Bing chat: 24/30

1. Collects data on network hosts that are not managed by a Cortex XDR agent.
2. /var/log/traps/
3. For Windows, Cortex XDR supports only CVEs related to the operating system.
4. DevTools
5. Explore App
6. Endpoints > Device Control Violations
7. Response > Action Center > Scripts Library
8. Key Artifacts
9. Merged incident takes the target incident assignee
10. Cytool proxy query
11. /opt/traps/bin/
12. 250
13. Analytics alerts
14. 1- Run cytool runtime stop \ start 2- If the issue is reproducible then collect full memory dump of cyveraservice.exe 3- Collect and investigate process monitor traces
15. Alert Grouping Status
16. WildFire
17. Download the image from Cortex XDR > Generate Token > Deploy the image on the supported platform > Access Broker VM WebUI to complete the configuration > Perform the registration using the token
18. Behavioral Indicator of Compromise
19. Navigate to Endpoints > Policy management > Profiles > Windows > select a Malware profile > Portable Executable and DLL Examination, add to Files and Folders Allow List.
20. Prevent future matching Alerts from appearing in the Cortex XDR Console / Remove matching Alerts from existing Incidents if the rule is applied to historic results
21. <https://status.paloaltonetworks.com>
22. cytool proxy query
23. Shift + Right-Click
24. Depending on the exception type, it enables bypassing or disabling Cortex agent modules through exemptions either globally or by a specifically assigned policy.
25. 10 minutes
26. Update ca
27. 300 seconds
28. PMD
29. Go to Cloud Identity Agent console then select File ->Debug
30. %ProgramData%\Cyvera\Logs
31. Bundle ID and Path
32. cytool log export
33. Run the command cytool log collect
34. —com.apple.systemuiserver
35. msiexec /i c:\install\cortexxdr.msi proxy\_list=”10.0.1.32:8888;10.0.1.33:8888”