

CounterSnipe – Network Security

- Welcome
- Amar Rathore

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

Customers

CAPITA



Intercontinental

BANK

A Subsidiary of Access Bank Plc



MAERSK



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 – Malware Prevention

Signature Group: [Search]

Signature Group Action:

Note: Policies tab enables you to create more refined security sy:
alert, then all of the signatures in all of the groups above are set
advised to fine tune the active rules by selecting each signature

Please also note that all setti

[Jump to local signatures]

Change action to:

- [View](#) 1:2018980:2 ET TROJA
- [View](#) 1:2020158:2 ET TROJA
- [View](#) 1:2023911:4 ET TROJA
- [View](#) 1:2019159:2 ET TROJA
- [View](#) 1:2019630:2 ET TROJA
- [View](#) 1:2018356:3 ET CURRE
- [View](#) 1:2018343:2 ET CURRE
- [View](#) 1:2018355:3 ET CURRE
- [View](#) 1:2020705:3 ET TROJA
- [View](#) 1:2020097:2 ET WEB_5
- [View](#) 1:2020096:3 ET WEB_5
- [View](#) 1:2020100:2 ET EXPLO
- [View](#) 1:2018344:3 ET CURRE
- [View](#) 1:2020557:2 ET WEB_5
- [View](#) 1:2018131:4 ET WORM
- [View](#) 1:2018132:4 ET WORM
- [View](#) 1:2018155:4 ET WORM
- [View](#) 1:2020101:2 ET EXPLO
- [View](#) 1:2021761:5 ET CURRE
- [View](#) 1:2021638:2 ET CURRE
- [View](#) 1:2021637:2 ET CURRENT_EVENTS CottonCastle/Niteris EK Sec
- [View](#) 1:2021588:3 ET CURRENT_EVENTS Job314/Neutrino EK Flash E
- [View](#) 1:2021589:5 ET CURRENT_EVENTS Job314/Neutrino EK Flash E

<input type="checkbox"/> Signature Name	Global Classification	Signature Precedence: Lowest
<input type="checkbox"/> 1:2024291:3 ET TROJAN Possible WannaCry DNS Lookup 1	disable	drop
<input type="checkbox"/> 1:2024293:3 ET TROJAN Possible WannaCry DNS Lookup 2	disable	drop
<input type="checkbox"/> 1:2024294:3 ET TROJAN Possible WannaCry DNS Lookup 3	disable	drop
<input type="checkbox"/> 1:2024295:3 ET TROJAN Possible WannaCry DNS Lookup 4	disable	drop
<input type="checkbox"/> 1:2024296:3 ET TROJAN Possible WannaCry DNS Lookup 5	disable	drop
<input type="checkbox"/> 1:2024298:3 ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1	disable	drop
<input type="checkbox"/> 1:2024299:3 ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2	disable	drop
<input type="checkbox"/> 1:2024300:4 ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3	disable	drop
<input type="checkbox"/> 1:2024301:3 ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4	disable	drop
<input type="checkbox"/> 1:2024302:3 ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 5	disable	drop

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

<input type="checkbox"/>	192.168.0.10	08:15:77:7C:2A:50
6	<input type="checkbox"/> 192.168.0.12	20:1A:06:A9:83:3F
7	<input type="checkbox"/> 192.168.0.13 (UNKNOWN)	C8:5B:76:80:2F:22
8	<input type="checkbox"/> 192.168.0.6 (Chromecast)	A4:77:33:CC:35:1E

Add to a new group called
 Clear compromised flag Set compromised flag
 Clear Suppressions Forget Apps
 Forget host Scan host

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 – Port Scanning

Asset Groups

[[New Group](#)]

	Asset Group Name	Number of Assets
<input type="checkbox"/>	blocked	4

Selected groups ... ▾

Delete Group(s)

Rescan if inactive (Mins) :

Scan group(s)

Scheduled scanning : Start time :

CounterSnipe – End Point Discovery and blocking

Group : Default Group

- Enable IPS events(Alert Handling must be configured for email alerts)
- Enable asset discovery notifications
- Enable active scanning and notifications
- Enable asset blocking

	MAC Address
1	FE:FF:00:00:70:DD
2	FE:FF:00:00:70:D1
3	FE:FF:00:00:70:D2
4	FE:FF:00:00:70:D5

Mac Address

Select file

Status	Delete
block	<input type="button" value="Delete"/>
unblock	<input type="button" value="Delete"/>
block	<input type="button" value="Delete"/>
unblock	<input type="button" value="Delete"/>

CounterSnipe – Alert Management

Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature for Host	Reactivate
high	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
medium	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Class C Alerts

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

Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature for Host	Reactivate
high	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Elapsed Time	Number of Events	Threshold
Last 5 mins	0	<input type="text"/>
Last hour	0	<input type="text"/>
Last day	0	<input type="text"/>

CounterSnipe – Intrusion Prevention

Action	Classification
drop	attempted-admin (High)
disable	attempted-dos (Medium)
disable	attempted-recon (Medium)
pass	attempted-user (High)
disable	bad-unknown (Medium)
disable	default-login-attempt (Medium)
reject	denial-of-service (Medium)
disable	icmp-event (Low)
alert	kickass-porn (High)

Policies

Signature Group: misc

Signature Group A

Note: Policies to alert, then all of advised to fine t

Please also note

[Jump to local sig

View

- info
- local
- misc
- multimedia
- mysql
- netbios
- nntp
- oracle
- other-ids
- p2p
- policy
- pop2
- pop3
- porn
- rpc
- rservices
- scan
- shellcode
- smtp
- snmp
- sql
- telnet
- tftp
- virus
- web-attacks
- web-cgi
- web-client
- web-coldfusion
- web-frontpage
- web-iis

Sensor - Console

Summary General DNS Email Clock Mode Opti

NOTE: The Current Status below reflects current

Current Status:
reject drop alert disable pass
0 0 0 0 1

Case Insensitive

Search Rules

Change action to: Submit

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 – V10 whats new

Firewall with quick management interface

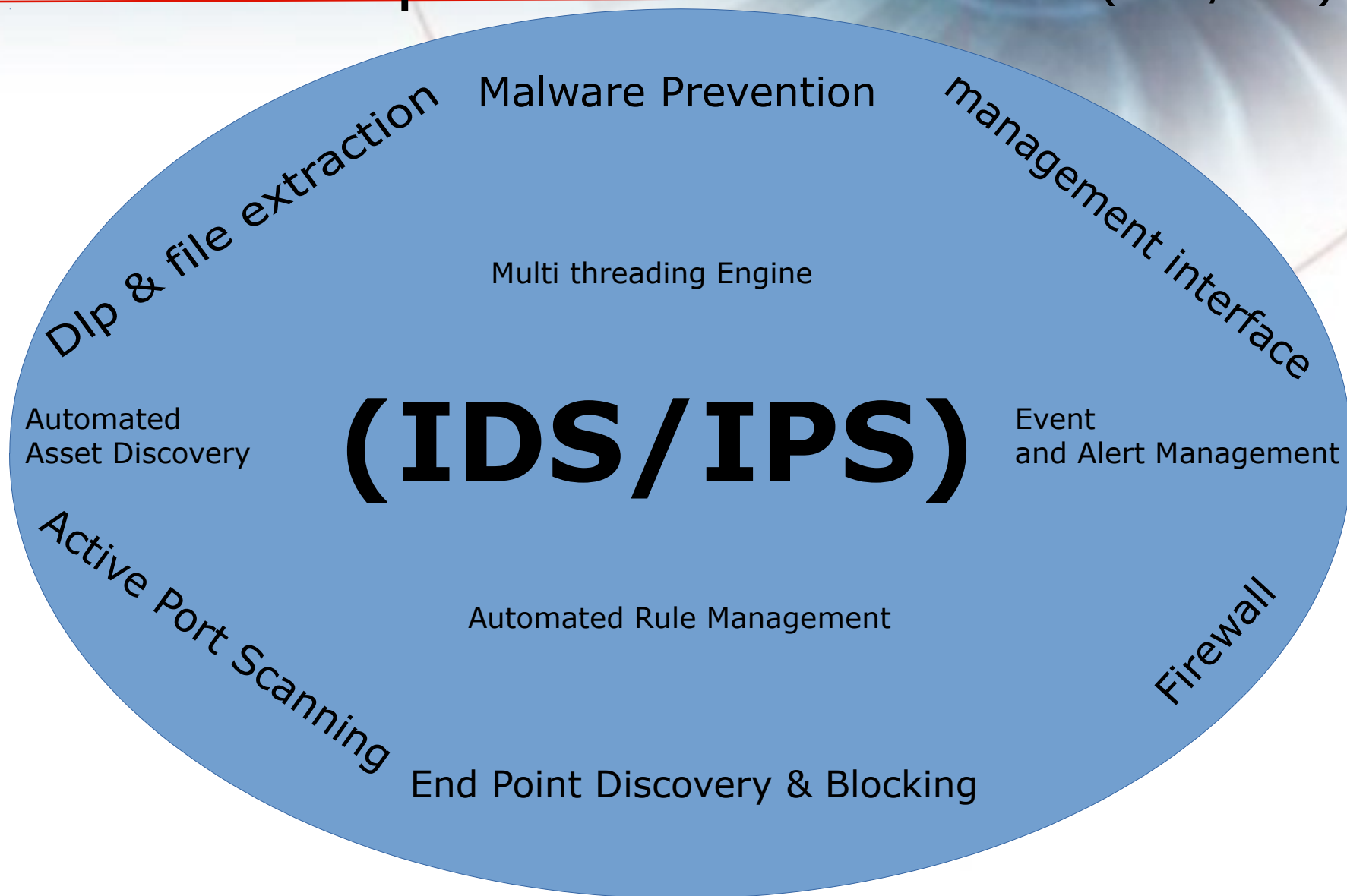
<input type="checkbox"/>		IPV	Option	Filter	Protocol	Source Ip	Source
<input type="checkbox"/>	edit	ipv4	P	OUTPUT			
<input type="checkbox"/>	edit	ipv4	P	FORWARD	select		
<input type="checkbox"/>	edit	ipv4	P	INPUT	select		
<input type="checkbox"/>	edit	ipv4	I	INPUT			
<input type="checkbox"/>	edit	ipv4	P	INPUT			
<input type="checkbox"/>	edit	ipv4	P	INPUT			
<input type="checkbox"/>	edit	ipv4	P	INPUT			
<input type="checkbox"/>	edit	ipv4	P	INPUT			

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

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

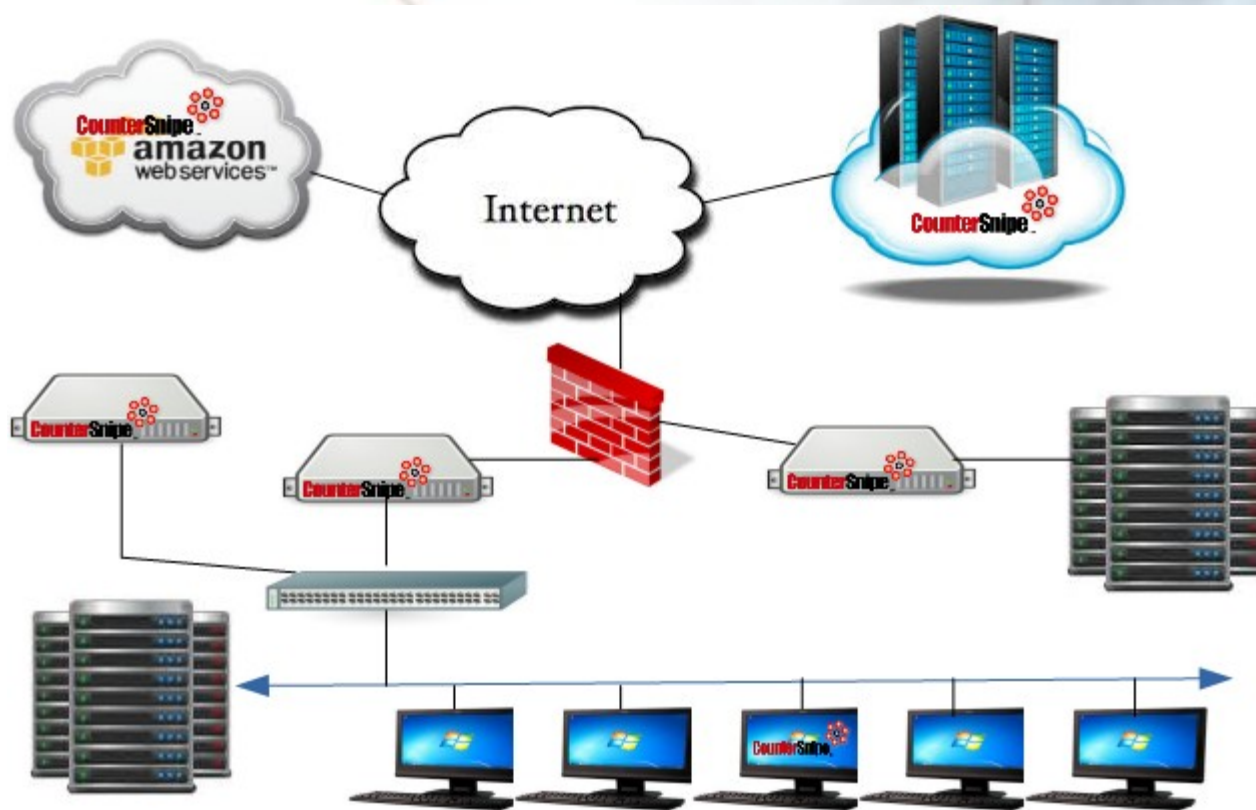
Country Name	Action
AFGHANISTAN	<input type="checkbox"/> Block
ALBANIA	<input type="checkbox"/> Block
ALGERIA	<input type="checkbox"/> Block
AMERICAN SAMOA	<input type="checkbox"/> Block
ANDORRA	<input type="checkbox"/> Block
ANGOLA	<input type="checkbox"/> Block
ANGUILLA	<input type="checkbox"/> Block
ANTIGUA AND BARBUDA	<input type="checkbox"/> Block
ARGENTINA	<input type="checkbox"/> Block

CounterSnipe – Intrusion Prevention (IDS/IPS)



CounterSnipe – Integrating into any infrastructure

Server | Desktop | Cloud | VM | Online | Inline



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 – Network Security

 **Demo**