How automated analytics IMPROVE DIGITAL SERVICES, SECURITY AND WORKFLOWS

FedScoop Report

The need for AIOps platforms and automated orchestration tools will continue to grow, but they are also proving instrumental in improving security and citizen services.

As federal civilian, health and defense agencies continue to grapple with torrents of operating and security data coming from all directions, the demand for robust platforms capable of managing and making sense of all that data has never been greater.

Fortunately, a new generation of AIOps and intelligent analytics platforms, that use artificial intelligence to support IT operations — as well sophisticated security orchestration, automation and response (SOAR) solutions — are giving agencies a leg up in managing, if not mastering, all of that data. But these intelligent solutions aren't just about achieving greater scale and performance.

AIOps, data analytics and SOAR solutions are also expected to play a larger and more instrumental role in achieving the vision laid out in the White House's May 12 "***Executive Order*** on Improving the Nation's Cybersecurity." Among other directives, agencies must begin implementing a variety of steps to modernize their cybersecurity practices and improve how they respond to cybersecurity vulnerabilities and threats.

Those requirements add new planning urgency to efforts outlined in the ***Federal Data Strategy 2020 Action Plan***, which call for agencies to take concrete steps to govern, manage, protect and leverage the value of federal data. Those plans include assessing data infrastructure maturity, automating information collection and enhancing data management.

What government agencies — from the U.S. Census Bureau to the Department of Veteran Affairs to the Defense Department — are discovering is how the deployment of powerful, integrated data analytics and automated response platforms can make a significant difference in their daily IT, DevOps, and security operations as well as improving mission services.

Leveraging AIOps

The challenge virtually every agency faces isn't just the volume of data getting generated and processed every day. It's how to effectively assemble so many types of structured and unstructured data emanating from so many disparate systems — and then, how to make sense of it in order to make timely business decisions or mitigate cybersecurity threats.

AIOps platforms provide a powerful, centrally managed engine that can perform five critical functions:

1. Ingesting and deduplicating data at scale, from multiple sources across the IT environment, regardless of vendor system or the type of data, while maintaining data fidelity.
2. Performing real-time analysis at the point of ingestion.
3. Performing historical analysis and pattern discovery of stored data.
4. Leveraging machine learning in order to identify recurring issues, anomalies and root causes of IT-related issues.
5. Initiating actions, based on insights and analytics, in order to implement solutions quickly and more precisely.

The number one thing organizations should ask themselves up front is 'Do they know the true health of their IT services?'

- Wylie Vasquez, Splunk

For IT security operations teams, having AI-powered platforms such as Splunk's ***IT Service Intelligence (ITSI)*** platform and ***Splunk SOAR*** can yield a number of immediate insights and benefits.

- They decrease the mean time to investigate and resolve issues.
- They also decrease mean detection-through-prediction time and increase time between failures.
- They reduce system noise dramatically, through machine learning.
- And by automating many common IT and security tasks, they can eliminate tedious and manual IT work, allowing IT teams to focus on higher value needs.

Most importantly, by detecting anomalies, as well as correlating and analyzing patterns quickly that can arise in the midst of cyber "event storms," Splunk's ITSI AIOps and Splunk SOAR give agencies a powerful set of tools to respond to cyber incidents rapidly and protect their data more effectively.

For agency and mission executives, those capabilities translate into important added benefits, from reduced downtime to more effective incident management to improved customer service.

Taking a "Data-to-Everything" approach

Splunk ITSI gives agencies more than a window into their IT operations; it also provides a platform for managing large-scale IT development projects. That was the ***case at the U.S. Census Bureau***, when Census officials made the bold decision to conduct the 2020 decennial census

online, requiring a massive effort to modernize their IT, security and data operations.

A critical step in accomplishing that goal involved creating a single-pane-of-glass view of all of the bureau's existing mission-critical database applications and platforms. Prior to that, pinpointing the root cause of an issue required searching individually through all of the tools tied to the IT operations, recalls Wylie Vasquez, leadership advisor for observability and AIOps markets at Splunk. With Splunk ITSI and its event analytics dashboard, IT project teams were able to readily identify or narrow the source of an issue across the bureau's technology stack, with the help of automated AI and machine learning tools.

Another advantage of ITSI, according to Vasquez, is the AI/ML and predictive analytics capabilities it provides to predict and prevent common IT issues, before they happen, reducing unnecessary costs in time and resources.

One reason agencies continue to turn to Splunk's ***Data-to-Everything Platform***, according to Vasquez, is its unique strengths to ingest and unify nearly any kind of data — structured or unstructured, including logs, metrics, text, wire, API or social-media — from nearly any tool and any system, on-premises or in the cloud.

When systems or applications start to run slow, or issues arise, it usually requires bringing in large teams of people and multiple calls a day to troubleshoot the problem, Vasquez explained. What IT teams ultimately face is "a really, really hard big data problem to solve. ITSI allows enterprises to bring all that data together and pre-analyze it, so they can avoid a lot of those 'war room' calls," he said.

Creating a common view in health IT systems

Another example where Splunk's Data-to-Everything Platform improved mission and service delivery took shape at the U.S. Department of Veterans Affairs (VA). As the pandemic forced the VA to dramatically scale up its reliance of online telehealth appointments, it also required a massive effort behind the scenes to ***sustain telehealth with data intelligence***, according to Ann Mehra, strategic healthcare programs leader at Splunk.

That included "the back-end solutions and systems that must be in place and operating and functioning normally… so that the provider as well as the patient have access to the data they need to then engage in a meaningful conversation," said Mehra, a former associate director at Massachusetts General Hospital, which pioneered telehealth practices.

As health organizations raced to scale up virtual appointments, they quickly recognized their systems weren't configured to handle the added volume. That in turn required a huge effort to reconcile where systems were breaking down. Mehra recalled one case where "close to 50 individuals were trying to get to the root cause of what was happening, utilizing a number of different tools. We stepped in and in 48 hours, we were able to look across the organization's networks, across its applications, and across its data sources and were able to identify the root cause," she said.

But it also had a direct impact on customer-facing services, helping one of Splunk's customers decrease teleconference call failures from thousands per day to less than 10, and improve bandwidth and call capacity from 50% of demand to nearly 100%. And it also exposed unknown interoperability gaps, she said.

How automation enhances continuity

There's one more dimension where leveraging Splunk SOAR and other automation solutions brings added benefits: By automating and institutionalizing routine and repeatable processes, agencies can also address chronic workforce challenges.

That's particularly useful in instances where staffs routinely move in and out of positions, as is the case ***across the military***, according to Eric Hennessey, staff consulting solutions engineer for national defense accounts at Splunk.

"Because people are constantly coming and going, user accounts have to be constantly created and removed.

Removing the error factor is one of the key benefits of automation… especially a task that you do over and over again.

- Eric Hennessey, Splunk

In one case, close to 50 individuals were trying to identify the root cause of what was happening, utilizing a number of different tools. In 48 hours, we were able to look across the organization's networks, applications and data sources and identify the root cause.

- Ann Mehra, Splunk

Those types of processes are pretty straightforward and repeatable and very easy to automate. By taking that workload off the service desk staff, they can concentrate on other more important things," he said.

Another benefit of automation is the ability to reduce potential errors or delays that can arise from gaps in continuity as personnel rotate in and out.

"Removing the error factor" is one of the key benefits of automation, he said. "Whenever you can take humans out of the loop on some of these tasks — especially a task that you do over and over again — and institutionalize these repetitive processes, using an automated playbook like we do with Splunk SOAR, you greatly reduce that opportunity for error."

Splunk SOAR gives network operations teams an open and extensible automation platform that provides multiple interfaces to most of the IT and security products out on the market, he explained. It combines security infrastructure orchestration, playbook automation and case management capabilities to integrate processes, security workflows and other tasks.

Splunk's automation and analytics capabilities are already widely in use across the military, analyzing everything from aircraft diagnostics data, to ship maintenance records, to weapons performance logs, according to Hennessey. That analysis in turn is being used to help predict when parts need to be replaced, or when system failures appear imminent.

As agencies increasingly depend on data and devices operating on the edge of their networks — and security risks continue to expand — the need for high-performance, enterprise-wide analytics and automation tools will only grow too.

But Vasquez stressed that the true value of tools like Splunk ITSI still depend on whether agencies are viewing the performance of their systems from the lens of their users and customers.

"The number one thing organizations should ask themselves up front," advised Vasquez, is, "Do they know the true health of their services?" That's where they need to start.

Learn more about how Splunk's Data to Everything Platform can help your agency improve performance and citizen's user experience.

This article was produced by FedScoop and underwritten by Splunk.

FEDSCOOP splunk>