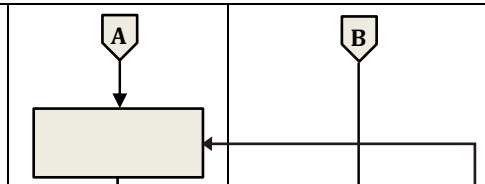
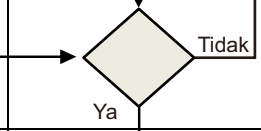
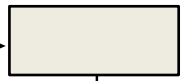
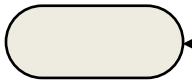
DINAS KOMUNIKASI DAN INFORMATIKA **KABUPATEN TRENGGALEK**	Nama SOP	SOP Pemanfaatan *Cyber Threat Intelligence (CTI)* dalam Monitoring Sistem Elektronik
	Nomor SOP	500.12.10/222/406.020/2025
	Tanggal Pembuatan	-
	Tanggal Revisi	-
	Tanggal Pengesahan	9 Desember 2025
	Disahkan Oleh	Plt. Kepala Dinas Komunikasi dan Informatika Kabupaten Trenggalek **ARIEF SETIAWAN, SE, M.Si** NIP. 19810507 201001 1 017

DASAR HUKUM	KUALIFIKASI PELAKSANA
1. Undang-undang Nomor 25 Tahun 2009 tentang Pelayanan Publik 2. Peraturan Menteri Pendayagunaan AparaturNegara dan Reformasi Birokrasi RI No 35 Tahun 2012 tentang Pedoman Penyusunan SOP Adminstrasi Pemerintahan 3. Peraturan Menteri Dalam Negeri No 52 tahun 2011 tentang SOP di Lingkungan PemerintahProvinsi dan Kabupaten/Kota 4. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah 5. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik 6. Peraturan Daerah Kabupaten Trenggalek Nomor 11 Tahun 2019 Tentang Pelayanan Publik 7. Peraturan Bupati (Perbup) Kabupaten Trenggalek Nomor 11 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah	1. Mampu mengoperasikan Komputer dengan baik; 2. Memiliki pengetahuan di bidang keamanan informasi dengan baik; 3. Memiliki kemampuan analisis dalam mengidentifikasi insiden siber; 4. Memahami prinsip-prinsip keamanan informasi; 5. Memiliki pengetahuan administrasi umum; 6. Memiliki kemampuan teknis dalam operasional server, jaringan dan instrument (tools) keamanan siber; 7. Memiliki kemampuan untuk melakukan koordinasi dengan pihak-pihak terkait.

KETERKAITAN	PERLENGKAPAN/PERSYARATAN
-	1. Laporan Insiden 2. Laptop/Printer; 3. Tools (Keamanan Siber) Perangkat Komputer; 4. Media Komunikasi; 5. Perangkat Lunak Security Information and Event Management (SIEM); 6. Instrumen Vulnerability Scanning;
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Jika SOP ini tidak berjalan maka akan mengakibatkan dampak yang mencakupketerlambatan perbaikan, peningkatan resiko siber, penurunan efisiensi, rusaknya reputasi organisasi, ketidaksesuaian dengan regulasi dan kerugian finansial; 2. Dapat menyebabkan potensi celah keamanan yang lebih besar; 3. Dapat menghambat pemulihan dan kelancaran operasional.	1. Dokumentasi Insiden; 2. Formulir Laporan Insiden 3. Dokumentasi Kegiatan; 4. Daftar Security Log Analysis 5. Laporan Insiden Siber.

NO	URAIAN PROSEDUR	PELAKSANA			MUTU BAKU			KETERANGAN
		TTIS TRENGGALEKKAB	KOORDINATOR TIM/KEPALA BIDANG STATISTIK & PERSANDIAN	KETUA TIM/KEPALA DINAS	Kelengkapan	Waktu	Output	
1	Login ke aplikasi monitoring (SIEM)				Laptop	5 Menit	Dashboard SIEM	Login ke Wazuh
2	Mengakses *dashboard* apllikasi monitoring (SIEM)				Laptop	5 Menit	Dashboard SIEM	Dashboard aplikasi monitoring (SIEM)
3	Melakukan analisis data keamanan pada daftar *Security Log Analysis*				Laptop, data-data log, Media Komunikasi	180 Menit	Catatan analisis data log	Mengakses fitur-fitur *security log analysis*, mencai referensi jenis-jenis serangan
4	JIka ditemukan Log Anomali maka dilanjutkan dengan pemeriksaan lebih mendalam pada log tersebut, jika tidak dilakukan analisis ulang	Tidak Ya			Laptop, data-data log, Media Komunikasi	1 Hari	Hasil analisis data log	Mempelajari bentuk serangan, skema, mitigasi, penanganan dan mencari penyebab insiden dari celah-celah kerentanan yang ditemukan
5	Melakukan *vulnerability Assessment log anomaly* untuk pembuktian FALSE POSITIVE atau FALSE NEGATIVE				Laptop, data-data log, Instrumen Vulnerability Assessment, Media Komunikasi	2 Hari		Menggunakan instrumen VA serta mengumpulkan PoC untuk menentukan FALSE POSITIVE atau FALSE NEGATIVE
6	Jika FALSE NEGATIVE maka buat laporan hasil temuan insiden siber, jika FALSE POSITIVE membuat laporan kerja	False Positive False Negative A B			Laptop, Media Komunikasi	1 Hari	Laporan insiden siber	Dilaksanakan berdasarkan hasil keputusan tim tanggap insiden siber

7	Mengirimkan Laporan hasil temuan untuk bahan verifikasi				Laptop, Media Komunikasi	5 Menit		Dikirim melalui media komunikasi
8	Melakukan verifikasi laporan untuk mendapatkan pengesahan				Laptop, Media Komunikasi	5 Menit	Laporan insiden siber yang diverifikasi	Dilakukan dan dikirim melalui media komunikasi
9	Melakukan pengesahan laporan insiden siber				Laptop, Media Komunikasi	5 Menit	Laporan insiden siber yang telah disahkan	Dilakukan melalui media komunikasi atau melalui laptop
10	Tim Insiden Siber membuat Surat Pemberitahuan kepada PSE, monitoring selesai				Laptop, Media Komunikasi	10 Menit	Surat pemberitahuan insiden siber	Dilakukan melalui media komunikasi atau melalui laptop