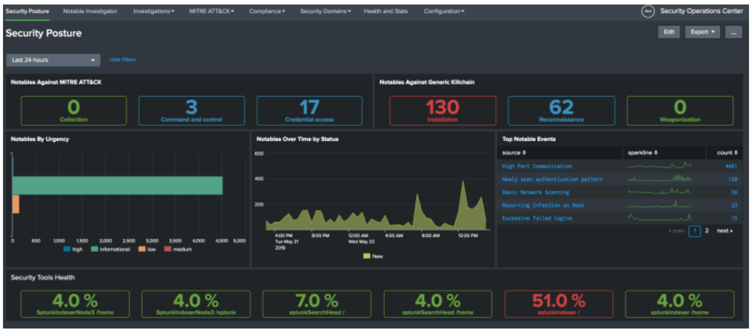
CATEGORY	:	INNOVATION RECOGNITION INFORMATION TECHNOLOGY
ORGANIZATION	:	GOVERNMENT SERVICE INSURANCE SYSTEM (Philippines)
CONTACT PERSON	:	Jonathan Pineda
NAME OF PROJECT	:	Security Analytics Project
OBJECTIVE AND NATURE OF PROJECT	:	Being a social security agency, the Government Service Insurance System (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&CK[1] (Adversarial Tactics, Techniques & Common Knowledge) Framework or the Lockheed Martin Cyber Killchain Process[2].  Security Posture Notable Investigator Investigations ▾ MITRE ATT&CK ▾ Compliance ▾ Security Domains ▾ Health and Stats Configuration ▾ Security Operations Center Security Posture Edit Export ▾ ... Last 24 hours Hide Filters Notables Against MITRE ATT&CK 0 Collection 3 Command and control 17 Credential access Notables Against Generic Killchain 130 Installation 62 Reconnaissance 0 Weaponization Notables By Urgency 0 500 1,000 1,500 2,000 2,500 3,000 3,500 4,000 4,500 5,000 high informational low medium Notables Over Time by Status 600 400 200 4:00 PM Tue May 21 2019 8:00 PM 12:00 AM Wed May 22 4:00 AM 8:00 AM 12:00 PM New Top Notable Events source sparkline count High Port Communication 4461 Newly seen authentication pattern 138 Basic Network Scanning 59 Recurring Infection on Host 23 Excessive failed logins 15 « prev 1 2 next » Security Tools Health 4.0 % SplunkIndexerNode3 /home 4.0 % SplunkIndexerNode3 /splunk 7.0 % splunkSearchHead / 4.0 % splunkSearchHead /home 51.0 % splunkIndexer / 4.0 % splunkIndexer /home GSIS Security Posture Dashboard
SUMMARY OF THE	:	GSIS implements information security to manage and monitor

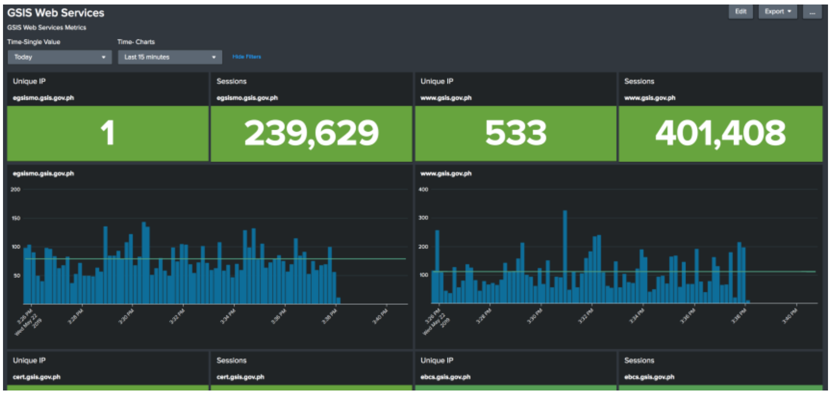
[1] https://attack.mitre.org/

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

<table>
<tr>
<td>PROJECT</td>
<td></td>
<td>

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

GSIS Web Services Metrics

Time-Single Value: Today

Time- Charts: Last 15 minutes

Unique IP egsismo.gsis.gov.ph 1

Sessions egsismo.gsis.gov.ph 239,629

Unique IP www.gsis.gov.ph 533

Sessions www.gsis.gov.ph 401,408

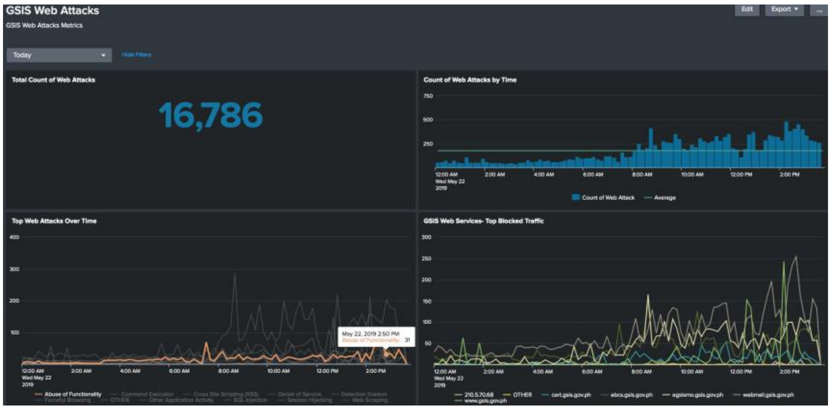
Unique IP cert.gsis.gov.ph

Sessions cert.gsis.gov.ph

Unique IP ebcs.gsis.gov.ph

Sessions ebcs.gsis.gov.ph

GSIS Web Services Dashboard



GSIS Web Attacks

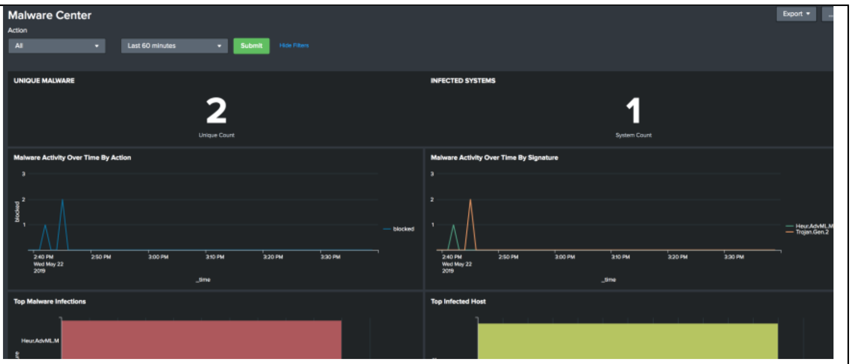
GSIS Web Attacks Metrics

Today

Total Count of Web Attacks 16,786

GSIS Web Attacks Dashboard

</td>
</tr>
</table>

		 Malware Center Export Action All Last 60 minutes Submit Hide Filters UNIQUE MALWARE 2 Unique Count INFECTED SYSTEMS 1 System Count Malware Activity Over Time By Action 3 2 1 blocked 2:40 PM Wed May 22 2019 2:50 PM 3:00 PM 3:10 PM 3:20 PM 3:30 PM _time blocked Malware Activity Over Time By Signature 3 2 1 2:40 PM Wed May 22 2019 2:50 PM 3:00 PM 3:10 PM 3:20 PM 3:30 PM _time Heur.AdvML.M Trojan.Gen.2 Top Malware Infections Heur.AdvML.M Top Infected Host GSIS Malware Attacks Dashboard