**Task 1: Adoption Plan Proposal**

Techfite Case Study

Name – C850 Emerging Technologies

Western Governors University

1. **Organizational Need**

Techfite makes medical devices for the NASA Space Program and the company is growing internationally. Techfite needs to implement a Security Information Event Management (SIEM) solution that will be utilized to analyze large amounts of real-time logging data generated by their two firewalls and the honeypot devices that are planned to be installed. The SIEM solution will also need to be able to provide real-time notifications of active security threats and analyze log behavior.

Since Techfite will be working with governmental organizations they will need to follow FISMA and NIST standards. With these standards they will need not only an analysis solution, but additionally will need a storage solution that will retain their current log data for one year. The storage solution will need the ability to scale for future growth.

1. **Emerging Technology Solution**

I am recommending Elastic Cloud – Elasticsearch Service on AWS i3 to meet the business needs of Techfite as it makes use of machine learning and cloud hosted services. The Elasticsearch will offer scalability and be a fully featured SIEM appliance when deployed on Amazon’s 13 infrastructure.

With Elasticsearch anomaly detection is performed by machine learning to detect anomalies in real-time streaming data and they are identified as they evolve for immediate mitigation. With the machine learning anomaly detection, the Kibana user interface provides context into the data and events contributing to the anomaly making it easier for users to extract value with minimal machine learning experience.

Techfite will have the ability to analyze and react in real-time to the incoming event log data through several modules that Elastic provides in their service offerings. This will be achievable with Elasticsearch and the provided dashboard and reporting Kibana application.

Techfite will be able to build out customized dashboards for viewing both real-time and archived event trends, track ongoing SIEM event investigations, and can configure machine learning to respond to real-time events and provide notifications. (Elastic, 2020)

1. **Adoption Process**

Next the solutions benefit, risks, and costs will need to be evaluated as it applies to Techfite’s business needs and current mode of operations. The financial costs can be obtained by using Elastic’s pricing calculator for the Elasticsearch Service at <https://cloud.elastic.co/pricing> (Elastic, 2020)

Benefits of the adoption:

* People – With the Elastic instance configured and running, man hours spent sorting through and evaluating security logs will be reduced greatly freeing up time for other tasks.
* Process – Elasticsearch service allows for many of the processes to automated which is a benefit to efficiency.
* Business – Added levels of security and efficiency received directly by Techfite will benefit their customers and positively their brand by raised their value and effectiveness as compared to their competitors.
* Infrastructure – With the Elastic Cloud infrastructure hosted on AWS i3 the need for additional on-site hardware and software resources will be alleviated and allow for scaling to meet future needs.

Risks of the adoption:

* Performance – The biggest performance risk is the availability of the AWS infrastructure but can partially be mitigated by having multiple physical connections to the cloud service and with service level agreements (SLAs) both with Elastic and AWS.
* Integration – The IT support staff will need to be trained on the configuration and maintenance of the Elastic instance and agents used to transport logs from the local devices to the Elasticsearch. Training costs can be incorporated into the project so that the training is not forgotten after the adoption.
* Penetration – Most of the time investment will be at the onset of the adoption but should taper off as the adoption progresses and this will free up time for the team overall. This is achieved with the time-saving automation and should drive the IT team to overall adoption of the solution.
* Costs – with the solution needed to meet compliance, the business would need to absorb the costs. The cost model does provide benefits with Techfite with the nature of their business growing. The costs start lower on the scale and grow in direct relation to the company’s future growth.

With careful planning and implementation, I believe the benefits to the solution outweigh the associated risks and most of the identified risks can be mitigated to acceptable levels.

I would recommend a 14-day trial period to run a pilot at no cost (Gupta, 2019). This would create an opportunity to connect one of the firewall devices the devices to the Elastic system and configure the automation for testing of the solution prior to full adoption. With the pilot it would be a great opportunity for on of the IT staff to be assigned to champion the project and help drive the adoption with the rest of the team after the pilot concludes.

1. **Technology Impact**

With cloud computing and machine learning, the positive impact of this emerging technology is the SIEM operations for Techfite will place them at the forefront of the industry and carry them into the future.

A potential negative effect of the solution is that will come at a cost to Techfite as all leading-edge technology does. The cost of the solution is mitigated by the automation that is being implemented with automation. Additionally, the cost of the solution is offset by cybersecurity staff being reduced since the increased head count would no longer be necessary. The option would remain that Techfite could retrain their personal to take on additional roles or be moved to different departments where their value add could still be recognized.

1. **Technology Comparison**

Elasticsearch Advantages -

* Elasticsearch is an end to end open source solution with premium services to fit any need that may arise.
* Elasticsearch offers dynamic greps and good visualizations when coupled with Kibana allows for changing the use case frequently.

Elasticsearch Disadvantages -

* One disadvantage is that Elasticsearch will require extra effort from Techfite for its success since it only offers a single SaaS platform paid module for deployment.
* With Elasticsearch one disadvantage is that Elastic does not come with its own GUI and must be inherited to a GUI interface such as Kibana

Splunk Advantages -

* With traditionally serving big enterprise clients giving them an advantage to working with big data.
* Splunk has the advantage of inbuilt and pre-configured features to allow data mapping of respective values and pre-loaded wizards which are easy and reliable to use.

Splunk Disadvantages -

* Splunk has a steep learning curve that would require additional costs going to training IT staff to install and manage the solution.
* Splunk traditionally runs on-premises which would require the purchase of new additional hardware to implement this as a solution.

1. **Adoption Success**

The method I have chosen is the number of logs analyzed per month. With AWS i3 and machine learning from Elasticsearch the number of logs analyzed would be 150,000 with an accuracy target of 80%. With the previous solution the cyberteam team could only analyst 15,000 logs per month with an accuracy of 60%. With the implementation Techfite should realize the success of the solution within 30 days from implementation with an increased log analysis and accuracy increase.

**References**

E. (n.d.). Elasticsearch Service pricing calculator. Retrieved August 07, 2020, from <https://cloud.elastic.co/pricing>

Elasticsearch Service: Managed Elasticsearch on AWS, Google Cloud, and Azure. (n.d.). Retrieved August 07, 2020, from <https://www.elastic.co/elasticsearch/service>

Gupta, A. (2019, April 01). Elasticsearch Service on Elastic Cloud Introduces New Pricing With Reduced Costs. Retrieved August 07, 2020, from <https://www.elastic.co/blog/elasticsearch-service-on-elastic-cloud-introduces-new-pricing-with-reduced-costs>

Migrating to Elastic from Splunk. (n.d.). Retrieved August 07, 2020, from <https://www.elastic.co/splunk-replacement?ultron=%5BEL%5D-%5BComp-Splunk%5D-%5BTrials%5D-%5BAMER%5D-%5BUS+CA%5D-Exact>