

A steady quarter, with improved visibility across our security operations.

During July to September 2026, security activity remained within expected levels for an environment of our size, with no confirmed compromises or material findings.

This quarter, we also gained direct access to live reporting from our Security Operations Centre (SOC) and completed our first formal operational review with Triskele Labs.

Alongside these operational improvements, we've continued progressing our security and assurance programme, with the next assessment and governance activities scheduled for November and December 2026.

0 confirmed

COMPROMISES

Across approximately 230 million analysed log events.

6 items

ESCALATED

Six security tickets referred to the youX team during the quarter, with no material findings.

Live

SOC REPORTING

Direct access to security monitoring dashboards, available to youX 24 hours a day, seven days a week.

Key outcomes · July — September 2026

The quarter was characterised by stable security operations, improved reporting visibility and continued progress against our planned assurance activities.

No material findings

NORMAL

Six security tickets were escalated to the youX team during the quarter. None resulted in a confirmed compromise or material finding.

One vulnerability reported through an external source was confirmed and remediated with support from our SOC partner.

Live SOC reporting implemented

NEW

youX now has direct access to Triskele Labs' reporting platform, providing live visibility of security service statistics and trends.

This gives our team access to current monitoring information throughout the quarter, rather than relying solely on periodic reporting.

First operational review completed

DELIVERED

Our first formal operational review with Triskele Labs was completed on 24 August 2026.

The review covered detection and response performance, including operational statistics, observations and recommendations.

These reviews will now take place quarterly as part of our ongoing security governance.

Assurance roadmap progressing

ON TRACK

The next assessment and governance activities are scheduled for November and December 2026.

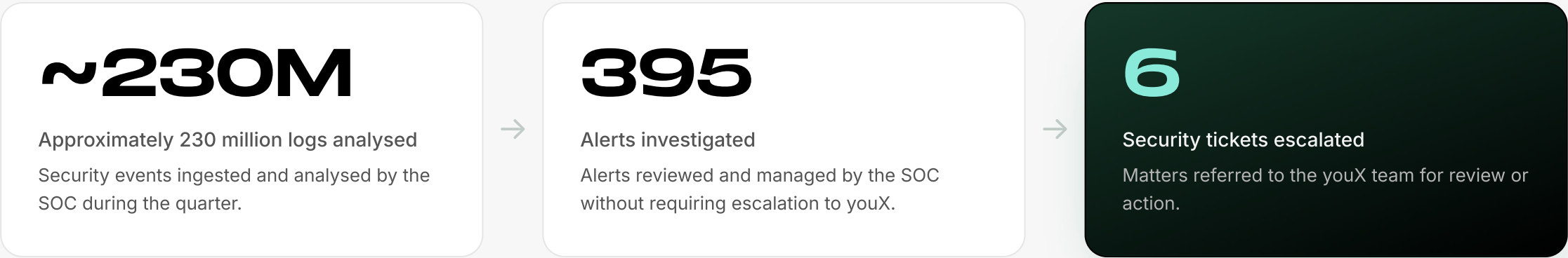
While the sequencing has moved by approximately one month since our previous update, the activities remain within the agreed Year 1 delivery period.

Monitoring activity · Q1 FY27

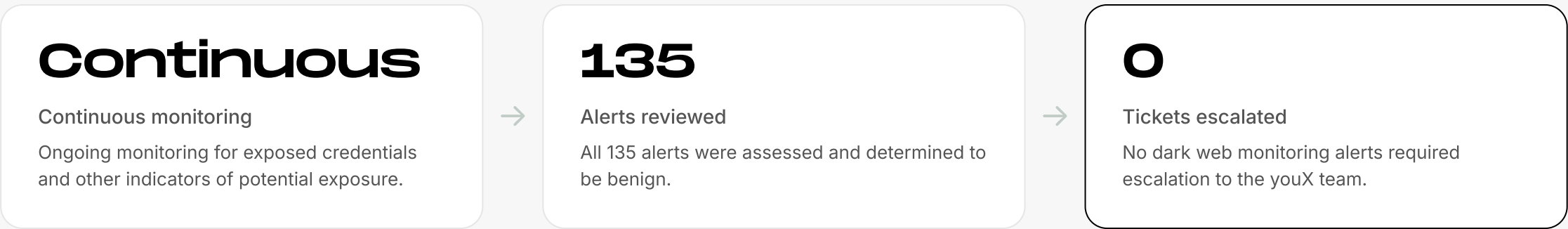
Our Security Operations Centre operates continuously, monitoring security activity, investigating alerts and escalating matters that require action from the youX team.

The results below summarise monitoring activity between July and September 2026.

SECURITY MONITORING · SIEM AND EDR



DARK WEB MONITORING



MONITORING OUTCOME

Of approximately 230 million log events analysed during the quarter, six matters were escalated to the youX team.

This level of activity was within expected operating levels for an environment of our size.

There were no confirmed compromises or material findings, and none of the escalated matters identified a specific area of weakness.

QUARTERLY RESULT

6

ESCALATIONS · 0 MATERIAL FINDINGS

External threat assessment · Triskele Labs

As part of our ongoing security monitoring, Triskele Labs provides an assessment of the threats currently affecting Australian organisations with a similar size and operating profile to youX.

The following assessment reflects the broader threat environment. It does not indicate that these threats have been detected within the youX environment.

THREAT CONDITION	CURRENT ACTIVITY	ACTIVITY LEVEL	RECOMMENDED CONTROLS
AI-driven threats	Attackers are increasingly using AI tools to identify vulnerabilities, develop exploits and create more targeted scams at scale.	HIGH	Detection and response capabilities that adapt to emerging threats, supported by appropriate governance of internal AI use.
Credential attacks	Information-stealing malware and exposed credential databases continue to enable unauthorised access using legitimate login details.	HIGH	Multi-factor authentication across staff and broker access, supported by credential exposure monitoring.
Zero-day vulnerabilities	Faster vulnerability discovery is reducing the time available to identify and remediate weaknesses before exploitation, particularly in internet-facing systems.	HIGH	Timely patching of critical systems, supported by continuous monitoring.
Ransomware and extortion	Threat groups continue to use data theft and extortion, including attacks that do not involve encrypting systems.	HIGH	Tested offline backups, endpoint detection and response, and secure remote access.
Phishing	AI-generated phishing attempts are becoming more convincing, with voice and SMS-based attacks increasing alongside email-based threats.	HIGH	Email security controls, staff awareness and regular testing.
Business email compromise	Compromised email conversations and synthetic voice technology are being used to make fraudulent payment requests appear legitimate.	HIGH	Independent payment verification and dual approval for changes to payment instructions.
Malicious insiders	The misuse of legitimate access by employees or contractors remains a risk, particularly where permissions exceed operational requirements.	ELEVATED	Least-privilege access and regular reviews of privileged accounts.



TRISKELE LABS ASSESSMENT

Fundamental monitoring is in place, supporting defence against the majority of common threats today. All six services operated continuously through the quarter. The roadmap ahead builds the fuller picture — assessing governance, assurance and a tested response, and maturing them where needed.

SOURCE: TRISKELE LABS · YOUX MANAGED DETECTION & RESPONSE BOARD REVIEW · OCTOBER 2026

Security services in operation

youX maintains six managed security services through Triskele Labs’ Australian sovereign Security Operations Centre.

These services operate 24 hours a day, 365 days a year, and all six remained operational throughout the reporting period without interruption or change.

24/7/365 MONITORING

Security information and event management (SIEM)

Continuous monitoring and investigation of security events, including suspicious authentication activity, potential intrusions and lateral movement.

ENDPOINT PROTECTION

Managed endpoint detection and response (EDR)

Monitoring and protection of laptops and servers against malware, ransomware and other endpoint-based threats.

VULNERABILITY MANAGEMENT

Internal and external vulnerability scanning

Scanning to identify potential weaknesses, including unpatched software and system misconfigurations.

TIER 1 RESPONSE

SOC-led response and automation

SOC-approved response actions designed to contain identified threats, including endpoint isolation and account restrictions where required.

EXPOSURE MONITORING

Dark web monitoring

Ongoing monitoring for exposed credentials, leaked information and potential misuse of the youX brand.

25-HOUR RETAINER

Incident response retainer and DFIR tooling

Access to incident response support and digital forensics and incident response (DFIR) tooling to assist with investigation, containment and recovery if required.

SUPPORTING SECURITY CONTROLS

ACCESS MANAGEMENT

Restricted administrative access, least-privilege reviews, credential rotation and secrets management.

INFRASTRUCTURE SECURITY

Private network architecture, segmented environments, controlled access through bastion hosts and encryption in transit, at rest and at the application level.

DATA MANAGEMENT

Defined processes covering data collection, encryption, retention, archiving and deletion. Retention requirements are mapped by data category and subject to board-level oversight.

Progress against our planned programme

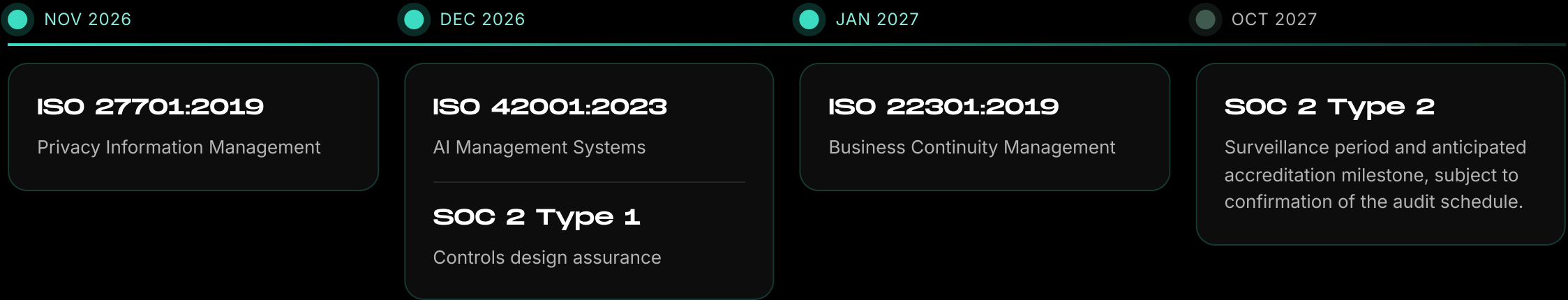
In June 2026, youX secured three ISO certifications.

Our next phase of work builds on these certifications, with further activities planned across privacy management, AI governance, business continuity and SOC 2 assurance.

In parallel, we’re working with Triskele Labs on a structured security maturity programme. This includes assessing our current controls, identifying areas for improvement, testing our security measures and formalising our incident response arrangements.

The objective is to establish a measured baseline, prioritise improvements and validate the effectiveness of our security controls over time.

PLANNED ACCREDITATION MILESTONES



The following activities form part of our agreed programme with Triskele Labs.

Assess & govern

Cyber Maturity Assessment

An independent assessment of our current security maturity and control environment.

Target: November–December 2026

36-month Prioritisation Roadmap

A structured plan identifying recommended improvements and their delivery sequence.

Target: December 2026

Cyber Health Check Scorecard

A recurring assessment to measure security maturity and track progress against agreed priorities.

Frequency: Quarterly, commencing January 2027

Test & assure

Penetration testing · 6 days

Independent testing designed to identify exploitable weaknesses in our systems and controls.

Frequency: Quarterly

User MFA review · VPN

Review of multi-factor authentication controls for remote access.

Frequency: Quarterly

Microsoft 365 Essentials review

Assessment of core Microsoft 365 security settings and configurations.

Frequency: Twice yearly, commencing February 2027

Threat hunting

Proactive investigation to identify potential threats that may not be detected through automated monitoring.

Target: January 2028

Prepare & respond

Incident Response Plan

Development of a documented incident response plan, including responsibilities, escalation procedures and response requirements.

Target: January 2027

Incident response tabletop exercise

A facilitated exercise to test incident response procedures, decision-making and team readiness.

Target: January 2027

Data and privacy review

Review of relevant legal, regulatory and privacy obligations.

Target: January 2027

Controls already in place

Our incident response retainer and DFIR tooling are already operational.

The planned Incident Response Plan and tabletop exercise will build on these existing capabilities by formalising procedures and testing how they operate in practice.

PROGRAMME TIMING

The dates above are indicative and may change as delivery is coordinated between youX and Triskele Labs.

Since our previous quarterly update, the assessment and governance activities have moved by approximately one month.

These activities remain scheduled for completion within the agreed Year 1 programme.

We will continue to report on progress and identify any material changes to scope or timing in subsequent updates.

What our partners can expect from youX

Our approach to security is based on maintaining effective controls, regularly assessing their performance and addressing identified risks as the platform evolves.

For our partners, this means continued investment in the systems, processes and oversight that support a secure and reliable operating environment.

Security throughout development

We continue to improve the youX platform while maintaining security as a core consideration in how changes are designed, developed and delivered.

Continued infrastructure investment

We remain focused on investing in Australian-hosted infrastructure, layered encryption and monitoring capabilities that support the ongoing protection of our systems and data.

Regular reporting

We will continue providing quarterly updates covering our security operations, progress against planned activities and any material changes affecting our security and assurance programme.

Direct accountability

Our leadership team remains accessible to partners who have questions about our security approach, operational controls or planned activities.

We believe direct communication and transparency are important parts of maintaining confidence in our platform.



A NOTE FROM OUR CEO

"Security is an ongoing responsibility, and we take it seriously.

This quarter, our monitoring operated as expected, with no confirmed compromises or material findings. We've improved our visibility through live SOC reporting, completed our first formal operational review and continued progressing the next stage of our assurance programme.

For our partners, our commitment remains the same: we'll do what we say we're going to do, measure the results and be transparent about our progress. Where we identify opportunities to improve, we'll act on them.

That's how we intend to keep building confidence in youX."

Simon Penhaligon

CHIEF EXECUTIVE OFFICER

NEXT UPDATE

January 2027

ISSUED BY

Drive IQ Technology Pty Ltd T/A youX Powered
ABN 40 638 678 136 · Sydney, Australia