Breaking the Habit
Continuous Security

Dolev Farhi

BSides Toronto

Hello 🙋‍♂️

- Principal Security Engineer at Wealthsimple
- Previously @ Paytm, F5 Networks, CyberArk
- DC416

We are hiring for Security!
jobs.lever.co/wealthsimple

BSIDES TORONTO

Agenda

- Problem Statement
- Traditional Scanning
- Continuous Security
- NERVE Project
- Demo

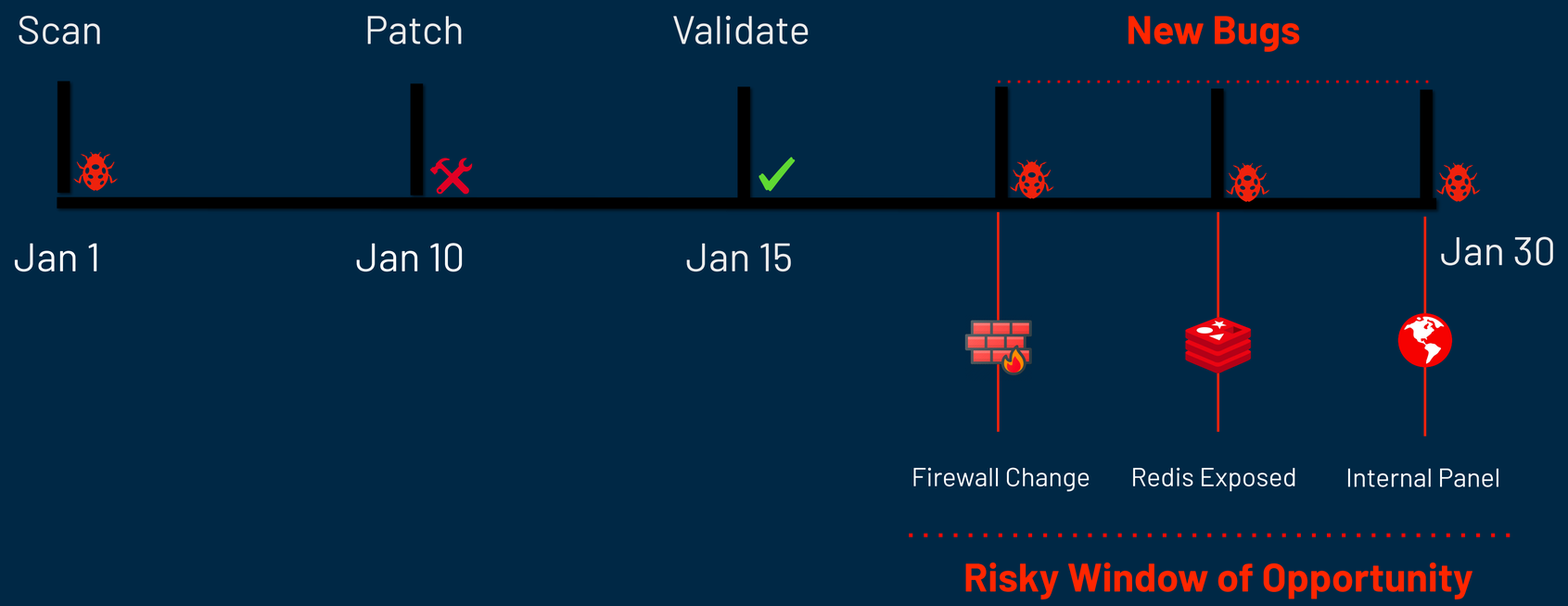
Problem Statement

Infrastructure and applications are continuously changing...

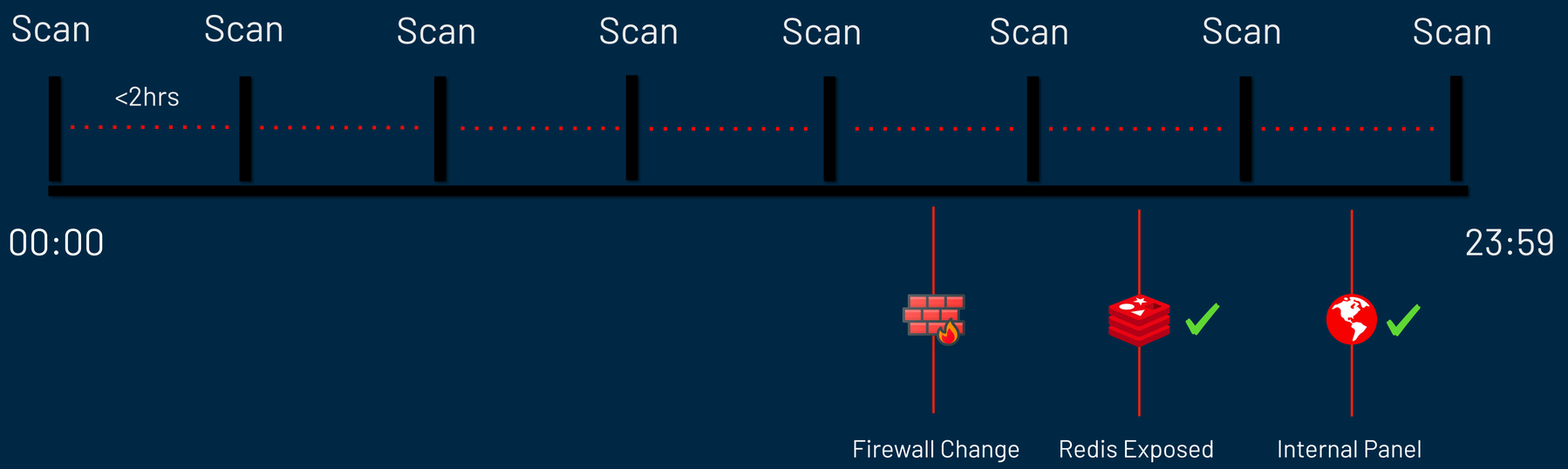
There can be hundreds of deployment **a day.**

How can we detect issues when the (attack) **surface is constantly changing?**

Traditional Scanning

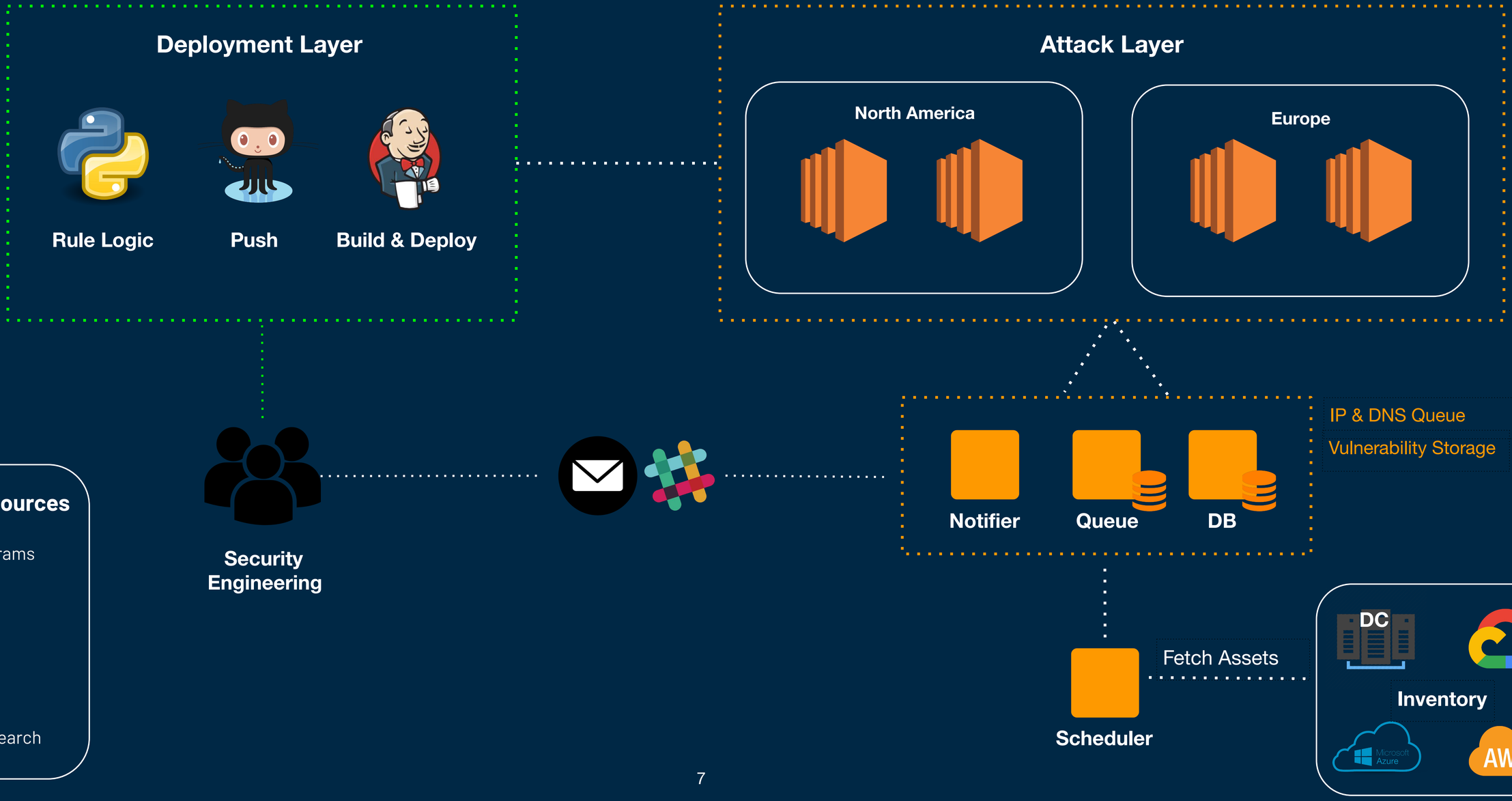


Continuous Security



Continuous Security

Building a Solution



Continuous Security

Building a Solution

- Actionable Alerts
- Remove Vendor Dependency
- Safe Lists /Exclusion Lists
- Capture Raw Requests and Responses
- Alert Management Interface
- Continuous Deployment Model

Continuous Security

Pros

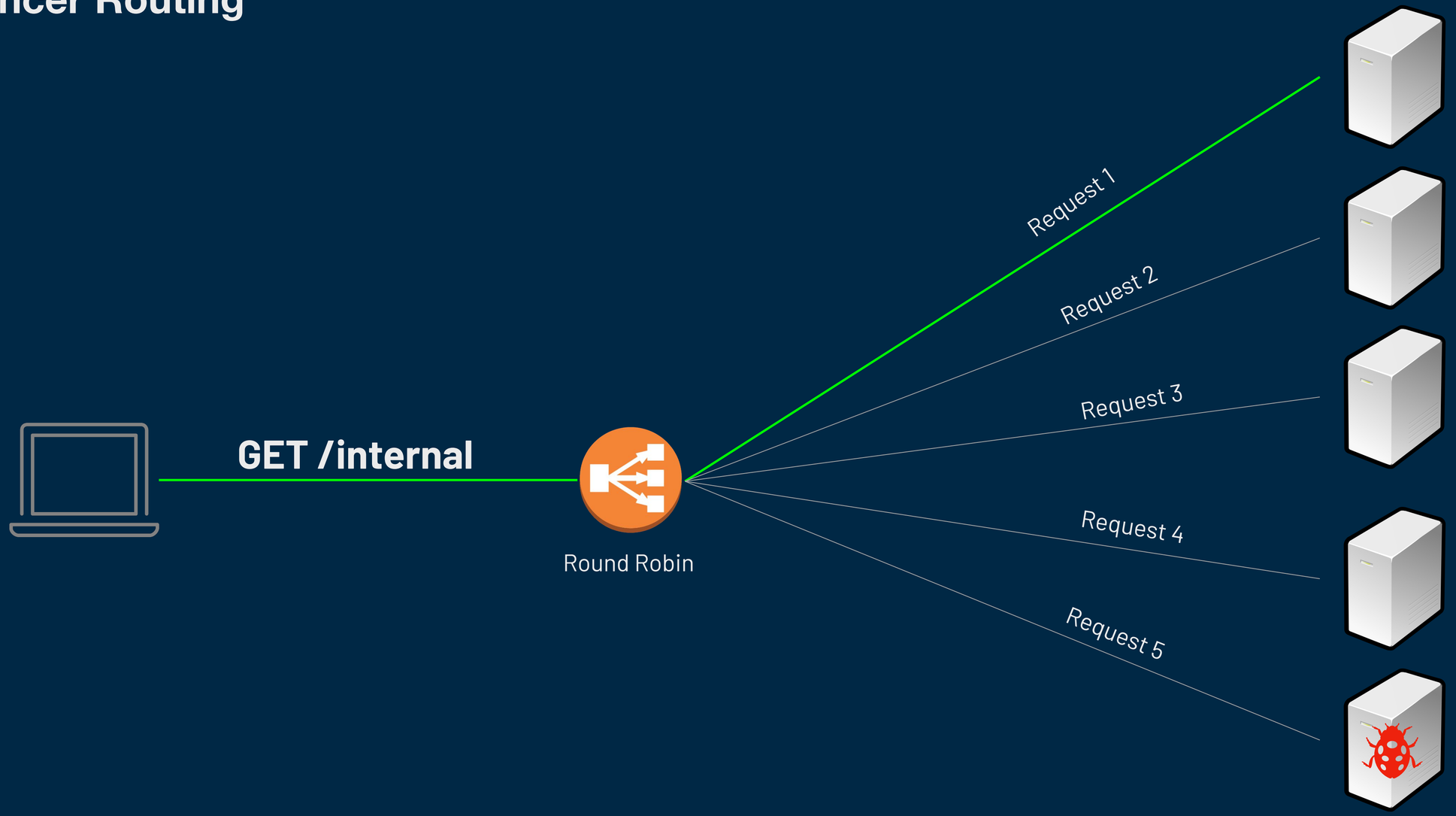
- You'll observe **weird** behaviours
- You'll discover **short-lived** issues
- Develop the ability to detect anomalies within hours or less
- Increased chances to win the MTTD race against Bug Bounty hunters & threat actors ;)

Cons

- Works well in dynamic and large environments, and less in smaller static ones.
- Your SRE may get angry

Continuous Security

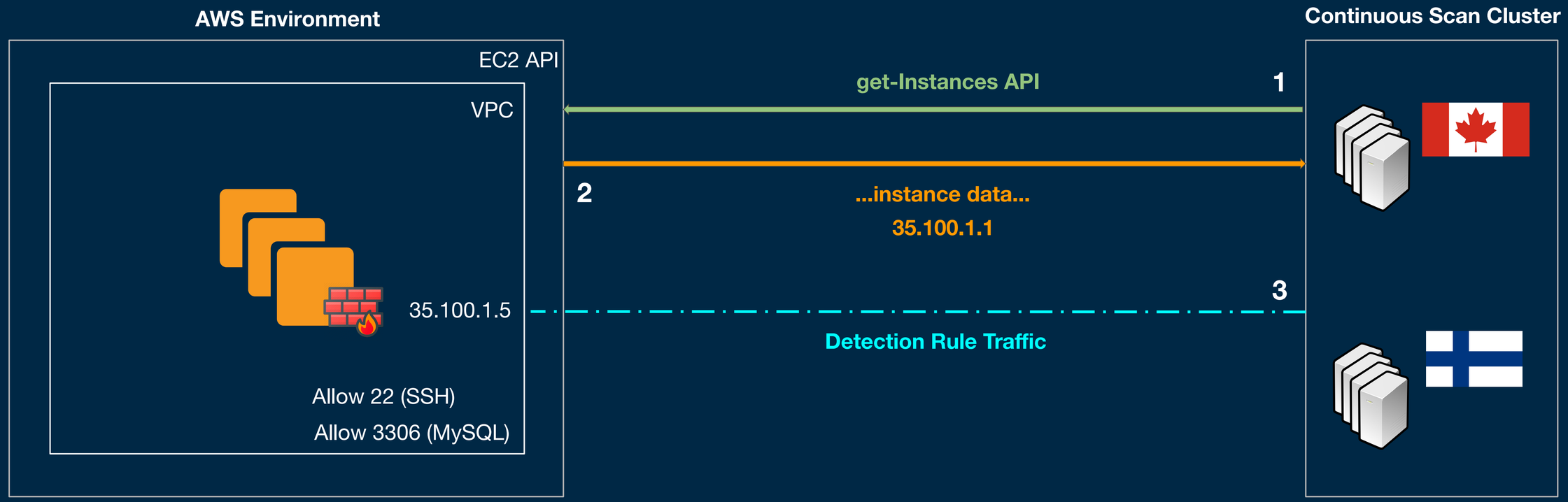
Load Balancer Routing



HTTP Request

Continuous Security

Elastic Addresses & Multi Origins



API Request

API Response

Friendly Attack Traffic

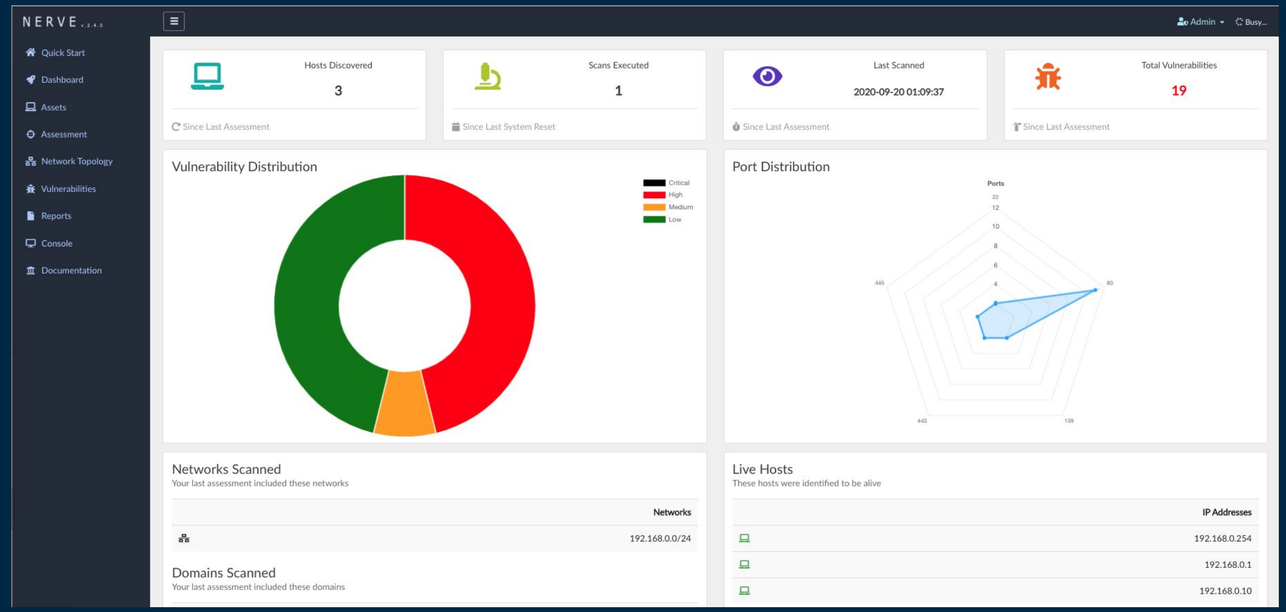
NERVE

Network Exploitation, Reconnaissance & Vulnerability Engine

NERVE

Features

- Graphical User Interface
- REST API
- Emphasis on High Signal Detection
- Notifications (Slack, Email, Web Hook)
- Reports (HTML, TXT, CSV, XML)
- Exclusions
- Customized Configurations
- Easy to Deploy
- Not an ASV replacement (Qualys, etc.)



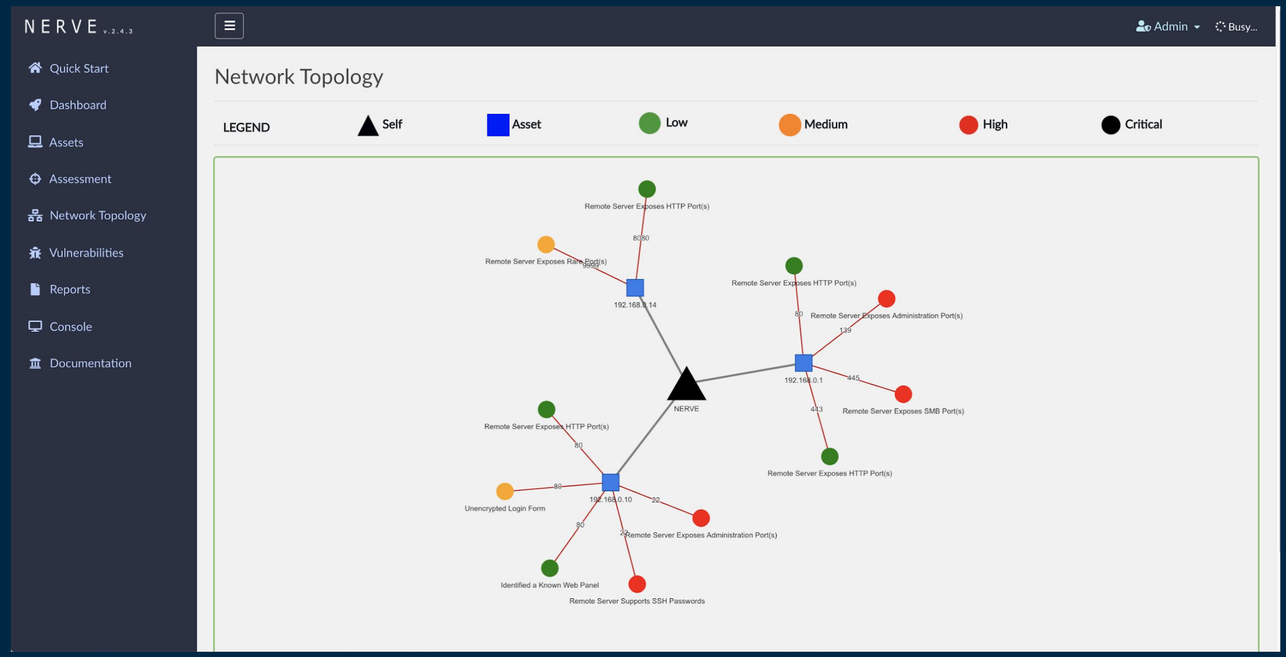
https://github.com/PaytmLabs/nerve

NERVE

Detections

- Subdomain Takeovers / Dangling DNS (S3, Beanstalk, etc)
- Misconfigured Frameworks (Django, Laravel, Flask, etc.)
- Cross Origin Resource Sharing Tests
- Brute Forcing (HTTP Basic Auth, SSH, FTP, Redis, etc.)
- Information Disclosures
- Directory Indexing
- Open git/svn repositories
- Injections (Host Header, CR LF, etc)
- Sensitive Panels (OpenAPI Swagger, Solr, PHPMyAdmin, etc)
- CVE Scans
- Best practices

& more



https://github.com/PaytmLabs/nerve

NERVE

Getting Started

1

Deploy NERVE

- Install on Bare Metal / VM
- Install using Docker

2

Collect Targets

Apps, Databases, Load Balancers, etc.

- AWS / GCP / Azure API
- Data Centre IP Pool

3

NERVE API

POST /api/scan

- Domains
- Subdomains
- IP Networks

4

Act on Result

GET /api/scan/status

- Analysis
- SOAR Flows
- Bug Trackers

Resources

https://github.com/PaytmLabs/nerve