

Scale Team Threat Hunting with Kestrel as a Service

Collaborate on Threat Hunting on a Container Environment



Kenneth Peeples

Principal Cybersecurity Architect

kpeeples@redhat.com | kenneth.peeples@outlook.com | 843.754.6248



Agenda



- ❖ Speaker Introductions
 - Kenneth Peeples, Principal Cybersecurity Architect
- ❖ Kestrel as a Service
 - Presentation
 - Overview of Research and Concepts
 - Components
 - Try it
 - Minikube Deployment
 - Simple Tutorial
 - Summing it up
- ❖ References

<https://www.securewv.org/eventer/kenneth-peeples-scale-team-threat-hunting-with-kestrel-as-a-service/edate/2023-10-21/>

The Abstract

“...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>

Threat hunting can be slow and tedious due to the manual steps required. Kestrel is an open-source project that provides a language for humans to express what to hunt and a machine interpreter that deals with how to hunt. Although Kestrel improves the time to detect, there are limitations to team capabilities in threat hunting tools and standards. The power of team threat hunting may be able to remove the limitations, therefore, increasing the MTTD, achieved by combining Kestrel with JupyterHub hunts with Kestrel huntbooks in order to be persistent and shared by team members.

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

Speaker Introduction



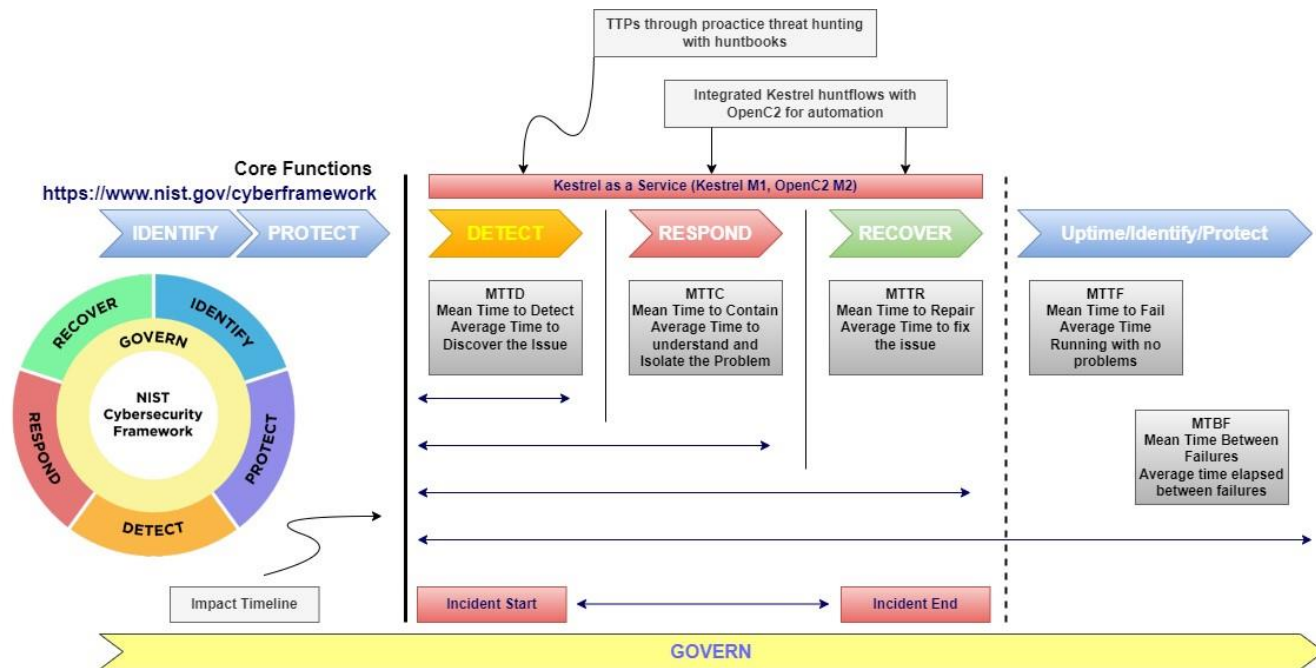
www.linkedin.com/in/kennethpeeples



<https://www.nist.gov/cybersecurity/cybersecurity-awareness-month/events/theme-days-october-2023>



Research and Project Overview



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

KaaS Components

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

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

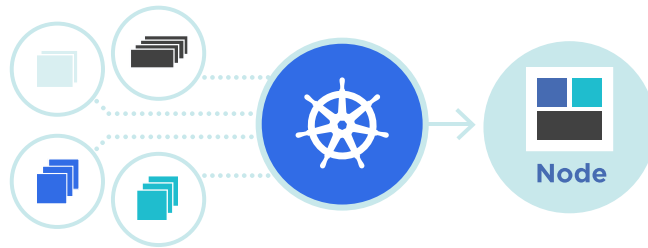
<https://opencybersecurityalliance.org/>

<https://www.darpa.mil/program/transparent-computing>

<https://www.darpa.mil/program/cyber-hunting-at-scale>

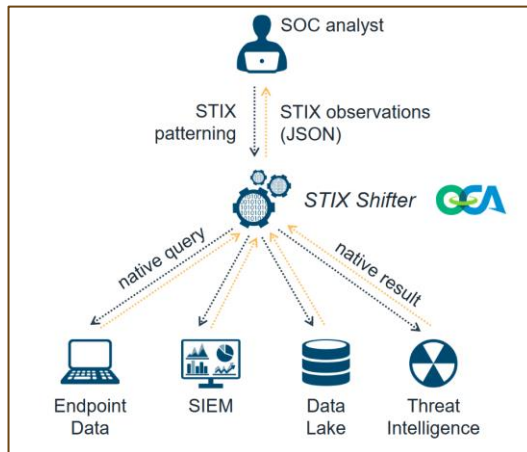
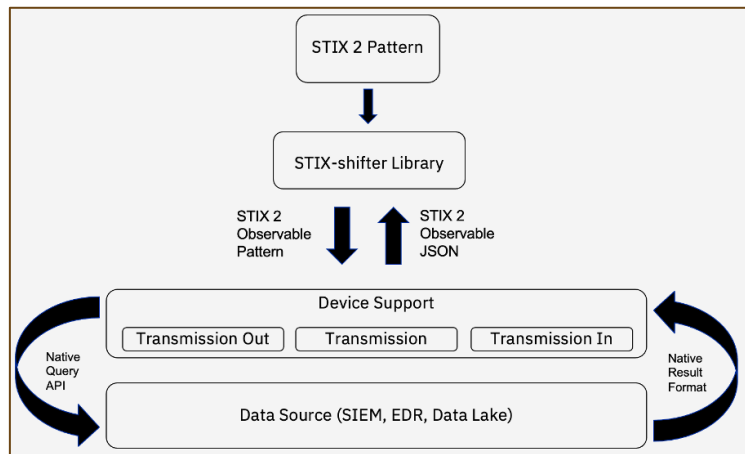
Kubernetes – k8s

Kubernetes - open-source system for automating deployment, scaling, and management of containerized applications.



STIX-Shifter

A federated search engine



Supported Connectors:

- IBM Qradar
- Elasticsearch ECS
- IBM Cloud Security Advisor
- IBM Guardium
- Splunk Enterprise Security
- Carbon Black Response
- Carbon Black Cloud
- Microsoft Defender ATP
- Microsoft Azure Sentinel
- AWS CloudWatch Logs
- Amazon Athena
- HCL BigFix
- Alertflex
- Micro Focus ArcSight

JupyterHub is made up of four subsystems:

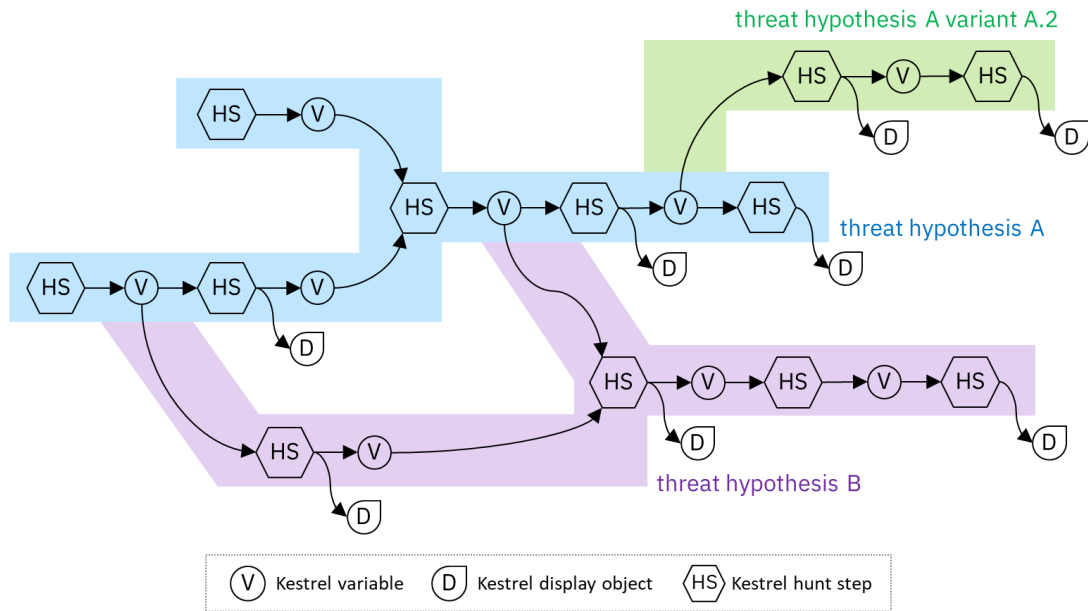
- a Hub (tornado process) that is the heart of JupyterHub
- a configurable http proxy (node-http-proxy) that receives the requests from the client's browser
- multiple single-user Jupyter notebook servers (Python/IPython/tornado) that are monitored by Spawners
- an authentication class that manages how users can access the system

Terminology

- Record
- Entity
- Hunt
- Hunt Step
 - Retrieval
 - Transformation
 - Enrichment
 - Inspection
 - Flow-Control
- Hunt Flow
- Huntbook

Key Concepts

- Entity-Based Reasoning
- Composable Hunt Flow
 - Fork
 - Merge



Hunt Fast

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

- Do NOT write the same TTP 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

A threat hunting language for a human to express **what to hunt**.

- expressing the knowledge of what in patterns, analytics, and hunt flows.
- composing reusable hunting flows from individual hunting steps.
- reasoning with human-friendly entity-based data representation abstraction.
- thinking across heterogeneous data and threat intelligence sources.
- applying existing public and proprietary detection logic as analytic hunt steps.
- reusing and sharing individual hunting steps, hunt-flow, and entire huntbooks.

Kestrel Runtime

A machine interpreter that deals with **how to hunt**.

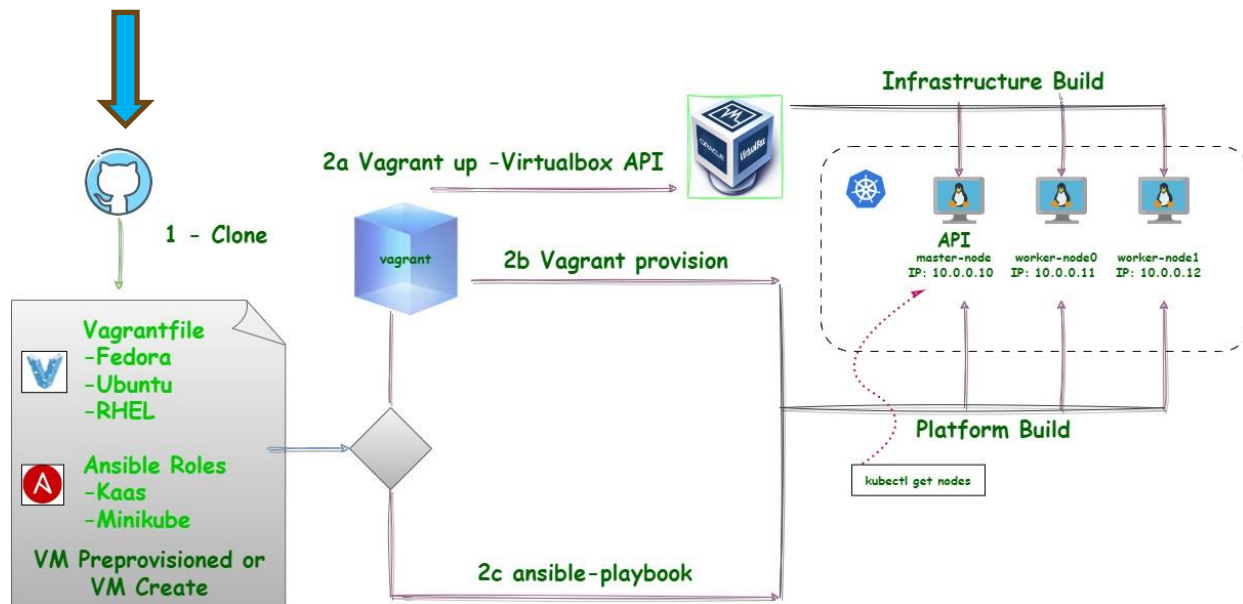
- compiling the what against specific hunting platform instructions.
- executing the compiled code locally and remotely.
- assembling raw logs and records into entities for entity-based reasoning.
- caching intermediate data and related records for fast response.
- prefetching related logs and records for link construction between entities.
- defining extensible interfaces for data sources and analytics execution.

Try it out

High level deployment – New or Existing Infra



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



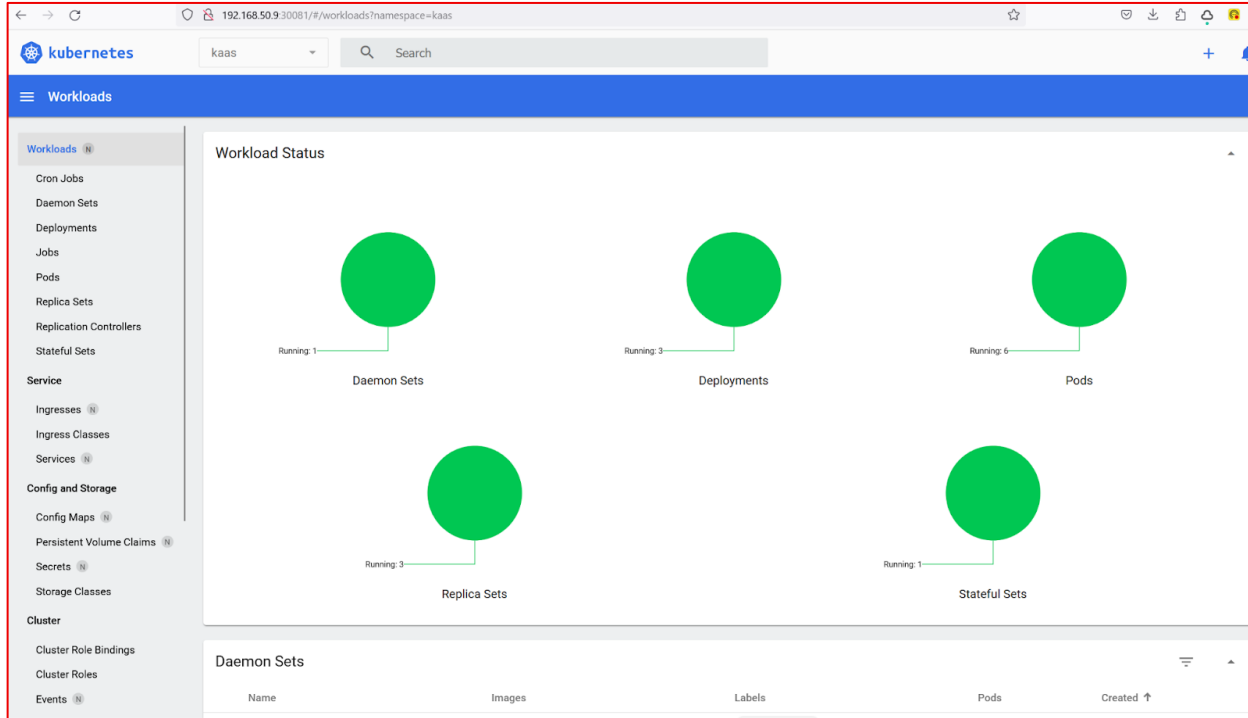
Keep in Mind

- A [no-cost red hat developer subscription](#) can be used when Red Hat Enterprise Linux (RHEL) is preferred as the developer account includes up to 16 systems.
- VSCode and code Walk through
- Dockerfile and Dockerhub
- Vagrant and vagrantbox
- Inventory and vagrantfile customization
- Full production cluster installation (NFS, Control-plane and workers)

The Developer Deployment - Minikube

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. <ul style="list-style-type: none">•http://192.168.50.9:30080 for the jupyterhub console•http://192.168.50.9:30081 for the kubernetes console

Container Platform



KaaS

jupyterhub

HomeToken

kpeeplesLogout

Server Options

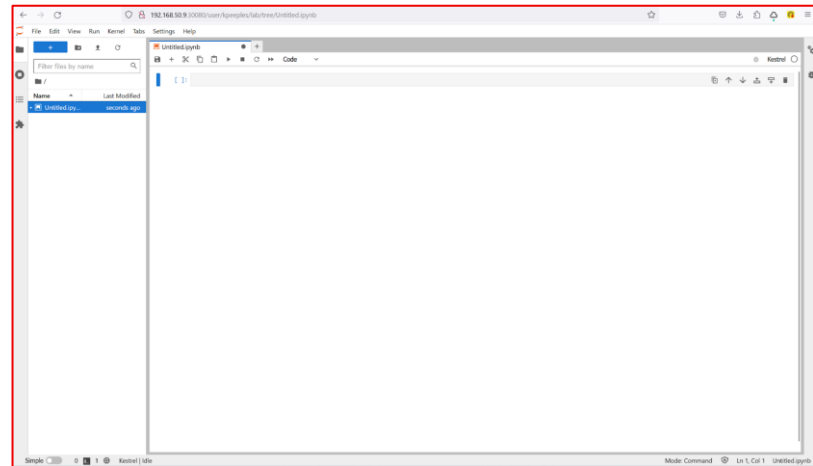
☒ Minimal environment

To avoid too much bells and whistles: Python.

☐ Kestrel Threat Hunting

Threat Hunting in Kube

Start



KaaS – Hello World

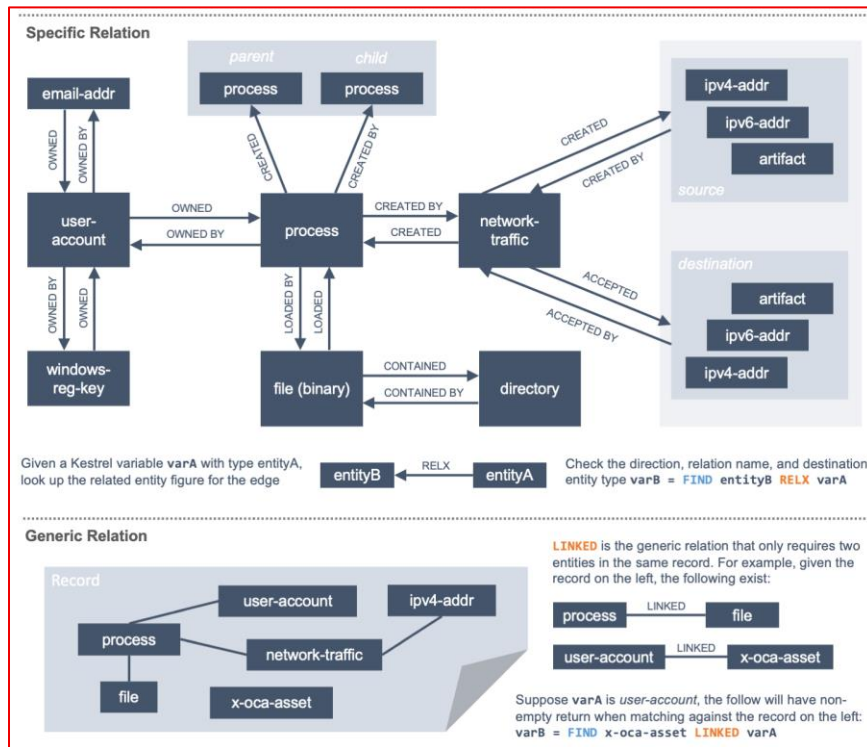
```
# create four process entities in Kestrel and store them in the variable
`proclist`
proclist = NEW process [ {"name": "cmd.exe", "pid": "123"}
                          , {"name": "explorer.exe", "pid": "99"}
                          , {"name": "firefox.exe", "pid": "201"}
                          , {"name": "chrome.exe", "pid": "205"}
                          ]

# match a pattern of browser processes, and put the matched entities in
variable `browsers`
browsers = GET process FROM proclist WHERE name IN ('firefox.exe',
'chrome.exe')

# display the information (attributes name, pid) of the entities in variable
`browsers`
DISP browsers ATTR name, pid
```


KaaS – Finding Connected Entities

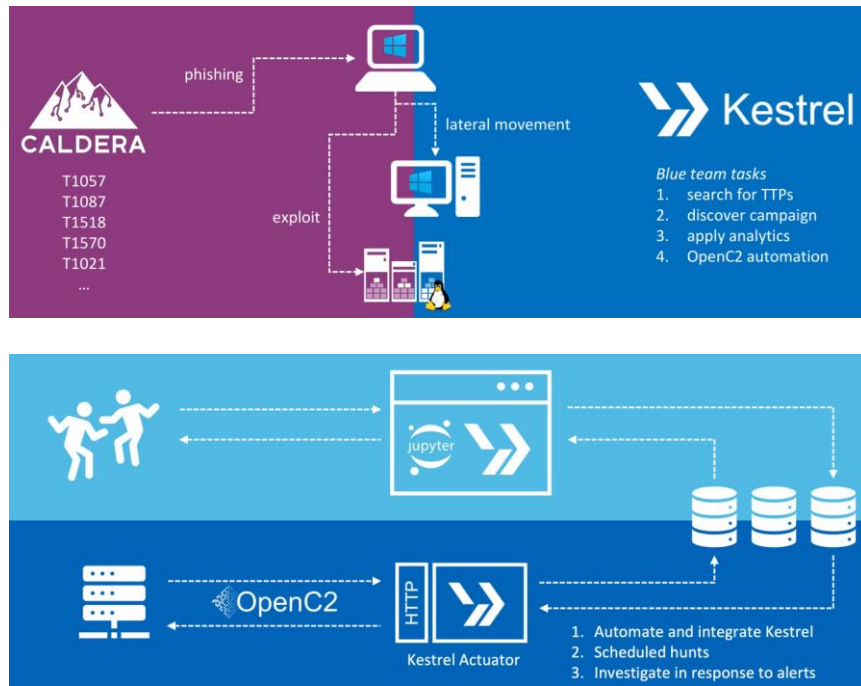
Given a list of processes, how to find their parent process? How to find their opened network connections? How to find files read/written by them?



KaaS – More Complex Example

A powerful federated data retrieval using the Structured Threat Information eXpression (STIX) standard and STIX-shifter and lift the results into an entity-relational data model. Then we will showcase analytic hunt steps besides data retrieval steps, compare the new Python analytics interface with the container-based interface, and execute analytics for context enrichment, de-obfuscation, and visualization. After creating, executing, saving, and re-executing huntbooks, we will connect Kestrel with the Open Command and Control (OpenC2) standard to respond to "investigate" commands and automate huntbook execution, data gathering, false positive elimination, and comprehensive analysis.

<https://www.youtube.com/watch?v=tf1VLpFefs>

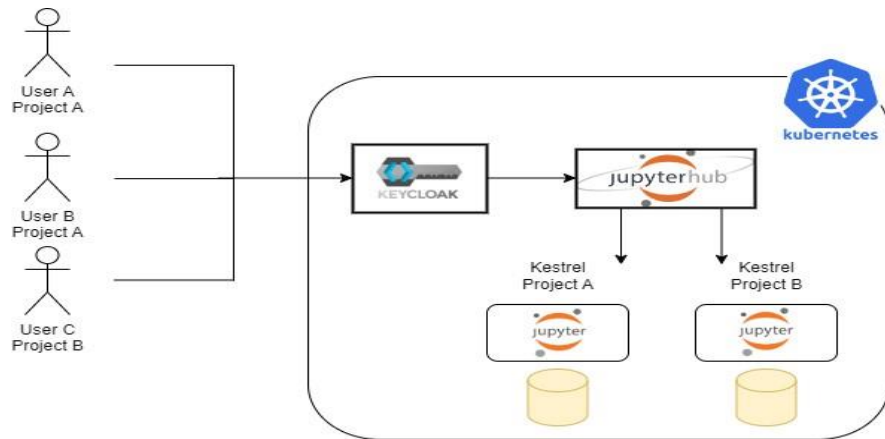


What's Next and Summary

Next Milestones

- Collaboration settings in the repository for automation
- Keycloak settings in the repository for automation
- Openshift deployment in the repository for a separation automation deployment
- Platform security Hardening through compliance as code
- Additional Community Huntbooks for multiple examples

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

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

 linkedin.com/company/red-hat

 youtube.com/user/RedHatVideos

 facebook.com/redhatinc

 twitter.com/RedHat

References

References

- ▶ Kubernetes Hardening Guide - <https://www.cisa.gov/uscert/ncas/current-activity/2022/03/15/updated-kubernetes-hardening-guide>
- ▶ Red Hat Openshift Security Guide - <https://www.redhat.com/en/resources/openshift-security-guide-ebook>

Deeper Dives

Holistic security dashboard for a next talk

