Team Name	Group 29
Project	Grid-SIEM
Report Period	Nov. 5 – Nov. 19

Summary of Progress in this Period

Progress Point	**Description**
Demo with Gravwell representative.	On November 14, we meet with a representative from the Gravwell team. They covered an overview of several features on their platform and recommmended talking to the developers directly through discord. They emphasised using Gravwell in addition to a SIEM tool, not entirely as a stand alone solution. They left us with a few pointers and resources to move forward.
Installation of Security Onion and Gravwell	Security Onion is running as a SIEM on the testbed environment
Fixed firewall issues. New Security Onion VMs in place	The master and one sensor node have been put in place on the PowerCyber testbed environment and firewall rules have been established.
Running Mitre Caldera Instance	Caldera has been installed on the Kali VM, and protocol plugins such as Modbus, dnp3, and BACnet have been installed.
Lightning Talks	After presenting one of our lightning talks in class we were told that our

	presentation was not detailed enough. We have since made sure to use every tool with purpose. Which I entirely agree with. However, it is important to mention that our adviser encouraged us to explore different options, and tools to use next semester.
News Report Youtube Video	We completed the news report video and did our best to speak from the heart about our project with our given roles. It served as a great opportunity to showcase the progress we made so far.

Pending Issues and Final Fall Semester Plans

Issue/ Pending Item	**Description**
Testing	Finish up the testing portion of the engineering project document.
Security Onion Improvements	There still should be two sensors that are being put up on the SIEM, and experimentation with traffic coming through as well, and rules should be put on the master node to catch logs.
Gravwell Improvements	We will continue to use Gravwell as a supplementary resource to our project. And Security Onion as our primary SIEM solution. Our next move with it is to figure out how to feed data into it

	for processing. But it won't be our main priority to be Gravwell experts.
Launch Attacks from Kali VM	The team should research attack payloads and use the Kali VM to launch non-invasive attacks to test if protocol plugins are working.
Review engineering design documentation.	Need to review the engineering design documentation to ensure that everything is updated as well as cohesive throughout the document.
Final Presentation	Need to work on the final presentation and build a story as well as flesh out talking points during the presentation.
PyTorch and ML	As one of the most difficult parts of our project our team will all work together to figure our how we can make use of ML to detect attacks. With the help of grad students and resources from our adviser.