

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 with the 'Table View' tab selected. The table lists alert details with columns for 'Title' and 'Value'. The 'fields.kibana.alert.url-0' row shows a long URL. The 'fields.kibana.alert.rule.description-0' row shows a detailed description of a security rule, with 'SHOW MORE' and 'SHOW LESS' buttons. The 'fields.process.pid-0' row shows the value '6537'. The 'fields.kibana.alert.rule.producer-0' row shows the value 'siem'.

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

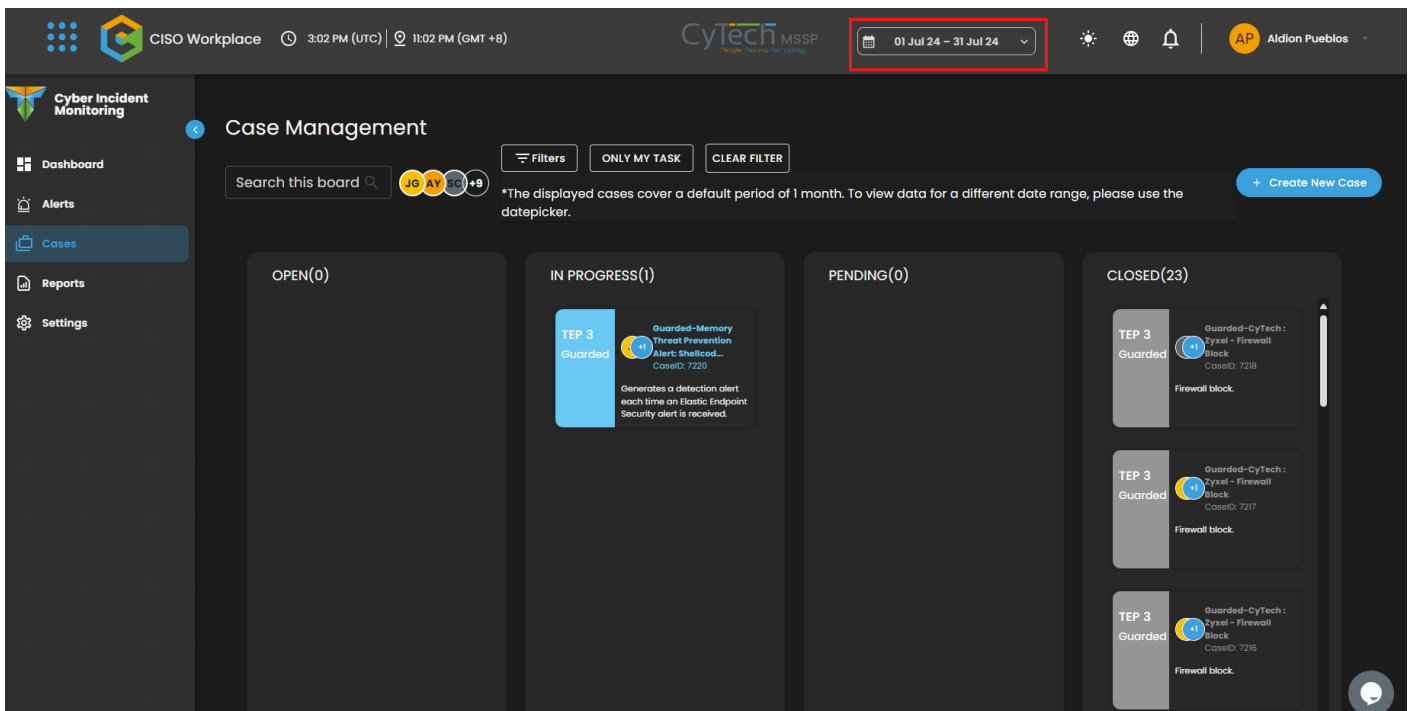
Value

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

