**SOC Learning Report – Windows Fundamentals 3**

**Analyst:** Inam Qadeer  
**Tool(s) Used:** Windows 10 VM, TryHackMe Lab Environment

**1. Executive Summary**

The Windows Fundamentals 3 lab explores core system security tools and settings within Windows, including the Windows Security application, antivirus protection, firewall management, and update control.  
This knowledge is crucial for SOC analysts to verify that endpoint security measures are active and properly configured during investigations.

**2. Investigation / Learning Steps**

1. **Windows Security Center**
   * Navigated the *Windows Security* application from the Start Menu.
   * Explored protection areas: *Virus & Threat Protection*, *Account Protection*, *Firewall & Network Protection*, *App & Browser Control*, *Device Security*, *Device Performance & Health*.
2. **Virus & Threat Protection**
   * Reviewed real-time protection settings.
   * Performed a quick scan to check for malware.
3. **Firewall & Network Protection**
   * Checked firewall status for Domain, Private, and Public networks.
   * Learned how to allow or block applications through the firewall.
4. **App & Browser Control**
   * Investigated SmartScreen settings for apps and browsers.
5. **Windows Update**
   * Checked for pending updates and learned the importance of timely patching.

**3. Findings**

* **Windows Security** centralizes security controls for system protection.
* **Real-time protection** helps block malware before it executes.
* **Firewalls** control inbound/outbound connections and should remain enabled across all profiles.
* **SmartScreen** warns against unrecognized or potentially malicious applications.
* **Regular updates** are essential to close known vulnerabilities.

**4. Importance for SOC Work**

* Verifying **antivirus and firewall status** ensures endpoints are not exposed.
* Reviewing **update history** can reveal if a system is missing critical patches.
* **App & browser protection settings** can indicate whether phishing or malicious file downloads will be blocked.

**5. Recommendations**

* Keep **real-time protection** enabled at all times.
* Ensure **firewall profiles** are all set to "On" and configured correctly.
* Enable **SmartScreen** for both apps and browsers.
* Apply critical security updates as soon as possible to mitigate known vulnerabilities.

**6. Conclusion**

Windows Fundamentals 3 reinforces the importance of built-in Windows security tools for protecting endpoints.  
For SOC analysts, the ability to quickly verify these settings is vital when assessing system security posture and responding to potential incidents.

