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: April 22nd, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Seattle Spring 2018	OnlineWAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced