

Incident Mitigation

This category asks whether you can stop an active incident from spreading (containment) and then fully remove the attacker's foothold (eradication).

Why it matters

- Speed decides scale. A phished account contained within the hour stays one person's bad day; left running overnight, it can become forwarding rules in the payroll office, changed direct deposit details or encrypted servers in every school.
- Resetting a password is not the same as removing the attacker. A new admin account, an approved third-party app with access to mail or a scheduled task on a server can let the attacker back in, so verified eradication is what lets the district reopen systems with confidence.
- Containment decisions have instructional consequences, such as shutting down a building's network during state testing or cutting the internet connection on a school day. Deciding in advance who may take those actions, and what each one disrupts, lets the district act fast without arguing about authority mid-incident.

Speed here decides whether a phished mailbox stays a nuisance or becomes encrypted servers and closed school days, and incomplete eradication is why districts get hit again weeks after they thought they had recovered. Insurers and forensics teams will scrutinize how fast affected systems were isolated and whether persistence was actually removed.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	Containment depends on whoever is available figuring it out in the moment. There are no written steps for a compromised account or an infected computer, and no one has decided in advance who may shut down a network segment or the internet connection. Moving up: Write down containment and eradication steps for your likely events and apply them the same way every time — a defined, consistent approach with collaborative problem solving is the bar for Repeatable.	<ul style="list-style-type: none"> • No containment runbooks; past incidents were closed when the symptoms stopped • No list of who is authorized to isolate devices, suspend accounts or cut network links after hours • Anti-malware alerts that are cleared without checking what else the attacker touched
2 · Repeatable	Written steps exist for the most likely events, and the team applies them the same way each time, working through problems together. Eradication is understood to mean more than resetting a password. Moving up: Make it routine: drill the containment runbooks, verify incidents are actually contained and eradicated rather than just quieted, and log every vulnerability found as either mitigated or a documented accepted risk.	<ul style="list-style-type: none"> • Draft runbooks for a compromised account, an infected device and ransomware • List of authorized staff and the admin console access each one needs to suspend accounts and isolate devices • Incident tickets showing the same containment steps applied to similar events
3 · Defined	Containment steps are practiced and followed every time. Incidents are confirmed contained and eradicated before they are closed, and every weakness an incident reveals is either fixed or written up as an accepted risk approved by the superintendent or a designee. Moving up: Add near-real-time capability — EDR with one-click host isolation and automatic quarantine — and deploy mitigation processes universally so every incident generates data you can review afterward.	<ul style="list-style-type: none"> • Completed eradication checklists on closed incidents: sessions revoked, forwarding rules and unapproved app access removed, credentials reset, exploited weakness fixed • Exercise record showing staff practiced isolating a device and suspending an account • Vulnerability tracker linking each incident finding to a fix or a signed risk acceptance
4 · Managed	Endpoint detection and response (EDR) or a managed service can isolate a device or block a threat within minutes, at any hour, in every school and office. The same mitigation process is used everywhere and records what was done and when, so containment times can be measured. Moving up: Get ahead of it: maintain a mitigation roadmap, catalog vulnerabilities across incidents, share best practices with peer districts, and secure leadership commitment to fund capability gaps as they are identified rather than after the next event.	<ul style="list-style-type: none"> • EDR console showing isolation available and automatic quarantine on for all district-managed computers and servers • Containment time records for significant incidents, reported to the superintendent twice a year • Domain Name System (DNS) or firewall blocking that can stop a malicious domain district-wide from one place

Level	What you would see	Artifacts that show it
5 · Optimized	The district keeps a roadmap for improving containment and funds it through the budget process as gaps are found. Vulnerabilities from every incident are cataloged and reviewed for patterns, and mitigation practices are shared and refined with peer districts and regional partners.	<ul style="list-style-type: none"> Containment improvement roadmap approved by the superintendent, with matching budget lines Catalog of vulnerabilities found across incidents, with notes on recurring patterns Runbooks or practice notes developed with peer districts, a Regional Educational Service Agency (RESA) or a state partner

Quick wins

Quick win and how	Cost	Effort	Usual owner
Write one-page containment runbooks for a phished account, an infected device, and ransomware For each scenario, list the first five actions in order, the console or device where each is done, who is authorized to do it and how it gets recorded in the incident ticket. Walk through each runbook in a tabletop and rewrite any step nobody could actually perform.	Free	Days	Technology director
Document break-glass steps: who can disable a VLAN, block a domain, or bulk-suspend accounts For each emergency action, such as shutting down a virtual local area network (VLAN) or building uplink, record exactly where it is done (core switch, firewall, Google or Microsoft admin console), two people who can do it and what needs superintendent approval first. Keep an emergency admin account protected and its credentials sealed in a controlled location so action is still possible if normal sign-in fails.	Free	Hours	Network and systems administrator
Practice suspending an account and revoking sessions and tokens in your Google or Microsoft admin console With a test account, in the Google Admin console suspend the user, reset sign-in cookies and remove connected apps and app passwords; in the Microsoft Entra admin center, block sign-in and revoke sessions, then check the mailbox for forwarding rules and delegates. Time the drill and write the exact steps into the account-compromise runbook.	Free	Hours	Network and systems administrator
Turn on automatic quarantine in your anti-malware or EDR tool In the endpoint protection console, set policies to quarantine or block detected threats automatically instead of alerting only, and enable device isolation if the product supports it. Apply the policy to every device group, including servers and business office computers, and confirm in the console that each device reports the new policy.	Free	Hours	Network and systems administrator
Ask MS-ISAC or your state about current terms for MDBR and EDR through CIS Endpoint Security Services Contact the Center for Internet Security, the Georgia Technology Authority and your Regional Educational Service Agency (RESA) to ask about current membership terms and pricing for Malicious Domain Blocking and Reporting and managed endpoint detection and response, and whether any state program or grant covers them. Take the answers to the business office before budget season, since both services carry fees.	Low cost	Days	Technology director

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

Common pitfalls

- Powering off infected computers by reflex. Shutting down can erase evidence held in memory; isolate the device from the network through the EDR console, the switch port or the cable, and power down only if it cannot be disconnected or forensics advises it.
- Resetting the password and calling it done. Attackers commonly add mail-forwarding rules, mailbox delegates, connected app grants or extra admin accounts; revoke sessions and check each of these before closing the incident.
- Leaving shutdown authority undecided. At 2 a.m. no one wants to cut a building's network without permission, so write down who may isolate segments or disconnect the internet and which actions need the superintendent first.
- Coordinating containment where the attacker can see it. If an admin account or email is compromised, the attacker may be watching the response; use out-of-band channels and reset privileged credentials from a device known to be clean.
- Restoring before eradicating. Bringing systems or backups back online before the entry point is closed can reinfect the network, so confirm the exploited weakness is fixed and credentials are reset before restoration starts.

Evidence that proves it

- One-page containment runbooks for top scenarios (account compromise, infected device, ransomware)
- EDR console policy showing host-isolation capability, or isolation logs from a real incident
- Change tickets documenting containment actions taken during an event
- Completed eradication checklist from a closed incident: persistence removed, credentials reset, patch applied
- Vulnerability remediation records or signed risk-acceptance memos tied to incidents
- Network diagram marking isolation points such as VLANs, uplinks, and site-to-site links

Who usually owns it

Technology director	Directs containment, confirms eradication before an incident is closed, and keeps runbooks, authorizations and the incident vulnerability tracker current.
Network and systems administrator	Carries out isolation, account suspension, blocking and credential resets, and keeps EDR and network controls ready to use at any hour.
Help desk	Recognizes likely compromise in incoming calls, follows the first containment steps in the runbook, and escalates instead of reimaging or simply resetting a password.
Superintendent	Authorizes disruptive containment such as building-wide network shutdowns and approves documented risk acceptances for weaknesses that cannot be fixed right away.

Insurance relevance · Medium

Underwriters approach containment mostly through questions about endpoint detection and response (EDR) coverage, network segmentation and after-hours alert response, which they treat as signs of how far an incident could spread. After a claim, the carrier's forensic firm will look at how quickly affected systems were isolated and whether the attacker's foothold was removed.

- Is EDR deployed on all workstations and servers, and can it isolate a device remotely?
- Is the network segmented so student devices, staff systems, servers and building systems are kept apart?
- Who can take containment action at night, on weekends and during school breaks?
- How do you confirm a compromised account or device is clean before returning it to service?

Tip: Describe the isolation capability you have actually tested rather than the product's feature list, and keep a record of the last time staff practiced isolating a device or suspending an account.

Funding and free help

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

- #StopRansomware Guide (CISA) <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>
- Known Exploited Vulnerabilities Catalog (CISA) <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Malicious Domain Blocking and Reporting (MDBR) (CIS) <https://www.cisecurity.org/ms-isac/services/mdbr>
- 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>
- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>