**TechFite Case Study**

TechFite makes medical devices for the space program. They are in Houston, Texas, near the Johnson Space Center. Security is a top priority for TechFite, partly because the company works with NASA, but also because the proprietary technology that TechFite is creating allows humans to work longer in space. TechFite has an IT department that currently consists of 4 employees: two entry-level specialists, a senior security specialist, and an IT security manager.

TechFite has a two-firewall system in which the outside firewall protects TechFite and its partners and the inner firewall protects the TechFite intranet.

The two-firewall system creates a three-ring network where the innermost ring is the most secure and the outermost ring connects directly to the Internet. Each one of these firewalls creates a log of all the network traffic that passes through each of the firewalls. The TechFite CIO has notably raised concerns about current infrastructure security implications, but she wants her staff to propose inexpensive solutions to meet future demands. There is a lot of traffic that passes through these firewalls due to companies that want to securely collaborate with TechFite and the need government agencies have to access TechFite’s information. TechFite administrators have been researching solutions currently available to meet the growing demands of secure collaboration, and all suggested resources fall outside of TechFite’s IT budget. Additionally, it is difficult to scan these logs manually, and TechFite has been exploring open source solutions to automate log correlation for both host-based and network appliances. However, the amount of storage space to keep these logs for at least a year is more than TechFite has onsite. (TechFite currently scans 10,000 log files manually per week with a 30% success rate in identifying intrusion signature patterns and has only 4 terabytes of storage allocated locally for log storage.)  One of the system administrators suggested using technology to not only review the logs but also store the log files.

TechFite is being pressured to comply with FISMA, using NIST as a security framework, when the company works on government contracts. Other restrictions have been observed by TechFite’s competitors concerning the handling of data across international boundaries, namely in the European Union. The company is also being asked to ensure FISMA compliance, even as budgets are shrinking, which is happening in part because there are fewer space missions planned. TechFite is also looking to work with the space programs of other countries, such as the European Space Agency, the Canadian Space Agency, and JAXA, the Japanese space agency. The company is interested in collaborating with other institutions and companies to expand its business, which may result in opening subsidiaries in other locations domestically and overseas. This may force the company to store its information for longer periods of time, and more locations means more log data will need to be stored.

Besides scanning the log data for potential attackers after systems have been compromised, the system administrators would like to be alerted by a new system that meets FISMA regulations when potential attacks are occurring on host and network systems. This means that real-time log scanning and behavior analysis of incoming network traffic will be needed to determine when a denial of service attack or advanced persistent threat is happening so the system administrators can catch the hackers. The system administrators also want to install honeypots to attract hackers, and the logs for those will also need to be stored even though these honeypots will not actually have real data on them.

The system administrators will be busy keeping up with the technology they have, and they will not have time to research new technologies that might help them do their jobs better.