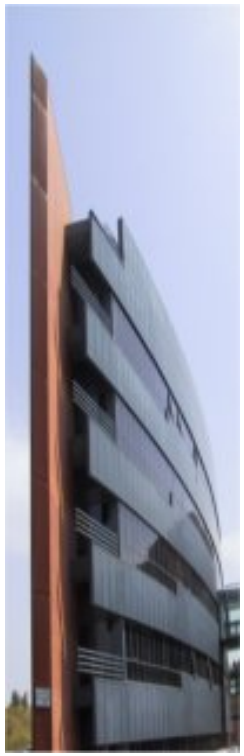
Análisis de Logs con SIEM en la UAM

GT2010 Salamanca

Víctor Barahona <victor.barahona@uam.es>

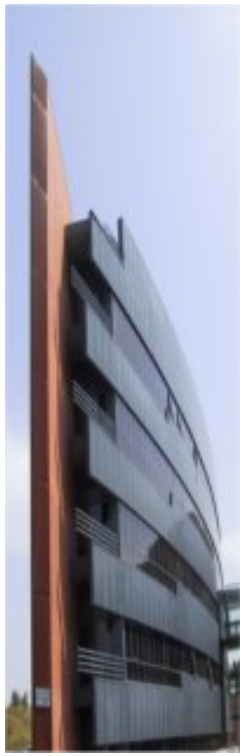
Tecnologías de la Información

Universidad Autónoma de Madrid



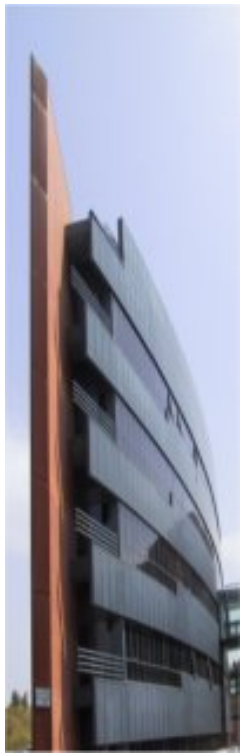
Security Information & Event Manager

- Appliance bajo linux.
- Recolecta, normaliza y correlaciona
- Multi-fabricante.
- Agrega flujos de red (layer 7) y busca anomalías.
- Vulnerability Assets.
- Orientado a seguridad y red.



Puntos fuertes

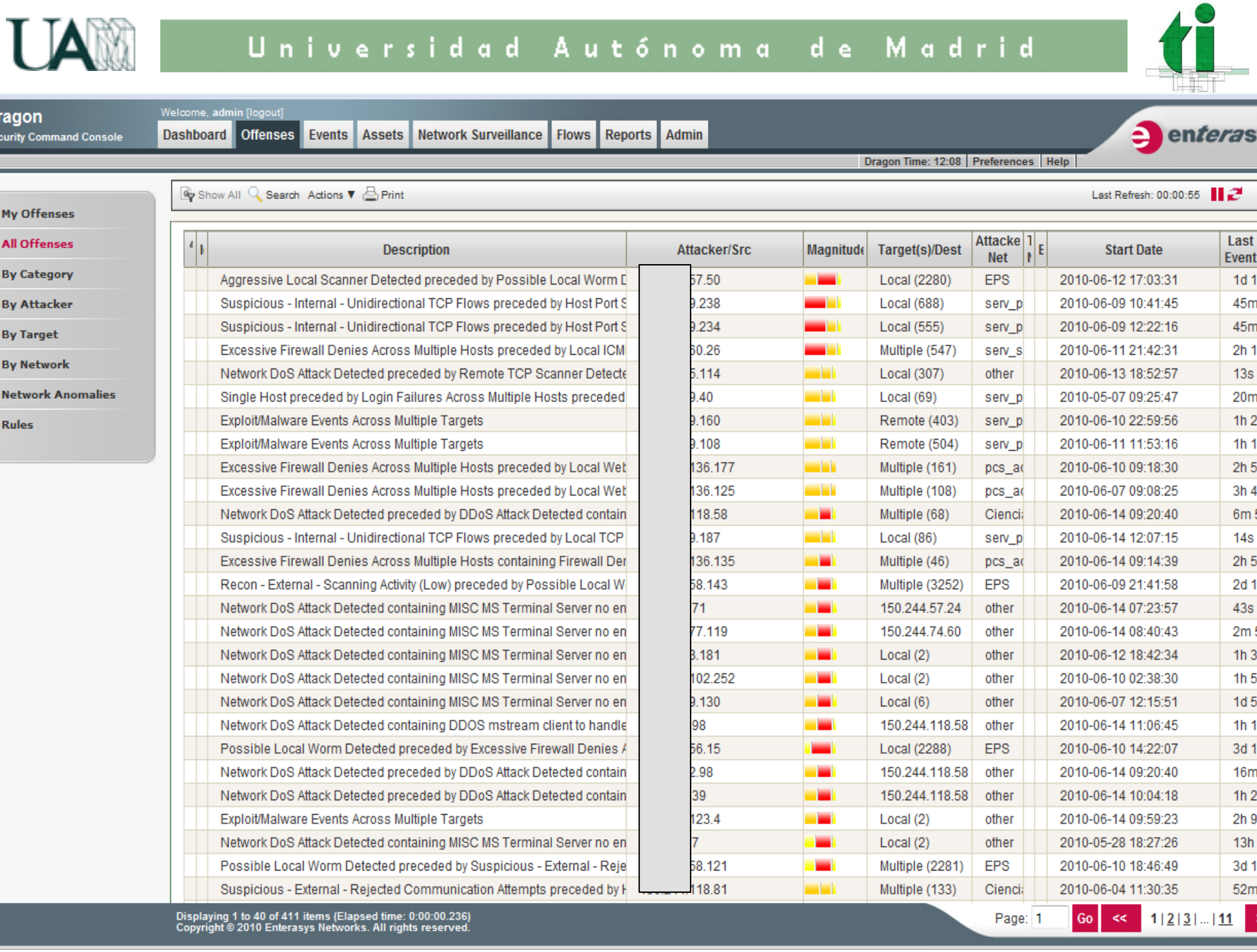
- Correla “out of the box”.
- Gestión de flujos integrada: netflow, J-Flow, Sflow, cFlowd, Packeteer.
- Gran cantidad de dispositivos soportados nativamente.
- Interfaz gráfica de gestión de eventos, ofensas y flujos.
- Consolidación de la información.
- Rápido en eventos de las ultimas 24H



Puntos fuertes

- Permite lanzar acciones ante ofensas.
- Reducción de información.
- Normaliza para correlacionar, pero almacena en crudo.


Universidad Autónoma de Madrid
Dragon
Security Command Console
Welcome, admin [logout]
Dashboard
Offenses
Events
Assets
Network Surveillance
Flows
Reports
Admin
enterasys
Dragon Time: 11:05
Preferences
Help
Add Item...
Next Refresh: 00:00:20
Offenses - New Offense Count
8 Hours
Time Series
Line Chart
Pie Chart
Legend
Security
Both
Events - Average Events Per Second
24 Hours
Time Series
Line Chart
Pie Chart
Legend
Top Log Sources
19
29
61
1,100
11,474
Top Rules (real-time)
Table
Bar Chart
Pie Chart
Legend
Most Severe Offenses
Offense Name
Magnitude
Aggressive Local Scanner Detected preceded by Possible Local Worm Detected preceded by Excessive Firewall Denies Across Multiple Hosts preceded by Local SSH Scanner Detected containing Firewall Deny
Excessive Firewall Denies Across Multiple Hosts preceded by Local ICMP Scanner containing Firewall Deny
Exploit/Malware Events Across Multiple Targets
Exploit/Malware Events Across Multiple Targets
Excessive Firewall Denies Across Multiple Hosts preceded by Local Web Scanner Detected preceded by Local TCP Scanner Detected containing Firewall Deny
Top Attackers
Attacker
Threat
Server Applications - Inbound Bytes
8 Hours
Time Series
Line Chart
Pie Chart
Legend
Server Applications - Outbound Bytes
8 Hours
Time Series
Line Chart
Pie Chart
Legend
Dragon Summary
Current Flows Per Second 1.5 K
Flows (Past 24 Hours) 68.3 M
Current Events Per Second 185
New Events (Past 24 Hours) 7.7 M
Updated Offenses (Past 24 Hours) 85
Data Reduction Ratio 94978 : 1
Powered by
QLabs


Universidad Autónoma de Madrid
Dragon
Security Command Console
Welcome, admin [logout]
Dashboard
Offenses
Events
Assets
Network Surveillance
Flows
Reports
Admin
enterasys
Dragon Time: 12:08
Preferences
Help
My Offenses
All Offenses
By Category
By Attacker
By Target
By Network
Network Anomalies
Rules
Show All
Search
Actions
Print
Last Refresh: 00:00:55
Description
Attacker/Src
Magnitude
Target(s)/Dest
Attacker Net
Start Date
Last Event
Aggressive Local Scanner Detected preceded by Possible Local Worm D
Local (2280)
EPS
2010-06-12 17:03:31
Suspicious - Internal - Unidirectional TCP Flows preceded by Host Port S
Local (688)
serv_p
2010-06-09 10:41:45
45m
Suspicious - Internal - Unidirectional TCP Flows preceded by Host Port S
Local (555)
serv_p
2010-06-09 12:22:16
45m
Excessive Firewall Denies Across Multiple Hosts preceded by Local ICM
Multiple (547)
serv_s
2010-06-11 21:42:31
Network DoS Attack Detected preceded by Remote TCP Scanner Detecte
Local (307)
other
2010-06-13 18:52:57
13s
Single Host preceded by Login Failures Across Multiple Hosts preceded
Local (69)
serv_p
2010-05-07 09:25:47
20m
Exploit/Malware Events Across Multiple Targets
Remote (403)
serv_p
2010-06-10 22:59:56
Exploit/Malware Events Across Multiple Targets
Remote (504)
serv_p
2010-06-11 11:53:16
Excessive Firewall Denies Across Multiple Hosts preceded by Local Wet
Multiple (161)
pcs_ac
2010-06-10 09:18:30
Excessive Firewall Denies Across Multiple Hosts preceded by Local Wet
Multiple (108)
pcs_ac
2010-06-07 09:08:25
Network DoS Attack Detected preceded by DDoS Attack Detected contain
Multiple (68)
Ciencia
2010-06-14 09:20:40
6m 5
Suspicious - Internal - Unidirectional TCP Flows preceded by Local TCP
Local (86)
serv_p
2010-06-14 12:07:15
14s
Excessive Firewall Denies Across Multiple Hosts containing Firewall Der
Multiple (46)
pcs_ac
2010-06-14 09:14:39
Recon - External - Scanning Activity (Low) preceded by Possible Local W
Multiple (3252)
EPS
2010-06-09 21:41:58
Network DoS Attack Detected containing MISC MS Terminal Server no en
150.244.57.24
other
2010-06-14 07:23:57
43s
Network DoS Attack Detected containing MISC MS Terminal Server no en
150.244.74.60
other
2010-06-14 08:40:43
2m 5
Network DoS Attack Detected containing MISC MS Terminal Server no en
Local (2)
other
2010-06-12 18:42:34
Network DoS Attack Detected containing MISC MS Terminal Server no en
Local (2)
other
2010-06-10 02:38:30
Network DoS Attack Detected containing MISC MS Terminal Server no en
Local (6)
other
2010-06-07 12:15:51
Network DoS Attack Detected containing DDOS mstream client to handle
150.244.118.58
other
2010-06-14 11:06:45
Possible Local Worm Detected preceded by Excessive Firewall Denies A
Local (2288)
EPS
2010-06-10 14:22:07
Network DoS Attack Detected preceded by DDoS Attack Detected contain
150.244.118.58
other
2010-06-14 09:20:40
16m
Network DoS Attack Detected preceded by DDoS Attack Detected contain
150.244.118.58
other
2010-06-14 10:04:18
Exploit/Malware Events Across Multiple Targets
Local (2)
other
2010-06-14 09:59:23
Network DoS Attack Detected containing MISC MS Terminal Server no en
Local (2)
other
2010-05-28 18:27:26
Possible Local Worm Detected preceded by Suspicious - External - Reje
Multiple (2281)
EPS
2010-06-10 18:46:49
Suspicious - External - Rejected Communication Attempts preceded by H
Multiple (133)
Ciencia
2010-06-04 11:30:35
52m
Displaying 1 to 40 of 411 items (Elapsed time: 0:00:00.236)
Copyright © 2010 Enterasys Networks. All rights reserved.
Page: 1
Go
<<
1 | 2 | 3 | ... | 11
>>

Universidad Autónoma de Madrid

Welcome, admin [logout]

and Console | Dashboard | Offenses | Events | Assets | Network Surveillance | Flows | Reports | Admin

enterasys

Dragon Time: 12:10 | Preferences | Help

es
es
ry
er
k
Anomalies

All Offenses > Offense 13300 (Summary)

Offense 13300

Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions ▼ | Print

Magnitude				**Relevance**	4	**Severity**	10	**Credibility**	3
Description	Aggressive Local Scanner Detected preceded by Possible Local Worm Detected preceded by Excessive Firewall Denies Across Multiple Hosts preceded by Local SSH Scanner Detected containing Firewall Deny		**Event count**	2424 events in 4 categories					
Attacker/Src	150.244		**Start**	2010-06-12 17:03:31					
Target(s)/Dest	Local (2280)		**Duration**	1m 12s					
Network(s)	Multiple (6)		**Assigned to**	Not assigned					
Notes									

Attacker Summary

Details

Magnitude		**User**	Unknown
Description	150.244.	**Asset Name**	Unknown
Vulnerabilities	0	**MAC**	Unknown
Location	red_uam.EPS	**Asset Weight**	0

Top 5 Categories

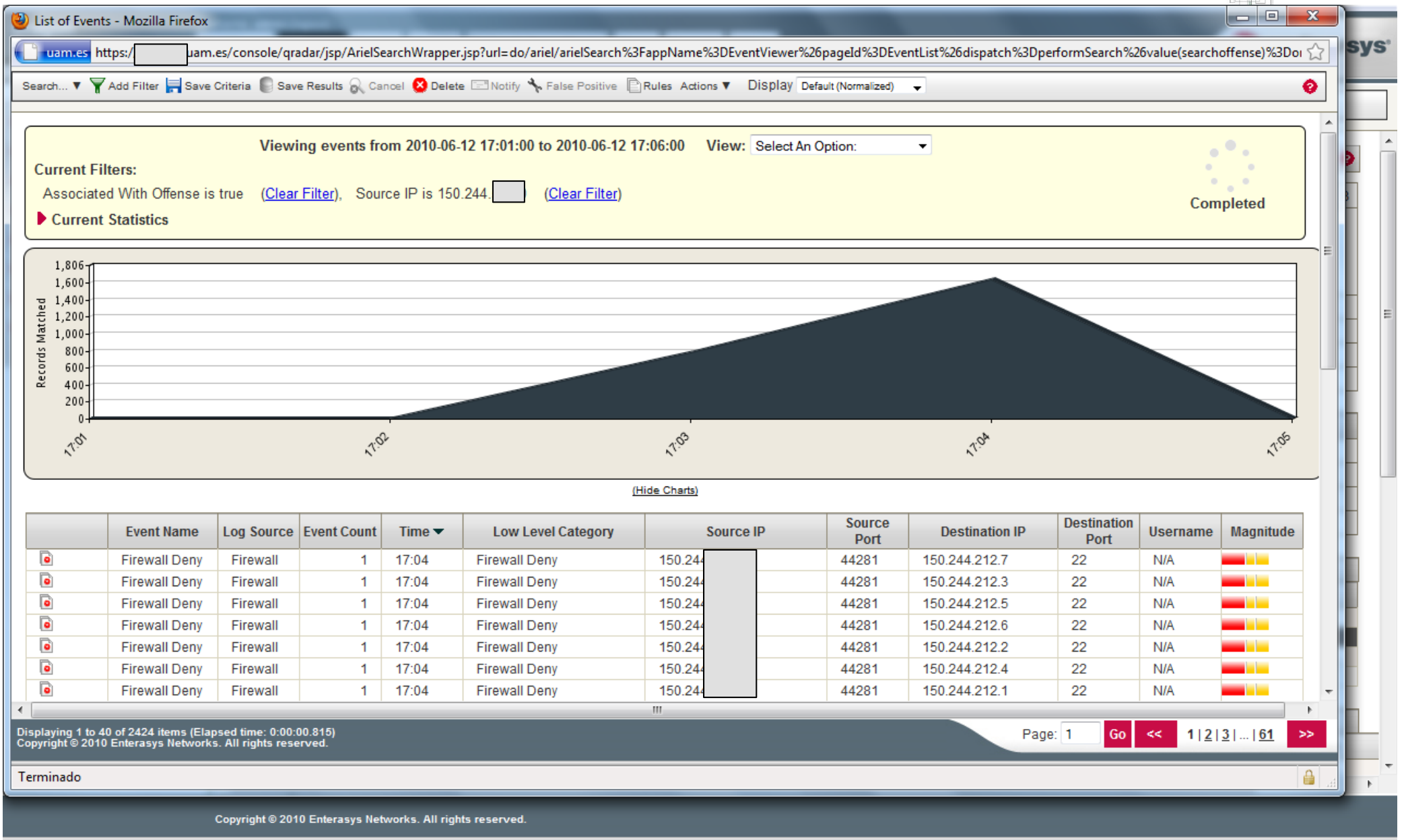
Categories

Name	Magnitude	Local Target Count	Events	Last Event
Potential worm activity		7	7	06-12 17:04:19
Network Sweep		57	57	06-12 17:04:21
Firewall Deny		2280	2280	06-12 17:04:44
Misc Recon Event		80	80	06-12 17:04:21

Top 5 Local Targets

Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location
150.24		Unknown	No	Unknown	Unknown	serv_publicos


List of Events - Mozilla Firefox
Search... Add Filter Save Criteria Save Results Cancel Delete Notify False Positive Rules Actions Display Default (Normalized)
Viewing events from 2010-06-12 17:01:00 to 2010-06-12 17:06:00 View: Select An Option:
Current Filters:
Associated With Offense is true (Clear Filter), Source IP is 150.244. (Clear Filter)
Current Statistics
Completed
Records Matched
1,806
1,600
1,400
1,200
1,000
800
600
400
200
0
17:01
17:02
17:03
17:04
17:05
(Hide Charts)
Event Name | Log Source | Event Count | Time | Low Level Category | Source IP | Source Port | Destination IP | Destination Port | Username | Magnitude
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.7 | 22 | N/A
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.3 | 22 | N/A
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.5 | 22 | N/A
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.6 | 22 | N/A
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.2 | 22 | N/A
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.4 | 22 | N/A
Firewall Deny | Firewall | 1 | 17:04 | Firewall Deny | 150.24 | 44281 | 150.244.212.1 | 22 | N/A
Displaying 1 to 40 of 2424 items (Elapsed time: 0:00:00.815)
Copyright © 2010 Enterasys Networks. All rights reserved.
Page: 1 Go << 1 | 2 | 3 | ... | 61 >>
Terminado
Copyright © 2010 Enterasys Networks. All rights reserved.

Flow List - Mozilla Firefox

uam.es https: am.es/console/do/qradar/dataminesearch?dispatch=performSearch&fromAddress=150.244.57.50&toAddress=&rangeStart=1276354891&rangeEnd=127635

Search... ▼ Add Filter Save Criteria Save Results Cancel Delete Notify Actions ▼ Display Default (Normalized)

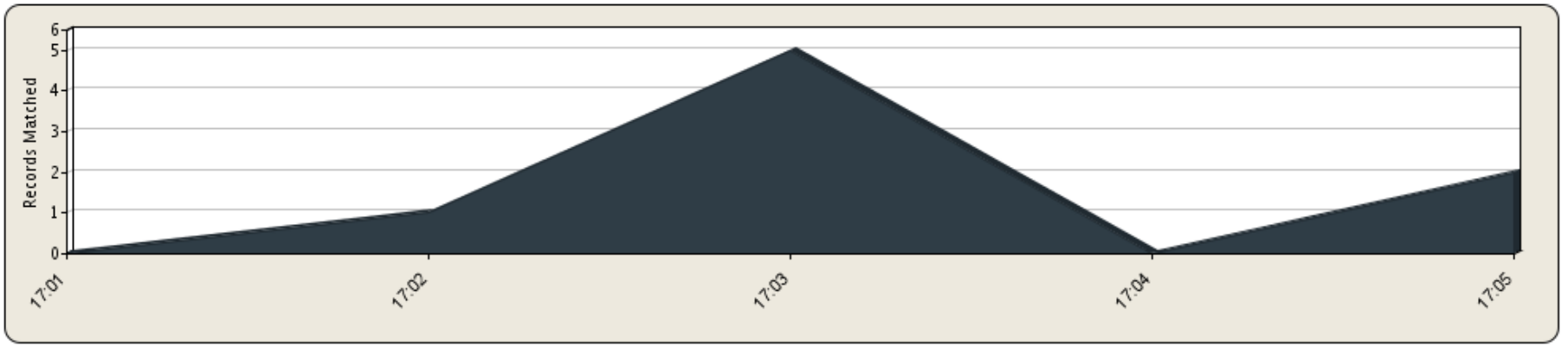
Viewing flows from 2010-06-12 17:01:31 to 2010-06-12 17:06:44 View: Select An Option:

Current Filters:

Source or Destination IP is 150.244 (Clear Filter), Flow Direction is any of L2L (Clear Filter),
Source or Destination Network is any of red_uam.EPS (Clear Filter)

Completed

Current Statistics



(Hide Charts)

Flow Typ	First Packet Time	Last Packet Time	Source IP	Source Port	Destination IP	Destination Port	Sou Byt	Des Byt	Tot Byt	Sou Pac	Des Pac	Tot Pac	Pro	App	ICM Typ	Sou Flag	Des Flag	Sou QoS	Des QoS	Flow Sou
	17:05	17:05	150.244	46912	150.244.9.237	22	55	1 1	1 6	7	7	14	tcp	SS	N/A	F,S	F,S	Be	Be	c:
	17:03	17:05	150.244	44281	150.244.1.2	22	0	17	17	0	4	4	tcp	SS	N/A		S,A	Be	Be	d
	17:03	17:03	150.244	44281	150.244.9.237	22	13	66	19	2	1	3	tcp	SS	N/A	S,F	S,A	Be	Be	c:
	17:03	17:03	150.244	44281	150.244.9.206	22	66	0	66	1	0	1	tcp	SS	N/A	S		Be	Be	c:
	17:03	17:03	150.244	44281	150.244.9.40	22	66	64	13	1	1	2	tcp	SS	N/A	S	R,A	Be	Be	c:

Displaying 1 to 8 of 8 items (Elapsed time: 0:00:00.042)

Terminado

Cerrar

Universidad Autónoma de Madrid

Dragon
Security Command Console

Welcome, admin [logout]

Dashboard | Offenses | Events | Assets | Network Surveillance | Flows | Reports | Admin

enterasys

Dragon Time: 12:25 | Preferences | Help

Global Views | Asset Map | Bookmarks | QRL Options

Time Until Refresh: 79

Pivot To

Base Views
- Applications
  - Client | Server
- Threats
- Geographic
- Flow Types
- Collector

Custom Views
- FlowShape

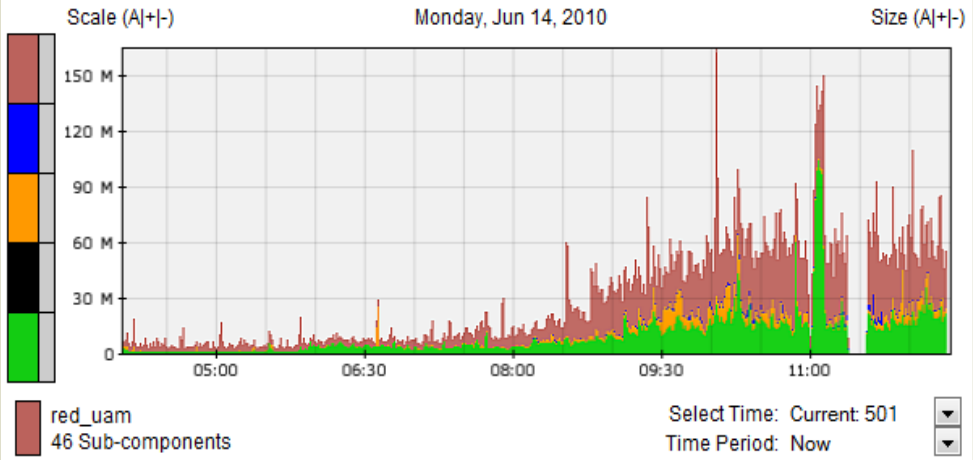
Layers

- Bytes/Second
  - Normal
    - Log
    - Bits/Second
    - Bytes/Packet
    - Bytes/Host
    - 1/X
- Packets/Second
- Number of Hosts
- Unique Ports

View Flows

View Flows | Search

Inbound Bytes (Normal)

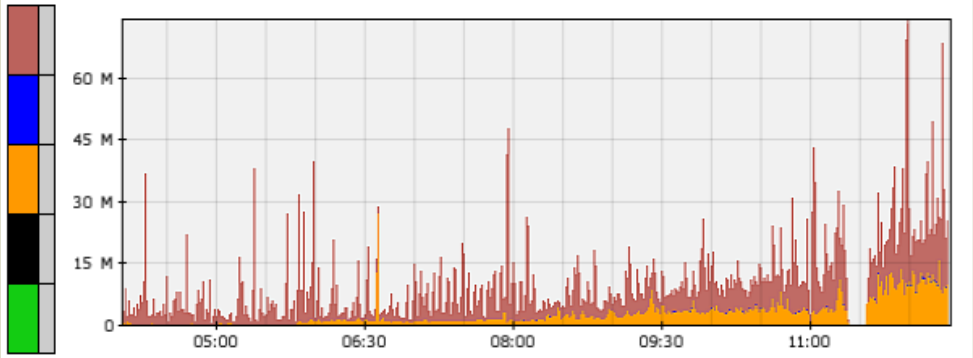


red_uam
46 Sub-components

Select Time: Current: 501
Time Period: Now

◄ View Sentries (54) ►◄ Add Sentry ►

Outbound Bytes (Normal)



red_uam
46 Sub-components

Select Time: Current: 501
Time Period: Now

◄ View Sentries (54) ►◄ Add Sentry ►

QRL Definition

View: nets
Layer: bytes
Derived Layer: Normal
Direction: all

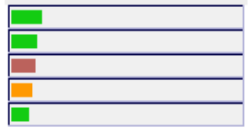
Networks:
All

Components:
All

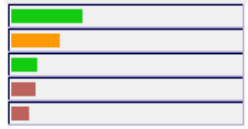
Removes:
None

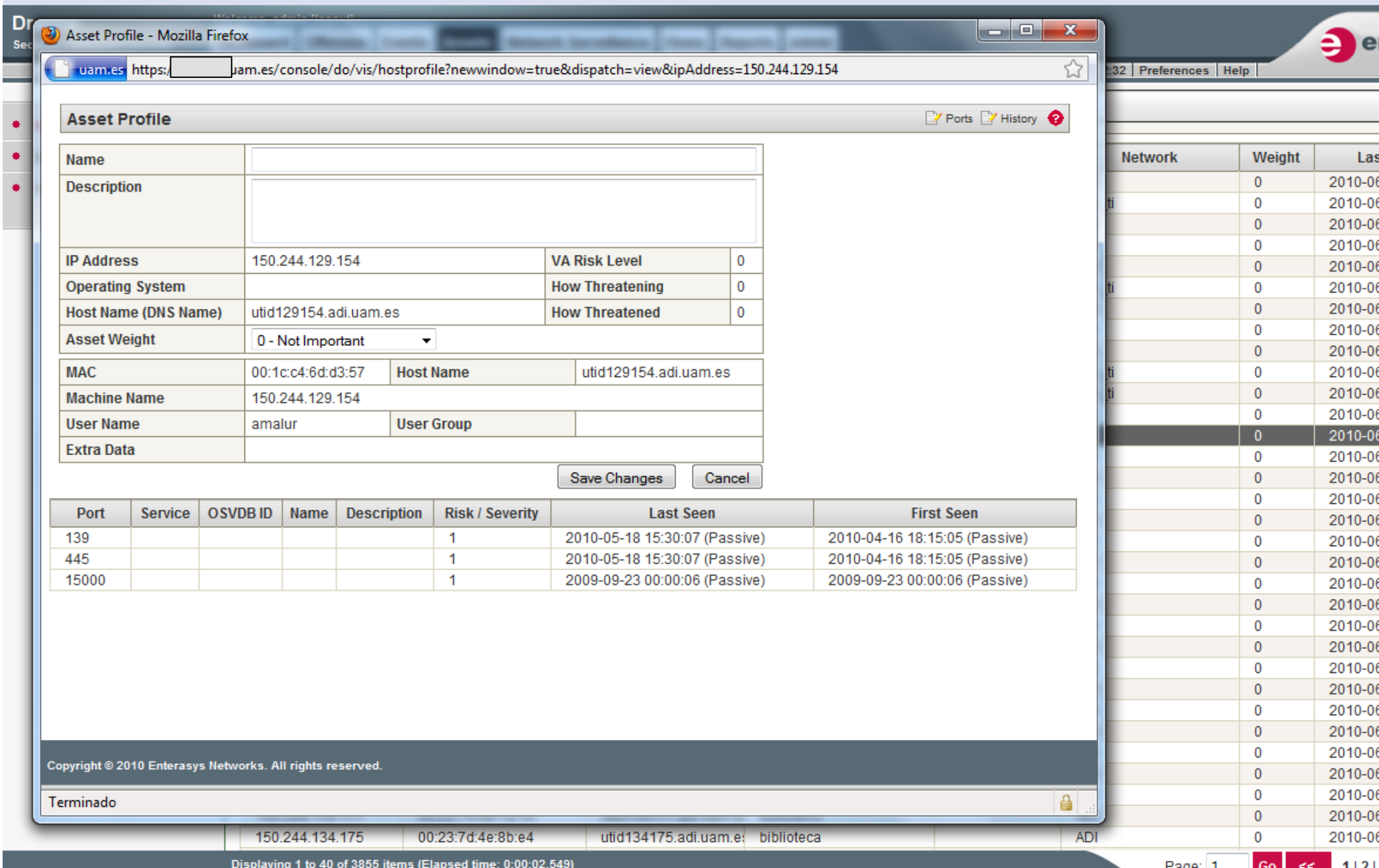
TopN

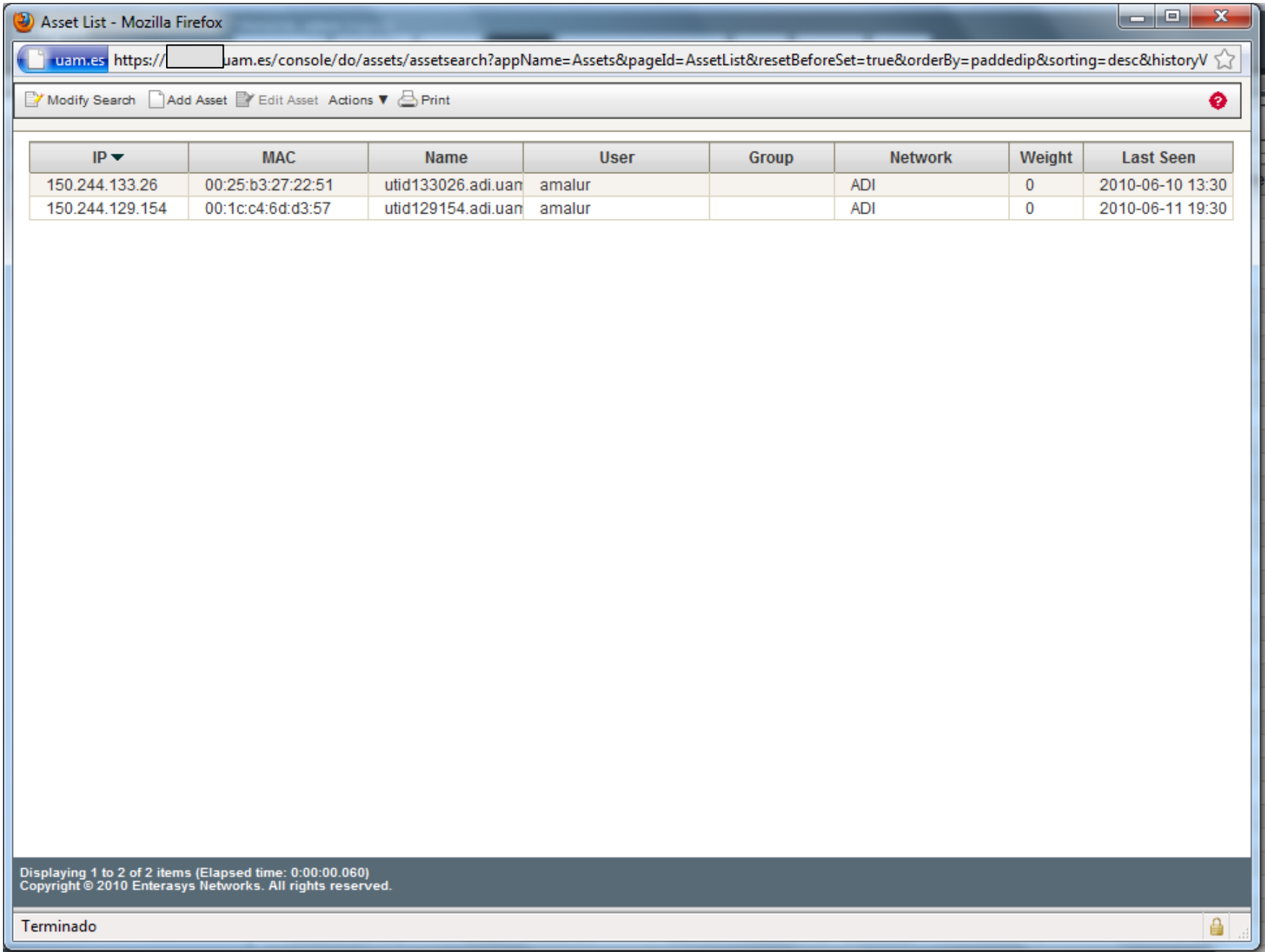
Inbound Bytes
3.0 GB (52.0 MB/s)

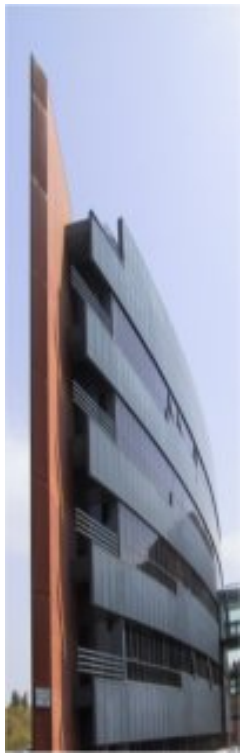


Outbound Bytes
2.6 GB (44.8 MB/s)



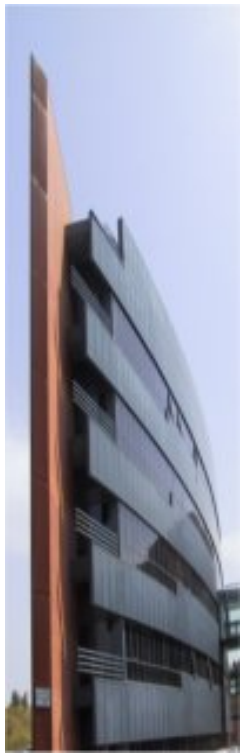

Asset Profile - Mozilla Firefox
https://utid129154.adi.uam.es/console/do/vis/hostprofile?newwindow=true&dispatch=view&ipAddress=150.244.129.154
Asset Profile
Ports
History
Name
Description
IP Address
150.244.129.154
VA Risk Level
0
Operating System
How Threatening
0
Host Name (DNS Name)
utid129154.adi.uam.es
How Threatened
0
Asset Weight
0 - Not Important
MAC
00:1c:c4:6d:d3:57
Host Name
utid129154.adi.uam.es
Machine Name
150.244.129.154
User Name
amalur
User Group
Extra Data
Save Changes
Cancel
Port
Service
OSVDB ID
Name
Description
Risk / Severity
Last Seen
First Seen
139
1
2010-05-18 15:30:07 (Passive)
2010-04-16 18:15:05 (Passive)
445
1
2010-05-18 15:30:07 (Passive)
2010-04-16 18:15:05 (Passive)
15000
1
2009-09-23 00:00:06 (Passive)
2009-09-23 00:00:06 (Passive)
Copyright © 2010 Enterasys Networks. All rights reserved.
Terminado
Preferences
Help
Network
Weight
150.244.134.175
00:23:7d:4e:8b:e4
utid134175.adi.uam.es
biblioteca
ADI
Displaying 1 to 40 of 3855 items (Elapsed time: 0:00:02.549)
Page: 1
Go


Asset List - Mozilla Firefox
uam.es https://[redacted]uam.es/console/do/assets/assetsearch?appName=Assets&pageId=AssetList&resetBeforeSet=true&orderBy=paddedip&sorting=desc&historyV
Modify Search
Add Asset
Edit Asset
Actions
Print
IP
MAC
Name
User
Group
Network
Weight
Last Seen
150.244.133.26
00:25:b3:27:22:51
utid133026.adi.uan
amalur
ADI
0
2010-06-10 13:30
150.244.129.154
00:1c:c4:6d:d3:57
utid129154.adi.uan
amalur
ADI
0
2010-06-11 19:30
Displaying 1 to 2 of 2 items (Elapsed time: 0:00:00.060)
Copyright © 2010 Enterasys Networks. All rights reserved.
Terminado
Preferences
Help
Weight
Displaying 1 to 40 of 3855 items (Elapsed time: 0:00:02.549)
Page: 1
Go
<<
1 | 2 |



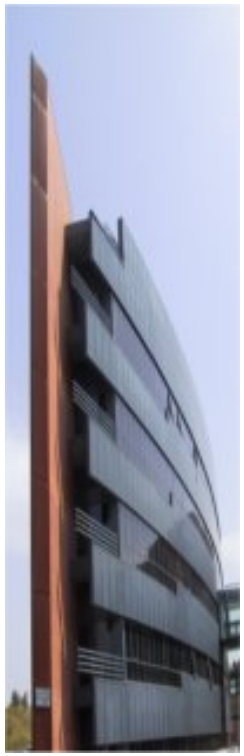
Puntos débiles

- En dispositivos no soportados, no correla, solo almacena.
- Dar soporte a un dispositivo no soportado se puede hacer pero no es trivial.
- Es una herramienta algo rígida.
- No esta pensada para interactuar con otras herramientas.



Puntos débiles

- Exportar información es poco practico.
- La gestión de listas blancas y negras es mejorable.
- En las acciones solo puedes usar como parámetro la IP.



Implantacion actual

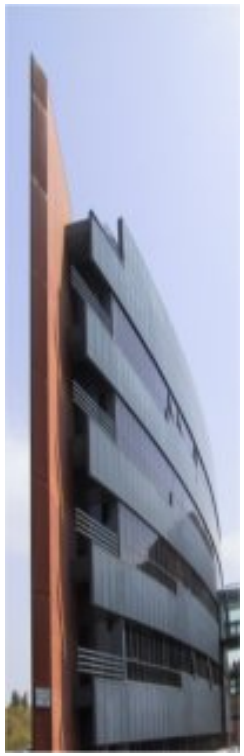
- Dispositivos integrados:

  Firewalls, IDS, DHCP, Wifi, VPN, Netflow, FDR, Radius (Accounting), Linux, ACLs, Antivirus, Directorio Activo.

- Por integrar:

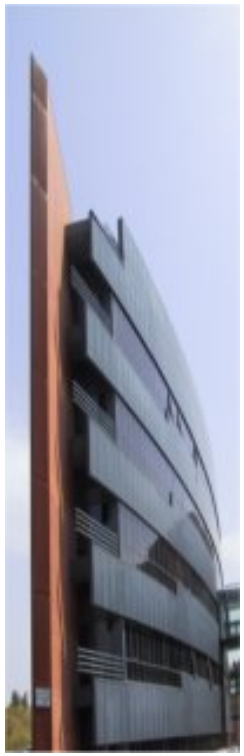
  Servidores Web, BBDD, Electronica de Red, DNS, Servidores correo, Proxy

- En proceso de Integración con sistema de cuarentena.



Nivel de satisfacción

- Estamos satisfechos con SIEM.
- Aporta mucha visibilidad.
- Más eficacia y eficiencia en la detección.
- Más detección = más trabajo
- Desarrollo del sistema de cuarentena.



Muchas Gracias