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: November 20th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Miami 2019	Miami, FLUS	Jan 21, 2019 - Jan 26, 2019	Live Event
Cyber Threat Intelligence Summit & Training 2019	Arlington, VAUS	Jan 21, 2019 - Jan 28, 2019	Live Event
SANS Dubai January 2019	Dubai, AE	Jan 26, 2019 - Jan 31, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NVUS	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LAUS	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS SEC504 Stuttgart 2019 (In English)	Stuttgart, DE	Feb 04, 2019 - Feb 09, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Vienna, VAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, GB	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Anaheim 2019	Anaheim, CAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Secure Japan 2019	Tokyo, JP	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TXUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Zurich February 2019	Zurich, CH	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Austin 2018	OnlineTXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced