black hat®
ARSENAL 2022

AUGUST 10-11

MANDALAY BAY / LAS VEGAS

#BHUSA @BlackHatEvents

black hat ARSENAL 2022

Streamlining and Automating Threat Hunting With Kestrel

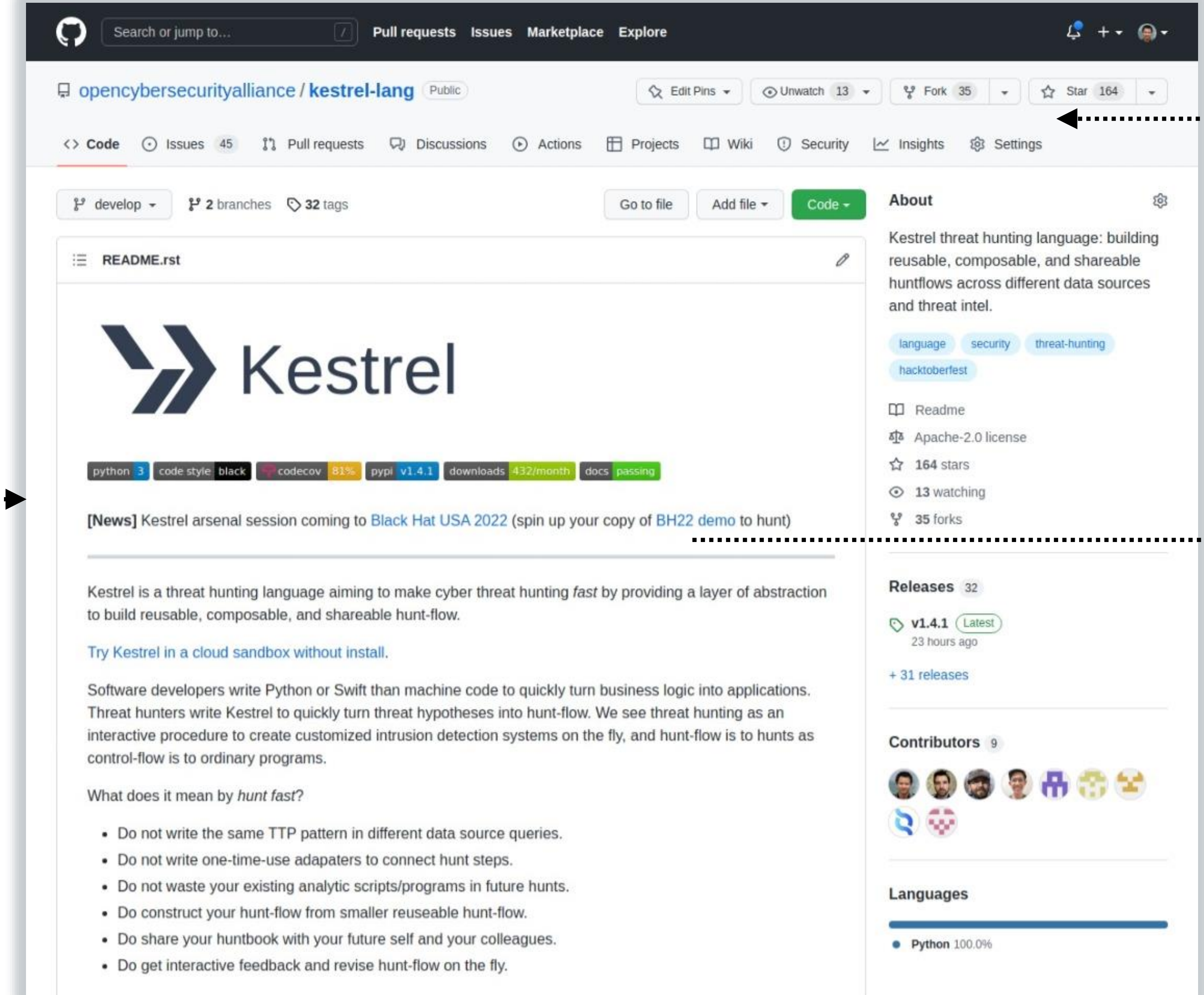
Xiaokui Shu, Paul Coccoli, Ian Molloy, Jiyong Jang

IBM Research & IBM Security

https://github.com/opencybersecurityalliance/kestrel-lang

3. star us

1. search *kestrel lang*



opencybersecurityalliance / **kestrel-lang** Public

2 branches 32 tags

README.rst

Kestrel

[News] Kestrel arsenal session coming to Black Hat USA 2022 (spin up your copy of BH22 demo to hunt)

Kestrel is a threat hunting language aiming to make cyber threat hunting *fast* by providing a layer of abstraction to build reusable, composable, and shareable hunt-flow.

Try Kestrel in a cloud sandbox without install.

Software developers write Python or Swift than machine code to quickly turn business logic into applications. Threat hunters write Kestrel to quickly turn threat hypotheses into hunt-flow. We see threat hunting as an interactive procedure to create customized intrusion detection systems on the fly, and hunt-flow is to hunts as control-flow is to ordinary programs.

What does it mean by *hunt fast*?

- Do not write the same TTP pattern in different data source queries.
- Do not write one-time-use adapaters 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.

About

Kestrel threat hunting language: building reusable, composable, and shareable huntflows across different data sources and threat intel.

language security threat-hunting hacktoberfest

Readme
Apache-2.0 license
164 stars
13 watching
35 forks

Releases 32

v1.4.1 Latest
23 hours ago

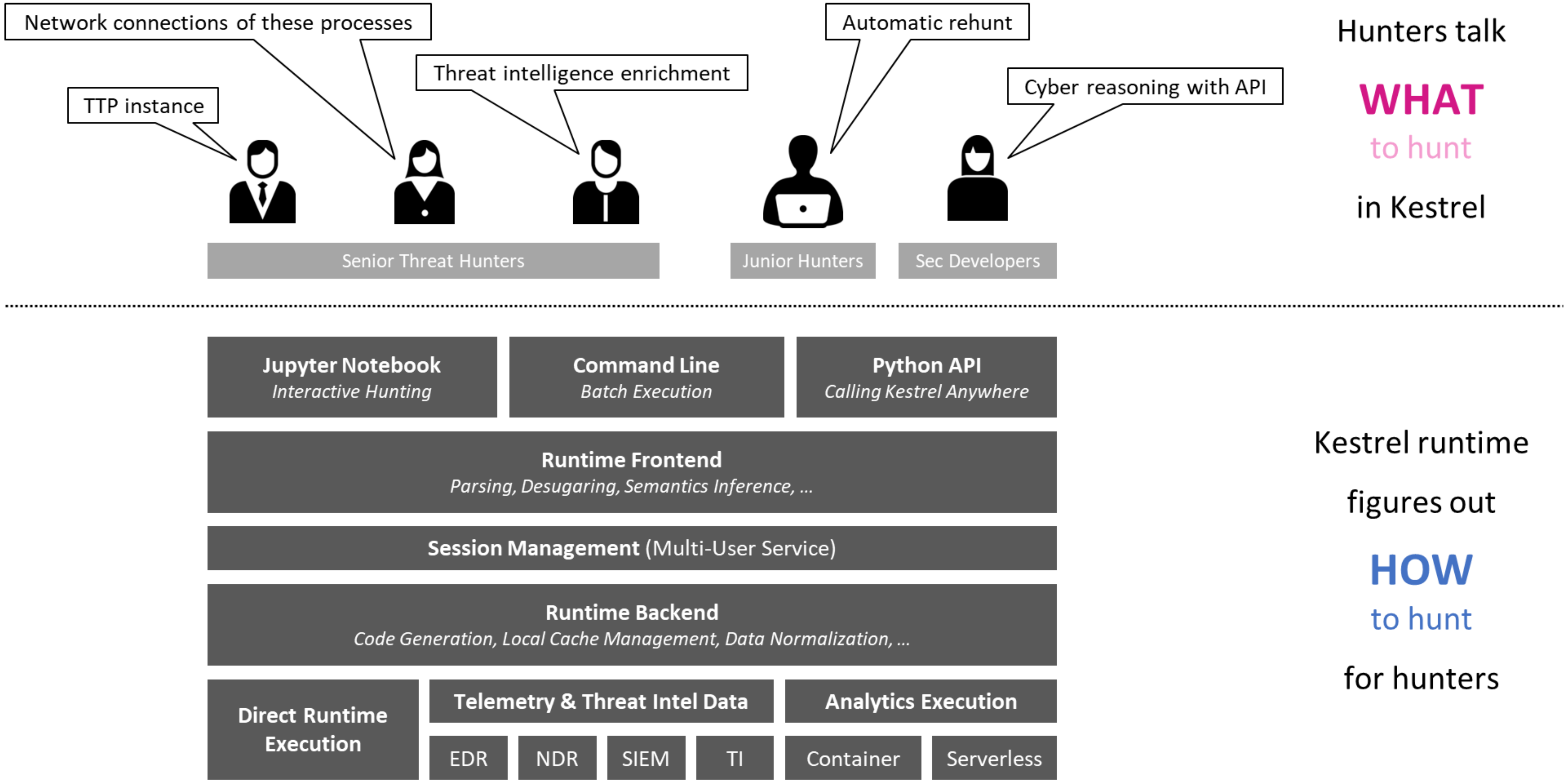
+ 31 releases

Contributors 9

Languages

Python 100.0%

2. launch your demo



TTP instance

Network connections of these processes

Threat intelligence enrichment

Automatic rehunt

Cyber reasoning with API

Senior Threat Hunters

Junior Hunters

Sec Developers

Jupyter Notebook
Interactive Hunting

Command Line
Batch Execution

Python API
Calling Kestrel Anywhere

Runtime Frontend
Parsing, Desugaring, Semantics Inference, …

Session Management (Multi-User Service)

Runtime Backend
Code Generation, Local Cache Management, Data Normalization, …

Direct Runtime Execution

Telemetry & Threat Intel Data
EDR
NDR
SIEM
TI

Analytics Execution
Container
Serverless

Hunters talk

WHAT

to hunt

in Kestrel

Kestrel runtime

figures out

HOW

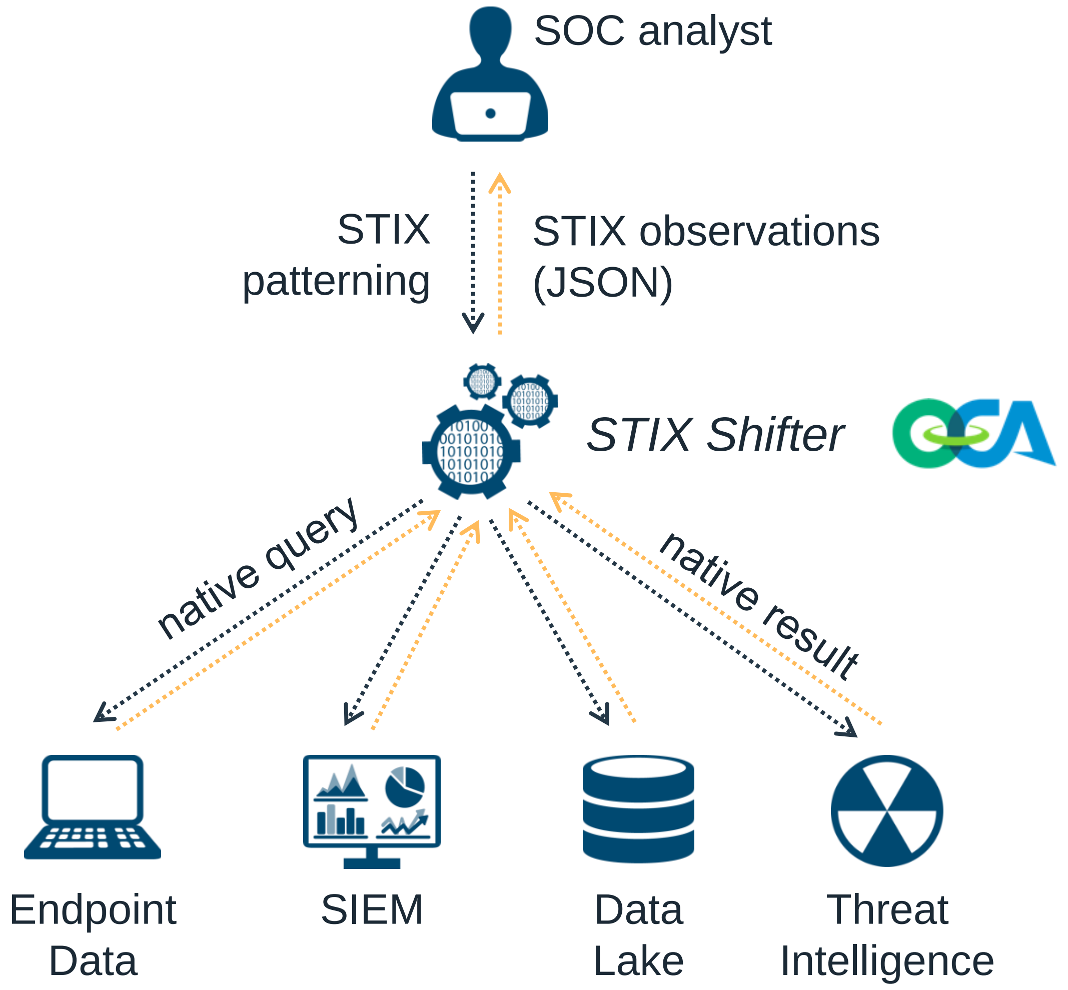
to hunt

for hunters

STIX Shifter: a federated search engine

Supported connectors:

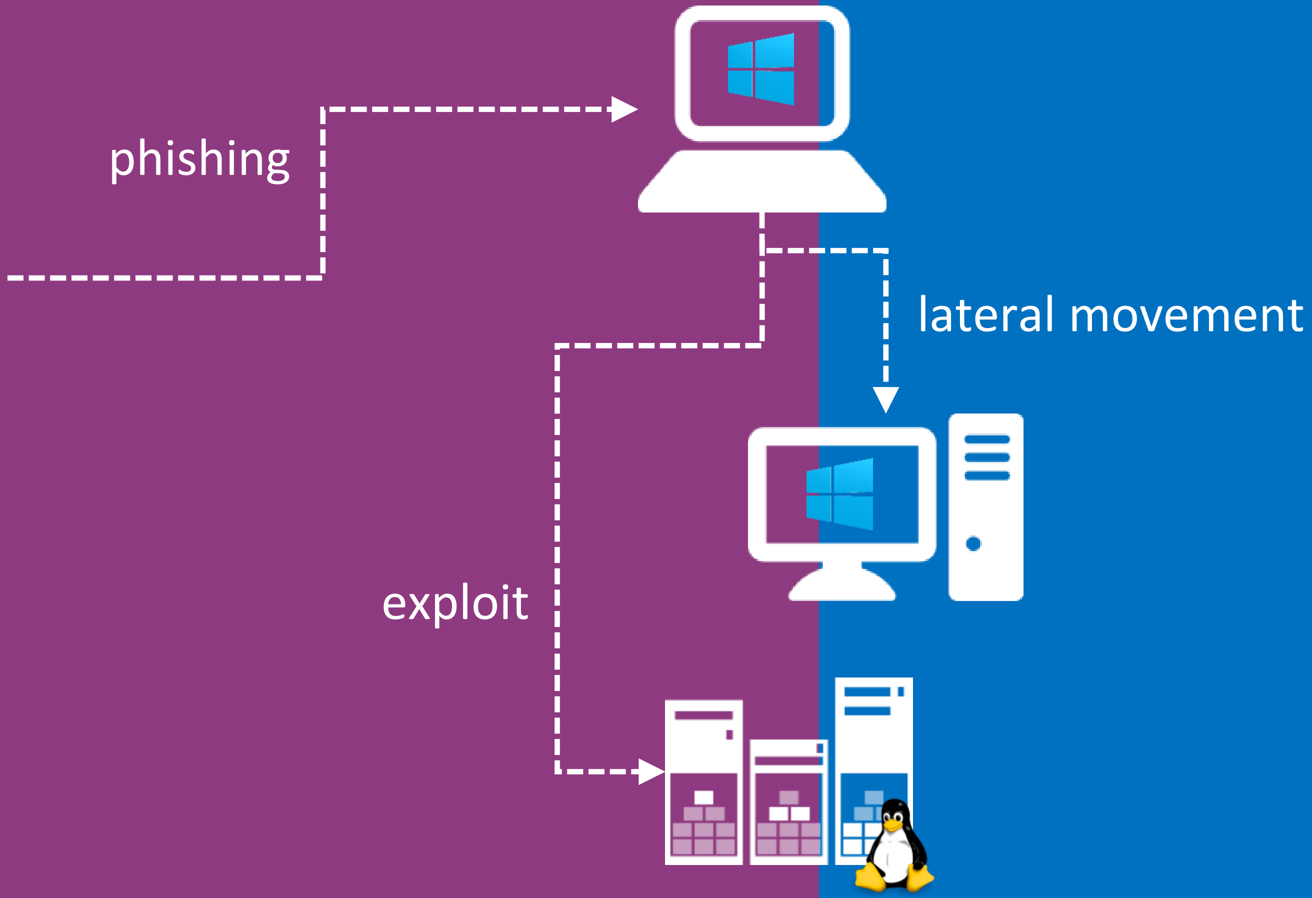
- Elasticsearch ECS
- IBM QRadar
- IBM Cloud Security Advisor
- IBM Guardium
- Splunk Enterprise Security
- Carbon Black Response
- Carbon Black Cloud
- Microsoft Defender ATP
- Microsoft Azure Sentinel
- AWS CloudWatch Logs
- Amazon Athena
- HCL BigFix
- Alertflex
- Micro Focus ArcSight



https://github.com/opencybersecurityalliance/stix-shifter

CALDERA

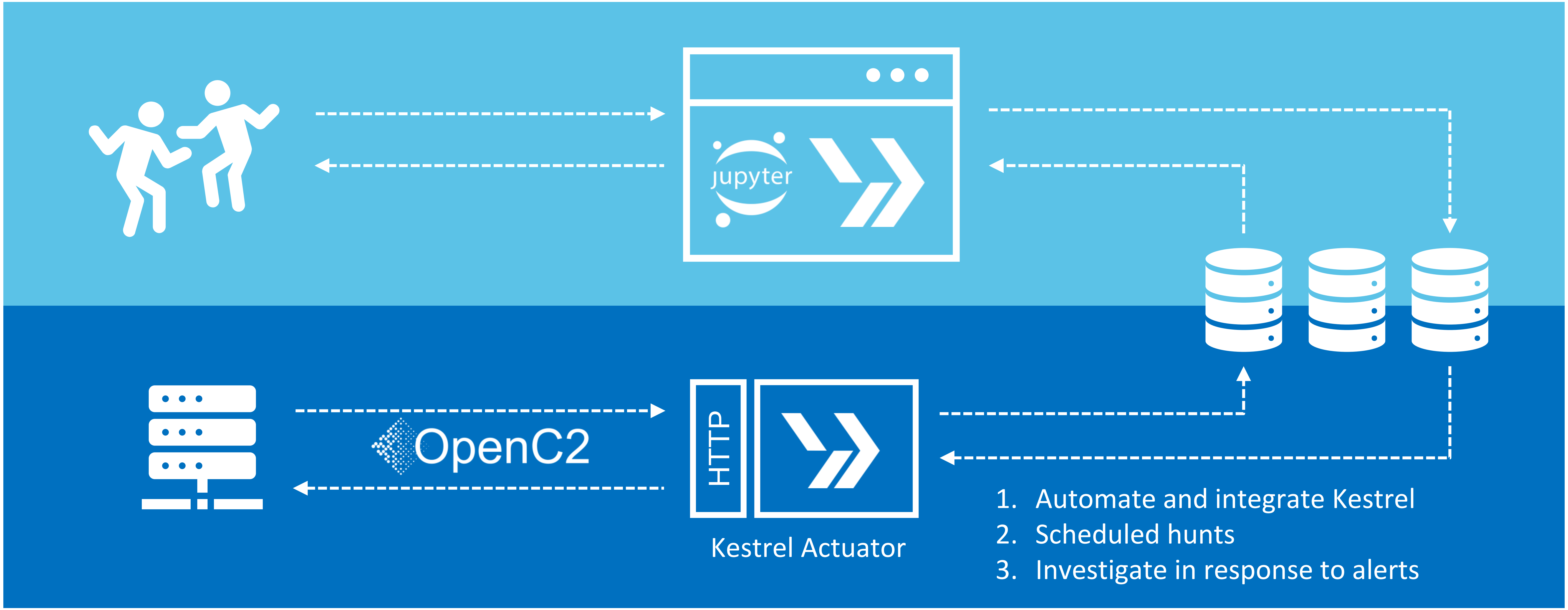
T1057
T1087
T1518
T1570
T1021
…



Kestrel

Blue team tasks

1. Search for TTPs
2. Discover campaign
3. Apply analytics
4. OpenC2 automation



1. Automate and integrate Kestrel
2. Scheduled hunts
3. Investigate in response to alerts

Thank you!

Jamie Clark
Paul Coccoli
Chet Ensign
Jiyong Jang
Jason Keirstead
Michael Le
Bill Lloyd
Scott McGrath
Ian Molloy
Claudia Rauch
Xiaokui Shu

Acknowledgement

Kestrel is an Open Cybersecurity Alliance (OCA)[1] project.

Kestrel is built upon work funded by

- DARPA Transparent Computing (TC)[2]
- DARPA Cyber Hunting at Scale (CHASE)[3]

[1] https://opencybersecurityalliance.org/
[2] https://www.darpa.mil/program/transparent-computing
[3] https://www.darpa.mil/program/cyber-hunting-at-scale