Apply Team Threat Hunting with AI and Automation

Speaker Introduction

Kenny Peeples is a Red Hat Principal Architect for North America Public Sector. He has extensive Cybersecurity experience in Cloud, Big Data and IoT for government agencies such as Department of Defense, Department of Homeland Security and NSA. He was also a Middleware Global Evangelist for the Red Hat Middleware Business Unit. He provided videos, whitepapers, code, etc to Solutions Architects, Consultants and Partners across the globe. He has a Bachelors and Masters in Computer Science and pursuing a Doctor of Engineering in Systems Engineering.

SECURITY bsides CHARLESTON, SC

Session Description

"…you still need to worry about the remaining 20%"

Threat hunting, also known as cyberthreat hunting, is a proactive approach to identifying previously unknown, or ongoing non-remediated threats, within an organization's network.

https://www.ibm.com/topics/threat-hunting

The rapid advancement of Generative AI has lowered the barrier for creating sophisticated malware, making less experienced hackers capable of propagating attacks in a matter of minutes. This new type of threat highlights the need to develop suitable tools to reduce detection time to a similar timeframe.

This talk introduces Kestrel as a Service (KaaS), empowering threat hunters with reusable threat hunting flows from the Kestrel language, effortlessly deployable in the cloud. Augmented by predictive AI model plugins, Kestrel optimizes threat detection, accelerating response times in case of attacks. Kestrel provides a layer of abstraction to stop the repetition involved in cyber threat hunting. Kestrel contains two main components, 1) A threat hunting language for a human to express what to hunt and 2) A machine interpreter that deals with how to hunt. The key objective is to use these components to hunt faster.

Join this talk to learn about Kestrel as a Service, AI Integration and standing up an environment quickly.

https://github.com/opencybersecurityalliance/kestrel-as-a-service

Agenda

- Speaker Introduction
- Overview
- Demonstration
- Q&A

Takeaway 1 - Understanding importance of Team Threat Hunting

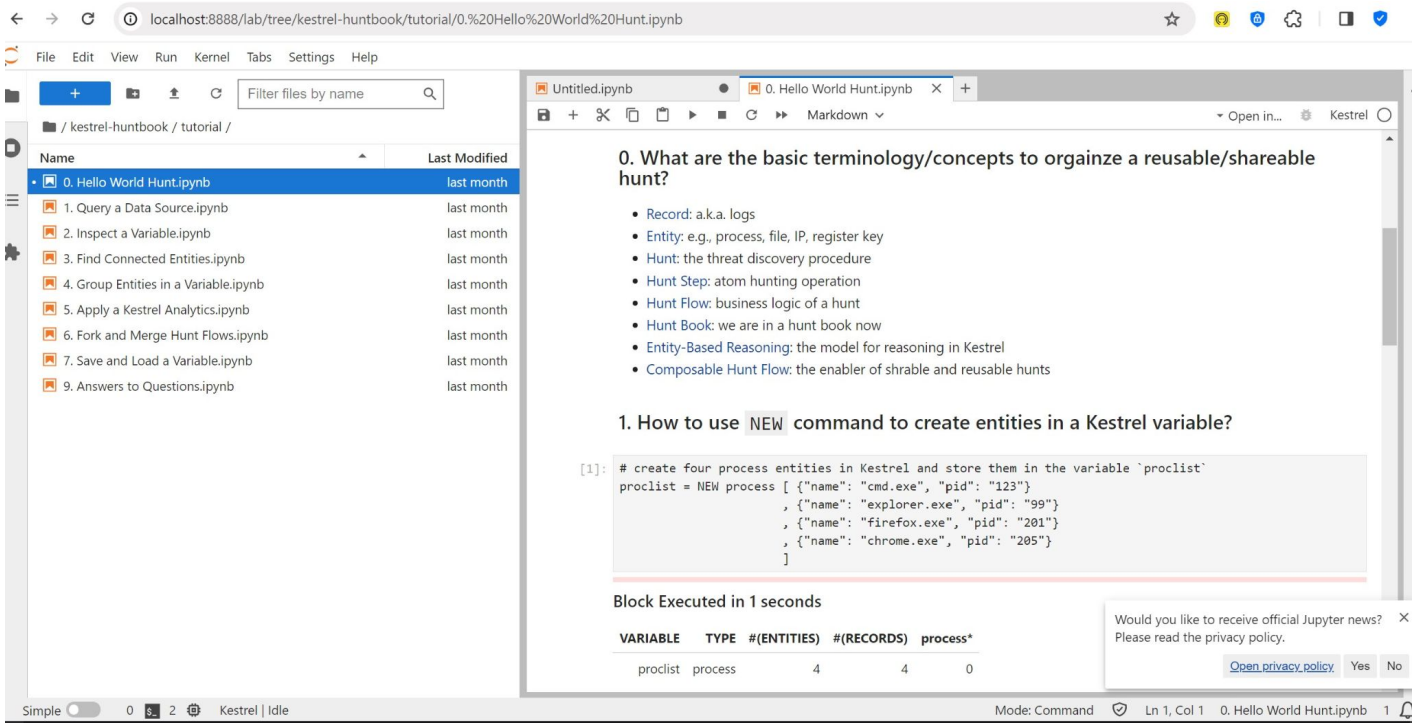
Takeaway 2 - Understanding of Kestrel/KaaS with Deployments

Takeaway 3 - Understanding of how to run the tutorials

https://github.com/opencybersecurityalliance/kestrel-as-a-service/blob/main/getting-started/conferences/Charleston%20BSides%2024%20-%20Threat%20Hunting.pdf

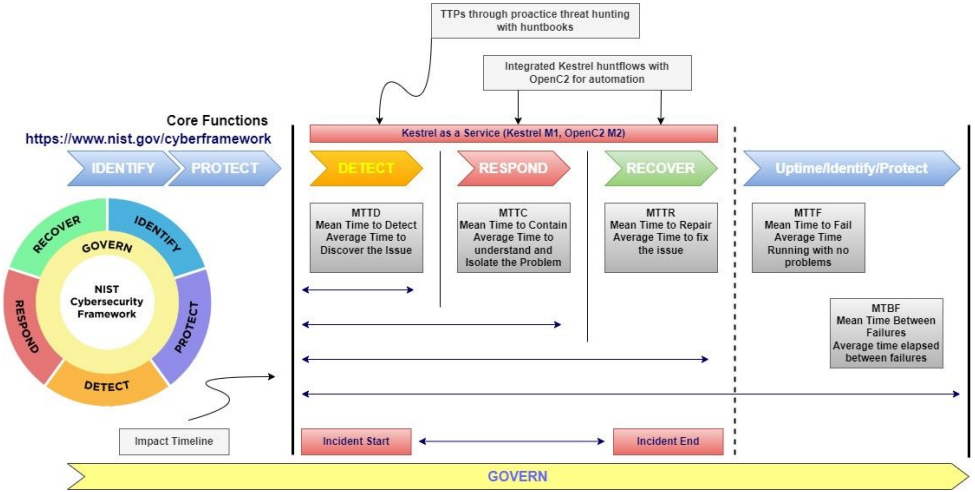
SECURITY bsides CHARLESTON, SC

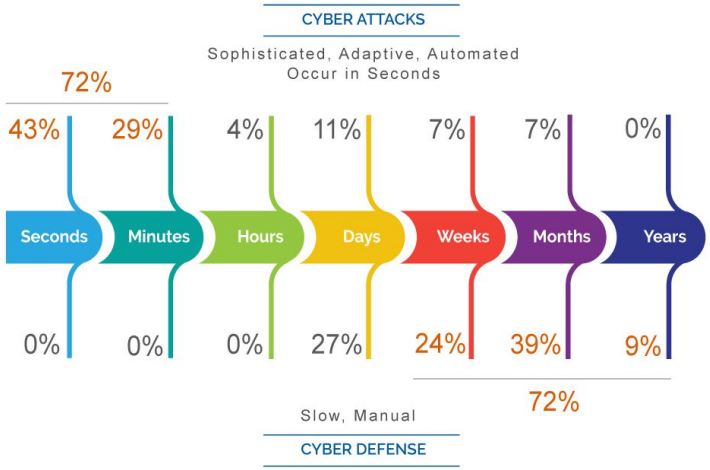
Kestrel/KaaS, Deployment, Usage



SECURITY sides
CHARLESTON, SC

Project Overview





https://research.redhat.com/blog/article/team-threat-hunting-on-a-container-platform-kestrel-as-a-service/

SECURITY sides
CHARLESTON, SC

Threat Intelligence vs Threat Hunting

- Threat Intelligence
  - Evidence Based
  - Attempted or successful intrusions
- Threat Hunting
  - Begins where intelligence ends
  - Possible threat indicators or hypothesis
  - Trigger, Investigation, Resolution

Kestrel

- Air Force Research Laboratory (ARFL) and Defense Advanced Research Agency (DARPA – Transparent Computing and Cyber-Hunting at Scale)
- Threat hunting language and runtime
- Threat hunting hypothesis development
- Open-source language
- Simplifies hunting and sharing

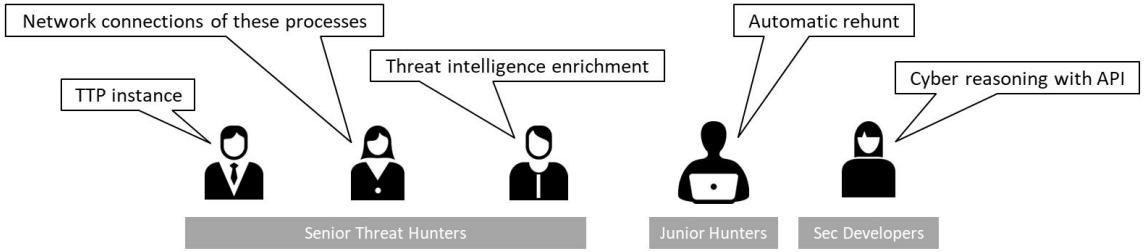
https://opencybersecurityalliance.org/
https://www.darpa.mil/program/transparent-computing
https://www.darpa.mil/program/cyber-hunting-at-scale

Hunt Fast

What does it mean by hunt fast? **ALL OF THESE TIE TO CROWD HUNTING!**

- Do NOT write the same TTP (Tactic, Technique, Procedure) pattern in **different** data source queries.
- Do NOT write **one-time-use** adapters to connect hunt steps.
- Do NOT **waste** your existing analytic scripts/programs in future hunts.
- Do construct your hunt-flow from smaller **reuseable** hunt-flow.
- Do **share** your huntbook with your future self and your colleagues.
- Do get interactive feedback and **revise** hunt-flow on the fly.

Kestrel Language and Runtime

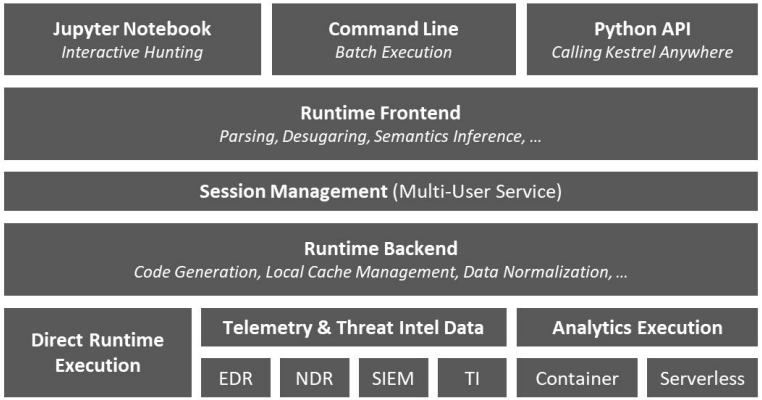


Hunters talk

WHAT

to hunt

in Kestrel



Kestrel runtime

figures out

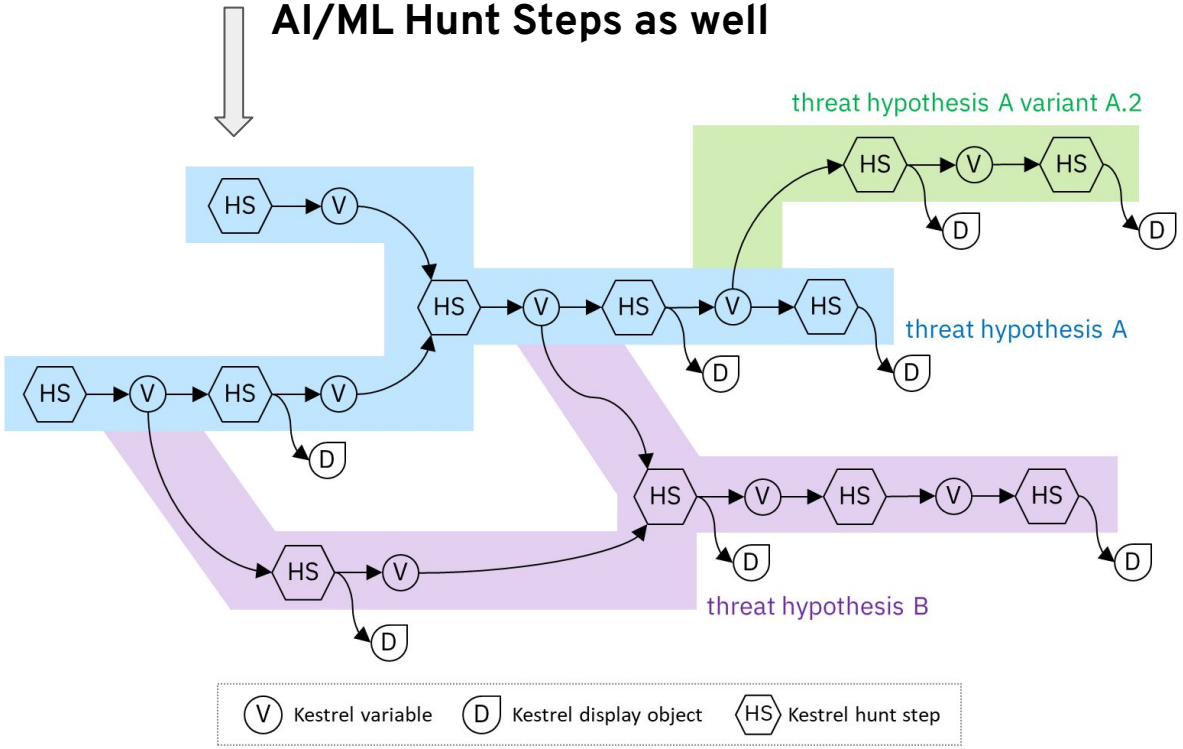
HOW

to hunt

for hunters

Key Concepts and Terminology

- Entity-Based Reasoning
- Composable Hunt Flow
  - Fork
  - Merge
- Record
- Entity
- Hunt
- Hunt Step
  - Retrieval
  - Transformation
  - Enrichment
  - Inspection
  - Flow-Control
  - AI/ML
- Hunt Flow
- Huntbook



KaaS Components

- Docker File
- OpenC2
- STIX-Shifter
- Jupyter/Jupyterhub – SaaS
- Kubernetes - PaaS
  - Minikube
  - Full cluster
  - Openshift/AI
- Infrastructure - IaaS
  - Ubuntu and Red Hat OS
  - Vagrant/Virtualbox
  - Baremetal
  - Cloud
- Ansible Core - Automation
- Keycloak – External Authentication
- Kestrel-lang

Development and Deployment

DEPLOYMENT

Developer Environment Deployment Tested Environments for Individual Threat Hunters

podman desktop

podman

docker

Test Collaborative Environment Deployment Tested Environment for a Small Team of Threat Hunters

HELM minikube

Production Collaborative Environment Deployment Tested Environment for a Enterprise Team of Threat Hunters

kubernetes

RED HAT OPENSHIFT

Red Hat OpenShift AI

DEVELOPMENT

Source Repositories

GitHub

OPEN CYBERSECURITY ALLIANCE

opencybersecurityalliance / **kestrel-as-a-service**

opencybersecurityalliance / **kestrel-lang**

opencybersecurityalliance / **kestrel-analytics**

opencybersecurityalliance / **kestrel-huntbook**

Image Repositories

docker hub

kpeeples/kaas-baseline

By kpeeples · Updated about 1 month ago

Kestrel as a Service (KaaS) container

IMAGE

DATA SCIENCE

Ubuntu Based - base-notebook

kpeeples/kaas-openshift ☆0

By kpeeples · Updated 19 days ago

IMAGE

RHEL Based - generic-datascience

SECURITY BSides CHARLESTON, SC

Container Deployment

From the command line from Fedora Workstation 38 using Podman (similar with docker):

1. Run *podman run -d -p 8888:8888 kpeeples/kaas-baseline:latest,* select docker.io for registry
2. Run *podman ps*
3. Run *podman exec -it <containerid> /bin/bash*
4. Run *jupyter server list* gives the token to copy to sign on
5. Browse to http://localhost:8888 and enter token

From the UI in Fedora Workstation 38 or Windows 11 using Podman Desktop:

1. In settings and registries add the credentials for Dockerhub
2. In images click pull image and pull the *kpeeples/kaas-baseline:latest* image
3. Start the KaaS container
4. From the terminal tab for the container get the token as from above
5. Browse to http://localhost:8888 and enter token

Minikube Deployment

Step	Manual or Auto	Description
1	Manual, Infrastructure	Install Vagrant from https://developer.hashicorp.com/vagrant/downloads
2	Manual, Infrastructure	Install Virtualbox from https://www.virtualbox.org/wiki/Downloads
3	Manual	Install git from https://github.com/git-guides/install-git
4	Manual	Clone the repo using **git clone https://github.com/opencybersecurityalliance/kestrel-as-a-service**
5	Auto, Infrastructure	Create the virtual machines by running **vagrant up** from the deployment scripts folder.
6	Manual	Connect to the Ansible Controller. Our controller example uses a f38 box, which is hosted on Vagrant Cloud. Our example uses a VM for minikube on RHEL. From the deployment scripts folder run the **~/deployment-scripts/controller-setup** script. A delay will occur with the setup controller script as it tries to copy the ssh keys and will need to timeout on the ssh copy. When vagrant up is used it downloads the box from https://app.vagrantup.com/kestrel-deployment/boxes/controller-f38
7	Auto, Platform	Deploy Kubernetes, supporting projects and KaaS by running the **~/deployment-scripts/deploy-minikube.sh** script.
8	Manual	Browse to the Kubernetes dashboard and KaaS dashboard. Make sure your firewall doesn't block the ports. • http://192.168.50.9:30080 for the jupyterhub console • http://192.168.50.9:30081 for the kubernetes console • Tutorial - https://github.com/opencybersecurityalliance/kestrel-huntbook/tree/main/tutorial

AI Integration

- Why should you use AI to enhance your hunt flows?
- AI in Kestrel analytics
  - Kestrel analytics is a type of hunt step that provides foreign language interfaces to non-Kestrel hunting module to apply any external logic like ML detection, TI enrichment, and visualization.
  - Previous work: Graph Learning-based Lateral Movement Detection, K-means clustering
  - See kestrel-analytics repository

Example: ranking suspicious processes

Example notebook: OpenAI suspicious processes ranking

[1]:
```
ps = GET process
     FROM https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/defense_evasion/host/cmd_mshta_vbscript_execute_psh.zip
     WHERE [process:binary_ref.name IN ('cmd.exe', 'powershell.exe') AND process:parent_ref.binary_ref.name != 'explorer.exe']
```

Block Executed in 2 seconds

VARIABLE	TYPE	#(ENTITIES)	#(RECORDS)	artifact*	directory*	file*	process*	user-account*	windows-registry-key*	x-oca-asset*	x-oca-event*
ps	process	1	515	516	620	622	519	4	398	516	516

*Number of related records cached.

[8]:
```
APPLY python://openai-suspicious-processes ON ps
```

Prompt: The following dataframe contains information about different processes running on a system: pid ... type 0 9572 ... process [1 rows x 37 columns]. Rank those processes by suspiciousness and give an explanation for the top 10. Focus on the `name` and `command_line` attributes of the processes.

Answer: To rank the processes by suspiciousness based on the `name` and `command_line` attributes, we need to look for any indicators of malicious activity or anomalies. Here are the top 10 processes ranked by suspiciousness: 1. powershell.exe - Suspiciousness: High - Explanation: PowerShell is commonly used by attackers to execute malicious commands or scripts. The command line includes a command to retrieve information about system services, which could be used for reconnaissance. 2. mshta.exe - Suspiciousness: High - Explanation: MSHTA can be used to execute malicious scripts or commands, and the command line includes a VBScript command to run PowerShell with no exit, indicating possible malicious activity. 3. svchost.exe - Suspiciousness: Medium - Explanation: Svchost is a legitimate Windows process, but it is commonly abused by malware to hide malicious activity. Further analysis of the command line is needed to determine if it is legitimate. 4. explorer.exe - Suspiciousness: Medium - Explanation: Explorer is a common process in Windows, but it can also be used by malware to perform malicious activities. Check the command line for any unusual behavior. 5. cmd.exe - Suspiciousness: Medium - Explanation: Command Prompt can be used by attackers to execute commands on the system. Check the command line for any suspicious or unusual commands being run. 6. conhost.exe - Suspiciousness: Low - Explanation: Conhost is a legitimate Windows process that is used to host console windows. It is less likely to be used for malicious purposes, but further analysis of the command line is recommended. 7. notepad.exe - Suspiciousness: Low - Explanation: Notepad is a legitimate Windows application, but it can be used by attackers to hide malicious code. Check the command line for any unusual behavior. 8. regsvr32.exe - Suspiciousness: Low - Explanation: Regsvr32 is a legitimate Windows program used to register and unregister DLLs. However, it can also be abused by attackers to execute malicious scripts. Verify the command line for any suspicious activity. 9. wscript.exe - Suspiciousness: Low - Explanation: Wscript is a legitimate Windows scripting host, but it can be used by malware to run malicious scripts. Check the command line for any suspicious scripts being executed. 10. taskmgr.exe - Suspiciousness: Low - Explanation: Task Manager is a legitimate Windows utility, but it can be used by attackers to monitor system activity or kill processes. Verify the command line for any unusual behavior.

[ ]:

Example: ranking suspicious processes

analytics.py

```
#!/usr/bin/env python3

import os
import pandas as pd

from openai import OpenAI


OPENAI_MODEL = "gpt-3.5-turbo"

PROMPT = """
    The following dataframe contains information about different processes running on a system: {}.
    Rank those processes by suspicioussness and give an explanation for the top 10.
    Focus on the `name` and `command_line` attributes of the processes.
    """
```

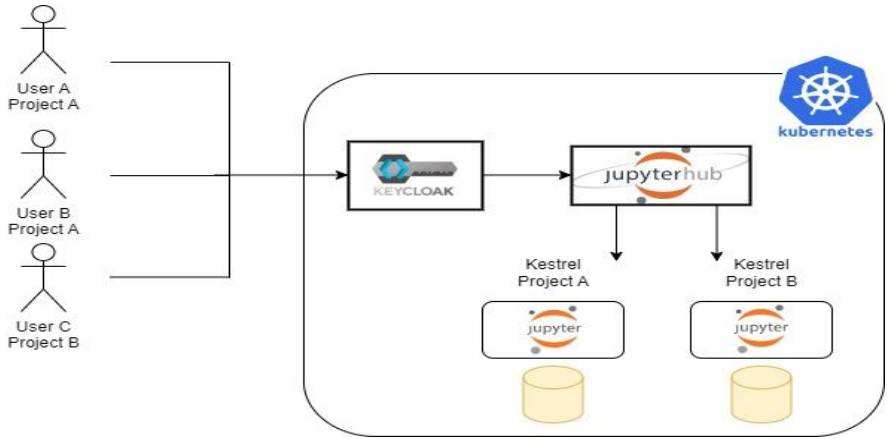
Example: ranking suspicious processes

```
client = OpenAI(
        api_key=os.environ.get("OPENAI_API_KEY"),
    )


def analytics(df):
    """
    Given a prompt and process information in the dataframe,
    rank the processes by suspiciousness and give an explanation
    for the top 10 suspicious processes.
    """

    complete_prompt = PROMPT.format(df.to_json())

    chat_completion = client.chat.completions.create(
        messages=[
            {
                "role": "user",
                "content": complete_prompt,
            }
        ],
        model=OPENAI_MODEL,
    )

    display = (
                f"<p><b>Prompt:</b> {PROMPT.format(df)} </p>"
                f"<p><b>Answer:</b> {chat_completion.choices[0].message.content}</p>"
              )

    return df, display
```

A look into the future

- Enhance analytics with an interface that allows more user flexibility for prompts
- Automatically initiate a hunt from an Indicator of Behavior (IoB)
- Provide an autocomplete feature for the Kestrel language

Get Involved



Everyone is welcome to participate in the Open Cybersecurity Alliance.

- Individuals can make technical contributions to OCA repositories via GitHub.
- Organizations can become OCA Sponsors. Gain a seat on the OCA Project Governance Board.
- Receive special recognition and promotional benefits .

Contact communications@oasis-open.org for more info

Join the Slack Channel and get involved!

Visit the website opencybersecurityalliance.org

SECURITY sides CHARLESTON, SC

Demo Time

- Repos in Git and Dockerhub
  - https://github.com/opencybersecurityalliance
  - https://github.com/OTRF/Security-Datasets/tree/master/datasets/atomic/windows/defense_evasion/host
  - https://hub.docker.com/r/kpeeples/kaas-openshift
  - https://hub.docker.com/r/kpeeples/kaas-baseline
- Podman (Developer Hunting)
- Openshift (Team Threat Hunting)

SECURITY bsides CHARLESTON, SC