

Continuous Monitoring

This category asks whether anyone — or anything — is actually watching your network, accounts, and devices for trouble, and whether you routinely scan for the weaknesses attackers find first.

Why it matters

- Attackers who get in through a phished staff account or an unpatched remote-access device often look around quietly before they encrypt anything, and they favor nights, weekends and school breaks when no one is at the console. If no one is watching, the first sign may be a locked student information system (SIS) and transportation software with no bus routes on a Monday morning.
- Cyber insurance carriers ask directly about endpoint detection and response (EDR) coverage, who answers alerts after hours, quarterly external scans and log retention, and many scan the district's public footprint themselves before quoting. Weak answers can mean higher premiums, exclusions or a declined renewal, and an answer the evidence does not support can complicate a claim.
- A routine of scans, account reviews and removal of unknown devices finds the forgotten things before attackers do: the departed employee whose account still works, the camera system with an open web login, the personal wireless router a teacher plugged in. Each fix is small and cheap when it is found on a Tuesday afternoon instead of in the middle of an incident.

Ransomware crews often dwell inside a district network for days or weeks before detonating, and they favor nights, weekends, and school breaks when no one is at the console. Cyber-insurance applications now ask pointedly about EDR coverage, external vulnerability scanning, and around-the-clock monitoring, so this category often decides premiums and eligibility.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	Monitoring happens when something breaks. No one is assigned to review alerts, external scans are not on a schedule, and unknown devices or accounts are found by accident, if at all. Moving up: Write down how you find and remove unknown devices and accounts, and put external vulnerability scans on a schedule — CISA's free service makes the schedule real. Documenting the process, even while it is still reactive, is the move to Repeatable.	<ul style="list-style-type: none"> No process or record for finding and removing unknown devices on staff, student or guest networks Firewall, content filter and cloud admin console logging left at defaults, with alerts going to no one or to a single inbox No external vulnerability scan, penetration test or account review on file from the past year; accounts of departed staff and old vendors still active
2 · Repeatable	The district has written down how it tracks assets and handles unknown devices, but work still starts from a complaint or an alert. A schedule for external scans and reviews is drafted but not yet running reliably. Moving up: Execute the schedule: quarterly external vulnerability scans actually run, an annual penetration test gets completed, and account reviews happen systematically with dated sign-offs. Consistency on a documented cadence, not new tooling, is what Defined requires.	<ul style="list-style-type: none"> Written procedure for finding and removing unauthorized devices and software, even if it is applied only when something is noticed Cyber Hygiene enrollment request or a draft calendar for quarterly external scans Google Workspace Alert Center or Microsoft 365 alert emails reaching a named person, reviewed when time allows
3 · Defined	Scans, reviews and cleanup happen on schedule whether or not anything seems wrong. External vulnerability scans run at least quarterly, an outside penetration test is completed each year, and account reviews are dated and signed. Moving up: Shift from periodic checks to continuous real-time detection embedded in daily operations — EDR with managed after-hours coverage — and act on findings with forensics, root-cause analysis, threat intelligence, and tracked corrective actions.	<ul style="list-style-type: none"> Four consecutive quarters of external scan reports paired with a remediation log showing what was fixed and when Annual external penetration test report with each finding tracked to closure Dated, signed account and firewall rule review records, plus a log of unknown devices found and removed using wireless controller and switch reports

Level	What you would see	Artifacts that show it
4 · Managed	Monitoring is continuous and part of daily work. EDR covers every server and staff computer, a managed service or a written on-call rotation answers alerts on nights, weekends and breaks, and significant findings get forensic review, root-cause analysis and tracked corrective action. Moving up: Use data — detection times, remediation times, alert outcomes — to verify your monitoring actually works, and run gap analyses across multiple technologies to expose blind spots and build failsafe measures. At Optimized, the metrics tune the program.	<ul style="list-style-type: none"> EDR console coverage report reconciled against the asset inventory, including domain controllers and file servers Managed detection and response contract or on-call rotation, with records of after-hours alerts and what was done Quarterly monitoring report to the superintendent covering detection coverage, scan and penetration test results, and remediation status
5 · Optimized	The district uses its own monitoring data to prove what works and fix what does not. Detection and remediation times are measured, blind spots are found by comparing what each tool can and cannot see, and failsafe measures cover the gaps.	<ul style="list-style-type: none"> Annual metrics review of time to detect, time to remediate and alert outcomes, with the resulting changes documented Gap analysis comparing coverage across EDR, firewall, DNS filtering, cloud consoles and external scans, with each blind spot assigned an owner Documented failsafe measures, such as a second alert path when the on-call person or managed provider cannot be reached

Quick wins

Quick win and how	Cost	Effort	Usual owner
Enroll in CISA Cyber Hygiene external scanning (free, one form, weekly reports) Email the Cybersecurity and Infrastructure Security Agency (CISA) at vulnerability@cisa.dhs.gov asking for Cyber Hygiene services, then return the signed authorization with every public IP address and domain the district owns. Get the full address list from your internet service or E-Rate contract so forgotten devices are included, and send the weekly reports to a shared mailbox.	Free	Days	Technology director
Join MS-ISAC and turn on MDBR DNS-layer blocking Apply through the Center for Internet Security, confirm your dues tier and whether Malicious Domain Blocking and Reporting is included, then point your internal DNS forwarders or the content filter's upstream resolvers to the MDBR resolvers. If dues are not in this year's budget, confirm that your content filter's malicious-domain blocking is turned on for staff, student and guest networks.	Low cost	Days	Technology director
Enable Google Alert Center / Microsoft 365 alerts and route them to two staff In the Google Admin console, open the alert rules for suspicious login, leaked password, government-backed attack and device compromise, and add a shared security mailbox as the recipient; in Microsoft 365, set the same mailbox on alert policies in the Microsoft Defender portal. Make sure at least two people read that mailbox and send a test alert to confirm it arrives.	Free	Hours	Network and systems administrator
Turn on audit logging on the firewall, content filter, and cloud admin consoles Turn on event logging on the firewall and content filter and send it to one collector, such as a syslog server or your EDR or managed monitoring platform, and confirm Microsoft 365 audit logging or Google Workspace audit logs are active. Record each system, what it logs and how long it keeps data on a one-page log inventory.	Free	Days	Network and systems administrator
Put quarterly account and firewall rule reviews on a standing calendar Set recurring reviews that fit the school year, such as before students return in August, after winter break, before the state testing window and at year end. Each review exports admin and inactive accounts from Google or Microsoft and the SIS, compares them with HR's active staff list, flags firewall rules with no owner or purpose, and saves the signed results as evidence.	Free	Hours	Technology director

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

Common pitfalls

- Sending alerts to one person's inbox. When that person is out sick, on summer leave or has moved on, alerts pile up unread; route them to a shared mailbox or group that at least two people read and test delivery each semester.
- Treating EDR as finished once the agent is purchased. Missing, outdated or quietly disabled agents on servers, old lab machines and the business office computer are the gaps investigators find after an incident, so reconcile the EDR console against the asset inventory every month and chase the difference.
- Buying a monitoring tool with no one to answer it after hours. An alert at 2 a.m. on a Saturday in July helps only if someone can act, so either contract a managed detection and response service that is authorized to isolate devices, or write an on-call rotation that covers holidays and summer.
- Scanning only the systems the district remembers. A forgotten remote-access appliance, camera recorder, HVAC controller or old test web server never shows up in a report you did not ask for, so pull the full list of public addresses from your provider and scan all of them.
- Monitoring people without a policy basis. Monitoring use of district technology should follow board-approved acceptable use procedures and the Children's Internet Protection Act (CIPA), and student activity monitoring tools collect data covered by student privacy law, so keep security monitoring and student-safety monitoring separately scoped, documented in board policy and reviewed by the data privacy officer.

Evidence that proves it

- MS-ISAC membership confirmation and recent advisory emails
- CISA Cyber Hygiene weekly external vulnerability scan reports
- EDR console report showing agent coverage across servers and staff devices
- Google Workspace Alert Center or Microsoft 365 alert policies and routing configuration
- Calendar entries and sign-offs for quarterly account and firewall rule reviews
- Most recent external penetration test report with remediation tracker
- MDR or SOC monitoring service contract or statement of work

Who usually owns it

Technology director

Owns the monitoring program: sets the scan, penetration test and review calendar, makes sure every alert source has someone answering it, and reports results and gaps to the superintendent.

Network and systems administrator

Maintains logging and EDR coverage, works the alert queue and unknown-device reports, and performs the dated account and firewall rule reviews.

Business and finance officer

Budgets for EDR, managed monitoring and the annual penetration test, and checks whether grant programs such as the State and Local Cybersecurity Grant Program can help before purchase.

Superintendent

Makes sure monitoring is resourced and staffed for after-hours coverage, receives escalations of significant findings, and reports on the program to the board.

Insurance relevance · High

Carriers probe this area directly: EDR coverage, round-the-clock alert monitoring, quarterly vulnerability scanning and log retention appear on typical applications, and many carriers scan the district's internet-facing systems themselves before quoting.

- Is endpoint detection and response (EDR) installed on every workstation and server, including domain controllers, and what share of devices report in?
- Who monitors and responds to security alerts at night, on weekends and during school breaks?
- How often do you scan internet-facing and internal systems for vulnerabilities, and how quickly are critical findings fixed?
- Do you collect authentication, endpoint, network and cloud logs centrally, and how long are they kept?

Tip: Answer from the EDR coverage report, the managed service contract and recent scan reports rather than from memory, and make sure the systems you say you scan match what the carrier's own external scan will find.

Funding and free help

GaDOE/GTA statewide security rating platform (Bitsight)

Launched 2022 · 2026 status unverified

GaDOE funded licenses for an external security rating and monitoring platform for every Georgia school district at no cost to districts, showing external vulnerabilities and a security scorecard.

CISA Cyber Hygiene Services (vulnerability and web application scanning)

Rolling enrollment

Free, continuous external vulnerability scanning of a district's public IP addresses with weekly reports and urgent alerts; optional web application scanning is also free.

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.

State and Local Cybersecurity Grant Program (SLCGP) – Georgia subawards

Georgia FY2024 round closed May 15, 2026 · watch for the FY2025 round

Federal cyber grant passed through the state to local governments, including school districts. Georgia accepted FY2024 subaward applications April 1 – May 15, 2026. Federal authority beyond September 30, 2026 depends on Congress.

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

Learn more

- Cyber Hygiene Services (CISA) <https://www.cisa.gov/cyber-hygiene-services>
- No-Cost Cybersecurity Services and Tools (CISA) <https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools>
- Best Practices for Event Logging and Threat Detection (CISA) <https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection>
- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (CIS) <https://www.cisecurity.org/ms-isac>