Legislative Cybersecurity Summary October 2024

KLOIS

CISA External Vulnerabilities

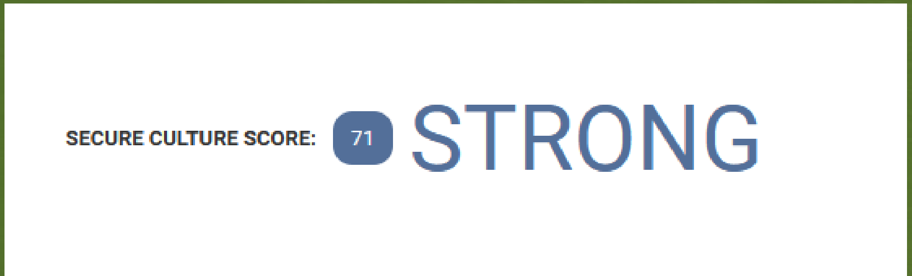
- Increased from 12 to 14
- Changes related to environmental maintenance, Exchange Online migration, and are expected to recede following decommissioning of obsolete equipment

Security and Operations Center Statistics

- In the past 10 days there have been:
  - 438,925,657 events analyzed
  - 89,854,760 events categorized as interesting
  - 12 investigations
  - 12 escalated alerts
- Benchmark risk score is down 0.1%
- Unresolved risks are down 1.2%
- 52 ticketed incidents have been investigated, remediated, and closed in the past 30 days
- 223 healthy scanning agents are deployed
- Agent scans for the week ending 10/27/24:
  - 404 new risks
  - 742 mitigated risks

*Note: This is the first time mitigated risks have been higher than new risks

Managed Security Awareness



SECURE CULTURE SCORE: 71 STRONG

- Awareness training statistics
  - 31% Session completion percentage
  - 93% average quiz score
  - 1% phishing simulation click rate
  - 30% remediation completion rate
- Edward Penner, Nathan Grey, and Luke Drury from KLRD are the current points leaders with 1,750 points each
- A special congratulations to Speaker Hawkins for earning 1,115 points month-to-date

Data Loss Prevention (DLP)

DLP allows Legislative IT to identify, monitor, and protect sensitive information across the Microsoft 365 Landscape.

DLP provides reports regarding unencrypted sensitive information sent or received via message, chat, attachment, etc., or uploaded into the Legislative Microsoft 365 tenant without proper classification and/or encryption.

- 57 DLP activities have occurred since activation
  - 43 occurred via Exchange
  - 14 occurred via file sharing/upload
- Improperly classified and/or secured sensitive information discovered included PII, credit card numbers, bank account numbers, and social security numbers.
- These activities pose the RISK of violating laws such as the U.S. Patriot Act, U.S. State Social Security Number Confidentiality Laws, and U.S. State Breach Notification laws

It is important to check all attachments for sensitive information before sending to ensure the communication can be properly encrypted and classified.

Ongoing Projects

- Microsoft Defender migration
- Infrastructure planning and upgrades
- Image and CIS Benchmark settings deployment
- Creation of administrative units and role-based access controls to facilitate the principle of least privilege and properly segment Legislative departments' environments
- Sensitivity label creation
- DLP tweaking
- Insider Risk Management activation

Questions?