



DAFTAR ISI

1	PENDAHULUAN	1
	1.1 Latar Belakang	1
	1.2 Tujuan	1
	1.3 Manfaat	2
	1.4 Ruang Lingkup	2
2	TINJAUAN PUSTAKA	2
	2.1 <i>Intrusion Detection System</i>	2
	2.2 Suricata	3
	2.3 <i>Security Information and Event Management</i>	3
	2.4 Elastic Stack	3
	2.5 Elasticsearch	3
	2.6 Logstash	3
	2.7 Kibana	4
	2.8 Filebeat	4
3	METODE	4
	3.1 Lokasi dan Waktu PKL	4
	3.2 Alat dan Bahan	4
	3.3 Prosedur Kerja	5
	3.3.1 Analisis	6
	3.3.2 Perancangan	6
	3.3.3 Implementasi	6
	3.3.4 Pengujian	6
4	KEADAAN UMUM BPPT (BADAN PENKAJIAN DAN PENERAPAN TEKNOLOGI)	6
	4.1 Sejarah	6
	4.2 Struktur Organisasi	9
5	Implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM pada Lab Development BPPT	10
	5.1 Analisis	10
	5.2 Perancangan	10
	5.3 Implementasi	12
	5.4 Pengujian	28
6	SIMPULAN DAN SARAN	46
	6.1 Simpulan	46



1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.

6.2 Saran	47
DAFTAR PUSTAKA	47
RIWAYAT HIDUP	48

DAFTAR TABEL

1 Komponen perangkat keras	5
2 Komponen perangkat lunak	5

DAFTAR GAMBAR

1 Prosedur kerja	5
2 Struktur Organisasi BPPT	10
3 Topologi jaringan IDS dan SIEM	11
4 Alur proses cara kerja sistem	12
5 Address-group	13
6 Konfigurasi suricata.yaml	14
7 Konfigurasi suricata.yaml	14
8 Konfigurasi ping.rules	15
9 Filebeat.yml	15
10 Unduh elasticsearch	16
11 Instal elasticsearch	16
12 Unduh logstash	17
13 Install logstash	17
14 Unduh kibana	17
15 Install kibana	18
16 Install nginx	18
17 Reverse proxy nginx	19
18 Konfigurasi elasticsearch.yml	20
19 konfigurasi elasticsearch.yml	20
20 Konfigurasi logstash.yml	21
21 Konfigurasi logstash.yml	21
22 Konfigurasi logstash.yml	21
23 Konfigurasi logstash.yml	21
24 Pipelines.yml	22
25 Pipeline logstash	22
26 Konfigurasi kibana.yml	22
27 Konfigurasi kibana.yml	23
28 Status elasticsearch	23
29 Status logstash	24
30 Status kibana	24
31 Filebeat Test Output	24
32 Pengaturan index	25
33 New visualization	25
34 Pilih index	26
35 Field visualization	26
36 Dashboard kibana	27





37	Editing dashboard kibana	27
38	Timestamp discover kibana	28
39	Remote SSH menggunakan Putty	29
40	Log /etc/log/suricata/eve.json	29
41	Discover kibana informasi ssh	30
42	Informasi SSH lanjutan	31
43	Dashboard event subtype SSH	32
44	Informasi SSH pengujian dua	33
45	Pengujian ping	34
46	Discover kibana informasi ping	34
47	Informasi ping lanjutan	35
48	Informasi ping lanjutan	36
49	Dashboard event subtype alert	36
50	Halaman DVWA	37
51	Discover kibana informasi http	37
52	Informasi lanjutan http	38
53	Informasi lanjutan http	39
54	Dashboard kibana http	39
55	FTP menggunakan FileZilla	40
56	Discover kibana informasi ftp	40
57	Informasi lanjutan ftp	41
58	Informasi lanjutan ftp	41
59	Dashboard kibana ftp	42
60	Dashboard anomali	43
61	Discover kibana info anomali	43
62	Informasi lanjutan anomali	44
63	Dashboard DNS	45
64	Discover informasi DNS	45
65	Informasi lanjutan DNS	46



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

- Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.