CounterSnipe – Network Security

- Welcome
- Amar Rathore

CounterSnipe™

CounterSnipe – Company

- Founded 2012 – Delaware LLC
- HQ – Boston US
- Sales/Logistics: Boston, London, Geneva, Denmark, New Delhi
- Privately funded and managed with no debt
- Strong on technology and technical support
- SCMagazine 4/5 Star

CounterSnipe™

Customers

CounterSnipe™

CounterSnipe

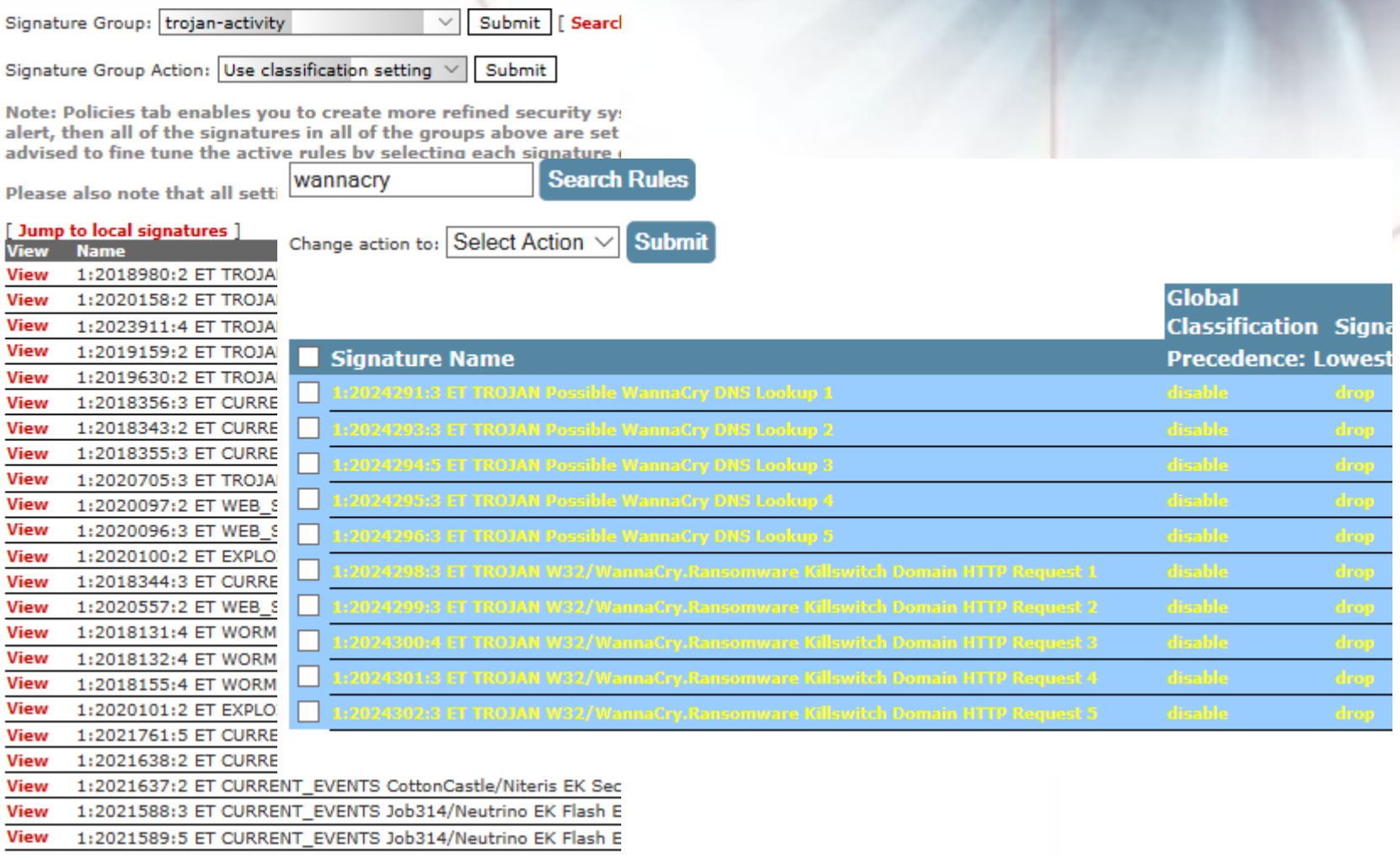
Single Suite of IDS/IPS software offers;

- Malware Prevention
- **Intrusion Detection and Prevention (IDS/IPS)**
- small Data Loss Prevention with forensics
- Automated Asset Discovery
- Active Port Scanning - manual or scheduled
- End Point Discovery and blocking
- Event correlation and Alert Management
- Firewall with quick management interface

http://countersnipe.com/index.php/ids-ips-explained

CounterSnipe™

CounterSnipe – Malware Prevention

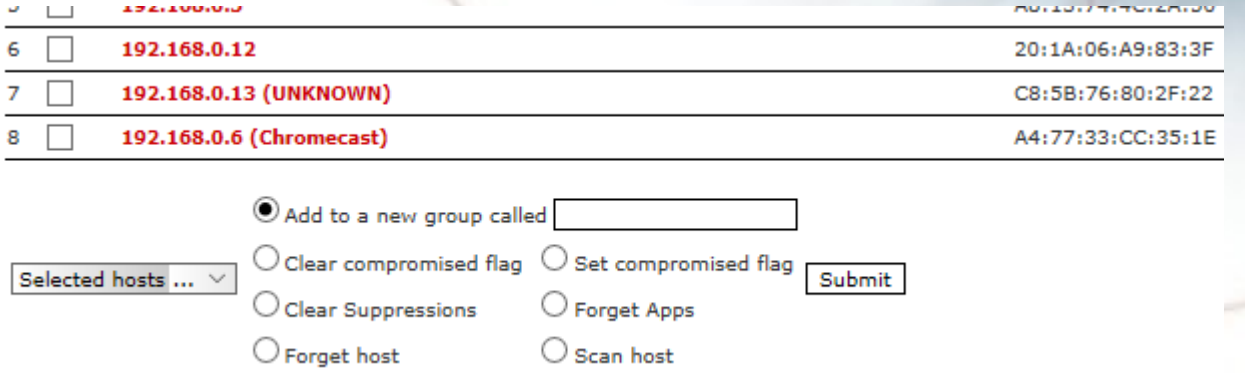


CounterSnipe™

CounterSnipe – dlp (file extraction and control)

- Alert on files with jpg or bmp extensions
- Store all files with jpg or pdf extension.
- Store all PDF files, regardless of their name.
- Unusually short file
- Simply store all files we encounter, no alerts.
- Store all JPG files, don't alert.
- Store all Windows executables
- Alert on PNG with 1x1 pixels (tracking)
- Alert on GIT with 1x1 pixels (tracking)
- Alert and store pdf attachment but not pdf file
- Alert and store files over SMTP

CounterSnipe – Automated Asset(End Points) discovery



6	☐	192.168.0.12	20:1A:06:A9:83:3F
7	☐	192.168.0.13 (UNKNOWN)	C8:5B:76:80:2F:22
8	☐	192.168.0.6 (Chromecast)	A4:77:33:CC:35:1E

Selected hosts ...

◉ Add to a new group called

○ Clear compromised flag ○ Set compromised flag

○ Clear Suppressions ○ Forget Apps

○ Forget host ○ Scan host

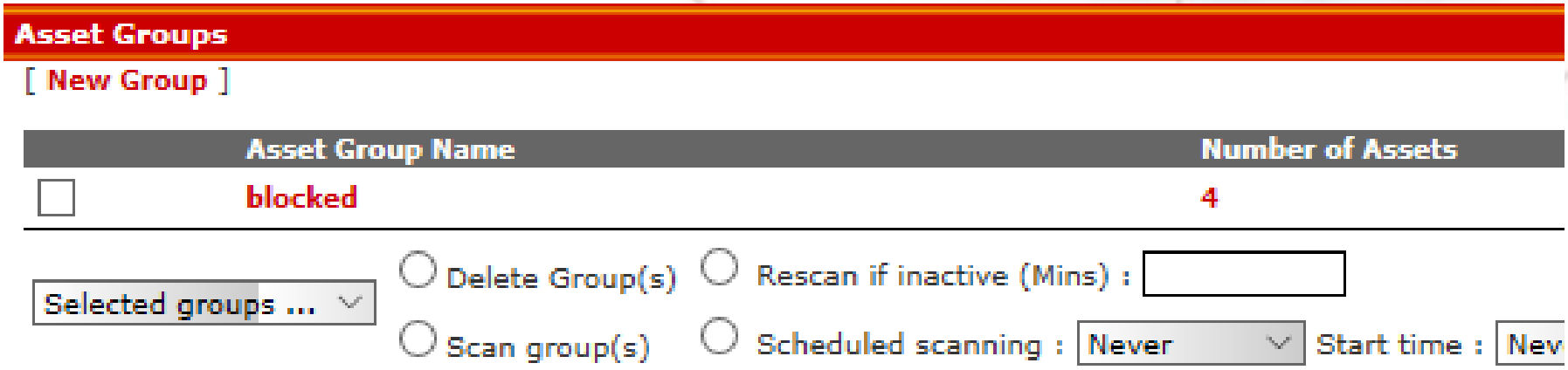
Submit

Apps	Remotely-Exploitable Vulnerabilities
2	
1	
2	
3	
3	

Discovered	Last Seen...
2017-05-19 17:37:07	2017-05-19 18:01:5
2017-05-19 17:24:18	2017-05-19 18:01:4
2017-05-19 17:25:11	2017-05-19 18:00:1
2017-05-19 17:24:41	2017-05-19 17:59:0

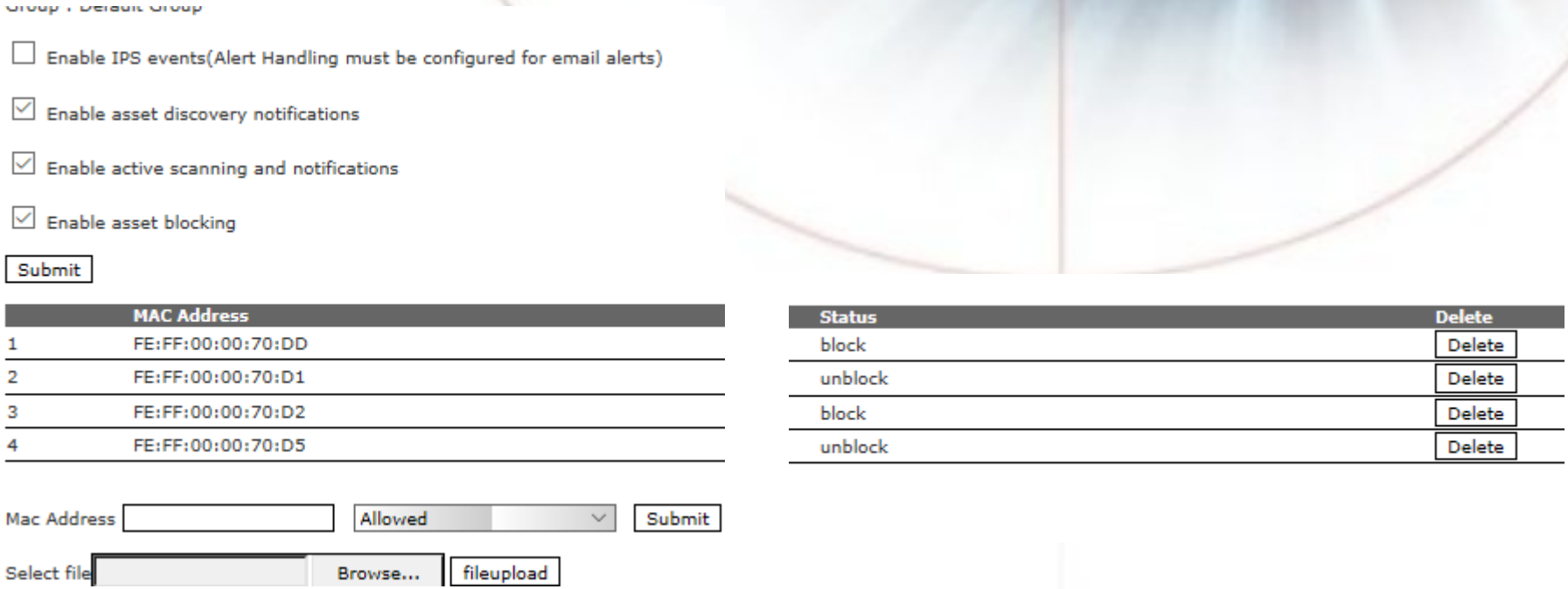
CounterSnipe™

CounterSnipe – Port Scanning



CounterSnipe™

CounterSnipe – End Point Discovery and blocking



CounterSnipe™

CounterSnipe – Alert Management

Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature for Host	Reactivate
high	☑	☐	☐	0
medium	☐	☑	☐	0
low	☐	☐	☐	0

Class B Alerts

From the standpoint of the destination host, these are alerts for which **all** of the criteria list

- SAK has identified a known asset
- SAK has identified open ports
- SAK has detected an active attack targetted at the open ports

Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature for Host	Reactivate
high	☑	☐	☑	0
medium	☐	☐	☐	0
low	☐	☐	☐	0

Class C Alerts

From the standpoint of the destination host, these are alerts for which **any** of the criteria lis

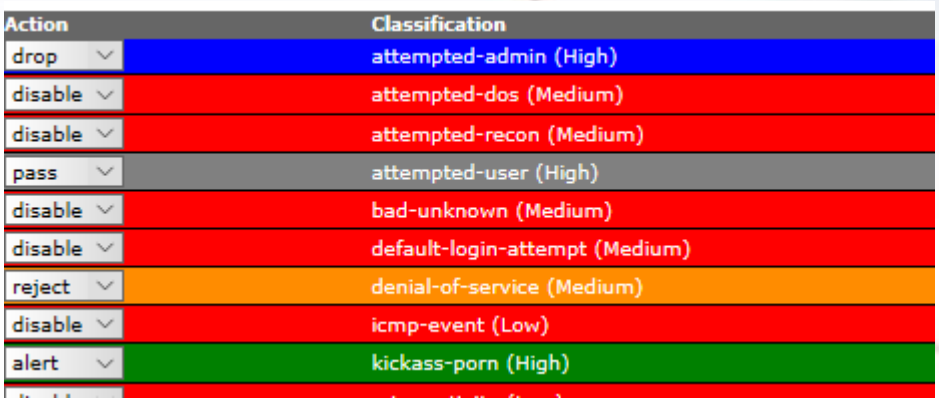
Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature for Host	Reactivate
high	☑	☐	☑	0
medium	☐	☐	☐	0
low	☐	☐	☐	0

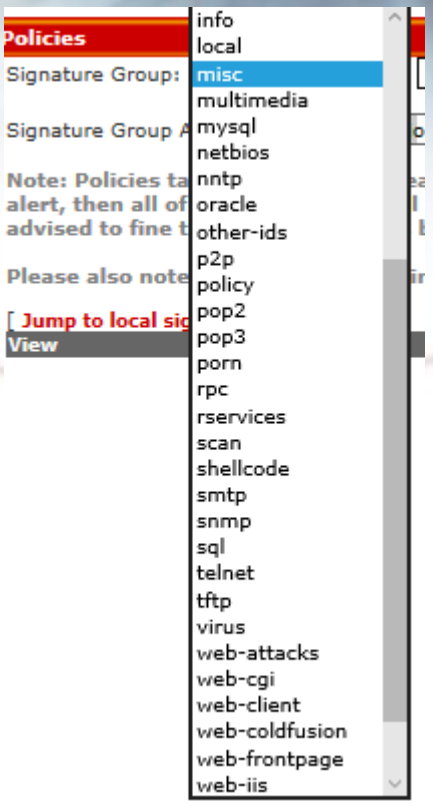
Submit

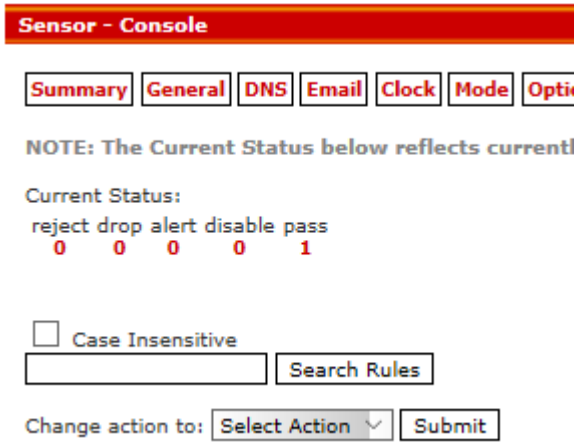
Elapsed Time	Number of Events	Threshold
Last 5 mins	0	
Last hour	0	
Last day	0	

CounterSnipe™

CounterSnipe – Intrusion Prevention







CounterSnipe™

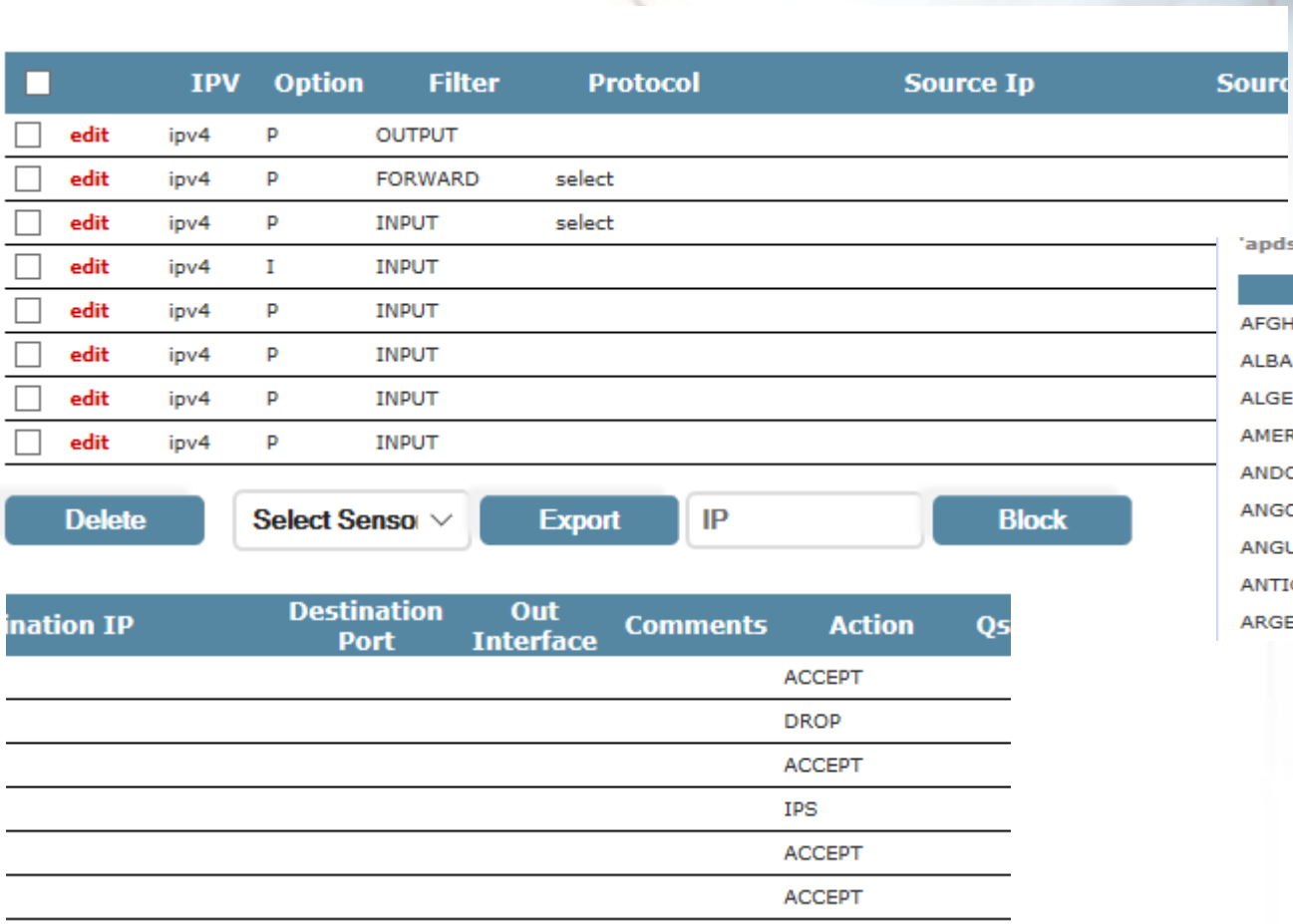
CounterSnipe – V10 whats new

- One click baseline creation for Automated Easy Configuration – take guessing out of security
- Enhanced rule management – timely auto deployment of latest rules
- 100% control over IPS selection
- New firewall management interface
- Enhanced Asset search utility
- Bespoke application additions

CounterSnipe™

CounterSnipe – V10 whats new

Firewall with quick management interface



		IPV	Option	Filter	Protocol	Source Ip	Sourc
☐	edit	ipv4	P	OUTPUT			
☐	edit	ipv4	P	FORWARD	select		
☐	edit	ipv4	P	INPUT	select		
☐	edit	ipv4	I	INPUT			
☐	edit	ipv4	P	INPUT			
☐	edit	ipv4	P	INPUT			
☐	edit	ipv4	P	INPUT			
☐	edit	ipv4	P	INPUT			

Delete | Select Senso | Export | IP | Block

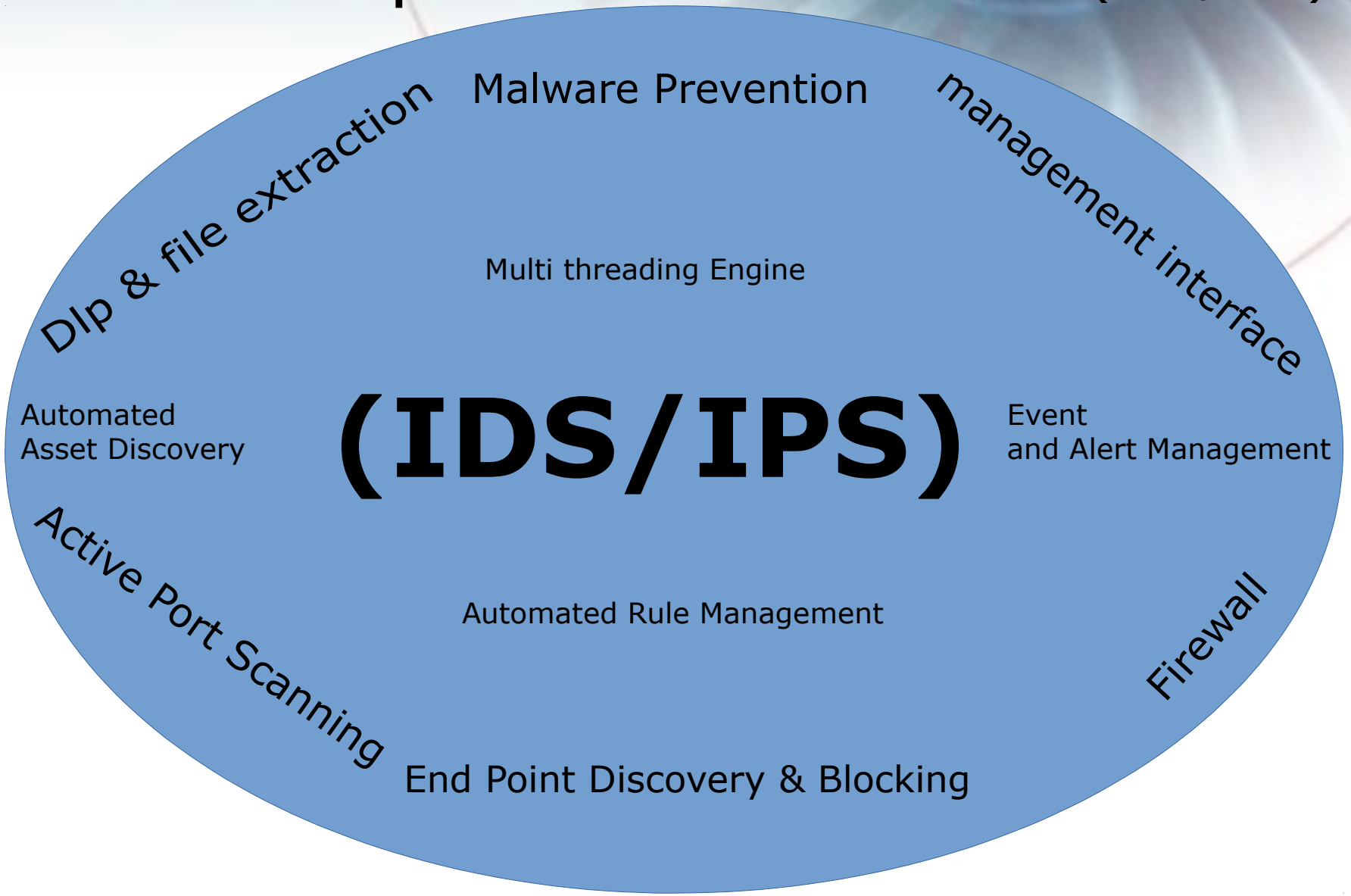
ination IP	Destination Port	Out Interface	Comments	Action	Qs
				ACCEPT	
				DROP	
				ACCEPT	
				IPS	
				ACCEPT	
				ACCEPT	

'apdsetup' at the backend(console) and then you will see

Country Name	Action
AFGHANISTAN	☐ Block
ALBANIA	☐ Block
ALGERIA	☐ Block
AMERICAN SAMOA	☐ Block
ANDORRA	☐ Block
ANGOLA	☐ Block
ANGUILLA	☐ Block
ANTIGUA AND BARBUDA	☐ Block
ARGENTINA	☐ Block

CounterSnipe™

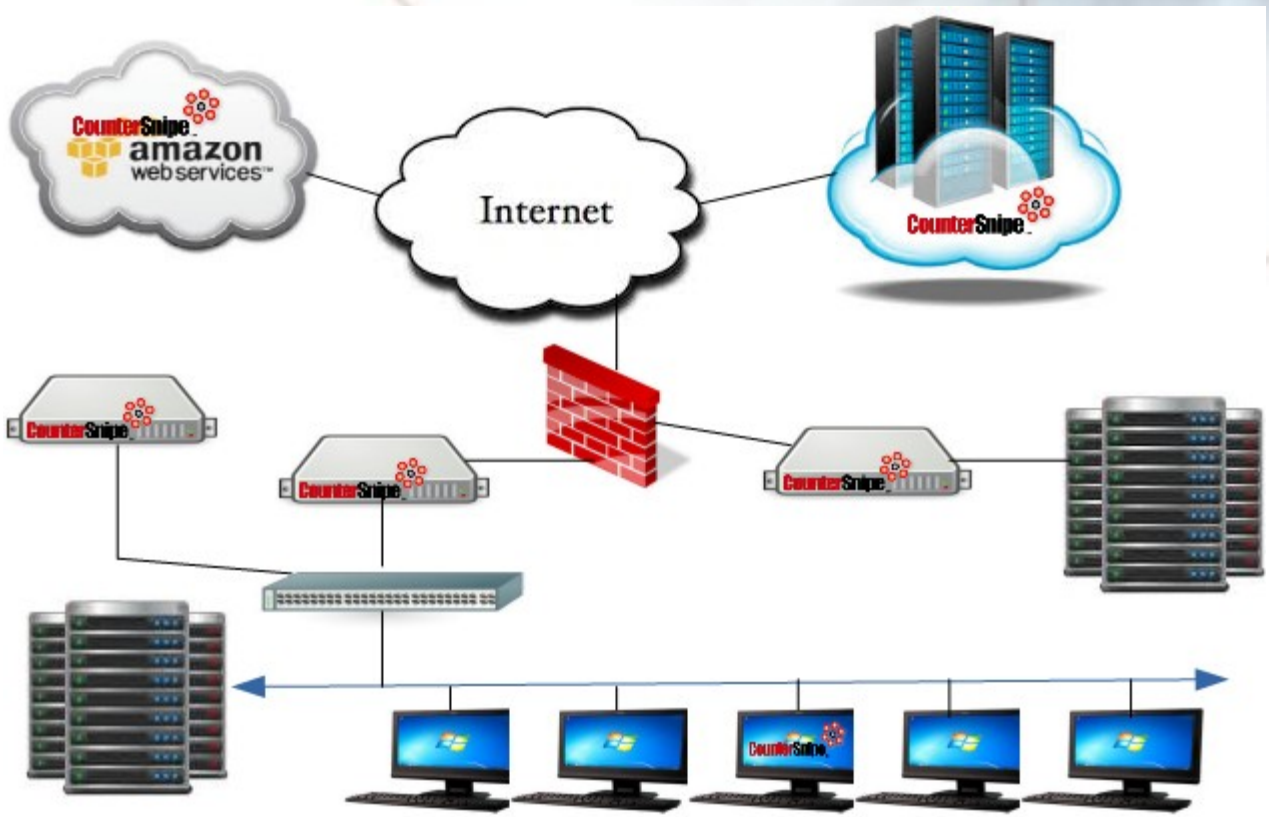
CounterSnipe – Intrusion Prevention (IDS/IPS)



CounterSnipe ™

CounterSnipe – Integrating into any infrastructure

Server | Desktop | Cloud | VM | Online | Inline



CounterSnipe™

CounterSnipe – Getting it going

- Licensing
  - Perpetual
    - One off cost based on number of end points
    - Yearly maintenance and support costs
  - Yearly Subscription
    - 3-5 year contract with yearly payments.
  - MSPP
    - Monthly subscription license
    - Available via Managed Service Provider Partners(MSPP)

CounterSnipe – Getting it going

- Physical Hardware or VMs
  - Ubuntu 14.04 LTS (supported until 2019)
  - Ubuntu 16.04 LTS available from 2017
  - Remote server based installation
  - 3 step initial configuration

- Certified Hardware

http://www.ubuntu.com/certification/server/

Any no label hardware will work just as well.

CounterSnipe – Security Management

How to buy

- Contact our international partner in your country
- Contact sales@countersnipe.com

Thank You

CounterSnipe™

CounterSnipe – Network Security

Demo

CounterSnipe™