

### Alert 1 - Ransomware behavior detected on bob's system

[illegible]

Future Interns Cyber Security | x | Cyber Security Task 2 – Future | x | Search | Splunk 10.0.x | Tshiamo Mantswe - Incident R | x

< Prev 1 2 3 Next >

i	Time	Event																																												
>	7/3/25 7:57:14.000 AM	2025-07-03 07:57:14   user=david   ip=10.0.0.5   action=file accessed host = DESKTOP-QC8GMS3   source = SOC_Task2_Sample_Logs.txt   sourcetype = sample logs																																												
v	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature  Event Actions v																																												
		<table border="1"> <thead> <tr> <th>Type</th> <th><input checked="" type="checkbox"/> Field</th> <th>Value</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td rowspan="3">Selected</td> <td><input checked="" type="checkbox"/> host v</td> <td>DESKTOP-QC8GMS3</td> <td>v</td> </tr> <tr> <td><input checked="" type="checkbox"/> source v</td> <td>SOC_Task2_Sample_Logs.txt</td> <td>v</td> </tr> <tr> <td><input checked="" type="checkbox"/> sourcetype v</td> <td>sample logs</td> <td>v</td> </tr> <tr> <td rowspan="4">Event</td> <td><input type="checkbox"/> action v</td> <td>malware detected</td> <td>v</td> </tr> <tr> <td><input type="checkbox"/> ip v</td> <td>10.0.0.5</td> <td>v</td> </tr> <tr> <td><input type="checkbox"/> threat v</td> <td>Rootkit</td> <td>v</td> </tr> <tr> <td><input type="checkbox"/> user v</td> <td>eve</td> <td>v</td> </tr> <tr> <td>Time ⚙</td> <td>_time v</td> <td>2025-07-03T07:51:14.000+02:00</td> <td></td> </tr> <tr> <td rowspan="4">Default</td> <td><input type="checkbox"/> index v</td> <td>main</td> <td>v</td> </tr> <tr> <td><input type="checkbox"/> linecount v</td> <td>1</td> <td>v</td> </tr> <tr> <td><input type="checkbox"/> punct v</td> <td>--:::_==_=_=_=_=_=_=_</td> <td>v</td> </tr> <tr> <td><input type="checkbox"/> splunk_server v</td> <td>DESKTOP-QC8GMS3</td> <td>v</td> </tr> </tbody> </table>	Type	<input checked="" type="checkbox"/> Field	Value	Actions	Selected	<input checked="" type="checkbox"/> host v	DESKTOP-QC8GMS3	v	<input checked="" type="checkbox"/> source v	SOC_Task2_Sample_Logs.txt	v	<input checked="" type="checkbox"/> sourcetype v	sample logs	v	Event	<input type="checkbox"/> action v	malware detected	v	<input type="checkbox"/> ip v	10.0.0.5	v	<input type="checkbox"/> threat v	Rootkit	v	<input type="checkbox"/> user v	eve	v	Time ⚙	_time v	2025-07-03T07:51:14.000+02:00		Default	<input type="checkbox"/> index v	main	v	<input type="checkbox"/> linecount v	1	v	<input type="checkbox"/> punct v	--:::_==_=_=_=_=_=_=_	v	<input type="checkbox"/> splunk_server v	DESKTOP-QC8GMS3	v
Type	<input checked="" type="checkbox"/> Field	Value	Actions																																											
Selected	<input checked="" type="checkbox"/> host v	DESKTOP-QC8GMS3	v																																											
	<input checked="" type="checkbox"/> source v	SOC_Task2_Sample_Logs.txt	v																																											
	<input checked="" type="checkbox"/> sourcetype v	sample logs	v																																											
Event	<input type="checkbox"/> action v	malware detected	v																																											
	<input type="checkbox"/> ip v	10.0.0.5	v																																											
	<input type="checkbox"/> threat v	Rootkit	v																																											
	<input type="checkbox"/> user v	eve	v																																											
Time ⚙	_time v	2025-07-03T07:51:14.000+02:00																																												
Default	<input type="checkbox"/> index v	main	v																																											
	<input type="checkbox"/> linecount v	1	v																																											
	<input type="checkbox"/> punct v	--:::_==_=_=_=_=_=_=_	v																																											
	<input type="checkbox"/> splunk_server v	DESKTOP-QC8GMS3	v																																											
>	7/3/25 7:46:14.000 AM	2025-07-03 07:46:14   user=bob   ip=10.0.0.5   action=login success host = DESKTOP-QC8GMS3   source = SOC_Task2_Sample_Logs.txt   sourcetype = sample logs																																												
>	7/3/25	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected																																												

Activate Windows  
Go to Settings to activate Windows.

### Alert 3 - Trojan detected on charlie's system

## Splunk dashboard