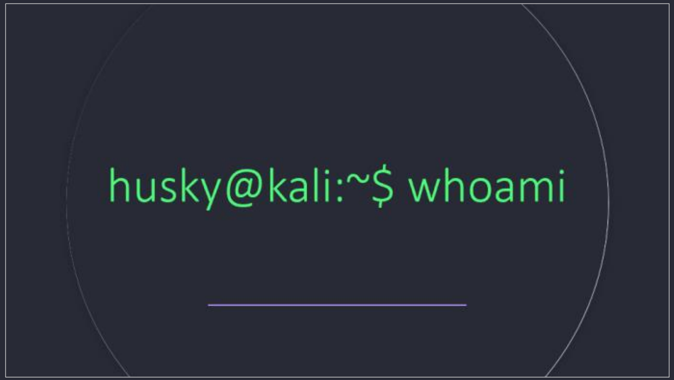
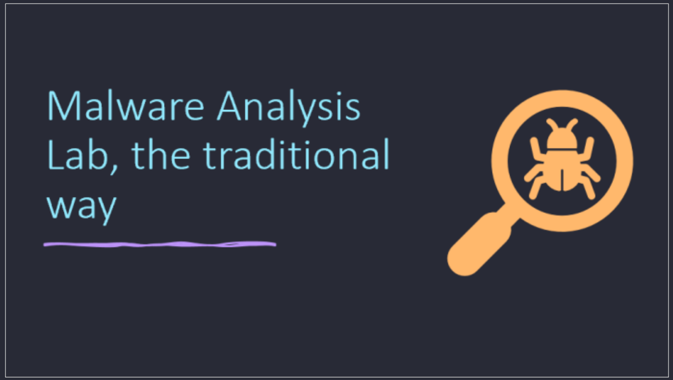
Cloudy with a Chance of Malware

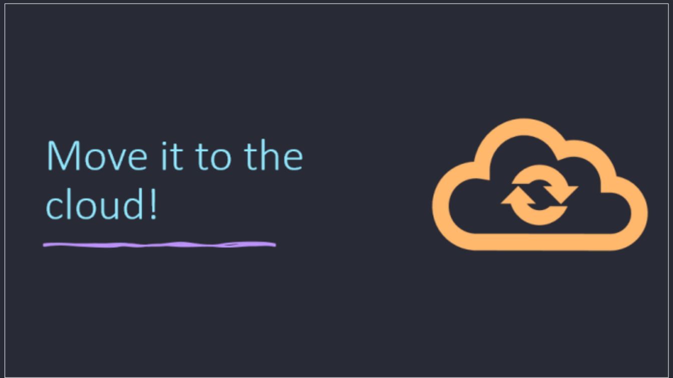
Overview



husky@kali:~$ whoami



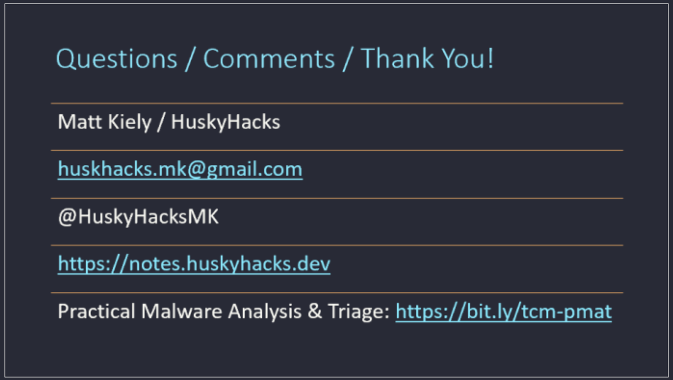
Malware Analysis Lab, the traditional way



Move it to the cloud!

Considerations, Security, & Guidelines

Tech Demo



Questions / Comments / Thank You!

Matt Kiely / HuskyHacks

huskhacks.mk@gmail.com

@HuskyHacksMK

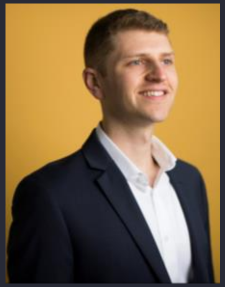
https://notes.huskyhacks.dev

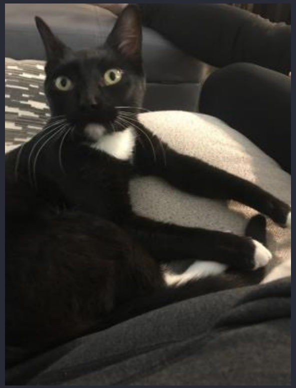
Practical Malware Analysis & Triage: https://bit.ly/tcm-pmat

husky@kali:~$ whoami

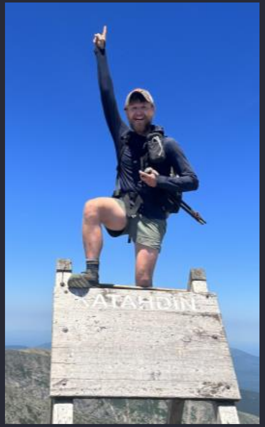
husky@kali:~$ whoami

- Matt Kiely
- Guy trying to learn stuff everyday
- Cat dad (Cosmo & Kiki)
- Appalachian Trail Thru Hiker (class of '23)
- Red teamer, malware reverse engineer
- USMC Vet
- MIT Lincoln Lab
- Content Author & Instructor
  - TCM Security
  - Co-Founder: The Taggart Institute
- Twitter: @HuskyHacksMK
- Blog/Notes: https://notes.huskyhacks.dev





Cosmo!

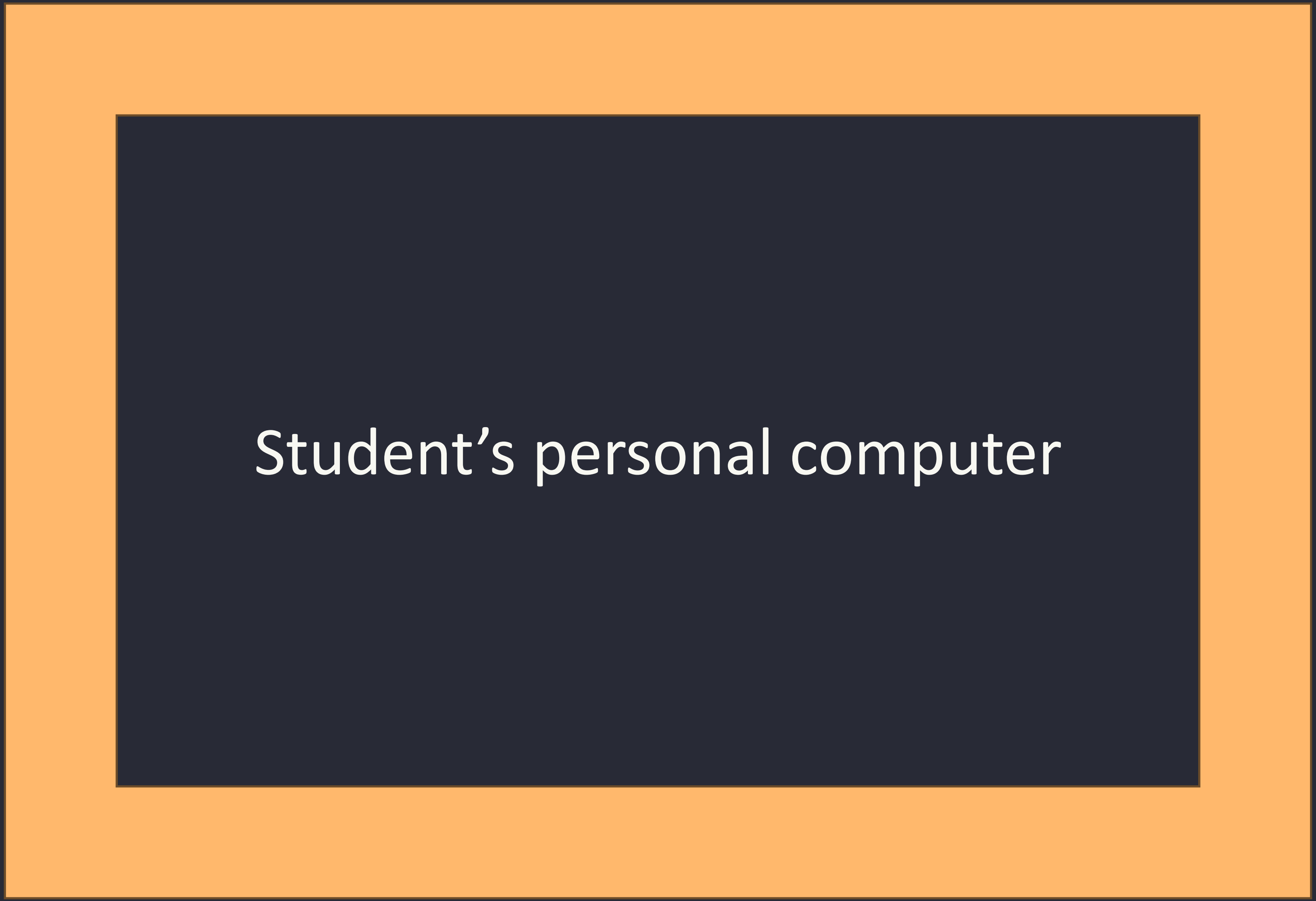


Malware Analysis Lab, the traditional way

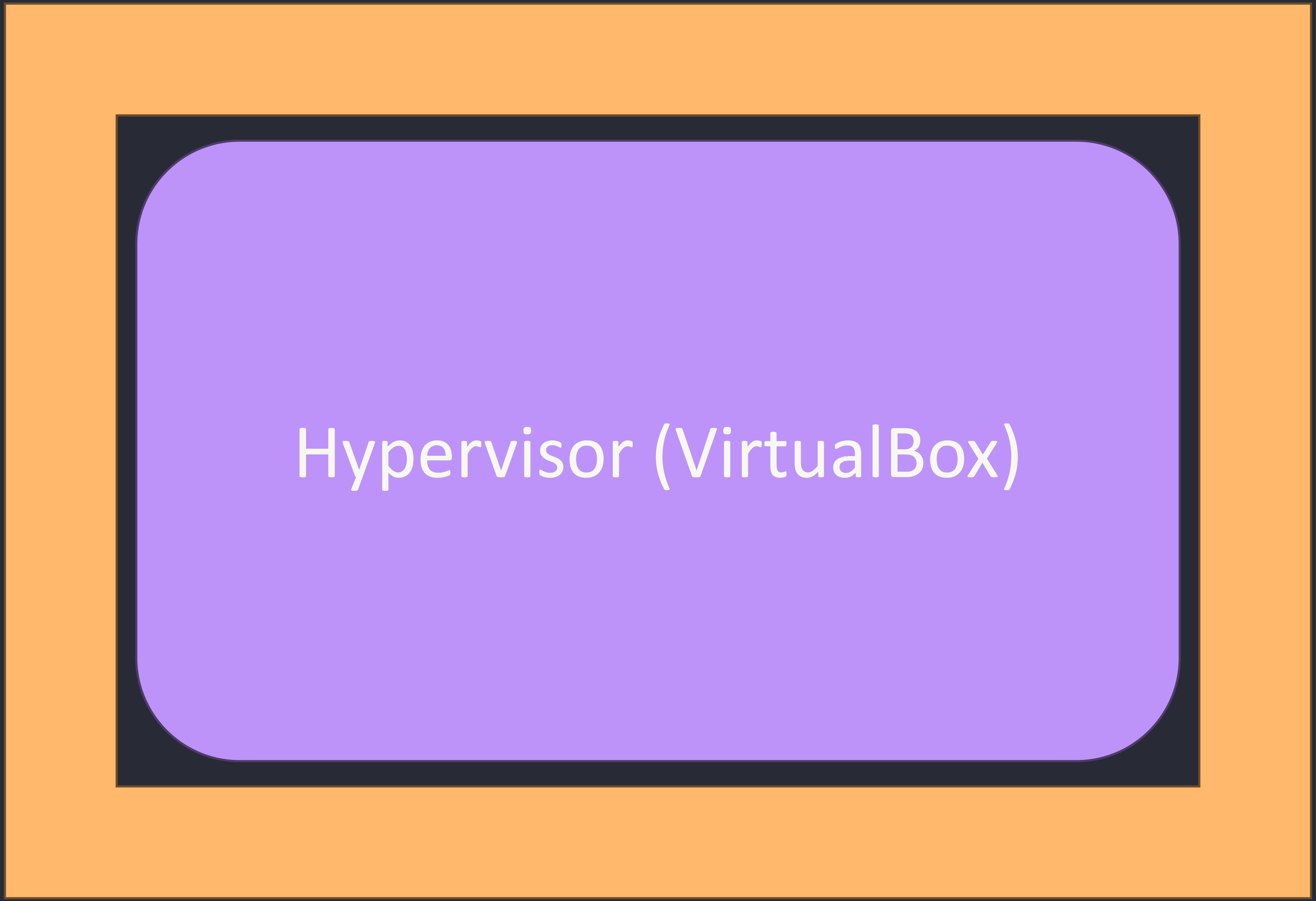
- Around 38k enrollments across the globe (TCM Security Academy)
- Teaches the art and science of malware analysis in an approachable way
- Centers on practical labs, training, and challenges
- This course requires you to roll up your sleeves and dissect malware in a lab
- Gives the student the tools of the industry malware analyst (set them up for success!)

PRACTICAL MALWARE ANALYSIS & TRIAGE

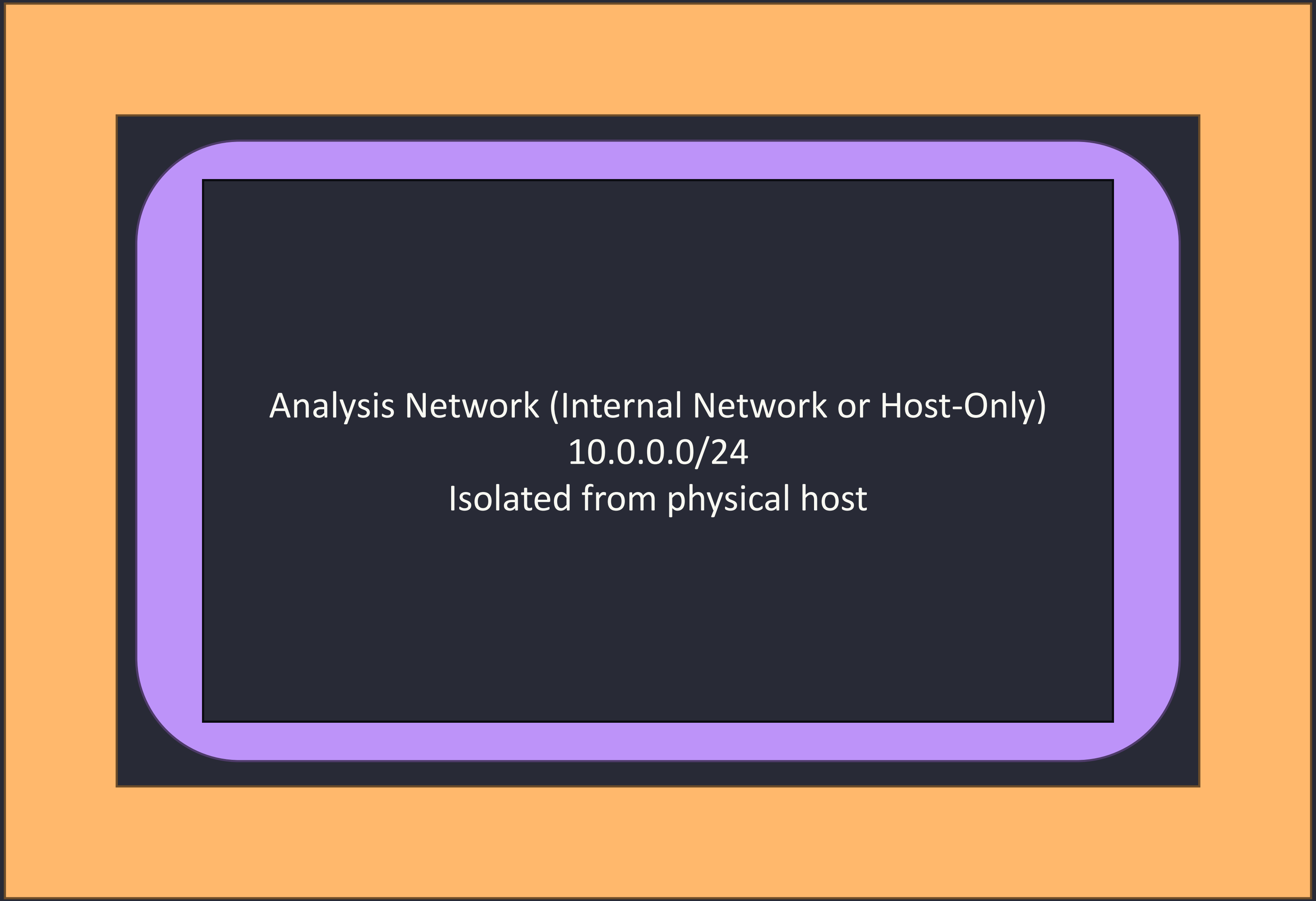
TCM SECURITY



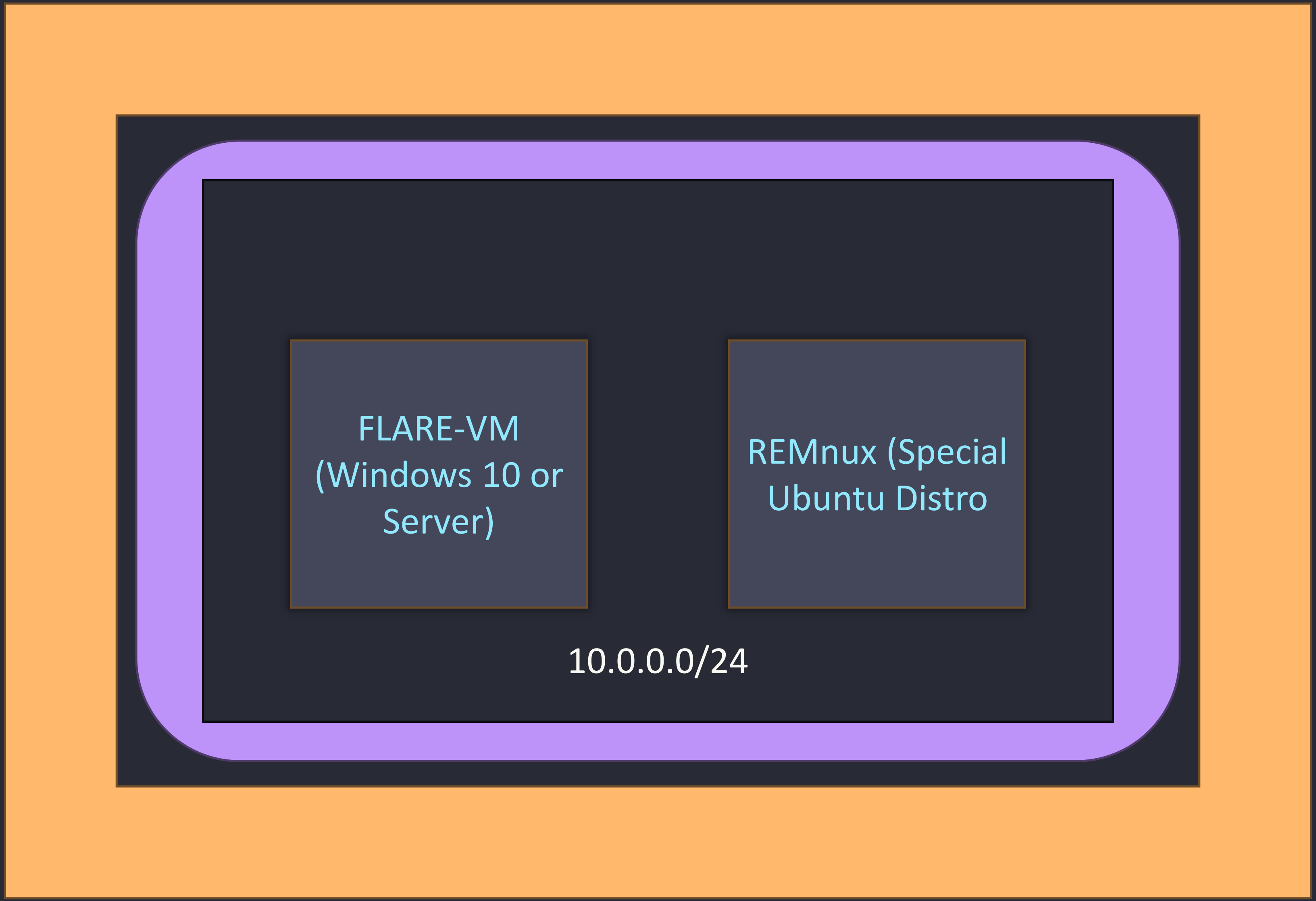
Student’s personal computer



Hypervisor (VirtualBox)



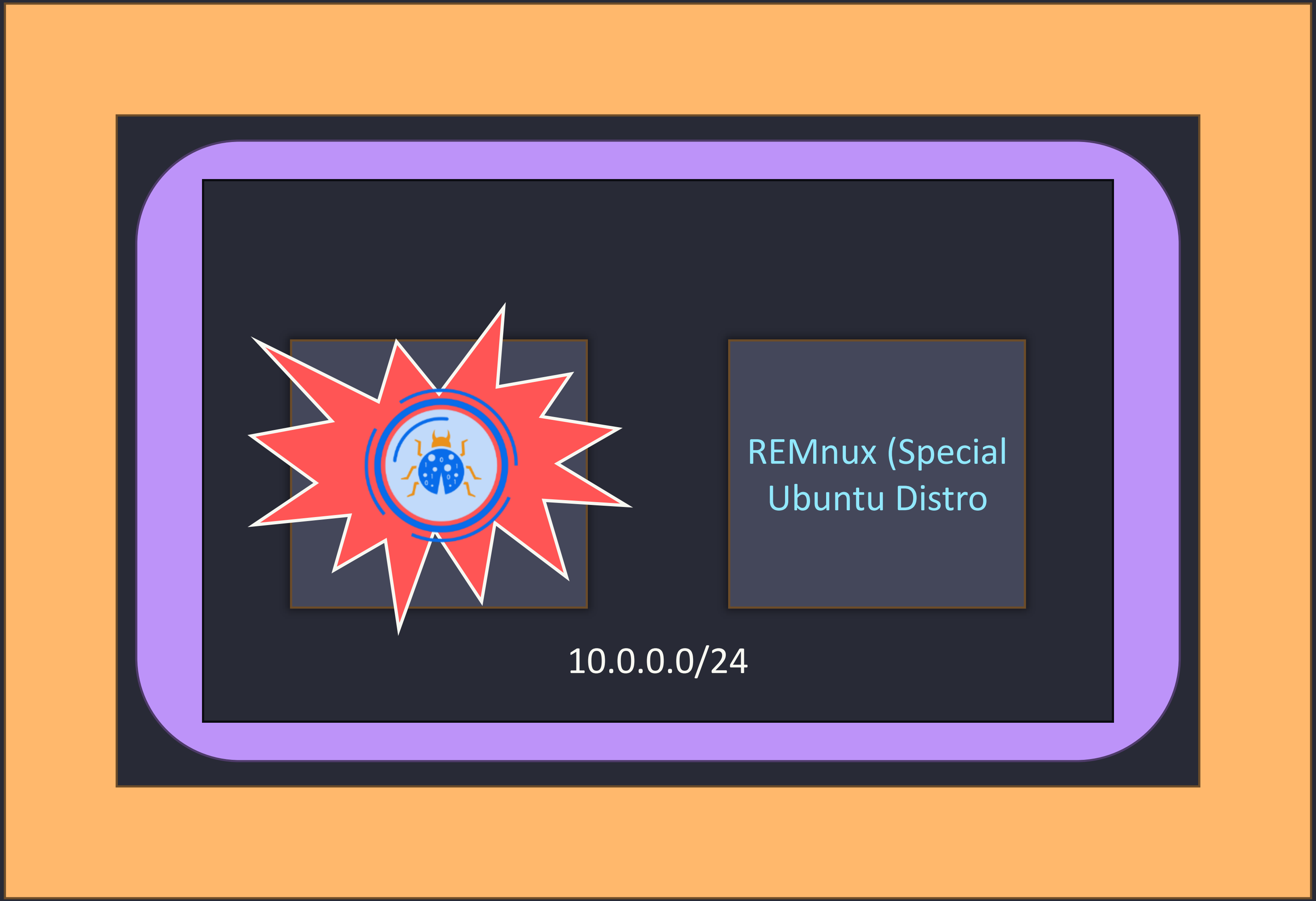
Analysis Network (Internal Network or Host-Only)
10.0.0.0/24
Isolated from physical host



FLARE-VM (Windows 10 or Server)

REMnux (Special Ubuntu Distro

10.0.0.0/24



REMnux (Special Ubuntu Distro

10.0.0.0/24

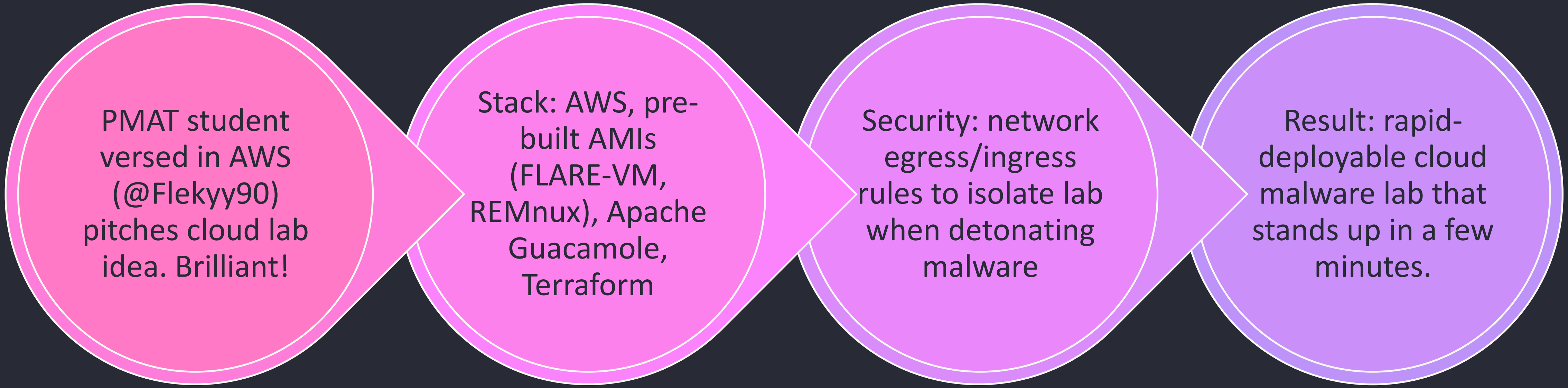
Malware Analysis lab, the traditional way

- Local virtual machines (VMWare, VirtualBox, etc)
- Doesn’t scale well
- Differences in student setups means harder to troubleshoot
- Takes time to set up (FLARE-VM installation, primarily)

Student (Analyst) Perspective - Common Challenges

- Inability to run the specified hypervisor (Mac m1/m2 chips)
- Variability in personal computer specs, VM performance
- **Risk!** “Is this really safe to do on my personal computer?”
- Can we benefit from moving to the cloud? **Yes.**

Move it to the cloud!



PMAT student versed in AWS (@Flekyy90) pitches cloud lab idea. Brilliant!

Stack: AWS, pre-built AMIs (FLARE-VM, REMnux), Apache Guacamole, Terraform

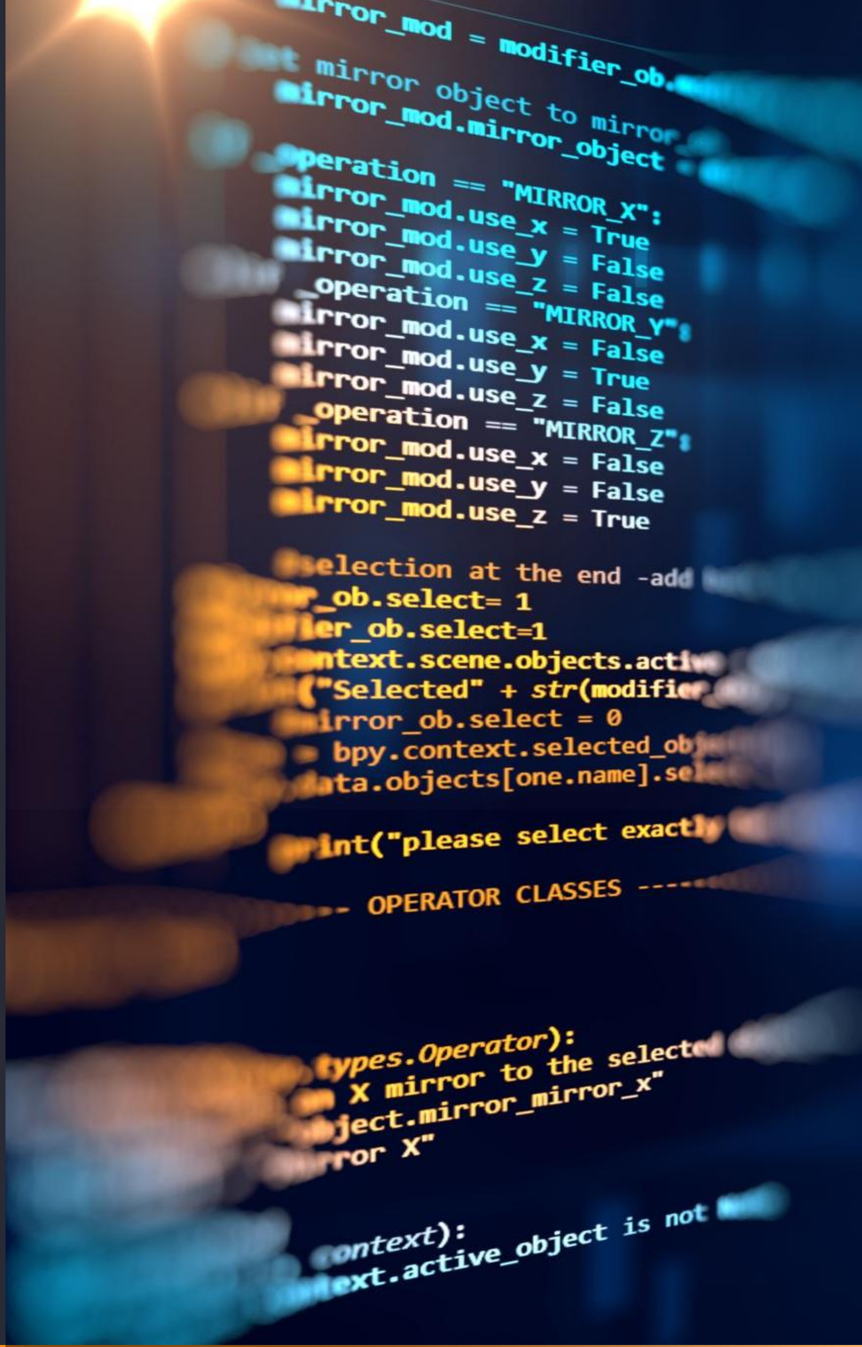
Security: network egress/ingress rules to isolate lab when detonating malware

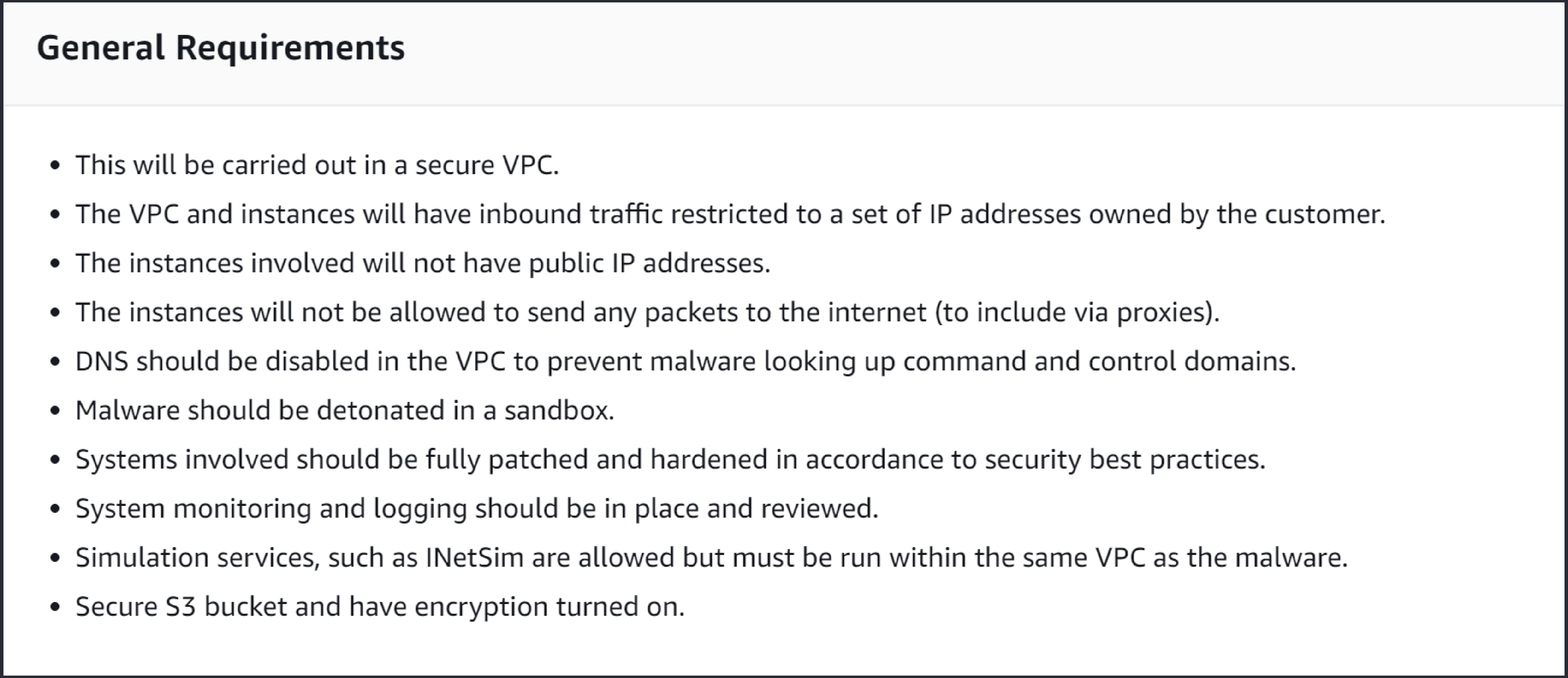
Result: rapid-deployable cloud malware lab that stands up in a few minutes.

Considerations, Security, & Guidelines

Considerations, Security, & Guidelines

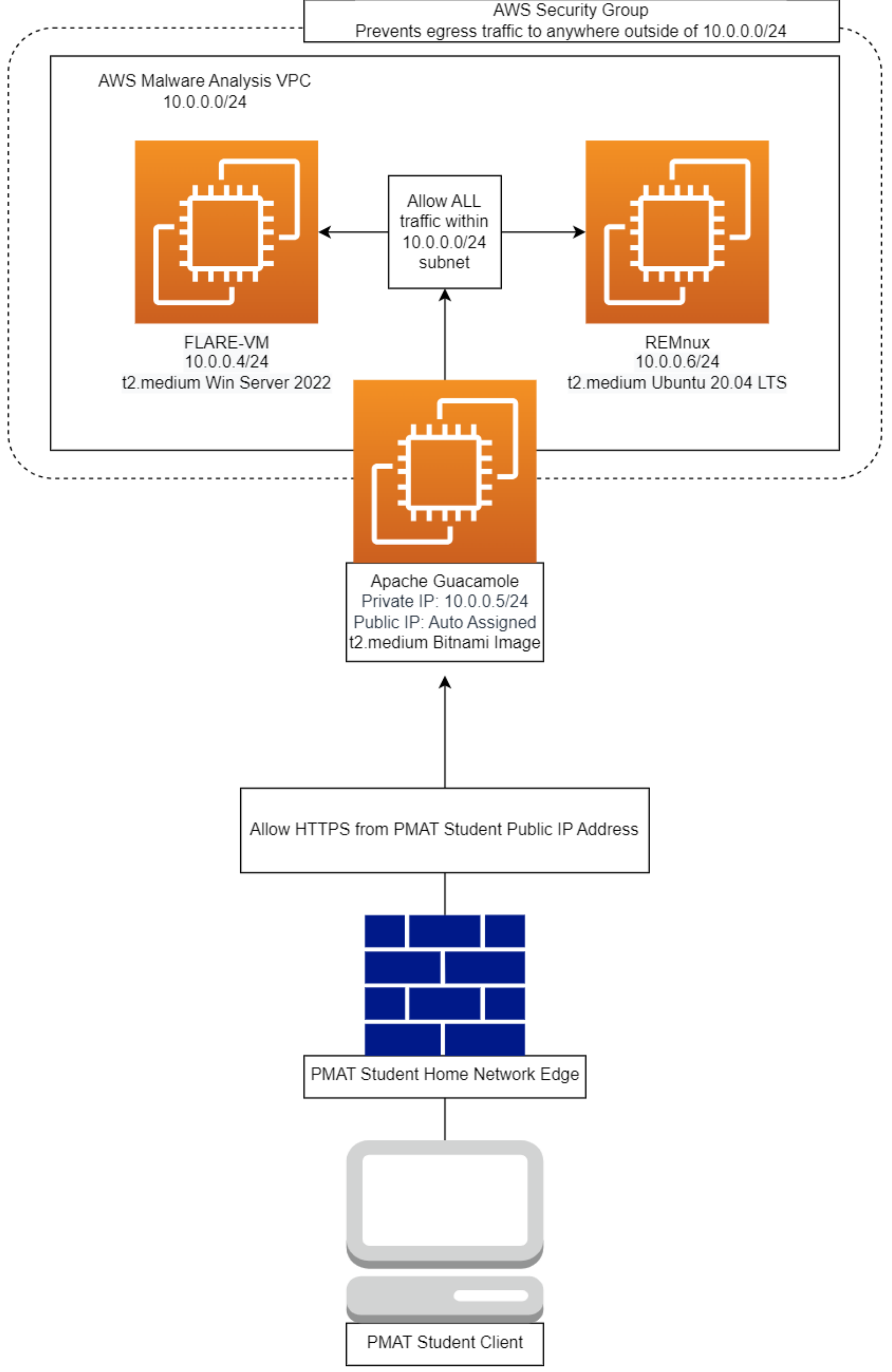
- AWS requires you to submit for permission to perform malware analysis (the Simulated Events form)
  - https://console.aws.amazon.com/support/contacts#/simulated-events
- Some assembly required
  - …as with all cloud provisioning, there's some setup (IAM, configuring aws-cli, getting Terraform to behave)
- Low cost but not without cost
  - As a point of reference, estimated $4 for instance time to complete the course
  - I foot the bill for the pre-built AMIs 😄





General Requirements

- This will be carried out in a secure VPC.
- The VPC and instances will have inbound traffic restricted to a set of IP addresses owned by the customer.
- The instances involved will not have public IP addresses.
- The instances will not be allowed to send any packets to the internet (to include via proxies).
- DNS should be disabled in the VPC to prevent malware looking up command and control domains.
- Malware should be detonated in a sandbox.
- Systems involved should be fully patched and hardened in accordance to security best practices.
- System monitoring and logging should be in place and reviewed.
- Simulation services, such as INetSim are allowed but must be run within the same VPC as the malware.
- Secure S3 bucket and have encryption turned on.



AWS Security Group
Prevents egress traffic to anywhere outside of 10.0.0.0/24

AWS Malware Analysis VPC
10.0.0.0/24

Allow ALL traffic within 10.0.0.0/24 subnet

FLARE-VM
10.0.0.4/24
t2.medium Win Server 2022

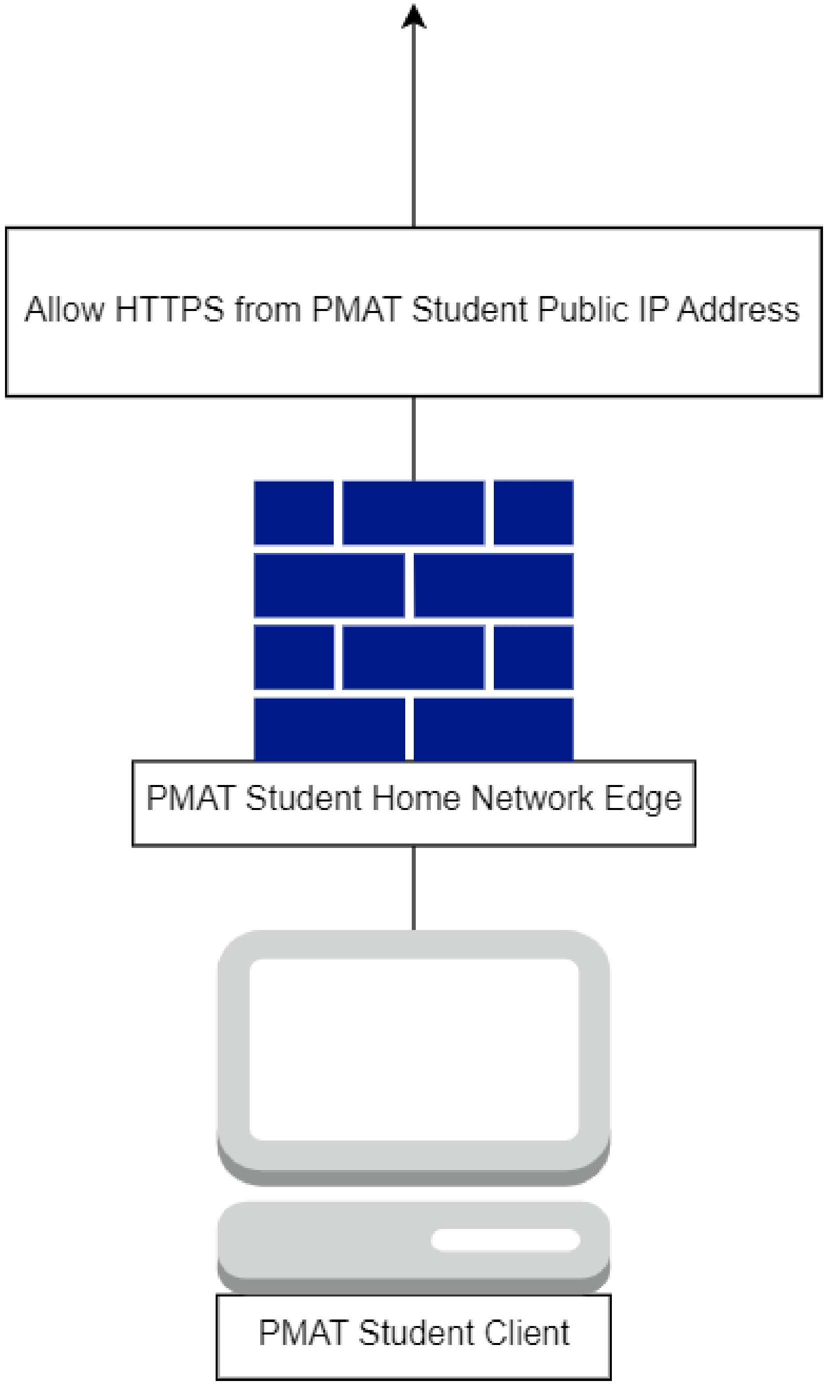
REMnux
10.0.0.6/24
t2.medium Ubuntu 20.04 LTS

Apache Guacamole
Private IP: 10.0.0.5/24
Public IP: Auto Assigned
t2.medium Bitnami Image

Allow HTTPS from PMAT Student Public IP Address

PMAT Student Home Network Edge

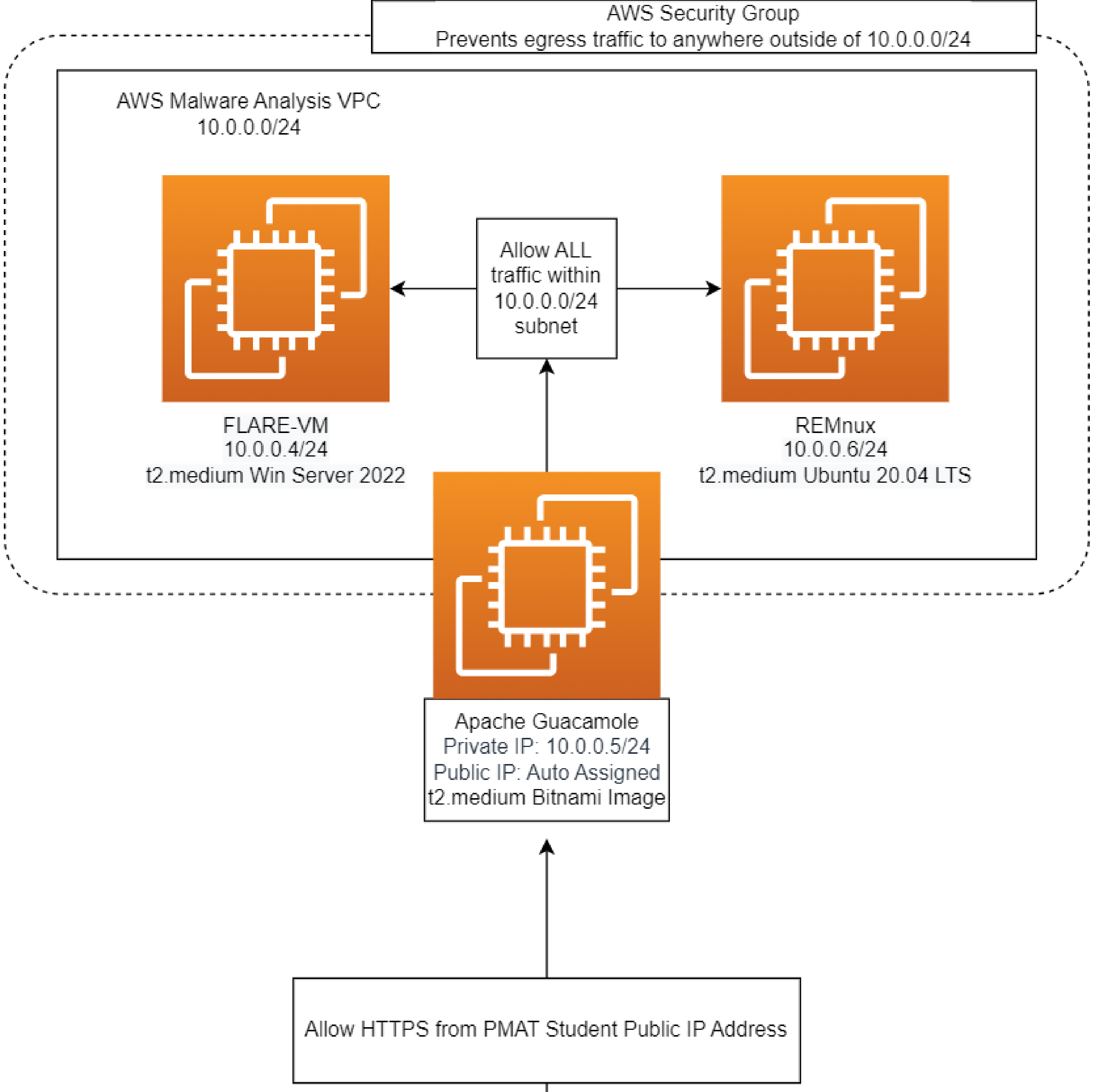
PMAT Student Client



Allow HTTPS from PMAT Student Public IP Address

PMAT Student Home Network Edge

PMAT Student Client



AWS Security Group
Prevents egress traffic to anywhere outside of 10.0.0.0/24

AWS Malware Analysis VPC
10.0.0.0/24

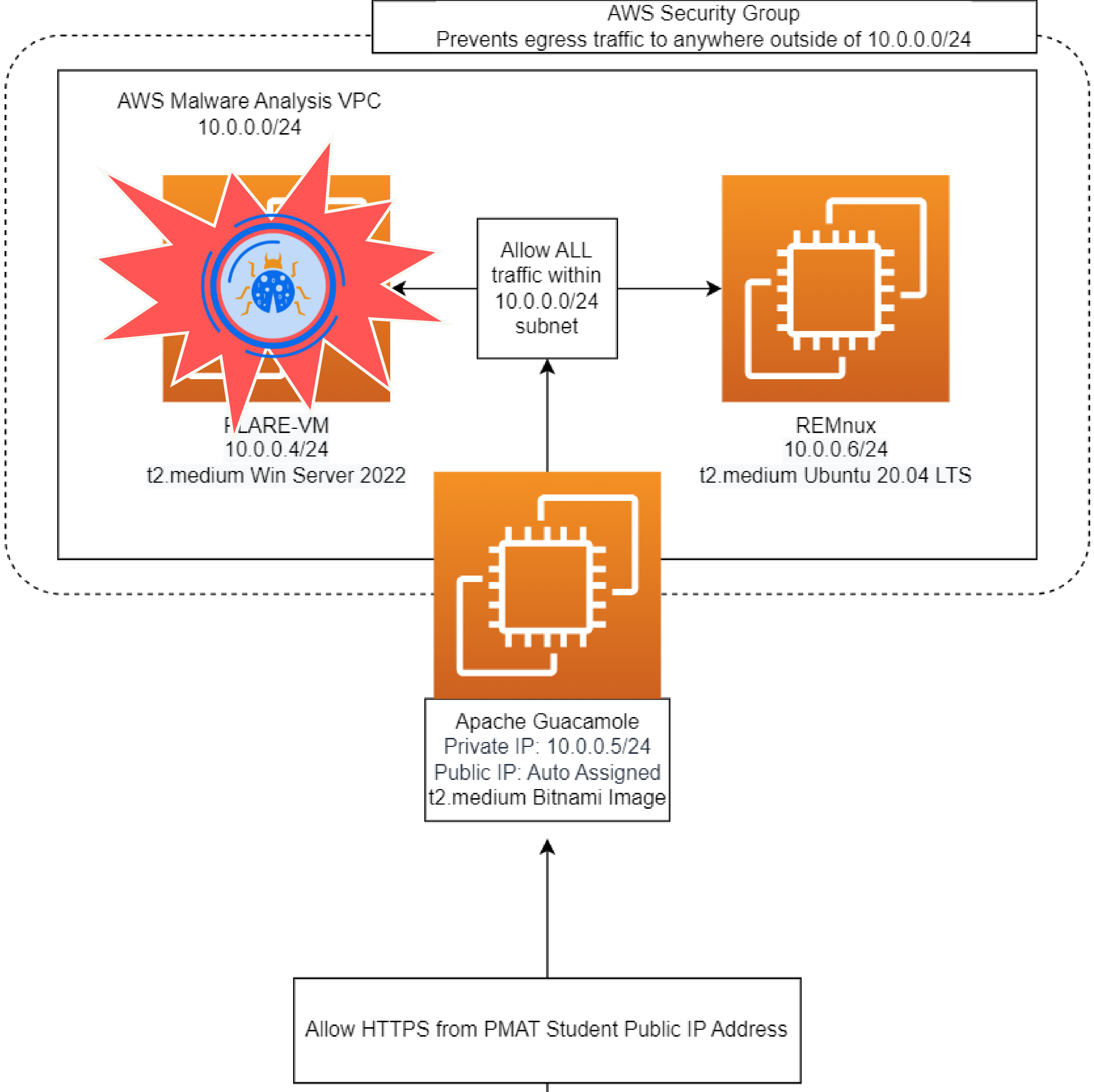
FLARE-VM
10.0.0.4/24
t2.medium Win Server 2022

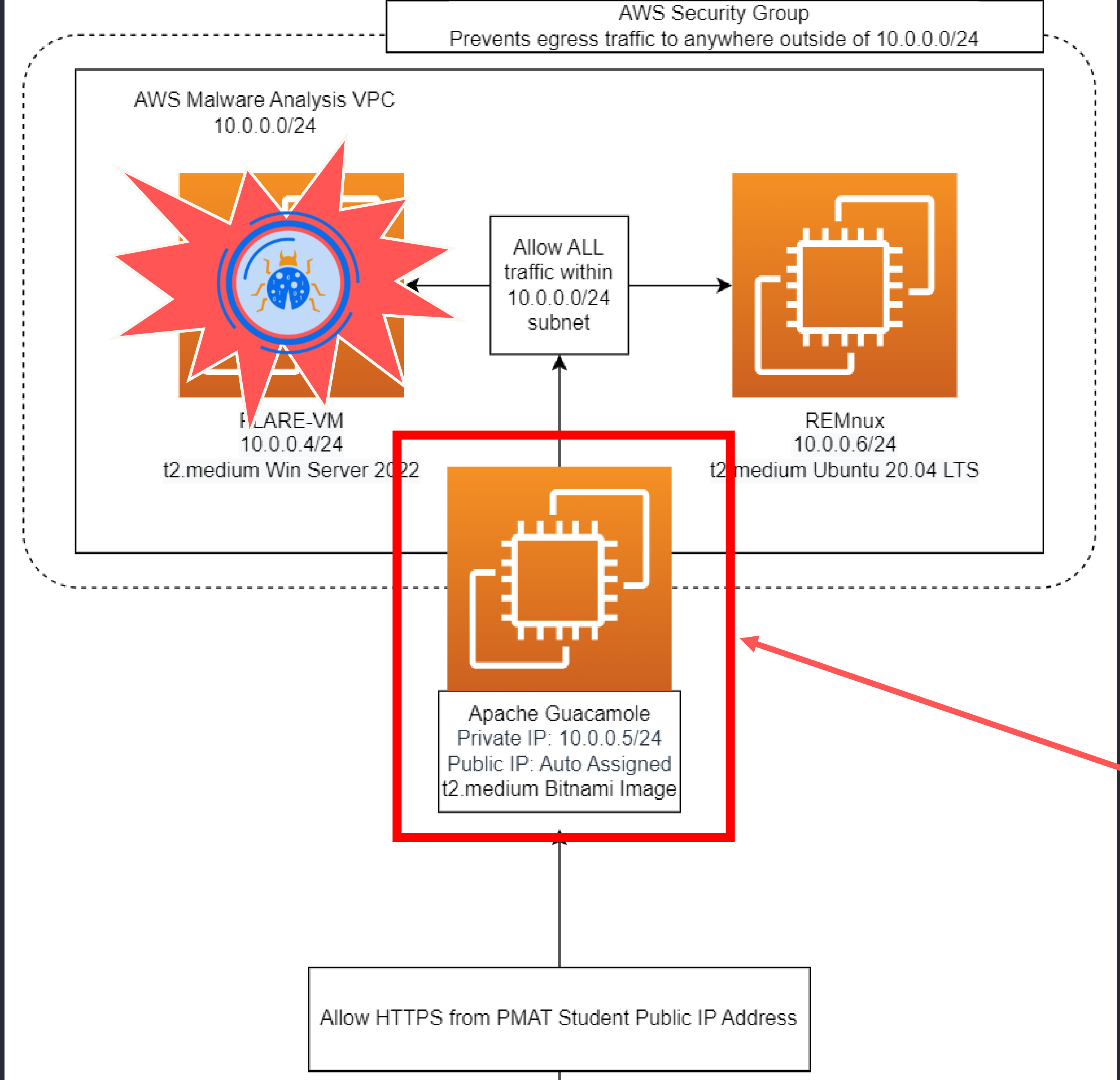
Allow ALL traffic within 10.0.0.0/24 subnet

REMnux
10.0.0.6/24
t2.medium Ubuntu 20.04 LTS

Apache Guacamole
Private IP: 10.0.0.5/24
Public IP: Auto Assigned
t2.medium Bitnami Image

Allow HTTPS from PMAT Student Public IP Address


AWS Security Group
Prevents egress traffic to anywhere outside of 10.0.0.0/24
AWS Malware Analysis VPC
10.0.0.0/24
Allow ALL traffic within 10.0.0.0/24 subnet
FLARE-VM
10.0.0.4/24
t2.medium Win Server 2022
REMnux
10.0.0.6/24
t2.medium Ubuntu 20.04 LTS
Apache Guacamole
Private IP: 10.0.0.5/24
Public IP: Auto Assigned
t2.medium Bitnami Image
Allow HTTPS from PMAT Student Public IP Address



AWS Security Group
Prevents egress traffic to anywhere outside of 10.0.0.0/24

AWS Malware Analysis VPC
10.0.0.0/24

FLARE-VM
10.0.0.4/24
t2.medium Win Server 2022

Allow ALL traffic within 10.0.0.0/24 subnet

REMnux
10.0.0.6/24
t2.medium Ubuntu 20.04 LTS

Apache Guacamole
Private IP: 10.0.0.5/24
Public IP: Auto Assigned
t2.medium Bitnami Image

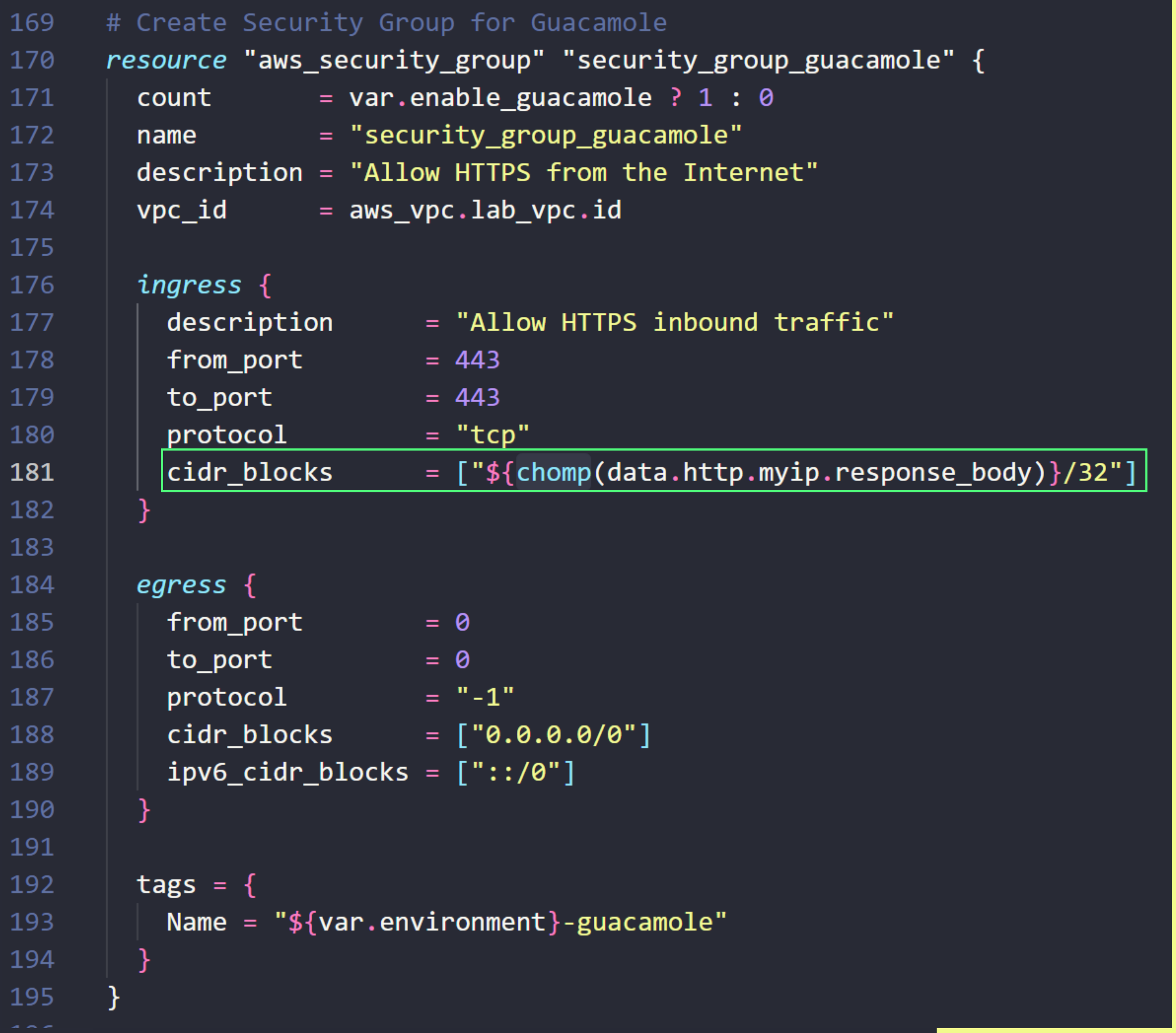
Allow HTTPS from PMAT Student Public IP Address

Our vantage point into the lab!

Pause! Hit go on the tech demo lab!

Security by Architecture, Architecture as Code

- Terraform makes the configuration identical, each time, every time
    - … with a few exceptions
    - Student’s home IP is discerned at runtime by Terraform and used to set up the security group rules
- VPC, subnet, ingress/egress are all handled by Terraform
- Provisioned without internet access by default, can manually add internet access security group to download malware/software



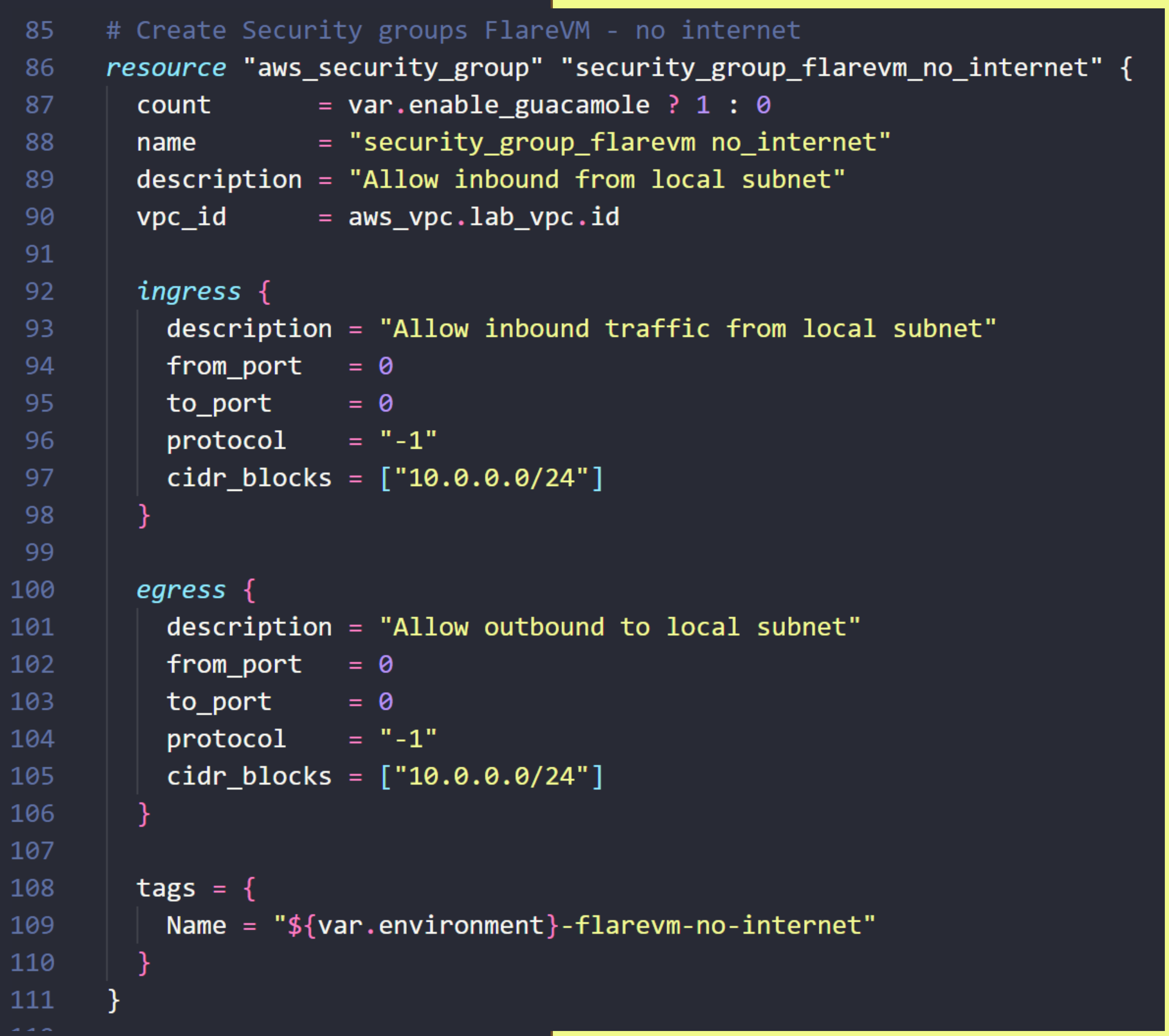
```
# Create Security Group for Guacamole
resource "aws_security_group" "security_group_guacamole" {
  count       = var.enable_guacamole ? 1 : 0
  name        = "security_group_guacamole"
  description = "Allow HTTPS from the Internet"
  vpc_id      = aws_vpc.lab_vpc.id

  ingress {
    description      = "Allow HTTPS inbound traffic"
    from_port        = 443
    to_port          = 443
    protocol         = "tcp"
    cidr_blocks      = ["${chomp(data.http.myip.response_body)}/32"]
  }

  egress {
    from_port        = 0
    to_port          = 0
    protocol         = "-1"
    cidr_blocks      = ["0.0.0.0/0"]
    ipv6_cidr_blocks = ["::/0"]
  }

  tags = {
    Name = "${var.environment}-guacamole"
  }
}
```

- Let FLARE-VM talk to everything in the VPC…
- … but don’t let it talk to anything outside the VPC!



```
# Create Security groups FlareVM - no internet
resource "aws_security_group" "security_group_flarevm_no_internet" {
  count       = var.enable_guacamole ? 1 : 0
  name        = "security_group_flarevm no_internet"
  description = "Allow inbound from local subnet"
  vpc_id      = aws_vpc.lab_vpc.id

  ingress {
    description = "Allow inbound traffic from local subnet"
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["10.0.0.0/24"]
  }

  egress {
    description = "Allow outbound to local subnet"
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["10.0.0.0/24"]
  }

  tags = {
    Name = "${var.environment}-flarevm-no-internet"
  }
}
```

Tech Demo

Questions / Comments / Thank You!

Matt Kiely / HuskyHacks

huskhacks.mk@gmail.com

@HuskyHacksMK

https://notes.huskyhacks.dev

Practical Malware Analysis & Triage: https://bit.ly/tcm-pmat

References

- Michael Mattes: Malware analysis with AWS (2022)
- https://github.com/adanalvarez/AWS-malware-lab