Contribution ID: **627** Contribution code: **contribution ID 627** Type: **Poster**

Flexible visualization of a 3rd party Intrusion Prevention (Security) tool: A use case with the ELK stack

A difficult aspect of cyber security is the ability to achieve automated real time intrusion prevention across various sets of systems. To this extent, several companies are offering comprehensive solutions that leverage an "accuracy of scale"and moving much of the intelligence and detection on the Cloud, relying on an ever-growing set of data and analytics to increase decision accuracy. Often, they provide tools to visualize the decision workflows in attack prevention (as well as tune the algorithm) but those solutions are not always practical as companies see the problem as "global"that is, from a unified Cyber-security standpoint. However, a key to a successful Cyber-security program is transparency and trust: from an experimental team viewpoint, this specifically means having the ability to immediately see what and from where, who has been blocked and being able to inform the community in case of a revoked access without the need for filing a "ticket"(that may eventually be answered) –in other words, rapid response to their user-base is essential but solutions targeting "sub-groups"in an organization are not often available.

We have come up with a versatile solution leveraging the ELK stack (Elasticsearch, Logstash, & Kibana) and an IPS (Intrusion Prevention System) based WAF (Web Application Firewall) from Signal Sciences. Signal Science allows the streaming of detailed logs in a Logstash format suitable for custom solutions for visualization. By combining these two tools, we have strengthened our security posture and enabled individual experiments to monitor their own traffic. Specifically, the IPS WAF provides unique data such as country of origin, protocol, response code, source IP, and paths accessed.

In this contribution, we will show how we engineered a solution so experiment groups could access a dashboard with predefined graphs but also, where they can create individual customizable dashboards used to visualize blocked traffic and troubleshoot latency issues. We will discuss the details and procedures for developing and configuring these tools and how it benefits cyber security postures across our scientific based environment.

Significance

References

Speaker time zone

Compatible with America

Primary authors: Mr FEDELE, Daniel (Brookhaven National Laboratory); LAURET, Jerome (Brookhaven National Laboratory); POAT, Michael (Brookhaven National Laboratory)

Presenter: POAT, Michael (Brookhaven National Laboratory)

Session Classification: Posters: Crystal

Track Classification: Track 1: Computing Technology for Physics Research