Getting Started with Red Hat Insights

Rob Williams & Will Nix
Management Business Unit
COMPLEXITY IS RISK

80%  
Percentage of commercial application outages caused by software failure and operational complexity

$336\text{k/hr}  
The median cost per hour of downtime for a production application for a large enterprise

$15\text{m/yr}  
Mean annualized cost of cybercrime defense and remediation for large US-based corporations

65%  
of CompTIA customers thought they were significantly behind in training and capabilities needed to manage their next generation infrastructure.
“...by 2018, 25% of the Global 2000 will have deployed an IT Operations Analytics platform (...) up from about 2% today.”

— WILL CAPPELLI, vice president & research analyst, Gartner
RED HAT INSIGHTS
Included with your Red Hat Enterprise Linux subscription

Assesses
customer’s Red Hat environments

Remediates
findings with prescriptive remediation steps or an Ansible playbook

Insights
rule contributions directly from Red Hat subject matter experts

Covers issues across availability, performance, stability and security
RED HAT INSIGHTS CAPABILITIES
RED HAT INSIGHTS
Now included with all Red Hat Enterprise Linux subscriptions

<table>
<thead>
<tr>
<th>Buy</th>
<th>Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat</td>
<td>Red Hat</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Insights</td>
</tr>
<tr>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VALUE OF EXPERIENCE

- Continuous identification of new risks driven by unique industry data
- Based on real-world results from millions of enterprise deployments

“85% of critical issues raised to Red Hat® support are already known to Red Hat or our partners.”

— RED HAT GLOBAL SUPPORT SERVICES
KEY RISKS DISCOVERED

Tailored resolution steps included for resolution

Performance issue
Network interface is not performing at maximum speed
Recommended action
Check cable, connections, and remote switch settings

Security risk detected
Privilege escalation
Recommended action
Apply mitigation and update the kernel

Availability
OpenShift operations fail if insufficient CPU or memory
Recommended action
Increase CPU and/or memory reservation

Stability
Filesystem has exceeded 95% capacity
Recommended action
Increase free space on the host.
Customer Stories

- Insights was able to immediately identify 10 issues on an Oracle RAC system that has been **plaguing a customer for 6 months**.
  - Oracle RAC systems are **EXPENSIVE**. Why not keep them running at **optimal** capacity?
- One prospect swore their 2,000 servers were up-to-date.
  - A demonstration of Red Hat Insights showed them that **400 of their servers were not up-to-date**, and therefore at **risk**.
How Insights Works
View results and alerts from Insights in either the Customer Portal or through the Satellite user interface.
REMEDIATION MADE SIMPLE

- Automatically tailored recommendations and remediation down to the per-host level
- Create and share maintenance plans to better coordinate responses within your team

“22% of disasters are caused by human error.”

– QUORUM DISASTER RECOVERY REPORT
MORE THAN JUST SECURITY

Red Hat Insights currently has over 600 rules—here is how they stack up across categories:

- Availability: 38.6%
- Security: 28.1%
- Stability: 21.7%
- Performance: 11.6%
WHAT IS RED HAT® INSIGHTS

- Proactive alerts and executive reporting
- Quick setup
- No added infrastructure cost
- SaaS
- Automated, validated, resolutions
- Tailored remediations
- Real-time risk assessment

SaaS
[root@host-10 ~]# insights-client --register

Automatic scheduling for Insights has been enabled.
Starting to collect Insights data for host-10.aws.company.com
Uploading Insights data.
Successfully uploaded report from host-10.aws.company.com to account 6216449.
[root@host-10 ~]#  

## High Risk Actions

<table>
<thead>
<tr>
<th>Rule</th>
<th>Added</th>
<th>Total Risk</th>
<th>Systems</th>
<th>Ansible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote privilege escalation/authentication bypass possible when a</td>
<td>6 months ago</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vulnerable Kubernetes API server is running (CVE-2018-10020105)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetworkManager DHCP script vulnerable to remote code execution</td>
<td>a year ago</td>
<td>89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(CVE-2018-1111)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote code execution vulnerability in NS5 via crafted base64 data</td>
<td>a year ago</td>
<td>93</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(CVE-2017-5461)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wpa_supplicant is vulnerable to man-in-the-middle attack via crafted</td>
<td>2 years ago</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA2 frames (CVE-2017-13077)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dnsmasq vulnerable to remote code execution via crafted DNS requests</td>
<td>2 years ago</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(CVE-2017-14491)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GETTING STARTED WITH INSIGHTS

ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?
You have Red Hat Insights at no additional cost:
https://cloud.redhat.com/insights

WOULD YOU LIKE TO LEARN MORE ABOUT RED HAT INSIGHTS?
For more info, visit: https://cloud.redhat.com
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHat