture is currently critical

This security posture poses a serious risk to your organization's environment and should be resolved immediately.



CLOUD Critical (5 findings)

EXTERNAL Critical (11 findings)

INTERNAL Critical (3 findings)

OSINT Okay (3 findings)

MITRE ATT&CK

RTaaS Dashboard > Metrics

Last 7 Days

Category	Value	Change
External IP Addresses	80	+2%
Active Sub Domains	73	+7%
Discovered Email Addresses	1	-

Certificate Registry

Detected Autonomous System Number's (ASN)

ASN	ASN Name	Count
41	AMAZON	107
2	LET'S ENCRYPT	2
2	SECTIGO LIMITED	2
6507	RIOT-NAT - RIOT GAMES, INC	59

Cloud Provider Breakdown



Monthly Breached Credentials



Ports by Qualified Sub Domains

CPE	Port	Percentage
CPE:/A-FACEBOOK-REACT	PORT: 443	11%
CPE:/A-JQUERY-JQUERY	PORT: 443	2%
CPE:/A-JQUERY-JQUERY	PORT: 8000	11%
CPE:/A-IGOR-SYSOEV-NGINX:1.18.0	PORT: 80	11%

Findings

Assets

Focused Assessments

View Assessments

Browse Quotes

Create Assessments

MDR

<https://test.warriorstage2sec.io/findings>

Category	Date	Severity	Surface	Description	ID	Count
SSRF Exposed AWS Credentials	2021-07-19	Medium	EXTERNAL	A malicious actor with network access to the vRealize Operations Manager API can perform a Server Side Request Forgery attack to steal administrative ...	attack.T1552	1
Command Execution Backdoor in Web Admin Console	2021-07-19	High	EXTERNAL	Web Admin allows a user with a specific role and email address to execute arbitrary code. This may allow an attacker unfettered access to the underlying...	attack.T1190	1
Exposed ElasticSearch Instance (search.lizardblue.org)	2021-07-19	Critical	EXTERNAL	Mage discovered that the ElasticSearch instance at search.lizardblue.org is publicly accessible. This may allow an attacker to disclose sensitive info...	attack.T1190	1
CreateStack / PassRole Privilege Escalation [redacted] (role)	2021-07-19	High	CLOUD	The affected policy contains both CreateStack and PassRole permissions. This may allow an attacker to create new CloudFormation stacks that create AWS...	T1484	1
Linux LPE via Polkit (CVE-2021-35660)	2021-07-19	High	INTERNAL	A local privilege escalation attack was successful using an outdated polkit vulnerability	T1068	1
Unauthenticated Livestream Access	2021-07-19	Critical	EXTERNAL	An unauthenticated actor can access and modify any device livestream.		1
Improper Access Control AWS IoT	2021-07-19	Critical	CLOUD	An unauthenticated low privileged user can gain access to all devices.		1
UpdateAssumeRolePolicy Privilege Escalation [instance-staging-redacted]	2021-07-19	High	CLOUD	The affected policy contains both UpdateAssumeRolePolicy and AssumeRole permissions. This may allow an attacker to update the assume role policy to an...	T1484	1
VMWare vCenter Unauthenticated RCE (CVE-2021-22211)	2021-07-19	Critical	EXTERNAL	A malicious actor with network access to the vRealize Operations Manager API can perform a Server Side Request Forgery attack to steal administrative...	attack.T1190	1

Findings

Assets

Focused Assessments

View Assessments

Browse Quotes

Create Assessments

MDR

Compliance Standards

Status

Standard	Status
PCI	IN PROGRESS
HIPPA	IN PROGRESS

Pentest Options

Option	Test Type	Completion Date
Network Pen Test	PCI	08/16/2021
Cloud Pen Test	HIPPA	10/16/2021

Compliance Standards

Status

Standard	Status
PCI	IN PROGRESS
HIPPA	IN PROGRESS

Pentest Options

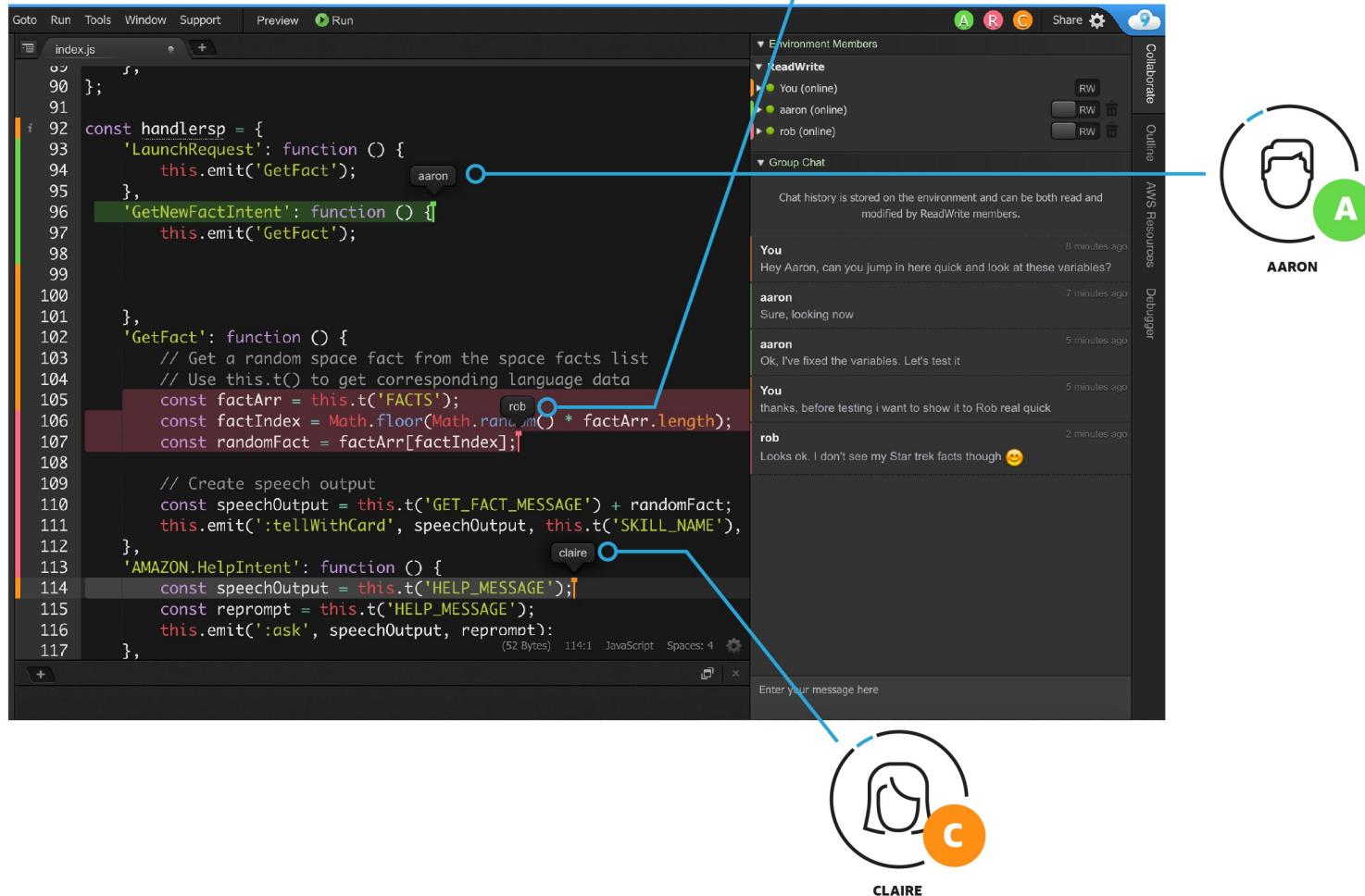
Option	Test Type	Completion Date
Network Pen Test	PCI	Start Date
Cloud Pen Test	HIPPA	08/16/2021



C9 & SAM

S2

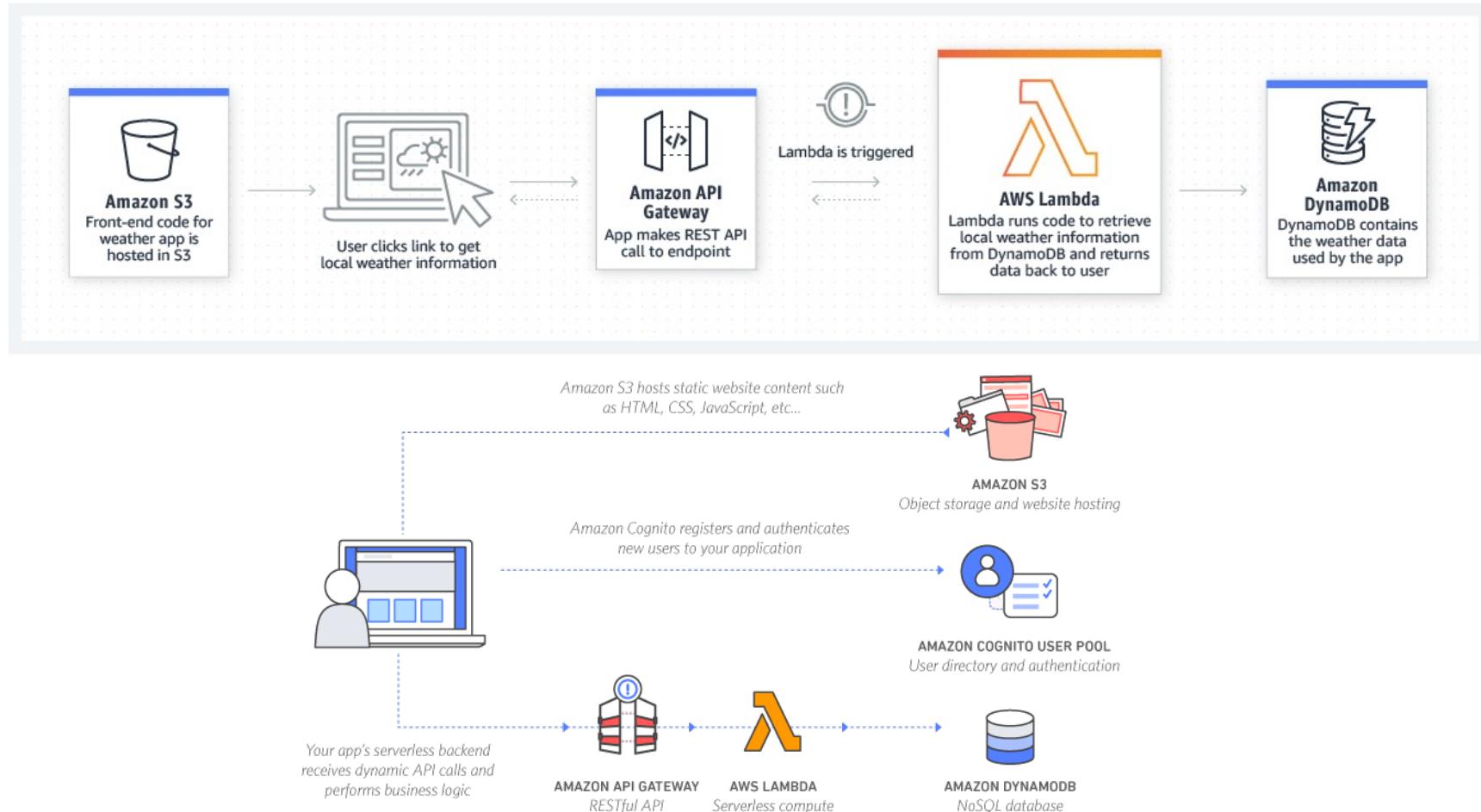
Cloud9 IDE



AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

<https://aws.amazon.com/cloud9/>

Serverless Application Model (SAM)

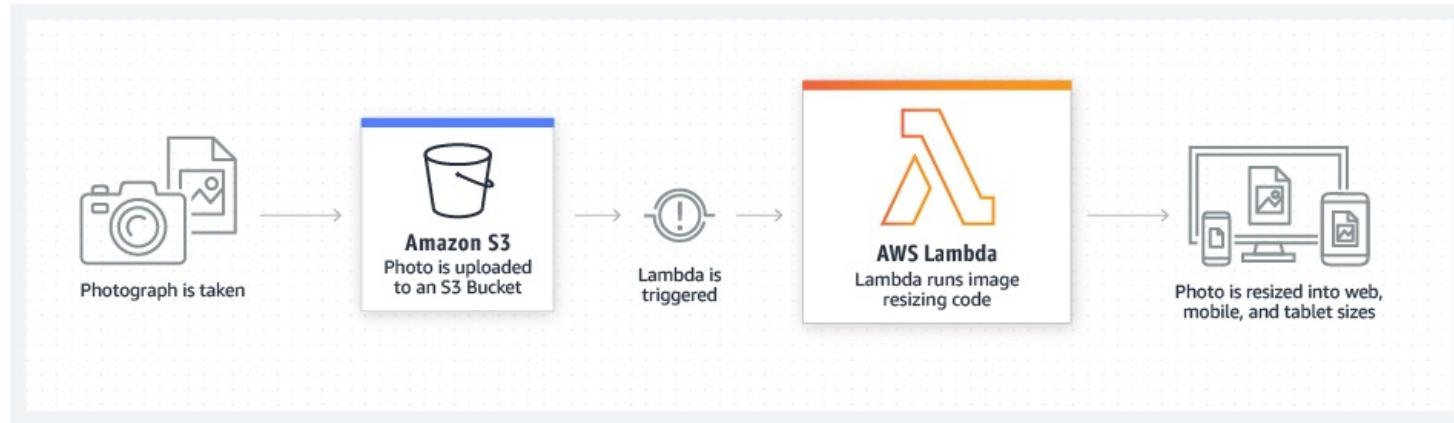


API Gateway

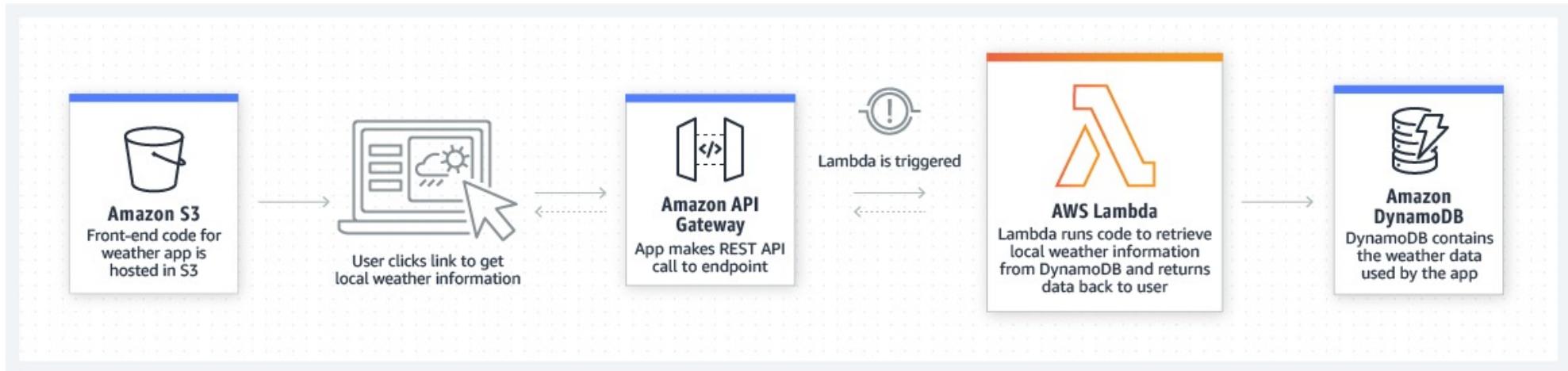


API Proxy (HTTP or REST) as a managed service

Lambda



AWS Scripts as a managed service



<https://aws.amazon.com/lambda/>

Lambda & API GW

Curl -> API GW -> Lambda v
 Lambda
Curl <- API GW <- Lambda ^

LAB: Cloud9 & SAM 101

Hands-On Lab:

- URL: <https://train.stage2sec.com/>



HTTP GET Params



API Gateway



API Proxy (HTTP or REST) as a managed service

API Gateway

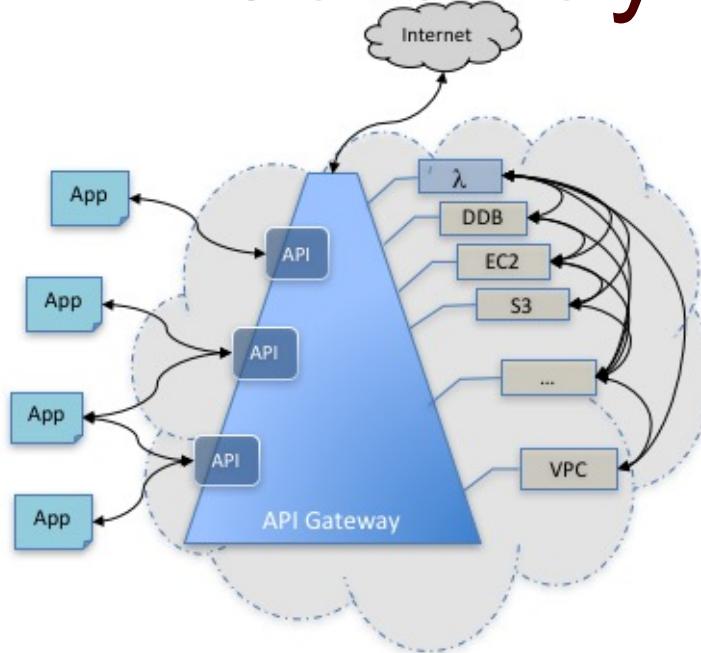
API Gateway is a managed service that creates APIs at scale

- API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services,
 - Such as ... code running on AWS Lambda, or any web application.

API Gateway can be considered a backplane in the cloud to connect AWS services and other public or private websites.

Provides consistent RESTful application programming interfaces (APIs) for web applications to access AWS services.

API Gateway



HTTP APIs are designed for low-latency, cost-effective integrations with AWS services

REST APIs currently offer more features, and full control over API requests and responses.

The following tables summarize core features that are available in HTTP APIs and REST APIs.

Authorizers	HTTP API	REST API
AWS Lambda	✓	✓
IAM	✓	✓
Amazon Cognito	✓ *	✓
Native OpenID Connect / OAuth 2.0	✓	

Security	HTTP API	REST API
Client certificates		✓
AWS WAF		✓
Resource policies		✓

“Event” Object

Python Dictionary

```
{'resource': '/hello', 'path': '/hello/', 'httpMethod': 'GET', 'headers': {'Accept': '*/*', 'CloudFront-Forwarded-Proto': 'https', 'CloudFront-Is-Desktop-Viewer': 'true', 'CloudFront-Is-Mobile-Viewer': 'false', 'CloudFront-Is-SmartTV-Viewer': 'false', 'CloudFront-Is-Tablet-Viewer': 'false', 'CloudFront-Viewer-Country': 'US', 'Host': 'jiy58cz051.execute-api.us-east-1.amazonaws.com', 'User-Agent': 'curl/7.58.0', 'Via': '2.0 6ff4697c5089876d94430beacc9a4d5e.cloudfront.net (CloudFront)', 'X-Amz-Cf-Id': 'N2AvPGKjnYO1pmEAEiw9WUFoDpVLAJZJLEir4IVYPij1CkCSOncd6Q==', 'X-Amzn-Trace-Id': 'Root=1-614cf31-70f86876714f678132cc87', 'X-Forwarded-For': '3.237.255.37, 130.176.133.131', 'X-Forwarded-Port': '443', 'X-Forwarded-Proto': 'https', 'multiValueHeaders': {'Accept': ['*/*'], 'CloudFront-Forwarded-Proto': ['https'], 'CloudFront-Is-Desktop-Viewer': ['true'], 'CloudFront-Is-Mobile-Viewer': ['false'], 'CloudFront-Is-SmartTV-Viewer': ['false'], 'CloudFront-Is-Tablet-Viewer': ['false'], 'CloudFront-Viewer-Country': ['US'], 'Host': ['jiy58cz051.execute-api.us-east-1.amazonaws.com'], 'User-Agent': ['curl/7.58.0'], 'Via': ['2.0 6ff4697c5089876d94430beacc9a4d5e.cloudfront.net (CloudFront)'], 'X-Amz-Cf-Id': ['N2AvPGKjnYO1pmEAEiw9WUFoDpVLAJZJLEir4IVYPij1CkCSOncd6Q=='], 'X-Amzn-Trace-Id': ['Root=1-614cf31-70f86876714f678132cc87'], 'X-Forwarded-For': ['3.237.255.37, 130.176.133.131'], 'X-Forwarded-Port': ['443'], 'X-Forwarded-Proto': ['https']}, 'queryStringParameters': {'AAAA': 'BBBB'}, 'multiValueQueryStringParameters': {'AAAA': ['BBBB']}, 'pathParameters': None, 'stageVariables': None, 'requestContext': {'resourceId': '8978if', 'resourcePath': '/hello', 'httpMethod': 'GET', 'extendedRequestId': 'Glx_yHemoAMFZPg=', 'requestTime': '23/Sep/2021:22:18:25 +0000', 'path': '/Prod/hello/', 'accountId': '580299357056', 'protocol': 'HTTP/1.1', 'stage': 'Prod', 'domainPrefix': 'jiy58cz051', 'requestTimeEpoch': 1632435505617, 'requestId': 'a8ad1156-d894-46c2-8c6d-c54a058ed420', 'identity': {'cognitoIdentityPoolId': None, 'accountId': None, 'cognitoIdentityId': None, 'caller': None, 'sourceIp': '3.237.255.37', 'principalOrgId': None, 'accessKey': None, 'cognitoAuthenticationType': None, 'cognitoAuthenticationProvider': None, 'userArn': None, 'userAgent': 'curl/7.58.0', 'user': None}, 'domainName': 'jiy58cz051.execute-api.us-east-1.amazonaws.com', 'apiId': 'jiy58cz051'}, 'body': None, 'isBase64Encoded': False}
```

“Event” Object

Python Dictionary

...

```
'queryStringParameters': {'AAAA': 'BBBB'},
```

...

aaaa

“Event” Object

Python Dictionary

...

```
'queryStringParameters': {'AAAA': 'BBBB'},
```

...

```
event['queryStringParameters']
```

```
event['queryStringParameters']['AAAA']
```

aaaa

LAB: HTTP GET Parameters

Hands-On Lab:

- URL: <https://train.stage2sec.com/>





Debug & Test

S2

Local Debug

```
if __name__=="__main__":
    event = dict({'queryStringParameters': {'AAAAA': 'BBBB'}, ...})
    context = "
lambda_handler(event, context)
```



Locally Hosted API

```
sam local start-api
```

```
curl http://127.0.0.1:3000/hello?AAAA=BBBB
```

aaaa

Lambda Function Execution

```
sam local invoke "HelloWorldFunction" -e events/event.json
```

```
sam local generate-event apigateway aws-proxy --body "" --path  
"hello" --method GET > /home/ubuntu/environment/debug-app-  
001/events/api-event.json
```

LAB: Local Debug & Testing

Hands-On Lab:

- URL: <https://train.stage2sec.com/>





Open Port Check

S2

Open Port Check

```
sock = socket.socket(socket.AF_INET,  
socket.SOCK_STREAM)  
sock.settimeout(2) #2 Second Timeout  
result = sock.connect_ex((sTargetIp,int(sTcpPort)))  
if result == 0:  
    print("Port is open")  
    sReturn = sTargetIp + ":" + sTcpPort + "/TCP is open"  
else:  
    print("Port is not open")  
    sReturn = sTargetIp + ":" + sTcpPort + "/TCP is closed"  
...  
aaaa
```

LAB: Open Port Check

Hands-On Lab:

- URL: <https://train.stage2sec.com/>





Subdomain Discovery

S2

Subdomain Discovery

```
filepath = 'namelist.txt'
```

```
    with open(filepath) as f:
```

```
    ...
```

```
    addrs_List = [str(i[4][0]) for i in socket.getaddrinfo(sFqdn,  
65535)]
```

```
    ...
```

```
    return {
```

```
        "body": sReturn
```

```
}
```

Subdomain Discovery

template.yaml

Policies:

- S3FullAccessPolicy:

 BucketName: batmanisbestman001

app.py

```
import boto3  
  
client.put_object(Body=sFileContents, Bucket=sBucketName,  
Key=sFileName)
```

Subdomain Discovery

[+] START

[+] Subdomain discovered: cdn.lizardblue.com -> 52.217.194.113

[+] Subdomain discovered: cdn2.lizardblue.com -> 52.219.105.19

[+] Subdomain discovered: hash.lizardblue.com -> 52.85.61.12,
52.85.61.64, 52.85.61.65, 52.85.61.94

[+] Subdomain discovered: images.lizardblue.com ->
52.219.142.28

[+] Subdomain discovered: ixhash.lizardblue.com ->
3.226.63.115, 3.228.53.222, 3.230.230.89, 3.232.236.175,
34.193.24.255, 52.73.45.196, 54.172.93.56, 54.80.73.136

[+] END

LAB: Subdomain Discovery

Hands-On Lab:

- URL: <https://train.stage2sec.com/>

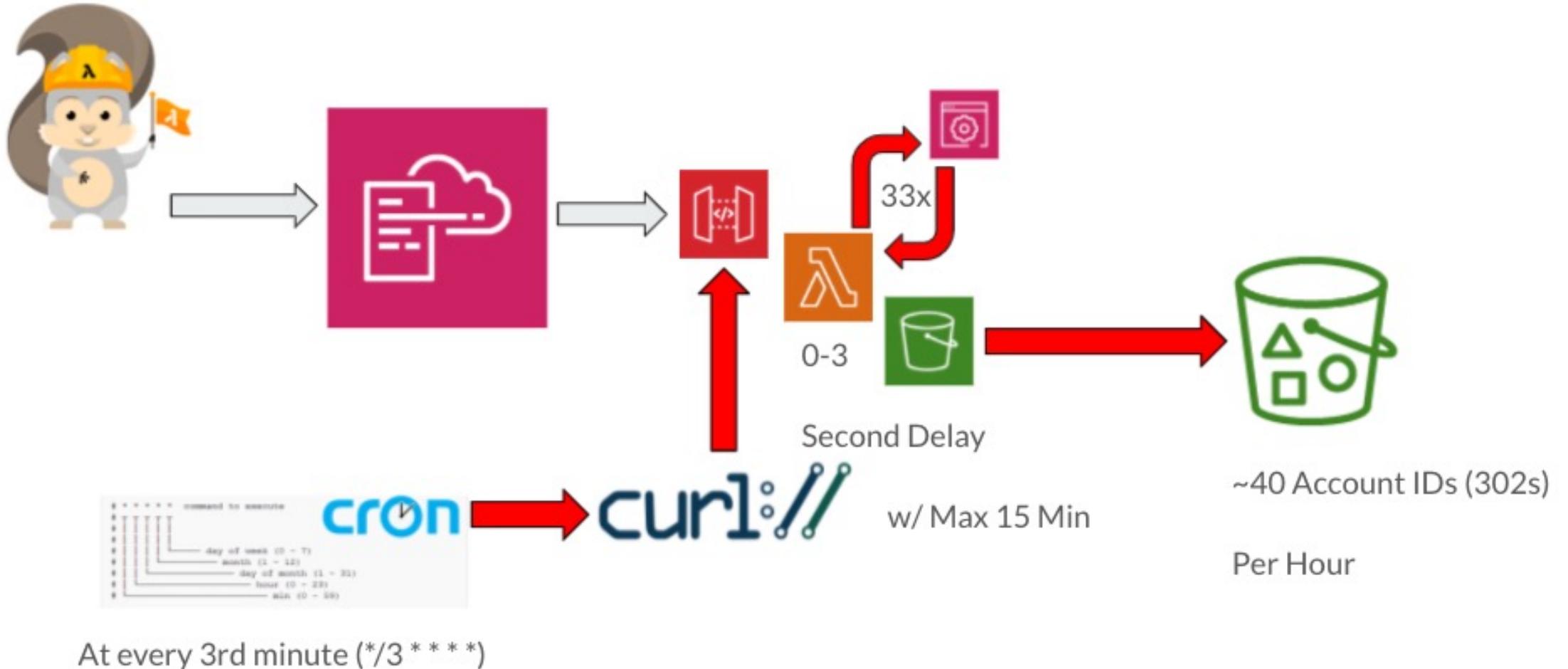




Account ID Discovery

S2

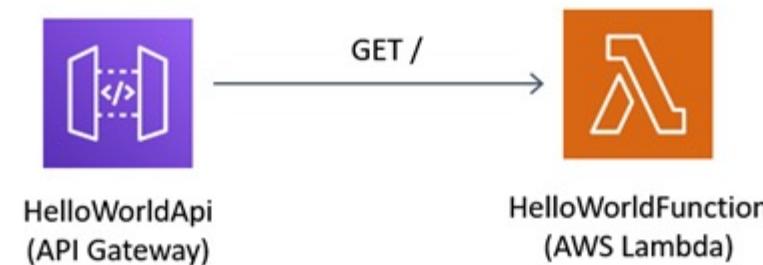
Finding Accounts



LAB: Account ID Discovery

Hands-On Lab:

- Code:
https://github.com/Stage2Sec/CaptureTheCloud/tree/master/account_discover_account_ids



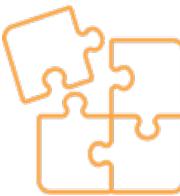
Conclusion

S2

S2 Secure Cloud MSS



Red Team-as-a-Service, MDR and Risk management in a single platform



Orchestrated platform of managed services that work together



Create consistent, automated processes and slash discovery & response times whether in cloud, container or on-premise



Focus on reducing IMMINENT RISK



Outcomes. Prioritized vulnerabilities, alerts and IMMINENT RISK



Track, measure and improve your security risk posture

PTaaS/RTaaS – Continuous Testing

Your security posture is currently critical

This security posture poses a serious risk to your organization's environment and should be resolved immediately.



CLOUD Critical: We found 5 findings on your CLOUD surface. Click here for more details about your findings. [VIEW](#)

EXTERNAL Critical: We found 11 findings on your EXTERNAL surface. Click here for more details about your findings. [VIEW](#)

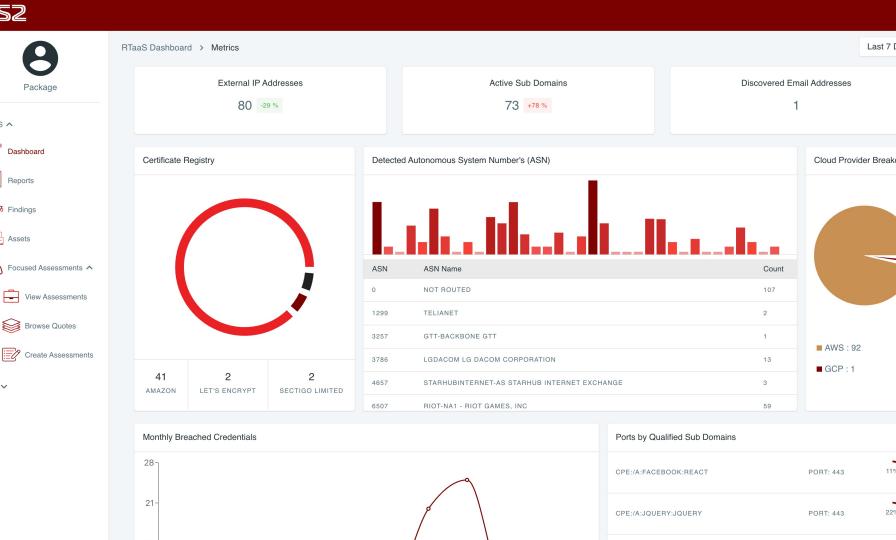
INTERNAL Critical: We found 3 findings on your INTERNAL surface. Click here for more details about your findings. [VIEW](#)

OSINT Okay: We found 3 findings on your OSINT surface. Click here for more details about your findings. [VIEW](#)

MITRE ATT&CK

RTaaS Dashboard > Metrics

Last 7 Days



ASN	ASN Name	Count
0	NOT Routed	107
1299	TELIANET	2
3257	GTT-BACKBONE GTT	1
3786	LGDA COM LG DACOM CORPORATION	13
4657	STARHUBINTERNET-AS STARHUB INTERNET EXCHANGE	3
6507	RIOT-NAT - RIOT GAMES, INC	59

Findings

<https://test.warrior.stage2sec.io/findings>

Category	Description	Date	Severity	Surface	Details
SSRF Exposed AWS Credentials	A malicious actor with network access to the vRealize Operations Manager API can perform a Server Side Request Forgery attack to steal administrative...	2021-07-19	Medium	EXTERNAL	attack.T1552
Command Execution Backdoor in Web Admin Console	Web Admin allows a user with a specific role and email address to execute arbitrary code. This may allow an attacker unfettered access to the underlying...	2021-07-19	High	EXTERNAL	
Exposed ElasticSearch Instance (search.lizardblue.org)	Mage discovered that the ElasticSearch instance at search.lizardblue.org is publicly accessible. This may allow an attacker to disclose sensitive info...	2021-07-19	Critical	EXTERNAL	attack.T1190
CreateStack / PassRole Privilege Escalation [redacted] (role)	The affected policy contains both CreateStack and PassRole permissions. This may allow an attacker to create new CloudFormation stacks that create AWS...	2021-07-19	High	CLOUD	T1484
Linux LPE via Polkit (CVE-2021-35660)	A local privilege escalation attack was successful using an outdated polkit vulnerability	2021-07-19	High	INTERNAL	T1068
Unauthenticated Livestream Access	An unauthenticated actor can access and modify any device livestream.	2021-07-19	Critical	EXTERNAL	
Improper Access Control AWS IoT	An unauthenticated low privileged user can gain access to all devices.	2021-07-19	Critical	CLOUD	
UpdateAssumeRolePolicy Privilege Escalation [instance-staging-redacted]	The affected policy contains both UpdateAssumeRolePolicy and AssumeRole permissions. This may allow an attacker to update the assume role policy to an...	2021-07-19	High	CLOUD	T1484
VMWare vCenter Unauthenticated RCE (CVE-2021-22010)	A malicious actor with network access to the vRealize Operations Manager API can perform a Server Side Request Forgery attack to steal administrative...	2021-07-19	Critical	EXTERNAL	attack.T1190

Compliance Standards

Standard	Status
PCI	IN PROGRESS
HIPPA	IN PROGRESS

Pentest Options

Service	Start Date	Completion Date
Network Pen Test	08/16/2021	10/16/2021
Cloud Pen Test		

MDR

Thank You! Bryce@Stage2Sec.com



Trainings: Hands-On Cloud Red Teaming

Code: [Github.com/Stage2Sec/CaptureTheCloud](https://github.com/Stage2Sec/CaptureTheCloud)

Slides: [SpeakerDeck.com/TweekFawkes](https://speakerdeck.com/TweekFawkes)

Bryce Kunz

@TweekFawkes





Thank You

Bryce@Stage2Sec.com