

# SELAMAT DATANG



DEPUTI PENANGGULANGAN DAN PEMULIHAN  
**BADAN SIBER DAN SANDI NEGARA**

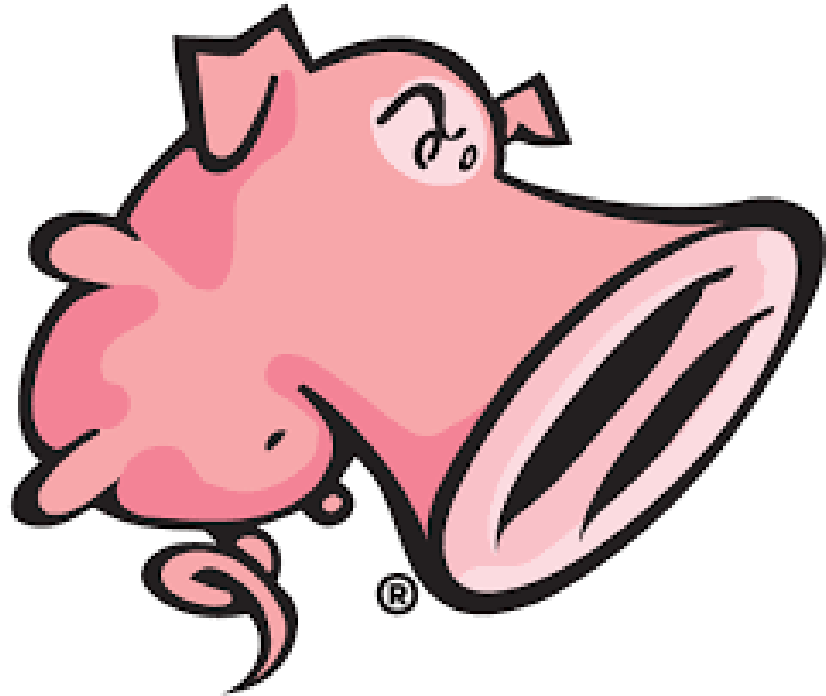
**CYBER SECURITY DRILL TEST**



INTERNET SECURITY TRAINING

[training@idsirtii.or.id](mailto:training@idsirtii.or.id)

# *Intrusion Detection System (IDS)*



**Nidaul Muiz Aufa**

 : [aufa@idsirtii.or.id](mailto:aufa@idsirtii.or.id)

 : [nidaul.muiz@bssn.go.id](mailto:nidaul.muiz@bssn.go.id)

 : [@sir\\_aufa](https://t.me/sir_aufa)

Ancol, 25 s.d 29 Maret 2019





# IDS

sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

[d.wikipedia.org/wiki/Sistem\\_deteksi\\_intrusi](https://d.wikipedia.org/wiki/Sistem_deteksi_intrusi)

“Sistem keamanan jaringan komputer yang terhubung ke internet harus **direncanakan** dan dipahami dengan baik agar dapat melindungi investasi dan sumber daya di dalam jaringan komputer tersebut secara **efektif**”



## Jenis-jenis IDS

**Network-based Intrusion Detection System (NIDS):** Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan.

**Host-based Intrusion Detection System (HIDS):** Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak.



# Intrusion Detection $\neq$ Intrusion Prevention

IDS itu sendiri bersifat **PASIF** karena hanya memantau aktifitas dalam sebuah jaringan internet, untuk memberitahukan apabila ada sebuah percobaan penyusupan ke sistem atau jaringan kita.

Kesuksesan Intrusion Detection tidak hanya tergantung kepada **teknologi**, namun juga kepada **policy** dan **management**. (1) Security policy, mendefinisikan apa yang boleh atau tidak boleh dilakukan. (2) Notifikasi, Bagaimana memberi peringatan. (3) Koordinasi dalam memberikan respon

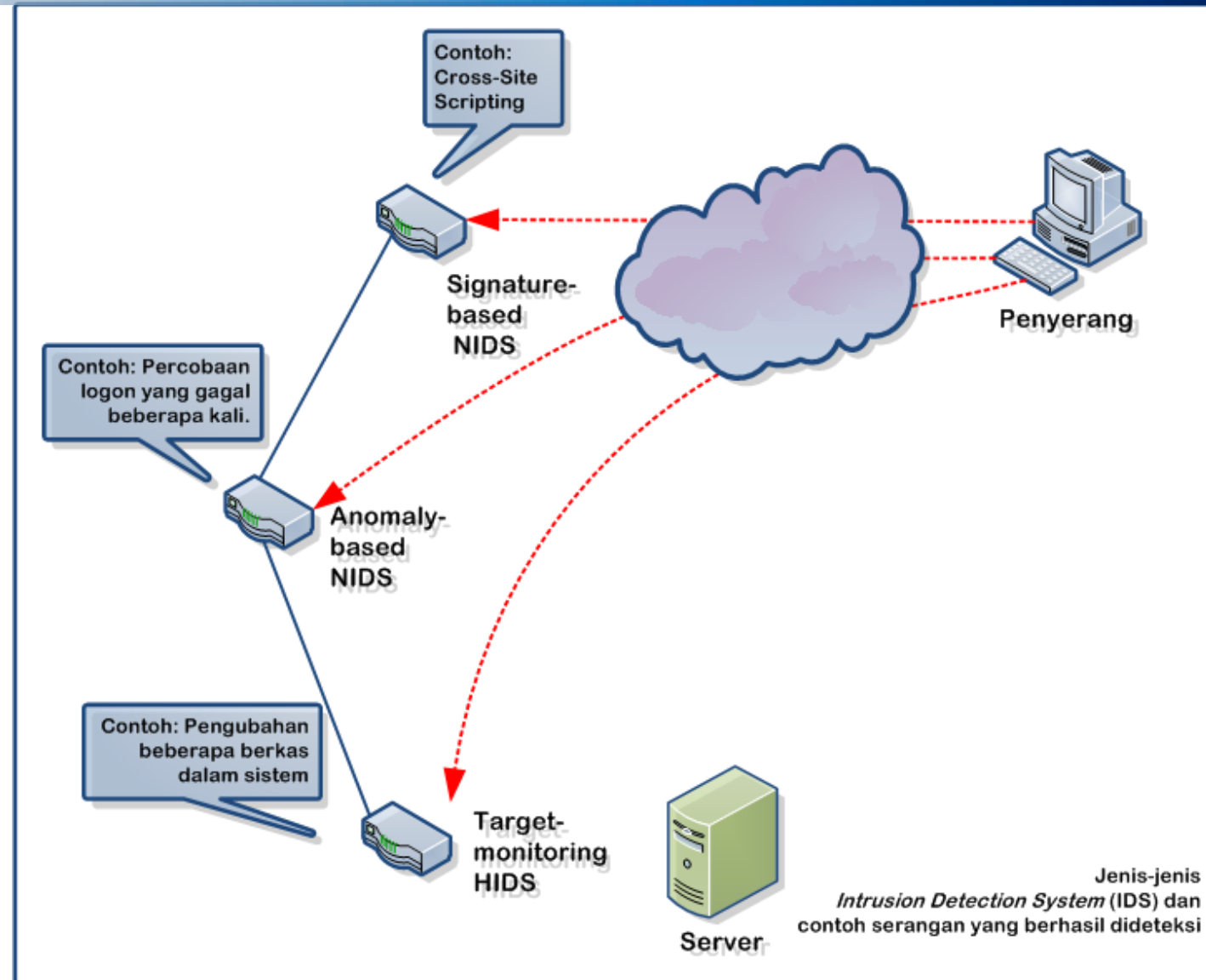


## Implementasi & Cara Kerja

**Signature Based** : Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data *signature* IDS yang bersangkutan.

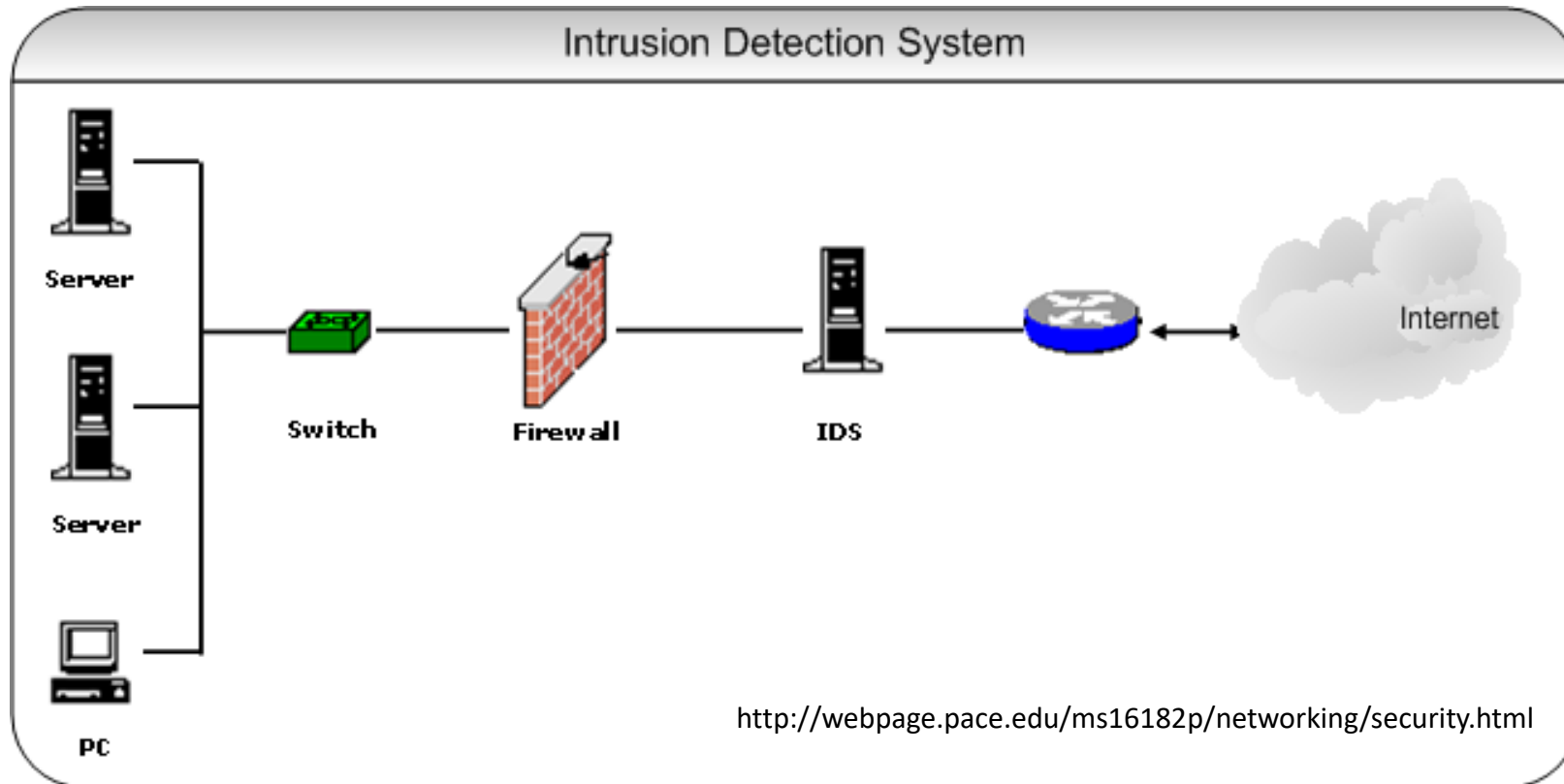
**AnomalyBased** : menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data *signature* IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan *false positive*

**PassiveIDS** : melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringkali diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.



<http://id.wikipedia.org/wiki/Berkas:IDS.png>

# Topologi IDS



# Kelebihan IDS

1. Dapat disesuaikan dengan mudah dalam menyediakan perlindungan untuk keseluruhan jaringan.
2. Dapat dikelola secara terpusat dalam menangani serangan yang tersebar dan bersama-sama.
3. Menyediakan pertahanan pada bagian dalam.
4. Menyediakan layer tambahan untuk perlindungan.
5. IDS memonitor Internet untuk mendeteksi serangan.
6. IDS melacak aktivitas pengguna dari saat masuk hingga saat keluar.
7. IDS menyederhanakan sistem sumber informasi yang kompleks.
8. IDS memberikan integritas yang besar bagi infrastruktur keamanan lainnya



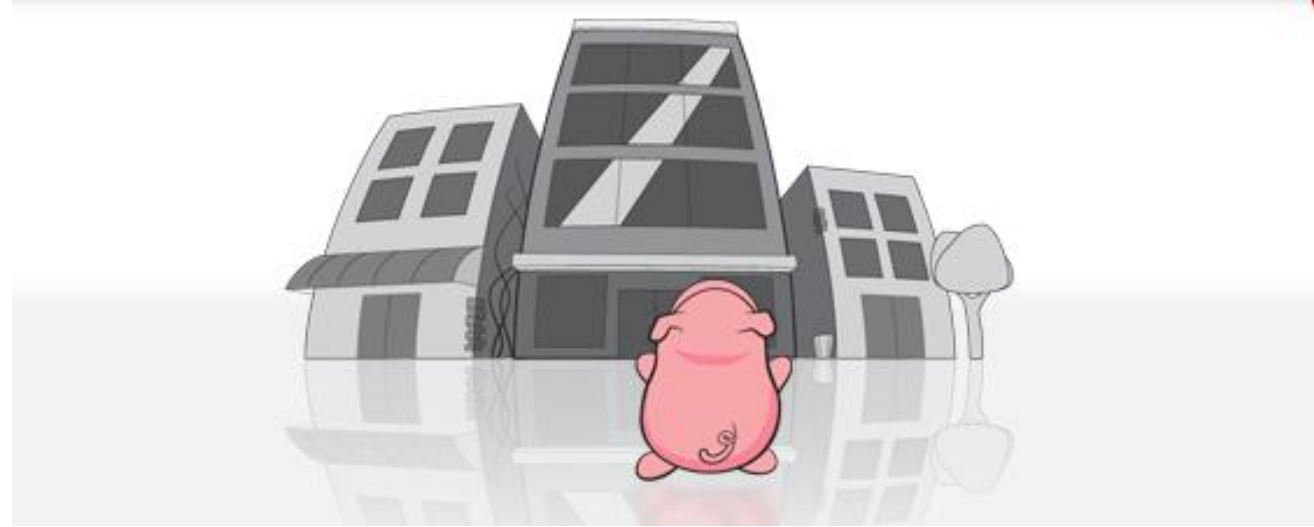
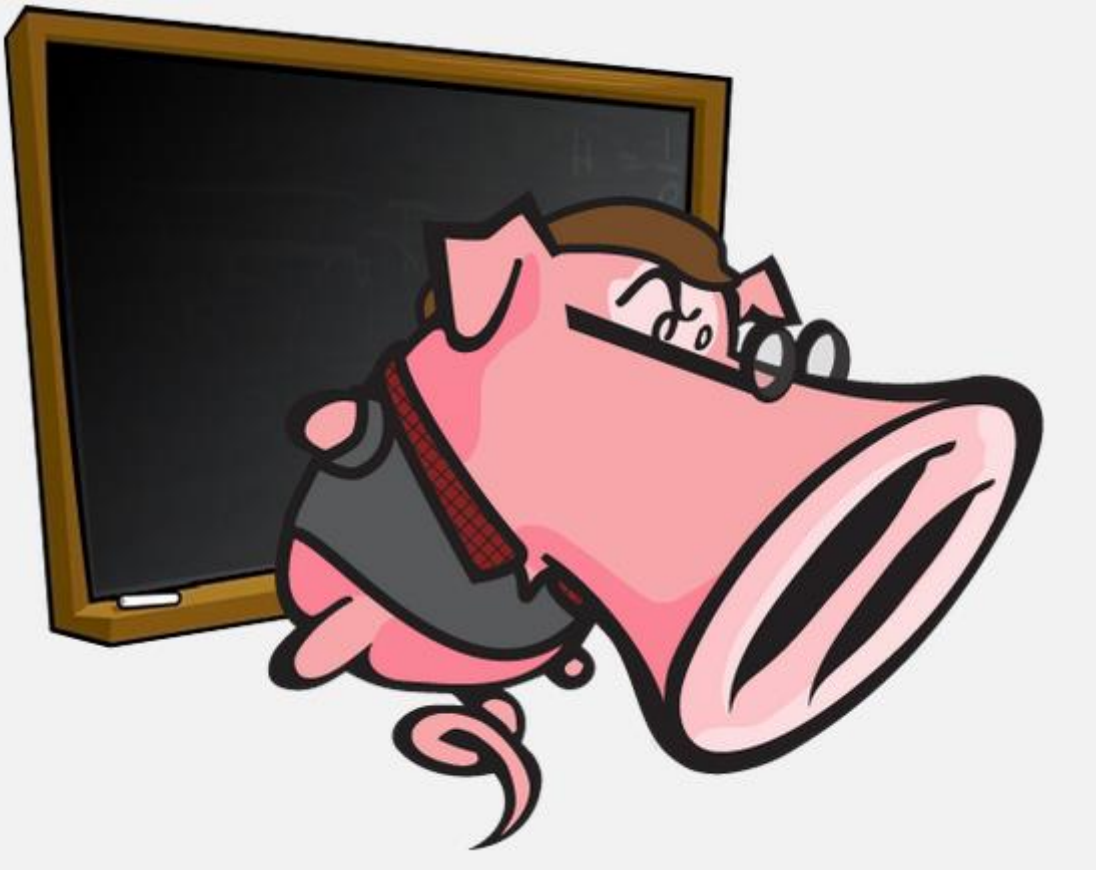
# Kekurangan IDS

1. Lebih bereaksi pada serangan daripada mencegahnya.
2. Menghasilkan data yang besar untuk dianalisis.
3. Rentan terhadap serangan yang “rendah dan lambat”.
4. Tidak dapat menangani trafik jaringan yang terenkripsi.
5. IDS hanya melindungi dari karakteristik yang dikenal.
6. IDS tidak turut bagian dalam kebijakan keamanan yang efektif, karena dia harus diset terlebih dahulu.
7. Network-based IDS dapat menyalahartikan hasil dari transaksi yang mencurigakan.

## Produk IDS

1. Real Secure dari Internet Security Systems (ISS).
2. Cisco Secure Intrusion Detection System dari Cisco Systems (yang mengakuisisi WheelGroup, yang memiliki produk NetRanger).
3. eTrust Intrusion Detection dari Computer Associates (yang mengakuisisi MEMCO, yang memiliki SessionWall-3).
4. Symantec Client Security dari Symantec.
5. Computer Misuse Detection System dari ODS Networks.
6. *Snort (open source)*.





Latar Belakang

Apa itu Snort?

Menggunakan Snort

Arsitektur Snort

*Third-Party*



# SNORT



# SNORT

**Snort** adalah salah satu NIDS (Network-based IDS) yang bekerja dengan cara menganalisa paket data yang dianggap serangan yang melintas melewati suatu network.

## MODE :

- ✓ Sniffer
- ✓ Packet Logger
- ✓ Forensic Data Analysis Tool
- ✓ Network Intrusion Detection System



## MODE SNIFFER



copyright Mark Dew

- ❑ Bekerja seperti tcpdump.
- ❑ Decodes packets dan dumps ke stdout.
- ❑ BPF filtering interface yang tersedia untuk membentuk lalu lintas jaringan yang ditampilkan.

```

E:\WINNT\System32\cmd.exe - snort -I F:\Snort\log -c F:\Snort\etc\snort.conf -A console
02/06-08:04:12.608089  [**] [1:1002:5] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] (TCP) 192.168.0.201:2572 -> 63.247.70.221:80
02/06-08:04:14.668090  [**] [1:1002:5] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] (TCP) 192.168.0.201:2574 -> 12.129.204.221:80
02/06-08:04:15.392294  [**] [1:1002:5] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] (TCP) 192.168.0.201:2575 -> 12.129.204.221:80
02/06-08:04:23.121186  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.201 -> 192.168.0.10
02/06-08:04:23.122320  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.10 -> 192.168.0.201
02/06-08:04:24.117107  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.201 -> 192.168.0.10
02/06-08:04:24.118246  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.10 -> 192.168.0.201
02/06-08:04:25.119651  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.201 -> 192.168.0.10
02/06-08:04:25.120761  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.10 -> 192.168.0.201
02/06-08:04:26.119631  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.201 -> 192.168.0.10
02/06-08:04:26.120806  [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 192.168.0.10 -> 192.168.0.201
  
```







# SNORT TCP DUMP

- 11:16:35.648944 10.1.1.8.23 > 10.1.1.6.1033: P 16:34(18) ack 16 win 8760 (DF) (ttl 255, id 49913)
  - 4500 003a c2f9 4000 ff06 a2b4 0a01 0108
  - 0a01 0106 0017 0409 1cf9 e7f6 001a e050
  - 5018 2238 31c6 0000 fffe 1fff fe23 fffe
  - 27ff fe24 fffa
- 11:16:35.649457 10.1.1.6.1033 > 10.1.1.8.23: P 16:19(3) ack 34 win 8727 (DF) (ttl 128, id 57861)
  - 4500 002b e205 4000 8006 02b8 0a01 0106
  - 0a01 0108 0409 0017 001a e050 1cf9 e808
  - 5018 2217 6f19 0000 fffc 1f20 2020



# MODE PACKET LOGGER

- ❑ Menyimpan packets ke disk (harddisk, removeable disk).
- ❑ Pilihan packet logging.
- ❑ Flat ASCII (teks), tcpdump format, XML, database (MySQL, MsSQL, ORACLE, dsb).
- ❑ Melakukan logging semua data dan kemudian diproses untuk mendeteksi aktivitas yang dicurigai.

```

+++++-----+++++-----+++++-----+++++-----+++++-----+++++-----+++++-----+++++
02/02-12:04:45.469685 00:0C:29:7E:FE:03 -> 00:0F:15:04:37:25 type:0x800 len:0x180
192.168.1.200:1120 -> 194.231.106.7:80 TCP TTL:128 TOS:0x0 ID:20733 IpLen:20 DgnLen:370 DP
***ARP*** Seq: 0xBEE38EFE Pk: 0x3B863F04 Win: 0x7FB6 TcpLen: 20
47 45 54 20 2F 72 70 2D 63 6F 6E 74 65 6E 74 2F GET /wp-content/
75 70 6C 6F 61 64 73 2F 32 30 31 32 2F 30 35 2F uploads/2012/05/
74 61 73 6B 62 61 72 39 2E 70 6E 67 20 40 54 54 taskbar2.png HT
50 2F 31 2E 31 0D 0A 40 6F 73 74 3A 20 69 66 63 P/1.1..Host: ifc
6F 6E 66 69 67 2E 64 6D 0D 0A 55 73 65 72 2D 41 onfig.dk..User-A
67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E gent: Mozilla/5.
30 20 20 57 69 6E 64 6F 77 73 20 4E 54 20 35 2E 0 (Windows NT 5.
31 3D 20 72 76 3A 31 30 2E 30 2E 32 29 20 47 65 i; rv:10.0.2) Ge
63 6D 6F 2F 32 30 31 30 30 31 30 31 20 46 69 72 cko/20100101 Fir
65 66 6F 70 2F 31 30 2E 30 2E 32 0D 0A 41 63 63 efox/10.0.2..Acc
65 70 74 3A 20 69 6D 61 67 65 2F 70 6E 67 2C 67 ept: image/png,i
6D 61 67 65 2F 2A 3B 71 3D 30 2E 30 2C 2A 2F 2A mage/*;q=0.8.*/*
3B 71 3D 30 2E 35 0D 0A 41 63 63 65 70 74 2D 4C ;q=0.5..Accept-L
61 6E 67 75 61 67 65 3A 20 64 61 2C 65 6E 2D 75 anguage: da,en-u
73 3B 71 3D 30 2E 37 2C 65 6E 3B 71 3D 30 2E 33 s;q=0.7.en;q=0.3
0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E ..Accept-Encodin
67 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 g: gzip, deflate
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 ..Connection: ke
65 70 2D 61 6C 69 76 65 0D 0A 52 65 66 65 72 65 ep-alive..Refere
72 3A 20 68 74 74 70 3A 2F 2F 69 66 63 6F 6E 66 r: http://ifconf
69 67 2E 64 6B 2F 0D 0A 0D 0A
+++++-----+++++-----+++++-----+++++-----+++++-----+++++-----+++++
    
```

**Source MAC  
address**

**Destination MAC  
adress**

**Source IP and  
port**

**Destination IP and  
port**





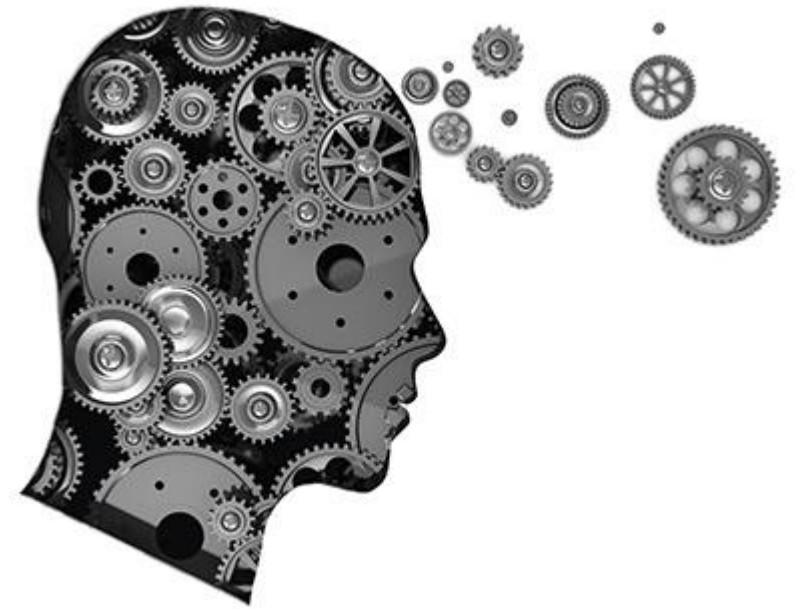
## MODE NIDS

- ❑ Menggunakan semua fase-kerja SNORT & plug-ins'nya untuk menganalisa traffic agar mendeteksi **penyalahgunaan** dan **anomalous** activities .
- ❑ Dapat melakukan **deteksi** portscanning, IP defragmentation, TCP stream reassembly, application layer analysis, normalisasi, dsb.

- ❑ Memiliki **rules** yang sangat banyak yang digunakan sebagai signature dari detection engine.
- ❑ Modus deteksi yang beragam :
  - ✓ Rules (signature)
  - ✓ Statistical anomaly
  - ✓ Protocol verification

## MATRIKS

- Portable (**Linux**, Windows, MacOS X, Solaris, BSD, IRIX, Tru64, HP-UX, etc)
- Cepat (probabilitas tinggi dari deteksi untuk serangan yang diberikan pada jaringan **100Mbps**)
- Mudah dikonfigurasi (**Rules**, Reporting/Logging)
- **Free** (GPL/Open Source Software)





## DESIGN



- Paket sniffing “lightweight” NIDS
- Libpcap-based sniffing interface
- Rules-based detection engine
- Plug-in system (memungkinkan fleksibilitas tak berujung)



# Third-Party

---

# WANNA TRY MORE?

## WE'LL MAKE A FRONTEND



1. Install Debian Wheezy on Virtual Box.
2. Make it Update
3. Configuring OS (Debian Wheezy)
4. Install Database
5. Configuring Database
6. Install IDS Engine
7. Configuring IDS Engine
8. Configuring Front-End (Snorby)
9. Running and Testing IDS.

# LOGIN PAGE

Snorby by  threat stack  
www.threatstack.com

Login

Email

**snorby@example.com**

Password

**snorby**

Welcome, Sign In

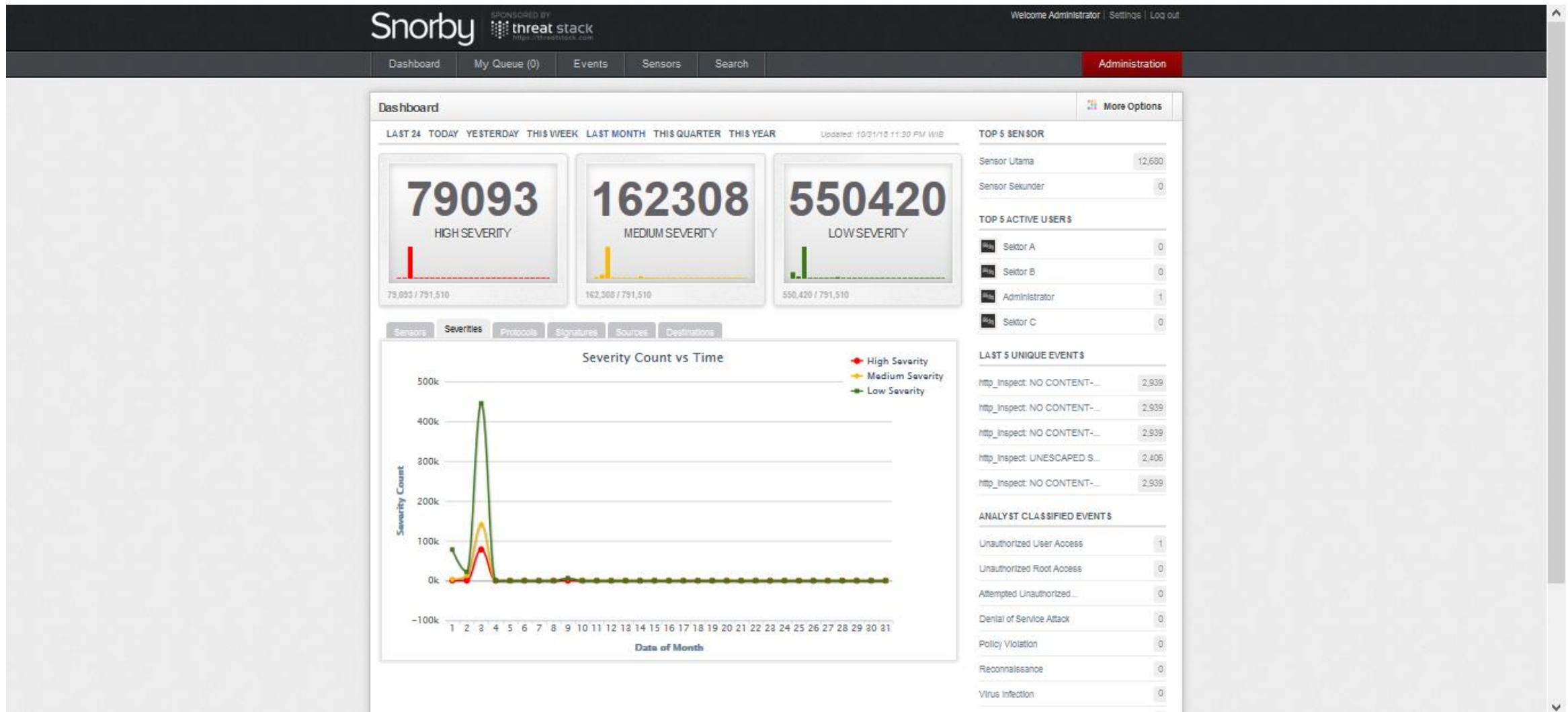
Forgot Password?

Remember me

© 2018 [Threat Stack, Inc](#) - Created By: Dustin Willis Webber

Snorby 2.6.3 - <https://github.com/Snorby/snorby>

# DASHBOARD



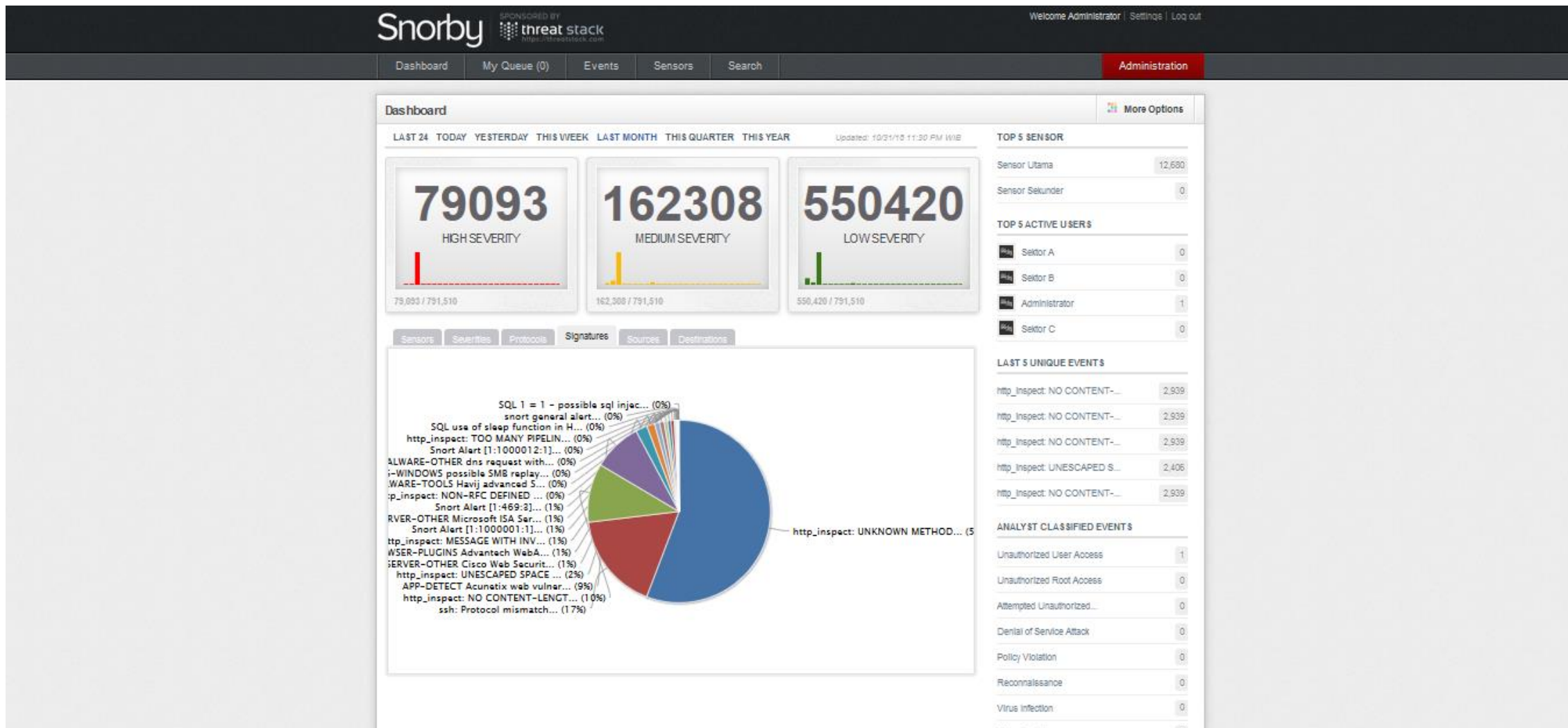
## CYBERSECURITY DRILL TEST SEKTOR PEMERINTAH

"Membangun Kesadaran Respon Insiden melalui Cybersecurity Drill Test"

*Intrusion Detection System (IDS)*



# DASHBOARD



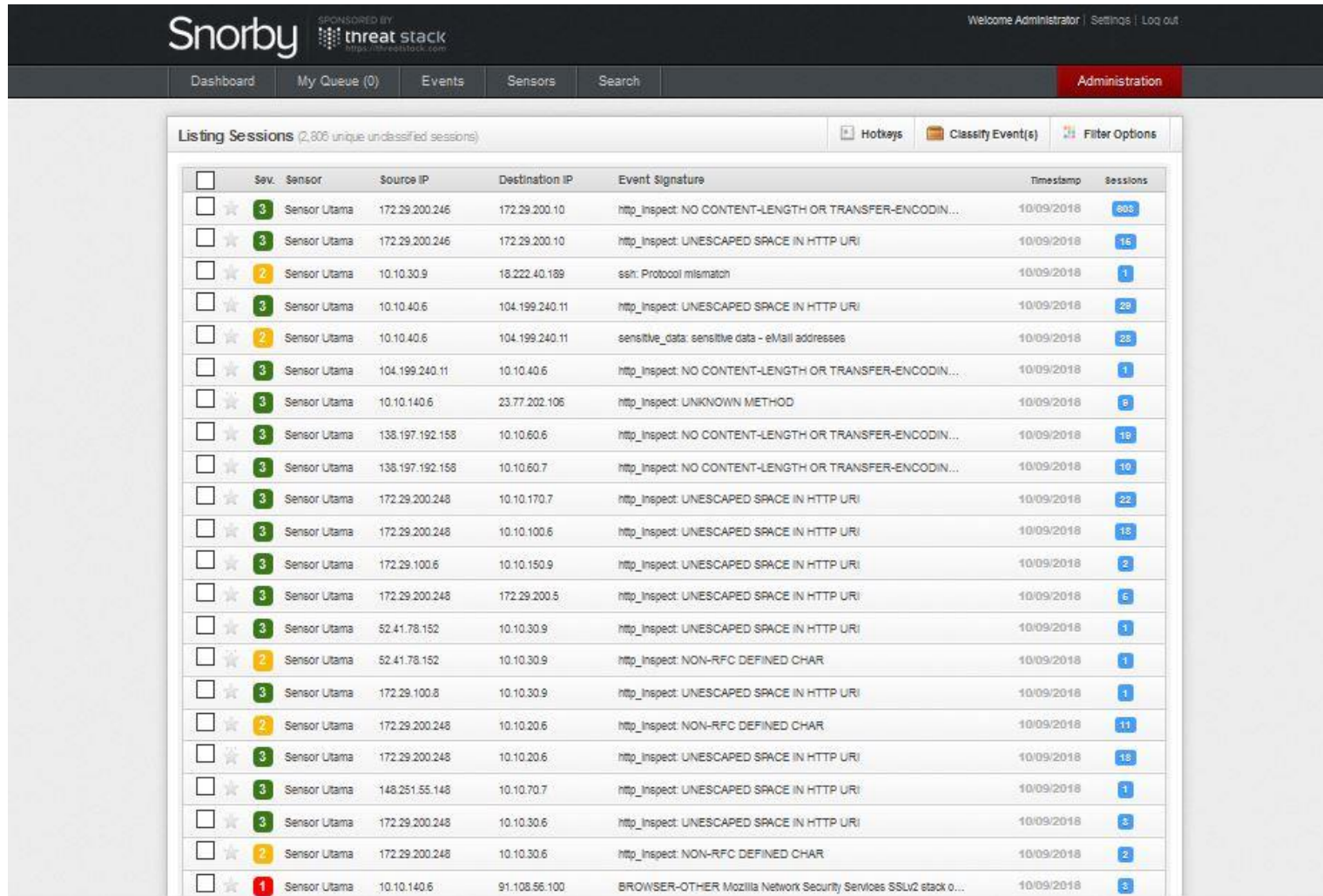
## CYBERSECURITY DRILL TEST SEKTOR PEMERINTAH

“Membangun Kesadaran Respon Insiden melalui Cybersecurity Drill Test”

*Intrusion Detection System (IDS)*



# EVENTS



Snorby SPONSORED BY threat stack  
Welcome Administrator | Settings | Log out

Dashboard My Queue (0) Events Sensors Search Administration

Listing Sessions (2,306 unique unclassified sessions) Hotkeys Classify Event(s) Filter Options

<input type="checkbox"/>	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
<input type="checkbox"/>	3	Sensor Utama	172.29.200.246	172.29.200.10	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN...	10/09/2018	803
<input type="checkbox"/>	3	Sensor Utama	172.29.200.246	172.29.200.10	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	16
<input type="checkbox"/>	2	Sensor Utama	10.10.30.9	18.222.40.189	ssh: Protocol mismatch	10/09/2018	1
<input type="checkbox"/>	3	Sensor Utama	10.10.40.6	104.199.240.11	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	29
<input type="checkbox"/>	2	Sensor Utama	10.10.40.6	104.199.240.11	sensitive_data: sensitive data - eMail addresses	10/09/2018	28
<input type="checkbox"/>	3	Sensor Utama	104.199.240.11	10.10.40.6	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN...	10/09/2018	1
<input type="checkbox"/>	3	Sensor Utama	10.10.140.6	23.77.202.106	http_inspect: UNKNOWN METHOD	10/09/2018	8
<input type="checkbox"/>	3	Sensor Utama	138.197.192.158	10.10.60.6	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN...	10/09/2018	18
<input type="checkbox"/>	3	Sensor Utama	138.197.192.158	10.10.60.7	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN...	10/09/2018	10
<input type="checkbox"/>	3	Sensor Utama	172.29.200.248	10.10.170.7	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	22
<input type="checkbox"/>	3	Sensor Utama	172.29.200.248	10.10.100.6	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	18
<input type="checkbox"/>	3	Sensor Utama	172.29.100.6	10.10.150.9	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	2
<input type="checkbox"/>	3	Sensor Utama	172.29.200.248	172.29.200.5	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	6
<input type="checkbox"/>	3	Sensor Utama	52.41.78.152	10.10.30.9	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	1
<input type="checkbox"/>	2	Sensor Utama	52.41.78.152	10.10.30.9	http_inspect: NON-RFC DEFINED CHAR	10/09/2018	1
<input type="checkbox"/>	3	Sensor Utama	172.29.100.8	10.10.30.9	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	1
<input type="checkbox"/>	2	Sensor Utama	172.29.200.248	10.10.20.6	http_inspect: NON-RFC DEFINED CHAR	10/09/2018	11
<input type="checkbox"/>	3	Sensor Utama	172.29.200.248	10.10.20.6	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	18
<input type="checkbox"/>	3	Sensor Utama	148.251.55.148	10.10.70.7	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	1
<input type="checkbox"/>	3	Sensor Utama	172.29.200.248	10.10.30.6	http_inspect: UNESCAPED SPACE IN HTTP URI	10/09/2018	3
<input type="checkbox"/>	2	Sensor Utama	172.29.200.248	10.10.30.6	http_inspect: NON-RFC DEFINED CHAR	10/09/2018	2
<input type="checkbox"/>	1	Sensor Utama	10.10.140.6	91.108.56.100	BROWSER-OTHER Mozilla Network Security Services SSLv2 stack o...	10/09/2018	3

## EVENTS

sensor01
182.253.201.28 203.34.119.69
APP-DETECT Acunetix web vulnerability scan attempt
4:08 PM

### IP Header Information

Perform Mass Classification
Event Export Options
Permalink

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
182.253.201.28	203.34.119.69	4	5	0	378	21179	0	0	63	6	9537

### Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (2/791656)	Category	Sig Info
1	25358	4	0.00%	web-application-attack	<span>Query Signature Database</span> <span>View Rule</span>

### TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
48001	80	2729770422	4166143875	8	0	24	730	33938	0

### References

Type	Value
url	www.acunetix.com

### Payload

Hex
Ascii

```

0000000: 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 75 6e 65 74 69 78 2d 41 GET /.HTTP/1.1..Acunetix-A
000001A: 73 70 65 63 74 3a 20 65 6e 61 62 6c 65 64 0d 0a 41 63 75 6e 65 74 69 78 2d 41 spect:.enabled..Acunetix-A
0000034: 73 70 65 63 74 2d 50 61 73 73 77 6f 72 64 3a 20 30 38 32 31 31 39 66 37 35 36 spect-Password:.082119f756
000004E: 32 33 65 62 37 61 62 64 37 62 66 33 35 37 36 39 38 66 66 36 36 63 0d 0a 48 6f 23eb7abd7bf357698ff66c..No
0000068: 73 74 3a 20 69 74 66 2e 6a 61 77 61 72 61 2e 69 64 73 69 72 74 69 69 2e 6f 72 st:.ctf.jawara.idsirtii.or
0000082: 2e 69 64 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 61 6c 69 76 .id..Connection:.Keep-aliv
000009C: 65 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 e..Accept-Encoding:.gzip,d
00000B6: 65 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c eflate..User-Agent:.Mosill
00000D0: 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 a/5.0.(Windows.NT.6.1;.WOW
00000EA: 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 32 31 20 28 4b 48 64).AppleWebKit/537.21.(KH
0000104: 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 34 31 TML,.like.Gecko).Chrome/41
000011E: 2e 30 2e 32 32 32 38 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e 32 31 0d 0a 41 .0.2228.0.Safari/537.21..A
0000138: 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a accept:.*/*....

```

### Notes

This event currently has zero notes - You can add a note by clicking the button below.

Add A Note To This Event

# EVENTS

High Severity Events 24 events found

Hotkeys Classify Event(s) More Options

<input type="checkbox"/>	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	POLICY-OTHER Adobe ColdFusion admin interface access attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	POLICY-OTHER Adobe ColdFusion admin interface access attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable Injection attempt	4:10 PM
<input type="checkbox"/>	★ 1	sensor01	172.16.6.251	172.16.1.14	APP-DETECT Acunetix web vulnerability scan attempt	4:08 PM
<input type="checkbox"/>	★ 1	sensor01	182.253.201.28	203.34.119.69	APP-DETECT Acunetix web vulnerability scan attempt	4:08 PM



## SEARCH



Snorby SPONSORED BY threat stack

Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard

My Queue (0)

Events

Sensors

Search

Administration

Snorby Advanced Search

More Options

Match **All** of the following rules:

Destination Address  is

Choose a query term...

Choose a query term...

Submit Search

Snorby SPONSORED BY threat stack

Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard

My Queue (0)

Events

Sensors

Search

Administration

Search Results 738 events found

Hotkeys

Classify Event(s)

More Options

<input type="checkbox"/>	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018
<input type="checkbox"/>	2	Sensor Utama	10.10.60.7	202.43.92.132	ssh: Protocol mismatch	10/09/2018

## CYBERSECURITY DRILL TEST SEKTOR PEMERINTAH

“Membangun Kesadaran Respon Insiden melalui Cybersecurity Drill Test”

*Intrusion Detection System (IDS)*



# Administration – General Setting

Welcome Administrator | [Settings](#) | [Log out](#)

Administration
[Dashboard](#)
[My Queue \(0\)](#)
[Events](#)
[Sensors](#)
[Search](#)

### General Settings

Company name

Company email (this email will be used as the report sender)

Signature lookup url (user \$\$sid\$\$ and \$\$qid\$\$ for the get request parameters)

Enable snorby update notifications  
(DEPRECATED Notification reminder when a new Snorby build is released)

Enable packet capture support  
(Enable the Snorby Packet Capture Plugin)

Daily reports  
(Send a report summarizing the captured traffic daily.)

Weekly reports  
(Send a report summarizing the captured traffic weekly.)

Monthly reports  
(Send a report summarizing the captured traffic monthly.)

Address lookups  
(This option enables the analyst to perform basic queries on source & destination addresses using external sources.)

Enable global event notifications  
(Show new event notifications globally. Event count since last check time.)

Geop  
(Display GeoIP information on the events list)

Prune database when event count is greater than   
(Prune the database automatically when the event count exceeds your specified limit.)

Save Settings
Cancel

Snorby 2.6.3 - <https://github.com/Snorby/snorby> © 2018 [Threat Stack, Inc](#) - Created By: Dustin Willis Webber



# Administration – Listing Sensor

Snorby SPONSORED BY **threat stack** https://threatstack.com Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard My Queue (0) Events Sensors Search **Administration**

### Listing Sensors

ID	Name	Hostname	Interface	Last Event	Event Count	Event %		
1	Sensor Sekunder	sensor:NULL	NULL	N/A	0	0.00%	<a href="#">View Events</a>	
2	Sensor Utama	sensor01	NULL	10/09/2018 5:00 PM	12,680	100.00%	<a href="#">View Events</a>	

Snorby 2.6.3 - <https://github.com/Snorby/snorby> © 2018 [Threat Stack, Inc](#) - Created By: Dustin Willis Webber



# Administration – Saverity Setting

Snorby SPONSORED BY  
 threat stack  
<https://threatstack.com>

Welcome Administrator [Settings](#) | [Log out](#)

Dashboard

My Queue (0)

Events

Sensors

Search

Administration

## Severity Settings

[+ Add Severity](#)

ID	Name	Background	Text	Signature Count	Event Count	Example	Edit	Destroy
1	High Severity	#ff0000	#ffffff	27,712	61	1	<input type="button" value="Edit"/>	<input type="button" value="Destroy"/>
2	Medium Severity	#fab908	#ffffff	4,008	6,341	2	<input type="button" value="Edit"/>	<input type="button" value="Destroy"/>
3	Low Severity	#3a781a	#ffffff	3,223	6,266	3	<input type="button" value="Edit"/>	<input type="button" value="Destroy"/>

Snorby 2.6.3 - <https://github.com/Snorby/snorby> © 2018 [Threat Stack, Inc](#) - Created By: Dustin Willis Webber





# Administration – Listing Signature

Snorby

SPONSORED BY  
 threat stack  
<https://threatstack.com>

Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard

My Queue (0)

Events

Sensors

Search

Administration

## Listing Signatures

Sev.	Signature Name	Event Count	
2	Snort Alert [1:469:3]	33.84%	<a href="#">View</a>
3	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	23.18%	<a href="#">View</a>
3	http_inspect: UNESCAPED SPACE IN HTTP URI	18.97%	<a href="#">View</a>
2	ssh: Protocol mismatch	7.75%	<a href="#">View</a>
3	http_inspect: TOO MANY PIPELINED REQUESTS	4.58%	<a href="#">View</a>
2	MALWARE-OTHER dns request with long host name segment - possible data exfiltration attempt	4.56%	<a href="#">View</a>
3	http_inspect: UNKNOWN METHOD	2.56%	<a href="#">View</a>
2	http_inspect: NON-RFC DEFINED CHAR	2.09%	<a href="#">View</a>
2	sensitive_data: sensitive data - eMail addresses	1.29%	<a href="#">View</a>
1	BROWSER-OTHER Mozilla Network Security Services SSLv2 stack overflow attempt	0.48%	<a href="#">View</a>
2	http_inspect: OVERSIZE REQUEST-URI DIRECTORY	0.29%	<a href="#">View</a>
3	http_inspect: SIMPLE REQUEST	0.10%	<a href="#">View</a>
2	SERVER-OTHER Cisco IOS XE IGMP denial of service attempt	0.08%	<a href="#">View</a>
2	sensitive_data: sensitive data - Credit card numbers	0.06%	<a href="#">View</a>





# Administration – Listing Signature

Snorby SPONSORED BY threat stack https://threatstack.com Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard My Queue (0) Events Sensors Search **Administration**

### Listing Signatures

Filter Signatures

Sev.	Signature Name	Event Count	
1	SERVER-WEBAPP Dell SonicWALL Global Management System SQL injection attempt	0.00%	<a href="#">View</a>
1	SERVER-WEBAPP Symantec Endpoint Protection Manager SQL injection attempt	0.00%	<a href="#">View</a>
1	SERVER-WEBAPP Symantec Endpoint Protection Manager SQL injection attempt	0.00%	<a href="#">View</a>
1	FILE-IMAGE Adobe Acrobat Pro malformed TIF heap overflow attempt	0.00%	<a href="#">View</a>
1	FILE-IMAGE Adobe Acrobat Pro malformed TIF heap overflow attempt	0.00%	<a href="#">View</a>
1	FILE-IMAGE Adobe Acrobat Pro malformed TIF heap overflow attempt	0.00%	<a href="#">View</a>
1	FILE-IMAGE Adobe Acrobat Pro malformed TIF heap overflow attempt	0.00%	<a href="#">View</a>
1	SERVER-WEBAPP Unitrends Enterprise Backup Appliance download-files command injection attempt	0.00%	<a href="#">View</a>
1	SERVER-WEBAPP Borland AccuRev Reprise License Server directory traversal attempt	0.00%	<a href="#">View</a>
1	MALWARE-CNC DNS suspicious .bit tcp dns query	0.00%	<a href="#">View</a>
1	SERVER-WEBAPP Crypttech CryptoLog logshares_ajax.php command injection attempt	0.00%	<a href="#">View</a>
1	SERVER-WEBAPP Crypttech CryptoLog login.php SQL injection attempt	0.00%	<a href="#">View</a>
1	MALWARE-CNC User-Agent known malicious user-agent string - Win.Backdoor.Chopper	0.00%	<a href="#">View</a>
1	MALWARE-CNC Win.Backdoor.Chopper web shell connection	0.00%	<a href="#">View</a>
1	MALWARE-CNC Win.Backdoor.Chopper web shell connection	0.00%	<a href="#">View</a>
1	MALWARE-CNC Win.Backdoor.Chopper web shell connection	0.00%	<a href="#">View</a>











# Administration – User Management

Snorby SPONSORED BY threat stack <https://threatstack.com> Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard My Queue (0) Events Sensors Search Administration

## User Management ➕ Add User

Enabled	Admin.	Name	E-mail	Login Count	Last Login IP	Last Login Time	Destroy
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 Administrator	snorby@example.com	22	172.16.6.121	10/31/2018 3:44 PM	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	 Sektor A	sektorA@mail.id	17	10.20.40.197	10/03/2018 6:11 AM	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	 Sektor B	sektorB@mail.id	12	10.20.40.164	10/03/2018 6:43 AM	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	 Sektor C	sektorC@mail.id	18	10.20.40.162	10/03/2018 6:51 AM	

Snorby 2.6.3 - <https://github.com/Snorby/snorby> © 2018 [Threat Stack, Inc](#) - Created By: Dustin Willis Webber

# User – General Setting



Snorby

SPONSORED BY  
 threat stack  
<https://threatstack.com>

Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard

My Queue (0)

Events

Sensors

Search

Administration

## User Settings

Name (please use first and last name)

Administrator

Email (example: snorby@example.com)

snorby@example.com

Password (leave blank if you don't want to change it)

Password

Password confirmation

Password Confirmation

Current password (we need your current password to confirm your changes)

Current Password

Note notifications: Yes

(Would you like to receive notifications when new notes are added?)

I would like to list 45 items per page

(select the default amount of events to list per page view)



Login Count: 21

Current Login IP: 172.16.6.121

Last Login: Thu Sep, 2018 11:11 AM WIB

Last Login IP: 172.16.6.115

Queued Event Count: 0

Notes Count: 0

(To change/add a avatar please visit <http://gravatar.com>)

Time zone: (GMT+07:00) Jakarta



Event summary report:

(Would you like to receive an event summary report every 30 minutes)



Administrator (should this user have administrative rights?)

Update Settings

Cancel

# Administration – Worker & Job Queue



SPONSORED BY

threat stack  
<https://threatstack.com>

Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard
My Queue (0)
Events
Sensors
Search

Administration

## Worker & Job Queue

↻ Restart Worker

Status	user	pid	created_at	runtime	command	cpu	memory
OK	root	2612	22:58:25	09:37:56	delayed_job	0.1%	2.6%

ID	Pri.	Attempts	Run At	failed_at	Last Error	Handler
3879	1	0	4 minutes	N/A	N/A	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">--- !ruby/struct:Snorby::Jo...</div> <span style="float: right; font-size: 0.8em;">🗑</span>

Snorby 2.6.3 - <https://github.com/Snorby/snorby> © 2018 [Threat Stack, Inc](#) - Created By: Dustin Willis Webber



# Kesimpulan

---

- ✓ Snort “**Detektor tool**” yang ampuh, tetapi memaksimalkan kegunaannya membutuhkan operator yang terlatih.
- ✓ **Menjadi mahir** dengan deteksi intrusi jaringan membutuhkan waktu 12 bulan; "Pakar"?
- ✓ Snort dianggap sebagai **NIDS** sangat **baik** bila dibandingkan dengan kebanyakan sistem komersial.
- ✓ Penyedia keamanan jaringan yang dikelola harus mengumpulkan informasi yang cukup untuk membuat **keputusan** tanpa menelepon klien untuk bertanya apa yang terjadi.

# Terima kasih

---



NB: Tidak ada babi yang tersakiti dalam pembuatan slide ini 😊