Create a remote log source to collect Windows logs (snippet)

> ⚠ Armor does not support the managed deployment of the WinCollect platform. Armor Support will not deliver any registrations keys to use with the WinCollect agents. As a result, you can use the following instructions as basic guidance.
>
> Armor officially supports Windows instances through one Wincollect agent per instance of Windows.
>
> Although WinCollect supports event collection from multiple sources, the Armor API will still require a log source to be created per Windows system.

1. Download and install the agent.
    - In this step, two files will be added to your local machine, including the **WinCollect Stanadlone Patch** installer. This GUI installer can be used to directly configured the WinCollect instance, as well as pull logs from other Windows system. (This process is not supported by Armor.)
2. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
3. Click **Log & Data Management**.
4. Click **Log Relay Source.**
5. Click the plus (+) sign.
    - If you do not have any log sources already created, then click **Add a New Log Source**.
6. Complete the missing fields:
    a. In **Endpoint**, select the available Armor Endpoint.
    b. In **Log Source Type**, select **Microsoft Windows Security Event Log**.
    c. In **Hostname**, enter the system hostname that matches the system for log collection.
        i. The hostname is case-sensitive and must match the exact same letters casing as the logs that are sent into this log source.
    d. In **Protocol**, based on your selection in **Log Source Type**, select the available protocol.
7. Click **Save Log Source**.
8. In the **Sources** screen, refresh the screen until the log source reaches an **Online** status.
9. In your local machine, launch the **WinCollect Configuration Utility** GUI.
10. In the left-side window, next to Destinations, click the (+) icon.
11. Click **Syslog TCP**.
12. In the top, right menu, click **Add New Destination**.
13. Enter a descriptive name, such as **Armor Defense Inc TLS**, and then click **Ok**.
    - The properties screen will appear.
14. Enter the fully qualified domain name (FQDN) for the event collector.
15. Enter the port that was allocated for your Windows Event Log source.
16. Configure a throttle limit, such as 500 EPS.
17. Click **Deploy Changes** to save.
18. In the left-side window, under Devices, right-click **Microsoft Windows Event Log**.
19. Click **Add New Device**.
20. Enter a descriptive name for your log source, such as the system name of your Windows host.
21. In **Device Address**, enter the local system hostname for the logs to be collected.
22. In **Security**, mark the box.
23. (Optional) For a DNS Active Directory or File Replication server, make the corresponding box.
24. In **Destinations**, click **Add**.
25. Select the name of destination you previously created, and then click **Ok**.
26. In the top, right menu, click **Deploy Changes**.

To use the command prompt:

1. Gather the following information:
    - Hostname
    - Armor Collector FQDN
    - Armor Log Source Port
    - Windows Services Hosted by System
        - Active Directory Collector
        - DNS Server
        - File Replication Service
2. Download and install the agent.
3. Right-click the WinCollect agent installation file, and then select Run as administrator.
4. Enter the following information into your command prompt:
    - wincollect-<version_number>.x86.exe /s /v"/qn INSTALLDIR=\"C:\Program Files \IBM\WinCollect\" HEARTBEAT_INTERVAL=6000 LOG_SOURCE_AUTO_CREATION_ENABLED= True LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice= DeviceWindowsLog&Component1. Action=create&Component1.LogSourceName= <hostname>&Component1.LogSourceIdentifier= <Armor_Collector_FQDN>&Component1.Dest.Name=QRadar&Component1 .Dest. Hostname=<Armor_Collector_FQDN>&Component1.Dest.Port= <armor_port>&Component1.Dest. Protocol=TCP&Component1.Log.Security=true&Component1 .Log.System=true&Component1.Log.Application=false &Component1.Log.DNS+Server=false&Component1.Log.File+Replication+ Service=false&Component1.Log. Directory+Service=false&Component1. RemoteMachinePollInterval=3000&Component1.EventRateTuningProfile=High+ Event+Rate+Server&Component1.MinLogs ToProcessPerPass=1250&Component1.MaxLogsToProcessPerPass=1875""""