Leveraging the SCADA Cloud for Fun and Profit

GIAC (GCIA) Gold Certification

Author: Matthew Hosburgh, matt.hosburgh@gmail.com
Advisor: Manuel Humberto Santander Peláez

Accepted: *TBD*

Abstract

Long live the operator! At a point in time, they were the backbone of the phone system, ensuring that calls were routed where they needed to go. In many organizations, an operator still exists in one form or another. A version of this operator is common in a Security Operation Center (SOC) and many Industrial Control System (ICS) networks. In the ICS and Supervisory Control and Data Acquisition (SCADA) world, centralized security monitoring is either non-existent or so limited that the information provided does not paint an accurate security picture. To compound the issue, many ICS and SCADA systems cannot be monitored with traditional monitoring vehicles due to latency issues, and often, traditional monitoring does not scale for many SCADA systems. By leveraging elements of the Cloud, Control System operators can effectively and rapidly monitor critical control processes and the security of the network from one location.

1. Introduction

> For three hours, a hacker had strolled through my system, reading whatever he wished. Unknown to him, my 1200-baud Decwriter had saved his session on eighty feet of single-spaced computer paper. Here was every command he issued, every typing mistake, and every response from the computer. This printer monitored the line from Tymnet. I didn't realize it, but a few of our 1200-baud lines weren't dial-in modem lines. Rather, they came from Tymnet, a communications company that interconnected computers around the world (Stoll, 1990).

In *The Cuckoo's Egg,* one of the first Security Operation Centers (SOC) is born. Mr. Stoll was effectively, but maybe not efficiently, monitoring the behavior of an attacker on his network. In this real example, the attacker's motives were not initially known because of the diverse networks he was interested in. The hacker targeted not only university networks, but he went after the Department of Defense (DoD), Intelligence Community (IC) and even nuclear power plants. Was it to steal nuclear weapons information, footprint the systems in use for further exploitation, or was it simply because the attacker was curious? This is not an easy answer, but it is one that can only be answered if the proper monitoring is in place. The events that unfolded in *The Cuckoo's Egg* took place nearly 25 years ago, yet the principles and attacks have only evolved moderately. Supervisory Control and Data Acquisition (SCADA) and other Industrial Control Systems (ICS) are frequent targets for attack because of the data they produce or the devices they control. A targeted attack on one of these systems can result in financial, operational and even human casualties. Traditional monitoring cannot always be adapted to fit these systems because of their distributed nature. The challenge of Network Security Monitoring (NSM) in a SCADA environment can be overcome by implementing traditional NSM methods, leveraging cloud resources and utilizing the operator for early detection.

2. A Brief History of NSM

Network Security Monitoring (NSM) is a key component to monitor Supervisory Control and Data Acquisition (SCADA) systems. In the late 1980s, computers became more interconnected. Universities and the U.S. Government were more reliant and dependent on the capabilities that these systems offered. Sharing data and communicating between these systems was easier, due in part, because these networks took advantage of the Plain Old Telephone Service (POTS). With this new convenience, came a new threat: the attacker. To counter this threat, NSM was born, and maybe with reckless abandon. In the *Cuckoo's Egg*, Cliff Stoll effectively set up one of the first NSM systems. His setup was crude, yet effective. It was clunky, yet sophisticated at the same time. "A printer or personal computer could be wired to each of these lines, recording every keystroke that came through. A kludge? Yes. Workable? Maybe. All we'd need are fifty teletypes, printers, and portable computers" (Stoll, 1990). This first system was just short of a full-packet capturing system, except that it produced hard-copy evidence. In *The Practice of Network Security Monitoring,* Todd Heberlein is credited with developing the first true NSM monitors in 1988. From this foundation, organizations such as the Air Force Computer Emergency Response Team (AFCERT) adopted and practiced NSM, informally (Bejtlich, 2013). Today's NSM systems are more streamlined and aid organizations in identifying attacks on their systems, often in the form of Security Operations Center (SOC). NSM that is properly deployed can aid the SOC in detecting threats, even in a SCADA environment.

2.1 The Role of the SOC in a SCADA Environment

A correctly integrated SOC can add the ability to detect attacks on the organization's SCADA environment. With the SOC as the security focal point of the organization, an organization can develop incident response plans. Based on the varying alerts and alarms, follow-on response activity can be conducted. This response is often handled by the operator or in a coordinated effort between the operator and the incident handler. When this model or process is mature, the SOC can provide an effective means to defend an organization's systems. In figures 1 and 2, a Control Center and SOC display monitors are shown, respectively.

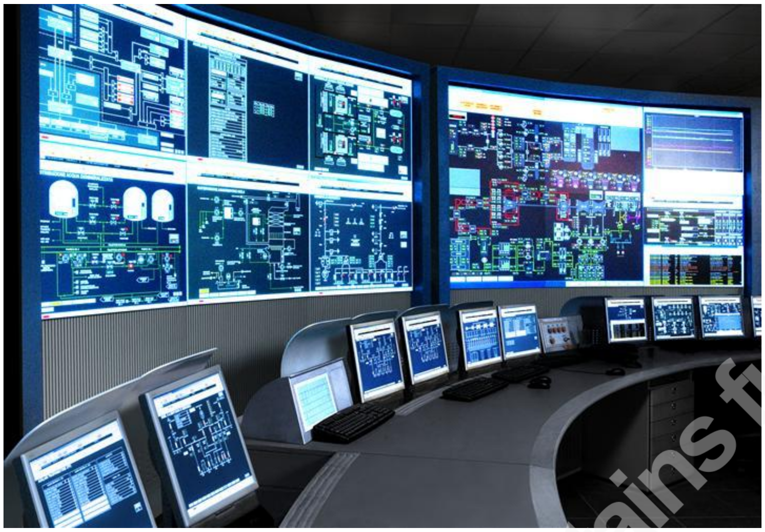


Figure 1. ICS Control Center displays (prohest, 2014).

Figure 2. Security Operations Center displays (NSA, 2012) .

Similar to a SOC is the Control Center, which provides monitoring for various SCADA systems.

2.2 The Regional Control Center

Analogous to a traditional SOC, a regional Control Center enables a centralized view of an organization's industrial functions. One example of this is an organization that monitors pipelines. Centralized monitoring allows for the operator to control and verify that the system is running as expected. If the operator is alerted to an issue, a process is initiated which provides the appropriate level of response. For example, if a pipeline were to reach a pressure that is unsafe, valves can be closed or opened to release pressure and hopefully, prevent a disaster.

Anomalous behavior such as low flow or no flow of gas through a pipeline can also be identified and the appropriate personnel dispatched to take a look at the physical pipeline if needed. This is very similar to the function of a SOC, with some differences. The most common difference is that SCADA systems are typically monitored for operation and not security. This fundamental disparity is due in part by how these systems were brought into operation.

3. The SCADA Difference

SCADA systems differ from traditional Information Technology (IT) systems in a few major ways. For the remainder of this paper, SCADA will be the focus, and must be clearly distinguished from ICS. "SCADA systems are considered to support coordination of infrastructures rather than exercising control over the discrete element of these infrastructure" (Macaulay & Singer, 2012). The more generic term of ICS encompasses the coordination and control over the infrastructure. (Macaulay & Singer, 2012) Although most systems can be setup to “store and forward” events when a connection is restored, if there is a considerable delay, there can be significant inaccuracies in the reporting. These inaccuracies could lead to decreased or increase revenue, the shutdown of operations, and damage to the environment or even loss of life. Weak passwords and clear-text data transmissions in a controlled environment over a network medium both have serious security implications. In the case of a geographically disperse system the meter, valve or other polling is often addressed by leveraging a Remote Terminal Unit (RTU) or specialized Programmable Logic Controller (PLC). In the case of SCADA, the actual control of a remote process is handled by an Intelligent Electronic Device (IED) (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014). During the data transmission, if the network is compromised, the resulting data cannot be guaranteed because it may have been sent in the clear or it may have been manipulated.

The second issue deals with the hardware or software that these SCADA systems reside on. In many cases, this hardware is very specialized or proprietary. This means that the traditional means of interfacing with this device is not always possible. To further compound the issue, many SCADA systems have been in operation for so long, that the hardware can be so unstable or mission critical that any interruption in service is not an option. To fully understand this issue, an example of a SCADA system will be discussed.

3.1 SCADA Example

Not all SCADA systems are created equal, but understanding the basics of these systems will help to recognize how to protect them. SCADA is a way to supervise the data that is being collected so that decisions can be made. Put another way, "SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time" (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014). A simple SCADA system is outlined in figure 3.

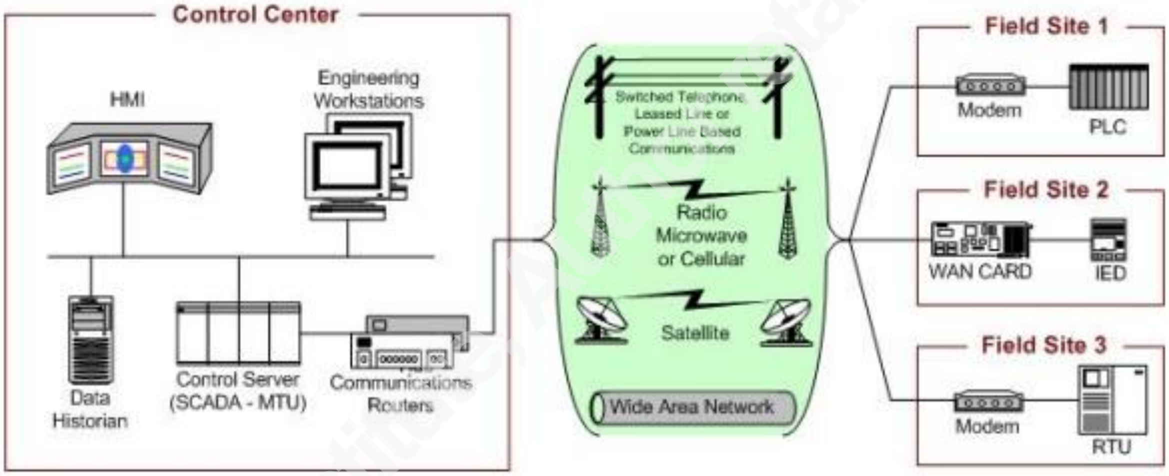


Figure 3. Simple SCADA system (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014).

In many organizations, there is a Primary or Regional Control Center. This Control Center takes various data feeds from remote sites and systems. The data is produced locally and polled or pushed back to the local and then the central Regional Control Center. Depending on the protocols and systems in use, they will dictate how this data is shipped back to the Control Center. At the remote field site, there may be a meter or sensor that reads from the mechanical system (pipeline or other device) and reports the findings via a fieldbus (field network) back to a PLC or Remote Terminal Unit (RTU). A PLC or RTU exists because the analog signal produced from the various sensors or regulators must be translated into a readable, digital signal that can be sent back to the Control Center. A common protocol could be DNP3, MODBUS or OPC. Once in these formats they can be sent across the wire as TCP/IP. By encapsulating into TCP/IP, these protocols can be sent over numerous communications mediums such as wireless, satellite or leased lines, making communication options more abundant. Once the data reaches the Control Center, it is fed into a control server and the results are sent to an HMI for human-readable displays. Often, and shown in figure 3, a data historian is used to archive and record the data being sent and received. By shipping the data to a centralized point, a myriad of monitoring options become available.

4. SCADA in the Cloud

The SCADA cloud is enabling businesses to move their traditional SCADA systems and monitoring to a centralized location. A cloud (and SCADA cloud) can be public, private and semi-private with varying degrees of managed services. In terms of the SCADA cloud the design must take into account regulatory requirements for segmentation and confidentiality, integrity and availability requirements. Additionally, the SCADA cloud would also be aligned to the service levels required by the business. Acquisitions, new facilities, and new exploration are examples of how a business can be presented with new systems and challenges. Given an acquisition that involves a competitor, there is a high probability that the systems in use are not identical in both hardware and software. In some cases, the operations of those systems can also be set to achieve a different goal. One system might be set to monitor the pressure of a liquids pipeline and another might be for a gas pipeline. This means that there is an entirely new system with hardware and software that now must be assimilated into the existing business. This creates a challenge and can be expensive if systems (hardware and software) must be upgraded or replaced. This is one of the major challenges in which the SCADA Cloud can be leveraged. If the centralized Control Center can speak a set of common protocols, then the remote or field systems need only speak one of these protocols to be able to communicate. A small change on the remote device or regional SCADA server could allow minimal change and smaller amounts of configuration time.

In terms of regulation, time would be saved in terms of building a compliant operator display console.

One example of the display requirements of a Control Center comes from the American Petroleum Institute's 1165 publication. This document "Assists pipeline companies and SCADA system developers in identifying items that are considered best practices when developing human machine interfaces. Design elements that are discussed include, but are not limited to, hardware, navigation, colors, fonts, symbols, data entry, and control selection techniques" (American Petroleum Institute, 2014). If this configuration and display is already setup, a large amount of time and effort can be saved, which means a company can rapidly take advantage of a centralized Control center. This is just one example of one particular industry; however, if a more stringent regulatory guidance is used than what is actually required, a more universal standard can be adopted. One such examples, is NIST's Cybersecurity Framework. Although not comprehensive, it shows an industry neutral, concerted effort tackling the security around Critical Infrastructure. Moving SCADA services to a cloud provider is not always welcomed with open arms.

4.1 The Nay-Sayers

Not all operators or security practitioners are comfortable with the notion of a SCADA cloud. More connections can mean more cost in terms of monitoring and security. In a traditional IT world as the business grows, a company may choose to send some or all of its IT services to the cloud. From data storage and email to Security Information and Event Management (SIEM) and SPAM filtering, a cloud based service exists to address nearly every computing need. Concerns of confidentiality, integrity and availability are very real concerns of a SCADA cloud provider. From a regulatory perspective, a company may be required to configure and audit systems on a routine basis. If this is not performed, fines and other threats to operations may exist. In many organizations, the availability of a system is one of the most commonly cited reasons why SCADA systems differ from traditional IT systems. Arguably, the integrity of the data is equally or even more important than just availability.

Moving a SCADA system to a cloud based environment, there are more concerns around the confidentiality of the system. However, the data in transit and rest are not just the issue. It becomes imperative that need-to-know is strictly enforced. The operator monitoring the various SCADA instances must be highly trained, cleared and aware of the systems that are being controlled and monitored. For example if an operator did not know the business and operational difference between a gas pipeline or fermentation tank at a brewery, an extended outage could mean disaster for the pipeline company. In terms of a brewery, this might not be as impactful. Centralizing operations can mean easier security monitoring.

4.2 SCADA SOC in the Cloud

For a Control Center to be in the cloud, it must be secured and monitored for anomalous behavior. A properly configured SCADA Cloud SOC can ensure that security events are detected and responded to appropriately. As the wise Dr. Eric Cole always says about security events: “prevention is ideal, but detection is a must.” Traditionally, SCADA systems are not widely monitored from a security perspective. This lack of monitoring is due to a myriad of reasons such as, antiquated equipment, budgetary reasons, geographically dispersed systems, lack of expertise and, often, operational pace. All of these reasons help to compound the issue of monitoring a SCADA system. Because “the control center is also responsible for centralized alarming, trend analyses, and reporting” (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014), the Control Center (or Cloud SCADA system) is optimally postured to support the security monitoring of these systems. The key to monitoring one of these systems would be in the deployment and architecture of the network environment. It truly depends on the environment, but monitoring a SCADA system can be a difficult task. Newer SCADA (including PLCs, RTUs, and modems) systems often support standards based protocols such as TCP/IP, IPSEC and syslog. Some of the newer systems run on Windows based operating systems (OS), which can be managed by existing security systems. Patching, log monitoring, anti-virus all become more accessible when a SCADA system is running on a commodity OS. Older systems may not have support for the most basic protocols. For this reason, a network based sensor may need to be deployed to monitor the traffic in an older environment. Newer environments may support direct monitoring. If the device does not support encryption or monitoring, a network router or firewall can be utilized to help secure the traffic between an RTU and the Control Center. Leveraging existing systems can be a very effective means to achieve NSM.

5. Tools to Extract the Data

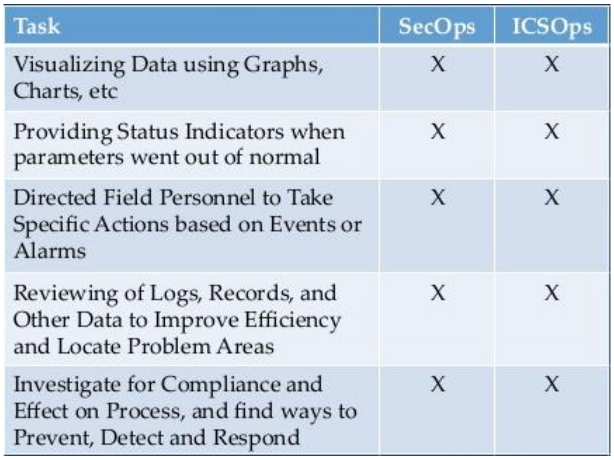
In a SCADA cloud SOC, there are tools that can be easily integrated into the existing environment to allow for security monitoring. In terms of a SCADA Cloud SOC, three toolsets that can provide a monitoring capability will be looked at. The first area is intrusion detection. Traditional IT systems, such as Intrusion Detection or Intrusion Prevention Systems (IDS/IPS), may not include industrial or SCADA signatures. For that reason, it is necessary to implement or install a system that can monitor for SCADA type attacks. Another general practice is that the systems being monitored should be known and the monitoring device should be contextual aware. Put another way, the signatures should be only looking for Windows based attacks if the environment is only running Windows. One toolset that can be implemented is the Quick Draw SCADA IDS Signatures, by Digital Bond. "Digital Bond's SCADA IDS signatures, or rules in Snort parlance, identify unauthorized requests, malformed protocol requests and responses, rar[e]ly used and dangerous commands, and other situations that are likely or possible attacks" (Digital Bond, 2014). One reason these signatures are appealing is that they can be imported into an existing Snort deployment.

Secondly, a way to actually see what is going on with the SCADA processes is necessary. Applications that provide limited control or data acquisition from a RTU or PLC may have the capability of reporting events to a data historian. Often, this system is in place due to regulatory mandates. Another tool by Digital Bond, Portaledge, can be used to help aggregate security events from these historians. Portaledge "…aggregates security events from a variety of data sources on the control system network and then correlates the security events to identify cyber attacks. Portaledge leverages the aggregation and correlation capability of OSIsoft's PI server, and its large installed base in the energy sector to provide this cyber detection capability in a system many industrial control system (ICS) owner / operators already have deployed" (Digital Bond, 2014). Another solution is Industrial Defender, which can be a one-stop-shop for event management in a control system environment. This system, unlike Porteledge, is not free, however can bring a more holistic view of the Control environment. "Industrial Defender ASM™ collects, normalizes, and analyzes the vast amount of information provided by your control systems in a single, unified view, providing you with the actionable intelligence needed to make accurate business decisions and to react to security events that really matter" (Lockeed Martin, 2014). Bringing all this data together is the final step.

Lastly, all of the alert data must be correlated and aggregated for it to provide a holistic view of the monitored SCADA network. After these tools are up and running, the alert data must be sent to a SIEM or other NSM system. In some cases, the system may be that like Industrial Defender's ASM. This will help to ensure that all alerts are sent to one location and that they can be correlated. In addition to the IDS and Portaledge alerts, any infrastructure device that is part of the SCADA system should be configured to send all syslogs to the SIEM or ASM. This approach will provide more alert coverage to ensure that all events are logged and detected. Integrating some of these security alerts into the operator's purview adds speed to incident response. The operator must be attentive to the task at hand, but if additional awareness can be raised in terms of security, the SOC or monitoring entity can be notified earlier, cutting down on response time.

6. Security Framework Mapping: NERC, NIST & SANS

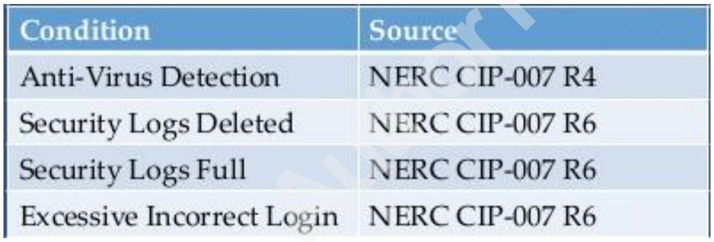
The security surrounding a Control Center as outlined in NIST 800-82 Revision 2, applies to an in-house Control Center as well as, one that would reside in the cloud. According to NIST, "the control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting" (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014). Ironically, there are parallels between the Control Environment and Security Operations as shown in figure 4.



Task	SecOps	ICSOps
Visualizing Data using Graphs, Charts, etc	X	X
Providing Status Indicators when parameters went out of normal	X	X
Directed Field Personnel to Take Specific Actions based on Events or Alarms	X	X
Reviewing of Logs, Records, and Other Data to Improve Efficiency and Locate Problem Areas	X	X
Investigate for Compliance and Effect on Process, and find ways to Prevent, Detect and Respond	X	X

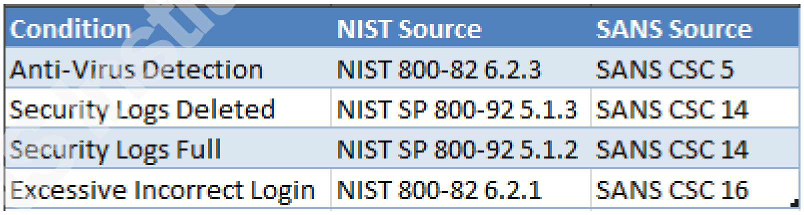
Figure 4. Parallels between Security and Control Center Operations (Toecker, 2013).

From an ICS perspective, centralized alarming is necessary for the Operator to take appropriate action. In many organizations, the Control Center is devoid of any security alerting. This causes a monitoring gap and increased response time between a security event and any incident handling procedures. By integrating these two functions, a higher degree of awareness can be achieved. According to Michael Toecker of Digital Bond, the alerts should be clear, derivable and actionable to not put any undue analytical strain on the operator (Toecker, 2013). In figure 5, these types of events are shown mapped to NERC standards. In figure 6, the events are shown mapped to NIST and SANS guidance.



Condition	Source
Anti-Virus Detection	NERC CIP-007 R4
Security Logs Deleted	NERC CIP-007 R6
Security Logs Full	NERC CIP-007 R6
Excessive Incorrect Login	NERC CIP-007 R6

Figure 5. A list of actionable events that map to NERC CIP (Toecker, 2013).



Condition	NIST Source	SANS Source
Anti-Virus Detection	NIST 800-82 6.2.3	SANS CSC 5
Security Logs Deleted	NIST SP 800-92 5.1.3	SANS CSC 14
Security Logs Full	NIST SP 800-92 5.1.2	SANS CSC 14
Excessive Incorrect Login	NIST 800-82 6.2.1	SANS CSC 16

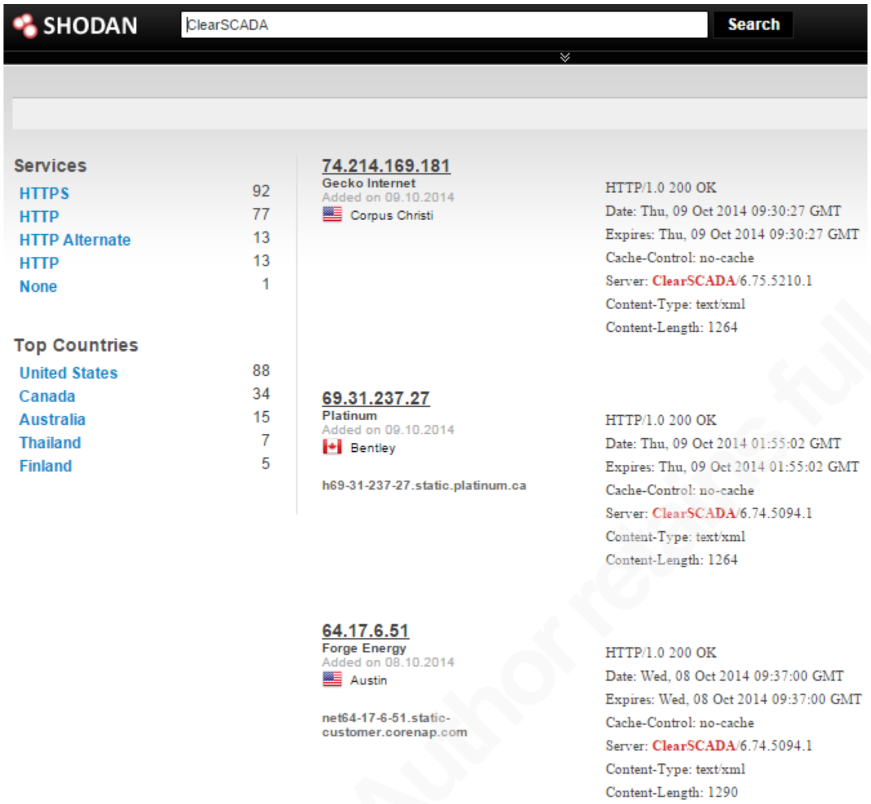
Figure 6. Actionable events mapped to NIST and SANS

The Control Center can be a vulnerability if not correctly protected. In terms of securing SCADA systems, it is clear that technical controls and physical controls are needed. Often times the Control Center must interact or utilize the corporate network and systems. Network transport, system updates, and back-ups are examples of this requirement. An air-gapped system is not necessarily more secure. With inconvenience comes complacency and can lead to security risks. As cliché as Stuxnet is, it is however, a prime example of how an air gap can be circumvented. Per NIST, at minimum, the Control Systems should be logically separated

(Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014). This allows for boundaries to be maintained while paying attention to budget. Logical segmentation is also a recommendation from the SANS Critical Security Control #19.

6.1 Security Framework: SANS Critical Security Control 19

The SANS Critical Security Control 19: Secure Network Engineering is an integral part in securing the SCADA Cloud. As with any network design, it is imperative to design the network in such a way that is can be defensible. In other words, when an attack happens, the infrastructure must be able to be manipulated in a way to prevent further damage. Preventing damage by proper segmentation is one method. In the SCADA Cloud, the infrastructure must be segmented in a way to allow for various levels of SCADA systems to exist in. The Human Machine Interface (HMI) should not be accessible directly from the corporate network or without first traversing a firewall or enforcement zone. Per the SANS Critical Security Control 19-1 a quick win for an organization can be segmentation of the network. “Design the network using a minimum of a three-tier architecture (DMZ, middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet” (SANS, 2014). A prime example of how this architecture is not followed is by conducting a simple Shodan search. In figure 7, “ClearSCADA” is the search term.



Services

HTTPS	92
HTTP	77
HTTP Alternate	13
HTTP	13
None	1

Top Countries

United States	88
Canada	34
Australia	15
Thailand	7
Finland	5

74.214.169.181
Gecko Internet
Added on 09.10.2014
Corpus Christi

```
HTTP/1.0 200 OK
Date: Thu, 09 Oct 2014 09:30:27 GMT
Expires: Thu, 09 Oct 2014 09:30:27 GMT
Cache-Control: no-cache
Server: ClearSCADA/6.75.5210.1
Content-Type: text/xml
Content-Length: 1264
```

69.31.237.27
Platinum
Added on 09.10.2014
Bentley

h69-31-237-27.static.platinum.ca

```
HTTP/1.0 200 OK
Date: Thu, 09 Oct 2014 01:55:02 GMT
Expires: Thu, 09 Oct 2014 01:55:02 GMT
Cache-Control: no-cache
Server: ClearSCADA/6.74.5094.1
Content-Type: text/xml
Content-Length: 1264
```

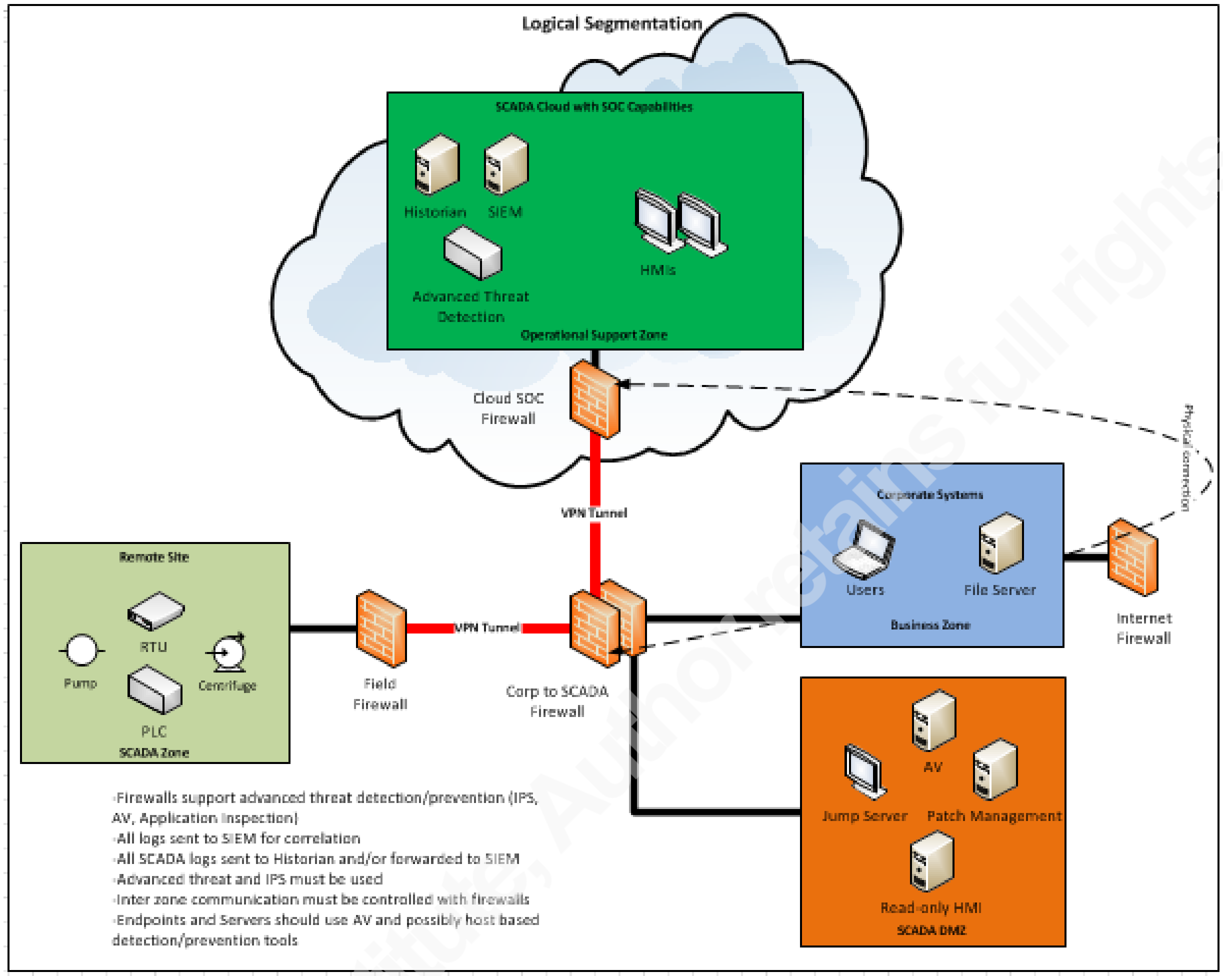
64.17.6.51
Forge Energy
Added on 08.10.2014
Austin

net64-17-6-51.static-customer.corenap.com

```
HTTP/1.0 200 OK
Date: Wed, 08 Oct 2014 09:37:00 GMT
Expires: Wed, 08 Oct 2014 09:37:00 GMT
Cache-Control: no-cache
Server: ClearSCADA/6.74.5094.1
Content-Type: text/xml
Content-Length: 1290
```

Figure 7. Shodan search results for direct to Internet connected SCADA systems.

In Figure 8, the SCADA network is shown with proper zone segmentation, which can help to reduce the attack surface and exposure of a sensitive system. This segmentation is based off of the Purdue Enterprise Reference Architecture (PERA).



-Firewalls support advanced threat detection/prevention (IPS, AV, Application Inspection)
-All logs sent to SIEM for correlation
-All SCADA logs sent to Historian and/or forwarded to SIEM
-Advanced threat and IPS must be used
-Inter zone communication must be controlled with firewalls
-Endpoints and Servers should use AV and possibly host based detection/prevention tools

Figure 8. Segmented SCADA network with a site-to-site VPN with the SCADA Cloud (SANS ICS, 2014)

In figure 9, the data flow between zones is shown. In this case, there is only one zone with direct Internet access. All inter-zone communication must be tightly controlled and restricted.

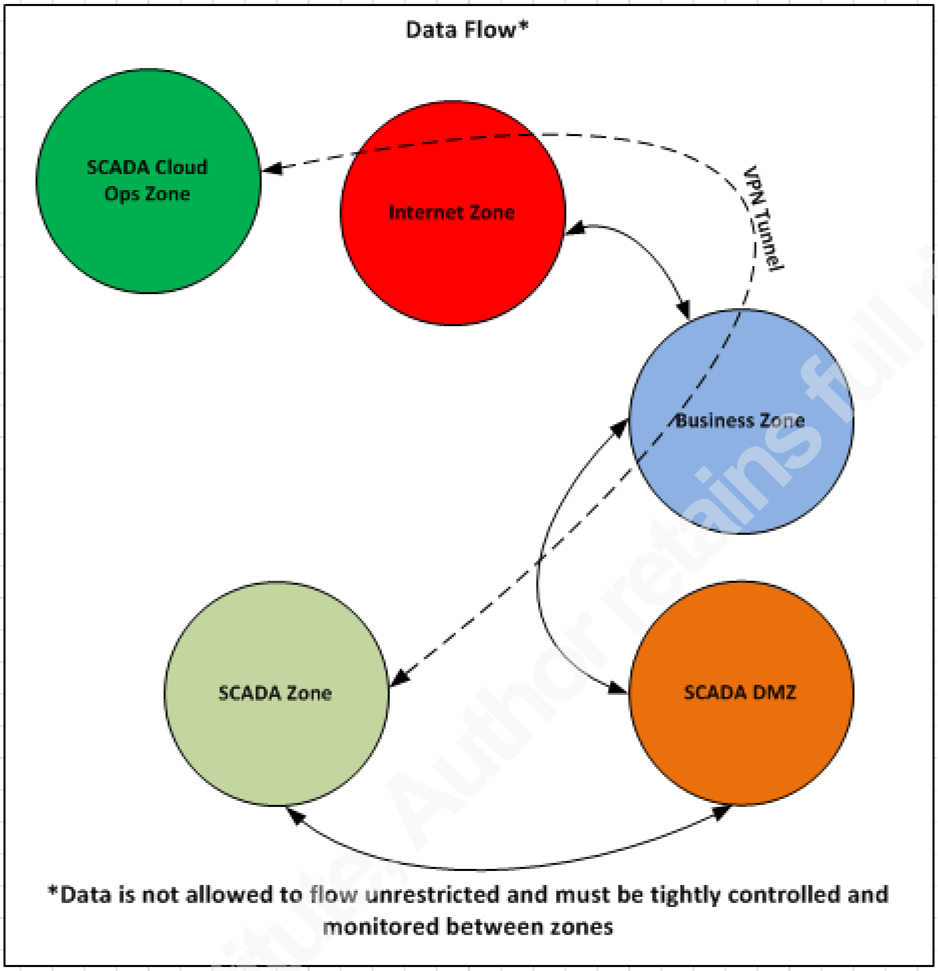

Data Flow*
SCADA Cloud Ops Zone
Internet Zone
VPN Tunnel
Business Zone
SCADA Zone
SCADA DMZ
*Data is not allowed to flow unrestricted and must be tightly controlled and monitored between zones

Figure 9. Proper ICS and SCADA zone segmentation (SANS ICS, 2014).

Furthermore, the ability to secure the data in transit is a requirement with the SCADA Cloud. Because the data may traverse semi-private or public networks, the data should be encrypted with a tunnel or VPN connection. This will help provide confidentiality and integrity as the data traverses intermediate networks.

7. Conclusion

In summary, the practices of monitoring traditional networks have direct applicability into SCADA and ICS networks. The difference is the level of interaction with the devices, which is why network monitoring utilizing varying methods of firewall segmentation and intrusion detection can scale better, with fewer impacts on operations. The principle of monitoring a network can be scaled not only to the Control Center, but also if the Control Center is moved to the cloud. The cloud is simply a mechanism for an organization to rapidly deploy and monitor new systems. The key with the SCADA Cloud is that it can also save time and administrative overhead because it can be configured with the relevant security controls based off of regulatory guidelines. This prevents an organization from having to go through a laborious certification or audit process every time a new Control Center is required. Moving a sensitive operation to the cloud does come with challenges, which is why it is important to leverage logical network segmentation between a corporate network and SCADA network, which is the minimum recommended guidance from NIST. This principle can be further expounded on with the SANS Critical Security Control 19: Secure Network Engineering. By segmenting and providing protection to data at rest a secure and efficient SCADA Cloud can be achieved. Although Security Operations Centers and other forms of Network Security Monitoring have been around for decades, opportunity is created when the SCADA Cloud is considered. Finally, the Control Center operator is at the core of the SCADA network. This individual is similar to a Security Operator, who monitors an organization's network for threats and takes appropriate action. Displaying basic and actionable security alerts to the Operator, the incident response time can be reduced. Focusing efforts and minimizing the time it takes to have new or existing systems monitored will help to better defend any nation's most critical assets.

8. References

American Petroleum Institute. (2014). *Publications.* Retrieved from American Petroleum Institute: http://www.api.org/~/media/Files/Publications/Catalog/Final-catalog.pdf

Bejtlich, R. (2013). The Practice of Network Security Monitoring. In *Understanding Incident Detection and Response.* San Francisco: No Startch Press, Inc.

Bejtlich, R. (2014, September 16). *A Brief History of Network Security Monitoring*. Retrieved from TaoSecurity: http://taosecurity.blogspot.com/2014/09/a-brief-history-of-network-security.html

Digital Bond. (2014, October 12). *Portaledge*. Retrieved from Digital Bond: http://www.digitalbond.com/tools/portaledge/

Digital Bond. (2014, October 12). *Quickdraw SCADA IDS*. Retrieved from digital bond: http://www.digitalbond.com/tools/quickdraw/

Kent, K., & Souppaya, M. (2006, September). *Special Publications (800 Series).* Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Knapp, E. D. (2011). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* Waltheim: Elsevier Inc.

Lockeed Martin. (2014, November 28). *Security Event Management*. Retrieved from Industrial Defender: http://id.lockheedmartin.com/products/security-event-management

Macaulay, T., & Singer, B. (2012). *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.* Boca Raton: CRC Press.

NSA. (2012). *NSA/CSS 60th Anniversary Timeline - 2000s*. Retrieved from NSA: https://www.nsa.gov/about/cryptologic_heritage/60th/interactive_timeline/Content/2000s/full_images/NSOC.jpg

prohest. (2014, August 5). *Why Not Protect Critical Infrastructure Systems with Whitelisting?* Retrieved from prohest: http://prohest.net/pruuha/protect-critical-infrastructure-systems-whitelisting/

SANS. (2014, October 16). *Critical Security Control: 19*. Retrieved from SANS: http://www.sans.org/critical-security-controls/control/19

SANS ICS. (2014). *SANS Industrial Control Systems.* Retrieved from SANS: https://www.sans.org/event-downloads/35470/brochure.pdf

Stoll, C. (1990). *The Cuckoo's Egg.* New York City: Pocket Books.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2014, May). *Special Publications (800 Series).* Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_draft.pdf

Toecker, M. (2013, September 24). *EnergySec*. Retrieved from EnergySec 9th Annual Security Summit Presentation Archive: http://www.slideshare.net/hyun/shlideshare