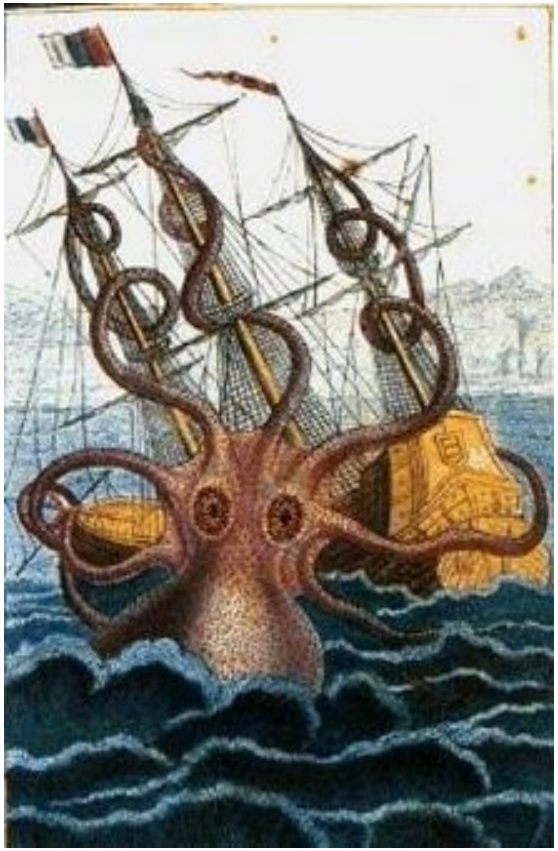


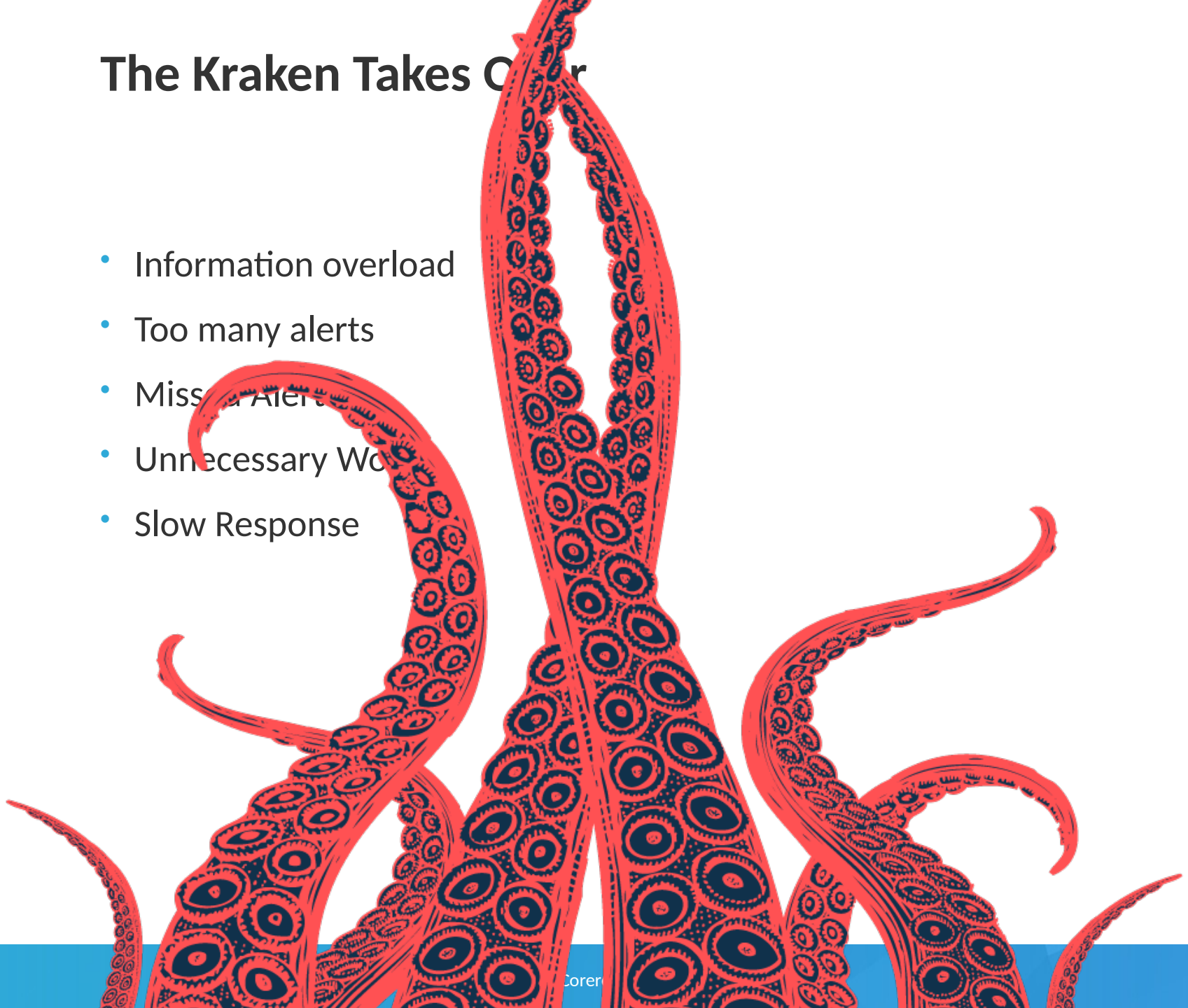
Michael Powell

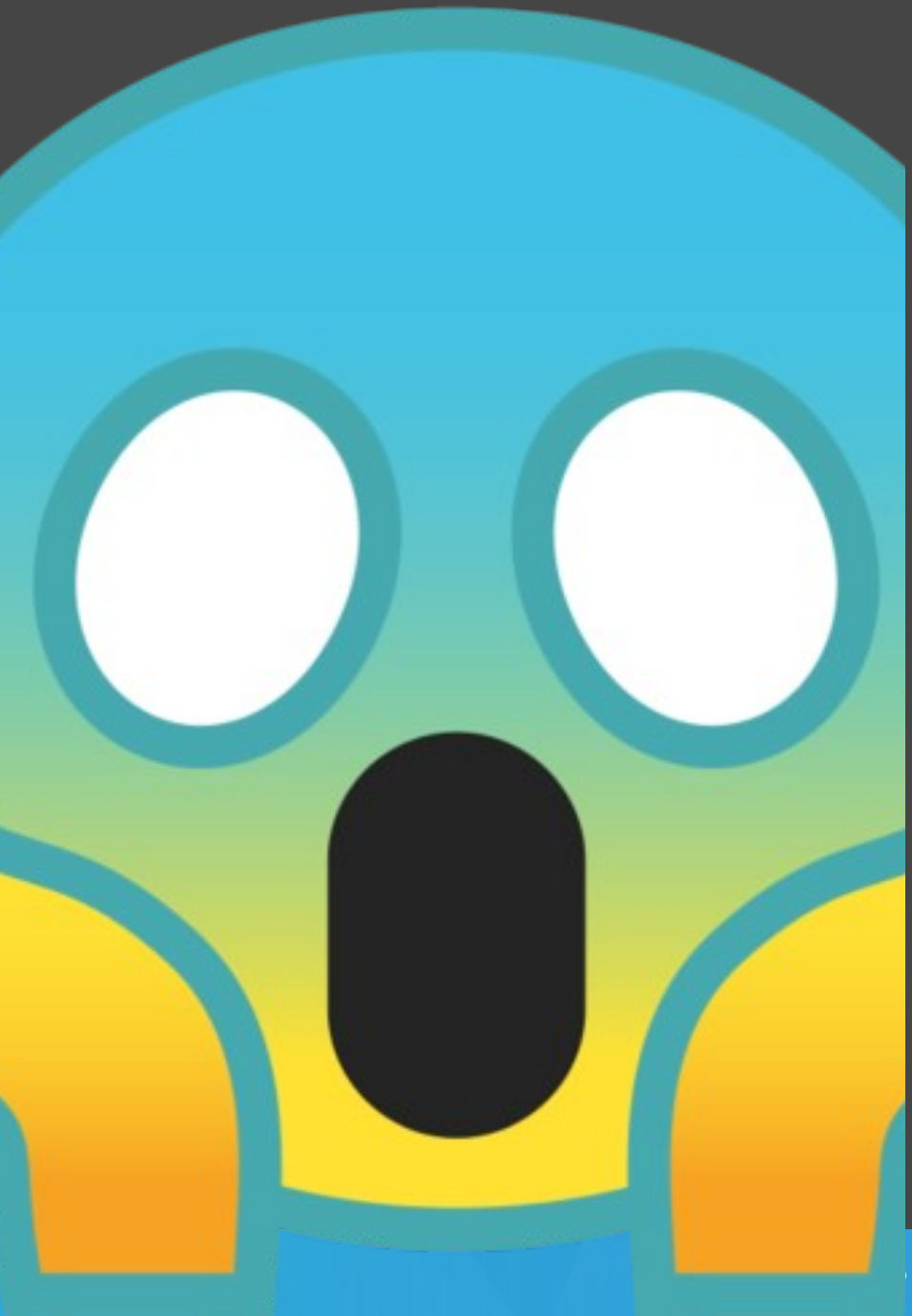
Sr. Security Engineer – Corero Network Security

Control the Kraken: Becoming a More Efficient NOC

The Kraken Takes O r

- Information overload
- Too many alerts
- Miss d Alert
- Unnecessary Wo
- Slow Response



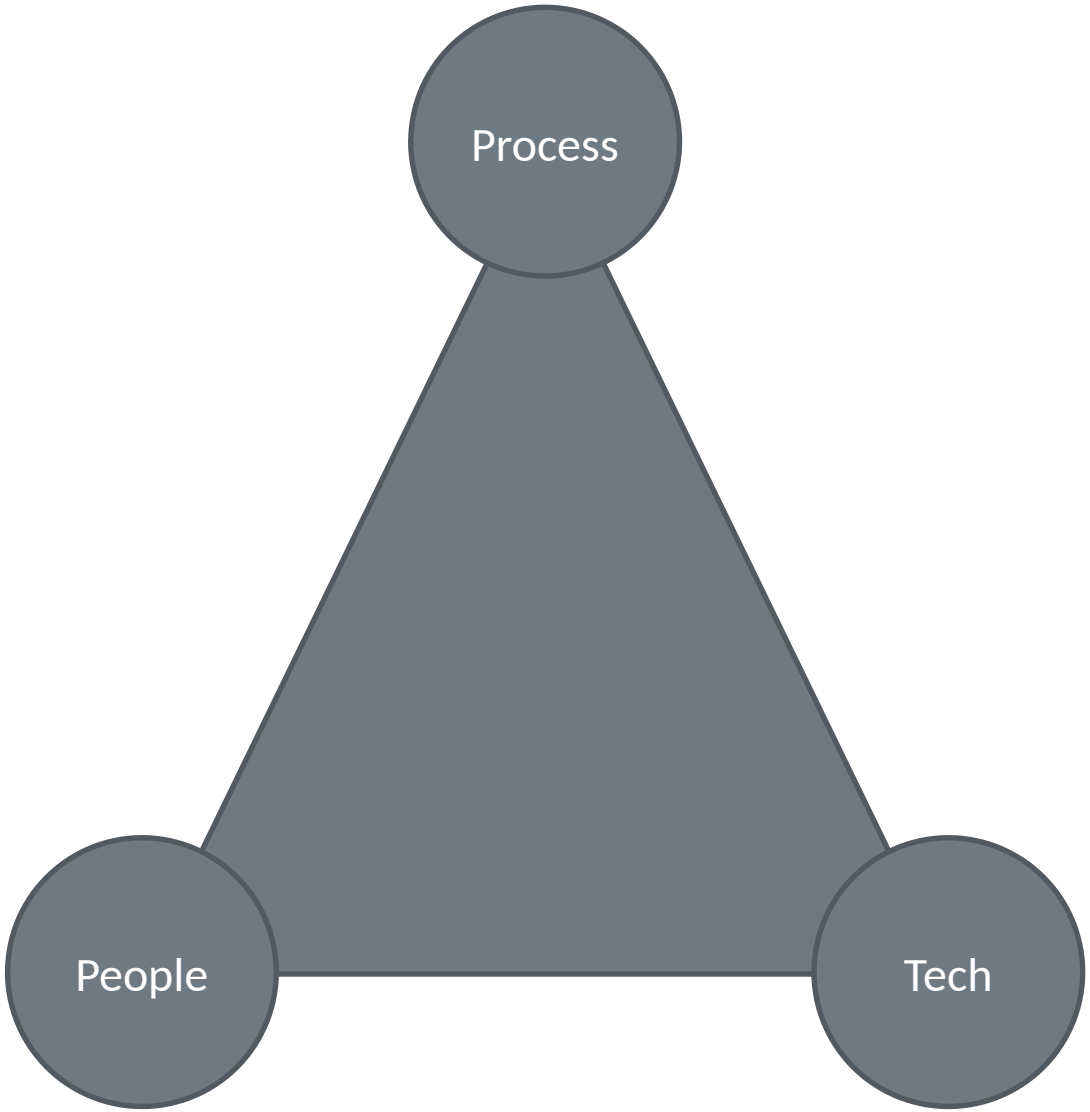


Or Worse Yet!

What is NOC Efficiency?

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

The Pyramid of NOC Efficiency Zen



Sounds Good…

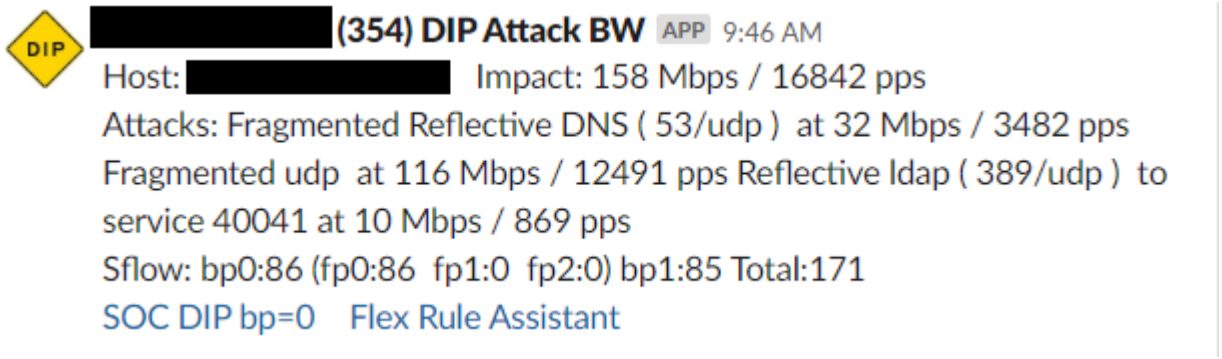
Free up resources to go digging

- 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

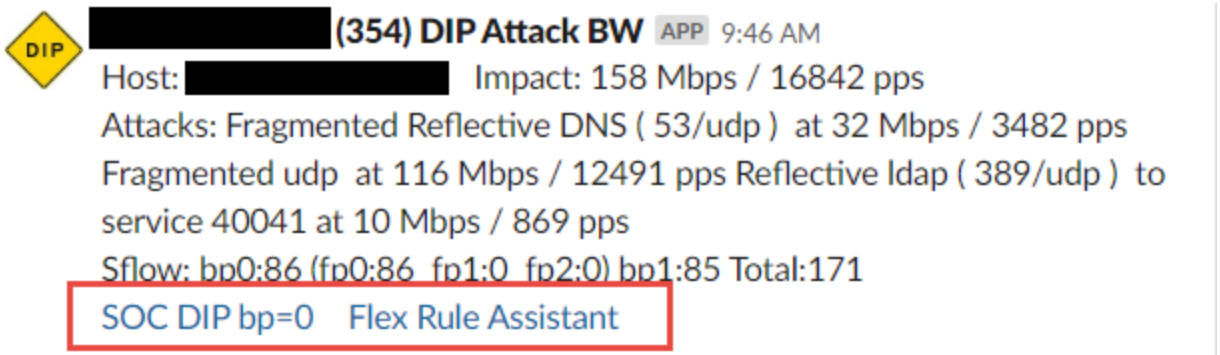
Respond More Quickly

- 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”

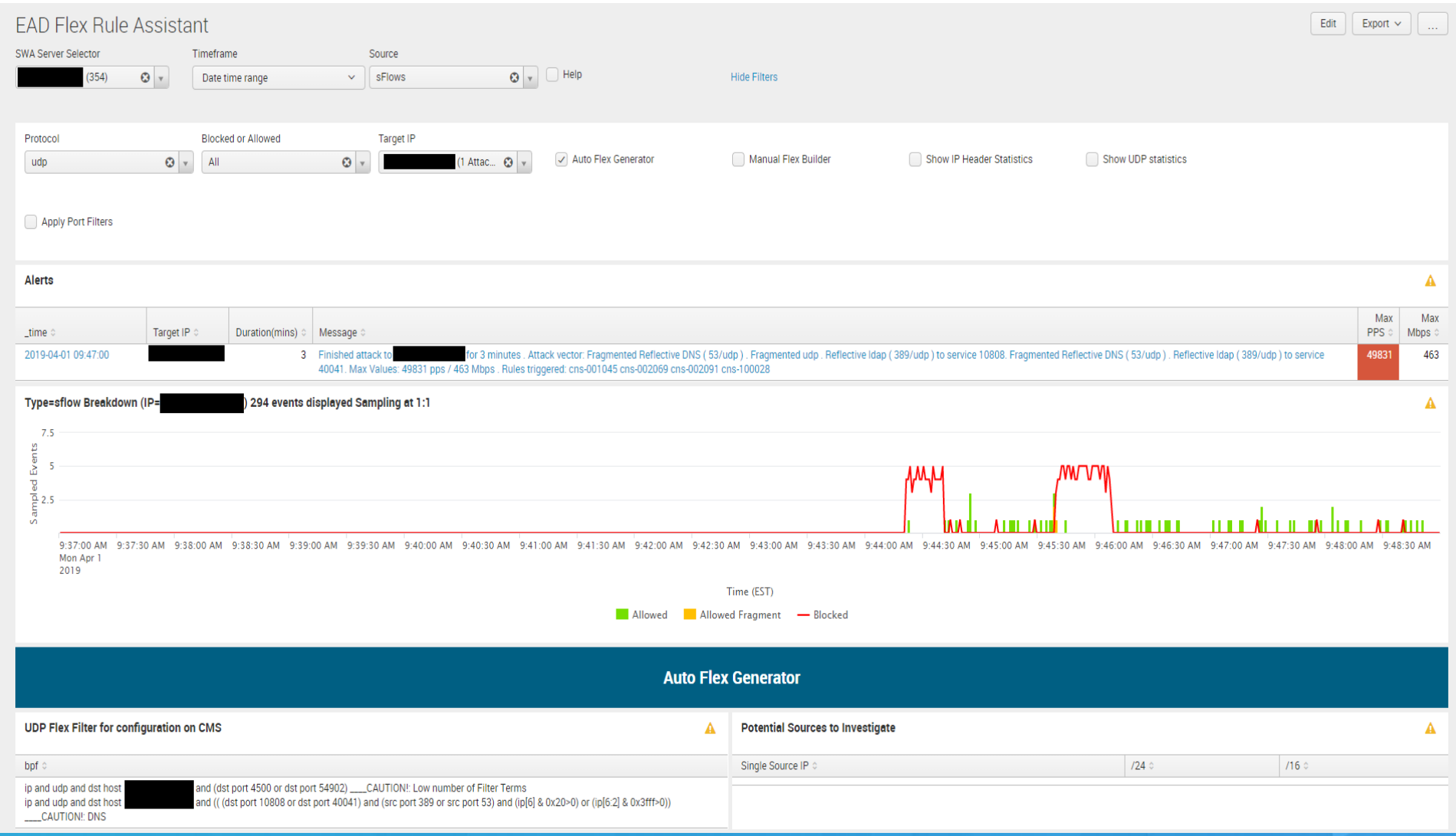


Respond More Quickly (cont.)

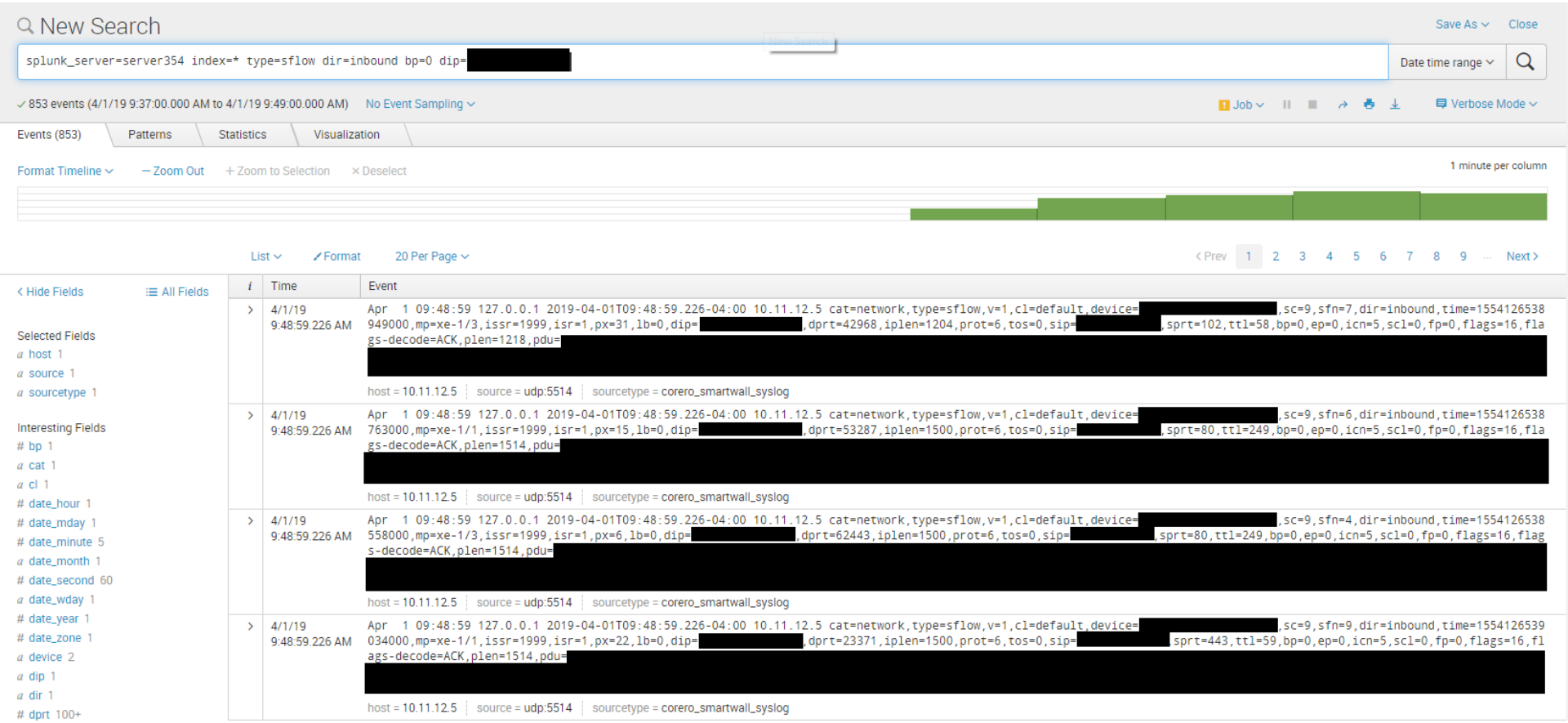
- Provide next step for your SOC engineers in the alert itself



Flex Rule Assistant on Alert



Unblocked Sflow Link on Alert



Automate Reporting

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

[redacted] Site Breakdown

Edit | Export | ...

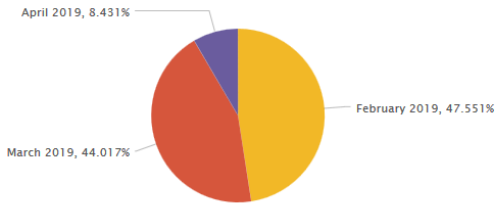
Select Timeframe

Last 2 months | Submit | Hide Filters

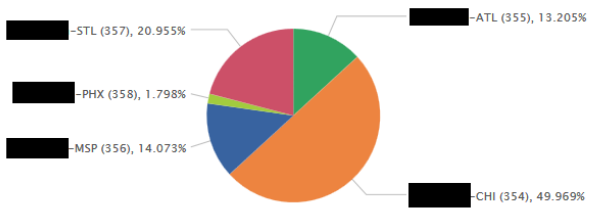
All Sites Attack Summary (Per Month)

Month	Attacks	Avg_Duration_Min	Max_Duration_Min	Avg_Gbps	Avg_PPS	Max_Gbps	Max_PPS
february, 2019	767	25	1320	2.15	253371	40.66	3875937
march, 2019	710	20	313	1.80	220250	25.60	9360788
april, 2019	136	16	152	1.14	136677	20.02	4184814

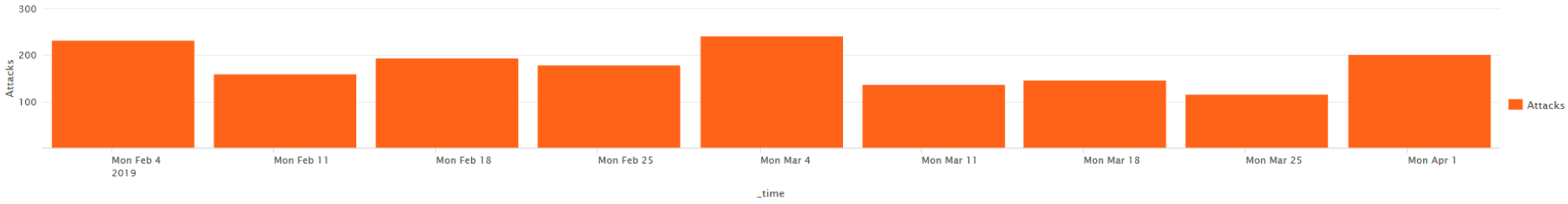
Attacks Per Month (All Sites)



Attacks Per Site (Selected Timeframe)



Attacks Per Week (All Sites)



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?