>CASE STUDY_

Accenture Federal Services Delivers Reliability, Speed, and Flexibility to Federal Agencies with Cribl Stream

HIGHLIGHTS

Accenture Federal Services are using Cribl Stream to deliver fast, accurate decisionmaking power to their major federal client.

Analysts at multiple federal agencies leverage Stream to improve Splunk performance.

Cribl gives Accenture Federal's clients control over outcomes in their high-volume, high-stakes environments.

The team at Accenture Federal Services (AFS) are working on a large scale data project at a major federal agency, and they're using Cribl Stream to help them deliver the high standard of reliability, speed, and flexibility required by their client to power fast, accurate decision making, reducing Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR).

Gared Seats is a Security Engineer at AFS, with a specialization in Splunk. His deep expertise in Splunk data ingestion is especially crucial to the team's project. Getting the correct data into Splunk quickly means their client can identify and solve issues of potentially national importance more quickly as well.

A high standard of reliability.

As part of the project, the primary federal client is aggregating data feeds from several other agencies across 90 separate sites, including Bro/Zeek, Palo Alto Networks, and InfoBlox traffic as well as a variety of types of custom sensor data. Current traffic levels are at around 5TB a day, and are expected to increase significantly during the project implementation. The team at AFS are using Stream to ensure the quality of the data coming in is clean and formatted as required for the client's use. Stream's internal metrics mean they can confirm the fidelity of that data with visibility into the integrity of the content being acquired and processed.

> "Our clients require a guarantee of accuracy. We capitalize on Stream's ability to get the right data in and formatted properly, and have confidence that things aren't getting dropped at ingest."
>
> — Gared Seats, Security Engineer, Accenture Federal Services

A high standard of speed.

When it's literally a matter of national security, rapid identification and resolution of issues is of critical importance. Analysts at many federal agencies use Splunk to dig into and clarify potential anomalies, and AFS brings Stream into the mix to ensure those analysts get the best performance possible.

> **"Analysts were building many searches just to build lookup tables; we had hundreds of searches scheduled just to build out IP lookups. Using Stream makes Splunk more efficientby letting you save your search resources for faster searching instead of having to build metrics to search."**
>
> — Gared Seats, Security Engineer, Accenture Federal Services

With Stream inline, analysts at the agency will be alerted instantly on notable events and be able to respond just as quickly, because their data will be rapidly enriched with notability indicator intelligence, threat actor, classification level, and other supporting data before it's indexed by Splunk, accelerating time to investigate, understand and resolve.

With Stream in their toolset, Accenture Federal Services can give their customers control over the outcome in high volume, high-stakes environment.

> **"There are so many ways to improve the quality of the data coming in: renaming fields, adding fields that are more useful, making fields SIEM-compliant, cleaning out unneeded content, fixing timestamps--you can do it all at the Stream layer, making Splunk more efficient, more affordable and the resulting data more actionable!"**
>
> — Gared Seats, Security Engineer, Accenture Federal Services

A high standard of flexibility.

Anyone who has had to bring in data from multiple disparate external systems and make it play nice together knows the challenges of ensuring the resultant events are standardized and can be correlated easily. With Stream, the AFS team can flexibly accept the data and bend it to their client's will on the fly without wasting time trying to convince other parties to cooperate. Instead, they can redirect their energy toward making their customer successful.

> **"I can definitely get 100% more done with Stream in the mix. No more having to go to individual systems to figure something out; no more having to talk to vendors to get them to fix their timestamps – we can do it ourselves in Stream. It's also easy because we run all of our Cribl deployment in our AWS GovCloud environment."**
>
> — Gared Seats, Security Engineer, Accenture Federal Services

With Stream, the AFS team can flexibly accept the data and bend it to their client's will on the fly without wasting time trying to convince other parties to cooperate.

Get what they have, and get control over your data.

Ultimately, what makes the difference in a high-volume, high-stakes environment is control over the outcome. With Stream in their toolset, the folks at Accenture Federal Services are delivering just that to their clients.

> **"I don't have to worry how people send me data. Stream gives me so much control I don't need to care about how it comes in. I can just say: "When I get done with this data, it will look like this, it will go into the right index, and the analysts will have what they need to make good decisions, fast."**
>
> — Gared Seats, Security Engineer, Accenture Federal Services

Learn how your organization can utilize the Data Engine for IT and Security to route, restructure, and enrich data in flight while cutting costs and simplifying operations. Get Cribl, and take control of your data.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, and Cribl Search, the industry's first search-in-place solution. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

CS-0012-EN-1-0224