

Ottawa Area ISD CSOC Overview: 2026 Q2

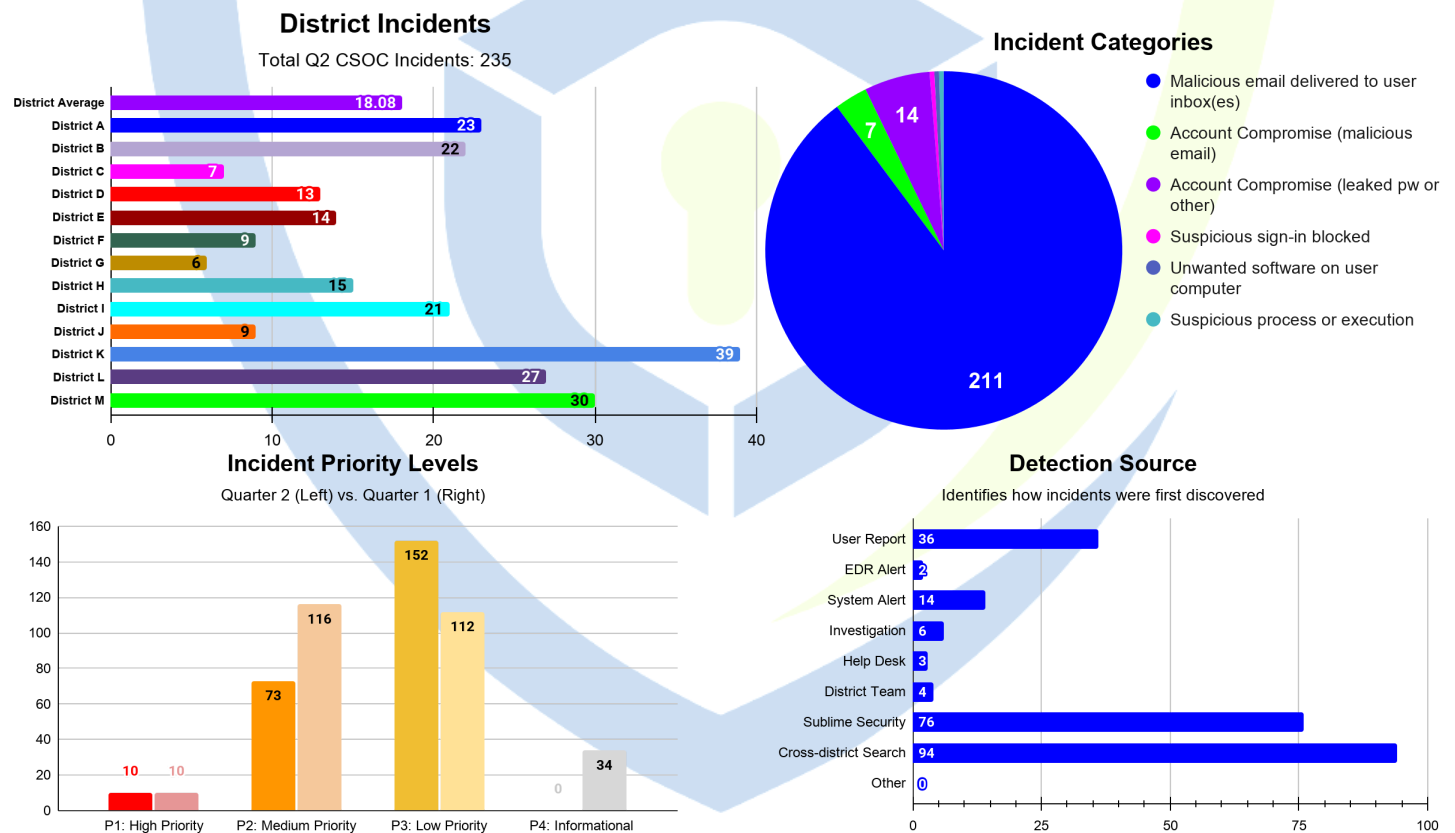
Prepared by the Ottawa Area Cybersecurity Operations Center | cybersecurity@oaisd.org

CSOC Updates, Threat Trends, & More:

Highlights from activity across all 13 CSOC-supported districts

- **Malicious email remained the primary threat vector.** Trusted senders and compromised accounts were used more frequently than suspicious domains, reinforcing that sender reputation alone is not a reliable indicator of legitimacy.
- **eCard phishing campaigns increased significantly.** Multiple account compromises highlighted the effectiveness of invitations and similar lures that capitalize on recipients' fear of missing out.
- The CSOC observed an **increase in phishing emails that delivered remote management software**, allowing attackers to access sensitive information and establish persistent access to compromised devices.
- **Social engineering tactics shifted toward curiosity.** While financial themes remained common, the CSOC observed more campaigns using invitations, shared documents, voicemail notifications, and similar unexpected messages to drive user engagement.
- **No new Priority 4 incidents were recorded during the quarter.** Investigation efforts remained focused on actionable security events while the CSOC continued expanding its internal detection capabilities, data analysis, and automation. These ongoing investments have **enabled the team to dedicate more time to strengthening security operations** and less time to coordinating infrastructure changes.

Incident Overview:



At a Glance

235 incidents across
13 districts

93% of total CSOC
incidents originated
from malicious emails

Incidents increasingly
contained at
lower severity

Cross-district searches
drove most incident
detections

Incident Response Effort and Efficiency

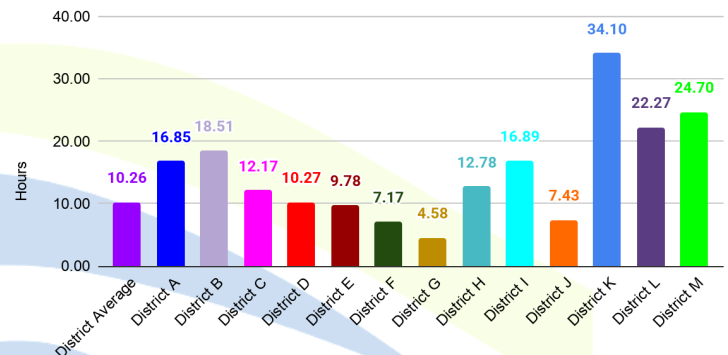
Estimates include **dedicated incident response time** and do not reflect broader CSOC cybersecurity work.

Total CSOC time
=
(Discovery Effort x 1)
+
(ALL District Impact Efforts)

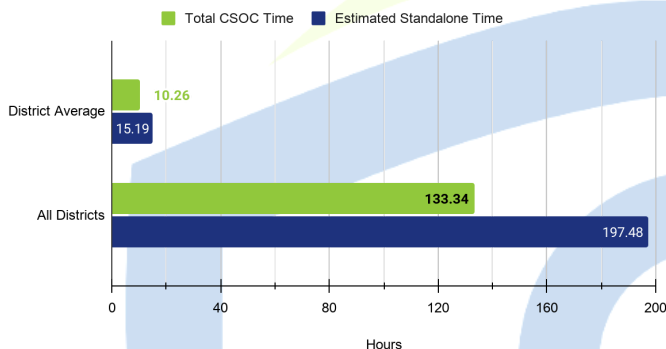
Estimated standalone time
=
(Discovery Effort x ALL)
+
(ALL District Impact Efforts)

CSOC Time Spent By District

Total Q2 CSOC Time: 129.34 hours



Q1 CSOC Time Comparison



CSOC Tasks NOT Included in Data:

Investigating false positives, alert tuning and detection rule refinement, infrastructure improvements, automation and script development or maintenance, threat hunting, vendor research, managing quarantines and email hygiene actions, environment investigations and security audits, phishing simulations and trainings, report development and metrics analysis, playbook updates and standardization, process and internal documentation, district communication, guidance, and follow-ups, etc...

Link Clicks

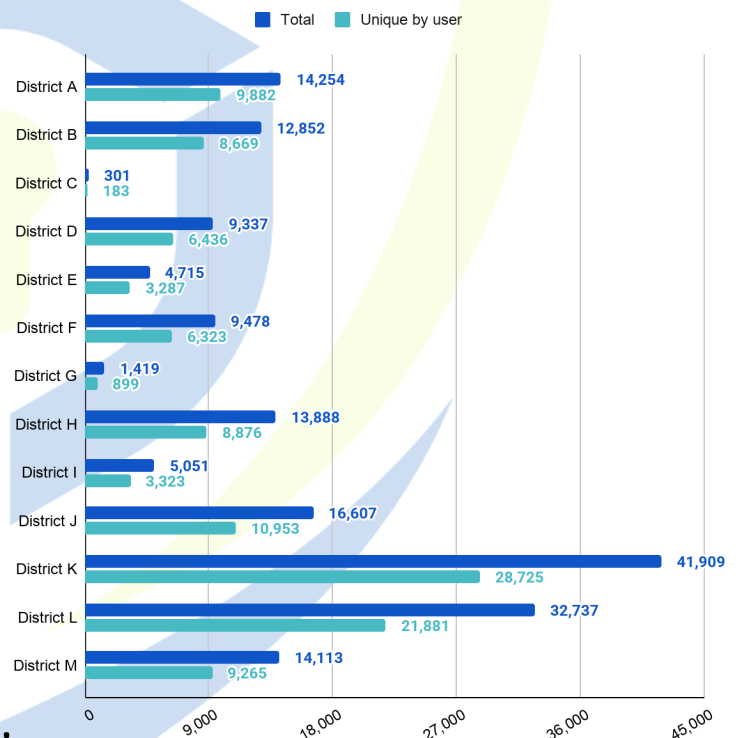
Data includes link click events between 6/1/2026 and 6/30/2026.

The CSOC now tracks the number of link clicks and the time it takes users to interact with links in emails. These metrics help establish user behavior baselines, identify trends by district, and improve future detection, response, and security awareness efforts.

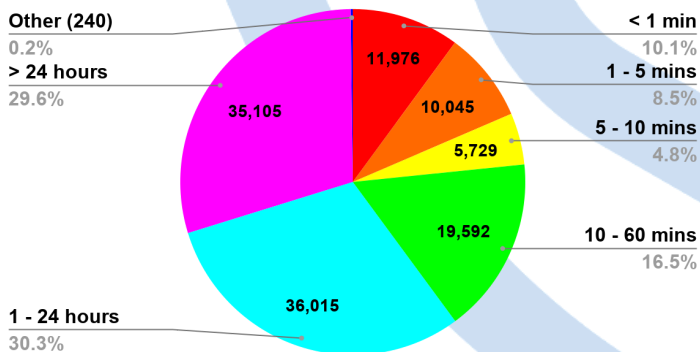
Note: Data displays *all* link clicks, not only malicious clicks.
Data captured in Google Workspace only.

Total Link Clicks

Total Link Clicks: 176,661 | Unique User Clicks per Email: 118,702



Time Until Link Clicks



"Other" accounts for emails where clicks happened before the email entered the delivery pipeline

CSOC Tips, Resources, & Forecast:

- 📖 **2026 Q2 CSOC Threat Report**
- Stay informed with the latest CSOC updates through our **new website** and subscribe to our blog for security news, threat insights, and announcements: <https://oaisd.org/csoc>
- Tech staff resources:** 📖 Google Workspace Phishing Remediation 📖 Site Takedown Resources
📖 Google Workspace User Compromise Remediation
- 📄 **Quarantine Rules Efficacy Report: 2026-06-01 - 2026-07-01.pdf**
- 📄 **Sublime Attack Insights: 2026-04-02 - 2026-07-01.pdf**