

Daily Update: July 31

Here are the main updates of the CISO Workplace:

CIM Updates:

In Alert Table View, added "Show More", "Show Less", and "Copy to Clipboard"

The screenshot displays the 'Alert Summary' window in a dark-themed interface. At the top, the title 'Alert Summary' is centered, with the subtitle 'The Summary of your Alert.' below it. A navigation bar contains five tabs: 'Summary', 'Investigation Guide', 'Table View' (which is selected and underlined), 'Raw File', and 'Timeline'. Below the tabs, there is a 'Filter by ...' input field and a refresh icon. The main content area is a table with two columns: 'Title' and 'Value'. The table contains four rows of data. The second row, which is highlighted in blue, contains a description of a security rule. This row has a red box around a document icon, another red box around the text 'SHOW MORE', and a third red box around the text 'SHOW LESS'. The other rows contain technical details like URLs, process IDs, and rule producers.

Title	Value
fields.kibana.alert.url-0	https://cytech-workplace.kb.us-east-1.aws.found.io:9243/s/cytech_developmentoperations/app/security/alerts/redirect/ea52bf11594c5cf51e88e1103fbb5...
fields.kibana.alert.rule.description-0	Identifies suspicious usage of unshare to manipulate system namespaces. Unshare can be utilized to escalate privileges or escape container security boundaries. Threat actors have utilized this binary to allow themselves to escape to the host and access other resources or escalate privileges.
fields.process.pid-0	6537
fields.kibana.alert.rule.producer-0	siem

This can also be seen in the Timeline Table View:

Alert Summary

The Summary of your Alert.

Timeline / End Point File Event

TABLE VIEW

RAW FILE

Filter by ...



Title

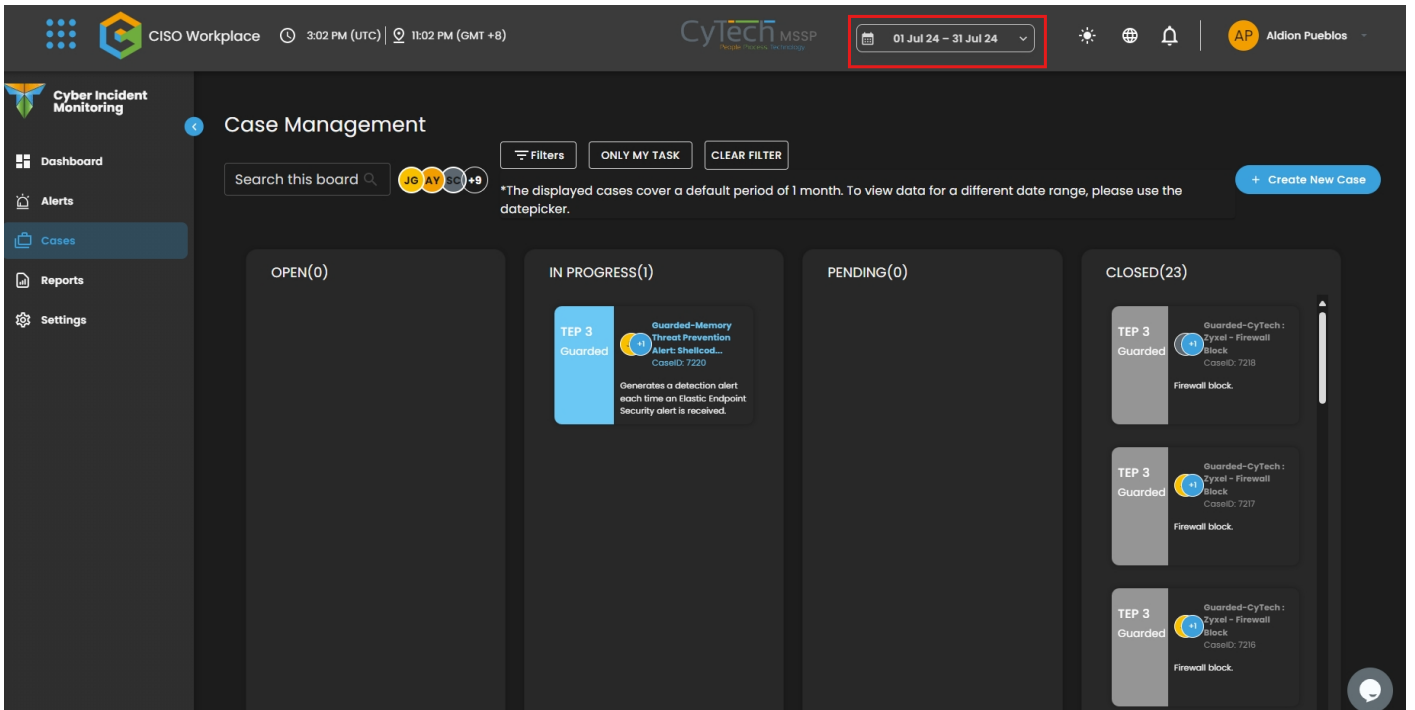
Value

fields.process.parent.command_line-0

```
/home/kylinii/BurpSuitePro/jre/bin/java -splash:/home/kylinii/BurpSuitePro/.install4j/s_sl5vaz.png --add-opens java.base/java.lang=ALL-UNNAMED --add-opens java.base/javax.crypto=ALL-UNNAMED --add-opens java.desktop/javax.swing=ALL-UNNAMED --add-opens java.desktop/java.awt.color=ALL-UNNAMED --add-opens jdk.crypto.cryptoki/sun.security.pkcs11=ALL-UNNAMED -XX:MaxRAMPercentage=50 -classpath /home/kylinii/BurpSuitePro/.install4j/i4jruntime.jar:/home/kylinii/BurpSuitePro/.install4j/launcherccf7dac9.jar:/home/kylinii/BurpSuitePro/burpsuite_pro.jar install4j.burp.StartBurp
```

SHOW LESS

Removed the Global Date Picker. It will only be displayed in Alerts and Cases.



VPT Updates:

Spanish Translation



VA/VM Updates:

Spanish Translation

