BUSINESS PROPOSAL

ADOPTION OF AN EMERGING TECHNOLOGY

Created by Patrice Godjo

Date: 05/06/2020

Course C850

Mentor: Tom Milham

For TechFite

Part A

TechFite is a company manufacturing medical devices. TechFite works closely with the National Aeronautics and Space Administration (NASA) and is currently on a project that will allows humans to stay longer in space. TechFite want to expand his boundaries by working with other countries that have space program, like European Space Agency or the Canadian Space Agency. This expansion may result in opening subsidiaries all over the country and abroad. In this effort to expanding its businesses, TechFite will collaborate with institutions and companies and that will inevitably increase the security risk. The company is already being pressured to comply with the Federal Information Security Management Act (FISMA) Therefore, the security is a prime concern for the company, especially the IT department.

TechFite security system is based on two (02) firewalls: the inner protects the intranet and the outer protects the company and its partners from internet. To comply with FISMA exigence and mitigate the security risks related to its expansion, TechFite Administrators need a new and robust system that can scan all logs data of every incoming network traffic that pass through the firewalls. These logs must be kept for, at least, a year which means TechFite will need a large amount of data storage unit as logs data will grow fast. To achieve these goals the company that can not only allow the review of all logs files but also keep them in a secured storage. The solution must also have a trusted and verified intrusion detection system that can alert the administrators when the intrusion is taking place, and behavior analysis tool.

PART B

I have chosen Amazon Web Services (AWS) Security as a Service because it makes the use of Artificial Intelligence (AI) and machine learning. According to Eliezer Yudkowsky, an

Artificial Intelligence researcher, an AI is defined as an “intelligent agents: any device that perceives its environment and takes actions that maximize its chance of success at some goal.” These recent years we have seen a type of computing that use Artificial Intelligence to revolutionize the Technology world and it is known as Cloud Computing. Steve Ranger, in its article on zednet.com, defined the cloud computing as “Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis.” Amazon Web Services (AWS) is categorized as cloud computing and offers multiple services such as Security as a Service. Security services were performed, back in the days, by Anti-virus owners like McAfee, Norton, or Kaspersky. Cloud computing itself is an emerging technology, thus the services provided by cloud computing are categorized as emerging technology.

PART C

Adopting an Emerging Technology (ET) is always critical within an organization. Gartner’s STREET technology adoption process is a tool that can help alleviate the burden and lead to a success when it is thoroughly followed. STREET IS in an acronym that stand for Scope – Track – Rank – Evaluate – Evangelize – Transfer. Let dive into each step that TechFite can take for the success.

Scope: This step helps an organization to define it needs that must be addressed. As expressed in PART A, one of the TechFite need is the cloud Security as a Service.

Track: In Gartner’s STREET process, this step is used to layout many technologies that can address the need defined in scope. There are some ET that can fulfill TechFite’s need. Amazon

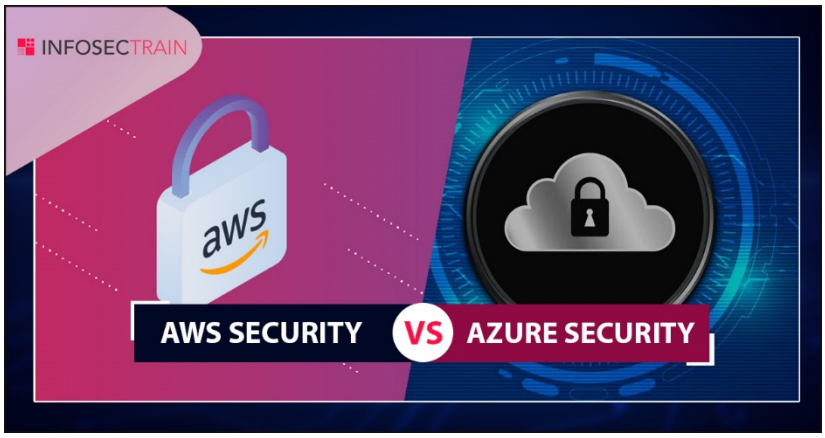
Web Services AWS, Microsoft AZURE, SPLUNK, etc. These ET will be ranked to determine which one is the most suitable for TechFite.

Rank: In this step I have considered two dominant Emerging Technology that I can chose from and recommend to TechFite in order to fulfill its security need: AWS Security as a Service and Microsoft AZURE. The following Table gives an idea of what led me to recommend AWS Security as a Service over AZURE.

The following table describe how AWS and AZURE implement their security on the cloud: (***Please see the table on the following page)***. This table was layout by Jayanthi Manikandan, Writer and editor, security researcher at InfoSecTrain. As we can see, AWS and AZURE have different ways to implement the Security as a Service. When we analyze this table, we can see that AWS Security as Service have more tools than Microsoft AZURE Security as a Service. In terms of Detection Controls, AWS has what they called *AWS Security Hub*. Published by AWS in November 2018, "With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. The nec plus Ultra, right? This feature is integrated in a category that TechFite can benefit from.

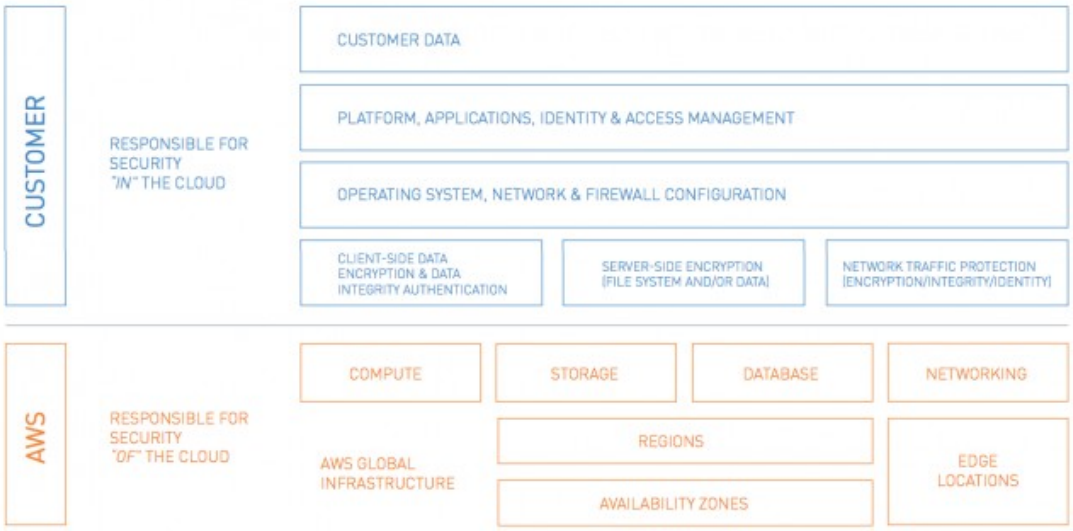
	AWS Security	**Azure Security**
Identity and access management	AWS Services that can be used to implement IAM: • AWS Secrets Manager • AWS Single Sign On • AWS STS	• Azure Active directory • Single sign on • multi-factor authentication

	• AWS Directory service • AWS organizations	
Detection controls	AWS services that can be used to provide monitoring and logging are: • Amazon GuardDuty • AWS Trusted advisor • Amazon VPC Flow logs • AWS Security Hub	• Azure Monitor logs • Azure Security Center monitors traffic, collects data and analyzes data for threats)
Infrastructure protection	• AWS System manager • AWS Firewall manager • AWS Direct connect • AWS Cloud formation	• Customer data is protected by: • Hypervisor firewall • Native host firewall • Host firewall
Data protection	• Client-side encryption • Server-side encryption • AWS Cloud HSM • Amazon S3 glacier • AWS certificate manager • Amazon Macie	• Encryption of data at rest • Encryption of data in transit • Azure Disk encryption • Key management with Azure Key Vault
Incident response	APIs for automating incident response • AWS CloudFormation • Performing forensics	The Security Incident Response team follows the Security Incident Response lifecycle: • Detect • Assess • Diagnose • Stabilize/Recover • Close

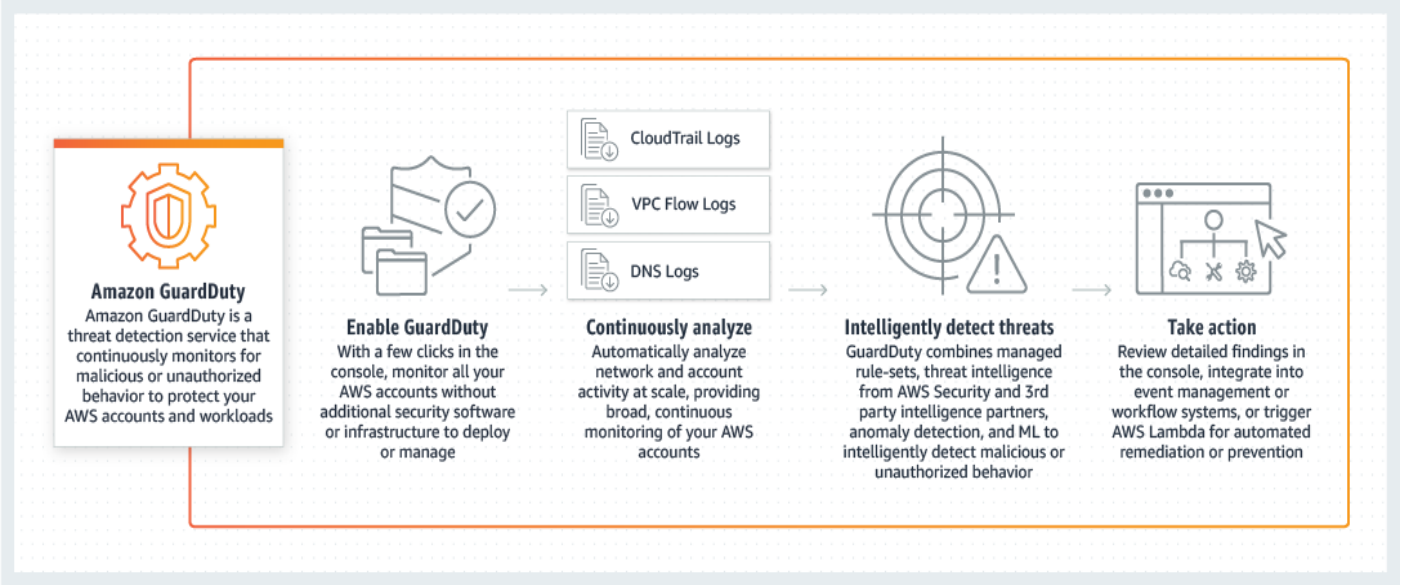


Picture: InfoSecTran

Also, the concept of the two layers approach and share responsibilities that AWS Security as a Service is based on is very interesting and englobe the security concern of TechFite: The security of the cloud and the security in the cloud. In this approach, TechFite's Administrators can configure their account that meet their need, they will have in charge the security in the cloud. AWS will have in charge the security of the cloud, which means they will secure the infrastructure. Microsoft AZURE has all securities in their hands Azure Security Center. I can trust more what I am participate in and have at least a broader view of what I am paying for. The drawback that TechFite is facing is the extensive training that the used of these tools need, but as professionals this should be overcome. The following scheme layout what the "Security of the cloud" and the "Security in the cloud" englobe and seen by Ajmal Kohgadai in its article "AWS infrastructure security best practices" published one of the McAfee's blog.



Evaluate: Amazon Web Services (AWS) Security as a Service is the solution, I recommend for TechFite to be successful. In the scope, I have said that TechFite need a security service that monitor and alert the Administrators when a potential attack is occurring on the network. Also, behavior analysis of incoming network traffic should be performed in real-time, so any denial of service (DoS) attack will be stopped and the hacker must be caught. AWS Security as a Service has a feature called Amazon GuardDuty. According to AWS website, “Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.” The following picture (pull from Amazon Web Services website) presents how the Artificial Intelligence (Amazon GuardDuty) works.



Amazon GuardDuty: How it works.

This tool will benefit TechFite as it will help the monitoring, the analysis, and alerting Administrators for any suspicious activities. Here are few benefits from Amazon GuardDuty:

- Threat detections developed and optimized for the cloud
- Automate threat response and remediation
- Threat severity levels for efficient prioritization

AWS Security as a Service is very flexible. TechFite can integrate Amazon's partners security pack. For example, Alert Logic SIEMless Threat Management is a security product approved by AWS Security and developed by ALERT LOGIC that can "Assess and detect the cyber threats relevant to your business running on the AWS ecosystem" according to AWS Security webpage.

Evangelize: This step allows ET team to praise the product that is chosen to implement the security system. The team should set up multiple meeting with the stakeholders and advocate their finding. In this case the team should evangelize AWS Security as a Service.

Transfer: AWS Security as a Service will be hand over to the entire IT department for implementation after the successful evangelization.

PART D

AWS Security as a Service, like all cloud computing, can have positives and negatives impact on TechFite business:

- ***One positive*** impact the implementation this emerging technology will have on TechFite is that the IT security team will be relieved and have peace of mind. The "security in the cloud" they will have in charge have bunch of security tools they can use to have peace. They even can get down to two staffers (senior security specialist and IT manager).
- ***One negative*** impact this implementation could have on TechFite business is the need for training. To be effective, TechFite's IT department will need ton of training. AWS have a plethora of security tools that TechFite's security staff will learn and this could impact the effectivity of the "security in the cloud" they will have in charge. To overcome this, TechFite could outsource the "security in the cloud" from AWS's partners. Indeed, AWS's flexibility allowed third party (like the giant SYMANTEC) to work with its customers for security related issue. Another solution is to hire AWS Security as a Service professional which can overlook the security "in the cloud".

PART E

An alternative to AWS Security as a Service is Microsoft Azure Security. The following table can summarize advantages and disadvantages for both AWS Security as a service and Microsoft Azure Security

Products	Advantages	Disadvantages
AWS Security as a Service	• Flexibility: allows users to integrate third party security features • Robust security tools like Amazon Security Hub, or GuardDuty.	• Not robust in term of hybrid cloud. • Too much services that eat up your bandwidth and everything slow down.
Microsoft AZURE	• Integrate its most popular applications like Office and SharePoint for secure collaboration • Proficient in hybrid cloud. TechFite can migrate gradually to the cloud.	• Most of Azure platform are Windows based which has higher rate of attack in Data Center • Storage Data encryption is managed only by AZURE team, there is no option for the customer to control its encryption key.

PART F

The method I recommend TechFite to use to determine if the adoption of this ET is a success or failure is to quantify how many hours it can save for the administrators in IT department. How many data logs can be reviewed in 24 hours period with this ET compare to the existing technology? TechFite is willing to review all logs of all incoming traffics. AWS GardDuty is an Artificial Intelligent tool that “analyzes tens of billions of events across multiple AWS data sources”, according to AWS Security webpage. This is far beyond what administrators can do.

References

Amazon GuardDuty. (2020). Retrieved May 6, 2020, from https://aws.amazon.com/guardduty/

Amidon, S. (2016). Security. Retrieved from https://aws.amazon.com/security/partner-solutions/#Consulting_Partners

Business, T. T. I. (n.d.). What is Artificial Intelligence and how did it start? Retrieved from http://blog.ttibusiness.com/what_is_artificial_intelligence_and_how_did_it_start

Introducing AWS Security Hub. (2018, November 28). Retrieved from https://aws.amazon.com/about-aws/whats-new/2018/11/introducing-aws-security-hub/

Kohgadai, A. (2019, November 9). 51 AWS Security Best Practices Everyone Should Follow: McAfee. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/aws-security-best-practices/

Manikandan, J. (n.d.). AWS Security vs Azure Security: Retrieved from https://www.infosectrain.com/blog/aws-security-vs-azure-security/

Ranger, S. (2018, December 13). What is cloud computing? Everything you need to know about the cloud, explained. Retrieved from https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/