# SIEMs and Google Chronicle

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Name | Description | Version |
| 01/08/2022 | Warrick Bickerton | First revision created | V1.0 |
| 06/08/2022 | Warrick Bickerton | Edited Revision | V1.1 |
| 13/09/2022 | Warrick Bickerton | Edited Revision | V1.2 |

Version Control

Contents

[SIEMs and Google Chronicle 1](#_Toc113961604)

[Introduction 3](#_Toc113961605)

[How does a SIEM work? 3](#_Toc113961606)

[Benefits and Disadvantages of a SIEM 4](#_Toc113961607)

[Google Chronicle 4](#_Toc113961608)

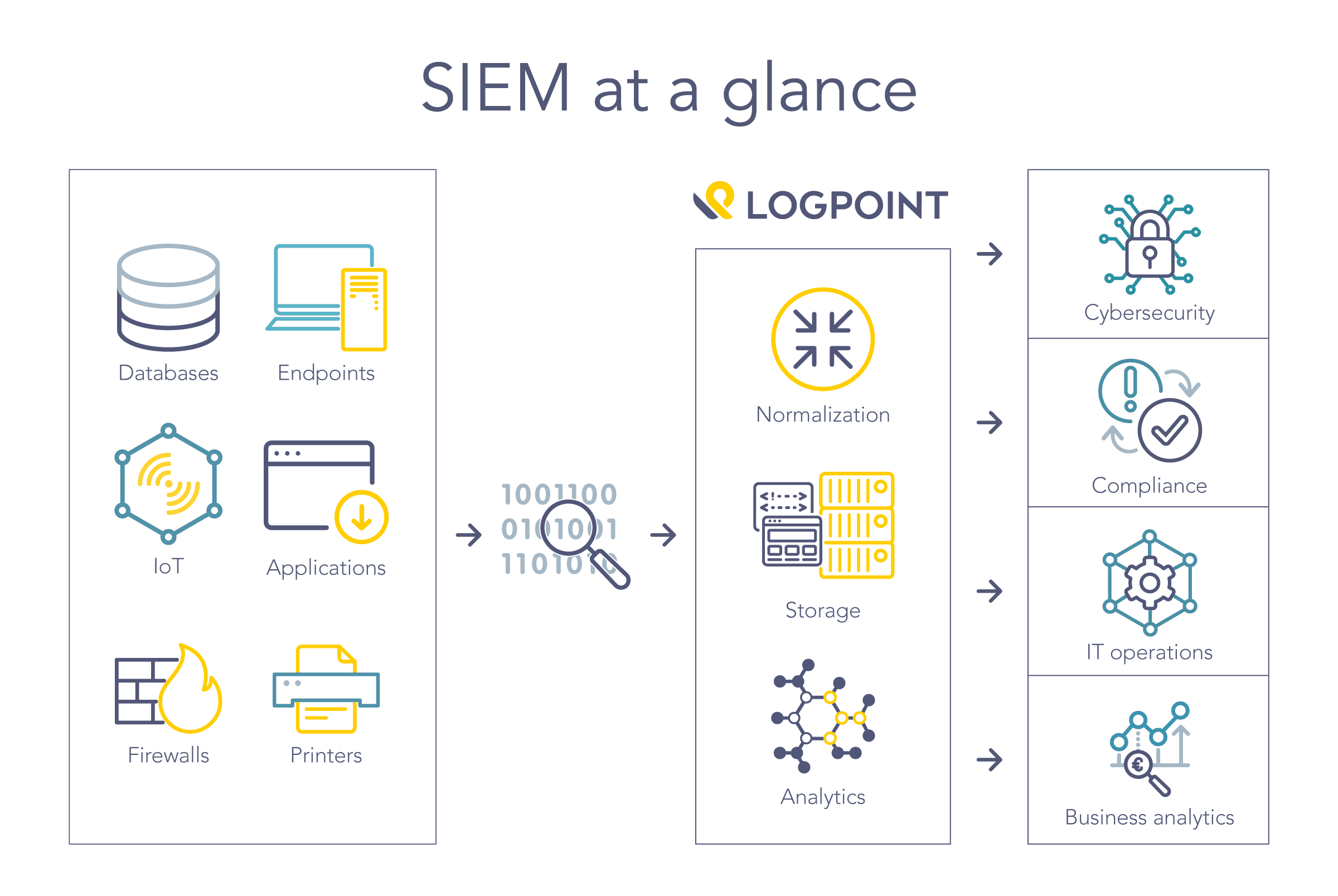
[Conclusion 6](#_Toc113961609)

[Reference list 6](#_Toc113961610)

## Introduction

International Business Machines Corporation (IBM) [1] states that Security information and event management (SIEM) is a security solution that enables companies like Redback operations to identify cyber security threats and vulnerabilities before they negatively impact business operations. There are multiple SIEM solutions currently used throughout the Cyber security industry which include Splunk, LogRhythm, IBM QRadar, and Microsoft Azure Sentinel. Because the Redbacks DevOps team has indicated they will be using google cloud It is recommended that the DevOps team implements the Google Chronicle SIEM in their cloud environment because of the ease of integration and included cost within google cloud.

## How does a SIEM work?

SIEMs combine several sources of security alerts, log data, and events into one easily accessible platform, enabling cybersecurity analysts to conduct real-time security monitoring [4]. The SIEM software works by collecting and storing ‘…log and event data produced from applications, devices, networks, infrastructure, and systems’ [4]. This can either take the form of an on-premises or Cloud SIEM solution. Implementing an on-premises or cloud SIEM enables the cybersecurity team to conduct analysis on daily operations and provides a single platform to view the entire organization’s information technology infrastructure activity. A high-level operation of the LOGPOINT SIEM can be seen in figure 1 below.

[7] From “What is SIEM? A complete guide to Security Information and Event Management” by LOGPOINT, N/A, <https://www.logpoint.com/en/understand/what-is-siem/>.

Figure 1 How the LOGPOINT SIEM works

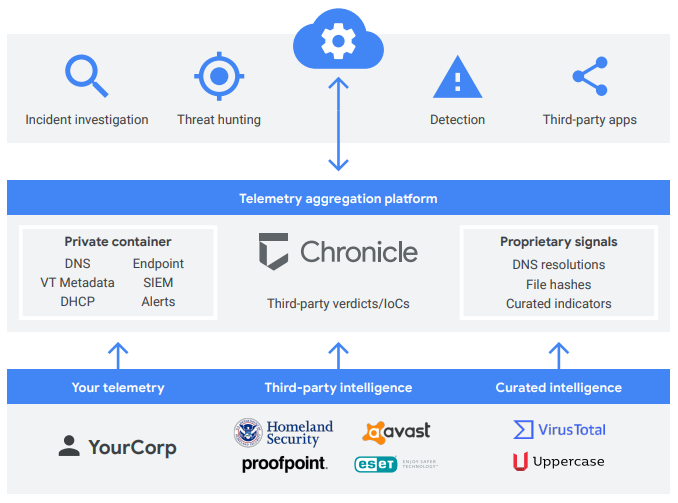
## Benefits and Disadvantages of a SIEM

No matter how big or small the organization’s IT infrastructure might be SIEM can provide benefits from data compliance to stop cyber-attacks. **PeerSpot [2]** states that the following list is the top five benefits of having a SIEM:

* **Improved efficiency and speed of security Operations**
* **Increased accuracy of security alerts and threat detection**
* **Higher level security of data**
* **Improved network visibility**
* **Compliance is increased**

**These befits don’t come without disadvantages. PeerSpot [2] argues that the main disadvantage is the cost of implementing a SIEM system. This cost can be up to thousands or tens of thousands of dollars, depending on the organization’s size. Another disadvantage can be the effort to configure a system. However, regarding Redback’s situation, google chronicle is a native google cloud SIEM platform which should keep costs low and make integration straightforward [3].**  Therefore, it is recommended that Redback operations implement Google Chronicle SIEM within their own google cloud environment to enable the organization to investigate and respond to any cyber-attack or data breaches that may occur.

## Google Chronicle

Google Cloud [5] states that its chronicle platform is “a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyse, and search the massive amounts of security and network telemetry they generate.” Google chronicle will also normalize and correlates this collected data on its own to provide real-time analysis of any suspicious activity occurring in the cloud environment [5]. Figure 2 below provides an overview of the google chronicle service.

From “Chronicle overview” by Google Cloud, N/A, <https://cloud.google.com/chronicle/docs/overview>.

[5] Figure 2 Overview of how Google Chronicle functions

Google [5] states that the security and network data can be collected in three ways:

* Forwarder – a small software component installed onto the Redbacks network that collects system logs, packet capture, and SIEM data repositories.
* Ingestion APIs: APIs allow the logs to be sent straight to the Chronicle platform, therefore additional hardware or software components like forwarders are not needed.
* Third-party integrations: Third-party APIs to allow the importation of security logs, e.g., Office 365 and Azure AD.

This security and network data can then be analysed through Google chronicle’s simple browser-based application. Enabling analysts to easily monitor the security of the cloud environment. This can be seen in figure 3 below.

From “Log in to Chronicle” by Google Cloud, n.d., <https://cloud.google.com/chronicle/docs/log-in-to-ui>.

[6] Figure 3 Log into Google Chronicle web browser landing page

Google [5] suggests that these analysts can use Chronicle features such as:

* Search – Google Chronicle has a Raw log scan function with can be used with regular expressions to find specific logs [5].
* Investigative Views – Can include enterprise insights to display domains and assets that require investigation [5]. Asset view can be used to identify if any piece of IT infrastructure has interacted with out-of-the-ordinary domains [5].
* Curated Information – Asset insight blocks can pinpoint the domains and alerts that security analysts should investigate in more detail [5].
* Detection Engine – Enables the automation of the search process to look through and discover security issues [5]. Specific rules can be created to search every piece of incoming data and alerts can be set up [5].
* Integration and tools - Malware identification sites like Virus Total can be integrated for easy access, and Chronicle has a chrome extension that enables the web application to be launched anywhere in the google chrome browser [5].

## Conclusion

In conclusion, SIEMs can be extremely beneficial to safeguard and monitor the security of Redback’s IT infrastructure. A SIEM will provide Redback with the tools to combine several sources of security data into a centralized place for analysis. The main benefits of doing this are the improvement of security operations efficiency and **increased accuracy of security alerts; With the main disadvantage being implementation cost. However, Google Chronicle mitigates these costs for Redback, as the DevOps team will be hosting their infrastructure on Google Cloud. Because of this, it is recommended that Google chronicle be implemented as Redback’s SIEM platform.**

## Reference list

[1] International Business Machines Corporation. (n.d.). What is SIEM? Security Information and Event Management Explained [Website]. Available: URL <https://www.ibm.com/au-en/topics/siem>

[2] PeerSpot. (n.d.). Best Security Information and Event Management (SIEM) Tools [Website]. Available: URL <https://www.peerspot.com/categories/security-information-and-event-management-siem>

[3] Google Cloud. (n.d.). Chronicle Security [Website]. Available: URL <https://chronicle.security/>

[4] K. Gast (2021, March). What is SIEM? And How Does It Work? [Website]. Available: URL <https://logrhythm.com/blog/what-is-siem>

[5] Google Cloud (n.d.). Chronicle overview [Website]. Available: URL <https://cloud.google.com/chronicle/docs/overview>

[6] Google Cloud (n.d.). Log in to Chronicle [Website]. Available: URL <https://cloud.google.com/chronicle/docs/log-in-to-ui>

[7] LOGPOINT (n.d.). What is SIEM? A complete guide to Security Information and Event Management [Website]. Available: URL <https://www.logpoint.com/en/understand/what-is-siem/>