Published on *Tux Machines* (http://www.tuxmachines.org)

Fedora, CNCF and IBM-Paid Puff Pieces

By *Roy Schestowitz*
Created *22/07/2019 - 11:13am*
Submitted by Roy Schestowitz on Monday 22nd of July 2019 11:13:45 AM Filed under Red Hat [1] Server [2]

- **Changing how we work [3]**

> As those of you who read the https://communityblog.fedoraproject.org/state-of-the-community-platform-engineering-team/ blog know, we are looking at changing workflows and organization around in the Community Platform Engineering team (of which, I am a member). So, I thought I would share a few thoughts from my perspective and hopefully enlighten the community more on why we are changing things and what that might look like.

- **Kubernetes policy project takes enterprise IT by storm [4]**

> An open source compliance as code project has gained a groundswell of popularity over the last six months among enterprise IT pros, who say it simplifies and standardizes Kubernetes policy management.
>
> The Open Policy Agent (OPA), an open source compliance as code project founded by former VMware employees, was used at Netflix as early as 2017 and accepted into the Cloud Native Computing Foundation (CNCF) as a sandbox project in March 2018. Netflix gave an OPA demonstration at KubeCon in December 2017, and Intuit and Capital One followed at KubeCon in December 2018. After the project advanced to the CNCF's incubating stage in April 2019, and was demonstrated a third time at KubeCon EU in May 2019, it began to generate mainstream buzz.
>
> [...]

> As Kubernetes environments grow to encompass Istio service mesh and Knative event-based orchestration in what Google calls the open cloud stack, the fact that OPA lends itself to Kubernetes policy enforcement but can expand to include those adjacent utilities boosts its appeal.

- **The Who, What, Where, When, and Why for Mainframe Security [5] [Ed: IBM pays Ponemon [6] for puff pieces]**

  > For most people, security is a bit of a nuisance. No-one likes having to keep updating their password and then needing to remember the new one. And then there?s all the different passwords that need to be remembered for different things. It all just seems like an administrative nightmare. It just makes getting a day?s work done harder. That?s what most users think right up until the moment there?s a breach. And suddenly the mood has changed. Now everyone wants to know exactly what?s happened. They want to know who has done what, where they?ve done it, when it occurred, how they got in, and a million other questions. Your phone is ringing off the hook. Your e-mail is filling up faster than usual. What can you do? Where can you access the information you need? How do you respond to the incident?

Red Hat Server

Source URL: http://www.tuxmachines.org/node/126137

Links:
[1] http://www.tuxmachines.org/taxonomy/term/142
[2] http://www.tuxmachines.org/taxonomy/term/147
[3] https://www.scrye.com/wordpress/nirik/2019/07/21/changing-how-we-work/
[4] https://searchitoperations.techtarget.com/news/252467102/Kubernetes-policy-project-takes-enterprise-IT-by-storm
[5] https://it.toolbox.com/blogs/trevoreddolls/the-who-what-where-when-and-why-for-mainframe-security-072119
[6] http://techrights.org/2011/07/10/ponemon-paid-for-studies/