

# 2015-12-11 Meeting notes

## Date

11 Dec 2015

## Attendees

- [George Vetticaden](#)
- Discover Gerdes
- [James Sirota](#)
- Noreen Santini
- Mark Bittmann
- Debo Dutta
- Oskar Zabik
- Brad Kolarov

## Goals

- Review Platform and UI Requirements for Metron

## Discussion items

1. Need to come up with Taxonomy for Metron so everyone is speaking the same language. Need to finalize and define terms such as:
  - a. Event
  - b. Alert
  - c. Incident
  - d. Asset
  - e. Risk
  - f. Threat
  - g. Urgency
2. For Rackspace, multi-tenancy requirements will be key. They will have multiple customers using shared infrastructure where data will need to flow into a single Metron cluster. So being able to identify an event associated with a specific customer are critical.
3. Different Personas of the users of the system include:
  - a. Junior Security Analyst
  - b. Senior Security Analyst
  - c. Admin
  - d. Customer Facing / Executives
4. Alerting Management Requirements
  - a. Suppress an Alert Temporarily and time based (suppress for 24 hours)
  - b. Suppress an Alert Permanently
5. Need examples of correlation and SIEM rules
6. Ability to search, pivot and build complex queries via UI (pivoting and clicking) will be important. E.g: Select a "Watchlisted Threat Alert", then click on Details, Select Destination Souce --> Right click and do Search as Source IP --> executes a Search
7. Approach to Requirements and Design
  - a. For Legacy SIM functionality --> Start with UI requirements and drive platform requirement
  - b. For Next Analytical functionality --> Start with Analytics and then drive UI requirement
8. What Next?
  - a. Need to create Customer Survey and send to SOC teams to collect and prioritize requirements
  - b. From requirements, create some wireframes
  - c. With wireframes, conduct "interviews" with various SOC teams with wireframes
  - d. Iterate on requirements and wireframes.

## Action items

1. George: Send out meeting minutes.
2. George: Send out shared doc for Customer Survey
3. George: Schedule weekly Requirements meeting invite every Thursday from 9 CST - 10:30 CST
4. Noreen and Oskar: Meet on UI and Customer Survey , start wireframes and then publish out meeting minutes to apache metron dev team

