NOZOMI NETWORKS

WHITE PAPER

Midstream Oil and Gas Industry: Improving ICS Visibility Boosts Operations & Cyber Security

July 2019

Table of Contents

Introduction—Improving ICS Visibility Boosts Midstream Operations & Cyber Security 1

1. Understanding Visibility and Cyber Security Challenges for Midstream Operators 2

I. An Undetected Cyberattack Impacts Flow Values and Stock Prices. 2

II. The High Number of Pipeline Producers Makes Cyber Security Challenging 3

III. New Solutions That Provide Real-time Visibility are Key to Cyber Security 4

2. Improving Network and Operational Visibility 5

I. Use Case: Recognizing Equipment Failure 5

i. PLC Breakdown Results in $1.9 Million Loss 5

TECHNOLOGY OVERVIEW | How ICS Network Monitoring Works 7

ii. Locating a "Dirty Gas" Problem Before Damage Occurs 9

iii. Identifying the Cause of Lost Oil or Gas 10

II. Use Case: Identifying a New Producer Tie-In 12

III. Use Case: Identifying the Cause of Poor Network Performance 13

3. Detecting Cyber Risks and Improving Cyber Resiliency 14

I. Use Case: Detecting Malware Present on the Industrial Network 14

II. Use Case: Addressing the ICS Cyber Security Skills Shortage. 17

III. Use Case: Improving Cyber Security Productivity. 19

Conclusion - Avoid Downtime with Pipeline Operational Visibility and Improve Cyber Security Too... 20

What to Look for in a Real-time ICS Visibility and Cyber Security Solution 21

See the Nozomi Networks Solution in Action. 21

Additional Resources 21

References. 22

INTRODUCTION

Improving ICS Visibility Boosts Midstream Operations & Cyber Security

The midstream oil and gas industry is forecast to grow significantly over the next decade, escalating the number of players involved and the complexity of operations. At the same time, increasing connectivity is amplifying cyber risk.

It's important to know that technology exists to significantly reduce cyber risk for midstream operations. Such solutions make sense of infrastructure complexity and have the added benefits of improving both productivity and cyber security.

There is no denying that digitization of operations in the midstream oil and gas industry has created tremendous opportunities to extend communications from production through to the business enterprise. This in turn hikes productivity, brings down costs, and enhances profitability.

The challenge is, though, that connecting operations and the business enterprise has opened organizations up to a litany of cyber security risks.

Those risks are not going to diminish as the discovery of oil and gas resources grows, commodity prices remain relatively low and global demand increases. Companies will need to invest in building new midstream infrastructure to transport, process, store, and export hydrocarbons.

According to a Polaris Market Research report[1], the U.S. midstream oil and gas equipment market is expected to grow from $697.17 billion in 2017 to $983.73 billion by 2026. This view is confirmed by The Interstate Natural Gas Association of America Foundation which sees capital expenditures (CAPEX) for new oil and gas infrastructure development reaching almost $800 billion over the next 18 years[2].

With growth continuing and digitization taking off, protecting the midstream oil and gas industry from cyberattacks, while optimizing operations, becomes paramount.

According to a Ponemon Institute study,[3] 68 percent of OT (Operational Technology) organizations have suffered a security compromise that resulted in the loss of confidential information or disruption to operations over the past 12 months. On top of that, on average, 46 percent of cyberattacks are believed by respondents to go undetected.

THE ROAD TO OIL & GAS CYBER SECURITY

Read this paper to learn how easy it is to gain operational visibility, reliability and cyber security using a real-time ICS monitoring and threat detection solution.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

1 Understanding Visibility and Cyber Security Challenges for Midstream Operators

I. An Undetected Cyberattack Impacts Flow Values and Stock Prices

To understand the challenges of securing midstream oil and gas operations, let's look at a real-world scenario that occurred awhile ago. A multi-use pipeline that transported oil and gas through North America was having allocation issues related to the volume of production reaching a refinery.

Staff at the refinery would say to producers "whatever you're reporting was not what we metered, and we are not going to pay for that." As the companies involved were public, the discrepancies had to be reported, and the news had a negative impact on their stock prices.

The allocation problems triggered an investigation. In the days before built-in visibility, workers would conduct their volume research by doing meter and transmitter calibrations. They would look at the way the code was written in the flow computers and review how data was moving from the flow computers to the control system. Then they would investigate the data historian, the accounting software and the product marketing system. Troubleshooting was a long, laborious process.

A deep investigation showed that while each allocation issue was relatively small, over time they added up, and had a significant impact on production volume. Furthermore, interesting patterns were revealed that were not random.

Eventually, the cause of the problem was identified as planned manipulation of the real production values by a foreign entity. They were able to access the pipeline system because a vendor that installed flow computers did not change the default passwords, and the machines were accessible on the Internet.

OPERATIONAL BLIND SPOTS

The pipeline organization did not know they had devices connected to the Internet, or that flow values were being changed.

The lack of operational visibility led to a significant cyberattack going undetected for a long time, and lowered share prices for multiple organizations. Meanwhile, the threat actor made significant financial gains by shorting stock.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

20/20 VISION IS ESSENTIAL

Real-time visibility of operational data, such as flow meter readings, is essential not only for production monitoring, but for detecting anomalous data that could indicate a cyberattack.

II. The High Number of Pipeline Producers Makes Cyber Security Challenging

This cyber incident is a perfect case of companies in the midstream market needing to know what technology, devices and networks they have running on their system. Then, once they know that, they need to be able to see and understand what is happening, especially any changes, in real-time.

This can present a problem for pipelines because of their sheer length, often vast, rural locations and large number of producers on the line.

In fact, a single pipeline could have a thousand producers utilizing it. The custody transfer points could be using equipment owned by different companies with different security practices. Until recently, a pipeline operator had to trust that these thousands of customers have robust security policies for the equipment connected to their line.

Like the stock shorting scenario, if an attacker can get on to a midstream company network and control system, they can cause harm. They could potentially operate remote relief valves and compressors, and override automatic shutdowns that protect against pipeline over-pressurization. This is a concerning scenario given there are so many independent entities connecting to a single pipeline.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

III. New Solutions That Provide Real-time Visibility are Key to Cyber Security

Industrial control systems (ICS), such as those used to operate today's pipelines, cover vast distances and include a highly diverse mix of equipment. Until recently, operators had the impossible task of managing and monitoring a system that was not thoroughly documented and not easy to visualize.

Furthermore, such systems produce reams of data. So much data that an operator doesn't really know what to focus on. And, if no one is looking at it from an analytics or security perspective, an issue can go unnoticed. Afterall, the people managing the pipeline are worrying about production throughput, downtime and safety issues, not security.

This is where a solution that automates the visualization, asset tracking and monitoring of the huge volume of data produced by a pipeline system comes in. Standard networking and cyber security tools rely heavily on direct programming and cannot address the complexity and volume of large industrial systems. However, new, advanced computer science techniques can help.

Machine learning, for example, solves problems by using artificial intelligence (AI) to learn from data. With the input of experts who have a deep understanding of ICS cyber security, structures that allow the machine learning algorithm to view and interpret network and process data correctly are created. Once AI algorithms are enabled in this way, they can rapidly analyze the high volumes of ICS data that are impossible to evaluate any other way.

The result is a real-time visualization of the industrial network, a comprehensive asset inventory, and process and security profiles specific for each ICS. Once baselines are established, ongoing anomaly detection, working with a regularly updated threat feed, monitors the system. The result is automated, rapid identification of changes to the network, cyberattacks, cyber incidents and critical process anomalies.

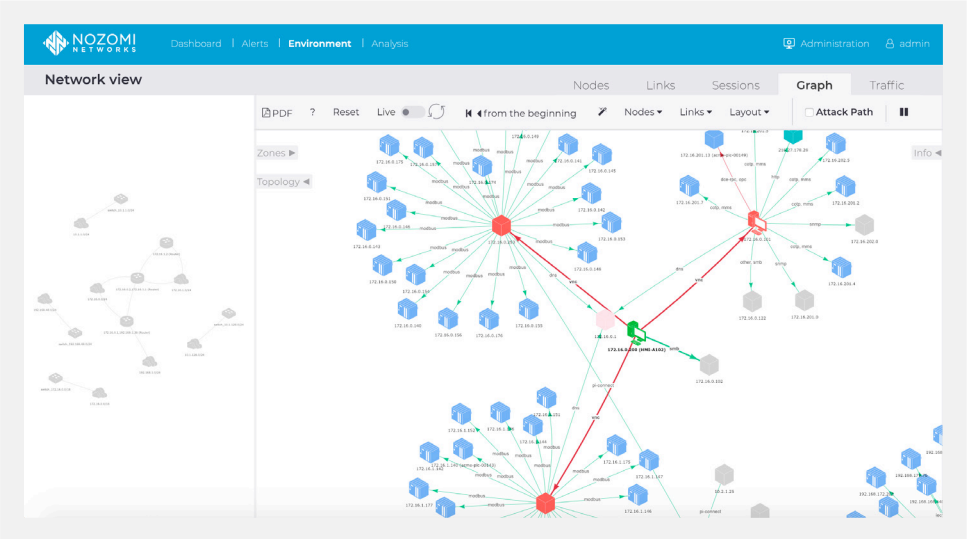


Figure 1 - Network Visualization Graph

Within minutes of deployment, an AI-powered real-time visibility solution displays the nodes of the industrial network in a live, interactive visualization. This interface improves situational awareness and speeds incident response and troubleshooting.

MAKING SENSE OF COMPLEX MIDSTREAM INFRASTRUCTURE

To understand how an **AI-powered real-time monitoring** and **cyber security solution** makes it easy to gain visibility, reliability and cyber security of your midstream operation, let's look at several use cases.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

2 Improving Network and Operational Visibility

I. Use Case: Recognizing Equipment Failure

i. PLC Breakdown Results in $1.9 Million Loss

An example of the challenges of identifying a potential problem is the case of a pipeline organization with a truck offload-onload skid. This facility pulls oil off a pipeline and hauls it away in tanker trucks.

When a PLC went down, the truck onload and offload terminal backed up to the point where it cost the company $1.9 million in lost revenue and downtime. In the midstream market, time is money. If you suffer unscheduled downtime, it's unlikely that you'll ever make up the lost time/revenue, because you're always moving product at high capacity.

However, if the pipeline operator had an automated network monitoring solution in place, they would have been able to predict a potential outage when the PLC started to behave abnormally. And, if the operator knew the type of PLC, the type of cards it was running, the firmware and the serial number, it would have been possible to quickly diagnose the problem.

On top of that, by adding an enterprise-wide centralized network monitoring solution, it would then be possible to look at all similar devices within the ecosystem. If one PLC behaved strangely and it cost $1.9 million, it's worthwhile to flag the 25 others and watch to see if they start behaving like the problem PLC. If they do, the issue can be mitigated before it causes a bigger problem.

In triaging this problem, one of the pipeline company workers said they noticed some "weird" operational values, but since no problems were triggered, they assumed it was normal behavior. It never really fell out of scope.

When asked how long he trended the data, the worker said, "Oh, just a few months." If it was already failing when he started observing the trend, the abnormal behavior looked like part of normal functioning, because the change was slow and gradual.

EARLY WARNING AVOIDS DOWNTIME

During the custody transfer of a resource, such as at this truck offload-onload skid, problems with control systems are very costly. Monitoring the industrial network identifies equipment problems before they result in downtime.

Photo courtesy of Endress+Hauser

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

The operator didn't trend the PLC back to when it was operating well. And, the operator didn't compare its behavior trend to similar devices to see how others were operating. He could have checked whether all devices with the same load were behaving similarly, or not.

In this case, the problem with the PLC was that it suffered from "ghost drift". This is when a device slowly and quietly slips out of scope over such a long period time that no one ever notices.

It is like watching your son grow through his teen years and not noticing that he shot up five inches over the last six months – until suddenly you have to get him a completely new wardrobe!

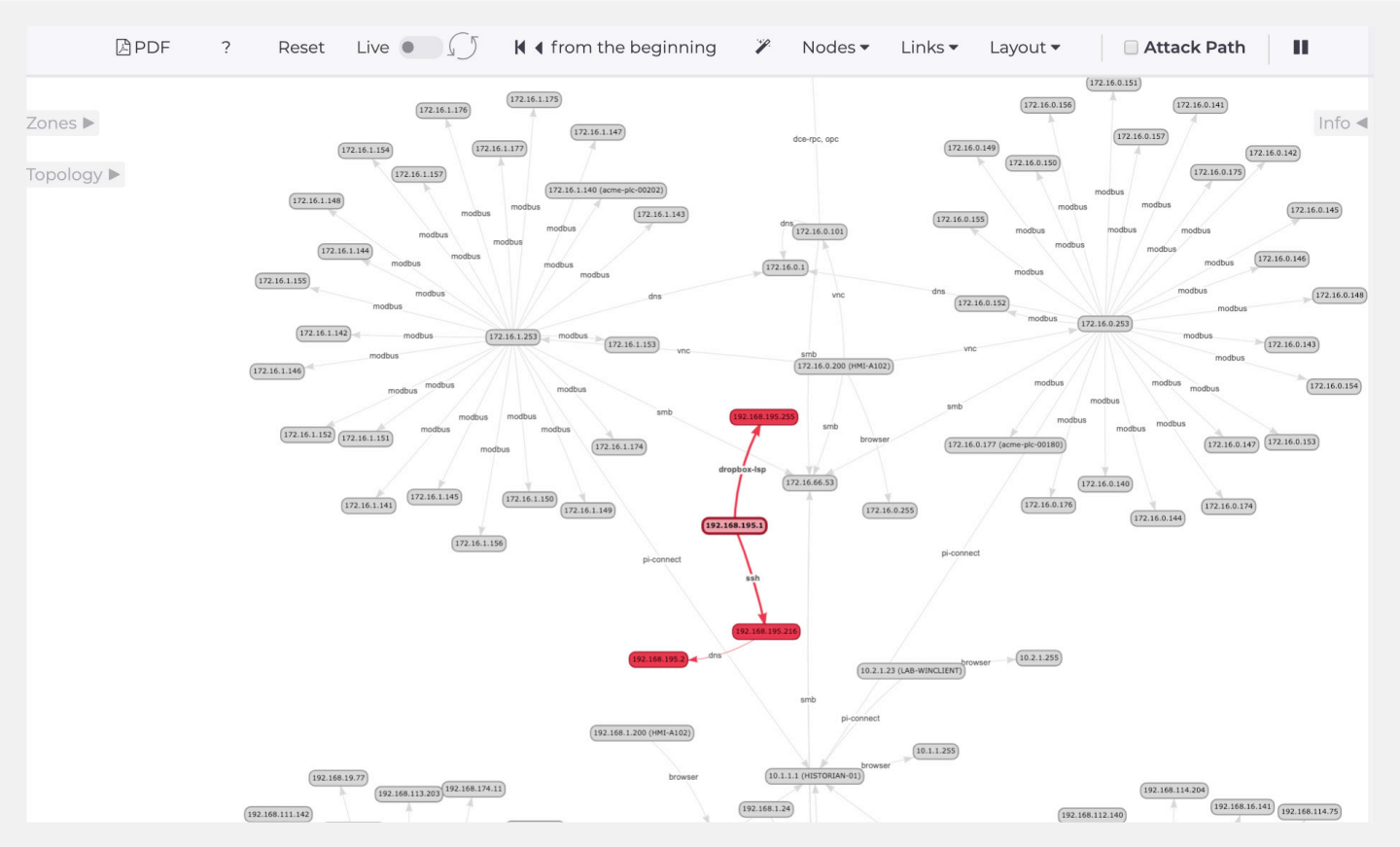


Figure 2 - Network Visualization Graph Showing Abnormal Devices

A real-time ICS monitoring solution visually identifies devices that are behaving differently than normal. Prompt investigation of such devices can prevent unplanned downtime.

Challenge

- PLC breakdown results in $1.9 million loss

How a real-time ICS visibility and cyber security solution helps

- It generates alerts identifying equipment behaving differently than normal, or unlike the same equipment across the network.
- Operators can act before a failure occurs.

Results

- Higher reliability
- Maximum revenue preservation
- $1.9 million savings

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

How ICS Network Monitoring Works

TECHNOLOGY OVERVIEW

In the PLC breakdown scenario, pipeline operational visibility comes into play. Today's ICS network monitoring solutions can detect when devices are starting to drift. They alert the operator that it's time to take a closer look before another unplanned downtime incident causes a $1.9 million loss.

If you not familiar with ICS network monitoring, here's how it works. Typically, an appliance is attached to a SPAN or mirror port of a switch or router on the pipeline. The passive application on the appliance observes network traffic and builds a model of the pipeline's network and operational behavior, employing machine learning and AI to deal with today's complex systems.

There are two phases to the implementation of the network monitoring application, the learning phase, and then an operational protect mode. After installation, the application quickly learns the system, and then starts detecting operational changes.

From a cyber security perspective, a potential problem is that when you first plug in the appliance, if you have a malicious malware beaconing out to an external server, the application learns that as normal behavior. To deal with this problem, the best ICS monitoring solutions use a technique called Dynamic Learning, where they go through the learning phase and then conduct a statistical process control analysis. If the system's behavior is within one standard deviation, it will tell you it has learned it, and will start monitoring based on that behavior.

Operationally, if ghost drift has been occurring over a period of time, that behavior will hide in the one standard deviation, and you have to go through the results with the operator and do the due diligence needed to eradicate the problem. One way to do it is to compare the operational behavior of similar devices across the pipeline system and see if the trend for one of the devices is different from the others.

This exercise can help you understand your processes inside and out!

When that happens, good cyber security becomes a byproduct, and the operator can flip the monitoring application into protect mode. Going forward, the operator will immediately know if there is any kind of drift or any kind of malicious attack, because the system will generate alerts with its laser-like focus.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

How ICS Network Monitoring Works

TECHNOLOGY OVERVIEW

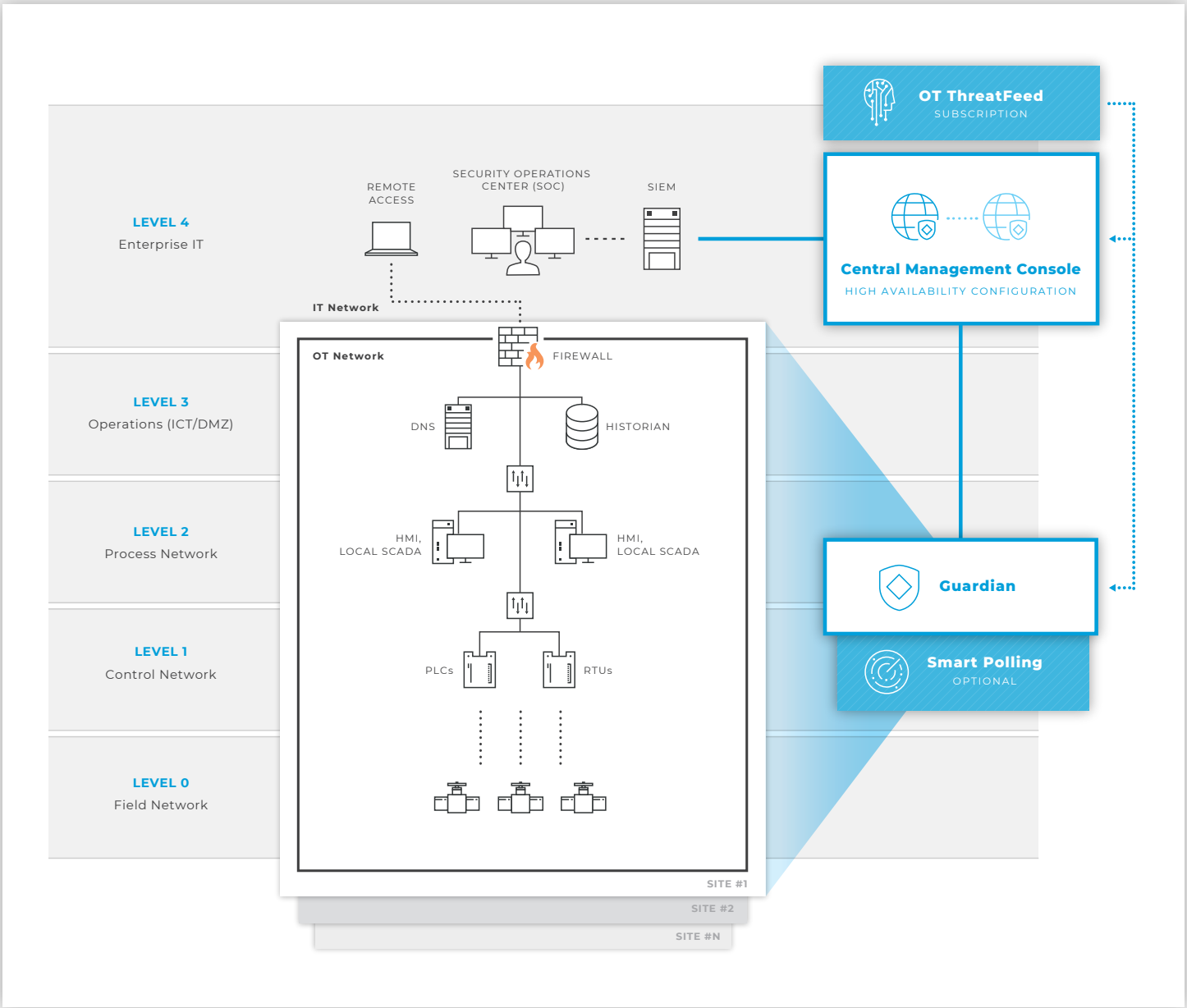


Figure 3 - Sample Deployment Architecture

Real-time network monitoring technology, such as the Nozomi Networks solution, is flexibly deployed to suit the ICS, and greatly improves visibility and cyber security.

Additionally, low-resource appliances **Remote Collectors™** can be added to capture data and monitor distant, unmanned locations.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

ii. Locating a "Dirty Gas" Problem Before Damage Occurs

In another situation, a gas pipeline company kept saying they were producing oil on one of the delivery meters. If a gas meter pulls oil through it, the meter could quickly wear out and fall apart, causing downtime.

The company kept investigating customers to find out who was sneaking dirty gas into the system, but couldn't determine who was responsible.

After building models around the company's compressor stations, it turned out that one of their compressors had a bad seal. It was leaking lube oil into the line, which was being measured as production volume.

A tool that knows what devices look like when they are operating in top condition could identify that issue in real-time. That is where assigning context to the data comes into play.

Pipeline operators focus on pushing product out the line and making sure the line stays incident free. In looking at the data, they may see a "weird outlier problem" they don't understand, but might be worth investigating. However, one of the hardest parts about operating and securing a pipeline is getting insight into what is truly happening in real time. Operators need data; and they need access to that data.

The challenge lies in correlating data across an entire pipeline system. As mentioned, operators are putting absolute trust in their customers producing on the line for security.

The massive length and volume on a pipeline make conducting regular audits impractical.

This is where technology can come into play, to monitor remote sites, remote stations, and remote tie-ins to understand what "normal looks like."

Figure 4 – Network Visualization Graph Showing Abnormal Devices

A real-time ICS monitoring solution visually identifies devices that are behaving differently than normal. Prompt investigation of such devices can prevent unplanned downtime.

Challenge

- Locating "dirty gas"

How a real-time ICS visibility and cyber security solution helps

- It generates alerts identifying equipment behaving differently than top condition.
- Operators can act before a failure occurs.

Results

- Faster problem resolution
- Improved operator productivity
- Better customer relations

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

iii. Identifying the Cause of Lost Oil or Gas

In a pipeline environment, there are times when people will hot tap into lines to pull out free oil or gas. Unless there is visibility indicating a sudden change in pressure, there could be a loss of profitable product.

There was one case in a U.S. state where the chief operating officer for the company said they were losing gas from their pipelines. Further investigation showed that the amount of gas being lost was significant, enough to set a major metropolitan city on fire.

The culprit was unexpected. The company was using polyethylene pipe exposed to the atmosphere. The sun was stressing the pipe to the point where fractures were occurring in multiple segments along the lines.

It was a slow seep, and because the pipeline was installed over such a wide area, the issue could have gone undetected forever. And, since it was a low-pressure gas environment, it would have been difficult to recognize the source of the leak.

Having a baseline of the environment would solve that problem. The operator would baseline the production numbers and the throughput of actual process variables to understand the flow rates. When a deviation is detected, a change in pressure will be noticed too. By comparing current numbers to normal behavior, it would become clear there was an issue.

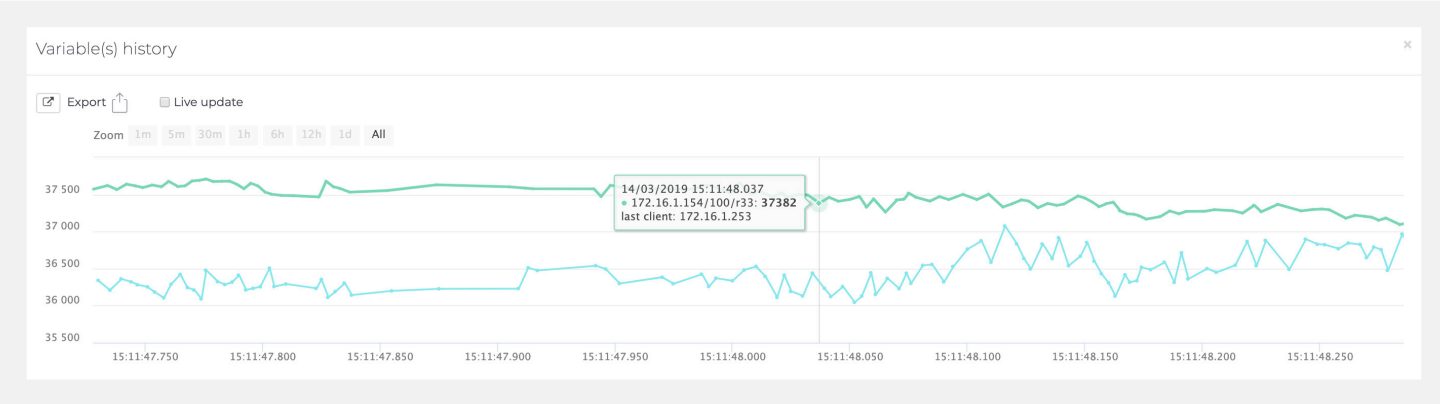


Figure 5 - Variables History Chart

The chart shows increasing, erratic pressure (lower line), compared to the normal flow rate (upper line). Rapid identification and investigation of this pattern would minimize the loss of a resource.

These leaks occurred over a large area. Nonetheless, it would be possible to pinpoint the leak if it was around control blocks and control valves that have pressure and temperature transmitters producing data.

If the operator lacks infrastructure and visibility, they may notice a pressure change, but it could be caused by anything, anywhere along the pipeline.

The more measurement equipment that's on the line, the easier it is to model the environment and see what is happening. It then becomes easier to attribute where the process variable data is coming from, and visually see that pressure from the control valve dropped.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

VISIBILITY SPEEDS TROUBLESHOOTING

In the end, it is all about visibility. Operators need to reduce their reliance on customers to ensure a secure pipeline. They need to be able to see what is truly going on, in real-time.

Challenge

- Identifying the cause of lost oil or gas

How a real-time ICS visibility and cyber security solution helps

- It generates alerts indicating that abnormal pressure values are occurring, and it identifies where on the pipeline the problem exists.
- Operators can act before a failure occurs.

Results

- Faster problem resolution
- Minimal resource loss
- Maximum revenue preservation

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

II. Use Case: Identifying a New Producer Tie-In

This becomes apparent from a security basis when there is a new tie-in and no one knows it happened. Operators will notice a production spike and they say “hey, this section of pipe pressured up way more than it should be, maybe we have an issue.” Then someone will say “no, the company tied in a new well, so it is fine.” But no one knows how they tied in. “What flow computers are they using? What is the HMI up there? Who is swinging the valves?”

Operational visibility answers a lot of these questions, by recognizing the anomalous activity, and creating an alert for the new tie-in. In this example, it’s easy to see how technology can be used to ensure a secure pipeline environment.

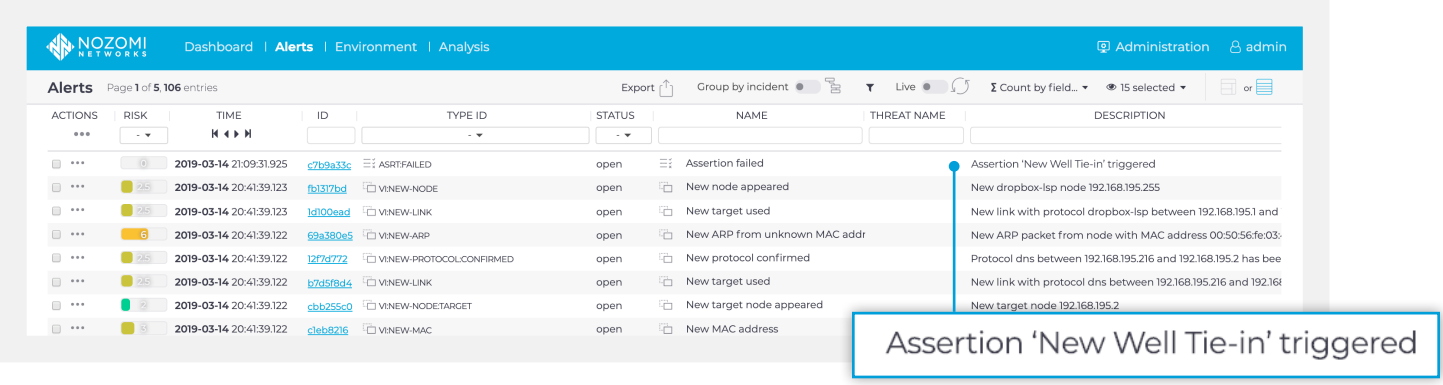


Figure 6 - Alerts Dashboard.
The first alert identifies that a new tie-in has occurred.

Challenge

- Identifying a pressure spike as a new producer tie-in

How a real-time ICS visibility and cyber security solution helps

- It generates an alert indicating a new producer tie-in has just occurred.

Results

- Faster understanding of system changes
- Improved operator productivity
- Better oversight of cyber security risk

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

III. Use Case: Identifying the Cause of Poor Network Performance

If operations and engineers know their process and understand how the valves swing, what it sounds like and how they should react, then security becomes a byproduct of operations.

If an operator is unfamiliar with their operations, and a change occurs, how would he or she know if it is security-related or operations-related?

A case in point was when one of the largest pipeline companies in the world was running a test. Immediately something did not seem right.

The operator was asked if they were spanning their switches the right way? Were they sure they were not duplicating their receive and transmit traffic, because there seemed to be quite a bit of noise on the network? "No," they said, "that is normal."

In addition, enterprise machines from the corporate network were talking to the pipeline control system. "No," they said, "that can't be right because we are using network segmentation."

It turned out that yes, they were doing almost everything right, but they failed to realize that a configuration error was causing a major problem. The entire corporation was authenticating through a small compressor station in the middle of nowhere, that had an anti-virus server in it.

Employees had been complaining for a year and a half that the network was very slow, that logging into accounts took a long time, and that IT updates took forever, preventing them from doing their work.

After connecting an ICS network monitoring device, it quickly became clear that everyone was authenticating at the remote location compressor station over a VSAT (very small aperture terminal) connection. The latency on the network was severe.

And on top of that, the company was getting charged heavily for the connection service, because the compressor station was remote, and a large amount of bandwidth was being used.

Correcting the problem saved the organization at least $200,000 in communications costs, not to mention the boost in employee productivity due to faster connectivity.

Challenge

- Identifying the cause of poor network performance

How a real-time ICS visibility and cyber security solution helps

- It highlights a network configuration error, including its location.

Results

- Faster problem resolution
- $200,000 savings in communications costs
- Improved employee productivity

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

3 Detecting Cyber Risks and Improving Cyber Resiliency

I. Use Case: Detecting Malware Present on the Industrial Network

A pipeline operator decided to run a Proof of Concept (PoC) to test an ICS visibility solution. Within minutes of connecting the appliance to the network, a malware alert was generated.

The first thing the operator asked was "Is this a false positive?" But several factors indicated the finding was true:

- The automation system in question had a history of being vulnerable.
- The computer identified as having the malware was public facing to the Internet.
- The computer in question connected to the corporate network and the control system network.

All things considered, it seemed that the malware discovery was valid, but how could the operator be sure?

Drawing on guidance from the vendor's system engineer, the organization started to dig deeper. Fortunately, the ICS visibility and monitoring solution being tested had the data and tools to support further analysis.

A next step in confirming the finding was to check the quality of rules that generated the result.

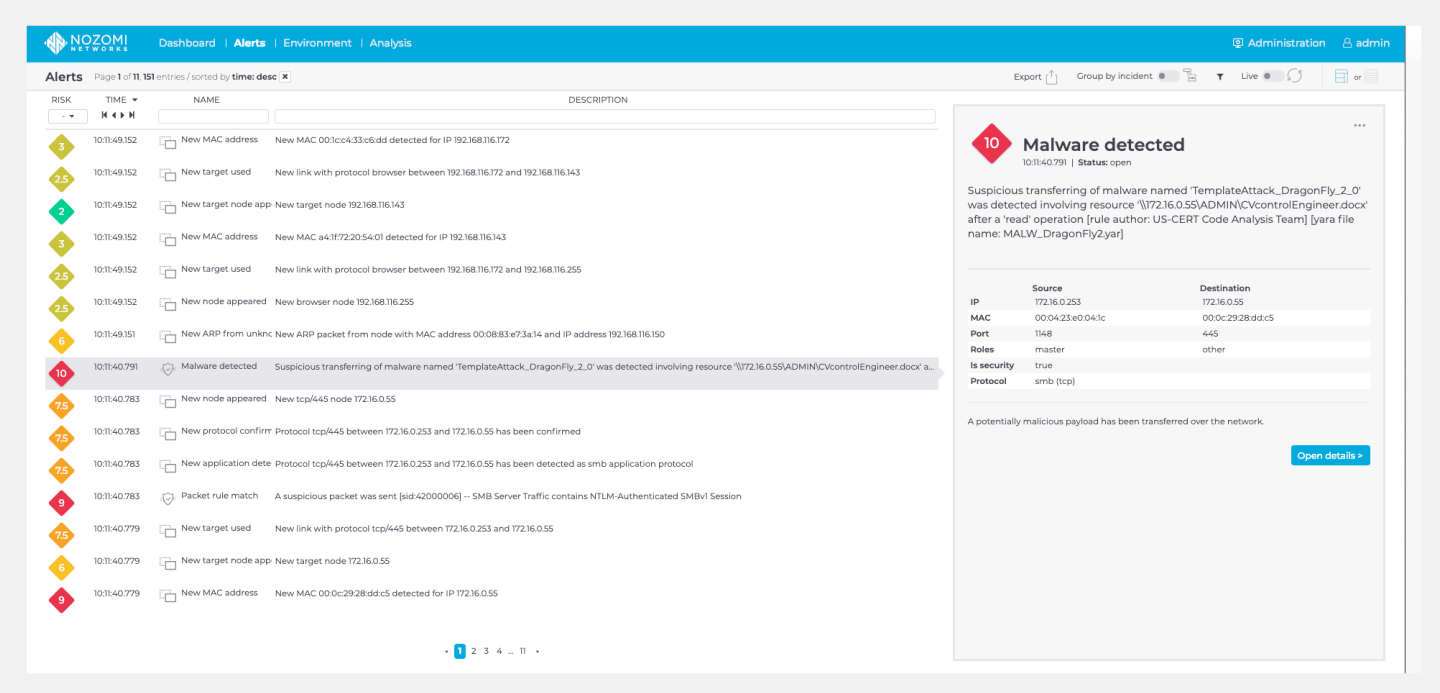


Figure 7 - Alert Dashboard Showing Malware Detected

Within minutes of installation of a real-time visibility and cyber security solution, a malware alert was generated.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

MALW_DragonFly2.yar

This is an OT Thread Feed provided by Nozomi Networks, it can't be modified

```
import "hash"

rule TemplateAttack_DragonFly_2_0
{
meta:
      description = "inveigh pen testing tools & related artifacts"
      author = "US-CERT Code Analysis Team"
      date = "2017/07/17"
      hash0 = "61C909D2F625223DB2FB858BBDF42A76"
      hash1 = "A07AA521E7CAFB360294E56969EDA5D6"
      hash2 = "BA756DD64C1147515BA2298B6A760260"
      hash3 = "8943E71A8C73B5E343AA9D2E19002373"
      hash4 = "04738CA02F59A5CD394998A99FCD9613"
      hash5 = "038A97B4E2F37F34B255F0643E49FC9D"
      hash6 = "65A1A73253F04354886F375B59550B46"
      hash7 = "AA905A3508D9309A93AD5C0EC26EBC9B"
      hash8 = "5DBEF7BDDAF50624E840CCBCE2816594"
      hash9 = "722154A36F32BA10E98020ABAD758A7A"
      hash10 = "4595DBE00A538DF127E0079294C87DA0"
strings:
      $s0 = "file://"
      $s1 = "/ame_1con.png"
      $s2 = "184.154.150.66"
      $s3 = { 87D081F60C67F5086A003315D49A4000F7D6E8EB12000081F7F01BDD21F7DE }
      $s4 = { 33C42BCB333DC0AD400043C1C61A33C3F7DE33F042C705B5AC400026AF2102 }
      $s5 = "(g.charCodeAt(c)^l[(l[b]+l[e])%256])"
      $s6 = "for(b=0;256>b;b++)k[b]=b;for(b=0;256>b;b++)"
      $s7 = "VXNESWJfSjY3grKEkEkRuZeSvkE="
      $s8 = "NlZzSZk="
      $s9 = "WlJTb1q5kaxqZaRnser3sw=="
      $s10 = "for(b=0;256>b;b++)k[b]=b;for(b=0;256>b;b++)"
      $s11 = "fromCharCode(d.charCodeAt(e)^k[(k[b]+k[h])%256])"
      $s12 = "ps.exe -accepteula \\%ws% -u %user% -p %pass% -s cmd /c netstat"
      $s13 = { 22546F6B656E733D312064656C696D733D5C5C222025254920494E20286C6973742E74787429 }
      $s14 = { 68656C6C2E657865202D6E6F6578974202D65786563574696F6E706F6C6963792062797061737320 2D636F6D6D616E6420222E202E5C496E76656967682E70 }
      $s15 = { 476F206275696C642049443A20226626433373937623163313465306531 }


//inveigh pentesting tools

      $s16 = { 24696E76656967682E7374617475735F71756575652E4164642822507265737320616E79206B657920746F2073746F70207265616C2074696D65 }

//specific malicious word document PK archive

      $s17 = { 2F736574746967732E786D6CB456616FDB3613FEFE02EF7F10F4798E64C54D06A14ED125F19A225E87C9FD0194485B }
      $s18 = { 6C732F73657474696E67732E786D6C2E72656C735540500010076A41275780B000104000000000400000000BD90B94E03311086EBF014D6F4D87B48214471D2 }
      $s19 = { 8D90B94E03311086EBF014D6F4D87B48214471D210A41450A0E50146EBD943F8923D41C9DBE3A54A240ACA394A240ACA39 }
      $s20 = { 8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56F8FC3AA9558B0B4 }
      $s21 = { 8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56F8FC3AA9558B0B4 }
      $s22 = "5.153.58.45"
      $s23 = "62.8.193.206"
      $s24 = "/1/ree_stat/p"
      $s25 = "/icon.png"
      $s26 = "/pshare1/icon"
      $s27 = "/notepad.png"
      $s28 = "/pic.png"
      $s29 = "http://bit.ly/2m0x8IH"

condition:
      ($s0 and $s1 or $s2) or ($s3 or $s4) or ($s5 and $s6 or $s7 and $s8 and $s9) or ($s10 and $s11) or ($s12 and $s13) or ($s14) or ($s15) or ($s16) or ($s17) or ($s18) or ($s19) o
```

author = "US-CERT Code Analysis Team"

Figure 8 - Rules for Detecting the Dragonfly 2.0 Malware

The ICS visibility and security solution provides the rules that led to the malware alert.

In this case, the rule that identified the Dragonfly malware was provided by the US-CERT Code Analysis Team. This provides confidence that the rule is valid and well-constructed, and that the malware detection finding is true.

The next step in the analysis was to look at the URLs captured by the rule.

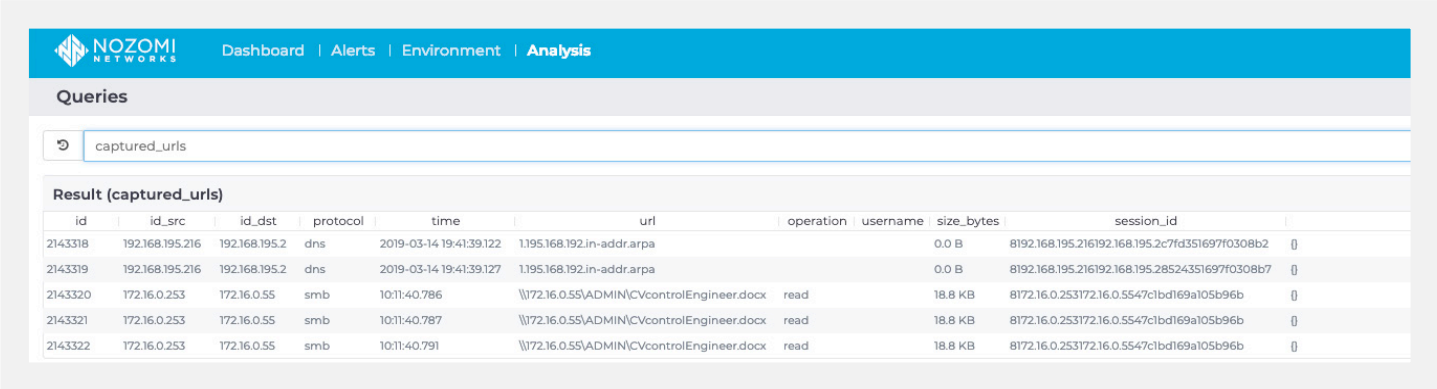


Figure 9 - Query Showing Captured URLs

The ICS visibility security solution has the tools and data needed to analyze the threat.

With the help of a powerful query tool, the operator can see that the captured URLs are suspect, with a dedicated IP address for the network share starting with "172". In addition, the use of the protocol SMB and the transfer of a Word document file are key indicators of suspicious activity. This is more concrete proof that the malware discovery is valid.

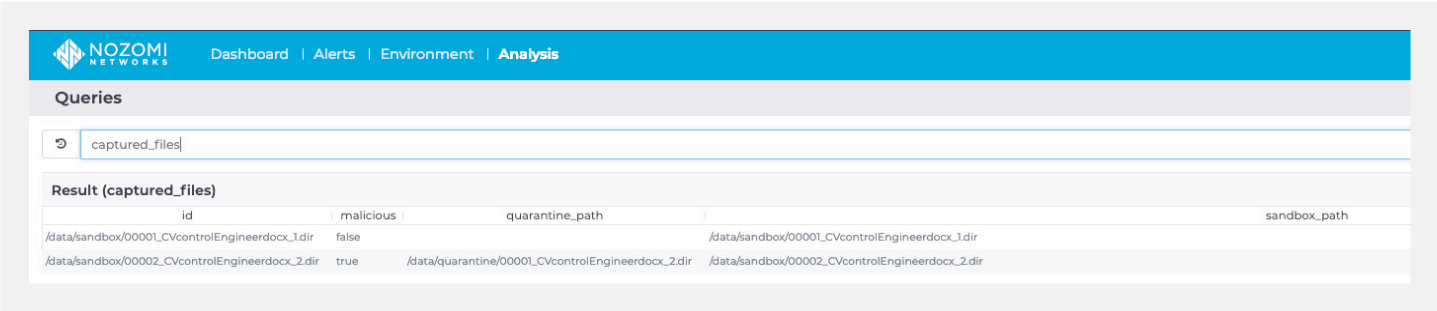


Figure 10 - Query Showing files in a Quarantined Sandbox

The ICS visibility and security solution has a local sandbox for further forensic tests.

With all signs pointing to a true detection of malware on the system, the immediate outcome of the PoC test was to trigger an incident response effort. The ICS visibility and cyber security solution not only identified the presence of malware, but provided forensic tools and data to speed analysis and response.

Challenge

- Organization is unaware that a malware attack is in process

How a real-time ICS visibility and cyber security solution helps

- It generates an alert identifying the presence of malware on the industrial network, and names the malware.
- It provides tools and data that confirm the finding.
- It provides forensic tools to speed analysis and response.

Results

- Immediate initiation of the incident response plan
- Mitigation and eradication of the threat

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

II. Use Case: Addressing the ICS Cyber Security Skills Shortage

There is an acute, global shortage of people with cyber security skills. In the midstream oil and gas market, this trend is even more severe due to the large numbers of transient workers and retiring baby boomers.

Hiring scarce cyber security talent is difficult. However, if technology that automates ICS network monitoring and threat detection is used, an organization can maintain reliability and cyber resiliency despite a changing workforce.

Using technology to aggregate data at a central site, enriched with as much operational and threat context as possible, can help alleviate the human resource gap. Such a system automatically highlights areas of concern, while at the same time helping people build in-depth knowledge of their systems.

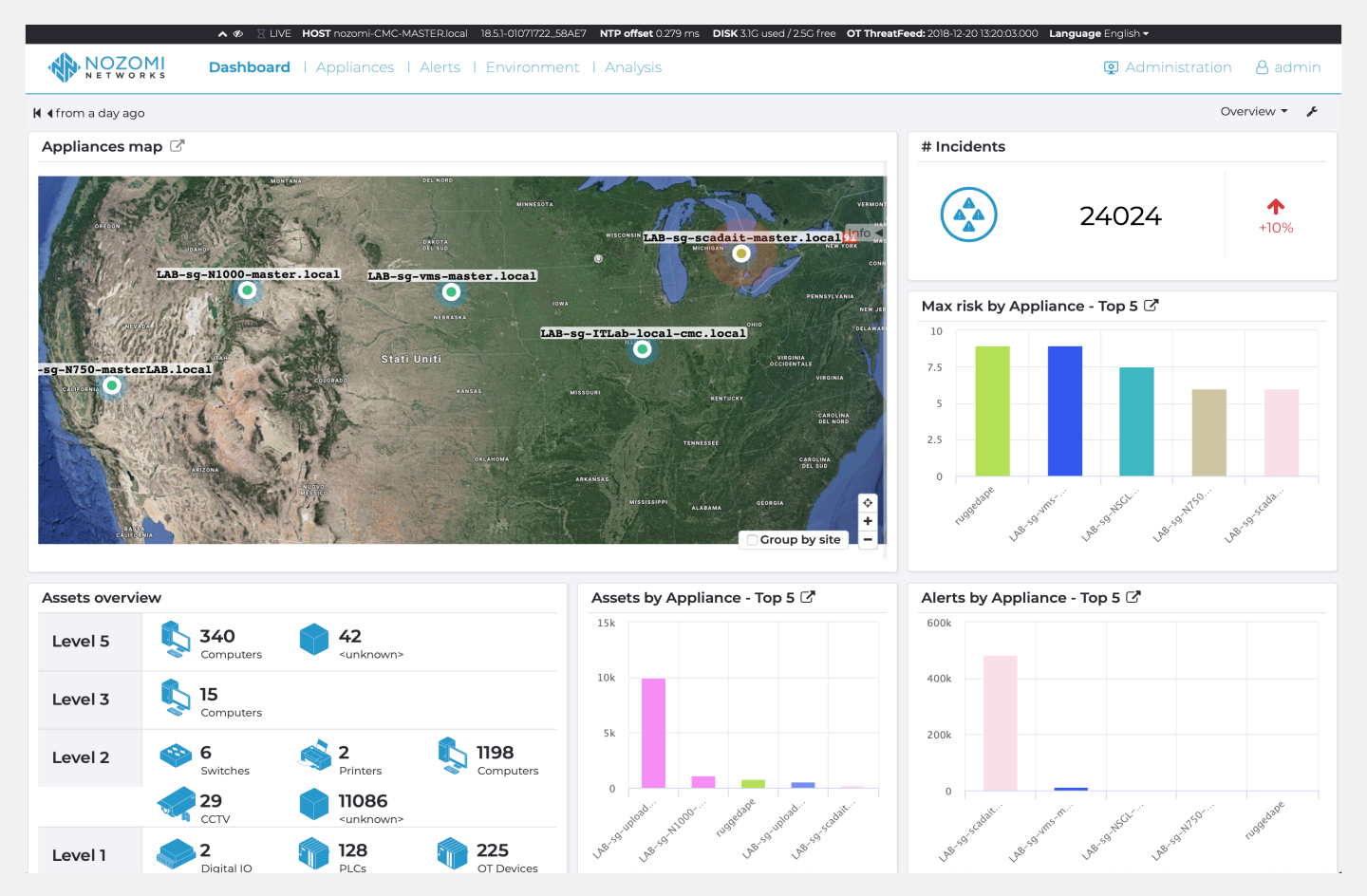


Figure 11 - Dashboard Showing Centralized OT Monitoring

Automated ICS network monitoring and threat detection greatly helps to maintain reliability and cyber resiliency despite a changing workforce.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

Staff quickly get to the point where they can write their own rules in the network monitoring solution to indicate, “Trigger an alert if x happens.” In short, technology elevates workers from entering data to truly analyzing data to make smarter and faster decisions.

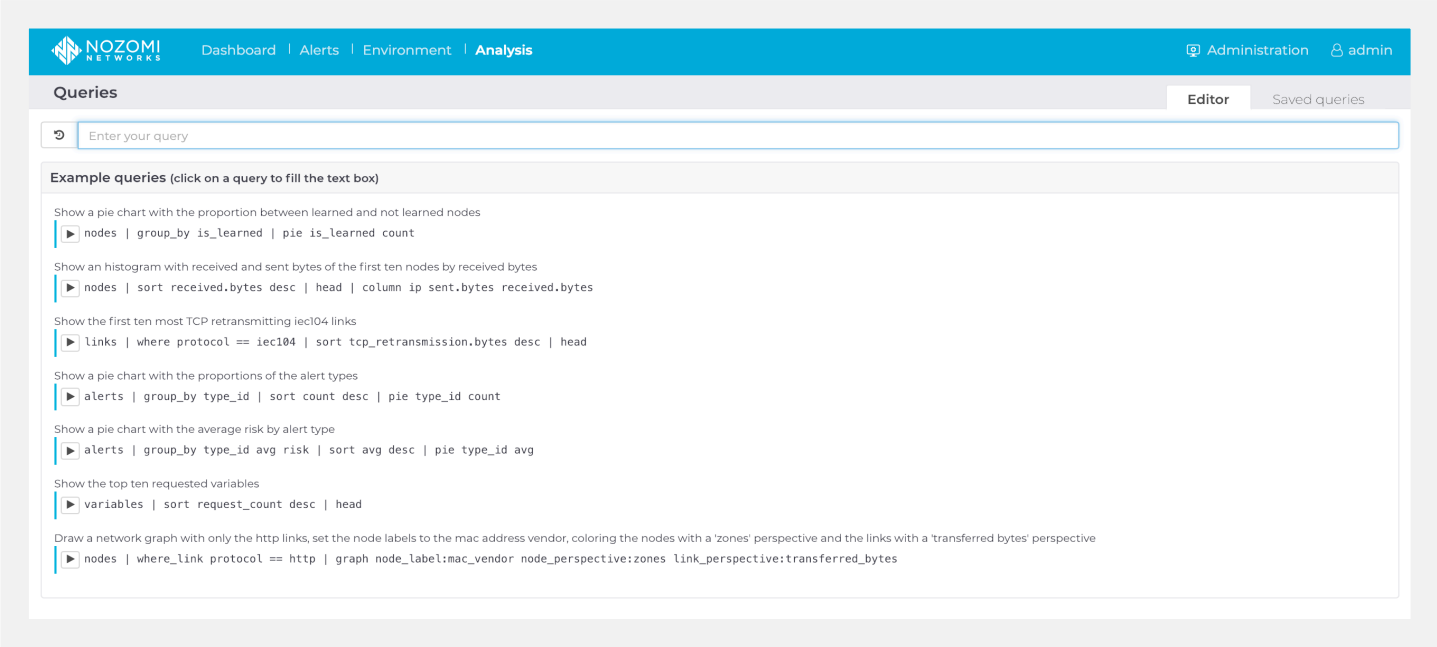


Figure 12 - Customized Queries for Exception Monitoring

Once a system is being monitored for its unique risk factors, it’s easier to change staff and maintain reliability and cyber resilience.

Challenge

- Organization has a shortage of cyber security skills

How a real-time ICS visibility and cyber security solution helps

- It immediately notifies staff of new threats and risks.
- It provides dashboards that summarize and rank threats.
- It facilitates OT system knowledge with real-time visualizations and detailed drill down information.

Results

- Good cyber resiliency despite a human resource gap
- Deeper OT system knowledge for the existing workforce

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

III. Use Case: Improving Cyber Security Productivity

Everyday, government and industry websites publish new Indicators of Compromise (IoCs) for malware threats along with new device vulnerabilities. Checking whether an industrial network has known IoCs or vulnerabilities is a fundamental cyber security measure. However, running checks can be time consuming.

An automated system that receives regular updates on threats and vulnerabilities and checks the system for them is a significant productivity booster. On a day-to-day basis, operators can save 20 percent of their time by eliminating manual checks for new risks.

Furthermore, AI-powered solutions are trained to identify the tactics, techniques and processes (TTPs) of threat actors, whereas most midstream operators are not. Using technology to identify attacks and anomalies is an effective way to reduce the workload related to good cyber security practices.

> *"Previously, it took me two to three hours to go through dozens of pages of information from three systems. Today, some of the cyber security system reviews I do take me as little as 15 minutes.*
>
> *Overall, the automated ICS visibility and security solution has helped me gain back between 10-12 hours a week."*
>
> **NOZOMI NETWORKS CUSTOMER**

Challenge

- Low cyber security productivity

How a real-time ICS visibility and cyber security solution helps

- It automatically checks the industrial network for IoCs, malware and vulnerabilities.
- It regularly receives threat feed updates for new threats and risks.

Results

- Improved employee productivity, by as much as 20%
- Lowered cyber security skills gap
- Enhanced cyber security

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

CONCLUSION

Avoid Downtime with Pipeline Operational Visibility—and Improve Cyber Security Too

You need to be able to see and know what you have before you can defend it.

Accurately documenting the network and asset infrastructure of a SCADA system like a long-distance pipeline used to be time-consuming and difficult, especially in terms of keeping it up-to-date. It was also next to impossible to monitor all the types of equipment involved. Now, thanks to technology advances, it's easy to implement industrial network monitoring that automatically provides real-time network visualization and asset discovery.

And, the great thing is that the same solution can be used to provide early detection of both operational problems as well as cyber security incidents. In the truck offload-onload skid scenario, the Realized ROI of a visibility solution is at least $1.9 million.

That's a significant return based on improved reliability, with added, unquantified cyber security benefits.

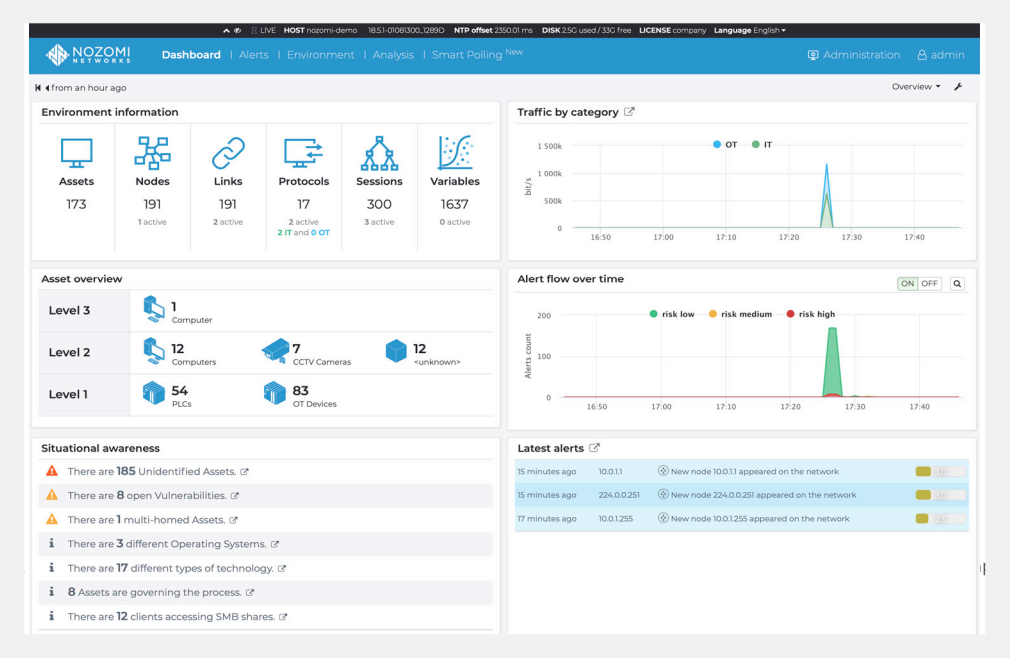


Figure 13 - Dashboard Facilitates Continuous Monitoring of the Industrial Network

A real-time visibility and cyber security solution improves situational awareness, productivity and cyber resiliency.

FIND OUT MORE

If you're a midstream operator you can benefit greatly from investigating network visibility, monitoring and cyber security solutions. Find out for yourself how easy they are to deploy and how quickly they boost visibility, operational reliability and cyber security.

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

What to Look for in a Real-time ICS Visibility and Cyber Security Solution

While increasing cyber threats dominate the news, there is reason to be optimistic.

New technology, such as the Nozomi Networks solution, is easy and safe to deploy, dramatically improves OT cyber security and integrates seamlessly with IT infrastructure.

When choosing a cyber security solution and vendor for your organization, make sure they have the advantages shown here.

- **Accurate OT Operational Visibility**
- **Advanced ICS Threat Detection**
- **Proven, Large-Scale Global Installations**
- **Swift Deployment Across Many Sites**
- **Easy IT/OT Integration**
- **Global Partner Ecosystem**
- **Passion for Customer Success**

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at **nozominetworks.com/contact**

Additional Resources

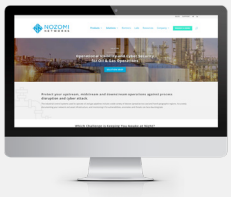
SOLUTION BRIEF

Nozomi Networks

DOWNLOAD

WEBPAGE

Solution: Oil & Gas



VISIT

WEBPAGE

Blog: Oil & Gas

VISIT

WHITE PAPER

Advancing ICS Visibility

DOWNLOAD

© 2019 Nozomi Networks, Inc. / www.nozominetworks.com

References

1. "U-S-Midstream-Oil-And-Gas-Equipment-Market U.S. Midstream Oil & Gas Equipment Market", Polaris Market Research, October, 2018.
https://www.openpr.com/news/1328254/U-S-Midstream-Oil-Gas-Equipment-Market-Industry-Growth-Factors-Applications-Regional-Analysis-Key-Players-and-Forecasts-by-2026.html

2. "North America Midstream Infrastructure through 2035", The Interstate Natural Gas Association of America (INGAA), June, 2018.
https://www.ingaa.org/File.aspx?id=34703

3. "The State of Cybersecurity in the Oil & Gas Industry: United States", Ponemon Institute, February 2017.
https://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf

About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cybersecurity and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.

For detailed information about our products, visit

www.nozominetworks.com

#thosewhoknowpicknozomi

NOZOMI NETWORKS

#thosewhoknowpicknozomi

© 2019 Nozomi Networks, Inc.
All Rights Reserved.

WP-O&G-8.5x11-003