**Introduction**

Security Information and Event Management Systems (SIEM) has been widely used as robust tools for detection, prevention, and response against attacks on information security as mentioned by González-Granadillo et al., SIEM solutions have been evolving to meet the demands of advancing technology. The systems are becoming more comprehensive to provide a wide range of visibility for the identification of high-risk areas and focusing on the mitigation strategies aimed at minimizing costs and time taken to respond to attacks. González-Granadillo et al., further states that SIEM systems today are built upon or are integrated with big data analytics and artificial intelligence tools [1].

Redback Operations is looking to invest in more robust and apprehensive SIEM systems to curb the increasing number of cyberattacks that have affected the information technology industry, which has substantially grown over the past years. Additionally, Redback Operations is implementing SIEM systems to operate legally in the industries. According to Miloslavskaya, this is due to the many complicated regulations and compliances that companies must conform to for them to stay operational as [2]. There are many SIEM systems today, however, this research will focus on Google SIEM. This paper will provide comprehensive research on the Google SIEM system. It will discuss the features of the Google SIEM systems, how it is going to be implemented into the GCP of the company, and the benefits the company will gain from implementing google SIEM.

# **Google SIEM**

Security Information and Event Management SIEM, is a technology that helps companies with threats detection, prevention, compliance, and security incident management by collecting and analyzing real-time and historical, security events, a wide range of other events, and appropriate data sources. SIEM system works by merging two technologies, Security Information Management (SIM), and Security Event Management (SEM) as suggested by a study [3]. SIM is used for collecting data from files for analyses and reporting security threats and occurrences. On the other hand, SEM works by conducting real-time system monitoring and notifying the network administrator of significant issues, and establishing associations between the security events [3].

A typical SIEM system works by providing real-time visibility across the organization’s information security system, establishing correlations between events gathered from the collected data and the security events, consolidating data from various sources, and automatically notifying the network administrator of any problem in the information security system (Díaz López et al., 2018). Many companies have developed their SIEM software to be used for detecting attacks and irregularities in the information technology system. Some of these companies include HP, IBM, McAfee, until, Google, RSA, Splunk, and many others.

Google's SIEM system is known as Chronicle. It is a software as a service (SaaS) product that is built on the core of Google infrastructure. From certain research [4], Chronicle utilizes data platforms used by Google to power its biggest products to deal with the collection, hunting, correlation, detection, and reporting of on-premises and multi-cloud, security logs. It uses raw and normalized logs by making them available for searching, detecting, and reporting. Additionally, Chronicle works by removing the existing barrier that has been between having a massive amount of data and slow performance, which has enabled its clients to scale and hunt millions of data [4]. Chronicle’s main objective is to deliver a modern threat detection and investigation system with integrated intelligence, using unprecedented speed and scale at a disruptive and affordable price.

Google SIEM system is built to perform analyses on such massive amounts of network and security telemetry that companies generate. It helps to normalize, index, correlates, and analyze data to supply instant analysis and the framework threats, and risks in the organization. The system helps the company to investigate the aggregated security information for a long period. This can be achieved by using the Chronicle search in all the domains that are accessible within the organization. Furthermore, it allows the organization to narrow the search to a specific domain, IP address, or asset to determine if any compromises have occurred.

# **Features and Capabilities of Google SIEM**

Today’s worst reality in the information technology sector is that no matter how advanced or robust technologies are, companies cannot stop all the cyberattacks presented in the IT environment. Often at times, viruses and malware find a way to infiltrate the networks. Therefore, without detection and prevention measures, the malware may end up residing in the network for months on end. For this reason, it is important to be aware of the features and capabilities of every system implemented in the company. In their paper, Mokalled et al., suggest that this knowledge enables a company to select the most suitable solution that will suit its needs and demands [5]. For the Google SIEM system, the company should look for the following features and capabilities:

1. Log management: One of the main features of the Google SIEM system is to collect and store data from multiple and heterogeneous sources. As mentioned by Mokalled et al., the data is then consolidated in a central location for Redback Operations’ information security team to access the information easily [6]. Additionally, the log management feature enables the Redback Operations to reformat the data, it receives and makes it more consistent, plus makes the process of analysis much easier.
2. Threat intelligence feeds connections: The SIEM system must be able to stay up to date with threat intelligence, which includes evolution, resolution, and propagation. The system should be able to provide real-time streams of data that provide information on the potential cyberattacks and risks
3. Integrations and APIs: The SIEM system should be able to provide high-performance APIs that will expose the functionality to downstream enterprises and tools. It should also be able to send data directly and smoothly within Redback Operations systems and networks such that members can easily access them. It should also be compatible with various systems within the company to ensure easy integration.
4. Security alerts: The system should keep the security team updated immediately when the system detects a potential threat [6].
5. Security events correlation: The SIEM system must be able to analyze and evaluate every accumulated data from the log management and investigate for any signs of cyberattack, data, breach, or threat infiltration. Additionally, the system should unify individual security telemetry into one timeline [6].
6. Machine learning: This is a new feature among SIEM solutions. It is however important for the solution to have a machine learning feature to allow the system to learn from historical events, as well as find indicators automatically, and be able to adapt to new environments without input from the security team. This makes the system more efficient and effective in terms of threat management.
7. Dashboard and reporting: The system should be able to simplify its findings from the intelligence feeds and present them to the security team, or the audience in ways that can be easily understood. This will give the security team an easy time making sense of the data presented by the Google SIEM system.

# **Implementing Google SIEM into GCP**

Many companies today are integrating Google Cloud Platforms (GCP) into their operations due to its stability and numerous built-in services. However, while the GCP security command center serves many purposes, it is limited to GCP-specific sources only. For this reason, it is recommended to implement the SIEM system to enable GCP to aggregate all the data and to ensure compliance within the platform. While many legacy SIEM systems do not support GCP, Google SIEM seamlessly integrates with the GCP. For Redback Operations to integrate GCP with the SIEM, there are two options to choose from. This includes pushing logs to logSentinel SIEM and pulling logs from GCB. Pulling logs is mostly used for on-premise SIEM setups which regularly take place in the background. This method allows Redback Operations to install SIEM locally and avoid exposing their systems to the Internet which is required to receive post loans from the GCP. Below is the illustration of the instructions to implement SIEM to GCP using the pulling logs method

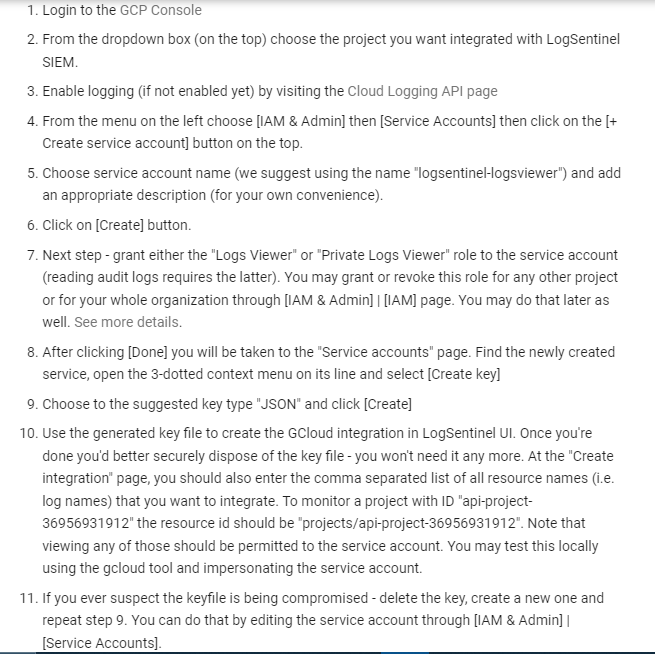


Figure 1: Steps to implementing Google SIEMS into the GCP using the pulling logs from GCP method

Pushing logs is more flexible, and relies more on the native GCP log router configuration. Below is the illustration of the instructions: to implement SIEM to GCP using the pushing logs method.

# **Benefits of Implementing Google SIEM**

Figure 2: Steps to implementing Google SIEMS into the GCP using the pushing logs to logSentinel SIEM method

Different organizations use SIEM systems for different purposes. Despite this, the general purpose of having a SIEM system is to ensure Redback Operations has consistent high-quality security and visibility of their network. SIEM is one of the most critical systems in the company. By implementing SIEM, the company will enjoy the following benefits:

1. Visibility and data aggregation: Despite the size of Redback Operations, the Google SIEM tool will provide real-time and comprehensive visibility across all networks, systems, databases, and applications in the organization. Additionally, given that the company generates massive data from numerous sources, and in various formats, the Google SIEM tool comes in handy to make sense of the data by automatically aggregating and normalizing the data. Not only will Google SIEM collect and store data in a centralized location, but it will also normalize data to uniform formats that can be easily compared to, analyzed, interpreted, and find correlations that will help in detecting and preventing security threats and incidences.
2. Threats and Vulnerabilities detection: Many organizations have suffered data breaches and malware infiltration that have cost them millions, and a damaged reputation. Additionally, cyberattacks have become more advanced and sophisticated in that they are now able to pass through detection systems and reside in the network for an unprecedented amount of time. Having implemented the Google SIEM system will help with collecting and analyzing log data generated by assets within Redback Operations, and can detect incidences that could be otherwise missed if the logs were not analyzed. Analyzing the data logs enables the system to recreate the occurrences that have happened and determine the exact nature of the attack or infiltration, and whether it succeeded or not. Once the infiltration or the threat has been detected, the system will alert the administrator or the IT security team and provide a report on the scope of the attack which will enable them to respond accordingly.
3. Enhanced efficiency: Implementing the Google SIEM tool will significantly improve the efficiency of the security team. Google SIEM tool simplifies and automates most of the security work that could have been handled by the security team. For instance, the system automatically analyses, interprets, finds correlations, and reports on its findings on risks and potential threats to the security of the network. Its reporting feature simplifies data and findings by presenting them in ways that can be easily interpreted by the security team. Additionally, it also has an automated mechanism that uses data correlation and analysis to stop attacks and infiltration as soon as they are detected, or when the attack is still in progress, thus minimizing the impact of the attack.
4. Simplified compliance reporting: According to Caldeira, every organization across all industries, have some regulations and policies they must comply with. It is difficult and time-consuming to ensure compliance with all the regulations, as well as provide evidence that the organization is complying [7]. Google SIEM system comes in handy through its capabilities of collecting, normalizing, and organizing log data which helps to simplify the compliance reporting process. Many compliance reports and customized reports that include all relevant long, security events across the company [7]. Implementing Google SIEM is beneficial to Redback Operations as it provides centralized logging capabilities. Redback Operations will no longer need to manually, retrieve the data from every database, network, system, and application within the IT environment, nor will it be forced to generate individual reports from the individual assets, then assemble them into a single report.

# **Conclusion**

Google SIEM system is a great security tool the company will significantly benefit from. Its objectives of providing real-time visibility across Redback Operations Company, information, and security system, establish relations between events gathered from the collecting data and security events, consolidate data from the resources, and automatically notify the administrator of any problem in the information security system, its robust capabilities, and features, and its numerous benefits, it is recommended that the company implement the Google SIEM system.

# **References**

[1] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. <https://doi.org/10.3390/s21144759>

[2] Miloslavskaya, N. (2017). Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. *Advances in Intelligent Systems and Computing*, 282–288. <https://doi.org/10.1007/978-3-319-63940-6_40>

[3] Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., Nespoli, P., & Gómez Mármol, F. (2018). Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. *Wireless Communications and Mobile Computing*, *2018*, 1–18. <https://doi.org/10.1155/2018/3029638>

[4] Uehara, M. (2021). Zero Trust Security in the Mist Architecture. *Complex, Intelligent and Software Intensive Systems*, *278*, 185–194. https://doi.org/10.1007/978-3-030-79725-6\_18

[5] Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2019). The Applicability of a SIEM Solution: Requirements and Evaluation. *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. <https://doi.org/10.1109/wetice.2019.00036>

[6] Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2020). The Guidelines to Adopt an Applicable SIEM Solution. *Journal of Information Security*, *11*(01), 46–70. <https://doi.org/10.4236/jis.2020.111003>

[7] Caldeira, H. (2021). *Security Information and Event Management (SIEM) Implementation Recommendations to Enhance Network Security - ProQuest*. Www.proquest.com. <https://www.proquest.com/openview/9e4526ef3c8c179fc9128f72132a9eee/1?pq-origsite=gscholar&cbl=18750&diss=y>