Using Data Science to Proactively Manage the Connected C-Store

Presenters:

Ashwin Swamy, Omega ATC

Thomas Duncan, Omega ATC

CONEXXUS

solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 15 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact arussell@conexxus.org for questions regarding a certificate of webinar attendance.

Email: **info@conexxus.org**

CONEXXUS
solve forward

Presenters

Conexxus Host
Allie Russell
Conexxus
arussell@conexxus.org

Moderator
Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speakers

Ashwin Swamy

Director of Cyber Resilience, Omega ATC
ashwin.swamy@omegaatc.com

Thomas Duncan

Senior Security Strategist, Omega ATC
thomas.duncan@omegaatc.com

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS
solve forward

2019 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 24, 2019	Who's Watching Your Network? What you should know about Managed Detection & Response (MDR)	Mark Carl Tom Callahan	ControlScan
February 28, 2019	Protect Your Business: PCI Resources for Securing Payment Data	Elizabeth Terry	PCI Security Standards Council
March 21, 2019	Proactive Defense in Depth	Brett Stewart DeWayne Mangan Mark Palmer	Acumera
May 30, 2019	Firewalls, LANS & WANS The Basics, The Benefits and The Security!	Simon Gamble	Mako Networks
June 27, 2019	Web Payment Asipirations	Ian Jacobs	W3C
July 25, 2019	Skimming	Linda Toth Paige Anderson Caleb Burke	Conexxus NACS CITGO
August 8, 2019	Application Security 101	Denis Sheridan	Synopsys

CONEXXUS
solve forward

2019-2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
August 29, 2019	Don't Get Phished!! Train Your Employees To Avoid Ransomware	Geoffrey Vaughan Ed Adams	Security Innovation
September 26, 2019	Using Data Science to Proactively Manage the Connected C-Store	Ashwin Swamy Thomas Duncan	Omega ATC Omega ATC
October 24, 2019	Easy PCI—How to Make PCI & Attestation Easier	Ajith Edakandi	Hughes
November 21, 2019	Applicability of PCI DSS requirements for Merchants and MNSP's	Sam Pfanstiel	ControlScan
December 5 and 12, 2019	EMV	TBD	TBD
January, 2020	TBD	TBD	Cybera

CONEXXUS
solve forward

NACS Show
October 1-4, 2019
Atlanta, GA

TECHEDGE

In partnership with CONEXXUS

Booth # 3755

Conexxus thanks our 2019 Annual Diamond Sponsors!

mSHIFT. Relevant. Mobile. Solutions.

Stuzo

Diebold Nixdorf

wex

HUGHES An EchoStar Company

GILBARCO VEEDER-ROOT

Cybera

SECURITY INNOVATION

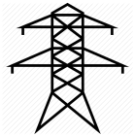
CONEXXUS solve forward

Using Data Science to Proactively Manage the Connected C-Store

CONEXXUS
solve forward

Using Data Science to Proactively Manage the Connected C-Store

Difficulties with managing connected and IoT devices.



Using industry analogs to navigate a digital transformation.

Use cases for more effectively managing the connected petroleum retail environment.

Tips for experimenting with predictive maintenance approaches.

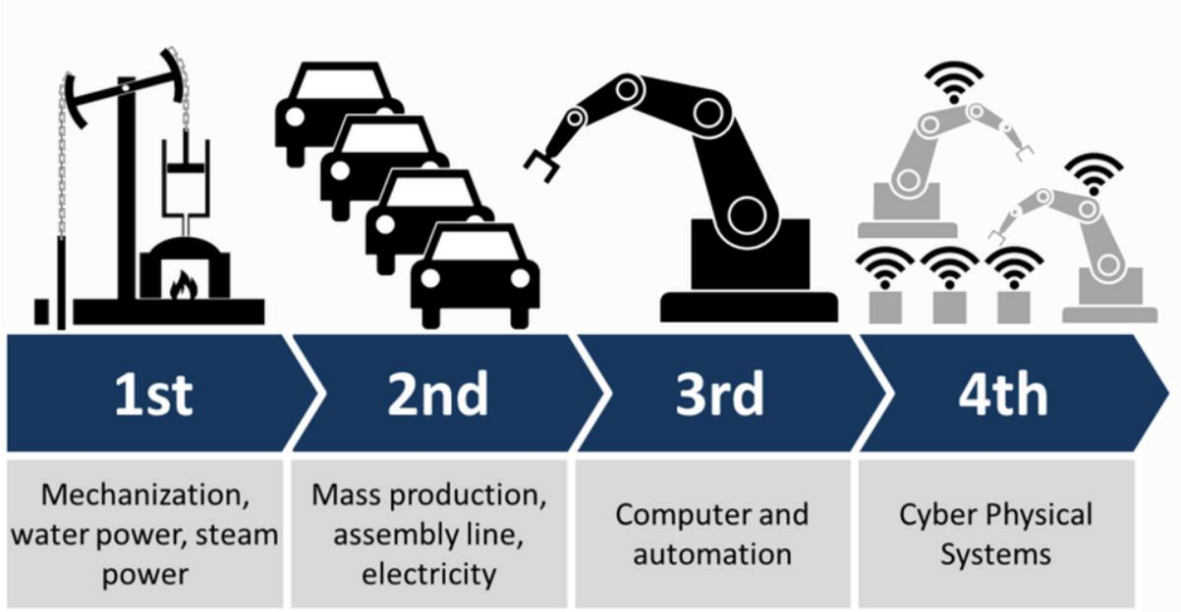
CONEXXUS
solve forward

The Fourth Industrial Revolution is in its earliest stages.

4IR

1. Big Data
2. Internet of Things
3. Artificial Intelligence
4. Robotics
5. Autonomous Transport
6. Augmented Reality

- Gray Taylor
(September 2018)



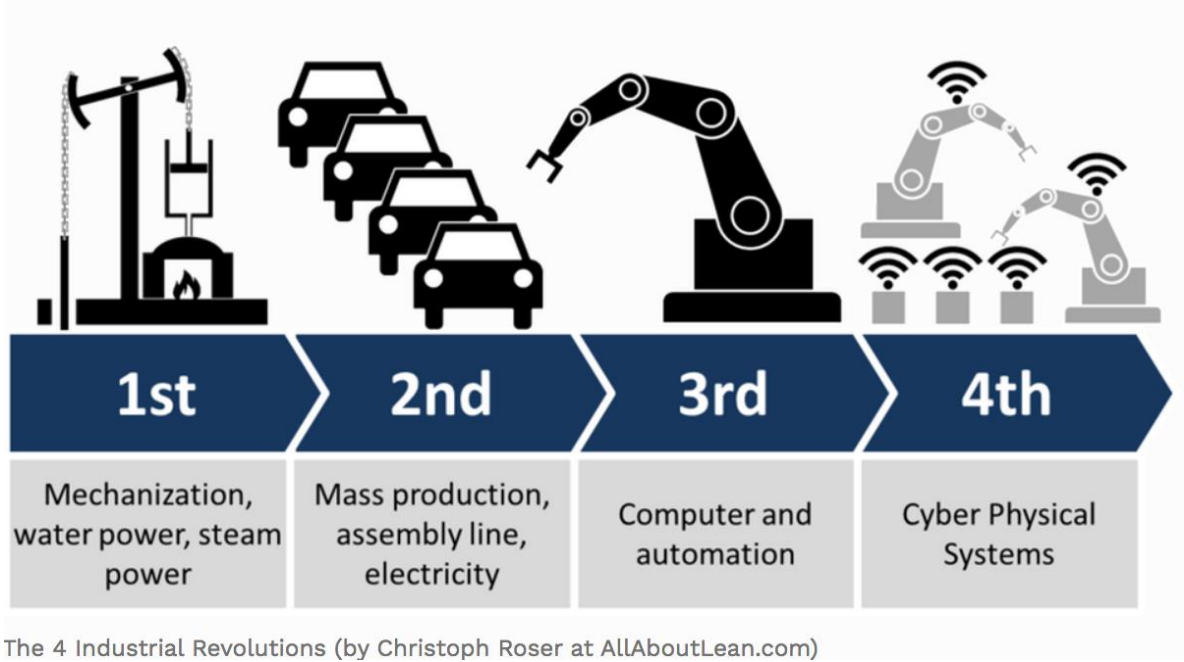
The 4 Industrial Revolutions (by Christoph Roser at AllAboutLean.com)

The Fourth Industrial Revolution is in its earliest stages.

4IR

1. Big Data
2. Internet of Things (IoT)
3. Artificial Intelligence
4. Robotics
5. Autonomous Transport
6. Augmented Reality

- Gray Taylor (September 2018)



The 4 Industrial Revolutions (by Christoph Roser at AllAboutLean.com)

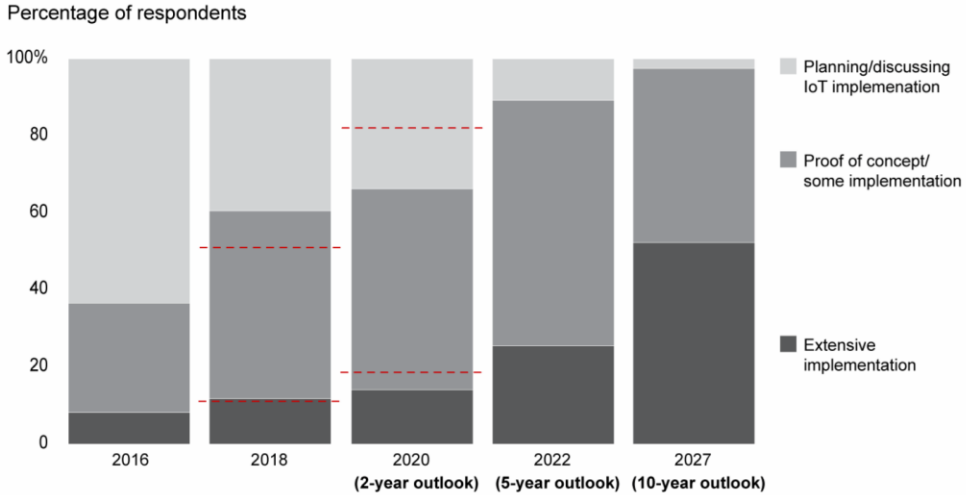
IoT adoption is in a holding pattern.

”…concerns over integration issues—in particular, technical expertise, data portability and transition risks—have become more acute over the past two years.”

- Bain IoT Customer Survey, 2018

Figure 1

The IoT outlook for 2020 has dampened, but long-term targets remain bullish



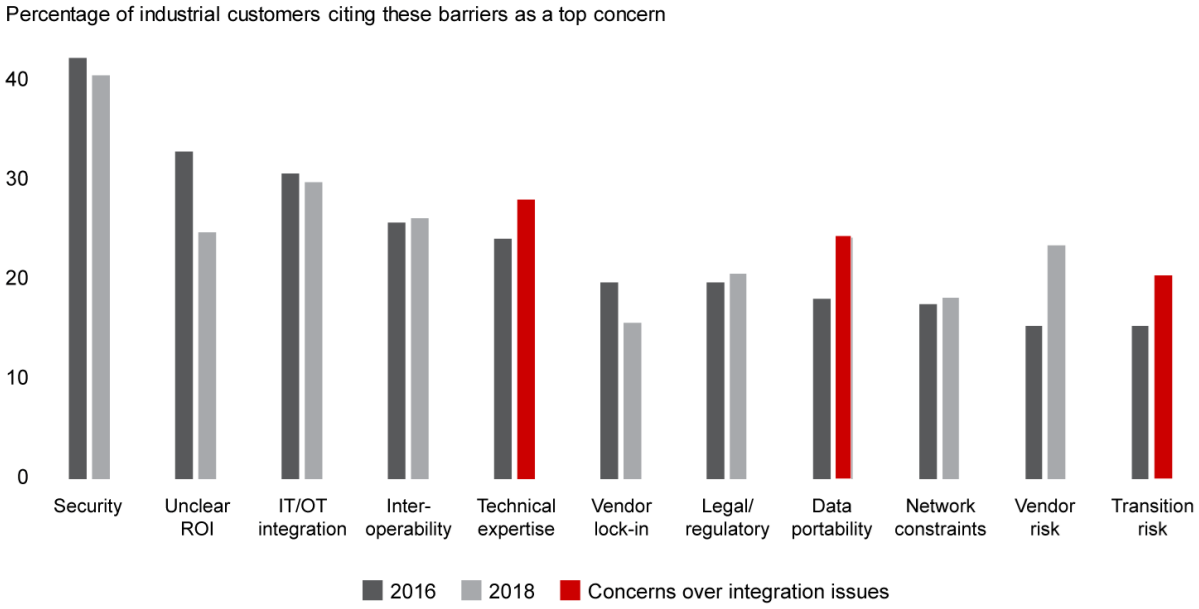
Sources: Bain IoT customer survey, 2016 (n=391); Bain IoT customer survey, 2018 (n=474)

CONEXXUS
solve forward

IoT adoption is in a holding pattern.

”…concerns over integration issues—in particular, technical expertise, data portability and transition risks—have become more acute over the past two years.”

- Bain IoT Customer Survey, 2018



Notes: Industrial segments include discrete manufacturing, process industries, production sites, building, infrastructure and utilities
Sources: Bain IoT customer survey, 2016 (n=533, industrial customers=182); Bain IoT customer survey, 2018 (n=627, industrial customers=329)

CONEXXUS
solve forward

The prospect of more devices is not always met with enthusiasm.

CONEXXUS
solve forward

The prospect of more devices is not always met with enthusiasm.

More devices out in the field means more servicing.

"I meet with the service team multiple times a week and get daily updates on the reliability of the vehicle. We -- the best service, of course, is no service. Like that's the vehicle just -- reliability and quality being so good that service is rarely required. That's what the main goal is like, eliminate the need for service."

- Elon Musk (July 26, 2019)

The predictive maintenance paradox

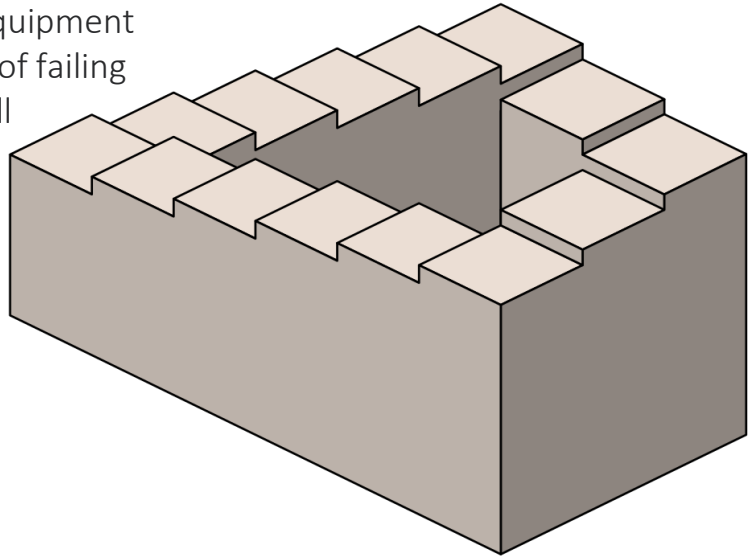
“Predictive maintenance is the prime example of a use case that vendors are ready to deploy, but customers are less excited about, as shown in the middle right panel. Its decline in attractiveness indicates customers face implementation barriers.”

- Bain IoT Customer Survey, 2018

The predictive maintenance paradox

We desire the ability to determine exactly when and why equipment or operations are at risk of failing in order to reduce overall maintenance costs.

In order to identify these signals, we require IoT devices to provide us with the data we need.



IoT devices inherently increase the number of failure points in the retail environment, and therefore can increase maintenance costs.

CONEXXUS
solve forward

Weighing the business case vs transition costs…

BUSINESS CASE

- Mitigate operational issues
- Easier Remote Management
- Better Customer Experience
- Safety improvements
- Reduced device failure rates
- Resource savings
- Better decision making

TRANSITION COSTS

- More frequent site visits
- Management hassle (another thing to deal with)
- Increase in number of operational issues and device failures
- Network issues
- Security issues

Microsoft and Amazon are making big bets on retail IoT.

Microsoft

"Announcing new Microsoft Dynamics 365 AI-driven insights applications and our vision for the future of retail."

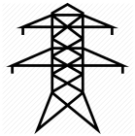
(September 23, 2019)

1. Aims to "help physical retailers understand and improve the in-store experience.
2. Analyze data from video cameras and the internet of things (IoT) sensors, which provide real-time and predictive insights to improve decision making.
3. Improve register experience, monitor refrigerator and freezer temperatures, etc.

How can we navigate this digital transformation in such a way that we realize the positive benefits and avoid the negative outcomes?

Using Data Science to Proactively Manage the Connected C-Store

Difficulties with managing connected and IoT devices.



Using industry analogs to navigate a digital transformation.

Use cases for more effectively managing the connected petroleum retail environment.

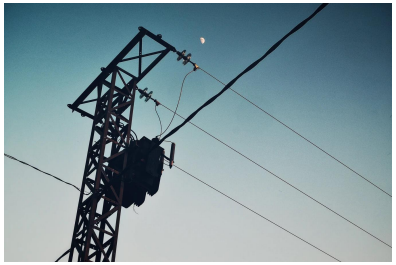
Tips for experimenting with predictive maintenance approaches.

CONEXXUS
solve forward

Other industries are undergoing similar transitions and can provide helpful analogs for managing complex and connected systems.

MANUFACTURING

Predicting device failures
(Condition-based maintenance)



ENERGY & UTILITIES

Outage management

TRANSPORTATION

Advanced Safety Systems

CONEXXUS
solve forward

Applying digital transformation lessons from other industries to convenience retail:

- CONDITIONED-BASED (PREDICTIVE) MAINTENANCE Identify features that can accurately determine the condition of in-service equipment in order to estimate when maintenance should be performed.

- OUTAGE MANAGEMENT Identify features that can help predict causes of outages and poor network performance; effectively model demand in order to help plan ahead.

- ADVANCED SAFETY SYSTEMS (SELF-HEALING) Implement backup/secondary processes that will automate responses when threats and issues arise .

The petroleum retail environment is critical to our country's resilience.

- "When most community residents are evacuating to safety, convenience stores typically remain in operation as long as they can without putting their own employees' safety and well-being in harm's way."
- "Their focus is to see how long can they stay open before the storm, and how they can be first to open when it is safe to do so—all while ensuring that they have power and supply. This means making sure fuel, food and other necessities are available for emergency workers and customers seeking a return to normalcy."

NACS DECEMBER 2017

CONEXXUS solve forward

The petroleum retail environment is critical to our country's resilience.

FEMA

CISA
CYBER+INFRASTRUCTURE

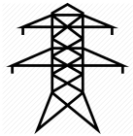
"There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Convenience stores fall into four categories:
Transportation, Emergency Services, Energy, Food and Agriculture,

CONEXXUS
solve forward

Using Data Science to Proactively Manage the Connected C-Store

Difficulties with managing connected and IoT devices.



Using industry analogs to navigate a digital transformation.

Use cases for more effectively managing the connected petroleum retail environment.

Tips for experimenting with predictive maintenance approaches.

CONEXXUS
solve forward

CONDITION-BASED MAINTENANCE

Using key signals to prioritize device maintenance and preempt device failures.

CONEXXUS
solve forward

How can we forecast device failures and avoid unnecessary and costly device maintenance?

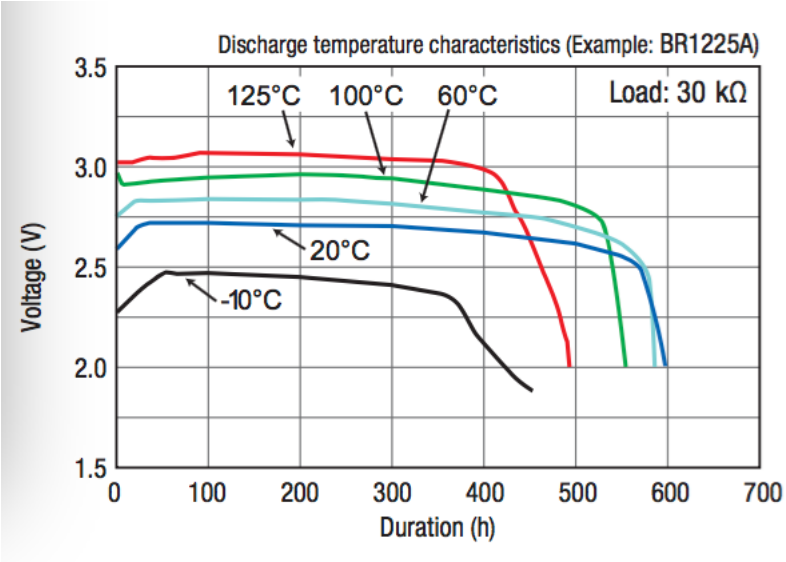
Condition-based maintenance for IoT.

1. When assessing an IoT device, start with its security. Ensure that it is (1) using secure communication protocols, the cloud environment (if it is cloud managed) has been thoroughly assed, and that the device itself will segmented away from the CDE.
2. Obtain the manufacturer's device info. Assess the parts to ensure they are up to standard, much as you would for ATGs.

    - CMOS battery
    - Processor type
    - Network Adaptor
    - Memory
    - Hard drive

Condition-based maintenance - study manufacturer information closely

1. Use data from the manufacturer to potentially set benchmarks and thresholds ahead of time.

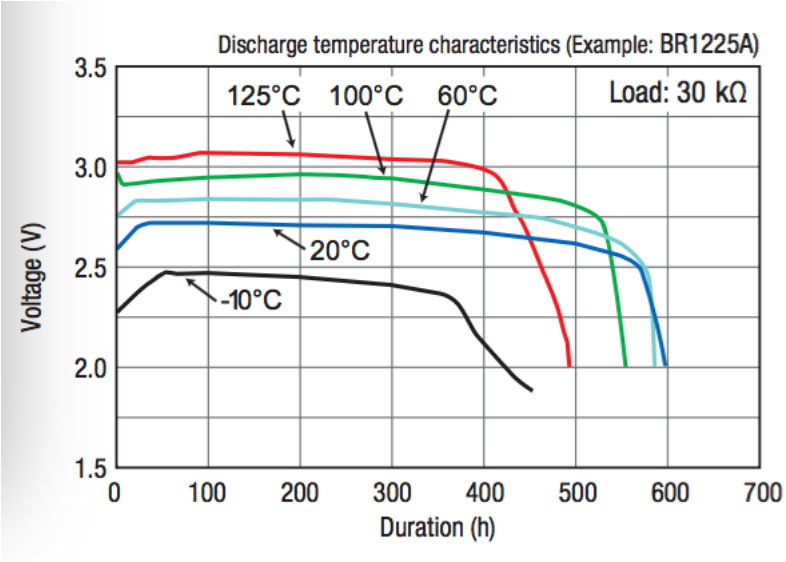


- Mean time to Failure (before purchase) and Mean time between failure
- Mean time to repair (total maintenance time/total number of repairs)

CONEXXUS
solve forward

Condition-based maintenance - study manufacturer information closely

1. Based on this information, start putting together an IoT device maintenance plan.



Condition-based maintenance - study manufacturer information closely

1. Measures like MTTF and MTBF are typically ranges (e.g. 2 – 5 years). This begs the question, what factors impact whether a device will fail at the lower end or higher end of the range?

Potential Features

- Device Temperature
- Device CPU/memory utilization
- Ping request responsiveness
- Battery/Power consumption (low battery)
- Other device alarms
- Previous maintenance activity

Condition-based maintenance – develop a plan to collect this data.

1. PCs at the store or another edge computing device, middleware, etc.
2. APIs available?
3. How are these devices networked locally?
4. How frequently should they be polled? 5 minutes, hourly, daily, weekly?
5. Setting thresholds.
6. What tools will analyze the data in the cloud?

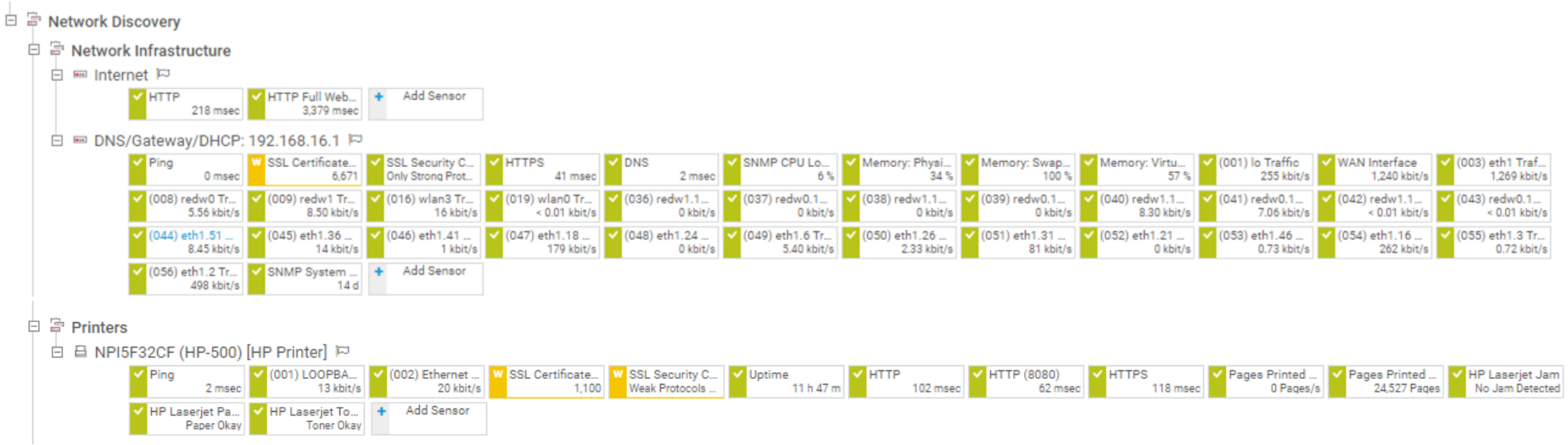
Securing Your Data

- Communication Protocols - Use industry best practice
  - Are outdated / insecure protocols in use?
    - SSL
    - Telnet
    - FTP
- Cloud environment assessment
  - What cloud environment are they hosting their servers on?
  - Do they have a vulnerability management program?
  - Do they have compliance attestations?
- Other best practices — segmentation
  - Segment IoT devices from CDE
  - Best practice to have a 3rd Party network segment

Collecting Data

- PC or Edge Computing device
  - Can the Back Office computer be used as a probe?
- Agent vs. Agentless
  - If software can be installed on the endpoint being monitored, typically more information is available
  - If software can't be installed, network probes can use available protocols to collect information
    - WMI
    - SNMP
    - Syslog
    - APIs (Calls to local devices or to cloud servers)
    - and more!

Use tools to collect data.



CONEXXUS
solve forward

Scripts!

python™

Windows Batch File

JS

```python
from pysnmp.hlapi import *
import sys


def walk(host, oid):
    for (errorIndication,
         errorStatus,
         errorIndex,
         varBinds) in nextCmd(SnmpEngine(),
                              CommunityData('public'),
                              UdpTransportTarget((host, 161)),
                              ContextData(),
                              ObjectType(ObjectIdentity(oid))):
        if errorIndication:
            print(errorIndication, file=sys.stderr)
            break
        elif errorStatus:
            print('%s at %s' % (errorStatus.prettyPrint(),
                                errorIndex and varBinds[int(errorIndex) - 1][0] or '?'),
                  file=sys.stderr)
            break
        else:
            for varBind in varBinds:
                print(varBind)


walk('192.168.1.52', 'iso.3.6.1.2.1.4.24.7.1.17.1.4.10.9.6.0.24.3.0.0.2.1.4.0.0.0.0')
```

CONEXXUS
solve forward

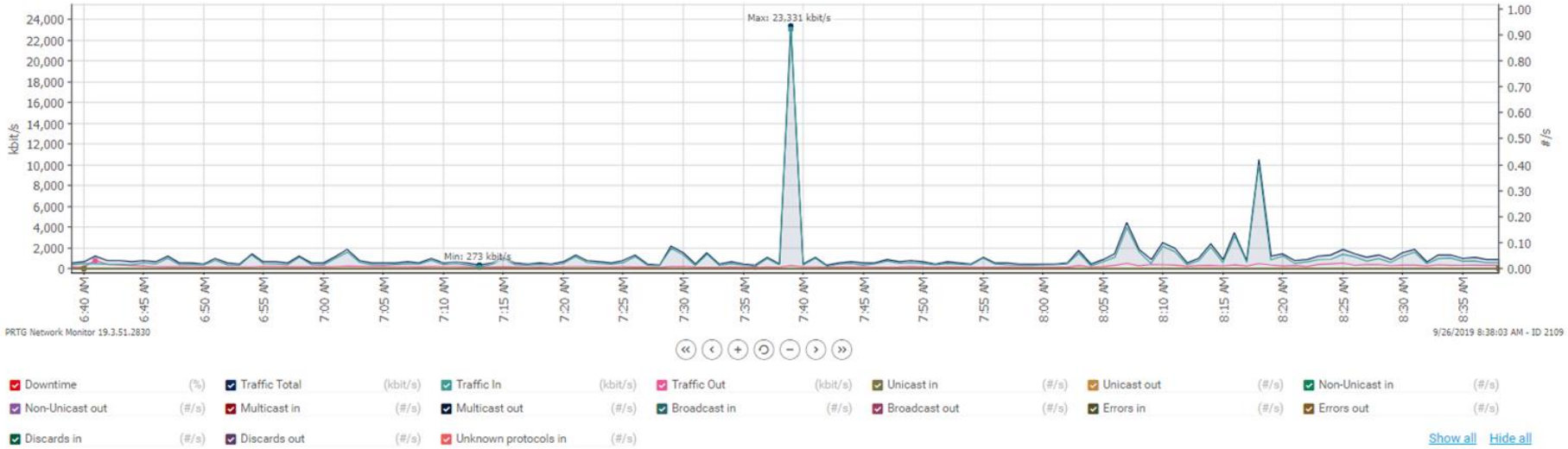
Sending Data to SIEM - Alerts vs Continuous Transfer vs. Reports

- Alerts
  - Can be used for real time issues
  - Small amount of network traffic
- Continuous Transfer
  - Real time information (not just issues)
  - Consistent network traffic
- Daily / Weekly results
  - Benchmarking
  - Performance review
  - Large amount of network traffic, but short amount of time
  - Use collected data to determine schedules for uploading data

What to do with this data?

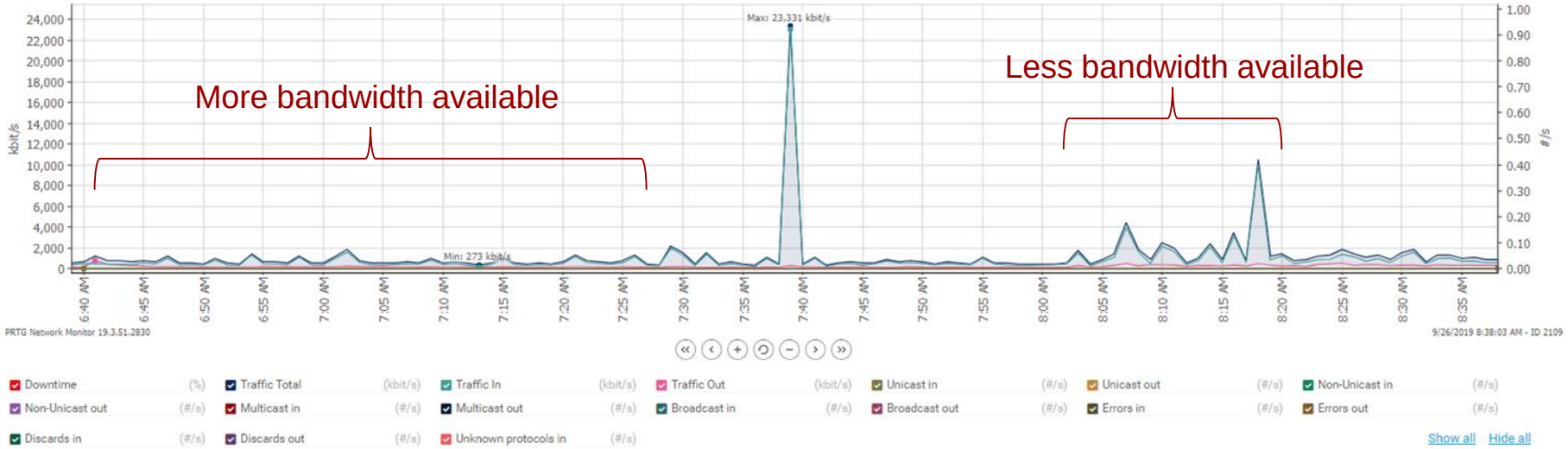
- Plan Scheduled Maintenance for less congested network times
  - Reduce failure of more “network demanding” tasks:
    - Security Patching
    - Updating in-store / at pump video content
    - Exporting information
    - Vulnerability scans
- Review trends in performance to identify:
  - Failing devices
  - Inefficiencies / areas of improvement
  - Ways to increase uptime

Have process in place to review collected data to better understand network performance



CONEXXUS
solve forward

Have process in place to review collected data to better understand network performance



CONEXXUS
solve forward

Sending Data to SIEM - Alerts vs Continuous Transfer vs. Reports

- Alerts
  - Can be used for real time issues
  - Small amount of traffic on network
- Continuous Data Transfer
  - Real time information (not just issues)
  - Consistent traffic on network
- Daily / Weekly results
  - Benchmarking
  - Performance review
  - Large amount of traffic on network, but short amount of time
  - Use collected data to determine schedules for uploading data

Condition-based maintenance – it's a dynamic process.

1. Don't ignore devices just because they are not failing.
2. If a set of devices fall beyond the median range for memory, CPU, temperature or another feature, ask why?
3. Can anything on that device be adjusted to bring it inline with the others?
4. Don't have to worry as much about devices that are performing well.
5. APIs available?
6. How are these devices networked locally?
7. How frequently should they be polled? 5 minutes, hourly, daily, weekly?
8. Setting thresholds.
9. What tools will analyze the data in the cloud?

OUTAGE MANAGEMENT

Using a diverse set of features to predict outages and manage overall network risk.

CONEXXUS
solve forward

Going beyond the local drive (in our heads).

1. Many IT teams make network related decisions using “tribal” knowledge about stores:
   - Stores that are in remote locations
   - Stores that get bad cell signal
   - Stores that are Oil Company A’s network, vs B’s network
   - Stores that have food services
   - Stores that have certain POS systems

Additional information can potentially create a more effective set of groups, especially when it comes to maintaining network infrastructure.

1. Site Information
2. Asset Information
3. Network Performance Data
4. Electric Power Data

Having a single source of truth, featuring a wide set of information, can have a meaningful impact in being able to triage issues quickly between multiple parties.

1. Service Contractors
2. Operations
3. IT
4. POS
5. Network Teams
6. Security Teams

Site Asset Data (according to Conexxus): XML schema provides for reporting of site information

(e.g., Site Name, Branding, Location, IDs), as well as devices, including but not limited to:

- POS terminals,
- Payment terminals,
- Scanners,
- Site controllers,
- Fuel controllers,
- Dispensers,
- Carwash controllers
- Tank gauges.

Information about these devices may include the:

- Vendor
- Model
- Versioning (e.g., hardware, software, operating system, firmware and/or kernels)
- Networking configuration
- Device capabilities (e.g., EMV or encryption).
- Device-specific information (e.g., blending capabilities and configuration for a dispenser) is also included in the schema.

Determine CLEAR methods for outage classification following incidents (post mortems)

1. Power Outage?
2. Environmental Related?
3. Human Error?
4. Network Bottlenecks?
5. ISP or Cellular Connectivity?
6. Hardware Failure?
7. Software Bug or Corruption?

Site Information Example

1. Building Age
2. Store Layout
3. Geographic Location
4. Brands, Equipment
5. Square Footage

Outage Data

Ticket #	Start Date	End Date	Start Time	End Time	Store #	Total Duration	Store Traffic	Root Cause
					097			Power Outage
					109			Human Error
					032			Hardware Failure
					056			Software Bug
					007			

Site Asset Data Included

Outage Duration	Store	Square Footage	Average Interface Response Time %	Router	Switch	Modem	Cables	ISP	Backup	Geographical Location	Traffic	Wifi?	Number IP range	Bandwidth	Throughput
5 hours	097	2,100	99	SonicWALL	Netgear	Arris BGW120	Cat5	ATT	Verizon MiFi		High	Yes			
1 hour	109	2,500	99	SonicWALL	Netgear	Arris BGW120	Cat5	ATT	Verizon MiFi		Medium	No			
5 hours	032	2,400	98	SonicWALL	Netgear	Netgear CM500	Cat5	Spectrum	Cradlepoint		Low	Yes			
1 hour	056	2,400	99	Meraki	Cisco	AC1750	Cat6	Comcast	Verizon MiFi		Medium	No			
3 hours	007	2,300	98	SonicWALL	Netgear	Arris BGW120	Cat5	ATT	Cradlepoint		Low	No			

Network Data Example

Back office Reboots	POS CPU Mean %	BACK OFFICE CPU Mean %	ATG CPU Mean %	POS Memory Mean %	Back Office Memory Mean %	ATG Memory Mean %

Back office Reboots	POS CPU Mean %	BACK OFFICE CPU Mean %	ATG CPU Mean %	POS Memory Mean %	Back Office Memory Mean %	ATG Memory Mean %	ATG Reboots

Total POS	Total BO systems	ATG Uptime %	POS Reboots	ATG Reboots

% of Pings Dropped	Packet Loss External	Packet Loss Internal	Average Interface Response Time	POS Uptime %	Back Office Uptime %

CONEXXUS
solve forward

Network Data Example

STORE	# of IPs	# OF MAJOR STORE NETWORK OUTAGES > 20 minutes	PRIMARY ISP MEAN THROUGHPUT (mbps)	CELLULAR MIFI MEAN THROUGhPUT (mbps)	TOTAL WIRELESS FAILOVER EVENTS (ISP drop) > 1 minute

Power Data

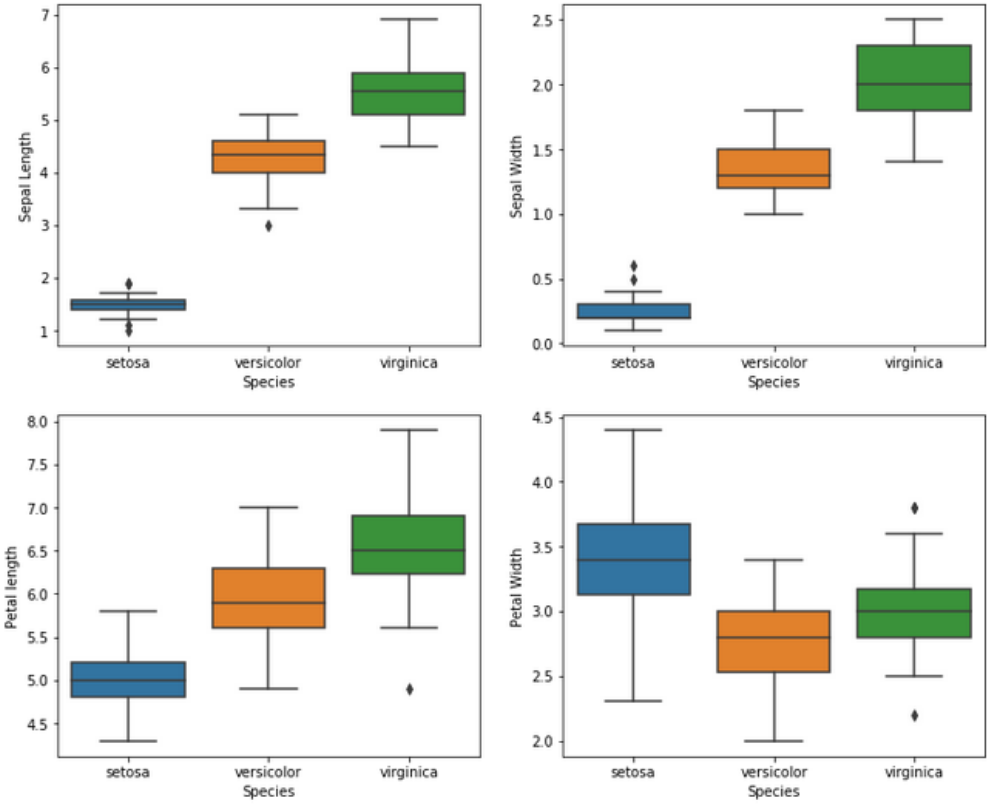
Store #	Mean POS Energy Consumption (kWh)	Mean ATG Energy Consumption (kWh)	Square Footage	Surge Protection During Event?	Mean Back Office Energy Consumption (kWh)	Mean Car Wash Energy Consumption (kWh)	Std. POS Energy Consumption (kWh)	Std. Car Wash Energy Consumption (kWh)	Std. ATG Energy Consumption (kWh)	Std. Back Office Energy Consumption (kWh)
097				Yes						
109				No						
032				Yes						
056				Yes						
007										

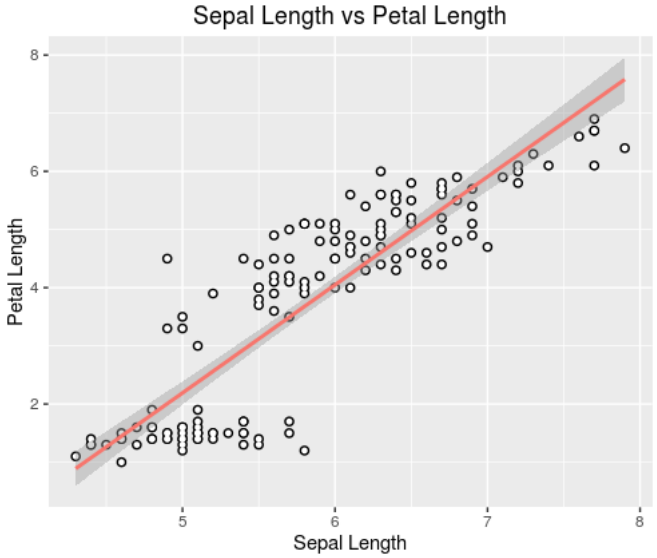
More Effective Methods for Classification.

Using data to forecast store requirements:

1. What stores need multiple WAN connections?
2. What stores need to have a certain wireless backup solution?
    1. ISP drops + MiFi performance
3. What stores need to have which data plan?
    1. Throughput metrics can determine that
4. What stores need to replace power infrastructure?
    1. No surge protection, older stores, UPS's without battery

Determining Unexpected Relationships





CONEXXUS
solve forward

Finding Inspiration

- A prediction is a definitive and specific statement about when and where an earthquake will strike: a major earthquake will hit Kyoto, Japan, on June 28.
- Whereas a forecast is a probabilistic statement, usually over a longer time scale: there is a 60 percent chance of an earthquake in Southern California over the next thirty years.

Nate Silver, *The Signal and the Noise*

“Small Data” can still help to improve probability.

	Prediction	Forecast
Statement	“Algorithm A gives a 2% increase in true positive detection of threat X over Algorithm B"	“We are targeting 80% of all servers of class Y to be have a security grade of at least A in the next 3 months”
Methodology	Use knowledge of potential threats to **hypothesize** security improvements	Combine business goals, gut feeling + data from multiple sources to set a **goal** for security performance
Guiding Question	What value should I assign this algorithm?	Given what we know about our threat model(s), how do we plan the path forward?

CNBC First reported on CNBC

CONEXXUS solve forward

Determining Unexpected Relationships

Site and Asset Relationship Examples

Connectivity Failures vs Backroom Temperature?
Connectivity Outages vs Building Age?
Connectivity Outages vs Food Vendor/QSR (yes or no)?
Connectivity Failures vs Square Footage?
Connectivity Outages vs Surge Protection State?

Network Relationship Example

Connectivity Failures vs Dropped Packets?
Connectivity Outages vs POS Reboots in the last year?
Connectivity Outages vs # VPN tunnels?
Connectivity Outages vs # IPs?
Connectivity Outages vs Throughput?

SELF-HEALING

Using simple, rule-based automation to implement self-correcting mechanisms on systems.

Self-healing POS application failures – a true story.

1. POS services not starting after reboots following application of weekly patches.

Set a baseline – measure the impact of the failure.

1. Number of stores impacted?
    - 40/100 stores
2. How long until the failure was noticed? Why not sooner?
    - 1 hour.
    - Absolutely critical or not-critical?
3. Duration of impact?

Measure What Matters

i	Time	Event
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3202server,Windows Service - POS Integration Manager 3 Scheduler Service,Failed,Restart Service-POS Integration Manager 3 Scheduler Service,Failed,0:09:01 Device = 3202server | Resolution = Failed | Service = Windows Service - POS Integration Manager 3 Scheduler Service | Trigger State = Failed
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3202server,Windows Service - POS Site Controller SSPDIManager,Failed,Restart Service-POS Site Controller SSPDIManager,Success,0:03:48 Device = 3202server | Resolution = Success | Service = Windows Service - POS Site Controller SSPDIManager | Trigger State = Failed
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3202server,Windows Service - POS Device Management Service,Failed,Restart Service-POS Device Management Service,Success,0:03:40 Device = 3202server | Resolution = Success | Service = Windows Service - POS Device Management Service | Trigger State = Failed
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3202server,Windows Service - POS CMC Bridge,Failed,Restart Service-POS CMC Bridge,Success,0:03:29 Device = 3202server | Resolution = Success | Service = Windows Service - POS CMC Bridge | Trigger State = Failed
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3202server,Windows Service - POS API Router,Failed,Restart Service-POS API Router,Success,0:03:40 Device = 3202server | Resolution = Success | Service = Windows Service - POS API Router | Trigger State = Failed
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3147server,Windows Service - POS Services,Failed,Restart Service-POS Services,Failed,0:16:47 Device = 3147server | Resolution = Failed | Service = Windows Service - POS Services | Trigger State = Failed
>	9/22/19 5:21:00.000 AM	2019-Sep-22 5:21,3147server,Windows Service - POS Integration Manager 3 Scheduler Service,Failed,Restart Service-POS Integration Manager 3 Scheduler Service,Failed,0:10:08 Device = 3147server | Resolution = Failed | Service = Windows Service - POS Integration Manager 3 Scheduler Service | Trigger State = Failed

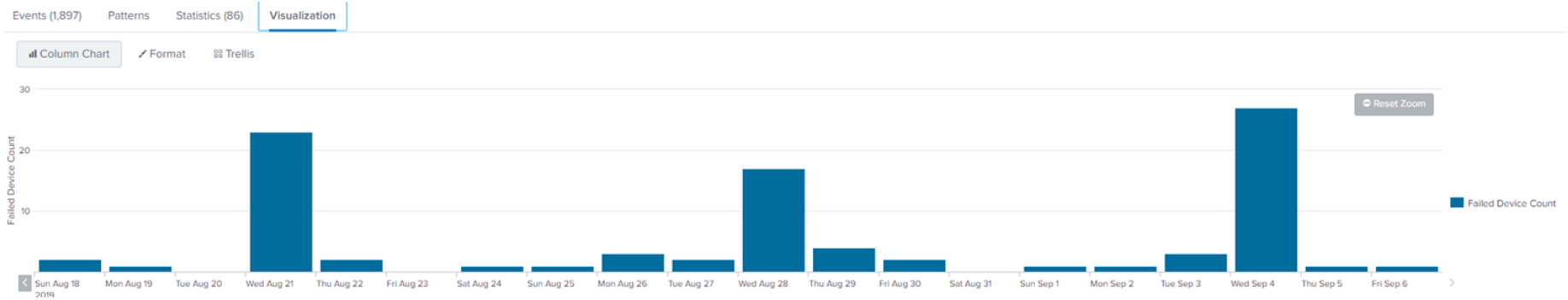
Name of device

Name of service

State of service

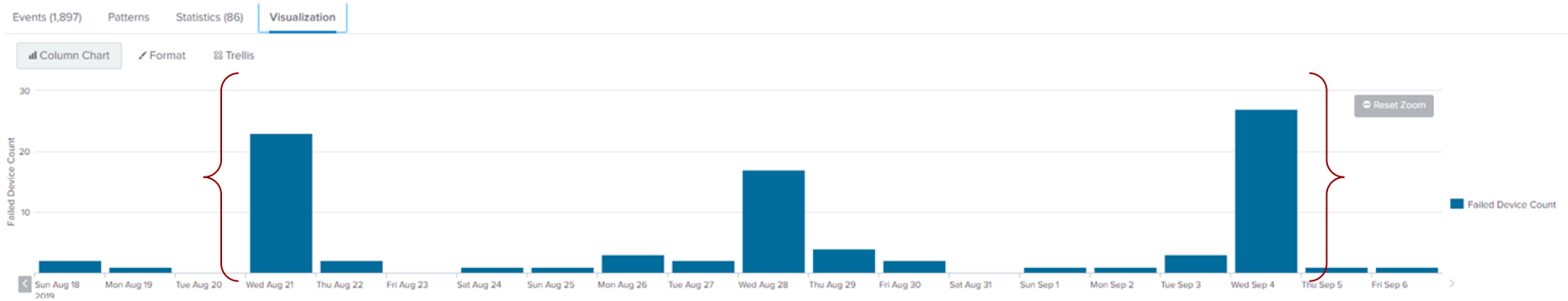
CONEXXUS
solve forward

Measure What Matters



CONEXXUS
solve forward

Measure What Matters



~ 25% - 30% of total endpoints are having
POS services stop on Wednesdays

CONEXXUS
solve forward

Develop hypotheses

1. Find a machine that had an issue and did not have an issue.
2. Look through events of both machines to identify which event happened on the machine that had the issue vs which did not have the issue.
3. Event was identified alongside additional dependent events.
4. Verified that the other failed machines also had the event.
5. To this point, still did not WHY the service was not starting. To this point, only knew that the machines were not starting post patches. Root cause analysis not yet done.

Develop hypotheses

HYPOTHESIS A – Resource consumption impacting ability for SQL service to start.

- Sample set of reboots…trying to get somewhere close to 40%, which then requires a sufficient set of machines. Went ahead – with customer's permission – and scheduled a set of reboots even though patches were not applied.

HYPOTHESIS B – Network-related

- Misconfiguration in SQL/POS software
- Issues related to the recently applied Windows patch.

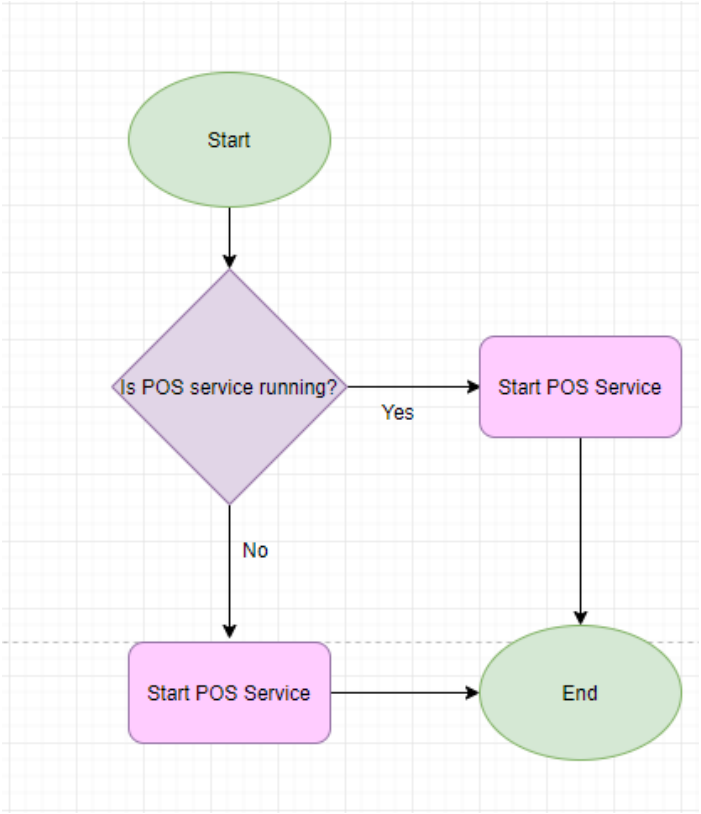
Root cause analysis – try to determine the critical relationship, either via correlation or domain-knowledge about dependencies.

1. Identified that reboots were the problem triggering the application failure.
2. Unfortunately, root cause is inherent in the system – Windows 7 does not provide options for priority on boot.
3. Still methods for implementing automated backup (self-healing action).
   - Automatic discovery and correction of faults.

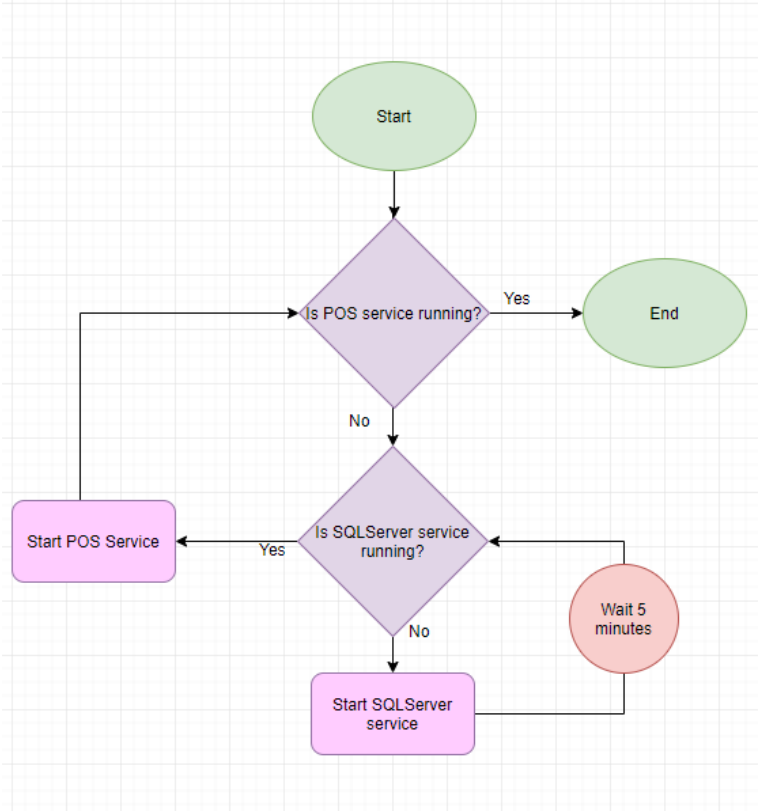
Implementing Self-Healing Actions

1. A/B tested different self-healing methods on a subset of machines following schedule reboots after patches to compare effectiveness of script.
2. Important to be granted to freedom of carrying out an experimental approach. Requires management support.
3. Continue ongoing performance monitoring.

Self Healing Actions



Self Healing Actions

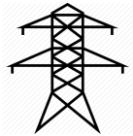


Lessons Learned – same approach can be followed for a variety of anomalous system failures that do not have a direct fix.

1. Rule-based power cycling using power distribution units (PDU), in the event of failed ping tests.
2. Application corrections.
3. So long as you are monitoring the right things and understand the dependencies, and you have the ability to remotely manage/remotely impact the device, then you can implement these rules in your enterprise.

Using Data Science to Proactively Manage the Connected C-Store

Difficulties with managing connected and IoT devices.



Using industry analogs to navigate a digital transformation.

Use cases for more effectively managing the connected petroleum retail environment.

Tips for experimenting with predictive maintenance approaches.

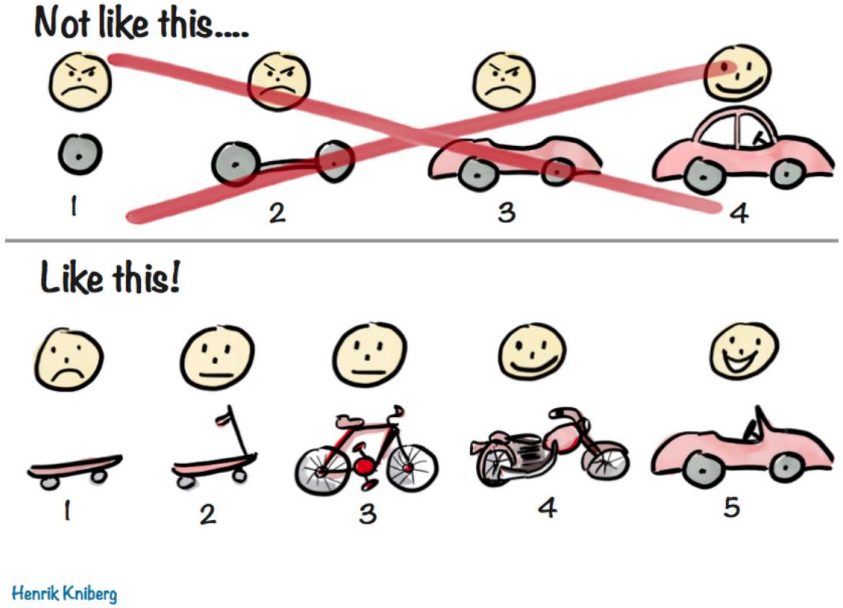
CONEXXUS
solve forward

Ask questions. Then ask more questions.

CONEXXUS
solve forward

Ask questions. Then ask more questions.

Develop minimal viable products to determine the potential impact of data products/strategies.

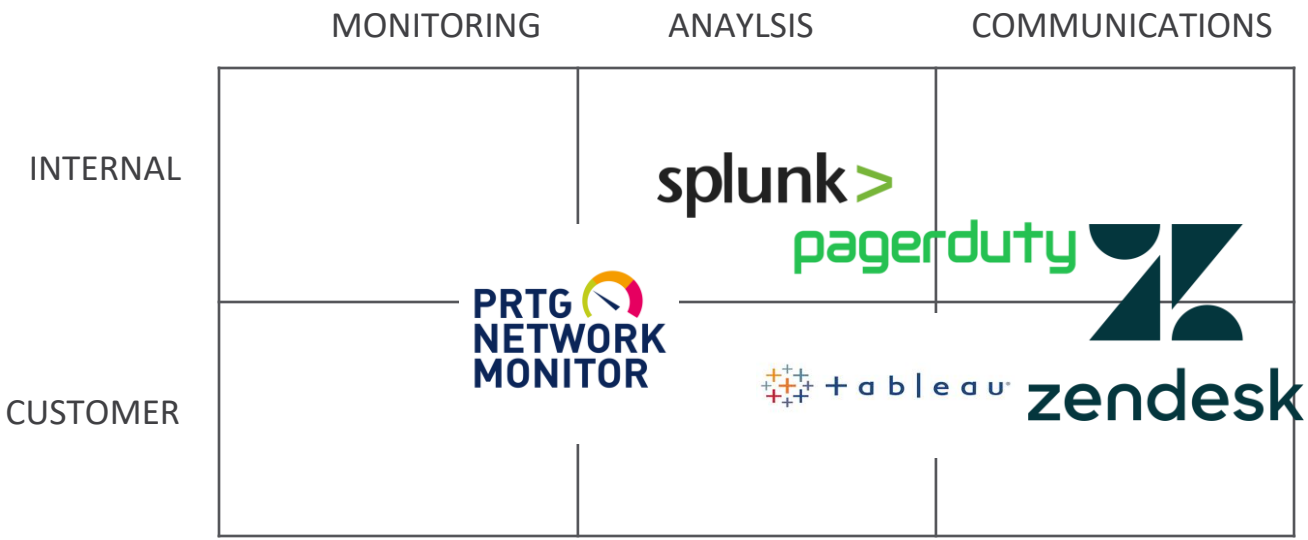


Monitoring and analysis tools used to be defined in separate product categories.

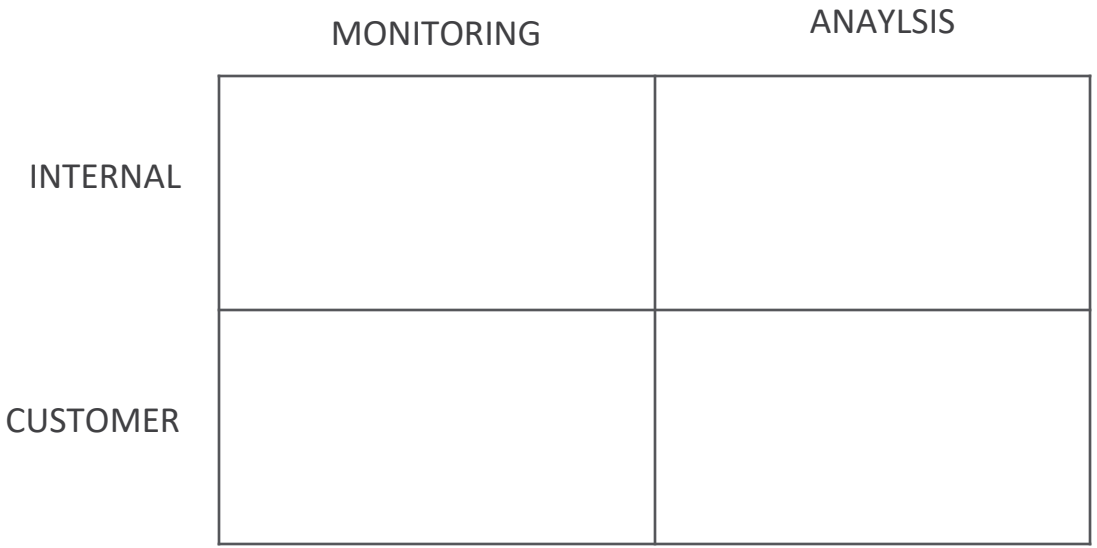
	MONITORING	ANAYLSIS	COMMUNICATIONS
INTERNAL		splunk>	pagerduty
CUSTOMER			zendesk

CONEXXUS
solve forward

Not the case today – application categories are merging.

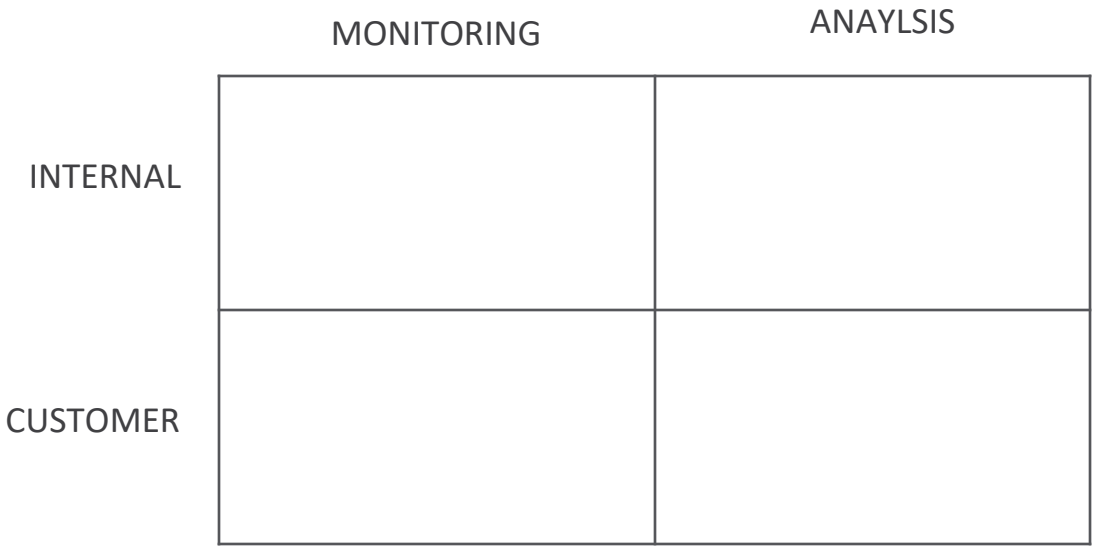


Explore new approaches to building your organization's technology/application stack.



"Dev ops," traditional monitoring, IT Service Management (ITSM), IT Operations Management (ITOM), Asset management, Alerting, Security Information and Event Management, Data Analysis/Data Science, and CRM tools have all crossed boundaries.

Leverage APIs to ensure that applications play well together.



”Dev ops,” traditional monitoring, IT Service Management (ITSM), IT Operations Management (ITOM), Asset management, Alerting, Security Information and Event Management, Data Analysis/Data Science, and CRM tools have all crossed boundaries.

CONEXXUS
solve forward

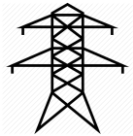
Communities and internal forums centered around certain tools (e.g. SIEM, data analytics, network monitoring) are great sources of knowledge, especially for answering questions like “what can I measure,” ”how can I measure it,” and “what insights can be made from the data?”

Leverage communities and events to find analogs that apply to your organization.

1. Data science meetups and Kaggle – great for seeing examples of data science being used in a wide variety of industry applications. Especially good for getting ideas on how to select features, ask questions, and structure data.
2. Pay attention to site reliability engineering (SRE) and DevOps communities – forums, tools, code, etc.
3. Talk to engineers from other analogous industries (energy & utilities, manufacturing, transportation, healthcare) to see how they think about ensuring availability and high performance of critical systems and devices.
4. Keep talking to vendors/manufacturers – know experts who can provide proper consultation about devices – their level of security, reliability, ease of management, etc.

Using Data Science to Proactively Manage the Connected C-Store

Difficulties with managing connected and IoT devices.



Using industry analogs to navigate a digital transformation.

Use cases for more effectively managing the connected petroleum retail environment.

Tips for experimenting with predictive maintenance approaches.

CONEXXUS
solve forward

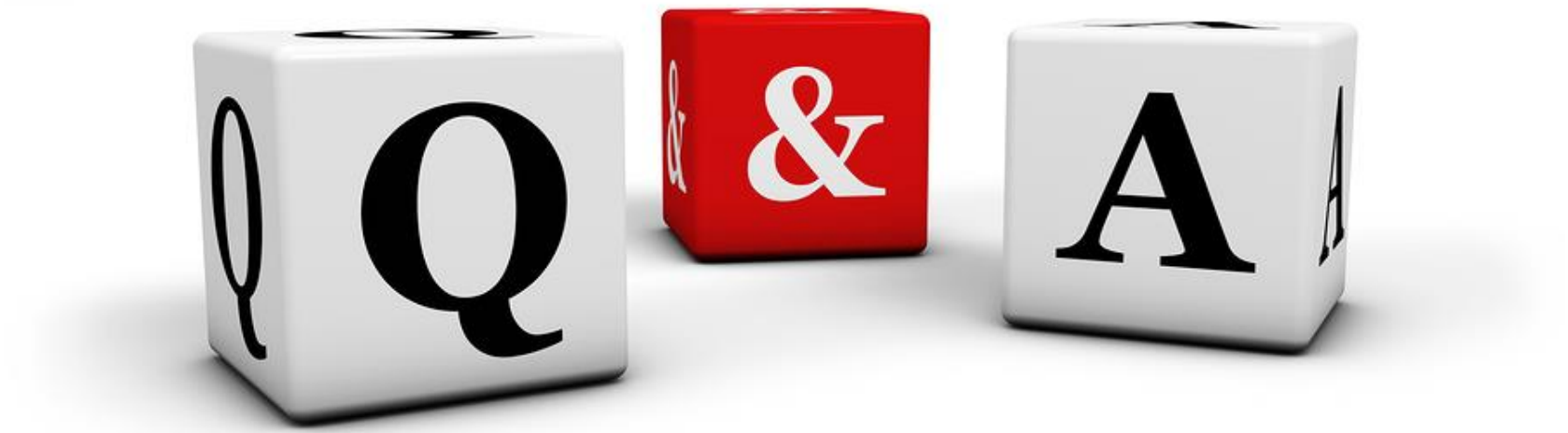
Key Takeaways

1. It is worth implementing new connected/IoT devices if the business case makes sense, the devices abide by the proper security standards, and the overall enterprise and operations is prepared to effectively manage the device following implementation.
2. Preparation includes ensuring that a wide array of data points are being collected, tracked, and made visible to the appropriate parties.
3. Preparation also includes having the right operations and monitoring tools in place to ensure that the right data can be collected.
4. Always have regular retrospective/post mortem meetings to ensure that any incidents/outage events are properly classified. You cannot collect data only when it's necessary; must be done long before.
5. Regularly perform exploratory data analysis using different variables to see whether any interesting relationships may exist that can help prevent failure or outages downstream.

Speakers

Ashwin Swamy
Director of Cyber Resilience, Omega ATC
ashwin.swamy@omegaatc.com

Thomas Duncan
Senior Security Strategist, Omega ATC
thomas.duncan@omegaatc.com



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.