Industrial Control Systems (ICS) Monitoring

October 2018

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> .conf18

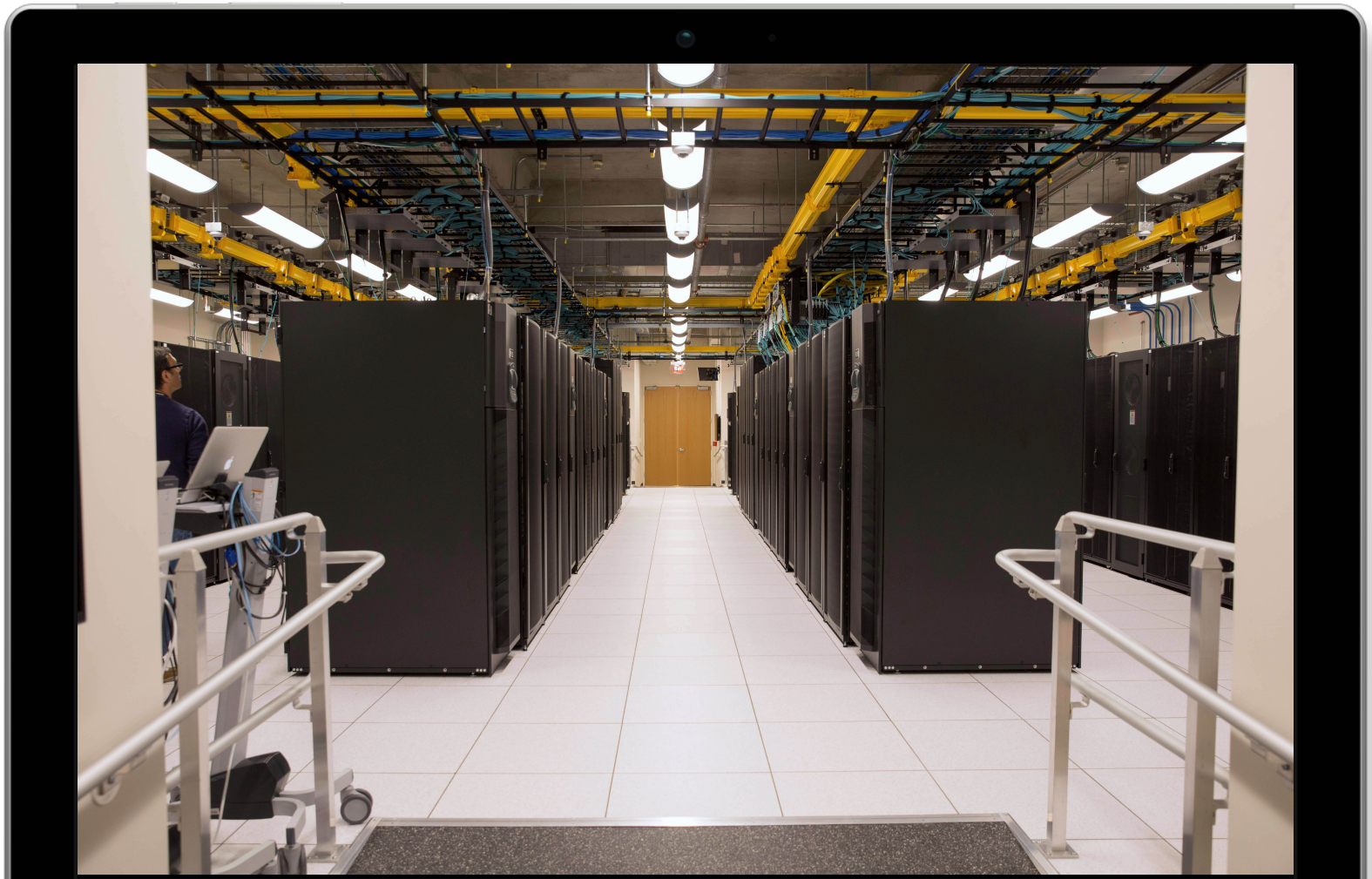
Why Infrastructure Monitoring?

Industrial Control Systems

- Power & cooling infrastructure
  - Foundational and critical to reliable application service delivery
  - Typically the domain of facilities and building management
- Impact of service availability: Business $$$
- We've created value by bringing infrastructure and traditional IT operations data together in Splunk
  - Gain visibility into power delivery and cooling system operation using the features of Splunk we use every day to analyze network and security data
  - Understand the demands that new equipment deployments and compute jobs place on the underlying infrastructure
  - Visualize the data from across all these systems in a way that makes it easy to understand and correlate

Our Environment

Data Center



- 60 Racks
- Hundreds of servers and network elements
- Mission-critical services for network security and operations

Our Supporting Infrastructure

Power, Cooling, Leak Detection, Temperature & Humidity

- Rack Power (3-phase 400V)
  - 2 550kVA Uninterruptable Power Supplies
  - 2 480 to 400V Transformers
  - 4 Power Submeters
  - 120 PDUs (2 per rack)

- Cooling Power (3-phase 400V)
  - 2 Automatic Transfer Switches

- Cooling (chilled water)
  - 20 In-Row Coolers

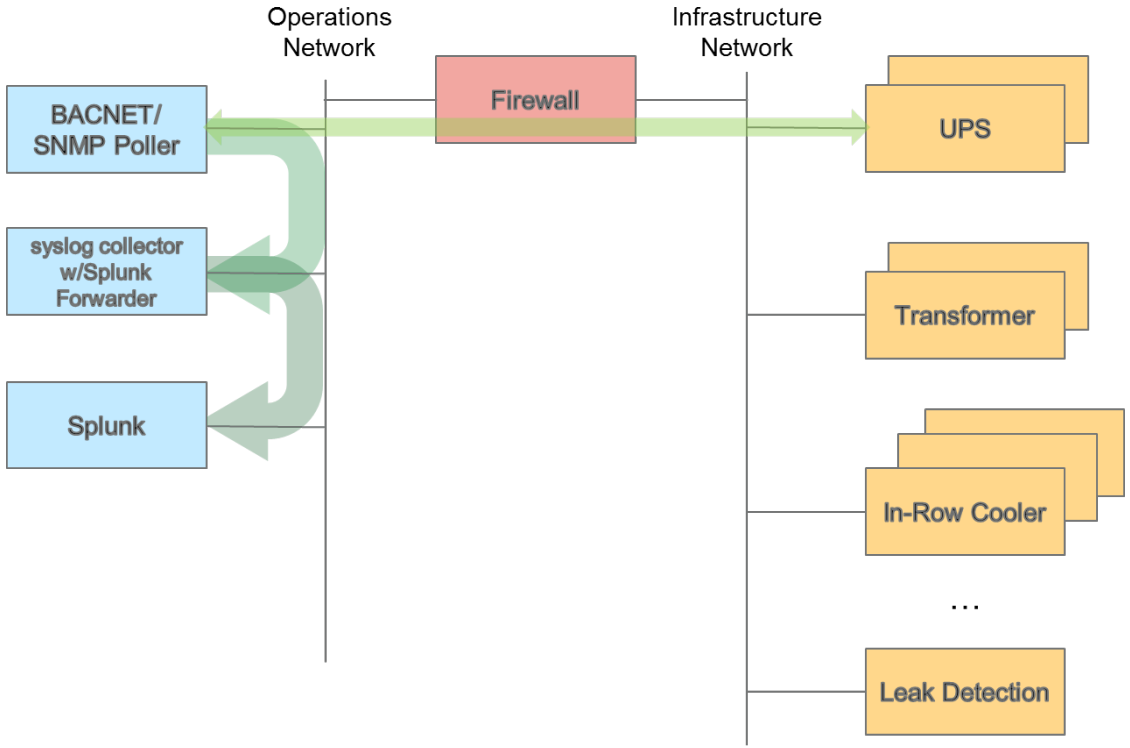
- Leak Detection
  - 2 Leak Detection Panels (covering 3 under-floor zones)

splunk> .conf18

Our Approach

Power, Cooling, Leak Detection

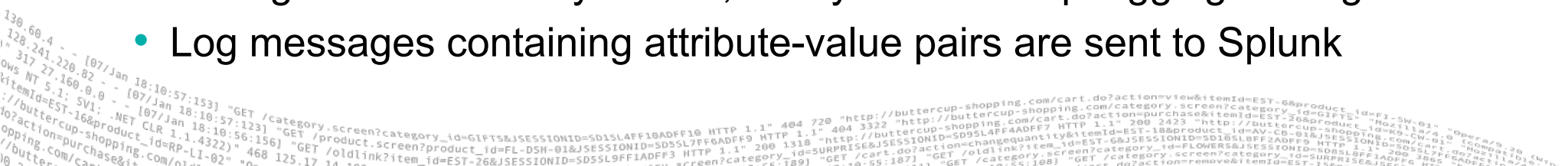
- Move infrastructure management interfaces to a protected, dedicated infrastructure network
  - Extend network presence to device locations
  - For security, infrastructure network is protected with firewall; only reachable from specified management hosts
- Poll infrastructure devices and put data into Splunk
  - Use same Splunk instance as operations data
  - Use Splunk search and reporting features to analyze data and dispatch infrastructure related alarms



Getting Data From Infrastructure Devices

Tools & Process

- SNMP
  - Net-SNMP open-source SNMP implementation
  - http://net-snmp.sourceforge.net
  - snmpget/snmpwalk utilities
- BACnet
  - BACnet Stack open-source BACnet implementation
  - http://bacnet.sourceforge.net
  - bacrp (ReadProperty) and bacrpm (ReadPropertyMultilple) utilities
- Use simple cron-dispatched shell script to poll devices
  - Small virtual machine with access to our private infrastructure network does all polling
  - Configured via table of attribute names and SNMP/BACnet object identifiers
  - Polling broken down by device, subsystem to keep logging manageable
  - Log messages containing attribute-value pairs are sent to Splunk



Sample Output

ATS polling attribute=value pairs

- Sep 11 16:00:01 vm-infrapoll ats[8632]: ats=ats-1 subsys=switch s1_volt_ab=477.000000 s1_volt_bc=472.000000 s1_volt_ca=480.000000 s1_freq=600.000000 s1_avail=active s1_pos_status=active s2_volt_ab=477.000000 s2_volt_bc=475.000000 s2_volt_ca=482.000000 s2_freq=600.000000 s2_avail=active s2_pos_status=inactive alarm=inactive auto_xfer_relay=inactive ats_not_auto=inactive num_xfers=15.000000
- Sep 11 16:00:02 vm-infrapoll ats[9652]: ats=ats-1 subsys=output rms_total_pwr=3536.389160 rms_total_pf=0.955148 rms_total_current=5.672077 rms_total_freq=60.029278 rms_a_pwr=1641.914551 rms_a_pf=0.771137 rms_all_voltage=474.008026 rms_aIn_voltage=274.337067 rms_a_current=5.986353 rms_b_pwr=1496.192871 rms_b_pf=0.690733 rms_bll_voltage=473.786957 rms_bIn_voltage=274.034943 rms_c_current=5.459862 rms_c_pwr=1529.051758 rms_c_pf=0.705848 rms_cll_voltage=477.158844 rms_cIn_voltage=274.347626 rms_c_current=5.575140

Adding Devices

The most time consuming aspect

- Adding a new device
  - Comb through vendor MIBs (SNMP) or register maps (BACnet) for objects of interest
  - Add attribute name, object identifier to polling script configuration tables
- Analogous to building management system (BMS) driver development
- Benefits
  - Initial upfront effort but lays the foundation to add new devices more easily later
  - Agility - No professional services engagement for new devices
  - Cost savings - No additional costs associated with polling additional attributes

Custom Dashboards

Splunk Dashboards

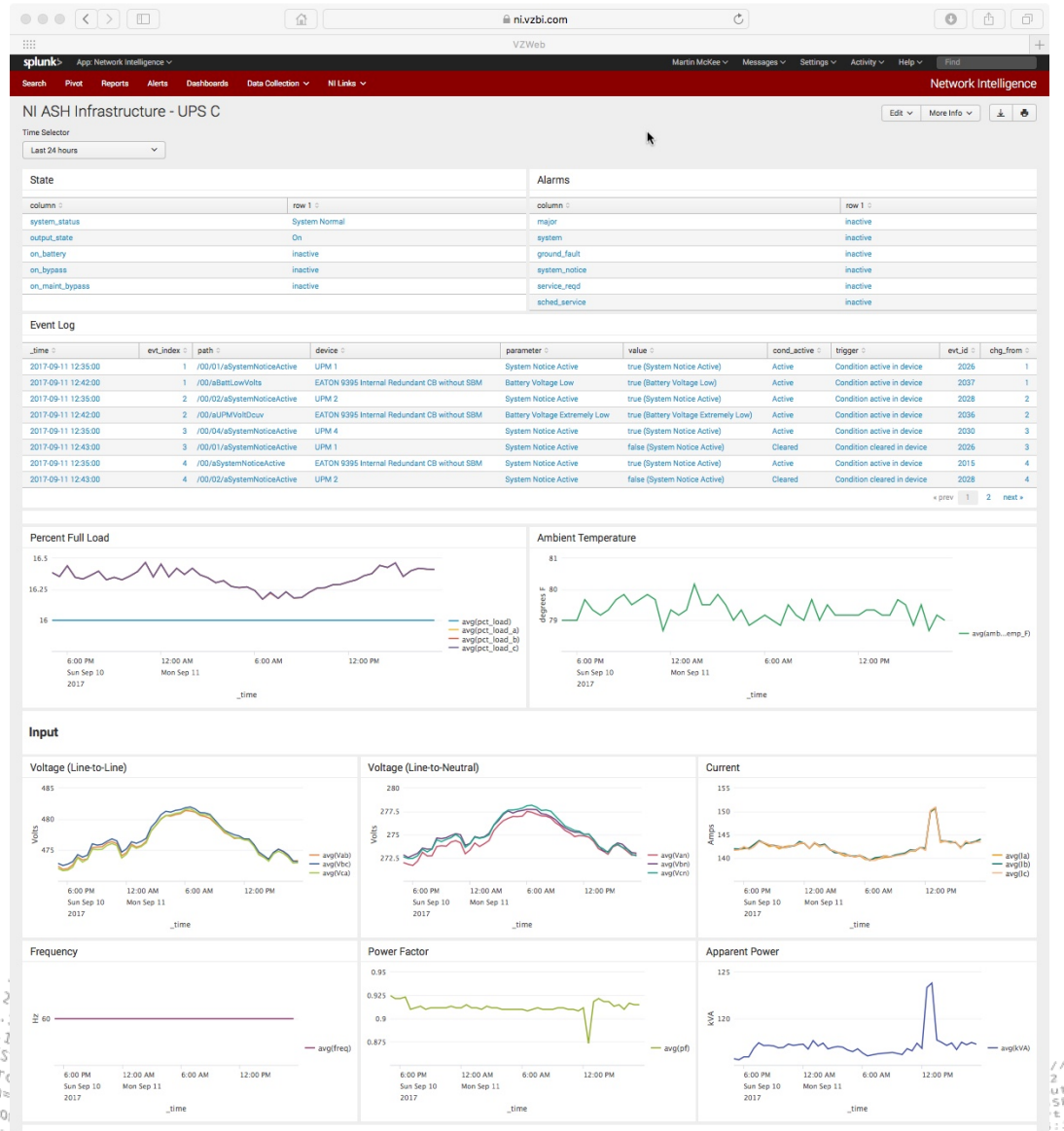
- Dashboards provide us the flexibility to present data on complicated infrastructure elements in a way that makes them easy to understand and relate to our environment
- With the understanding of how these systems are linked, we are able to develop dashboards that:
  - Detail all stages of power delivery from the street all the way to the racks
  - Relate CPU load, power draw, and temperature per rack
  - Reconcile inputs/outputs of linked systems
- Dashboards have provided us with a thorough understanding of our entire data center environment
- Developed concise dashboards for wall display panels in the data center for constant at-a-glance infrastructure status information

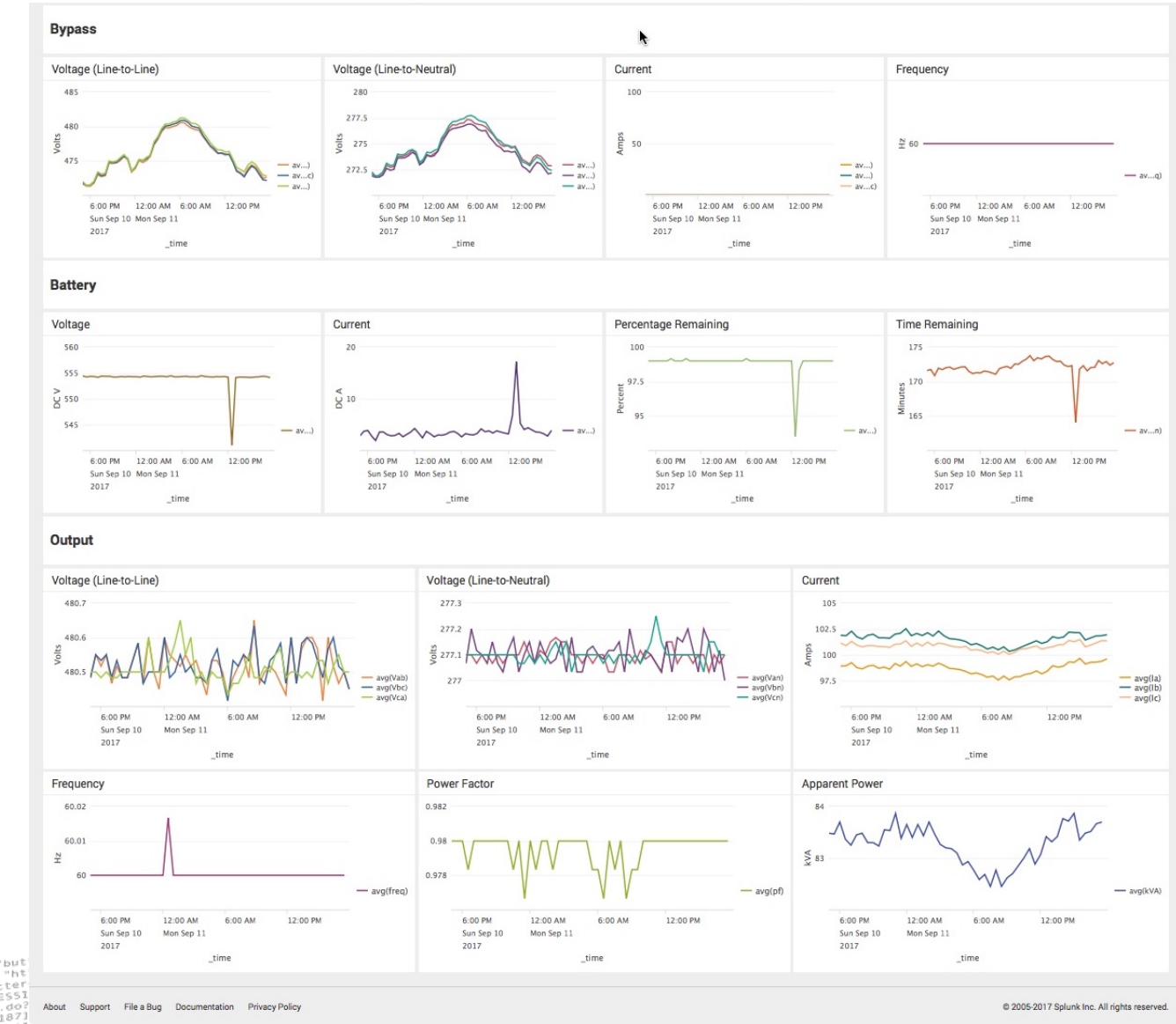
Custom Dashboard

Automatic Transfer Switch

Custom Dashboard

UPS





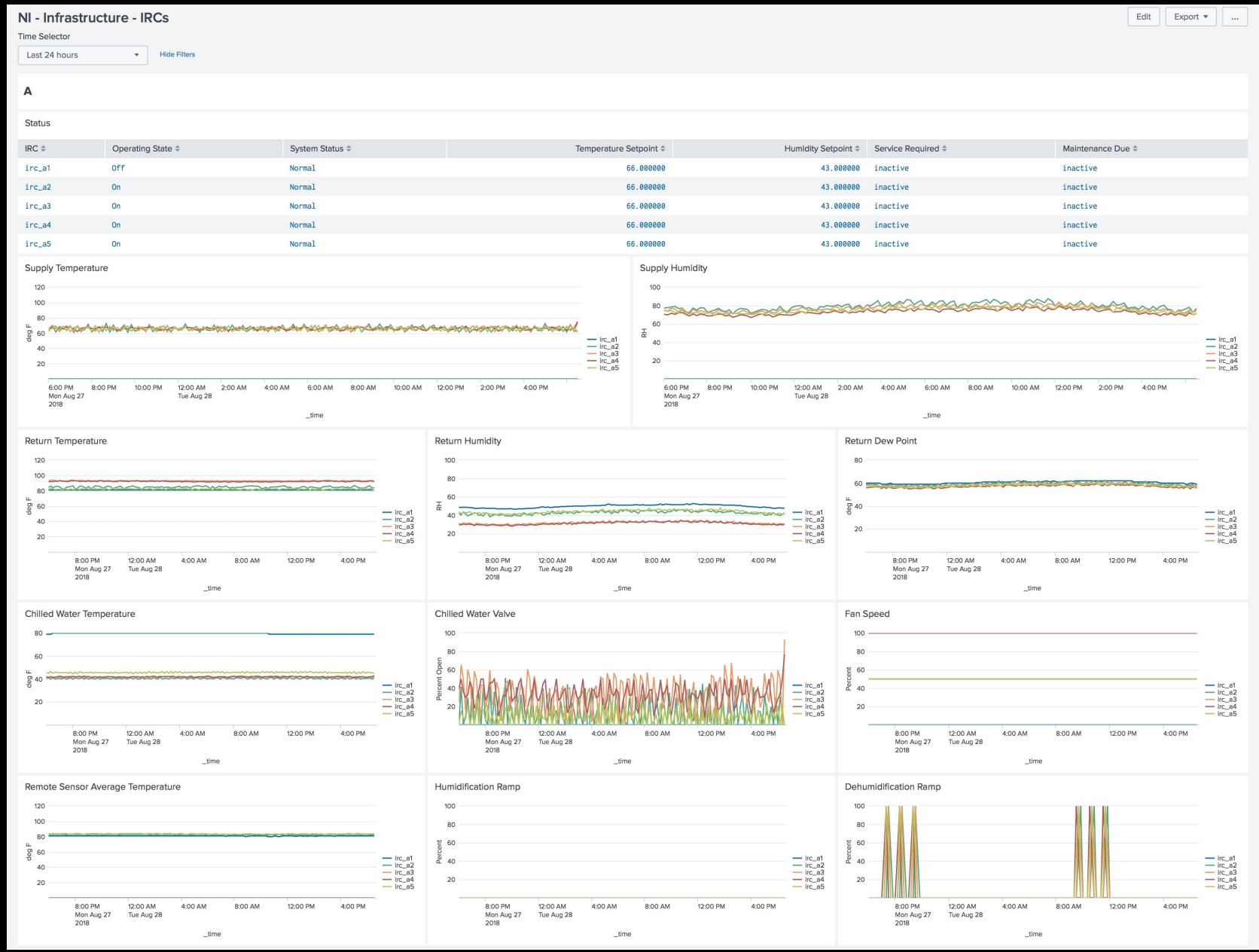
UPS Dashboard

Power Outage

Distinct voltage & frequency signature of generator activity

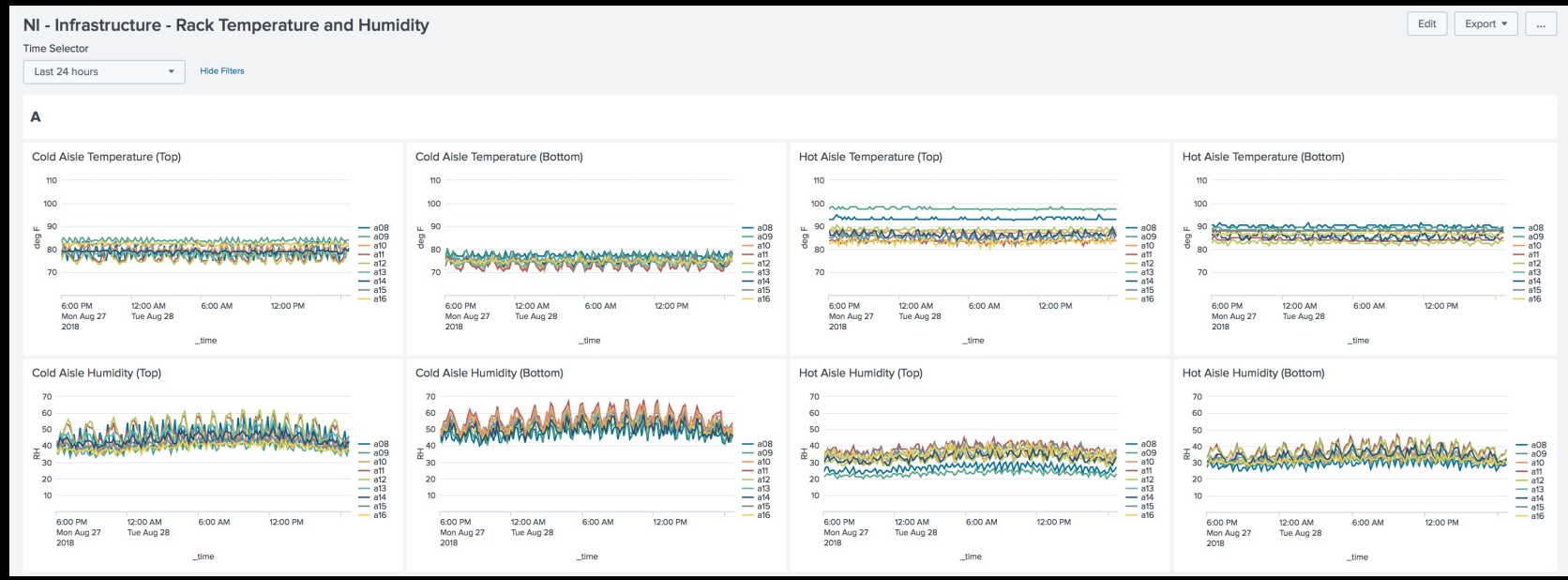
Custom Dashboard

In-row Coolers



Custom Dashboard

Temperature & Humidity



splunk> .conf18

Custom Alert Action

Meaningful alert notifications

- Email building facilities and operations staff for device alarms and threshold based alerts
- Extract values from search results to provide an easily understood, detailed description of the alarm and suggested course of action
- Facilities addresses the building infrastructure issue
- Operations staff can mitigate the impact to service delivery, if necessary

One or both of the UPSes that delivers power to the data center are running on battery. This condition would indicate that there has been a power failure and the campus generator is _*not*_ delivering power.

Pay careful attention to **time_remain** (battery time left in seconds). If both UPSes are impacted and the generator does not come online, data center equipment will need to be shut down before the battery is depleted.

```
Sep 6 17:15:01 vm-infrapoll ups_battery[9468]: ups=ups-c subsys=battery DCV=525.199951 IDC=8.899994
pct_remain=95.000000 time_remain=7567 energized=active current_limit=inactive check_batt=inactive
check_batt_ground=inactive voltage_low=inactive voltage_extreme_low=inactive voltage_high=inactive
total_discharge=inactive unable_to_charge=inactive on_battery=active
```

splunk> .conf18

Custom Alert Action

Voice Call – Text to Speech

- Facilities staff prefers call-outs in addition to messaging for after-hours alarms
- Created custom alert action to place a voice call via outbound calling service
  - Extract values from search results to provide an easily understood, detailed description of the alarm; service converts text to a voice message

    “Leak detected in zone 1 at 20 feet in the data center […]”

    “UPS A is currently running on battery with 50 minutes capacity remaining […]”
  - Call launched through simple REST API from custom alert action
  - Calling service provides call delivery status info (answer, no answer, voicemail, call duration, etc.)

    Call delivery status logged to Splunk for tracking of alarm dispatch and response

Conclusions

- We now have a comprehensive view into every aspect of the infrastructure that enables delivery of our services
- We've gained a much better understanding of our power and cooling infrastructure, making us more informed customers when dealing with our facilities staff, landlord, and vendors
- There is significant value in combining traditional IT operations data with building infrastructure data
  - Relate computational activity to demands on the power and cooling infrastructure
  - Understand the impacts of building infrastructure events on the compute infrastructure

Next Steps

- Lots of potential to be explored with Splunk features
  - Predict command
  - Splunk Machine Learning
  - Are there other data sources needed to help with ML?

Questions or Suggestions?

Thank You

Don't forget to rate this session in the .conf18 mobile app