# Kestrel

## Overview

Kestrel is a cyberthreat hunting language and runtime developed under the Open Cybersecurity Alliance (OCA) project.  It provides an abstraction for threat hunters to focus on the high-value and composable threat hypothesis development instead of specific realization of hypothesis testing with heterogeneous data sources, threat intelligence, and public or proprietary analytics.  It is composed of Python for the most part and can be hosted in Jupyter Notebook.

## Goal

The purpose of Kestrel is to make cyber threat hunting fast by providing a layer of abstraction to build reusable, composable, and shareable hunt-flow, following the “Do Not Repeat Yourself” guidelines. The runtime aims to cover the “how to hunt” aspect so humans can focus on “what to hunt” (the language), maximizing the strengths of both sides. Eventually, the hope is to train AI to the point where it can look for “what to hunt” on its own, but that is a milestone far off in the future.

## Current Team Members

| | | | | |
|---|---|---|---|---|
| **Xiaokui Shu** | *Megan Huang* | *David Coletta* | Jaisal Patel | Joshua Kloepfer |
| **Xiaokui.Shu@ibm.com** | *huangm11* | *coletd* | patelj8 | kloepj2 |

(Key: **External Project Lead**; *students taking RCOS for credit*)

## Milestones

September: Get familiar with Kestrel

- Read main site documentation for background (Assigned Reading)
- Go through Kestrel’s interactive tutorial
  - Basic terminology + data parsing
  - How to make, fork, and merge hunt flows
  - **Kestrel Analytics tutorial** (for later reference)
- Learn about how to contribute
  - Making hunt flows + demos
  - Frontend/backend code development
- Watch Black Hat demo recording (Red Team Tool: Caldera)
- Tinker with Black Hat hunting lab
- (Optional) Setup the runtime environment locally

October: Start contributing

- Work on Hacktober Issues of choice in pairs
- Independent work on other issues
- Learn about analytics of the MSTI interface
- Consider working on designing hunt flows

November: Work on bigger projects as a team

- ➢ Start working on major task(s) in MSTI analytics as a team
- ➢ Merging MSTI analytics into Kestrel documentation

December:

- ➢ TBD (schedule may be postponed as needed)

## Useful Resources

Documentation

Kestrel Runtime API – Python Analytics Interface
Language Specification – Data Sources and Analytics Interfaces
Kestrel Slides (Project Pitches)

---

Github Repositories

Kestrel Analytics
Analytics – Data Exfiltration Modeling
Kestrel Huntbook Github
Kestrel Jupyter
Kestrel Language

---

InfoSec Jupyterthon 2021 Kestrel Demo
Pentester – Looking at a defense from an attacker's perspective?

---

Cybersecurity – Hacking Training

Try Hack Me
Hack the Box
RPI SEC Fairgame (Intro CTF) – RPI SEC Tools + Main Website