

Sprint Backlog Grooming Meeting Minutes:

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

Start time: 6 P.M.

End time: 7 P.M.

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

Discussed and prioritized:

- **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).

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

Added/Replaced:

User Story 17: Configure role-based access control (RBAC) for Microsoft Sentinel to limit access to specific roles (2 points).

User Story 18: Implement multi-factor authentication (MFA) for accessing the Azure portal and Sentinel resources (3 points).

User Story 19: Simulate a brute-force attack using Nmap to validate detection rules in Microsoft Sentinel (4 points).

User Story 20: Perform regular log validation to ensure logs are being correctly ingested and parsed by Microsoft Sentinel (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).

User Story 25: Research how Microsoft Sentinel collects and processes logs from different Azure services (1 point).

User Story 26: Install and verify that Microsoft Sentinel is enabled in the Azure environment (2 points).

User Story 27: Set up a test Log Analytics workspace in Azure to store security logs (2 points).

User Story 28: Connect a virtual machine (Kali) to the Log Analytics workspace to start collecting logs (2 points).

User Story 29: Configure a basic data connector in Microsoft Sentinel to collect logs from an Azure resource (2 points).

User Story 30: Use the Azure portal to view and confirm that logs are being collected in Sentinel (2 points).

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: Configure role-based access control (RBAC) for Microsoft Sentinel to limit access to specific roles (2 points).

User Story 18: Implement multi-factor authentication (MFA) for accessing the Azure portal and Sentinel resources (3 points).

User Story 19: Simulate a brute-force attack using Nmap to validate detection rules in Microsoft Sentinel (4 points).

User Story 20: Perform regular log validation to ensure logs are being correctly ingested and parsed by Microsoft Sentinel (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).

User Story 25: Research how Microsoft Sentinel collects and processes logs from different Azure services (1 point).

User Story 26: Install and verify that Microsoft Sentinel is enabled in the Azure environment (2 points).

User Story 27: Set up a test Log Analytics workspace in Azure to store security logs (2 points).

User Story 28: Connect a virtual machine (Kali) to the Log Analytics workspace to start collecting logs (2 points).

User Story 29: Configure a basic data connector in Microsoft Sentinel to collect logs from an Azure resource (2 points).

User Story 30: Use the Azure portal to view and confirm that logs are being collected in Sentinel (2 points).

The user stories below are completed.

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).