Team Name	Group 29
Project	Grid-SIEM
Report Period	Oct. 22 – Nov. 5

Summary of Progress in this Period

Progress Point	**Description**
Set up a demo with Gravwell representative.	Our group is meeting with a Gravwell representative the week of Nov 13. To help us out with any questions we might have run into during the installation process and learn more about the platform's features.
Access to PowerCyberLab	In addition to some of the diagrams that give us a better sense of the PowerCyber topology. Our adviser has granted us access to the PowerCyber virtual machine resources. We can begin the installation phase.
Fix firewall issues.	We ran into some issues when setting up Security Onion. They had to do with firewall traffic policies not allowing TCP traffic to the Master Node. They have been resolved by our adviser and hopefully won't become a problem with Gravwell services in the future.

Pending Issues

Issue	Description
Security Onion documentation.	We are currently working on writing documentation that outlines the installation process of Security Onion. In addition a document over our current installation and configuration of Security Onion.
Security Onion Installation	Complete installation of Security Onion on the ubuntu-SIEMMaster-2-SO virtual machine. We are also working on the firewall rules for the machine to allow the sensors using Security Onion to interact with each other.
Gravwell Documentation	We are currently working on writing documentation that outlines the installation process of the Gravwell platform.
Gravwell Installation	Complete installation of Gravwell on the ubuntu-SIEMMaster-2-Gravwell virtual machine.
Testing Documentation	Finish up the testing portion of the engineering project document.
Develop weekly slide deck to showcase progress to our project adviser.	Stay prepared for in-class lightning talks. In order to be prepared to present during the in-class lighting talks our group needs to develop a new slide deck covering project planning. As well as a secondary slide deck to

	showcase new findings to our project adviser.

Plans for Upcoming Reporting Period

Pending Item	**Description**
Kali attack VM	Make use of the Kali Linux VM to research attacks that can be run against our environment and setup the installations for the attacks.
Review engineering design documentation.	Got some feedback from Dr. Tyagi regarding the overall engineering design of the project. Our group now needs to go back and be more specific and direct. Make sure that every tool has a purpose.
Integration of machine learning into project.	For an analyst to do the incident handling portion of the project would be overwhelming. Which is why we have a SIEM to help collect and parse the noise from the real threats. The next step above that is to train a machine learning model to detect a new previously unknown threat based on prior threat signatures.
Integrate MITRE Caldera into project to deploy attacks on OT systems.	Since this is one of the portions of the project that will be implemented last, it follows that we have not done enough research to thoroughly understand how testing with MITRE Caldera will be

	accomplished. We will use the newly available Kali linux virtual machines for this
Security Onion Installation	Continue to work on Security Onion Installation, we are switching the Master node to Sensor 3 instead of the original and testing if adding two NICs to each VM solves the communication issue.
Project Tools	Continue to explore new and different varieties of tools we can explore and integrate into our project.
Final Presentation	Prepare for Faculty Design Review Presentation in December. Go through design document and remove questions and check for design errors.