

Critical alerts are read within 11 minutes; the warehouse network is still unwatched

Since the night shift started in May, the time to read a critical alert has fallen from **46 minutes to 11**. Coverage reached 96% of servers. The warehouse control network, where an outage costs most, has sensors on 16 of its 38 systems.

Prepared for
Meridian Freight

Service
Managed detection and response

Period
July to September 2026

Time to read a critical alert

11 min
▼ 35 min since January

Servers with a sensor

96 %
▲ 15 points since June

Alerts read by an analyst

1,293
9 escalated to you

Incidents

2
both contained within
six hours

The night shift cut the wait for a critical alert by three quarters

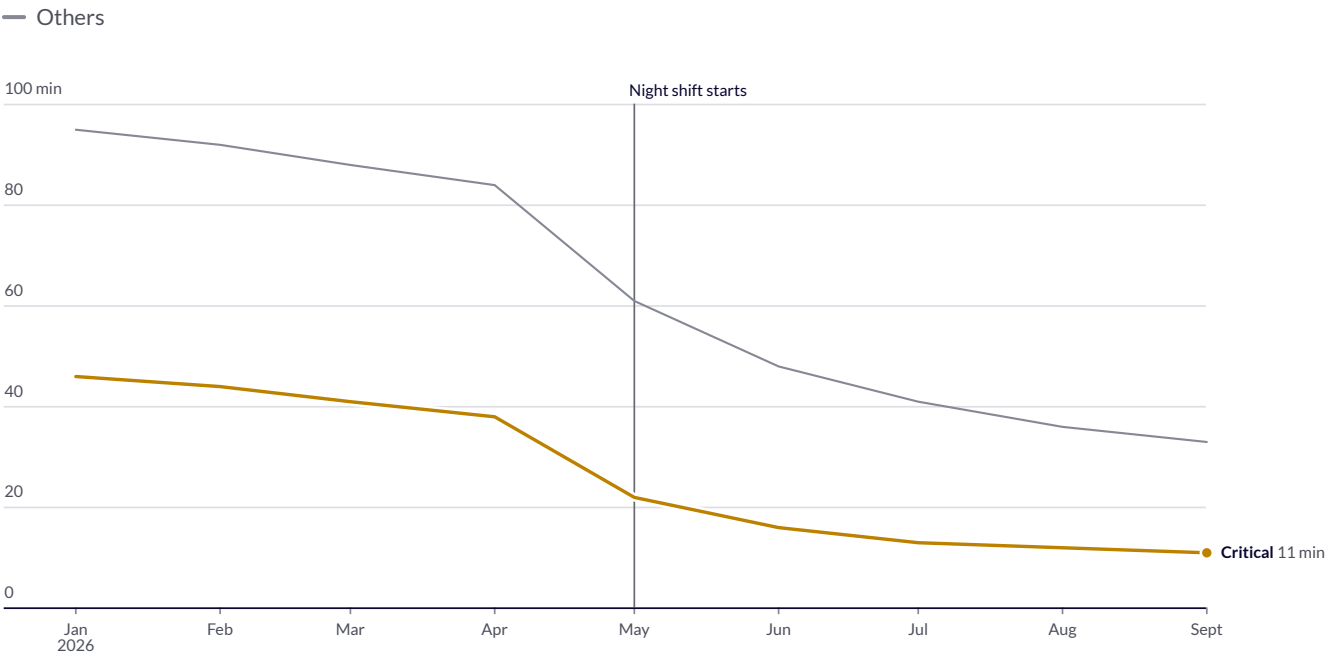
Until May, an alert that fired after 18:00 waited for the morning. Since then an analyst is on shift around the clock, and the median wait has fallen every month. High-severity alerts followed the same curve at a slower pace, because critical ones are read first.

How we count

From the moment an alert is raised to the moment an analyst opens it.
Median of all alerts of that severity in the month.

Critical alerts are read within 11 minutes, down from 46

Median minutes from alert to first read, by severity, 2026



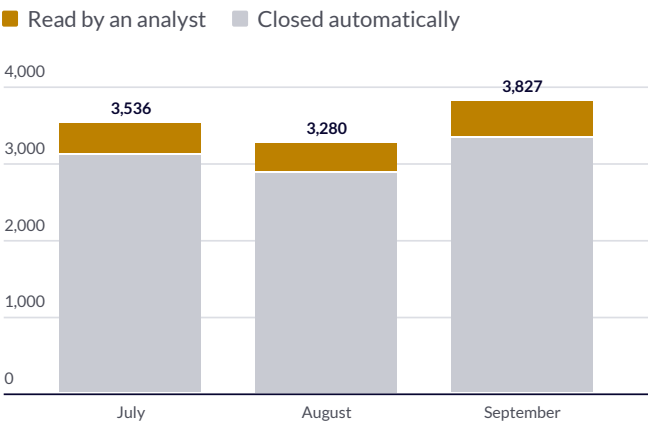
Source: detection platform, January to September 2026. Target for critical alerts: 15 minutes.

Nine in ten alerts close without a person, and four in ten of the rest arrive after hours

The platform raised 10,643 alerts in the quarter. Automation closed 9,350 of them. Analysts read the other 1,293 and escalated nine to your team.

The share that needs a person is steady at about 12%

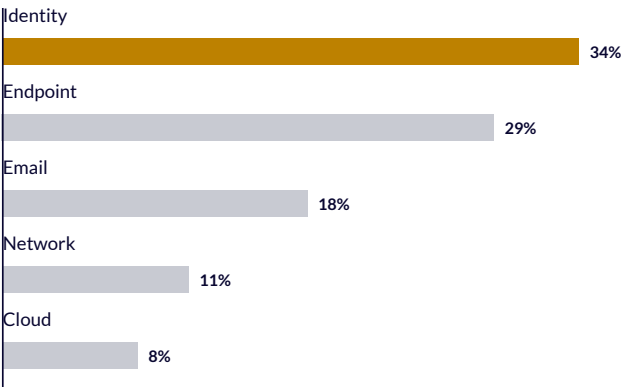
Alerts by month and outcome



Source: detection platform.

Identity is the largest source of alerts an analyst reads

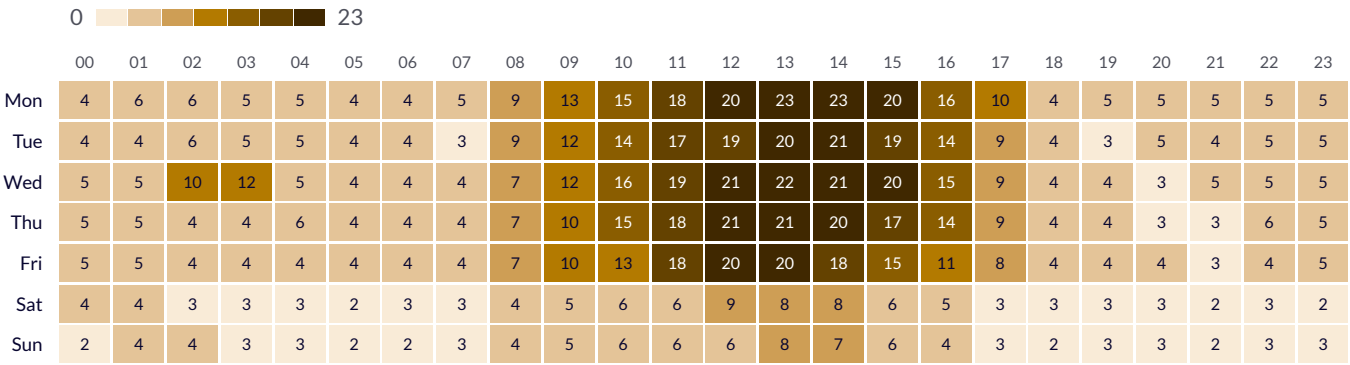
Alerts read by an analyst, by source, %



Source: 1,293 alerts, July to September 2026.

Weekday afternoons are busiest, and nights are never empty

Alerts read by an analyst, by weekday and hour of the day (UTC), July to September 2026



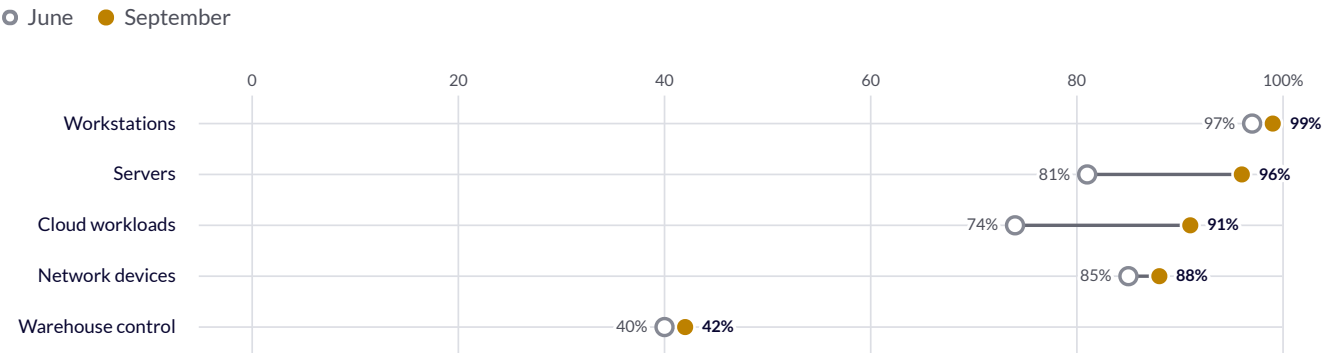
Source: detection platform. 40% arrived outside 08:00 to 18:00 on weekdays. The cluster on Wednesday night is a weekly maintenance job.

Coverage rose everywhere except the warehouse control network

A system without a sensor cannot raise an alert. Cloud workloads gained most this quarter, after the deployment was added to the build pipeline. The warehouse control network did not move: 22 of its 38 systems run software the sensor does not support.

Warehouse control is the only group below 85%

Systems with a working sensor, % of the group, June and September 2026



Source: asset inventory and sensor check-ins, 30 June and 30 September 2026.

Coverage by group, 30 September 2026

Group	Systems	With a sensor	Status
Workstations	2,310	99%	● On target
Servers	412	96%	● On target
Cloud workloads	184	91%	● On target
Network devices	126	88%	▲ Logs only
Warehouse control	38	42%	◆ At risk
All systems	3,070	97%	

Two incidents, both contained the same night

Nine alerts were escalated. Seven were confirmed as harmless within the hour. Two were incidents.

3 Aug

Commodity malware on a contractor laptop

Blocked on execution and isolated 40 minutes after the alert. No other system involved.

16 Sep

An intruder reached the domain controller

First alert at 01:50, read in four minutes; accounts disabled by 07:20. See incident report IR-2026-031.

Three ways to watch the warehouse network

Passive network sensor

Listens at the two switches that carry all control traffic. Covers all 38 systems, changes none of them. Four weeks.

Upgrade the 22 systems

Makes them fit for the standard sensor. Needs two maintenance windows per warehouse; realistic by June.

Logs from the jump host only

A week of work. Shows who connected, not what they did.

Recommendation

Install the passive sensor in November, then upgrade at the pace the warehouses allow

It is the only option that covers every control system this year without touching one.

Method

An alert counts as read when an analyst opens it. Coverage is the share of systems in the asset inventory whose sensor checked in during the last seven days of the quarter. Times are UTC.

Hunt & Hackett, 8 October 2026. An example review: Meridian Freight and every figure in it are invented.