**Task 1: Business Case, White Paper, Research, Diction**

**C768 – Technical Communication**

**Jeffrey Robert Lynch**

**Western Governors University**

# Table of Contents

[Table of Contents 2](#_Toc107933898)

[A. Organization Description 3](#_Toc107933899)

[A1. Products or Services Produced 3](#_Toc107933900)

[A2. Organization Size and Number of Locations 3](#_Toc107933901)

[A3. Organization’s Industry 4](#_Toc107933902)

[B. Related Source Research 7](#_Toc107933903)

[B1. Summary and B2. Importance 7](#_Toc107933904)

[C. White Paper 11](#_Toc107933905)

[Introduction 12](#_Toc107933906)

[Business Analytics Solutions 13](#_Toc107933907)

[IT Operations and Infrastructure Solutions 14](#_Toc107933908)

[Cybersecurity Solutions 14](#_Toc107933909)

[Conclusion 15](#_Toc107933910)

[D. Explanation of Diction 17](#_Toc107933911)

[E. References 19](#_Toc107933912)

## **Organization Description**

## A1. Products or Services Produced

Nimble English Language Solutions, commonly known as Nimble, is a language school and translation liaison service based in Akron, Ohio. Nimble provides English language instruction, editing, lesson plans and translation services to clients all over the world. These services are provided via the company’s website or mobile app. Whereas many language schools provide classes for children using an “edutainment” model, Nimble primarily serves adult students, businesses, and professionals wishing to expand into English-speaking markets.

The major competitive advantage Nimble has in their market is their centralized operation leads to better quality control and more consistent offerings. Most ESL, English as a second language, service providers hire contractors from multiple regions. This leads to a decentralized operation with little quality control and inconsistent offerings. Nimble’s centralized locus of operation also allows for a more agile approach to the life cycle of services, allowing courses to be updated and disseminated rapidly.

## A2. Organization Size and Number of Locations

Nimble was founded in 2016 and currently retains 600 employees at its office in downtown Akron, Ohio. The facility contains an administrative office building for administrative and operations departments such as Marketing, Customer Service, Human Resources, etc. The ESL Services Department, the department that delivers services directly or indirectly to clients, occupies an adjacent large warehouse. This warehouse is divided into offices, studios, and other creative workspaces as project needs dictate. A second, smaller warehouse houses the Information Technology Department and all associated equipment such as servers.

The majority of Nimble’s employees provide ESL services as translators, editors, content creators or instructors. Nimble also employs robust Marketing and Customer Service departments to attract and retain clients in an international environment. Currently, the Information Technology department is growing rapidly to support the needs of the organization as Nimble transitions away from contractors and towards in house solutions. In this vein, Nimble has recently founded their own Security Operations Center in response to growing Cybersecurity threats.

## A3. Organization’s Industry

As a leader in the ESL education industry, Nimble offers multi-tier language English language solutions to businesses and professionals in the form of courses, translation, editing and live instruction. Nimble offerings are of higher quality and greater consistency than their competitors due to their practice of retaining in house talent rather than contractors. Likewise, their centralized operational structure allows Nimble a higher level of quality control in the design and implementation of services. Their mission is to provide clients with tailored services that eliminate language as an obstacle when expanding into new markets.

Nimble was founded by Chuntao Carston in 2016. Chuntao Carston was born Cai Chuntao in Chengdu, Sichuan, China. Mrs. Carston credits learning English as fundamental to her success in business, love, and self-actualization. Reflecting on her successes later in life, Mrs. Carston wanted to offer the same personal and professional opportunities to others across the world. She chose to start Nimble in Akron, Ohio for two reasons. First, Akron was the birthplace of her American husband, Daniel Carston and the two already owned a home there. Second, many Northeast Ohio residents speak English with what is known as “non-regional accent and diction”, which makes them desirable instructors for international ESL students. Chuntao Carston invested much of her own substantial personal wealth into the founding of the Nimble and it remains privately-owned to this day.

Nimble has few true competitors within the highly saturated ESL industry. Most companies use a business model of decentralized operations with low overhead. They hire contractors with dubious credentials that offer services of varying quality due to lack of quality control and oversight. Most companies within the industry spend more of their revenue on marketing rather than on retaining quality talent and offering quality services. Many of these ESL startups enter the industry with minimal investment and cash out after a few years of operation.

Nimble, using the opposite approach, invests in their talent, infrastructure, and service offerings so they can continue to grow their market share year after year. Nimble expects continued growth as they retain current clients and expand into new markets with a strong reputation in the industry. Recently, Nimble also has committed to innovation and adaptability by investing heavily in a robust Information Technology department. For these reasons Nimble expects to have longevity far beyond that of their competition. The majority of Nimble’s services are delivered to clients via their website. Since Nimble serves clients all over the world their offices are occupied and functioning 24 hours a day.

# B. Related Source Research

The topic of this white paper will be Splunk Enterprise 9.0, a software platform used to search, analyze, and visualize machine data from devices, servers, databases, applications, sensors, networks, virtual machines and more. This data can be monitored in real-time, used to generate alerts, used to generate reports, queried using Splunk Search Processing Language (SPL) and more.

## B1. Summary and B2. Importance

**Splunk Use Case: Domino’s Success Story**

This source is from Vardhan’s blog on the website Edureka.co (Vardhan, 2021, July 29). Vardhan is a Senior Research Analyst for Edureka.co. This blog post outlines how Domino’s used Splunk to analyze consumer behavior to build data-driven business strategies. This sounds simple in practice. However, due to the size and complexity of the data set, the unstructured nature of the data, and the immense number of data streams in multiple formats, Domino’s needed Splunk to aggregate the data to draw insights. “Up until implementing Splunk, managing the company’s application and platform data was a headache, with much of its log files in a giant mess” (Vardhan, 2021, July 29). Implementing Splunk allowed Domino’s to use applications such as: Interactive Maps, Real time feedback, KPI Dashboards, Payment Process, Promotional Support, and Performance Monitoring. This monitoring provided clearer Operational Intelligence than they had previously.

This source is important and relevant because it shows how useless data and data collection is on its own. Domino’s was drowning in data from multiple streams but needed Splunk to turn that data into true actionable Operational Intelligence and Business Intelligence. Likewise, having the capability to monitor these data streams in real-time provides insights that a company can capitalize on in real-time to be more agile within their industry.

**Recipes for Monitoring and Alerting**

This source is from Naveen’s blog on Intellipaat.com (Naveen, 2022, January 22). It covers a plethora of uses for Splunk when it comes to real- time monitoring and alerts. It presents multiple situations in which there is a business problem and then presents a solution using Splunk. an overview of what the Azure Sphere product offering is and how it works. It also provides a scenario as an example of the benefits that Azure Sphere brings to a business solution. This business scenario is centered around a smart internet connected dishwasher. The source also introduces the seven properties Microsoft deems as important for highly secured devices. Azure Sphere is then described in detail with these properties as a focus.

This source is important and relevant because it shows how a company can use Splunk for real-time monitoring and alerts. It presents not only the hypothetical situation but also examples of actual implementation using code. The situations provided are common to many businesses and organizations and are certainly relevant to Nimble.

**Splunk Enterprise Overview**

This source is a summary of the features of Splunk enterprise provided by Splunk on their official website Splunk.com (Splunk, n.d.). Splunk Enterprise has the capability to index machine data from multiple sources. Once indexed, this data can be searched using Search Processing Language or SPL. Searches can be run manually, or they can be saved to generate reports to populate dashboards to provide real-time monitoring. Alerts can notify when search results meet configured conditions. Alerts can be configured to trigger actions such as sending an email or running a script. Dashboards can display the results of saved searches running in the background, providing real-time system information.

This source is important and relevant because it is an inclusive list of all the features of Splunk enterprise as of the current 9.0 build. This is the exact product and version of Splunk enterprise that Nimble should be adopting to meet the needs of their business.

**Splunk Case Study: ING Bank Śląski S.A.**

This source is a case study of ING Bank provided by Splunk’s official website Splunk.com (Splunk, n.d.). It documents the challenges faced by ING Bank which led to their decision to adopt Splunk Enterprise. They used Splunk Enterprise to streamline their IT operations, gain real-time insight into application performance, maintain 200 business applications, gain greater insight into customer behavior by monitoring their digital journey in real time, and make better business decisions in real-time. “The IT department needed real-time insight into application performance in order to spot any potential issues to keep these applications running 24/7, with a minimum 99 percent uptime” (Splunk, n.d.). They used Splunk in a holistic manner, achieving benefits in Business Analytics, IT Operations and Cybersecurity.

This is important and relevant because Nimble would be using Splunk Enterprise in a similar way to ING Bank. Though they occupy different industries, both companies interact with their customers primarily via their website or mobile application. Nimble collects the same information from their site and servers from customers and can potentially use it in the same way ING Bank. This reflects the benefits Nimble could gain in Business Analytics, IT Operations and Cybersecurity.

# C. White Paper

Jeffrey Robert Lynch

Splunk Integration for Business Intelligence

Western Governors University

C768 Technical Communication

## Introduction

Since its founding in 2016, Nimble’s goal has been to set a new standard for excellence in the ESL Education industry. Rather than relying on contractors to provide ESL services to its clients, Nimble hired and retained a workforce comprised of hundreds of credentialed teachers, translators, and content creators. Where the competition offers regurgitated lesson plans, Nimble provides creative, tailored English language solutions for businesses and professionals. Instead of hiring outside companies to meet operational needs, Nimble invested in the creation of robust Marketing, Customer Service, and Information Technology departments to develop business solutions internally. There is no competitor in the ESL Education industry Nimble can emulate to attain greater success. The only way forward is for Nimble to look within to better understand their own operations, clients, infrastructure, threats, and opportunities. This can only be realized by gaining a better understanding of the data we already collect and achieving greater Operational Intelligence.

Splunk Enterprise is a software platform that allows organizations to search, analyze, and visualize the machine data gathered from devices, servers, websites, applications, sensors, networks, virtual machines and more. Splunk indexes the data stream and parses it into a series of individual events that can be viewed or searched. Searches allow users to gain insight from their data by calculating metrics, identifying patterns, and even predicting future trends. Alerts can notify users when search results meet configured conditions, such as a system usage threshold, and alerts can be configured to trigger a resulting action like sending an email notification or running a custom script. Dashboards can be used to display the results of searches, especially searches running continuously in the background to allow real-time monitoring of systems or situations. In short, Splunk Enterprise will allow Nimble to utilize the data we are already collecting for a variety of benefits.

## Business Analytics Solutions

Domino’s, though well-known for being a giant pizza delivery industry, is also an e-commerce giant. As an omni-channel business with a huge customer base and several parallel systems for sales and delivery, Domino’s systems generated a huge volume of unstructured data. “Up until implementing Splunk, managing the company’s application and platform data was a headache, with much of its log files in a giant mess” (Vardhan, 2021, July 29). Domino’s implemented Splunk to index their disparate data streams and achieve a higher degree of Operational Intelligence. They created interactive maps to show delivery orders across the United States, tracked how various promotional offers were performing, and used dashboards to track metrics and KPIs. These solutions were also updated in real-time, creating powerful tools for Business Analytics.

Nimble, though a smaller entity than Domino’s, can leverage its data in much the same way. Server logs and web data can determine the location of customers and potential customers via their IP address. This can be used to determine conversion and customer satisfaction rates geographically. Nimble could find that certain geographical regions are underserved compared to other populations. Likewise, Nimble can use the same data to identify the effectiveness of different marketing campaigns in different regions. This would allow Nimble to identify which campaigns and regions have the greatest return on investment (ROI) and why. If culturally insensitive marketing campaigns or web design are Nimble would want to know this so it could be rectified. Finally, customers navigating the website could be monitored in real- time to draw insights about their behavior and how their experience can be improved.

## IT Operations and Infrastructure Solutions

ING Bank Śląski S.A., a member of the ING Group, needed a solution to improve the reliability of their IT Operations and Infrastructure. “The IT department needed real-time insight into application performance in order to spot any potential issues to keep these applications running 24/7, with a minimum 99 percent uptime” (Splunk, n.d.). Their IT unit is responsible for supporting 200 business applications, 20 of which are considered mission critical. Splunk Enterprise allows them to monitor multiple IT systems and provide alerts for issues and potential issues as they arise in real-time. This allows them to respond quickly to situations by notifying the proper authority who can then provide support.

Nimble, though occupying a different industry than ING Bank Śląski S.A., faces many of the same challenges. Both organizations possess global reach, a global customer base, and a need for 24/7 functionality across multiple time zones. Both also interact with their customer base primarily through their website and mobile applications. Nimble can benefit from timely alerts when IT infrastructure fails or, more ideally, before it fails. Automating alerts can streamline the ticketing process, achieving faster resolutions and reducing downtime for critical systems. Real-time monitoring provided by user-friendly dashboards delivers more accurate and efficient forecasting of IT systems capacity. Finally, spikes in system usage, such as network traffic, can be more easily identified and accommodated with Splunk.

## Cybersecurity Solutions

Today, Nimble faces increased Cybersecurity threats targeting their website, networks, intellectual properties, customer’s personal information, and even processing power. As a company with global reach and a global customer base, Nimble presents a large attack surface. In 2021 Nimble was the target of a sophisticated cyberattack. The company’s devices were infected with a form of malware known as bots, creating a botnet. This meant that another party, the bot herder or bot controller, could commandeer Nimble’s devices for their own malicious purpose. Typically, botnets are used to initiate Distributed Denial-of-Service (DDOS) attacks against other targets. In Nimble’s case, however, the bot herder was using the botnet to steal small amounts of processing power across several devices to mine cryptocurrency in a practice known as Botnet Mining. The security breach went undetected for almost two months and led to the establishment of Nimble’s Security Operations Center (SOC).

Splunk can help Nimble’s SOC prevent these types of exploits by monitoring devices to ensure properly configured and updated firewalls and antivirus software. Alerts can be configured to trigger in several situations that could indicate a security breach. For example, an alert could trigger the notification of system administrators any time privileges are escalated unexpectedly. Similarly, Remote Desktop Protocol (RDP) sessions, commonly used by the IT department to access remote desktops and fix issues without being on site, can also be used by malicious actors as an exploit to access devices. These RDP session logs can be configured to trigger alerts under specific conditions. Finally, by tracking system performance in real-time using dashboards, anomalies can be identified such as a large percentage of processing power being used for unauthorized purposes. These are just a handful of ways that Splunk, properly configured, would empower Nimble’s SOC to prevent or mitigate attacks like the one that occurred in 2021.

## Conclusion

The only way for Nimble to move forward is to develop a better grasp of their data. Splunk Enterprise will allow Nimble to meaningfully utilize the machine data they already collect from the various components of their IT infrastructure or business. Splunk will allow Nimble to leverage the data it already collects to achieve greater Operational Intelligence. This will create opportunities in the realms of Business Analytics by recognizing opportunities for expansion, identifying underserved markets and better understanding user experience. Likewise, these insights will create opportunities for Nimble to streamline their Information Technology Operations and decrease downtime across all systems. Finally, ensuring Nimble’s capability to visualize and monitor their data will lead to improved outcomes in terms of identifying and mitigating Cybersecurity threats.

# Explanation of Diction

The intended audience for this white paper is my new supervisor, the head of Nimble’s IT department. I avoided contractions to be more formal, less casual. I also referred to Nimble in the third person (“Nimble” or “they” or “the company”) because it seemed more professional, detached, and objective. I did not use the first person (“I believe” or “my opinion” or “our goals” or “we at Nimble”) though I theoretically could have since I work for Nimble. Likewise, I did not use the second person (“you” or “your”) though I logically could have since the primary audience is a department head at Nimble.

It can be assumed, as the head of a department, this person has at least a modicum of general business knowledge, so I did not feel the need to explain terminology such Operational Intelligence, Business Analytics, ROI or KPIs. I used the acronym ROI but made explicit I was discussing “return on investment” so it could not be misunderstood as “rate of interest”. I did not explicitly state that KPIs were “key performance indicators” because as the head of a department, this person certainly knows and uses KPIs daily. As the head of a department at a company that provides English as a Second Language services, I felt the reader would understand the acronym ESL without making the meaning explicit.

As the head of Nimble’s IT department, I assumed the reader had at least a general understanding of IT technology and practices, but I did not want to assume too much in depth knowledge. Sometimes the head of an IT department comes from a business background rather than a technical background. I assumed the reader would know what a dashboard is in the context of monitoring and tickets in the context of an IT ticketing system. I also assumed the reader would know what an IP address is though I did explicitly state how additional information could be derived from an IP address.

The head of the IT department is ostensibly also the head of the Security Operations Center so it can be assumed the reader has a general understanding of Cybersecurity terminology, practices, and technologies. I was more explicit than I needed to be in explaining terms like DDOS, Botnets, and Botnet Mining because I wanted the reader to feel confident that I, as the writer, understood the Cybersecurity attack Nimble faced in 2021. This foundation was important to lay because I went on to explain explicitly how certain components of Splunk could be used to create practices to prevent or mitigate those specific attacks in the future.

I did not do a deep dive into the architecture of Splunk, Search Processing Language (SPL), or any code as I felt it was not relevant to my focus of how implementing Splunk Enterprise to aggregate machine data from logs would aid Nimble in the realms of Business Analytics, IT Operations and Cybersecurity Operations.

# 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/>