mesoform

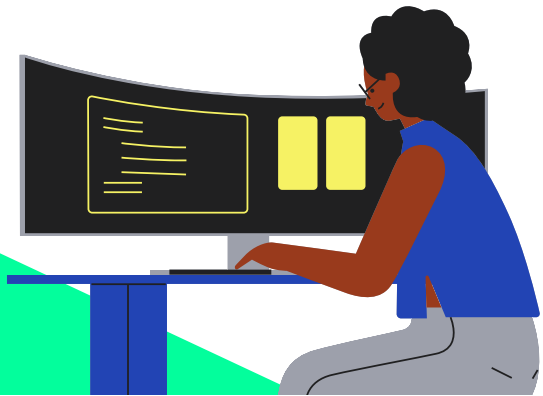
CENTRALISED SIEM

How did Mesoform help large financial institution create a centralised and efficient SIEM?

WHAT IS SIEM?

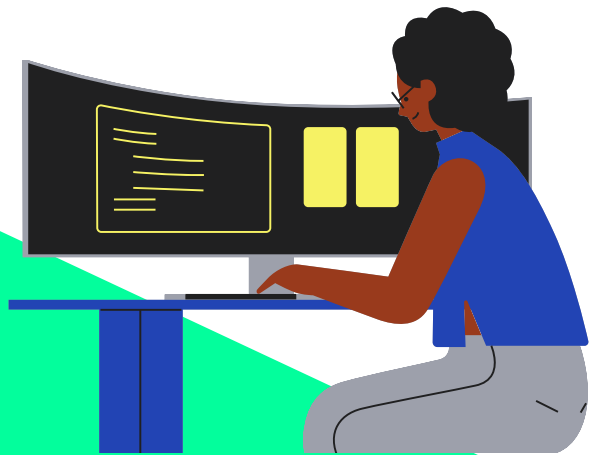
Security **I**nformation management and security **E**vent **M**anagement is a well-defined area of cyber security. It covers the following main areas:

- Collection and storage of log messages and audit trails (a detailed, chronological record whereby accounting records or other financial data are tracked and traced).
- Real-time monitoring, correlation of events, notifications and console views, threat analysis, intrusion prevention and damage reduction.
- Coverage of events for: connectivity and bandwidth, networking, identity and access, operating systems, applications, virtualisation and cloud platforms, disaster recovery among others.
- Events often include authentication, anti-virus, anti-malware/spyware and intrusion detection.



THE CHALLENGE

- As a large financial organisation the company has strict security requirements. One of which is having a central SIEM monitored by a Security Operations Centre.
- This means Cloud platform and any other (i.e. OS) audit events need to be sent to the centralised system for analysis, notification and action.
- In some cases this can include waiting for logs to be copied into a storage location ready for collection but this can be a slow process. Ideally these events need to be processed and analysed as close to real-time as possible.



THE SOLUTION

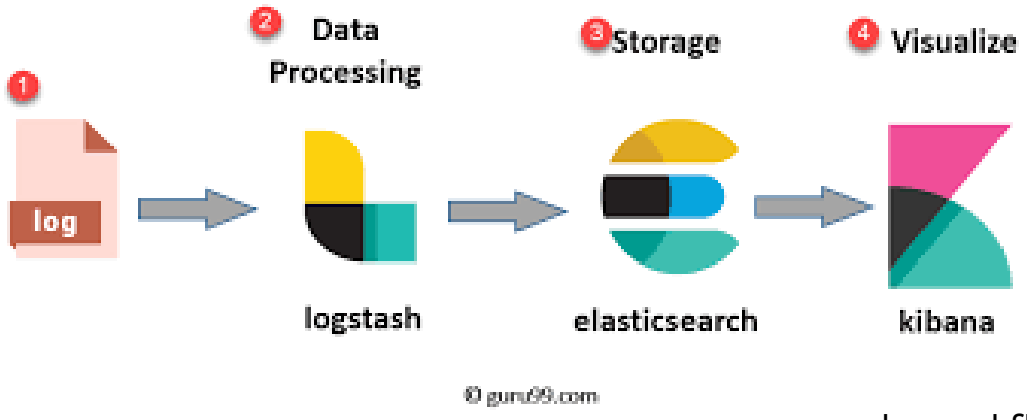
- We added a log agent to VM base images to send machine logs to Google Cloud Logging.
- Created a log router for these logs and all Cloud audit logs to send to Google Pub/Sub.
- With a Compute Engine Managed Instance Group we deployed auto-scaling instances of Elastic Logstash which subscribed to pull these messages.
- The Compute Engine deployments made use of metadata and other external information to determine what sort of environment it was running in.
- Logstash then filtered, and where necessary, mutated logs to be consumed easily by the SIEM
- Logstash then forwarded the messages over a Direct Interconnect to the SIEM

- We chose Elastic Logstash because of its native plugin for Pub/Sub. It is also highly scalable and performant at filtering and modifying messages in flight, preventing the SIEM from performing this CPU-intensive operation.

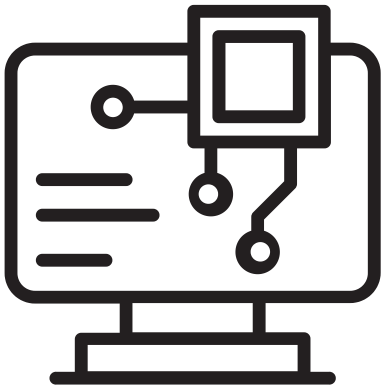
- Our initial requirements also specified that we needed to send messages to the central system over a specifically required protocol which Logstash had already built-in support for.

- Google Pub/Sub is one of 3 standard export types from Cloud Logging, making it simple and quick to set up.

- Lastly we also created a custom app to process authentication logs from Google Cloud Identity.



example workflow



THE RESULTS

- Using pre-built Compute Images, Instance templates and managed instance groups with metadata, gave us the ability to deploy identical Logstash instances between development and production and do thorough testing of updates and changes.

- Logstash gave us the ability to perform contextual changes of audit log data useful for SIEM and shift processing away from the SIEM to a much more scalable environment.

- Pub/Sub provided us guaranteed delivery of events, message retention in case of issues and near real-time processing.

- The custom app used Google APIs and allowed us to pull in logs from Cloud Identity because these were not natively accessible on Cloud Logging at the time.

Even with very strict controls in place, we were able to deliver this whole service which could be used by all users of the financial organisation in a controlled and agile manner in only a few weeks.

TO FIND OUT HOW MESOFORM CAN HELP YOUR BUSINESS BECOME MORE SECURE, STABLE AND EFFICIENT, CONTACT:

HELLO@MESOFORM.COM

As IT specialists, Mesoform can help your business overcome similar challenges and provide efficient solutions in comparison to competitors.