What is Splunk and what is it used for?

Tell Me

This FAQ provides supplemental information for the Guideline for Security of Endpoints.

1. The ITS Security team uses Splunk Alerts for Security, Incident and Event Management (SIEM) to aggregate and correlate log data e.g. monitor login activity, traffic pattern analysis.
2. ITS works with IT staff and customers if suspicious activity is detected.
3. The solution varies depending on issue for example:
   a. suspicious password activity: If suspicious activity occurs (e.g. there are several attempts to change a password from multiple countries in a short amount of time) passwords are scrambled.
   b. endpoint vulnerability scans
4. For questions about Splunk, contact the IT Security group at security-group@uncc.edu.

Related FAQs

- How do I request an exception from University IT Guidelines for Endpoints, Systems and Applications?
- How do I request a new firewall rule?
- How do I request a privileged account for system/application administration?
- What vulnerability management tools are used at UNC Charlotte?
- What operating systems are supported on university servers?