

B
L
U
E
T
E
A
M

W
R
I
T
E
U
P

H
O
W
T
O
R
E
S
P
O
N
S
E

DENIAL OF SERVICE (DOS)



BAPANG CSIRT

An incident investigation walkthrough based on ISO/IEC 27035



TABLE OF CONTENTS

03 Introduction

04 Scope

05 ISO/IEC 27035-3 Phases

00 I-Detection

00 II-Notification

00 III-Triage

00 IV-Analysis

00 V-Response

00 VI-Reporting

W
H
A
T

INTRODUCTION

Dokumen ini merupakan dokumentasi penanganan insiden dari Blue Team dalam simulasi penanganan insiden pada BaPang CSIRT. Penanganan dan respon insiden dilakukan berdasarkan standar ISO/IEC 27035 bagian 3 tentang Pedoman Operasi Tanggap Insiden TIK.

Dokumen ini dapat digunakan untuk memberikan gambaran terkait proses investigasi dan penanganan insiden siber.

Insiden yang terjadi berupa Denial of Service (DoS) terhadap layanan website yang dijalankan, sehingga menyebabkan terganggunya kinerja server dalam menangani request dari pengguna.

I
S
T
H
I
S



OBJECTIVE

Menangani insiden serangan Denial of Service (DoS) yang menargetkan layanan web berbasis HTTP/HTTPS.

Tujuan mencakup identifikasi serangan, pemulihan layanan, mitigasi serangan aktif, serta analisis untuk mencegah insiden serupa di masa depan.

R
U
A
N
G

MISSION

1. Mengidentifikasi bukti anomali lalu lintas dan sumber serangan.
2. Mengisolasi jaringan dari lalu lintas mencurigakan.
3. Menghapus koneksi serangan aktif.
4. Mengembalikan layanan website ke kondisi normal.
5. Pelaporan: Menyusun laporan insiden.

L
I
N
G
K
U
P



Sesuai dengan ruang lingkup yang ditentukan, tahapan penanganan insiden yang dilakukan terdiri dari:

1. **Deteksi (Identify, Detect, & Report)**
2. **Notifikasi (Identify, Detect, & Report)**
3. **Triase (Assessment & Decision)**
4. **Analisis (Assessment & Decision)**
5. **Respon (Response)**
6. **Pelaporan (Response)**

STEP 1: DETECTION



Pendeteksian insiden dilakukan oleh **Sistem Otomasi Respon Insiden SIEM Wazuh**. Wazuh menerima log dari berbagai sumber/endpoint secara realtime. Apabila terdapat log dari sumber (Wazuh Agent, Firewall, atau IDS) yang sesuai dengan *rules*, maka Alert akan muncul.

The screenshot shows the Wazuh Data Explorer interface. On the left, there's a sidebar with a dropdown menu set to "wazuh-alerts-*". Below it is a "Filter by type" section with several options like "previous_output", "rule.firetimes", and "rule.frequency". The main area has a search bar with the query "rule.id: Is one of 100001, 100002" and a "DQL" button. A histogram titled "31 hits" shows event counts per hour from July 6 to July 10. Below the histogram is a table with columns: TIME, agent.ip, agent.name, full_log, rule.description, and rule.level. Two rows are visible: one for a Web Defacement Attack and another for a DoS attack. The second row is highlighted with a red box. At the bottom, there's a detailed view of the "full_log" field for the DoS attack entry, which is also highlighted with a red box.

TIME	agent.ip	agent.name	full_log	rule.description	rule.level
> Jul 9, 2025 @ 22:12:07.835	172.20.10.114	LAB_Ubuntu	File '/var/www/makary.org/index.html' modified. Mode: realtime Changed attributes: size, mtime, md5, sha1, etag +8000 [GET / HTTP/1.1] 400 491 "TESTING_PURPOSES ONLY"	Web Defacement Attack_Detected: /var/www/html/makaryo/index.html	12
> Jul 9, 2025 @ 22:05:45.182	172.20.10.114	LAB_Ubuntu	172.20.10.112 - - [09/Jul/2025:15:05:42 +0000] "GET / HTTP/1.1" 400 491 "TESTING PURPOSES ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.152 Safari/537.36Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.75.14 (KHTML, like Gecko) Version/7.0.3 Safari/537.75.14"	DoS Attack Detected on Web Service	12

full_log

```
172.20.10.112 - - [09/Jul/2025:15:05:42 +0000] "GET / HTTP/1.1" 400 491 "TESTING PURPOSES ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.152 Safari/537.36Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.75.14 (KHTML, like Gecko) Version/7.0.3 Safari/537.75.14"
```

Selain sistem deteksi pada SIEM dan Sistem Otomasi Respon Insiden, pendeksteksian insiden juga dapat dilakukan berdasarkan laporan dari stakeholder, pengguna, atau anggota organisasi yang terdampak insiden.

STEP 2 : NOTIFICATION



Apabila Alert yang muncul di Wazuh sesuai dengan kondisi yang mengindikasikan terjadinya suatu insiden, maka Alert tersebut akan diolah oleh Sistem Otomasi Respon Insiden. Alert akan diteruskan menjadi Notifikasi melalui **Telegram** kepada Tim Tanggap Insiden Siber.

NFA IR-SOC Lab

Wazuh Alert Detected (#1752071509.5936765)

Description: DoS Attack Detected on Web Service
Severity Level: 12
Agent: LAB_Ubuntu
Timestamp: 2025-07-09T14:31:49.079+0000

Rule ID: 100001
Category: ['aggregation', 'customdos', 'web', 'attack', 'custom']

Mohon ditinjau segera. 9:32 PM

Meskipun telah dikirimkan notifikasi di Grup Telegram, notifikasi dapat diteruskan ke pihak lain (jika diperlukan) seperti Stakeholder atau Pimpinan yang tidak tergabung dalam grup. Media notifikasi juga bisa menggunakan Email.

STEP 3 : TRIAGE

Pada tahap ini, Incident Responder melakukan assessment terhadap alert insiden yang diterima dan menentukan apakah alert tersebut **false positive** atau **true positive**.



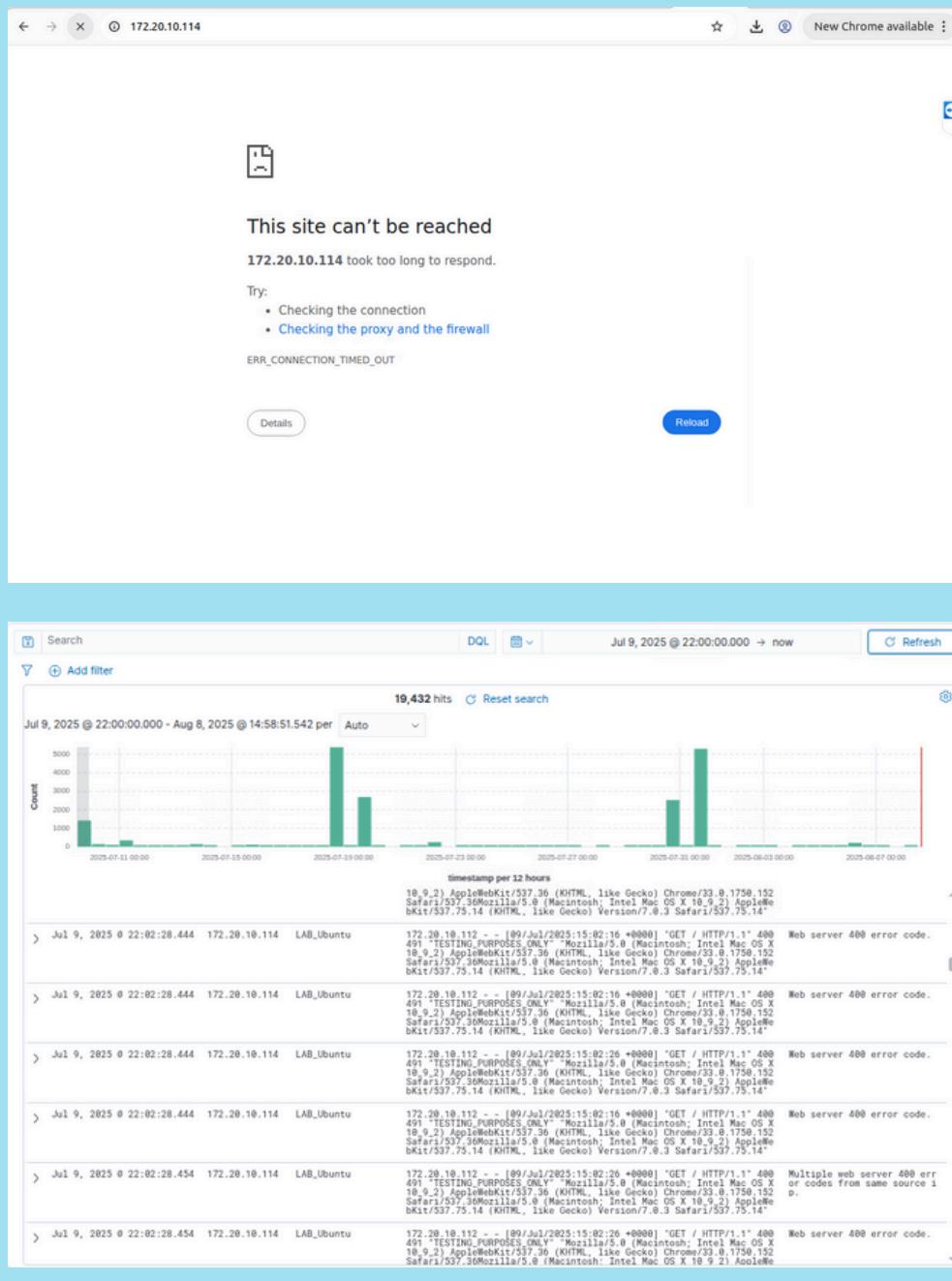
Sistem Otomasi Respon Insiden telah membuatkan **Case** insiden pada **DFIR IRIS** secara otomatis setelah Alert muncul. Incident Responder dapat menggunakan platform DFIR IRIS sebagai platform manajemen insiden dan kolaborasi terkait proses penanganan insiden seperti **penambahan IoC**, **pengunggahan evidence**, dan **pendelegasian tugas**.

A screenshot of the DFIR IRIS web interface. The URL is https://172.20.10.109/case?cid=211. The page title is "#211 - Wazuh Alert: DoS Attack Detected on Web Service on LAB_Ubuntu". The summary section shows the alert was opened on 2025-07-10 by administrator and owned by administrator. It has a severity of Low and is categorized as Unknown. Customer is Analyst01 and SOC ID is SOC-NFA. Below the summary are buttons for Manage, Processors, Pipelines, Request review, Generate report, and Activity report. The Case summary section contains a note about receiving an alert from Wazuh/Suricata and ongoing analysis. It lists initial information: Agent: LAB_Ubuntu, Waktu: 2025-07-09T15:05:45.182+0000, Severity: 12, Deskripsi Rule: DoS Attack Detected on Web Service, and Kategori: ['aggregation', 'customdos', 'web', 'attack', 'custom']. A note at the bottom states: "Case ini dibuat secara otomatis untuk kebutuhan triase dan investigasi awal." The bottom left corner shows the IRIS logo with version v2.4.20.

Setelah dilakukan analisis awal, Analis dapat menentukan apakah Case Insiden akan dieskalasi (**true positive**) atau ditutup (**false positive**). Analisis awal dapat dilakukan dengan memeriksa log di **SIEM** maupun perangkat perimeter lainnya.

STEP 3 : TRIAGE (CONT)

Berikut hasil pemeriksaan log alert di SIEM dan pemeriksaan tampilan halaman website. Terjadi eror dengan status **code 400** secara berulang kali pada layanan web. Browser juga **tidak bisa memuat** halaman web.



Dapat disimpulkan bahwa insiden ini benar terjadi (*true positive*). Tahapan berlanjut ke Analisis.

STEP 4 : ANALYSIS

Analisis dapat dilakukan melalui beberapa cara berikut:

1. **Pemeriksaan IoC** ke Virustotal/MISP/CTI lainnya
2. **Pemindaian evidence** atau antivirus
3. **Analisis log** (jaringan maupun aplikasi), dll



Sistem akan secara otomatis melakukan analisis dasar berupa pemeriksaan IoC (IP Address) ke **Virustotal** yang ditampilkan hasilnya di bagian **Note** pada Case insiden terkait.

The screenshot shows a Wazuh interface for Case ID #270. The top navigation bar includes tabs for Summary, Notes, Assets, IOC, Timeline, Graph, Tasks, Evidence, and several icons. The 'Notes' tab is active. A sidebar on the left shows a folder icon labeled 'Analysis' with a sub-item 'Basic Enrichment with Virustotal (Case ID #270)'. The main content area displays a note titled 'Basic Enrichment with Virustotal (Case ID #270)' with a timestamp '#26 - b642a39f-178f-43dd-b3f3-7ba13823bd8a'. Below the title are various note-taking icons. The note content is as follows:

```
Hasil analisis Virustotal:  
1  {'malicious': 0, 'suspicious': 0, 'undetected': 94,  
2   'harmless': 0, 'timeout': 0}  
3  
4  *Hasil pemindaian evidence dapat dilihat di mesin  
target (victim) pada direktori  
/var/www/html/makaryo/webagent_thor_* .html
```

On the right side of the note, there are two text boxes with translations of the note content:

Hasil analisis Virustotal: ['malicious': 0, 'suspicious': 0, 'undetected': 94, 'harmless': 0, 'timeout': 0]

Hasil pemindaian evidence dapat dilihat di mesin target (victim) pada direktori /var/www/html/makaryo/webagentthor.html

Untuk hasil yang lebih komprehensif, lakukan analisis lanjutan secara **manual** seperti analisis log jaringan maupun koneksi jaringan untuk mendeteksi potensi ancaman. **Jangan lupa tambahkan hasil analisis manual di Case insiden.**

STEP 5 : RESPONSE



Untuk insiden *Denial of Service* ini, *incident responder* dapat menentukan untuk menjalankan *workflow respon otomatis* atau melakukannya secara manual. Apabila memilih otomatis, maka sistem akan melakukan **pemblokiran alamat IP sumber** dan memuat kembali (*restart*) **web server**.

Berikut adalah hasil respon insiden otomatis berupa pemblokiran alamat IP sumber.

```
root@webagent:~# sudo iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    DROP       all  --  172.20.10.112      0.0.0.0/0
2    DROP       all  --  172.20.10.112      0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
root@webagent:~#
```

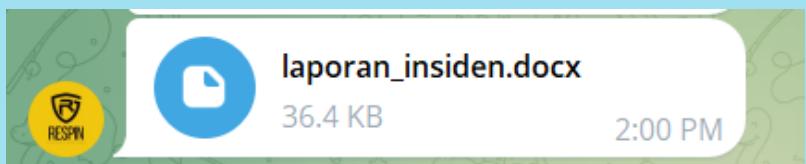
Layanan website sudah bisa diakses kembali seperti semula.



STEP 6 : REPORTING



Tahapan terakhir adalah pembuatan laporan. Tahapan ini melakukan pembuatan laporan secara otomatis dan mengirimkannya kepada tim melalui Telegram. Selain itu, dilakukan juga penambahan informasi ancaman ke MISP.



Dokumen format laporan yang dihasilkan secara otomatis oleh sistem masih belum lengkap, sehingga diperlukan penambahan data dan informasi oleh analis pada dokumen agar menghasilkan laporan yang komprehensif.

The screenshot shows a Microsoft Word document with the title "LAPORAN-HASIL-PENANGANAN-INSIDEN". The content is organized into several sections:

- Denial-of-Service-pada-Layanan-Web**:
Formulir-ini-digunakan-untuk-pelaporan-hasil-penanganan-insiden-siber-oleh-Badan-Pangan-CSIRT.
- Informasi-Insiden**:

Waktu-Pelaporan	2025-08-06T15:05:45.182+0000
Nama-Pelapor	-
Waktu-Respons	2025-08-06T15:05:45.182+0000
Nama-Personel	-
Aset-Terdampak	172.20.10.114
Bukti-Insiden-(Screenshots)	[Lampiran-Screenshot]
- Identifikasi-Insiden**:
Wazuh-mendeteksi-eror-code-400-berulang-dalam-kurun-waktu-yang-singkat-pada-layanan-web.
- Penyelidikan-Insiden**:
DoS-Attack-Detected-on-Web-Service
- Tindakan-Penanganan-Insiden**:
Blokir-IP-sumber-dan-webserver-direstart.
- Pemulihan-Insiden**:
restart-webserver
- Dampak-Insiden**:

Dampak-Finansial-dan-Biaya	Tidak-ada-kerugian-finansial-langsung
Dampak-Operasional	Layanan-tidak-dapat-digunakan-dan-diakses selama-waktu-tertentu

P
E
N
U
T
U
P



*Ingatlah, Bahwa Kechilafan Satu
Orang Sahaja Tjukup Sudah
Menjebabkan Keruntuhan Negara*

P
E
N
U
T
U
P

