Splunk As An Intelligent Platform: From Log Aggregation To Machine-assisted Analysis

Gopal Brugalette

Sr Architect, Nordstrom

Ashwin Kothari

Sr Manager, Nordstrom

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.

About Nordstrom

- Founded 1901
- 65,000 Employees
- 121 Nordstrom stores
- 194 Rack stores
- E-Commerce

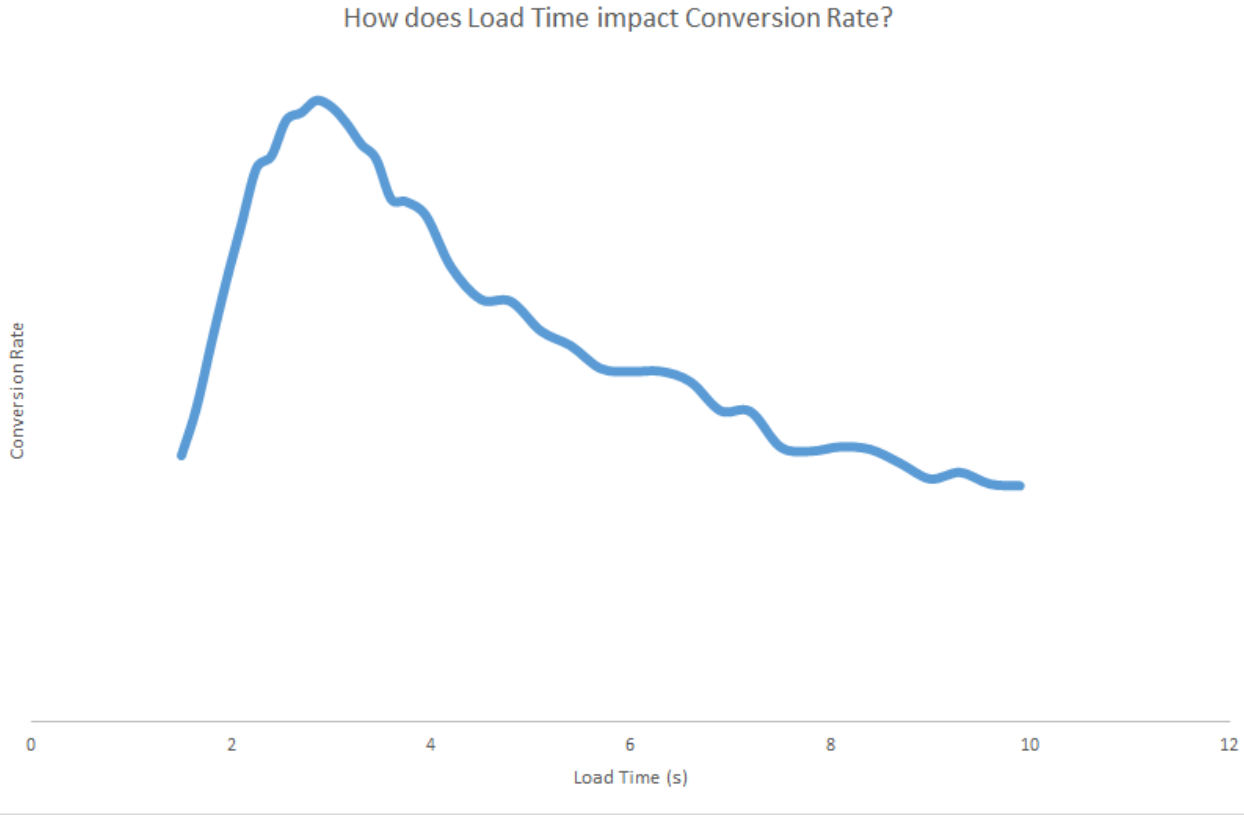
About Gopal

- Senior Applied Architect, Performance Engineering
- 6 Years at Nordstrom
- Splunking for 5 years
- Besides my life in IT:
  - Nuclear physicist
  - Farmer
  - Wood working

About Ash

- Senior Manager, Platform and Performance Engineering
- 6 Years at Nordstrom
- Test and Performance Engineering
- Besides my life in IT:
  - Fitness Evangelist
  - Cars
  - Beers

Performance And The Customer Experience



Preparing For Nordstrom's Major Events

Early Access

Holiday

Before Splunk: Too Much Test Data

- Too many servers, too many logs
- Analyzed only samples of test results
- Analysis took days
- Forced to scale back testing and analysis

Increased Risk of Customer Impact

"Without Splunk, we'd have to essentially log into each and every server and look at the logs to try to determine which servers were having a problem."

Splunk Comes Along

- Initial target - production support teams
- Performance engineering enthusiastic early adopters
- Eventual spread to Dev and beyond

"I saw Splunk and immediately recognized its power and what a great tool it was for solving some of our major problems"

The Splunk Journey

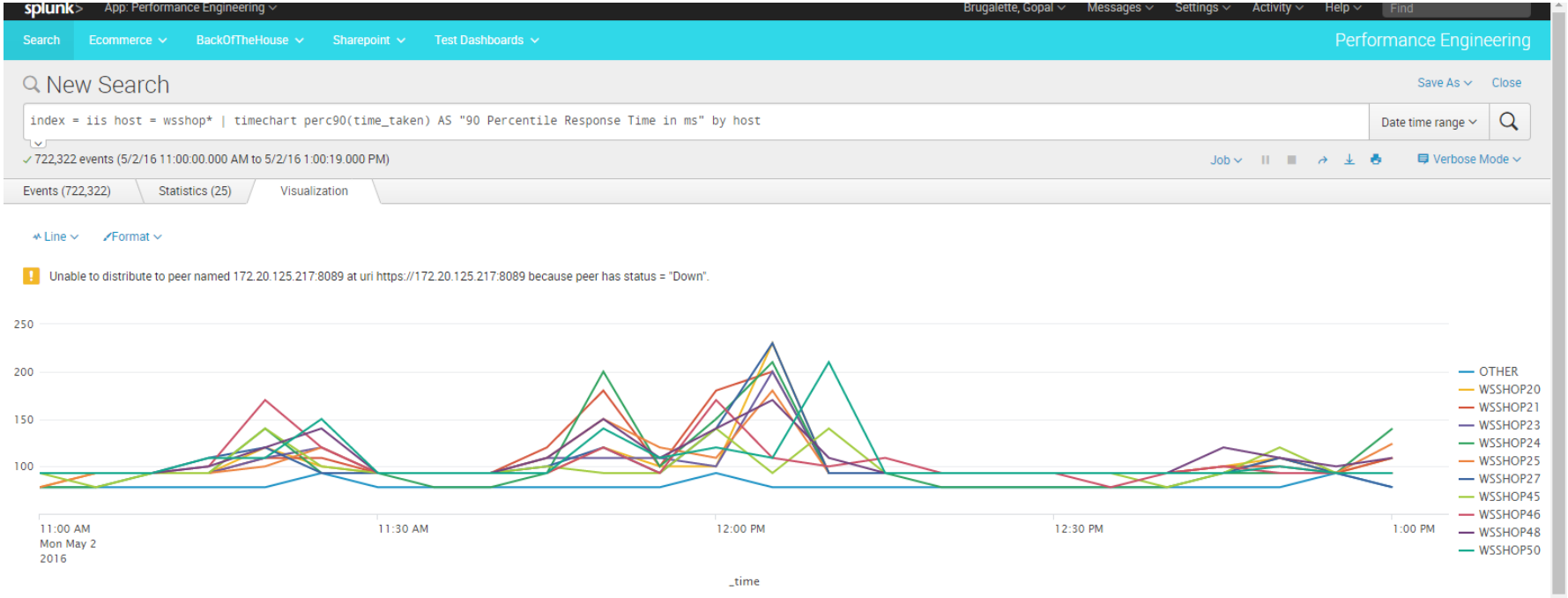
Proliferation

- Initial Adopters
- Gradual Expansion
- Explosive Use

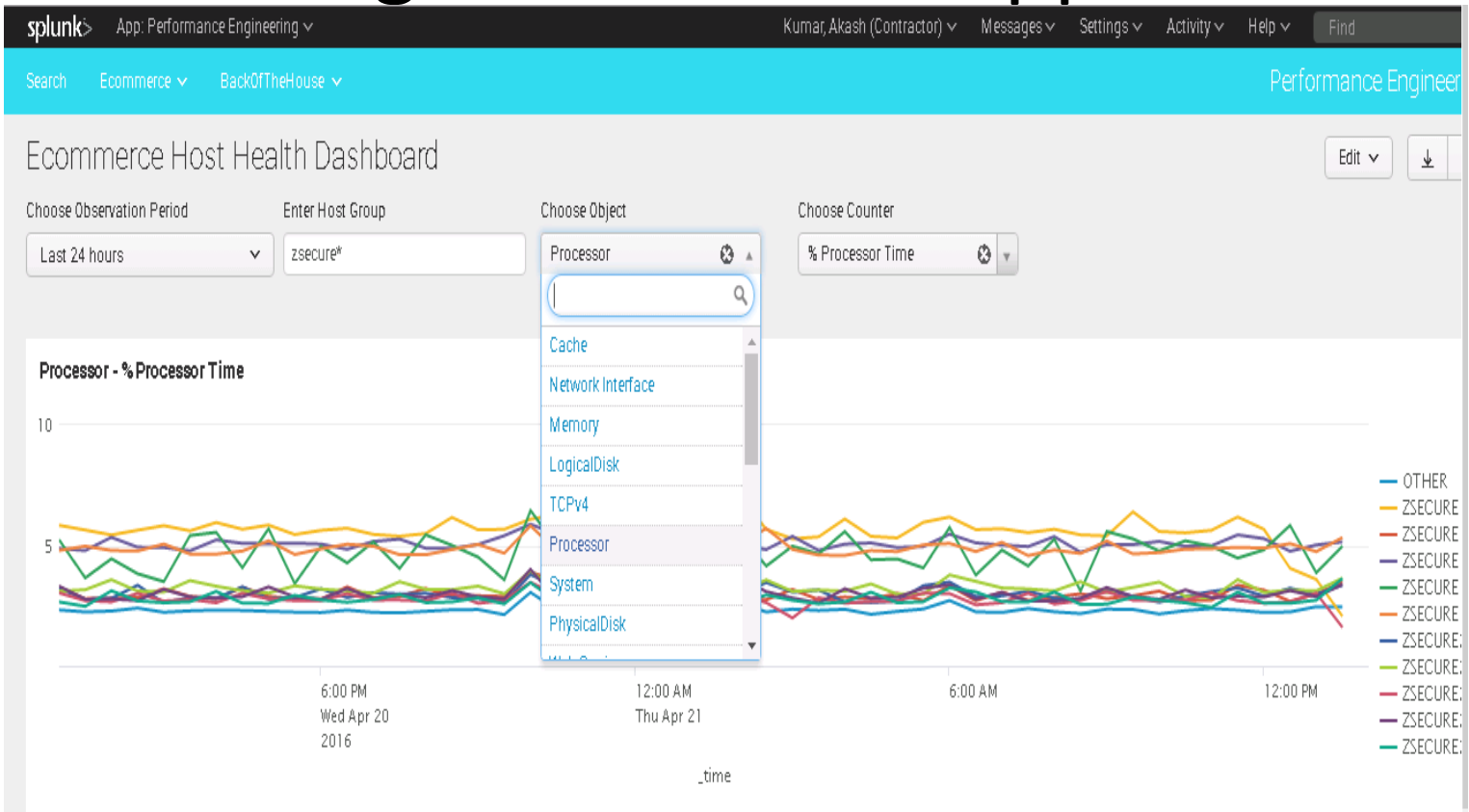
Evolution

- Log Aggregation
- Dashboards
- Machine-Assisted Analysis

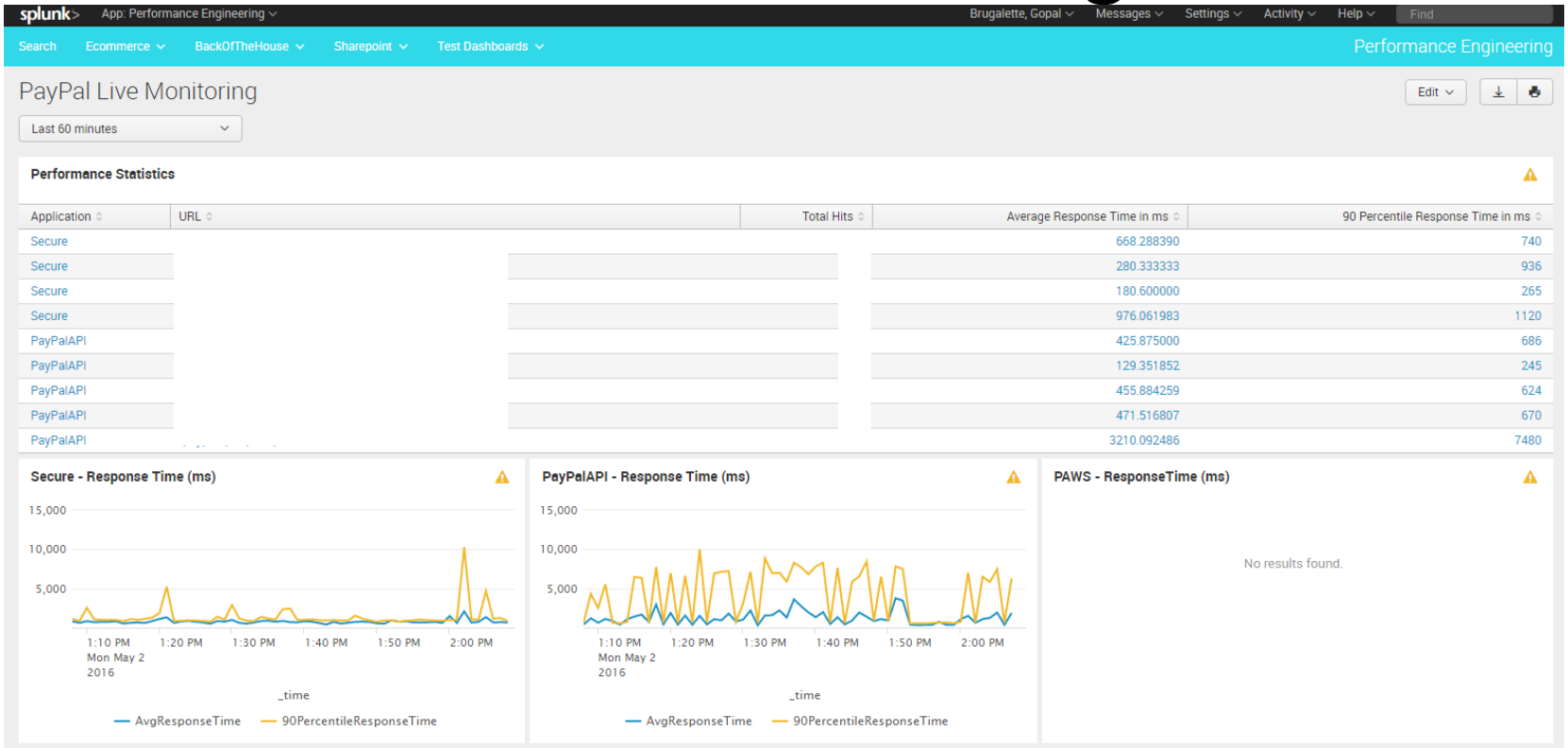
Log Aggregation



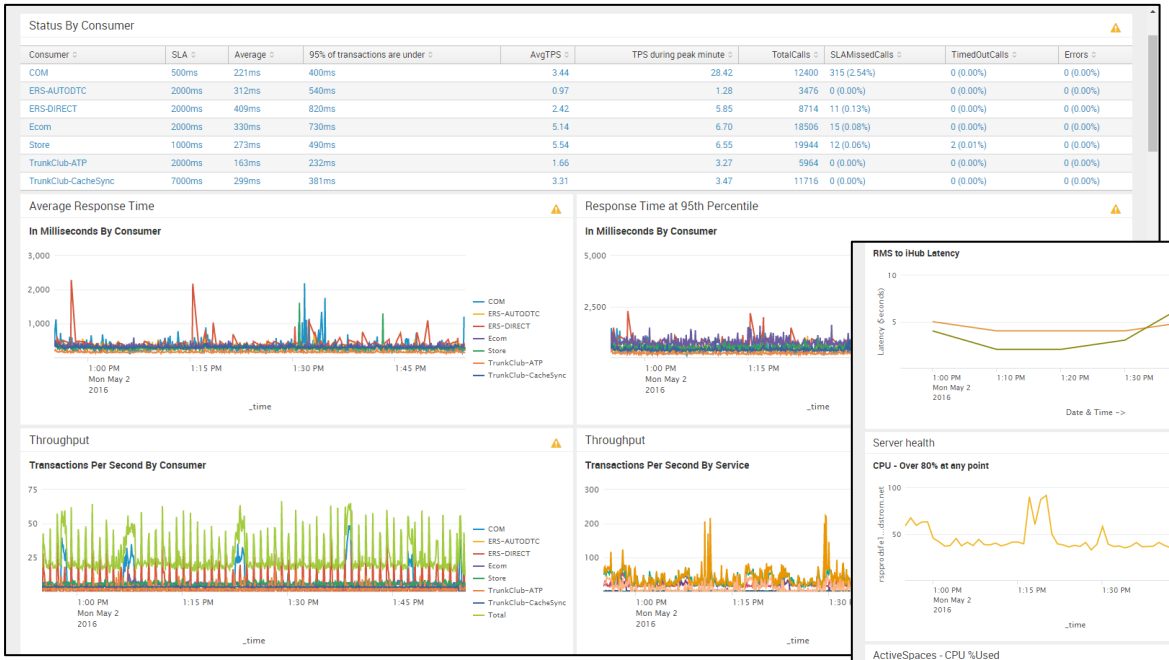
Logs In A Nice Wrapper



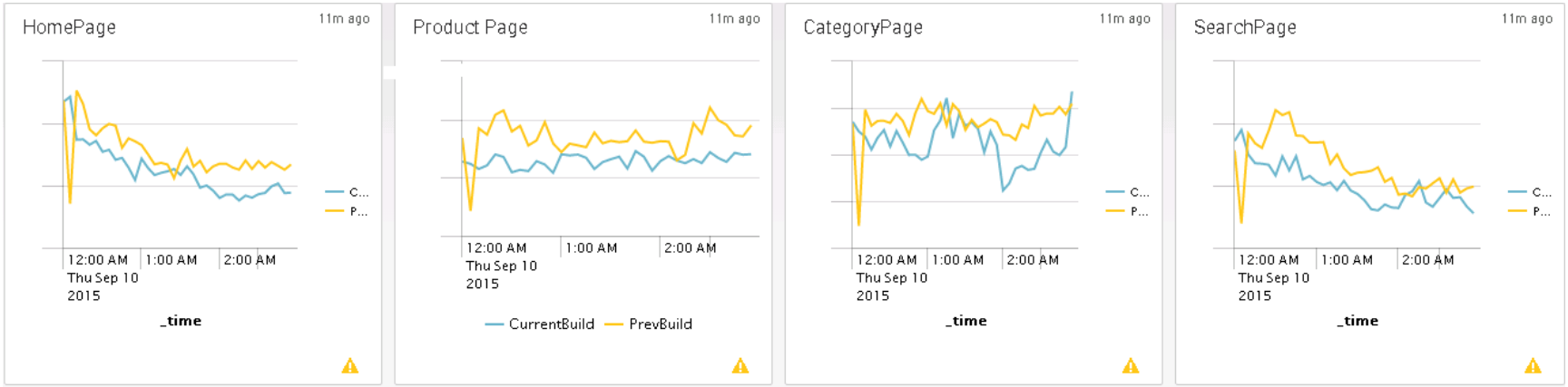
Multi-Dimensional Log Data



Multiple Graphs In One Dashboard

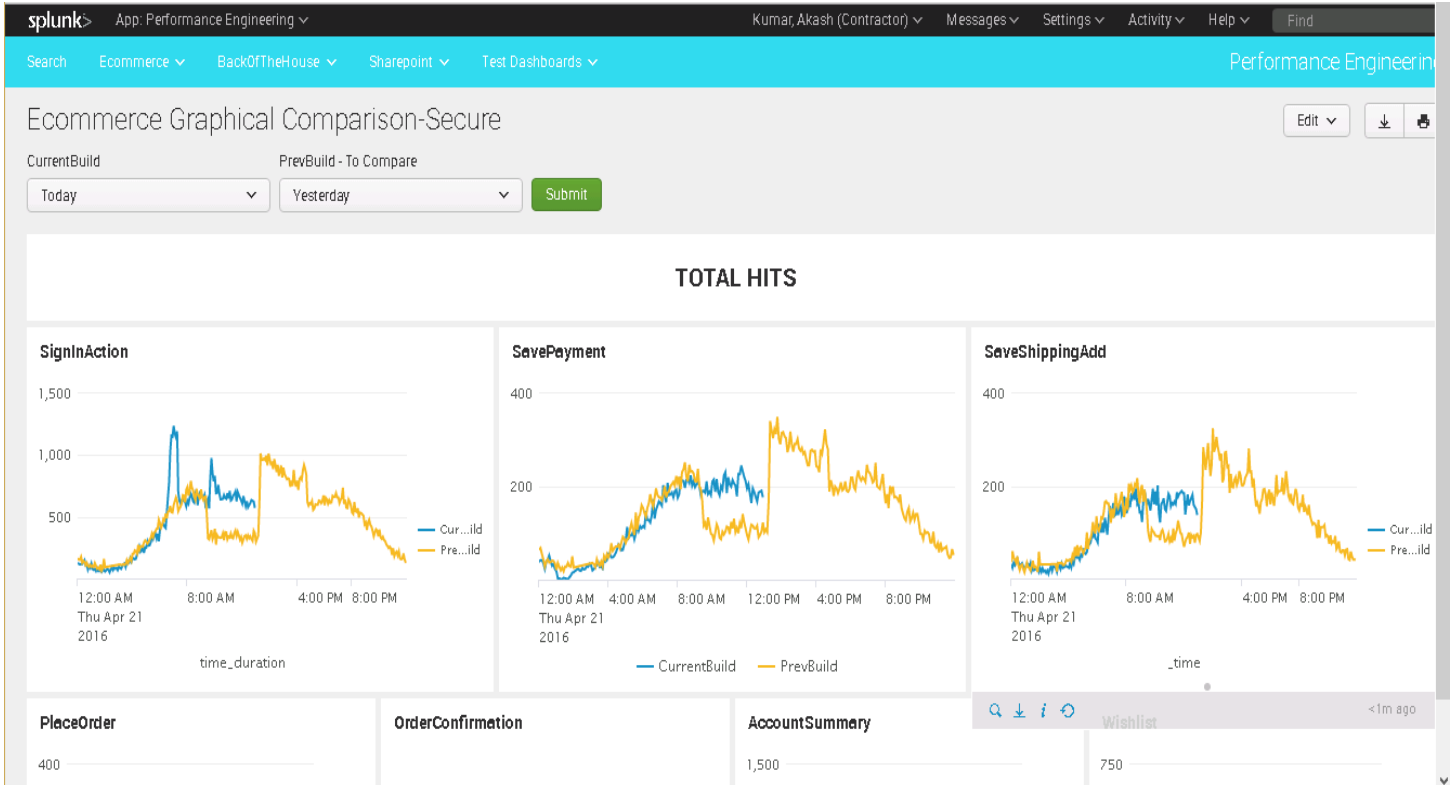


Complex & Calculated Data

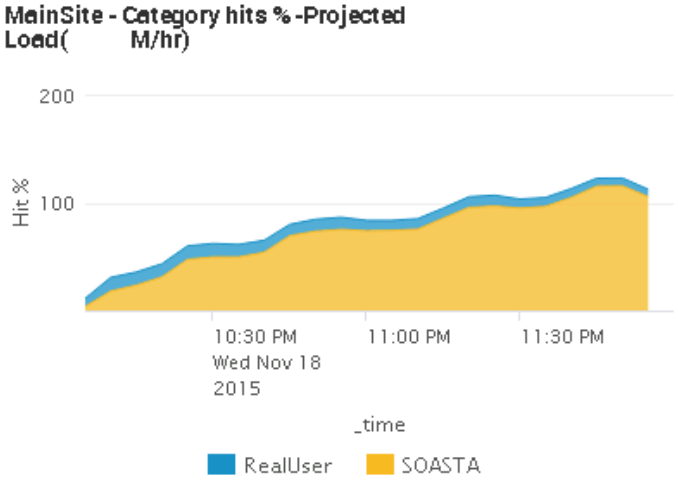


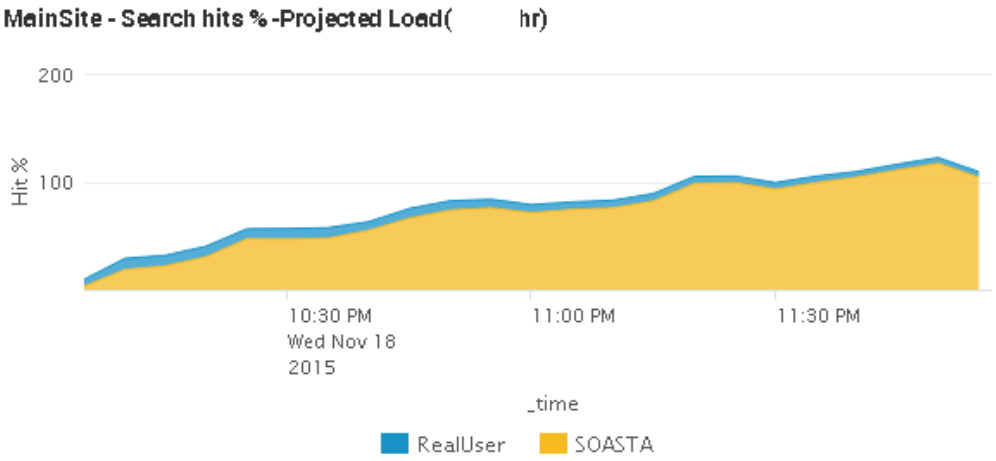
- Compares hits from day to day

Same Approach For Test Comparison



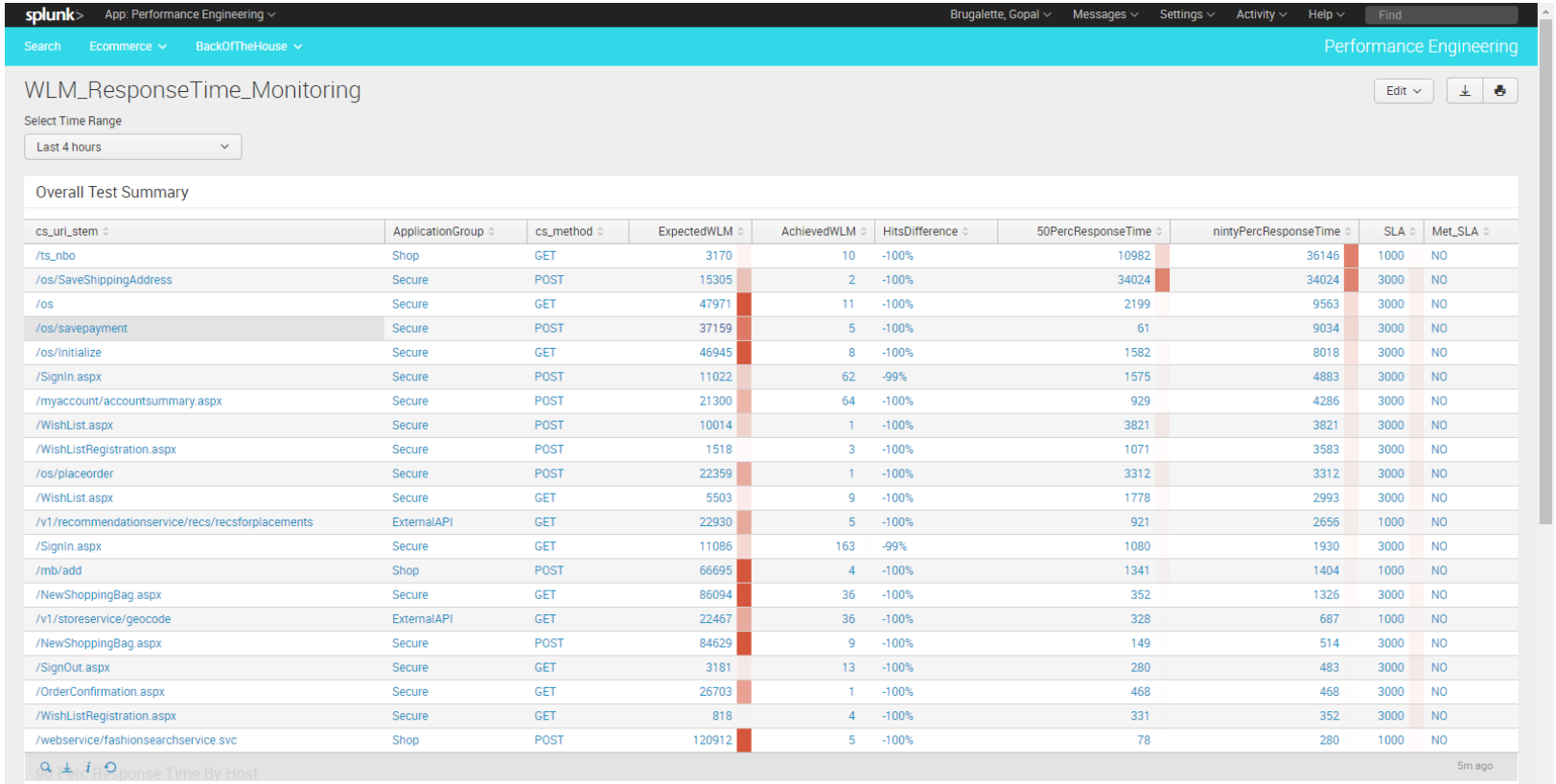
Increasingly Complex & Calculated Data





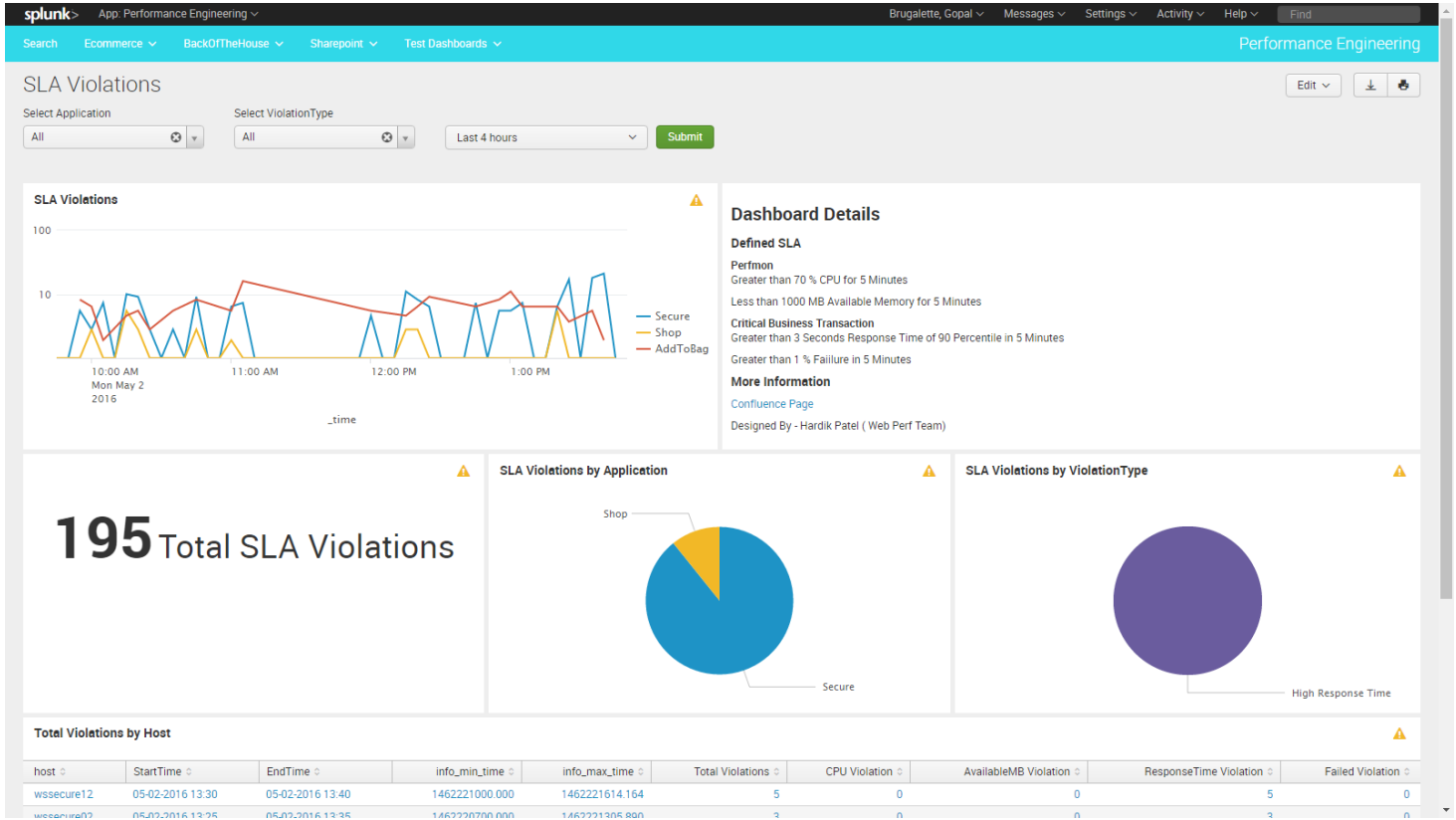
- Use case: Full Scale Load testing in production
- Graph: A sum total of real user traffic + synthetic load testing traffic as a percentage of projected load
- Used during major events for dynamic capacity modeling

Toward Machine-Assisted Analysis

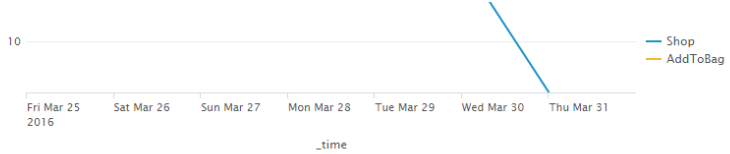


cs_uri_stem	ApplicationGroup	cs_method	ExpectedWLM	AchievedWLM	HitsDifference	50PercResponseTime	nintyPercResponseTime	SLA	Met_SLA
/ts_nbo	Shop	GET	3170	10	-100%	10982	36146	1000	NO
/os/SaveShippingAddress	Secure	POST	15305	2	-100%	34024	34024	3000	NO
/os	Secure	GET	47971	11	-100%	2199	9563	3000	NO
/os/savepayment	Secure	POST	37159	5	-100%	61	9034	3000	NO
/os/Initialize	Secure	GET	46945	8	-100%	1582	8018	3000	NO
/SignIn.aspx	Secure	POST	11022	62	-99%	1575	4883	3000	NO
/myaccount/accountsummary.aspx	Secure	POST	21300	64	-100%	929	4286	3000	NO
/WishList.aspx	Secure	POST	10014	1	-100%	3821	3821	3000	NO
/WishListRegistration.aspx	Secure	POST	1518	3	-100%	1071	3583	3000	NO
/os/placeorder	Secure	POST	22359	1	-100%	3312	3312	3000	NO
/WishList.aspx	Secure	GET	5503	9	-100%	1778	2993	3000	NO
/v1/recommendationservice/recs/recsforplacements	ExternalAPI	GET	22930	5	-100%	921	2656	1000	NO
/SignIn.aspx	Secure	GET	11086	163	-99%	1080	1930	3000	NO
/mb/add	Shop	POST	66695	4	-100%	1341	1404	1000	NO
/NewShoppingBag.aspx	Secure	GET	86094	36	-100%	352	1326	3000	NO
/v1/storeservice/geocode	ExternalAPI	GET	22467	36	-100%	328	687	1000	NO
/NewShoppingBag.aspx	Secure	POST	84629	9	-100%	149	514	3000	NO
/SignOut.aspx	Secure	GET	3181	13	-100%	280	483	3000	NO
/OrderConfirmation.aspx	Secure	GET	26703	1	-100%	468	468	3000	NO
/WishListRegistration.aspx	Secure	GET	818	4	-100%	331	352	3000	NO
/webservice/fashionsearchservice.svc	Shop	POST	120912	5	-100%	78	280	1000	NO

Increasing Machine Assisted Analysis



Cont'd



Less than 1000 MB Available Memory for 5 Minutes

Critical Business Transaction

Greater than 3 Seconds Response Time of 90 Percentile in 5 Minutes

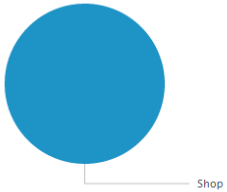
Greater than 1 % Failure in 5 Minutes

More Information

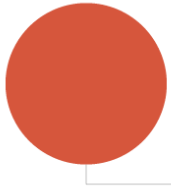
Confluence Page

2,332 Total SLA Violations

SLA Violations by Application



SLA Violations by ViolationType



5m ago

Total Violations by Host

host	StartTime	EndTime	info_min_time	info_max_time	Total Violations	CPU Violation	AvailableMB Violation	ResponseTime Violation	Failed Violation
wsshop50	03-28-2016 02:25	03-28-2016 02:35	1459157100.000	1459157708.188	6	0	0	6	0
wsshop02	03-27-2016 04:25	03-27-2016 04:35	1459077900.000	1459078507.055	4	0	0	4	0
wsshop02	03-28-2016 14:10	03-28-2016 14:22	1459199400.000	1459200158.908	4	0	0	4	0
wsshop02	03-30-2016 02:40	03-31-2016 06:40	1459330800.000	1459431630.228	4	0	0	4	0
wsshop03	03-25-2016 04:10	03-25-2016 04:20	1458904200.000	1458904830.315	4	0	0	4	0
wsshop03	03-26-2016 04:10	03-26-2016 04:20	1458990600.000	1458991224.809	4	0	0	4	0
wsshop04	03-27-2016 02:30	03-27-2016 02:40	1459071000.000	1459071609.120	4	0	0	4	0
wsshop04	03-29-2016 03:15	03-30-2016 22:11	1459246500.000	1459401111.259	4	0	0	4	0
wsshop05	03-29-2016 04:05	03-30-2016 22:33	1459249500.000	1459402396.566	4	0	0	4	0
wsshop08	03-28-2016 14:15	03-28-2016 14:28	1459199700.000	1459200522.321	4	0	0	4	0

« prev 1 2 3 4 5 6 7 8 9 10 next »

Real Gains In Efficiency

- Performance Test Analysis From Days to Minutes
- 50-60% reduction in test iterations
- Analyzing Event WLM from Months to Hours

"Instead of displaying 20 servers and making the engineers scan and look for issues, Splunk displays the one server that's out of standard deviation. All you have to do is fix that server."

Building Expertise Into Splunk

- Performance Engineering process
  - **Identify** there is an issue
  - **Localize** where the issue is
  - **Drill Down** to determine root cause and solution

- Build that expertise into the platform & share it across the team and enterprise

"Splunk is a great tool for collecting all manner of performance information… which we can then use to build our expertise into the platform."

Empowering DevOps

Accessible Data = Accessed Data

- Common across Environments & Apps
- Integrated into SDLC
- Data available to everyone

Enabling Dev Ops

Splunk @Nordstrom

Stores, E-Comm, Mobile, Corporate, Everywhere

Performance Metrics

Security Data

Debug Troubleshooting

Usage Behavior

3.0 TB Ingested Daily, Over 1000 Users

Prod, Test, Security

10,000+ Forwarders

35 Indexers

15 Search Heads

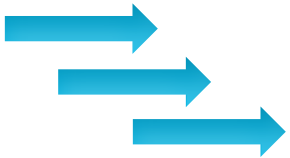
6 Deployment Servers

Splunk Best Practices

- Log in the right format
- Log the information to answer your business and customer questions
- Don't log it if you never look at it
- Use the system to do multiple analytic steps
  - Machine assisted analysis

Splunking Ahead….

- Expand in machine assisted analysis – including pulling Dynatrace -> Splunk
- Build our expertise into the Splunk platform to not only build efficiency but….
- Disperse expertise through Splunk to the entire Nordstrom enterprise



THANK YOU

splunk>