CND Splunk Customer Success Story

Half the Work for Twice the Detections with RBA!

Background:

With a background in Security Operations, I have always felt most at home when delivering Professional Services related to Splunk Enterprise Security (ES), so I was very excited when Splunk introduced me to a small public sector Security Operation Centre (SOC) team with a distributed Splunk build in need of some TLC. As a team they had a great deal of security competency and a number of, mostly network based, detections relevant to their remit. What they were missing was a seasoned security engineer with experience of Splunk and ES. My first few engagements with them were spent building out their Splunk infrastructure into a resilient, clustered and performant base that they could build their SOC workflow on. They had been using ES but really only for the 'Incident Review' page. With a solid Splunk foundation we reviewed all their detection logic to utilise CIM data modelling, implemented the ES asset and Identity framework, and I showed them how they could benefit from other features of ES like it's Threat Hunting and Situational Awareness dashboards. One challenge still remained, they had only 2 security analysts and hundreds of alerts every day. While the analysts were skilled and well-motivated, they would never be able to triage every alert and alert fatigue had long since set in.

Solution:

By now many of the team had taken the opportunity to participate in Splunk's EDU courses and were becoming more familiar with the online Splunk community, they started to suggest blog posts and conf videos to me (instead of the other way around)! A common theme at the time was a strategy of Risk Based Alerting (RBA). Given that it claimed to address our most pressing issue, after some discussion, we dove into making decisions about the fidelity and accuracy of the current searches. We assigned every correlation search a risk score and set up some new dashboards to test this novel concept along side the existing alerting. The analysts were quickly won over by the marked reduction in alerts they were faced with and the intuitive event sequencing that RBA offered.

Client

Public Sector, SOC Team

London, January - December 2023

Key Challenges

- Short staffed SOC team, suffering alert fatigue, little scope for further alert tuning.

Key Results

- Fewer alerts sent to analysts for review while increasing the number of malicious detections.

Outcome

The latest version of ES was made available with a host of new features specifically related to RBA, so on my next engagement with this customer we upgraded and got to grips with using them. The entire customer workflow had been migrated over to a risk-based approach, building on the out of the box ES functionality with customer specific dashboards and drilldowns.

Analysts were now reviewing fewer alerts but were also seeing more true positive detections and were often able to take swift action to protect their user base. They even found a long-term issue for which their existing detections had triggered alerts, but which had never before presented as a priority for review. On a recent engagement with this customer, I was told their leadership had given a presentation evangelising their successes with RBA to a small but international crowd in their industry vertical. This resulted in a lively discussion and several of their peers went home with plans to implement RBA in their own Security Operations Centre.

It's been a pleasure to watch this team's journey from Splunk novices to influencing how other Splunker's use and deploy ES as a SIEM. I have myself become a strong advocate of RBA and hope to help more SOC's find success with Splunk and ES as a result.