Incident Response Report

Project Title: SIEM-Based Simulated Incident Detection & Response
Analyst: Gautam Singh Patwal
Date: 16 July 2025
Tools Used: Splunk Free Trial (v9.4.1), Windows Event Logs, Sysmon, PerfMon logs

1. Executive Summary

During this simulated exercise, Splunk was used to ingest diverse Windows logs (System, Security, Sysmon, Performance Metrics). A series of suspicious activities were identified, triaged, and classified. A comprehensive incident response process was followed, including root cause analysis and suggested remediation.

2. Log Intake & Search Strategy

- Indexes Monitored:
  - winEventLog:System – OS-level events (e.g. EventCode=1014)
  - winEventLog:Security – Authentication & privilege changes
  - sysmon – Process execution, network behavior
  - main – Performance counters (bytes sent/received)

- Key Searches Executed:
  - index=winEventLog:System host="DESKTOP-8HOT83H"
  - index=sysmon host="DESKTOP-8HOT83H"
  - index=main or index=*

3. Alert & Activity Findings

A. Repeated System-Level Warnings (Event Codes 19 & 1014)
- Observed: Multiple entries within a short span
- Analysis: Possible DNS issues or malicious script behavior

B. Privilege Escalation Events (Security EventCodes 464, 4672, 4624)
- Observed: Sysmon logged 4 alerts
- Analysis: Potential unauthorized elevated access

C. Abnormal Performance Metrics
- Observed: High network traffic
- Analysis: Possible exfiltration or Command & Control activity

4. Incident Classification

Incident	Tactic (MITRE)	Severity	Status
Abnormal system logs	Reconnaissance/Initial Access	Medium	Closed (benign)
Privilege escalation	Credential Access / Persistence	High	Open (needs review)
Data exfiltration attempt	Exfiltration / C2	High	Open (under response)

5. Remediation Recommendations

1. System Warnings & Errors
- Whitelist benign DNS/registry traffic.
- Resolve network latency.

2. Privilege Escalation
- Review service accounts and admin roles.
- Use MFA.
- Eliminate local admin use.

3. Exfiltration Prevention
- Isolate affected host.
- Apply egress filtering.
- Enable session logs.

6. Lessons Learned

- Sysmon logs help identify process and account abuse.
- Monitoring performance metrics highlights abnormal data transfers.
- Alert tuning reduces false positives.

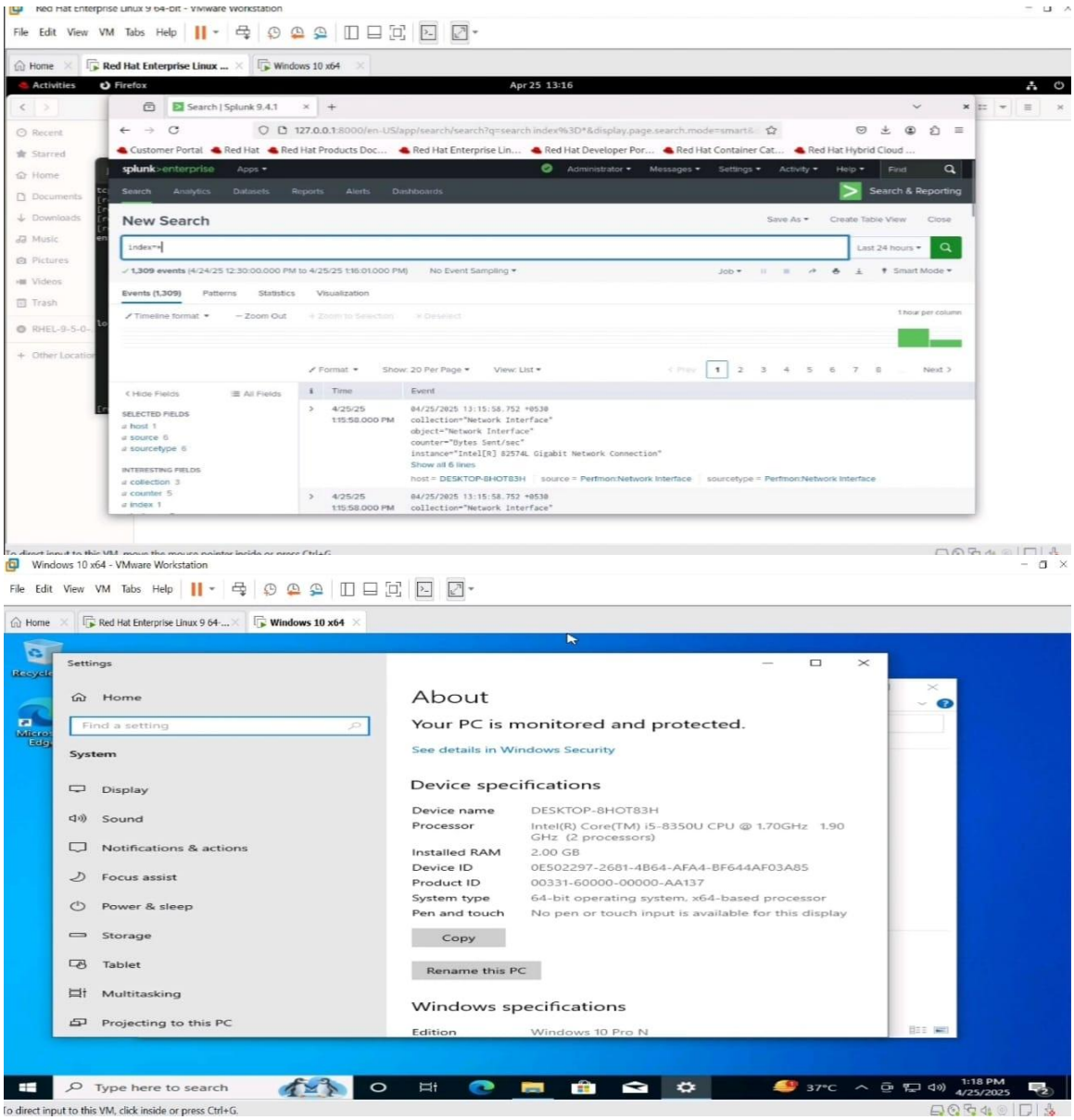
7. Conclusion

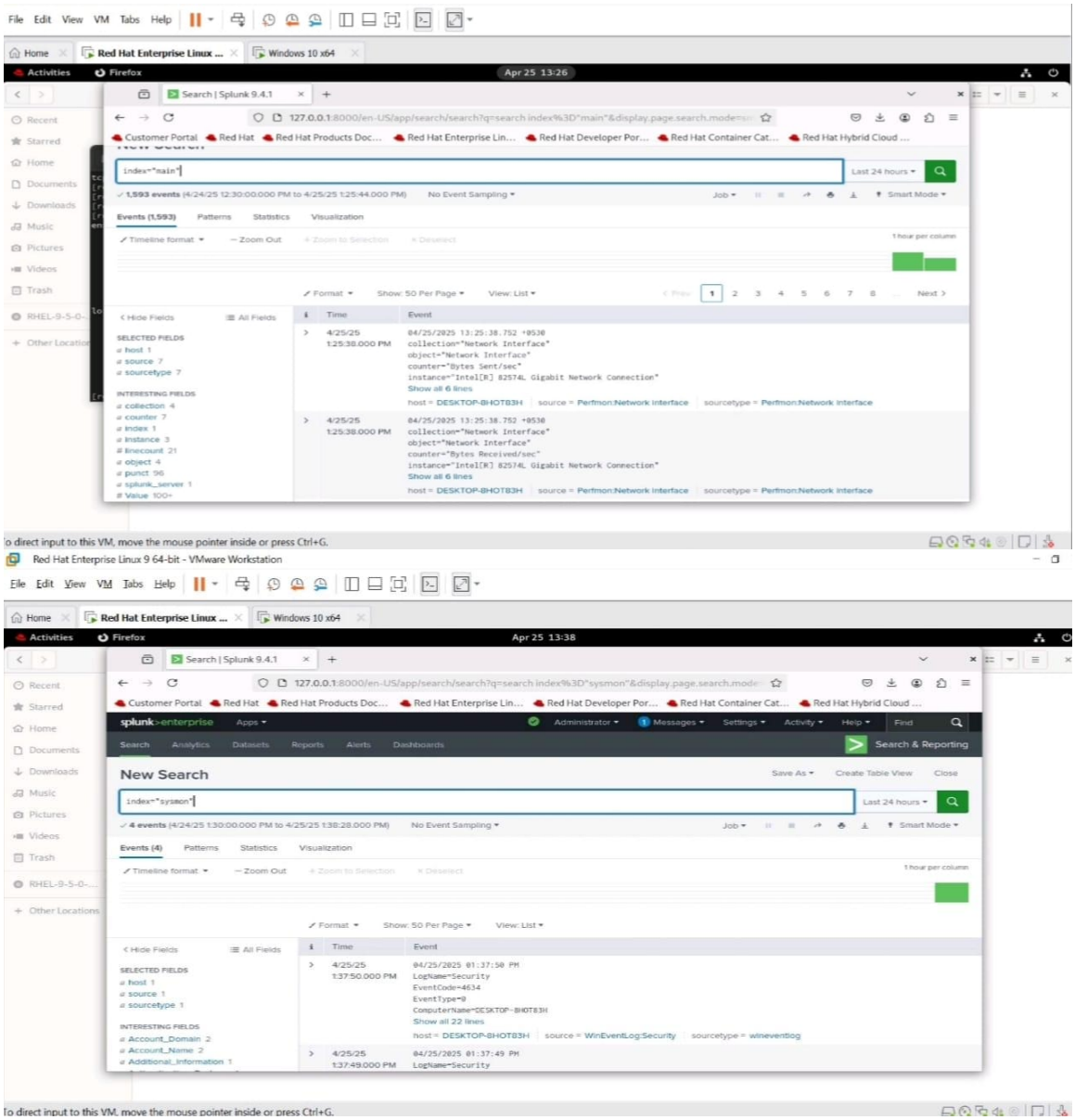
The simulated environment demonstrated the power of SIEM (Splunk + Sysmon) for real-time detection of reconnaissance, credential abuse, and data exfiltration techniques. Recommendations like privilege hardening and alert tuning improve defenses.

8. Appendices

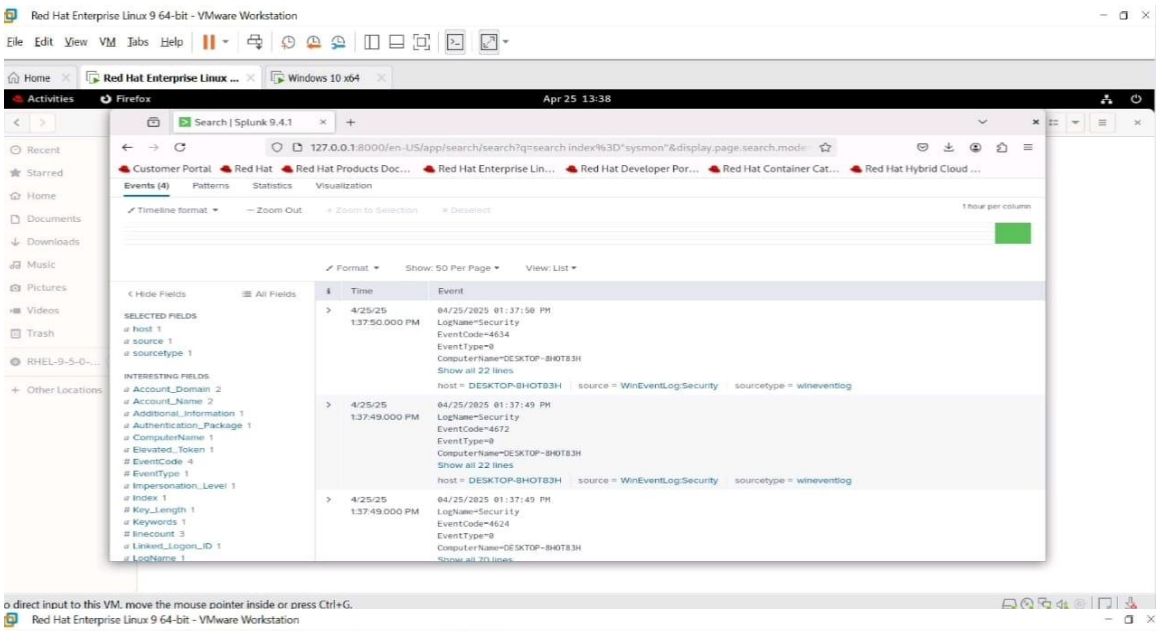
- A: Splunk search queries & screenshots
- B: Timeline of detected critical activities

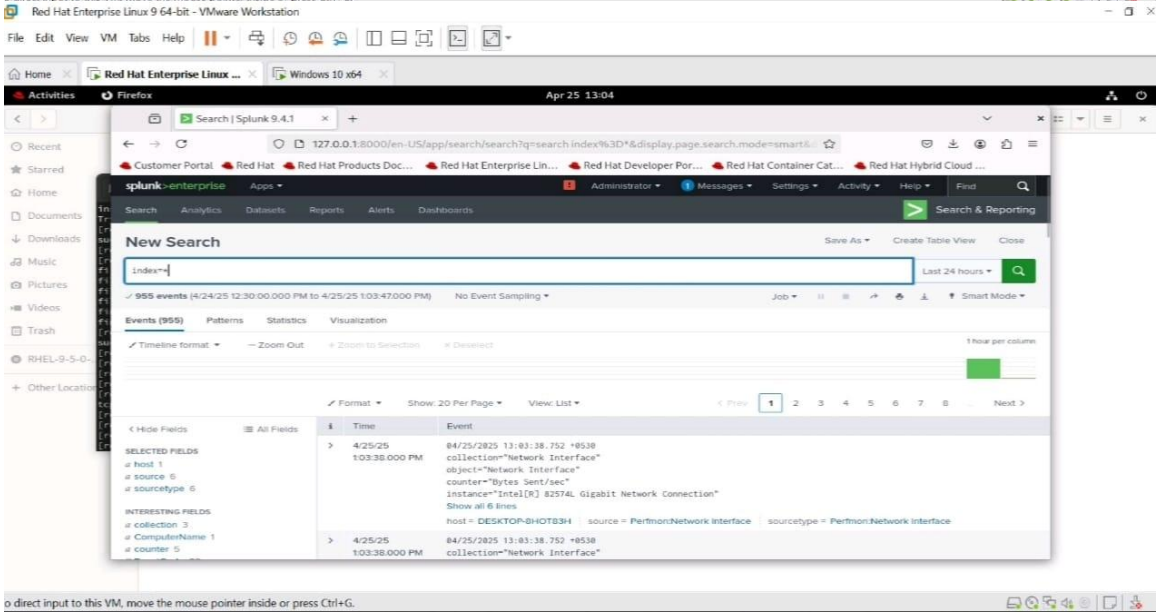
- C: IOC Summary
- D: Incident Response Runbook

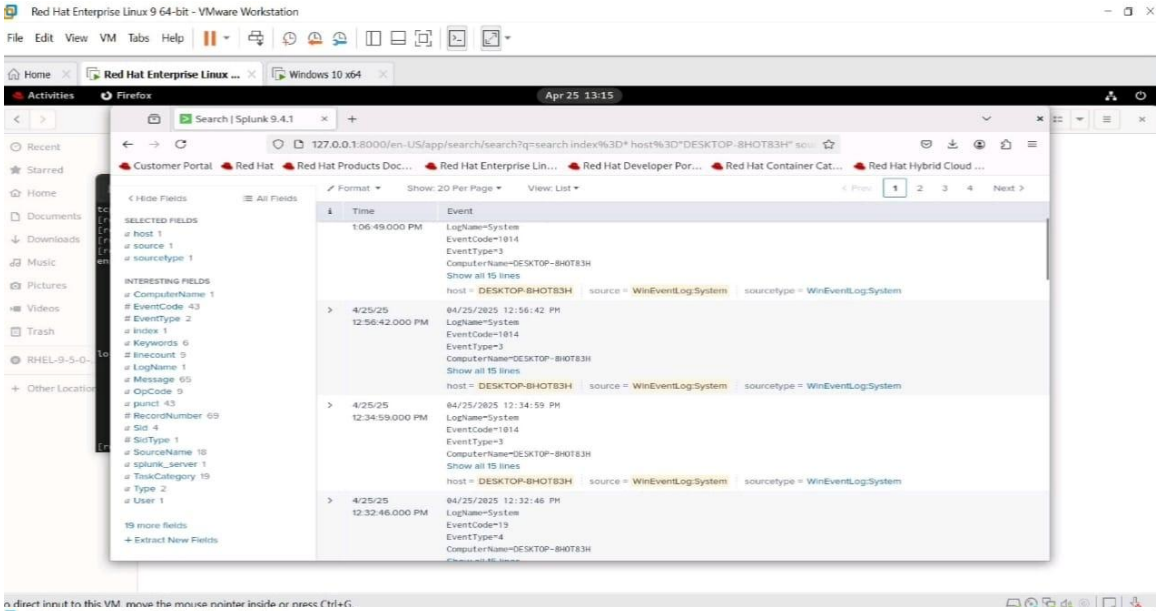


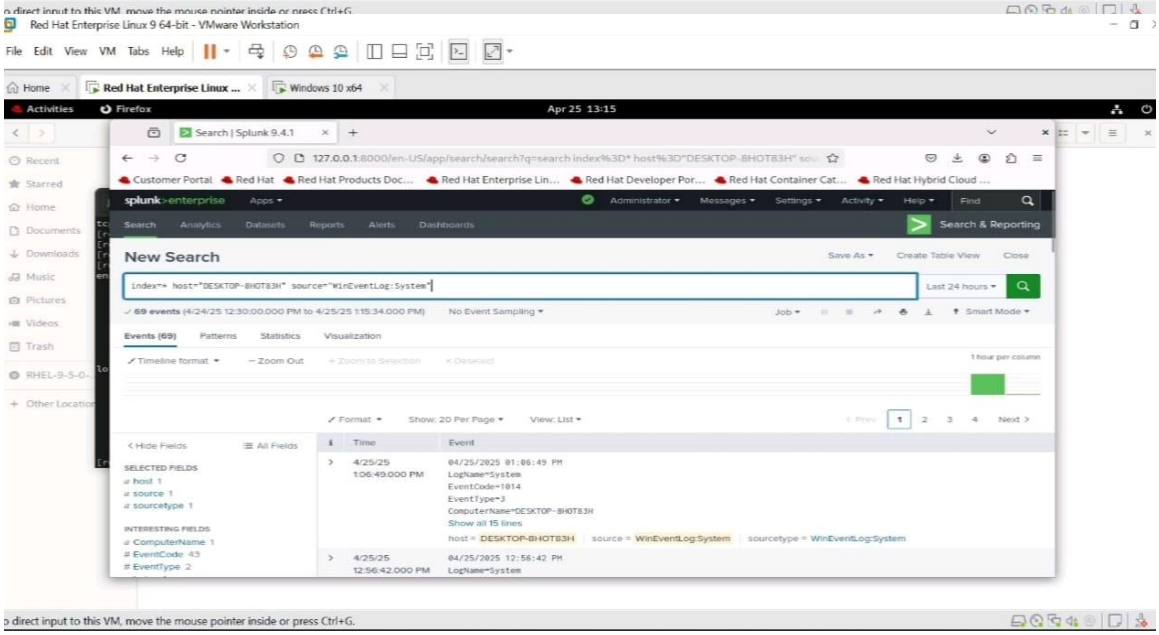

File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:26
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D"main"&display.page.search.mode=
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
index="main"
Last 24 hours
1,593 events (4/24/25 12:30:00.000 PM to 4/25/25 1:25:44.000 PM)
No Event Sampling
Job
Smart Mode
Events (1,593)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 50 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 7
sourcetype 7
INTERESTING FIELDS
collection 4
counter 7
index 1
instance 3
linecount 21
object 4
punct 96
splunk_server 1
Value 100+
4/25/25 1:25:38.000 PM
04/25/2025 13:25:38.752 +0530
collection="Network Interface"
object="Network Interface"
counter="Bytes Sent/sec"
instance="Intel[R] 82574L Gigabit Network Connection"
Show all 6 lines
host = DESKTOP-8HOT83H
source = Perfmon:Network Interface
sourcetype = Perfmon:Network Interface
4/25/25 1:25:38.000 PM
04/25/2025 13:25:38.752 +0530
collection="Network Interface"
object="Network Interface"
counter="Bytes Received/sec"
instance="Intel[R] 82574L Gigabit Network Connection"
Show all 6 lines
host = DESKTOP-8HOT83H
source = Perfmon:Network Interface
sourcetype = Perfmon:Network Interface
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
RHEL-9-5-0...
Other Locations
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

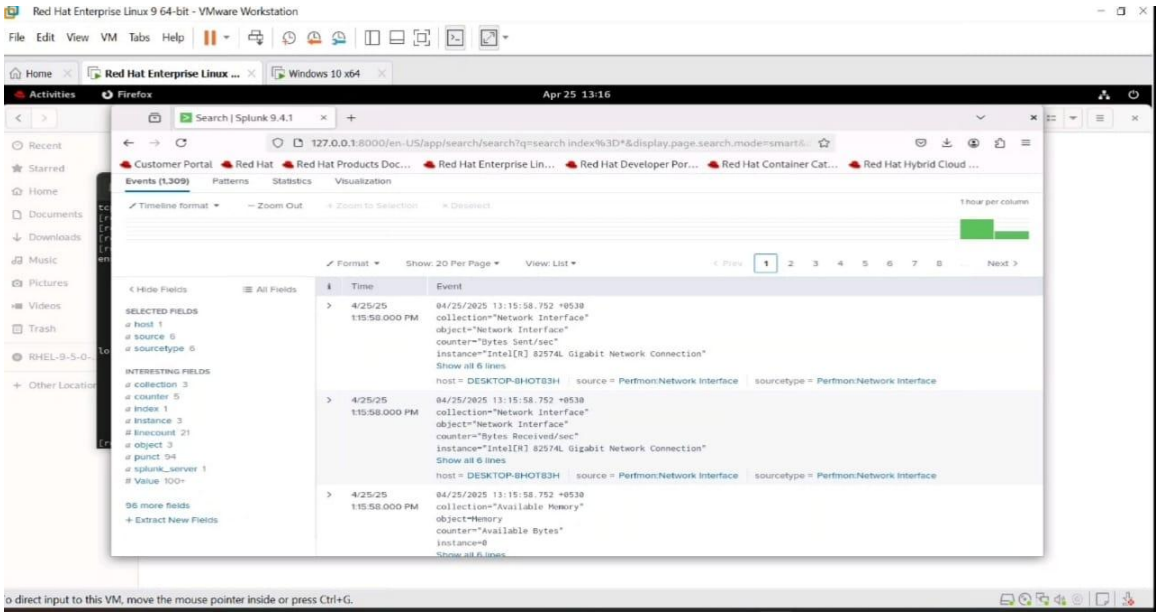
Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:38
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D"sysmon"&display.page.search.mode=
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="sysmon"
Last 24 hours
4 events (4/24/25 1:30:00.000 PM to 4/25/25 1:38:28.000 PM)
No Event Sampling
Job
Smart Mode
Events (4)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
Account_Domain 2
Account_Name 2
Additional_Information 1
4/25/25 1:37:50.000 PM
04/25/2025 01:37:50 PM
LogName=Security
EventCode=4634
EventType=0
ComputerName=DESKTOP-8HOT83H
Show all 22 lines
host = DESKTOP-8HOT83H
source = WinEventLog:Security
sourcetype = wineventlog
4/25/25 1:37:49.000 PM
04/25/2025 01:37:49 PM
LogName=Security
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
RHEL-9-5-0-...
Other Locations
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:38
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D"sysmon"&display.page.search.mode
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
Events (4)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
Account_Domain 2
Account_Name 2
AdditionalInformation 1
Authentication_Package 1
ComputerName 1
Elevated_Token 1
EventCode 4
EventType 1
Impersonation_Level 1
Index 1
Key_Length 1
Keywords 1
linecount 3
Linked_Logon_ID 1
LogName 1
4/25/25 1:37:50.000 PM
04/25/2025 01:37:50 PM
LogName=Security
EventCode=4634
EventType=0
ComputerName=DESKTOP-8HOT83H
Show all 22 lines
host = DESKTOP-8HOT83H source = WinEventLog:Security sourcetype = wineventlog
4/25/25 1:37:49.000 PM
04/25/2025 01:37:49 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=DESKTOP-8HOT83H
Show all 22 lines
host = DESKTOP-8HOT83H source = WinEventLog:Security sourcetype = wineventlog
4/25/25 1:37:49.000 PM
04/25/2025 01:37:49 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=DESKTOP-8HOT83H
Show all 70 lines
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:04
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D*&display.page.search.mode=smart&
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=*
Last 24 hours
955 events (4/24/25 12:30:00.000 PM to 4/25/25 1:03:47.000 PM)
No Event Sampling
Job
Smart Mode
Events (955)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1 2 3 4 5 6 7 8
Next
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 6
sourcetype 6
INTERESTING FIELDS
collection 3
ComputerName 1
counter 5
4/25/25 1:03:38.000 PM
04/25/2025 13:03:38.752 +0530
collection="Network Interface"
object="Network Interface"
counter="Bytes Sent/sec"
instance="Intel[R] 82574L Gigabit Network Connection"
Show all 6 lines
host = DESKTOP-8HOT83H source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface
4/25/25 1:03:38.000 PM
04/25/2025 13:03:38.752 +0530
collection="Network Interface"
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:15
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D* host%3D"DESKTOP-8HOT83H"
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
EventCode 43
EventType 2
Index 1
Keywords 6
linecount 9
LogName 1
Message 65
OpCode 9
punct 43
RecordNumber 69
Sid 4
SidType 1
SourceName 18
splunk_server 1
TaskCategory 19
Type 2
User 1
19 more fields
+ Extract New Fields
4/25/25 1:06:49.000 PM
LogName=System
EventCode=1014
EventType=3
ComputerName=DESKTOP-8HOT83H
Show all 15 lines
host = DESKTOP-8HOT83H source = WinEventLog:System sourcetype = WinEventLog:System
4/25/25 12:56:42.000 PM
04/25/2025 12:56:42 PM
LogName=System
EventCode=1014
EventType=3
ComputerName=DESKTOP-8HOT83H
Show all 15 lines
host = DESKTOP-8HOT83H source = WinEventLog:System sourcetype = WinEventLog:System
4/25/25 12:34:59.000 PM
04/25/2025 12:34:59 PM
LogName=System
EventCode=1014
EventType=3
ComputerName=DESKTOP-8HOT83H
Show all 15 lines
host = DESKTOP-8HOT83H source = WinEventLog:System sourcetype = WinEventLog:System
4/25/25 12:32:46.000 PM
04/25/2025 12:32:46 PM
LogName=System
EventCode=19
EventType=4
ComputerName=DESKTOP-8HOT83H
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:15
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D* host%3D"DESKTOP-8HOT83H"
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* host="DESKTOP-8HOT83H" source="WinEventLog:System"
Last 24 hours
69 events (4/24/25 12:30:00.000 PM to 4/25/25 1:15:34.000 PM)
No Event Sampling
Job
Smart Mode
Events (69)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
EventCode 43
EventType 2
4/25/25 1:06:49.000 PM
04/25/2025 01:06:49 PM
LogName=System
EventCode=1014
EventType=3
ComputerName=DESKTOP-8HOT83H
Show all 15 lines
host = DESKTOP-8HOT83H source = WinEventLog:System sourcetype = WinEventLog:System
4/25/25 12:56:42.000 PM
04/25/2025 12:56:42 PM
LogName=System
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Red Hat Enterprise Linux ...
Windows 10 x64
Activities
Firefox
Apr 25 13:16
Search | Splunk 9.4.1
127.0.0.1:8000/en-US/app/search/search?q=search index%3D*&display.page.search.mode=smart&
Customer Portal
Red Hat
Red Hat Products Doc...
Red Hat Enterprise Lin...
Red Hat Developer Por...
Red Hat Container Cat...
Red Hat Hybrid Cloud ...
Events (1,309)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next >
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 6
sourcetype 6
INTERESTING FIELDS
collection 3
counter 5
index 1
instance 3
linecount 21
object 3
punct 94
splunk_server 1
Value 100+
96 more fields
+ Extract New Fields
Time
Event
4/25/25 1:15:58.000 PM
04/25/2025 13:15:58.752 +0530
collection="Network Interface"
object="Network Interface"
counter="Bytes Sent/sec"
instance="Intel[R] 82574L Gigabit Network Connection"
Show all 6 lines
host = DESKTOP-8HOT83H
source = Perfmon:Network Interface
sourcetype = Perfmon:Network Interface
4/25/25 1:15:58.000 PM
04/25/2025 13:15:58.752 +0530
collection="Network Interface"
object="Network Interface"
counter="Bytes Received/sec"
instance="Intel[R] 82574L Gigabit Network Connection"
Show all 6 lines
host = DESKTOP-8HOT83H
source = Perfmon:Network Interface
sourcetype = Perfmon:Network Interface
4/25/25 1:15:58.000 PM
04/25/2025 13:15:58.752 +0530
collection="Available Memory"
object=Memory
counter="Available Bytes"
instance=0
Show all 6 lines
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
RHEL-9-5-0...
Other Locations
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.