

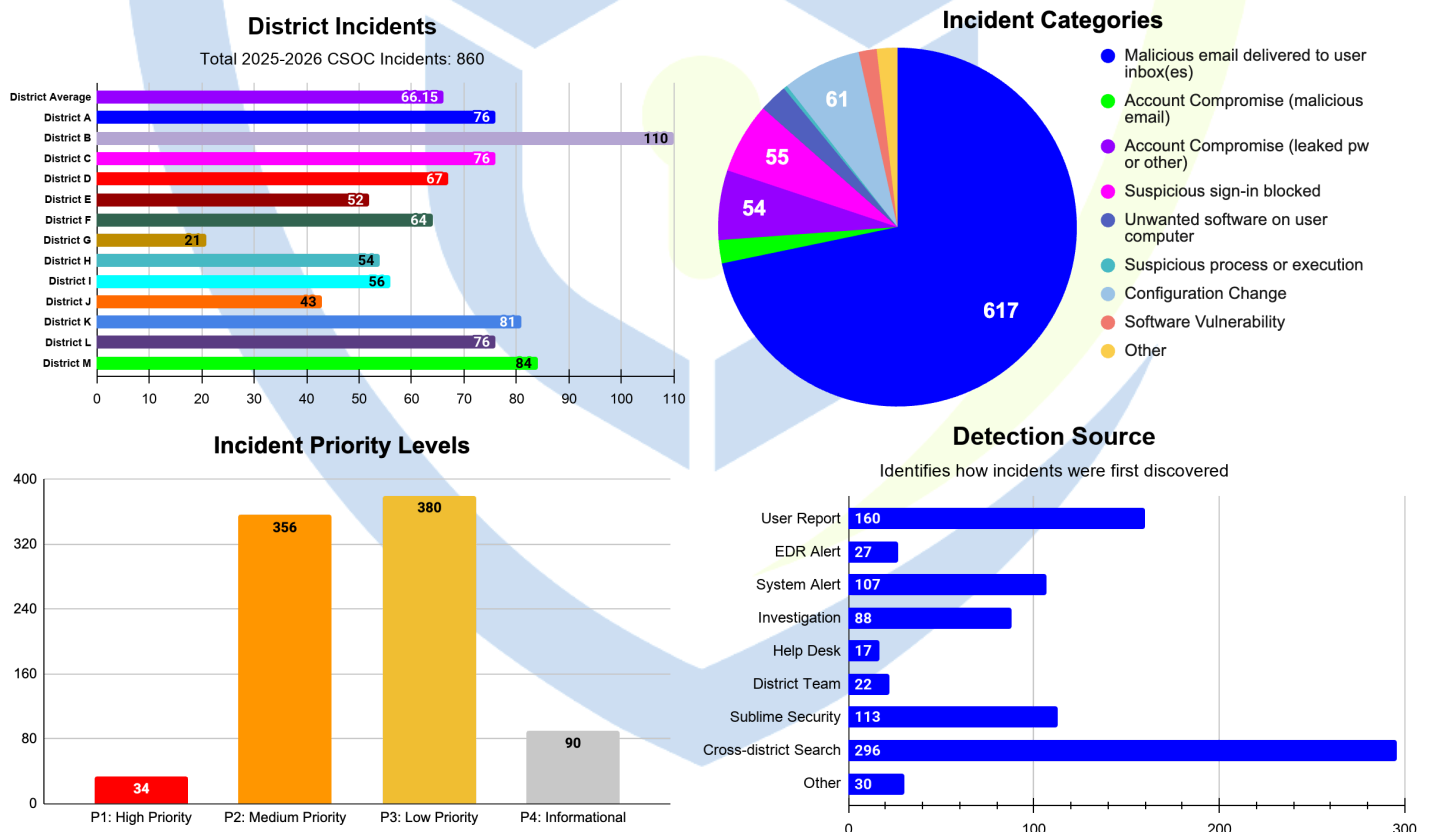
Annual CSOC Overview: 2025-2026

Prepared by the Ottawa Area Cybersecurity Operations Center

Major CSOC Accomplishments:

- Built the regional Ottawa Area Cyber Security Operations Center (CSOC)**
 Prior to the formation of the CSOC, cybersecurity responsibilities were handled on a best-effort basis alongside other technology duties. Over the past year, a dedicated team of four cybersecurity analysts and one manager was established, creating a consistent approach to cybersecurity for the region. The CSOC currently supports 13 school districts across West Michigan and has standardized incident response procedures and playbooks to ensure security events are handled consistently, efficiently, and with clear communication and documentation. This effort has created a more proactive and resilient approach to cybersecurity across supported districts.
- Strengthened Email Security and Threat Response**
 New email security technology was implemented to provide more advanced detection and remediation of phishing, malware, and other malicious messages before they reach staff and student inboxes. The team has also developed custom rules tailored to the threats targeting K-12 schools, allowing many malicious emails to be automatically blocked or removed before users ever have an opportunity to interact with them. Automated response actions now handle many common threats without requiring manual intervention, allowing analysts to focus on more complex investigations.
- Expanded Security Monitoring and Data Analysis**
 Significant progress was made toward consolidating security logs and other data sources into a centralized platform. Bringing this information together allows the team to identify suspicious activity more quickly, establish normal patterns of behavior, improve the speed and accuracy of incident investigations, and develop custom alerts that detect unusual activity before it becomes a larger security issue. Increased automation has also reduced repetitive manual tasks, improving response times while allowing analysts to spend more time investigating and responding to meaningful security events.

Incident Overview:



Keeping up with the CSOC:

- 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>