CND Splunk Customer Success Story

Bring Out Your Dead

Client Challenge

The client had a self-managed cloud environment with approximately 800-2000 servers (Windows, Linux, Solaris) that would run on any given day. At times this could spike up to 18,000 servers to handle peak load demand from end users, the client uses Splunk to monitor for fraud, malign-activity, and general platform availability.

The client made the decision to outsource to an India based IT consultancy the support of much of their infrastructure some years prior, it is apparent that the relationship there is not entirely functional and there are significant shortcomings in the contract leaving the client with many obsolete configurations. For Splunk this means running version 7.x dating from 2019 and before, which has created numerous incompatibilities and left the client struggling to run Splunk.

This self-managed infra would then exfil data to Splunk Cloud (SaaS), resulting in a very disjointed environment from archaic on premise to fully managed, patched and supported in Splunk SaaS.

If it works, don't fix it?

Unfortunately for the client this is not a viable support strategy. Splunk generally has a 24 month release and support strategy, this is good because for many clients it nudges them to constantly patch and stay on top of releases ensuring obsolescence doesn't set it. For clients who have not adjusted to meet this tempo and the benefits it brings, it can leave them exposed once several years behind the release cycle. The client had UF's version 6.x on some Unix platforms. 7.x, 8.x on Windows, Mac, Linux and a significant variety of configurations and releases. Furthermore, many of the Splunk servers had not been patched or rebooted for over 4 years, would they return to service on power cycling?

Furthermore, the client had a significantly under-resourced HF being used for large API pulls with only 6 cores, it was falling over so regularly under peak load that the admin team had an auto-restart script in place to automate the reboot of it. This was highly inefficient and a false economy versus purchasing the vCPU it required. It took some persuasion but eventually the client accepted the approach was perhaps flawed.

Client

Public Sector, Education
United Kingdom, December 2023

Key Challenges

- Client lacked a viable support strategy.
- Due to unsuccessful outsourced relationship the client was left with obsolete configurations.
- Under-resourced HF resulted in large API pulls with only 6 cores and constant rebooting.

Key Results

- Client shown best practise methods resulting in effective simplified administration.
- Due to unsuccessful outsourced relationship the client was left with obsolete configurations.
- Under-resourced HF resulted in large API pulls with only 6 cores and constant rebooting.

Splunk x CND

CND Splunk Customer Success Story

Bring Out Your Dead

Approach:

I asked the client to accept a fix-forward approach, there were a lot of variables and we only had 7 PS days allocated to the clean-up work. What this meant is that we would attempt to get them to a supportable position running 9.0.x with apps and TA's aligned to current releases. They would need to accept a fair amount of stability risk given the build-up of tech debt.

The client accepted and we rebooted then patched two of the six Heavy Forwarders. Both returned to service ok, and we upgraded them from 7.0.x to 8.1.14 (the last version of 8.1.x) and this allowed us to get significantly forward. We then left these for the weekend and ensured stability before proceeding with the other HF's and supporting platforms. Having ensured data onboarding was stable we proceeded to upgrade from 8.1.14 to 9.0.5 which is fully supported until June 2024. We waited overnight and then repeated for the remaining platforms.

Fixing-Forward:

Whilst the Splunk platform upgrades is a standard admin item, what was more challenging that required experience and client buy-in was the variety of challenges with TA's and apps. Some of their old TA's and App's would now longer work above version 8 or below version 9.x dependant on the given item. Furthermore the stakeholders using each app was unclear and communications to end users limited. We set to work dealing with each challenge in turn, prioritising where possible and ensuring that data volumes were inline with anticipated levels.

Client

Public Sector, Government
United Kingdom, December 2023

Use the DS

The tech-debt also extended to the Deployment Server, the client had many configurations that were in the local directories of the HF's only. We packaged and sent to the DS all possible configurations to ensure a homogenous rollout across the HF's and allow for scalable infra that is straight-forward to backup. The clients support team hadn't really used to DS to effect previously and were very pleased to have us show them the best practice method that hugely simplified their administration.

Conclusion

The client was impressed by this accept risk and fix approach, they had for too long taken no action for fear of disruption. This had lead to a near unsupportable environment and only by obtaining a change window and permission for disruption were we able to overhaul the entire estate in just 7 days. The client is now able to take advantage of modern TA's and the new field extractions, CIM compliance etc and is looking to work with us again to ensure they don't fall behind and take full advantage of all Splunk has to offer.

Splunk x CND