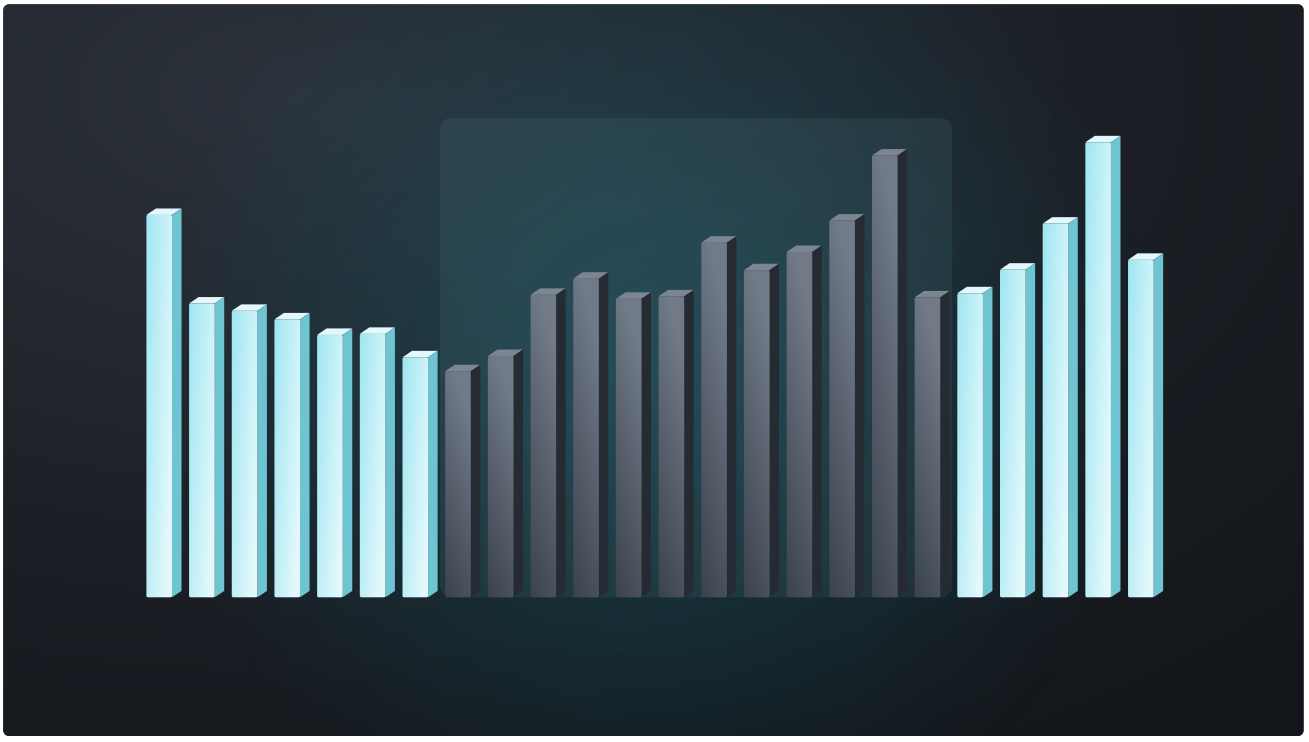
Black Shard

RESEARCH REPORT

Security events by hour: what our monitoring sees

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	1.4
First published	26 October 2026
This edition	29 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.

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.

Over the full days 2 to 25 October 2026, 49.8 per cent of events arrived outside 07:00 to 19:00 AEST, and 50.2 per cent inside it.

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.

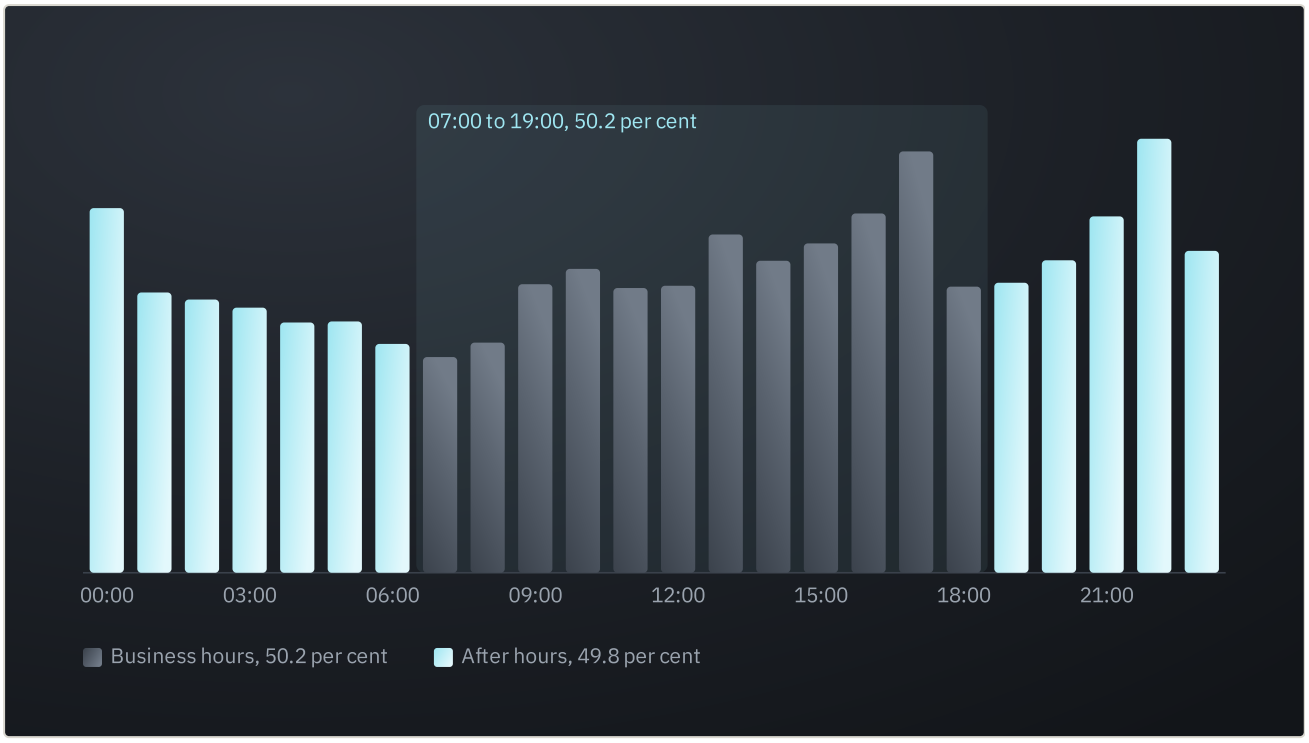
- Collect the logs that show what an attacker does after the first sign-in: process starts, PowerShell, privilege use and sign-ins.
- Let detection act at night without waiting for a person, on a short list of high-confidence threats, with every action reversible.
- Keep a phone number that is staffed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

Method

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 the 24 full days from 2 to 25 October 2026, in Australian Eastern Standard Time. Every hour of the day is counted the same number of times.

When the events arrive

EVENTS BY HOUR OF THE DAY, AEST



Half of all events arrived outside 07:00 to 19:00. Source: Our security monitoring, 2 to 25 October 2026 AEST.

Over the full days 2 to 25 October 2026, 49.8 per cent of events arrived outside 07:00 to 19:00 AEST, and 50.2 per cent inside it.

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.

Weekends carried nearly the load of a weekday: there is no day of the week when nothing happens.

Measure it on your own estate

The after-hours share is a figure any firm can read from its own logs. Count the events your sign-in, endpoint and mail logs record in each hour of the day across a fortnight, then add up the hours outside 07:00 to 19:00.

A share near half means the business runs, and can be attacked, through the night. A share well below it usually means some sources stop logging when the office closes. Find that gap before an incident needs those hours.

SOURCE	WHAT TO COUNT EACH HOUR	THE QUESTION FOR THE NIGHT
Sign-ins, in Microsoft 365 or Google Workspace	Successful and failed sign-ins	Who signs in at 02:00, and from where?

SOURCE	WHAT TO COUNT EACH HOUR	THE QUESTION FOR THE NIGHT
Laptops and servers	Process starts and blocked actions	Which machines work through the night, and why?
Mail	Inbox rules created and messages sent	Does a new rule or a send at 23:00 raise an alert?
Backups and scheduled jobs	Job starts and failures	Does a failure at night reach anyone before morning?

A worksheet for a fortnight of your own logs.

Then follow one alert raised at 02:00 on a Saturday: who sees it, what acts on it before anyone wakes, and where the record of it is kept.

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.

When an alert fires

Clients reach us on the 24/7 incident line: 1800 370 270.

Jetstone, our cyber defence software, is designed for 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.

The record is as held at 29 October 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified 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 holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- 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.

Sources

- Our security monitoring, 26 October 2026
- The running tally of our scale figures, measured 26 October 2026 at 00:45 AEST