

Ottawa Area ISD CSOC Overview: 2026 Q1

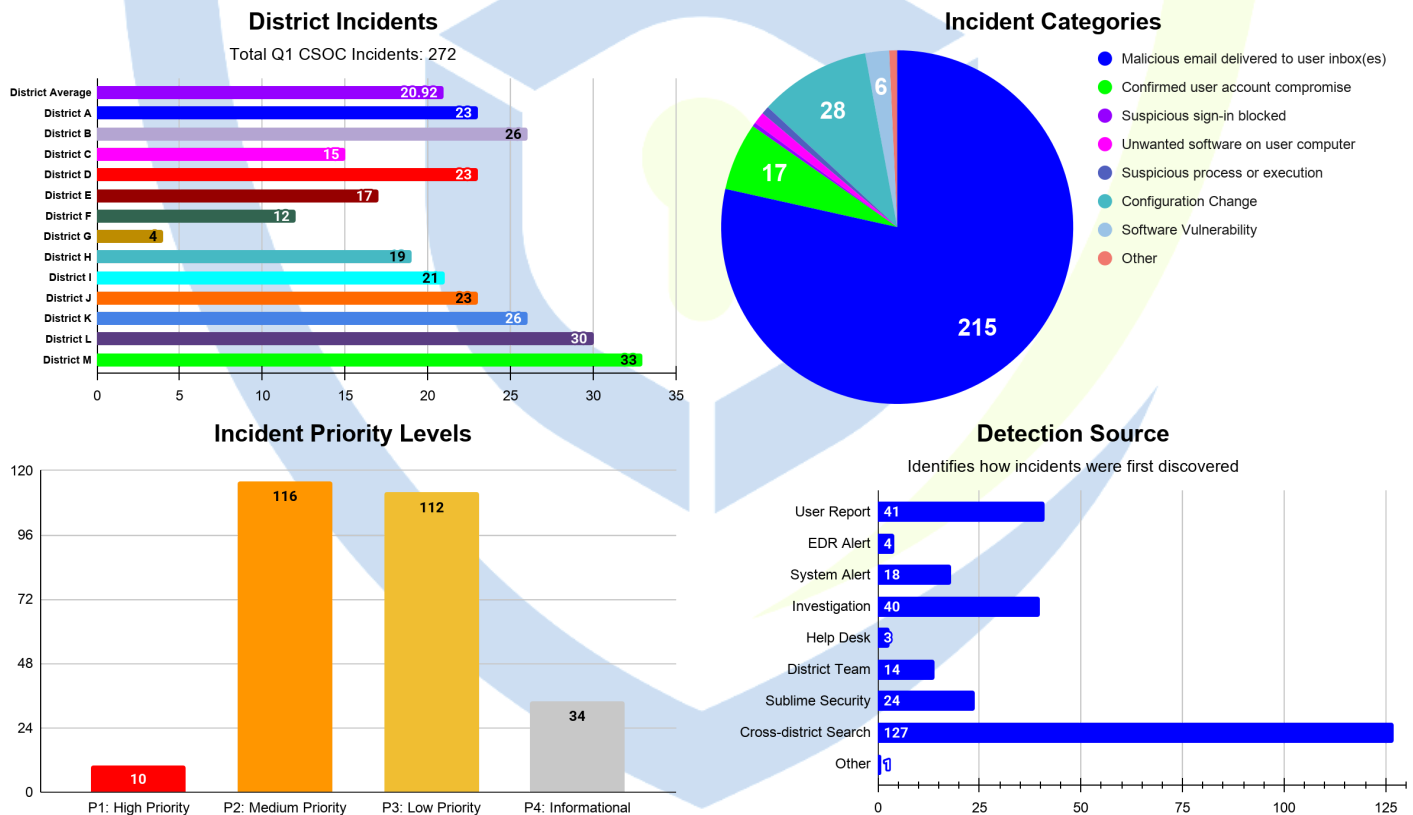
Prepared by the Ottawa Area Cybersecurity Operations Center | cybersecurity@oaisd.org

CSOC Updates, Threat Trends, & More:

Highlights from activity across all 13 CSOC-supported districts

- **Malicious emails remain the primary threat vector**, with Business Email Compromise (BEC) emails leveraging AI-generated content, which creates increasingly convincing phishing campaigns. These attacks are more likely to prompt user interaction and, when successful, can quickly escalate into account compromise, internal phishing, and broader operational impact.
- **Attackers are adopting more evasive techniques**, including the use of trusted platforms (Google Drive, Dropbox, etc) to deliver malicious payloads, domain lookalikes, and calendar invites to bypass traditional security controls.
- **An increase in lower-severity (P3) incidents** indicates a trend toward more targeted campaigns with limited scope, along with earlier intervention by the CSOC or existing security measures.
- **Student & staff-driven risks & threats**, including installation of unwanted software or browser extensions and attempts to bypass controls, continues to highlight gaps in visibility and opportunities for proactive hardening.
- **Implementation of Sublime Security for all CSOC-supported districts** has improved visibility and enabled faster removal of malicious emails, reducing exposure and response time.
- **Expanded sign-in monitoring and log enrichment** has improved early detection of account compromise, with continued development to strengthen real-time response capabilities.

Incident Overview:



At a Glance

272 incidents across
13 districts

78% 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.

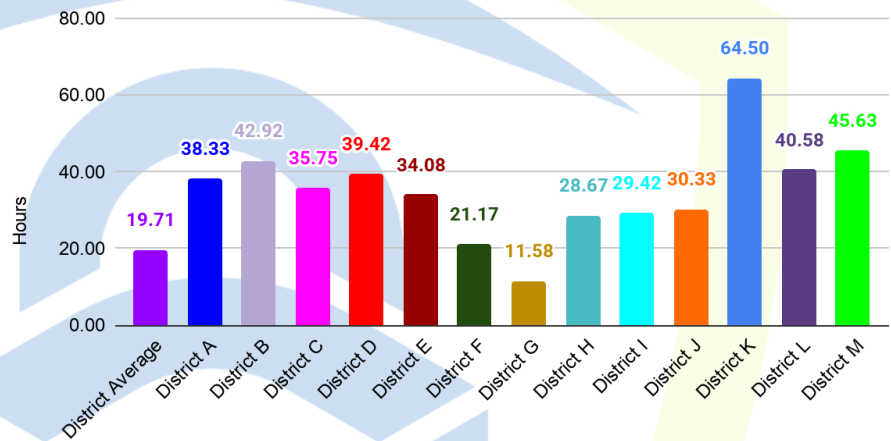
Beginning this quarter, the CSOC is tracking incident response efforts to better reflect the scope of work and the efficiency gained through centralized analysis and coordinated response. This approach highlights both the total effort involved and the time saved by avoiding duplicated investigation across districts.

The CSOC tracks incident response effort using two components:

- **Discovery Effort:** Time spent once per incident to identify scope, determine impact, and define required remediation actions.
- **District Impact Effort:** Time spent per district to execute remediation, gather evidence, and complete reporting.

CSOC Time Spent By District

Total Q1 CSOC Time: 256.21 hours



Total CSOC time

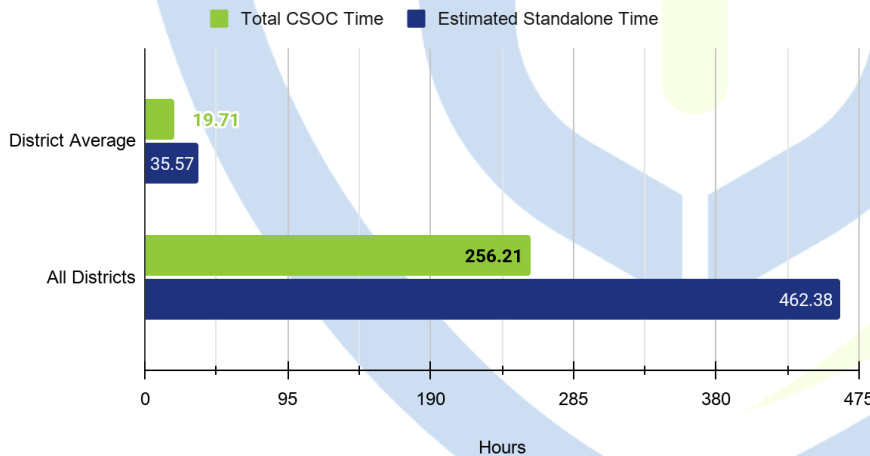
$$= (\text{Discovery Effort} \times 1) + (\text{ALL District Impact Efforts})$$

Estimated standalone time

$$= (\text{Discovery Effort} \times \text{ALL}) + (\text{ALL District Impact Efforts})$$

To estimate time without centralized CSOC efforts, we assume each district would repeat discovery:

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...

The difference between these two totals demonstrates the time saved through centralized analysis and coordinated response, rather than duplicated effort.

CSOC Tips, Resources, & Forecast:

- [2026 Q1 CSOC Threat Report](#)
- [Monthly CSOC Newsletter Archive](#)
- Breakdown of roles, services, and support: [K12 Cybersecurity Support: CSOC and MiSecure](#)
- Request **in-person trainings or tabletop exercises** for staff and tech teams: [CSOC Training & Exercise Requests](#)
- Resource for personal compromised accounts: [Account Remediation Checklist](#)
- The CSOC is assessing **BitLocker implementation** to strengthen device-level data protection.