Cloud Security Event Processing and Alerting Platform

The Capstone Experience

Team Rook
Bradley Baker
Alex Fall
Jake Fenton
Brian Jones
Kaushik Sridasyam

Department of Computer Science and Engineering
Michigan State University
Fall 2017
Functional Specifications

• Maintain features from current engines
• Manage and enable rules from web interface
• Manage addition of clients from web interface
  ▪ Lambdas automatically handle new data
• Stretch: Allow testing of new rules
Design Specifications

- Security Analysts arrive at the Dashboard view for status
- Able to add and edit rules (CRUD)
- Can view client profiles
  - See all current rules for clients
- View performance of rule prospect.
Screen Mockup: Status/Landing Page
Screen Mockup: Update Rule

- Rule name: 
- Architecture: Palo Alto
- Occurrences until alert: 12
- Rule specification json

Submit  Cancel
Screen Mockup: Rule List View

Available Rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Architecture</th>
<th>Edit / Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad smelling packet</td>
<td>Seracotta</td>
<td>[edit icon] [remove icon]</td>
</tr>
<tr>
<td>Foreign SSH</td>
<td>Palo Alto</td>
<td>[edit icon] [remove icon]</td>
</tr>
<tr>
<td>Foreign SSH</td>
<td>Seracotta</td>
<td>[edit icon] [remove icon]</td>
</tr>
<tr>
<td>Netflix</td>
<td>Custom</td>
<td>[edit icon] [remove icon]</td>
</tr>
<tr>
<td>Cryptolocker C&amp;C</td>
<td>Palo Alto</td>
<td>[edit icon] [remove icon]</td>
</tr>
</tbody>
</table>

New Rule
## Screen Mockup: Client Profiles

### Client Profile

- **Add Rule**
- **Edit Rule**
- **Delete Rule**

### Current Rules For Client

<table>
<thead>
<tr>
<th>Rule</th>
<th>Who To Contact</th>
<th>Last Broke</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Event</td>
<td><a href="mailto:bobbyD@gmail.com">bobbyD@gmail.com</a></td>
<td>20:00DEC2016</td>
</tr>
<tr>
<td>Bad Smelling Packet</td>
<td><a href="mailto:support@rook.com">support@rook.com</a></td>
<td>14:30NOV207</td>
</tr>
<tr>
<td>Too many Requests</td>
<td><a href="mailto:stan@theman.com">stan@theman.com</a></td>
<td>22:30APR22</td>
</tr>
</tbody>
</table>

### Client Contacts

- [Diagram of client contacts]
Technical Specifications

• Master Lambda function
  - Pull new entries from ElasticSearch
  - Segregate by client and firewall architecture
  - Pass data to spawned child function

• Child Lambda function
  - Process client- and arch- specific events
  - Create tickets and/or send emails

• Python Django API
  - CRuD for the rules
System Architecture

Backend

- **django**
  - children
  - Email alerts
  - Master
  - Rule Bucket

ElasticSearch

- The Internet
  - Filtering

Frontend

- Stretch Goal

Existing

- archive

Team Rook Project Plan
System Components

• Hardware Platforms
  ▪ AWS Lambda Functions
  ▪ AWS EC2 Django Server
  ▪ AWS EC2 Frontend Server

• Software Platforms / Technologies
  ▪ Python Django
  ▪ AWS Lambda Functions
  ▪ ReactJS/Redux
  ▪ SQLite
Testing

• Testing the Correlation Engine
  ▪ Using sanitized archived data to simulate events
• Testing The Front End
  ▪ Jest testing the React portion of our project
• Prototyping via Rook Personnel
• Django API
  ▪ Postman
Risks

• Lambda Timing Out
  ▪ Potential loss of vision on events

• Cannot currently reach Rook demo backend
  ▪ Difficult to integrate UI when we can’t truly move through the state

• Django server needs access to S3 buckets
  ▪ AWS credentials are sensitive

• Sending emails from engine
  ▪ Not sure what our capabilities will be
Questions?