October 28, 2020

The Tale of Smokey and the Crypto Bandits

How Okteto uses Falco to keep users happy and our platform healthy

Ramiro Berrelleza

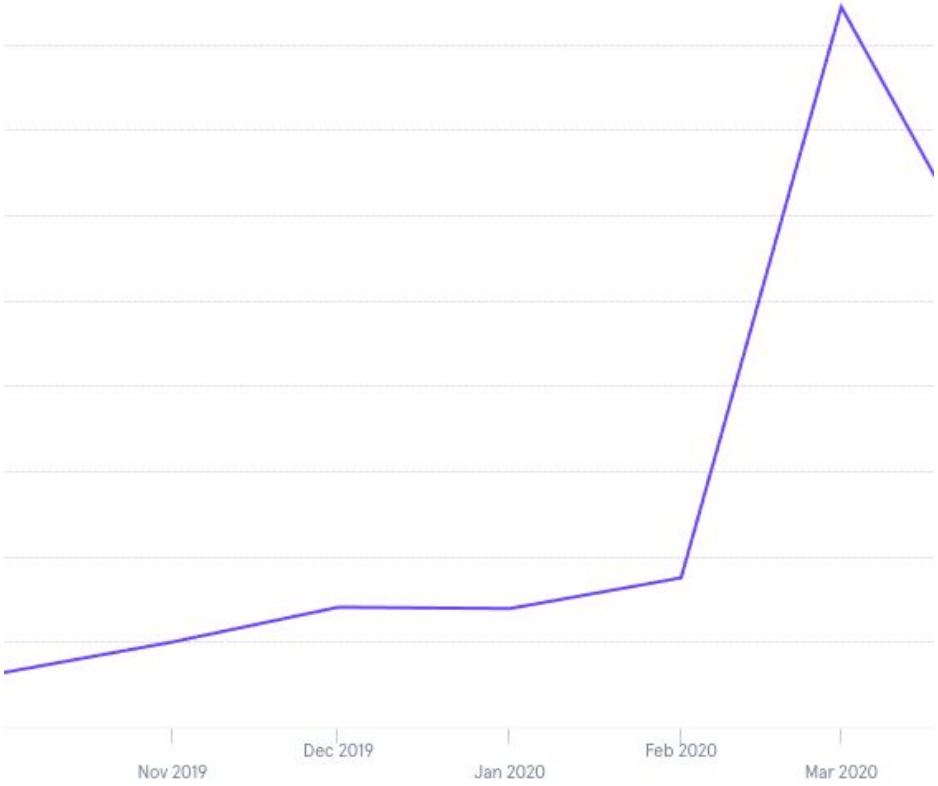
Hey everyone!

- Co-founder of Okteto
- Former architect @ Atlassian, Software Engineer @ Azure
- @rberrelleza

About Okteto

- Developer platform, powered by Kubernetes
- Go from source to deploy in one click, on any language or stack
- Every developer gets to their own k8s namespace

A few months ago...



GCP was not thrilled

Re: [#XXXXXX] Action Required: Suspicious Activity Observed on Google Cloud Project okteto-prod

Google Cloud Support <esupport@google.com>
to me,

Hi Ramiro,

Open Source to the rescue!

Attempt #1 - We were young and naive

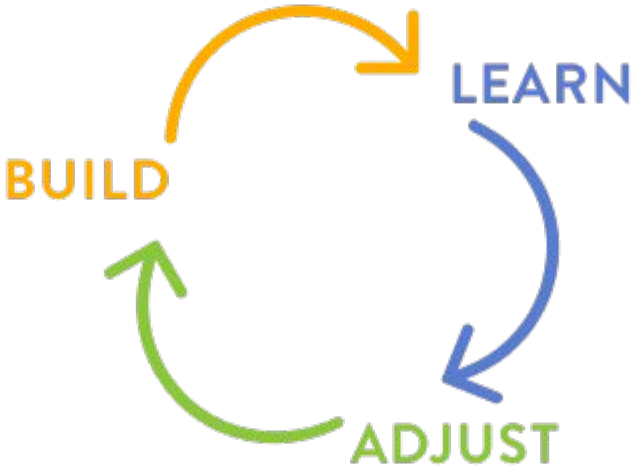
- Installed Falco in the clusters
- Configured it with the default rules plus our own
- Sent notifications to a slack channel

Attempt #1 - The result

Attempt #1 - The Postmortem

- The default falco rules are not well suited for a dev platform
- The processing overhead is non-trivial
- Falco's eBPF module + ContainerOS was not very performant

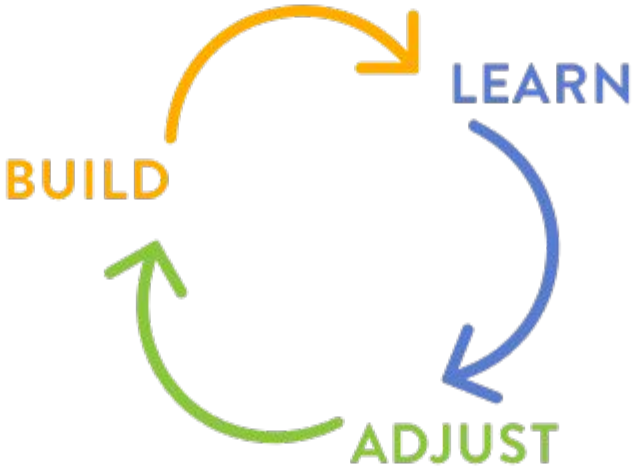
Iteration is key



Current Implementation

- Built a tool to automatically reload falco on rule changes
- Rules: monitor well known IPs, binary names, forbidden k8s actions
- Action: Notify to slack for human banhammer
- Use Ubuntu instead of ContainerOS

Iteration is key



Future Ideas

- Move back to eBPF module to reduce our OS footprint
- Smarter rules based on user behavior
- Automatically respond to malicious actions without requiring human intervention

October 28, 2020

The Tale of Smokey and the Crypto Bandits

Ramiro Berrelleza