

Adverse Event Analysis

Detection tools only matter if someone makes sense of what they produce.

Why it matters

- The difference between one compromised teacher account and a district-wide outage is often how quickly someone recognizes the first odd sign-in or new mail forwarding rule for what it is. Without a written picture of normal and clear declaration criteria, warning signs get explained away until the student information system (SIS), payroll or the phone system goes down.
- When student records may have been exposed, the district must work out what data was touched and whose, so counsel can advise on the Family Educational Rights and Privacy Act (FERPA), Georgia's student data privacy law, family notifications and carrier requirements. Logs that aged out or were never collected can leave the district unable to rule anyone out, which widens notifications and raises cost.
- After an incident, the carrier, the forensic firm, counsel and the board will reconstruct what the district knew and when. A dated alert review log and an event write-up showing who decided what, and why, protects the district's credibility and supports the claim.

This category asks whether your district can pull event data together from multiple systems, tell normal from abnormal, size up impact, and formally declare an incident when defined criteria are met. The gap between a contained phishing account and district-wide ransomware is often the hours between the first odd login and someone deciding it matters — and after a breach, insurers, regulators, and counsel will ask exactly what you knew and when.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Events are examined only after someone complains. There is no description of normal activity, no one is assigned to analyze events, and logs from different systems are never looked at together.</p> <p>Moving up: Assign a named staff member to analyze event impact and start writing down how event data gets collected and reviewed — even a simple checklist counts. Aim for consistent anomaly detection first; the rubric expects reliable noticing before elegant process.</p>	<ul style="list-style-type: none"> • No baseline of normal sign-in hours and locations, network traffic, admin activity or expected data flows • No written criteria for when an event becomes an incident; the call depends on who happens to notice • Logs left at default retention in each console and opened only after something breaks
2 · Repeatable	<p>Anomalies such as impossible-travel sign-ins or a sudden burst of outbound email are noticed consistently, but each is handled case by case. A named staff member investigates events and is building skill, and a collection and review process is being drafted.</p> <p>Moving up: Document the full workflow — collect and correlate event data from multiple systems, analyze detected anomalies against an established network baseline — and put evidence-collection and forensics procedures in writing. Defined means a new hire could run the process from the documentation, with pattern-recognition tooling in use.</p>	<ul style="list-style-type: none"> • Named event analysis duty in a job description or technology department duty list • Draft procedure listing which logs exist, where they live and how long each system keeps them • Help desk tickets showing suspicious sign-ins and phishing reports investigated, with notes on what was found
3 · Defined	<p>A documented process brings event data from several systems to one review point, compares it with a maintained baseline and analyzes anomalies the same way every time. Evidence preservation and forensic steps are written down, and pattern-recognition tools such as behavior-based EDR or cloud anomaly alerts are in use.</p> <p>Moving up: Go deeper than closing alerts: run formal analysis of activity outside normal behavior at the application and database level, use root-cause analysis to find underlying vulnerabilities, and track those findings to closure with reporting to leadership.</p>	<ul style="list-style-type: none"> • Current baseline covering normal sign-in hours and countries, admin accounts and what they touch, typical bandwidth including testing windows, and expected data flows to the SIS and other vendors • Weekly alert review log with dates, findings, dispositions and reviewer initials • Written incident declaration criteria and an evidence preservation checklist naming what to export, who holds it and where it is stored

Level	What you would see	Artifacts that show it
4 · Managed	<p>Analysis goes past closing alerts. The team studies unusual activity inside key applications such as the SIS, finance and HR systems, uses root-cause analysis to learn why a weakness existed, and tracks findings to closure with regular reporting to leadership.</p> <p>Moving up: Automate the triage: combine threat intelligence with behavioral analytics so abnormal activity is separated from normal and alerted in real time, triggering rapid response without waiting for the weekly review. Staff tune the system; the system does the watching.</p>	<ul style="list-style-type: none"> • Reviews of SIS and finance system audit trails for unusual bulk exports, grade changes or vendor banking changes outside normal patterns • Root-cause write-ups for significant events with corrective actions, owners and due dates • Quarterly findings report to the superintendent showing open and closed items
5 · Optimized	<p>Detection works in real time. Threat intelligence and analytics separate normal from abnormal automatically and alert or act at once, for example by ending a risky session or isolating a device, while staff tune the rules after each incident.</p>	<ul style="list-style-type: none"> • Automated response rules in EDR, managed monitoring or cloud identity tools, such as session revocation on high-risk sign-ins, with test records • Threat intelligence indicators feeding detection rules, with a change history • Annual review of the baseline, declaration criteria and detection rules that records lessons learned from each declared incident

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Write a one-page baseline of normal logins, traffic, and admin activity</p> <p>Pull a typical week of sign-in data from the Google Admin console audit logs or Microsoft Entra sign-in logs, plus firewall bandwidth graphs, and write down normal hours, sign-in countries, peak periods such as state testing, and every account with admin rights. Store it where the whole team can find it and refresh it each semester.</p>	Free	Hours	Network and systems administrator
<p>Alert on (or block) logins from countries where you have no users</p> <p>If your licenses include Conditional Access in Microsoft Entra or Context-Aware Access in Google Workspace, block or challenge sign-ins from countries with no users; otherwise add a location filter on sign-in logs to the weekly review. Write a simple exception process for staff traveling abroad so the rule is not quietly switched off.</p>	Free	Hours	Network and systems administrator
<p>Define three concrete incident-declaration triggers and share them with the team</p> <p>Choose triggers such as EDR isolating a server, an administrator sign-in from an unexpected country, or new forwarding rules on several staff mailboxes, and for each one name who gets called and who can declare an incident. Add the page to the incident response plan and walk the superintendent through it.</p>	Free	Hours	Technology director
<p>Export or extend cloud audit log retention beyond the defaults</p> <p>Check how long Google Workspace audit logs and Microsoft 365 audit search keep data, then schedule a regular export to protected district storage or forward the logs to your collector or managed monitoring platform. Record the resulting retention for each system so the insurance application answer matches reality.</p>	Low cost	Days	Network and systems administrator
<p>Block 30 minutes weekly on the calendar for alert and trend review</p> <p>Set a recurring block, ideally Monday morning to catch weekend activity, and work a short checklist: cloud console alerts, EDR detections, spikes in failed sign-ins, new admin accounts, new mail forwarding rules, and current advisories. Record the date, what was reviewed and any follow-up in a shared log; that log is your evidence.</p>	Free	Hours	Network and systems administrator

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Wiping before preserving. Reimaging a laptop or resetting an account right away can erase the evidence needed to know what was accessed, so follow a short preservation checklist first: export the relevant logs, isolate the device rather than wiping it, and write down the time.
- Treating everything as an incident, or nothing. If every reported phish triggers the full plan, staff stop escalating, and if the bar is undefined, real compromises sit for days; write tiered criteria so single low-risk events stay tickets and defined combinations go straight to declaration.
- Watching the network but not the applications that hold student data. Firewall and email logs will not show a compromised SIS account exporting a full roster or changing grades, so turn on and review audit trails in the SIS, finance and HR systems and ask each vendor what logs they keep and how you get them during an investigation.
- Letting logs age out. Cloud consoles and firewalls keep data for a limited window and intrusions are often discovered well after they began, so set retention deliberately, export what you would need for a breach analysis and document the result.
- Keeping analysis in one person's head. When the only analyst is also the help desk and the network administrator, findings leave with them; keep a simple event log and written procedures so a backup, the managed provider or an outside incident responder can pick up the work.

Evidence that proves it

- Documented baseline of normal network activity, login patterns, and admin behavior
- Written incident declaration criteria mapping alert types to severity and action
- Centralized log or alert console evidence (syslog server, EDR/MDR dashboard, SIEM)
- Weekly alert and anomaly review log with dates, findings, and reviewer initials
- Audit log retention settings or export procedure for Google/Microsoft environments
- Sample event impact write-up listing affected systems, data, and user counts
- Tickets or notes showing MS-ISAC advisories checked against district systems

Who usually owns it

Technology director

Maintains the baseline and incident declaration criteria, names the event analyst, and decides with the superintendent when an event becomes a declared incident.

Network and systems administrator

Forwards logs to the central review point, runs the weekly alert review, and records the scope and impact of events as they unfold.

Data privacy officer

Helps determine whether student or staff records were involved and works with counsel on FERPA and state student privacy obligations.

Superintendent

Serves as the escalation point once an incident is declared and coordinates notifications with counsel, the carrier and any required authorities.

Insurance relevance · Medium

Applications ask how alerts are triaged and escalated and whether someone investigates them around the clock. After a claim, the carrier's breach coach and forensic firm test those answers against your logs and review records.

- Do you review security alerts on a defined schedule, with a documented process for escalating suspected incidents?
- Are security alerts investigated around the clock, either in-house or through a managed provider?
- How long are sign-in, endpoint and firewall logs kept, and could you show which records an attacker accessed?
- Who has authority to declare an incident and contact the carrier's claims or breach response line?

Tip: Keep the weekly review log and a few recent examples of alerts reviewed, dismissed or escalated with the reason recorded, so a yes on the triage question is backed by records.

Funding and free help

MS-ISAC membership (Center for Internet Security)

Paid membership · rolling

Threat intelligence, 24x7 SOC advisories, incident response help and services for state and local governments. Fee-based since October 2025, tiered by operating budget; some CIS tools remain free.

CISA K-12 cybersecurity resources and toolkit

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- Best Practices for Event Logging and Threat Detection (CISA) <https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection>
- SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST) <https://csrc.nist.gov/pubs/sp/800/61/r3/final>
- Known Exploited Vulnerabilities Catalog (CISA) <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (CIS) <https://www.cisecurity.org/ms-isac>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>