

Ottawa Area ISD CSOC Overview: 2025 Q4

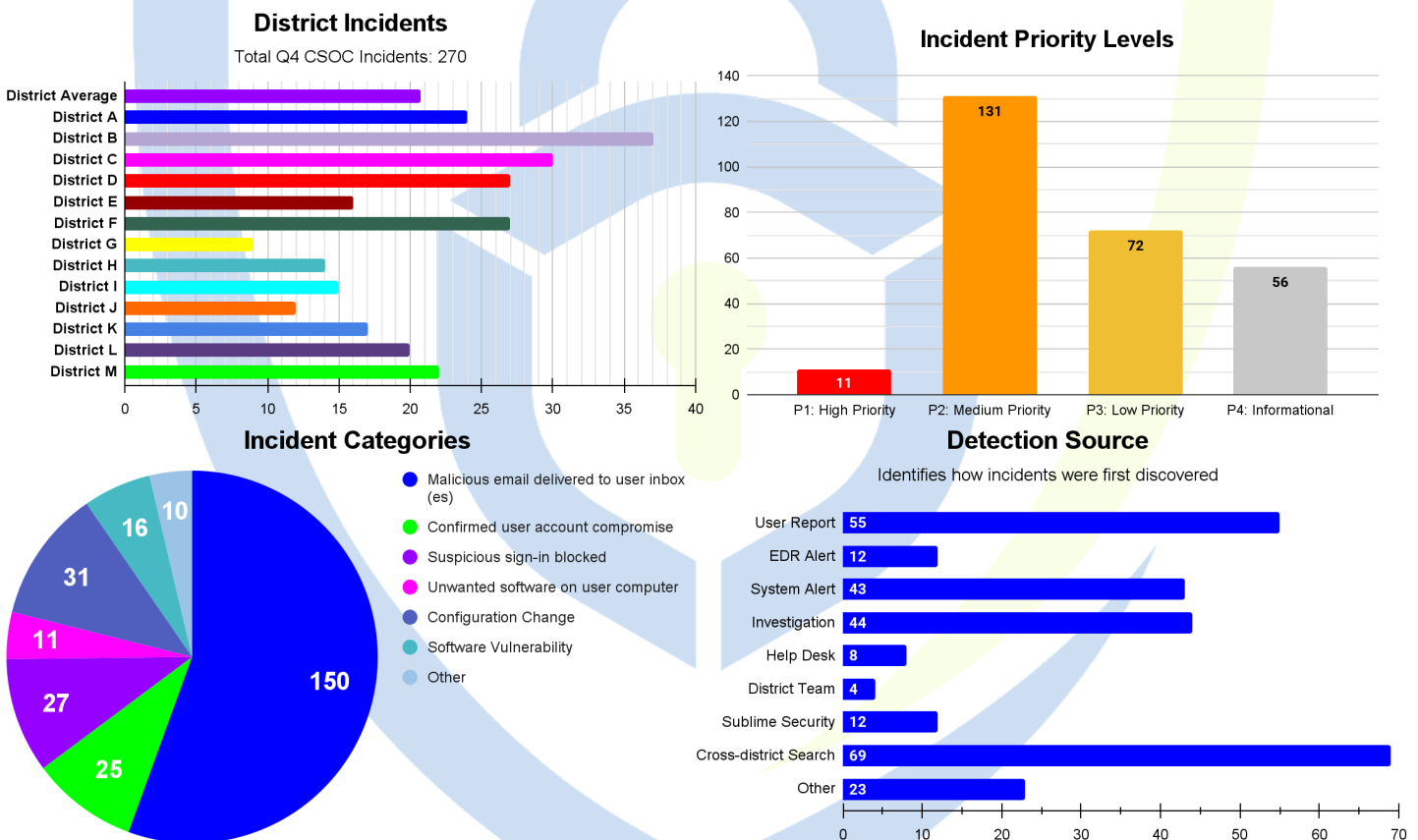
Prepared by the Ottawa Area Cybersecurity Operations Center

CSOC Updates, Threat Trends, & More:

Highlights from activity across all 13 CSOC-supported districts

- **Credential-theft phishing remains the most common threat**, with repeated campaigns impersonating DocuSign, Microsoft, Google, HR, and financial offices, and new campaigns using calendar invites. Most users did not submit credentials, which prevented account takeover and avoided extensive recovery work.
- **Compromised student accounts remain a key attack vector**, including cases where attackers used Google Apps Scripts as a backdoor to continue sending phishing messages from compromised accounts even after being signed out. Rapid resets, new restricted scopes on CSOC accounts, and close monitoring prevented broader disruption.
- **Malicious or unwanted software was detected and removed before causing harm**. Early detection prevented performance issues, reduced security exposure, and avoided the cost of manual remediation.
- **The CSOC expanded automated alert enrichment**, adding more context, linked data, and indicators directly into alerts, which helps filter false positives, speeds triage, and gives analysts the information they need more quickly.
- **After a surge in incidents in November, activity slowed at the end of the quarter**, allowing for focus on project work including software vulnerability review, hardening configurations, and broader improvements that reduce long-term risk.

Incident Overview:



CSOC Tips, Resources, & Forecast:

- The CSOC is preparing to deploy Sublime Security across all districts and have standardized our documentation and workflow to support consistent implementation: [Sublime Security: Onboarding Overview](#)
- [Monthly CSOC Newsletter Archive](#)
- A checklist is available for staff and tech teams to use when personal accounts are compromised or when compromised passwords affect multiple systems: [Account Remediation Checklist](#)
- District tech teams should **review where Google Apps Script is legitimately needed**, as the CSOC will be evaluating the impact of restrictions to prevent attackers from using scripts as backdoors.
- The CSOC team can be contacted at cybersecurity@oaisd.org for assistance or questions.