Patch log data

Keeping operating systems and applications updated with the latest bug fixes and security patches is an essential task that can prevent unplanned downtime, random application crashes and security breaches. Although commercial apps and operating systems often have embedded patching software, some organizations use independent patch management software to consolidate patch management and ensure the consistent application of patches across their software fleet and to build patch jobs for custom, internal applications. Patch management software keeps a patch inventory using a database of available updates and can match these against an organization’s installed software. Other features include patch scheduling, post-install testing and validation and documentation of required system configurations and patching procedures. In the Common Information Model, antivirus data is typically mapped to the Updates data model.

Operations teams use patch logs to verify the timely and correct application of scheduled patches, identify unpatched systems and applications, and alert to errors in the patching process. Security teams can use patch logs to monitor system updates and determine which assets could be at risk, due to failed or out-of-date patches.

Application

When your Splunk deployment is ingesting patch log data, you can use it to accomplish security and compliance and IT Ops use cases.

- Maintaining Microsoft Windows systems
- Maintaining *nix systems
- Complying with General Data Protection Regulation
- Detecting Log4j remote code execution
- Deleting web shells automatically

Sources

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud).