

**ANALISIS PENANGANAN DAN PENCEGAHAN  
INSIDEN SERANGAN SIBER PADA *WEBSITE*  
MENGUNAKAN METODE NIST 800-61**

**Tugas Akhir**

**Diajukan Untuk Memenuhi Salah Satu Persyaratan Mencapai Derajat  
Sarjana Teknik Informatika**



Dibuat Oleh :

**Charles**

**14 07 07999**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS ATMA JAYA YOGYAKARTA  
2019**

# LEMBAR PENGESAHAN

Analisis Penanganan dan Pencegahan Insiden Serangan Siber Pada *Website*  
Menggunakan Metode NIST 800-61

Yogyakarta, 12 Maret 2019

Charles

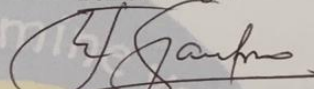
140707999

Pembimbing I



Th. Adi Purnomo Sidhi, S.T.,M.T

Pembimbing II



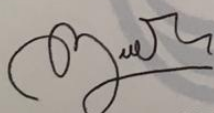
Dr. Ir. Alb. Joko Santoso, M.T.

Penguji I



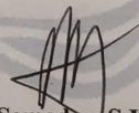
Th. Adi Purnomo Sidhi, S.T.,M.T

Penguji II



Dr. Pranowo, S.T.,M.T.

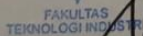
Penguji III



Joseph Eric Samodra, S.Kom.,MIT

Mengetahui,

Dekan Fakultas Teknologi Industri



FAKULTAS  
TEKNOLOGI INDUSTRI

Dr. A. Teguh Siswanto, M.Sc.

## Pernyataan Originalitas & Publikasi Ilmiah

Saya yang bertanda tangan di bawah ini:

Nama Lengkap : Charles  
NPM : 140707999  
Program Studi : Teknik Informatika  
Fakultas : Teknologi Industri  
Judul Penelitian : Analisis Penanganan dan Pencegahan Insiden  
Serangan Siber Pada *Website* Menggunakan NIST  
800-61

Menyatakan dengan ini:

1. Tugas Akhir ini adalah benar tidak merupakan salinan sebagian atau keseluruhan dari karya penelitian lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa Hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum atas pelanggaran Hak Cipta dalam pembuatan Tugas Akhir ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 12 Maret 2019

Yang menyatakan,



Charles

140707999

## **HALAMAN PERSEMBAHAN**



**Tugas Akhir ini penulis persembahkan untuk :**

**Tuhan Yesus Kristus dan Bunda Maria**

**Mama, bapak, adik, dan semua anggota keluarga yang memberikan dukungan dan doa, serta sahabat dan teman-teman yang selalu memberikan dukungan dan doa terkasih**

## KATA PENGANTAR

Puji dan syukur penulis hanturkan kepada Tuhan Yesus Kristus karena atas kebaikan dan kasih karuniaNya penulis senantiasa diberikan kelancaran dari awal pembuatan tugas akhir “Analisis Penanganan dan Pencegahan Insiden Serangan Siber Pada *Website* Menggunakan Metode NIST 800-61” hingga menyelesaikannya dengan baik.

Tugas akhir atau yang lebih dikenal dengan skripsi ini bertujuan untuk memenuhi salah satu syarat yang wajib ditempuh oleh mahasiswa untuk mencapai derajat sarjana Teknik Informatika khususnya mahasiswa dari Program Studi (Prodi) Teknik Informatika Fakultas Teknologi Industri (FTI) Universitas Atma Jaya Yogyakarta (UAJY).

Dalam proses pembuatan tugas akhir, penulis mendapat pertolongan dari berbagai pihak dalam bentuk dukungan, doa, dan juga bimbingan. Untuk itu, pada kesempatan kali ini penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yesus Kristus dan Bunda Maria atas segala rahmat, pertolongan, kesehatan dan tuntunanNya kepada penulis sehingga penulis dapat menyelesaikan pembuatan tugas akhir dengan baik dan tepat waktu.
2. Lambertus Manseo dan Maria Yuliati sebagai ayah dan ibu yang selalu memberikan semangat, dukungan, dan selalu mempercayai penulis dapat menyelesaikan tugas akhir ini.
3. Seluruh keluarga besar penulis yang telah membantu memberikan semangat kepada penulis.
4. Bapak Dr. A. Teguh Siswanto, M.T. selaku Dekan Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta.
5. Bapak Th. Adi Purnomo Sidhi, S.T.,M. selaku Dosen Pembimbing I yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.

6. Bapak Dr. Ir. Alb. Joko Santoso, M.T. selaku Dosen Pembimbing II yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
7. Bapak Wilfridus Bambang Tri H., S.T., M.Cs. yang telah memberikan masukan yang bermanfaat kepada penulis untuk menyelesaikan tugas akhir ini.
8. Bhante Dhammasubho Mahathera yang telah memberikan motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
9. Clara Christina Gunawan yang telah memberikan saran, motivasi, dan dukungan kepada penulis untuk menyelesaikan tugas akhir ini.
10. Seluruh dosen dan staf Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta atas bimbingan maupun bantuannya selama proses kuliah.
11. Tri Purnomo Aji, William Yuto, Swandi, Dwiki Setiawan, Siddharta Chandra, Robby Arundra, Venansius Budiono, Antonius Felix Kinarto selaku teman dalam melakukan kekonyolan yang tidak ada gunanya yang sangat menghibur penulis dalam mengerjakan tugas akhir ini.
12. Teman-teman maupun pihak lain yang tidak dapat disebutkan satu per satu yang juga membantu penulis.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan tugas akhir ini. Dengan rendah hati penulis menerima saran dan masukan yang membangun penulis menjadi insan yang berkembang maju menjadi lebih baik. Penulis berharap tugas akhir ini dapat menjadi manfaat untuk semua pihak dan menjadi amal ibadah di sisi-Nya.

Yogyakarta, 12 Maret 2019

Penulis

## DAFTAR ISI

<b>JUDUL .....</b>	<b>i</b>
<b>LEMBAR PENGESAHAN .....</b>	<b>ii</b>
<b>Pernyataan Originalitas &amp; Publikasi Ilmiah .....</b>	<b>iii</b>
<b>HALAMAN PERSEMBAHAN.....</b>	<b>iv</b>
<b>KATA PENGANTAR.....</b>	<b>v</b>
<b>DAFTAR ISI.....</b>	<b>vii</b>
<b>DAFTAR GAMBAR.....</b>	<b>ix</b>
<b>DAFTAR TABEL.....</b>	<b>x</b>
<b>INTISARI.....</b>	<b>xi</b>
<b>BAB I. PENDAHULUAN.....</b>	<b>1</b>
<b>1.1 Latar Belakang.....</b>	<b>1</b>
<b>1.2 Rumusan Masalah.....</b>	<b>6</b>
<b>1.3 Batasan Masalah.....</b>	<b>6</b>
<b>1.4 Tujuan Penelitian.....</b>	<b>7</b>
<b>1.5 Metode Penelitian.....</b>	<b>7</b>
1.5.1 Teknik Pengumpulan Data.....	9
1.5.2 Tahap-tahap Penelitian.....	10
<b>1.6 Sistematika Penelitian.....</b>	<b>10</b>
<b>BAB II. TINJAUAN PUSTAKA.....</b>	<b>12</b>
<b>2.1 Penelitian Terdahulu.....</b>	<b>12</b>
<b>BAB III. LANDASAN TEORI.....</b>	<b>16</b>
<b>1.1 Penanganan Insiden.....</b>	<b>16</b>
<b>1.2 Pencegahan Insiden.....</b>	<b>16</b>
<b>1.3 Serangan Siber.....</b>	<b>17</b>
1.3.1 Modus Kejahatan Cyber Crime.....	18
1.3.2 Penyebab Terjadinya Cyber Crime.....	21
1.3.3 Penanganan dan Pencegahan Cyber Crime.....	21
1.3.4 Tindakan Hukum Bagi Pelaku Cyber Crime.....	23
<b>1.4 Website.....</b>	<b>26</b>

3.4.1 Serangan Pada Website.....	28
<b>1.5 NIST.....</b>	<b>30</b>
<b>1.6 Definisi SOP.....</b>	<b>34</b>
1.6.1 Tujuan SOP.....	35
1.6.2 Manfaat SOP.....	36
<b>1.7 Perbedaan NIST 800-61 dan Cobit V5.....</b>	<b>37</b>
<b>1.8 Perbedaan NIST 800-61 dan ISO 27001.....</b>	<b>38</b>
<b>1.9 Perbedaan NIST 800-61 dan ITIL V3.....</b>	<b>38</b>
<b>BAB IV. ANALISIS DAN PERANCANGAN SOP.....</b>	<b>40</b>
<b>4.1 Analisis SOP.....</b>	<b>40</b>
<b>4.2 Lingkup Masalah.....</b>	<b>40</b>
<b>4.3 Perancangan .....</b>	<b>41</b>
4.3.1 Perancangan Arsitektur.....	41
4.3.2 Proses Penanganan dan Pencegahan Insiden.....	42
4.3.3 Proses Sebelum Insiden Serangan Dikerjakan.....	43
4.3.4 Persiapan Penanganan Insiden.....	45
4.3.5 Identifikasi dan Analisis.....	47
4.3.6 Penanganan Serangan.....	48
4.3.7 Penghapusan Serangan.....	49
4.3.8 Pemulihan Sistem.....	50
4.3.9 Pasca Insiden Serangan.....	52
<b>BAB V. IMPLEMENTASI DAN PENGUJIAN.....</b>	<b>54</b>
<b>5.1 Implementasi Pembuatan SOP.....</b>	<b>54</b>
5.1.1 Pembuatan SOP.....	54
<b>5.2 Pengujian SOP.....</b>	<b>61</b>
<b>5.3 Hasil Pengujian SOP Terhadap Pengguna.....</b>	<b>62</b>
<b>BAB VI. KESIMPULAN DAN SARAN.....</b>	<b>71</b>
<b>6.1 Kesimpulan.....</b>	<b>71</b>
<b>6.2 Saran.....</b>	<b>71</b>
<b>DAFTAR PUSTAKA.....</b>	<b>72</b>

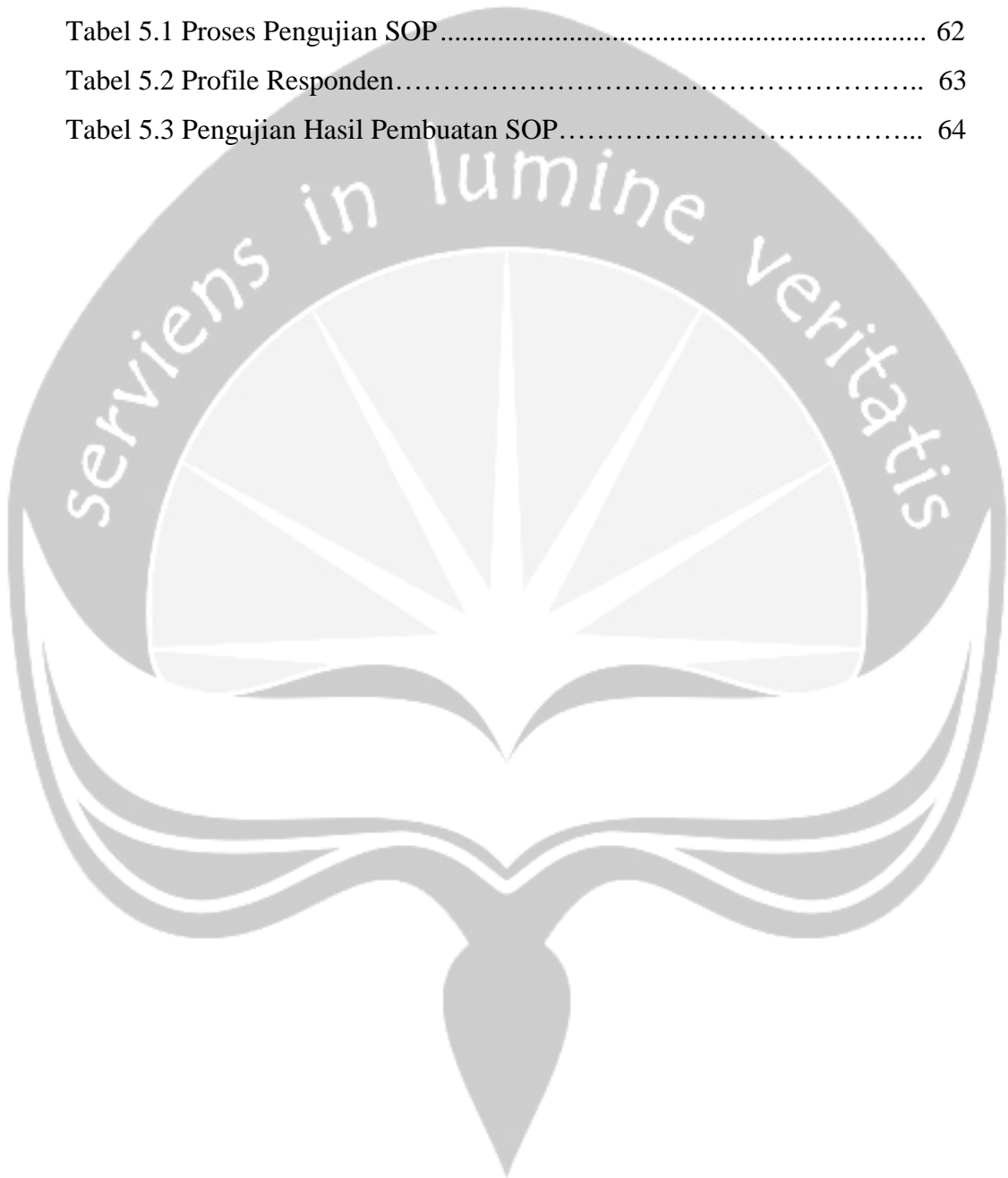


## DAFTAR GAMBAR

Gambar 1.1 Traffic laporan insiden serangan tahun 2016 di Indonesia .....	3
Gambar 1.2 Grafik insiden serangan website .....	3
Gambar 1.3. sepuluh global teknik serangan yang terjadi pada tahun 2014, 2015, dan 2016.....	4
Gambar 1.4. Skema proses penelitian .....	8
Gambar 3.1. Tahap incident handling berdasarkan NIST 800-61 .....	31
Gambar 3.2. siklus hidup respon insiden Cobit v5 .....	37
Gambar 3.3. siklus hidup respon insiden NIST 800-61 .....	37
Gambar 3.4. siklus hidup respon insiden ISO 27001 .....	38
Gambar 3.5. siklus hidup respon insiden ITIL v3.....	39
Gambar 4.1. Rancangan Arsitektur proses terjadinya penanganan insiden ...	41
Skema 4.2. Proses Penanganan dan Pencegahan Insiden .....	42
Skema 4.3. Proses Sebelum Insiden Serangan dikerjakan.....	43
Skema 4.4. Proses Persiapan Penanganan insiden .....	45
Skema 4.5. Proses Identifikasi dan Analisis .....	47
Skema 4.6. Proses Penanganan Serangan .....	48
Skema 4.7. Proses Penghapusan Serangan .....	49
Skema 4.8. Proses Pemulihan Sistem .....	50
Skema 4.9. Proses Pasca Insiden Serangan.....	52
Gambar 5.1. Tahap Preparation Incident Handling berdasarkan NIST 800-61 .....	55
Gambar 5.2. Tahap Detection & Analysis Incident Handling berdasarkan NIST 800-61.....	56
Gambar 5.3. Tahap Containment, Eradication, & Recovery Incident Handling berdasarkan NIST 800-61 .....	58
Gambar 5.4. Tahap Post-Incident Activity Incident Handling berdasarkan NIST 800-61.....	60
Gambar 5.5 Pengujian kemudahan SOP .....	65
Gambar 5.6 Pengujian penggunaan SOP .....	66
Gambar 5.7 Pengujian standar penanganan SOP .....	67
Gambar 5.8 Pengujian mempercepat proses penanganan .....	68
Gambar 5.9 Pengujian membantu penanganan insiden .....	69
Gambar 5.10 Pengujian kesimpulan SOP .....	70

## DAFTAR TABLE

Tabel 2.1 Perbandingan Penelitian Penanganan Insiden.....	15
Tabel 5.1 Proses Pengujian SOP.....	62
Tabel 5.2 Profile Responden.....	63
Tabel 5.3 Pengujian Hasil Pembuatan SOP.....	64



## INTISARI

*Website* menjadi salah satu sarana yang digunakan oleh sebuah instansi untuk menampilkan berbagai data dan informasi. *Website* yang aman sudah menjadi kewajiban bagi instansi yang memanfaatkan teknologi informasi dalam proses bisnisnya. Keamanan merupakan salah satu faktor penting dalam membangun sebuah *website*, operasi keamanan ini ditunjukkan bagi data dan informasi yang dimiliki oleh sebuah instansi. Meskipun sebuah instansi sudah memperhatikan keamanan sistem, terkadang masih memungkinkan terjadinya sebuah insiden serangan. Insiden tersebut juga termasuk penyerangan terhadap *website* yang dimiliki sebuah instansi. Jenis-jenis serangan yang sering menyebabkan gangguan pada *website* antara lain: *SQL Injection*, *Web Deface*, dan *DDoS (Distributed Denial of Service)*.

Berdasarkan dampak yang ditimbulkan oleh serangan atau kasus diatas, maka diperlukan sebuah standar operasional prosedur (SOP) yang dapat menangani penanganan insiden serangan pada *website*. Dalam mewujudkan hal tersebut, pembuatan standar operasional prosedur dibuat dengan berpedomankan dengan metode NIST 800-61. Metode NIST 800-61 adalah sebuah metode khusus yang dikeluarkan oleh NIST (*National Institute of Standards and Technology*) yang membahas mengenai penanganan insiden (*incident handling*) dan bersifat umum dimana metode NIST 800-61 dapat digunakan oleh siapa saja asalkan masih terkait dengan *cybersecurity*.

Hasil dari penelitian ini adalah sebuah Standar Operasional Prosedur (SOP) yang dapat digunakan sebagai panduan dalam menangani insiden serangan pada *website*. SOP ini bersifat umum yang mana dapat digunakan sebagai panduan untuk menangani berbagai jenis insiden serangan yang terjadi pada *website*. Dalam SOP ini juga akan dibahas mengenai usaha-usaha yang harus dilakukan oleh seorang yang menangani insiden serangan (*incident handler*) untuk mencegah apabila terjadi serangan pada *website*.

**Kata kunci:** *Website*, *Serangan pada website*, *Incident Handling*, *SOP*, *NIST 800-61*.

Dosen Pembimbing I : Th. Adi Purnomo Sidhi, S.T.,M.T.

Dosen Pembimbing II : Dr. Ir. Alb. Joko Santoso, M.T.

Jadwal Sidang Tugas Akhir : Selasa, 19 Maret 2019