Harnessing AI to Disrupt and Evaluate Security (HADES)

An AI-powered app for emulating cyber adversaries during blue team exercises.

Vic Fernandez III @cyberphor

ARTIST - HTTPS://WWW.COLLINSIEBENER.COM

Cyber Defense Training Experiences in the Military

SOC Manager

CSSP Manager

Threat Hunter

Cyber Defense Training Experiences in the Military

SOC Manager

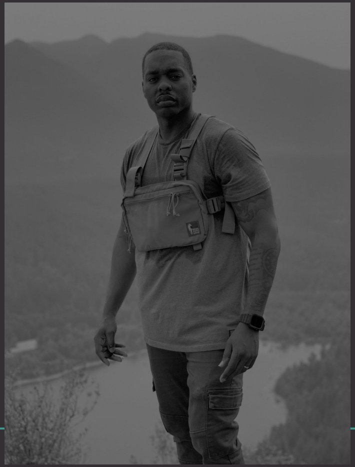
CSSP Manager

Threat Hunter

Cyber Defense Training Experiences in the Military

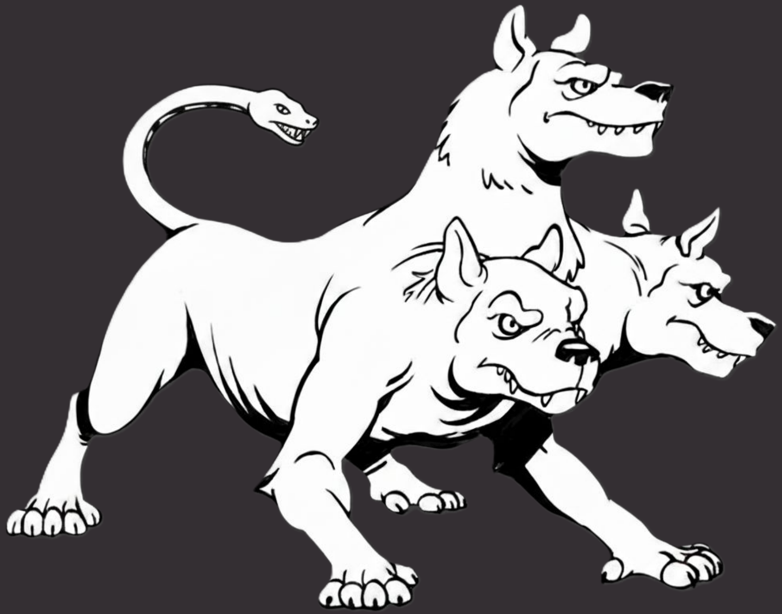
SOC Manager

CSSP Manager



Threat Hunter

Centralized Training: A Three-Headed Problem



inefficient **schedules** ✖

unrealistic **environments** ✖

distracting **complexity** ✖

ARTIST - HTTPS://LIBRARYFORKIDS.COM

Taming the Beast

Cyber defenders need training capabilities that are:

- On-Demand
- Intuitive
- Realistic
- Affordable
- Interoperable

ARTIST - HTTPS://WWW.FREEPIK.COM

HADES

github.com/deathlabs/hades

An AI-powered cyber adversary emulation app for dynamically introducing realistic scenarios during blue team training exercises.

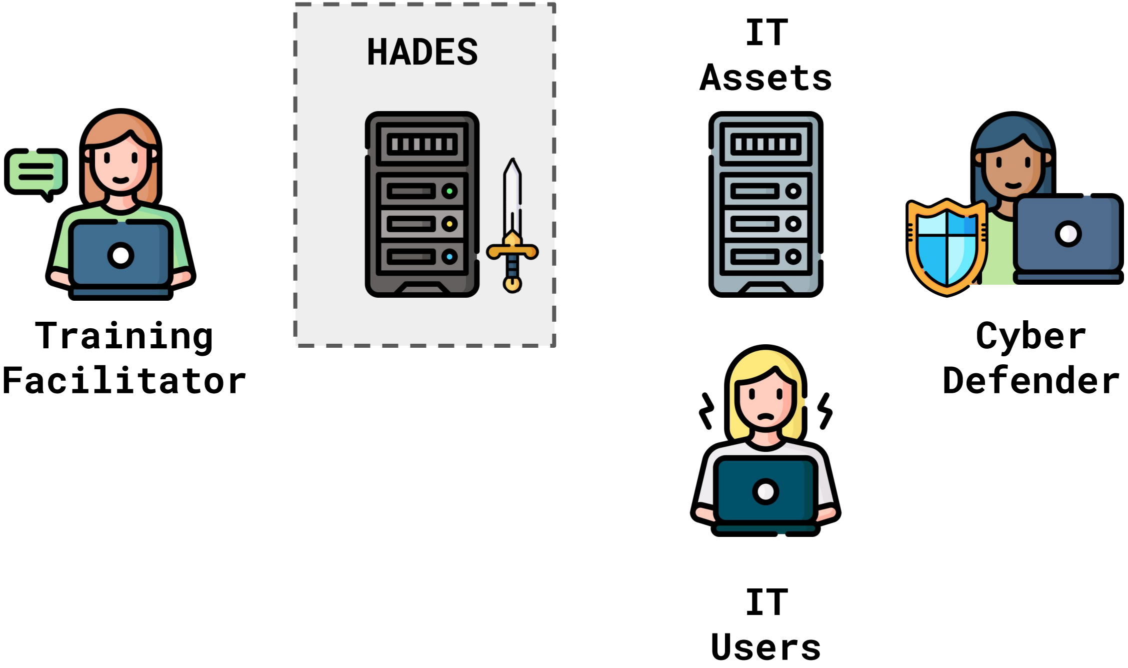
- ✓ **On Demand:** containerized
- ✓ **Realistic:** intelligent
- ✓ **Interoperable:** standards-based
- ✓ **Intuitive:** user-focused
- ✓ **Affordable:** free and open source

ARTIST - HTTPS://WWW.COLLINSIEBENER.COM

HADES Tactics & Tools

Tactic	Technique	Tool	Dev Status
Recon	*Active scanning*	Nmap	**Implemented ✔**
Execution	*Command interpreter*	BASH	**In progress ⏳**
Initial Access	*Exploiting web apps*	Metasploit	**Implemented ✔**
Initial Access	*Phishing*	GoPhish	**Not started ✖**
Credential Access	*Password guessing*	Hydra	**In progress ⏳**
C2	*Encrypted C2 channels*	Metasploit	**Implemented ✔**
Exfiltration	*Data exfiltration*	Metasploit	**Implemented ✔**

HADES Architecture



HADES

IT Assets

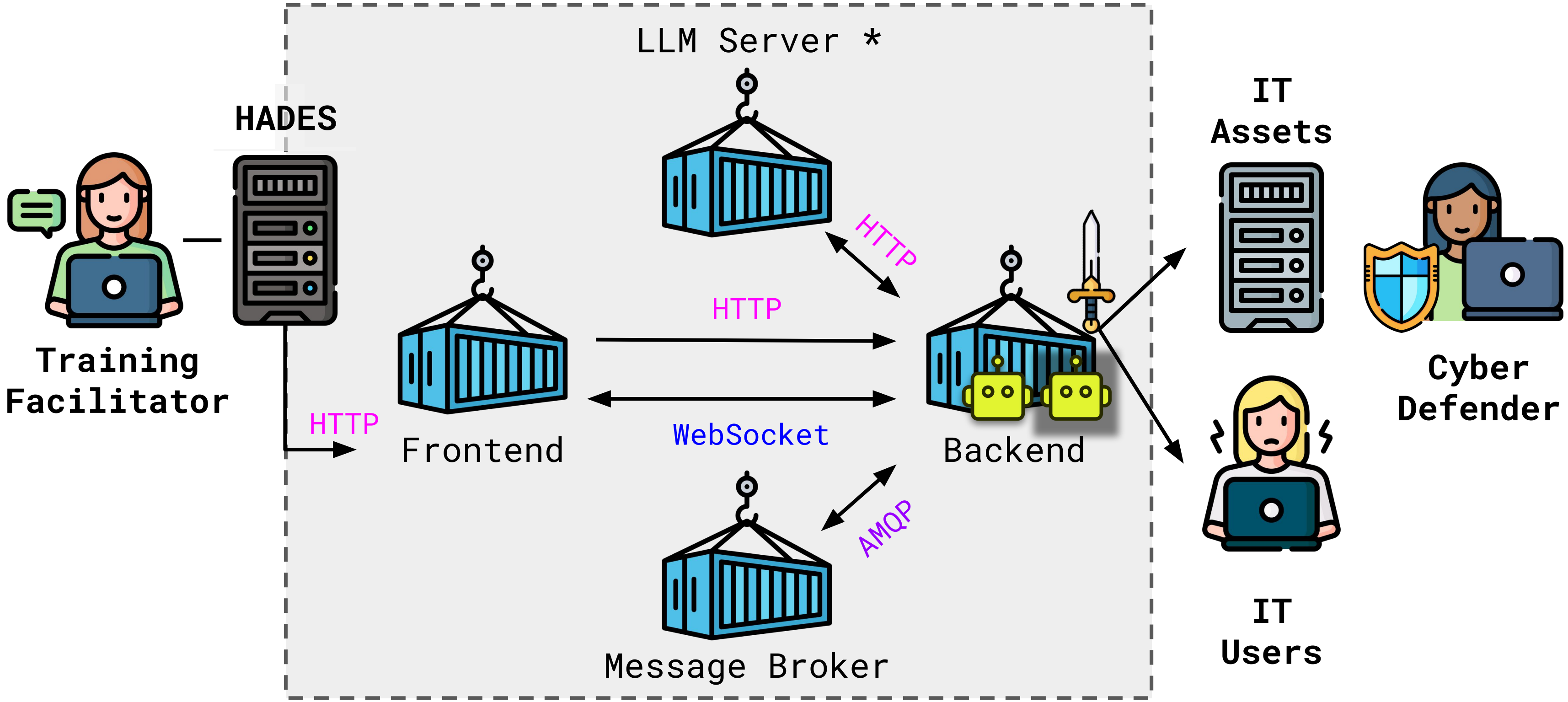
Training Facilitator

Cyber Defender

IT Users

ARTIST - HTTPS://WWW.FREEPIK.COM

HADES Architecture



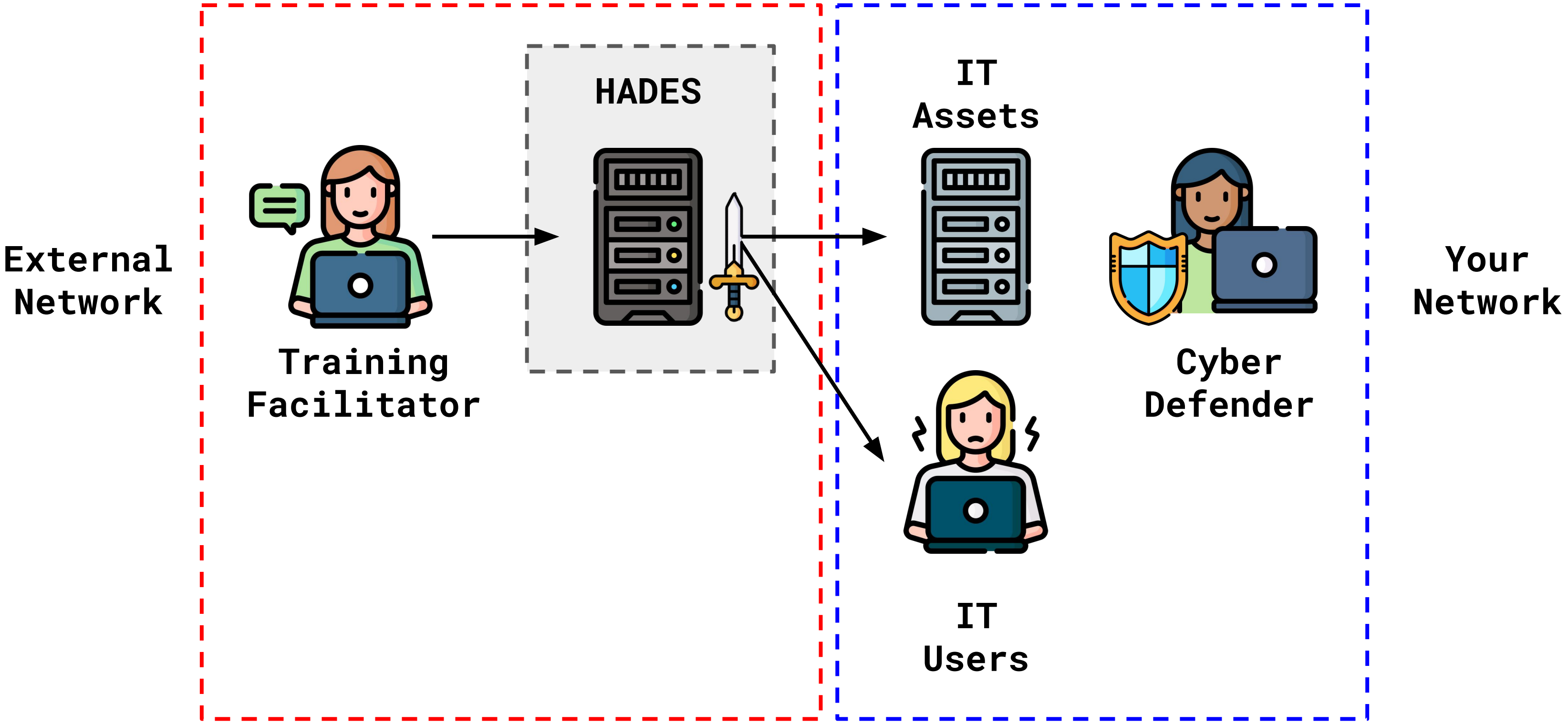
ARTIST - HTTPS://WWW.FREEPIK.COM

Use Cases

- Use Case #1: Simulating an External Threat
- Use Case #2: Simulating an Internal Threat
- Use Case #3: Conducting Self-Development

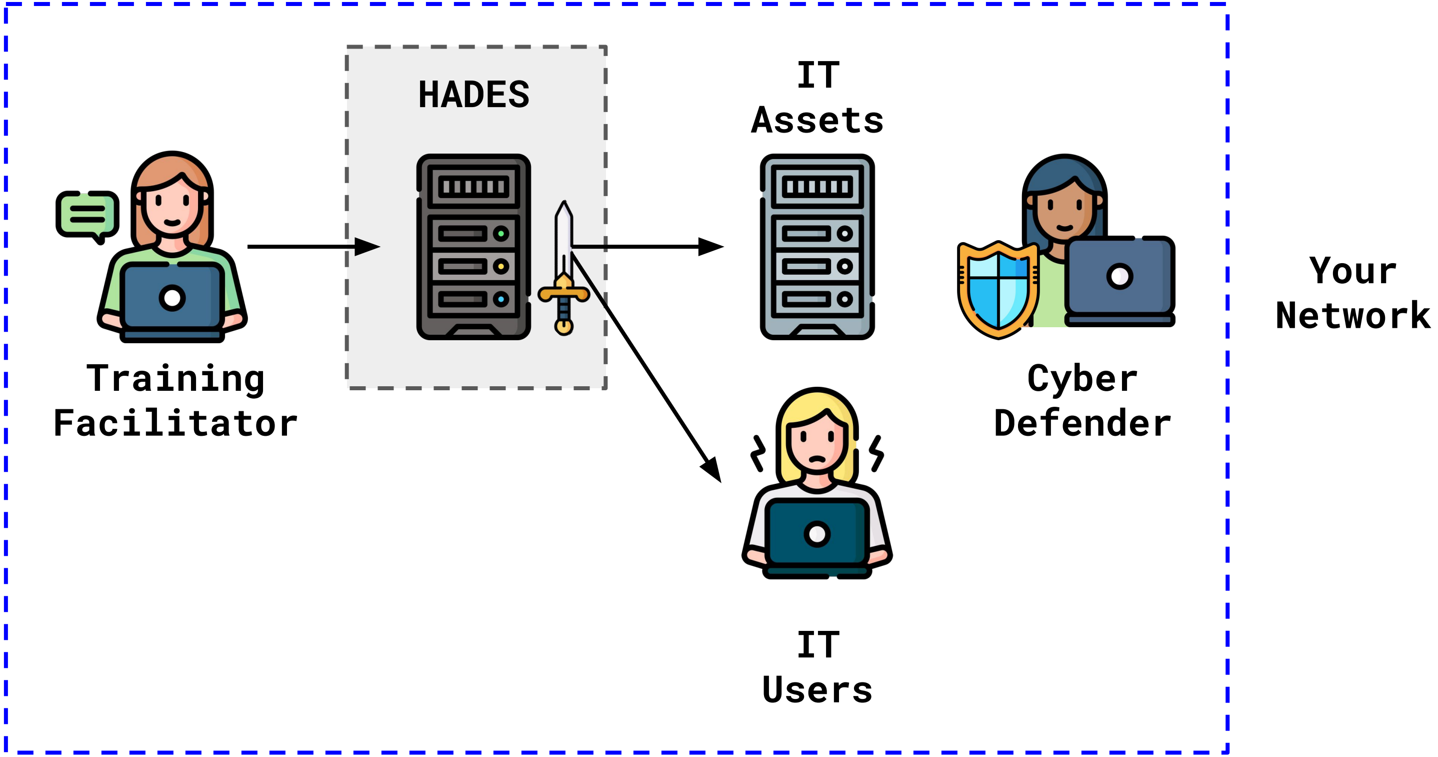
ARTIST - HTTPS://WWW.FREEPIK.COM

Use Case #1: Simulating an External Threat



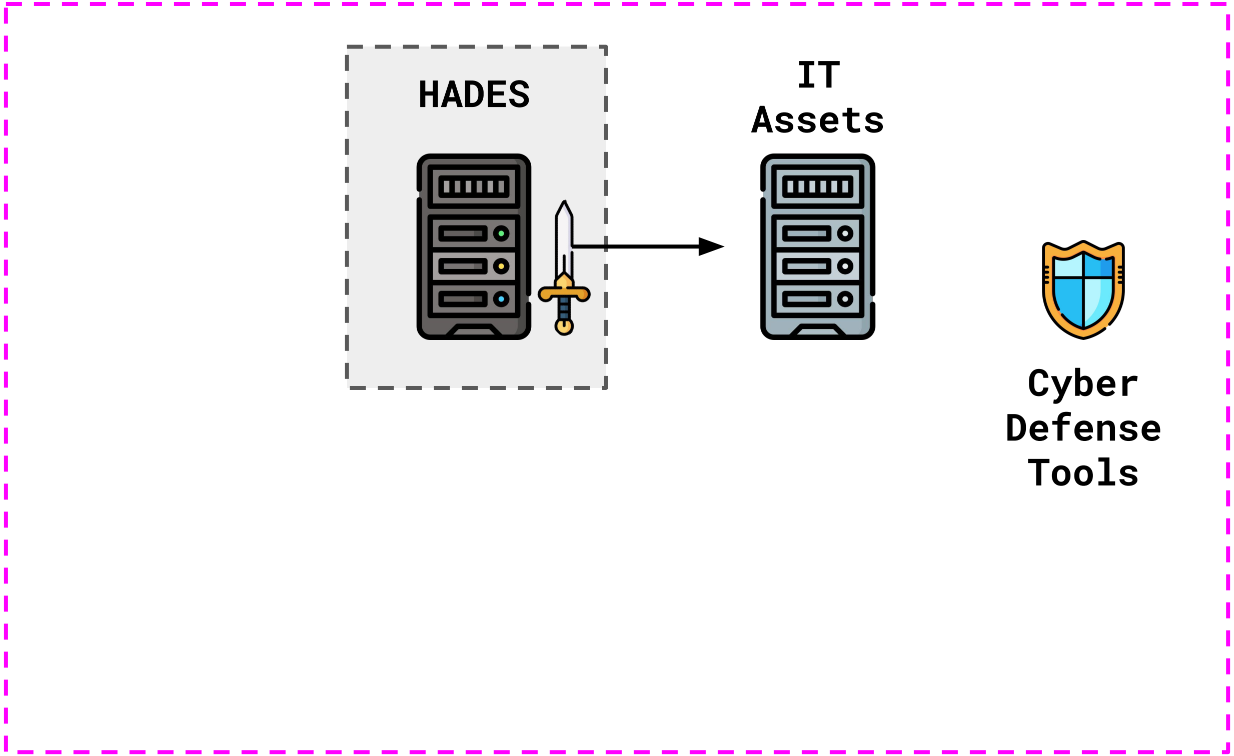
ARTIST - HTTPS://WWW.FREEPIK.COM

Use Case #2: Simulating an Internal Threat



ARTIST - HTTPS://WWW.FREEPIK.COM

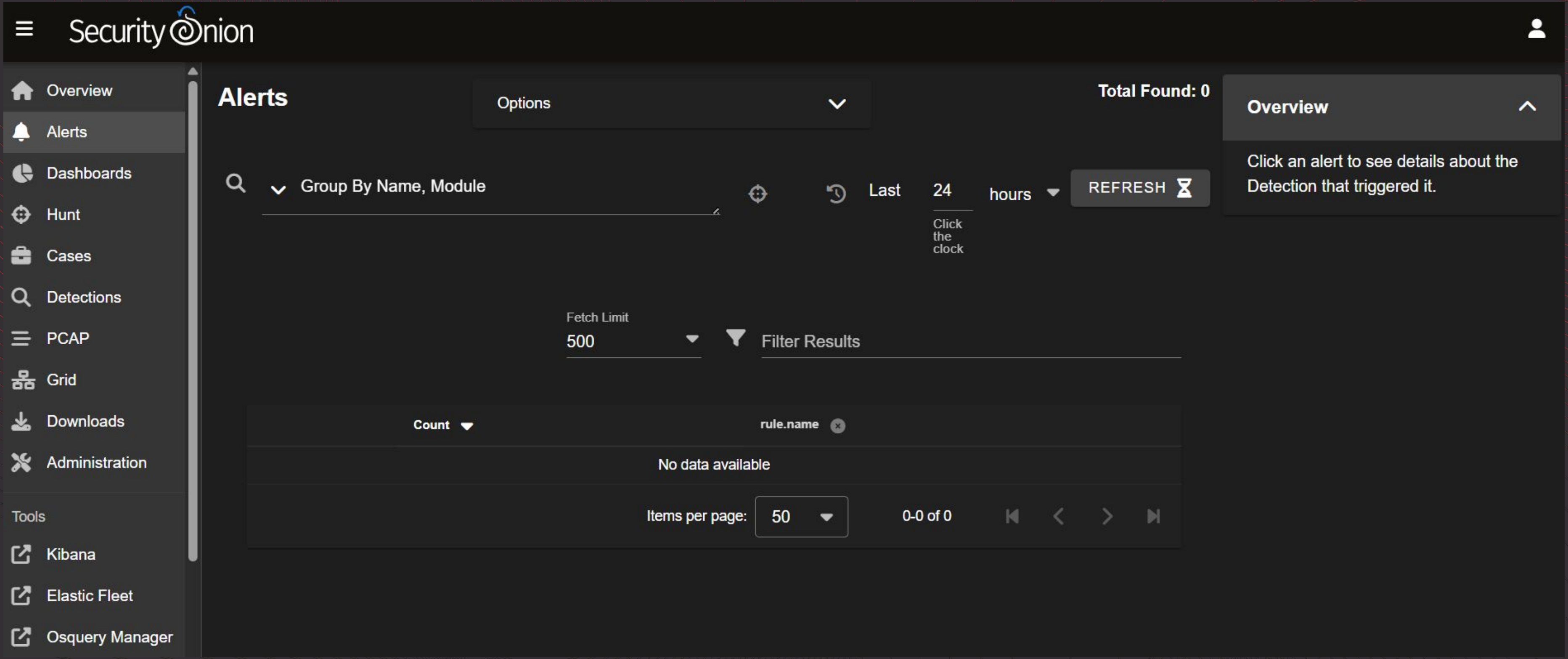
Use Case #3: Conducting Self-Development



Your
Laptop

ARTIST - HTTPS://WWW.FREEPIK.COM

Demo



Alerts

Total Found: 0

Group By Name, Module

Last 24 hours

Click the clock

Fetch Limit 500

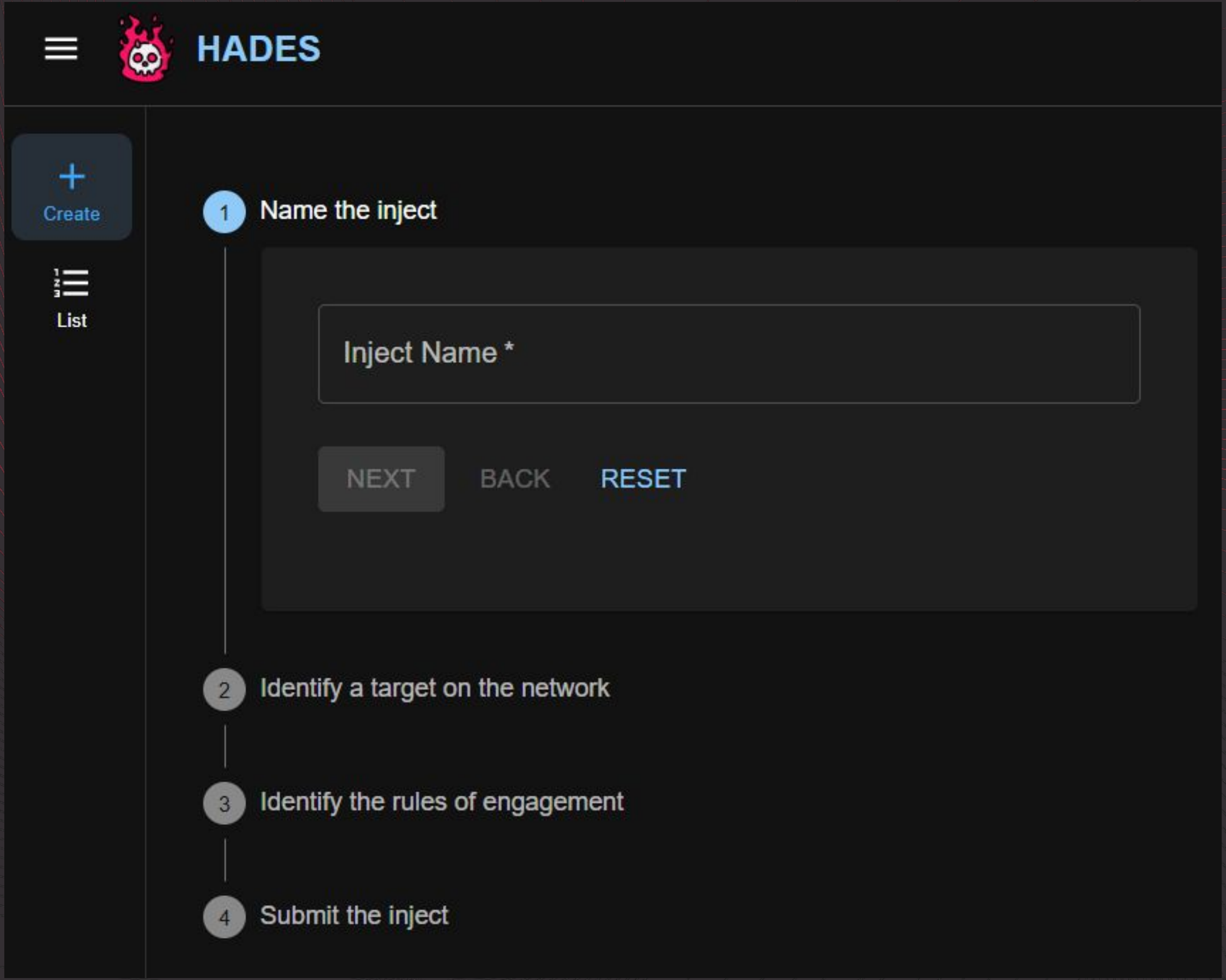
Filter Results

Count	rule.name
No data available	

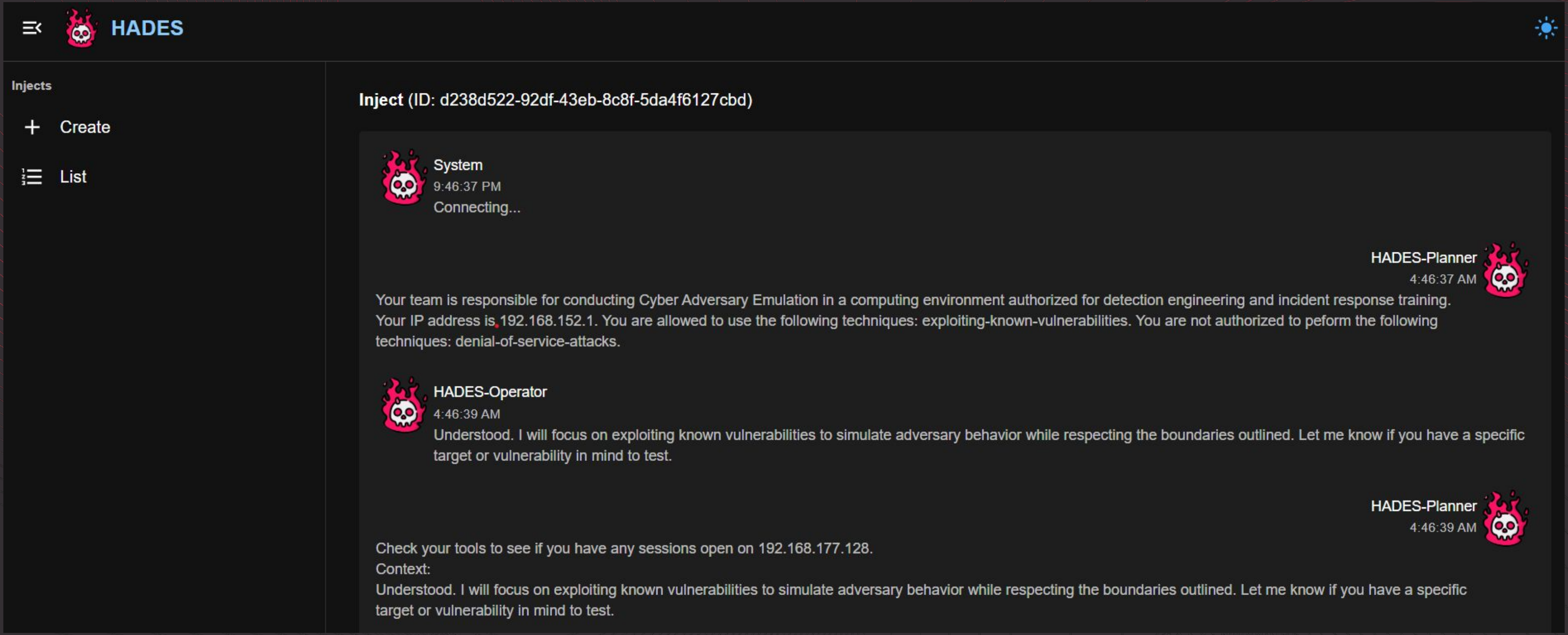
Items per page: 50 0-0 of 0

Overview

Click an alert to see details about the Detection that triggered it.



HADES
Create
List
1
Name the inject
Inject Name *
NEXT
BACK
RESET
2
Identify a target on the network
3
Identify the rules of engagement
4
Submit the inject



Inject (ID: d238d522-92df-43eb-8c8f-5da4f6127cbd)

System
9:46:37 PM
Connecting...

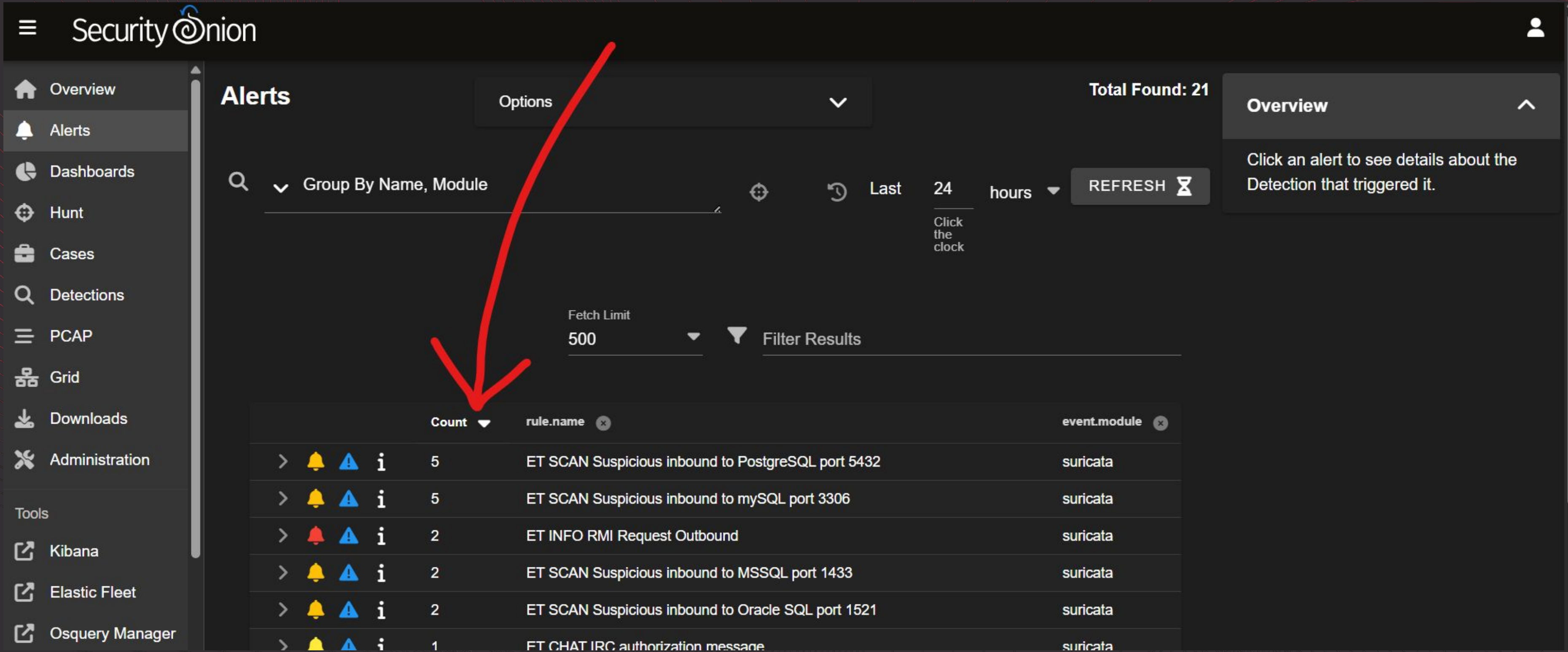
HADES-Planner
4:46:37 AM

Your team is responsible for conducting Cyber Adversary Emulation in a computing environment authorized for detection engineering and incident response training. Your IP address is 192.168.152.1. You are allowed to use the following techniques: exploiting-known-vulnerabilities. You are not authorized to peform the following techniques: denial-of-service-attacks.

HADES-Operator
4:46:39 AM
Understood. I will focus on exploiting known vulnerabilities to simulate adversary behavior while respecting the boundaries outlined. Let me know if you have a specific target or vulnerability in mind to test.

HADES-Planner
4:46:39 AM

Check your tools to see if you have any sessions open on 192.168.177.128.
Context:
Understood. I will focus on exploiting known vulnerabilities to simulate adversary behavior while respecting the boundaries outlined. Let me know if you have a specific target or vulnerability in mind to test.



Alerts

Total Found: 21

Group By Name, Module

Last 24 hours

Fetch Limit 500

Overview

Click an alert to see details about the Detection that triggered it.

Count	rule.name	event.module
5	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata
5	ET SCAN Suspicious inbound to mySQL port 3306	suricata
2	ET INFO RMI Request Outbound	suricata
2	ET SCAN Suspicious inbound to MSSQL port 1433	suricata
2	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata
1	ET CHAT IRC authorization message	suricata