

Michael Powell

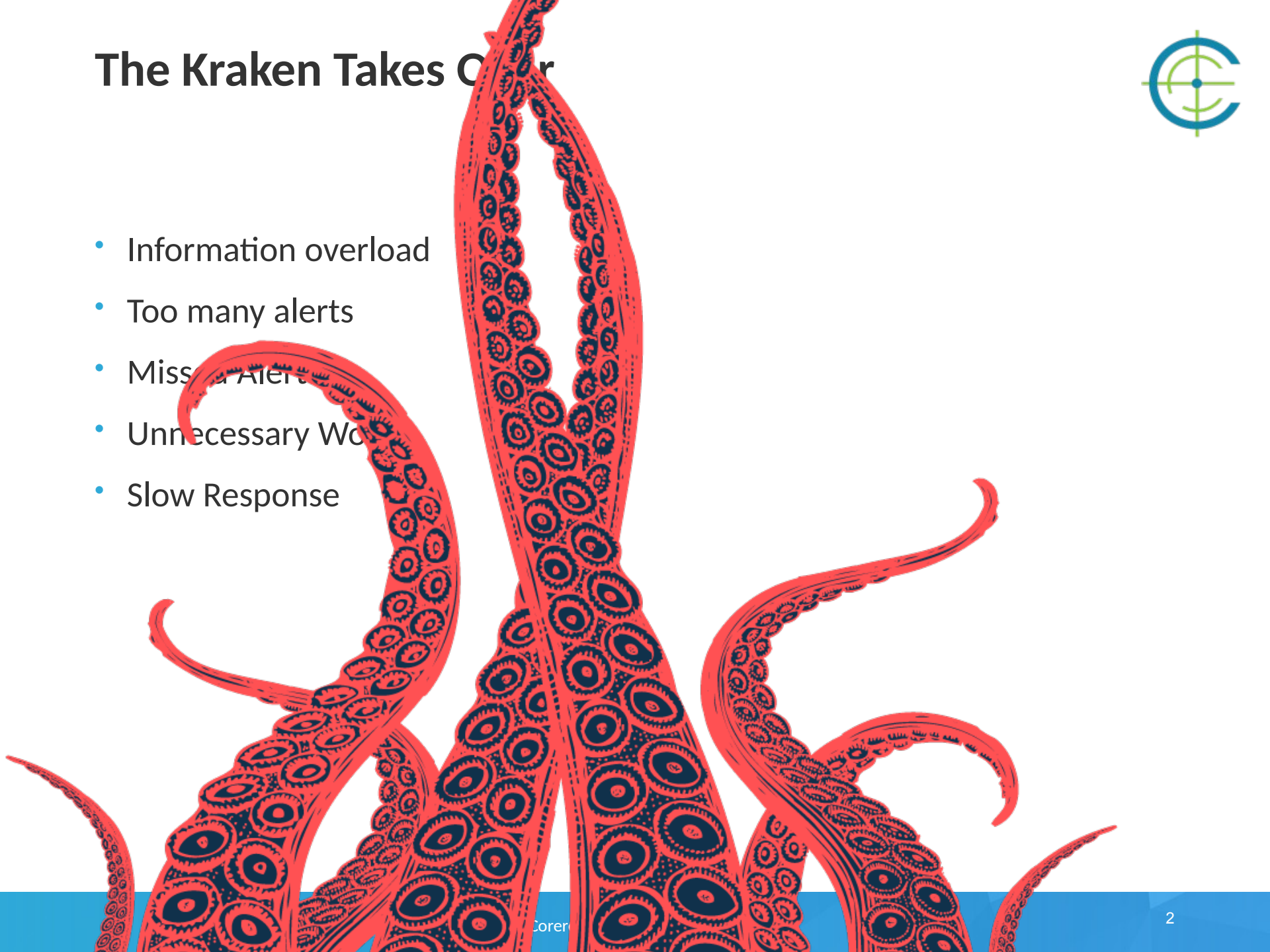
Sr. Security Engineer – Corero Network Security

## Control the Kraken: Becoming a More Efficient NOC

# The Kraken Takes Over



- Information overload
- Too many alerts
- Missed Alerts
- Unnecessary Work
- Slow Response





Or Worse  
Yet!



# What is NOC Efficiency?



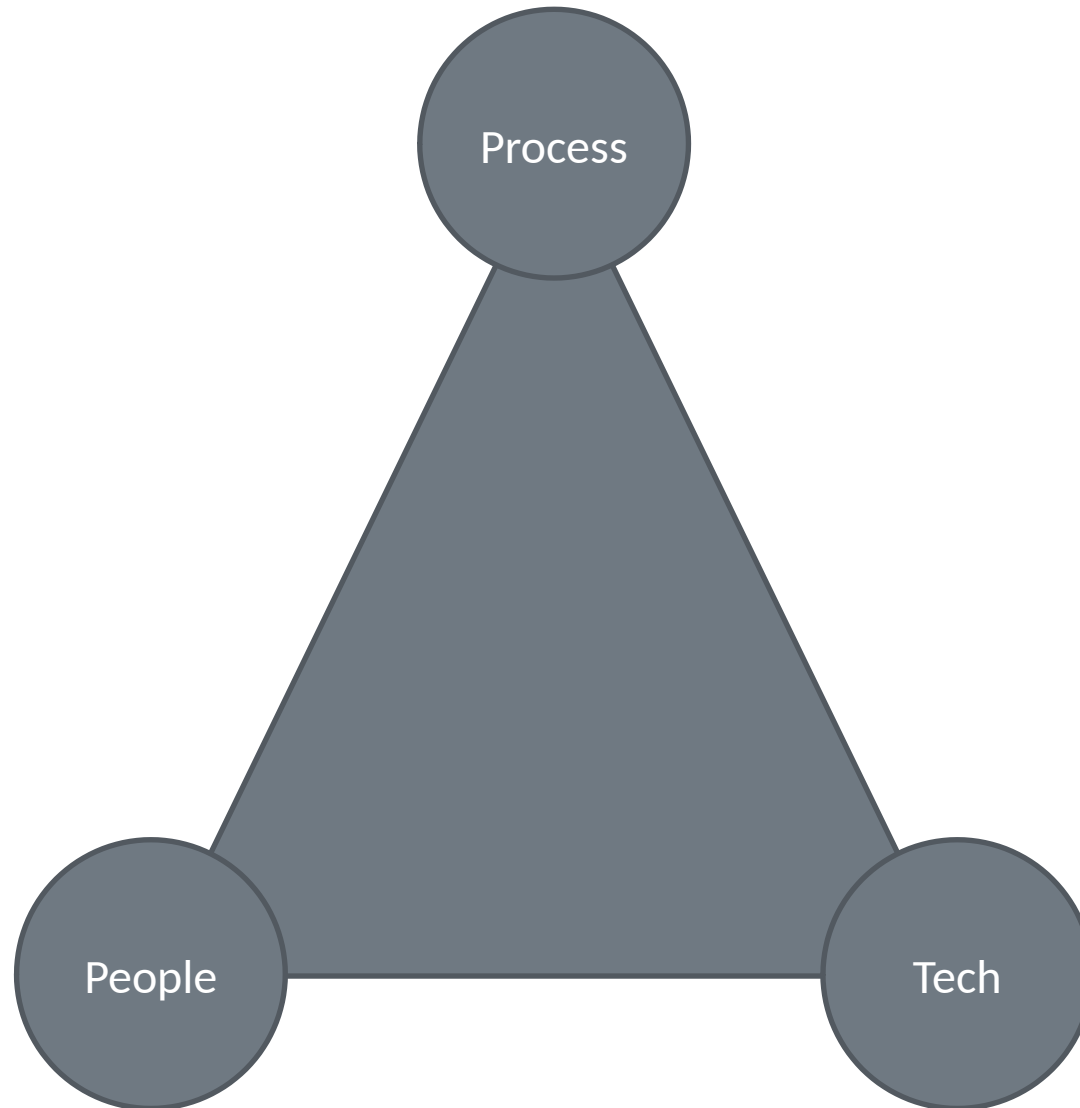
- Getting more out of your resources than you did before
- More What?:







# The Pyramid of NOC Efficiency Zen



Sounds Good...

**BUT HOW?**



# Free up resources to go digging



- Automate the day to day tasks that you can
- Reduce the number of alerts/alarms so you can focus on the important ones
- Create a good alerting system and trust it

Time	server	dip_pps	dip_mbps	myemailmessage	values_rule_mbps_pps	unblocked_sflow	blocked_sflow	allowed_pps
04/01/2019 09:44 EDT	server354	16842	158	Time:04/01/2019 09:44 EDT Host: [REDACTED] Impact: 158 Mbps / 16842 pps Attacks: Fragmented Reflective DNS ( 53/udp ) at 32 Mbps / 3482 pps Fragmented udp at 116 Mbps / 12491 pps Reflective ldap ( 389/udp ) to service 40041 at 10 Mbps / 869 pps Sflow stats: Unblocked:86 EP:0 Total:171 Unblocked Sflow fp0:86 fp1:0 fp2:0	cns-001045 at 32 Mbps / 3482 pps cns-002069 at 9 Mbps / 1131 pps cns-002091 at 10 Mbps / 869 pps cns-100028 at 107 Mbps / 11360 pps	86	85	17040



# Respond More Quickly



- Integrate your alerting system with your team communication system
- A non-actionable alert is an alert that should not have fired
- Be sure to include valuable info in the alert itself, not just “hey something happened”



**(354) DIP Attack BW** APP 9:46 AM

Host: [REDACTED] Impact: 158 Mbps / 16842 pps

Attacks: Fragmented Reflective DNS ( 53/udp ) at 32 Mbps / 3482 pps

Fragmented udp at 116 Mbps / 12491 pps Reflective ldap ( 389/udp ) to service 40041 at 10 Mbps / 869 pps

Sflow: bp0:86 (fp0:86 fp1:0 fp2:0) bp1:85 Total:171

SOC DIP bp=0 Flex Rule Assistant

# Respond More Quickly (cont.)



- Provide next step for your SOC engineers in the alert itself



[REDACTED] **(354) DIP Attack BW** APP 9:46 AM

Host: [REDACTED] Impact: 158 Mbps / 16842 pps

Attacks: Fragmented Reflective DNS ( 53/udp ) at 32 Mbps / 3482 pps

Fragmented udp at 116 Mbps / 12491 pps Reflective ldap ( 389/udp ) to service 40041 at 10 Mbps / 869 pps

Sflow: bp0:86 (fp0:86 fp1:0 fp2:0) bp1:85 Total:171

SOC DIP bp=0 Flex Rule Assistant

# Flex Rule Assistant on Alert



## EAD Flex Rule Assistant

Edit Export ...

SWA Server Selector (354) Timeframe Date time range Source sFlows Help

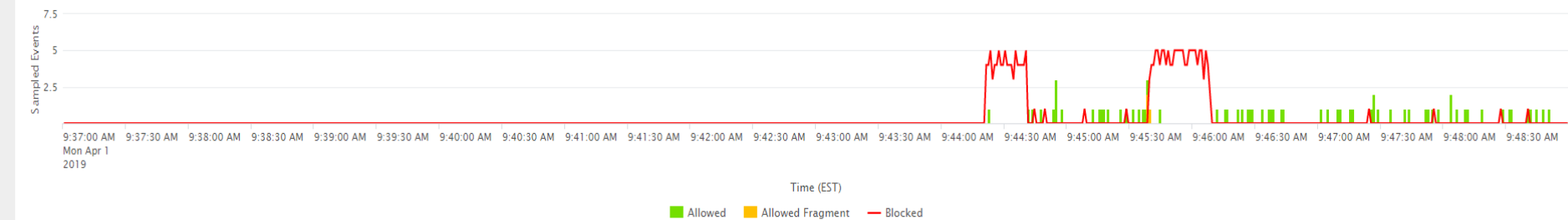
Hide Filters

Protocol udp Blocked or Allowed All Target IP (1 Attac... Auto Flex Generator Manual Flex Builder Show IP Header Statistics Show UDP statistics Apply Port Filters

### Alerts

_time	Target IP	Duration(mins)	Message	Max PPS	Max Mbps
2019-04-01 09:47:00		3	Finished attack to for 3 minutes . Attack vector: Fragmented Reflective DNS ( 53/udp ) . Fragmented udp . Reflective ldap ( 389/udp ) to service 10808. Fragmented Reflective DNS ( 53/udp ) . Reflective ldap ( 389/udp ) to service 40041. Max Values: 49831 pps / 463 Mbps . Rules triggered: cns-001045 cns-002069 cns-002091 cns-100028	49831	463

### Type=sflow Breakdown (IP= ) 294 events displayed Sampling at 1:1



### Auto Flex Generator

#### UDP Flex Filter for configuration on CMS

bpf ip and udp and dst host and (dst port 4500 or dst port 54902) \_\_\_\_CAUTION!: Low number of Filter Terms ip and udp and dst host and (((dst port 10808 or dst port 40041) and (src port 389 or src port 53) and (ip[6] & 0x20>0) or (ip[6:2] & 0x3fff>0)) \_\_\_\_CAUTION!: DNS

#### Potential Sources to Investigate

Single Source IP /24 /16

# Unblocked Sflow Link on Alert



New Search Save As Close

splunk\_server=server354 index=\* type=sflow dir=inbound bp=0 dip=[REDACTED] Date time range Q

✓ 853 events (4/1/19 9:37:00.000 AM to 4/1/19 9:49:00.000 AM) No Event Sampling Job Verbose Mode

Events (853) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 9 Next

< Hide Fields

Selected Fields

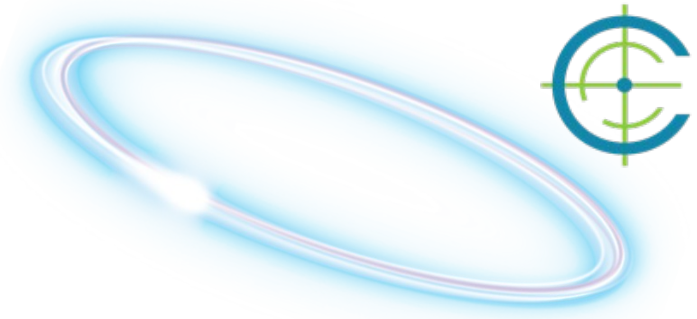
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields

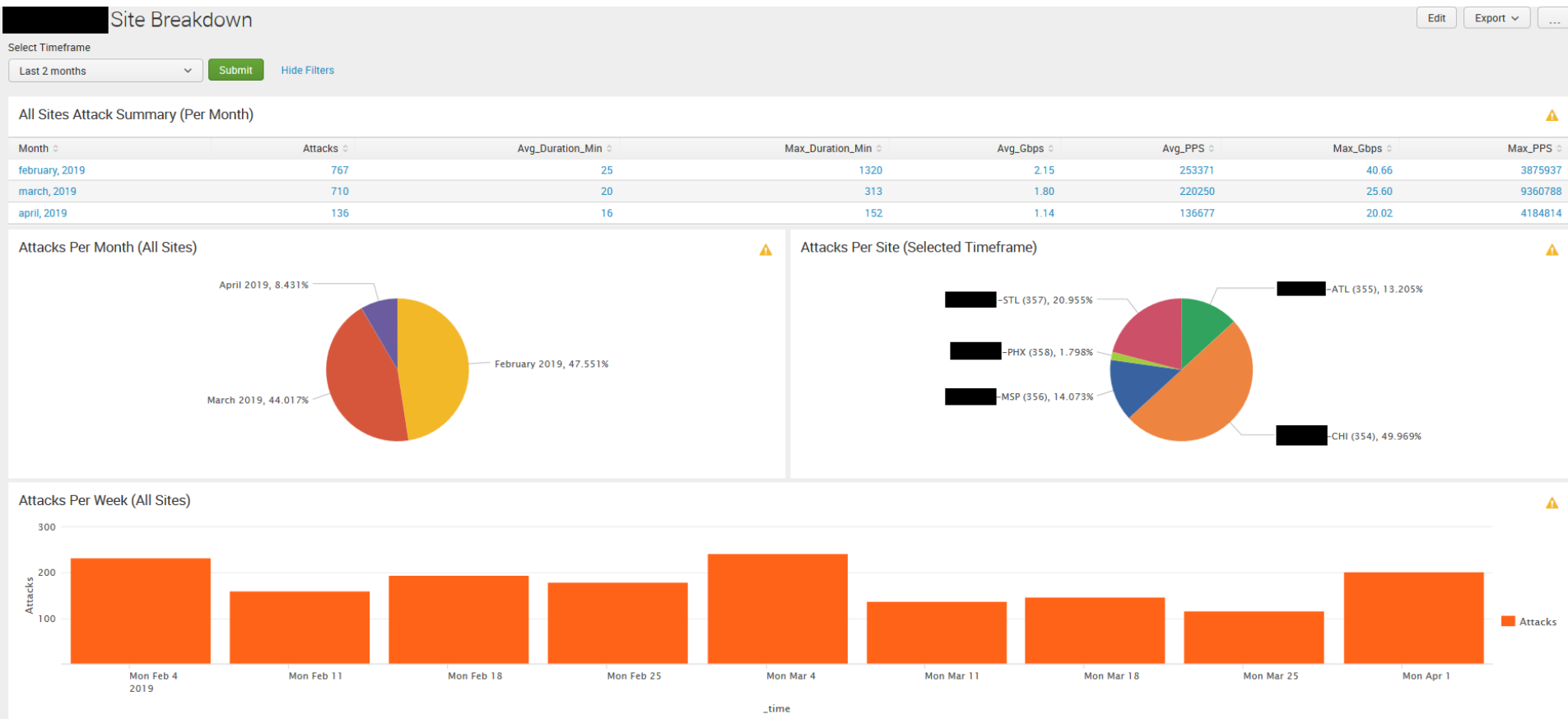
- # bp 1
- a cat 1
- a cl 1
- # date\_hour 1
- # date\_mday 1
- # date\_minute 5
- a date\_month 1
- # date\_second 60
- a date\_wday 1
- # date\_year 1
- # date\_zone 1
- a device 2
- a dip 1
- a dir 1
- # dprt 100+

i	Time	Event
>	4/1/19 9:48:59.226 AM	Apr 1 09:48:59 127.0.0.1 2019-04-01T09:48:59.226-04:00 10.11.12.5 cat=network,type=sflow,v=1,cl=default,device=[REDACTED],sc=9,sfn=7,dir=inbound,time=1554126538 949000,mp=x-1/3,issr=1999,isr=1,px=31,lb=0,dip=[REDACTED],dprt=42968,iplen=1204,prot=6,tos=0,sip=[REDACTED],sprt=102,ttl=58,bp=0,ep=0,icn=5,sc1=0,fp=0,flags=16,flags-decode=ACK,plen=1218,pdu=[REDACTED] host = 10.11.12.5   source = udp:5514   sourcetype = corero_smartwall_syslog
>	4/1/19 9:48:59.226 AM	Apr 1 09:48:59 127.0.0.1 2019-04-01T09:48:59.226-04:00 10.11.12.5 cat=network,type=sflow,v=1,cl=default,device=[REDACTED],sc=9,sfn=6,dir=inbound,time=1554126538 763000,mp=x-1/1,issr=1999,isr=1,px=15,lb=0,dip=[REDACTED],dprt=53287,iplen=1500,prot=6,tos=0,sip=[REDACTED],sprt=80,ttl=249,bp=0,ep=0,icn=5,sc1=0,fp=0,flags=16,flags-decode=ACK,plen=1514,pdu=[REDACTED] host = 10.11.12.5   source = udp:5514   sourcetype = corero_smartwall_syslog
>	4/1/19 9:48:59.226 AM	Apr 1 09:48:59 127.0.0.1 2019-04-01T09:48:59.226-04:00 10.11.12.5 cat=network,type=sflow,v=1,cl=default,device=[REDACTED],sc=9,sfn=4,dir=inbound,time=1554126538 558000,mp=x-1/3,issr=1999,isr=1,px=6,lb=0,dip=[REDACTED],dprt=62443,iplen=1500,prot=6,tos=0,sip=[REDACTED],sprt=80,ttl=249,bp=0,ep=0,icn=5,sc1=0,fp=0,flags=16,flags-decode=ACK,plen=1514,pdu=[REDACTED] host = 10.11.12.5   source = udp:5514   sourcetype = corero_smartwall_syslog
>	4/1/19 9:48:59.226 AM	Apr 1 09:48:59 127.0.0.1 2019-04-01T09:48:59.226-04:00 10.11.12.5 cat=network,type=sflow,v=1,cl=default,device=[REDACTED],sc=9,sfn=9,dir=inbound,time=1554126539 034000,mp=x-1/1,issr=1999,isr=1,px=22,lb=0,dip=[REDACTED],dprt=23371,iplen=1500,prot=6,tos=0,sip=[REDACTED],sprt=443,ttl=59,bp=0,ep=0,icn=5,sc1=0,fp=0,flags=16,flags-decode=ACK,plen=1514,pdu=[REDACTED] host = 10.11.12.5   source = udp:5514   sourcetype = corero_smartwall_syslog

# Automate Reporting



- Value Demonstration
- Even if it's just to show everything working



# Summary



- Increase efficiency and customer delight by...
- 1) Freeing up resources to go digging to build delight ahead of incidents
- 2) Respond to incidents more quickly with tools and process
- 3) Automate Reporting and value demonstration







# Questions?