ISE6100 GIAC Enterprises - Open Source SIEM - Read Me First

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.]

========== end assignment ==========

Thank you,

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

Last Updated: August 5th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Reboot - NOVA 2020	Arlington, VAUS	Aug 10, 2020 - Aug 15, 2020	Live Event
SANS FOR508 Sydney August 2020	Sydney, AU	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Virginia Beach 2020	Virginia Beach, VAUS	Aug 30, 2020 - Sep 04, 2020	Live Event
SANS London September 2020	London, GB	Sep 07, 2020 - Sep 12, 2020	Live Event
SANS Philippines 2020	Manila, PH	Sep 07, 2020 - Sep 19, 2020	Live Event
SANS Baltimore Fall 2020	Baltimore, MDUS	Sep 08, 2020 - Sep 13, 2020	Live Event
SANS Munich September 2020	Munich, DE	Sep 14, 2020 - Sep 19, 2020	Live Event
SANS Network Security 2020	Las Vegas, NVUS	Sep 20, 2020 - Sep 25, 2020	Live Event
SANS Australia Spring 2020	, AU	Sep 21, 2020 - Oct 03, 2020	Live Event
SANS Northern VA - Reston Fall 2020	Reston, VAUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS San Antonio Fall 2020	San Antonio, TXUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS FOR500 Milan 2020 (In Italian)	Milan, IT	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Amsterdam October 2020	Amsterdam, NL	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Brussels October 2020	Brussels, BE	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Prague October 2020	Prague, CZ	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS London October 2020	London, GB	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS Orlando 2020	Orlando, FLUS	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS October Singapore 2020	Singapore, SG	Oct 12, 2020 - Oct 24, 2020	Live Event
SANS Stockholm October 2020	Stockholm, SE	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Dallas Fall 2020	Dallas, TXUS	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Rome October 2020	Rome, IT	Oct 19, 2020 - Oct 24, 2020	Live Event
Cloud & DevOps Security 2020	Denver, COUS	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS SEC504 Rennes 2020 (In French)	Rennes, FR	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Geneva October 2020	Geneva, CH	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS SEC560 Lille 2020 (In French)	Lille, FR	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS San Francisco Fall 2020	San Francisco, CAUS	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS Cologne October 2020	Cologne, DE	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS Krakow November 2020	Krakow, PL	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS London November 2020	London, GB	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Rocky Mountain Fall 2020	Denver, COUS	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS DFIRCON 2020	Miami, FLUS	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Sydney 2020	Sydney, AU	Nov 02, 2020 - Nov 21, 2020	Live Event
SANS OnDemand	OnlineUS	Anytime	Self Paced
SANS SelfStudy	Books & MP3s OnlyUS	Anytime	Self Paced