TECHFITE CASE STUDY

C850 – Emerging Technologies

JT PAYNE

Organizational Need

TechFIte is produces medical equipment for not only NASA, but several other space agencies around the world. With the inclusion of the international community TechFite must maintain a strict adherence to security compliances such as FISMA and NIST. As of right now, TechFite scans its security logs manually causing a bottleneck with its governmental contract obligations. At this time I am recommending a that we use Snort, which is an open source application..

Emerging Tech Solution

My proposal is that TechFlite utilizes Snort to begin with, this intrustion protection system will use a its own rules or ones that we set to find packets that match and generate alerts for our IT staff. We don't have to only rely on our own definitions to make sure we are secure, Snort has a Subscriber Ruleset that is developed and tested by Cisco Talos, which is a regular intelligence update that highlights the biggest threats and other security news. According to fellow peer Alan Matson, CCNA:S of Insight, "It (Snort) is well suited for a high energy environment with a lot of traffic…" (TrustRadius, N.D.)

Adoption Process

I have chosen the Gartner STREET method as the adoption process as the best way to approach this issue. By utilizing this method, new technologies can be introduced and deployed more effectively in meeting the company's objectives.

Scope: Snort will allow for TechFlite IT staff to monitor in real time packets that may or may not have malicious content. (Snort, N.D.) This will take place of the manual sorting of the packets coming in and alleviate the stress on the four members of the IT staff. Analysis during this process on the competition and build scenarios can show us what business problems may occur as well as opportunities.

Track: Activities in tracking can enable our organization to see how mature the emerging technology is and will identify whether the emerging technology is beneficial for us. TechFlite will be able to keep ahead of the threats that possible out there with Cisco Talos intelligence. The current IT staff may miss something that is out there, and Talos will allow for more complete coverage of any incoming threat.

Rank: Ranking technology solutions allows an organization to consider other technology solutions and decide which is worth the risk. Snort and Cisco offer the same level of protection, what it really comes down to is the ability to set the ruleset for the intrusion detection system. Snort relies on the Cisco Talos threat intelligence, which is constantly upadated, whereas Cisco Firepower relies on the rules you have set and needs to be updated constantly. Cisco does have a graphical user interface, though outdated compared to Cisco's newer products, which is easier to use then Snort's command line interface. (TrustRadius, Viero, 2019)

Evaluate: TechFlite IT staff will set up a lab environment for the initial Snort install to make sure it is a viable technology that it is interfaceable with the current three-tiered networking system that we implement. Snort is a Linux based utility that is easy to deploy and to configure to monitor incoming network traffic for intrusion attempts, log them, and take whatever action the administrator has specified. Cisco in this, though not a Linux based system, uses its own operating system can provide for expandability, though deploying it may be more difficult. (TrustRadius, Viero, 2019)

Evangelize: In this stage is the need to get the decision makers excited about the emerging technology and to show them the benefits of taking the risk of the emerging tech. TechFlite will have to inform its customers that they are moving forward with locking down their network and becoming more compliant with NIST and FISMA. Emails sent out to them should inform the customers that steps are being taken to increase internal IT integrity, but also to

ensure the customers security as well. Keeping the emails to the point and energized to get the necessary resourcing to adopt the new tech.

Transfer: TechFlite IT staff will have to ensure a safe transfer from a lab environment to a working environment. A phased approach of deploying the new server would allow for more flexibility to encompass any problems that might be encountered. Allowing customers and users to become more comfortable with the new technology being put in place.

Technology Impact

When adopting a new technology one must weigh the pros and cons of each step not only with the tech itself, but within the organization itself. One positive impact is that the implementation of Snort is not going to effect the internal user as much as it will the external user who is trying to collaborate with the internal user. One negative impact is that users could get confused on the new security systems. To avoid the confusion is to set up time in the lab environment for each user to alleviate any concerns as well as familiarize them with the requirements of the program.

Technology Comparison

Snort offers real time analysis of incoming packets through the Cisco Talos network. (Cisco Talos. n.d.) Snort also offers new rulesets you can utilize on the fly and integrate into the system. A coupe of disadvantages for Snort it that it can be hard to set up and you will get plenty of false positives in the beginning. Cisco Fire power offers a graphical user interface(Cisco N.D.), though outdated, it still preferred over command line interfaces like Snort. Another advantage that Cisco offers is its low false positive rate, but it has to be maintained more so then Snorts. A couple of disadvantages to Cisco Firepower is it that fine tuning it the policies can be time consuming and tedious. Also Firepower is meant for larger organizations and may not be best suited for a smaller business.

Adoption Success

The method I have chosen to determine whether or not the adoption of SNORT will be successful to meet Techfite's needs is the number of man hours saved. Before Techfite implemented SNORT, the company manually scanned all of its security logs, which took 20 hours weekly. After implementing SNORT, Techfite will automate all log scanning and it will only take 5 hours weekly. This noticeable time savings will help Techfite to harden its security while meeting FISMA and NIST regulations.

References:

Snort. (n.d.) http://www.snort.org

Cisco Talos. (n.d.) https://www.talosintelligence.com

Cisco (n.d.) https://www.cisco.com/c/en/us/products/security/firepower-management-center/index.html

Trustradius (n.d.) https://www.trustradius.com/compare-products/cisco-firepower-ngips-vs-cisco-snort