Ottawa Area ISD Technology Services

Ottawa Area ISD CSOC
07/01/2026 - 09/30/2026

Ottawa Area ISD CSOC Overview: 2026 Q3

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

CSOC Updates, Threat Trends, & More:

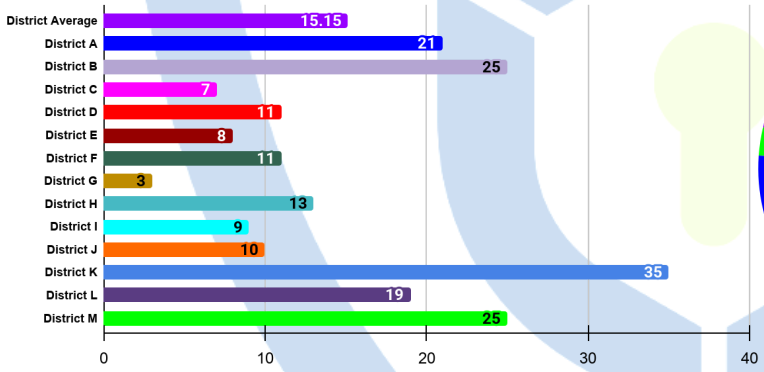
Highlights from activity across all 13 CSOC-supported districts

- **Phishing expanded beyond the inbox.** Attackers increasingly used Google Drive shares and Calendar invitations, creating blind spots where traditional email controls and investigation tools have less visibility.
- **Malicious Google Docs were shared at scale.** These documents frequently impersonated district leadership and directed users to phishing pages. Tech admins cannot remove externally owned documents shared with users as viewers, limiting remediation options. The CSOC worked with Google Support and submitted a feature request to address this gap.
- **Attackers increasingly targeted user devices.** ScreenConnect and fake CAPTCHA campaigns attempted to install remote access tools or execute malicious commands, moving beyond credential theft alone.
- **Compromised accounts were weaponized to continue attacks.** Attackers used legitimate accounts to distribute phishing at scale, create malicious content, and hide activity through inbox rules or deleted security alerts.
- **Personal and work activity increasingly overlapped.** Personal email forwarding and access from personal devices can create alternate paths around organizational security controls and visibility. The CSOC discourages mixing personal and work activity for this reason.
- **High-priority incidents increased despite fewer incidents overall.** More complex attacks required greater investigation and response time as staff returned from summer break. Attacks also showed greater sophistication across delivery, persistence, and evasion techniques, a trend that may be accelerated by attackers' growing use of AI.

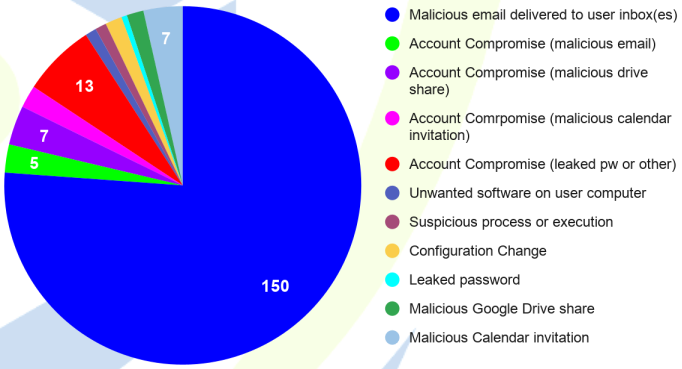
Incident Overview:

District Incidents

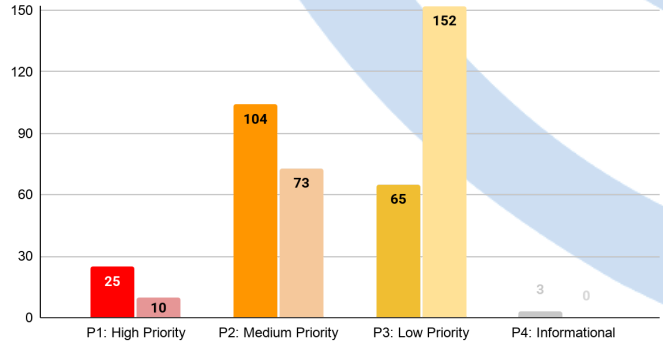
Total Q3 CSOC Incidents: 197



Incident Categories

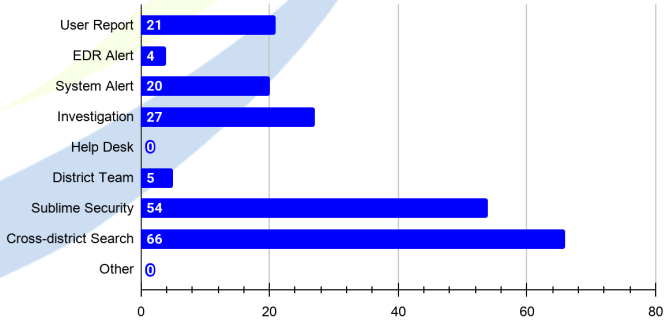


Incident Priority Levels



Detection Source

Identifies how incidents were first discovered



At a Glance

197 incidents across 13 districts

89% of total CSOC incidents originated from malicious emails

Higher-severity incidents increased with threat sophistication

Cross-district searches drove most incident detections

Ottawa Area ISD® Technology Services

Ottawa Area ISD CSOC

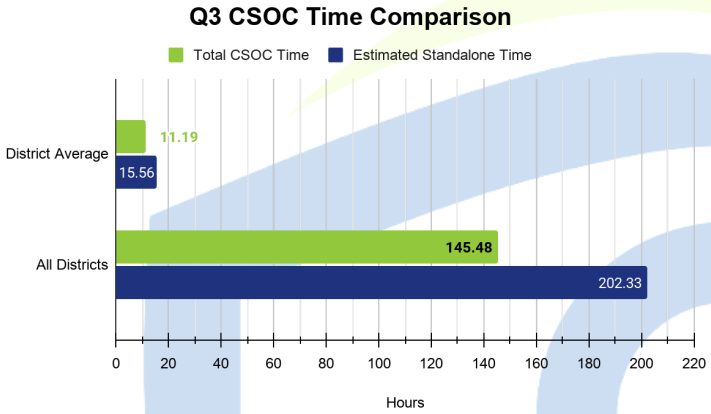
07/01/2026 - 09/30/2026

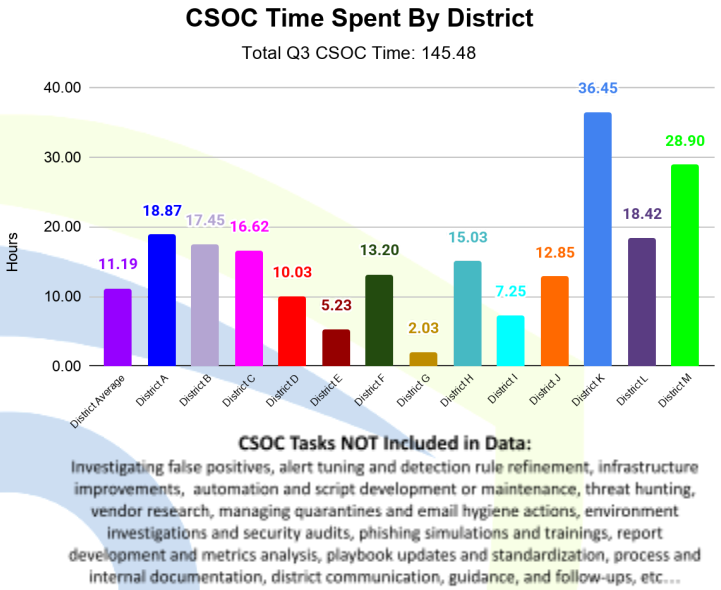
Incident Response Effort and Efficiency

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)





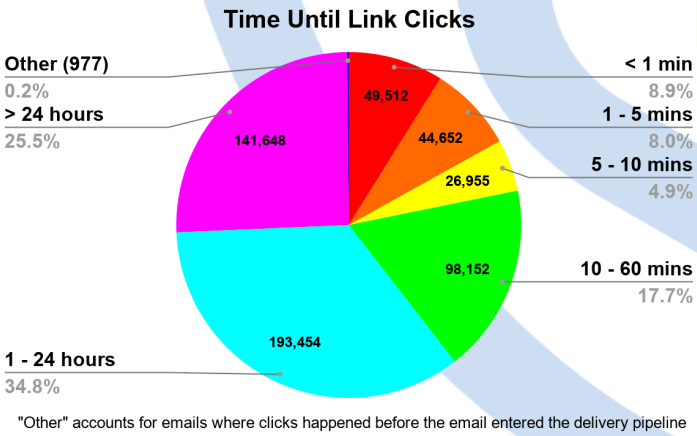
CSOC Tasks NOT Included in Data:

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...

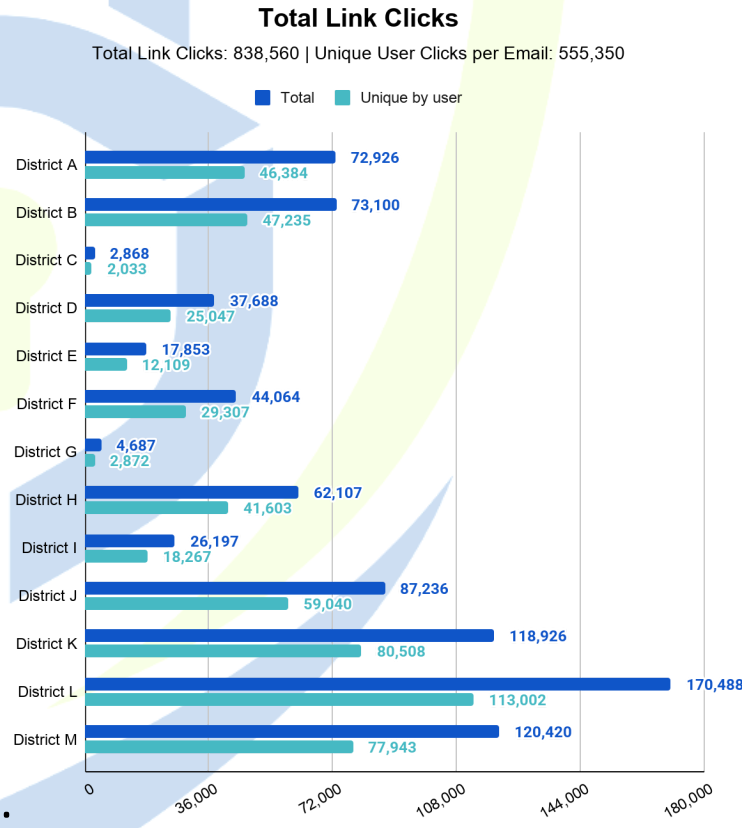
Link Clicks

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

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.



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



CSOC Tips, Resources, & Forecast:

- **2026 Q3 CSOC Threat Report**
- The **CSOC Insights Blog** is designed for a semi-technical audience, with updates posted on the 15th of each month: **Click the bell icon to subscribe to updates** 🔔
- The **CSOC's technical documentation** is posted to the CSOC Website, with guides and flow charts tech staff can follow during cybersecurity incidents: **CSOC Technical Documentation**
- **Quarantine Rules Efficacy Report- 2026-07-01 - 2026-09-30.pdf**
- **OAISD Sublime-Attack-Insights_2026-07-01_2026-09-30.pdf**