**Types of Tools Used**

1. **Detection & Management Tools**
   * Monitor system activity
   * Identify suspicious or abnormal events
   * Examples: SIEM systems, IDS/IPS, endpoint detection tools
2. **Documentation Tools**
   * Collect and compile evidence
   * Track observations during investigations
   * Example: **Incident Handler's Journal** (your first tool)
3. **Investigative Tools**
   * Analyze incidents in-depth
   * Examples:
     + **Packet sniffers** (e.g., Wireshark)
     + **Log analyzers**
     + **Forensic tools**

**What is Documentation?**

* Any **recorded content** used for a specific purpose:
  + Digital (e.g., Google Docs, Jira)
  + Audio or video recordings
  + Handwritten notes
* Helps provide **instruction**, **guidance**, or **evidence**

**Common Types of Incident Documentation**

1. **Incident Handler's Journal**
   * Tracks the 5 W's: **Who, What, Where, When, Why**
2. **Playbooks**
   * Step-by-step operational guides
   * Like a product manual for responding to incidents
3. **Policies & Plans**
   * Formal rules and procedures (e.g., incident response plan)
4. **Final Reports**
   * Post-incident documentation detailing findings and outcomes

**Importance of Effective Documentation**

* Reduces **confusion** and **uncertainty**, especially during high-pressure incidents
* Supports **clear communication** and **swift decision-making**
* Critical for:
  + **Audit trails**
  + **Legal and compliance** requirements
  + **Post-incident analysis** and lessons learned

Bad documentation = unclear, inconsistent, or misleading instructions  
Good documentation = clear, consistent, and actionable

**Popular Documentation Tools**

* **Word Processors**: Google Docs, Notepad++, OneNote, Evernote
* **Ticketing Systems**: Jira, ServiceNow
* **Spreadsheets**: Google Sheets, Excel
* **Multimedia Tools**: Audio recorders, cameras
* **Manual Notes**: Handwritten journals, incident notebooks

**Intrusion Detection & Prevention Systems**

**🔍 Intrusion Detection System (IDS)**

* **What it does**:
  + Monitors **system** and **network activity**
  + Detects **suspicious or abnormal behavior**
  + Sends **alerts** to security teams but **does NOT block** activity
* **Analogy**: Like a **home alarm system**
  + Detects intrusions via sensors
  + Sends an alert to your phone if a window is broken

**🛡️ Intrusion Prevention System (IPS)**

* **What it does**:
  + Monitors for intrusions **and actively prevents** them
  + Can **block traffic**, terminate sessions, or modify firewall rules
* **Analogy**: Like a **storefront with a sensor** that not only detects a broken window, but also **deploys a steel barrier** to block access

**IDS vs. IPS**

| **Feature** | **IDS** | **IPS** |
| --- | --- | --- |
| Monitors traffic | ✅ | ✅ |
| Sends alerts | ✅ | ✅ |
| Takes action/blocking | ❌ | ✅ |

**Popular IDS/IPS Tools**

* **Snort**
* **Suricata** (covered in future lessons)
* **Zeek**
* **Kismet**
* **Sagan**

Many tools are **hybrid**, functioning as both IDS and IPS depending on how they're configured.