



splunk>

Splunk + GE Digital PREDIX: Industrial IoT

Steve D'Aurora & Joan Chen

GE Digital PREDIX

October 2018 | Version 1.0



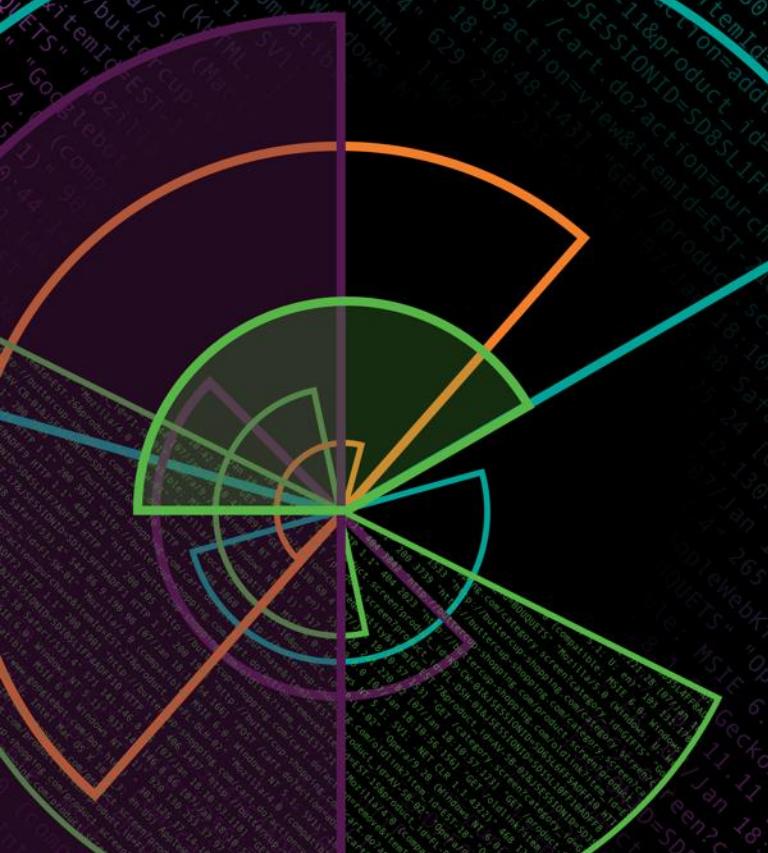
Forward-Looking Statements

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 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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

Meaningful Telemetry Is Hard



Tool Sprawl vs Effective Operations

Logs + Metrics + Events + App Trace + Synthetics + Alerts + Reports + ...

- ▶ Logs, Metrics, Events
 - Sensor all the things
 - Measure all the things

All the things need to be actionable

- ▶ App Trace, Synthetics
 - Actual application health
 - App instance interaction

Synthetic testing is a key data set

- ▶ ITOM
 - Taking action against KPIs needs to be operationalized
 - Needs to feed into the rest of the business operations

Having a valid, up to date source of truth can be an actual thing



The GE You Don't Know

GE Power

Big rotating things



GE Power

Atlanta Power Monitoring and Diagnostics



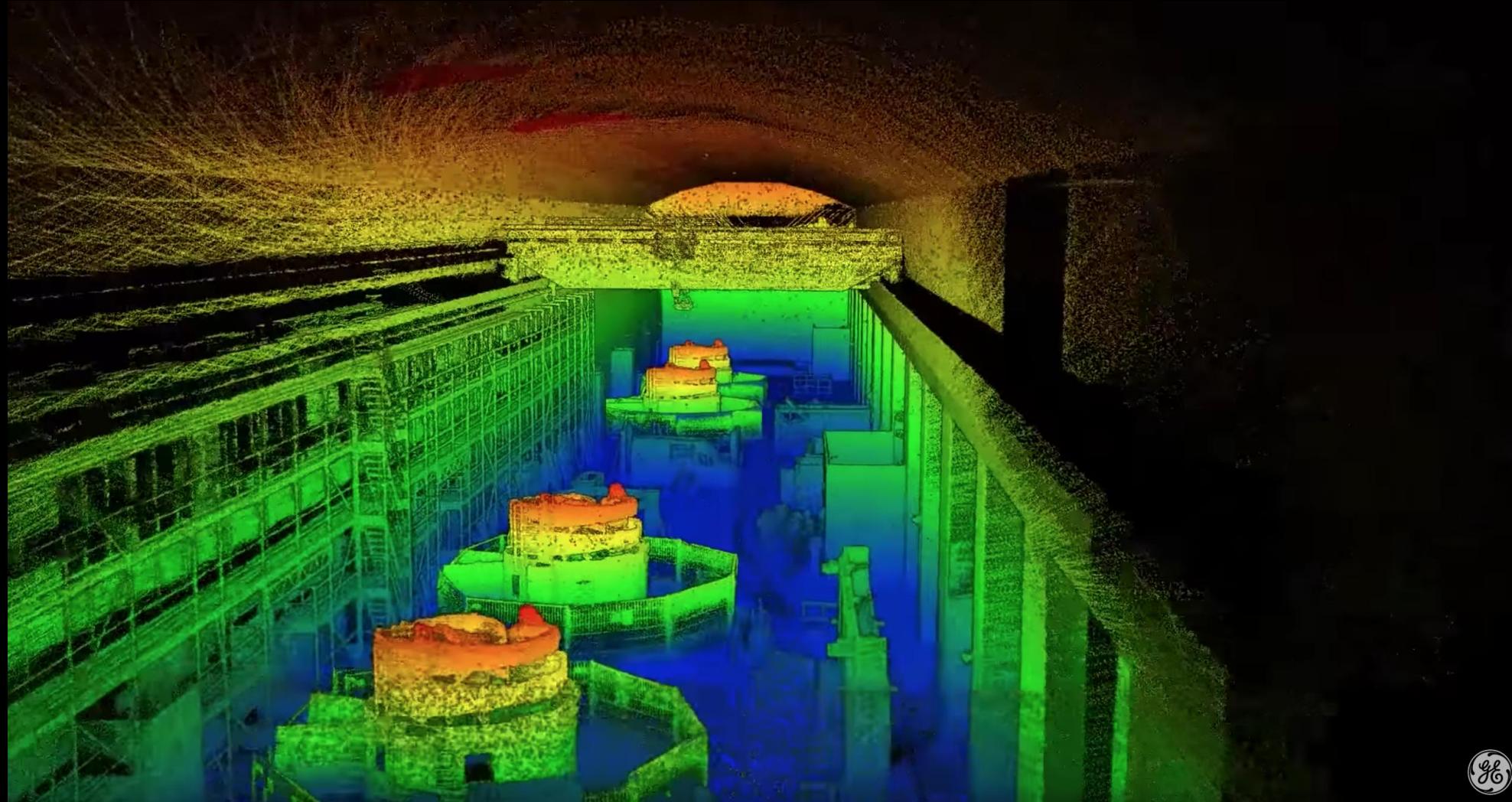
GE Renewables

Largest and most powerful offshore wind turbine



GE Renewables

Better models to avoid unplanned downtime



GE Renewables

Alpine Battery



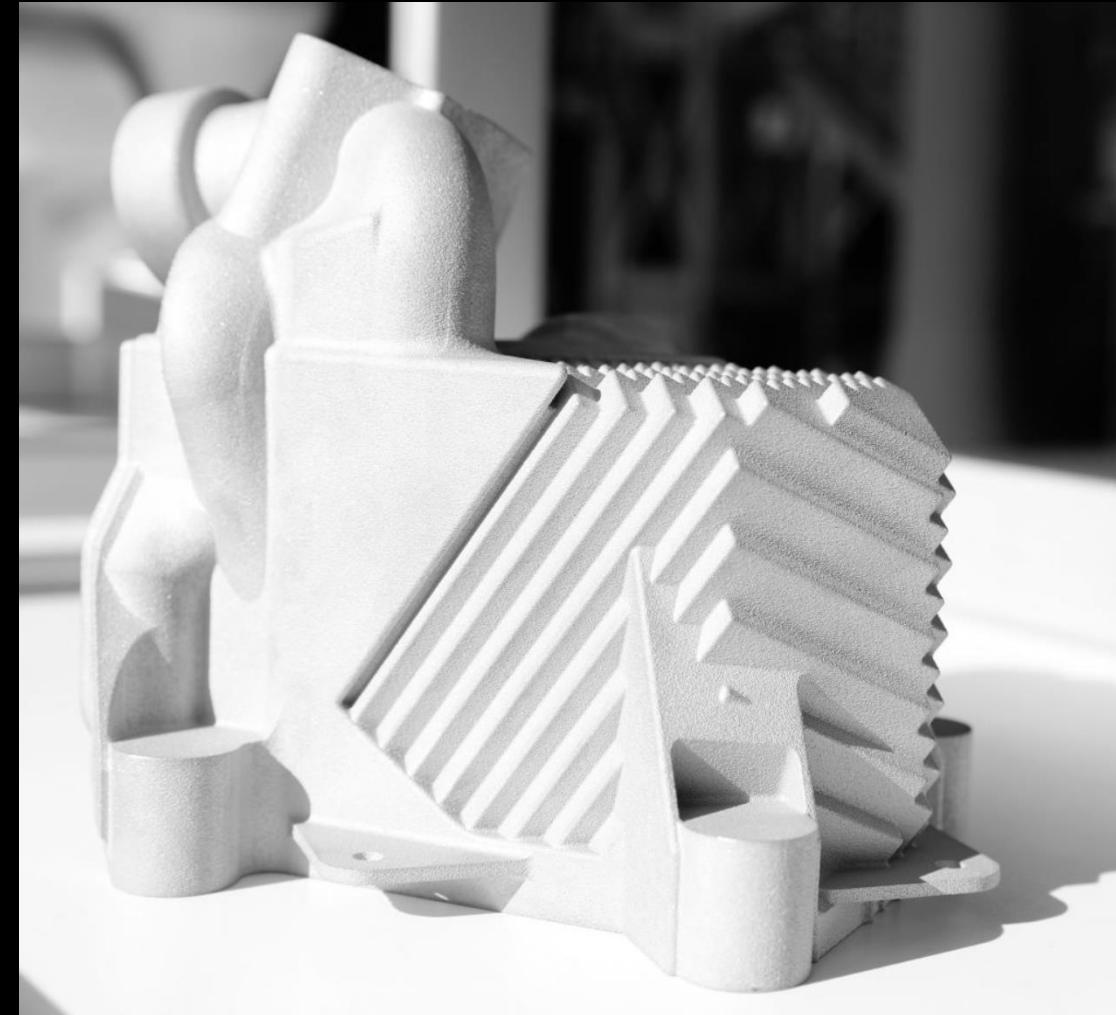
GE Aviation

Every 2 seconds a GE powered aircraft takes off



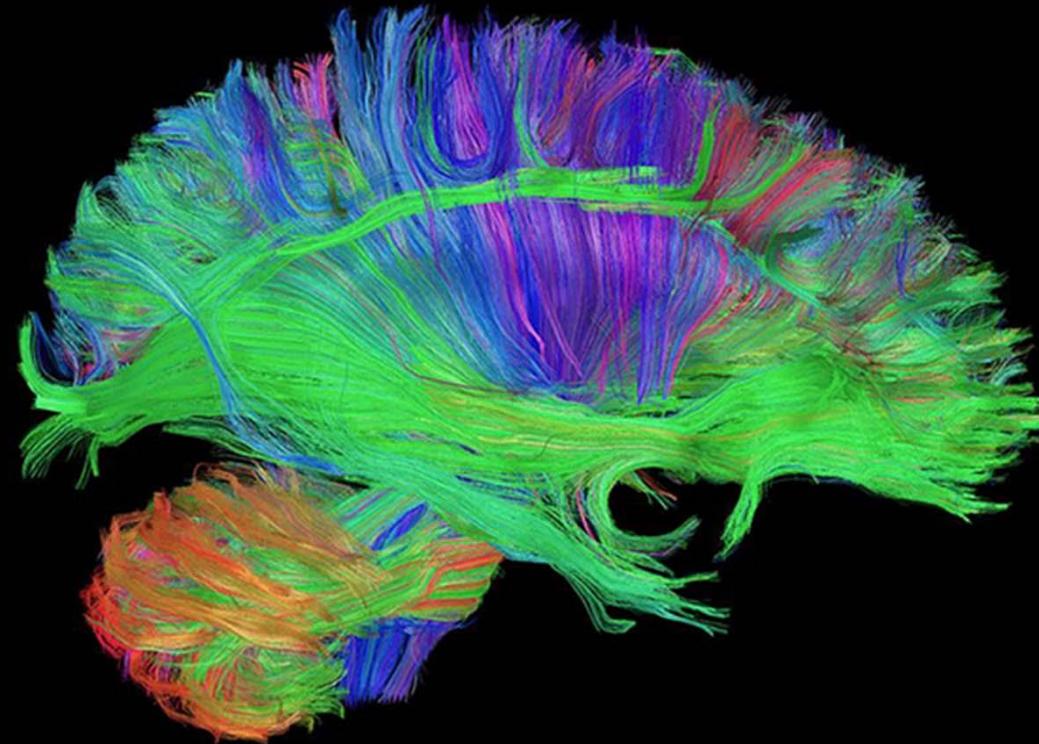
GE Aviation

Creating impossibly complex parts



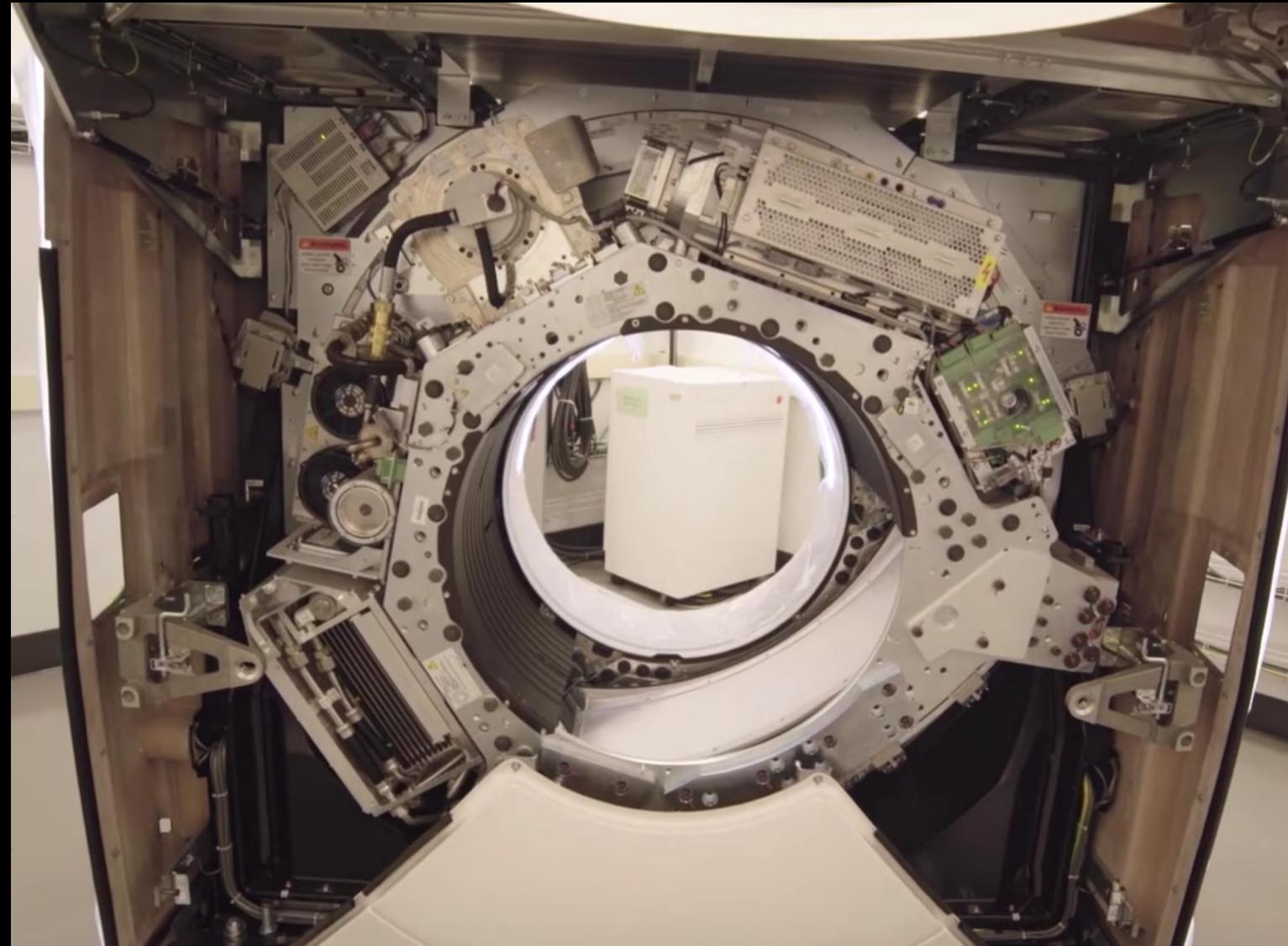
GE Healthcare

Medical Imaging and Cancer Moonshot



GE Healthcare

Medical Imaging

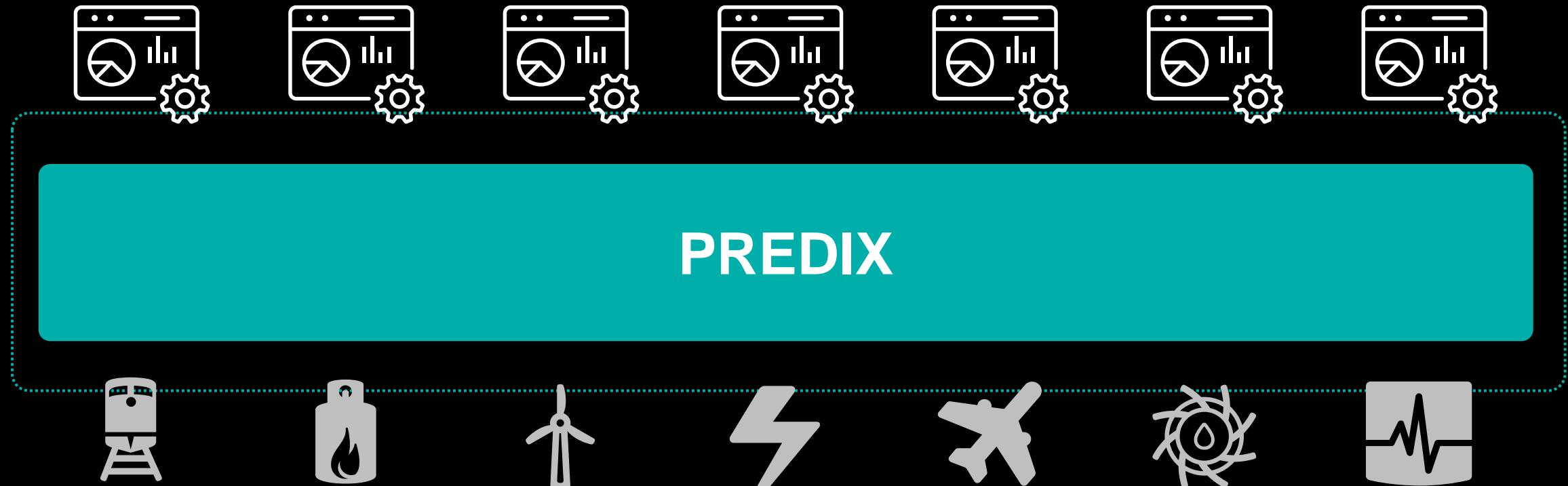


Industrial IoT at GE



GE Industrial IoT Platform

Industrial Applications



Industrial Assets

Implementation Landscape

Exciting Challenges!



splunk>



Cyber

PREDIX



Engineering



Support

Predix Journey with Splunk

Predix Platform service owners adoption of Splunk



12
TB/day
ingestion



Indexers,
1PB storage



Active users



Agents



Events per
day

138,60,4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F2-SW-a" 128,241,220,82 ~ [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=plus&itemId=EST_26&product_id=F2-SW-a" 317,27,160,0,0 ~ [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST_18&product_id=F2-SW-a" 468,125,17,14,30 ~ [07/Jan 18:10:57:187] "GET /oldlink?item_id=EST_6&JSESSIONID=SD10SLBF2ZADFF9 HTTP 1.1" 200 551 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_6&product_id=F2-SW-a" 10,7,10,10 ~ [07/Jan 18:10:57:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLBF2ZADFF9 HTTP 1.1" 200 551 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_6&product_id=F2-SW-a" 128,241,220,82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F2-SW-a" 128,241,220,82 ~ [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=plus&itemId=EST_26&product_id=F2-SW-a" 317,27,160,0,0 ~ [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST_18&product_id=F2-SW-a" 468,125,17,14,30 ~ [07/Jan 18:10:57:187] "GET /oldlink?item_id=EST_6&JSESSIONID=SD10SLBF2ZADFF9 HTTP 1.1" 200 551 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_6&product_id=F2-SW-a" 10,7,10,10 ~ [07/Jan 18:10:57:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLBF2ZADFF9 HTTP 1.1" 200 551 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_6&product_id=F2-SW-a"

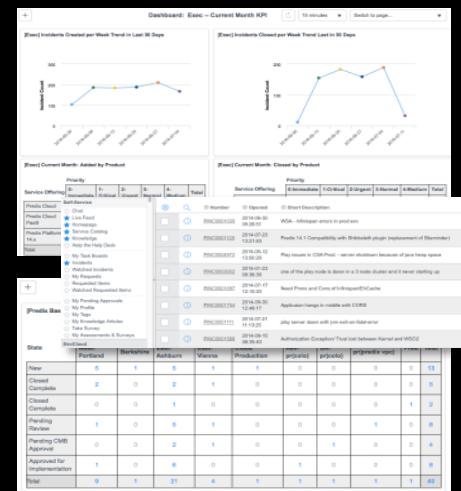
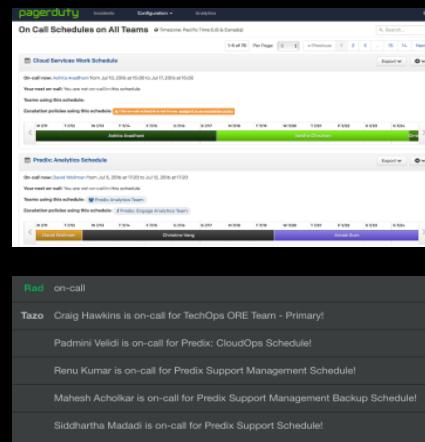
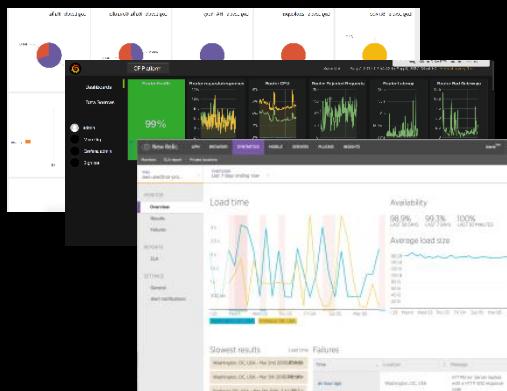
Strategies



Telemetry is good

Tool sprawl is not so good

- ▶ Logs, Metrics, App Trace, Synthetics
 - ▶ Notifications, Alarms
 - ▶ Ticketing, Incident management



splunk> .conf18

Meaningful telemetry is better

What problem are you trying to solve?



One source of truth to get to all of the data

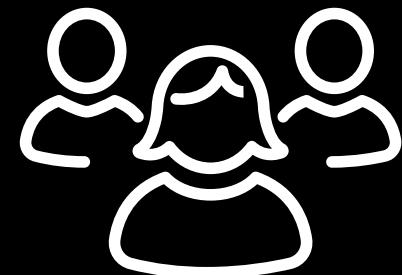
- ▶ Events
- ▶ Metrics
- ▶ Alerts
- ▶ Dashboards
- ▶ Enable SEIM
- ▶ 3rd party integrations

Execute with the smallest team possible

- ▶ Fewest tools to enable most teams
- ▶ Buy versus build
- ▶ On-prem versus SaaS
- ▶ Multi-cloud considerations

Service Ownership Framework

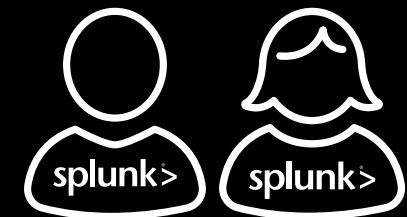
Accountability and Collaboration



SPLUNK Users



Shared Responsibility



SPLUNK Admins

Versatile Onboarding Approach

Key to Successful Self-Service



Wiki/Repo



Brown Bags



Help Desk



White Glove

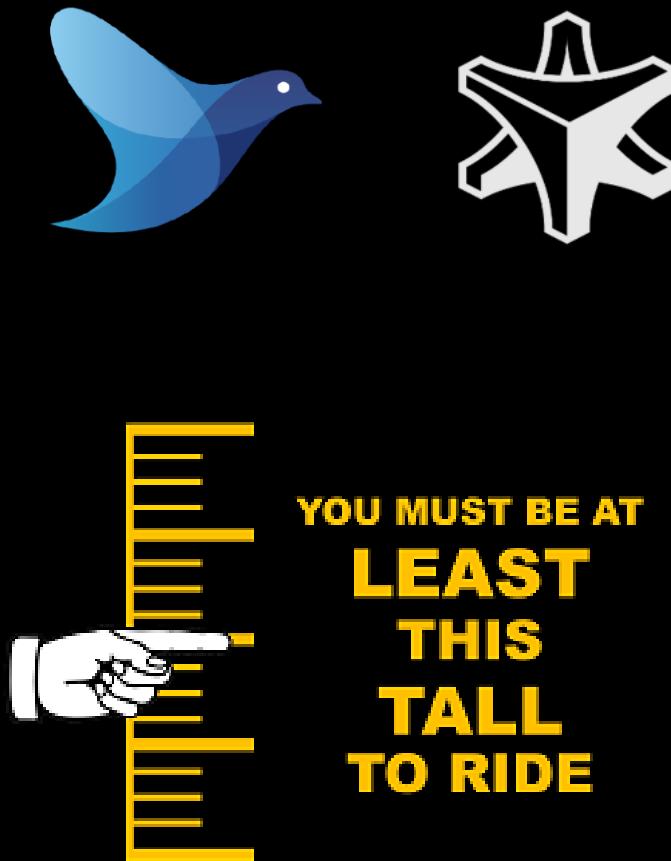


Do it or ...

Low Barrier to Entry

- ▶ Support a finite set of transport methods
 - ▶ Iterate onboarding
 - ▶ Start from pain points, not tools
 - ▶ Empower content creation
 - ▶ Celebrate small wins

“Perfection is the enemy of Good.”



Be DevSecOps Practitioners

Unless it looks and feels familiar, it's scary

The screenshot shows a GitHub repository page for 'PCE-CAP / tf_aws_splunk_infrastructure'. The repository has 481 commits, 44 branches, 1 release, and 19 contributors. The commit history lists several changes, including adding Appeng policy to Splunk, Azure initial commit, and adding .editorconfig and README files. A pull request titled '212559554' is shown, along with other pull requests and issues.

PCE-CAP / **tf_aws_splunk_infrastructure**

Terraform module to hold all splunk related infrastructure.

Add topics

481 commits 44 branches 1 release 19 contrib

Branch: master New pull request Create new file Upload files Find file Clone

212559554 Added Appeng policy to splunk

aws Added Appeng policy to splunk

azure/west-us Azure initial commit

.editorconfig Add .editorconfig to make sure all files have new lines.

.gitignore add architecture diagram to readme and add outputs of existing elbs for

PULL_REQUEST_TEMPLATE.md Create PULL_REQUEST_TEMPLATE.md

Predix_Reference_Architecture.png add architecture diagram to readme and add outputs of existing elbs for

README.md Describe folder structure

predix_eu_deployment.png Adding Readme

README.md

Predix Splunk Terraform

- ▶ Treat everything as code: infra, app config, app deploy, automation, content
- ▶ Build highly reusable code: no snowflakes
- ▶ Open access to github and wiki

Foster DevSecOps Culture

Unless it looks and feels familiar, it's scary

The screenshot shows a Jenkins pipeline interface for the 'Branch master' branch of the 'predix-splunk-ansible' project. The left sidebar contains navigation links like Up, Status, Changes, Build Now, View Configuration, Open Blue Ocean, Full Stage View, Job Config History, GitHub, Embeddable Build Status, and Pipeline Syntax. The main area displays the 'Stage View' for the 'Branch master' pipeline. It includes a summary of average stage times (29s) and full run time (~6min). Below this, a table shows four stages: 'Declarative: Checkout SCM' (29s), 'Checkout' (4s), 'Tar' (25s), and 'us-west-2' (1min 28s). To the left, a 'Build History' section lists recent builds, including #340 (Aug 21, 2018, 12:57, 2 commits), #339 (Aug 20, 2018, 15:37, No Changes), #338 (Aug 20, 2018, 15:07, 1 commit), #337 (Aug 17, 2018, 6:21 PM), #336 (Aug 16, 2018, 10:05 PM), #335 (Aug 16, 2018, 7:25 PM), and #334 (Aug 15, 2018, 5:17 PM).

- ▶ Use the same CI/CD pipeline
- ▶ Leverage as many common services as possible
- ▶ Achieved 30 minute full prod deploy

Agility by default

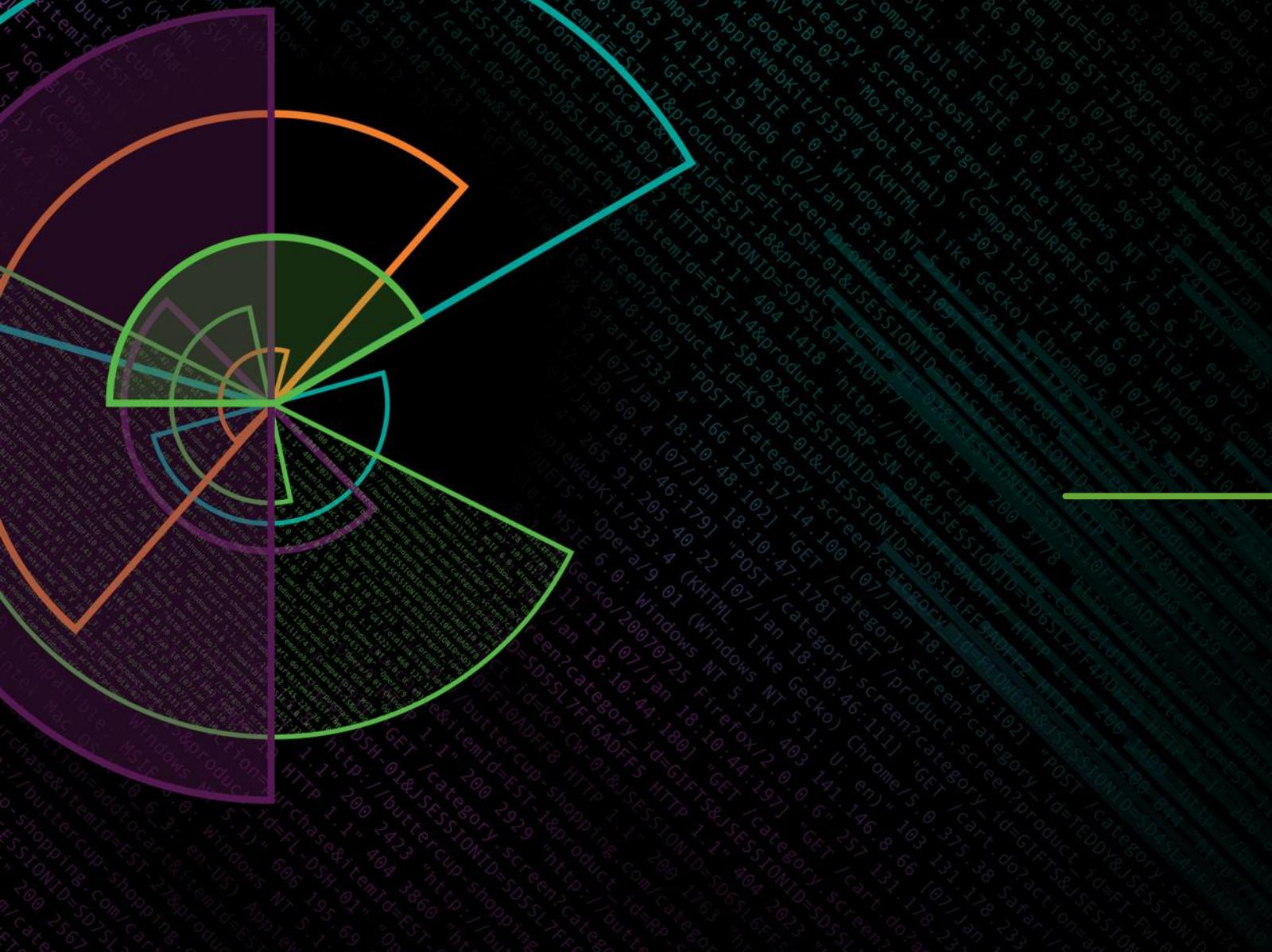
You're one PR away

The screenshot shows the Splunk Search Catalog Home page. At the top, it says "Splunk Search Catalog: Home". Below that is a welcome message: "Welcome to the Splunk Search Catalog! Use this app to explore and create Splunk Search Queries and Knowledge Objects that correlate to critical Predix services and events. This application is powered by a lookup table that is populated with queries for searches, dashboards and inventories. Select the button below to begin searching the catalog!" A green button labeled "Click to begin searching" is centered below the message. Below the message is a large word cloud of various keywords related to Splunk, Predix, and AWS services. Some prominent words include "predix", "app", "uaa", "service", "infrastructure", "support", "edge manager", "apm", "prod", "uua", "doc", "predix service", "aws", "us", "west", "cloud", "foundry", "data", "sources", "group", "deleted", "credentials", "group", "client", "update", "onboarded", "client", "delete", "file", "application", "shutdown", "gorouter", "policy", "account", "name", "public", "ip", "password", "change", "success", "spl", "metadata", "read", "license", "hosts", "added", "tenant", "troubleshooting", "client", "update", "success", "cloud", "foundry", "client", "create", "success", "authorization", "failure", "blobstore", "external", "ip", "predix", "saas", "created", "admin", "guard", "duty", "received", "widget", "tms", "data", "storage", "account", "name", "spl", "tstats", "spl", "mvexpand", "service", "billing", "production", "overview", "identity", "provider", "listening", "on", "port", "logging", "registration", "setup", "billing", "spl", "mvappend", "timeseries", "system", "device", "model", "spl", "mvindex", "wazuh", "benchmark", "onboarded", "tenant", "public", "ip", "password", "spl", "mvindex", "events", "dashboards", "tables", "search_type", "count", "events", "86", "dashboards", "28", "tables", "11", "Total Searches: 124", "Total Keywords: 225".

- ▶ Internal community contributions welcome
- ▶ Teams can create their own apps
- ▶ Or contribute to a platform app we built
- ▶ Anyone can make a pull request

Tomorrow

What's Next?



When we have table stakes covered

All the data in one place



Cyber SIEM integration Endpoint protection



DevOps + Support

Platform and Service Monitoring

Troubleshooting

Problem Discovery



IT Operations
Rapidly resolve RCAs
Safe ad-hoc searches

Beyond Preventative

True business insights



Drive Operational Excellence
Predictive Analysis
Proactive Operations
Runbook automation



Broad Correlation
Continuous Performance Testing
Transaction Tracing
Cost to Serve



Predix Customer Sat
Deep Business Insights
Tie Business Catalog to Operations
System of Record

Key Takeaways

You already know how

1. Automate
2. Cultivate Culture
3. Evangelize