



# Managing HPC Security at LANL using Splunk and Nessus

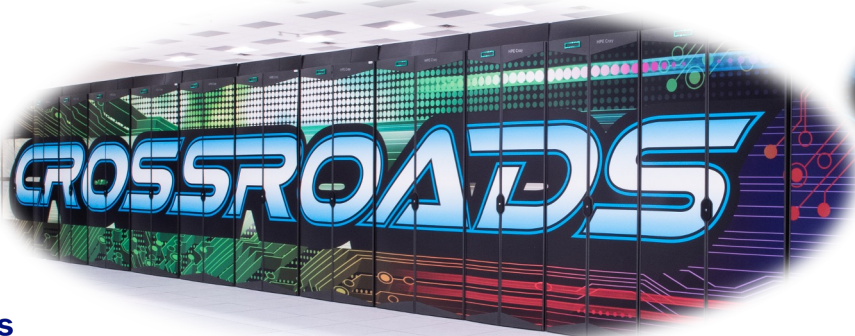
David Shrader  
LANL HPC ISSO

21 May 2024

LA-UR-24-24852

# What We're Going to Talk About

1. LANL HPC's current Security Motivations
2. Integrating Data into Splunk
3. Using that Data
  1. Operational Monitoring
  2. Continuous Security Monitoring
4. Enable Interactions based on that Data
  1. Automated Cyber Baseline
  2. Vulnerability Management



# HPC Security

- Effective security requires the use of:
  - Varied sources of data
  - Multiple tool sets
- Typically, each tool will have a standalone interface for interaction
  - Viewing results for the tool
  - Controlling the tool
- Combining data integration and tool control in Splunk can effectively turn it into a unified security engine

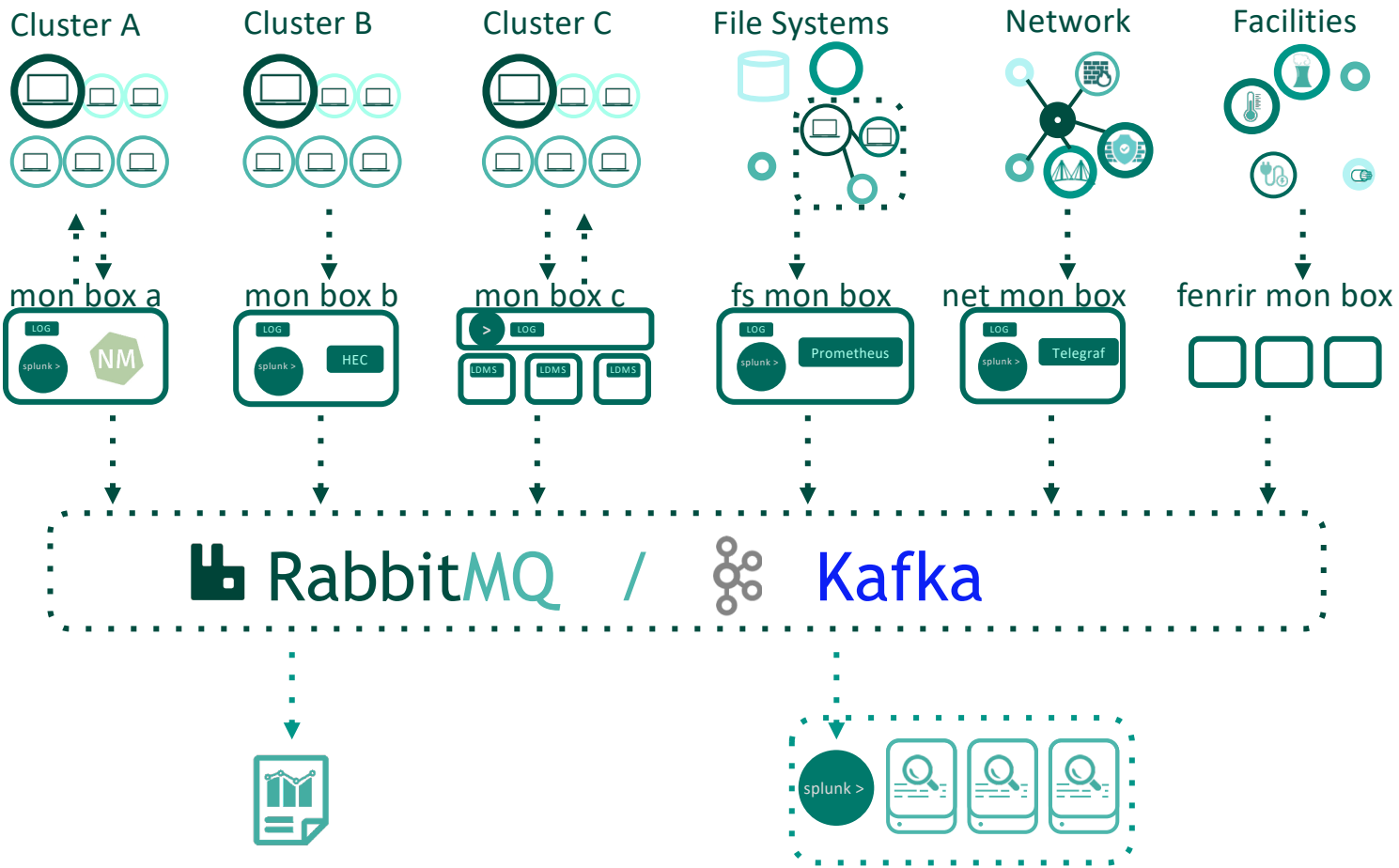
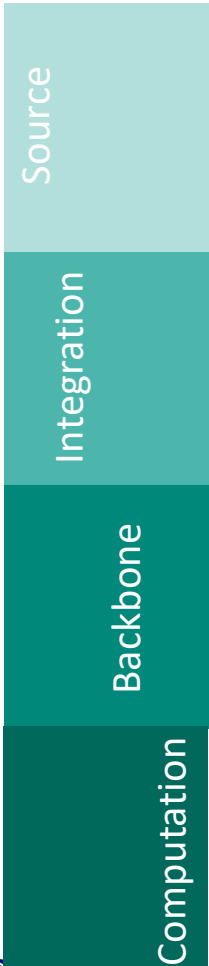


# Motivation For Pursuing a Unified Security Engine

- Having multiple security tools is great for increasing the scope of what is known about systems being managed
- Manually integrating the results between Tool X and Tool Y is not
- With each new tool comes a new management interface and more time spent context switching to carry out day to day tasks
- By creating a single location for both data and control, more time can be spent using the tools instead of managing them

# Integrating Data in Splunk

- The most straight forward step to creating a unified security engine
- Integrating data is the fundamental function of Splunk
- Allows HPC to combine data from multiple sources and correlate the results
  - Syslog (e.g., system logs, admin scripts, Slurm logs + queries)
  - Network logs (e.g., firewall)
  - Tenable vulnerability scans
  - Message Broker (e.g., Kafka, RabbitMQ)
- Ingesting system logs simply requires setting up a data source in Splunk
- For third-party tools, typically a Splunk app exists to do the integration
  - Tenable Add-On for Splunk handles Tenable data ingestion



# Use the Data

- Monitor and correlate data from different sources
- Provide Dashboards and Reports for various support roles
  - Operations
  - Admins
  - Cyber Analysts
- Alerts, alerts, alerts
- Operations Monitoring and Continuous Security Monitoring

# 24/7 Operations Monitoring

- HPC Cluster Monitoring
  - Interactive Dashboards
    - Highly customized to LANL HPC Operations Center
  - Custom acknowledgeable events
    - Alert Management
- Shared Resources (networks, filesystems, facilities)
  - High Visibility for Operators
  - Service Administrators can drill down to troubleshoot



# 24/7 Operations Monitoring

Home Clusters File Systems and Services HPC Websites DST Acknowledged Events Facilities Search Help Operations Team 1.3.3

Home Edit Export ...

HPC Websites Calendar On-call Tech Ops Wiki

Red=Page on-call Yellow=email Blue=DST

low

**Services**

monitoring 7x24

low

**Fenrir**

monitoring 7x24

low

**Campaign**

monitoring 5x9

low

**Lustre**

monitoring 7x24

low

**Logs**

monitoring 5x9

low

**ba** 96.97%

monitoring 5x9

DST

**cp** On DST

monitoring 5x9

low

**fg** 0.0%

monitoring 5x9

low

**gr** 34.36%

monitoring 5x9

low

**ko** 90.98%

monitoring 5x9

low

**sn** 98.1%

monitoring 5x9

severe

**tt** 16.50%

monitoring 5x9

low

**wc** 48.3%

monitoring 5x9

Network Status

| index   | Status |
|---------|--------|
| badger  | low    |
| fenrir  | low    |
| fog     | low    |
| grizzly | low    |
| kodiak  | low    |
| snow    | low    |

hw\_logger (Last Week)

| cluster | _time               | message   |
|---------|---------------------|---|
| fire    | 2019-04-01 16:56:24 | CABLE:ej316-cl16p3::REPLACE:replaced_part_number_and_description='10026784' replacement_part_number='' problem_description='link int error.' inSN='AF005H' outSN='WVG0097' part_from='Fire cab':td  |
| grizzly | 2019-04-01 15:41:30 | NODE:gr0556::CADDY_SLAM:Node was not responsive and thus a caddy slam has been performed.:robbieg   |
| grizzly | 2019-04-01 15:41:05 | NODE:gr0635::CADDY_SLAM:Node was not responsive and thus a caddy slam has been performed.:robbieg   |
| grizzly | 2019-04-01 15:40:48 | NODE:gr0629::CADDY_SLAM:Node was not responsive and thus a caddy slam has been performed.:robbieg   |
| badger  | 2019-04-01 15:29:17 | NODE:ba438:P100189257::PART_RESEAT:Node was having link errors so, the card has been reseated. If this fails then a temp will be ran.:robbieg   |
| badger  | 2019-04-01 15:29:14 | NODE:ba438:P100189257::PART_RESEAT:Node was having link errors so, the card has been reseated. If this fails then a temp will be ran.:robbieg   |
| badger  | 2019-04-01 15:27:43 | NODE:ba379:P100189115::PART_RESEAT:Node was having lboot and link errors. Reseated all hardware.:robbieg  |
| grizzly | 2019-04-01 15:23:49 | CLUSTER::NOTE:gr-ngmt-sw18 wash power cycled per request of Chuck Wilder:robbieg  |
| cyclone | 2019-04-01 10:18:34 | SERVER:cy-master:p100182146::REPLACE:replaced_part_number_and_description='10025873' replacement_part_number='' problem_description='cy-master was having connection issues with the opa link. A temporary cable was installed and issue went away. Removed defective cables, relabeled new cable, and pushed cable ends to the top of the racks.' inSN='s5177aa089d' outSN='s5178aa003c' part_from='From the cyclone parts cabinet that Bob our penguin parts professional keep stocked':NJB/rcc |

< prev 1 2 3 next >

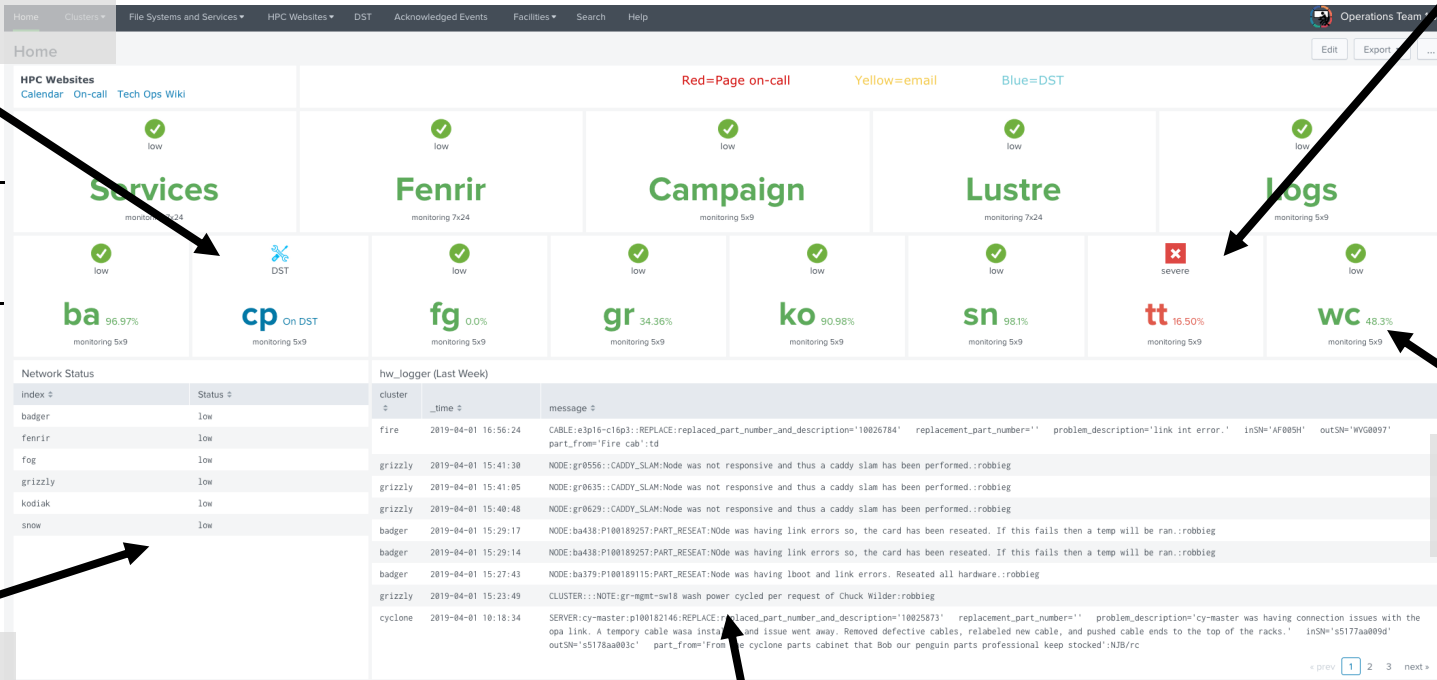
# 24/7 Operations Monitoring

Automatic DST  
Detection – Alerts  
Suppressed

Errors Bubble Up

Shared Systems

Clusters



Utilization  
Snapshot

HSN Status

Ops Hardware  
Notes Logged

# Panel Drilldown with Acknowledgments

## Kodiak

Kodiak specific dashboard because it has infiniband

### kodiak Utilization and Temperature (Past 48 hours)

Notes

— select time to ignore future events —

[more info!](#)

select username

Submit

### Averages Per Node (Past 24 hours)

---

### Network Errors

#### IBMON Errors (Last 48 Hours)

No results found.

#### Dead Gateway Detection (Last Hour)

Not all messages below require action  
Please reference [wiki](http://wiki.lanl.gov/ore/DGGenarMessages) to find which teams to alert depending on CRITICAL or FAIL messages

No results found.

---

### System Messages

#### GPU Slowdown

Please drain node: The GPU is being throttled due to temperature or power issues.  
For more information ssh to node and run `nvidia-smi -q`

No results found.

---

### Slurm Status

| Time                | Device | Type     | message             | Severity                             |
|---------------------|--------|----------|---------------------|--------------------------------------|
| 2019-04-01 19:53:05 | kodiak | slurctid | slurctid is running | <span style="color: green;">●</span> |

Slurmdbd Queue Filling

After hours page 4-0109  
During normal business please confirm dim-team@lanl.gov has been notified

No results found.

### Ping Errors (Last 5 minutes)

| Time                | Device | message                    | Severity                           |
|---------------------|--------|----------------------------|------------------------------------|
| 2019-04-01 19:58:05 | ko105  | compute node ko105 is down | <span style="color: red;">●</span> |
| 2019-04-01 19:58:05 | ko029  | compute node ko029 is down | <span style="color: red;">●</span> |
| 2019-04-01 19:58:05 | ko016  | compute node ko016 is down | <span style="color: red;">●</span> |

No results found.

---

### EDAC Errors (Last 7 days)

No results found.

---

### Out of Memory Errors

No results found.

---

### Rectifier Status Errors

No results found.

---

### Fan Speed Errors (Last 15 minutes)

No results found.

---

### Temperature Errors (Last 15 minutes)

No results found.

---

### CDU - Unable to communicate (Last 48 hours)

No results found.

---

### CDU - Thresholds triggered (Last 48 hours)

[More CDU info Here](#)

No results found.

---

### IPMI-Sensor Errors (Last 15mins)

No results found.

---

### System Event Log is Full

Please check and clear the SEL to avoid losing logs on the node  
[Here to check SEL, ssh to node and run ipmi-sel](#)  
[How to clear SEL, ssh to node and run ipmi-sel -clear](#)

# Panel Drilldown with Acknowledgments

**Kodiak**  
Kodiak specific dashboard because it has infiniband

**kodiak Utilization and Temperature (Past 48 hours)**  
Utilization: 100  
Averages Per Node (Past 24 hours): Max Fan Speed, Temperature

**Network Errors**  
IBMON Errors (Last 48 Hours)  
No results found.

**System Messages**  
GPU Slowdown  
Please drain node: The GPU is being throttled due to temperature or power issues.  
For more information run `nvdiagsaml -q`  
No results found.

**Slurm Status**  
Slurmd Queue Filling  
After hours page 4-0189  
During normal business please confirm dim-team@lanl.gov has been notified

| Time                | Device | Type   | message             | Severity |
|---------------------|--------|--------|---------------------|----------|
| 2019-04-01 19:53:05 | kodiak | slurmd | slurmdId is running | Info     |

Cluster Usage

Acknowledgments  
With Timeframe

Errors that can be  
Ack'd or Bubble  
up to Top Page

Fixed Panels  
looking for  
Known Errors

**Ping Errors (Last 5 minutes)**

| Time                | Device | message                    | Severity |
|---------------------|--------|----------------------------|----------|
| 2019-04-01 19:58:05 | ko105  | compute node ko105 is down | Critical |
| 2019-04-01 19:58:05 | ko029  | compute node ko029 is down | Critical |
| 2019-04-01 19:58:05 | ko016  | compute node ko016 is down | Critical |

**EDAC Errors (Last 7 days)**  
No results found.

**Rectifier Status Errors**  
No results found.

**Temperature Errors (Last 15 minutes)**  
No results found.

**CDU - Unable to communicate (Last 48 hours)**  
No results found.

**IPMI-Sensor Errors (Last 15mins)**  
No results found.

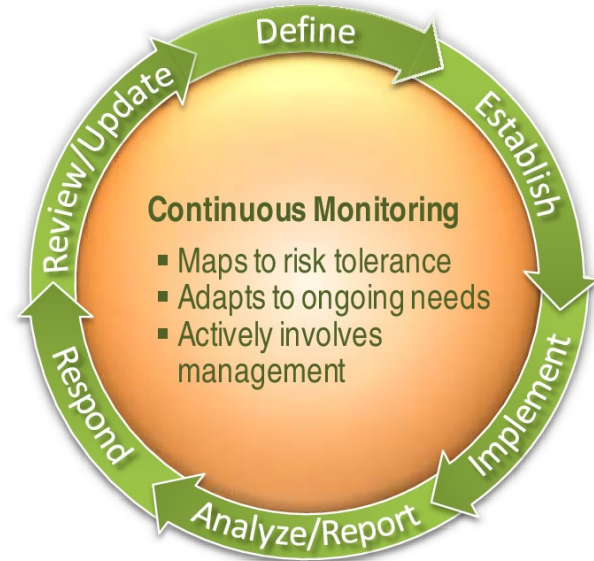
**System Event Log is Full**  
Please check and clear the SEL to avoid losing logs on the node  
How to check SEL: `ssh to node and run ipmi-sel`  
How to clear SEL: `ssh to node and run ipmi-sel -clear`  
No results found.

# Alerts on the Cyber Panel

- Empty most of the time
- Alerts when thresholds are reached for:
  - Illegal Escalation Attempts
  - Failed Gateway Logins
  - Failed Cluster Logins
  - Login by Invalid User
- Allows 24/7 Operators to monitor for known cyber events, frees up Cyber folks

# Continuous Security Monitoring

- Big picture for NIST 800-137
  - Information Security Continuous Monitoring
  - Continuous Diagnostics and Mitigation
- OS Versions
- Track Downtime
- Vulnerabilities
- Firewall policy trigger counts
- Recording known attack surfaces

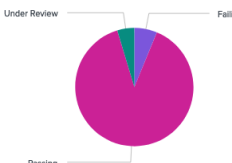


# Continuous Security Monitoring

## Executive Overview

Home page for Continuous Security Monitoring

Edit Export ...

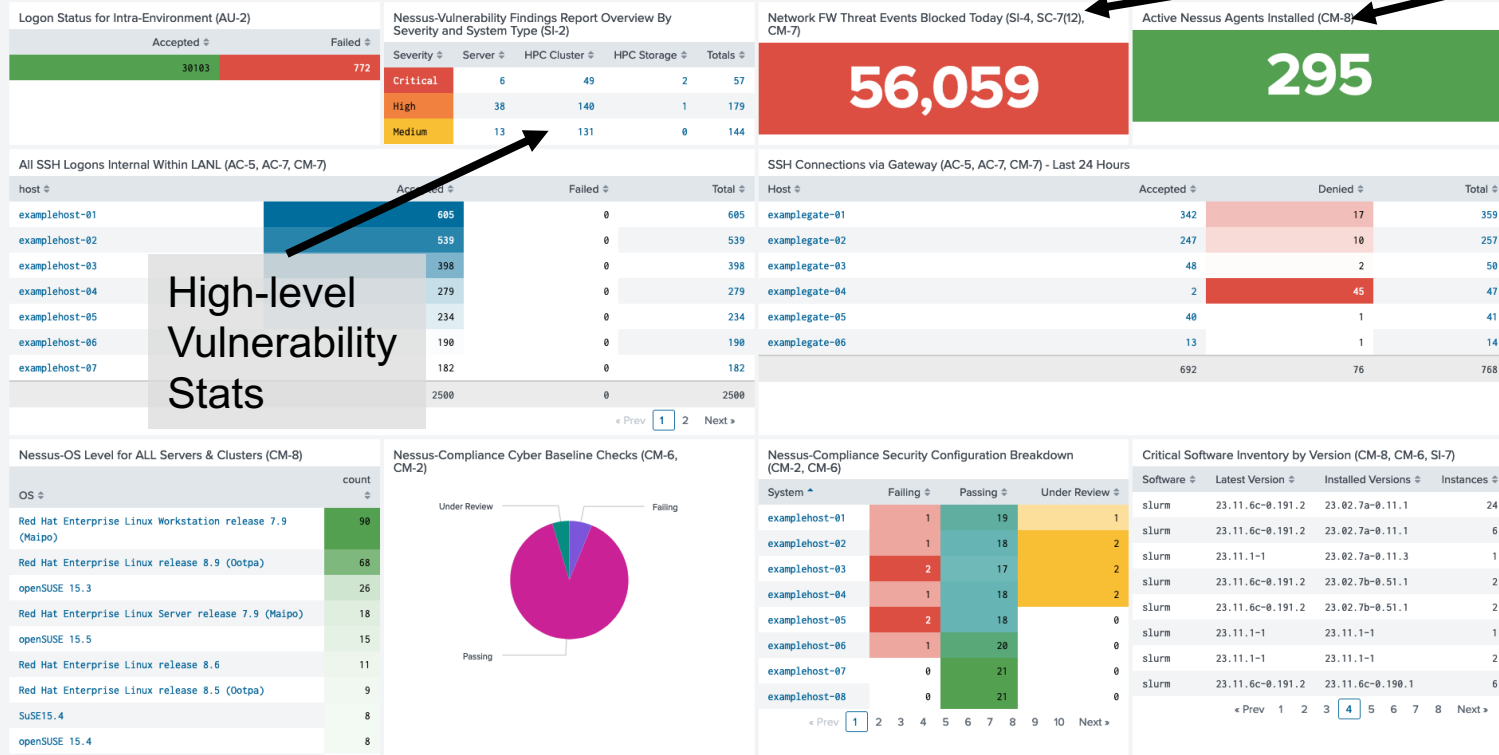
| <b>Logon Status for Intra-Environment (AU-2)</b><br>Accepted <span>38103</span> Failed <span>772</span>   |                  | <b>Nessus-Vulnerability Findings Report Overview By Severity and System Type (SI-2)</b><br>Severity <span>Server <span>6</span> HPC Cluster <span>49</span> HPC Storage <span>2</span> Totals <span>57</span></span><br>High <span>38</span> 140 1 179<br>Medium <span>13</span> 131 0 144 |              |  |      |  | <b>Network FW Threat Events Blocked Today (SI-4, SC-7(12), CM-7)</b><br><div style="background-color: red; color: white; padding: 20px; text-align: center; font-size: 2em; font-weight: bold;">56,059</div> |               |                | <b>Active Nessus Agents Installed (CM-8)</b><br><div style="background-color: green; color: white; padding: 20px; text-align: center; font-size: 2em; font-weight: bold;">295</div> |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
|---|------------------|--|--------------|--|------|--|--|---------------|----------------|---|----|---------------|----------------|--------------------------------------|----|--|----------------|----------|---|---------------|----------------|--|---|-----|--|-----|---|--------|----------------|---------|--------------|----------------|----------------|-----|---|----------------|--------------|-------------|----------|----------------|---|----|---|----------------|---|------|----------|----------------|-------|----------------|-----|----------------|-----|----------------|-----|----------------|-----|----------------|----|----------------|----|----------------|---|--|----|----------------|----------|----------------|--------------------|----------------|-------|------------------|-----------------|--------------|------------|------------------|-----------------|---|-------|-----------|-----------------|---|-------|------------------|-----------------|---|-------|------------------|-----------------|---|-------|-----------|-----------|---|-------|-----------|-----------|---|-------|------------------|------------------|---|
| <b>All SSH Logons Internal Within LANL (AC-5, AC-7, CM-7)</b><br><table border="1"> <thead> <tr> <th>host</th> <th>Accepted</th> <th>Failed</th> <th>Total</th> </tr> </thead> <tbody> <tr><td>examplehost-01</td><td>605</td><td>0</td><td>605</td></tr> <tr><td>examplehost-02</td><td>539</td><td>0</td><td>539</td></tr> <tr><td>examplehost-03</td><td>398</td><td>0</td><td>398</td></tr> <tr><td>examplehost-04</td><td>279</td><td>0</td><td>279</td></tr> <tr><td>examplehost-05</td><td>234</td><td>0</td><td>234</td></tr> <tr><td>examplehost-06</td><td>190</td><td>0</td><td>190</td></tr> <tr><td>examplehost-07</td><td>182</td><td>0</td><td>182</td></tr> <tr><td><b>Total</b></td><td><b>2500</b></td><td><b>0</b></td><td><b>2500</b></td></tr> </tbody> </table> |                  |  |              |  | host | Accepted                                     | Failed   | Total         | examplehost-01 | 605   | 0  | 605           | examplehost-02 | 539                                  | 0  | 539  | examplehost-03 | 398      | 0 | 398           | examplehost-04 | 279  | 0 | 279 | examplehost-05   | 234 | 0 | 234    | examplehost-06 | 190     | 0            | 190            | examplehost-07 | 182 | 0 | 182            | <b>Total</b> | <b>2500</b> | <b>0</b> | <b>2500</b>    | <b>SSH Connections via Gateway (AC-5, AC-7, CM-7) - Last 24 Hours</b><br><table border="1"> <thead> <tr> <th>Host</th> <th>Accepted</th> <th>Denied</th> <th>Total</th> </tr> </thead> <tbody> <tr><td>examplegate-01</td><td>342</td><td>17</td><td>359</td></tr> <tr><td>examplegate-02</td><td>247</td><td>10</td><td>257</td></tr> <tr><td>examplegate-03</td><td>48</td><td>2</td><td>50</td></tr> <tr><td>examplegate-04</td><td>2</td><td>45</td><td>47</td></tr> <tr><td>examplegate-05</td><td>48</td><td>1</td><td>41</td></tr> <tr><td>examplegate-06</td><td>13</td><td>1</td><td>14</td></tr> <tr><td><b>Total</b></td><td><b>692</b></td><td><b>76</b></td><td><b>768</b></td></tr> </tbody> </table> |    |   |                |   | Host | Accepted | Denied         | Total | examplegate-01 | 342 | 17             | 359 | examplegate-02 | 247 | 10             | 257 | examplegate-03 | 48 | 2              | 50 | examplegate-04 | 2 | 45   | 47 | examplegate-05 | 48       | 1              | 41                 | examplegate-06 | 13    | 1                | 14              | <b>Total</b> | <b>692</b> | <b>76</b>        | <b>768</b>      |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| host  | Accepted         | Failed   | Total        |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-01  | 605              | 0  | 605          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-02  | 539              | 0  | 539          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-03  | 398              | 0  | 398          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-04  | 279              | 0  | 279          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-05  | 234              | 0  | 234          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-06  | 190              | 0  | 190          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-07  | 182              | 0  | 182          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| <b>Total</b>  | <b>2500</b>      | <b>0</b>   | <b>2500</b>  |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Host  | Accepted         | Denied   | Total        |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplegate-01  | 342              | 17   | 359          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplegate-02  | 247              | 10   | 257          |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplegate-03  | 48               | 2  | 50           |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplegate-04  | 2                | 45   | 47           |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplegate-05  | 48               | 1  | 41           |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplegate-06  | 13               | 1  | 14           |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| <b>Total</b>  | <b>692</b>       | <b>76</b>  | <b>768</b>   |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| <b>Nessus-OS Level for ALL Servers &amp; Clusters (CM-8)</b><br><table border="1"> <thead> <tr> <th>OS</th> <th>count</th> </tr> </thead> <tbody> <tr><td>Red Hat Enterprise Linux Workstation release 7.9 (Maipo)</td><td>90</td></tr> <tr><td>Red Hat Enterprise Linux release 8.9 (Ootpa)</td><td>68</td></tr> <tr><td>openSUSE 15.3</td><td>26</td></tr> <tr><td>Red Hat Enterprise Linux Server release 7.9 (Maipo)</td><td>18</td></tr> <tr><td>openSUSE 15.5</td><td>15</td></tr> <tr><td>Red Hat Enterprise Linux release 8.6</td><td>11</td></tr> <tr><td>Red Hat Enterprise Linux release 8.5 (Ootpa)</td><td>9</td></tr> <tr><td>SUSE15.4</td><td>8</td></tr> <tr><td>openSUSE 15.4</td><td>8</td></tr> </tbody> </table>  |                  | OS   | count        | Red Hat Enterprise Linux Workstation release 7.9 (Maipo) | 90   | Red Hat Enterprise Linux release 8.9 (Ootpa) | 68   | openSUSE 15.3 | 26             | Red Hat Enterprise Linux Server release 7.9 (Maipo)   | 18 | openSUSE 15.5 | 15             | Red Hat Enterprise Linux release 8.6 | 11 | Red Hat Enterprise Linux release 8.5 (Ootpa) | 9              | SUSE15.4 | 8 | openSUSE 15.4 | 8              | <b>Nessus-Compliance Cyber Baseline Checks (CM-6, CM-2)</b><br> |   |     | <b>Nessus-Compliance Security Configuration Breakdown (CM-2, CM-6)</b><br><table border="1"> <thead> <tr> <th>System</th> <th>Failing</th> <th>Passing</th> <th>Under Review</th> </tr> </thead> <tbody> <tr><td>examplehost-01</td><td>1</td><td>19</td><td>1</td></tr> <tr><td>examplehost-02</td><td>1</td><td>18</td><td>2</td></tr> <tr><td>examplehost-03</td><td>2</td><td>17</td><td>2</td></tr> <tr><td>examplehost-04</td><td>1</td><td>18</td><td>2</td></tr> <tr><td>examplehost-05</td><td>2</td><td>18</td><td>0</td></tr> <tr><td>examplehost-06</td><td>1</td><td>20</td><td>0</td></tr> <tr><td>examplehost-07</td><td>0</td><td>21</td><td>0</td></tr> <tr><td>examplehost-08</td><td>0</td><td>21</td><td>0</td></tr> </tbody> </table> |     |   | System | Failing        | Passing | Under Review | examplehost-01 | 1              | 19  | 1 | examplehost-02 | 1            | 18          | 2        | examplehost-03 | 2   | 17 | 2 | examplehost-04 | 1 | 18   | 2        | examplehost-05 | 2     | 18             | 0   | examplehost-06 | 1   | 20             | 0   | examplehost-07 | 0   | 21             | 0  | examplehost-08 | 0  | 21             | 0 | <b>Critical Software Inventory by Version (CM-8, CM-6, SI-7)</b><br><table border="1"> <thead> <tr> <th>Software</th> <th>Latest Version</th> <th>Installed Versions</th> <th>Instances</th> </tr> </thead> <tbody> <tr><td>slurm</td><td>23.11.6c-0.191.2</td><td>23.02.7a-0.11.1</td><td>24</td></tr> <tr><td>slurm</td><td>23.11.6c-0.191.2</td><td>23.02.7a-0.11.1</td><td>6</td></tr> <tr><td>slurm</td><td>23.11.1-1</td><td>23.02.7a-0.11.3</td><td>1</td></tr> <tr><td>slurm</td><td>23.11.6c-0.191.2</td><td>23.02.7b-0.51.1</td><td>2</td></tr> <tr><td>slurm</td><td>23.11.6c-0.191.2</td><td>23.02.7b-0.51.1</td><td>2</td></tr> <tr><td>slurm</td><td>23.11.1-1</td><td>23.11.1-1</td><td>1</td></tr> <tr><td>slurm</td><td>23.11.1-1</td><td>23.11.1-1</td><td>2</td></tr> <tr><td>slurm</td><td>23.11.6c-0.191.2</td><td>23.11.6c-0.190.1</td><td>6</td></tr> </tbody> </table> |    |                | Software | Latest Version | Installed Versions | Instances      | slurm | 23.11.6c-0.191.2 | 23.02.7a-0.11.1 | 24           | slurm      | 23.11.6c-0.191.2 | 23.02.7a-0.11.1 | 6 | slurm | 23.11.1-1 | 23.02.7a-0.11.3 | 1 | slurm | 23.11.6c-0.191.2 | 23.02.7b-0.51.1 | 2 | slurm | 23.11.6c-0.191.2 | 23.02.7b-0.51.1 | 2 | slurm | 23.11.1-1 | 23.11.1-1 | 1 | slurm | 23.11.1-1 | 23.11.1-1 | 2 | slurm | 23.11.6c-0.191.2 | 23.11.6c-0.190.1 | 6 |
| OS  | count            |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Red Hat Enterprise Linux Workstation release 7.9 (Maipo)  | 90               |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Red Hat Enterprise Linux release 8.9 (Ootpa)  | 68               |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| openSUSE 15.3   | 26               |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Red Hat Enterprise Linux Server release 7.9 (Maipo)   | 18               |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| openSUSE 15.5   | 15               |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Red Hat Enterprise Linux release 8.6  | 11               |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Red Hat Enterprise Linux release 8.5 (Ootpa)  | 9                |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| SUSE15.4  | 8                |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| openSUSE 15.4   | 8                |  |              |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| System  | Failing          | Passing  | Under Review |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-01  | 1                | 19   | 1            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-02  | 1                | 18   | 2            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-03  | 2                | 17   | 2            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-04  | 1                | 18   | 2            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-05  | 2                | 18   | 0            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-06  | 1                | 20   | 0            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-07  | 0                | 21   | 0            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| examplehost-08  | 0                | 21   | 0            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| Software  | Latest Version   | Installed Versions   | Instances    |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.6c-0.191.2 | 23.02.7a-0.11.1  | 24           |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.6c-0.191.2 | 23.02.7a-0.11.1  | 6            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.1-1        | 23.02.7a-0.11.3  | 1            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.6c-0.191.2 | 23.02.7b-0.51.1  | 2            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.6c-0.191.2 | 23.02.7b-0.51.1  | 2            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.1-1        | 23.11.1-1  | 1            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.1-1        | 23.11.1-1  | 2            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |
| slurm   | 23.11.6c-0.191.2 | 23.11.6c-0.190.1   | 6            |  |      |  |  |               |                |   |    |               |                |                                      |    |  |                |          |   |               |                |  |   |     |  |     |   |        |                |         |              |                |                |     |   |                |              |             |          |                |   |    |   |                |   |      |          |                |       |                |     |                |     |                |     |                |     |                |    |                |    |                |   |  |    |                |          |                |                    |                |       |                  |                 |              |            |                  |                 |   |       |           |                 |   |       |                  |                 |   |       |                  |                 |   |       |           |           |   |       |           |           |   |       |                  |                  |   |

# Continuous Security Monitoring

NIST 800-53 control reference

## Executive Overview

Home page for Continuous Security Monitoring



High-level Vulnerability Stats

Login Events

Inventory and Compliance



# Expand Usability of Splunk by Allowing Interaction

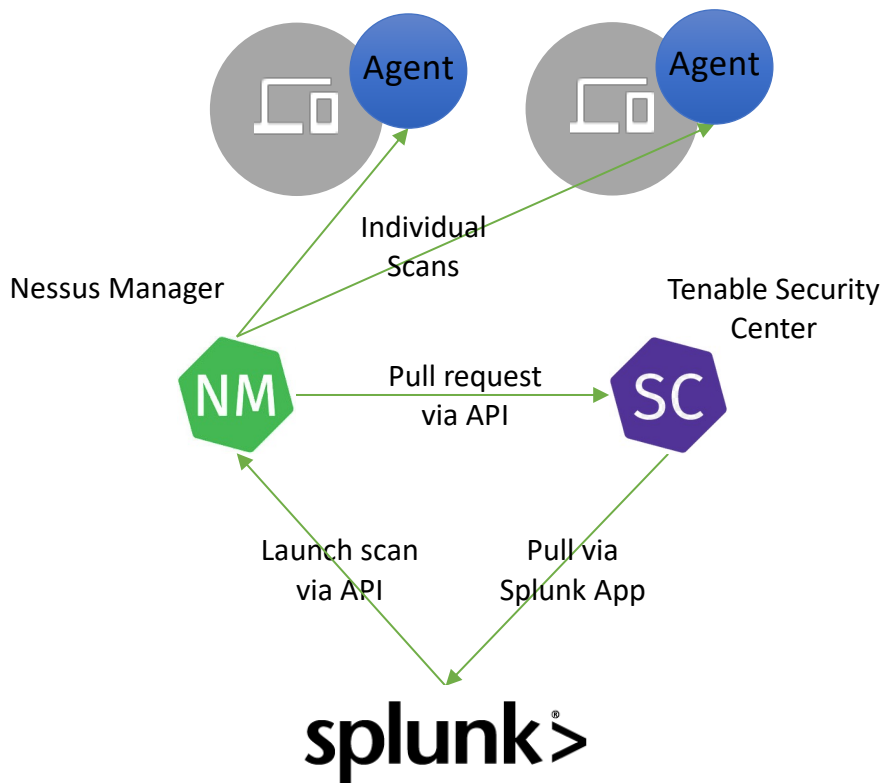
- Two types of interaction: stateful information and other tool control
- Stateful information
  - Allows admins to provide information about data in the context of that data
  - Utilizes Splunk kvstores
- Other Tool control
  - Allow controlled access to security tools without directly accessing the tool itself
  - Empowers administrators to fix system issues before they become a problem
  - Helps make security more transparent to the administrators
    - Fewer surprise security notices
- Two areas where this interaction is leveraged
  - Automated Cyber Baseline (Compliance Check)
  - Vulnerability Management

# Adding Control Capabilities to Splunk

- The not so straight forward way of using Splunk
- Having to log into multiple interfaces to get updated data is tedious
- The preferred method is to perform these operations from where data is being viewed
  - Singular familiar interface
- Motivating factor was launching Tenable's Nessus Agent scans
  - Utilized for both Automated Cyber Baseline and Vulnerability Scans



# Interacting With Nessus from Splunk



- Achieved using custom searches that use the Tenable API
- A button on dashboards will use JavaScript to launch searches using the Splunk API
- The custom searches use Python for handling Tenable API calls
- Scan progress is provided as feedback on the dashboard

# Automated Cyber Baseline – Multi-Host View

## Systems With Non-Passing Controls

| Systems ⇅      | Failing Controls ⇅ | Needs Admin Review ⇅ | Acknowledged by Admin ⇅ |
|----------------|--------------------|----------------------|-------------------------|
| examplehost-01 | 1                  | 0                    | 0                       |
| examplehost-02 | 1                  | 3                    | 0                       |
| examplehost-03 | 1                  | 1                    | 1                       |
| examplehost-05 | 0                  | 1                    | 0                       |
| examplehost-06 | 0                  | 0                    | 1                       |
| examplehost-07 | 0                  | 1                    | 0                       |

## Passing Systems

| System ⇅       | Passing Since ⇅             |
|----------------|-----------------------------|
| examplehost-04 | 05/07/2024 07:43:34.0000000 |

# Automated Cyber Baseline – Multi-Host View

All Hosts in a Group are viewable

Total number of each type of control:

- Failing
- Needs Admin Review
- Acknowledged

## Systems With Non-Passing Controls

| Systems ⇅      | Failing Controls ⇅ | Needs Admin Review ⇅ | Acknowledged by Admin ⇅ |
|----------------|--------------------|----------------------|-------------------------|
| examplehost-01 | 1                  | 0                    | 0                       |
| examplehost-02 | 1                  | 3                    | 0                       |
| examplehost-03 | 1                  | 1                    | 1                       |
| examplehost-05 | 0                  | 1                    | 0                       |
| examplehost-06 | 0                  | 0                    | 1                       |
| examplehost-07 | 0                  | 1                    | 0                       |

## Passing Systems

| System ⇅       | Passing Since ⇅             |
|----------------|-----------------------------|
| examplehost-04 | 05/07/2024 07:43:34.0000000 |

Screen Shot of the Multi-Machine view of the Automated Cybe Baseline Dashboard

# Automated Cyber Baseline – Host & Control View

Latest Scan of examplehost-03

**2024-05-07 07:37:10**

► Please allow a minute for results to update

Relaunch Scan

► more info?

## Overview of examplehost-03

| Control ↕ | NIST 800-53r4 ↕          | Info ↕                                 | Result ↕              |
|-----------|--------------------------|--|-----------------------|
| HPC001    | CM-3, IA-2               | Hostbased Auth Configuration           | Pass                  |
| HPC003    | AC-2, AC-6               | Radius Configuration                   | Pass                  |
| HPC004    | IA-5, AC-17              | Static Passwords and Remote Root Login | Pass                  |
| HPC005    | IA-2, IA-5               | Kerberos Configuration                 | Pass                  |
| HPC006    | AC-2, AC-3, AC-6, IA-5   | Service and User Accounts              | Needs Admin Review    |
| HPC009    | AC-8                     | DOE Warning and Consent Banner         | Pass                  |
| HPC010    | CM-7                     | Listening Ports                        | Pass                  |
| HPC012    | AC-6, CM-6, SI-7         | Configuration Management               | Pass                  |
| HPC013    | CM-7                     | Service Configuration                  | Fail                  |
| HPC015    | AU-2, AU-3, AU-4         | Log Message Configuration              | Acknowledged by Admin |
| HPC016    | AC-17, AC-23, CM-5, SC-2 | Firewall Configuration                 | Pass                  |
| HPC017    | SI-2                     | Nessus Agent                           | Pass                  |
| HPC018    | AC-6, AU-6               | Auditd Configuration                   | Pass                  |
| HPC019    | SI-3                     | Security Tools                         | Pass                  |
| HPC021    | SI-2                     | OS Version Check                       | Pass                  |
| HPC022    | SI-2, RA-5               | Vulnerability Management               | Pass                  |

# Automated Cyber Baseline – Host & Control View

Latest Scan of examplehost-03  
**2024-05-07 07:37:10**

► Please allow a minute for results to update

Overview of examplehost-03

Relaunch Scan

more info?

Tenable interaction through Splunk

| Control | NIST 800-53r4            | Info                                   | Result                |
|---------|--------------------------|--|-----------------------|
| HPC001  | CM-3, IA-2               | Hostbased Auth Configuration           | Pass                  |
| HPC003  | AC-2, AC-6               | Radius Configuration                   | Pass                  |
| HPC004  | IA-5, AC-17              | Static Passwords and Remote Root Login | Pass                  |
| HPC005  | IA-2, IA-5               | Kerberos Configuration                 | Pass                  |
| HPC006  | AC-2, AC-3, AC-6, IA-5   | Service and User Management            | Needs Admin Review    |
| HPC009  | AC-8                     | DOE Warning                            | Pass                  |
| HPC010  | CM-7                     | Listening Ports                        | Pass                  |
| HPC012  | AC-6, CM-6, SI-7         | Configuration Management               | Pass                  |
| HPC013  | CM-7                     | Service Configuration                  | Fail                  |
| HPC015  | AU-2, AU-3, AU-4         | Log Message Configuration              | Acknowledged by Admin |
| HPC016  | AC-17, AC-23, CM-5, SC-2 | Firewall Configuration                 | Pass                  |
| HPC017  | SI-2                     | Network Monitoring                     | Pass                  |
| HPC018  | AC-6, AU-6               | System Time                            | Pass                  |
| HPC019  | SI-3                     | System Time                            | Pass                  |
| HPC021  | SI-2                     | System Time                            | Pass                  |
| HPC022  | SI-2, RA-5               | System Time                            | Pass                  |

Manual review by admin leads to security admin review

LANL HPC specific configurations to fulfill NIST 800-53

# Automated Cyber Baseline - Acknowledgments

Latest Scan of examplehost-03

**2024-05-07 07:37:10**

▶ Please allow a minute for results to update

Relaunch Scan

▶ more info?

## Breakdown of Control

Summary for examplehost-03

Control ID

HPC015

| Sub-Controls | Result                | Info  | Return Value   | Previous Return Value   |
|--------------|-----------------------|---|--|---|
| HPC015-01    | Acknowledged by Admin | Check that at least one log message was received each hour over the last 48H      | 43   | 42  |
| HPC015-02    | Pass                  | Check that at least one SSHD log has been received in the 10 days                 | No known logins since 2024-04-24   | No SSHD logs  |
| HPC015-03    | Pass                  | List of splunk systems where logs are stored.<br>Recorded for reporting purposes. | splunkexample-01.lan1.gov<br>splunkexample-02.lan1.gov<br>splunkexample-03.lan1.gov<br>splunkexample-04.lan1.gov | splunkexample-01.lan1.gov<br>splunkexample-02.lan1.gov<br>splunkexample-03.lan1.gov |

## New Acknowledgement

System Selection

examplehost-03

Enter comments regarding reviewed controls and security exemptions

Acknowledgement Comment

Optional RT ticket number

Submit Undo

Submitting as John Smith

## Current Acknowledgements

| Time                | Comment   | Exemption Expires | ticketNum | Acknowledger |
|---------------------|---|-------------------|-----------|--------------|
| 2024-05-08 07:00:53 | Logging was interrupted due to a misconfiguration and has been fixed. Logs have started reaching Splunk again |                   | N/A       | John Smith   |



# Automated Cyber Baseline - Acknowledgments

Latest Scan of examplehost-03

**2024-05-07 07:37:10**

▶ Please allow a minute for results to update

Relaunch Scan

▶ more info?

**Sub-controls**

Summary for examplehost-03

Control ID: HPC015

| Sub-Controls | Result                | Info   | Return Value   | Previous Return Value  |
|--------------|-----------------------|--|--|--|
| HPC015-01    | Acknowledged by Admin | Check that at least one log message was received each hour over the last 48H   | 43   | 42   |
| HPC015-02    | Pass                  | Check that at least one SSHD log has been received in the 10 days              | No known logins since 2024-04-24   | No SSHD logs   |
| HPC015-03    | Pass                  | List of splunk systems where logs are stored. Recorded for reporting purposes. | splunkexample-01.lan1.gov<br>splunkexample-02.lan1.gov<br>splunkexample-03.lan1.gov<br>splunkexample-04.lan1.gov | splunkexample-01.lan1.gov<br>splunkexample-02.lan1.gov<br>splunkexample-03.lan1.gov<br>splunkexample-03.lan1.gov |

**Sub-control info**

**Test Output**

**New Acknowledgement**

System Selection: examplehost-03

Enter comments regarding reviewed controls and security exemptions

Acknowledgement Comment

Optional RT ticket number

Submitting as John Smith

**Current Acknowledgements**

| Time                | Comment   | Exemption Expires | ticketNum | Acknowledger |
|---------------------|---|-------------------|-----------|--------------|
| 2024-05-08 07:00:53 | Logging was interrupted due to a misconfiguration and has been fixed. Logs have started reaching Splunk again |                   | N/A       | John Smith   |

Sub-controls

Sub-control info

Test Output

Multi-machine entry

Sys Admin Acknowledgement

Submitted Acknowledgements

# Automated Cyber Baseline - Acknowledgments

Latest Scan of examplehost-03  
**2024-05-07 07:37:10**

► Please allow a minute for results to update

**Relaunch Scan**  
► more info?

### Breakdown of Control

Summary for examplehost-03

Control ID: HPC015

| Sub-Controls | Result                | Info   | Return Value   | Previous Return Value   |
|--------------|-----------------------|--|--|---|
| HPC015-01    | Acknowledged by Admin | Check that at least one log message was received each hour over the last 48H   | 43   | 42  |
| HPC015-02    | Pass                  | Check that at least one SSHD log has been received in the 10 days              | No known logins since 2024-04-24   | No SSHD logs  |
| HPC015-03    | Pass                  | List of splunk systems where logs are stored. Recorded for reporting purposes. | splunkexample-01.lan1.gov<br>splunkexample-02.lan1.gov<br>splunkexample-03.lan1.gov<br>splunkexample-04.lan1.gov | splunkexample-01.lan1.gov<br>splunkexample-02.lan1.gov<br>splunkexample-03.lan1.gov |

### New Acknowledgement

Response:

- ✓ Please Select and Option
- Passes
- Fails
- Needs More Review
- Exemption

Submit

Submitting as John Smith

### Current Acknowledgements

| Time                | Comment   | Exemption Expires | ticketNum | Acknowledger |
|---------------------|---|-------------------|-----------|--------------|
| 2024-05-08 07:00:53 | Logging was interrupted due to a misconfiguration and has been fixed. Logs have started reaching Splunk again |                   | N/A       | John Smith   |

**Security Admin Acknowledgement**

# Vulnerability Management – Multi-Host View

## Systems That Need Addressing

Issues that have less than 30 days to be addressed

| System ▾       | Critical ▾ | High ▾ | Medium ▾ |
|----------------|------------|--------|----------|
| examplehost-01 | 0          | 1      | 0        |
| examplehost-02 | 0          | 1      | 0        |
| examplehost-03 | 0          | 1      | 0        |
| examplehost-04 | 0          | 1      | 0        |
| examplehost-05 | 0          | 1      | 0        |
| examplehost-06 | 0          | 1      | 1        |
| examplehost-07 | 0          | 1      | 0        |
| examplehost-08 | 1          | 1      | 0        |
| examplehost-09 | 0          | 2      | 0        |
| examplehost-10 | 1          | 1      | 0        |

« Prev 1 2 3 4 5 Next »

## Overview of All Missing Patches

| System ▾       | On CISA KEV ▾ | Critical ▾ | High ▾ | Medium ▾ | Low ▾ |
|----------------|---------------|------------|--------|----------|-------|
| examplehost-03 | 0             | 1          | 6      | 2        | 0     |
| examplehost-07 | 0             | 1          | 6      | 2        | 0     |
| examplehost-11 | 0             | 1          | 6      | 2        | 0     |
| examplehost-12 | 0             | 1          | 6      | 2        | 0     |
| examplehost-13 | 0             | 1          | 6      | 2        | 0     |
| examplehost-16 | 0             | 1          | 6      | 2        | 0     |
| examplehost-17 | 0             | 1          | 6      | 2        | 0     |
| examplehost-20 | 0             | 1          | 6      | 2        | 0     |
| examplehost-21 | 0             | 1          | 6      | 2        | 0     |
| examplehost-23 | 0             | 1          | 6      | 2        | 0     |

« Prev 1 2 3 4 5 Next »

# Vulnerability Management – Multi-Host View



# Vulnerability Management – Dealing with Findings

Latest Scan of examplehost-01

**2024-05-07 06:06:19**

► Please allow a minute for results to update

Relaunch Scan

► more info?

## Needs Addressing

Issues with less than 30 days to address

| System ▾       | Plugin ▾                           | Plugin ID ▾ | On CISA KEV ▾ | Severity ▾ | First Seen ▾        | Patch Due By ▾      |
|----------------|------------------------------------|-------------|---------------|------------|---------------------|---------------------|
| examplehost-01 | RHEL 7 : tigervnc (RHSA-2024:2880) | 194622      | False         | high       | 2024-05-01 09:01:42 | 2024-05-31 09:01:42 |

Switch to all vulns

## Selected Vulnerabilities

Add "Needs Addressing" Clear selected vulns

Will need to be clicked for each page of the "Requires Deviation" panel if it has multiple pages

No Vulnerabilites Selected

## New Deviation Request

Please patch or request a deviation for all vulnerabilities that have exceeded patch timelines. For help on requesting a deviation, click "Help for Requesting a Deviation" below

► Help for Requesting a Deviation

Deviation Justification

Mitigations

Optional RT ticket number

Submit Undo

Submitting as John Smith

# Vulnerability Management – Dealing with Findings

The screenshot shows the Tenable vulnerability management interface. At the top, it displays the latest scan for 'examplehost-01' on 2024-05-07 at 06:06:19. A green 'Relaunch Scan' button is visible. Below this, a 'Needs Addressing' section shows a table of vulnerabilities. One vulnerability is highlighted: System 'examplehost-01', Plugin 'RHEL 7 : tigervnc (RHSA-2024:2080)', Plugin ID '194622', On CISA KEV 'False', Severity 'high', First Seen '2024-05-01 09:01:42', and Patch Due By '2024-05-31 09:01:42'. A 'Switch to all vulns' button is next to it. Below the table, the 'Selected Vulnerabilities' section shows 'No Vulnerabilities Selected' and buttons for 'Add "Needs Addressing"' and 'Clear selected vulns'. A 'New Deviation Request' form is also visible, with a 'Submit' button. Annotations with arrows point to various parts of the interface: 'Relaunch Scan' button, 'Needs Addressing' section, 'Switch to all vulns' button, 'Add "Needs Addressing"' button, 'New Deviation Request' form, and 'Submit' button.

Latest Scan of examplehost-01  
2024-05-07 06:06:19

► Please allow a minute for results to update

Needs Addressing  
Issues with less than 30 days to address

| System         | Plugin                             | Plugin ID | On CISA KEV | Severity | First Seen          | Patch Due By        |
|----------------|------------------------------------|-----------|-------------|----------|---------------------|---------------------|
| examplehost-01 | RHEL 7 : tigervnc (RHSA-2024:2080) | 194622    | False       | high     | 2024-05-01 09:01:42 | 2024-05-31 09:01:42 |

Switch to all vulns

Selected Vulnerabilities

Add "Needs Addressing" Clear selected vulns

No Vulnerabilities Selected

New Deviation Request

Submit Undo

Submitted as John Smith

Tenable interaction through Splunk

Select Vulnerabilities to get more info

Display all Findings or just those that need to be addressed within 30 days

Submitted Deviation Requests tracked below

Deviation Requests for Unpatchable Findings

- Will be reviewed by Security Admin
- Able to submit for multiple hosts

# Wrap Up

- LANL HPC has been able to create an effective infrastructure for gathering, monitoring, alerting on, and interacting with HPC system and security data
- This has allowed easier integrations with the human components of HPC
- Our Current Future Plans
  - Improved notifications for system administrators to enable more timely vulnerability management information
  - Integration with the fledging LANL vulnerability deviation request process
  - NIST 800-53 rev. 5 compliance in Dashboards
  - Monitoring containerized service solutions
  - STIG scanning integration
  - Investigation of AI support



# Thank You!

Questions?



Over 70 years at the  
forefront of supercomputing.