Intro to Endpoint Security

## **Intro to Endpoint Security — Notes**

### **1. Overview**

* **Endpoint Security** focuses on protecting endpoints (PCs, laptops, servers) from malicious activities.
* Key aspects include:
  + Securing **core system processes**.
  + Enabling **logging & monitoring**.
  + Analyzing logs for threat detection.

### **2. Endpoint Security Fundamentals**

* **Core Windows Processes**:
  + Essential system processes (e.g., lsass.exe, svchost.exe, winlogon.exe) must be protected and monitored.
  + Suspicious modification or replacement often indicates compromise.
* **Sysinternals Suite**:
  + Tools like Process Explorer, Autoruns, TCPView for process and startup analysis.

### **3. Endpoint Logging & Monitoring**

* **Windows Event Logging**:
  + Captures system, security, and application events.
* **Sysmon**:
  + Advanced logging of process creation, file changes, and network connections.
* **OSQuery**:
  + SQL-like querying of system data.
* **Wazuh**:
  + Open-source SIEM for log monitoring, file integrity, intrusion detection.

### **4. Endpoint Log Analysis**

* **Baselining**:
  + Documenting normal behavior so anomalies can be detected quickly.
* **Event Correlation**:
  + Linking related events to understand malicious activity context.
* **Artefact Collection**:
  + Recording malicious file names, hashes, IPs, domains for further investigation.
* **Lateral Impact Check**:
  + Identifying other potentially affected systems.

### **5. Investigation Takeaways**

* Baseline documents help differentiate benign vs malicious events.
* Event correlation gives deeper understanding of attack timelines.
* Artefact tracking ensures thorough remediation.
* Always inspect related systems after compromise indicators are found.

