SANS Institute
InfoSec Reading Room

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.

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: July 21st, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced