ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #35818

The Fast and Practical Approach to Effectively Securing a Cloud Computing System with Today's Technology

Mr. Emmanuel Sunday Kolawole

Emmanuel S Kolawole is a PHD Student at Prairie View A&M University and currently working as a Network Security Engineer in one of the giant Semi-Conductor/IT Industries in USA. In his current role, he is responsible for planning, design and build security architectures. Emmanuel supervise the implementation of network and computer security and ensuring compliance with corporate cyber security policies and procedures.He monitors cyber security requirements for local area networks (LAN), wide area networks (WAN), virtual private networks (VPN), routers, firewalls, proxy and related network devices. He is skilled in security assessments of applications and systems using vulnerability testing and risk analysis by not only implementing software fixes (patches) to remve system vulnerabilities, but also provide cyber security-related incident responses through post-event analysis. He is practically oriented and loves to troubleshoot issues and provide neccessary solutions at all times.

Dr. Penrose Cofie, Prairie View A&M University

Dr. Penrose Cofie is a professor in Electrical and Computer Engineering at Prairie View A&M University, College of Engineering, Texas. His research interests are in Power Systems including Renewable Power Supplies, Power Electronics, Controls and Motor Drives. He is currently working on Renewable Energy Generation, Micro Grid and Advanced Electric Vehicle Technology Systems.

Dr. John Fuller P.E., Prairie View A&M University

Professor at Prairie View A&M University in the Department of Electrical and Computer Engineering. Also Texas A&M System Regents Professor with 45 years of teaching and research at PVAMU. Primary area of research is power with present concentration on solar energy research. Currently designing and procuring a solar energy system on the campus of PVAMU.

The Fast and Practical Approach to Effectively Securing a Cloud Computing System with Today's Technology

Emmanuel S Kolawole, Dr Penrose Cofie, Dr Warsame Ali, Dr John Fuller
Electrical/Computer Engineering Department
Prairie View A&M University, Prairie View, Texas

Abstract

The daily evolution of technological advancement has embodied the rapid growth of information Technology infrastructure. The invention of the internet has continued to increase the use of computers and mobile devices. Nowadays, many people in the world use these devices, and as a result, a large amount of data is stored in these devices and each device on the internet is required to be connected to each other because of sharing information. This innovation has brought about Cloud computing which is Internet-based computing where shared resources, software, and information are provided to computers and devices on-demand. Since cloud computing uses distributed resources in an open environment, it is important to provide security and trust to share the data in a secured manner for developing cloud computing applications. In this paper, emphases are laid on the practical ways to secure the IT including Cloud security with the use of one of the latest technologies, Stealthwatch. Deploying Stealthwatch in a cloud environment ensures security best practice and set of controls are anchored, implemented, and use for key security baselines. Also, using Stealthwatch tool to create a security baseline for both on-prem and cloud environment contributes to risk mitigation and sound security hygiene. In recent times, securing our IT environment has become the key factor in the industry. Therefore, using the right tools to enhance optimum security both on-prem and cloud environments are discussed.

Introduction

The expansion in Cloud adoption has raised some security issues in cloud computing environments. Because Cloud computing uses distributed resources in open environment, it is important to provide the security and trust to share the data in computing applications. Cloud infrastructures generally are large, so the greatest benefit in this standardization and automation are keeping management costs low [1]. The cloud infrastructure can operate under the complete control of the hardware owner, who provides security and control, as with private cloud deployments. Because it is quite expensive to establish, smaller companies and individuals typically use cloud infrastructures as a service. If you are deploying a cloud, you are deploying a network of systems from which you offer computing resources to remote users (business or consumer). There are generally three ways a cloud can be deployed. The first one is public cloud which is provisioned for open use and is managed by a dedicated cloud service provider. The public cloud resides on premises with the cloud provider, and it may be owned, managed, and operated by a business, academic institution, or government organization, or any combination of the three. Second is the private cloud which comes with benefits such as cost savings, energy savings, rapid deployment, and customer empowerment. When a company has hired a private cloud service, the private cloud will scale by pooling IT resources under a single cloud operating system or management platform. The last one is the hybrid cloud which is a combination of public and private clouds [7]. Hybrid clouds enable you to retain control over data as with private clouds while maintaining the flexibility and reach of public clouds. For hybrid solutions to

provide data protection, we must take great care regarding traffic management. If sensitive data passes the public cloud infrastructure, it can still be compromised. A hybrid cloud deployment involves utilizing a private cloud within a company's firewall, in addition to public cloud services from a service provider.

The Key Cloud Service Delivery Models

In a traditional data center, the IT staff is responsible for the entire stack, which includes hardware, networking, physical storage, the operating system, application data and the application software, and so on. Cloud service models describe how cloud services are made available to clients. Most fundamental service models include a combination of System layer called IaaS (Infrastructure as a service), the Platform layer called PaaS (Platform as a service), and the Application layer called SaaS (software as a service) [2].

[a] *Infrastructure as a Service Model (IaaS)*

IaaS, also described as cloud infrastructure services, can deliver computer infrastructure (typically, a platform virtualization environment) as a service which is represented in figure 1. With IaaS, pre-configured hardware resources are provided to users through a virtual interface [3].

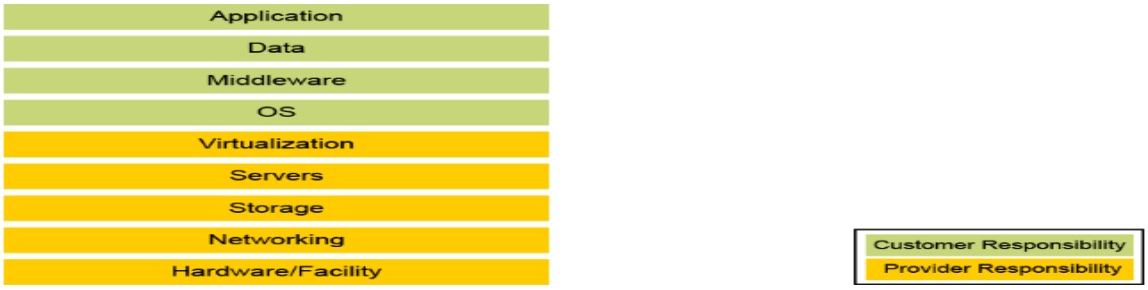

Figure 1: Security responsibilities in Infrastructure as a Service Model (IaaS)

[b] *Platform as a Service Model (PaaS)*

PaaS is the delivery of a computing platform and solution stack as a service. When using PaaS, the customer is only responsible for the application software and application data as shown in Figure 2. The customer is not required to run the operating system or any middleware that is running to support the application.

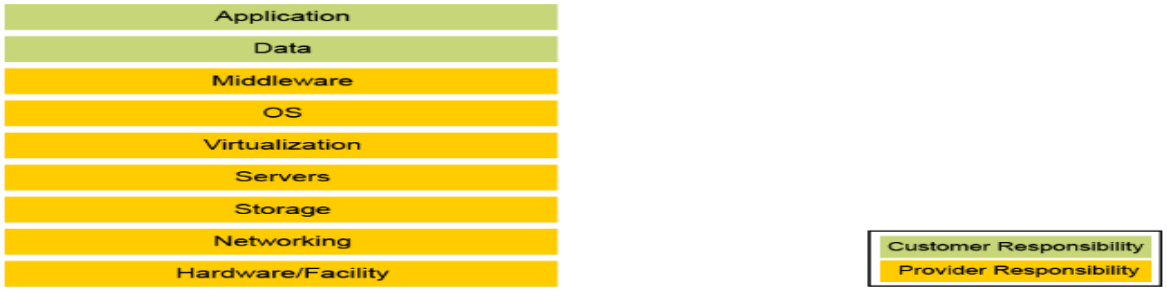

Figure 2: Security responsibilities in Platform as a Service Model (PaaS)

[c] *Software as a Service Model (SaaS)*

With the SaaS model, cloud service providers offer ready-to-use applications or software that runs on a cloud infrastructure to the end customers as shown in Figure 3. The applications are accessible from various client devices through either a thin-client interface, SaaS is a software licensing and delivery model where a fully functional and complete software product is delivered to users over the web on a subscription basis [3]. The only thing that a SaaS customer is responsible for is the secure utilization of the application in question [5].

Figure 3: Security responsibilities in Software as a Service Model (SaaS)

Common Cloud Security Attacks for Cloud Based Computing

In today's technology, the cloud had opened a whole new frontier for storage, access, flexibility, and productivity which has enhanced a new world of security concerns. SaaS, PaaS and IaaS also disclose information security issues and risks of cloud computing systems. Though Cloud computing might be seen as a remedial solution to all problems but despite its advantages, there are several considerable drawbacks that should be taken into consideration Transferring enterprise IT to the cloud is a complex task that includes both technical and organizational challenges. [4,8,9].

Some top Security Concerns for Cloud-Based Services:

- *Data Breaches*: It is defined as the leakage of sensitive customers' or organizations' data to unauthorized users. In the same scenario, data breach from organization can have a very huge impact on its business regarding finance, trust, loss of customers as well as loss of intellectual properties [3,11].
- *Hijacking of Accounts*: Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [10].
- *Insider Threat*: Inside Track on Insider Threats is an attack from within the organization. which was the misuse of information through malicious intent, accidents or malware. Employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information [10].
- *Malware Injection*. Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves [3,11].

Network Attacks: A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.

- *Multi-tenancy:* Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server [10].
- *Abuse of Cloud Services:* The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily [3,11]. Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking or password [10].
- *Insecure API:* Application Programming Interfaces (API) give users the opportunity to customize their cloud experience. APIs give programmers the tools to build their programs to integrate their applications with other job-critical software. The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks [10].
- *Insufficient Due diligence:* In today's technology, security gap occurs when an organization does not have a clear plan for its goals, resources, and policies for the cloud [3,11]. Additionally, insufficient due diligence can pose a security risk when an organization migrates to the cloud quickly without properly anticipating that the services will not match customer's expectation.
- *Shared Vulnerabilities*: Cloud security is a shared responsibility between the provider and the client. This partnership between client and provider requires the client to take preventative actions to protect their data [3,11]. The bottom line is that clients and providers have shared responsibilities and omitting yours can result in your data being compromised.
- *Data Loss*: Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider [3,11]. Losing vital information can be devastating to businesses that don't have a recovery plan.
- *Malware Injection*: Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves [3]. Hackers exploit vulnerabilities of a web application and embed malicious codes into it changing the course of its normal execution.

Design and Implementation of Fast and Practical Approach to Securing a Cloud Environment Using Secure Network Analytics (Stealthwatch)

Organizations use cloud monitoring to proactively prevent issues with access, performance, and security in the cloud environment [6]. The goal of cloud monitoring is to detect and correct issues before they affect applications, users, or business objectives. In this paper, we will showcase how Stealthwatch Enterprise/Cloud infrastructure as one of today's technologies can effectively secure both the on-prem and cloud services. Cisco Stealthwatch drastically enhances threat defense by giving detailed network visibility and security analytics. It helps you know every host, record every conversation, understand what is normal, it alerts you to change, and enables you to respond to threats quickly. Stealthwatch applies machine learning and statistical modeling to the network telemetry collected from across the extended network, including data center, branch, endpoints and cloud. Stealthwatch collects telemetry from every part of the

network and applies advanced security analytics to the data. It creates a baseline of normal web and network activity for a network host and applies context-aware analysis to automatically detect anomalous behaviors. Stealthwatch can identify a wide range of attacks, including malware, zero-day attacks, distributed denial-of-service (DDoS) attempts, advanced persistent threats (APTs), and inside threats. Figures 4 and 5 show the design architecture of Stealthwatch from our LAB, which is a physical testing environment where this implementation was carried out. It is an isolated environment where some virtual machines (VMs) are created for installing the Flow Sensor, Flow Collectors and SMC to carry out the practical analysis and simulations for real practical analysis and monitoring.

As shown in Figure 4 below, the Flow Sensor is configured and designed to receive all spanning traffic flows for the environments though the switch and send them to Flow collector. The flow collector receives the traffic flows from Flow Sensor, compressed it in which SMC (Stealthwatch Central Management) then pulled for analytics and make decision based on baseline and policy deployments. If there are any deviations from the baseline or threshold based on policy configured in the environments, alerts/alarm will be generated for immediate action be it mitigation/ remediation or blocks as the case may be.

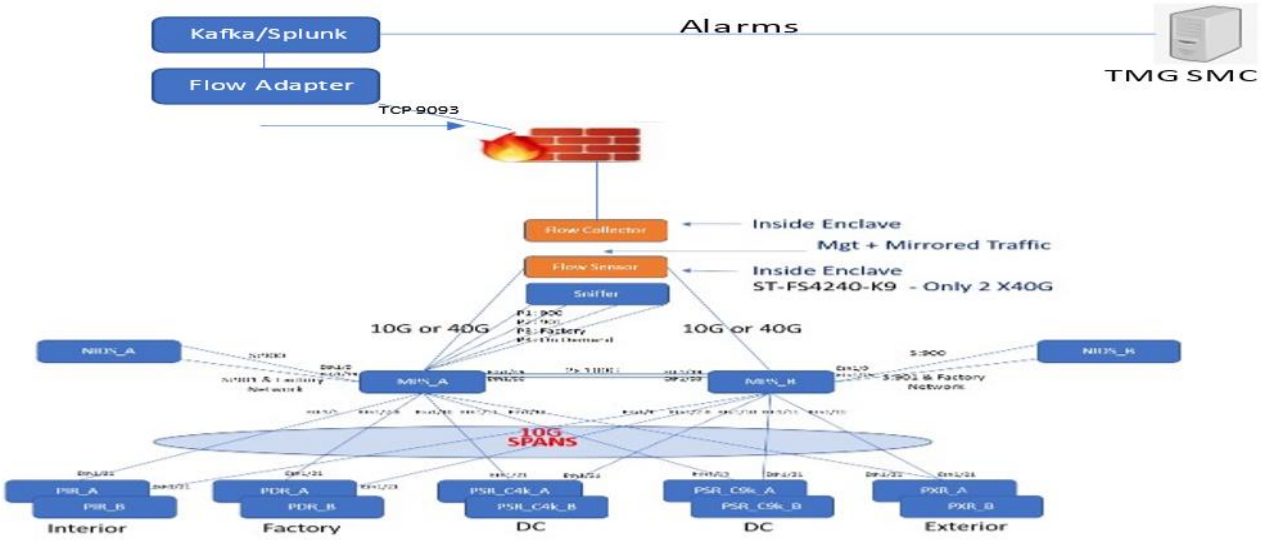

Figure 4: StealthWatch design

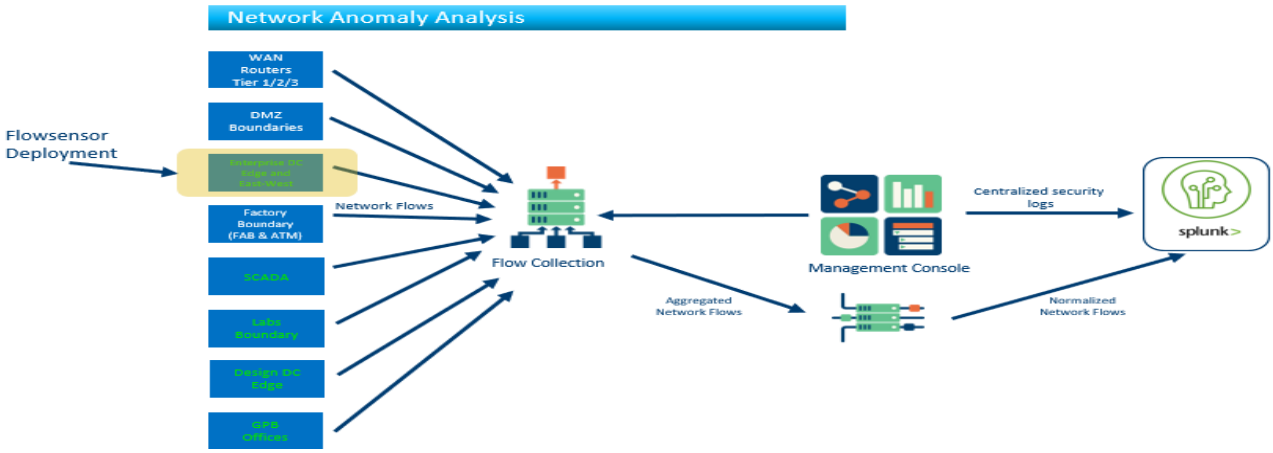

Figure 5: Network Flow Anomaly Analysis Framework

Secure Network Analytics Implementation Results and Simulations

Once the design was completed and all the components were connected per the design as shown in Figure 4, Figure 6 show the Stealthwatch simulation results and how attacks are identified and mitigated based on analytics information gathering in the LAB [Isolated testing environment] based on alarm categories.

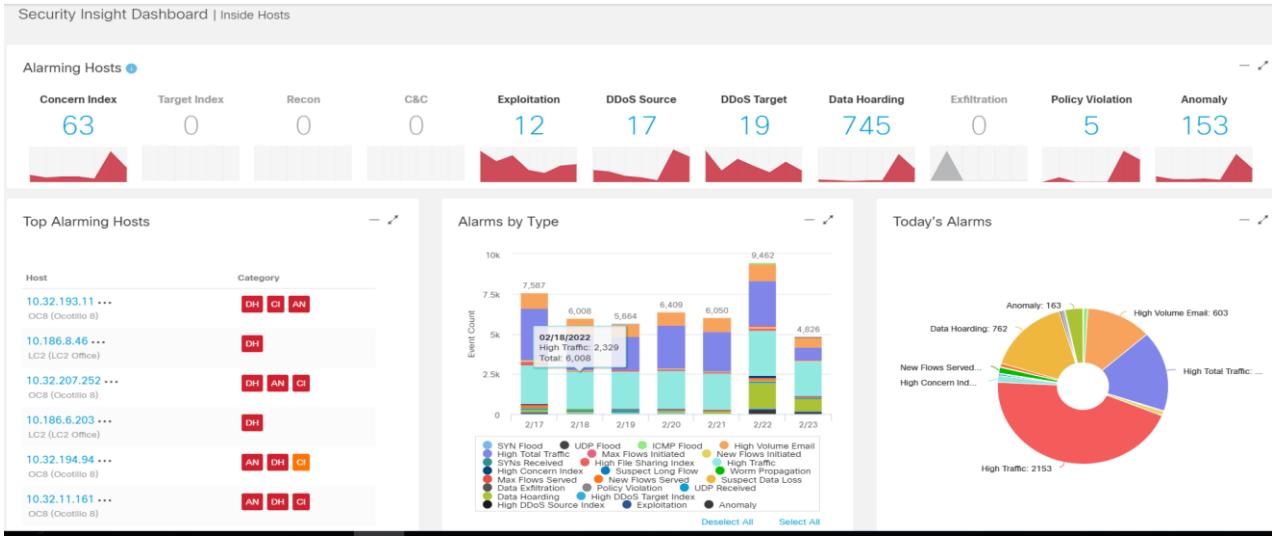

Figure 6: Network Security analytics dashboard

Alarm Categories

An alarm category is a “bucket” toward which a defined list of security events contributes index points. When network activity meets or exceeds a defined set of criteria specified for this alarm category, it triggers an alarm. Each alarm category has its own list of security events that contribute index points to it and can cause it to generate alarms. A security event is an algorithm that looks for specific behavior and can alert on that behavior on your network, depending on settings applied in policies. Below are details on the dashboard alarm categories shown in Figure 6.

Concern Index and Target Index

Tracks hosts whose concern index has either exceeded the Concern Index (CI) threshold or rapidly increased. If an event is triggered by a source host, it results in a Concern Index alarm. If an event is triggered by a target host, it results in a Target Index alarm.

Recon

Indicates the presence of unauthorized and potentially malicious scans using TCP or UDP and being run against your organization's hosts.

Command & Control

Indicates the existence of bot-infected servers or hosts in your network attempting to contact a C&C server.

Exploitation

Tracks direct attempts by hosts to compromise each other, such as through worm propagation and brute force password cracking.

DDoS Source

Indicates that a host has been identified as the source of a DDoS attack.

DDoS Target

Indicates that a host has been identified as the target of a DDoS attack.

Data Hoarding

Indicates that a source or target host within a network has downloaded an unusual amount of data from one or more hosts.

Exfiltration

Tracks inside and outside hosts to which an abnormal amount of data has been transferred. If a host triggers a number of these events exceeding a configured threshold, it results in a Data Exfiltration alarm.

Policy Violation

The subject is exhibiting behavior that violates normal network policies.

Anomaly

Tracks events that indicate that hosts are behaving abnormally or generating traffic that is unusual but is not consistent with another category of activity.

Figures 7 and 8 below show flow collection thread and top applications that have been consumed or used based on defined baseline polices for analysis. It displays the flow thread based on baseline defined and if there is any anomaly.

Figure 7: Network Security analytics flows gathering on SMC WEB GUI

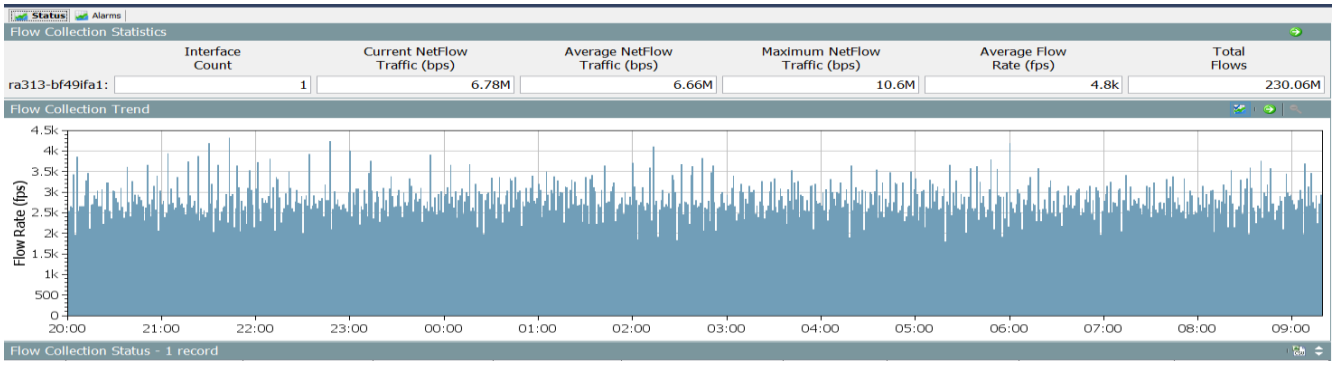

Figure 8: Network Security analytics flows gathering on SMC CLIENT

Comments on Results

From the above real practical experiments as shown in Figures 4 and 5 display how the main components of Stealthwatch tools such as Flow Sensor, Flow Collector and Stealthwatch Management Console (SMC) are connected for proper visibility into the entire

environments/Networks for traffic and flow analysis. The simulations in Figures 7 and 8 show effectively how Stealthwatch tool can detect any anomaly on the network that has been deviated from the baseline by watching the flows level which generates alerts if something happens. Also, the dashboard as shown in Figure 6 display every second, the current behavior on the network and send alerts to the administrator if something deviates from the baseline, for immediate action. This is achieved by the alerts that generates from the SMC based on the analytics baseline configurations and send alerts to the administrator in case of any issue for immediate action.

Summary and Conclusion

In this paper, we have been able to explore and explain what cloud services are and its importance in this growing economy and technology. We are able to show that cloud computing is the over-the-internet delivery of computing services to offer faster innovation, flexible resources, and economies of scale. Thus, not all clouds are the same and no one type of cloud computing is right for every situation. Understanding the different models, types, and services available can enable one to find the right solution. Overall, we demonstrate the practical analysis using one of the latest technology tools in the industry, "Stealthwatch", today to show-case the effectiveness of Cloud security monitoring. From there, we can see how the tool can capture anomaly behaviors on the entire network every second and take proper action by either blocking or sending alerts to the administration for remediation or any other actions needed based on the level of severity. Sometimes, there might be some type of false positive alerts, but with the help of proper policy tunning and configurations, those alerts are automatically taken care of based on baseline definitions. This tool has proved to be very effective with this real practical scenario by properly tracking every activity on the network and sending alerts or taking appropriate action if any behavior deviates from the baseline, which then relates to the effectiveness of the Stealthwatch tool for immediate remediation or mitigation of attacks. To expand this research, we will explore how to effectively use the Stealthwatch tool to monitor and protect the Electrical Smart Grid from DDoS Cyber-Attack.

References

[1] NIST, "The NIST definition of cloud computing", http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.p df. Accessed on 12 Aug, 2015.

[2] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy," Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

[3] http://en.wikipedia.org/wiki/Cloud_computing

[4] Kashif M and Prof Dr. Sellapan P, "Framework for Secure Cloud Computing". International Journal on Cloud Computing Services and Architecture, (IJCCSA), Vol. 3, No. 2, April 2013.

[5] J. Stirling, "HP unveils more public loud service info", http://www.itpro.co.uk/639508/hp-unveils-more-public-clouds service-info. 12.3.2012.

[6] https://www.cisco.com

[7] Te-Shun Chou, "Security Threats on Cloud Computing Vulnerabilities International Journal of," Computer Science & Information Technology (IJCSIT) Vol. 5, No 3, June 2013

[8] Kolawole, E.S., Ali, W.H., Penrose, C. and Fuller, J.C. (2017), Practical Approaches to Securing an IT Environment. Communications and Network, 9, 275-290.

[9] Emmanuel k, etal, "Security Issues, Threats and Possible Solutions in Cloud Computing". American Journal of Information Science and Computer Engineering Vol. 5, No. 2, 2019, pp. 38-46.

[10] Kashif M and Prof Dr. Sellapan P, "Framework for Secure Cloud Computing International Journal on Cloud Computing" Services and Architecture, (IJCCSA), Vol. 3, No. 2, April 2013.

[11] https://www.incapsula.com/blog/top-10-cloud-security-concern