splunk> Partnerverse

OUTPOST SECURITY

Outpost Security Customer Success Story
ZERO to ONE Splunk App for ES

CUSTOMER SUCCESS STORY

Key Challenges

Splunk Customer needed to leverage ES and RBA to bring scale and efficiency to their security alerting program.

Key Results

The Outpost Security ZERO to ONE Splunk App for ES unlocked the power of ES & RBA in two weeks.

Industry: SaaS

Solutions: Outpost Security ZERO to ONE Splunk App, Splunk Enterprise Security

Date: November 2023

"Working with Outpost Security exponentially sped up our implementation of RBA in ES" – IR Team Lead

This security team wanted to be better. Already an established SaaS company with over 5,000 employees and well over $1 billion in revenue, they still had plans for big growth in the near future. They knew they NEEDED to be better.

But just like many Splunk customers, they struggled to get the results they needed out of Splunk Enterprise Security. "Our ES implementation wasn't done the best it could have been, and that was before I started working here" their Incident Response Security Engineer told us. On top of that "we tried to do Risk Based Alerting (RBA) on our own and only made some progress."

This progress was not enough. The IR Team Lead quantified the gap "a year ago we worked with the SOC team to calculate what our current false positive rate was. We determined it was 97%." The SaaS company's team knew that RBA was the solution to the high volume, low fidelity alerts they were currently responding to. They wisely realized that in order to be successful, they would need an experienced outside perspective.

Turning Data Into Security Outcomes

- Over 40% reduction in alert volume
- Assets & Identity build-out
- Integration of Threat Intelligence feeds
- SOC analyst review and IR of RBA alerts
- Decrease in false positive alerts

Overwhelmed and under-resourced the SaaS company's team contacted Will Robus & Stuart McIntosh at Outpost Security. The Outpost Security team conducted a free review of the customers's Splunk ES environment and prescribed the Outpost Security ZERO to ONE App for Splunk ES with RBA. The customer also purchased Outpost's rapid implementation package and team trainings, a package designed to supercharge ES implementation and make RBA come to life in two weeks.

Outpost Security is a boutique cyber defense company. As an Elite Splunk Partner, they are focused on delivering security outcomes with Splunk Enterprise Security and Risk Based Alerting (RBA).

Implementing ES Fundamentals

"Looking back there were a few specific areas of ES we were struggling with" their Security Engineer told us. "We had built out a few custom approaches that didn't work very well." Visibility into users authenticating for the first time was a critical alert for the SaaS company's team, and to accomplish this they built out a custom data model.

"Turns out Splunk has a built-in feature that accomplished what we needed – Stuart simply pointed us to it and configured it. That alone was huge!"

Next on the list of challenges were assets and identities. "Our identities were ok, but the assets were kind of a mess. We tried to populate them with a master lookup file we populated with various SPL search results."

The ZERO to ONE app made this process much simpler, with several asset population searches included in the app that instantly snap into the asset matching framework.

Threat intelligence was also a pain point for the team. "We had it in kind of an ad-hoc state of configuration, with a couple things hooked into it, but not really producing meaningful results".

> Looking back there were a few specific areas of ES we were struggling with — We had built out a few custom approaches that didn't work very well. — We had it in kind of an ad-hoc state of configuration, with a couple things hooked into it, but not really producing meaningful results"
>
> **IR Security Engineer**

ZERO to ONE solved that problem as well. It highlights available threat feeds and then automatically incorporates any matches from all threat intelligence sources into the RBA alerts.

> In the 30 days since we began implementation of the ZERO to ONE app we've seen a 40% decrease in notable volume. Since last year we've had a goal to reduce our false positives from 97% to between 65%-75% - thanks to RBA we've already made a huge move in that direction.
>
> **IR Team Lead**

Bringing ES & RBA Together into a Security Program

The foundational work in ES is essential to RBA success in any environment, but that is just the first step. The ZERO to ONE app includes over 50 vetted RBA detections designed to produce contextually rich alerts that give analysts a new perspective. Thanks to the app, the team was able to deploy almost 20 new RBA detections by the end of the 2nd week of the implementation – and get them in front of SOC analysts shortly after.

"The Analyst Workbench page was awesome for the SOC. The ability to quickly pivot out of the notable they were investigating to a related risk object as well as seeing all of the individual risk attributions is huge help for them during investigations."

Alerting metrics were also impacted as quickly as a result. "In the 30 days since we began implementation of the ZERO to ONE app we've seen a 40% decrease in notable volume" the IR Team Lead reported to us. "Since last year we've had a goal to reduce our false positives from 97% to between 65%-75% - thanks to RBA we've already made a huge move in that direction."

Outpost Security is a boutique cyber defense company. As an Elite Splunk Partner, they are focused on delivering security outcomes with Splunk Enterprise Security and Risk Based Alerting (RBA).

> Going through the app implementation placed more emphasis on what our current processes are – honing them to make them tighter.
>
> **IR Team Lead**

> The ZERO to ONE app gives me visibility into what ES is doing.
>
> **IR Security Engineer**

While Helping to Build a Foundation for Growth

People and technology are cornerstones of a successful security program, but as important is the 3rd leg of that stool, which is process.

"Going through the app implementation placed more emphasis on what our current processes are – honing them to make them tighter," the IR Team Lead reflected shortly after the implementation concluded.

"Stuart was also a great sounding board – we would tell him about how we were thinking about a specific process or technique. Sometimes he said 'yeah, you are right on', other times he said 'have you thought about doing it this way'".

That experience is also built into the ZERO to ONE app itself – enabling the SaaS company's team to continuously improve independently.

"The ZERO to ONE app gives me visibility into what ES is doing", their Security Engineer reported to us. Allowing them to easily keep tabs on the asset and identity sources, counts, and priorities, as well as what the threat intelligence feeds are doing; seeing exactly what and how many matches are produced.

The app also has some critical features that contribute to successful tuning of detections and notables. Their Security Engineer expanded on that for us: "I use the app to tune a lot of things. It allows me to go in, quickly see performance of individual detections, and see which things are the noisiest. It tells me exactly what needs to be tuned first."

A new reality for the security program

After the implementation concluded, The IR Team Lead shared with us what's next for the SaaS company's security team.

"The reduction in notable volume so far has been great, but we think we can get an additional decrease of 10% to 20% with the tasks we have left on our list. Because of this we can feed more things to the SOC." Which includes deploying the remaining use cases and detections in the ZERO to ONE app.

"We also have our existing set of detections that we want to turn into RBA alerts. Thanks to working with Outpost Security to tighten up our systems and processes, what was going to take us years will now take us months. Without a doubt you've exponentially sped up our success with RBA in ES."

> Thanks to working with Outpost Security to tighten up our systems and processes, what was going to take us years will now take us months. Without a doubt you've exponentially sped up our success with RBA in ES.
>
> **IR Team Lead**

Outpost Security is a boutique cyber defense company. As an Elite Splunk Partner, they are focused on delivering security outcomes with Splunk Enterprise Security and Risk Based Alerting (RBA).