

Coolware – Cloud Security Tool

Evan Duffield, Dylan Morris, Bennett Wiley

A dark blue diagonal gradient bar that starts from the bottom left corner and extends towards the top right corner, covering the lower half of the slide.

Our Product



Cloud Security Tool

- Cloud services have low barrier of entry
- Looks for vulnerable configurations
- Monitor resources
- Can recommend advice to users how to secure their cloud infrastructure

Target Demographic

- Cloud customers who are unfamiliar with cloud security protocols.
- Inexperienced developers that have the risk of financial and data loss from publicly hosting content.
- Cloud computing has become an accessible and convenient alternative to self-hosting servers in recent years



Cloud Vendors

Our Cloud Security Tool Supports The Following Cloud Vendors

- Amazon's AWS

- Microsoft Azure

- Google Cloud



Why People Need Our Product

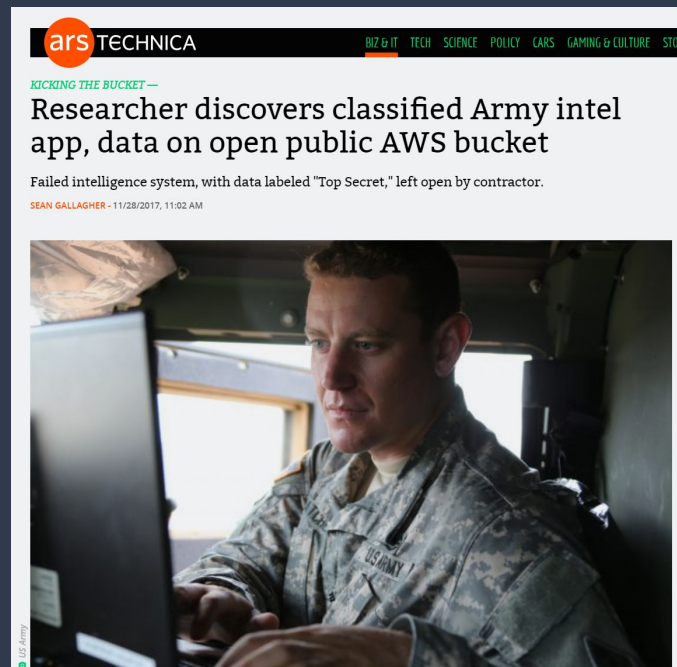
Developers

- Cloud Hosting has become a fast and cost-effective way for new web infrastructure to be brought online.
- With cloud providers making it easier for anyone to launch web resources, the number of inexperienced users with insecure setups grows.
- Individuals can be confused by the “burden of security” i.e. what are their responsibilities vs the provider for securing resources.

IT

- Cloud Hosting is more complicated than traditional networking, making experienced professionals novices in some domains.
- Permissive roles being given to too many people can leave holes in an infrastructure's security - too many cooks.

Security is Hard





filetype:pdf "Not For Public Release" site:*.s3.amazonaws.com



All Images News Videos Forums More

Tools

About 931 results (0.33 seconds)



Amazon Web Services

<https://imlive.s3.amazonaws.com> PDF

NOT FOR PUBLIC RELEASE SAFEGUARD IAW FAR ...

1.1 Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials,
90 pages



Amazon Web Services

<https://imlive.s3.amazonaws.com> PDF

452 Security Forces Squadron

This information is for contracted businesses and **not for public release**. 3. For any other questions, you may contact the 452 SFS Police Services Program ...
17 pages



Amazon Web Services

<https://imlive.s3.amazonaws.com> Attachment_2... PDF

PERFORMANCE WORK STATEMENT (PWS) For Cyber ...

PROCUREMENT SENSITIVE INFORMATION – **NOT FOR PUBLIC RELEASE**. SAFEGUARD IAW FAR 3.104 (PROCUREMENT INTEGRITY ACT). PROCUREMENT SENSITIVE INFORMATION – **NOT...**

A-52 Cyberspace Operations Analyst

Experience: A minimum of five (5) years' prior military experience and/or significant civilian occupational experience in Cyberspace Operations (Defensive Cyberspace Operations, Offensive Cyberspace Operations, or Cyberspace Situational Awareness).

Education: Undergraduate degree in Computer Science or Computer Engineering from an accredited institution. Coursework shall include computer programming (e.g., Fundamentals of Programming, Computer Forensics) and coding (e.g., C, C++, Python, Java). Equivalent job experience may be considered.

Proficiencies: Knowledge of Cyberspace Warfare including, but not exclusively, computer programming, software design, cyber security (defensive or offensive), and cyber forensics.

Qualifications: Desired Certifications: CISSP, Global Industrial Cyber Security Professional (GICSP), GIAC Enterprise Defender (GCED), GIAC Information Security Professional (GISP).

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-53 Electromagnetic Spectrum Operations Analyst

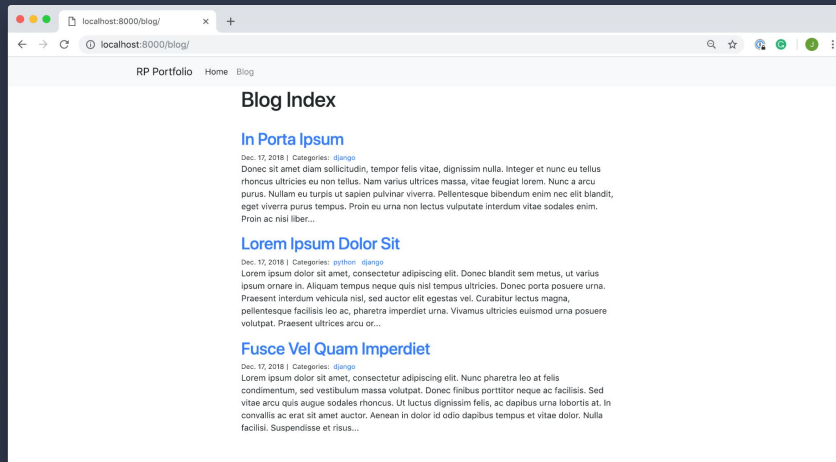
Experience: A minimum of five (5) years' experience in operational EW, Spectrum Management Operations, and Signals Intelligence planning,

87

PROCUREMENT SENSITIVE INFORMATION – **NOT FOR PUBLIC RELEASE SAFEGUARD IAW FAR 3.104 (PROCUREMENT INTEGRITY ACT)**

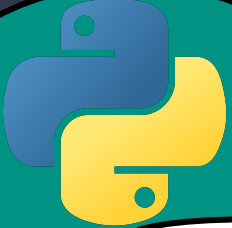
Case Study: Jared's Django Blog

- Jared is an undergraduate who thinks they have a hit new app that they developed in a MCB course.
- They quickly set up their blog in AWS, written in the Django framework, doing the bare minimum to make sure that their domain name connects to their server.
- However, the default settings aren't secure, leaving Jared's blog exposed to attackers who could expose confidential data and drive up his provider costs.



DEMO

Technologies used



Python

- Backend logic
- Local web server with Flask
- Communicates with cloud API.



JSON

- Data storage for information received from cloud provider APIs
- Data persistence for next launch.



HTML

- Frontend presentation for any generated reports
- Javascript for basic logic

Testing with Terraform

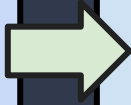


- One of our major hurdles during this project was setting up realistic development environments in the cloud, which is both costly and time consuming when using the provider UIs.
- Terraform is a configuration program that allows you to setup and destroy planned cloud environments at will.
- Terraform helped minimize our costs, and protected our cloud environments by only hosting vulnerable resources for a brief time.

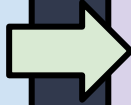
```
resource "aws_instance" "blog_instance" {  
  ami           = "ami-0b0ea68c435eb488d"  
  instance_type = "t2.micro"  
  security_groups = [aws_security_group.blog_sg.name]  
  
  user_data = <<-EOF  
  #!/bin/bash  
  sudo apt update  
  sudo apt install python3-pip python3-dev libpq-dev postgresql postgresql-contrib nginx curl -y  
  sudo pip3 install virtualenv  
  mkdir ~/myproject  
  cd ~/myproject  
  virtualenv myprojectenv  
  source myprojectenv/bin/activate  
  pip install django gunicorn psycopg2  
  django-admin startproject exampleblog .  
  # Additional setup like configuring settings.py for production can be added here  
  EOF  
  
  tags = {  
    Name = "ExampleBlogInstance"  
  }  
}
```

Business Plan

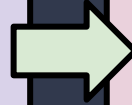
Market Analysis



Target Market



Competition



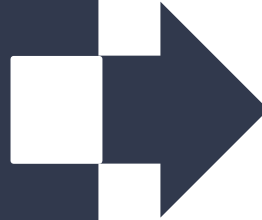
Strategy

Market Analysis



- Cloud security market is “valued at \$35.8 billion in 2022 and is projected to reach \$125.8 billion by 2032” - *Allied Market Research*
- With this information it shows that our cloud security tool will be entering a very competitive market.

Target Market



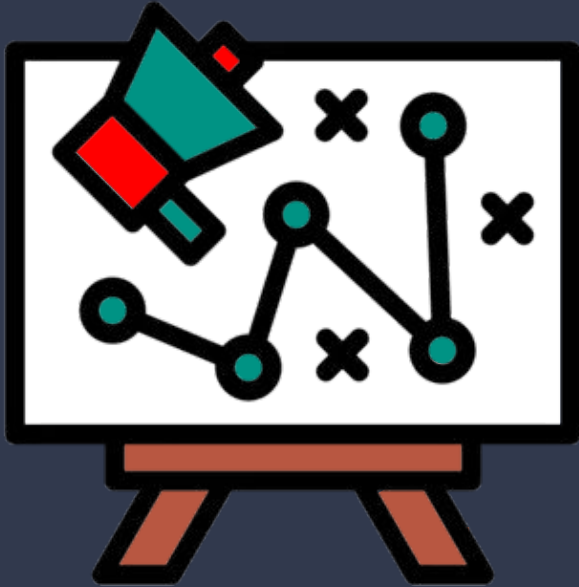
- Our product will focus on helping consumers who are not experienced using cloud infrastructure and do not understand the importance of secure configurations.
- Our overall goal is to create a cloud security tool to help guide users and teach them about how to make their cloud environment more secure.

Competition



- Competitors are closed source so you don't know how it works.
- It's not locally running, which means you are giving other machines access to your resources.
- Competitors only have paid options and don't offer any free tiers for their users.

Strategy



- Our product will be entering a matured industry with no signs of slowing down. The best way stay ahead of our competitors is to offer what they don't have.
- We will be implementing the focus strategy by marketing our product to the inexperienced cloud users. Will make it clear that our cloud security tool is...
 - ✓ Open source so users know how it works
 - ✓ Locally run so no outside devices can access your resources
 - ✓ Free for individual use until more than 50 services.
- We're expecting junior IT/development staff to use this tool independently, then ask for access in a corporate environment once they're in the professional sector.

Pricing Options

FREE for individual use until you use more than 50 services (object storage services, compute services, database services, and container services) you will then need to choose a payment option of...



\$4.99 / Month



\$49.99 / Year

Thank You For Your Time

Let Us Know If You Have Any Questions