Steps to fingerprinting the cloud attack surface

Alejandro Ortuño

Typeform Security Team
@aomanzanera

MEET THE TEAM

DISCLAIMERS

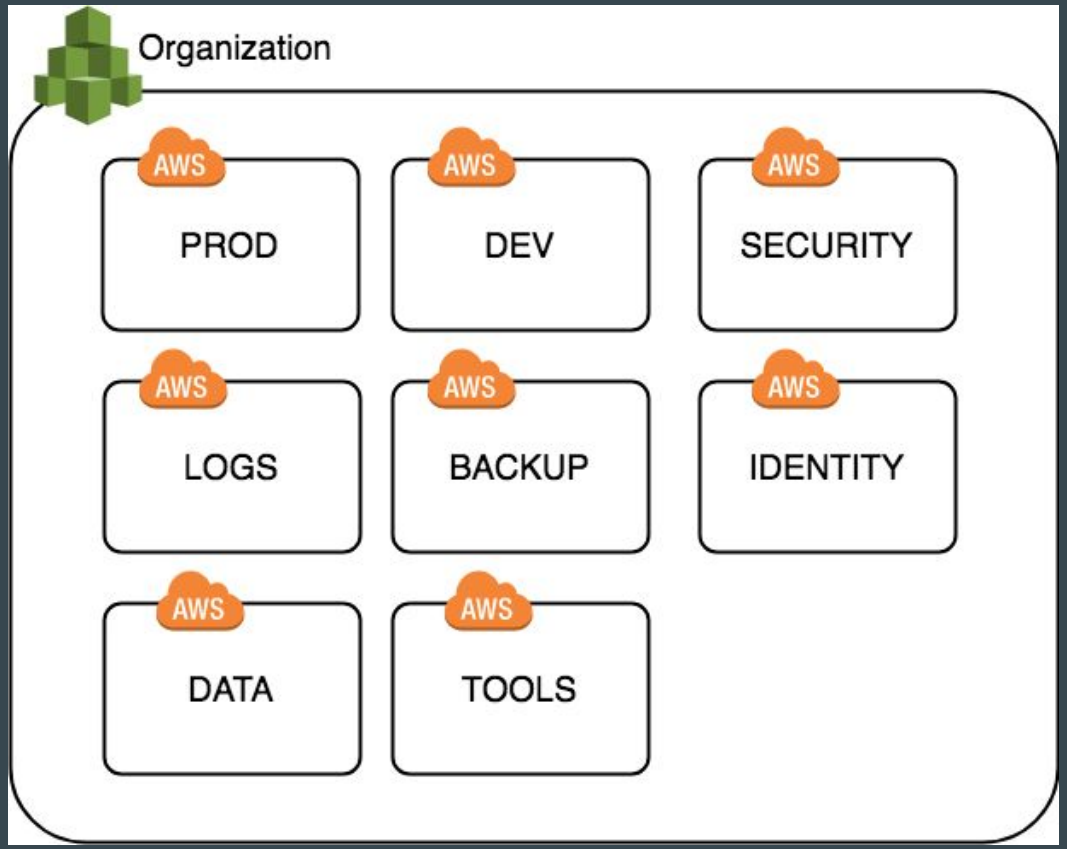
“You might want to request AWS pen test approval before taking any actions explained on presentation.”

COOL KIT

bugcrowd

AWS SECURITY

GOOD PRACTICES



NEWS

Tesla Has Its C
Mining

February 22, 2

Hacker
Jenkins

By Catalin Ci

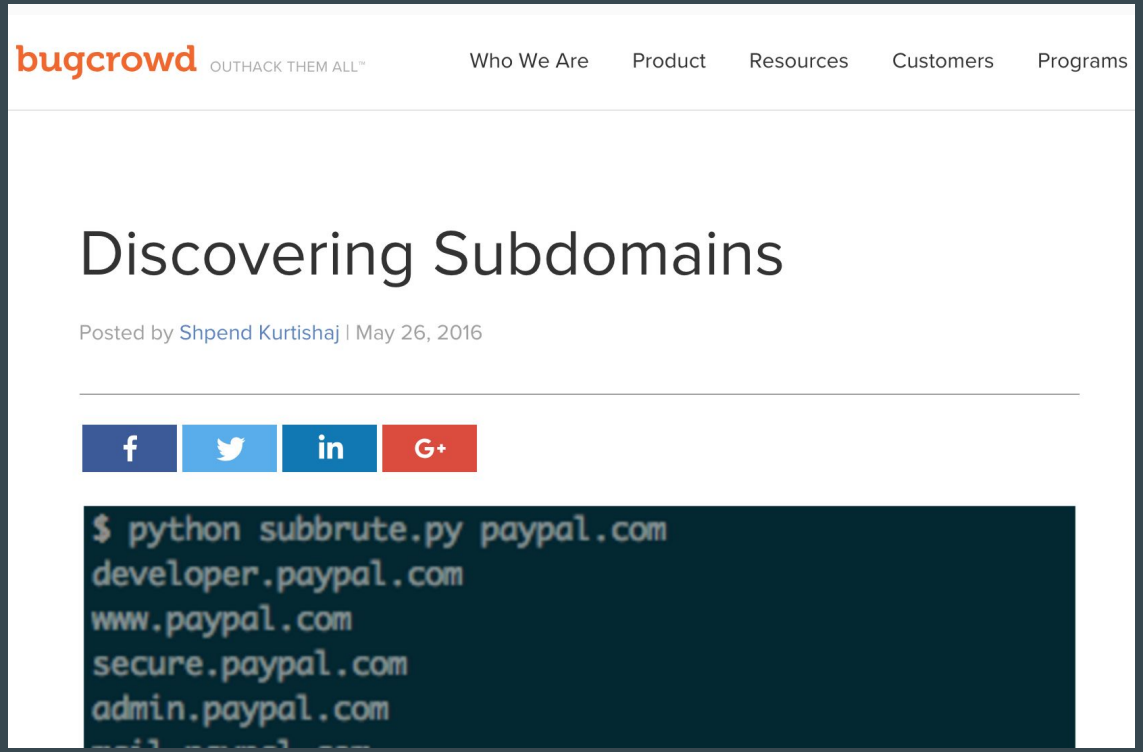
Home > News > Security > Exposed Docker APIs Continue to Be Used for Cryptojacking

Exposed Docker APIs Continue to Be Used for Cryptojacking

By Lawrence Abrams

October 27, 2018 09:11 AM 0

BAD ACTORS ARE QUICK



https://www.bugcrowd.com/discovering-subdomains/

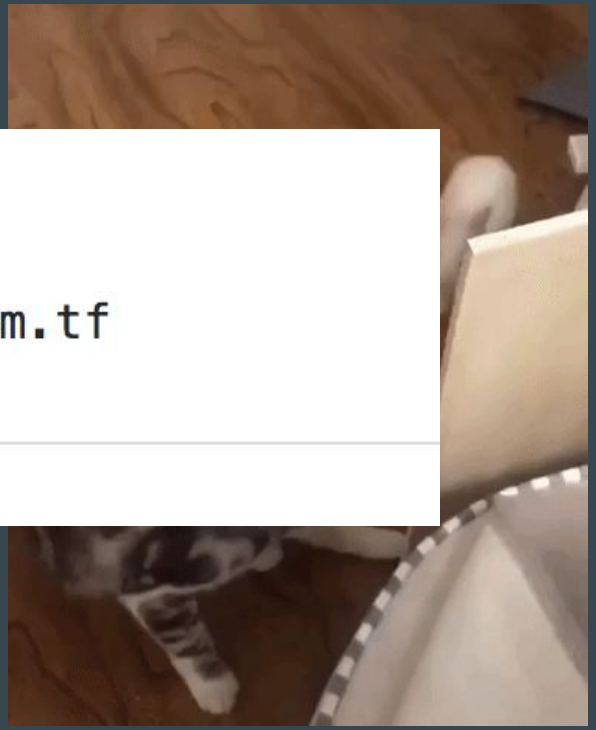
GOAL

“Detect if a service becomes public either intentionally or by mistake before bad actors do”

PREWORK

INTERIM SOLUTION

```
70  [redacted]typeform.com
71  [redacted].typeform.com
72  [redacted]-staging.typeform.tf
73  a[redacted].typeform.tf
```



PRINCIPLES

- Minimum viable product - MVP
- No servers maintenance
- Ideally no devops / security expertise
- Easy monitoring and alerting
- Low cost $$$

CHALLENGES

- No easy way to export / run nmap as lambda
- AWS Lambda limits
- Run lambda from a lambda
- Scan hundreds of domains - orchestrator

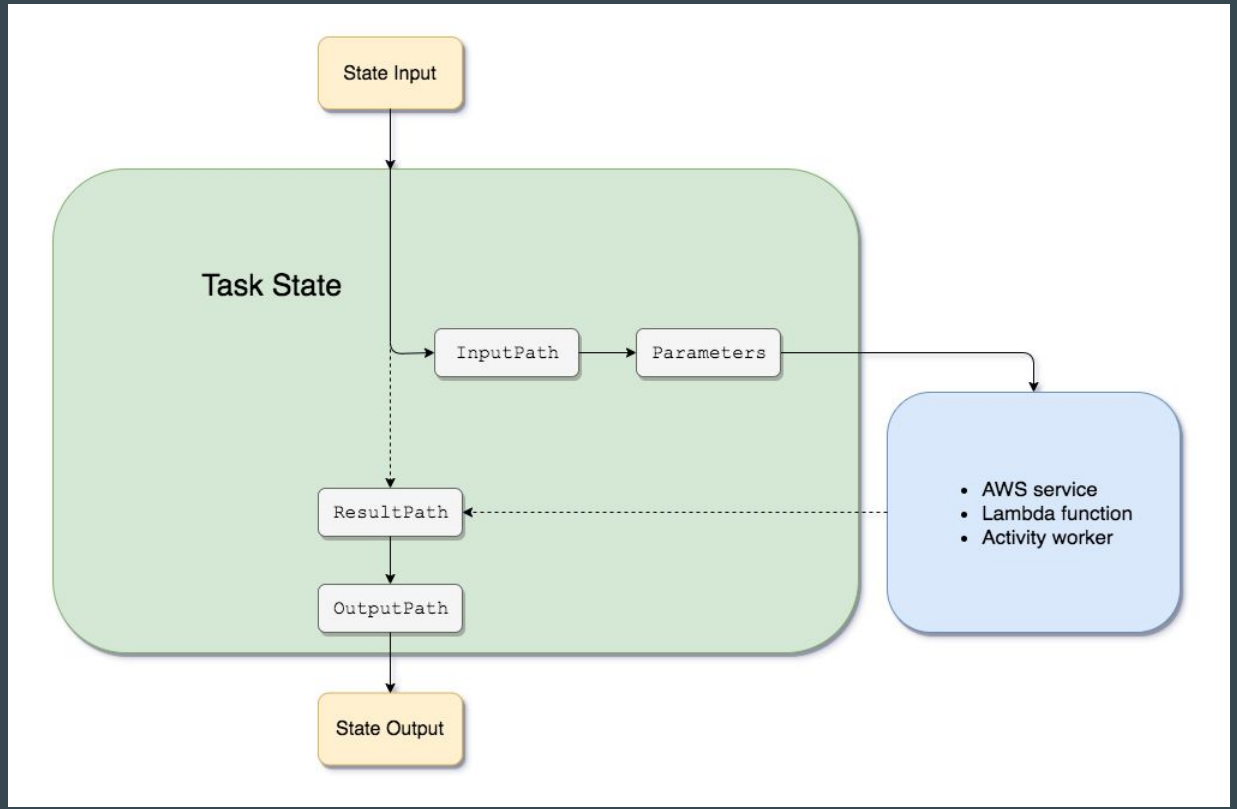
STEP FUNCTIONS TO THE RESCUE

"AWS Step Functions coordinate multiple AWS services into serverless workflows so you can build / update apps quickly"

DA MACHINE

- Finite state machine - Start and End
- States
  - Task
  - Choice
  - Fail / Succeed
  - Pass
  - Wait
  - Parallel
- Cost: per state transition (4000 free/month then $0.025 per 1,000 transitions)

PASSING STATE AROUND

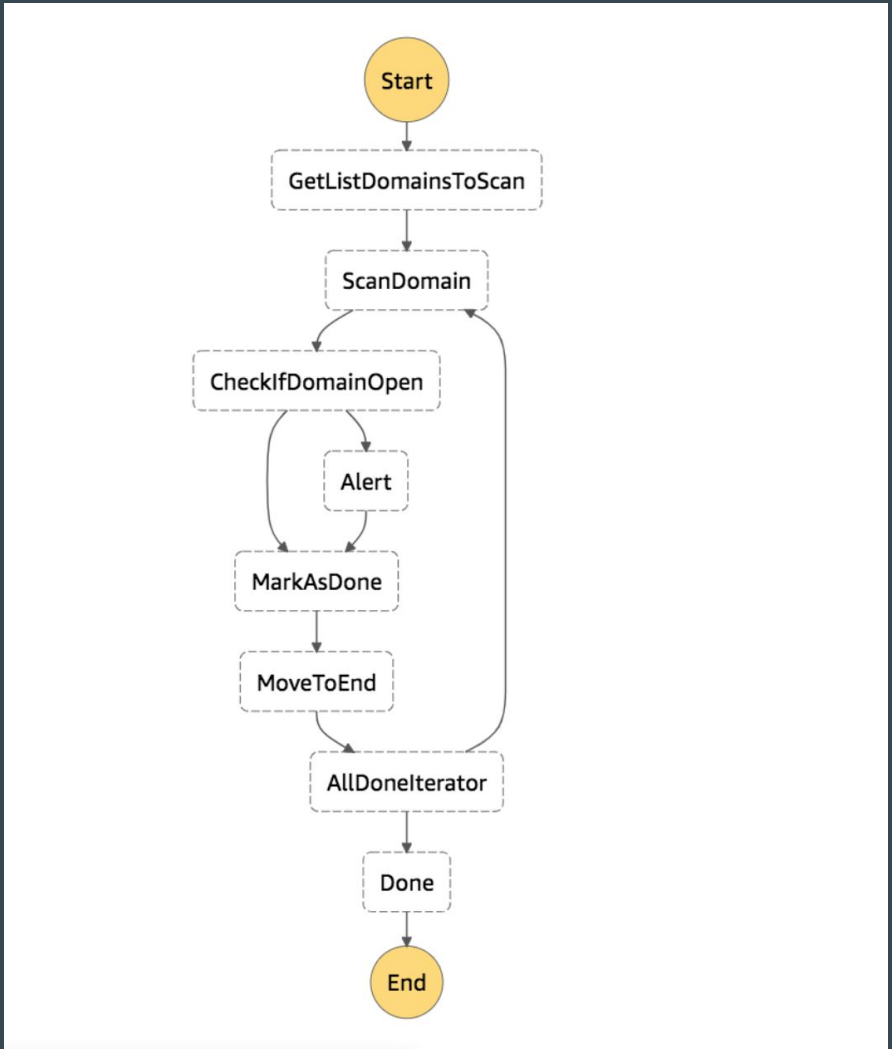


STEPS JSON

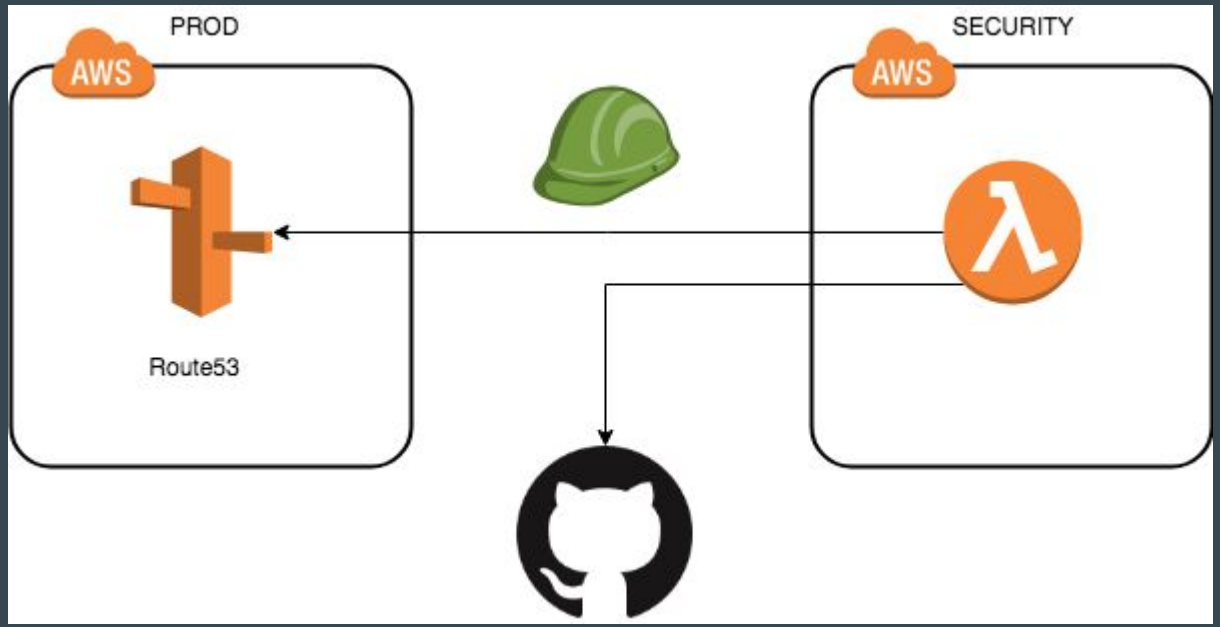
```
{
        "Comment": "Open domain scanner",
        "StartAt": "GetListDomainsToScan",
        "States": {

          "GetListDomainsToScan": {
            "Type": "Task",
            "Comment": "Lambda to get the list of domains",
            "ResultPath": "$.domains",
            "Resource": "arn:aws:lambda:[redacted]:function:steps_get_list_of_domains",
            "Next": "ScanDomain"
          },
          "AllDoneIterator": {
            "Type": "Choice",
            "Choices": [
              {
                "Variable": "$.domains[0].done",
                "BooleanEquals": true,
                "Next": "Done"
              }
```

MAGIC


Start
GetListDomainsToScan
ScanDomain
CheckIfDomainOpen
Alert
MarkAsDone
MoveToEnd
AllDoneIterator
Done
End

GET LIST DOMAINS TO SCAN

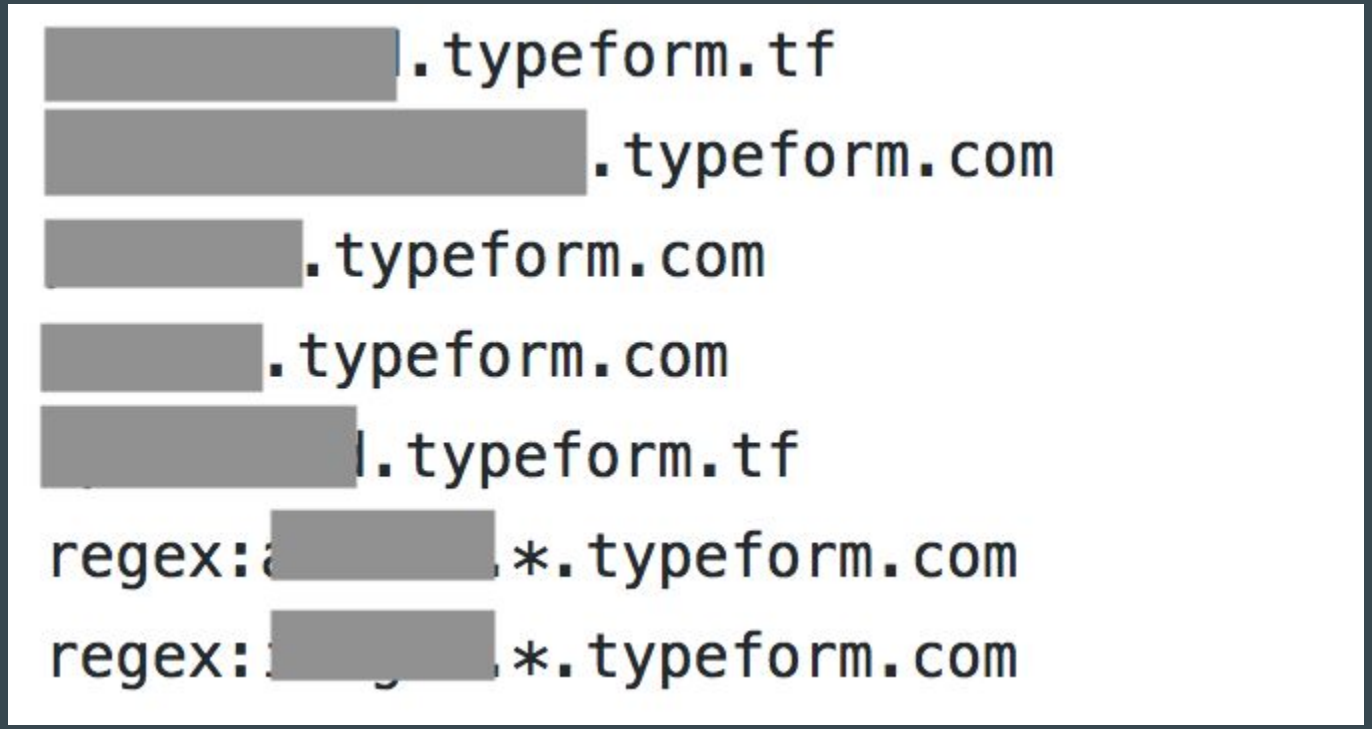


CNAME

A

AAAA

GET LIST DOMAINS TO SCAN



OUTPUT - STATE

```
domain_records.append({
    "domain": domain,
    "done": "false",
    "open": "false"
})
```

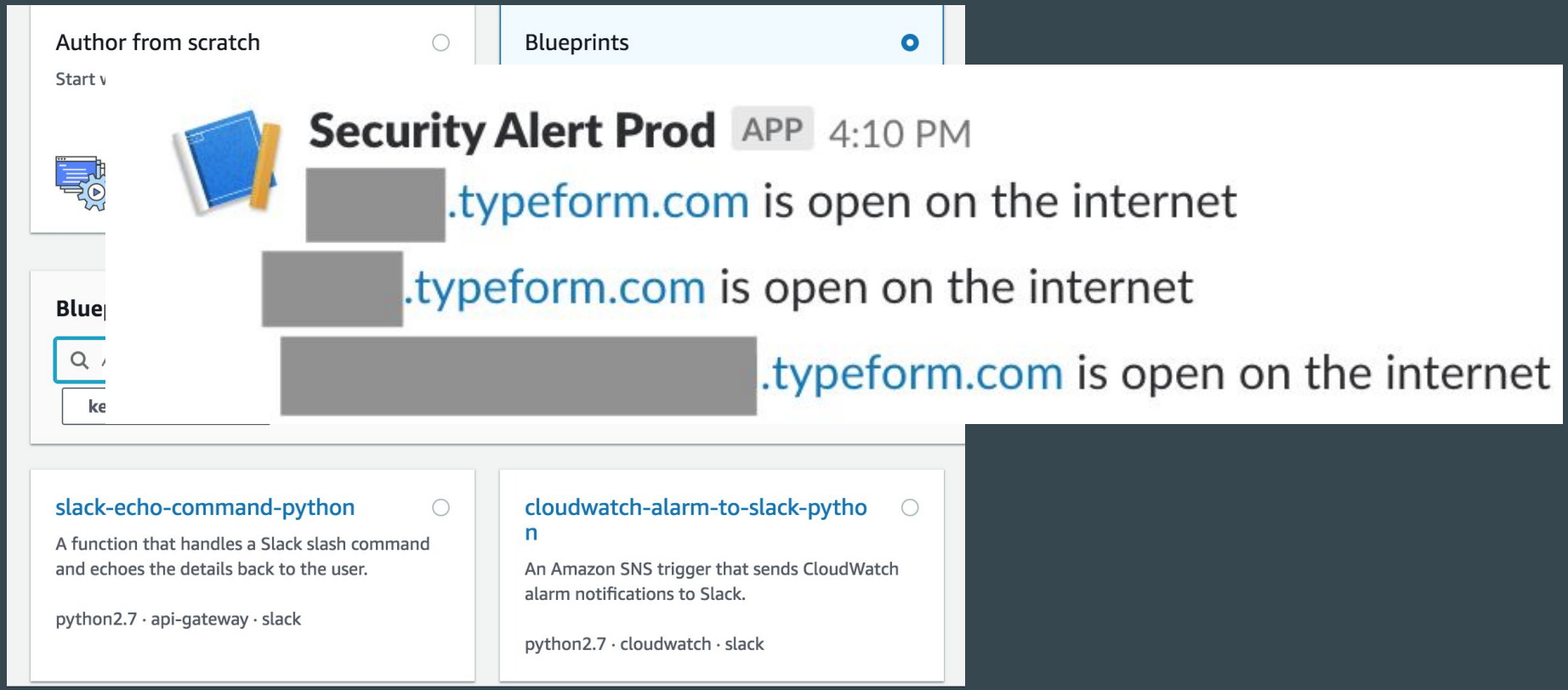
SCAN DOMAIN - **MVP**

```
def open_port(domain, port):
    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        s.connect((domain, port))
        s.sendall(" ")
        s.shutdown(socket.SHUT_WR)
        s.close()
        return True
    except Exception:
        logger.info("Socket connection raised an Exception")
        return False


def lambda_handler(event, context):
    domain = str(event['domain'])
    logger.info("Scanning domain: " + domain)

    if open_port(domain, 443) or open_port(domain, 80) or \
            open_port(domain, 8080) or open_port(domain, 22):
        return True
    return False
```

ALERT


Author from scratch
Blueprints
Security Alert Prod APP 4:10 PM
[redacted].typeform.com is open on the internet
[redacted].typeform.com is open on the internet
[redacted].typeform.com is open on the internet
slack-echo-command-python
A function that handles a Slack slash command and echoes the details back to the user.
python2.7 · api-gateway · slack
cloudwatch-alarm-to-slack-python
An Amazon SNS trigger that sends CloudWatch alarm notifications to Slack.
python2.7 · cloudwatch · slack

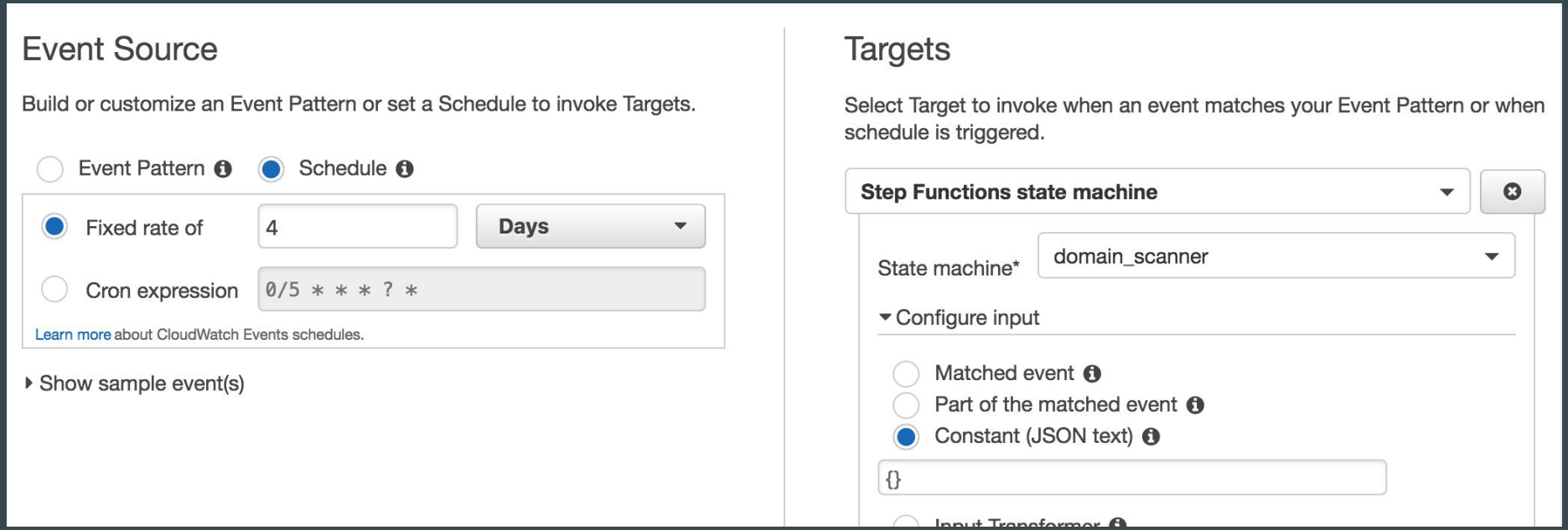
THE REST

```
"CheckIfDomainOpen": {
  "Type": "Choice",
  "Choices": [
    {
      "Variable": "$.domains[0].open",
      "BooleanEquals": true,
      "Next": "Alert"
    }
  ],
  "Default": "MarkAsDone"
},
```

```
"MarkAsDone": {
  "Type": "Pass",
  "InputPath": "$.domains[0]",
  "ResultPath": "$.domains[0].done",
  "Result": true,
  "Next": "MoveToEnd"
},
```

```
"Done": {
  "Type": "Pass",
  "End": true
}
```

TRIGGER - CLOUDWATCH EVENT



COST OF THE SOLUTION

Service	Oct 1, 2018	Nov 1, 2018	Dec 1, 2018	Service Total
Total cost ($)	0.02	0.02	0.15	0.24
Lambda ($)	0.02	0.02	0.04	0.13
Step Functions ($)			0.12	0.12

IMPROVEMENTS

- If domain is no longer open, modify file on Github
- Use parallel task
- Cross check with what Terraform says


SENORGIF.COM
WE ARE HIRING

@aomanzanera

alejandro.ortuno@typeform.com