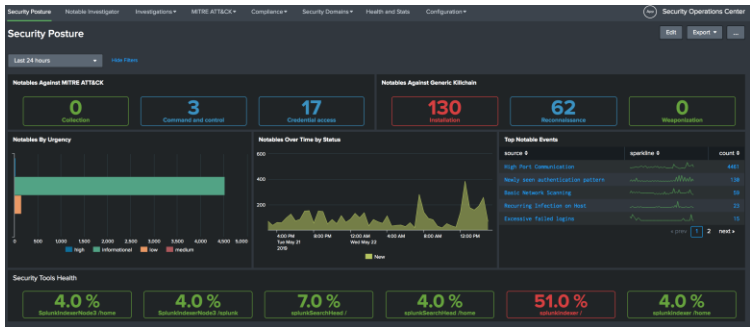


CATEGORY	:	INNOVATION RECOGNITION INFORMATION TECHNOLOGY
ORGANIZATION	:	GOVERNMENT SERVICE INSURANCE SYSTEM (Philippines)
CONTACT PERSON	:	Jonathan Pineda
NAME OF PROJECT	:	Security Analytics Project
OBJECTIVE AND NATURE OF PROJECT	:	Being a social security agency, the Government Service Insurance System (GSIS) is responsible for the protection of the personal and sensitive personal information of over 2.5 million members and pensioners. GSIS has implemented various automation tools to bring its services closer to members. However, doing so, presents various risks, notably cyber security risks since these systems are delivered online. The Security Analytics Project was implemented to be the backbone of the GSIS Information Security Office in monitoring , detecting, preventing and responding to cyber threats in the shortest time possible.
WHY IT SHOULD BE RECOGNIZED	:	The Security Analytics Project has helped GSIS to bring down response times to minutes instead of the usual hours or days which in turn helps provide information assurance to its members and pensioners. The Project enabled GSIS to collect, aggregate and correlate various log events from various security tools and IT Systems to provide visibility and actionable alerts to the Information Security Office. The implementation of the Security Analytics Project gave GSIS the capability to detect adversaries using either the MITRE ATT&CK¹ (Adversarial Tactics, Techniques & Common Knowledge) Framework or the Lockheed Martin Cyber Killchain Process².  GSIS Security Posture Dashboard
SUMMARY OF THE	:	GSIS implements information security to manage and monitor

¹ <https://attack.mitre.org/>

² <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

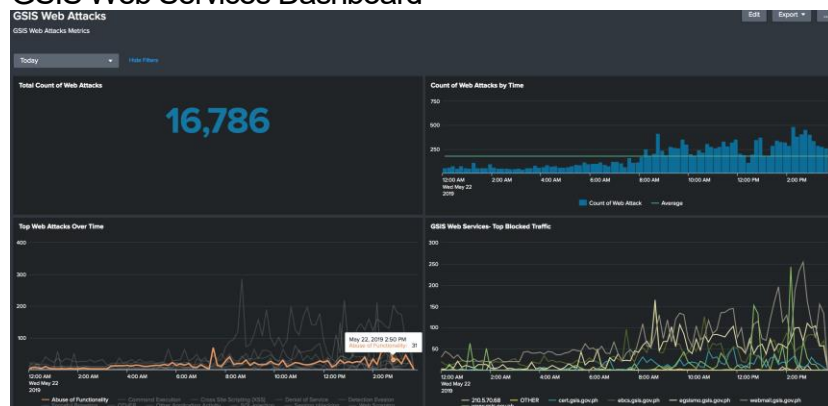
PROJECT

various security control solutions, providing defense in depth protection to GSIS information and information systems to protect member data. These solutions vary from gateway protection systems consisting of next-gen firewalls, web application firewalls, intrusion detection and prevention systems, web and mail security and endpoint protection systems. In order to manage and monitor all these solutions, the data and logs they generate needs to be accessible and usable.

The Security Analytics Project was implemented to be the backbone for the GSIS Security Operations team. This project is a key component as this provides the GSIS the capability to collect, aggregate, and correlate logs and events from various security sources so they can provide actionable alerts and searchable events. At present, GSIS collects a minimum of 30 million logs and events per day and these are translated to less than 100 actionable items. The project made it easier for GSIS to analyze incidents and threats to filter out the false positives. It also provides a single system for multiple dashboards that the System can use to monitor web traffic, web attacks, and other cyber threat vectors such as email and endpoints at near real time. Automating the alerts through the Security Analytics Project provided GSIS the capability to respond faster to cyber-attacks and incidents, thereby reducing the risks on the personal information of its members and pensioners.



GSIS Web Services Dashboard



GSIS Web Attacks Dashboard

