What is Splunk?
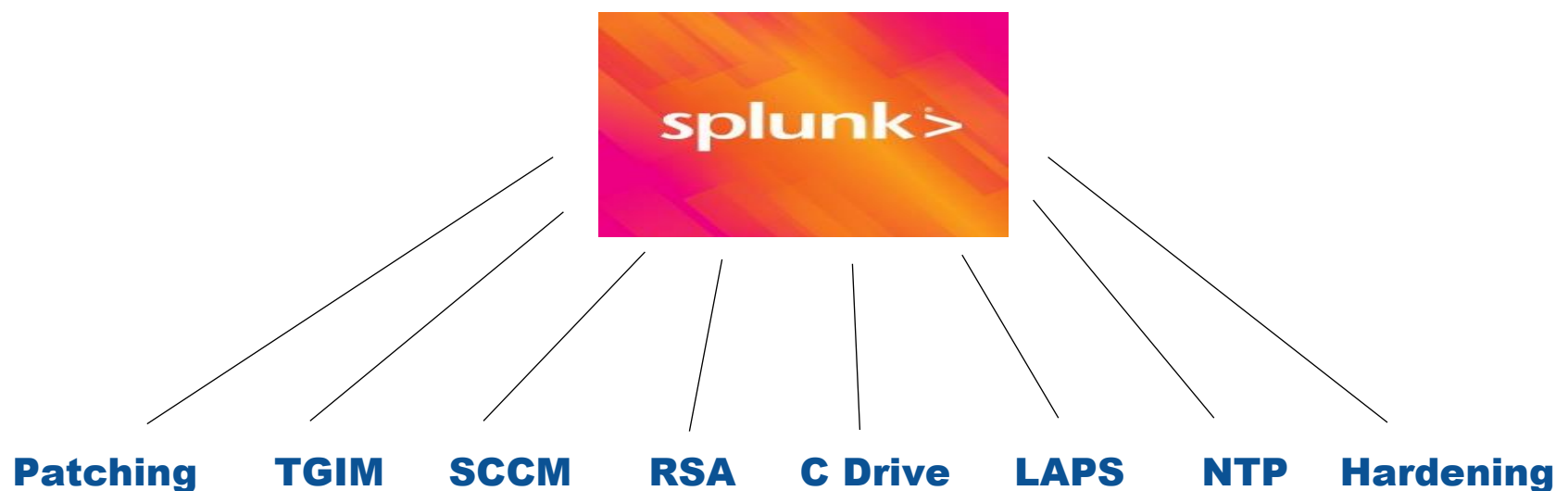
An Analytical Tool (Head/Parent Tool for monitoring all other important parameters of a server).

Some Major Parameters Monitored:

Patching   TGIM   SCCM   RSA   C Drive   LAPS   NTP   Hardening

Checkpoints to Troubleshoot:

> **Latest Kernel Version Should Be Installed:**

- 7.2 on Linux (Current)

- 7.3 on Windows (Current)

> **Make Sure Ports are Open from Source to Destination**

- telnet destination_IP port_no

  DEV:

  o telnet 172.17.11.61 8089, telnet 172 .17.11.61, 9997

  PROD:

  o telnet 172.17.8.179 8089, telnet 172.17.8.197 9997, telnet 172.17.8.198 9997

  > **Configuration Files should be Inline.**

  1. inputs.conf

  2. deploymentclient.conf

  3. server.conf

Please refer to snaps below for respective files and their content:

Some Points to be Noted:

> **Hostname should be the same on all 4:**

- **On Server**
- **In Personal Inventory owned by respective OS Teams.**
- **In Centralized Inventory (updated on weekends).**
- **In Splunk/Master Inventory (updated on weekends).**

PLEASE NOTE : THESE ARE SUBJECT TO CHANGES WRT IMPLEMENTATION OF CMDB.

> **Ensure server is not Powered Off/Decommissioned**

- **Please check current status of server and make sure respective status is updated in inventory for correct reflection.**

> **Any other Server – Specific / OS Related Issue:**

- **Server Not reachable due to network/hang state issue.**
- **Space Issue on Server (unable to install new version)**