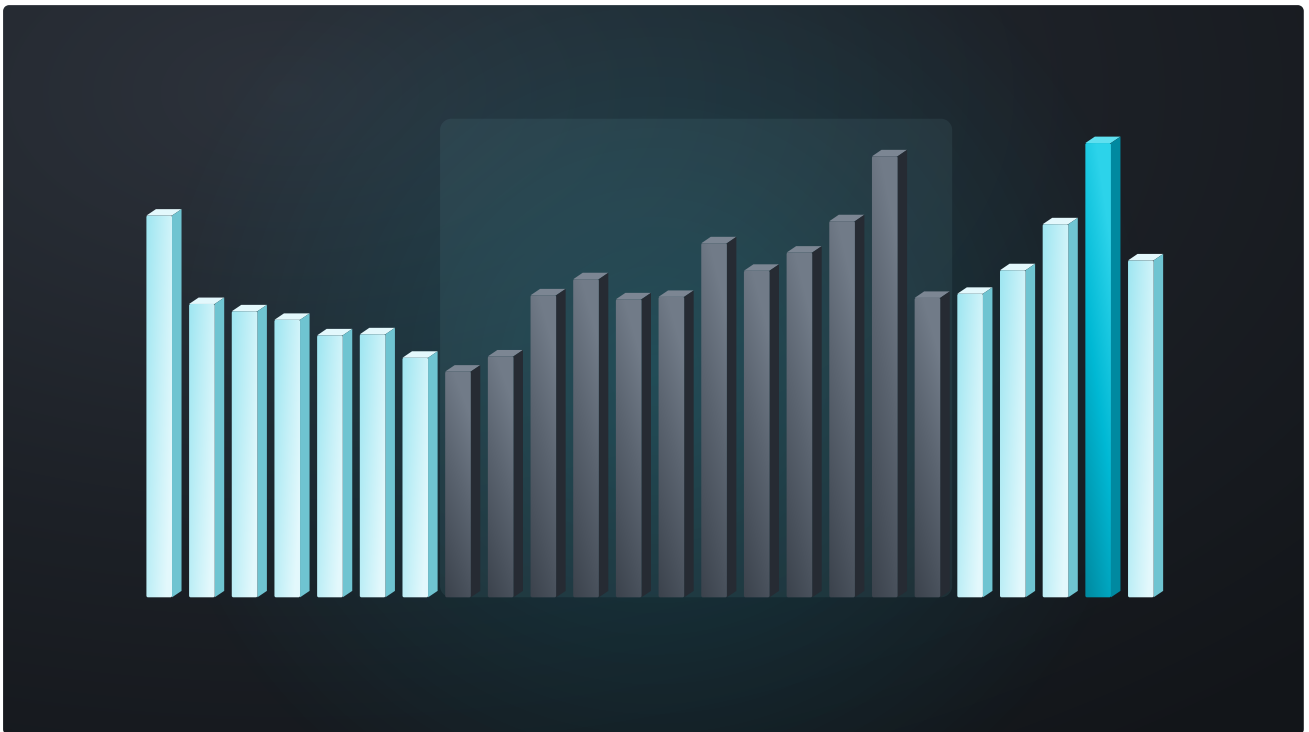




What our first 430 million security events look like

Half of what our security monitoring reads arrives outside business hours. A small firm's defences have to act when nobody is watching, and they need the logs that show what an attacker does once inside.



Entity Black Shard Pty Ltd · ABN 66 696 910 773

Document ID BS-RPT-02

Classification Public

Version 1.1

Published 26 October 2026

Figures Measured 26 Oct 2026, 00:45 AEST

Executive summary

Our security monitoring analysed its first 430 million security events from 1 October to 26 October 2026, counted at 00:45 AEST. 420,450,384 events in the 24 full days from 2 to 25 October 2026, an average of 17,518,766 a day and more than 200 every second.

The stream is the record of what happens on every machine: which programs ran, which files they touched, who raised their privileges, what scripts executed, which domains were looked up, and who signed in from where. Most of it is routine. The line that matters is in there with the rest, and rules find it, because no person can read a stream this size.

49.8 per cent of events arrived outside 07:00 to 19:00 AEST, and 50.2 per cent inside it. The busiest hour was 22:00 to 23:00 AEST, with 5.96 per cent of a day's events; the quietest was 07:00 to 08:00, with 2.96 per cent.

The stream does not keep office hours, and neither do the people who attack small firms. A business that only looks at its security during the working day is looking at half of what happens to it.

- Collect the logs that show what an attacker does after the first sign-in: process starts, PowerShell, privilege use and sign-ins.
- Let detection act at night without waiting for a person, on a short list of high-confidence threats, with every action reversible.
- Keep a phone number that is staffed when the alert fires.

Method

Every event counted here was received, decoded and checked against detection rules by our central security monitoring. The archive keeps each event whether or not a rule fired on it, so an investigation can go back over what happened before anyone knew to look.

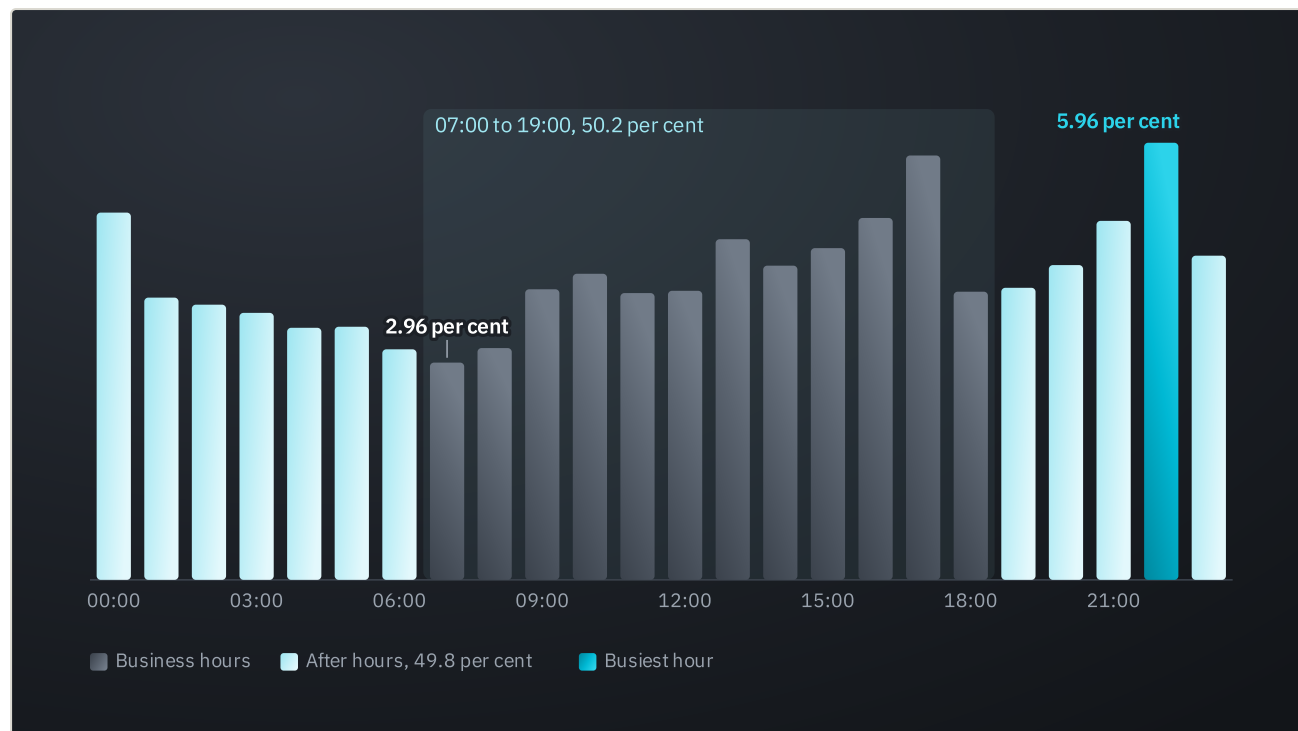
The headline is the figure our running tally measured at 00:45 AEST on 26 October 2026, counting from the first archived day, 1 October. Our security monitoring analysed its first 430 million security events from 1 October to 26 October 2026, counted at 00:45 AEST.

The pattern figures cover every full day from 2 to 25 October 2026 in Australian Eastern Standard Time, so every hour of the day is counted the same number of times. We ran read-only aggregations over the archive on 26 October 2026: a count by hour of the day and a count by day. Events recovered later from backlog are left out, as the tally leaves them out.

No client is named. We print no count of devices, servers or users, no breakdown by source, and no count of alerts: an alert count measures how a rule set is tuned more than what happened.

When the events arrive

EVENTS BY HOUR OF THE DAY, AEST



Half of all events arrived outside 07:00 to 19:00, and the busiest hour was 22:00. Source: Our security monitoring, 2 to 25 October 2026 AEST.

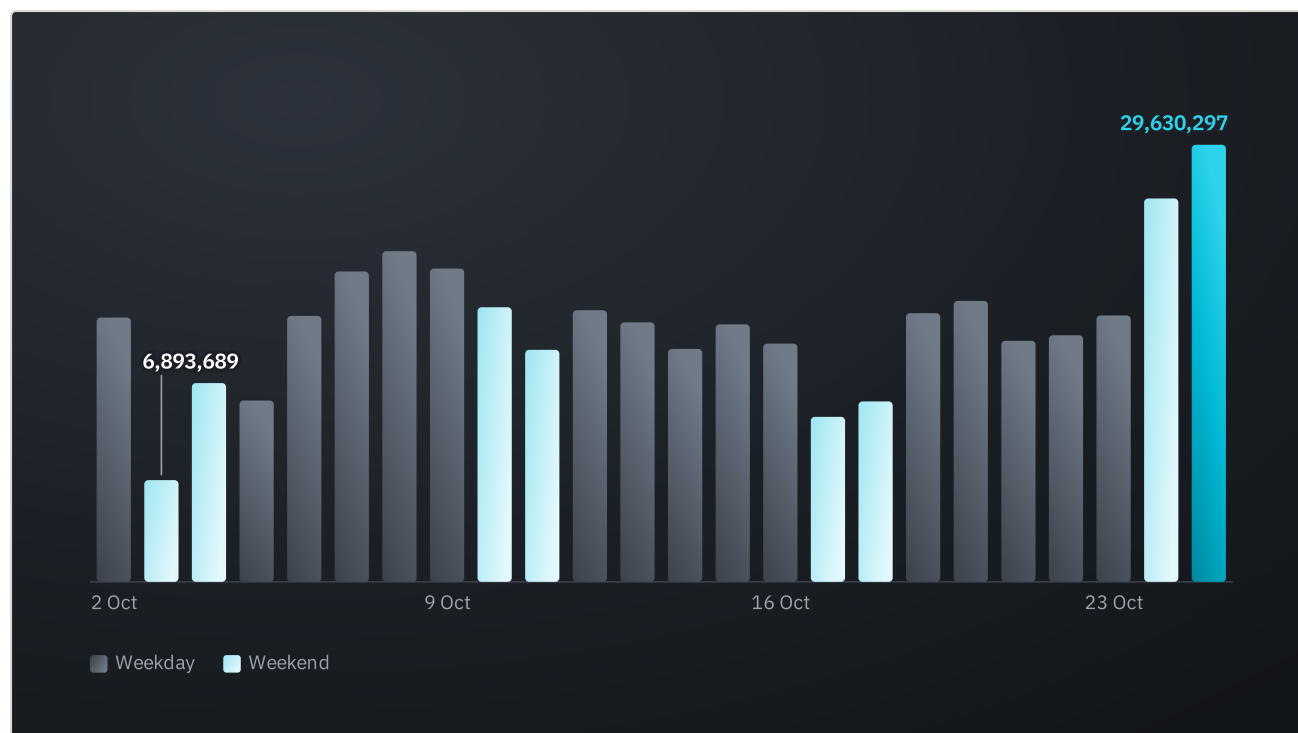
49.8 per cent of events arrived outside 07:00 to 19:00 AEST, and 50.2 per cent inside it. The busiest hour was 22:00 to 23:00 AEST, with 5.96 per cent of a day's events; the quietest was 07:00 to 08:00, with 2.96 per cent.

Machines work through the night: scheduled jobs, builds, backups, updates and the automation that runs a modern business all write to the logs while the office is empty. The stream is never quiet enough for a change to stand out on its own, which is why detection has to be written as rules and run by software.

Attackers know the hours as well. Ransomware crews stage their work at night and over weekends because nobody is watching, and a mailbox taken over on a Friday evening can be read all weekend before anyone notices. The hours a small firm is closed are the hours its defences have to act alone.

Day by day

EVENTS BY DAY, 2 TO 25 OCTOBER 2026



A weekend day carried nearly as many events as a weekday. Source: Our security monitoring, 2 to 25 October 2026 AEST.

The busiest day carried 29,630,297 events and the quietest 6,893,689; a weekend day averaged 16,717,860 against 17,919,218 on a weekday.

Volume rises with the work the estate does: a day of releases, migrations or a large backup writes more than a quiet one. Weekends carried nearly the load of a weekday, which is the point for a buyer: there is no day of the week when nothing happens.

What to collect

The sources that matter most are the ones that record what happens on a machine after someone is in: which programs ran, which files they touched, who raised their privileges and what scripts executed. They are the sources an attacker cannot avoid writing to once inside, and the ones most small firms never collect.

PowerShell is the tool attackers use most once they are on a Windows machine, because it is already installed and trusted. Its script block and module logging record the commands themselves, which is why it is worth keeping. Most small firms leave it switched off, and lose the record of what was run.

The Security log carries sign-ins, privilege use and process creation. WMI activity records the management interface that attackers use to move between machines and to persist. Together they let an investigator rebuild the order of events after the fact, which is the question every incident ends on.

DNS queries are small and cheap to keep, and they answer a question nothing else does: which machine looked up the attacker's domain, and when. Sign-in logs from the cloud platforms carry the account takeovers. The smallest sources by volume are among the most useful per event: a sign-in from a new place, a new administrator, a changed

system file or a configuration that drifted from its baseline is a single line in a stream of hundreds of millions, and it is often the line that matters.

From event to response

Events become action in four steps. Every event is decoded and checked against detection rules as it arrives. A rule that fires raises an alert with the evidence attached. Alerts that meet a threshold go to the people who act on them on our own estate. And every event stays in the archive, so an investigation can go back over what happened before anyone knew to look.

- Central security monitoring of every system we run, with immutable log retention.
- Phishing-resistant multi-factor authentication on every account, with just-in-time administrative access.
- Application control and attack surface reduction enforced on managed devices.
- Immutable off-site backups, restore-tested every day.

Clients reach us on the 24/7 incident line: 1800 370 270. A call to the line rings through to our response team, and a call that is not picked up goes to voicemail and is returned.

Jetstone, our cyber defence software for Australian businesses, is designed to bring the same model to a firm with a handful of devices: the telemetry collected on the device, detection rules mapped to known attacker techniques, and a response that will act on its own against a published list of high-confidence threats, with every action undoable.

What to do

1. Switch on PowerShell script block and module logging, process creation auditing and command-line capture on every Windows machine.
2. Send sign-in logs from Microsoft 365 or Google Workspace somewhere they are kept for at least as long as an investigation needs.
3. Keep DNS query logs: they are small, and they show which machine reached an attacker's server.
4. Write the short list of threats you would want stopped in the middle of the night without a phone call, and set your tools to act on those alone.
5. Make every automatic action reversible, so the fear of a false alarm never stops you turning protection on.
6. Check every day that each machine is still sending its logs. A silent machine is the one an attacker has switched off.
7. Keep a number to call when an alert fires out of hours, and test that it answers.

Our record

Black Shard builds and defends the systems Australian organisations run on. Every figure here comes from the monitoring we run on our own estate.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027, on the CyberCert register.
- Essential Eight Maturity Level 3, assessed September 2026.

- Pre-qualified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Our CISO is an Exemplar Global Certified Lead Auditor for ISO/IEC 27001:2022.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 1 January 2026.

24/7 incident line: 1800 370 270. The evidence behind each line goes out on request to info@blackshard.com.au.

Sources

- Our security monitoring: the event archive, read-only aggregations run 26 October 2026
- The running tally of our scale figures, measured 26 October 2026 at 00:45 AEST