

Task 2

Executive Summary C768 – Technical Communication

**Jeffrey Robert Lynch
Western Governors University**

Table of Contents

Table of Contents.....	2
A. Executive Summary.....	3
D. References.....	5

A. Executive Summary

Nimble has distinguished itself in the ESL education space through operational independence and internal innovation. But as the company scales globally, it faces new challenges in data visibility, operational efficiency, and cybersecurity resilience. To maintain its leadership and support sustainable growth, Nimble must turn inward to leverage the untapped machine data it already collects.

Splunk Enterprise enables organizations to index, monitor, and analyze real-time machine data across their digital infrastructure. By adopting Splunk, Nimble can gain significant advantages in three key areas:

Business Analytics:

Web traffic, server logs, and conversion data can be segmented geographically to uncover regional performance differences. This enables Nimble to tailor marketing campaigns, landing pages, and customer messaging to align with cultural expectations—boosting conversion and retention. Marketing spend can be directed to the highest-performing regions and adjusted in underperforming markets for higher ROI. Custom dashboards offer real-time insight into KPIs and user behavior, accelerating decisions and improving precision.

IT Operations:

Real-time monitoring and automated alerting help detect IT infrastructure issues before they escalate. Splunk’s dashboards enable forecasting and capacity planning, while automation accelerates ticket resolution and reduces downtime. For context, ING Bank uses Splunk to

monitor over 200 applications—20 of them mission critical—achieving 99% uptime across 24/7 operations.

Cybersecurity:

In 2021, a botnet breach exploited Nimble’s digital infrastructure undetected for nearly two months, consuming system resources for unauthorized cryptocurrency mining. Had it been used for a distributed denial-of-service (DDoS) attack, Nimble could have faced legal exposure and reputational damage. Splunk enables the Security Operations Center (SOC) to detect privilege escalations, monitor remote access, and flag performance anomalies to prevent such attacks in the future.

Splunk Enterprise offers more than visibility—it’s a force multiplier. It equips Nimble with the operational intelligence to scale, secure, and optimize its global digital infrastructure. The time to act is now.

D. References

- Naveen. (2022, January 22). *Recipes for Monitoring and Alerting*. Retrieved June 22, 2022, from <https://intellipaat.com/blog/tutorial/splunk-tutorial/recipes-for-monitoring-and-alerting/>
- Splunk. (n.d.). *Splunk Enterprise Overview*. Retrieved June 22, 2022, from <https://docs.splunk.com/Documentation/Splunk/9.0.0/Overview/AboutSplunkEnterprise>
- Splunk. (n.d.). *Splunk Case Study: ING Bank Śląski S.A.*. Retrieved June 22, 2022, from <https://www.splunk.com/pdfs/customer-success-stories/splunk-at-ing.pdf>
- Vardhan. (2021, July 29). *Splunk Use Case: Domino's Success Story*. Retrieved June 22, 2022, from <https://www.edureka.co/blog/splunk-use-case/>