Network Box SIEM+
Windows Server Integration

1. Download the winglogbeat zip file from https://www.elastic.co/downloads/beats/winlogbeat

   - winlogbeat is a lightweight agent that runs on the server and transmits log messages originating from the event system to our log ingestion endpoint.

2. Extract the contents into C:\Program Files

3. Rename the winglogbeat-<version> directory to winglogbeat

4. Open PowerShell as an Administrator (Right-click on the PowerShell icon and select Run-as Administrator)

5. Retrieve the certificate and key files from NBUSA Support. They should be attached to the SIEM+ onboarding ticket:

   - Save these files to C:\Program Files\winlogbeat

   - Rename them to siem-key.pem and siem-certificate.pem

6. Edit the winlogbeat.yml file located in C:\Program Files\winlogbeat

   - Run Notepad (or your preferred text editor) as an administrator and then open the file from within the application.

COPYRIGHT © 2019 NETWORK BOX USA, LLC.

- Copy the text in the black box below and replace all the contents of the file (winlogbeat.yml) with this content.

winlogbeat.yml

```
output.logstash:
  enabled: true
  hosts: ["ap.siem.network-box.com:20182"]
  ssl:
    certificate: C:\Program Files\winlogbeat\siem-certificate.pem
    key: C:\Program Files\winlogbeat\siem-key.pem
  verification_mode: full
  logging.to_files: true
  logging.files:
    path: C:\ProgramData\winlogbeat\Logs
  logging.level: info
  tags: ["windows", "iis"]
winlogbeat.event_logs:
  - name: Application
  - name: System
  - name: Security
```

Please note: if you want to create this on your own you must NOT use any Tab for the indents; the indents need to be made with 2 spaces. The YML markup is very specific and will cause syntax errors if you use Tab.

7. From the PowerShell prompt, run the following commands to install the service:

```
PS C:\Users\Administrator> cd 'C:\Program Files\Winlogbeat'
PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1
PS C:\Program Files\Winlogbeat> Start-service winlogbeat
```

8. Once the service has started, open the Services application:

```
PS C:\Users\Administrator> services.msc
```

9. Go to winlogbeat service, double click and change the following:

- On the General tab, change the Startup type to Automatic.

- On the Recovery tab, change the First Failure, Second Failure, Subsequent Failures to Restart the Service

COPYRIGHT © 2019 NETWORK BOX USA, LLC.