Forward by Stephen Northcutt. Three students from the SANS Technology Institute, (Alyssa Robinson, David Fletcher, and Wes Whitteker) were assigned the following project for their ISE-M 6100 coursework. There are three files, a Step by Step, a presentation, and a Lessons Learned document.

Assignment:
Your topic will be: Step by Step Instructions for OSS SIEM Implementation

Assignment Scenario:
Your company, GIAC Enterprises, is a small to medium sized growing business (1,000 employees, two data centers, 200 people in central business and IT) and is the largest supplier of Fortune Cookie sayings in the world. They also have a large number of individual contractors, (in the US these are called 1099 based on their tax status), that submit fortune cookie sayings via a mobile application. The CIO calls you in for a special tiger team project.

GIAC has finally reached a point where our network is too complex to manually analyze the logs. We looked into commercial SIEM and that stuff is pricey. One of our analysts came across a LinkedIn post from some guy named Northcutt:
https://www.linkedin.com/pulse/open-source-siem-stephen-northcutt

It seems like there are some interesting alternatives to using commercial products. Decide on the tool(s) you think make the most sense and develop a pilot implementation.

Assignment Deliverables:
You will research and develop the following resources or deliverables:

1.0 Project Plan. (10% of final grade) NOTE: plan is not shown in the Reading Room.

2.0 Step by Step description of your solution. (50% of final grade) Screenshots, explanations, etc.; what you would expect to see in a Step by Step guide or “How To”.

3.0. Analysis/Lessons Learned/Debrief. (30% of final grade) Things do not always go according to plan; a promising solution might prove not to be so promising. This paper is where you will explain why you made the choices you made, problems you ran into and how you solved them to create the Step by Step. There should also be a lessons learned section, “if we had it to do over again, we would have”.

4.0. Short slide deck presentation serving as an end of the project debriefing, (10% of final grade). 15 PowerPoint slides, (with Notes), that deal with the most important material. Include a title slide, introduction and conclusion slide, which gives you 12 content slides to work with. [Team does not virtually or orally give a presentation from the slide deck.]

Thank you,

Stephen Northcutt, Director Academic Advising
The SANS Technology Institute (www.sans.edu)
# Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>SANS OnDemand</th>
<th>OnlineUS</th>
<th>Anytime</th>
<th>Self Paced</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>