

Sprint Backlog Grooming Meeting Minutes:

Attendees: Mateo Escobar, Nikohl Fuentes, Ryan Hamel, Sebastian Medina, Marian Mora

Start time: 1 P.M.

End time: 2 P.M.

The following user stories were created/discussed/refined/prioritized.

Discussed and prioritized:

- **User Story 25:** Gain a complete attack map to start working on presentation resources (1 point).
- **User Story 26:** Begin collaborating on creating the poster to show the progress and development of the project (3 points).
- **User Story 27:** Work on the assigned videos using footage of the project along with strong editing to meet the requirements (2 points).
- **User Story 28:** Work on the overall documentation of the project, along with collecting whatever scripts and pictures we need. (3 points).

Removing: No stories were replaced by other versions of the user story.

Added/Replaced:

Existing Stories:

User Story 1: Create a free Azure subscription using a personal email and credit card to establish the cloud environment (2 points).

User Story 2: Create a resource group in Azure to organize and contain the SOC lab resources (2 points).

User Story 3: Create a virtual network (VNet) in the same region as the resource group to provide network connectivity (3 points).

User Story 4: Create a Windows 10 virtual machine in the resource group and attach it to the virtual network (3 points).

User Story 5: Edit the security rules within our virtual network to make it as vulnerable as needed (3 points).

User Story 6: Establish a connection with Windows Remote Desktop in order to access the virtual machine created in Azure (2 points).

User Story 7: Edit the security settings in the virtual machine's Windows Defender (2 point).

User Story 8: Ping to the public IP address created on the virtual machine (3 points).

User Story 9: Make sure that we can view any logs through the event viewer in order to see any traffic, more specifically by failing logins. (2 points).

User Story 10: Configure a log repository in order to begin setting up the SIEM to collect logs. (2 points).

User Story 11: Finally create and establish Microsoft's SIEM known as Sentinel (2 points).

User Story 12: Successfully connect our VM to log analytics workspace (3 points).

User Story 13: Acquire an understanding of KQL in order to create queries that allow us to view certain security events. (3 points).

User Story 14: Use KQL in order to view the logs of the failed login attempts (4 points).

User Story 15: Upload geolocation data into Azure in order to determine where the IPs of the attackers are on a map.(3 points).

User Story 16: Create a KQL query that will allow us to view the records of failed login attempts displaying new geolocation data. (2 points).

User Story 17: Figure out how to take our geolocation data and associate with our logs (2 points).

User Story 18: Begin working on how to create our complete attack map (3 points).

User Story 19: Perform regular log validation to ensure logs are being correctly ingested and parsed by Microsoft Sentinel (4 points).

User Story 20: Perfect the JSON file to properly show all aspects of the attack map required, using Azure's workbooks (2 points).

User Story 21: Document the setup process and create a step-by-step guide for future use or replication of the SIEM setup (2 points).

User Story 22: Generate a report from Microsoft Sentinel summarizing detected threats, alerts, and system performance metrics (3 points).

User Story 23: Install and open Wireshark on the Kali Linux VM to confirm it captures network packets (2 points).

User story 24: Explore the Microsoft Sentinel interface to understand its key features and navigation (1 point).

The user stories below are completed.

User Story 1: Create a free Azure subscription using a personal email and credit card to establish the cloud environment (2 points).

User Story 2: Create a resource group in Azure to organize and contain the SOC lab resources (2 points).

User Story 3: Create a virtual network (VNet) in the same region as the resource group to provide network connectivity (3 points).

User Story 4: Create a Windows 10 virtual machine in the resource group and attach it to the virtual network (3 points).

User Story 5: Edit the security rules within our virtual network to make it as vulnerable as needed (3 points).

User Story 6: Establish a connection with Windows Remote Desktop in order to access the virtual machine created in Azure (2 points).

User Story 7: Edit the security settings in the virtual machine's Windows Defender (2 point).

User Story 8: Ping to the public IP address created on the virtual machine (3 points).

User Story 9: Make sure that we can view any logs through the event viewer in order to see any traffic, more specifically by failing logins. (2 points).

User Story 10: Configure a log repository in order to begin setting up the SIEM to collect logs. (2 points).

User Story 11: Finally create and establish Microsoft's SIEM known as Sentinel (2 points).

User Story 12: Successfully connect our VM to log analytics workspace (3 points).

User Story 13: Acquire an understanding of KQL in order to create queries that allow us to view certain security events. (3 points).

User Story 14: Use KQL in order to view the logs of the failed login attempts (4 points).

User Story 15: Upload geolocation data into Azure in order to determine where the IPs of the attackers are on a map.(3 points).

User Story 16: Create a KQL query that will allow us to view the records of failed login attempts displaying new geolocation data. (2 points).

User Story 17: Figure out how to take our geolocation data and associate with our logs (2 points).

User Story 18: Begin working on how to create our complete attack map (3 points).

User Story 19: Perform regular log validation to ensure logs are being correctly ingested and parsed by Microsoft Sentinel (4 points).

User Story 20: Perfect the JSON file to properly show all aspects of the attack map required, using Azure's workbooks (2 points).

User Story 21: Document the setup process and create a step-by-step guide for future use or replication of the SIEM setup (2 points).

User Story 22: Generate a report from Microsoft Sentinel summarizing detected threats, alerts, and system performance metrics (3 points).

User Story 23: Install and open Wireshark on the Kali Linux VM to confirm it captures network packets (2 points).

User story 24: Explore the Microsoft Sentinel interface to understand its key features and navigation (1 point).