BAB V
PENUTUP

5.1. Kesimpulan

Kesimpulan yang diperoleh dari penelitian ini didasarkan pada hasil analisis sistem berjalan dan pengujian yang telah dilakukan. Kesimpulan yang diperoleh adalah sebagai berikut.

1. Rancangan sistem Security Orchestration, Automation, and Response (SOAR) menggunakan Shuffle berhasil mengorkestrasikan Wazuh, MISP, dan IRIS dalam satu platform. Hasil implementasi sistem pada FIK dan UPA TIK menunjukkan berbagai upaya serangan berhasil dideteksi.
2. Shuffle dirancang dengan pendekatan semi-otomatis yang melibatkan input pengguna melalui Google Chat untuk memberikan visibilitas sekaligus kontrol lebih terhadap eksekusi setiap *workflow*. Shuffle memanfaatkan mekanisme *cache* yang digunakan untuk menyimpan dan mengambil peristiwa, sehingga repons melalui Google Chat dapat diterima kembali oleh Shuffle tanpa kehilangan informasi dari *workflow* sebelumnya.
3. Sistem deteksi utama menggunakan Wazuh yang diintegrasikan dengan MISP. Sistem ini mampu mendeteksi serangan berbasis aplikasi web dan *malware*. Namun, sistem memiliki keterbatasan dalam mengidentifikasi serangan yang tidak menghasilkan HTTP *request* atau memunculkan pola *payload* yang dapat dianalisis. Berdasarkan hasil pengujian, rata – rata waktu deteksi (MTTD) tercatat sebesar 6.66 detik, rata – rata waktu yang dibutuhkan tim keamanan untuk mengakui dan menentukan tindakan (MTTA) adalah 18 detik, dan rata – rata waktu respons (MTTR) dalam menanggapi peristiwa mencapai 10 detik, serta setiap *workflow* dapat dieksekusi kurang dari 35 detik.

5.2. Saran

Saran yang diberikan sebagai hasil evaluasi perancangan adalah sebagai berikut.

1. Meningkatkan kemampuan deteksi dengan menambah dan menyesuaikan peraturan sesuai dengan kebutuhan dalam menangani tingkat keparahan maupun serangan.
2. Menyesuaikan orkestrasi berdasarkan kebutuhan, bisa melalui pendekatan semi-otomatis maupun otomatis, serta menambah ataupun mengurangi *workflow* untuk menekan waktu.
3. Melakukan lebih banyak skenario pengujian seperti pengujian dengan aplikasi web, jaringan, dan *malware*.
4. Menambahkan perangkat keamanan seperti Firewall dan IDS beserta dengan *rule*-nya untuk meningkatkan kemampuan inspeksi dari sisi jaringan.
5. Mengembangkan LLM secara lokal untuk megurangi ketergantungan terhadap layanan eksternal.
6. Diperlukan sumber daya manusia untuk memantau sistem secara periodik serta melakukan validasi dalam menentukan tindakan ketika suatu peristiwa terjadi.