C850 Emerging Technologies

Task 1

Damian J Yates

2020

Contents

[Requirements of Techfite 1](#_Toc43038061)

[Proposed Technology Solution 1](#_Toc43038062)

[Organizational Adoption Plan 1](#_Toc43038063)

[Technological Impact to the Organization 1](#_Toc43038064)

[Proposed TEchnology comparision 2](#_Toc43038065)

[Quantify Adoption of New Technology 2](#_Toc43038066)

[Works Cited 4](#_Toc43038067)

# Requirements of Techfite

Techfite is manufacturer of medical apparatuses for use by NASA and the Federal Government. The devices produced are used to extend the length of time and quality of life the astronauts have while deployed in space. Due to the critical and proprietary nature of these products, NASA has increased pressure on Techfite to establish 100% compliance with the United States Federal Information Security Modernization Act of 2014 by following the National Institute of Standard and Technology Special Publication 800-171 in order to maintain its relationship with the government. Currently, Techfite has fulfilled this requirement up to 75% compliance and is looking to this proposal to reach the 100% mandated goal. The Proposed solution will address Techfite’s need to implement a Security Information and Event Management Platform. This proposal will address notification, monitoring, collection, security, storage, reporting and archival of data collated.

# Proposed Technology Solution

We have chosen Fire-Eye Endpoint Security as the emerging technology used to fill the SIEM requirements of Techfite. Fire-Eye makes effective use of Artificial Intelligence Machine Learning technologies coupled with endpoint and network security to protect, detect and respond to attacks both internal and external to the organization (FireEye, Inc., 2020). Primary interest includes the Network Security and Forensics capabilities of the solution that encompasses network and endpoints both domestic and foreign. This functionality will be used to bolster the organizations ability to meet and possibly exceed the FISMA requirements set by NASA and the US Government.

# Organizational Adoption Plan

We will suggest the use of Gartner’s STREET in the adoption process that the organization should use to integrate the suggested emerging technology into its internal processes. Performing each of the adoption process tasks will provide a solid foundation and roadmap to successfully acceptance and integration of the new technology (UCertify, Inc., 2020). Below are the tasks to be performed and the importance of each to Techfite success:

* Defining the **Scope** – This task will require the organization to define the purpose the proposed initiative should meet. Identify which organizational objectives are to be met and what problems that the solution should resolve. It is at this step the ETG (Emerging Technology Group) should work to produce a competitive analysis, visioning and scenario building and identify business opportunities and problems. The resulting benefit of this exercise is a set of clear parameters and establish goals as a guide for the following task to remain within.
* **Track** (identify relevant technologies) – Here the ETG will begin to identify candidate technologies that fall within the defined scope. The identified candidates should be derived from a wide range of sources and encompass varying platforms. Upon completion of this task will have a clear understanding of the available emerging technologies that are available to meet the needs of the scope. The results of this task should be communicated to others in the organization so that further decisions can be made.
* **Rank** each of the relevant technologies – At this phase of the “STREET” process, a “thinning of the herd” will be performed to narrow the list of candidates identified in the Track activity. Identifying the strengths and shortcomings of each candidate by means of impartial, data driven analysis and decisions based on criteria derived from the “Scope” activity. This activity ensures that each candidate is objectively analyzed to determine which are to be considered as a top-ranked candidate to be passed on to the evaluation phase.
* **Evaluate** the top three ranked technologies – In the Evaluate activity, the ETG will perform a deeper analysis of the top candidates utilizing prototyping, piloting, and investigations to determine the total value of each technology. The result of this task will result in the selection of a final candidate that will proceed through the last two phases of the STREET process.
* **Evangelize** to obtain support for selected technology – The ETG will use this phase of the process to inspire, educate and involve those individuals with the authority to enforce the adoption of the emerging technology into the organization and its processes. Obtaining the support and cooperation of these individuals is key because normally organizational opposition to change leading to an aversion to accepting the new technologies.
* **Transfer** ownership to implementation team – Being the final phase of the “STREET” process, it is at this point that responsibility of the new technology to the team or department that will continue to drive the deployment and implementation of the new technology. In addition to knowledge transfer, education and transfer of personnel are normally performed at this stage. The ETG is relieved of all responsibilities and implementation teams begin their process for deploying the new technology to meet the requirements initially identified in the Scope phase of the STREET process.

# Technological Impact to the Organization

As with all technologies, emerging or mature, there are positive and negative impacts that will ensue with its implementation and adoption. Once fully integrated into the organizations existing processes and infrastructure, response to zero-day exploits and intrusion attempts will become more visible, documented, and easier to respond to by trained staff. This ability to quickly respond and identify threats to the company’s assets will greatly improve the security posture of Techfite and meet the requirements set by FISMA. In addition to the added benefit of meeting FISMA’s standards there is also the adverse effect of the complexity of configuration and use of the new technology. The severity of the negative impact of this complexity can be diminished or even averted by ensuring that resources from FireEye are allocated to the project to facilitate adequate training for engineering, managerial, and other staff. Ensuring that proper configuration and referential documentation is handed off to the technology team would be of great use as well. As a final step to diminish the negative returns on the implementation of the new technology, fostering continuing education on the product and the technology behind it will better position all individuals that work with it to remain current on the subject.

# Proposed TEchnology comparision

Why choose a cloud-based SIEM like FireEye over a locally provisioned and managed open-source SIEM like AlienVault. Like most technologies, the reasons for using one over the other is dependent on resources, knowledgebase, and need. Here are a few advantages to adopt FireEye:

* FireEye removes the need to plan, budget, install and maintain additional physical infrastructure to support the solution
* FireEye offers an incident response service that removes the need to dedicate Techfite resources and reduces response times as well as ensure around the clock real-time mitigation of organizational resources.

A few disadvantages in using FireEye include:

* Loss of total control, cradle to grave, of data and information collected by the SIEM.
* The amount of data captured, analyzed, and retained directly affects the costs incurred in utilizing the SIEM.

Utilization of an on-premise open source SIEM such as AlienVault has several advantages:

* Organization maintains complete control over all aspects of the SIEM, hardware, software, collected data, and its maintenance.
* Increase in data security is another advantage of an on-premise solution. Logged data does not leave the perimeter of the organization network removing the potential of interception or manipulation of said data.

Like FireEye, AlienVault has its disadvantages as well:

* The ROI for AlienVault takes longer to emerge due to the additional capital expenditures and time to ramp up.
* Investment in personnel and ongoing training resources may be needed to ensure proper operation and maintenance of the solution if they are not readily available within the technology team.

# Quantify Adoption of New Technology

To determine whether the adoption of the proposed emerging technology solution is successful, the method of quantifying the number of logs analyzed with in a 24-hour period will be used. Historically, log analysis was performed on an as needed basis taking up to 8 hours to aggregate and parse the needed data. Additionally, Techfite lacked data retention policies for its server logs and found that needed historical data was not readily available for analysis. Successful adoption of FireEye into the Techfite will be apparent when 80% of all infrastructure equipment and software, within a 24-hour period, is processed and made available in the cloud repository at FireEye data centers for 7 consecutive days.

# Works Cited

*Endpoint Security Software and Solutions | FireEye*. (2020, July). Retrieved from FireEye: https://www.fireeye.com/solutions/hx-endpoint-security-products.html

*Processes for Implementing Emerging Technologies*. (2020, July). Retrieved from WGU Ucertify: https://wgu.ucertify.com/?func=ebook&chapter\_no=2#top