sonatype

CUSTOMER SUCCESS STORY

Equifax Success in Security Transformation

Open Source Monitoring with Nexus Lifecycle

EQUIFAX

Equifax — Security Transformation through Sonatype Nexus

When Bryson Koehler (CTO) and Jamil Farshchi (CISO) were tasked with rebuilding the technical and security infrastructure at Equifax following the breach in 2017, their first concern was the cultural changes that would have to happen at the company before any technology solution could be considered. They needed to get the technology team and the security team aligned around the same vision. That vision encompasses 57 data centers, 64,000 items in the ITM environment, and 5500 databases in 24 countries.

The first step in reshaping the culture was to take a hard look at the team of 8500 technology professionals around the world. What they learned was that 20% of the team had a technology background, while 80% were focusing on compliance and administration. They had to remove entire teams in order to enforce new policies and let the company know they were serious about change. There was a turnover of 25% of the technology team in the first year. Now the team is composed of 79% technical professionals.

Their first concern was the cultural changes that would have to happen at the company before any technology solution could be considered. They needed to get the technology team and the security team aligned around the same vision.

"We changed the reporting lines so the security teams reported directly to the CEO. We were the first publicly traded company to institute a security metric into performance reviews for everyone," says Farshchi. Every bonus eligible employee throughout Equifax has their bonus structure based upon meeting security marks. "If you're in HR, help us with the talent. If you're in finance, make sure we have the funding to execute on our commitments. Every person has a role to play."

The new structure ensures the information security teams are embedded in the other community tribes within the company. From a day-to-day operating perspective, the lines are being erased between security and tech. It's one of the biggest cultural shifts in company.

"Security is the canary in a coal mine for a poorly operating IT organization. If there are security issues, a lot of times it stems back to poor IT and technology practices."

— JAMIL FARSHCHI, CISO, EQUIFAX

Farshchi describes the philosophy behind his approach to company wide security. "Security is the canary in a coal mine for a poorly operating IT organization. If there are security issues, a lot of times it stems back to poor IT and technology practices. When there are vulnerabilities in applications that are in production, many times it's because you're using a manual process, or you don't have security tools integrated into the CI/CD pipeline."

Site reliability engineers (SRE) are responsible for the well being of their environments. They focus on understanding the tools and the capabilities they have at their disposal. They need to confirm what they are running is being utilized to the full extent of its capabilities. 'You build it. You run it. You own it."

Using Nexus Lifecycle and Nexus Repository to support CI/CD across their open source pipeline.

The practice of managing open source libraries and frameworks was at a very low maturity and adoption stage within the organization when Koehler and Farshchi arrived in 2018. The prior team had been doing due diligence just around solving the challenges of library maintenance. With the new culture, they needed to work on a more complete and holistic approach in their thinking. The Nexus Platform, including Nexus Lifecycle and Nexus Repository, was a part of that solution set. According to Koehler, "Using the Nexus Platform now is not optional. It's a part of the solution set stack. It is part of the overall CI/CD thinking and pipeline."

Koehler talks about using the Nexus Platform to help manage and monitor the production environment. "As you move into infrastructure as code, and you follow the right discipline in cloud development, your artifact repository is your production repository. If you're really following a 'deploy and destroy' model, you should be able to absolutely know what is running in production." As part of the solution set pipeline, Equifax uses Nexus Lifecycle to monitor open source components in real time within production, including the creation of a Software Bill of Materials, generated against what is being deployed into the production environment.

"As we move into our cloud environments, we're enforcing the discipline of making sure that, if we want to know what production looks like, we should be able to look at our repository and know - from an infrastructure stack, from a library stack, from an application stack - exactly what is being deployed in production at any given time."

— BRYSON KOEHLER, CTO, EQUIFAX

"As we move into our cloud environments, we're enforcing the discipline of making sure that, if we want to know what production looks like, we should be able to look at our repository and know - from an infrastructure stack, from a library stack, from an application stack - exactly what is being deployed in production at any given time."

Using the Nexus Platform to monitor open source usage and consumption is "important for us. We don't view patching as something we do in response to a vulnerability. We view patching as something we need to do proactively." As libraries and components get updated in the open source community, Nexus Lifecycle monitors the components within production and notifies the Equifax team when a new version is available. This proactive approach allows the team to keep production quality high through an automated discovery and notification process.

"Nexus Lifecycle gives us confidence that we're not missing anything."

— BRYSON KOEHLER, CTO, EQUIFAX

The teams need to assess the risk, what is contained in the patches, and how they might affect the current environment. "Whether we know there is an exposed vulnerability or a way to exploit the problem, is NOT the way to look at it," Koehler explains. "If there is a known problem and someone in the open source community has fixed it, we should fix it. If you don't stay on top of it, you're going to

miss something that's really important. We are leveraging Nexus Lifecycle to make sure we're staying on top of that. Nexus Lifecycle gives us confidence that we're not missing anything."

Nexus Lifecycle is part of the solution set that helps assess and map those risks as part of the company's ongoing creation of security metrics.

"If you're not moving at the pace of an organization that is coming off a breach, then you're not moving fast enough as it is."

— JAMIL FARSHCHI, CISO, EQUIFAX

Preparing for the future through DevSecOps cultural transformation.

Equifax is pushing for a seven year transformation within a three year time frame. The change from a "database perspective" to Google Cloud as their primary cloud provider for data made it possible to transform the company from the infrastructure on up. The Nexus Platform helps Equifax provide a meaningful, competitive advantage as the cultural transition continues.

"We're not moving the data, we're re-ingesting it," explains Koehler. "That allows us to apply all the rules, security or regulated, from the ground up." Such a transition would be impossible without security automation within the production pipeline. "You have to build in that sense of urgency into the culture of the organization. It's the only way you can be competitive, long term."

Farshchi agrees. "If you are not operating at the pace of an organization that is coming off a breach, then you're not moving fast enough as it is. We're not 'patching' production anymore. We're just deploying new environments. This is such a radical change in thinking, database to the cloud, it is a complete mindset change."

Visit www.sonatype.com/customer-success to see how other customers automate open source security.

Headquarters
8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
5 Martin Place, Level 14
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com