



Refactor's New Security Integrations and Capabilities Make Automating Security Easy and Collaborative

The DevSecOps automation platform now integrates with 13 tools, notably new capabilities for security benchmarks and assessing.

SEATTLE, July 7, 2020 – Refactor, the DevSecOps automation platform enabling organizations through their next shift to IT-as-Code, announced today the immediate release of new integrations and capabilities. The new features focus primarily on security tools in response to a lag in automation solutions for security processes. So far, automation solutions are largely directed at engineering teams, but security teams benefit from DevOps methodologies around culture and automation, too.

“Today’s remote work environment is accelerating demand for software-defined everything. As a result, we have more cloud-based vulnerabilities. Now, there is a greater urgency to make security a priority in the production process,” said Mike Fraser, CEO of Refactor. “Our latest batch of features is hyper-focused on security integrations that not only prioritize the role and work of security professionals, but also enhance the level of collaboration happening across tech teams.”

New integrations and capabilities:

- **CIS-CAT Assessor:** The Center for Internet Security’s (CIS’s) CIS-CAT® configuration assessment tool can now be added directly to pipelines, enabling powerful remote scanning and reporting functionality. Both the Lite and Pro versions are supported.
- **OpenSCAP:** Built-in support for this industry-standard, open source compliance assessment tool enables users to quickly add compliance scanning and automated report generation to their pipelines.
- **Kubectrl:** Deeper integration with the Kubernetes CLI allows users to easily authenticate, deploy apps, and perform management operations on their Kubernetes clusters.
- **Self-hosted runner agent:** With the beta release of Refactor’s self-hosted runner agents, users can now execute pipeline runs on custom infrastructure or inside their own private networks. This addition opens the door to much more powerful pipelines that may require additional tools, resources, or privileged access.

“Integrating CIS-CAT with the Refactor platform increases our reach to teams eager to merge processes between engineering and security,” said Curtis Dukes, CIS Executive Vice President of Security Best Practices. “The more security becomes a part of the development process, the straighter an organization’s security posture becomes. We’re thrilled to be partnering with Refactor on realizing our common goal to automate security in our connected world.”

Refactor is helping all tech teams design and deliver complex, secure cloud infrastructure and applications through its all-in-one, visual automation platform. The DevSecOps automation platform currently integrates with AWS Cloud Formation, Azure Resource Manager, Git, Google Deployment Manager, Hashicorp Terraform, Kubernetes API, Node, Powershell, Python and Shell Scripts, Red Hat Ansible, OpenSCAP, and CIS-CAT.

Currently in contract with the United States Air Force AFWERX Small Business Innovation Research (SBIR) 20.1 Phase 1, Refactor is helping customers like the Air Force and Fortinet to

deploy virtual machines to Azure, deploy Kubernetes EKS clusters on AWS, and use Burpsuite to run web application security tests against a running web server. Refract is currently pursuing a SBIR Phase 2 contract from the United States Air Force and raising its seed round.

About Refract

Refract is a Seattle-based DevSecOps startup founded in 2017 by military veteran and industry experts in cloud and cybersecurity. Its mission is to accelerate adoption of DevSecOps methodologies among security and DevOps teams. Refract provides a simple and collaborative automation platform that enables tech teams to visually design and run modern, software-defined IT-as-Code solutions including infrastructure, configuration, integrations and security. Technology changes, people adapt. Refract innovates to make the world more agile through the next shift of digital transformation into IT-as-Code. Learn more at <https://refractr.it>

About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

###

Contact:

Steph Yeo

steph@refractr.it

866.493.9367 x804