GUARDIAN

BLUE RIDGE IT SOLUTIONS

● SOC ONLINE · 24/7/365

A security operations center for your district.

Analysts watching your computers and your network every hour of every day, with the authority to stop an attack while it is still happening.

WE WATCH

Every endpoint and the network edge, continuously — nights, weekends, holidays.

WE ACT

Isolate the machine, kill the process, block the address. Minutes, not tickets.

WE EXPLAIN

Reports your board and your insurer can read, backed by sealed evidence.

Blue Ridge IT Solutions
Church Hill, Tennessee

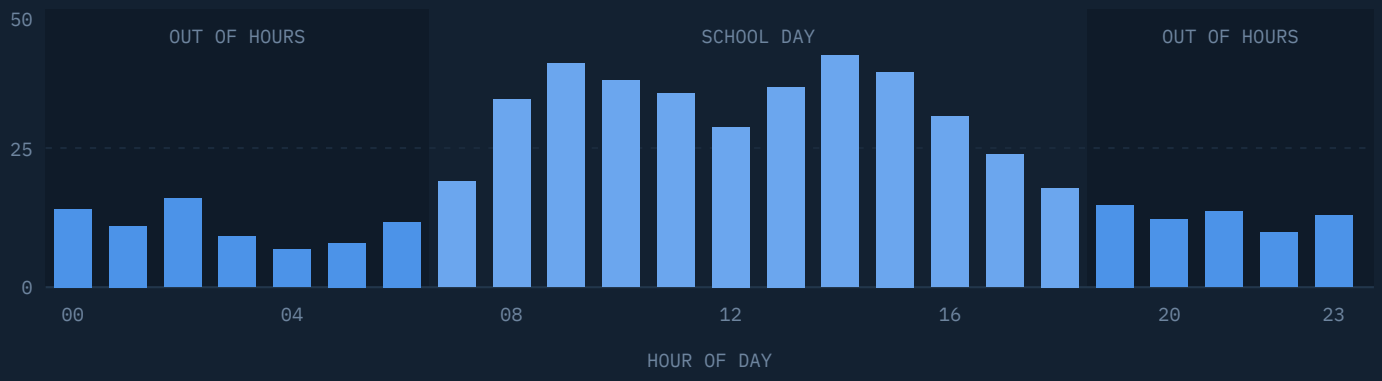
(423) 292-1922
blueridge-us.com

Attacks do not wait for the school day.

Nearly a third of what we catch arrives outside school hours, when nobody at the district is looking. That is the entire reason a security operations center exists.

When detections actually arrive

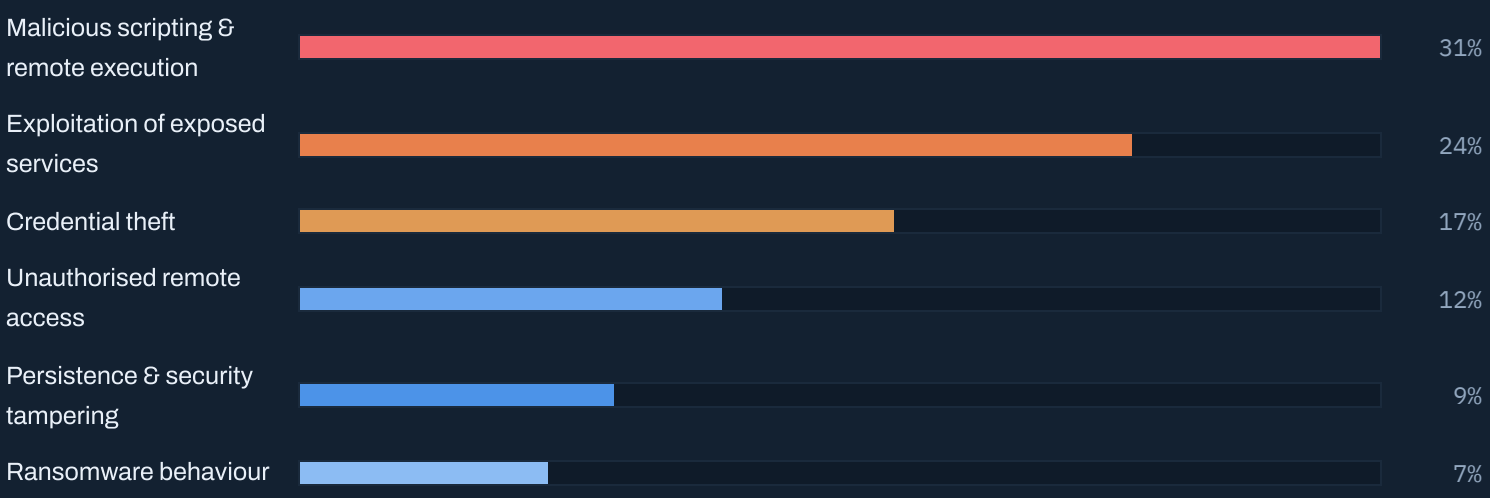
DETECTIONS BY HOUR · REPRESENTATIVE WEEK



Representative distribution across a monitored network. The shaded bands are the hours when a district has nobody watching and we do.

What the detections are

SHARE OF DETECTIONS



Why your inbox stays quiet

MEASURED ON A LIVE NETWORK

95
security events examined by the platform

19
opened as incidents worth an analyst's time

1
escalated to a person at your district

The failure of most security tooling in a district is not that it misses things — it reports everything, a small team learns to ignore it, and the one that mattered scrolls past. We do the filtering on our side.

This is what reaches you, and what we already did about it.

You are not handed a log file. You get a finding in plain language, the evidence behind it, and the action already taken.

CRITICAL **Credential theft attempt on a domain controller** 02:14 · Tue

HOST
DISTRICT-DC01

ACCOUNT
svc_backup

TECHNIQUE
Credential Access

CONFIDENCE
High

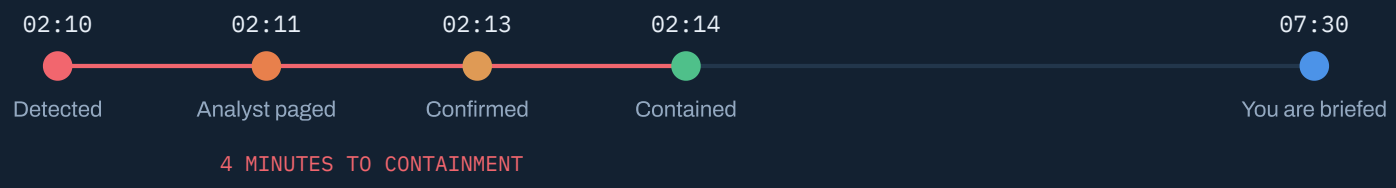
What happened. A process running as a service account tried to read the memory of the Windows component that holds every password used on that server. Nothing legitimate on a domain controller does this. It is the step an attacker takes after getting a foothold and before moving to the rest of the network.

What it means. Treat the service account as compromised. If this had succeeded, the credentials it recovered would have opened every server in the district.

● CONTAINED 02:14 — host isolated from the network, process terminated, 4 min after detection

From detection to containment

THE SAME NIGHT, WHILE THE DISTRICT SLEPT



4 MINUTES TO CONTAINMENT

The seven things that get you a phone call at 3am

SHORT ON PURPOSE

1. Something is actively destroying your files, and we have stopped it.
2. Malware got past your antivirus and ran.
3. Security software was switched off, and we did not do it.
4. A Windows security log was erased.
5. Two or more computers stopped reporting at the same time.

Everything below is the service, not an upgrade.

24/7 monitored endpoints

Workstations, servers and domain controllers watched around the clock for the behaviour that precedes a breach, not just for malware someone already catalogued.

Network sensor

Traffic in and out of the district inspected continuously, including devices that can never run security software: printers, cameras, building systems.

Remote containment

Isolate a machine, end a process, block an address, quarantine a file. Every action logged and attributed to a named analyst.

Digital forensics

Evidence collected remotely — what ran, when, under which account — without taking the computer away from a teacher.

Antivirus health, managed

We configure and monitor the protection built into Windows, add a second engine for deep scans, and alert when it is switched off or goes stale.

Decoy systems

Systems no legitimate user has any reason to touch. Anyone who does has announced themselves — often the earliest warning available.

Reporting for leadership

A monthly summary a superintendent reads in five minutes, and incident reports written for the board or the insurer.

Tamper-evident records

Every alert, decision and action written to a sealed audit trail that cannot be quietly edited afterwards.

What it takes to start

DEPLOYMENT

ENDPOINTS	One signed installer per Windows machine, pushed with whatever management tool you already use. Nothing to install on Chromebooks.
NETWORK	A single sensor at your internet edge. No rack of equipment, no change to how staff work.
YOUR TEAM	Keeps running the district's technology. We watch, investigate and contain alongside them.

Start with a conversation, not a demo.

Fifteen minutes tells us both whether this fits your district. We will ask what you run today and what your insurer has started asking for. Blue Ridge IT Solutions is local — you will deal with the same people every time.

Blue Ridge IT Solutions
Church Hill, Tennessee

(423) 292-1922
blueridge-us.com