SCHOOL OF INFOCOMM

IXIA ThreatARMOR Analytics Dashboard Apps for Splunk

Partner Organisation: ***IXIA***

Project Overview

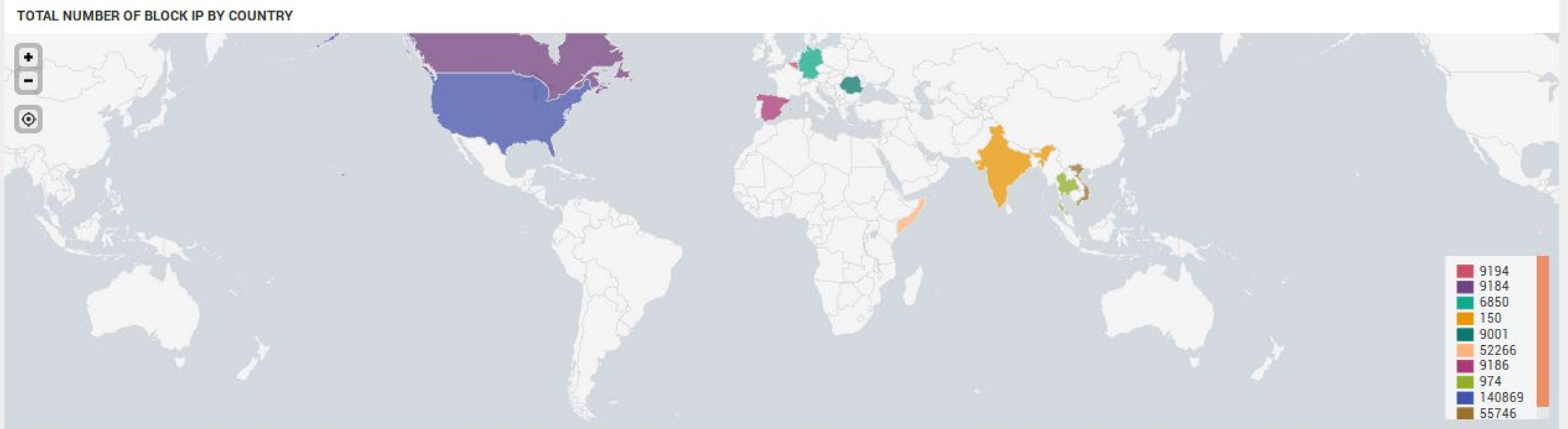
Problem: To develop an analytics dashboard for Ixia ThreatARMOR log analysis and visualization

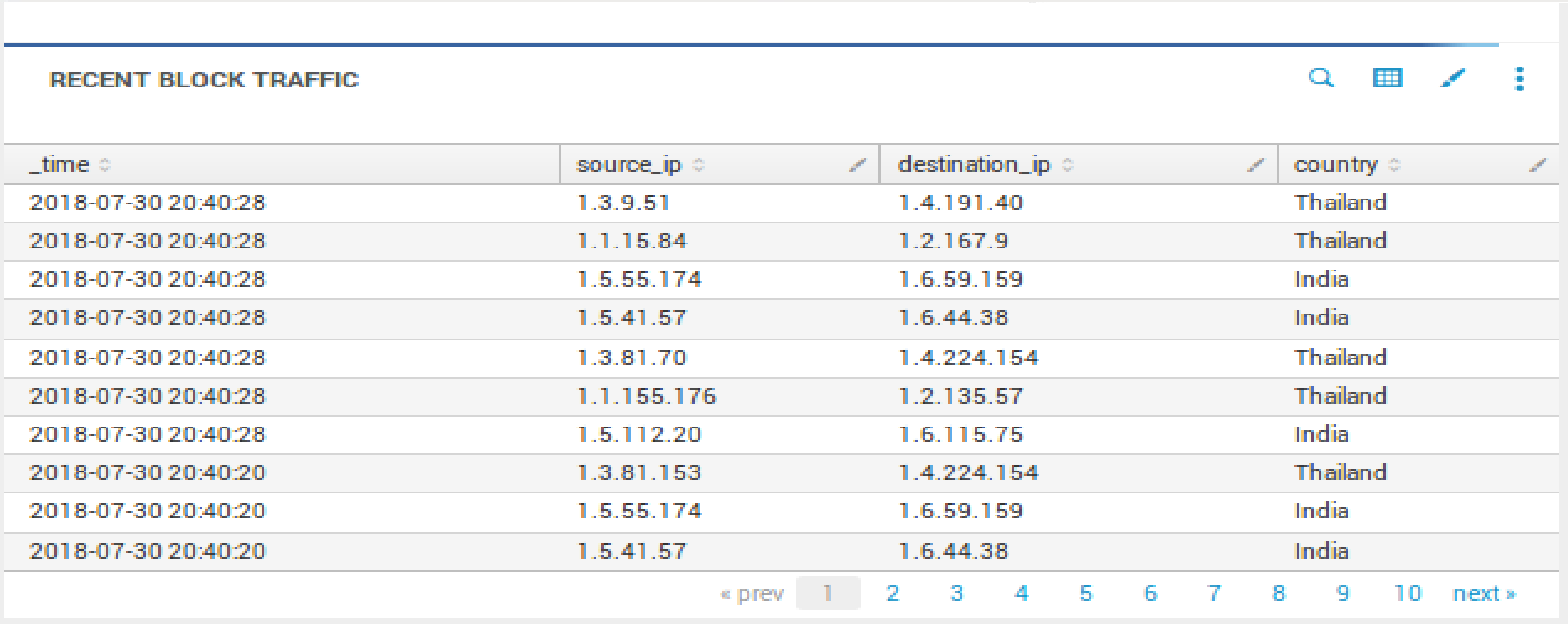
Requirements:

1. The IXIA ThreatARMOR will be sending out syslogs of its blocked IP addresses to Splun
2. Splunk app needs to take in these syslogs and create visualizations
3. Creating indexes and classification for the data
4. To develop reporting modules that will summarise and correlate as a situational analysis of the threat landscape
5. Map and show Dashboards, reporting, alert functions, output functions
6. Install geolocation and GeoIP to mapping the data to the map

Solution: Design dashboard, correlating events to visualise network logs given by IXIA.

Technologies: Splunk, Python, Ubuntu Linux, XML


TOTAL NUMBER OF BLOCK IP BY COUNTRY


RECENT BLOCK TRAFFIC

_time	source_ip	destination_ip	country
2018-07-30 20:40:28	1.3.9.51	1.4.191.40	Thailand
2018-07-30 20:40:28	1.1.15.84	1.2.167.9	Thailand
2018-07-30 20:40:28	1.5.55.174	1.6.59.159	India
2018-07-30 20:40:28	1.5.41.57	1.6.44.38	India
2018-07-30 20:40:28	1.3.81.70	1.4.224.154	Thailand
2018-07-30 20:40:28	1.1.155.176	1.2.135.57	Thailand
2018-07-30 20:40:28	1.5.112.20	1.6.115.75	India
2018-07-30 20:40:20	1.3.81.153	1.4.224.154	Thailand
2018-07-30 20:40:20	1.5.55.174	1.6.59.159	India
2018-07-30 20:40:20	1.5.41.57	1.6.44.38	India

Team Members
Leong Wai Kiat,
Tam Wei Cheng,
Siah Wee Boon
Ms Mapel Yap (Supervisor)

REPUBLIC POLYTECHNIC
DISCOVER. TRANSFORM. ACHIEVE