Executive summary · October 2026

Monthly cybersecurity report

Professional services firm · Two offices in Québec

One new account with access to shared project files was outside the policy requiring multifactor authentication. A laptop stopped reporting, leaving its current protection unknown.

October 1–31 · Québec time · Issued November 2, 2026

October at a glance

6 / 6
Endpoint detections reviewed
One file quarantined

47 / 48
Workstations reporting
One laptop last seen Oct 19

51 / 52
User accounts covered by MFA policy
Includes all 3 administrators

Client decision · Due November 3

Close the sign-in gap for the new user.

The client IT lead should approve adding the user to the existing multifactor authentication (MFA) policy. If enrollment cannot be completed by November 3, decide whether to suspend interactive sign-in until the user is ready.

What changed this month

Endpoint alert	One reporting workstation quarantined a potentially unwanted installer. DITC checked the record and a follow-up scan. The reviewed evidence supported closing the alert on that workstation.
Patch exposure	44 of 48 workstations met the agreed patch target, up from 41 of the same 48 in September. Three known exceptions and one unknown remain. The unknown is the laptop that stopped reporting.

What this example covers

DITC reviews endpoint detections during agreed hours and checks workstation patch and identity policy records. Client IT owns account changes. Mailbox content, cloud workloads and a full incident investigation are outside this review.

Alert review · October 2026

Why we closed the alert

An endpoint protection alert on October 14 led to a file quarantine. The workstation continued reporting for the rest of the month. The offline laptop is a different device.

Disposition of the six endpoint detections

4 Approved administration · 1 Verified updater · 1 Quarantined installer

Five detections matched approved activity. One identified potentially unwanted software and led to quarantine. No incident was confirmed among the six records reviewed.

From detection to closure

Date and time	Evidence and analyst judgment
OCT 14 09:12	**The sensor quarantined the file.** The CrowdStrike event identified one installer on one workstation. The action record showed a completed quarantine.
OCT 14 09:37	**DITC checked the surrounding activity.** The reviewed process events showed the download. DITC found no recorded launch of the installer on that workstation.
OCT 14 10:26	**The follow-up scan completed.** The scan recorded no additional detection. DITC confirmed the sensor was reporting and closed the alert with the event, quarantine and scan records.
OCT 31 Month-end	**DITC checked for recurrence.** The workstation continued to report. No matching detection reappeared in its available records through the reporting cutoff.

When to reopen the case

A matching detection on another device, evidence that the installer ran, or a failed quarantine would trigger a new review and notification to the client security lead. The conclusion above applies to the records reviewed on this workstation.

Action register · October 2026

Three open security actions

The earliest decision concerns one user account. The other two actions address missing visibility and overdue patches. Each owner has a due date and evidence to record before closure.

Owner and target date	Action and closure evidence
NOV 03 Client IT lead	**Protect one enabled standard account** Apply the approved MFA policy and verify a sign-in that satisfies it. If access is suspended instead, record the block and keep enrollment open until protection is verified.
NOV 04 Client site lead	**Locate the laptop last seen October 19** Confirm who holds the device. DITC verifies a fresh sensor check-in and patch scan after reconnection. If it remains unaccounted for, notify the client security lead that day and keep the case open.
NOV 06 DITC endpoint lead	**Resolve the three known patch exceptions** Coordinate two restarts. Test the deferred update with the application owner before deployment. Close each exception after a fresh scan shows the device meets the patch target.

Month-end evidence

How to read the coverage figures

Endpoint visibility	CrowdStrike check-ins matched to the NinjaOne inventory. A device counts as reporting if it checked in within 24 hours of October 31 at 23:59, Québec time. The offline device stays in the total of 48.
Identity coverage	Effective Microsoft Entra ID sign-in policies matched to 52 enabled human accounts. All three administrator accounts were covered. Guest and service identities are outside this count.
Patch target	A NinjaOne scan within 24 hours and no approved OS security patch outstanding for more than 14 days. The offline laptop’s patch status is unknown.

November 9 follow-up

DITC and the client IT lead will review the three actions. Record any suspended account or retired device separately so a change in the denominator is visible. Carry outstanding items forward with the owner and a revised date.