NIST SP 800-53 configuration management

You need to monitor configuration and change management within your information technology enclave to ensure compliance to NIST SP 800-53 rev5.

Required data

- Data normalized to the following Common Information Models:
  - Change
  - Inventory

To optimize the searches shown below, you should specify an index and a time range.

Access restrictions for change

Part of your job as a system software administrator is to define, document, approve, and enforce physical and logical access restrictions associated with changes to the system. This search helps you monitor changes.

Windows

```
| tstats count FROM datamodel=Change WHERE All_Changes.vendor_product="Microsoft Windows" BY All_Changes.dest All_Changes.user All_Changes.result All_Changes.action
| search (All_Changes.user="*") (All_Changes.result="*") (All_Changes.dest="*") (All_Changes.action="*")
| rename All_Changes.user AS User All_Changes.result AS "System Activity" All_Changes.action AS Status All_Changes.dest AS Host
| dedup User, "System Activity"
```

Linux

```
| tstats count FROM datamodel=Change WHERE sourcetype=linux* BY All_Changes.dest All_Changes.user All_Changes.result All_Changes.action
| search (All_Changes.dest="*") (All_Changes.user="*") (All_Changes.result="*") (All_Changes.action="*")
| rename All_Changes.user AS User All_Changes.result AS "System Activity" All_Changes.action AS Action All_Changes.dest AS Host
```

User-installed software

While your users are allowed to install software on their systems, you need to monitor their activity at regular intervals for policy compliance.
Count of unapproved software

If you have lookup files of servers or workstations, you can get a count of the number of unapproved software installed on your organizational systems. If needed, change where is_server to where is_workstation and change your lookup accordingly.

```
| tstats count FROM datamodel=Inventory WHERE nodename=All_Inventory.OS All_Inventory.vendor_product=* BY All_Inventory.vendor_product, All_Inventory.dest
| rename All_Inventory.vendor_product AS product, All_Inventory.dest AS host
| lookup system_list system_name AS host
| where is_server = 1
| dedup product
| lookup approved_software_servers product AS product
| eval approval_status = if(is_approved == 1, 1, 0)
| stats count BY approval_status
| where approval_status = 0
| stats sum(count)
| rename sum(count) AS Unapproved_Vendor_Product_Instances
```

Approval status of servers

If you have lookup files of servers or workstations, you can get the approval status of software installed on your organizational systems. If needed, change where is_server to where is_workstation and change your lookup accordingly.

```
| tstats count FROM datamodel=Inventory WHERE nodename=All_Inventory.OS All_Inventory.vendor_product=* BY All_Inventory.vendor_product, All_Inventory.dest
| rename All_Inventory.vendor_product AS product, All_Inventory.dest as host
| lookup system_list system_name AS host
| where is_server = 1
| dedup product
| lookup approved_software_servers product AS product
| eval approval_status = if (is_approved == 1,"Approved_Vendor_Product","Unapproved_Vendor_Product")
| chart count BY approval_status
```

Server approval status by host

If you have lookup files of servers or workstations, you can get approval information and counts for all software installed on different hosts on your system. If needed, change where is_server to where is_workstation and change your lookup accordingly.

```
| tstats count FROM datamodel=Inventory WHERE nodename=All_Inventory.OS All_Inventory.vendor_product=* BY All_Inventory.vendor_product, All_Inventory.dest
| rename All_Inventory.vendor_product AS product, All_Inventory.dest AS host
| lookup system_list system_name AS host
| where is_server = 1
| search (host="*") (product="*")
| lookup approved_software_servers product AS product
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
eval approval_status = if (is_approved == 1,"Approved_Vendor_Product","Unapproved_Vendor_Product")

| stats sum(count) AS count BY host, approval_status, product
| sort -approval_status

Next steps

After running these access controls and taking appropriate action, you may want to look into other NIST SP 800-53 rev5 controls:

- Access control
- Audit and accountability
- Incident response
- Identification and authentication
- Risk assessment
- System and information integrity