PHYLEX
BY PHOENIX STRATOS SECURA

Untuk CIO, CISO & tim TI

SECURITY & ARCHITECTURE FACT SHEET

Phylex Respond: agen di perangkat Anda, data tetap terpisah.

Ringkasan teknis untuk tim TI dan CISO: apa yang dipasang di perangkat, data apa yang keluar, bagaimana data satu klien dipisahkan dari klien lain, dan di mana manusia tetap memegang keputusan.

Arsitektur singkat

LAPISAN	LETAK	YANG TERJADI
Agen di perangkat	Laptop, PC, dan server klien (Windows, macOS, Linux)	Agen Wazuh (sumber terbuka) membaca log keamanan dan integritas berkas, lalu mengirimnya ke server Wazuh milik klien. Tidak membuka port masuk di perangkat.
Server Wazuh klien	Satu VM khusus per klien di Google Cloud Jakarta (asia-southeast2)	Menganalisis log. Log mentah disimpan di VM ini dan arsip di bucket milik klien tersebut, tidak dikirim ke Phylex Console.
Phylex Console	Google Cloud Jakarta (asia-southeast2)	Hanya menerima ringkasan alert tingkat ≥ 10 dan status armada tanpa IP perangkat. Di sini insiden dicatat, ditangani, dan dilaporkan.

Hak akses dan beban agen

Hak akses

Agen berjalan sebagai layanan sistem agar bisa membaca log keamanan sistem operasi. Agen hanya membuat koneksi keluar ke server Wazuh klien (port 1514/1515). Pendaftaran agen wajib kata sandi pendaftaran per klien.

Beban CPU dan RAM

Agen Wazuh dirancang ringan (dokumentasi Wazuh menyebut rata-rata sekitar 35 MB RAM). Pemakaian nyata diukur di perangkat pertama saat penyiapan, sebelum agen dipasang ke perangkat lain.

Tanpa pemblokiran otomatis

Phylex tidak mengaktifkan respons aktif (blokir IP, matikan proses, karantina) di perangkat klien. Tidak ada risiko salah blokir dari agen. Tindakan penahanan dijalankan tim klien sesuai playbook.

Pemasangan bertahap

Agen dipasang di satu perangkat dulu. Setelah berstatus Aktif dan bebannya diperiksa, baru dipasang ke perangkat lain. Agen bisa dicopot kapan saja oleh tim TI klien.

ISOLASI DATA DAN ENKRIPSI

Satu klien, satu server. Tidak ada data yang tercampur.

Isolasi antar-klien

Setiap klien Cloud dan Government mendapat VM, IP, service account, bucket arsip, dan kunci agen sendiri. Firewall memblokir lalu lintas internal antar-server Respond, sehingga server satu klien tidak bisa menjangkau server klien lain.

Enkripsi

Komunikasi agen ke server Wazuh dienkripsi (protokol bawaan Wazuh). Server Wazuh mengirim ringkasan alert ke Phylex lewat HTTPS dengan kunci agen khusus organisasi tersebut. Dasbor dan SSH server hanya bisa diakses lewat Google IAP.

Residensi data

Server Wazuh, arsip, dan Phylex Console berada di Google Cloud region Jakarta. Arsip terhapus otomatis setelah 12 bulan. Saat berhenti berlangganan, data diserahkan atau dihapus sesuai DPA.

Penyamaran data sebelum AI

Sebelum teks dikirim ke Asisten AI (Vertex AI, Google), nama aset, IP, email, dan rahasia diganti penanda seperti [aset], [ip], [email], dan [rahasia]. Model diminta tidak menebak nilai aslinya.

Manusia tetap memegang keputusan

LANGKAH	YANG DISIAPKAN SISTEM	YANG MEMUTUSKAN
Alert agen menjadi insiden	Antrean alert dan sinyal per host	Analis Phylex meninjau setiap hari kerja; tim klien memutuskan tindakan.
Pemberitahuan UU PDP 3×24 jam	Hitung mundur dan draf oleh AI	Pemilik organisasi menyetujui draf, lalu klien sendiri yang mengirim.
Ringkasan pimpinan dan laporan BSSN	Draf oleh AI berkerangka TTIS	Pemilik organisasi meninjau dan mengirim.
Takedown dari insiden	Formulir jalur cepat	Hanya pemilik organisasi; tim Phylex memverifikasi mandat dulu.

Jejak audit dan ketersediaan

- Setiap insiden punya linimasa: siapa melakukan apa dan kapan
- Tindakan penting tercatat di log audit organisasi
- Laporan pasca-insiden dan laporan bulanan PDF untuk pimpinan

- Server Wazuh mengirim status setiap 15 menit
- Alarm ke tim Phylex bila server diam > 60 menit atau disk ≥ 85%
- Data console dilindungi pemulihan titik waktu dan cadangan harian

Batas yang perlu diketahui. Analis Phylex menanggapi pada jam kerja (Senin–Jumat 08.00–17.00 WIB), bukan 24/7. Phylex terdaftar sebagai PSE Lingkup Privat Komdigi (PB-UMKU 81200141421780011000l); pendaftaran ini bukan sertifikasi keamanan. Rincian SLA ada di dokumen SLA & Matriks Eskalasi.