SELAMAT DATANG

DEPUTI PENANGGULANGAN DAN PEMULIHAN
BADAN SIBER DAN SANDI NEGARA

Intrusion Detection System (IDS)

Nidaul Muiz Aufa

: aufa@idsirtii.or.id

nidaul.muiz@bssn.go.id

: @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

"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 ≠ 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.

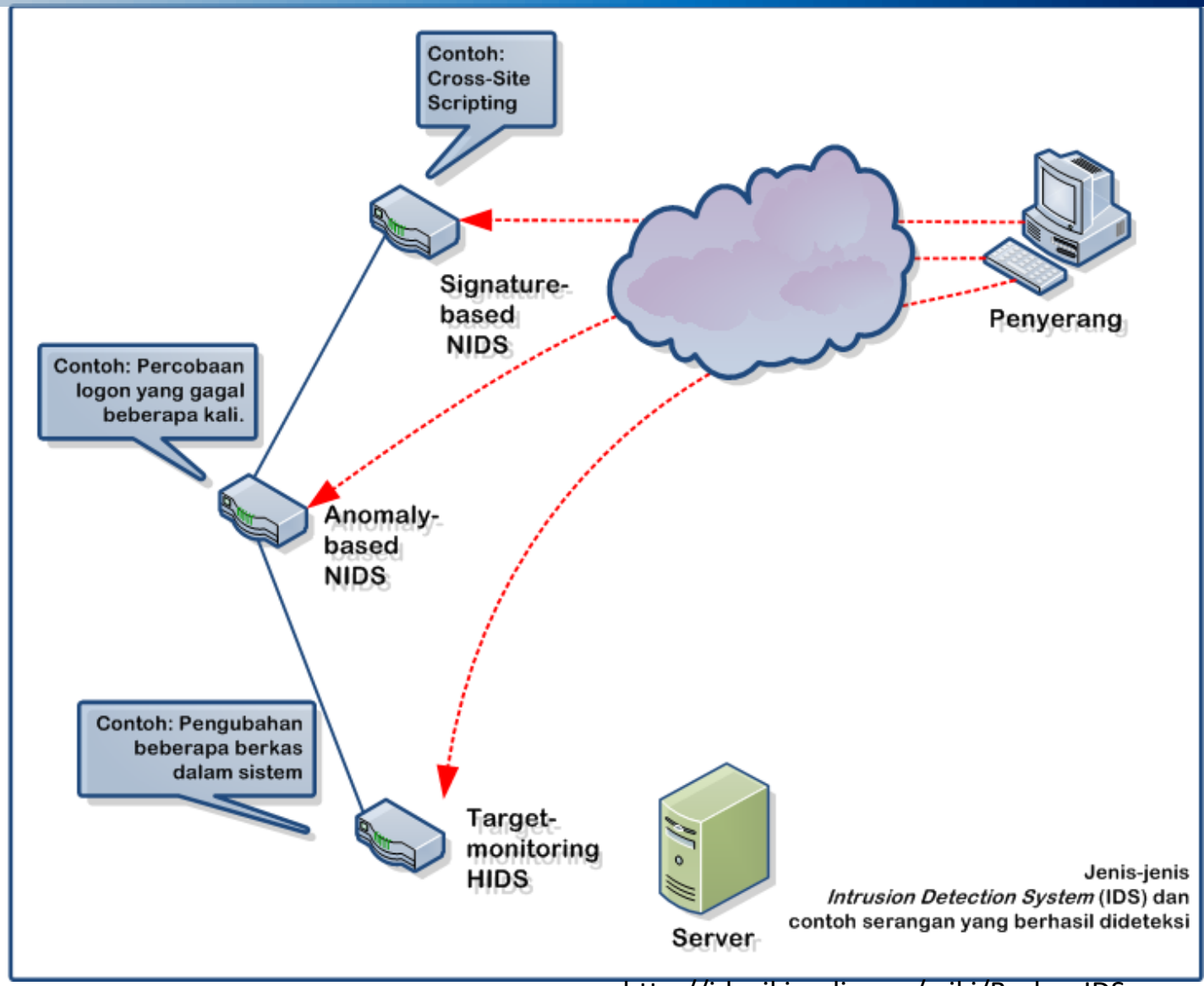
Kesuksesan Intrusion Detection tidak hanya tergantung kepada **teknologi**, namun juga kepada **policy** dan **management**. **(1)** Security policy, mendefinisikan apa yang boleh atau tidak boleh dilakukan. **(2)** Notifikasi, Bagaimana memberi peringatan. **(3)** Koordinasi dalam memberikan respon

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*

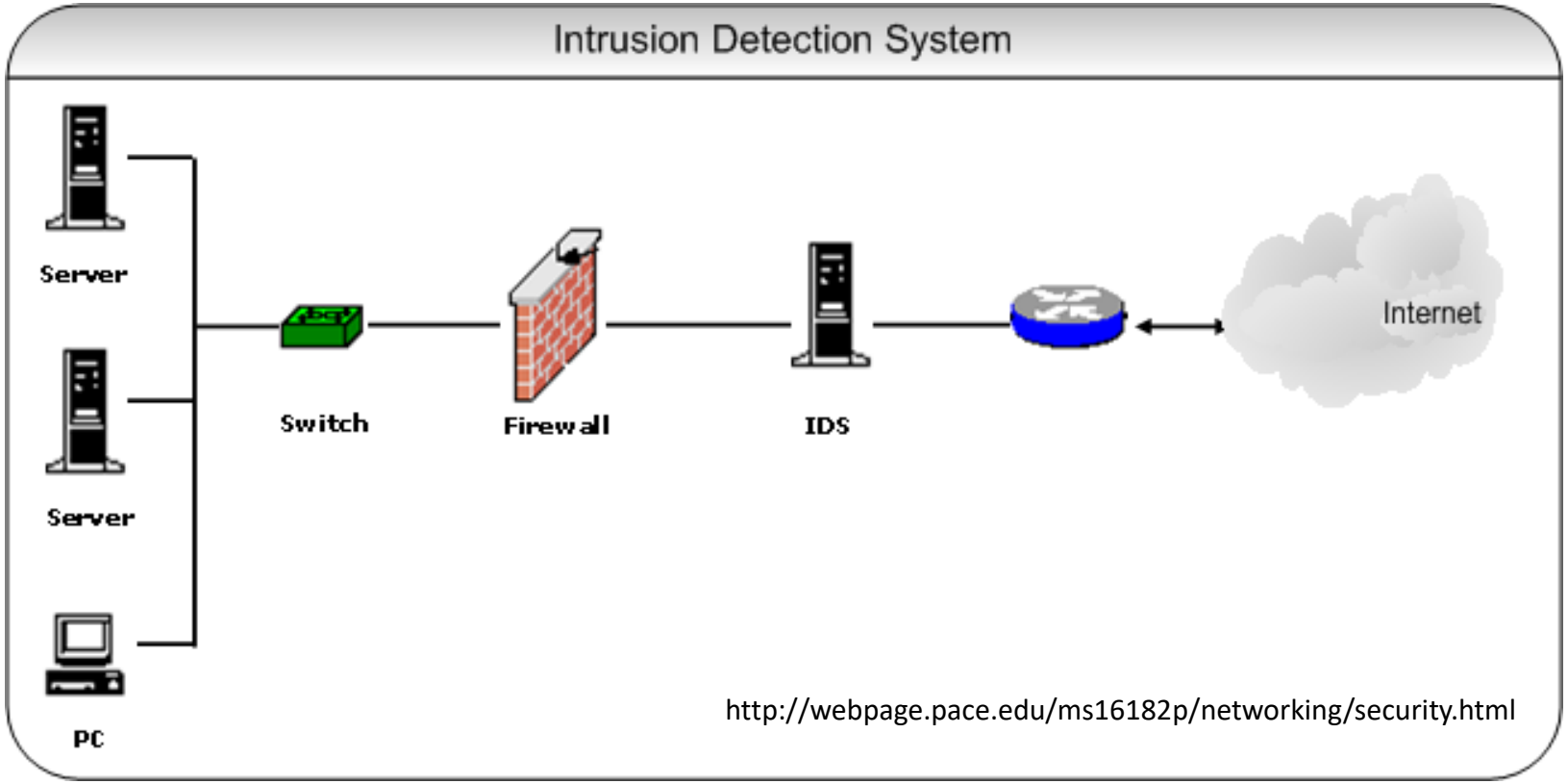
PassiveIDS : melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.



Jenis-jenis *Intrusion Detection System* (IDS) dan contoh serangan yang berhasil dideteksi

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

Topologi IDS



http://webpage.pace.edu/ms16182p/networking/security.html

Kelebihan IDS

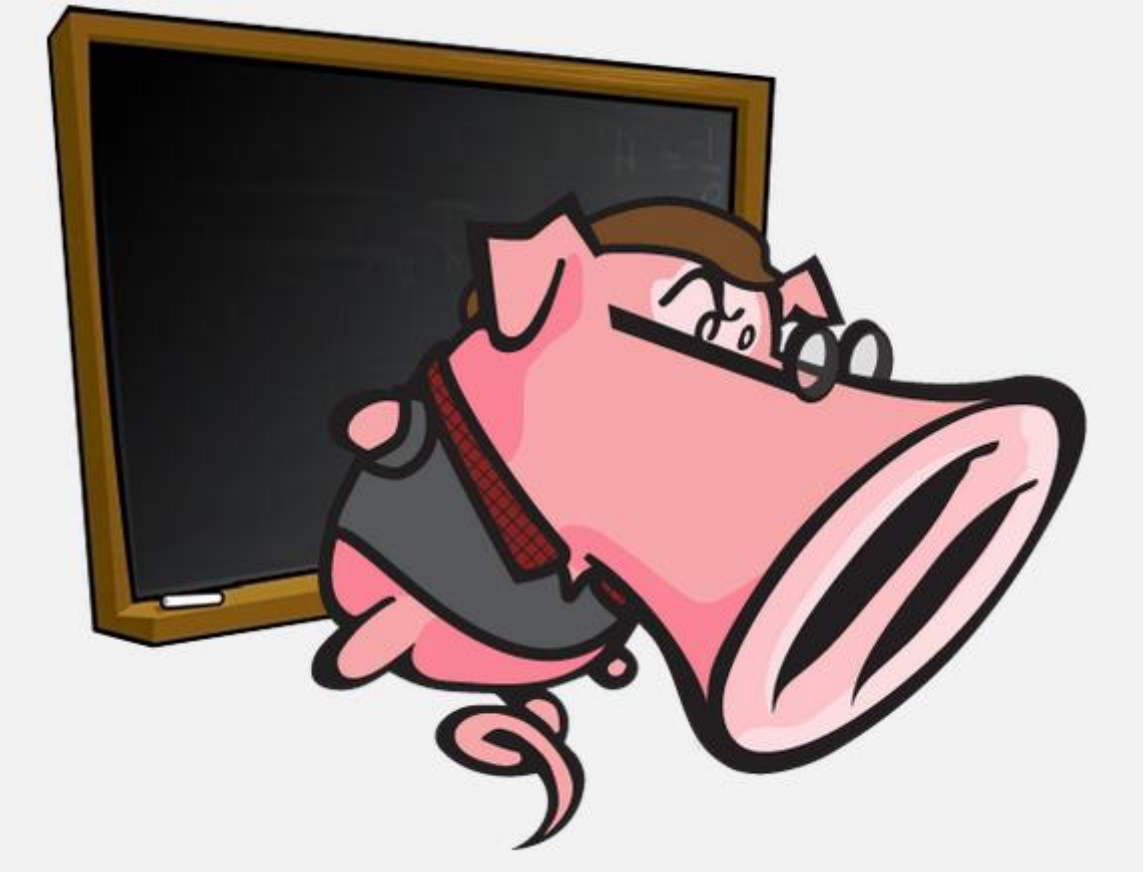
1. Dapat disesuaikan dengan mudah dalam menyediakan perlindungan untuk keseluruhan jaringan.
2. Dapat dikelola secara terpusat dalam menangani serangan yang tersebar dan bersama-sama.
3. Menyediakan pertahanan pada bagian dalam.
4. Menyediakan layer tambahan untuk perlindungan.
5. IDS memonitor Internet 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

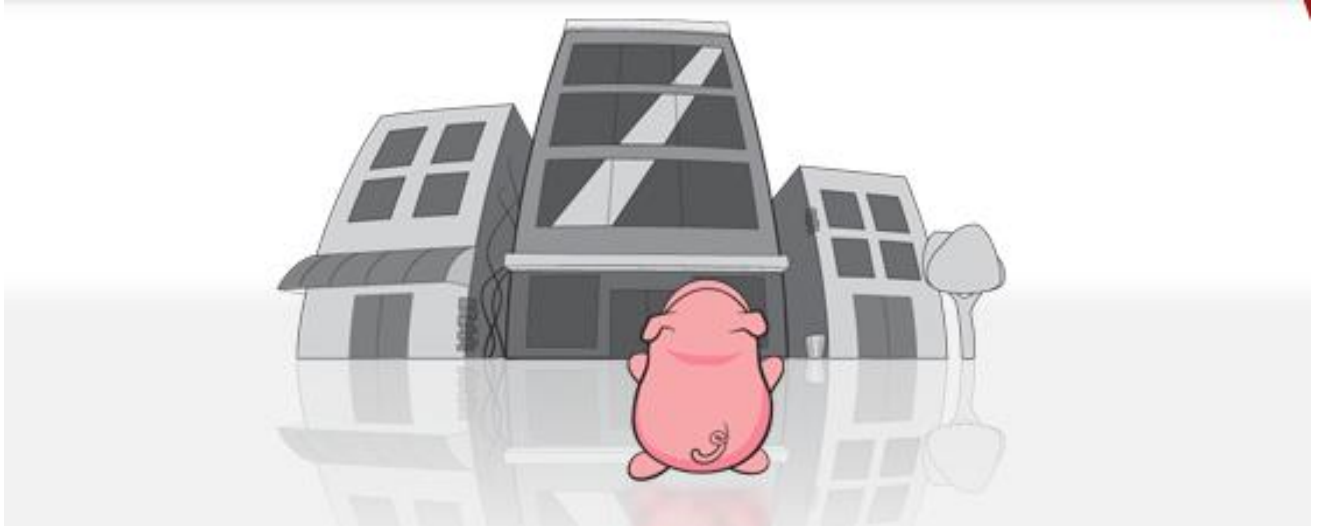
Kekurangan IDS

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 mengakusisi 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*

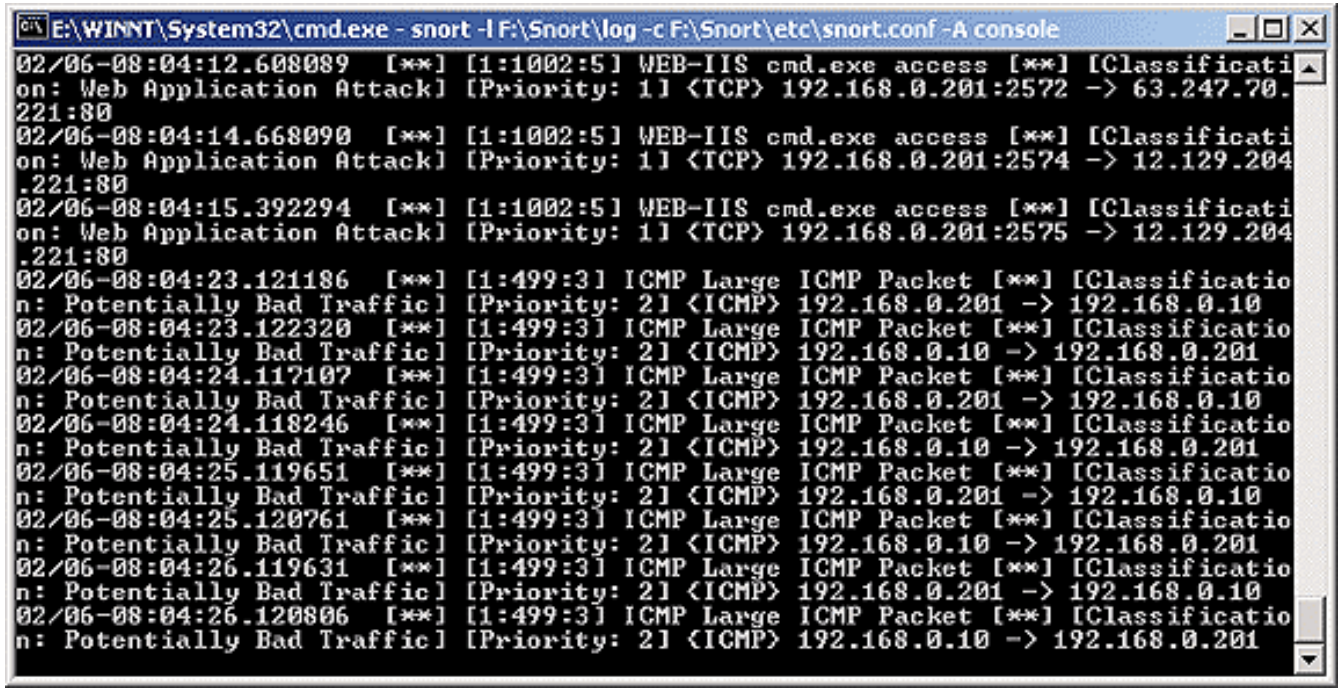
Snort adalah salah satu NIDS (Network-based IDS) yang bekerja dengan cara menganalisa paket data yang dianggap serangan yang melintas melewati suatu network.

MODE :

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

MODE SNIFFER

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



SNORT PACKET DUMP

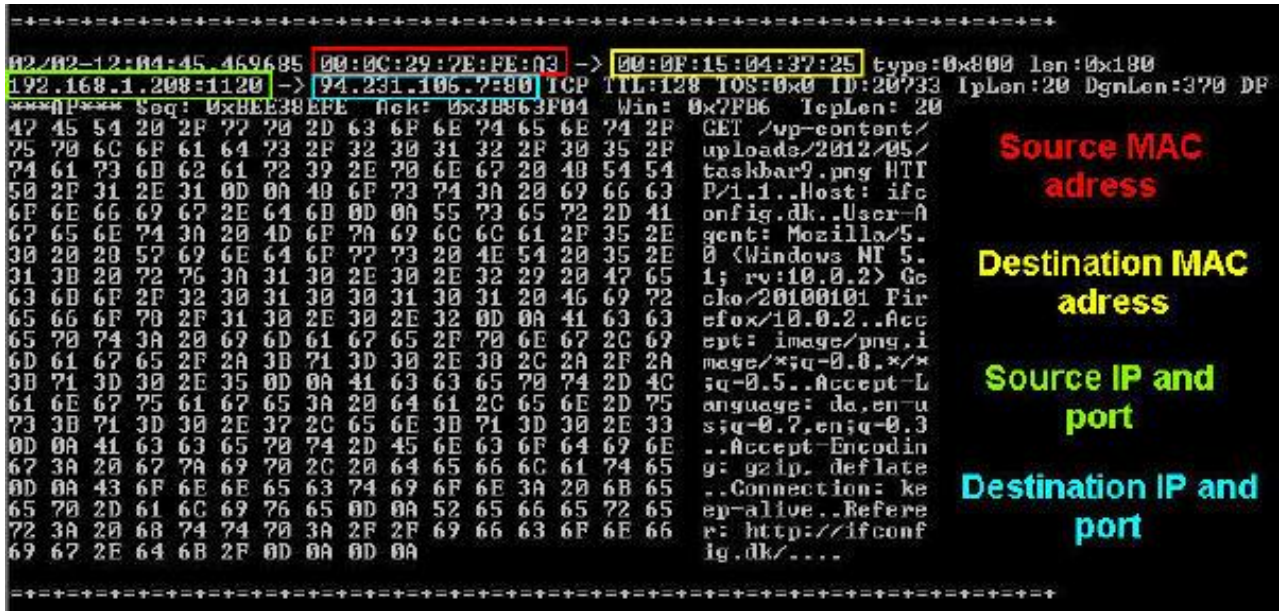
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/09-11:12:02.954779 10.1.1.6:1032 -> 10.1.1.8:23
TCP TTL:128 TOS:0x0 ID:31237 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x16B6DA  Ack: 0x1AF156C2  Win: 0x2217  TcpLen: 20
FF FC 23 FF FC 27 FF FC 24 FF FA 18 00 41 4E 53  ..#..'..$....ANS
49 FF F0                                         I..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/09-11:12:02.956582 10.1.1.8:23 -> 10.1.1.6:1032
TCP TTL:255 TOS:0x0 ID:49900 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1AF156C2  Ack: 0x16B6ED  Win: 0x2238  TcpLen: 20
0D 0A 0D 0A 53 75 6E 4F 53 20 35 2E 37 0D 0A 0D  ....SunOS 5.7...
00 0D 0A 0D 00                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

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.

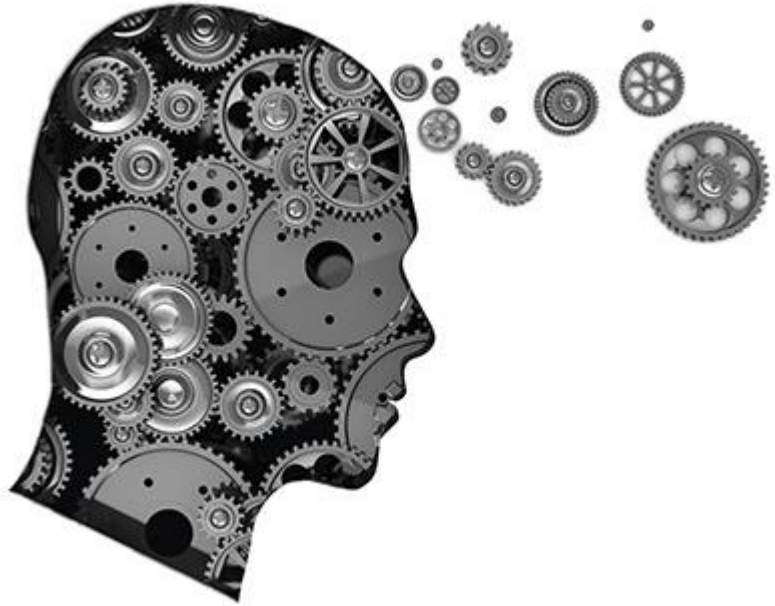


MODE NIDS

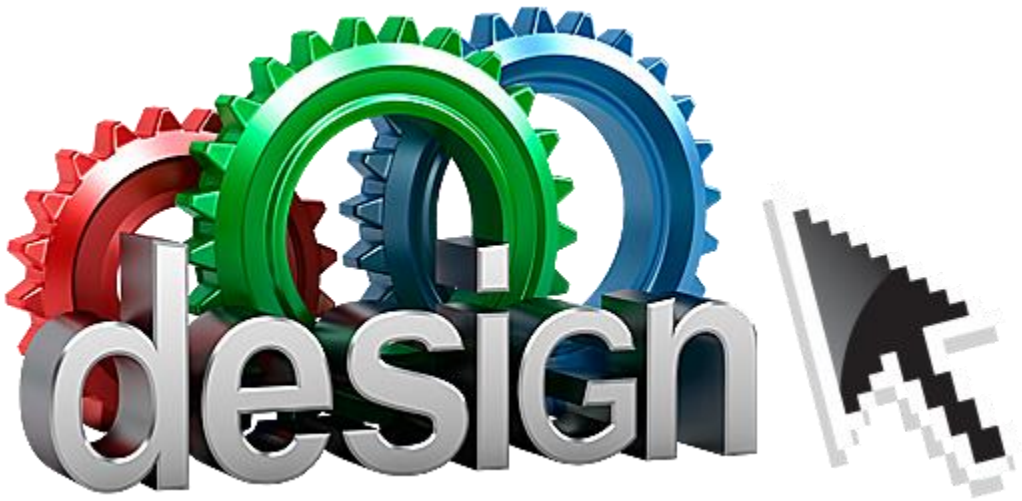
- Menggunakan semua fase-kerja SNORT & plug-ins'nya untuk menganalisa traffic agar mendeteksi **penyalahgunaan** dan **anomalous** activities .
- Dapat melakukan **deteksi** portscanning, IP defragmentation, TCP stream reassembly, application layer analysis, normalisasi, dsb.
- Memiliki **rules** yang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



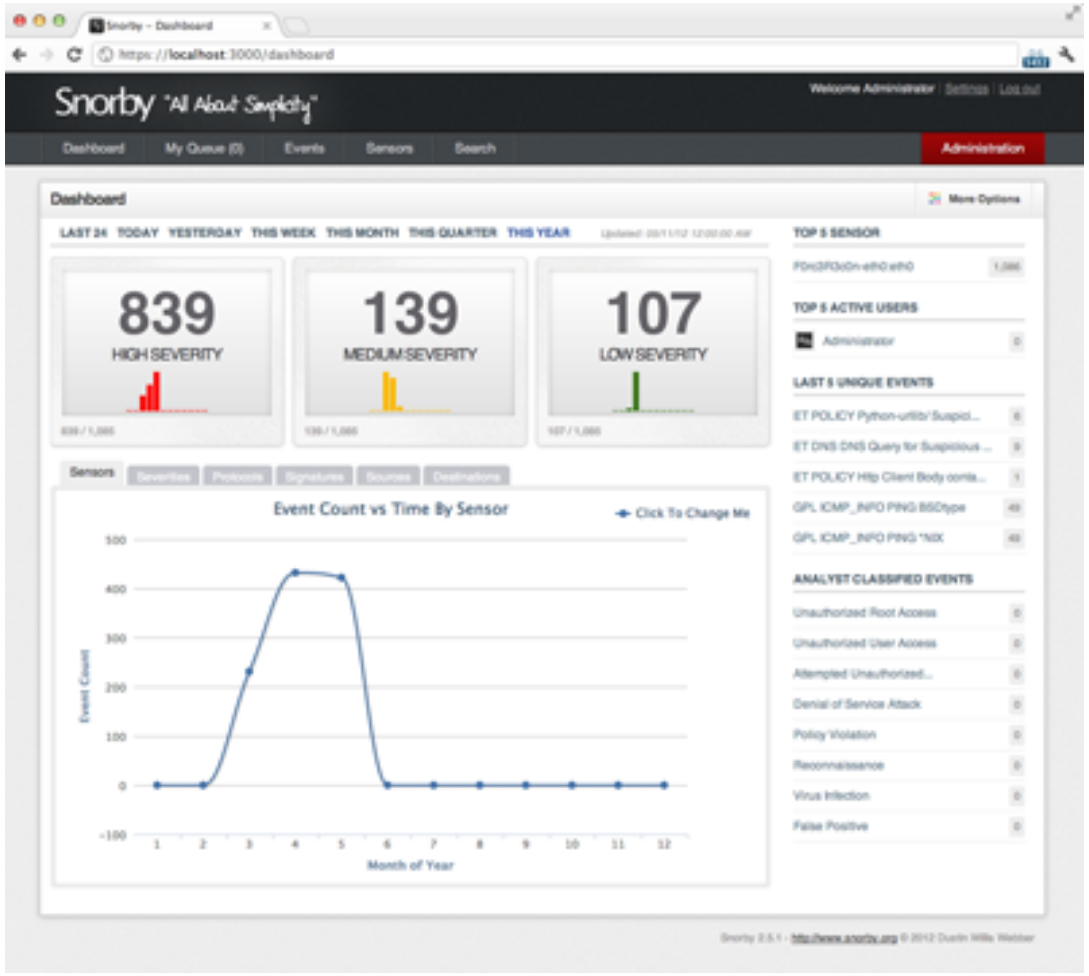
DESIGN



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

Third-Party

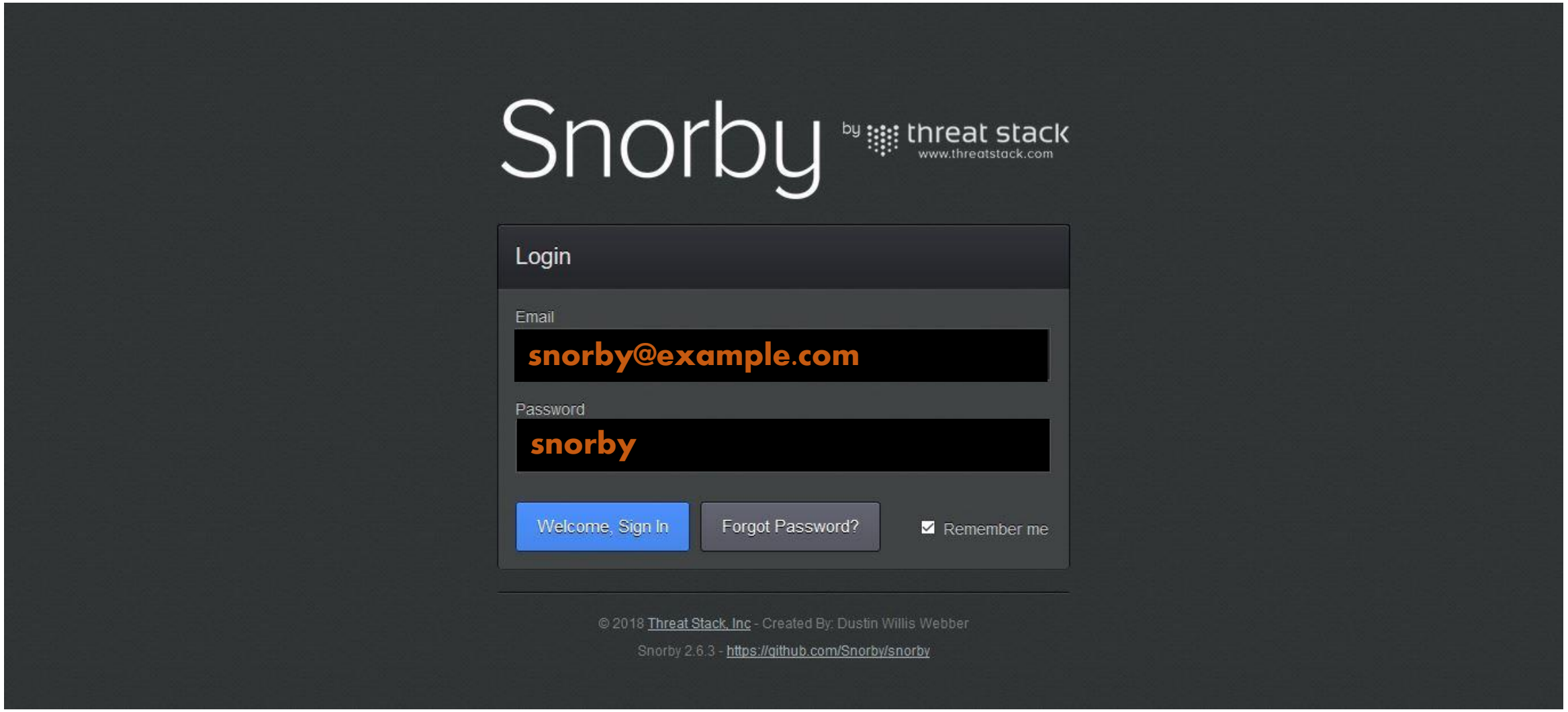
WANNA TRY MORE?



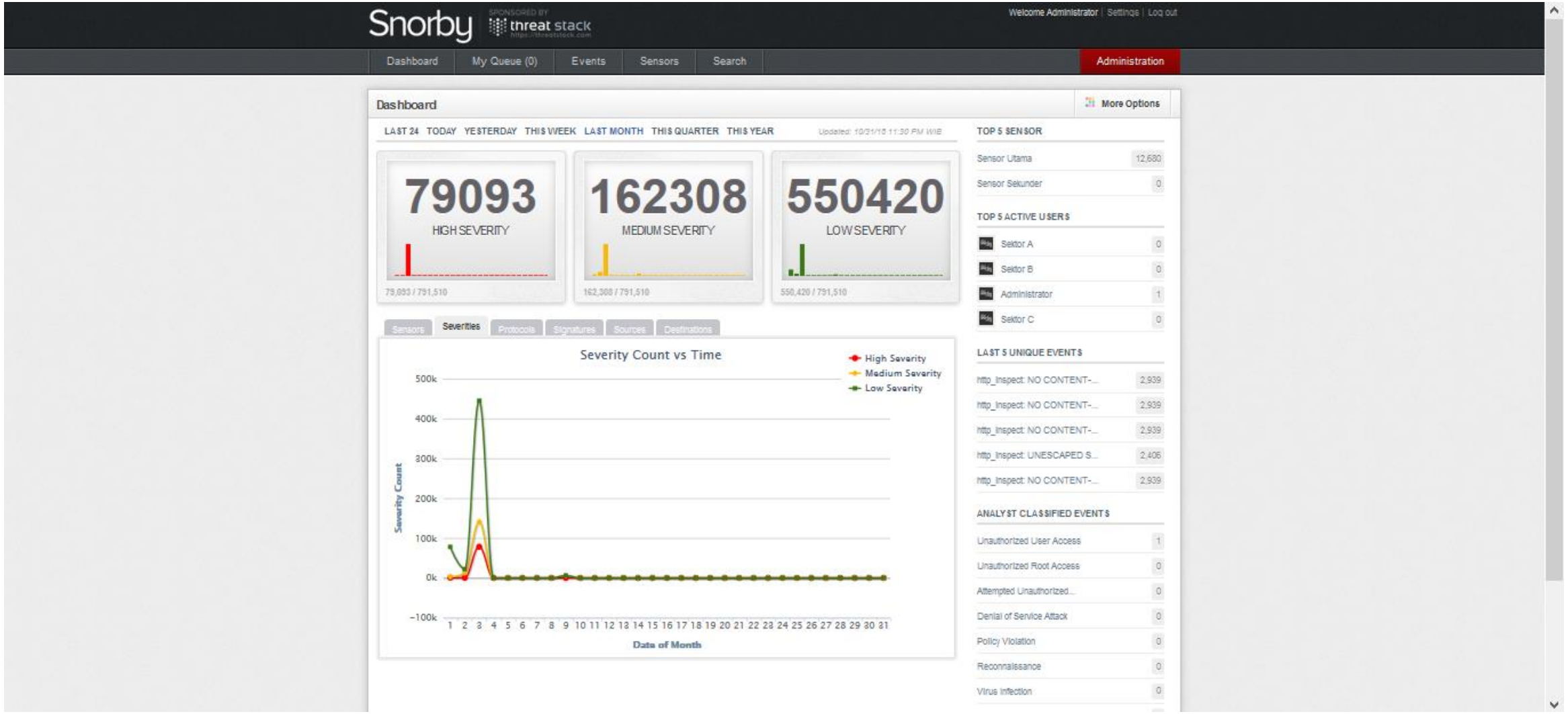
WE'LL MAKE A FRONTEND

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.

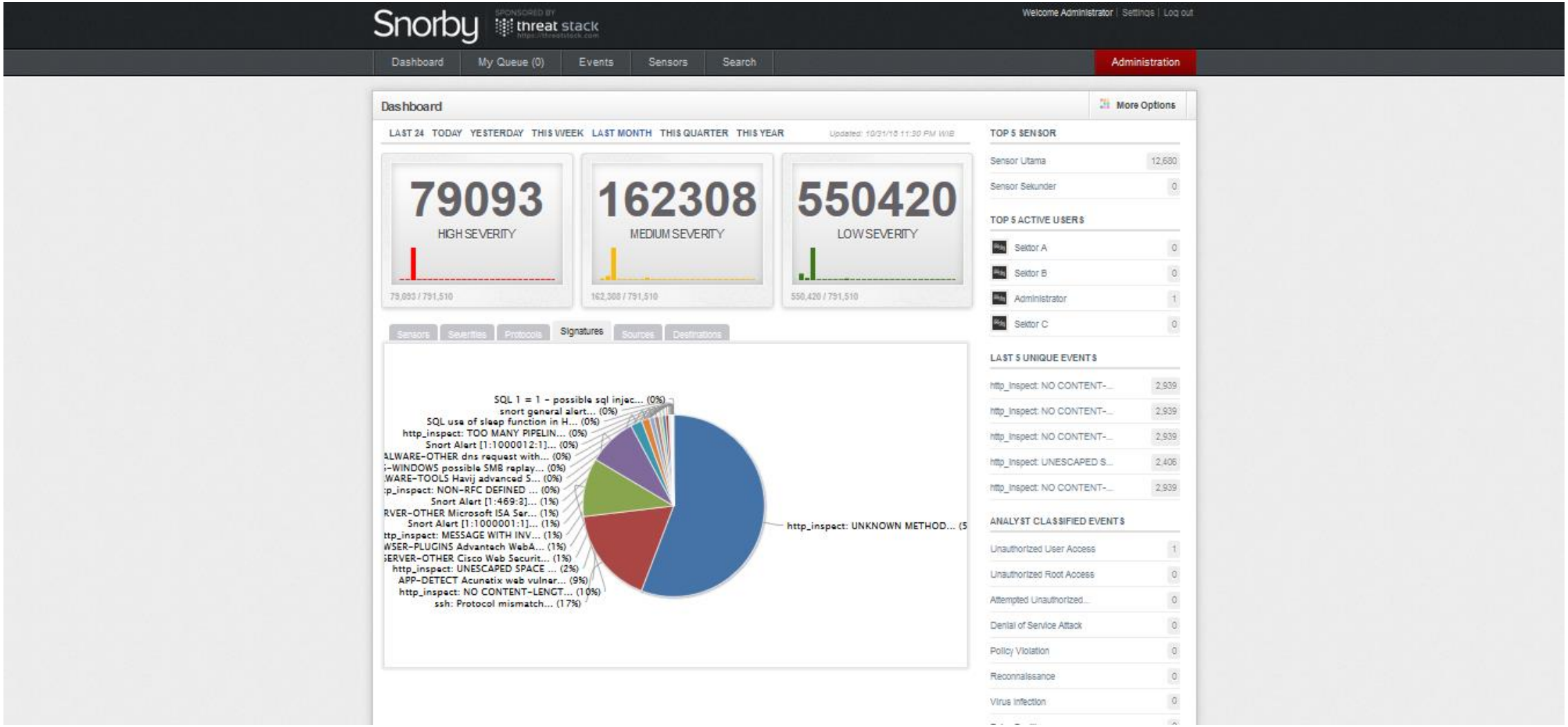
LOGIN PAGE


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

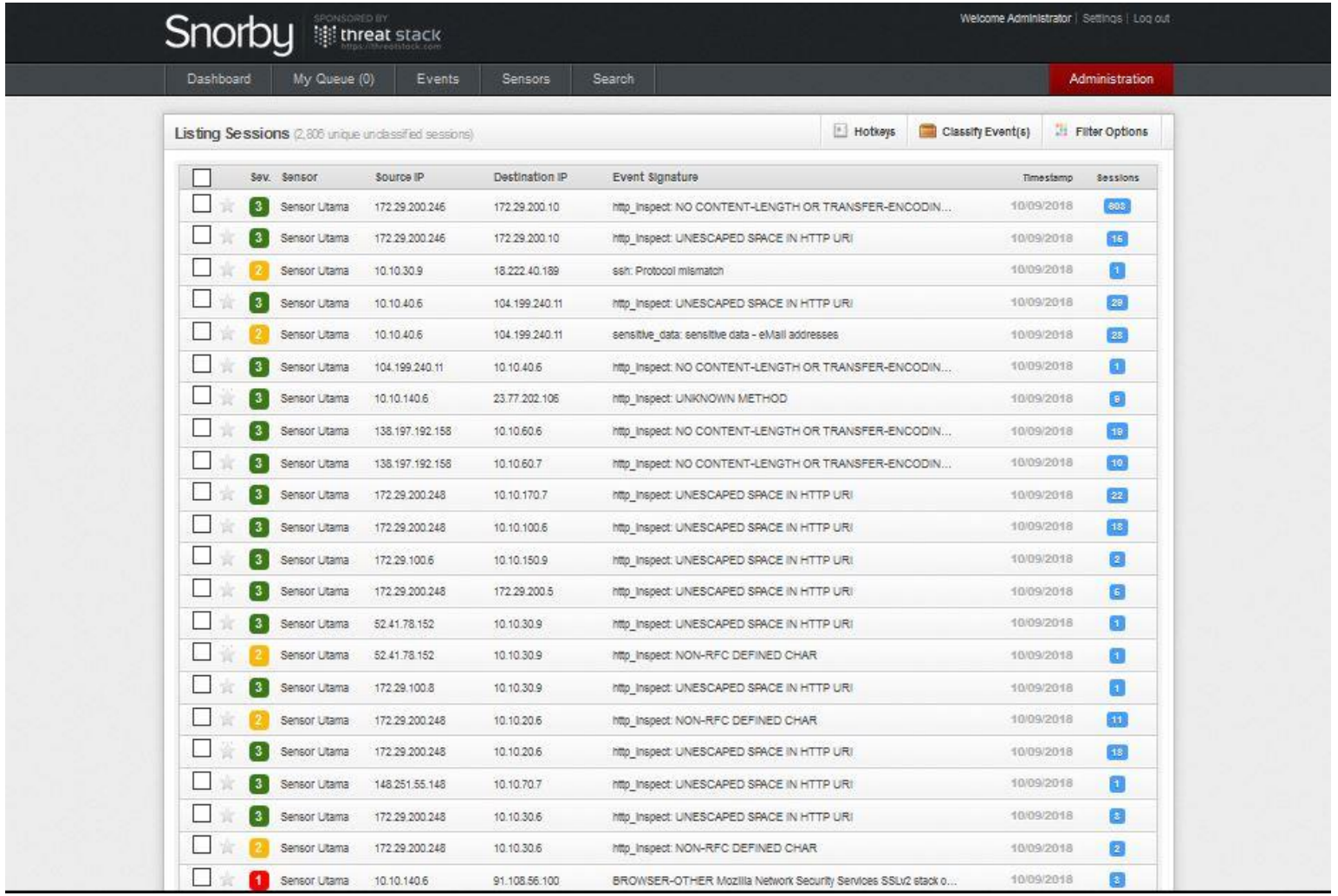
DASHBOARD


Snorby
SPONSORED BY threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Dashboard
More Options
LAST 24 TODAY YESTERDAY THIS WEEK LAST MONTH THIS QUARTER THIS YEAR
79093
HIGH SEVERITY
79,093 / 791,510
162308
MEDIUM SEVERITY
162,308 / 791,510
550420
LOW SEVERITY
550,420 / 791,510
Sensors
Severities
Protocols
Signatures
Sources
Destinations
Severity Count vs Time
High Severity
Medium Severity
Low Severity
500k
400k
300k
200k
100k
0k
-100k
Severity Count
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Date of Month
TOP 5 SENSOR
Sensor Utama 12,680
Sensor Sekunder 0
TOP 5 ACTIVE USERS
Sektor A 0
Sektor B 0
Administrator 1
Sektor C 0
LAST 5 UNIQUE EVENTS
http_inspect: NO CONTENT-... 2,939
http_inspect: NO CONTENT-... 2,939
http_inspect: NO CONTENT-... 2,939
http_inspect: UNESCAPED S... 2,406
http_inspect: NO CONTENT-... 2,939
ANALYST CLASSIFIED EVENTS
Unauthorized User Access 1
Unauthorized Root Access 0
Attempted Unauthorized... 0
Denial of Service Attack 0
Policy Violation 0
Reconnaissance 0
Virus Infection 0

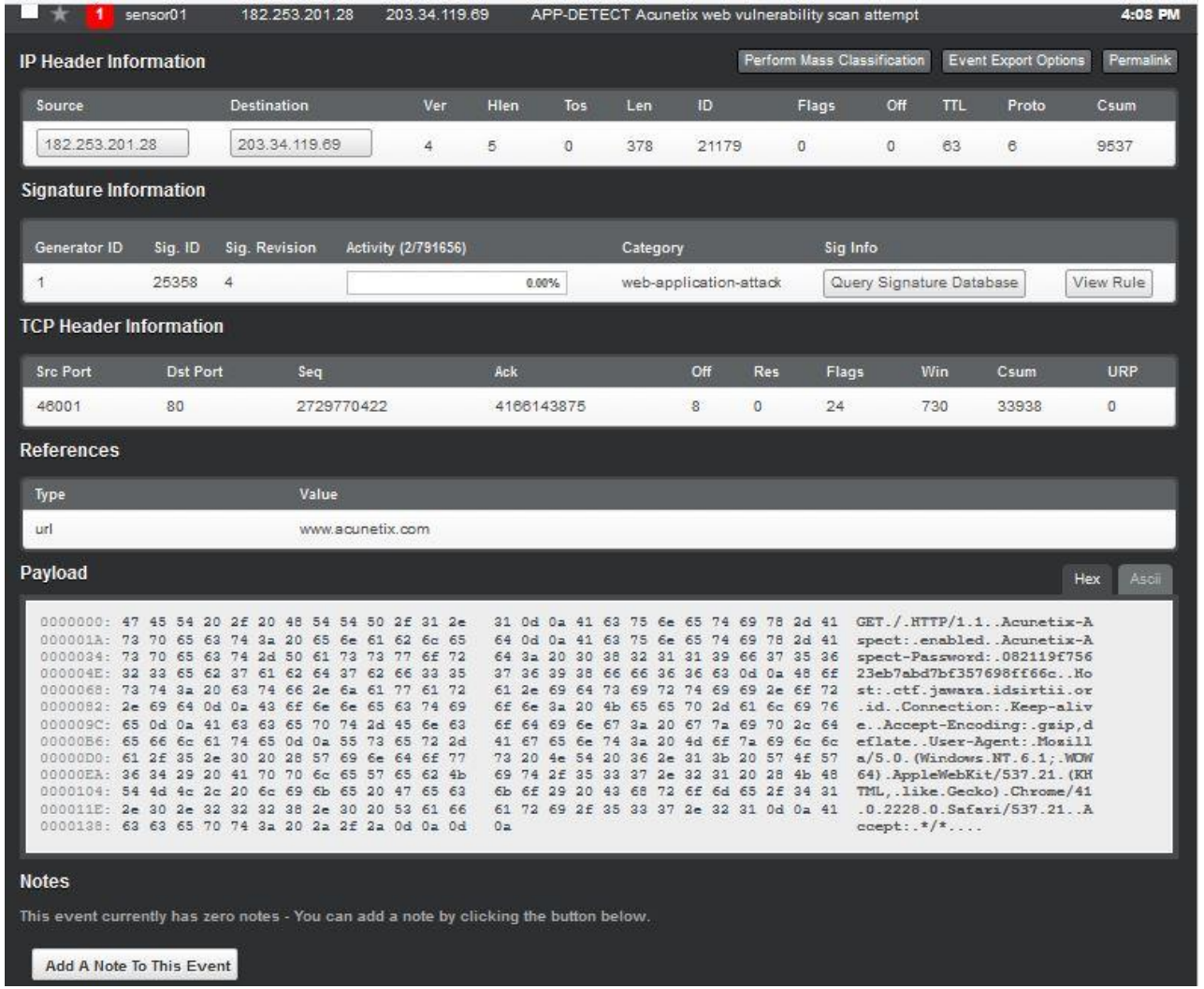
DASHBOARD


Snorby
SPONSORED BY threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Dashboard
More Options
LAST 24 TODAY YESTERDAY THIS WEEK LAST MONTH THIS QUARTER THIS YEAR
79093
HIGH SEVERITY
162308
MEDIUM SEVERITY
550420
LOW SEVERITY
Sensors Severities Protocols Signatures Sources Destinations
SQL 1 = 1 - possible sql injec... (0%)
snort general alert... (0%)
SQL use of sleep function in H... (0%)
http_inspect: TOO MANY PIPELIN... (0%)
Snort Alert [1:1000012:1]... (0%)
ALWARE-OTHER dns request with... (0%)
-WINDOWS possible SMB replay... (0%)
WARE-TOOLS Havij advanced S... (0%)
p_inspect: NON-RFC DEFINED ... (0%)
Snort Alert [1:469:3]... (1%)
RVER-OTHER Microsoft ISA Ser... (1%)
Snort Alert [1:1000001:1]... (1%)
ttp_inspect: MESSAGE WITH INV... (1%)
WSER-PLUGINS Advantech WebA... (1%)
SERVER-OTHER Cisco Web Securit... (1%)
http_inspect: UNESCAPED SPACE ... (2%)
APP-DETECT Acunetix web vulner... (9%)
http_inspect: NO CONTENT-LENGT... (10%)
ssh: Protocol mismatch... (17%)
http_inspect: UNKNOWN METHOD... (5
TOP 5 SENSOR
Sensor Utama 12,680
Sensor Sekunder 0
TOP 5 ACTIVE USERS
Sektor A 0
Sektor B 0
Administrator 1
Sektor C 0
LAST 5 UNIQUE EVENTS
http_inspect: NO CONTENT-... 2,939
http_inspect: NO CONTENT-... 2,939
http_inspect: NO CONTENT-... 2,939
http_inspect: UNESCAPED S... 2,406
http_inspect: NO CONTENT-... 2,939
ANALYST CLASSIFIED EVENTS
Unauthorized User Access 1
Unauthorized Root Access 0
Attempted Unauthorized... 0
Denial of Service Attack 0
Policy Violation 0
Reconnaissance 0
Virus Infection 0

EVENTS


Snorby
SPONSORED BY threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Listing Sessions (2,806 unique unclassified sessions)
Hotkeys
Classify Event(s)
Filter Options
Sev. Sensor Source IP Destination IP Event Signature Timestamp Sessions
3 Sensor Utama 172.29.200.246 172.29.200.10 http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN... 10/09/2018 803
3 Sensor Utama 172.29.200.246 172.29.200.10 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 16
2 Sensor Utama 10.10.30.9 18.222.40.189 ssh: Protocol mismatch 10/09/2018 1
3 Sensor Utama 10.10.40.6 104.199.240.11 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 29
2 Sensor Utama 10.10.40.6 104.199.240.11 sensitive_data: sensitive data - eMail addresses 10/09/2018 28
3 Sensor Utama 104.199.240.11 10.10.40.6 http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN... 10/09/2018 1
3 Sensor Utama 10.10.140.6 23.77.202.106 http_inspect: UNKNOWN METHOD 10/09/2018 9
3 Sensor Utama 138.197.192.158 10.10.60.6 http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN... 10/09/2018 19
3 Sensor Utama 138.197.192.158 10.10.60.7 http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODIN... 10/09/2018 10
3 Sensor Utama 172.29.200.248 10.10.170.7 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 22
3 Sensor Utama 172.29.200.248 10.10.100.6 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 18
3 Sensor Utama 172.29.100.6 10.10.150.9 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 2
3 Sensor Utama 172.29.200.248 172.29.200.5 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 6
3 Sensor Utama 52.41.78.152 10.10.30.9 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 1
2 Sensor Utama 52.41.78.152 10.10.30.9 http_inspect: NON-RFC DEFINED CHAR 10/09/2018 1
3 Sensor Utama 172.29.100.8 10.10.30.9 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 1
2 Sensor Utama 172.29.200.248 10.10.20.6 http_inspect: NON-RFC DEFINED CHAR 10/09/2018 11
3 Sensor Utama 172.29.200.248 10.10.20.6 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 18
3 Sensor Utama 148.251.55.148 10.10.70.7 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 1
3 Sensor Utama 172.29.200.248 10.10.30.6 http_inspect: UNESCAPED SPACE IN HTTP URI 10/09/2018 5
2 Sensor Utama 172.29.200.248 10.10.30.6 http_inspect: NON-RFC DEFINED CHAR 10/09/2018 2
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

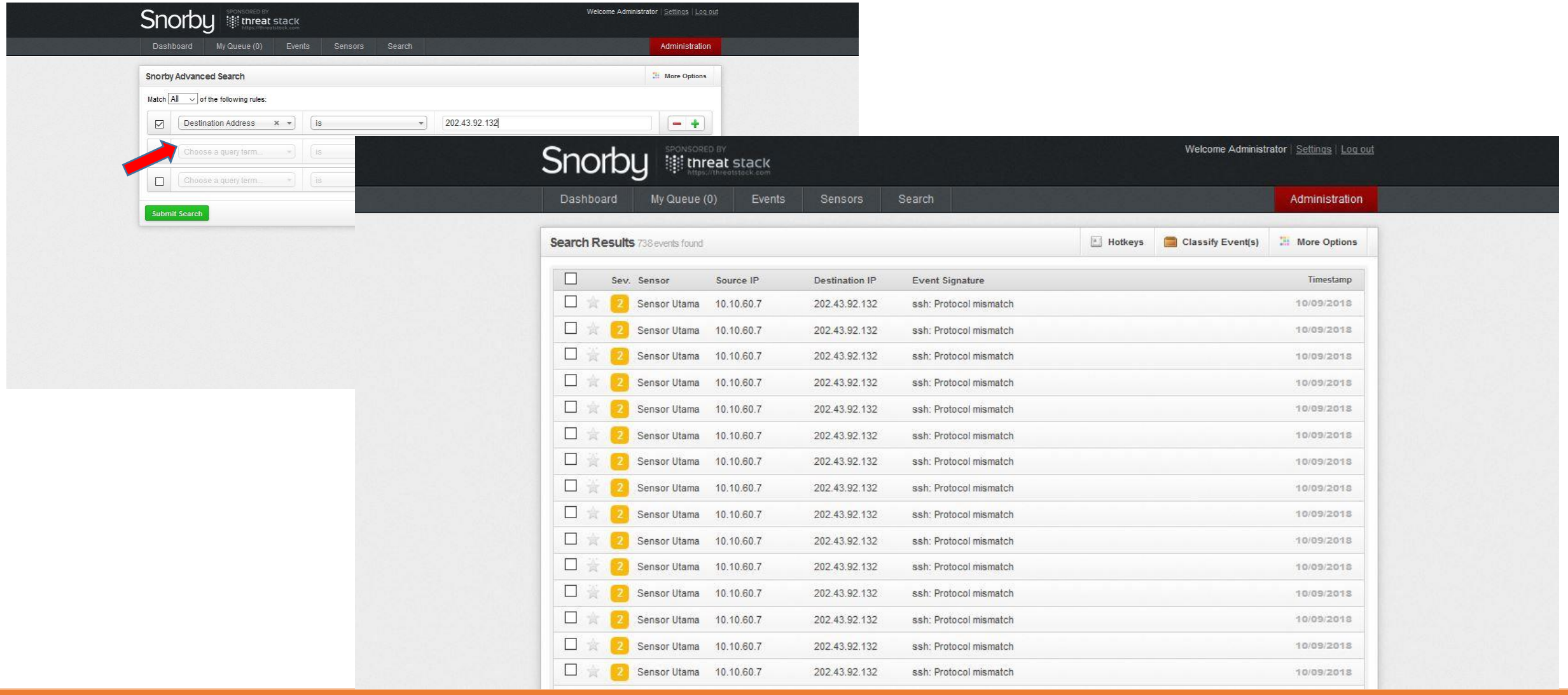

1 sensor01 182.253.201.28 203.34.119.69 APP-DETECT Acunetix web vulnerability scan attempt 4:08 PM
IP Header Information
Perform Mass Classification
Event Export Options
Permalink
Source Destination Ver Hlen Tos Len ID Flags Off TTL Proto Csum
182.253.201.28 203.34.119.69 4 5 0 378 21179 0 0 63 6 9537
Signature Information
Generator ID Sig. ID Sig. Revision Activity (2/791656) Category Sig Info
1 25358 4 0.00% web-application-attack Query Signature Database View Rule
TCP Header Information
Src Port Dst Port Seq Ack Off Res Flags Win Csum URP
46001 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..Ho
0000068: 73 74 3a 20 63 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:.Mozill
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 ccept:.*/*....
Notes
This event currently has zero notes - You can add a note by clicking the button below.
Add A Note To This Event

EVENTS

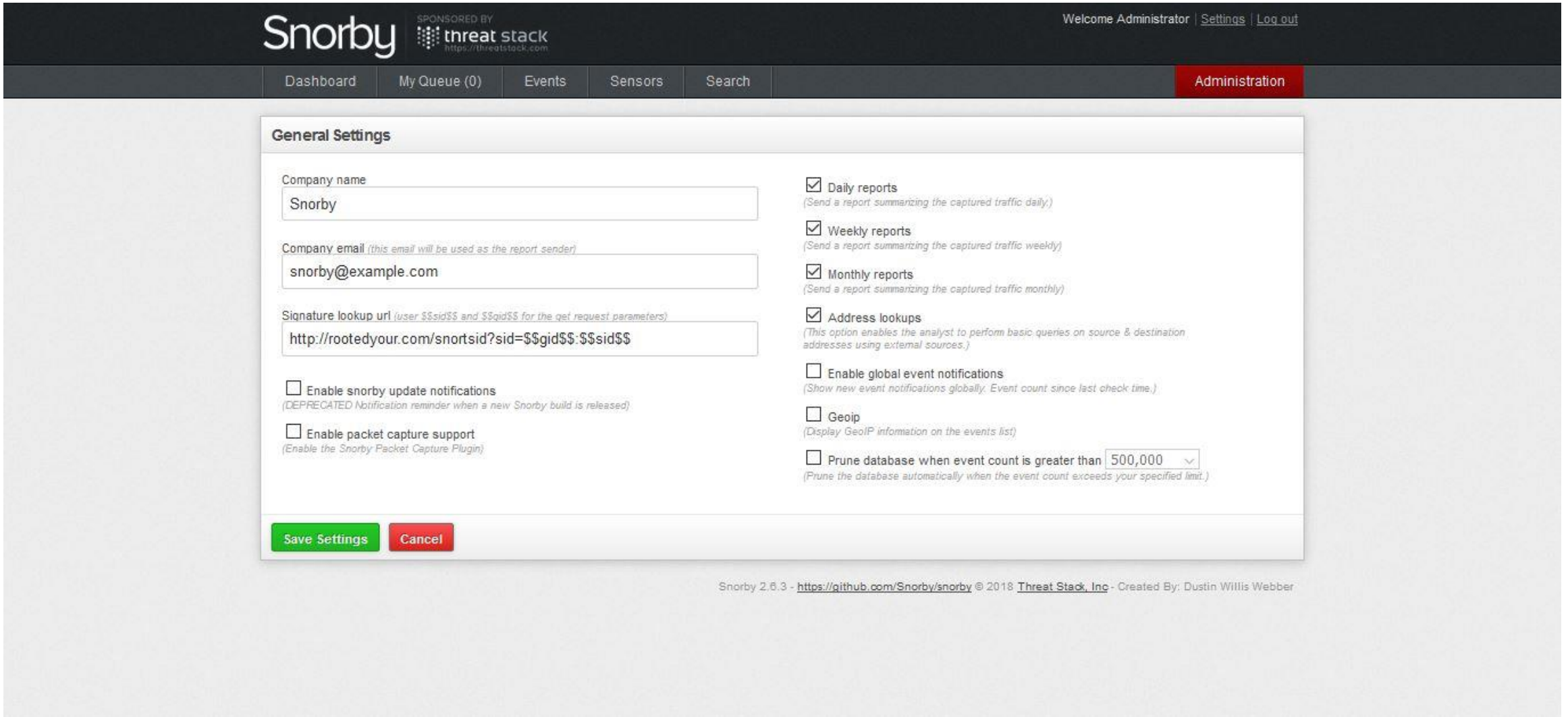
High Severity Events 24 events found

☐		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	POLICY-OTHER Adobe ColdFusion admin interface access attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	POLICY-OTHER Adobe ColdFusion admin interface access attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	OS-OTHER Bash CGI environment variable injection attempt	4:10 PM
☐	☆	1	sensor01	172.16.6.251	172.16.1.14	APP-DETECT Acunetix web vulnerability scan attempt	4:08 PM
☐	☆	1	sensor01	182.253.201.28	203.34.119.69	APP-DETECT Acunetix web vulnerability scan attempt	4:08 PM

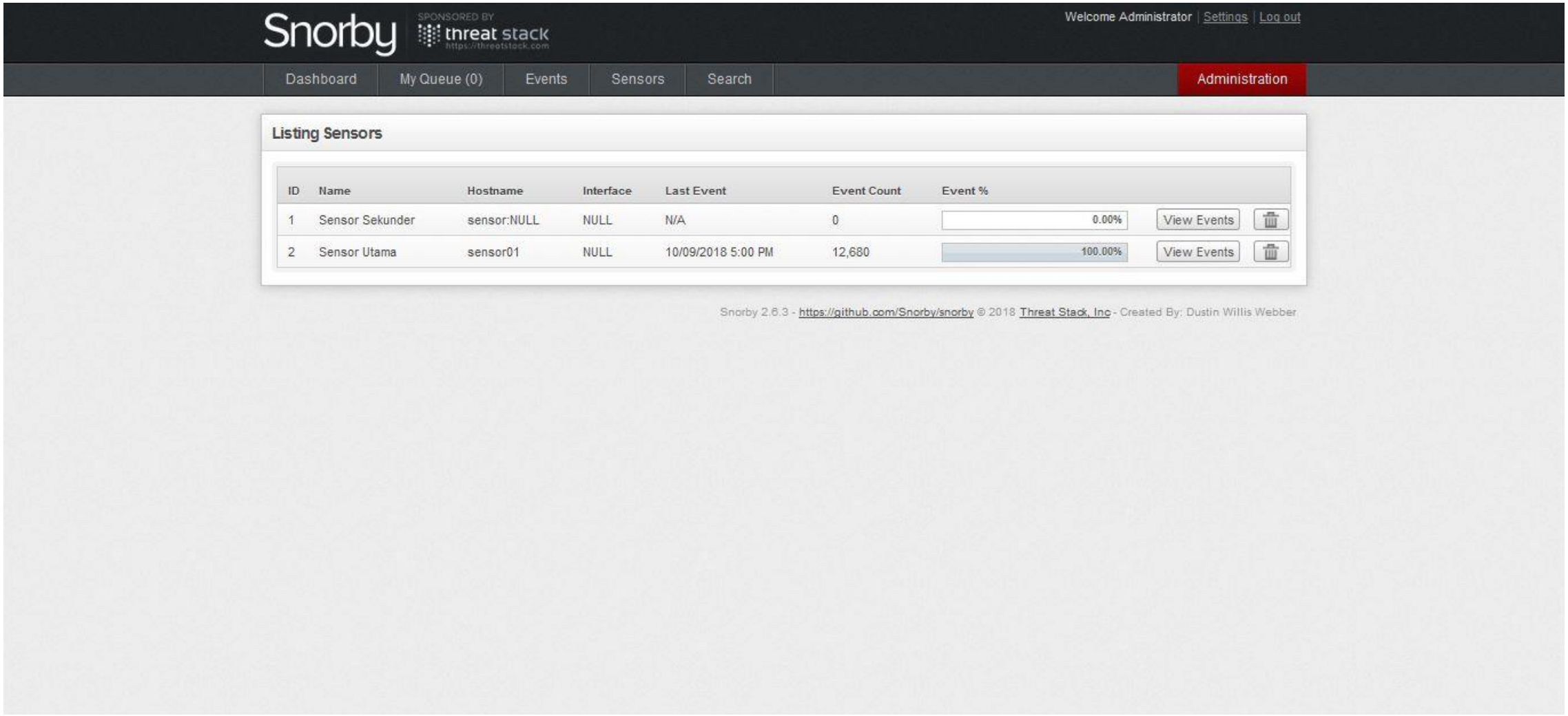
SEARCH


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
202.43.92.132
Choose a query term...
Submit Search
Search Results 738 events found
Hotkeys
Classify Event(s)
More Options
Sev. Sensor Source IP Destination IP Event Signature Timestamp
Sensor Utama 10.10.60.7 202.43.92.132 ssh: Protocol mismatch 10/09/2018

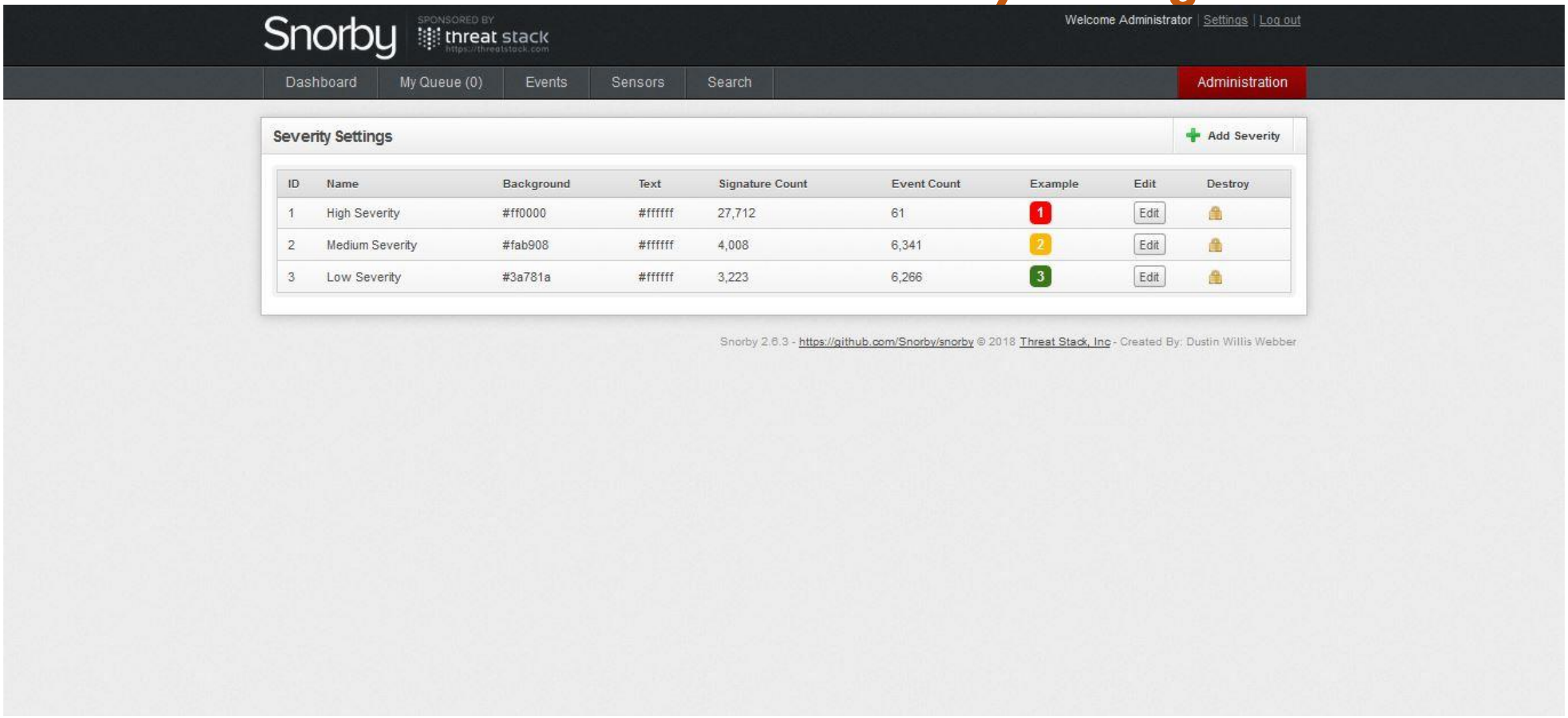
Administration – General Setting



Administration – Listing Sensor



Administration – Saverity Setting



Administration – Listing Signature

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

Welcome Administrator | Settings | Log out

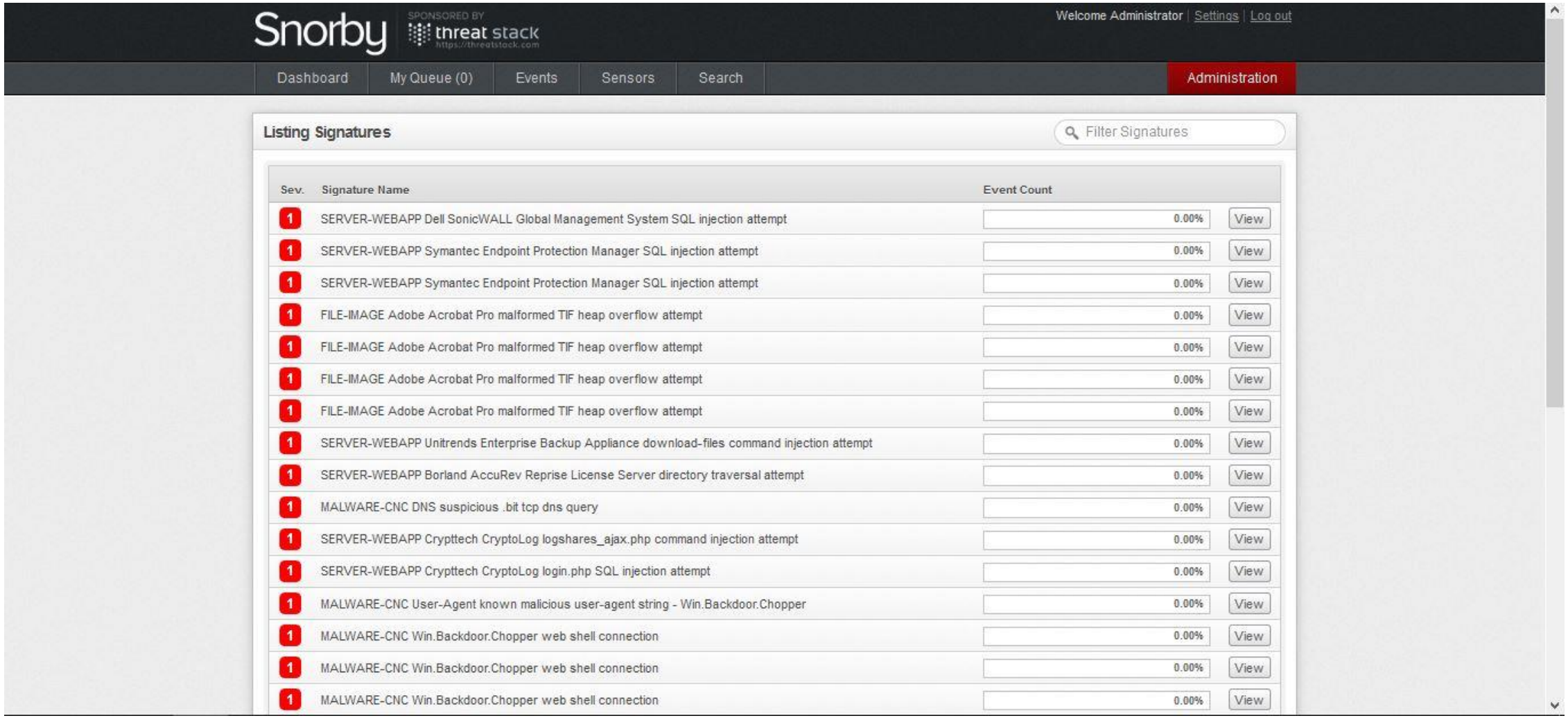
Dashboard | My Queue (0) | Events | Sensors | Search | Administration

Listing Signatures

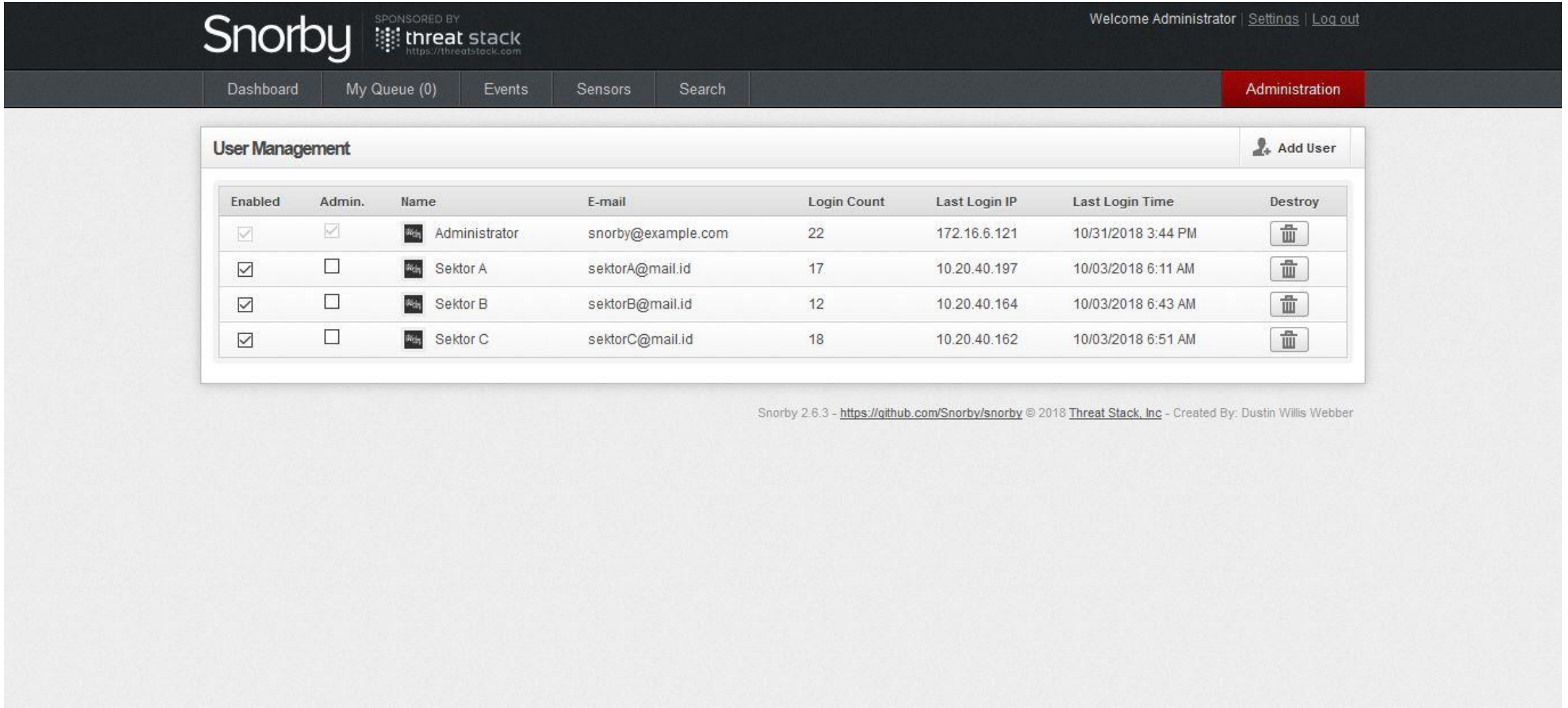
Filter Signatures

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

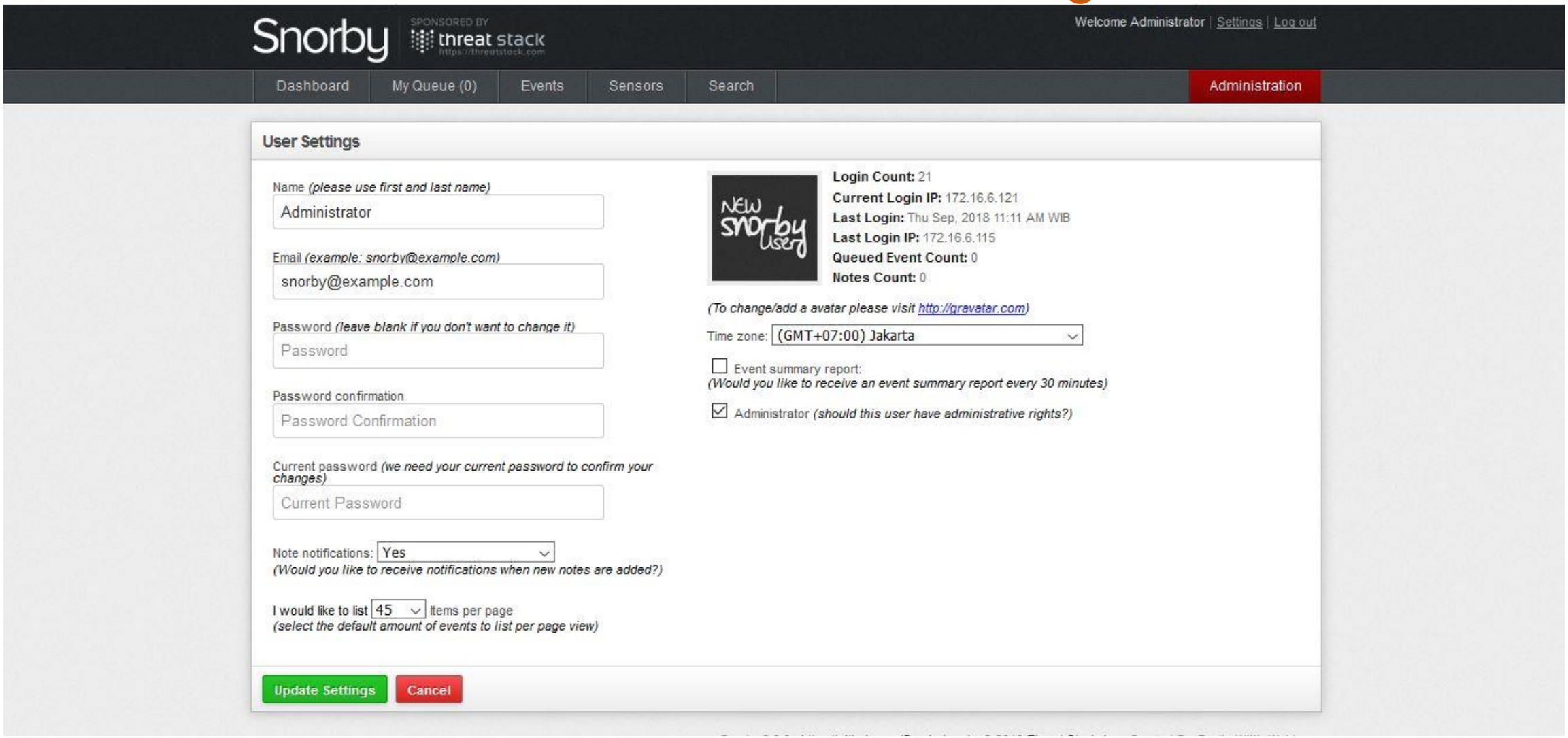
Administration – Listing Signature



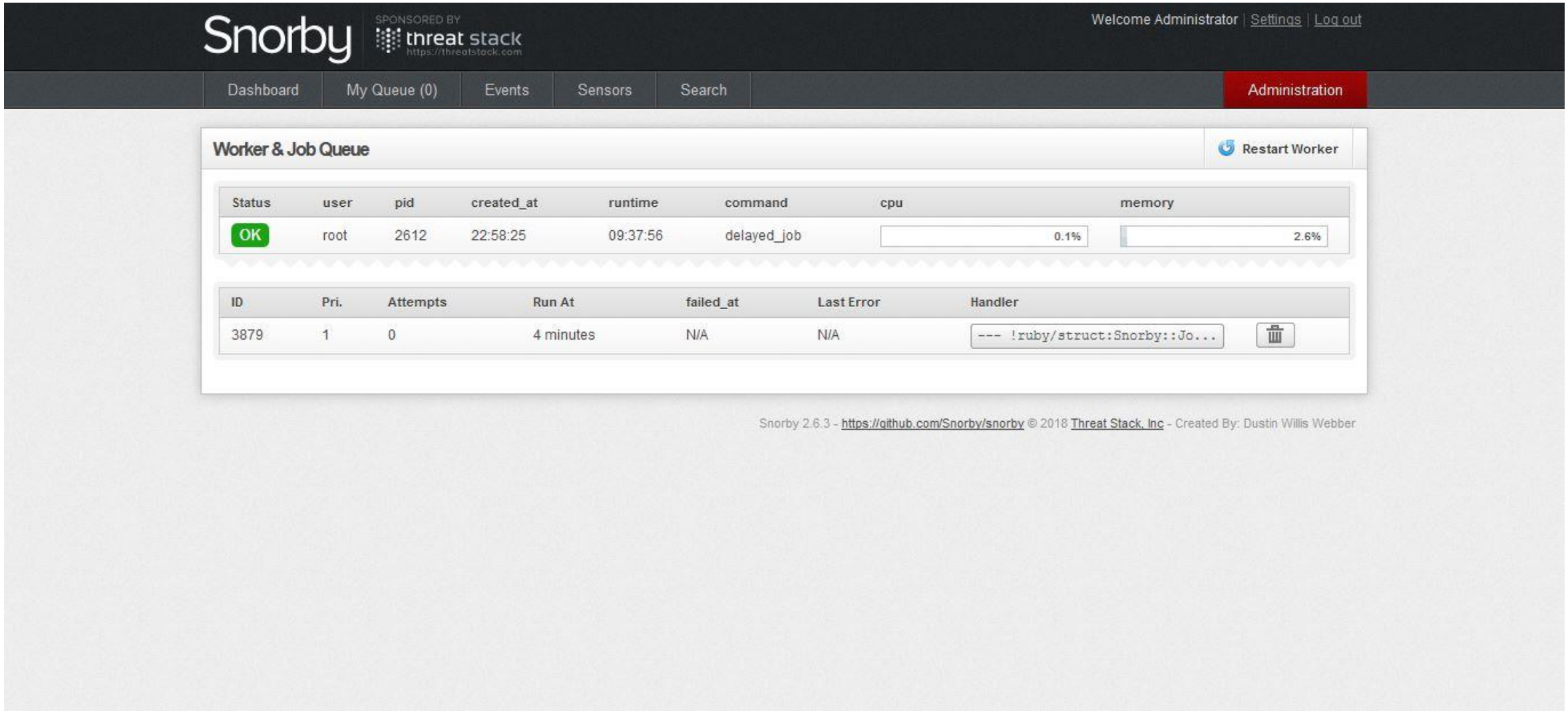
Administration – User Management



User – General Setting



Administration – Worker & Job Queue



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 ☺