

Daily Update: July 23

Here are the main updates of the CISO Workplace:

New Module: **Virtual Penetration Testing**

SOAR Improvements

- Display all actions of rule

Control Panel

Alerts Tagging

Alert Rules

Tools

Alert Rules

Alerts

Rule Name:

Malware - Detected - Elastic Endgame [cytech_developmentoperations]

Active

About:

Elastic Endgame detected Malware. Click the Elastic Endgame icon in the event.module column or the link in the rule.reference column for additional information.

Severity:

Critical

Risk Score:

99

Tags:

Data Source: Elastic Endgame

Action

Perform the actions when these rules are triggered.

Search

Q

+ New Action

Malware

Summary Alert

- Display all actions of alert tag

Control Panel

Alerts Tagging

Alert Rules

Tools

Alert Tagging

Organize and manage your Alerts with Custom Tags

Search

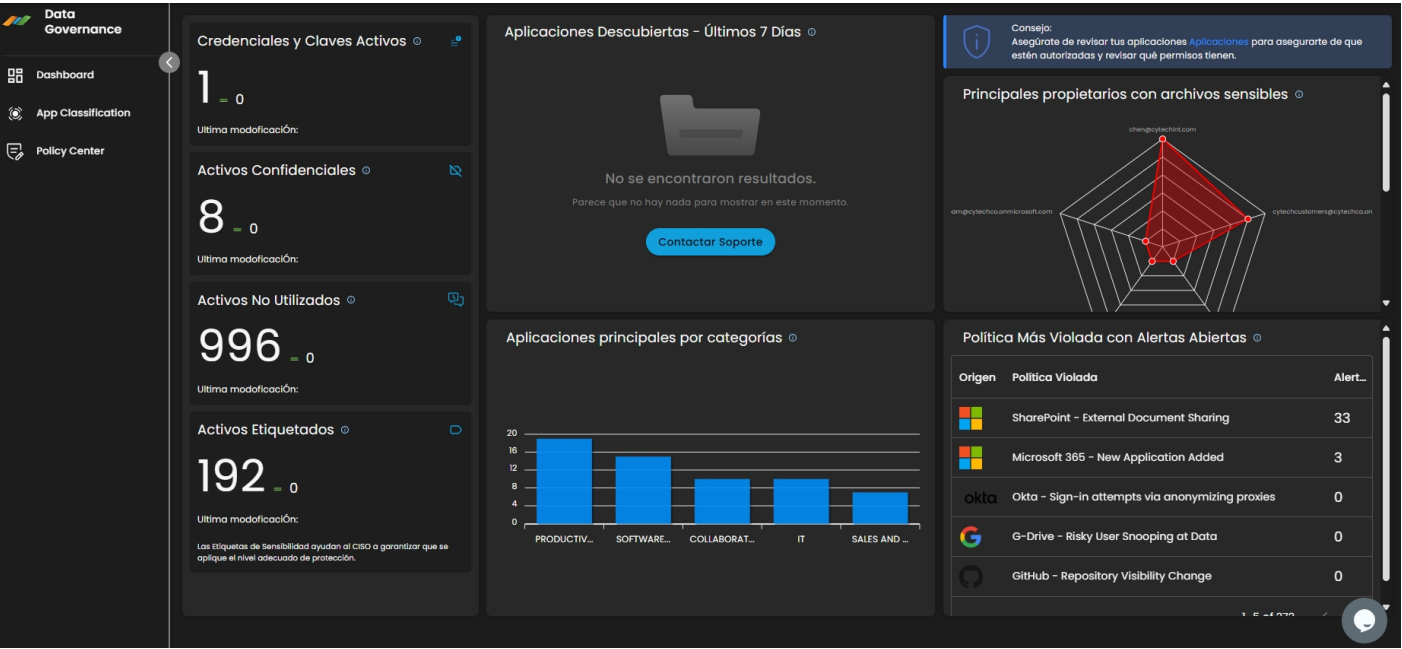
Q

Tag	Actions
CVE	+ Add Action
Continuous Monitoring	+ Add Action
Data Source: APM	+ Add Action
Data Source: AWS	+ Add Action
Data Source: AWS CloudWatch	+ Add Action
Data Source: AWS Cloudtrail	+ Add Action
Data Source: AWS EC2	+ Add Action
Data Source: AWS IAM	+ Add Action
Data Source: AWS KMS	+ Add Action
Data Source: AWS Lambda	+ Add Action

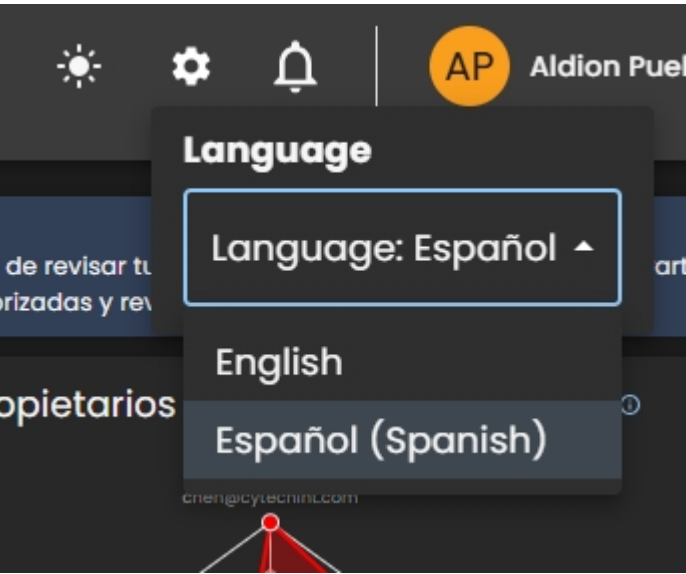
1-10 of 106 < >

Data Governance Improvement

- Initial Spanish Translation



Change in Language Select Menu



Bug Fixes:

- SOAR Bug Fixes
- Phishing Simulation Module Bug Fixes
- Risk Management Bug Fixes

