ATP Configuring and Monitoring

1. Under **Dectections** Select **Entity Tag**
2. Notice two accounts types on the right pane **Honeytoken** and **Sensitive**
3. Select **Exclusions.** View the exclusions on the right.
4. Select

Suspected NTLM authentication tampering

5. Notice the user information. Click on **Suspected NTLM** … again to collapse the selection.

6. Select **suspicious additions to sensitive groups**. Collapse the selection by click on that selection again.

7. Click on **suspected brute force attack.** Click to collapse the selection.

8. Click on **supicious VPN connections.** Click to collapse.

9. Select **notifications** from the left Menu. Turn on the option for "**A new Alert is detected"**

10. Turn on "**A new Health issue is detected**"

11. Under **Syslog notification** select **configure**

12. Click the down arrow to the right of Select

13. Select **Mainpc20**

14. Click the down arrow to the right of **UDP**

15. Click the **Cancel** button

16. From the menu on the left select **scheduled reports**

17. Click on Schedule to the right of **Passwords exposed in cleartext**

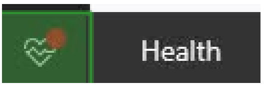
18. Notice the options for sending the report. Close the window.

19. Click on **updates** from the top left menu

20. Turn on **Domain Controller restart during updates**

21. Turn on Mainpc20. Turn back off **Domain Controller restart during updates,** then click on **Save**.

22. Select the Health Icon



23. Read the options, then click the question mark by All(1)

24. Select **Reports**

25. Click the timeline button