BRANDEFENSE COUNTRY REPORT · MALAYSIA 2026

Brandefense Laporan Landskap Ancaman Siber Malaysia 2026

Identiti, kebergantungan pembekal dan dakwaan bawah tanah

Odin by Brandefense
Tempoh penyelidikan: 1 Januari–22 November 2026
Versi 1.0 · Edisi Penyelidikan Awam · TLP:CLEAR · 22 November 2026

250
entri domain organisasi terpilih merentasi 11 sel sektor

8,748–9,196
siaran relevan dalam set bertag Malaysia dikekalkan

87
penyenaraian Malaysia pada laman kebocoran perisian tebusan dalam tempoh pelaporan

35
entri perbankan dan kewangan dalam portfolio terpilih

KANDUNGAN

Kandungan

Translated with AI

Edisi ini diterjemahkan dengan AI daripada teks induk bahasa Inggeris. Jika terdapat perbezaan, edisi bahasa Inggeris diguna pakai.

01	Ringkasan eksekutif	04
	Peta laporan	08
02	Konteks digital dan ancaman di Malaysia	09
03	Pendedahan kebangsaan: portfolio 250 domain terpilih	14
04	Pemerhatian kami di web gelap	23
05	Insiden dan dakwaan mengikut sektor	35
06	Hacktivisme dan DDoS	47
07	Pelaku ancaman	52
08	Ekonomi penipuan	59
09	Penelitian perbankan dan kewangan	66
10	Respons kawal selia dan kebangsaan	71
11	Tinjauan	76
12	Pelan tindakan	81
A	Lampiran A. Skop dan bukti	89
B	Lampiran B. Daftar bukti	92
C	Lampiran C. Sumber	93
D	Lampiran D. Glosari	96
	Tentang laporan ini	98

Lembaga dan eksekutif	01 03 11 12
CISO dan ketua keselamatan	03 05 07 09 10 12
SOC dan perisikan ancaman	04 06 07 08 Lamp. A–B
Penipuan dan perlindungan pelanggan	04 08 09 12
Undang-undang dan komunikasi	05 06 10 12

Tentang edisi ini

Diterjemahkan dengan bantuan AI daripada edisi induk bahasa Inggeris. Jika terdapat perbezaan, edisi bahasa Inggeris diguna pakai.

Analisis dan penggubalan dibantu AI. Laporan membezakan pemerhatian dikekalkan, dakwaan pelaku dan keterangan awam. Edisi bahasa Inggeris ialah teks induk.

BAB 01

Ringkasan eksekutif

01

SOALAN YANG DIJAWAB BAB INI

Bukti manakah perlu ditindaklanjuti dahulu oleh pemimpin?

55 daripada 249

entri dinilai mempunyai kelayakan disenaraikan untuk dijual ketika disemak

1.1 Lima dapatan untuk pemimpin 05

1.2 Empat keputusan untuk pemimpin 06

1.3 Angka tahun ini 06

BAB 01

Ringkasan eksekutif

RINGKASAN

Bukti identiti semasa wajar menerima keputusan pengesahan pertama. Daripada 249 entri portfolio dinilai, 55 mempunyai kelayakan disenaraikan untuk dijual ketika disemak; satu entri terpilih kekal tidak diketahui. Keterangan awam menerangkan sempadan perkhidmatan dan pembekal berbeza. Iklan bawah tanah kekal dakwaan, sementara amaran rasmi terkini membezakan respons bayaran, akaun dan peranti. Tetapkan pemilik identiti, kesinambungan dan penipuan, sahkan bukti berkaitan dan rekodkan perkara yang menutup setiap tindakan.

1.1 Lima dapatan untuk pemimpin

1. Penyenaraian semasa memerlukan pengesahan akaun. Daripada 249 entri dinilai, 55 mempunyai kelayakan disenaraikan untuk dijual ketika disemak pada 22 November. Nilai utama Atlas kebangsaan ialah 48/100. Satu daripada 250 entri terpilih tiada hasil pendedahan boleh digunakan. Ini pemerhatian portfolio, bukan kelaziman kebangsaan atau akses akaun semasa disahkan. [S1][S2]

Populasi dinilai sama mempunyai 485,462 perkaitan peranti yang direkodkan dan 3,686,480 perkaitan rekod kelayakan sejarah. Kedua-dua jumlah bukan bilangan individu atau insiden baharu 2026. Sahkan status akaun, tarikh bukti dan pemilikan peranti sebelum memutuskan respons.

2. Jumlah bawah tanah memerlukan sempadan liputan. Brandefense Blackhole merekodkan 782,224 siaran bertag Malaysia dalam tempoh pelaporan. Bahan tag negara dikekalkan mengandungi 25,355 siaran berbeza, maka laporan tidak menganggap pandangan dikekalkan itu seluruh populasi bertag. Rujukan negara tidak membuktikan penyasaran. [S3]

Pandangan terkini 8–22 November mengandungi 922 siaran bertag, termasuk lapan siaran forum bertag. Pandangan forum berasingan mengandungi 14 siaran; populasi ini bertindih dan tidak ditambah. Jumlah, tarikh dan dakwaan pemilikan diiklankan memerlukan bukti pengukuh berasingan.

3. Penerbitan pemerasan kekal berasingan daripada pengesahan insiden. Ransompedia mengandungi 87 penyenaraian Malaysia bertarikh dalam tempoh, termasuk enam bertarikh 8–22 November. Qilin muncul dalam 18 penyenaraian dan The Gentlemen dalam 12. Label ini menerangkan penerbitan sumber; label tidak membuktikan laluan masuk, akses aktif atau insiden berbeza secara kebangsaan. [S4]

4. Sempadan perkhidmatan dan pembekal menentukan keputusan kesinambungan. Keterangan awam membezakan perkhidmatan terminal terganggu, akses pelaporan kredit dan persoalan fail sokongan. Keterangan itu turut membezakan laman web awam daripada perkhidmatan kewangan. Kekalkan sempadan serta tarikh dinyatakan setiap sumber, kemudian uji kebergantungan perniagaan sebenar dan bukti pemulihannya. [S5][S6][S7][S8]

5. Respons penipuan bergantung pada perkara diserahkan atau dijalankan pengguna. Nasihat MyCERT November menerangkan umpan maklumat bayaran bertema bantuan dan umpan akaun pemesejan komputer riba percuma. Nasihat skrip Jun menerangkan keputusan peranti akhir berbeza. Tentukan tindakan pengguna, kemudian halakan persoalan kad, akaun dan peranti kepada pemilik berkaitan. [S9][S10][S11]

1.2 Empat keputusan untuk pemimpin

1. Berikan setiap penyenaraian kelayakan semasa berkaitan pemilik identiti dan keputusan bertarikh. Sahkan status aktif dan aktiviti pengukuh sebelum mengisytiharkan akses akaun.
2. Uji sandaran disahkan bagi kredit, dagangan, logistik dan kebergantungan luar lain. Tutup latihan dengan transaksi diselaraskan dan keputusan kembali berkhidmat oleh pemilik perniagaan.
3. Pisahkan penerimaan kad bayaran, akaun pemesejan dan peranti akhir. Tentukan maklumat diserahkan dan sama ada fail dijalankan sebelum memilih respons.
4. Petakan kesiapsiagaan pemberitahuan kepada entiti dan aktiviti sebenar. Kekalkan tarikh pengesanan, penilaian dan pemulihan perkhidmatan, serta minta pasukan undang-undang mengesahkan kewajipan terpakai.

1.3 Angka tahun ini

782,224

Siaran Blackhole bertag Malaysia bertarikh dalam tempoh pelaporan

BATAS TAFSIRAN

Bukan insiden kebangsaan atau individu terjejas

25,355

Siaran berbeza dalam pandangan tag negara dikekalkan

BATAS TAFSIRAN

Bukan seluruh populasi bertag

922

Siaran bertag bertarikh 8–22 November

BATAS TAFSIRAN

Bukan organisasi berbeza yang baru terjejas

250

Entri domain organisasi terpilih

BATAS TAFSIRAN

Bukan bancian kebangsaan atau bilangan entiti undang-undang bebas

249

Entri dengan pemerhatian pendedahan Atlas boleh digunakan

BATAS TAFSIRAN

Bukan liputan pendedahan lengkap portfolio terpilih

55 / 249

Entri dinilai dengan penyenaraian kelayakan semasa

BATAS TAFSIRAN

Bukan akaun aktif atau pencerobohan disahkan

48/100

Nilai utama Atlas kebangsaan bagi entri dinilai

BATAS TAFSIRAN

Bukan penarafan sektor atau anggaran kelaziman kebangsaan

485,462

Perkaitan peranti yang direkodkan merentasi entri dinilai

BATAS TAFSIRAN

Bukan individu unik atau peranti baru terjejas

3,686,480

Perkaitan rekod kelayakan sejarah

BATAS TAFSIRAN

Bukan kata laluan aktif unik

199 / 250

Domain terpilih dengan pemerhatian pasif lengkap

BATAS TAFSIRAN

Bukan penilaian kebersihan kebangsaan lengkap

87

Penyenaraian Malaysia Ransompedia dalam tempoh pelaporan

BATAS TAFSIRAN

Bukan insiden disahkan secara bebas

1,244

Kad bayaran berbeza yang dikaitkan dengan Malaysia

BATAS TAFSIRAN

Bukan kecurian kad kebangsaan atau kerugian penipuan

Angka mengekalkan populasi dan tarikh masing-masing. Angka tidak boleh ditambah untuk menghasilkan jumlah insiden atau mangsa kebangsaan. [S3][S1][S12][S4][S13]

DAPATAN UTAMA

01

Sahkan bukti akaun semasa sebelum meningkatkan dakwaan menjadi dapatan insiden.

02

Kekalkan pemilik respons identiti, pembekal, perkhidmatan dan penipuan yang berbeza.

03

Wajibkan bukti penyempurnaan dan kekalkan hasil tidak diketahui dalam rekod lembaga.

Peta laporan

Dua belas bab, lima laluan pembaca. Mulakan dengan soalan sepadan peranan anda, kemudian ikuti bukti kepada pemilik pengesahannya.

Lembaga dan eksekutif	Keputusan manakah wajar menerima sumber dan apakah yang membuktikan penyempurnaan?	Pergi ke 1 3 11 12
CISO dan ketua keselamatan	Bukti manakah milik kami dan respons manakah didahulukan?	Pergi ke 3 5 7 9 10 12
SOC dan perisikan ancaman	Apakah diperhatikan, apakah didakwa dan apakah menyokong hubungan?	Pergi ke 4 6 7 8 Lamp. A–B
Penipuan dan perlindungan pelanggan	Tindakan pengguna manakah menentukan respons bayaran, akaun atau peranti?	Pergi ke 4 8 9 12
Undang-undang dan komunikasi	Sempadan perkhidmatan dan kewajipan pemberitahuan manakah boleh disokong?	Pergi ke 5 6 10 12

Bab	Persoalan dijawab
1 Ringkasan eksekutif	Dapatan dan keputusan manakah penting dahulu
2 Konteks	Kebergantungan identiti, pembekal dan perkhidmatan manakah membentuk bukti
3 Portfolio terpilih	Perkara yang boleh dan tidak boleh dibuktikan oleh 250 pemerhatian domain terpilih
4 Web gelap	Tawaran dan siaran terkini manakah wajar disahkan
5 Sektor	Sempadan dilaporkan manakah penting kepada setiap sektor
6 Hacktivisme dan DDoS	Perkara dibuktikan dakwaan dan cara mengesahkan kesan
7 Pelaku	Hubungan dan pemerhatian penyenaraian manakah disokong
8 Ekonomi penipuan	Cara menghalakan keputusan bayaran, akaun dan peranti akhir
9 Perbankan	Perbezaan sempadan perkhidmatan kewangan dan pelanggan
10 Kawal selia	Entiti, aktiviti, pencetus dan tarikh kuat kuasa manakah terpakai
11 Tinjauan	Senario bersyarat dan petunjuk perubahan manakah perlu dirancang
12 Pelan tindakan	Pihak yang perlu bertindak dan bukti penyempurnaan diperlukan lembaga

BAB 02

Konteks digital dan ancaman di Malaysia

02

SOALAN YANG DIJAWAB BAB INI

Kebergantungan manakah yang menjelaskan insiden dalam laporan ini, dan apakah yang perlu dilindungi bersama oleh organisasi di Malaysia?

4

sempadan berulang: identiti, pembekal, laman web awam dan perkhidmatan operasi

2.1 Ketersambungan isi rumah yang tinggi meluaskan sempadan perkhidmatan 10

2.2 Perkhidmatan boleh gagal di luar organisasi yang dikenali pelanggan 10

2.3 Maklumat pelanggan dan akses semasa ialah perkara berbeza 11

2.4 Umpan pemesejan merentasi sempadan pelanggan dan tempat kerja 11

2.5 Laman web awam dan sistem operasi memerlukan kenyataan status berasingan 12

2.6 Amaran rasmi dan kewajipan undang-undang mempunyai tujuan berbeza 12

BAB 02

Konteks digital dan ancaman di Malaysia

RINGKASAN

Pelaporan awam di Malaysia menerangkan beberapa masalah berbeza: tawaran data jenayah, pancingan data, laman web awam yang terdedah dan gangguan perkhidmatan kewangan serta logistik. Setiap masalah memerlukan bukti dan pemilik tanggungjawab berbeza. Pembekal yang terjejas tidak membuktikan akses kepada setiap sistem pelanggan. Iklan data oleh pelaku tidak membuktikan pencerobohan baharu. Petakan kebergantungan perkhidmatan dan data kritikal, kemudian uji kawalan identiti serta pemulihan pada setiap sempadan.

2.1 Ketersambungan isi rumah yang tinggi meluaskan sempadan perkhidmatan

Keluaran ICT DOSM yang diterbitkan pada 23 April 2026 melaporkan akses internet dalam 97.1% isi rumah bagi tahun rujukan 2025. Angka ini mengukur akses isi rumah. Keluaran sama melaporkan penggunaan internet oleh 98.3% individu berumur 15 tahun ke atas. Metadata mentakrifkan populasi tinjauan dan tempoh penggunaan. Kedua-duanya bukan pemerhatian 2026, dan penyebutnya tidak boleh saling menggantikan. [S14] [S15]

Bagi pasukan pertahanan, akses isi rumah yang tinggi menjadikan proses digital pelanggan relevan secara meluas. Angka itu tidak mengukur pendedahan kepada kempen tertentu. Soalan perancangan yang berguna ialah sama ada pelanggan dan kakitangan boleh mengenali serta melaporkan transaksi, mesej atau permintaan akaun mencurigakan melalui saluran yang ditetapkan.

Perkhidmatan digital turut bergantung pada maklumat dan penyedia di sekelilingnya. Pengesahan identiti, sokongan pelanggan, pemprosesan bayaran dan pemulihan boleh mempunyai pemilik tanggungjawab berbeza. Insiden dalam laporan ini memperjelas sempadan tersebut tanpa mencadangkan bahawa satu angka ketersambungan menjelaskan kekerapannya.

2.2 Perkhidmatan boleh gagal di luar organisasi yang dikenali pelanggan

Kes 2026 menunjukkan sebab rangkaian organisasi sendiri hanya sebahagian daripada sempadan operasinya. Sebuah kumpulan perkhidmatan teknologi mengakui insiden yang menjejaskan sebahagian persekitaran IT. Sebuah terminal kontena melaporkan gangguan dan pemulihan berperingkat. Sebuah penyedia pelaporan kredit mendedahkan akses tanpa kebenaran dalam satu persekitaran perniagaan. Skop pendedahan berbeza, tetapi setiap satu menuntut keputusan daripada organisasi yang berkaitan. [S16][S5][S6]

Bagi organisasi yang berurusan dengan pelanggan, persoalan praktikalnya ialah transaksi atau set data yang bergantung pada persekitaran tersebut. Hubungan pembekal sahaja tidak membuktikan pelanggan terjejas. Sebaliknya, rangkaian dalaman yang tidak terjejas tidak menentukan sama ada maklumat pelanggan yang disimpan di tempat lain telah diakses. Respons perlu menjejaki data dan perkhidmatan berkaitan, kemudian mengekalkan perbezaan itu dalam komunikasi.

Peta kebergantungan yang berguna mengenal pasti penyedia, proses perniagaan, data yang ditukar dan kaedah operasi alternatif. Peta itu juga perlu menamakan individu yang boleh mengesahkan kenyataan penyedia. Senarai kontrak tanpa butiran ini membiarkan persoalan operasi tidak terjawab apabila perkhidmatan terhenti.

Oleh itu, laporan ini menganggap pendedahan pembekal sebagai sempadan yang perlu disahkan. Laporan ini tidak menyimpulkan satu kempen rantaian bekalan daripada insiden yang tidak berkaitan. Kesan perniagaan yang serupa tidak membuktikan infrastruktur, laluan masuk atau pengendali yang sama.

2.3 Maklumat pelanggan dan akses semasa ialah perkara berbeza

Pada 21 Jun, pelaporan kenyataan MKN dan NACSA menyebut bahawa dakwaan data peribadi yang tersebar dipercayai berkaitan insiden sebelum 2022. Kenyataan itu membezakan dakwaan tersebut daripada platform semasa dan merujuk siasatan yang berterusan. Itulah penilaian pihak berkuasa pada tarikh tersebut. Penilaian itu tidak menentukan asal setiap fail yang diiklankan kemudian. [S17]

Perbezaan ini penting kepada pasukan identiti dan penipuan. Iklan yang diterbitkan pada 2026 boleh menerangkan maklumat yang diperoleh lebih awal. Tarikh siaran terkini membuktikan pengiklanan terkini, bukan semestinya pemerolehan terkini. Laporan mengekalkan tarikh siaran sambil merekodkan secara berasingan tarikh data yang didakwa atau dibuktikan secara bebas.

Maklumat identiti lama masih boleh relevan apabila penipu menggunakannya untuk meyakinkan penerima mesej. Itu ialah senario pertahanan, bukan dapatan bahawa set data tertentu yang diiklankan telah digunakan. Organisasi perlu menguji sejauh mana proses pemulihan dan pengesahan pelanggan bergantung pada maklumat peribadi statik.

Keputusan kata laluan dan sesi memerlukan ujian berbeza. Perkaitan sejarah tidak menunjukkan sama ada akaun masih aktif, pemiliknya menukar kata laluan, atau sesi masih boleh digunakan. Kesahan dan pemilikan semasa mesti ditentukan sebelum respons yang mengganggu operasi. Pasukan identiti perlu mengekalkan keputusan beralasan dan tidak menganggap setiap rekod sejarah sebagai insiden aktif.

2.4 Umpan pemesejan merentasi sempadan pelanggan dan tempat kerja

Amaran MyCERT pada Jun menerangkan skrip Windows berbahaya yang dihantar melalui WhatsApp Desktop atau Web. Nasihat itu melibatkan umpan berbentuk dokumen dan pemasangan pengurusan jauh selepas pelaksanaan. Nasihat itu tidak menerangkan kerentanan dalam aplikasi pemesejan mudah alih. [S11]

Nasihat November menerangkan hasil berbeza. Portal bertema bantuan meminta maklumat identiti, kad dan kata laluan sekali guna. Umpan komputer riba percuma meminta kod log masuk akaun pemesejan dan kata laluan dua langkah. Saluran komunikasi serupa, tetapi aset yang berisiko berbeza. [S9][S10]

Bagi pasukan pertahanan, soalan pertama perlu mengenal pasti tindakan pengguna. Menerima mesej, membuka halaman, menyerahkan nombor identiti, memasukkan nombor kad bayaran dan menjalankan skrip ialah peristiwa berasingan. Setiap tindakan memerlukan respons sepadan. Satu arahan umum untuk menetapkan semula semua kata laluan boleh terlepas aset berkaitan.

Sempadan tempat kerja sama pentingnya. Kakitangan boleh menggunakan akaun pemesejan peribadi pada peranti kerja. Kemungkinan itu memerlukan semakan peranti akhir dan akaun apabila disokong bukti. Kemungkinan tersebut tidak membuktikan bahawa sistem majikan atau pangkalan data pelanggan telah diakses.

2.5 Laman web awam dan sistem operasi memerlukan kenyataan status berasingan

Amaran NC4 pada akhir Jun menerangkan serangan melibatkan sambungan pengurusan kandungan yang terdedah. Vendor menerbitkan kemas kini dan panduan bagi pemasangan lama. Secara berasingan, pelaporan November memetik kenyataan sebuah bank bahawa masalah laman web korporat tidak menjejaskan perkhidmatan perbankan, deposit atau maklumat pelanggan. Kedua-duanya episod berbeza dengan keterangan sumber berbeza. [S18][S19][S8]

Pengajaran pertahanan bersama ialah menentukan sempadan perkhidmatan sebelum menerangkan kesan. Laman web awam, pengesahan pelanggan, pemprosesan transaksi, perkongsian fail dan pangkalan data teras ialah aset berbeza. Dakwaan tentang laman web perlu mencetuskan semakan berkaitan tanpa menjadi dakwaan tentang semua sistem yang bersambung.

Kes sektor kesihatan turut membezakan akses fail sokongan daripada ketersediaan perkhidmatan pesakit (Kes H). Batasnya perlu diletakkan bersama dakwaan, bukannya dalam nota kaki yang jauh. [S7]

Pasukan komunikasi perlu menyediakan matriks perkhidmatan sebelum insiden. Setiap baris memerlukan keadaan semasa, bukti sokongan, pemilik tanggungjawab dan cap masa. Ini memudahkan kenyataan berskop khusus dipertahankan dan dikemas kini berbanding dakwaan luas bahawa semuanya selamat.

NACSA secara berasingan menilai gangguan produktiviti awan sebagai lebih berkemungkinan berkaitan masalah teknikal atau infrastruktur daripada serangan siber. Laporan ini mengecualikan keterangan itu daripada set kes lapan peristiwanya. Notis tersebut tidak menentukan dakwaan lain, dan penjelasan teknikal tidak menghapuskan keperluan menguji kesinambungan perkhidmatan. [S20]

2.6 Amaran rasmi dan kewajipan undang-undang mempunyai tujuan berbeza

Nasihat MyCERT mengenal pasti kempen dan langkah respons praktikal. NACSA dan NC4 menyediakan penyelarasan serta amaran kebangsaan. BNM dan pengawal selia data peribadi mempunyai peranan penyeliaan berasingan. Amaran tentang kempen bukan dapatan bahawa setiap penerima terjejas. Bab 10 membezakan kewajipan berkaitan dan tarikh kuat kuasa. [S11][S18][S9][S10]

Pemisahan sama terpakai kepada jaminan rasmi. Pada 18 November, seorang menteri menyifatkan dakwaan web gelap yang tersebar sebagai belum disahkan dan mungkin melibatkan data lama. Laporan mengaitkan kenyataan itu dengan sumber dan tarikhnya. Laporan tidak menggunakannya untuk menafikan insiden individu yang diakui di tempat lain sepanjang tahun. [S21]

Bagi CISO, objektif praktikalnya ialah rekod yang menyokong keputusan teknikal dan penilaian pemberitahuan. Rekod itu perlu menyatakan perkara yang diketahui, perkara belum disahkan, data atau perkhidmatan terlibat dan masa organisasi menyedarinya. Pasukan undang-undang dan operasi kemudian boleh menerapkan kewajipan berkaitan kepada fakta yang sama.

DAPATAN UTAMA

01

Insiden pembekal, laman web awam dan platform operasi memerlukan sempadan kesan berasingan.

02

Pengiklanan terkini tidak membuktikan kecurian terkini atau akses akaun semasa.

03

Halakan insiden pemesejan mengikut tindakan yang diambil dan aset yang didedahkan, kemudian sahkan perkhidmatan atau akaun berkaitan.

BAB 03

Pendedahan kebangsaan: portfolio 250 domain terpilih

SOALAN YANG DIJAWAB BAB INI

Apakah maklumat daripada portfolio terpilih, dan kesimpulan manakah di luar buktinya?

250

entri domain organisasi terpilih merentasi 11 sel sektor

3.1 Kad populasi 15

3.2 Bezakan dasar diterbitkan daripada kesan sebenar 16

3.3 Pemerhatian TLS dan halaman utama menjawab soalan khusus 18

3.4 Penyenaraian semasa dan perkaitan sejarah memerlukan pengesahan berasingan 18

3.5 Domain seiras, dokumen dan sebutan ialah petunjuk siasatan 21

3.6 Tukarkan bab ini kepada baris pengesahan 21

BAB 03

Pendedahan kebangsaan: portfolio 250 domain terpilih

RINGKASAN

Daripada 249 entri portfolio dinilai, 55 mempunyai kelayakan disenaraikan untuk dijual ketika disemak. Nilai utama Atlas kebangsaan ialah 48/100. Satu daripada 250 entri terpilih tiada hasil pendedahan boleh digunakan. Pemerhatian pasif meliputi 199 entri. Ini hasil domain terpilih, bukan kelaziman kebangsaan. Sahkan penyenaraian semasa dengan pemilik identiti, kemudian semak perkaitan peranti dan kelayakan bertarikh.

3.1 Kad populasi

Portfolio menyediakan penyebut ditakrifkan bagi bab ini. Jenama berkaitan, syarikat kumpulan dan perkhidmatan tempatan boleh bertindih. Domain terpilih tidak semestinya entiti undang-undang bebas. [S2]

Perkara	Takrif
Populasi	250 entri domain organisasi merentasi 11 sel sektor
Pemilihan	Portfolio bertujuan berdasarkan pengetahuan awam meliputi badan awam, perkhidmatan kewangan, perniagaan utama dan perkhidmatan penting
Unit	Satu domain utama terpilih bagi setiap entri portfolio
Pemerhatian domain	245 entri memberikan respons DNS; lima tidak memberikan respons dalam pemerhatian dikekalkan
Pemilikan	Respons domain dan kandungan halaman biasa tidak membuktikan pemilikan undang-undang bebas
Perbandingan	Hasil deskriptif portfolio ini; tiada kelaziman kebangsaan atau pemeringkatan keselamatan sektor
Pertindihan	Organisasi berkaitan, jenama dan populasi perkhidmatan boleh bertindih
Tarikh	Pemerhatian awam dan daftar pemilihan bertarikh 22 November 2026

Domain tanpa respons ialah pemerhatian tidak diketahui. Ia bukan bukti organisasi tidak aktif, tidak selamat atau tiada. Lima entri kekal dalam penyebut portfolio, sementara hasil khusus kawalan mengekalkan penyebut yang benar-benar boleh dinilai.

Sel sektor menyediakan pengelompokan deskriptif. Sel itu bukan dakwaan bahawa laporan mewakili setiap organisasi atau perkhidmatan dalam sektor.

Sektor	Entri portfolio	Batas pembacaan
Kerajaan	40	Badan dan aktiviti perkhidmatan berbeza
Perbankan dan kewangan	35	Merangkumi lebih daripada bank berlesen atau pengeluar kad
Insurans	15	Penanggung insurans terpilih dan perkhidmatan berkaitan
Tenaga dan utiliti	20	Aktiviti tenaga dan perkhidmatan awam berbeza
Pengangkutan dan logistik	20	Mod dan perkhidmatan sokongan berbeza
Telekomunikasi dan teknologi	20	Perniagaan rangkaian dan perkhidmatan teknologi
Pendidikan	25	Institusi terpilih dan kumpulan berkaitan
Penjagaan kesihatan	15	Hubungan penyedia dan kumpulan boleh bertindih
Peruncitan dan syarikat pegangan	25	Jenama dan kumpulan induk boleh bertindih
Pembuatan dan industri	20	Perniagaan industri dan pengguna terpilih
Hospitaliti dan media	15	Sel deskriptif gabungan bagi perniagaan perkhidmatan
Jumlah	**250**	**Entri terpilih, bukan kelaziman kebangsaan**

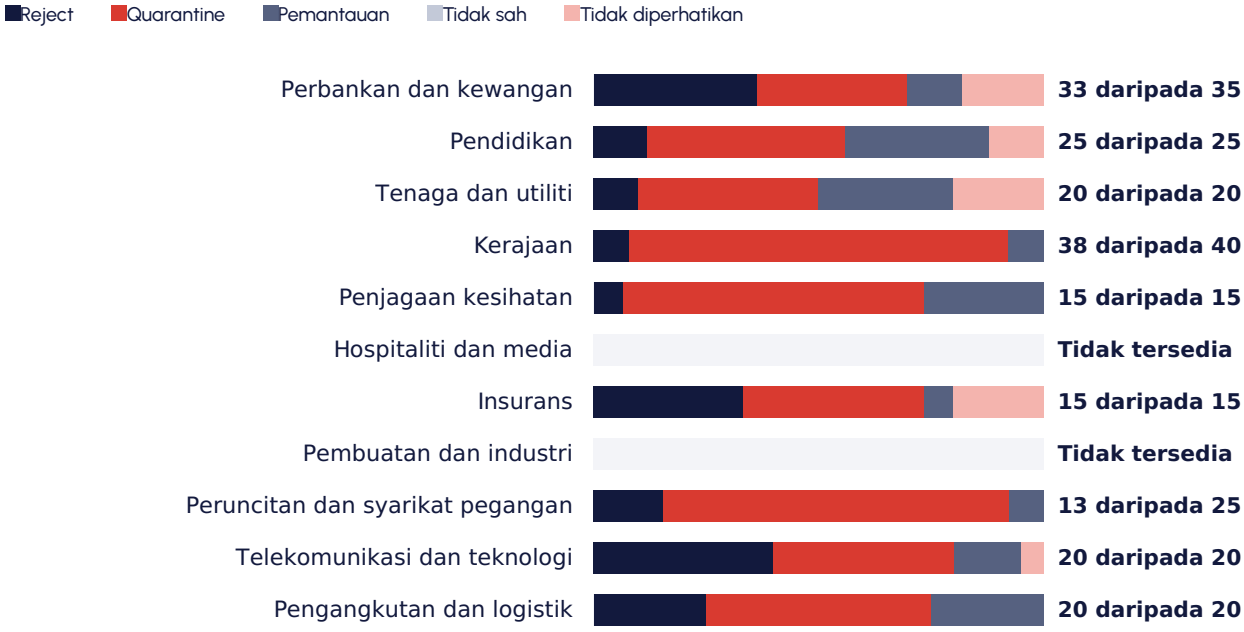
3.2 Bezakan dasar diterbitkan daripada kesan sebenar

Hasil domain mel melibatkan dasar diterbitkan yang diperhatikan. Dasar penolakan atau kuarantin ialah dapatan konfigurasi berguna. Ia tidak membuktikan setiap mesej tertakluk pada dasar atau setiap laluan penyamaran disekat. Oleh itu, laporan tidak menganggap kehadiran dasar sebagai penguatkuasaan sejagat. [S12]

Langkah praktikal seterusnya ialah pengesahan bersama pemilik pemesejan. Pemilik perlu menentukan penghantar sah yang menggunakan domain, sama ada mesej dimaksudkan disahkan dan pengecualian yang masih ada. Perubahan konfigurasi lengkap apabila perkhidmatan masih berfungsi seperti dimaksudkan dan hasil disokong rekod.

Rekod tandatangan yang tidak diperhatikan juga mempunyai batas. Ia tidak membuktikan organisasi tidak menandatangani mel. Rekod delegasi DNSSEC bukan pengesahan seluruh rantaian kepercayaan. Perbezaan ini mengelakkan jadual kehadiran kawalan menjadi keputusan keselamatan lebih luas.

Dasar mel diterbitkan berbeza merentasi portfolio terpilih



Sumber: pemerhatian pasif, 22 November 2026 [S12]. 199 entri mempunyai hasil pasif; setiap sektor mengekalkan penyebut sendiri. Dasar diterbitkan tidak membuktikan penguatkuasaan; hasil tidak tersedia tidak membuktikan kawalan tiada.

Pemerhatian pasif lengkap meliputi 199 daripada 250 domain terpilih. Daripada 245 domain yang memberikan respons DNS, 46 tiada pemerhatian pasif lengkap; lima domain terpilih tidak memberikan respons DNS. Hasil tidak tersedia ini kekal tidak diketahui. [S12]

Pemerhatian	Hasil	Penyebut
Dasar penolakan DMARC diterbitkan	41	199 pemerhatian lengkap
Dasar kuarantin DMARC diterbitkan	106	199 pemerhatian lengkap
Dasar pemantauan diterbitkan	35	199 pemerhatian lengkap
Tiada dasar DMARC diperhatikan	17	199 pemerhatian lengkap
Rekod SPF diperhatikan	181	199 pemerhatian lengkap
Rekod tandatangan DKIM diperhatikan	136	199 pemerhatian lengkap
Rekod delegasi DNSSEC diperhatikan	60	199 pemerhatian lengkap
TLS sah / tidak sah / belum selesai	158 / 10 / 31	199 pemerhatian lengkap
Halaman utama menjawab / tidak muktamad	150 / 49	199 pemerhatian lengkap
HSTS diperhatikan	110	150 halaman utama menjawab

Hasil kawalan sektor yang tidak tersedia kekal tidak diketahui. Liputan pasif tidak lengkap tidak menyokong penilaian kebersihan kebangsaan lengkap.

3.3 Pemerhatian TLS dan halaman utama menjawab soalan khusus

Pemerhatian TLS melibatkan hasil sambungan dan sijil pada tarikh dinyatakan. Hasil sah tidak membuktikan aplikasi ditampal. Hasil tidak sah berbeza daripada pemerhatian belum selesai, dan kedua-duanya berbeza daripada halaman utama yang tidak menjawab.

Hasil pengepala halaman utama menggunakan halaman menjawab sebagai penyebut. Hasil tidak patut dibahagi dengan setiap domain terpilih apabila sesetengah halaman tidak memberikan respons. Hasil hilang atau tidak muktamad kekal tidak diketahui, bukannya menjadi kawalan gagal.

Pemilik perkhidmatan perlu mengesahkan dapatan konfigurasi dilaporkan berdasarkan perkhidmatan dimaksudkan. Ini termasuk mengesahkan sama ada domain terpilih ialah titik masuk betul dan sama ada pemerhatian melibatkan induk, subsidiari atau perkhidmatan bersama. Sempadan domain terpilih laporan tidak menentukan hubungan organisasi tersebut.

3.4 Penyenaraian semasa dan perkaitan sejarah memerlukan pengesahan berasingan

Penyenaraian pasaran kelayakan semasa, rekod kelayakan sejarah dan perkaitan peranti dijangkiti ialah petunjuk berbeza. Petunjuk tidak patut ditambah menjadi bilangan individu atau insiden. Perkaitan boleh memerlukan siasatan tanpa membuktikan kesahan semasa akaun atau pemilikan peranti.

Daripada 249 entri dinilai, 55 mempunyai kelayakan disenaraikan untuk dijual ketika disemak pada 22 November 2026. Satu entri terpilih tiada hasil pendedahan boleh digunakan. Portfolio terpilih mengandungi 250 entri, maka status penyenaraian entri selebihnya tidak diketahui. [S1]

Nilai utama Atlas kebangsaan ialah **48/100** bagi 249 entri dinilai. Hanya penarafan kebangsaan diterbitkan. Jadual sektor mengandungi petunjuk diperhatikan, dengan penyebut terpilih dan dinilai berasingan. Jadual tidak memberikan penarafan sektor atau anggaran kelaziman kebangsaan.

Petunjuk pendedahan diperhatikan merentasi sektor terpilih

	Perkaitan peranti	Peranti pekerja	Sejarah kelayakan	Penyenaraian semasa	Sejarah penyenaraian	Dokumen
Perbankan dan kewangan (35)	86%	66%	86%	26%	23%	74%
Pendidikan (25)	96%	96%	96%	44%	44%	96%
Tenaga dan utiliti (20)	95%	80%	95%	20%	20%	55%
Kerajaan (40)	92%	85%	95%	20%	20%	68%
Penjagaan kesihatan (15)	93%	87%	87%	7%	7%	67%
Hospitaliti dan media (15)	80%	60%	80%	13%	13%	47%
Insurans (15)	100%	67%	100%	27%	27%	67%
Pembuatan dan industri (19)	63%	53%	89%	5%	5%	58%
Peruncitan dan syarikat pegangan (25)	88%	80%	100%	20%	20%	84%
Telekomunikasi dan teknologi (20)	90%	85%	95%	25%	25%	75%
Pengangkutan dan logistik (20)	90%	85%	95%	25%	25%	70%

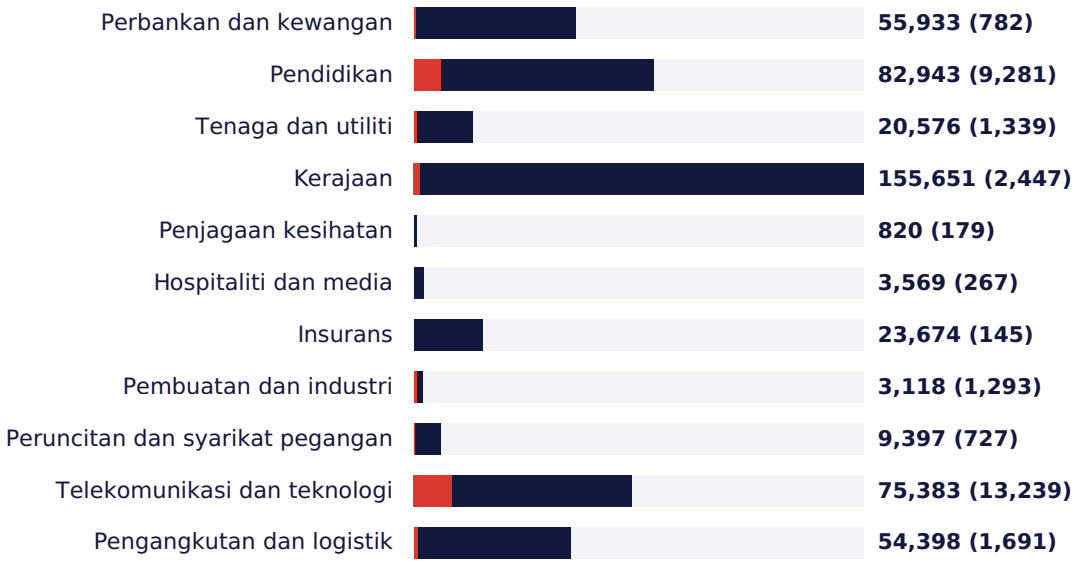
Penyenaraian kelayakan semasa mengikut sektor (warna karang). Penyebut ialah entri dinilai. Sumber: pemerhatian pendedahan Brandefense, 22 November 2026 [S1][S2]. 250 entri terpilih, 249 dinilai. Perkaitan terkumpul boleh bertindih; bukan individu unik atau insiden baharu.

Pemerhatian	Hasil	Batas
Entri dinilai / entri terpilih	249 / 250	Satu entri tidak tersedia
Entri dengan penyenaraian kelayakan semasa	55 / 249	Kesahan akaun belum disahkan
Entri dengan rekod kelayakan sejarah	231 / 249	Rekod sejarah, bukan individu unik
Entri dengan perkaitan peranti	221 / 249	Pemilikan dan status semasa belum disahkan
Entri dengan peranti dikelaskan pekerja	193 / 249	Pengelasan memerlukan pengesahan pemilik
Entri dengan perkaitan dokumen	176 / 249	Kerahsiaan belum disahkan

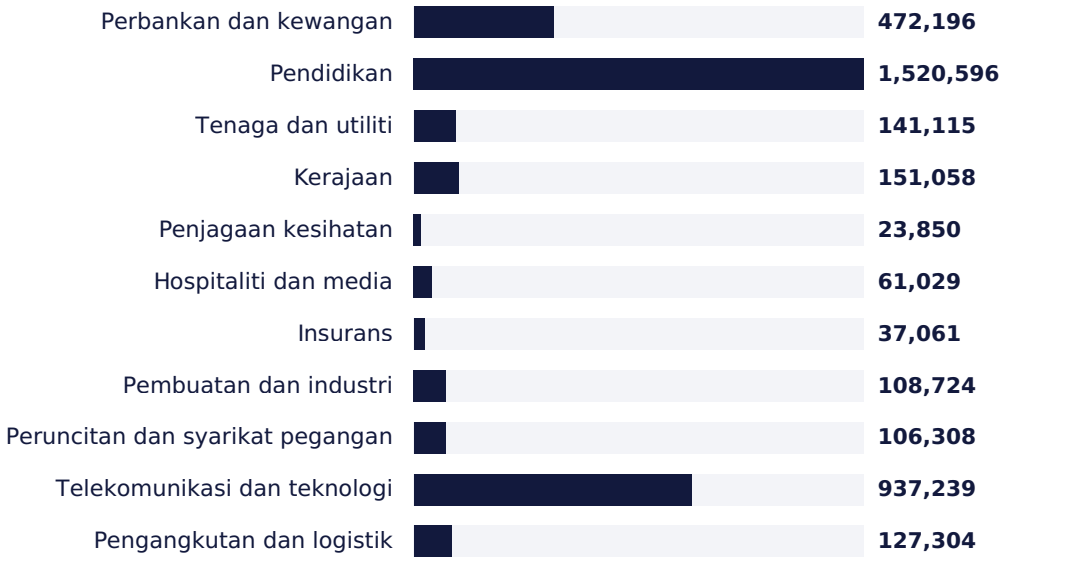
Perkaitan peranti dan kelayakan mengikut sektor

Perkaitan peranti pekerja Perkaitan peranti lain

Perkaitan peranti (subset pekerja dalam kurungan)



Perkaitan rekod kelayakan sejarah (skala berasingan)



Sumber: pemerhatian pendedahan Brandefense, 22 November 2026 [S1][S2]. 250 entri terpilih, 249 dinilai. Perkaitan terkumpul boleh bertindih; bukan individu unik atau insiden baharu.

Entri dinilai mempunyai 485,462 perkaitan peranti yang direkodkan, termasuk 31,390 perkaitan dikelaskan pekerja. Perkaitan peranti lain tidak dibuktikan sebagai milik pelanggan. Pertindihan rentas domain mungkin berlaku. Ini pemerhatian sumber terkumpul, bukan peranti baru terjejas sepanjang 2026. [S1]

Perkaitan rekod kelayakan sejarah berjumlah 3,686,480: 900,247 rekod pangkalan data pelanggaran, 1,216,827 baris log pencuri maklumat dan 1,569,406 entri combolist. Log pencuri maklumat ialah rekod yang dihasilkan oleh perisian hasad pencuri maklumat. Combolist ialah himpunan gabungan nama pengguna/kata laluan. [S57] Rekod ini bukan akaun unik, kata laluan aktif atau insiden disahkan. Jumlah sahaja tidak menentukan pemilikan atau kebaharuan.

Pendidikan menyumbang 1,520,596 perkaitan rekod kelayakan; telekomunikasi dan teknologi menyumbang 937,239. Jumlah itu menerangkan portfolio terpilih ini. Jumlah tidak membandingkan keselamatan kedua-dua sektor. Hubungan kakitangan, pelajar, pelanggan dan perkhidmatan bersama memerlukan pengesahan berasingan.

Perkaitan dokumen berjumlah 4,318. Konteks penerbitan dan kerahsiaan kekal belum disahkan. Kandungan serupa atau rujukan berulang boleh merentasi domain, maka ini bukan bilangan fail sulit unik.

Organisasi yang menerima penyenaraian semasa perlu mengenal pasti akaun berkaitan dan statusnya dahulu. Jika aktif, pasukan identiti perlu menyemak bukti log masuk dan sesi yang sesuai. Akaun istimewa atau akses jauh boleh memerlukan tindakan segera mengikut pelan insiden organisasi sendiri.

Rekod sejarah memerlukan tarikh dan konteks pemulihannya. Akaun dinyahaktifkan tanpa aktiviti terkini berkaitan berbeza daripada akaun digunakan semasa dengan aktiviti pengukuh. Rekod perlu menyatakan pernyataan disahkan dan bukti yang menyokong keputusan.

Perkaitan peranti memerlukan perhatian sama. Rekod berkaitan pekerja boleh membimbing siasatan peranti kakitangan. Perkaitan lain tidak secara automatik milik pelanggan. Pemilik perkhidmatan dan pasukan peranti akhir perlu menentukan pemilikan serta kaitan sebelum membuat kesimpulan itu.

3.5 Domain seiras, dokumen dan sebutan ialah petunjuk siasatan

Nama kelihatan serupa bukan bukti domain berbahaya. Dokumen menyebut organisasi bukan bukti dokumen sulit. Siaran menamakan negara atau syarikat tidak semestinya serangan terhadapnya. Setiap pernyataan memerlukan konteks berkaitan.

Pemerhatian domain seiras meliputi 19 Oktober–18 November 2026, secara berasingan daripada tarikh tutup pelaporan. Terdapat 33,811 perkaitan calon merentasi 178 entri dinilai. Nama serupa boleh tidak berkaitan; ini bukan laman pancingan data disahkan. Pembilang pendedahan lain menerangkan rekod dipegang ketika disemak pada 22 November. [S1]

Bagi domain berpotensi menyamar, soalan pertama melibatkan tujuan, konteks pengehosan dan penggunaan diperhatikan. Bagi dokumen, pemilik perlu mengenal pasti pengelasan maklumat dan konteks penerbitan sah. Bagi siaran, penganalisis perlu membezakan sebutan umum, iklan dan dakwaan akses khusus.

3.6 Tukarkan bab ini kepada baris pengesahan

Baris kerja berguna membezakan pengesahan konfigurasi daripada siasatan insiden. Dapatan dasar awam diletakkan bersama pemilik perkhidmatan. Bukti akaun semasa diletakkan bersama identiti dan respons insiden. Pernyataan pembekal atau akses data memerlukan pemilik perniagaan serta privasi berkaitan.

Baris kerja perlu merekodkan aset, tarikh bukti, pernyataan, pemilik, tindakan seterusnya dan syarat penyempurnaan. Hasil tidak diketahui perlu dikekalkan dan tidak digugurkan diam-diam. Ini menjadikan bab berguna tanpa meminta pembaca menganggap portfolio bertujuan sebagai ukuran keselamatan kebangsaan.

DAPATAN UTAMA

01

250 entri mentakrifkan portfolio domain terpilih, bukan 250 entiti undang-undang yang disahkan secara bebas.

02

Dasar diterbitkan, hasil TLS dan respons halaman utama mempunyai penyebut dinilai berbeza.

03

Sahkan setiap dapatan bersama pemilik berkaitan dan kekalkan hasil tidak diketahui sebagai tidak diketahui.

BAB 04

Pemerhatian kami di web gelap

04

SOALAN YANG DIJAWAB BAB INI

Apakah yang dibuktikan iklan data dan akses Malaysia, dan dakwaan manakah memerlukan siasatan berasingan?

8,748–9,196

siaran relevan dalam set bertag Malaysia dikekalkan

4.1 Jumlah menerangkan keterlihatan sumber 24

4.2 Tawaran bertindih 26

4.3 Enam iklan, enam pernyataan berbatas 27

4.4 Peredaran ialah bukti tawaran, bukan asalnya 32

4.5 Dakwaan tambahan kekal terlihat tanpa menjadi jumlah 33

BAB 04

Pemerhatian kami di web gelap

RINGKASAN

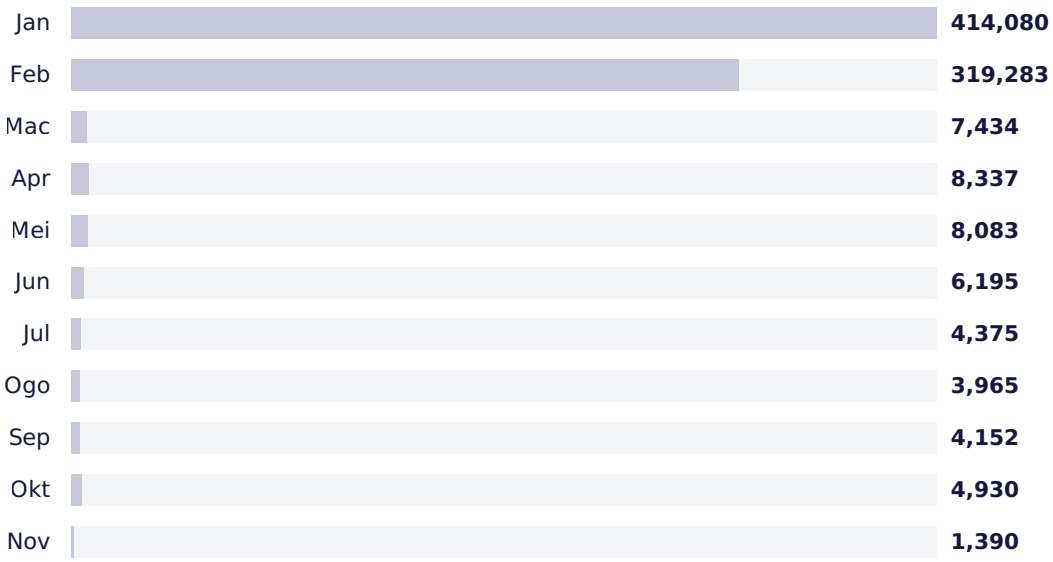
Sumber merekodkan 782,224 siaran bertag Malaysia sepanjang 1 Januari–22 November 2026. Set bertag dikekalkan mengandungi 25,355 siaran, termasuk julat relevan 8,748–9,196. Ini populasi siaran, bukan jumlah insiden atau mangsa. Iklan menawarkan maklumat pengguna, data kewangan dan akses perniagaan. Pengulangan dan jaminan penjual tidak membuktikan ketulenan atau kompromi baharu. Gunakan kad bukti untuk menetapkan skop pengesahan, mengenal pasti pemilik tanggungjawab dan menentukan bukti yang mewajarkan eskalasi.

4.1 Jumlah menerangkan keterlihatan sumber

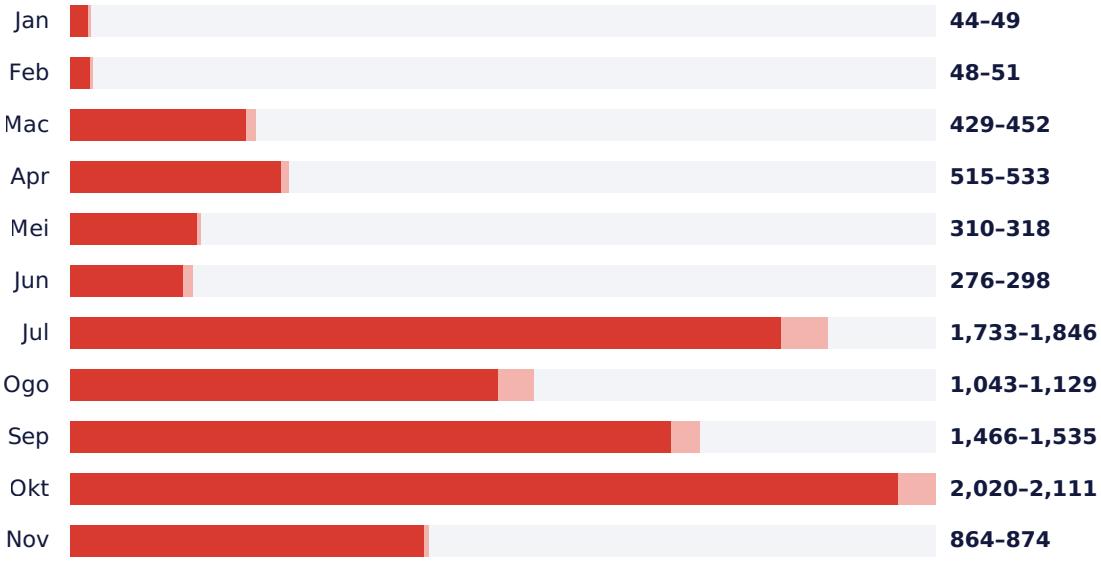
Bilangan siaran tidak mengukur kelaziman insiden Malaysia. Bilangan sumber 782,224 dan 25,355 siaran bertag dikekalkan menerangkan populasi liputan berbeza. Kedua-duanya bukan bancian serangan. Rujukan negara boleh melibatkan pasaran, set data didakwa, laporan berita atau perkhidmatan diiklankan. [S3]

Jumlah siaran bulanan mempunyai liputan tidak sekata dan tidak membuktikan pertumbuhan ancaman

Siaran bertag negara



Julat siaran relevan (skala berasingan; liputan tidak sekata)



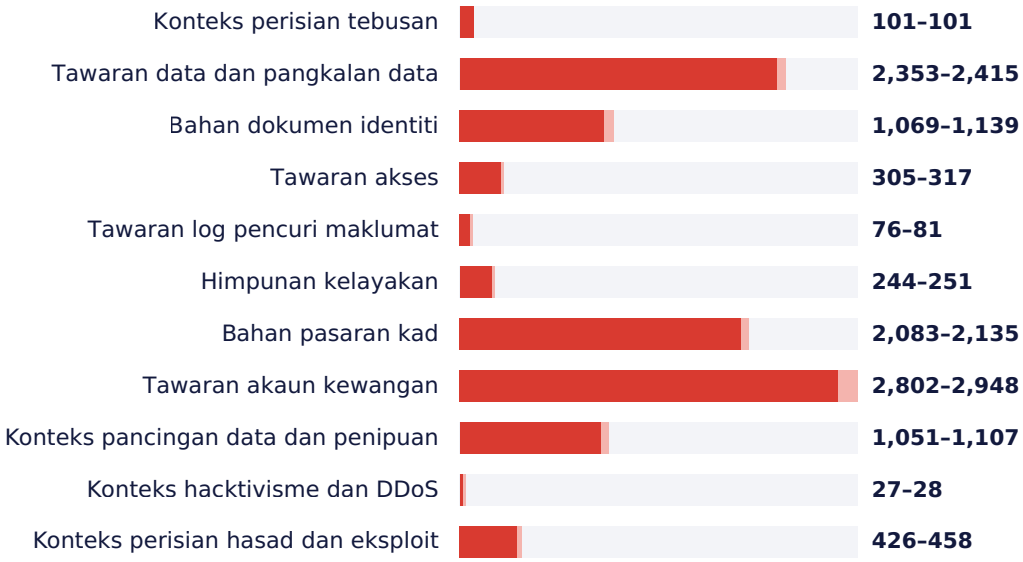
Sumber: Brandefense Blackhole, siaran bertag Malaysia, 1 Januari–22 November 2026; November belum lengkap [S3]. Bahan dikekalkan mempunyai liputan tidak sekata; siaran dan tema bertindih bukan insiden disahkan.

Januari dan Februari mendominasi bilangan bertag sumber, sementara bulan kemudian menyumbang lebih banyak bahan relevan dikekalkan. Perbezaan itu tidak membuktikan peningkatan serangan berjaya. Komposisi sumber dan liputan berbeza sepanjang tempoh. November berakhir pada 22 November dan ialah bulan tidak lengkap. [S3]

Julat relevan dikekalkan ialah 8,748–9,196 siaran. Batasnya menerangkan ketidakpastian dalam populasi siaran ini. Batas itu tidak menganggarkan insiden tersembunyi, individu unik atau kebarangkalian iklan tulen. Tawaran asas sama boleh muncul dalam beberapa siaran, bahasa atau tempat. [S3]

4.2 Tawaran bertindih

Tawaran akaun kewangan dan data berulang merentasi tema siaran bertindih



Sumber: Brandefense Blackhole, siaran bertag Malaysia, 1 Januari–22 November 2026; November belum lengkap [S3]. Bahan dikekalkan mempunyai liputan tidak sekata; siaran dan tema bertindih bukan insiden disahkan.

Tema diperhatikan	Siaran relevan dikekalkan	Batas bukti
Tawaran akaun kewangan	2,802–2,948	Ketersediaan diiklankan tidak membuktikan akaun boleh digunakan atau akses sistem bank
Tawaran data dan pangkalan data	2,353–2,415	Tajuk dan medan sampel tidak membuktikan asal atau rekod sah
Bahan pasaran kad	2,083–2,135	Siaran berasingan daripada pemerhatian kad terhad dalam Bab 9
Bahan dokumen identiti	1,069–1,139	Kesahan dokumen dan bilangan individu terjejas kekal persoalan berasingan
Konteks pancingan data dan penipuan	1,051–1,107	Promosi dan pelaporan tidak membuktikan penipuan selesai
Tawaran akses	305–317	Penerangan keistimewaan ialah dakwaan penjual sehingga disahkan
Kompilasi kelayakan	244–251	Label geografi tidak membuktikan insiden organisasi

Baris bertindih dan tidak boleh ditambah. Satu siaran boleh menawarkan akses akaun, bahan identiti dan perkhidmatan bayaran. Sumber merekodkan kandungan di bawah tema ini tanpa mengesahkan transaksi diiklankan berlaku. Bab 8 mempertimbangkan pernyataan penipuan; Bab 9 memberikan angka kad dengan skop berasingan. [S3]

Bahan berbahasa Inggeris dan Cina sama-sama menyumbang banyak kepada set dikekalkan. Bilangan batas atas relevan ialah 3,897 siaran berlabel Inggeris dan 3,519 siaran berlabel Cina. Bahasa tidak mengenal pasti kewarganegaraan pengendali atau membuktikan arahan negara. Ungkapan asal juga penting apabila terjemahan automatik menukar istilah komersial menjadi tuduhan. [S3]

4.3 Enam iklan, enam pernyataan berbatas

Kes berikut menggunakan petikan tulen disunting daripada siaran dikekalkan. Kes menunjukkan persoalan pengesahan berbeza. Kes bukan enam pelanggaran disahkan, dan tarikh sumbernya ialah tarikh siaran. Kuantiti dan butiran pengenalan ditahan daripada dipersembahkan sebagai kesan disahkan. [S3]

A

KES A

Tawaran data sektor awam memerlukan bukti asal usul

Kad bukti B01 | 9 Jan 2026 | Iklan forum yang disimpan | Sektor awam

Dakwaan belum disahkan

DAKWAAN	Iklan forum 9 Januari menawarkan maklumat sensitif di bawah label sektor awam Malaysia.
BUKTI DISIMPAN	Iklan dan ungkapannya dikekalkan. Ia membuktikan dakwaan diterbitkan.
PENJELASAN ALTERNATIF	Tawaran boleh melibatkan bahan lama, maklumat dibungkus semula, pelabelan tidak tepat atau rekod tulen. Siaran tidak menentukan kemungkinan itu.
BATAS	Ketulenan, tarikh pemerolehan, kelengkapan dan akses semasa belum disahkan. Sumber ini tidak membuktikan pengesahan organisasi.
RESPONS	Pemilik keselamatan dan privasi perlu menilai kaitan medan dengan rekod dibenarkan, kemudian menyiasat sempadan akses atau pendedahan yang disokong bukti pengukuh.

Kesimpulan

Sahkan asal usul dan sempadan pendedahan yang berkaitan sebelum menerima label sektor awam.

KES B

B

Label sektor kewangan tidak membuktikan akses bank

Kad bukti B02 | 8 Mei 2026 | Iklan forum yang disimpan | Perkhidmatan kewangan

Dakwaan belum disahkan

DAKWAAN	Siaran forum bertarikh 8 Mei mengiklankan pangkalan data yang dikaitkan dengan institusi kewangan Malaysia.
BUKTI DISIMPAN	Tajuk, dakwaan sektor dan bahagian sampel disunting dikekalkan.
PENJELASAN ALTERNATIF	Maklumat pelanggan boleh berasal daripada beberapa hubungan. Label sektor kewangan tidak mengenal pasti sistem yang membekalkannya, jika ada.
BATAS	Sumber tidak membuktikan ketulenan, bilangan akaun terjejas, akses semasa atau pengesahan institusi.
RESPONS	Pasukan penipuan dan keselamatan perlu menguji sempadan data didakwa melalui bukti dibenarkan sebelum mengambil tindakan akaun yang mengganggu operasi.

Kesimpulan

Tentukan sempadan data yang berkaitan sebelum menyimpulkan bahawa institusi kewangan telah diakses.

Kad bukti B01 — 9 Jan 2026

Persona penjual | Iklan forum yang disimpan | Forum | Inggeris

TEKS ASAL

i have [REDACTED_ORGANISATION] OF MALAYSIA data databse i.e confidential, sensitive

TERJEMAHAN

Saya mempunyai pangkalan data [REDACTED_ORGANISATION] MALAYSIA, iaitu data sulit dan sensitif.

Nota. Petikan asal yang disunting. Kuantiti yang dinyatakan penjual dan butiran pengenalan tidak dipaparkan. Tarikh hantaran bukan tarikh insiden.

Bukti disimpan
Iklan forum dan ungkapannya disimpan.

Belum disahkan
Kesahihan, sumber maklumat, akses semasa, kelengkapan dan insiden yang disahkan belum dibuktikan.

Kad bukti B02 — 8 Mei 2026

Persona penjual | Iklan forum yang disimpan | Forum | Inggeris

TEKS ASAL

[REDACTED_ORGANISATION], Malaysia Database

TERJEMAHAN

Pangkalan data [REDACTED_ORGANISATION], Malaysia

Nota. Petikan asal yang disunting. Kuantiti yang dinyatakan penjual dan butiran pengenalan tidak dipaparkan. Tarikh hantaran bukan tarikh insiden.

Bukti disimpan
Iklan yang disimpan, label sektor kewangan dan bahagian sampel yang disunting.

Belum disahkan
Kesahihan dan asal usul pangkalan data, bilangan akaun terjejas serta pencerobohan terhadap institusi belum dibuktikan.

KES C

C ■ Maklumat pengguna dan aktiviti akaun ialah dakwaan berasingan

Kad bukti B03 | 23 Ogo 2026 | Iklan forum yang disimpan | Maklumat pengguna

Dakwaan belum disahkan

DAKWAAN	Iklan forum bertarikh 23 Ogos menawarkan maklumat pengguna Malaysia dan mendakwa akaun pemesejan berkaitan aktif.
BUKTI DISIMPAN	Iklan dengan tajuk campuran Inggeris dan Cina dikekalkan.
PENJELASAN ALTERNATIF	Senarai hubungan beredar, semakan akaun tidak tepat dan bahan dibungkus semula boleh menghasilkan iklan serupa.
BATAS	Persetujuan, asal, kebaharuan, bilangan individu unik dan kesahan akaun kekal belum disahkan. Siaran sahaja tidak membuktikan insiden organisasi.
RESPONS	Pemilik privasi dan penipuan perlu menilai kategori medan dinyatakan serta senario penyamaran berkaitan tanpa menghubungi individu diiklankan atau menganggap setiap entri sah.

Kesimpulan

Nilai asal usul data hubungan dan senario umpan tanpa menganggap akaun yang diiklankan telah disahkan.

KES D

D ■ Janji kebaharuan ialah dakwaan tentang usia

Kad bukti B04 | 6 Sep 2026 | Iklan forum yang disimpan | Pemasaran kewangan

Dakwaan belum disahkan

DAKWAAN	Siaran forum 6 September menawarkan maklumat pemasaran kewangan Malaysia dan mendakwa rekod diperoleh dalam 30 hari.
BUKTI DISIMPAN	Iklan mengandungi usia didakwa dan kuantiti dinyatakan penjual.
PENJELASAN ALTERNATIF	Tarikh mungkin menerangkan pembungkusan, penerimaan penjual atau promosi berulang, bukan pemerolehan asal.
BATAS	Usia didakwa dan kuantiti tidak dibuktikan secara bebas. Tawaran tidak mengenal pasti insiden institusi disahkan.
RESPONS	Pemilik perniagaan dan privasi perlu menentukan asal usul data yang sah serta menilai senario umpan berkaitan sebelum menerima penerangan kebaharuan penjual.

Kesimpulan

Sahkan tempoh pemerolehan yang didakwa secara berasingan daripada tarikh hantaran.

Kad bukti B03 — 23 Ogo 2026

Persona penjual | Iklan forum yang disimpan | Forum | Inggeris

TEKS ASAL

This is a database of property owners in Malaysia who are active on WS Rows: [record count withheld]

TERJEMAHAN

Ini ialah pangkalan data pemilik hartanah di Malaysia yang aktif di WS. Baris: [bilangan rekod ditahan]

Nota. Petikan asal yang disunting. Kuantiti yang dinyatakan penjual dan butiran pengenalan tidak dipaparkan. Tarikh hantaran bukan tarikh insiden.

Bukti disimpan
Iklan yang disimpan dan tajuk medan sampelnya dalam bahasa Inggeris dan Cina.

Belum disahkan
Persetujuan, asal usul, kemutakhiran, bilangan individu unik, kesahihan akaun dan insiden organisasi belum dibuktikan.

Kad bukti B04 — 6 Sep 2026

Persona penjual | Iklan forum yang disimpan | Forum | Inggeris

TEKS ASAL

FRESH DATABASE [record count withheld] Malaysia Crypto & Forex Leads All records sourced within 30 days.

TERJEMAHAN

PANGKALAN DATA BAHARU [bilangan rekod ditahan] prospek kripto dan forex Malaysia. Semua rekod diperoleh dalam tempoh 30 hari.

Nota. Petikan asal yang disunting. Kuantiti yang dinyatakan penjual dan butiran pengenalan tidak dipaparkan. Tarikh hantaran bukan tarikh insiden.

Bukti disimpan
Iklan yang disimpan, kuantiti yang didakwa dan usia data yang didakwa.

Belum disahkan
Kuantiti, usia, ketepatan, persetujuan, asal usul dan insiden melibatkan organisasi tertentu belum dibuktikan.

KES K

K

Tawaran data pelanggan November tidak menentukan tarikh pencerobohan

Kad bukti B05 | 19 Nov 2026 | Iklan forum yang disimpan | Perniagaan pengguna

Dakwaan belum disahkan

DAKWAAN	Iklan forum bertarikh 19 November menawarkan rekod pelanggan di bawah label perniagaan pengguna Malaysia.
BUKTI DISIMPAN	Tajuk forum dan bahagian sampel disunting dikekalkan.
PENJELASAN ALTERNATIF	Iklan mungkin menerangkan peredaran terdahulu, hubungan sumber lain atau produk dilabel tidak tepat.
BATAS	Ketulenan, bilangan rekod tepat, kompromi semasa dan tarikh insiden belum disahkan. Siaran hampir tarikh tutup tidak membuktikan pencerobohan baharu November.
RESPONS	Pemilik keselamatan dan privasi perlu menentukan sempadan data pelanggan didakwa dan meningkatkan tindakan apabila perbandingan dibenarkan atau bukti akses menyokongnya.

Kesimpulan

Iklan pada November tidak membuktikan pencerobohan berlaku pada November.

L

KES L

Akses pentadbir ialah keupayaan diiklankan

Kad bukti B06 | 1 Feb 2026 | Iklan forum yang disimpan | Perniagaan sektor swasta

Dakwaan belum disahkan

DAKWAAN	Siaran penjual berbahasa Rusia bertarikh 1 Februari mengiklankan akses berkaitan perniagaan Malaysia dan mendakwa keistimewaan pentadbir.
BUKTI DISIMPAN	Satu siaran dikekalkan mengandungi dua entri berlabel Malaysia dan dakwaan keistimewaan.
PENJELASAN ALTERNATIF	Entri mungkin melibatkan akses tidak berkaitan, akses lapuk atau penerangan tidak tepat. Penjual sama tidak membuktikan satu pencerobohan atau pengendali.
BATAS	Kesahan akses, ketekalan, pemilikan, sistem terjejas dan tarikh insiden kekal belum disahkan. Butiran perniagaan dan sistem yang mengenal pasti sasaran ditahan.
RESPONS	Pemilik identiti dan infrastruktur perlu menyemak akaun istimewa, sesi dan akses jauh berkaitan menggunakan bukti dalaman sebelum menerima keupayaan diiklankan.

Kesimpulan

Semak akses berkeistimewaan melalui bukti dalaman; dakwaan penjual bukan pengesahan.

Kad bukti B05 — 19 Nov 2026

Persona penjual | Iklan forum yang disimpan | Forum | Inggeris

TEKS ASAL

[REDACTED_ORGANISATION] Shopping & Customer Database

TERJEMAHAN

Pangkalan data beli-belah dan pelanggan [REDACTED_ORGANISATION]

Nota. Petikan asal yang disunting. Kuantiti yang dinyatakan penjual dan butiran pengenalan tidak dipaparkan. Tarikh hantaran bukan tarikh insiden.

Bukti disimpan
Tajuk forum yang disimpan dan bahagian sampel yang disunting.

Belum disahkan
Kesahihan, pencerobohan semasa, bilangan rekod atau individu yang tepat, tarikh insiden dan pengesahan institusi belum dibuktikan.

Kad bukti B06 — 1 Feb 2026

Persona penjual | Iklan forum yang disimpan | Forum | Rusia

TEKS ASAL

Доступ Malaysia [identifying details withheld] Domain Admin

TERJEMAHAN

Akses Malaysia [butiran pengenalan ditahan] Pentadbir Domain

Nota. Petikan asal yang disunting. Kuantiti yang dinyatakan penjual dan butiran pengenalan tidak dipaparkan. Tarikh hantaran bukan tarikh insiden.

Bukti disimpan
Satu hantaran penjual dengan dua entri berlabel Malaysia dan dakwaan hak pentadbir.

Belum disahkan
Kesahihan dan ketahanan akses, pemilikan sebenar, sistem terjejas, tarikh insiden serta pengendali bersama bagi entri berbeza belum dibuktikan.

4.4 Peredaran ialah bukti tawaran, bukan asalnya

Perbincangan forum dikekalkan mempersoalkan asal usul iklan data pengguna Malaysia. Cabaran itu ialah bukti balas berguna terhadap naratif kebaharuan tanpa kelayakan, tetapi tidak membuktikan pencabarnya betul. Kedua-dua dakwaan memerlukan bukti sendiri. [S3]

Iklan berbahasa Cina memasukkan Malaysia dalam menu pelbagai negara dan menjanjikan bahan aktif bermutu tinggi. Ungkapan itu menerangkan jaminan penjual. Ungkapan tidak membuktikan mutu data, kewarganegaraan, pemilikan atau jualan selesai. Katalog berulang boleh mengekalkan keterlihatan pernyataan tanpa menunjukkan pemerolehan baharu. [S3]

Kad bukti B07 10 Feb 2026

Peserta forum Perbincangan forum yang disimpan Forum Inggeris

TEKS ASAL

All your sample data can be found in publicly available databases.

TERJEMAHAN

Semua data sampel anda boleh ditemukan dalam pangkalan data yang tersedia kepada umum.

Nota. Kenyataan yang diterbitkan sahaja; bahan yang ditawarkan belum disahkan secara bebas.

Bukti disimpan
Cabaran terhadap asal usul data dalam perbincangan yang disimpan.

Belum disahkan
Sama ada data dibungkus semula, jumlah pertindihan, kemutakhiran dan pihak yang betul belum dibuktikan.

Kad bukti B09 8 Mac 2026

Persona penjual Hantaran saluran yang disimpan Telegram Cina

TEKS ASAL

全网低价包活出售 顶级质量 先到先得欢迎咨询

TERJEMAHAN

Dijual pada harga rendah di seluruh rangkaian, dijamin aktif. Mutu terbaik, siapa cepat dia dapat; pertanyaan dialu-alukan.

Nota. Kenyataan yang diterbitkan sahaja; bahan yang ditawarkan belum disahkan secara bebas.

Bukti disimpan
Iklan dan dakwaannya tentang harga rendah, ketersediaan dan mutu.

Belum disahkan
Kesahihan, status aktif, asal usul data, kewarganegaraan, insiden organisasi tertentu dan pengendali bersama belum dibuktikan.

Varian katalog berbahasa Cina turut mengiklankan produk pengguna perbankan berlabel Malaysia bersama tawaran asing tidak berkaitan. Menu dipendekkan ialah petunjuk jualan data. Ia tidak membuktikan insiden bank bernama, set data disahkan atau pengendali bersama di sebalik ungkapan serupa. Keluarga katalog kekal sebutan dan bukan satu lagi kes disahkan. [S3]

4.5 Dakwaan tambahan kekal terlihat tanpa menjadi jumlah

Siaran tambahan yang dikekalkan mengandungi sebutan berasaskan peranan tentang organisasi sektor awam, pendidikan, kesihatan, teknologi, perjalanan dan industri. Sesetengah siaran menerangkan muat naik semula atau tempoh data terdahulu. Yang lain melibatkan perkhidmatan pertanyaan, katalog kelayakan atau rekod didakwa dengan perkaitan Malaysia yang tidak pasti. Sebutan ini tidak membuktikan insiden tambahan yang disahkan. [S3]

Tajuk berulang di tempat lain membuktikan peredaran. Ia tidak mengesahkan set data secara bebas, membuktikan insiden kedua atau mengenal pasti penjual pertama. Begitu juga, perkhidmatan pertanyaan diiklankan tidak membuktikan akses sistem kerajaan. Individu dalam set data didakwa tidak semestinya mengenal pasti organisasi sumbernya.

Bagi organisasi terjejas, hasil berguna pertama ialah pernyataan berskop: medan didakwa, tarikh sumber, sempadan dalaman berkaitan dan bukti diperlukan untuk pengesahan. Siasatan perlu mengekalkan dapatan pengukuh dan bercanggah. Eskalasi perlu mengikut bukti tersebut, dengan pemilik dinamakan bagi keputusan akaun, privasi dan kesinambungan.

DAPATAN UTAMA

01

Bilangan siaran relevan dikekalkan menerangkan keterlihatan sumber, bukan jumlah insiden kebangsaan.

02

Dakwaan data, akses dan kebaharuan memerlukan pengesahan berasingan walaupun iklan berulang.

03

Tetapkan pemilik dan bukti penutupan bagi setiap pernyataan berkaitan sebelum meningkatkan dakwaan kesan.

BAB 05

Insiden dan dakwaan mengikut sektor

05

SOALAN YANG DIJAWAB BAB INI

Sempadan perkhidmatan manakah yang dikenal pasti pelaporan awam, dan apakah respons awal yang diperlukan setiap sektor?

6

perspektif sektor dengan status bukti dikekalkan

5.1 Cara membaca contoh sektor 36

5.2 Pembekal teknologi: bezakan kemungkinan akses daripada salah guna yang disahkan 39

5.3 Perkhidmatan kewangan: ketersediaan dagangan dan kesan data adalah berasingan 39

5.4 Perkhidmatan bayaran pengguna: selaraskan pemulihan operasi biasa 40

5.5 Telekomunikasi: pendedahan terpencil tidak membuktikan kemasukan rangkaian 40

5.6 Logistik: pemulihan mesti merangkumi aliran kerja yang bersambung 41

5.7 Pelaporan kredit: satu persekitaran bukan keseluruhan simpanan data 42

5.8 Penjagaan kesihatan: fail sokongan memerlukan sempadan akses sendiri 43

5.9 Transaksi perkhidmatan awam: integriti boleh memerlukan siasatan tanpa gangguan 44

5.10 Perkhidmatan berhadapan orang ramai: peristiwa laman web tidak mengenal pasti laluan masuk di tempat lain 45

5.11 Notis pembekal penerbangan: kemungkinan kesan pelanggan bukan pengesahan akses sistem syarikat penerbangan 45

5.12 Paparan awam memerlukan pelan akses vendor dan pengasingan 46

5.13 Tindakan perlindungan tidak membuktikan dapatan insiden yang lengkap 46

BAB 05

Insiden dan dakwaan mengikut sektor

RINGKASAN

Pelaporan awam menerangkan insiden pembekal, laman web, dagangan, pelaporan kredit, logistik dan fail sokongan. Pengesahan insiden tidak mengesahkan identiti pelaku, bilangan rekod yang diiklankan atau laluan masuk yang didakwa. Sesetengah laporan menerangkan sekatan berjaga-jaga dan belum membuktikan kecurian. Gunakan contoh sektor untuk mengenal pasti sempadan perkhidmatan anda, meminta bukti sokongan dan menetapkan langkah pengesahan pertama.

5.1 Cara membaca contoh sektor

Bab ini membezakan pengakuan organisasi, keterangan pihak berkuasa dan dakwaan pelaku. Semua itu boleh melibatkan episod sama tanpa membuktikan perkara yang sama. Organisasi boleh mengesahkan akses tanpa kebenaran sedangkan jumlah yang diiklankan penjual masih belum disahkan. Sekatan semasa siasatan juga boleh melindungi perkhidmatan yang tidak terjejas.

Kes di bawah mengekalkan label sasaran umum. Label itu ialah pilihan privasi, bukan kenyataan tentang kepentingan organisasi. Tarikh mengenal pasti kronologi yang dilaporkan. Tarikh itu tidak menentukan masa data mula diperoleh melainkan sumber menyatakannya.

Lajur respons awal ialah cadangan untuk organisasi dengan kebergantungan setanding. Lajur itu tidak membayangkan organisasi dalam kes berkenaan gagal mengambil tindakan tersebut. Laporan tidak menyimpulkan kelaziman sektor kebangsaan daripada contoh ini.

Perkhidmatan teknologi

DIPERHATIKAN ATAU DILAPORKAN

Insiden menjejaskan sebahagian persekitaran IT pembekal; dokumen mungkin diakses

STATUS DAN BATAS

Notis syarikat; kemungkinan akses data, tiada salah guna disahkan pada tarikh notis

RESPONS AWAL

Kenal pasti dokumen dan hubungan dalam persekitaran terjejas

Perbankan dan kewangan

DIPERHATIKAN ATAU DILAPORKAN

Gangguan laman web, sekatan broker dan gangguan pelaporan kredit

STATUS DAN BATAS

Peristiwa berasingan; jangan gabungkan skop perkhidmatan atau datanya

RESPONS AWAL

Sahkan pengesahan identiti, transaksi dan status laman awam secara berasingan

Logistik

DIPERHATIKAN ATAU DILAPORKAN

Gangguan terminal diikuti pemulihan berperingkat

STATUS DAN BATAS

Insiden pengendali diterangkan dalam pelaporan industri; dakwaan kumpulan dan kecurian kekal berasingan

RESPONS AWAL

Uji pemprosesan manual dan bukti yang diperlukan sebelum membuka semula antara muka

Penjagaan kesihatan

DIPERHATIKAN ATAU DILAPORKAN

Akses terhad platform fail sokongan pada November

STATUS DAN BATAS

Keterangan rasmi dipetik dalam pelaporan; pelaku atau jumlah data tidak ditentukan

RESPONS AWAL

Semak skop fail, perkongsian luar dan keistimewaan akaun

Perkhidmatan awam

DIPERHATIKAN ATAU DILAPORKAN

Serangan sambungan pengurusan kandungan dan pancingan data bertema bantuan

STATUS DAN BATAS

Amaran teknikal rasmi; pancingan data tidak membuktikan akses kepada sistem yang ditiru

RESPONS AWAL

Buktikan keadaan sambungan yang dibaiki dan lindungi saluran pengesahan identiti

Perkhidmatan pengguna

DIPERHATIKAN ATAU DILAPORKAN

Umpan tugasan kerja, bantuan dan akaun pemesejan

STATUS DAN BATAS

Amaran kempen; jumlah dilaporkan menggunakan tempoh masing-masing

RESPONS AWAL

Bezakan tindakan penerima dan halakan respons akaun, peranti serta bayaran

Keterangan awam yang dikekalkan mengakui lapan insiden dengan skop individu dalam bab ini. Ini ialah set kes laporan, bukan jumlah kebangsaan. Bilangan insiden dalam pelaporan komponen broker yang lebih luas tidak diketahui. Sekatan berjaga-jaga, notis kempen dan kemungkinan kesan pembekal berada di luar kiraan lapan peristiwa ini.

Tempoh pelaporan	Peranan umum	Sempadan yang diakui	Batas
Notis April; insiden Februari	Kumpulan perkhidmatan teknologi	Sebahagian persekitaran IT; kemungkinan akses dokumen	Tiada salah guna disahkan pada tarikh notis
Jun–Julai	Platform perkhidmatan bayaran pengguna	Gangguan berkaitan serangan siber dan pemulihan	Jangkauan perkhidmatan bersama bukan kiraan insiden berasingan
Pelaporan Julai–Ogos	Penyedia telekomunikasi	Pendedahan maklumat pelanggan tanpa kebenaran yang terpencil	Insiden pelanggan yang lebih luas tidak dibuktikan
September	Pengendali terminal kontena	Gangguan keselamatan siber dan mula semula berperingkat	Pelaku, jumlah kecurian dan akses kawalan industri belum disahkan
September	Penyedia pelaporan kredit	Satu persekitaran perniagaan pengguna dan perkhidmatan pelaporan	Tiada kesimpulan tentang setiap set data atau institusi pelanggan

Tempoh pelaporan	Peranan umum	Sempadan yang diakui	Batas
Oktober	Institusi kewangan	Insiden operasi dan pemulihan perkhidmatan berperingkat	Pelaku atau laluan masuk belum disahkan
29 Oktober	Sistem paparan awam perbandaran	Kandungan tanpa kebenaran dan penutupan paparan	Laluan akses, pengendali dan sempadan rangkaian lebih luas belum ditentukan
November	Platform sokongan sektor kesihatan	Akses terhad kepada fail sokongan	Ketersediaan klinikal tidak menjawab setiap persoalan fail

Sempadan lapan peristiwa mengikut keterangan awam masing-masing dengan batasnya dikekalkan. [S16][S22] [S23][S5][S6][S24][S7][S25][S26]

5.2 Pembekal teknologi: bezakan kemungkinan akses daripada salah guna yang disahkan

Sebuah kumpulan perkhidmatan teknologi mendedahkan insiden 10 Februari dalam notis April. Kumpulan itu berkata dokumen yang mengandungi maklumat peribadi terhad mungkin diakses atau dipindahkan keluar. Notis menerangkan maklumat identiti, hubungan dan pekerjaan serta menyatakan tiada salah guna disahkan dikenal pasti ketika itu. [S16]

Ini menyokong soalan khusus kepada pembekal: dokumen dan hubungan perniagaan manakah yang terdapat dalam persekitaran terjejas? Ini tidak menyokong kesimpulan bahawa setiap sistem pelanggan dicapai. Ketiadaan salah guna disahkan pada tarikh notis juga tidak membuktikan maklumat itu tidak akan digunakan.

Pelanggan perlu meminta kategori dokumen terjejas, tarikh berkaitan dan bukti yang menyokong sempadan penyedia. Mereka perlu mengesahkan perubahan luar jangka kepada arahan bayaran melalui saluran yang ditetapkan. Kawalan itu sesuai dengan konteks hubungan dan perniagaan yang didedahkan tanpa menganggap kerugian bayaran yang tidak dilaporkan.

5.3 Perkhidmatan kewangan: ketersediaan dagangan dan kesan data adalah berasingan

Pelaporan Mac membawa kenyataan bursa tentang insiden dalam komponen tertentu yang digunakan beberapa broker. Kenyataan itu menyebut insiden telah dibendung dan integriti pasaran yang lebih luas kekal terpelihara. Episod broker kemudian perlu dinilai berdasarkan tarikh serta skop perkhidmatannya sendiri. [S27]

Pada akhir Oktober, broker dalam talian mengesahkan sekatan selepas mengesan cubaan keselamatan siber. Respons bertulisnya menerangkan saluran pesanan ekuiti domestik terjejas sementara fungsi lain kekal tersedia. Broker itu berkata penilaiannya pada tarikh tersebut tidak menemukan bukti kehilangan data. [S28]

Pengajaran operasi ialah menyediakan kaedah sandaran khusus mengikut saluran. Broker perlu mengetahui pesanan yang masih boleh diterima, cara arahan manual disahkan dan cara arahan beratur diselaraskan. Laporan tidak menganggap sekatan berjaga-jaga sebagai bukti bahawa kecurian berjaya.

Keterangan Oktober yang berasingan melibatkan institusi kewangan yang mengesan aktiviti mencurigakan pada 7 Oktober. Pelaporan kenyataannya menyebut perkhidmatan teras disambung pada 12 Oktober. Sesetengah fungsi penetapan semula, pendaftaran dan akaun baharu masih tidak tersedia pada tarikh tersebut. Institusi itu berkata dana pelanggan selamat. [S24]

Ini menyokong ujian pemulihan mengikut fungsi. Pemprosesan transaksi, pemulihan akaun dan penerimaan pelanggan memerlukan pengesahan masing-masing sebelum organisasi menyatakan pemulihan penuh. Sumber tidak menentukan kumpulan atau laluan masuk, dan laporan tidak menambah atribusi sedemikian.

Kes pelaporan kredit September mewujudkan kebergantungan berbeza. Pemberi pinjaman boleh mengekalkan sistem sendiri tetapi kehilangan akses kepada laporan luar yang diperlukan untuk keputusan. Pasukan kredit, penipuan dan operasi perlu menyetujui pengendalian permohonan tertangguh, semakan lewat dan penyelarasan susulan. Kes G menghuraikan sempadan itu.

5.4 Perkhidmatan bayaran pengguna: selaraskan pemulihan operasi biasa

Pelaporan Julai memetik pengumuman bahawa platform bayaran pengguna kembali dalam talian selepas serangan siber. Laporan menyebut notis gangguan bermula pada 30 Jun dan pemulihan diumumkan pada 2 Julai. Pelaporan itu turut merekodkan aduan pengguna tentang baki. Aduan tersebut bukan jumlah dana hilang yang diukur. [S22]

Platform bersama boleh menyokong banyak pihak berkuasa perkhidmatan tanpa menghasilkan jumlah pencerobohan berasingan yang sama. Oleh itu, laporan mengekalkan gangguan itu sebagai satu peristiwa berskop individu. Laporan tidak menerbitkan dakwaan jumlah pengguna atau menyimpulkan akses kepada setiap pihak berkuasa yang bersambung.

Bagi pengendali, pemulihan perlu merangkumi proses penyelarasan transaksi dan baki. Sokongan pelanggan memerlukan cara membezakan paparan lewat, baki dipertikaikan dan percanggahan perakaunan yang disahkan. Pasukan keselamatan perlu mengesahkan sempadan perkhidmatan sementara pemilik perniagaan menyelesaikan pengecualian operasi.

Bukti penyempurnaan perlu mengenal pasti rekod yang dibandingkan, cara pengecualian dikendalikan dan pihak yang meluluskan operasi biasa. Aplikasi yang berfungsi sahaja tidak menutup pertanyaan baki pelanggan. Ini ialah kawalan yang dicadangkan, bukan dakwaan bahawa pengendali mengabaikannya.

5.5 Telekomunikasi: pendedahan terpencil tidak membuktikan kemasukan rangkaian

Pelaporan akhir Julai dan awal Ogos memetik penyedia telekomunikasi yang menerangkan pendedahan maklumat akaun pelanggan tanpa kebenaran secara terpencil. Syarikat berkata seorang individu dikenal pasti dan tiada petunjuk insiden lebih luas melibatkan pelanggan lain. Itulah keterangannya pada tarikh berkenaan, bukan bukti tentang setiap dakwaan kemudian. [S23]

Kes ini melibatkan akses dan pendedahan maklumat. Kes ini tidak membuktikan pencerobohan rangkaian korporat. Laporan menggugurkan butiran individu, akaun, bil dan amaun kerana semuanya tidak diperlukan untuk keputusan pertahanan.

Pemilik tanggungjawab berkaitan perlu mengesahkan peranan yang boleh melihat atau mendedahkan maklumat pelanggan, cara akses dilog dan cara permintaan luar biasa diluluskan. Semakan perlu membezakan akses sokongan sah daripada pendedahan di luar proses dibenarkan. Bukti kes khusus perlu dikekalkan tanpa meluaskan dakwaan kepada kakitangan lain.

Pendedahan maklumat akaun boleh memerlukan keputusan privasi dan respons pelanggan walaupun akses sistem lebih luas tidak dibuktikan. Pemilik perkhidmatan dan ketua privasi perlu menggunakan fakta sama, termasuk skop maklumat serta asas bagi pengecualian lebih luas.

5.6 Logistik: pemulihan mesti merangkumi aliran kerja yang bersambung

F

KES F

Gangguan terminal dan mula semula berperingkat

Pengangkutan dan logistik

Gangguan perkhidmatan dilaporkan

PERISTIWA DILAPORKAN	Pengendali terminal kontena melaporkan insiden keselamatan siber pada September. Pelaporan industri menerangkan gangguan operasi, sistem dipulihkan dan penyambungan semula operasi secara berperingkat. [S5]
KRONOLOGI	Pelaporan industri pada 11 September menerangkan insiden sejurus sebelum tengah malam pada 9 September dan mula semula berperingkat. Ini tarikh status perkhidmatan, bukan garis masa pencerobohan yang disahkan.
PERKARA YANG DAPAT DIPASTIKAN	Bahan sumber menyokong gangguan, pemulihan berperingkat dan pemulihan sistem yang dilaporkan. Bahan itu tidak membuktikan kren, pengawal industri atau setiap rakan logistik yang bersambung telah dikompromi.
PENJELASAN ALTERNATIF	Dakwaan kecurian data dan gangguan operasi boleh mempunyai sebab atau skop berbeza. Penerbitan pihak yang mendakwa sahaja tidak menentukan hubungannya.
BATAS	Laporan tidak memiliki rekod forensik pihak sasaran. Atribusi perisian tebusan dan jumlah kecurian yang diiklankan kekal sebagai dakwaan berasingan melainkan disahkan pengendali atau pihak berkuasa.
RESPONS	Pasukan operasi dan keselamatan perlu berlatih proses manual pintu terminal, kargo dan penghantaran sensitif suhu. Tetapkan pihak yang mengesahkan antara muka dan menyelaraskan transaksi sebelum perkhidmatan biasa disambung.

Kesimpulan

Uji proses sandaran dan penyelarasan; pemulihan tidak membuktikan pelaku atau jumlah data yang dicuri.

Latihan logistik perlu mengikuti transaksi merentasi antara muka penting. Ujian boleh bermula dengan sistem terminal tidak tersedia dan berakhir dengan rekod kargo yang diselaraskan. Ujian perlu merangkumi komunikasi kepada pengangkut dan pelanggan, pengendalian pengecualian serta kembalinya pemprosesan biasa.

Pemulihan berjaya hanyalah satu kriteria penyempurnaan. Pemilik perniagaan juga perlu mengesahkan rekod tertangguh atau diproses secara manual adalah lengkap. Pasukan keselamatan perlu mendokumentasikan perkara yang disahkan sebelum penyambungan semula. Ini mengelakkan aplikasi berfungsi dianggap sama dengan perkhidmatan yang diselaraskan sepenuhnya.

5.7 Pelaporan kredit: satu persekitaran bukan keseluruhan simpanan data

G

KES G

Maklumat pengguna dalam persekitaran pelaporan kredit

Perkhidmatan maklumat kewangan

Penyedia mengakui akses

PERISTIWA DILAPORKAN	Penyedia pelaporan kredit mendedahkan akses tanpa kebenaran kepada satu persekitaran perniagaan pengguna pada 23 September. Pemfailannya menyebut fail yang mengandungi subset terhad maklumat pengguna telah diakses. Sesetengah perkhidmatan pelaporan tidak tersedia buat sementara. [S6]
KRONOLOGI	Pendedahan 23 September menerangkan sempadan awal akses dan gangguan. Pendedahan itu sendiri tidak menentukan keadaan pemulihan kemudian. Setiap kenyataan status perkhidmatan susulan memerlukan sokongan bertarikh sendiri.
PERKARA YANG DAPAT DIPASTIKAN	Bahan sumber menyokong akses kepada persekitaran yang diterangkan dan gangguan perkhidmatan. Bahan itu tidak membuktikan setiap set data biro atau institusi kewangan pelanggan terjejas.
PENJELASAN ALTERNATIF	Rakan boleh mengalami kelewatan pelaporan tanpa rangkaiannya sendiri diakses. Oleh itu, skop data dan perkhidmatan mesti diperiksa secara berasingan.
BATAS	Laporan tidak menukar anggaran kewangan bersyarat yang kemudian kepada kerugian insiden yang diukur. Laporan tidak mempunyai jumlah bebas pengguna terjejas.

RESPONS	Pemilik kredit dan penipuan perlu mengenal pasti keputusan yang dibuat menggunakan laporan lewat atau alternatif. Semak semula pengecualian selepas pemulihan dan dokumentasikan bukti bagi setiap keputusan.

Kesimpulan

Sahkan sempadan laporan dan data terjejas, kemudian selaraskan keputusan yang dibuat ketika gangguan.

Penerangan khusus penyedia perlu membimbing soalan pertama. Fail manakah terlibat? Laporan manakah tidak tersedia? Pelanggan manakah menerima perkhidmatan berubah? Jawapannya boleh berbeza. Pasukan pertahanan perlu mengekalkan perbezaan tersebut dalam notis pelanggan dan log keputusan dalaman.

Disiplin sama membantu komunikasi kepada subjek data. Akaun dalam persekitaran tidak terjejas tidak patut digambarkan sebagai terdedah semata-mata kerana tergolong dalam kumpulan korporat sama. Sebaliknya, gangguan perkhidmatan boleh memerlukan tindakan operasi sebelum skop penuh data diketahui.

5.8 Penjagaan kesihatan: fail sokongan memerlukan sempadan akses sendiri

H

KES H

Akses terhad fail sokongan didedahkan pada November

Penjagaan kesihatan

Penjelasan rasmi tentang akses terhad

KETERANGAN RASMI	Kenyataan sektor kesihatan yang dipetik dalam pelaporan menyebut insiden dikesan pada 12 November. Keterangan itu menerangkan akses tanpa kebenaran yang terhad kepada platform penyimpanan dan perkongsian fail sokongan di sebuah fasiliti. [S7]
KRONOLOGI	Kenyataan dilaporkan pada 14 November. Kenyataan itu menerangkan sekatan akses, penetapan semula kata laluan, audit dan pengesahan lebih kukuh. Itu langkah yang dinyatakan institusi, bukan tindakan pengarang laporan ini.
PERKARA YANG DAPAT DIPASTIKAN	Kenyataan menyebut sistem operasi utama dan perkhidmatan pesakit tidak terjejas. Dapatan awalnya menyebut pangkalan data utama tidak disulitkan. Ini kenyataan berbeza tentang skop perkhidmatan dan penyulitan.
PENJELASAN ALTERNATIF	Tiada penyulitan pangkalan data utama tidak membuktikan tiada fail dilihat atau dipindahkan keluar. Platform sokongan boleh memerlukan siasatan walaupun rawatan diteruskan.

BATAS	Tiada kaitan pelaku rasmi atau jumlah data terjejas ditentukan dalam keterangan yang dipetik. Laporan tidak menggabungkan episod ini dengan insiden laman web berasingan atau dakwaan pemerasan pelaku.
RESPONS	Pemilik platform perlu mengenal pasti fail, pautan luar dan kebenaran akaun dalam sempadan terjejas. Operasi klinikal perlu mengesahkan status perkhidmatan dan pengaturan kesinambungan secara bebas.

Kesimpulan

Bezakan ketersediaan perkhidmatan pesakit daripada persoalan fail sokongan dan privasi.

Kes ini menunjukkan sebab organisasi kesihatan memerlukan lebih daripada senarai sistem klinikal. Perkhidmatan perkongsian fail boleh menyimpan maklumat operasi atau peribadi walaupun tidak menyediakan rawatan. Pemiliknya perlu mengetahui cara perkongsian luar diluluskan, akses disemak dan pautan digantung tanpa kehilangan rekod yang diperlukan.

Keputusan komunikasi perlu mengikut bukti. Kenyataan tentang rawatan tanpa gangguan menjawab soalan ketersediaan. Kenyataan itu tidak menjawab setiap persoalan privasi. Pasukan keselamatan, privasi dan operasi klinikal perlu menyetujui persoalan yang dijawab setiap ayat.

5.9 Transaksi perkhidmatan awam: integriti boleh memerlukan siasatan tanpa gangguan

Laporan Ogos membawa keterangan pengarah agensi bertanggungjawab tentang kelulusan tanpa kebenaran pada platform transaksi perkhidmatan awam. Laporan menerangkan operasi penguatkuasaan bersama pada Julai. Laporan itu ialah keterangan siasatan pihak berkuasa, bukan dapatan mahkamah atau pengesahan bebas setiap butiran teknikal yang didakwa. [S30]

Kes ini menyokong persoalan berbeza daripada pemantauan ketersediaan: adakah transaksi diluluskan seperti yang dimaksudkan? Platform boleh terus memberikan respons sementara integriti kelulusannya memerlukan siasatan. Laporan tidak menyimpulkan perkara ini berlaku pada perkhidmatan awam lain atau menggabungkannya dengan gangguan teknikal yang dilaporkan berasingan.

Bagi pemilik perkhidmatan, semakan pertama melibatkan sejarah transaksi, akses istimewa dan aliran kelulusan. Kenyataan penyiasat tentang penglibatan yang didakwa perlu kekal dikaitkan dengan mereka. Semakan pertahanan boleh menguji pengasingan tugas dan akses pembekal tanpa menyalahkan sesiapa atau membuat dakwaan lebih luas tentang pekerja.

Bukti penyempurnaan perlu menghubungkan setiap kelulusan berkaitan dengan rekod dibenarkan serta individu atau perkhidmatan yang dibenarkan melakukannya. Pengecualian belum selesai perlu kekal terlihat kepada pemilik perniagaan dan insiden. Halaman awam yang normal tidak menjawab persoalan integriti ini.

5.10 Perkhidmatan berhadapan orang ramai: peristiwa laman web tidak mengenal pasti laluan masuk di tempat lain

Amaran sambungan pada akhir Jun dan keterangan laman web korporat November sama-sama melibatkan kandungan menghadap internet, tetapi tidak membuktikan kempen bersama. Amaran Jun menamakan kerentanan teknikal. Pelaporan November memetik penjelasan teknikal pihak ketiga. Laporan mengekalkan keterangan sumber itu secara berasingan. [S18][S8]

Organisasi perlu menyimpan inventori sambungan pengurusan kandungan, pemilik kemas kini dan laluan kepada sumber pemulihan dipercayai. Halaman utama yang kembali normal tidak cukup untuk membuktikan ketiadaan akaun atau fail tanpa kebenaran. Kes E dalam Bab 7 menerangkan panduan versi yang disahkan.

Bagi organisasi kewangan atau perkhidmatan awam, komunikasi status perlu menamakan fungsi terjejas. "Laman web korporat tidak tersedia" lebih tepat daripada kenyataan tentang semua operasi digital. Matriks perkhidmatan sokongan perlu tersedia kepada ketua insiden apabila fakta berubah.

Episod laman web awam turut menunjukkan perbezaan antara pemerhatian dan kenyataan sebab. Pelaporan menerangkan perubahan luaran laman web; institusi memberikan penjelasan teknikal pihak ketiga. Laporan ini merekodkan kedua-duanya tanpa menyimpulkan pencerobohan lebih luas. [S31][S8]

Perkara	Pemerhatian awam	Keterangan institusi	Perkara belum terjawab
Laman web	Sebuah penerbitan melaporkan kandungan laman awam diubah [S31]	Institusi menerangkan masalah laman korporat [S8]	Pemerhatian sahaja tidak membuktikan akses dalaman
Skop perkhidmatan	Keadaan luaran laman tidak mengukur akses transaksi atau data	Institusi berkata perkhidmatan perbankan, deposit dan maklumat pelanggan tidak terjejas [S8]	Laporan tidak mempunyai rekod forensik bebas tentang peristiwa itu
Sebab	Perubahan yang kelihatan tidak menentukan sebabnya	Institusi merujuk masalah teknikal pihak ketiga [S8]	Dakwaan pelaku yang lebih luas memerlukan sokongan berasingan

5.11 Notis pembekal penerbangan: kemungkinan kesan pelanggan bukan pengesahan akses sistem syarikat penerbangan

Laporan 1 November memetik kenyataan laman web sebuah syarikat penerbangan pada 31 Oktober tentang pembekal tempahannya. Kenyataan menyebut sebahagian data pelanggan yang diproses antara Ogos 2023 dan September 2026 mungkin terjejas. Kenyataan membezakan insiden pembekal daripada sistem IT sendiri dan melaporkan tiada bukti akses maklumat kewangan pada tarikh itu. [S32]

Tarikh tersebut menerangkan tempoh pemprosesan, bukan tempoh pencerobohan yang disahkan. Kemungkinan kesan pelanggan bukan jumlah individu terjejas yang disahkan. Laporan tidak memindahkan bilangan tempahan syarikat penerbangan lain kepada pelanggan Malaysia atau menganggap seluruh pangkalan pelanggan pembekal terjejas.

Keterangan kekal dikaitkan dengan pelaporan kenyataan syarikat. Keterangan itu dianggap pendedahan kebergantungan pembekal di luar kiraan lapan insiden berskop individu. Laporan mengekalkan kelayakan kemungkinan kesan dan ketiadaan bukti.

Pemilik perjalanan dan perkhidmatan pelanggan perlu mengenal pasti tempahan serta medan yang diliputi notis pembekal. Mereka perlu meminta kenyataan kesan bertarikh dan mengekalkan perbezaan antara data tempahan, maklumat bayaran serta sistem syarikat penerbangan sendiri. Amaran pelanggan perlu sepadan dengan sempadan itu dan tidak mengulangi dakwaan pelaku yang lebih besar.

5.12 Paparan awam memerlukan pelan akses vendor dan pengasingan

Pada 29 Oktober, sistem paparan awam perbandaran memaparkan kandungan tanpa kebenaran. Pelaporan memetik pihak berkuasa yang berkata paparan ditutup dan siasatan dijalankan bersama vendor. Polis kemudian mengesahkan siasatan. Laluan akses, pengendali dan sempadan rangkaian lebih luas tidak ditentukan dalam pelaporan yang disemak. [S25][S26]

Ini satu insiden sistem yang dilaporkan, bukan insiden berasingan bagi setiap paparan. Insiden ini tidak membuktikan perisian tebusan atau akses sistem kawalan operasi. Masukkan paparan yang diurus pihak luar dalam inventori aset, hadkan pentadbiran vendor dan uji prosedur pengasingan serta pemulihan yang selamat.

5.13 Tindakan perlindungan tidak membuktikan dapatan insiden yang lengkap

Pada 10 November, pelaporan memetik pengerusi sebuah badan awam yang menerangkan kerjasama perlindungan berhubung aktiviti laman web yang disyaki. Pengerusi berkata laporan penuh masih belum diterima. Laporan ini mengekalkan sebutan aktiviti disyaki tanpa menganggapnya akses sistem, kecurian data atau gangguan perkhidmatan yang disahkan. [S33]

Ketua insiden perlu membezakan tindakan perlindungan daripada siasatan lengkap. Rekodkan bukti perkhidmatan dan akses yang tersedia, soalan belum terjawab dan individu yang bertanggungjawab bagi kemas kini seterusnya. Halaman yang normal kemudian tidak dengan sendirinya menentukan dakwaan terdahulu.

DAPATAN UTAMA

01

Kekalkan sempadan setiap penyedia, platform dan perkhidmatan secara berasingan, termasuk semasa pemulihan.

02

Pengesahan insiden tidak mengesahkan pelaku, jumlah diiklankan atau sebab.

03

Berikan setiap proses terjejas pemilik tanggungjawab, kaedah sandaran dan bukti untuk kembali kepada perkhidmatan biasa.

BAB 06

Hacktivisme dan DDoS

06

SOALAN YANG DIJAWAB BAB INI

Apakah yang boleh dibuktikan masing-masing oleh kenyataan persona, dakwaan ketersediaan dan amaran rasmi laman web?

27–28

siaran relevan dikekalkan yang membawa tema hacktivisme atau DDoS

6.1 Ketersediaan, pengubahan dan akses ialah pernyataan berbeza 48

6.2 Penafian berbahasa Melayu ialah kenyataan persona 48

6.3 Amaran rasmi laman web mempunyai sempadan bukti berasingan 49

6.4 Dakwaan perlu mencetuskan tugas pengesahan berbatas 50

6.5 Pisahkan retorik daripada bukti 50

BAB 06

Hacktivisme dan DDoS

RINGKASAN

Set relevan dikekalkan mengandungi 27–28 siaran bertema hacktivisme atau DDoS. Ini pemerhatian kandungan, bukan gangguan disahkan. Kenyataan persona berbahasa Melayu menafikan penggodaman dan mengingatkan tentang penyamaran. Secara berasingan, pelaporan teknikal rasmi menerangkan serangan melibatkan sambungan laman web. Tiada hubungan antara pernyataan itu dibuktikan di sini. Sahkan kesan perkhidmatan, akses dan kepengarangan secara berasingan menggunakan pemantauan, log dan keterangan insiden organisasi.

DDoS bermaksud penafian perkhidmatan teragih: serangan daripada pelbagai sumber yang bertujuan mengganggu akses kepada sistem atau perkhidmatan. [S58]

6.1 Ketersediaan, pengubahan dan akses ialah pernyataan berbeza

Sumber merekodkan 27–28 siaran relevan dikekalkan yang membawa tema hacktivisme atau DDoS. Julat terhad ini tidak mengukur seluruh aktiviti DDoS negara, pengubahan laman web disahkan atau pencerobohan berjaya. Sebutan negara, label saluran atau slogan pelaku tidak membuktikan perkhidmatan Malaysia terjejas. [S3]

Tangkap layar ketersediaan boleh menunjukkan satu pemerhatian pada satu masa. Ia tidak membuktikan tempoh, sebab atau kesan gangguan kepada pelanggan. Penerangan serangan pihak yang mendakwa juga tidak membuktikan sama ada akses melangkaui laman web awam.

Halaman diubah ialah pernyataan berbeza daripada banjir trafik. Kedua-duanya boleh memberi kesan perniagaan, tetapi setiap satu memerlukan bukti sokongan. Pasukan pertahanan perlu mengekalkan rekod perkhidmatan, log akses berkaitan dan sempadan pemulihan sebelum menentukan sebab atau menerima keterangan pelaku.

6.2 Penafian berbahasa Melayu ialah kenyataan persona

Siaran dikekalkan bertarikh 9 Mac muncul di bawah label MalaysiaHacktivist. Kenyataan menafikan penggodaman laman web kerajaan atau individu lain dan mengingatkan tentang penyamaran. Ia membuktikan perkara diterbitkan persona tersebut. Ia tidak membuktikan pengarang, kebenaran penafian atau tanggungjawab terhadap peristiwa lain. [S3]

Kad bukti B08 9 Mac 2026

MalaysiaHacktivist Hantaran saluran yang disimpan Telegram Melayu

TEKS ASAL

Pihak Kami tidak melalukan perbuatan menggodam website kerajaan atau individu lain.

TERJEMAHAN

Kami tidak melakukan perbuatan menggodam laman web kerajaan atau individu lain.

Nota. Kenyataan persona sahaja; tiada hubungan dengan kejadian laman web lain dibuktikan.

Bukti disimpan
Kenyataan itu sendiri dan label persona yang menerbitkannya.

Belum disahkan
Identiti penulis, kebenaran penafian, pihak yang melakukan aktiviti lain dan hubungan dengan kejadian laman web berasingan belum dibuktikan.

[GROUP malaysia-persona]

Kenyataan penting kerana nama boleh beredar secara berasingan daripada pengarangnya. Identiti didakwa tidak patut secara automatik mewarisi tanggungjawab siaran atau peristiwa laman web berasingan. Sebaliknya, penafian bukan bukti bebas bahawa peristiwa tidak berlaku. Siasatan mesti mengekalkan perbezaan antara kenyataan diterbitkan dan atribusi disahkan.

6.3 Amaran rasmi laman web mempunyai sempadan bukti berasingan

Amaran NC4 pada akhir Jun menerangkan serangan melibatkan sambungan JCE untuk Joomla. Sumber vendor dan Program CVE menangani kerentanan serta sempadan versi dibaiki. Sumber menyokong pemulihan teknikal tanpa mengenal pasti pihak yang menyebabkan setiap peristiwa laman web dalam tempoh itu. Bab 7 menghuraikan kes teknikal dan batasnya. [S18][S19][S34]

Kenyataan Mac dikekalkan tidak membuktikan hubungan dengan amaran Jun. Tarikh, subjek dan jenis bukti berbeza. Istilah laman web serupa atau rujukan kebangsaan tidak menyediakan hubungan yang hilang.

9 Mac 2026	**Kenyataan persona** Siaran Melayu dikekalkan menafikan penggodaman dan mengingatkan tentang penyamaran; identiti dan kebenaran kekal belum disahkan. [S3]
26 Jun 2026	**Amaran teknikal** NC4 menerangkan serangan melibatkan sambungan laman web; amaran tidak mengatribusi setiap peristiwa laman web sezaman. [S18]

Garis masa meletakkan dua pemerhatian mengikut urutan. Ia bukan rantaian kempen, dapatan atribusi atau bukti penyelarasan. Nasihat rasmi kemudian tidak boleh mengesahkan kenyataan persona terdahulu secara retrospektif.

6.4 Dakwaan perlu mencetuskan tugas pengesahan berbatas

Pernyataan diterima	Pemilik pertama	Bukti yang menjawabnya	Syarat eskalasi
Perkhidmatan tidak tersedia	Operasi perkhidmatan	Sejarah ketersediaan dan rekod trafik huluan	Kesan perkhidmatan berterusan atau material disokong pemantauan
Kandungan awam diubah	Pasukan web dan keselamatan	Perbandingan kandungan dipercayai dan aktiviti pentadbiran	Perubahan tanpa kebenaran atau bukti akses
Akses dalaman didakwa	Respons insiden	Rekod akaun, sesi dan sistem berkaitan	Akses kepada sempadan didakwa disokong bukti pengukuh
Fail didakwa diperoleh	Pasukan keselamatan dan privasi	Perbandingan medan serta asal usul dibenarkan	Rekod berkaitan atau pendedahan disokong bukti
Identiti persona didakwa	Ketua insiden	Kepengarangan dan hubungan disokong secara bebas	Bukti menghubungkan persona dengan peristiwa khusus

Organisasi boleh mengesahkan masalah perkhidmatan sementara pelaku, sebab dan jumlah data didakwa belum ditentukan. Oleh itu, pemulihan perlu merekodkan perkara dipulihkan, akses dibuang dan soalan masih terbuka. Halaman utama normal sahaja tidak membuktikan keadaan perkhidmatan dalaman.

Komunikasi operasi perlu menyatakan sempadan diketahui dan keputusan seterusnya. Insiden ketersediaan mungkin memerlukan saluran pelanggan alternatif. Dapatan pendedahan disokong mungkin memerlukan penilaian privasi. Dakwaan tanpa bukti pengukuh masih wajar menerima keputusan didokumentasikan, dengan pencetus pembukaan semula.

6.5 Pisahkan retorik daripada bukti

Laporan tidak mengambil pendirian politik daripada bahan pihak yang mendakwa. Slogan dan label pelaku ialah kenyataan sumber. Bahasa tidak membuktikan kewarganegaraan, dan tema politik tidak membuktikan arahan negara atau penyelarasan antara persona.

Soalan pertahanan berguna ialah pernyataan perkhidmatan atau data yang boleh diuji. Ini menumpukan perhatian kepada kesinambungan, kawalan akaun dan bukti privasi. Ini juga mengelakkan dakwaan berulang, siaran disampaikan semula atau penafian dianggap sebagai bilangan serangan bebas.

DAPATAN UTAMA

01

27–28 siaran relevan tidak mengukur insiden DDoS disahkan.

02

Kenyataan persona dan amaran rasmi laman web menyokong pernyataan berbeza, tanpa hubungan dibuktikan.

03

Sahkan kesan, akses dan kepengarangan secara berasingan, kemudian ikat komunikasi pemulihan kepada sempadan disokong.

BAB 07

Pelaku ancaman

07

SOALAN YANG DIJAWAB BAB INI

Pernyataan tentang pelaku manakah disokong, dan bagaimanakah pasukan pertahanan boleh menggunakannya tanpa melebih-lebihkan atribusi?

87

penyenaraian Malaysia pada laman kebocoran perisian tebusan dalam tempoh pelaporan

7.1 Cara membaca hubungan 53
7.2 Bukti teknikal tanpa atribusi pelaku 54
7.3 Dakwaan hacktivis memerlukan bukti ketersediaan dan akses 55
7.4 Perisian tebusan dan pemerasan 55
7.5 Persona jenayah dan pernyataan data 58

BAB 07

Pelaku ancaman

RINGKASAN

Ransompedia merekodkan 87 penyenaraian Malaysia bertarikh 1 Januari–22 November 2026. Qilin dan The Gentlemen menyumbang 30 daripadanya. Itu penerbitan pemerasan, bukan pencerobohan disahkan atau bilangan unik individu terjejas. Amaran teknikal dan kenyataan insiden rasmi menjawab persoalan berbeza. Gunakan maklumat pelaku untuk membimbing pengesahan dan perancangan pemulihan, sambil mengikat identiti, sebab serta kesan kepada bukti masing-masing.

7.1 Cara membaca hubungan

Peta hubungan menunjukkan perkaitan sumber penyenaraian Ransompedia dengan Qilin dan The Gentlemen, serta kenyataan B08 yang diterbitkan persona. Hubungan ini membuktikan label penyenaraian dan penerbitan, tanpa mengesahkan pencerobohan, kepengarangan atau kebenaran kenyataan.

Disiplin sama terpakai kepada perisian tebusan. Ransompedia ialah sumber data milik Brandefense bagi pemerhatian penyenaraian. Hubungannya dengan pelaku dalam peta bermakna sumber itu menyimpan penerbitan menggunakan nama tersebut. Ia tidak membuktikan pengesahan organisasi terhadap dakwaan atau kawalan eksklusif pelaku ke atas insiden. [S4]



Sebarang pengelompokan lebih luas tanpa hubungan sokongan konkrit ialah model analisis. Laporan tidak menyimpulkan pengendali bersama daripada rujukan negara sama, tema politik serupa atau dua iklan dengan medan sama. Pasukan pertahanan tidak patut menggabungkan baris siasatan berasingan semata-mata kerana label pelaku menyerupai satu sama lain.

7.2 Bukti teknikal tanpa atribusi pelaku

KES E

E

Amaran sambungan pengurusan kandungan memerlukan bukti tampalan dan pembasmian

Amaran teknikal rasmi

Laman web untuk orang ramai

KETERANGAN RASMI	Amaran NC4 pada akhir Jun menerangkan serangan melibatkan sambungan JCE untuk Joomla. Rekod CVE menerangkan CVE-2026-48907 sebagai membenarkan penciptaan profil penyunting tanpa pengesahan yang boleh membawa kepada muat naik PHP dan pelaksanaan kod. [S18] [S34]
SKOP VERSI	Rekod CVE menyenaraikan JCE 1.0.0–2.9.99[.]4 sebagai terjejas. Keluaran pertama yang ditampal ialah 2.9.99[.]5. Pasang keluaran vendor serasi terkini, 2.9.99[.]9 atau lebih baharu; nasihat itu menyediakan tampalan sementara untuk pemasangan lama. Kemas kini tidak membersihkan laman yang sudah terjejas. [S34][S19]
PERKARA YANG DAPAT DIPASTIKAN	Sumber menyokong kerentanan dan serangan dilaporkan yang melibatkannya. Sumber tidak menentukan pelaku yang bertanggungjawab bagi setiap insiden laman web dalam tempoh itu.
PENJELASAN ALTERNATIF	Laman web boleh diubah melalui komponen terdedah lain, akaun pentadbir dicuri atau masalah pengehosan. Halaman yang kelihatan serupa tidak menentukan laluan masuk.
BATAS	Laporan tidak memiliki rekod forensik pemasangan individu yang terjejas. Laporan tidak menerbitkan domain mangsa atau mendakwa setiap pencacatan laman Jun menggunakan kelemahan ini.
RESPONS	Pemilik web perlu membuktikan sambungan terpasang telah dibaiki dan menyiasat profil serta fail tanpa kebenaran secara berasingan. Jika perlu, pulihkan keadaan dipercayai dan sahkan akaun pentadbir sebelum membuka semula perkhidmatan.

Kesimpulan

Buktikan keadaan sambungan yang telah dibaiki dan tentukan secara berasingan sama ada akses tanpa kebenaran masih wujud.

Perbezaan penting ialah mencegah kemasukan baharu dan membuang akses yang sudah diwujudkan. Kemas kini boleh menjawab soalan pertama sementara soalan kedua belum terjawab. Oleh itu, bukti penyempurnaan perlu merangkumi versi terpasang, hasil siasatan dan kelulusan pemilik perniagaan untuk mengembalikan perkhidmatan kepada operasi biasa.

Ketua insiden juga perlu mengekalkan sempadan masa. Imbasan bersih atau halaman utama normal yang diperoleh kemudian ialah pemerhatian pada masa kemudian. Ia tidak membuktikan laman itu tiada fail tanpa kebenaran dalam tempoh terdahulu. Laporan mencadangkan log berkaitan dikekalkan dan ketidakpastian itu didokumentasikan.

Kerentanan sahaja tidak menentukan identiti pelaku negara atau jenayah. Penjelasan teknikal sumber berguna tanpa menambah keterangan geopolitik yang tidak disokong. Peraturan sama terpakai kepada alat pengurusan jauh dalam amaran skrip pemesejan Jun: kehadiran alat tidak membuktikan penggunanya. [S11]

7.3 Dakwaan hacktivis memerlukan bukti ketersediaan dan akses

Pihak yang mendakwa boleh menamakan laman web awam, menunjukkan tangkap layar atau merujuk semakan ketersediaan. Bahan itu perlu direkodkan mengikut nilai buktinya. Bahan tersebut sendiri tidak membuktikan tempoh perkhidmatan tidak tersedia, pelanggan terjejas atau kewujudan akses dalaman.

Bagi organisasi yang dinamakan dalam dakwaan, pengesahan pertama perlu sepadan dengan pernyataan. Dakwaan ketersediaan memerlukan pemantauan perkhidmatan dan rekod trafik huluan. Dakwaan fail dalaman memerlukan semakan akses berskop. Dakwaan akaun istimewa memerlukan semakan akaun dan sesi. Respons perlu ditingkatkan apabila disokong bukti pengukuh.

Keterangan platform sokongan kesihatan dan keterangan laman web bank yang berasingan menunjukkan sebab naratif pelaku luas boleh mengelirukan. Penjelasan rasmi masing-masing menerangkan sempadan berbeza. Laporan tidak menggantikan mana-mana keterangan itu dengan penerangan pelaku yang lebih luas. [S7][S8]

Atribusi perlu kekal terikat pada sumbernya. Bahasa, rujukan negara dan slogan pelaku bukan bukti kewarganegaraan atau arahan negara. Laporan tidak mengulangi pembingkaian berat sebelah atau membuat kesimpulan dasar awam daripada kenyataan pihak yang mendakwa.

7.4 Perisian tebusan dan pemerasan

Ransompedia merekodkan 87 penyenaraian Malaysia dalam tempoh pelaporan. Bilangan terbesar ialah Qilin dengan 18 dan The Gentlemen dengan 12. Bersama-sama, kedua-duanya menyumbang 30 daripada 87 penyenaraian, atau 34.5%. Baki 57 penyenaraian menggunakan nama kumpulan lain. [S4]

Malaysia mempunyai 87 penyenaraian dalam tempoh sama dengan empat negara serantau setanding



Sumber: Brandefense Ransompedia, 1 Januari–22 November 2026; November belum lengkap [S4]. Penerbitan berlabel negara, bukan pencerobohan disahkan atau pemeringkatan keselamatan kebangsaan.

Negara-negara perbandingan dipilih sebagai contoh semata-mata untuk memberikan konteks; pemilihan ini tidak menunjukkan sebarang pemeringkatan atau penilaian politik.

Perbandingan serantau menerangkan keterlihatan sumber. Perbandingan itu tidak melaraskan populasi, bilangan organisasi, amalan pendedahan atau liputan pelaporan kebangsaan.

Negara	Penyenaraian dalam tempoh	Kumpulan terbesar disenaraikan	Batas pembacaan
Malaysia	87	Qilin, 18	Penerbitan yang menamakan organisasi Malaysia
Singapura	110	Qilin, 12	Ekonomi dan liputan pendedahan berbeza
Indonesia	74	Nova, 9	Skala negara berbeza
Thailand	125	The Gentlemen, 43	Tempoh penerbitan sama
Filipina	49	Qilin, 17	Komposisi sektor dan sumber berbeza

Negara setanding dipilih kerana relevan kepada perniagaan dan pembekal serantau. Singapura menyediakan perbandingan kewangan serta perkhidmatan digital berjiran. Indonesia menambah ekonomi digital berjiran yang lebih besar. Thailand menambah konteks pembuatan dan pelancongan. Filipina menambah konteks perkhidmatan dan operasi disumber luar. Ini perbandingan operasi, bukan pemeringkatan keselamatan negara.

Bilangan bulanan Malaysia berjulat daripada tiga pada September kepada 18 pada Oktober. Oktober menyumbang 20.7% daripada 87 penyenaraian dalam tempoh itu. November menyumbang lapan hingga tarikh tutup dan belum lengkap. Tarikh penerbitan ini tidak menentukan masa pencerobohan bermula. [S4]

Enam rekod penyenaraian Malaysia yang dikekalkan bertarikh 8–22 November. Ini penerbitan terkini, bukan enam pencerobohan baharu yang disahkan. [S4]

Label sektor sumber meletakkan sembilan penyenaraian masing-masing dalam hospitaliti dan logistik, serta lapan masing-masing dalam perundingan dan pembuatan. Label itu menerangkan penyenaraian dan berbeza daripada sektor organisasi terpilih laporan. Jangan gabungkannya seolah-olah populasinya sama. Label suapan luas atau tidak pasti tidak ditetapkan semula kepada sektor lebih khusus tanpa bukti.

Qilin

Jenama penyenaraian perisian tebusan dan pemerasan | Nama kumpulan yang dikaitkan dengan pemerhatian penyenaraian Ransompedia

DI MALAYSIA, 2026

2026

18 penyenaraian Malaysia bertarikh 1 Januari–22 November

SASARAN DIDAKWA

Organisasi yang dinamakan dalam penerbitan laman kebocoran; identiti individu tidak dipaparkan

DALAM PELAPORAN AWAM

[S4] 18 daripada 87 penyenaraian Malaysia dalam tempoh laporan

PENILAIAN KAMI

Bilangan penyenaraian diperhatikan. Pencerobohan asas, jumlah data terjejas dan tanggungjawab pelaku memerlukan pengesahan masing-masing. Perancangan pemulihan tidak seharusnya bergantung pada satu nama kumpulan.

KEYAKINAN

Tinggi bagi bilangan penyenaraian yang disimpan; dakwaan asas belum disahkan

The Gentlemen

Jenama penyenaraian perisian tebusan dan pemerasan | Nama kumpulan yang dikaitkan dengan pemerhatian penyenaraian Ransompedia

DI MALAYSIA, 2026

2026

12 penyenaraian Malaysia bertarikh 1 Januari–22 November

SASARAN DIDAKWA

Organisasi yang dinamakan dalam penerbitan laman kebocoran; identiti individu tidak dipaparkan

DALAM PELAPORAN AWAM

[S4] 12 daripada 87 penyenaraian Malaysia dalam tempoh laporan

PENILAIAN KAMI

Bilangan penyenaraian diperhatikan. Pencerobohan asas, jumlah data terjejas dan tanggungjawab pelaku memerlukan pengesahan masing-masing. Perancangan pemulihan tidak seharusnya bergantung pada satu nama kumpulan.

KEYAKINAN

Tinggi bagi bilangan penyenaraian yang disimpan; dakwaan asas belum disahkan

Bagi perancangan pemulihan, perkara berguna ialah beberapa jenama pemerasan muncul, tanpa satu nama meliputi keseluruhan set diperhatikan. Sandaran diuji, keputusan pembendungan, kebergantungan pembekal dan saluran komunikasi perlu berfungsi tanpa mengira kumpulan yang menerbitkan dakwaan. Ketiadaan kumpulan daripada senarai bukan alasan menangguhkan siasatan insiden yang berasas.

7.5 Persona jenayah dan pernyataan data

Persona, jenama penjual, iklan dan set data yang didakwa ialah entiti berbeza. Satu persona boleh mengiklankan beberapa produk tidak berkaitan. Beberapa persona boleh mengulangi iklan serupa. Kedua-dua pemerhatian tidak mengenal pasti sumber data asal, membuktikan pemilikan atau membuktikan transaksi selesai.

Laporan merekodkan pernyataan terkuat yang disokong setiap kad dikekalkan. Tawaran mungkin membuktikan harga diminta dan senarai medan. Tajuk berulang mungkin membuktikan penyebaran. Penyenaraian kelayakan semasa boleh mewajarkan baris pengesahan. Semua itu tidak patut diam-diam menjadi pencerobohan disahkan dalam ringkasan atau pelan tindakan.

Disiplin ini turut mencegah profil pelaku yang mengelirukan. Keyakinan terpakai kepada pernyataan, seperti tarikh siaran atau senarai medan sepadan. Keyakinan tidak patut dilekatkan pada seluruh persona seolah-olah setiap dakwaan masa depan mewarisi kebolehpercayaan yang sama.

DAPATAN UTAMA

01

Qilin dan The Gentlemen menyumbang 30 daripada 87 penyenaraian Malaysia yang diperhatikan, setiap satu masih dakwaan.

02

Amaran teknikal boleh menyokong pemulihan tanpa menentukan pelaku.

03

Sahkan hubungan dan kesan secara berasingan, kemudian gunakan pelan pemulihan yang tidak bergantung pada nama kumpulan.

BAB 08

Ekonomi penipuan

08

SOALAN YANG DIJAWAB BAB INI

Bagaimanakah umpan yang dilaporkan menukar maklumat identiti, pemesejan dan bayaran kepada baris respons pasukan pertahanan?

3

laluan respons: bayaran, akaun dan peranti akhir

8.1 Keputusan kawalan akaun dan bayaran 60
8.2 Pemerhatian kad bayaran: pandangan terhad 60
8.3 Umpan bantuan meminta maklumat bayaran dan identiti 61
8.4 Umpan komputer riba percuma meminta kawalan akaun pemesejan 62
8.5 Umpan dokumen memerlukan respons peranti akhir 63
8.6 Harga dan tawaran tidak mengukur hasil pasaran 63
8.7 Perkara yang disokong bukti kempen 63
8.8 Amaran kempen mengekalkan batas masing-masing 64

BAB 08

Ekonomi penipuan

RINGKASAN

Bukti kempen awam terkuat melibatkan umpan pemesejan yang meminta pengguna menyerahkan data atau menjalankan fail. Respons berkaitan bergantung pada perkara yang didedahkan atau dilancarkan. Butiran identiti dan bayaran, kod log masuk pemesejan dan skrip Windows mewujudkan laluan siasatan berbeza. Wujudkan rekod penerimaan ringkas, halakannya kepada pemilik tanggungjawab yang betul dan sahkan akaun, kad atau peranti terjejas.

8.1 Keputusan kawalan akaun dan bayaran

Laporan penipuan perlu bermula dengan tindakan diminta dan tindakan sebenar. Tawaran tugasan berbayar berbeza daripada permintaan kod log masuk akaun. Bayaran kepada penerima baharu berbeza daripada nombor kad dimasukkan ke borang. Pengelompokan sebagai satu kategori boleh menyembunyikan kawalan yang memerlukan perhatian.

Laporan tawaran tugasan atau pekerjaan perlu mengenal pasti tahap penerima diminta menghantar wang. Bayaran kecil awal atau tugasan selesai tidak patut menggantikan pengesahan permintaan kemudian. Laporan mencadangkan arahan bayaran dan respons sebenar pengguna direkodkan.

Bagi bank atau majikan, titik campur tangan berguna ialah peralihan daripada tugasan kecil kepada permintaan bayaran. Laporan mencadangkan saluran eskalasi jelas bagi kakitangan atau pelanggan yang diminta membiayai tugasan. Kes perlu mengekalkan destinasi serta masa bayaran melalui saluran insiden biasa tanpa menerbitkan semula butiran peribadi.

Organisasi juga perlu membezakan dakwaan akses penipu daripada penggunaan maklumat yang diperoleh di tempat lain. Mesej yang mengandungi nama sebenar atau butiran akaun boleh meyakinkan. Ia tidak membuktikan penghantar boleh mengakses sistem organisasi. Kakitangan perkhidmatan pelanggan memerlukan prosedur yang mengelakkan pengesahan butiran sensitif tambahan kepada pemanggil.

8.2 Pemerhatian kad bayaran: pandangan terhad

SKOP ANGKA KAD

Angka kad bayaran mempunyai liputan terhad. Angka ini tidak menganggarkan kecurian kad kebangsaan, kebolehgunaan kad atau kerugian penipuan di Malaysia.

Agregat kad bayaran mengandungi 1,244 kad berbeza yang dikaitkan dengan Malaysia merentasi 1,534 kemunculan. Agregat ini merangkumi 1,256 rekod sumber, 190 julat pengenalan pengeluar berbeza dan 13 pengeluar bernama. Subset bank pengeluar dalam Bab 9 mengandungi 945 kad tersebut. Ini penyebut berbeza, bukan jumlah kebangsaan tambahan. [S13]

Bahan kad ialah satu pandangan terhad terhadap masalah penipuan lebih luas. Rekod kad diperhatikan tidak membuktikan transaksi berjaya, kad masih boleh digunakan atau bank pengeluar ialah sumber. Respons pengeluar perlu berdasarkan pengesahan dan bukti transaksinya sendiri.

Persoalan operasi berkaitan ialah perkara yang dimasukkan pemegang kad dan sama ada aktiviti berkaitan muncul dalam rekod pengeluar. Laporan halaman mencurigakan tidak patut ditukar kepada arahan pengeluaran semula kad secara pukal tanpa penilaian itu. Respons mesti mengekalkan perbezaan antara pendedahan, cubaan penggunaan dan kerugian disahkan.

8.3 Umpan bantuan meminta maklumat bayaran dan identiti

KES I

Portal pancingan data bertema bantuan

Penyamaran perkhidmatan awam

Nasihat kempen MyCERT

KETERANGAN RASMI	Nasihat MyCERT pada 11 November menerangkan umpan bertema bantuan yang diedarkan melalui SMS dan WhatsApp. Nasihat menyebut portal mengumpulkan maklumat identiti, kad bayaran dan kata laluan sekali guna. MyCERT merekodkan pengesahan pada 26 Oktober. [S9]
PERKARA YANG DAPAT DIPASTIKAN	Sumber menyokong umpan dan medan pengumpulannya. Sumber tidak memberikan jumlah mangsa sebenar, bayaran disahkan atau kerugian penipuan.
PENJELASAN ALTERNATIF	Penerima boleh menemui halaman tanpa menyerahkan apa-apa. Individu yang memasukkan butiran identiti memerlukan respons berbeza daripada individu yang turut menyerahkan maklumat kad atau kod pengesahan.
BATAS	Peniruan program awam tidak membuktikan akses kepada sistem program itu. Laporan tidak mengulangi dakwaan kelayakan sebagai fakta tentang manfaat sebenar.
RESPONS	Tanya pengguna perkara yang dimasukkan. Halakan butiran kad kepada pengeluar, kelayakan atau kod akaun kepada pemilik akaun berkaitan, dan aktiviti peranti disyaki kepada siasatan peranti akhir.

Kesimpulan

Kenal pasti maklumat yang dihantar dan urus keputusan pembayaran, akaun serta peranti secara berasingan.

Proses penerimaan perlu cukup ringkas untuk meja bantuan atau pusat panggilan. Proses itu perlu mengenal pasti saluran komunikasi, masa, halaman dilawati, maklumat diserahkan dan sebarang transaksi atau log masuk susulan. Ini rekod respons yang dicadangkan, bukan dakwaan tentang tingkah laku mangsa kempen.

Apabila kod pengesahan diserahkan, pemilik akaun perlu meneliti sesi aktif dan perubahan terkini. Apabila maklumat bayaran diserahkan, pengeluar perlu menilai cubaan transaksi melalui proses ditetapkan. Tindakan ini boleh berjalan serentak jika pengguna menyerahkan kedua-duanya.

8.4 Umpan komputer riba percuma meminta kawalan akaun pemesejan

J

KES J

Semakan kelayakan palsu meminta kod log masuk

Akaun pemesejan

Nasihat kempen MyCERT

KETERANGAN RASMI	Nasihat MyCERT pada 20 November menerangkan poster komputer riba percuma yang membawa kepada semakan kelayakan palsu. Halaman itu meminta maklumat peribadi, kod log masuk akaun pemesejan dan kata laluan dua langkah. MyCERT merekodkan pengesahan semula pada 13 November. [S10]
PERKARA YANG DAPAT DIPASTIKAN	Nasihat menyokong mekanisme pancingan data aktif pada tarikh dinyatakan. Nasihat tidak membuktikan setiap penerima kehilangan akaun atau sistem majikan diakses.
PENJELASAN ALTERNATIF	Pengguna mungkin menyerahkan maklumat peribadi tanpa kod log masuk, atau kod tanpa melengkapkan langkah kemudian. Respons perlu menentukan urutan sebenar.
BATAS	Umpan serupa tidak membuktikan pengendali bersama. Sebarang penilaian sumber tentang gelombang terdahulu perlu mengekalkan keyakinannya sendiri dan tidak menjadi dakwaan identiti.
RESPONS	Semak dan tamatkan sesi tanpa kebenaran, pulihkan kata laluan dua langkah yang unik dan semak mesej yang dihantar seterusnya. Jika peranti kerja terlibat, siasat mengikut bukti pelaksanaan atau akses.

Kesimpulan

Semak sesi dan mesej yang diteruskan tanpa menyimpulkan bahawa sistem majikan mengalami insiden.

Perbezaan penting daripada Kes I ialah aset yang diminta halaman. Akaun pemesejan boleh membawa perbualan dan hubungan dipercayai walaupun tiada medan kad bayaran. Laporan mencadangkan mesej susulan diperiksa kerana pemilik akaun perlu mengetahui tindakan selepas akses disyaki.

Organisasi perlu memberikan kakitangan cara melaporkannya dengan cepat. Individu yang bimbang tentang akaun pemesejan peribadi mungkin tidak menyedari kaitannya dengan peranti kerja atau perbualan perniagaan. Meja bantuan perlu bertanya soalan berasaskan fakta tanpa menganggap organisasi sendiri mengalami insiden data.

8.5 Umpan dokumen memerlukan respons peranti akhir

Nasihat MyCERT pada 22 Jun menerangkan VBScript Windows yang dihantar melalui WhatsApp Desktop atau Web. Nasihat menyebut pelaksanaannya memasang ejen pengurusan jauh yang dikawal penyerang. Urutan itu berbeza daripada umpan borang pelayar November. Soalan teknikal pertama ialah sama ada skrip atau pemasang dijalankan. [S11]

Pasukan peranti akhir perlu mengekalkan bukti proses dan pemasangan berkaitan. Mereka perlu meneliti aktiviti skrip luar jangka dan perisian pengurusan jauh dalam konteks laporan pengguna. Laporan tidak mencadangkan setiap pemasangan pengurusan jauh sah dianggap berbahaya.

Jika pelaksanaan tidak dibuktikan, rekod insiden perlu menyatakannya. Jika dibuktikan, siasatan perlu menentukan penggunaan akaun dan tindakan susulan sebelum kes ditutup. Ini respons bersyarat kepada mekanisme nasihat, bukan dapatan bahawa peranti pekerja tertentu dijangkiti.

8.6 Harga dan tawaran tidak mengukur hasil pasaran

Harga diminta menerangkan permintaan penyiar. Harga itu tidak membuktikan harga dibayar, bilangan pembeli, mutu bahan diiklankan atau hasil penjual. Oleh itu, tawaran berulang membuktikan aktiviti pengiklanan dan bukan jualan selesai.

Batas sama terpakai kepada pakej yang merangkumi beberapa negara atau institusi. Rujukan Malaysia boleh menjadi satu bahagian produk lebih luas. Laporan tidak menganggap rujukan itu sebagai penyasaran eksklusif atau mengaitkan seluruh pakej diiklankan kepada Malaysia.

Bagi pasukan penipuan, senarai medan boleh lebih berguna daripada harga diminta. Senarai itu mencadangkan soalan pengesahan yang boleh dijawab individu yang memegang maklumat didakwa. Tindakan sepadan ialah menguji proses berkaitan menggunakan data sintetik dan mengurangkan kebergantungan tidak perlu pada fakta peribadi statik.

8.7 Perkara yang disokong bukti kempen

Nasihat awam menyokong tiga laluan respons. Data bayaran dihalakan kepada penilaian pengeluar. Kelayakan dan kod akaun dihalakan kepada pengesahan akaun serta sesi. Pelaksanaan fail dihalakan kepada siasatan peranti akhir. Sesetengah laporan memerlukan lebih daripada satu laluan.

Tindakan pengguna	Pemilik utama	Pengesahan pertama	Bukti penyempurnaan
Hanya menerima umpan	Meja bantuan atau sokongan pelanggan	Tentukan sama ada halaman, fail atau borang digunakan	Rekod penerimaan dan amaran sesuai
Menyerahkan butiran identiti	Pasukan privasi dan penipuan	Kenal pasti medan serta proses pengesahan terjejas	Risiko dan keputusan komunikasi didokumentasikan
Menyerahkan maklumat kad	Pengeluar kad	Semak status kad dan cubaan transaksi berkaitan	Keputusan pengeluar mengikut proses responsnya
Menyerahkan kod atau kata laluan akaun	Pemilik identiti atau akaun	Semak sesi, log masuk dan perubahan akaun	Sesi diselesaikan dan akses dipulihkan dengan selamat
Menjalankan fail atau pemasang	Respons peranti akhir	Sahkan aktiviti proses dan pemasangan	Siasatan berskop dan keputusan pembendungan

Laluan ini menjadikan bukti boleh ditindaklanjuti tanpa mendakwa setiap umpan dilaporkan menyebabkan mudarat. Laluan itu turut menyediakan bahasa bersama kepada pasukan keselamatan, penipuan dan sokongan pelanggan. Kes kekal terbuka sehingga pemilik merekodkan perkara disahkan dan tindakan susulan.

8.8 Amaran kempen mengekalkan batas masing-masing

Notis kempen rasmi menerangkan laluan berbeza daripada mesej meyakinkan kepada tindakan bayaran atau akaun. Notis itu tidak menyokong satu angka gabungan kerugian kebangsaan. Jadual mengekalkan mekanisme dan batas pembacaan setiap amaran.

Diterbitkan	Pihak berkuasa	Mekanisme diterangkan	Keputusan pertahanan
Februari	PDRM	Umpan bertema beli-belah, penghantaran dan sumbangan	Teliti bayaran atau maklumat diminta dan bukan cerita emosi
Ogos	BNM	Sokongan pelaburan deepfake yang muncul semula	Sahkan dakwaan melalui saluran terbitan pihak berkuasa sendiri
Oktober	BNM dan Suruhanjaya Sekuriti	Sokongan pelaburan palsu	Semak kebenaran berkaitan dan jangan bergantung pada video
November	MyCERT	Halaman saman trafik palsu meminta maklumat kad dan pengesahan	Halakan butiran bayaran dan kod diserahkan kepada pemilik berkaitan

Notis dikaitkan dengan pihak yang mengeluarkannya. Notis menerangkan amaran dan mekanisme, bukan populasi mangsa sebenar yang diukur. Amaran sokongan pelaburan Ogos dan Oktober tidak membuktikan satu operasi bersama. [S35][S36][S37][S38]

Nasihat saman trafik MyCERT diterbitkan pada 6 November dan menerangkan pemerhatian pada 28–30 Oktober. Nasihat menyokong halaman pancingan data dan maklumat diminta. Nasihat tidak membuktikan transaksi sebenar, kerugian mangsa atau aktiviti berterusan pada tarikh tutup laporan. Respons perlu menentukan perkara yang dimasukkan sebelum menetapkan tindakan akaun atau bayaran. [S38]

Nasihat MyCERT seterusnya yang diterbitkan pada 22 November menerangkan halaman pendaftaran bantuan tunai palsu yang meminta kod log masuk pemesejan dan kata laluan dua langkah. Amaun bayaran didakwa ialah sebahagian umpan. Nasihat tidak menentukan jumlah mangsa atau kerugian. Persamaan dengan umpan komputer riba bukan bukti pengendali bersama. [S39]

Bagi organisasi, tindakan bersama ialah mengesahkan transaksi atau perubahan akses diminta melalui saluran dipercayai. Prinsip itu boleh diuji menggunakan senario sintetik pelaburan, pekerjaan, beli-belah dan bantuan. Ujian perlu merekodkan sama ada individu atau proses berhenti apabila wang, kelayakan atau kod diminta.

DAPATAN UTAMA

01

Umpan bantuan, komputer riba dan dokumen mewujudkan risiko aset berbeza.

02

Pemerhatian kad dan harga diminta tidak mengukur penipuan berjaya atau hasil jenayah.

03

Rekodkan tindakan sebenar pengguna, kemudian tutup laluan bayaran, akaun dan peranti akhir dengan bukti.

BAB 09

Penelitian perbankan dan kewangan

09

SOALAN YANG DIJAWAB BAB INI

Keputusan identiti, pelanggan dan pembekal manakah boleh dibuat organisasi kewangan daripada bukti laporan ini?

35

entri perbankan dan kewangan dalam portfolio terpilih

9.1 Takrifkan populasi kewangan sebelum mentafsirkannya 67
9.2 Laman web korporat dan perkhidmatan perbankan boleh mempunyai keadaan berbeza 68
9.3 Sekatan dagangan memerlukan alternatif disahkan 68
9.4 Pelaporan kredit mewujudkan kebergantungan keputusan luar 69
9.5 Pisahkan respons penipuan mengikut maklumat diserahkan 69
9.6 Umpan Android memerlukan siasatan peranti dan akaun bersama 70
9.7 Kesiapsiagaan kawal selia memerlukan sempadan aktiviti tepat 70

BAB 09

Penelitian perbankan dan kewangan

RINGKASAN

Portfolio kewangan mengandungi 35 entri terpilih, termasuk institusi dan perkhidmatan selain bank berlesen serta pengeluar kad. Kes awam menerangkan sempadan laman web, dagangan dan pelaporan kredit berasingan. Nasihat penipuan menerangkan permintaan maklumat dan pengesahan tanpa membuktikan akses sistem bank. Kekalkan populasi berbeza, sahkan bukti identiti semasa dahulu dan uji proses pelanggan serta pembekal yang bergantung pada perkhidmatan terjejas.

9.1 Takrifkan populasi kewangan sebelum mentafsirkannya

35 entri ialah portfolio perkhidmatan kewangan terpilih. Portfolio merangkumi aktiviti perbankan, pelaburan, pembangunan, dana dan infrastruktur pasaran. Entri bukan 35 bank berlesen bebas atau 35 pengeluar kad. Laporan tidak menyimpulkan penyebut pengeluar daripada set lebih luas ini. [S2]

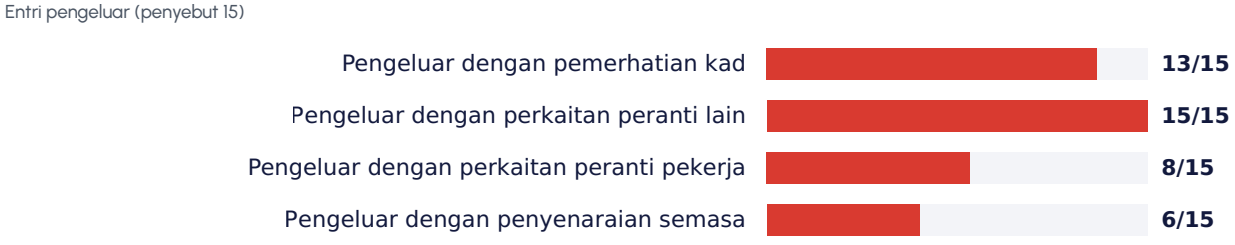
Perbezaan itu penting setiap kali angka kad dipersembahkan. Kad yang dikaitkan dengan pengeluar menerangkan pemerhatian kad bayaran dalam skop terhad §8.2. Ia tidak menunjukkan sistem pengeluar ialah sumber. Penyenaraian akaun semasa pula ialah populasi lain.

Kesemua 35 entri kewangan terpilih mempunyai hasil pendedahan boleh digunakan. Sembilan mempunyai kelayakan disenaraikan untuk dijual ketika disemak. Tiga puluh mempunyai perkaitan peranti dan rekod kelayakan sejarah, sementara 23 mempunyai perkaitan peranti dikelaskan pekerja. Pemerhatian ini menerangkan portfolio kewangan tanpa penarafan sektor. [S1]

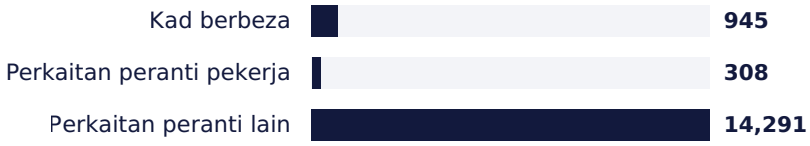
Portfolio mempunyai 55,933 perkaitan peranti yang direkodkan, termasuk 782 perkaitan dikelaskan pekerja, dan 472,196 perkaitan rekod kelayakan sejarah. Pemilikan peranti dan kesahan akaun semasa kekal belum disahkan. 1,250 perkaitan dokumen tidak dibuktikan sebagai fail sulit.

Subset pengeluar meliputi 15 entri bank pengeluar kad dalam portfolio kewangan lebih luas. Tiga belas mempunyai pemerhatian kad, berjumlah 945 kad berbeza dalam skop terhad §8.2. Enam mempunyai penyenaraian kelayakan semasa. Perkaitan pengeluar tidak membuktikan akses kepada infrastruktur bank. [S13] [S1]

Pemerhatian pengeluar mengekalkan populasi kad dan peranti berbeza



Populasi pemerhatian berasingan



Tiga bilangan kad pengeluar terbesar mewakili 67.4% daripada 945 kad; bukan kerugian penipuan. Sumber: pemerhatian pengeluar [S13][S1]. 15 pengeluar dalam 35 entri kewangan. Populasi kad, kelayakan dan peranti adalah berasingan; perkaitan pengeluar tidak membuktikan akses kepada infrastruktur bank.

15 entri pengeluar itu mempunyai 308 perkaitan peranti dikelaskan pekerja dan 14,291 perkaitan peranti lain yang tidak dikelaskan sebagai peranti pekerja. Perkaitan lain tidak dibuktikan sebagai milik pelanggan. Tiga bilangan kad pengeluar terbesar mewakili 67.4% daripada 945 kad. Penumpuan menerangkan pemerhatian, bukan kerugian penipuan atau keselamatan bank.

Pemerhatian pasif meliputi 33 daripada 35 entri kewangan terpilih. Dasar DMARC diterbitkan merangkumi 12 penolakan, 11 kuarantin dan empat hasil pemantauan; tiada dasar diperhatikan bagi enam entri. Dua entri kekal tanpa pemerhatian lengkap. TLS sah bagi 32 entri diperhatikan dan tidak sah bagi satu. [S12]

Daripada 33 entri diperhatikan, 23 halaman utama menjawab; HSTS diperhatikan pada kesemua 23 halaman menjawab. Ini pemerhatian konfigurasi, bukan bukti setiap aplikasi kewangan dilindungi. Kekalkan penyebut halaman utama berasingan daripada portfolio 35 entri.

9.2 Laman web korporat dan perkhidmatan perbankan boleh mempunyai keadaan berbeza

Pelaporan November memetik kenyataan institusi kewangan bahawa masalah laman web korporat tidak menjejaskan perkhidmatan perbankan, deposit atau maklumat pelanggan. Laporan mengekalkan sempadan dan tarikh dinyatakan. Laporan tidak menggunakan perubahan laman web yang kelihatan sebagai bukti akses sistem teras. [S8]

Bagi organisasi kewangan, respons perlu mengekalkan rekod berasingan bagi laman awam, pengesahan pelanggan, pemprosesan transaksi dan data. Setiap rekod memerlukan pemilik bertanggungjawab dan sumber bukti semasa. Perubahan satu baris perlu mencetuskan siasatan berkaitan tanpa mengubah setiap baris lain secara diam-diam.

Proses komunikasi perlu mengikut struktur sama. Kenyataan transaksi masih tersedia tidak menjawab setiap persoalan integriti laman web. Kenyataan laman awam dipulihkan tidak menentukan hasil siasatan data berasingan. Sempadan tepat memudahkan pemahaman kemas kini kemudian.

9.3 Sekatan dagangan memerlukan alternatif disahkan

Keterangan broker Oktober menerangkan sekatan selepas cubaan dikesan, dengan sesetengah saluran kekal tersedia. Responsnya tidak membuktikan kehilangan data pada masa pelaporan. Ini menyokong latihan kesinambungan tertumpu pada laluan pesanan sebenar terjejas. [S28]

Pemilik perniagaan perlu menentukan arahan yang boleh dikendalikan secara manual, cara pelanggan disahkan dan cara arahan diselaraskan selepas perkhidmatan biasa kembali. Pasukan keselamatan perlu mengesahkan saluran dipulihkan sebelum diterima pemilik. Latihan perlu mengekalkan perbezaan antara sekatan berjaga-jaga dan transaksi tanpa kebenaran disahkan.

Pelaporan Mac tentang insiden dalam komponen broker tertentu menyediakan contoh sempadan kedua. Pengendali pasaran berkata integriti pasaran lebih luas kekal terpelihara. Oleh itu, insiden peringkat komponen tidak patut ditulis semula sebagai insiden seluruh bursa. [S27]

Laporan tidak menganggap peristiwa Mac dan Oktober berkongsi pembekal, laluan masuk atau pelaku. Persamaannya bersifat operasi: setiap satu memerlukan penerangan jelas saluran terlibat. Hubungan lebih kuat memerlukan bukti tambahan.

9.4 Pelaporan kredit mewujudkan kebergantungan keputusan luar

Kes penyedia kredit dalam Bab 5 melibatkan satu persekitaran dan beberapa perkhidmatan pelaporan terganggu. Pelanggan kewangan mungkin memerlukan sandaran sementara penyedia menentukan skop penuh data. Ini tidak membuktikan akses kepada sistem pelanggan kewangan sendiri. [S6]

Pasukan kredit dan penipuan perlu menyetujui cara merekodkan keputusan menggunakan sumber alternatif atau laporan lewat. Pasukan perlu mengenal pasti permohonan yang memerlukan semakan kemudian dan cara memaklumkan pelanggan jika sesuai. Bukti penyempurnaan perlu merangkumi penyelarasan selepas penyedia memulihkan perkhidmatan.

Pasukan risiko pembekal juga perlu mengekalkan perbezaan antara gangguan dan akses data. Individu bertanggungjawab terhadap status perkhidmatan mungkin berbeza daripada individu penilaian privasi. Kedua-duanya perlu mencapai ketua insiden organisasi melalui saluran ditetapkan.

9.5 Pisahkan respons penipuan mengikut maklumat diserahkan

Nasihat bantuan dan komputer riba MyCERT menerangkan maklumat bayaran serta akaun pemesejan sebagai objektif berbeza. Laporan pelanggan perlu menentukan medan dan kod diserahkan. Laporan tidak patut diringkaskan kepada fakta pelanggan melihat mesej mencurigakan. [S9][S10]

Bagi maklumat kad bayaran, pengeluar perlu menggunakan proses pengesahan dan semakan transaksi ditetapkan. Bagi kod atau kata laluan log masuk pemesejan, pemilik akaun perlu menyemak sesi serta perubahan. Jika fail dijalankan pada peranti, respons peranti akhir perlu menilai aktiviti itu. Laluan boleh bertindih tanpa menjadi satu insiden tanpa pembezaan.

Organisasi kewangan perlu menguji prosedur pemulihan akaun dan perubahan bayaran menggunakan data peribadi sintetik. Tujuannya mengetahui sama ada pengetahuan nama sebenar, nombor telefon atau butiran statik lain boleh menggantikan pengesahan dimaksudkan. Mesej meyakinkan tidak patut dibenarkan menentukan laluan pengesahan.

9.6 Umpan Android memerlukan siasatan peranti dan akaun bersama

Nasihat MyCERT Jun dan Oktober menerangkan umpan Android melibatkan aplikasi dipasang dari luar gedung rasmi. Tingkah laku dilaporkan merangkumi penyalahgunaan Accessibility, tindihan log masuk bank, penangkapan kod dan kawalan peranti. Nasihat Oktober mengaitkan variannya dengan kempen Jun. Hubungan sumber itu tidak patut menjadi kiraan insiden kebangsaan berasingan. [S40][S41]

Soalan penerimaan berkaitan ialah sama ada aplikasi dipasang dan kebenaran yang diberikan. Menerima mesej bertema bungkusan, pekerjaan atau utiliti berbeza daripada memasang aplikasinya. Tindakan akaun juga boleh memerlukan siasatan sebelum kerugian kewangan dibuktikan.

Laporan mencadangkan pengendalian bersama pemilik akaun, pasukan penipuan dan respons peranti akhir. Pasukan akaun perlu meneliti log masuk dan perubahan bayaran berkaitan. Pasukan peranti perlu menilai pemasangan dan kebenaran. Kes perlu mengekalkan hubungan keputusan itu tanpa menganggap setiap umpan dilaporkan menghasilkan kawalan peranti.

Penetapan semula sahaja tidak patut menutup persoalan peranti. Sebaliknya, siasatan peranti tidak patut membiarkan sesi akaun berkaitan tanpa semakan. Bukti penyempurnaan perlu menyatakan pernyataan aplikasi dan akaun disahkan, tindakan susulan serta ketidakpastian yang masih ada.

9.7 Kesiapsiagaan kawal selia memerlukan sempadan aktiviti tepat

Bab 10 membezakan rangka data peribadi, kewajipan NCII dan dasar perkhidmatan bayaran Mac 2027. Kumpulan kewangan sama boleh mengandungi aktiviti berbeza dengan pemakaian berbeza. Laporan tidak menetapkan satu tarikh akhir kepada kesemua 35 entri portfolio. [S42][S43][S44]

Pasukan undang-undang dan pematuhan perlu mengenal pasti entiti serta aktiviti pemprosesan berkaitan lebih awal. Pemilik teknologi dan perniagaan perlu menyediakan fakta diperlukan bagi penilaian pemberitahuan tepat pada masanya. Terma pembekal perlu menyokong aliran maklumat diperlukan.

Contoh penguatkuasaan April melibatkan insiden 2024. Pengumuman 2026 tergolong dalam konteks tadbir urus, bukan kiraan pencerobohan tahun ini. Ia perlu mencetuskan soalan tentang bukti kawalan berterusan tanpa digabungkan dengan dakwaan kemudian yang tidak berkaitan. [S45]

DAPATAN UTAMA

01

Sampel kewangan lebih luas daripada bank berlesen atau pengeluar kad.

02

Sahkan pernyataan laman web, dagangan, pelaporan kredit dan akaun dalam sempadan masing-masing.

03

Jalankan semakan identiti, kawalan penipuan pelanggan dan kerja kesinambungan pembekal dengan pemilik serta bukti penyempurnaan berbeza.

BAB 10

Respons kawal selia dan kebangsaan

10

SOALAN YANG DIJAWAB BAB INI

Kewajipan manakah terpakai kepada organisasi tertentu, dan tempoh manakah perlu direkodkan dahulu oleh ketua insiden?

3

persoalan pemakaian sebelum keputusan pemberitahuan

10.1 Tentukan pemakaian sebelum menggunakan tarikh akhir 72
10.2 Kewajipan NCII bermula dengan penetapan dan pengetahuan 73
10.3 Kewajipan data peribadi memerlukan penilaian peristiwa dan mudarat 73
10.4 Kesiapsiagaan pegawai perlindungan data ialah tugas pengurusan 74
10.5 Dasar 2026 boleh memerlukan persediaan 2027 74
10.6 Tarikh penguatkuasaan bukan tarikh pencerobohan 75
10.7 Tindakan CISO sekarang 75

BAB 10

Respons kawal selia dan kebangsaan

RINGKASAN

Kewajipan siber dan data peribadi Malaysia mempunyai skop berbeza. Entiti infrastruktur maklumat kritikal yang ditetapkan mempunyai kewajipan insiden khusus. Pemberitahuan data peribadi bergantung pada aktiviti terpakai, peristiwa dan penilaian mudarat. Dasar teknologi perkhidmatan bayaran yang diterbitkan pada Mac berkuat kuasa pada Mac 2027. Petakan entiti dan aktiviti pemprosesan anda kepada peraturan berkaitan, rekodkan fakta awal diketahui dan jalankan keputusan pemberitahuan seiring siasatan teknikal.

10.1 Tentukan pemakaian sebelum menggunakan tarikh akhir

Akta Keselamatan Siber 2024 menetapkan kewajipan tertentu kepada entiti NCII yang ditetapkan. NCII bermaksud sistem komputer dalam takrif fungsi penting dan kesan memudaratkan menurut Akta. Industri syarikat sahaja tidak membuktikan penetapan. Kewajipan insiden melibatkan NCII berkaitan yang dimiliki atau dikendalikan entiti. [S43]

Akta Perlindungan Data Peribadi mempunyai skop berbeza. Panduan pemakaian rasmi meliputi pemprosesan berkaitan transaksi komersial, tertakluk pada peruntukan wilayah Akta. Panduan mengecualikan Kerajaan Persekutuan dan Negeri. Perniagaan pelaporan kredit di bawah Akta Agensi Pelaporan Kredit 2010 juga di luar pemakaiannya. [S42]

Sempadan ini penting dalam laporan. Populasi organisasi terpilih merangkumi badan awam, syarikat dan perkhidmatan kewangan dengan aktiviti berbeza. Ini bukan senarai entiti yang boleh diberikan satu tarikh akhir pemberitahuan. Ketua insiden perlu merekodkan entiti, aktiviti dan data terlibat sebelum menerapkan tempoh.

Jadual mengenal pasti kewajipan dan tarikh daripada teks rasmi dipetik. Jadual ialah panduan operasi kepada persoalan berkaitan, bukan nasihat undang-undang.

Peraturan	Pemakaian	Pencetus dan tempoh	Persediaan diperlukan
Akta Keselamatan Siber 2024	Entiti NCII ditetapkan serta NCII dimiliki atau dikendalikannya	Maklumkan Ketua Eksekutif dan peneraju sektor berkaitan apabila kewajipan insiden berkanun terpakai	Kekalkan rekod penetapan, sektor dan hubungan
Peraturan insiden NCII	Insiden yang telah atau mungkin berlaku, apabila diketahui dalam skop dikawal selia	Pemberitahuan segera; butiran dalam 6 jam; maklumat tambahan dalam 14 hari, seperti ditetapkan	Kekalkan saluran diperlukan dan kaedah sandaran didokumentasikan
Kewajipan pelanggaran data peribadi	Pemprosesan dan entiti dalam pemakaian Akta	Pemberitahuan berkanun secepat yang praktik; panduan Pesuruhjaya menyediakan rangka penilaian dan pelaporan	Rekodkan kesedaran, fakta, penilaian mudarat dan keputusan pemberitahuan

Peraturan	Pemakaian	Pencetus dan tempoh	Persediaan diperlukan
Kewajipan pegawai perlindungan data	Pengawal dan pemproses yang memenuhi syarat pelantikan	Kewajipan pelantikan serta pendaftaran mengikut panduan terpakai	Rekodkan pelantikan, butiran hubungan dan pengurusan bertanggungjawab
Dasar teknologi perkhidmatan bayaran	Entiti bukan bank perkhidmatan bayaran yang ditakrifkan, dengan layanan dan pengecualian ditetapkan	Dikeluarkan 12 Mac 2026; berkuat kuasa 12 Mac 2027	Lengkapkan penilaian pemakaian dan kesiapsiagaan sebelum tarikh kuat kuasa

Jadual merujuk Akta, peraturan pemberitahuannya, pindaan dan garis panduan Pesuruhjaya serta dasar BNM. Skopnya tidak patut digabungkan menjadi peraturan sejagat. [S43][S46][S47][S48][S49][S44]

10.2 Kewajipan NCII bermula dengan penetapan dan pengetahuan

Peraturan pemberitahuan memerlukan pemberitahuan elektronik segera apabila insiden yang memenuhi syarat diketahui. Peraturan memerlukan butiran ditetapkan dalam enam jam selepas diketahui dan maklumat lanjut, setakat yang praktik, dalam 14 hari selepas pemberitahuan. Kemas kini juga boleh diwajibkan. Saluran dinyatakan ialah Sistem NC4, dengan komunikasi sandaran ditetapkan ketika gangguan. [S46]

Oleh itu, laporan yang memenuhi syarat tidak patut ditangguhkan sehingga setiap persoalan forensik terjawab. Pasukan respons perlu membezakan pemberitahuan awal daripada maklumat sokongan kemudian. Pasukan perlu mengekalkan fakta tersedia pada setiap peringkat dan masa individu bertanggungjawab mengetahuinya.

Bagi organisasi yang tidak pasti penetapan atau sempadan perkhidmatannya, tindakan pertama ialah menyelesaikan status bersama hubungan undang-undang dan sektor. Laporan tidak menetapkan status NCII kepada mana-mana organisasi sampel. Laporan juga tidak menganggap setiap iklan belum disahkan sebagai insiden dalam skop statut.

Rekod tadbir urus perlu menghubungkan infrastruktur dikawal selia kepada pelan insiden. Rekod memerlukan pemilik perkhidmatan, ketua insiden, hubungan sektor berkaitan, saluran pelaporan dan kaedah sandaran. Senarai pengawal selia umum tidak cukup jika pasukan tidak dapat menentukan penerima laporan awal.

10.3 Kewajipan data peribadi memerlukan penilaian peristiwa dan mudarat

Pindaan 2024 memperkenalkan peruntukan pegawai perlindungan data dan pemberitahuan pelanggaran. Peruntukan itu berkuat kuasa pada 1 Jun 2025. Pindaan turut meluaskan kewajipan Prinsip Keselamatan kepada pemproses. Pelantikan pegawai tidak menghapuskan akauntabiliti pengawal atau pemproses. [S47][S50]

Garis panduan Pesuruhjaya menyatakan 72 jam dari kejadian dalam §6.1. Contoh §6.2 menjelaskan tempoh melalui pengetahuan atau pengesahan dalam keadaan berbeza. Penilaian pemberitahuan Pesuruhjaya merangkumi kriteria mudarat dan syarat skala melebihi 1,000 individu terjejas. Contoh tidak mewajarkan menunggu kepastian forensik lengkap. Pemberitahuan individu terjejas mengikut ujian mudarat ketara dan tempohnya sendiri. [S48]

Garis panduan menetapkan pemberitahuan individu terjejas tanpa kelewatan tidak perlu dan selewat-lewatnya tujuh hari selepas notis awal Pesuruhjaya, apabila kewajipan terpakai. Skala sahaja bukan ujian bagi komunikasi itu. Pasukan insiden perlu merekodkan keputusan Pesuruhjaya dan keputusan individu terjejas sebagai entri berasingan. [S48]

Oleh itu, rekod respons perlu bermula dengan laporan pertama dan fakta diketahui. Rekod perlu mengenal pasti aktiviti pemprosesan, kategori maklumat, kemungkinan mudarat dan pemilik penilaian. Bukti kemudian boleh mengemas kini rekod. Keputusan untuk memaklumkan, tidak memaklumkan atau mendapatkan fakta lanjut memerlukan asas dan masa semakan didokumentasikan.

Terma pembekal perlu menyokong proses ini. Pelanggan memerlukan maklumat cukup cepat untuk menilai kewajipannya sendiri. Kenyataan penyedia bahawa siasatan berterusan tidak menghapuskan keperluan penilaian awal. Begitu juga, kontrak pelanggan tidak membuktikan setiap insiden penyedia dilaporkan tertakluk pada peraturan data peribadi sama.

10.4 Kesiapsiagaan pegawai perlindungan data ialah tugas pengurusan

Garis panduan DPO merangkumi pemprosesan maklumat lebih daripada 20,000 individu, atau maklumat sensitif termasuk kewangan bagi lebih daripada 10,000 individu. Pemantauan sistematik berkala ialah satu lagi syarat. Pengawal mendaftarkan pelantikan dan butiran hubungan dalam 21 hari selepas pelantikan. [S49]

Pengurusan perlu menilai aktiviti pemprosesan sebenar berdasarkan panduan itu. Bukti penyempurnaan ialah keputusan pemakaian dan, jika diwajibkan, pelantikan direkodkan dengan akses jelas kepada proses insiden. Nama dalam carta organisasi tidak menunjukkan pegawai menerima fakta diperlukan semasa insiden.

Peranan pegawai perlu diuji sebelum keputusan pemberitahuan sebenar. Latihan simulasi boleh menguji sama ada kakitangan teknikal boleh menerangkan data terlibat, pembekal boleh memberikan fakta tepat pada masanya dan pengurusan boleh meluluskan notis awal. Tujuannya mengenal pasti maklumat hilang dan tanggungjawab tidak jelas.

10.5 Dasar 2026 boleh memerlukan persediaan 2027

BNM mengeluarkan keperluan teknologi perkhidmatan bayaran pada 12 Mac 2026, dengan tarikh kuat kuasa 12 Mac 2027. Dasar terpakai kepada entiti bukan bank perkhidmatan bayaran yang ditakrifkan, dengan layanan bertingkat dan pengecualian. Dasar tidak patut digambarkan sebagai menggantikan rangka teknologi perbankan berasingan. [S44]

Organisasi terjejas perlu menggunakan tempoh sebelum kuat kuasa untuk mengenal pasti peruntukan terpakai, menetapkan pemilik tanggungjawab dan mengekalkan bukti penyempurnaan. Pelan tindakan perlu membezakan kerja di bawah kewajipan sedia ada daripada kesiapsiagaan bagi tarikh kuat kuasa masa depan. Ini mengelakkan kawalan dirancang dilaporkan seolah-olah sudah diwajibkan dasar baharu.

Perbezaan itu amat relevan kepada bayaran dan teknologi disumber luar. Penyedia dan pelanggan dikawal selia boleh mempunyai kewajipan berbeza. Perjanjian insiden dan perkhidmatan perlu menetapkan maklumat yang diperlukan masing-masing tanpa menganggap status kawal selia satu organisasi berpindah kepada yang lain.

10.6 Tarikh penguatkuasaan bukan tarikh pencerobohan

Kenyataan April sebuah institusi kewangan menangani penalti kawal selia dan secara jelas meletakkan insiden asas pada 2024. Laporan menganggap kenyataan itu konteks kawal selia 2026, bukan pencerobohan 2026. [S45]

Persoalan pengurusan berguna ialah bukti yang menunjukkan penambahbaikan kawalan berterusan. Bayaran penalti sahaja bukan kriteria penutupan teknikal. Lembaga perlu meminta pasukan bertanggungjawab mengenal pasti kawalan, pengesahan dilakukan dan baki pengecualian, jika ada.

Laporan tidak menggunakan insiden lama untuk menyokong dakwaan pelaku atau peristiwa laman web kemudian. Konteks institusi serupa bukan bukti laluan masuk bersama atau akses berterusan. Setiap pernyataan memerlukan sokongan bertarikh sendiri.

10.7 Tindakan CISO sekarang

Pertama, kekalkan rekod pemakaian ringkas. Rekod perlu membezakan penetapan NCII, aktiviti data peribadi dan keperluan khusus sektor. Pasukan undang-undang perlu bertanggungjawab terhadap tafsiran; pemilik perniagaan dan sistem berkaitan perlu menyediakan fakta operasi.

Kedua, kekalkan log pemberitahuan bersama garis masa teknikal. Rekodkan masa maklumat diterima, perkara dibuktikan, pihak yang menilai dan tarikh akhir atau pengecualian dipertimbangkan. Bezakan fakta awal daripada pengesahan kemudian tanpa memadamkan mana-mana satu.

Ketiga, latih insiden pembekal dengan maklumat tidak lengkap. Minta penyedia memberikan sempadan perkhidmatan serta data yang khusus, kemudian uji sama ada organisasi boleh membuat dan mengemas kini keputusan sendiri. Latihan perlu berakhir dengan rekod lengkap dan saluran dikenal pasti bagi soalan belum selesai.

DAPATAN UTAMA

01

Peraturan NCII, data peribadi dan perkhidmatan bayaran mempunyai ujian pemakaian berbeza.

02

Rekodkan pengetahuan serta penilaian segera; notis awal dan kemas kini kemudian ialah kewajipan berasingan.

03

Anggap tarikh kuat kuasa Mac 2027 sebagai kerja kesiapsiagaan dan sahkan kewajipan setiap organisasi berdasarkan teks rasmi.

BAB 11

Tinjauan

11

SOALAN YANG DIJAWAB BAB INI

Senario bersyarat manakah wajar disediakan, dan bukti manakah perlu mengubah pelan?

5

pertimbangan dengan asas dan petunjuk perubahan yang jelas

11.1 Pertimbangan utama 77

11.2 Perkara yang mengubah penilaian 78

11.3 Senario bersyarat 79

BAB 11

Tinjauan

RINGKASAN

Bukti menyokong persediaan menghadapi penyalahgunaan identiti, dakwaan data, gangguan pembekal, insiden laman web awam dan pemerasan. Bukti tidak menentukan kebarangkalian serangan kebangsaan atau pengendali bersama merentasi populasi ini. Senario di bawah ialah andaian perancangan yang dikaitkan dengan mekanisme diperhatikan. Tetapkan pemilik setiap petunjuk perubahan dan semak respons apabila bukti pengukuh diterima.

11.1 Pertimbangan utama

Keyakinan terpakai kepada pernyataan dalam setiap baris. Keyakinan tidak meramalkan kemungkinan organisasi diserang. Pemerhatian yang disokong kukuh masih boleh membiarkan dakwaan asas pelaku belum disahkan.

Pertimbangan	Keyakinan dan asas	Sempadan	Petunjuk perubahan
Pengesahan identiti dan akaun kekal pelaburan awal berguna	Tinggi bagi mekanisme kempen diperhatikan dan keperluan mengesahkan akses semasa	Rekod diiklankan atau sejarah tidak semestinya masih boleh digunakan	Akaun atau sesi aktif disahkan yang dikaitkan dengan organisasi
Insiden pembekal memerlukan keputusan operasi dan privasi bersama	Tinggi bagi sempadan gangguan serta akses dilaporkan dalam kes dikekalkan	Tiada penyedia atau kempen bersama disimpulkan	Penyedia mengesahkan perkhidmatan atau data organisasi dalam skop terjejasnya
Dakwaan laman web memerlukan semakan kesan bebas	Tinggi bagi perbezaan antara kandungan awam dan perkhidmatan operasi	Perubahan luaran tidak membuktikan akses dalaman	Rekod trafik, aplikasi atau akaun menyokong kesan didakwa
Kesiapsiagaan pemerasan tidak patut bergantung pada satu nama pelaku	Tinggi bagi 87 penyenaraian merentasi beberapa jenama	Penyenaraian kekal dakwaan dan tidak mengukur kelaziman kebangsaan	Dakwaan pelaku sepadan dengan fail dikekalkan, bukti sistem atau pengesahan rasmi
Umpan pemesejan memerlukan laluan bayaran, akaun dan peranti akhir berasingan	Tinggi bagi mekanisme MyCERT	Aktiviti nasihat tidak menentukan jumlah mangsa atau kerugian sebenar	Laporan pengguna membuktikan maklumat diserahkan atau pelaksanaan fail

Asasnya ialah pemerhatian data sendiri dan kes awam dikekalkan dalam Bab 3–9. Pertimbangan mengekalkan sempadan sumber. Pertimbangan tidak menukar jumlah penerbitan kepada kebarangkalian insiden. [S4][S9] [S10][S11]

Pertimbangan pengesahan akaun bergantung pada penerimaan bukti berkaitan oleh organisasi. Ketua keselamatan perlu memastikan bukti sampai kepada pasukan bertanggungjawab dahulu. Pasukan itu kemudian boleh menentukan kebaharuan, pemilikan dan kesahan semasa sebelum memutuskan kewajaran penetapan semula atau pembendungan.

Pertimbangan pembekal melibatkan liputan keputusan dan bukan dakwaan peningkatan insiden. Kes terminal, pelaporan kredit dan perkhidmatan teknologi menunjukkan cara berbeza persekitaran luar boleh memberi kesan. Kes itu mewajarkan ujian kebergantungan berkaitan tanpa menyokong anggaran trend kebangsaan.

11.2 Perkara yang mengubah penilaian

Laporan mencadangkan set kecil petunjuk yang boleh mengubah respons. Setiap satu perlu diterima melalui saluran insiden ditetapkan dengan pemilik tanggungjawab dan cap masa. Dakwaan baharu sahaja perlu direkodkan, tetapi tindakan bergantung pada perkara dibuktikannya.

Bukti baharu	Perubahan	Pemilik bertanggungjawab
Kelayakan disenaraikan sepadan dengan akaun aktif dan aktiviti terkini berkaitan	Beralih daripada pengesahan pendedahan kepada siasatan identiti berskop	Ketua identiti dan respons insiden
Pembekal mengesahkan akses kepada fail atau komponen perkhidmatan yang digunakan organisasi	Semak kebergantungan terjejas, kesan pelanggan dan kewajipan pemberitahuan	Pemilik pembekal, ketua privasi dan operasi
Pemantauan ketersediaan menyokong dakwaan gangguan	Aktifkan pelan perkhidmatan serta mitigasi yang diuji	Pemilik perkhidmatan dan operasi rangkaian
Rekod dalaman menyokong fail atau laluan akses diiklankan	Kekalkan bukti dan bendung sempadan yang disokong	Respons insiden dan pemilik data
Pengguna mengesahkan penyerahan kod atau pelaksanaan fail	Ikuti laluan akaun atau peranti akhir berkaitan	Meja bantuan, identiti dan respons peranti akhir
Teks rasmi mengubah kewajipan terpakai atau tarikh kuat kuasa entiti	Kemas kini pelan, saluran hubungan dan sasaran penyempurnaan	Undang-undang dan pematuhan

Sesetengah dapatan juga boleh mengecilkan respons. Akaun sejarah yang dinyahaktifkan sebelum iklan tidak mewajarkan tindakan sama seperti akaun istimewa semasa. Pengecualian persekitaran organisasi oleh penyedia yang disokong bukti boleh mengurangkan skop berkaitan. Rekod perlu mengekalkan sebab keputusan berubah.

Ketiadaan bukti pengukuh bukan bukti dakwaan palsu. Ia boleh bermaksud bukti tersedia tidak menentukannya. Ketua insiden perlu menetapkan tarikh semakan dan mengenal pasti bukti tambahan yang material, supaya siasatan tidak dibiarkan terbuka tanpa pemilik selama-lamanya.

11.3 Senario bersyarat

Senario 1: tawaran identiti menjadi insiden akses semasa. Siaran atau amaran pendedahan menamakan domain organisasi. Pasukan identiti mengesahkan akaun aktif dan menemukan aktiviti yang memerlukan siasatan. Andaian perancangan ialah pasukan boleh mendapatkan log berkaitan dan menghubungi pemilik akaun segera. Latihan perlu menguji kebergantungan itu.

Keputusan pertama ialah sama ada bukti menyokong pembatalan sesi, sekatan akaun atau pembendungan peranti. Bukti penyempurnaan perlu merekodkan status akaun, aktiviti berkaitan dan tindakan diambil. Penetapan semula pukal tanpa alasan ini boleh membiarkan persoalan asas peranti atau sesi belum terjawab.

Senario 2: perkhidmatan pembekal terhenti ketika skop data tidak pasti. Operasi memerlukan kaedah sandaran sebelum penyedia melengkapkan siasatan. Privasi dan undang-undang memerlukan fakta mencukupi untuk menilai kewajipan. Andaian perancangan ialah kontrak dan saluran hubungan menyokong kenyataan awal khusus diikuti kemas kini.

Latihan perlu menguji proses perniagaan sebenar, seperti keputusan kredit atau transaksi logistik. Latihan perlu berakhir dengan baris kerja diselaraskan dan keputusan kembali berkhidmat yang didokumentasikan. Tiada andaian senario patut dibentangkan sebagai bukti pembekal benar-benar gagal memberikan maklumat tepat pada masanya.

Senario 3: laman web awam berubah dan pelaku mendakwa akses lebih luas. Pemilik perkhidmatan melihat masalah nyata sementara media sosial membawa dakwaan lebih besar. Andaian perancangan ialah pemantauan status boleh membezakan laman web daripada pengesahan, transaksi dan sistem teras.

Pasukan komunikasi perlu menerbitkan hanya sempadan disokong dan mengemas kininya apabila bukti berubah. Pasukan keselamatan perlu menguji dakwaan teknikal secara berasingan. Halaman utama dipulihkan tidak patut menutup persoalan akses dalaman yang belum disiasat.

Senario 4: umpan bantuan mencapai kakitangan dan pelanggan serentak. Sesetengah pengguna menyerahkan maklumat peribadi; yang lain memberikan kod pengesahan atau menjalankan fail. Andaian perancangan ialah meja bantuan boleh menghalakan laporan ini tanpa memaksanya menjadi satu jenis insiden.

Latihan perlu menguji penyerahan antara pasukan bayaran, akaun dan peranti akhir. Latihan juga perlu menguji kefahaman kakitangan bahawa masalah akaun pemesejan peribadi boleh relevan kepada peranti kerja atau perbualan perniagaan. Hasilnya perlu berupa keputusan lengkap bagi setiap laluan.

Senario ini bukan ramalan masa atau kerugian. Senario ialah latihan daripada jenis bukti dalam laporan. Lembaga perlu bertanya sama ada organisasi boleh mengesan petunjuk perubahan, membuat keputusan dan membuktikan penutupan.

DAPATAN UTAMA

01

Rancang berdasarkan akses disahkan, kebergantungan perkhidmatan dan tindakan pengguna, bukan jumlah mentah dakwaan.

02

Berikan setiap petunjuk perubahan pemilik dan ambang respons didokumentasikan dalam pelan organisasi sendiri.

03

Nilai semula apabila bukti baharu mengubah sempadan, dan kekalkan sebab setiap keputusan.

BAB 12

Pelan tindakan

12

SOALAN YANG DIJAWAB BAB INI

Siapakah perlu melakukan apa dalam 90 hari seterusnya, dan bukti manakah perlu diterima lembaga?

20

tindakan dengan pemilik dan bukti penyempurnaan

12.1 30/60/90 hari 82

12.2 Bukti yang boleh digunakan lembaga 85

12.3 Mengikut peranan 86

12.4 Cara Brandefense boleh membantu 86

BAB 12

Pelan tindakan

RINGKASAN

Mulakan dengan menyediakan bukti pendedahan dan insiden berkaitan kepada pemilik tanggungjawab yang dinamakan. Sahkan petunjuk identiti semasa, tentukan sempadan pembekal serta perkhidmatan, dan petakan kewajipan pemberitahuan terpakai. Kemudian, perbaiki kawalan dan proses sandaran berkaitan mekanisme diperhatikan. Akhiri dengan latihan bermasa dan rekod lembaga yang meliputi setiap tindakan. Gunakan lajur bukti untuk membezakan kerja selesai daripada perubahan dirancang.

12.1 30/60/90 hari

Fasa dikira daripada penerimaan pelan ini, bukan dakwaan tentang kematangan organisasi sedia ada. Tindakan terpakai apabila syarat dinyatakannya hadir. Pemilik perlu merekodkan alternatif beralasan apabila kawalan atau perkhidmatan di luar skop.

1Hari 1–30

Wujudkan saluran amaran kelayakan, peranti dan insiden luar semasa berkaitan bagi domain organisasi

PEMILIK BERTANGGUNGJAWAB

CISO dan ketua perisikan ancaman

BUKTI PENYEMPURNAAN

Penerima dinamakan, penghantaran diuji dan baris triage dengan pemilik

Sahkan setiap penyenaraian kelayakan semasa diterima; utamakan akaun istimewa aktif, akses jauh dan kakitangan

PEMILIK BERTANGGUNGJAWAB

Ketua identiti

BUKTI PENYEMPURNAAN

Status akaun, semakan aktiviti dan keputusan setiap item

Siasat bukti peranti berkaitan pekerja apabila melibatkan akaun atau sesi semasa

PEMILIK BERTANGGUNGJAWAB

Ketua peranti akhir dan identiti

BUKTI PENYEMPURNAAN

Pemilikan, tarikh berkaitan dan tindakan akaun/peranti direkodkan

Kenal pasti pembekal kritikal yang memproses data berkaitan atau menyokong transaksi penting

PEMILIK BERTANGGUNGJAWAB

Pemilik risiko pembekal dan perniagaan

BUKTI PENYEMPURNAAN

Peta perkhidmatan/data dengan hubungan, terma notis dan sandaran

Sahkan pemakaian peraturan NCII, data peribadi dan sektor

PEMILIK BERTANGGUNGJAWAB

Undang-undang dan pematuhan

BUKTI PENYEMPURNAAN

Matriks pemakaian diluluskan dan hubungan pemberitahuan diuji

Semak pemasangan Joomla bagi skop versi JCE dalam Kes E; siasat sistem terjejas secara berasingan daripada tampalan

PEMILIK BERTANGGUNGJAWAB

Pemilik web dan infrastruktur

BUKTI PENYEMPURNAAN

Bukti versi dibaiki serta penilaian pembasmian berskop

Wujudkan penerimaan laporan penipuan meliputi lawatan halaman, medan diserahkan, kod dan pelaksanaan fail

PEMILIK BERTANGGUNGJAWAB

Ketua penipuan dan sokongan pelanggan

BUKTI PENYEMPURNAAN

Penghalaan diuji kepada pemilik bayaran, akaun dan peranti akhir

Sediakan matriks status perkhidmatan yang membezakan laman web awam, pengesahan, transaksi dan sistem teras

PEMILIK BERTANGGUNGJAWAB

Ketua insiden dan komunikasi

BUKTI PENYEMPURNAAN

Pemilik, sumber pemantauan dan templat kenyataan diluluskan

2Hari 31–60

Perkenalkan atau luaskan pengesahan tahan pancingan data bagi akses istimewa dan jauh jika disokong

PEMILIK BERTANGGUNGJAWAB

Pemilik identiti dan platform

BUKTI PENYEMPURNAAN

Laporan penggunaan, pemulihan diuji dan pengecualian bertarikh

Semak dasar domain mel diterbitkan dan alihkan domain sesuai kepada penolakan atau kuarantin disahkan

PEMILIK BERTANGGUNGJAWAB

Pemilik pemesejan

BUKTI PENYEMPURNAAN

Pengesahan dasar, semakan penghantar sah dan pelan pengecualian

Semak perkongsian fail luar pada platform sokongan dan kerjasama

PEMILIK BERTANGGUNGJAWAB

Pemilik data dan platform

BUKTI PENYEMPURNAAN

Semakan akses, pengendalian pautan luput dan pengecualian diluluskan

Uji proses perubahan bayaran dan pemulihan pelanggan menggunakan maklumat peribadi sintetik

PEMILIK BERTANGGUNGJAWAB

Pemilik penipuan, kewangan dan perkhidmatan

BUKTI PENYEMPURNAAN

Ujian direkodkan dan langkah pengesahan lemah diperbaiki

Uji pemprosesan manual bagi kebergantungan dagangan, kredit atau logistik kritikal

PEMILIK BERTANGGUNGJAWAB

Ketua kesinambungan perniagaan dan operasi

BUKTI PENYEMPURNAAN

Sandaran bermasa, arahan disahkan dan rekod penyelarasan

Latih insiden pembekal dengan maklumat perkhidmatan dan data tidak lengkap

PEMILIK BERTANGGUNGJAWAB

Pemilik pembekal, privasi dan undang-undang

BUKTI PENYEMPURNAAN

Keputusan awal, permintaan kemas kini dan penilaian pemberitahuan

Nilai dasar perkhidmatan bayaran Mac 2027 jika terpakai

PEMILIK BERTANGGUNGJAWAB

Kepimpinan pematuhan dan teknologi

BUKTI PENYEMPURNAAN

Pelan kesiapsiagaan setiap peruntukan dengan pemilik bertanggungjawab

3Hari 61–90

Jalankan pemulihan bermasa sistem kritikal daripada sumber pemulihan dipercayai

PEMILIK BERTANGGUNGJAWAB

Pemilik infrastruktur dan perniagaan

BUKTI PENYEMPURNAAN

Masa pemulihan, pengesahan integriti dan penerimaan perniagaan

Latih gangguan laman web bersama dakwaan akses data lebih luas

PEMILIK BERTANGGUNGJAWAB

Respons insiden, rangkaian dan komunikasi

BUKTI PENYEMPURNAAN

Semakan kesan berasingan, keputusan kenyataan dan log eskalasi

Latih umpan bantuan dan akaun pemesejan merentasi saluran kakitangan serta pelanggan

PEMILIK BERTANGGUNGJAWAB

Penipuan, meja bantuan dan respons peranti akhir

BUKTI PENYEMPURNAAN

Keputusan bayaran/akaun/peranti lengkap

Selesaikan atau terima secara rasmi dapatan DNS, TLS dan halaman utama tertunggak

PEMILIK BERTANGGUNGJAWAB

Pemilik infrastruktur dan perkhidmatan

BUKTI PENYEMPURNAAN

Pemulihan disahkan atau pengecualian ditandatangani serta bertarikh

Bentangkan daftar tindakan penuh dan jurang bukti belum selesai kepada lembaga

PEMILIK BERTANGGUNGJAWAB

CISO dan pemilik risiko eksekutif

BUKTI PENYEMPURNAAN

Status dan pautan bukti bagi kesemua 20 tindakan

Fasa pertama menangani prasyarat dan pengesahan segera. Fasa kedua mengubah kawalan dan menguji sempadan perniagaan. Fasa ketiga membuktikan pemulihan dan penyelarasan. Fasa kemudian tidak patut melambatkan pembendungan segera apabila bukti semasa sudah mewajarkannya.

Setiap pasukan perlu mengekalkan perbezaan antara perubahan konfigurasi dan pengesahannya. Penerbitan dasar mel tidak membuktikan setiap penghantar sah masih berfungsi. Pemulihan aplikasi tidak membuktikan transaksi manual telah diselaraskan. Penutupan penyenaraian tanpa menyemak akaun tidak menjawab persoalan akses semasa.

12.2 Bukti yang boleh digunakan lembaga

Rekod lembaga berguna melaporkan penyempurnaan, pengecualian dan bukti belum selesai. Rekod perlu mengelakkan penggabungan populasi tidak berkaitan menjadi satu jumlah risiko. Insiden sama boleh menghasilkan beberapa item kerja tanpa menjadi beberapa insiden.

Soalan lembaga	Bukti diminta	Batas pembacaan
Adakah amaran identiti semasa dinilai?	Usia baris kerja, keputusan akaun aktif dan pemilikan belum selesai	Jumlah amaran bukan bilangan pelanggaran
Bolehkah perkhidmatan kritikal diteruskan semasa gangguan pembekal?	Ujian sandaran bermasa dan penyelarasan	Latihan simulasi berjaya bukan jaminan pengeluaran sebenar
Bolehkah organisasi menyatakan sempadan kesannya?	Matriks perkhidmatan diuji dan keputusan komunikasi	Perkhidmatan khusus yang bersih tidak mengesahkan setiap platform
Adakah keputusan undang-undang tepat pada masanya dan disokong?	Rekod pemakaian, kesedaran dan penilaian	Tarikh akhir tanpa skop boleh mengelirukan
Adakah kawalan kritikal disahkan?	Bukti pengesahan identiti, mel, perkongsian dan tampalan	Kewujudan konfigurasi bukan keberkesanan sejagat
Bolehkah organisasi memulih dan menyelaras?	Hasil pemulihan dan pengesahan transaksi	Sistem berfungsi bukan keseluruhan hasil pemulihan

Rekod perlu menunjukkan kesemua 20 tindakan, termasuk yang dianggap tidak terpakai. Rekod perlu mengenal pasti pihak yang meluluskan pengecualian dan masa ia disemak semula. Peratus penyempurnaan agregat tanpa butiran itu boleh menyembunyikan kebergantungan belum selesai yang paling kritikal.

Apabila tindakan masih terbuka, lembaga perlu menerima bukti yang belum ada dan akibatnya. Contohnya, pemilik akaun tidak diketahui menghalang keputusan identiti akhir. Proses pesanan manual belum diuji membiarkan andaian kesinambungan perkhidmatan belum selesai. Ini jurang keputusan konkrit, bukan amaran umum.

12.3 Mengikut peranan

CISO dan kepimpinan keselamatan. Wujudkan saluran bukti dan tetapkan akauntabiliti baris triage. Hubungkan keputusan identiti, peranti akhir, pembekal dan privasi daripada menganggapnya latihan pelaporan berasingan. Tingkatkan pendedahan semasa disahkan mengikut pelan insiden organisasi.

SOC dan perisikan ancaman. Kekalkan pernyataan yang disokong setiap siaran atau amaran. Bezakan dakwaan asal, penyampaian semula dan bukti perkhidmatan pengukuh. Jangan menukar tag negara, alias bersama atau iklan fail menjadi pencerobohan disahkan.

Pasukan identiti dan peranti akhir. Sahkan status akaun semasa dan aktiviti peranti berkaitan bersama-sama. Perubahan kata laluan boleh membiarkan persoalan peranti atau sesi terbuka. Rekodkan aset dinilai dan bukti yang menyokong penutupan.

Penipuan dan perlindungan pelanggan. Tanya perkara diserahkan atau dilancarkan. Halakan data bayaran, kod akaun dan pelaksanaan fail kepada pemilik sesuai. Gunakan kes sintetik untuk menguji sama ada butiran peribadi statik boleh mengatasi proses pengesahan selamat.

Pemilik perniagaan dan pembekal. Kenal pasti transaksi dan set data yang bergantung pada setiap penyedia kritikal. Uji sandaran dan kembalinya pemprosesan biasa. Kekalkan rekod penyelarasan supaya mula semula perkhidmatan tidak menyembunyikan pengecualian belum selesai.

Undang-undang, privasi dan komunikasi. Gunakan fakta bertarikh sama seperti pasukan teknikal. Terapkan skop entiti dan aktiviti berkaitan, kekalkan keputusan pemberitahuan dan nyatakan hanya sempadan perkhidmatan atau data yang disokong. Kemas kini rekod apabila bukti baharu mengubahnya.

12.4 Cara Brandefense boleh membantu

Laporan menggunakan pemerhatian Brandefense untuk menyokong penilaian dakwaan bawah tanah dan konteks penyenaraian perisian tebusan. Bukti pendedahan berkaitan perlu memaklumkan keputusan organisasi bersama log dan rekod perkhidmatannya sendiri. Langkah seterusnya yang berguna ialah aliran kerja yang menghubungkan bukti luar kepada pemilik dalaman bertanggungjawab.

Bagi organisasi yang menggunakan pemantauan luar, langkah praktikal pertama ialah menentukan domain, penerima dan pemilik pengesahan. Hasil berguna ialah baris kerja boleh ditindaklanjuti dengan keputusan didokumentasikan. Hasil pemantauan tidak menggantikan semakan akaun, siasatan forensik atau penilaian undang-undang organisasi.

Bincangkan aliran kerja bukti dan keputusan dengan Brandefense: https://brandefense.io/request-a-demo/

DAPATAN UTAMA

01

Tetapkan pemilik pemantauan dan sahkan petunjuk semasa sebelum menganggapnya insiden lengkap.

02

Uji kawalan perkhidmatan, pembekal dan penipuan bersama pemilik perniagaan yang perlu menggunakannya.

03

Berikan lembaga bukti dan pengecualian bagi kesemua 20 tindakan menjelang hari 90.

LAMPIRAN

Lampiran

A–D

SOALAN YANG DIJAWAB BAB INI

Populasi dan batas manakah perlu kekal bersama setiap kesimpulan?

5

populasi bukti berbeza, tidak pernah ditambah menjadi jumlah insiden kebangsaan

Lampiran A. Skop dan bukti 89
Lampiran B. Daftar bukti 92
Lampiran C. Sumber 93
Lampiran D. Glosari 96

Lampiran A. Skop dan bukti

Negara-negara perbandingan dipilih sebagai contoh semata-mata untuk memberikan konteks; pemilihan ini tidak menunjukkan sebarang pemeringkatan atau penilaian politik.

A.1 Tempoh dan kategori sumber

Tempoh pelaporan ialah 1 Januari–22 November 2026. Pemerhatian siaran bertarikh mengikut penerbitan, bukan tarikh ia memasuki sumber dikekalkan. Bahagian aktiviti terkini meliputi 8–22 November. Keterangan insiden awam boleh mengandungi tarikh berbeza bagi akses, pengesanan, pendedahan dan pemulihan; laporan mengekalkan makna itu secara berasingan.

Pemerhatian sendiri berasal daripada Brandefense Blackhole, Ransompedia, Atlas dan semakan domain awam portfolio terpilih. Sumber awam merangkumi nasihat rasmi dan teks undang-undang, kenyataan organisasi, pelaporan berita serta panduan keselamatan vendor. Kategori ini menjawab persoalan berbeza. Bilangannya tidak digabungkan menjadi jumlah insiden kebangsaan.

Lima populasi utama ialah siaran, penyenaraian laman kebocoran, entri domain terpilih, notis kempen awam dan insiden dilaporkan. Satu siaran boleh menerangkan beberapa negara. Beberapa notis boleh melibatkan satu insiden. Penyenaraian boleh kekal belum disahkan. Domain terpilih bukan sampel rawak organisasi kebangsaan.

A.2 Siaran bawah tanah

Bilangan sumber ialah 782,224 siaran bertag Malaysia. Pandangan bertag dikekalkan mengandungi 25,355 siaran berbeza, dengan 8,748–9,196 pemerhatian relevan. Perbezaan mencerminkan sempadan liputan dan kaitan, bukan anggaran serangan tidak didedahkan. [S3]

Tempoh terkini mengandungi 922 siaran bertag Malaysia, termasuk lapan siaran forum bertag. Pandangan forum berasingan mengandungi 14 siaran, dan populasi bertag berlabel Melayu mengandungi 15. Populasi ini bertindih. Populasi tidak ditambah bersama atau digambarkan sebagai insiden unik.

Iklan terkini tidak membuktikan pemerolehan terkini. Tajuk atau senarai medan sepadan tidak membuktikan fail sama, pemilikan, jualan atau pengendali bersama. Laporan membezakan siaran dikekalkan daripada dakwaan asas.

Bilangan siaran menerangkan keterlihatan dalam sumber dikekalkan. Bilangan tidak mengukur kekerapan serangan, hasil jenayah, individu terjejas atau akses berjaya. Bilangan rendah atau ketiadaan dakwaan tidak membuktikan ketiadaan insiden.

A.3 Portfolio domain organisasi terpilih

Portfolio mengandungi 250 entri terpilih merentasi 11 sel sektor. Portfolio dipilih untuk kaitan deskriptif perniagaan dan perkhidmatan awam. Ia bukan pemeringkatan rasmi teratas 250, bancian atau sampel rawak. Kumpulan berkaitan, jenama dan hubungan perkhidmatan tempatan boleh bertindih. [S2]

Satu domain utama terpilih mewakili setiap entri. Respons DNS atau halaman utama bukan bukti muktamad pemilikan undang-undang bebas. Hasil tidak diketahui kekal tidak diketahui, dengan penyebut dinilai dinyatakan bersama setiap hasil kawalan awam.

A.4 Penarafan dan perkaitan pendedahan

Pemerhatian pendedahan disemak pada 22 November meliputi 249 daripada 250 entri terpilih; satu tidak tersedia. Daripada entri dinilai, 55 mempunyai kelayakan disenaraikan untuk dijual ketika disemak. Nilai utama Atlas kebangsaan ialah 48/100. Tiada penarafan sektor atau kumpulan diterbitkan. [S1]

Pembilang peranti, kelayakan, dokumen dan penyenaraian ialah rekod terkumpul ketika semakan, bukan insiden khusus 2026. Calon domain seiras meliputi 19 Oktober–18 November 2026. Pemerhatian sebutan meliputi 365 hari terdahulu berakhir pada 22 November 2026. Populasi boleh bertindih dan tidak boleh ditambah menjadi jumlah individu atau insiden.

Apabila pembaca menerima bukti pendedahan berkaitan organisasinya, penyenaraian semasa, kelayakan sejarah dan perkaitan peranti memerlukan pengesahan berasingan. Itu bukan individu unik atau akses semasa disahkan. Respons dicadangkan bergantung pada pemilikan, tarikh, kesahan dan aktiviti pengukuh.

A.5 Pemerhatian domain awam

Hasil awam melibatkan dasar mel, rekod DNS, TLS dan halaman utama menjawab pada tarikh pemerhatian dinyatakan. Dasar penolakan atau kuarantin diterbitkan bukan dakwaan penguatkuasaan sejagat. Rekod tandatangan tidak diperhatikan tidak membuktikan tiada tandatangan. Rekod delegasi tidak membuktikan rantaian DNSSEC disahkan sepenuhnya. [S12]

Hasil TLS sah, tidak sah dan belum selesai adalah berasingan. Dapatan pengepala halaman utama menggunakan halaman menjawab sebagai penyebut. Laporan tidak mentafsir permintaan tidak berjawab sebagai kawalan gagal disahkan.

A.6 Pemerhatian kad bayaran

Pemerhatian kad bayaran mempunyai liputan terhad. Angka ini tidak menganggarkan kecurian kad kebangsaan, kebolehgunaan kad, penggunaan sebenar atau kerugian penipuan.

Pemerhatian peringkat pengeluar tidak membuktikan sistem pengeluar ialah sumber. Pemerhatian perlu menyokong proses pengesahan pengeluar bersama bukti transaksinya sendiri. Pemerhatian kad bayaran tidak ditambah kepada populasi peranti, akaun atau insiden.

A.7 Penyenaraian perisian tebusan

Ransompedia menyediakan 87 penyenaraian Malaysia bertarikh dalam tempoh pelaporan. Perbandingan serantau tempoh sama meliputi Singapura, Indonesia, Thailand dan Filipina. Tarikh penerbitan tidak menentukan tarikh pencerobohan, dan penyenaraian tidak membuktikan peranan pihak yang mendakwa atau pengesahan organisasi. [S4]

Label sektor sumber penyenaraian berbeza daripada sektor domain terpilih laporan. Populasi tidak digabungkan seolah-olah sama. Bilangan kebangsaan berbeza boleh mencerminkan perbezaan liputan serta pendedahan selain aktiviti asas.

A.8 Insiden dan kempen awam

Laporan menggunakan keterangan insiden rasmi, nasihat kempen, notis organisasi dan pelaporan sokongan. Insiden diakui, jumlah didakwa, laluan masuk, identiti pelaku dan kesan perniagaan ialah pernyataan berasingan. Laporan mengekalkan atribusi serta tarikh setiap sumber.

Liputan kekal separa. Insiden dan jualan persendirian boleh tidak meninggalkan keterangan awam. Siaran dibuang awal boleh tiada. Kenyataan awam boleh membiarkan skop belum selesai. Ketiadaan insiden daripada laporan ini bukan bukti bahawa insiden tidak berlaku.

Gangguan teknikal tidak dikira secara automatik sebagai aktiviti berniat jahat. Pengumuman penguatkuasaan bertarikh secara berasingan daripada insiden yang menghasilkannya. Amaran mekanisme munasabah tidak secara automatik menjadi kempen disahkan. Sempadan ini terpakai sama kepada ringkasan, jadual dan kad.

A.9 Keyakinan dan penamaan

Keyakinan tinggi menerangkan pemerhatian disokong atau pernyataan bersumber jelas. Ia tidak memindahkan kebolehpercayaan kepada setiap kenyataan persona. Tafsiran mengekalkan asas dan alternatifnya. "Belum disahkan" bermaksud belum dibuktikan secara bebas, bukan palsu atau disahkan.

Sasaran dakwaan belum disahkan menggunakan label yang boleh sesuai dengan beberapa organisasi. Organisasi dinamakan hanya apabila insiden disahkan secara rasmi, dilaporkan meluas dan direkodkan dalam daftar penamaan awam. Penerangan serta pautan sumber mengekalkan perlindungan sama. Butiran hubungan pelaku, petunjuk mangsa dan maklumat peribadi tidak diterbitkan.

Atribusi sumber tidak menjadikan retorik pelaku pandangan pengarang. Laporan mengekalkan pernyataan relevan keselamatan dan menggugurkan ungkapan berat sebelah. Cadangan menerangkan tindakan pertahanan dicadangkan; cadangan tidak mendakwa organisasi bernama atau tidak bernama gagal melakukannya.

Lampiran B. Daftar bukti

Daftar menghubungkan kad siaran awam kepada bahagian kemunculannya. Pernyataan "bukti disimpan" kad menerangkan pemerhatian. Batasnya menerangkan perkara yang tidak dibuktikan pemerhatian.

Kad	Tarikh siaran	Wadah	Alias	Bahasa	Dipaparkan dalam
B01	2026-01-09	Iklan forum yang disimpan	Persona penjual	Inggeris	§4.3
B02	2026-05-08	Iklan forum yang disimpan	Persona penjual	Inggeris	§4.3
B03	2026-08-23	Iklan forum yang disimpan	Persona penjual	Inggeris	§4.3
B04	2026-09-06	Iklan forum yang disimpan	Persona penjual	Inggeris	§4.3
B05	2026-11-19	Iklan forum yang disimpan	Persona penjual	Inggeris	§4.3
B06	2026-02-01	Iklan forum yang disimpan	Persona penjual	Rusia	§4.3
B07	2026-02-10	Perbincangan forum yang disimpan	Peserta forum	Inggeris	§4.4
B08	2026-03-09	Hantaran saluran yang disimpan	MalaysiaHacktivist	Melayu	§6.2
B09	2026-03-08	Hantaran saluran yang disimpan	Persona penjual	Cina	§4.4

ID kad awam ialah rujukan dalam laporan ini, bukan pautan kepada saluran jenayah atau aset mangsa.

Lampiran C. Sumber

Pemerhatian Brandefense sendiri tiada alamat sumber awam. Setiap entri luar merekodkan tarikh bahan sokongan disemak. Jika artikel mengenal pasti sasaran ditahan, petikan akhbar atau pengeluar rasmi menggunakan akar laman penerbit dan menyatakan URL artikel ditahan. Petikan sedemikian yang lain tiada URL awam.

S1: Brandefense Atlas, Malaysian selected-domain exposure snapshot, 22 November 2026; lookalike observations 19 October–18 November 2026. Verified on 22 November 2026.

S2: Odin by Brandefense, Selected Malaysian organisation population and scope register, 22 November 2026. Verified on 22 November 2026.

S3: Brandefense Blackhole, Malaysian post observations dated 1 January–22 November 2026. Verified on 22 November 2026.

S4: Brandefense Ransompedia, Ransomware leak-site listings for Malaysia, Singapore, Indonesia, Thailand and the Philippines, 1 January–22 November 2026. Verified on 22 November 2026.

S5: The Loadstar, Container-terminal incident and phased restoration, September 2026. https://theloadstar.com/ (article URL withheld). Verified on 23 November 2026.

S6: Bernama, Credit-reporting provider disclosure, September 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S7: Bernama, quoting the official statement, Health-sector support-platform incident account, 14 November 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S8: Malay Mail, quoting the institution, Corporate-website disruption and stated service boundary, 7 November 2026. https://www.malaymail.com/ (article URL withheld). Verified on 22 November 2026.

S9: MyCERT, MA-1501.112026: assistance-themed phishing, 11 November 2026. https://www.mycert.org.my/portal/advisory?id=MA-1501.112026. Verified on 22 November 2026.

S10: MyCERT, MA-1511.112026: free-laptop messaging-account phishing, 20 November 2026. https://mycert.org.my/portal/details?id=8b8bb3b1-ff5c-42b2-b34c-4d3c2c1574d2&menu=431fab9c-d24c-4a27-ba93-e92edafdefa5. Verified on 22 November 2026.

S11: MyCERT, MA-1464.062026: malicious Windows scripts delivered through messaging, 22 June 2026. https://mycert.org.my/portal/advisory?id=MA-1464.062026. Verified on 22 November 2026.

S12: Odin by Brandefense, Public DNS, TLS and homepage observations for selected Malaysian domains. Verified on 22 November 2026.

S13: Brandefense Blackhole, Malaysian-attributed payment-card observations, 1 January–22 November 2026. Verified on 22 November 2026.

S14: OpenDOSM, ICT survey population and use-period metadata. https://open.dosm.gov.my/data-catalogue/icths_internet_device. Verified on 22 November 2026.

S15: Department of Statistics Malaysia, ICT use and access by individuals and households, reference year 2025; released 23 April 2026. https://www.dosm.gov.my/site/downloadrelease?id=ict-use-and-access-by-individuals-and-households-survey-report-2025&lang=English. Verified on 23 November 2026.

S16: Company public notice, Technology-services incident notice, April 2026. (article URL withheld). Verified on 22 November 2026.

S17: Bernama, reporting MKN and NACSA, Official assessment of circulating personal-data claims, 21 June 2026. https://www.bernama.com/en/general/news.php?id=2571178. Verified on 23 November 2026.

S18: NACSA, Official alert index: late-June JCE extension warning. https://www.nacsa.gov.my/alert.php. Verified on 23 November 2026.

S19: JCE, Security update and free patch for older sites. https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites. Verified on 23 November 2026.

S20: NACSA, Assessment of a cloud-productivity disruption. https://www.nacsa.gov.my/ (article URL withheld). Verified on 22 November 2026.

S21: Bernama, Ministerial assessment of circulating leak claims, 18 November 2026. https://web26.bernama.com/en/news.php?id=2636239. Verified on 22 November 2026.

S22: Malay Mail, quoting service announcements, Consumer payment-platform interruption and restoration, July 2026. https://www.malaymail.com/ (article URL withheld). Verified on 22 November 2026.

S23: The Edge, quoting the provider, Isolated telecommunications customer-information disclosure, July–August 2026. https://theedgemalaysia.com/ (article URL withheld). Verified on 22 November 2026.

S24: Lowyat, quoting the institution, Financial-institution service restoration, October 2026. https://www.lowyat.net/ (article URL withheld). Verified on 22 November 2026.

S25: Malay Mail, Council account of a municipal public-display incident, 30 October 2026. https://www.malaymail.com/ (article URL withheld). Verified on 22 November 2026.

S26: The Star, Police account of a municipal public-display investigation, 30 October 2026. https://www.thestar.com.my/ (article URL withheld). Verified on 22 November 2026.

S27: Bernama, reporting the market operator statement, Broker-component incident statement, 12 March 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S28: The Edge, quoting a written response, Online broker restrictions following a detected attempt, 30 October 2026. https://theedgemalaysia.com/ (article URL withheld). Verified on 22 November 2026.

S30: Bernama, quoting the responsible authority, Public-service transaction-approval investigation, August 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S31: Lowyat, Public-website observation, November 2026. https://www.lowyat.net/ (article URL withheld). Verified on 22 November 2026.

S32: Bernama, quoting a company statement, Airline reservation-supplier disclosure, November 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S33: Bernama, Authority account of suspected public-website activity, 10 November 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S34: CVE Program, CVE-2026-48907: Joomla CNA record. https://cveawg.mitre.org/api/cve/CVE-2026-48907. Verified on 23 November 2026.

S35: PDRM, emotional shopping/delivery/donation lures, 2026-02-19. https://www.rmp.gov.my/arkib-berita/keratan-akhbar/page/25. Verified on 22 November 2026.

S36: BNM, official impersonation deepfake investment lure, 2026-08-25. https://www.bnm.gov.my/-/amaran-20260825. Verified on 22 November 2026.

S37: BNM, deepfake investment endorsements, 2026-10-13. https://amlcft.bnm.gov.my/web/guest/-/scamalert. Verified on 22 November 2026.

S38: MyCERT, MA-1499.112026: false traffic-summons phishing, 6 November 2026. https://www.mycert.org.my/portal/advisory?id=MA-1499.112026. Verified on 22 November 2026.

S39: MyCERT, MA-1513.112026: false cash-assistance registration and messaging-account phishing, 22 November 2026. https://www.mycert.org.my/portal/advisory?id=MA-1513.112026. Verified on 22 November 2026.

S40: MyCERT, MA-1451.062026: Android banking-malware lure advisory, 6 June 2026. https://www.mycert.org.my/portal/advisory?id=MA-1451.062026. Verified on 22 November 2026.

S41: MyCERT, MA-1482.102026: related Android malware variants, 18 October 2026. https://www.mycert.org.my/portal/advisory?id=MA-1482.102026. Verified on 22 November 2026.

S42: Personal Data Protection Department, Application and non-application of the Act. https://www.pdp.gov.my/en/akta/application-and-non-application-of-the-act/. Verified on 22 November 2026.

S43: Attorney General's Chambers, Cyber Security Act 2024, Act 854. https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/2177706_BI/Act%20854.pdf. Verified on 22 November 2026.

S44: Bank Negara Malaysia, Technology requirements for payment-services regulatees, March 2026. https://www.bnm.gov.my/documents/20124/943361/pd-tecreq-psr-mar2026.pdf. Verified on 23 November 2026.

S45: Institution public statement, Response to the administrative penalty, 1 April 2026. https://dmedia.penerangan.gov.my/ (article URL withheld). Verified on 22 November 2026.

S46: Attorney General's Chambers, Cyber Security (Notification of Cyber Security Incident) Regulations 2024. https://lom.agc.gov.my/ilims/upload/portal/akta/outputp/2303986/PUA220_2024.pdf. Verified on 22 November 2026.

S47: Personal Data Protection Department, Personal Data Protection (Amendment) Act 2024, Act A1727. https://www.pdp.gov.my/wp-content/uploads/2024/11/Act-A1727.pdf. Verified on 22 November 2026.

S48: Personal Data Protection Commissioner, Data Breach Notification Guideline. https://www.pdp.gov.my/wp-content/uploads/2025/08/GP_DBN_ENG.pdf. Verified on 22 November 2026.

S49: Personal Data Protection Commissioner, Appointment of Data Protection Officer Guideline. https://www.pdp.gov.my/wp-content/uploads/2025/08/GP_DPO_ENG.pdf. Verified on 22 November 2026.

S50: Federal Gazette, Commencement notification P.U.(B)522. https://www.pdp.gov.my/wp-content/uploads/2024/12/PENETAPAN-TARIKH-PERMULAAN-KUAT-KUASA.pdf. Verified on 22 November 2026.

S51: RFC Editor, RFC 7489: DMARC. https://www.rfc-editor.org/rfc/rfc7489. Verified on 23 November 2026.

S52: RFC Editor, RFC 7208: SPF. https://www.rfc-editor.org/rfc/rfc7208. Verified on 23 November 2026.

S53: RFC Editor, RFC 6376: DKIM. https://www.rfc-editor.org/rfc/rfc6376. Verified on 23 November 2026.

S54: RFC Editor, RFC 4033: DNSSEC. https://www.rfc-editor.org/rfc/rfc4033. Verified on 23 November 2026.

S55: RFC Editor, RFC 8446: TLS. https://www.rfc-editor.org/rfc/rfc8446. Verified on 23 November 2026.

S56: RFC Editor, RFC 6797: HSTS. https://www.rfc-editor.org/rfc/rfc6797. Verified on 23 November 2026.

S57: Flare Systems, Combolists & the Dark Web: The Different Types of Leaked Credentials. https://flare.io/learn/resources/blog/combo-lists-the-dark-web-understanding-leaked-credentials. Verified on 23 November 2026.

S58: MS-ISAC, MS-ISAC Guide to DDoS Attacks. https://www.cisecurity.org/insights/white-papers/ms-isac-guide-to-ddos-attacks. Verified on 23 November 2026.

Lampiran D. Glosari

Istilah ini menjelaskan bukti dan keputusan dalam laporan. Istilah tidak menambah kesimpulan teknikal atau undang-undang di luar bab dipetik.

Istilah	Maksud mudah
MKN	Majlis Keselamatan Negara [S17]
NACSA / NC4	Agensi Keselamatan Siber Negara dan Pusat Penyelarasan dan Kawalan Siber Negara, yang mengeluarkan amaran kebangsaan [S18][S46]
PDRM	Polis Diraja Malaysia [S35]
BNM	Bank Negara Malaysia, bank pusat [S44]
Nilai utama Atlas	Penarafan pendedahan kebangsaan Brandefense bagi portfolio dinilai pada skala 0–100; nilai lebih tinggi menunjukkan lebih banyak pendedahan diperhatikan. Ia bukan penarafan sektor atau anggaran kelaziman [S1]
DMARC	Domain-based Message Authentication, Reporting, and Conformance: dasar domain untuk mengendalikan dan melaporkan hasil pengesahan e-mel [S51]
SPF	Sender Policy Framework: membolehkan domain menetapkan pelayan yang dibenarkan menghantar e-mel menggunakannya [S52]
DKIM	DomainKeys Identified Mail: tandatangan digital mengaitkan domain penandatangan dengan mesej dan membantu mengesan perubahan kandungan yang ditandatangani [S53]
DNSSEC	Domain Name System Security Extensions: mengesahkan asal usul dan integriti data DNS [S54]
TLS	Transport Layer Security: melindungi komunikasi rangkaian daripada intipan, pengubahan dan pemalsuan mesej [S55]
HSTS	HTTP Strict Transport Security: dasar laman web yang mengarahkan pelayar menggunakan sambungan selamat [S56]
Log pencuri maklumat	Rekod yang dihasilkan oleh perisian hasad pencuri maklumat [S57]
Combolist	Himpunan gabungan nama pengguna/kata laluan [S57]
DDoS	Penafian perkhidmatan teragih: serangan daripada pelbagai sumber yang bertujuan mengganggu akses kepada sistem atau perkhidmatan [S58]
Iklan	Siaran menawarkan atau meminta produk; ia tidak membuktikan transaksi selesai

Istilah	Maksud mudah
Penyenaraian kelayakan semasa	Tawaran diperhatikan berkaitan akaun atau domain pada masa pemerhatian; kesahan semasa akaun masih perlu diperiksa
Perkaitan peranti	Bukti mengaitkan peranti dengan akaun atau domain; pemilikan dan status semasa memerlukan pengesahan
NCII	Sistem komputer dalam takrif fungsi penting dan kesan memudaratkan Akta Keselamatan Siber [S43]
Pegawai perlindungan data	Individu dilantik yang menyokong tanggungjawab data peribadi terpakai; akauntabiliti kekal pada organisasi [S49]
Pemberitahuan pelanggaran data	Notis diwajibkan mengikut peraturan peristiwa, skop dan penilaian terpakai [S48]
Kata laluan sekali guna	Kod pengesahan sementara yang boleh diminta halaman pancingan data [S9]
JCE	Sambungan penyunting Joomla yang diliputi panduan kemas kini keselamatan vendor [S19]
Ejen pengurusan jauh	Perisian yang menyokong pentadbiran peranti jauh; nasihat Jun menerangkan pemasangan dikawal penyerang selepas pelaksanaan skrip [S11]
Penyenaraian	Penerbitan pemerasan diperhatikan dalam sumber; bukan insiden disahkan secara bebas [S4]
Andaian perancangan	Syarat dalam latihan atau senario, bukan ramalan
Hasil tidak diketahui	Pernyataan yang tidak ditentukan pemerhatian dikekalkan

Tentang laporan ini

Disediakan oleh Odin by Brandefense untuk siri Brandefense Country Report. Tempoh penyelidikan ialah 1 Januari–22 November 2026. Laporan mengutamakan pemerhatian Brandefense dikekalkan dan menggunakan sumber awam bagi keterangan insiden, panduan teknikal serta konteks undang-undang.

Ini laporan landskap ancaman deskriptif, bukan bancian insiden siber Malaysia. Laporan membezakan pemerhatian, dakwaan, keterangan rasmi dan pertimbangan analisis. Edisi bahasa Inggeris ialah teks induk. Edisi Melayu membawa notis terjemahan AI dan mengekalkan angka, ID sumber, ID kad serta arahan yang sama.

© 2026 Brandefense. Hak cipta terpelihara.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO