Conquering The IDS Alert Challenge With Splunk

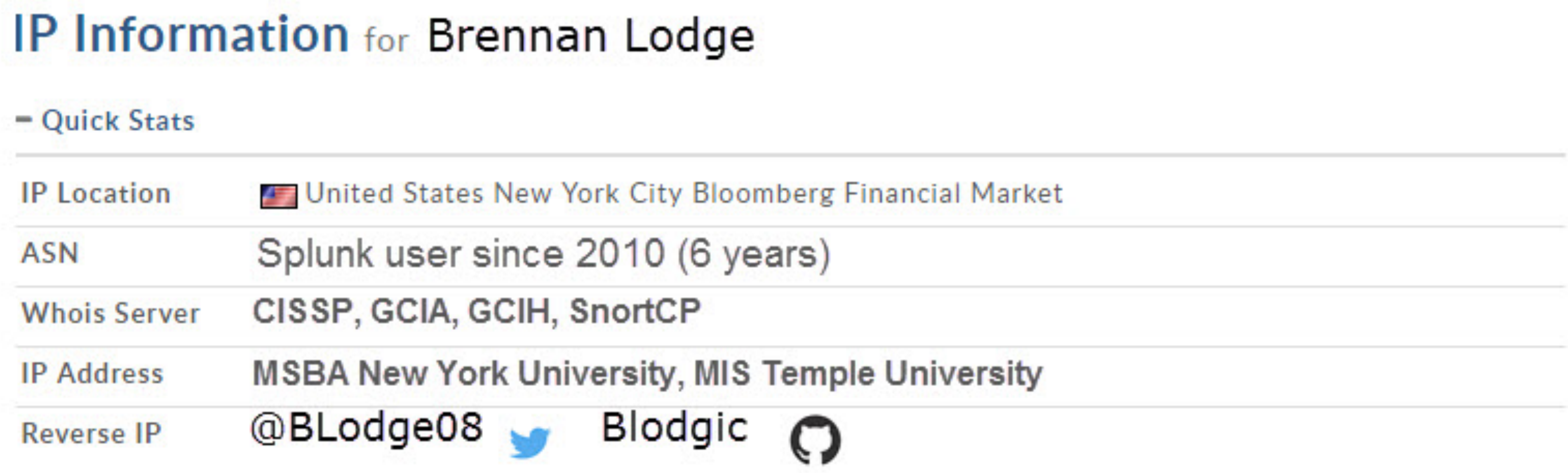
Brennan Lodge

Cyber Security Analyst, Bloomberg LP

.conf2016

splunk>

Whois Lookup



IP Information for Brennan Lodge

− Quick Stats

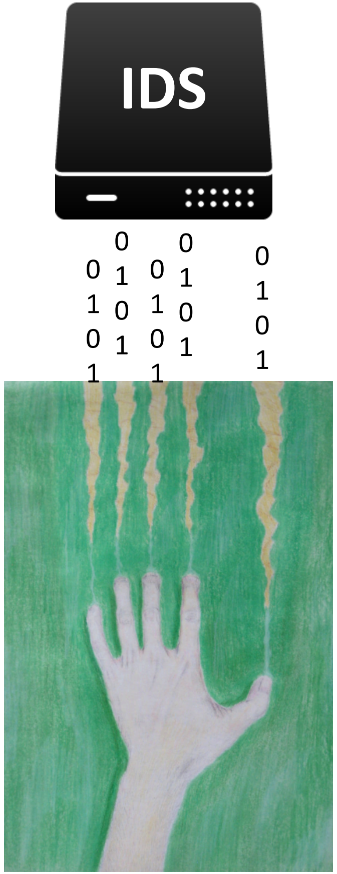
IP Location	🇺🇸 United States New York City Bloomberg Financial Market
ASN	Splunk user since 2010 (6 years)
Whois Server	CISSP, GCIA, GCIH, SnortCP
IP Address	MSBA New York University, MIS Temple University
Reverse IP	@BLodge08 Blodgic

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

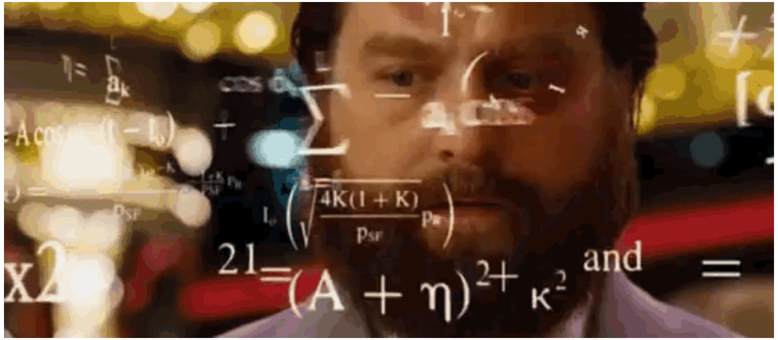
The Challenge

- Intrusion Detection Systems Alerts
- Few analysts to triage IDS alerts + every other security log to review
- IDS alerts are influx
- Many, many, many false positive alerts = noise
- However IDS is a huge value add to the success of a information security program
- MUST be managed accordingly



IDS By The Numbers

- A basic install of snort with community and open source Emerging Threat signatures comes with **20,000 + IDS rules**
- There are **50+ categories** of rules
- There are **25+ class types** of rules
- With snort sensor sitting on the perimeter of an Amazon EC2 instance the average count per day for a months time, alerts fired on average **585 times per day**



Why Throw IDS At Splunk

- IDS – notifies analysts of cyber security attacks in progress
- Goal of IDS – 100% accuracy and 0% false positives
  - You don't want your IDS to cry wolf
  - You don't want to let attacks pass undetected
  - Correlate attacks
  - Provide context to analysts on an attack
  - Find evil
  - Let Splunk do all of this for you!

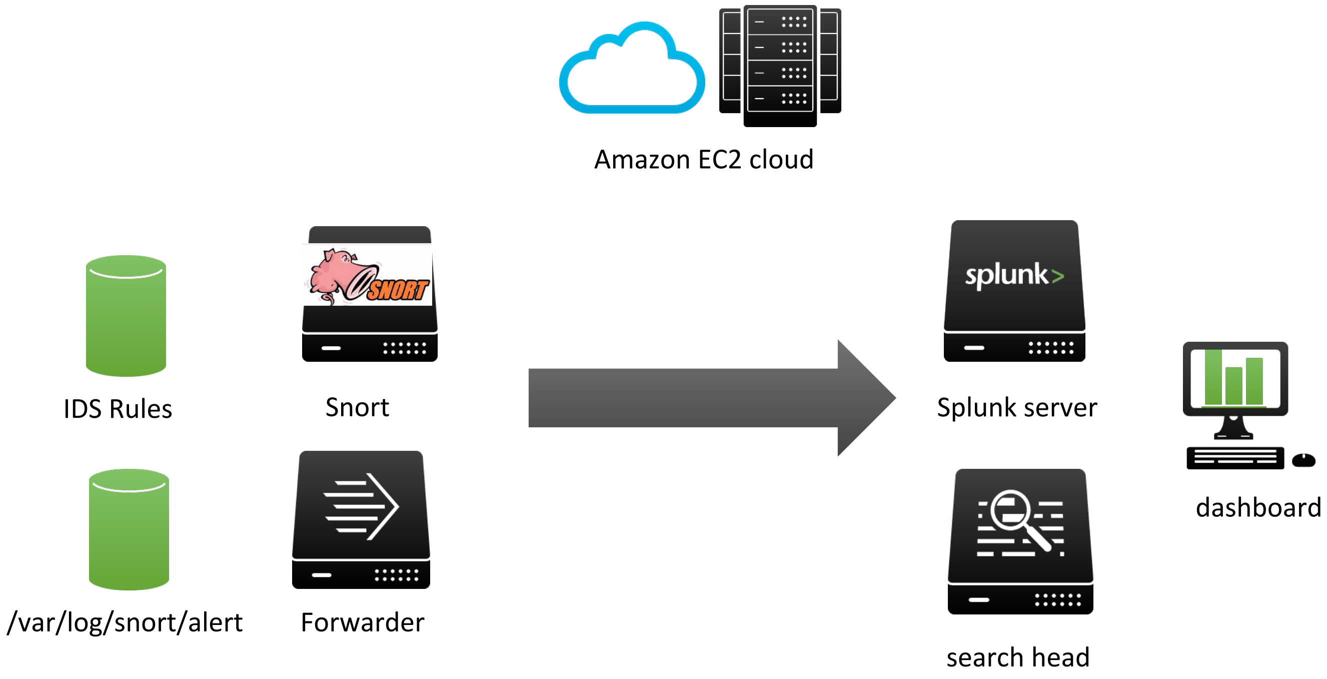
#Winning With IDS & Splunk

- IDS + Splunk allows for the following wins:
- IDS complements the security controls in an organization
- Splunk complements all the logs collected from the security controls in an organization
- Splunk allows the flexibility to correlate the IDS logs + the IDS signatures = analyst context for triaging an event which may lead to an incident and escalation
- Dashboards Dashboards Dashboards

Agenda

- The Research Environment Diagram
- Understand Your Rules And Alerts
- Breaking Down And Understanding Your Signatures
- The IDS Dashboard
- Anomaly Detection
- Continue To Tune
- Questions

Research Environment



Amazon EC2 cloud

IDS Rules

Snort

/var/log/snort/alert

Forwarder

Splunk server

search head

dashboard

Understand Your Rules And Alerts

- Help better understand your environment
- Know which IDS alerts to tune out
- Know who is attacking you
- Know which IDS sensors are generating the greatest / least amount of traffic
- Correlate IDS with other log sources (proxy, dns, windows logs, etc)

Make Sense Of Your Signatures

- Regex your signatures into a lookup table
- Break IDS signatures into the following categories:
  - SEIM Category, CVE, classtype, destination ip, destination port, msg, msg_type, protocol, rule_who, sid#, signature_all, source ip, source port

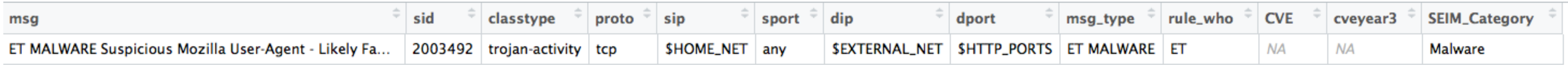
Example IDS Signature

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)"; flow:to_server,established; content:"User-Agent|3a| Mozilla/4.0|0d 0a|"; fast_pattern; nocase; http_header; content:!"/CallParrotWebClient/"; http_uri; content:!"Host|3a| www|2e|google|2e|com|0d 0a|"; nocase; http_header; content:!"Cookie|3a| PREF|3d|ID|3d|"; nocase; http_header; content:!"Host|3a 20|secure|2e|logmein|2e|com|0d 0a|"; nocase; http_header; content:!"Host|3a 20|weixin.qq.com"; http_header; nocase; content:!"Host|3a| slickdeals.net"; nocase; http_header; content:!"Host|3a| cloudera.com"; nocase; http_header; content:!"Host|3a 20|secure.digitalalchemy.net.au"; http_header; content:!".ksmobile.com|0d 0a|"; http_header; reference:url,doc.emergingthreats.net/2003492; classtype:trojan-activity; sid:2003492; rev:20;)
```

Example IDS Signature

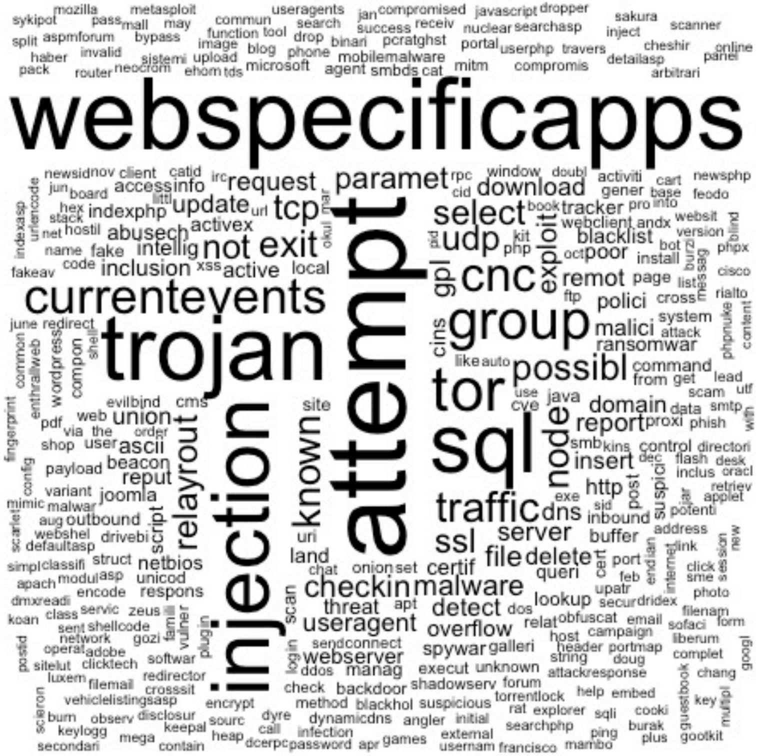
```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Suspicious
Mozilla User-Agent - Likely Fake (Mozilla/4.0)"; flow:to_server,established; content:"User-
Agent|3a| Mozilla/4.0|0d 0a|"; fast_pattern; nocase; http_header; content:!"/
CallParrotWebClient/"; http_uri; content:!"Host|3a| www|2e|google|2e|com|0d 0a|";
nocase; http_header; content:!"Cookie|3a| PREF|3d|ID|3d|"; nocase; http_header;
content:!"Host|3a 20|secure|2e|logmein|2e|com|0d 0a|"; nocase; http_header;
content:!"Host|3a 20|weixin.qq.com"; http_header; nocase; content:!"Host|3a|
slickdeals.net"; nocase; http_header; content:!"Host|3a| cloudera.com"; nocase; http_header;
content:!"Host|3a 20|secure.digitalalchemy.net.au"; http_header; content:!".ksmobile.com|0d
0a|"; http_header; reference:url,doc.emergingthreats.net/2003492; classtype:trojan-activity;
sid:2003492; rev:20;)
```

Rule Break Down



msg	sid	classtype	proto	sip	sport	dip	dport	msg_type	rule_who	CVE	cveyear3	SEIM_Category
ET MALWARE Suspicious Mozilla User-Agent - Likely Fa...	2003492	trojan-activity	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	ET MALWARE	ET	*NA*	*NA*	Malware

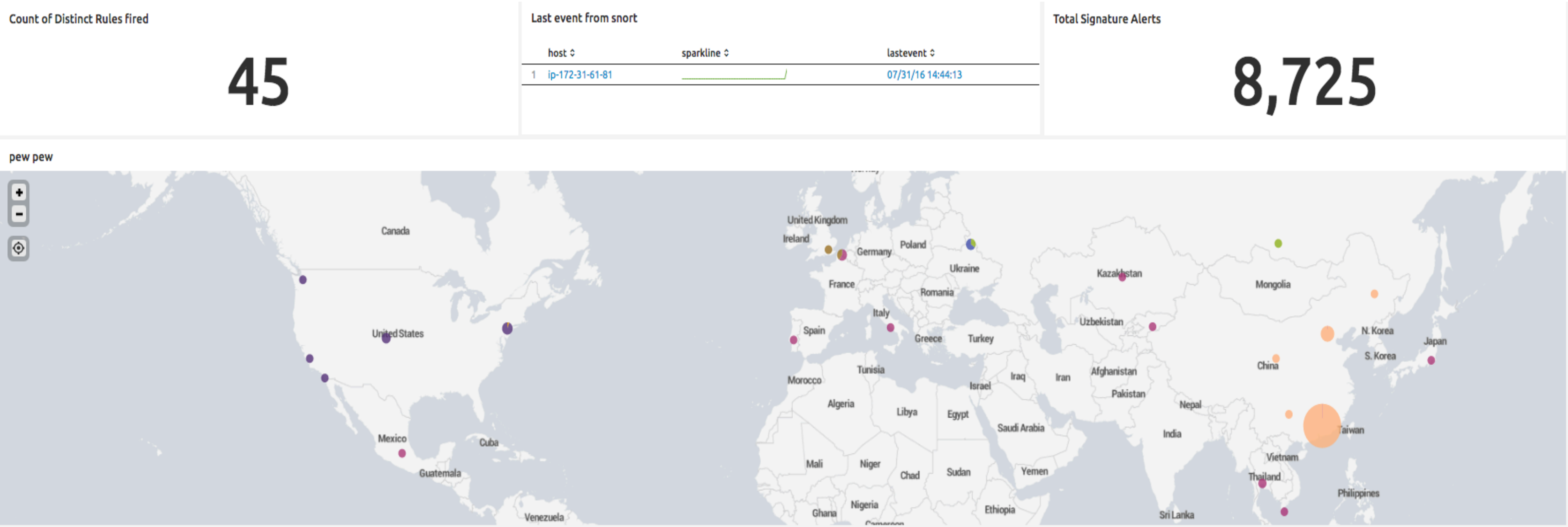
Rule Message Word Cloud



Pulling It All Together In A Splunk Dashboard

- - Distinct rule count
- - Alerts by Host
- - Total Signatures alerted
- - Signature lookup
- - The signature rollup and activity
- - Top signatures firing
- - Signatures broken out by port hits
- - Rule class distribution
- - Anomaly detection

Dashboard Break Down



Count of Distinct Rules fired

45

Last event from snort

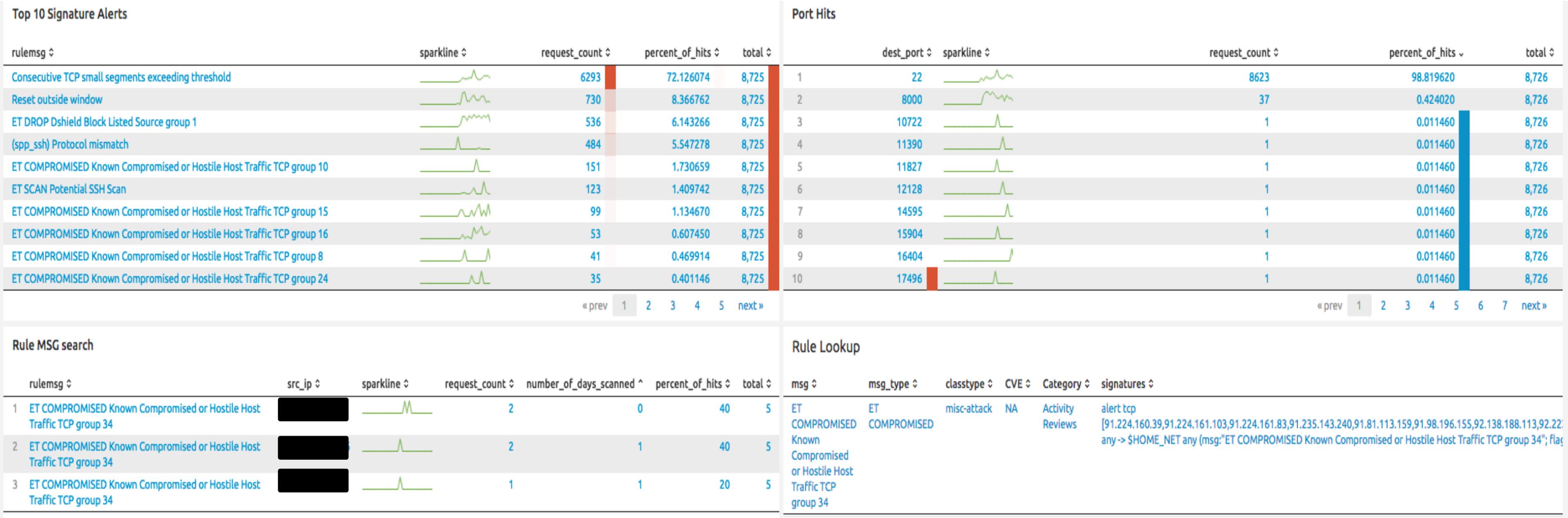
	host ⇕	sparkline ⇕	lastevent ⇕
1	ip-172-31-61-81		07/31/16 14:44:13

Total Signature Alerts

8,725

pew pew

Alerts In The Dashboard



Top 10 Signature Alerts

rulemsg	sparkline	request_count	percent_of_hits	total
Consecutive TCP small segments exceeding threshold		6293	72.126074	8,725
Reset outside window		730	8.366762	8,725
ET DROP Dshield Block Listed Source group 1		536	6.143266	8,725
(spp_ssh) Protocol mismatch		484	5.547278	8,725
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 10		151	1.730659	8,725
ET SCAN Potential SSH Scan		123	1.409742	8,725
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 15		99	1.134670	8,725
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 16		53	0.607450	8,725
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 8		41	0.469914	8,725
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 24		35	0.401146	8,725

« prev 1 2 3 4 5 next »

Port Hits

	dest_port	sparkline	request_count	percent_of_hits	total
1	22		8623	98.819620	8,726
2	8000		37	0.424020	8,726
3	10722		1	0.011460	8,726
4	11390		1	0.011460	8,726
5	11827		1	0.011460	8,726
6	12128		1	0.011460	8,726
7	14595		1	0.011460	8,726
8	15904		1	0.011460	8,726
9	16404		1	0.011460	8,726
10	17496		1	0.011460	8,726

« prev 1 2 3 4 5 6 7 next »

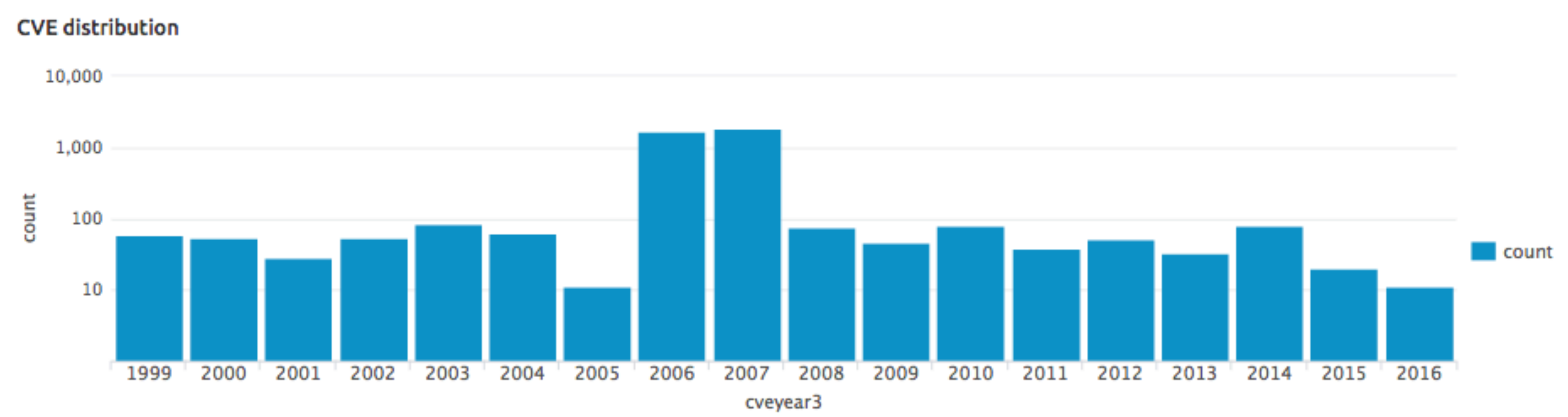
Rule MSG search

	rulemsg	src_ip	sparkline	request_count	number_of_days_scanned	percent_of_hits	total
1	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 34	[redacted]		2	0	40	5
2	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 34	[redacted]		2	1	40	5
3	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 34	[redacted]		1	1	20	5

Rule Lookup

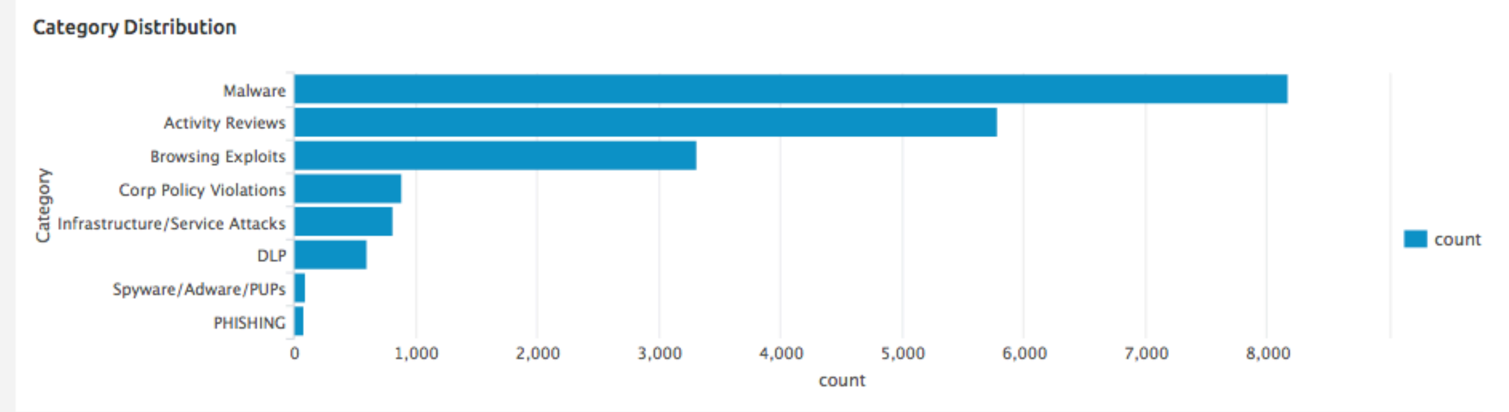
msg	msg_type	classtype	CVE	Category	signatures
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 34	ET COMPROMISED	misc-attack	NA	Activity Reviews	alert tcp [91.224.160.39,91.224.161.103,91.224.161.83,91.235.143.240,91.81.113.159,91.98.196.155,92.138.188.113,92.22 any -> $HOME_NET any (msg:"ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 34"; flag

CVE’S


CVE distribution
10,000
1,000
100
10
count
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
cveyear3
count

SEIM Category

- Malware - worm|exploit|activex|ciarmy|trojan|botcc|dshield|owned
- Activity Reviews – catch all
- Browsing Exploits - browser|plugin|flash|silverlight|java|php|internet explorer
- Corp Policy Violations – “policy”
- Infrastructure / Service Attacks – server |denial|successful-recon|network-scan|scan|sql
- DLP - ftp
- Spyware / Adware / PUPs - spware|adware|PUP
- PHISHING – “phish”



Anomaly Detection

- Anomaly Detection
- Statistical breakdown of signatures firing:
- Sparklines
- Counts
- Number of Days attackers attacking
- Correlation among other security log sources
- Top Attackers
- Baseline by Custom Category Type

The IDS Dashboard

DEMO

Continuous Tuning

- Given the results from the Dashboard anomalies you can put signatures on silent (don't appear to analysts)
- Still record in case you need to correlate an attack that was not originally identified through IDS
- Continue to measure the effectiveness of signatures
- Organize a meeting with analysts and engineers to decide on false positive alerts that should be tuned accordingly
- Correlate IDS alerts with other splunk alerts for more accurate "evil" events

THANK YOU

.conf2016

splunk>