Global Information Assurance Certification Paper

Case Study: Energy and Utilities Defense Response Based on 2014 Attack Pattern Statistics

GIAC (GSLC) Gold Certification

Author: Adi Sitnica, adi.sitnica@gmail.com
Advisor: Manuel Humberto Santander Peláez

Accepted: November 22nd, 2014

Abstract

Based on the Verizon 2014 Data Breach Investigations Report, three incident classification patterns account for 83% of known and reported security incidents in the Energy and Utilities industry. That means if we concentrate our defense in depth against those three specific patterns, we can limit and/or reduce our threat-vector surface up to 83%. Industry standards provide guidance for a systematic approach to security, it does not emphasize industry specific attacks, but rather a baseline security framework. An example is securing your systems to a standard that improves your overall security and meets requirements and/or guidelines, but does not enhance the security against specialized attacks, specific to your own industry, and based on latest threat-vector statistics. If you know where 83% of the attacks are coming from, would it not be wise to dedicate special effort to protect against those known threat-vectors rather than non-industry specific ones? With implementation of critical security controls from SANS, leveraging a minimal toolset, this case study paper will provide guidance on how to start the effort to decrease the Energy and Utilities industry attack surface, specifically against targeted industry attacks, and with that cut the industry specific threat-vectors by up to 83%.

1. Introduction

False sense of security and management not understanding the value of cyber security are just a few of the issues why the Energy and Utilities industry are behind in terms of elevating cyber security to a status level on par or higher with physical security. Research by Baker, Filipiak, and Timlin (2011) shows that cyber-attacks against the Energy and Utilities industry or critical infrastructure has seen accelerating threats and vulnerabilities. So what is the industry doing to protect itself? According to the Ponemon Institute, LLC (2011), "Many companies are not doing enough to protect their systems and are rushing to adopt new technologies (such as smart grid) without the appropriate security technologies or controls in place" (p. 1). The key finding states, "According to 71 percent of respondents, the management team in their organizations does not understand or appreciate the value of IT security" (p. 2). So what can we do to improve this statistic? This case study paper will provide guidance on what can be done to drastically decrease the cyber-attack threat surface against the Energy and Utilities industry. Verizon (2014) reports that 83% of known and reported security incidents within the Energy and Utilities industry can be traced to three incident classification attack patterns. Likewise, that means 83% of known and reported cyber-attacks can be used as lessons learned to improve one's own cyber defenses, and limit the overall threat-vector risk by up to 83%. Specifically, these are web application attacks which account for 38%, crimeware which account for 31%, and denial of service (DoS) which account for 14%. In total, the three attack patterns combined account for 83% of the known and reported security incidents in the Energy and Utilities industry in 2014.

Web application attacks are one of the most common methods of cyber-attacks regardless of the industry because of the vast usage of web applications. A Web application is any software that is developed for use and/or interaction with web browsers. Anybody with a computer these days understands what Internet Explorer (IE) is, a web browser. Web browsers are the pathways for web application attacks through the use of programing languages that are used with and/or in conjunction with web browsers such as HTML, JavaScript, Flash, php, etc. Ponemon Institute, LLC (2011) states that 40% of the Energy and Utility's top information technology (IT) security

adi.sitnica@gmail.com

threats were due to insecure web applications, on par with Verizon's 2014 Data Breach Investigations Report (DBIR) statistics. Most of the known and reported breaches seem to have used the pathway of web application attacks or negligent users, from which a percentage fall directly under usage of the internet.

Crimeware attacks are malware-type attacks that are not specific to a specialized attack such as point-of-sale attacks, similar to what happened to Target in the recent months. Majority of crimeware attacks come from internet browsing attack vector. That is, download infected files or visiting infected sites. Those two attack vectors account for 84% of crimeware attack vectors (Verizon, 2014). An Energy and Utility industry example that is high profile can be found in the Stuxnet malware attack. While the original attack was directed, the ability of the Stuxnet infection spread beyond its original target. Stuxnet takes advantage of seven vulnerabilities to spread and infect its targets, the most notable being a vulnerability that allows auto-execution on Universal Serial Bus (USB) drives or portable media (Wueest, 2014), which account for 1% of the attack vectors according to Verizon (2014).

DoS attacks are one of the most publically known attacks due to the wide usage and media coverage. Based on statistics by McAfee (2014), they account for 25% of overall network threats. These attacks are usually used to limit or completely disable a target's ability to perform their regular or standard actions. A real-world example which is widely known is the hacktivist group 'Anonymous' use of DoS attacks to take down Visa and MasterCard's websites in response to those companies cutting ties with WikiLeaks website. There are various forms of DoS attacks and further information can be found online in places such as CERT technical tips website (Tips, n.d.) or SANS Security Laboratory website (Security Laboratory: Methods of Attack Series, n.d.).

An Energy and Utility industry example can be found in the distributed denial of service (DDoS) mitigation report for the energy sector (Prolexic Technologies Inc, 2014). The report explains how a DDoS attack, a form of DoS attack, took down a large metropolitan utility company's website and its pay-by-phone automated billing system for 48 hours. This in turn caused a lot of chaos, including inability for its customers to

adi.sitnica@gmail.com

pay through the website or automated phone billing system, as well as the utilities employees being unable to receive external email.

One of the hardest issues in cyber security is the ability to provide a basis for implementing a solution which will cost upfront, but not provide a return on sale or direct revenue. In a typical managerial structure the decisions that are made are based on profit, thus providing funding to pursue solutions which do not return direct revenue, or for that matter may not even be used, seems illogical. That however is the world we live in; at best we can provide evidence within our industry of such issues, and relate the cost that our competitors and partners have exhausted to deal with the after effects. SANS Institute (2013b, p. 237) has provided a simple approach to measurement; interrelate the risks, threats and vulnerabilities into a simple formula to demonstrate that risk is directly related to the level of threat and vulnerability to you, your systems, or your networks face. Taking information from within the industry and making decisions based on known threat-vectors, associated risks and your organization's vulnerabilities will provide a strong basis to obtain funding to pursue a solution that may not have affected your organization, yet.

2. Threat Mitigation

So now that you know about the majority of attacks against the Energy and Utility industry based on 2014 statistics, are you going to react? And if so, how? There are many options an organization may take to enhance their cyber security defense, but this case study paper will concentrate on specific solutions to the three attack patterns noted in the introduction, which account for 83% of known and reported incidents. One should note that a successful attack can cost the organization an average of $156,000 to resolve (Ponemon Institute, LLC, 2011, p. 5). Taking into consideration the cost, and known threat-vectors, the last part is to make an intelligent choice of how to put this information to good use to make a financially-smart choice. There are some questions one should ask him/herself and the organization:

adi.sitnica@gmail.com

- Have you had an incident in the last 12 months that can be contributed to an incident classification attack pattern from one of the three (web application, crimeware, DoS) that account for 83% of known and reported incidents in 2014?
    - If so, was this incident contained? How much did it cost?
- If not, have you had any attacks and/or breaches against your organization in the last 12 months?
    - If so, what type of incident classification attack pattern was used, or is it not known?

If you believe you have not had any attacks against your organization, you most likely do not have a sufficient process or personnel in-place for detection of such attacks and/or breaches. Now that you have the answers, what do we do with them? One option is to make this process visual and easier to understand by leveraging the capabilities of SecurITree, a software package for attack tree-based threat risk analysis. Within "Figure 1. Disrupt Power Systems, (2014)" you will find high level attack tree analysis demo specific to industrial control systems (Amenaza Technologies Limited, 2014).

To help us visualize our path to a solution within the Energy and Utilities Industry we are going to leverage the SANS Industrial Control Systems (ICS) Security Resource Poster, (SANS Industrial Control Systems, 2013). When looking at possible solutions to implement, one needs to understand the structure and/or layout of the organization, and how the different zones interact with each other. For industrial control systems the operations zone, or the zone where the equipment will be used in its operating state is not the only important aspect to take into consideration. There is also the business and demilitarized zone. The business zone is the overarching umbrella of ICS, a zone in which design and possibly part of development of in-house equipment is done and/or where the procurement of third-party equipment is processed. The demilitarized zone is a more secure zone where the back-end databases run for the enterprise businesses as well as development environments and internet facing security infrastructure is located. In addition there are also zone separation areas which have restricted access and act as gateways for traffic which will also be discussed. Based on your organizational structure and layout the solution may need to be adjusted, but the final product, within the operations zone is similar across most Energy and Utilities industry.

adi.sitnica@gmail.com

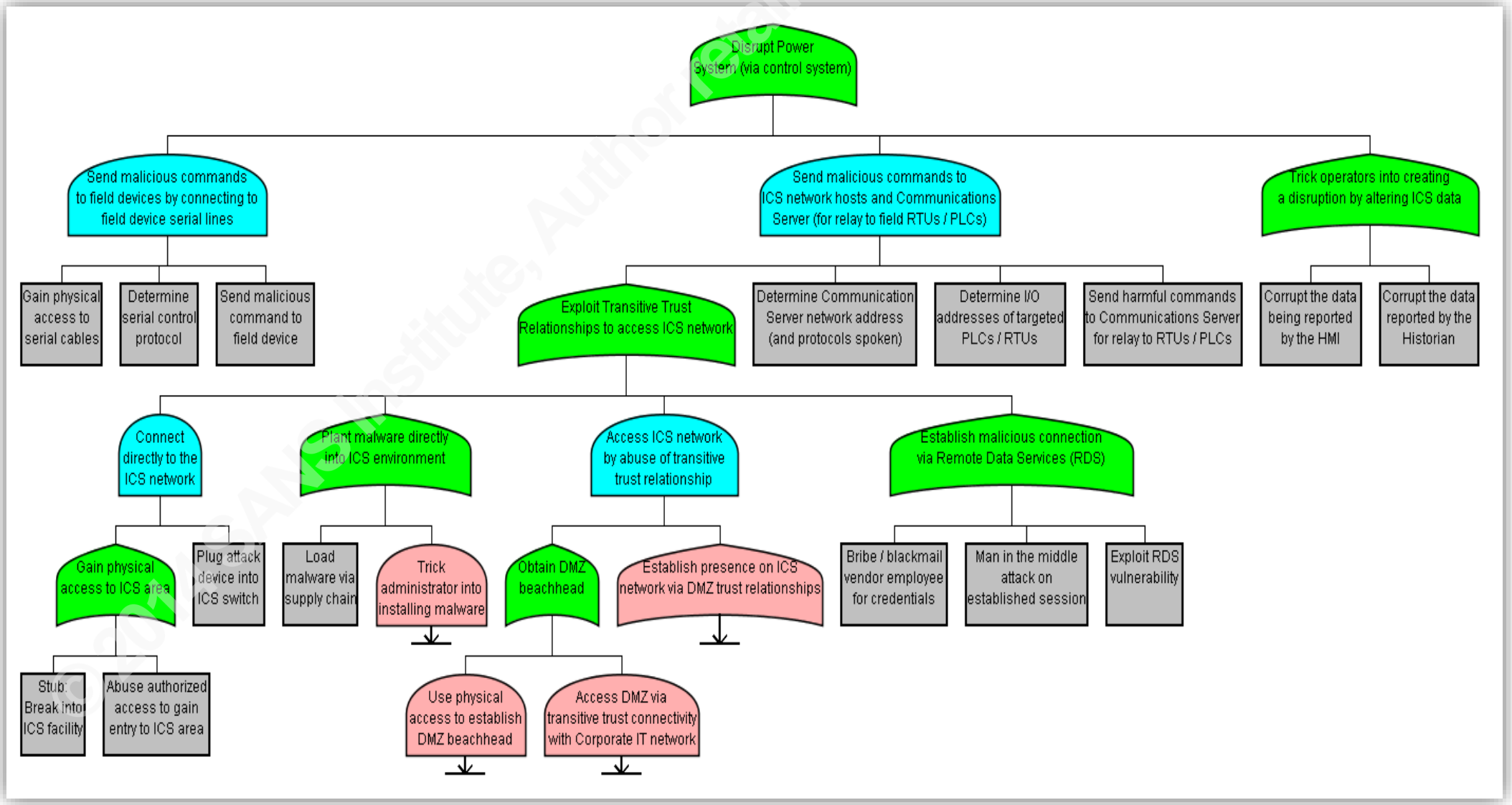

Figure 1. Disrupt Power System Example. Attack tree example that illustrates an attack against a control system.

adi.sitnica@gmail.com

While the goal is to secure the systems within the operations zone, the approach of cyber security is that you are as secure as your least secured asset. You may have the perfect security solution for your servers, but if you use workstations to connect to your servers and those are in an internet café, then your server security is only as good as your workstation security. Having said that, there is a higher chance of web application and DoS attacks on your internet facing assets, located in the business and possibly demilitarized zone, than in your operations zone due to the connectivity pathways to the internet. As an example referenced by SANS Institute (2013c, p. 224), a hacker who called himself 'pr0f' penetrated a South Houston, Texas water-treatment plant to showcase that Internet exposure of supervisory control and data acquisition (SCADA) equipment, located in the operations zone is not wise and that the breach was trivial for him. What does this mean for my organization? Isolation and/or separation of your zones is critical, and protection starts at your lowest, least secure level, preferably in design phase.

The approach taken by this case study paper to enhance the security of the organization will leverage the SANS Critical Security Controls (CSC) (SANS Institute, 2014). In addition it will provide information on tool(s) that can help enhance the visibility and/or protect the organization against the three specific attack patterns; web application, crimeware and DoS. The most cost effective approach is to try and leverage a protective solution that enhances protection against more than just one of the three attack patterns. However note that no one solution is perfect. Defense in depth is ultimately the best security.

2.1. Web Application

Web application attacks account for 38% of the 83% in Verizon's 2014 DBIR, which also means that it is the most used attack vector in the Energy and Utility industry. WhiteHat Security (2014) has provided detailed information on the state of website security across all industries. Within the Energy industry .NET is the most widely used. Overall two of the most common type of web application attacks are Cross Site Scripting attacks and SQL injection attacks. At a high level some of the protection/detection solutions that can implemented to help us against this pattern are standard configurations,

adi.sitnica@gmail.com

restricted use of web-browser and its toolset, and if possible, limited and/or restricted use of internet traffic. In addition better authentication, configuration management, protection against brute force attacks, and monitoring of our internet-facing assets will drastically reduce the attack surface and provide us better visibility. With all these options, where should one start? Taking the approach of improving security by eliminating the easy-fix problems first, and planning for the more complex solutions overtime is the approach one should take. While ideally an organization should take the SANS CSCs and resolve them all one by one, realistically the approach should be to apply controls which are already implemented or close to being implemented. After that, plan for the more complex controls which can be solved, or at least initiated without a major change or influence in the work flow within the organization. To help with this approach each attack pattern will be separated into Easy and Complex Implementation sections. By doing so, the organization will have an ability to start implementation right away with the Easy Implementation section, while working on a plan for the Complex Implementation section which may require extensive time and labor to be completed. The goal is to create a better defense in depth method for the organization with the use of the SANS CSCs, specifically against the web application threat vector.

2.1.1. Easy Implementation

The best approach to security is to enhance your protective strategy by getting rid of low hanging fruit, simple change or changes that will help mitigate the risk without intensive time and/or cost. Let us start at the interface of the web application attack threat, the web browser; the gateway for the attacker. While the root of the problem may lie in the web application code, the code is developed to run in a web browser. Ask yourself whether you have standardized on a web browser in your organization? If not, you may need to investigate further on why that is. In an enterprise environment the standardization of tools provides better streamlining, monitoring and support capability. If you give the end user access to any and all web browsers, you must be willing to invest labor and money into multiple security and support solutions, which in the end may not be required if the organization, or business unit does not have specific web browser requirement(s). Reference the ICS Security Resource Poster, (SANS Industrial Control

adi.sitnica@gmail.com

Systems, 2013); within your operations zone typically there are hardware and software requirements by the vendors of the equipment you are using. The first step should be to create an inventory of your equipment and the software you are using within the operations zone.

Business Situational Awareness is the ability to identify, process, and comprehend the critical elements of information about the surroundings/situation with regards to the organizational mission (SANS Institute, 2013a, pp. 6-7). Understanding the current situation is key to making correct decisions; from a security perspective we need to understand the business first before we can make security changes/implementations. By using SANS CSC #1 and #2 we can gather the technical information necessary to understand how the business works. That is, what are we trying to protect? What impact do security changes have on the business? Is there a different security posture between business units, and/or zones? Who are the individuals responsible for the equipment? The approach that we are taking is securing your end product, in this case your money-generating assets within the operations zone. From there we are going to leverage our implemented security solutions and expand upon them to secure the demilitarized and business zone, if applicable. For example, if we investigate the operations zone and find out that we are required to only have one version of IE as our browser, why would we support and/or install Google Chrome or Firefox within the environment? It only adds to the threat vector space, and should be eliminated unless there is a strong business case for it. Situations will arise where individuals within the organization will be against streamlining or using a standardized browser. An example of this is a user using Firefox to do their work because they use Firefox at home and are familiar with it. This does not constitute the extraordinary effort needed to secure and support both IE and Firefox. Thus, the first step in protecting ourselves against web application attacks is to catalogue the hardware and software assets that we use within our operations zone. To tie those two together, knowing what web browsers we have and what they are used on will help us pin-point what we need to protect, and how. For example, if we have only one server within the operations zone that requires the use of IE, then to enhance our security from web application attacks we can implement secure IE configurations as well as limit the server traffic to where and how it is needed within the environment. Consecutively, we

adi.sitnica@gmail.com

can restrict the use of IE and possibly remove it from other equipment which does not require it. While the goal is to enhance our security against the web application threat vector specifically, the inventory collection will support enhancement of security overall, including the other threat vectors discussed within this case study paper, by knowing what we need to protect and dedicating our resources to a specific sub-set of equipment and software. This in turn will reduce our need to investigate non-applicable items, as well as limit the security data required to keep us up-to-date, that is antivirus definitions, patches and updates for our systems.

One of the first steps is to create a repeatable process for the gathering of inventory information of assets, with the goal of automating it in the future. A simple starting point is to leverage the network infrastructure, in this case within the operations zone, and find out what is interconnected. Build the layout from your connectivity point between the demilitarized and the operations zone, the enforcement zone. From there leverage your core network devices and trace all the connectivity paths. While doing so, you should note the network addresses, machine name(s), purpose of the assets, the owner responsible for the device and the business unit/department associated with the device. In addition it should be noted whether the assets are portable and/or personal devices. Built-in tools can and should be leveraged for this task, such as data tables of your core networking equipment; mac address and IP tables. Keep in mind that while these can be spoofed quiet easily, this is only one of the first steps; further steps will build upon this information, including verification and confirmation. Once the inventory has been collected, all assets that cannot be assigned to an owner and/or business unit should be marked. Resolving the unassigned items may be labor intensive, and further detail will be provided in the complex implementation section of web application. The rest of the assets can now be further investigated; if they are capable of using a web browser, is there a requirement for a specific one? Once that information is gathered, provide the conclusion on what web browsers are used and/or needed as shown in Figure 2.

adi.sitnica@gmail.com

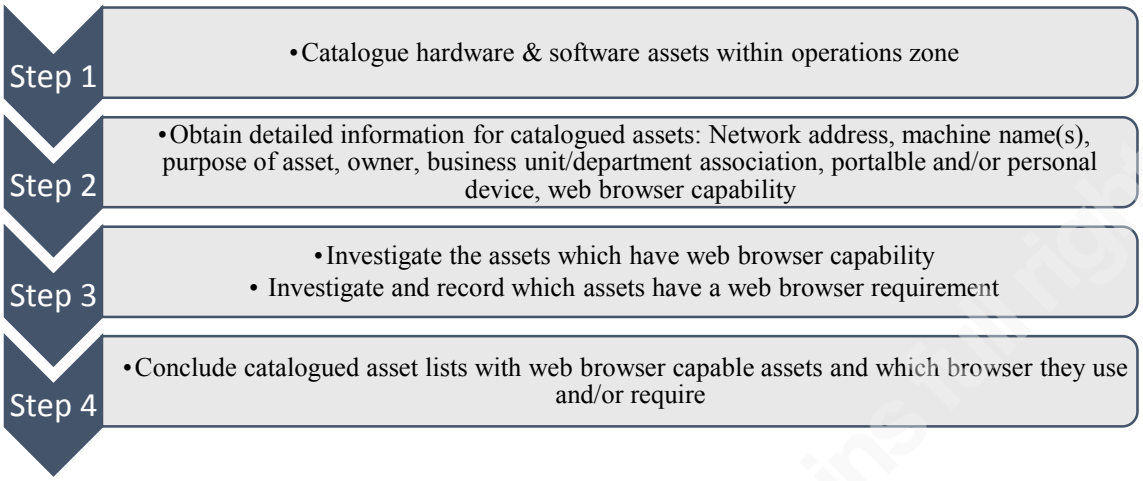

Figure 2. Information progression. Gathering information with follow-up details.

With that information move into implementing a better, more robust web browser configuration. To help with this, leverage security hardening standards such as Center for Internet Security (CIS) benchmarks. Note that some industries have standards available to them; that should be the first step, and CIS should only be leveraged in-addition or when there is a lack of a standard configuration. Implementing secure configurations will depend on what is required for the operations zone to operate normally. If, after the inventory gathering the web browser requirement is IE only, and the only asset that requires the usage of it is a web application which is only accessed through Server X and Y, then we can limit IE as well as our security configuration (CIS Benchmarks or similar) to those servers only. In addition we should limit the IE capability beyond the standard security configuration by levering the web application requirement data sheet. For example, if the web application requires UDP/514 and TCP/3000, 6514, the server X and Y configuration should be limited (via use of host-firewall or similar) to allow communication only on those ports. Another quick-win is to keep the web application up-to-date, especially leveraging the vendor security recommendations. Note that keeping assets up-to-date within the operations zone will require extensive testing and validation, as any changes may affect the operability of the assets.

Now that we have a more secure web browser solution, proceed to standardize on a web browser or browsers, and remove all others from your operations zone, including the blocking of installation/usage of other browsers. This can be achieved through the use

adi.sitnica@gmail.com

of whitelisting software; only allowing your organization's approved web browsers to be used, that is, only allowing software that you approve (whitelist). Alternate options are available such as limiting installation capabilities to authorized individuals or creating a clean baseline configuration and checking changes against it. The latter options may not be as effective as whitelisting software, but are better than no security implementation at all. The most important factor is to test and validate any type of change; whether that is streamlining of a web browser or setting a standard security configuration across the organization as shown in Figure 3. In the end you have to make sure it allows the organization to continue operating with the implemented changes. If you enhance your security to a point where your organization cannot continue operating, then it does not matter whether you are secure or not, you will not be in business because you are not making any money.

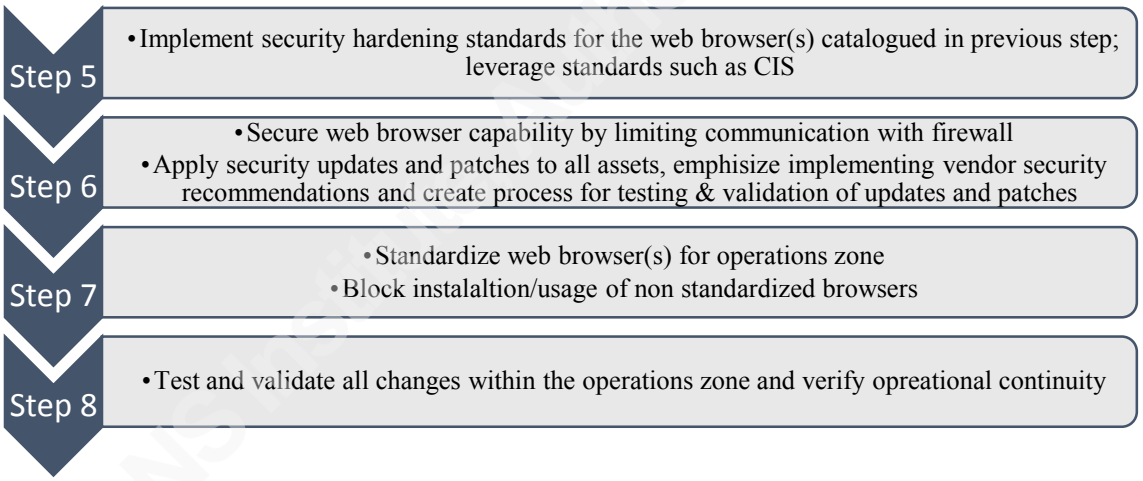

Figure 3. Information progression. Enhancing the web browser.

A comprehensive solution to web application threat vector as well as all others is to have a centralized logging mechanism, such as Security Information and Event Management (SIEM) appliance. From all of the other security implementations, a centralized logging mechanism that is capable of alerting on unusual activity should be one of the top priorities. A properly configured SIEM appliance that gathers information from all of your catalogued assets will provide a detailed insight into the organization's daily activities. From there we can leverage the SIEM to alert upon changes or non-normalized activity. There are many solutions out there for a SIEM or a sub-set of a SIEM, some which require funding (McAfee) and some which are open-source (OSSEC).

adi.sitnica@gmail.com

In addition, most operating systems have ability to log events and configure log settings; those logs can then be exported to a correlation engine, and there are many available, both commercial and open source. The goal is to be able to gather log data from all of your assets and create a standardized picture, then alert on any non-standardized activity. For example, if your daily activity is for two users to log onto server Z, then if you see 50 attempts by non-regular users or just a multitude of failed attempts, it should trigger an alert to investigate further. To correlate this to web application attacks, your web application(s) should be configured to send logs to the SIEM as well, and in this case the same example noted above may apply.

As we are dealing with the inventory collection at a network level, we should also investigate the ability to incorporate 802.1x into our environment. Note that this may not be possible for all equipment, especially on level zero of the operations zone. However we are not looking for a perfect solution from the get-go, but rather a comprehensive approach. There are multiple solutions which can be used to authorize equipment onto our network, however 802.1x is one of the more robust ones, and also a standardized method by Institute of Electrical and Electronics Engineers (IEEE). Further information can be found in the IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control (Institute of Electrical and Electronics Engineers, 2010). Note that the implementation of 802.1x should be in addition to your other security solutions, it will not act as a silver bullet solution.

In a lot of cases organizations are implementing solutions which over-restrict, thereby creating a negative atmosphere within the work environment. From a security perspective that is the ideal approach, but from a business perspective it cause issues which decrease the business efficiency. To alleviate that issue start the overall approach by involving your business/departmental leads to create a test/pilot group. Leverage the SANS CSC #16 to achieve this. Knowing what accounts are used in your organization is the one of the first steps. In our case we are concentrating on the operations zone within your organization. Collection of this may be simple, however linking each account to a legitimate use may take time. There is no need to purchase tools for this step as this can be done manually and/or with built-in tools (such as Active Directory for Windows

adi.sitnica@gmail.com

domain networks), depending on your system architecture. Once this list gets compiled, disable all accounts which cannot be traced or associated with a business process and/or owner. If issues arise from disabling accounts; that means that somebody has to be associated with it, which is also a way of finding what is used and who the owner is. Once a complete list is compiled, and all accounts can be accounted for within the organization, ensure that all accounts have an expiration date set. Due to many accounts not being user accounts, there are a few caveats to consider. For non-user accounts that cannot be set to expire, passwords should be very complex, which can be created with the help of password generation tools such as PasswordSafe. Monitoring and alerting on its use should also be enhanced; non-user accounts can be attributed to specific tasks, and any tasks deviating from that should be reported, and possibly immediately disabled. Once all accounts have been configured correctly, create a process of reporting that can be reviewed individually or automatically using software. These should include locked-out accounts, disabled accounts, accounts that do no expire, new accounts, accounts with passwords that exceed the maximum password age, power-user accounts and administrative accounts as shown in Figure 4.

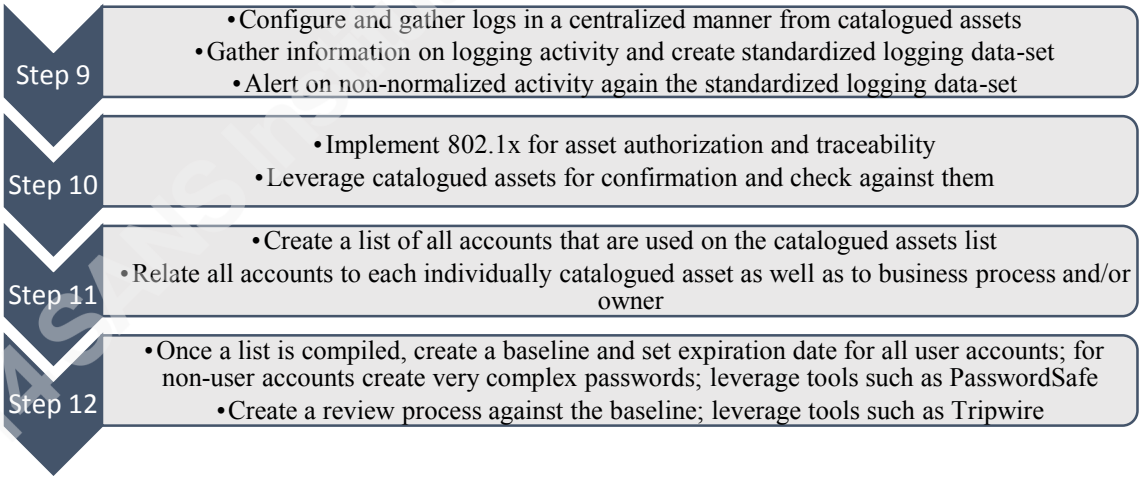

Figure 4. Information progression. Logging, 802.1x and account oversight.

If you prefer a more automated solution, Tripwire provides the capability to create a baseline of your choosing and report against it in real-time. In detail, you have the ability to create an Active Directory Users baseline and report when any changes are detected, such as addition of a user or disabling/deletion of a user. This can help automate the process against a clean baseline, and provide a report of any discrepancies to

adi.sitnica@gmail.com

Administrators. With that we should establish a documented process for disabling accounts upon notification of termination for individuals; this process may include steps of creation for new accounts as well. Use monitoring tools to detect changes against the baseline list, provided by your original report. That is, any new accounts being created, accounts being locked out, accounts being used during non-standard times, accounts being used to access assets beyond the scope of the account, such as logging into other workstations or starting services. With monitoring and reporting enabled, next steps are to create technical policies to log off users automatically after a set period of inactivity. In addition, screen locks that require re-authentication should be set on all assets. Correlate logs to the baseline standard, if accounts are not being used notify the user and user's manager and disable those accounts if they are not needed. If however they are needed, note as such in your reports and monitor exceptions as shown in Figure 5.

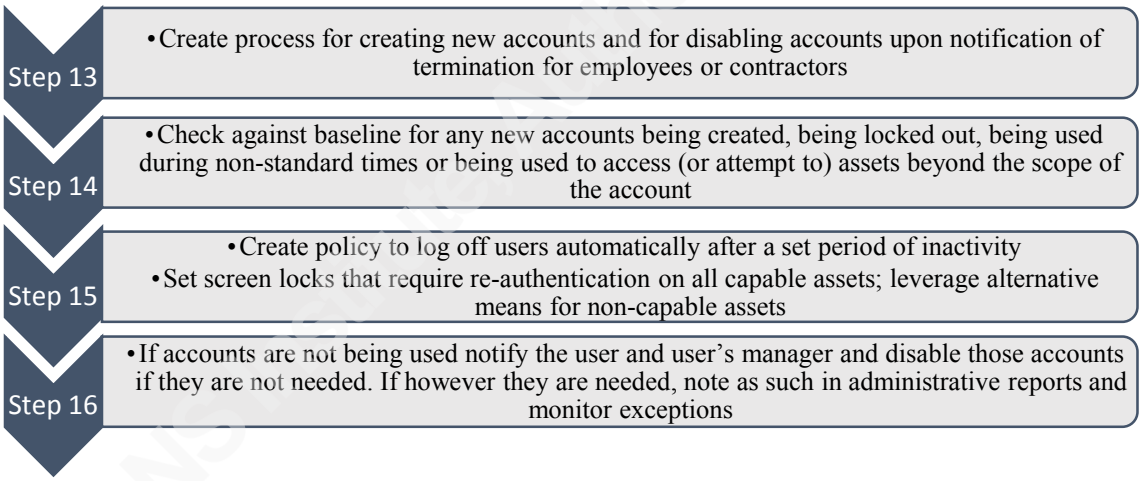

Figure 5. Information progression. Account baseline checks.

The organization should apply a configuration standard when it comes to password settings. One such that can be applied is the CIS standard as discussed previously, however it should be based on your organization needs and capabilities. The values at a minimum which should be set are password complexity, age, history, length and lockout settings. The monitoring aspect of account security should be set as a recurring process. An example of this is to what managers match active employees and contractors on a scheduled basis to ensure individuals are still employed, and still have a need to know associated with the user account. If individuals are no longer employed, or have changed job tasks, the administrator should disable those accounts. Furthermore,

adi.sitnica@gmail.com

monitoring of deactivated or disabled accounts should be alerted upon. This could alert the organization of attack attempts, and further investigation could lead to locating the specific target vector.

With the information gathered thus far you should have a solid view of the infrastructure layout from a user-base perspective; who the users are and what equipment/business unit they are associated with. You will now have contact information for the users which should be related to the business unit owners. That information can be used to help create the test/pilot group for the overall organizational changes, even beyond the operations zone. Specifically the business unit owners can provide you with the end-user resources, technical leads of each of the individual's business units/departments and/or equipment. Having those on a list will help you test/pilot all of the changes required to help with the defense in depth of this case study paper.

Let us go back to the standardization of the web browser and web browser security configuration. You now have the resources required to help you test and validate the changes to the security posture of your organization; leverage them as shown in Figure 6.

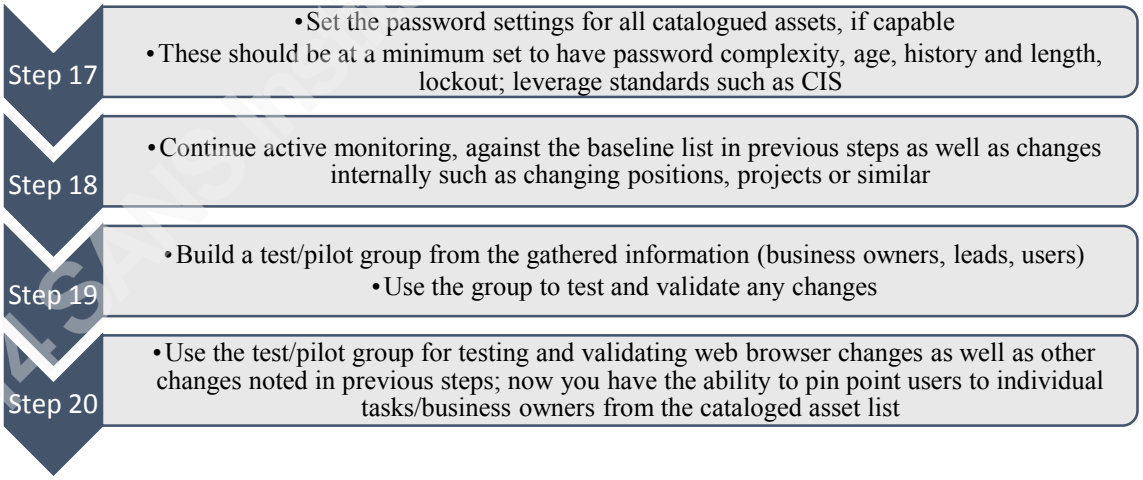

Figure 6. Information progression. Password settings, active monitoring and test/pilot group.

With it, you also need to create processes for future recurring changes, such as keeping your web browsers up-to-date and compliant with the latest security configuration benchmarks. The goal is for your technical leads to confirm the changes does not impact their business unit/department and/or equipment; this may be costly, so

adi.sitnica@gmail.com

you will need risk management to figure out the detail. Are web browsers critical to the work you do? If not, and they are only used for non-critical activities (e-mail, browsing, documentation) you may not need to be as diligent. If however you are a software company that builds web applications, this will impact your business profit margin and should be investigated thoroughly. So what does this do in terms of protection against the web application threat vector?

If we incorporate all of the above solutions we will have limited the web application threat vector space a much more minimalistic sub-set. In detail we know what equipment we have, who the owner and operators are, what they are used for, what they are connected to. With that we have the ability to have a recurring test done on the equipment that is more prone to web application attacks and we have implemented a sub-set of SANS CSCs that will help alleviate the web application threat vector, but also other threat vectors as we will note further below in crimeware and DoS sections. Keep in mind that these solutions are a quick-win approach, simple change or changes that will help reduce the threat vector without much effort. The next section will delve into the more in-depth solutions that will further lower the threat vector space by web application attacks.

2.1.2. Complex Implementation

While working on the Easy Implementation section, a plan should be laid out for solutions which may require an adjustment to the organization framework and/or toolset/standards. Let's take a step back and discuss the unassigned assets in the easy implementation section. Due to the nature where these unassigned assets are located, it will require very detailed investigation, as turning off connectivity to these assets may have a negative cascading effect in the operations zone. We should start with creating a table of unassigned assets and involve all of the technical leads and/or owners noted in our discovery effort. With that we should be able to pin-point what the unassigned assets are, and in the case of inability to do so, we need to create a risk management plan of what can happen with and/or without the assets. That plan will need to be presented to senior management and owners to decide to next step forward in terms of risk for the organization.

adi.sitnica@gmail.com

Moving on, a more complex yet very effective security addition is the use of multi-factor authentication. For organizations without multi-factor authentication, there are commercial options available such as RSA solutions or in-house solutions such as addition of a smart-cards or biometrics. In most organizations these days the employee is mobile, meaning that multi-factor authentication will need to be setup to be used across multiple locations; the office, home and other remote locations. If biometric access is built-in within the organization headquarters, what is being used for at home usage or remote location usage? One of the multi-factor authentication solutions available to the organizations is RSA SecurID; the use of a token in combination of the user's password (Something you have and something you know). In this case the approach should be at the operations zone, and the investigation of demilitarized and business zone should follow afterwards. To tie multi-factor authentication back to web application attacks; there are two primary paths to attack web applications. Through the use of insecure coding or stolen credentials. The security is increased beyond a password's capability against the latter with multi-factor authentication. Now the attacker requires not only the username and password, but also a third piece of information. In addition, multi-factor authentication enhances the security on any username/password authentication process that is capable of incorporating a multi-factor solution. This means that it can be leveraged to enhance the authentication security of all capable assets from our discovery list in the previous section. In addition it will also enhance the security against crimeware and DoS, which will be discussed in latter sections of this case study paper. The result is an overall improved security stance.

Concentrating directly on web application threat vectors we are going to leverage the SANS CSC #6, Application Software Security. In most cases within the Energy and Utilities industry a secure coding standard is mostly non-existent and is only catching up to the Information Technology industry due to the nature of endpoints (sensors, gauges, etc.) being analog. The digital portion that other industries depend on is just recently being incorporated, and thus the standardization and secure standards are behind in terms of other technology industries. Having said that, one of the items the Energy and Utilities industry excels in is independent verification and validation, specifically items that deal with critical infrastructure. While that may be a rigorous process, it does not necessarily

adi.sitnica@gmail.com

concentrate on possible code vulnerabilities with correct code, but incorrect syntax, or correct code with incorrect input possibilities. Keep in mind that writing code is not necessarily something that is done within the operations zone; in most cases it is done within the business or demilitarized zone, or the code is provided by a third-party. If however the organization writes/develops code, the very first step should be to train the coders/developers in secure code writing practices. In most cases within the Energy and Utilities industry, to date, secure code writing is not a priority. That may be changing, but is behind in terms of other industries. For this there are various options available. Please refer to the critical security controls solution providers poster, under section 6, Application Software Security (SANS, 2014). Once a secure coding training has been established, the coders/developers should have a new perspective in terms of creation of applications. As noted above, for web applications there are two primary attack paths; through the use of insecure coding and stolen credentials. In this case we are concentrating on insecure coding, or in most cases incorrect validation of input. One of the first steps is create multiple, separate environments; for production and nonproduction systems. The production systems should follow strict development guidance as well as monitoring using solutions such as the SIEM mentioned in the previous section. Next, the coders/developers should create applications that provide limited output to end-users when errors occur. In other words, provide non-descriptive output so that a regular non-administrative users cannot leverage the output or errors as an attack vector. While secure coding training will provide the coders/developers with more insight, the developed applications should still be tested for common security weaknesses using automated remote web application scanners. These will help with detection of security weaknesses such as input/output validation which will help protect against Cross Site Scripting and SQL Injection attacks, as mentioned in beginning of Section 2. In addition the code should be scanned for coding errors and potential vulnerabilities using static code and analysis software, as well as manual testing and inspection as shown in Figure 7. Some of the tools that can be leveraged for this are HP's Fortify tool or WhiteHat's Sentinel service. For further solutions please reference the Critical Security Controls Solution Providers poster (SANS, 2014).

adi.sitnica@gmail.com

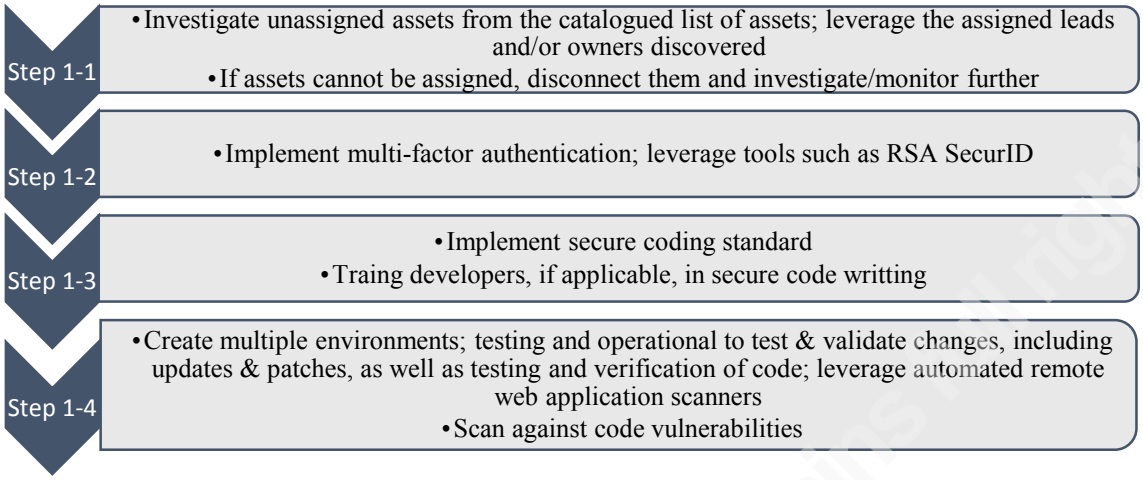

Figure 7. Information progression. Unassigned asset investigation, multi-factor authentication, secure coding, and multiple environments to help with testing and validation.

The final product that will be released and used should always be free of undocumented code, and should only leverage what is needed to operate; i.e. if libraries are not required or called upon, they should be removed from the final product. Finally, if the applications rely on a database, a standard security hardening configuration templates. But what about the products that are not developed in-house, such as commercial off the shelf (COTS) products? The approach for those should be to involve your technical leaders to research various solutions and compare them with security in-mind. That is, examine the products and the companies that developed them: What is their history of security vulnerabilities in their product line? What is their process for customer notification when new vulnerabilities arise? What is their patching/remediation process? How do they handle security issues as part of risk management for the customer-base?

In conclusion, there is no solution that will provide complete protection. Defense in depth is the ultimate solution, and the approach provided in this case study paper will guide you towards a more secure environment overall, while still concentrating on limiting the noted threat vectors, in this case the web application threat vector. In addition, the operations zone is what we are trying to protect, but protection starts even before the business zone; in the design phase. The process used in the operations zone should be used as a template for the demilitarized and business zone, and should expand as per the need of the organization. Note that web application attacks are in the end,

adi.sitnica@gmail.com

'web' applications which should be completely limited, if not completely isolated within the operations zone.

2.2. Crimeware

Crimeware attacks account for 31% of the 83% in Verizon's 2014 DBIR. While crimeware is considered a different attack pattern, it uses a lot of similar attacks as the web application attack pattern, thus the solutions for web application attack patterns will also support protection against crimeware. The ultimate goal is to leverage solutions that help with the enhancement of protection against multiple threat vectors as the approach in this case study paper. Something to note is that web-downloads and drive-bys are most common infection vectors as noted in Verizon's 2014 DBIR (Verizon, 2014). Various solutions used to enhance protection against web application threat vector will also enhance the protection against crimeware, whose primary goal is to take over assets as a platform to leverage for various attacks including stealing legitimate credentials, performing DDoS attacks, or spamming. At a high level some of the protection/detection solutions that can implemented to help us against this pattern are standard configurations, restricted use of web-browser and its toolset, and if possible, limited and/or restricted use of internet traffic. This happens to be exactly the same solutions as noted for web application pattern which is the goal of this case study paper, to build upon defense in depth that helps protect multiple threat vectors. In addition device control and enhanced monitoring that leverages threat feeds and incorporates that information into active blocking and/or alerting, as well as better authentication and centralized anti-malware solutions. The goal will be to provide another layer of defense, with specific anti-crimeware solutions that will support other threat vectors such as DoS which will be expanded upon as the last piece of this case study paper.

2.2.1. Easy Implementation

By taking the approach of getting rid of low hanging fruit as noted in the web application section, let us apply what most organizations these days already have in-place; an anti-virus or –malware solution. However, the one piece that may not be available, is a centralized solution. That is, a solution that manages all of the anti-malware endpoints in a central location, being able to continuously monitor and alert and

adi.sitnica@gmail.com

log, as well as distribute new definitions centrally, whether through a manual or automated process. In addition, the ability to check the version of definitions on each endpoint, as well as leverage information on known hashes for files, i.e. file reputation. There are various solutions out there, so the one that should be chosen should depend on two primary factors: relationship to vendor and ability to expand beyond just anti-malware. Relationship to vendor is beneficial if your organization already has a partnership; you can leverage large discounts on multiple solutions. To add to that, the ability to expand beyond just anti-malware is important, especially when you have the ability to have a centralized location for multiple security solutions. One example is the Lumension Endpoint Management and Security Suite (LEMSS). With the suite you have the ability to leverage anti-virus/malware, device control, patch management and whitelisting amongst others. Note that while the goal is to incorporate various different solutions to keep the bad guys in-check, the ability to have a central location for multiple solutions improves the ability to support the security solution as well as to respond to incidents and/or vulnerabilities. The integration of a suite of tools is a more complex task and will require extensive testing and configuration, but in the long run will provide a more streamlined approach to security which in the end will save time and money.

Let us take the example of the Stuxnet malware; its primary noted distribution vector is through removable media, or more specifically an USB flash drive. There are many threats that spread through removable media, and removable media is also one threat vector that can introduce malicious code into isolated, non-connected systems as well. Thus, the first step is to configure all of the assets that were discovered in the previous section and disable the auto-run feature, regardless of the media; USB, hard drive, CD/DVD, etc. In addition, the assets should be configured to automatically conduct an anti-malware scan when they are detected. The more comprehensive solution would be to enforce device control, which we will discuss in the next section. So what do these additional quick wins provide? They limit malware introduction into the operations zone, where the connectivity path is usually isolated or through a data diode. But does this also apply to the demilitarized and business zone? Yes, but additional steps must be taken in those zones, specifically because the main threat-vector in those levels is the introduction of malware via web-downloads, drive-by downloads or e-mail attachments.

adi.sitnica@gmail.com

As an example that is guided towards the business zone, the scanning and blocking of all e-mail attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. For example an AutoCAD drawing being sent via e-mail to an organization that does not use AutoCAD. In addition, the scanning should be performed before the e-mail in in the user's inbox.

So what does this do in terms of protection against the crimeware threat vector? In addition to leveraging the web application solutions, if we incorporate all of the above solutions we will furthermore have limited the crimeware threat vector, in addition to supporting the overall defense in depth which will also come in play against DoS threat vector.

2.2.2. Complex Implementation

Let us start with the centralized anti-malware solution and expand that to add device control and whitelisting, preferably in a suite of products as mentioned in the previous section. To choose the best solution for the organization will require system architects, security specialists, technical leads and supply chain. Supply chain must be involved to choose the most appropriate solution and obtain the correct pricing as well as agreement. The system architects must understand the organizational layout to provide input to the possible solutions and how they can be implemented and the security specialists must investigate the ability to leverage the security solution to keep all assets in-check. The technical leads will be used a pilot to test the solution will not impact their work. This together will take a long time and should be planned properly by project management. Since this suite will provide the most productivity and capability for the dollar, it needs to be properly assessed as to its capabilities in terms of the organization. In most cases you would want a centralized solution, however when you have isolated environments that can become tricky. Note that a default deny-all cannot be implemented in the operations zone because it would cause the operations zone to work improperly, or in worst case, shut down partially or fully causing a cascading negative effect which may impact the boundaries beyond just the organization. Proper investigation needs to be done, which will require extensive time for testing and validation, especially in the use of whitelisting.

adi.sitnica@gmail.com

Next let us add device control, the ability to restrict your assets, in this case within the operations zone, to disable any non-approved attachments such as USBs, CD/DVDs, removable drives, etc. This type of solution is very powerful, as most operational zone assets do not have to worry about direct internet connectivity threat vectors, but rather the ones that pass the enforcement zone, whether that is via data diode, restricted communication or removable media. The involvement of all of your asset owners, as discovered in the web application section, is key to succeeding. All assets must be accounted for, and allowed before a deny-all is implemented. This means testing and validation in separate environments for the devices in question.

Finally the most complex item, whitelisting. With the previous inventory of software, if correctly accomplished, whitelisting approach will be similar to device control. Whitelisting software will be run in monitor mode to confirm the requirements by the allowed software. To properly accomplish this a clean baseline will need to be created, preferably exactly as within the operations zone. The ability to monitor a clean baseline and make that the whitelisting enforcement policy is crucial. If you are monitoring a system that has already been defeated but not detected, you may create a whitelisting enforcement policy that by default allows the malicious code, unknown to you, to execute. Beyond the suite, the ability to monitor and alert in a centralized manner is key. All logs should be forwarded to the SIEM, as discussed previously and rules should be created to alert on specific actions. For example, if an USB is plugged into any of the assets, an alert should be trigged and security notified.

As stated in the web application section, there is no solution that will provide complete protection. Defense in depth is the ultimate solution, and in this case the goal of the case study paper, to build upon solutions that can protect against a wide range of attack vectors as well as provide additional information to the business leaders, whether they are in security or not. Crimeware specifically noted in this section is one of the more common attack vectors within the isolated environments, common environments within the Energy and Utilities industry, or as described within the poster [Reference], the operations zone. In a lot of cases the crimeware does not get through the network but rather through mobile devices (USB's, CD/DVD's, etc.) and usually during maintenance.

adi.sitnica@gmail.com

Stringency should be put on all assets within the operations zone, whether they are operational equipment or equipment that is used for maintenance.

2.3. Denial of Service

DoS accounts for 14% of the 83% in Verizon's 2014 DBIR. At a high level some of the protection/detection solutions that can implemented to help us against this pattern are secure network hardware configurations, defense response documented plan, isolation and explicit monitoring of internet-facing assets. Some of the protection/detection solutions used with web application and crimeware attack patterns also support protection against DoS attack pattern. What we hear and see on TV these days are usually targeted DDoS attacks, massive network traffic generated by botnets or similar against a specific target. DoS attacks however are not only limited via the network path; it can be done in many ways. For example creating an exponential if-then loop in a program, or a more simplistic method, cutting a power cable to a server. The end result is inability to access the asset/service, hence DoS.

2.3.1. Easy Implementation

The first step should be to leverage what we already have in place, in this case our network equipment knowledge as researched in the above sections. Using the catalogued inventory of hardware we can now pin-point exactly what type of networking equipment we have within the operations zone. That is, firewalls, routers and switches. With that information in-hand, we need to create a secure configuration baseline template for each of the device types. Since majority of this equipment will already be operational, we can leverage the configuration that is already active and verify and validate it. In detail, verification of access control lists (ACLs) and current configuration. In our test environment we can furthermore improve the security by adding or adjusting the configuration to a secure standard (Such as CIS). Once we create a secure baseline for each of the device types, we need to document the changes and/or additions, as well as previous configuration in detail. That is, we need to document the security configuration (baseline) and have it reviewed by the technical leads which the network hardware supports. For example, if we have two switches, one of which is handling the communication of data center rack A which houses the sensors and one which is handling

adi.sitnica@gmail.com

the monitoring system communication, we can involve the sensors technical lead and the monitoring system technical lead for testing and verification, and ultimately have them be part of each of the organization's change control board. With a new secure standard configuration we are able to track any and all changes to our network equipment. While this can be a manual task, the best approach is to leverage a security product such as Tripwire and use it for configuration management of all equipment, specifically in this case specifically the network equipment. Tripwire works by taking the secure, clean configuration that was created previously and creating a baseline within its system. Once done, Tripwire acts as a check; when there are any adjustments made to the configuration it can be setup to alert or take an action. For example, if somebody adds an administrator username to one of my switch configuration, Tripwire would detect the change and alert upon it. In addition it would provide the exact detail of the change in comparison to the original baseline. Additionally if the changes are legitimate, the system can be used to document configuration change, provide notes as to why it was done, and update the new configuration to a new baseline to check against. The multi-factor authentication solution provided in the crimeware section can be leveraged here to increase the security of network equipment authentication as well. With the configuration management system in place, the ability to update and/or patch security vulnerabilities for the networking gear become a much easier task to perform, with detailed visibility. These changes in turn increase the security posture of our network equipment, providing exact detail of the configuration within our operations zone. However that alone does not protect us against DoS attacks. DoS attacks can be done externally, internally, via malicious software, bad system configuration or just plain old usage of stolen and valid credentials. What does this mean? The steps we took in the above sections all support with the enhancement of security against DoS. In addition one of the most important steps to take is to have a process in place when a DoS attacks does happen. That is, what are the steps to take if the DoS is against our network, what about if it is against a specific asset? Who do we call if our systems fail to protect us? A detailed plan of action needs to be available. In addition, the organization's provider will in most cases have an anti-DDoS solution; leverage it. This may apply more towards the demilitarized and business zone, but may apply to the operations zone depending on the interconnectivity. Also note that it is not a full-proof

adi.sitnica@gmail.com

solution; it will fail, especially if the provider starts to concentrate on their network versus your organization, in cases everybody is getting attacked.

If we incorporate all of the above solutions we will furthermore have limited the DoS threat vector, in addition to supporting the overall defense in depth. Keep in mind that these solutions are a quick-win approach, simple change or changes that will help reduce the threat vector without much effort. The next section will delve into the more in-depth solutions that will further lower the threat vector space by DoS attacks.

2.3.2. Complex Implementation

Expand upon the network layout architecture data collected in previous sections. We need to be able to understand how communication is working within the operations zone with all of the changes we have made thus far. Once we understand the traffic flow and the needs for our systems within the operations zone, we need to enhance the separation between them, especially between different zones such as operations zone and demilitarized or business zone. Direct internet access within operations zone is highly restricted or even unavailable while within the business zone it is very lax. We have to consider the usage of data diodes between the zones, if feasible. If not, we need to enhance our ACLs, especially in the operations zone to only allow communication with the operations systems, and deny any other communication.

As stated in the web application and crimeware sections, there is no solution that will provide complete protection. Defense in depth is the ultimate solution, and in this case the goal of the case study paper, to build upon solutions that can protect against a wide range of attack vectors as well as provide additional information to the business leaders, whether they are in security or not. While DoS is not a high risk item for isolated systems, mostly located in the operations zone, it is still possible to create a DoS scenario; maliciously or via bad configuration. DoS does not necessarily mean what is heard on the news; it can be created as easily as a bad network switch configuration during troubleshooting or non-network issue such as malicious code getting onto the isolated system that takes over the systems resources thereby slowing down or completely stopping the operation of the system. There are many scenarios; once you understand the infrastructure (both network and system) and have resources aligned as

adi.sitnica@gmail.com

technical leads and/or owners, if a system is operating outside the norm (i.e. high resource load or high traffic, both possible DoS issues) there should be a plan/process in place to tackle that type of situation. What happens if you disconnect the asset? What happens if you reboot it? It is important that within the operations zone there is minimal or no single point of failures, that is a single asset that if taken out (via DoS or other) it would cause a negative cascading effect or similar. As noted in above sections, understanding your organization, both from a technical and business perspective, and having resources aligned to your assets will take you a long way in troubleshooting possible issues as well as defending against attacks.

3. Expected Results

If the organization implements all of the above discussed solutions they would not only limit the threat vectors against the three attack patterns (web application, crimeware and DoS), but also against many others which are not mentioned. In addition, by incorporating the solutions above it would increase the baseline security posture of the organization and provide in-depth knowledge to the security team to act more efficiently against threats. The organization would have solutions available to leverage for the other ICS zones (demilitarized & business) as a template, and would also meet up to 21% of all SANS CSCs as described in "Figure 8. SANS 20 Critical Security Controls (2014)." What does that mean? Based on the noted Energy and Utilities industry attacks of this case study paper, including information gathered from within the industry, you would have the ability to present a solid case to obtain funding for the security solutions discussed above; both with loss of monetary value within the industry and ability to leverage the solutions beyond the scope of discussed attacks, increasing the security intelligence quotient of the organization as well as business leadership.

adi.sitnica@gmail.com

SANS Critical Security Controls - Version 5	# of Controls	Controls applied via Easy Implementation	Controls applied via Complex Implementation
Inventory of Authorized and Unauthorized Devices	7	2	
Inventory of Authorized and Unauthorized Software	9	2	
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	10	1	
Continuous Vulnerability Assessment and Remediation	10		
Malware Defenses	11	4	
Application Software Security	11	2	7
Wireless Access Control	10		
Data Recovery Capability	4		
Security Skills Assessment and Appropriate Training to Fill Gaps	5		
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	6	3	1
Limitation and Control of Network Ports, Protocols, and Services	7	2	
Controlled Use of Administrative Privileges	14		
Boundary Defense	14		
Maintenance, Monitoring, and Analysis of Audit Logs	10	2	
Controlled Access Based on the Need to Know	5		
Account Monitoring and Control	17	11	1
Data Protection	15		
Incident Response and Management	7		
Secure Network Engineering	4		
Penetration Tests and Red Team Exercises	8		
Percantage (%) met overall	**100%**	**16%**	**5%**

Figure 8. SANS 20 Critical Security Controls. SANS CSCs met with implementation of solutions within this case study paper.

adi.sitnica@gmail.com

4. References

Amenaza Technologies Limited. (2014). SecurITree 4.1 - Build 006 - 2014/07/15 [Software]. Available from http://www.amenaza.com

Baker, S., Filipiak, N., & Timlin, K. (2011, April 19). In the Dark: Crucial Industries Confront Cyber Attacks. Retrieved from http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

Institute of Electrical and Electronics Engineers. (2010, February 5). IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control. IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004), vol., no., pp.C1, 205. doi: 10.1109/IEEESTD.2010.5409813

McAfee. (2014, June). McAfee Labs Threats Report. Retrieved from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf

Ponemon Institute, LLC. (2011, April). State of IT Security: Study of Utilities & Energy Companies. Retrieved from http://www.ponemon.org/local/upload/file/Q1_Labs%20_WP_FINAL_3.pdf

Prolexic Technologies Inc. (2014). DDoS Attack Mitigation Report. Energy. Retrieved from http://www.prolexic.com/knowledge-center-ddos-mitigation-case-study-utility.html

SANS Institute. (2013a). 512.1 Managing the plant, network and information architecture. The SANS Institute.

SANS Institute. (2013b). 512.2 IP concepts, attacks against the enterprise, and defense-in-depth. The SANS Institute.

SANS Institute. (2013c). 512.4 The value of information. The SANS Institute.

SANS Institute. (2014). Critical security controls for effective cyber defense. Retrieved from http://www.sans.org/critical-security-controls

SANS Industrial Control Systems. (2013). SANS ICS Security Resources Poster. Retrieved from https://ics.sans.org/resources/ics-security-resource-poster#ics_request_form

adi.sitnica@gmail.com

SANS. (2014). SANS Critical Security Controls Poster. Retrieved from https://www.sans.org/media/critical-security-controls/fall-2014-poster.pdf

Security Laboratory: Methods of Attack Series. (n.d.). Retrieved from http://www.sans.edu/research/security-laboratory

Tips. (n.d.). Retrieved from https://www.us-cert.gov/ncas/tips

Verizon. (2014). 2014 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/DBIR/2014/

WhiteHat Security. (Fall 2014, 13th Edition). 2014 Website Security Statistics Report. Retrieved from http://info.whitehatsec.com/rs/whitehatsecurity/images/statsreport2014-20140410.pdf

Wueest, C. (2014, January 13). Targeted Attacks Against the Energy Sector. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

adi.sitnica@gmail.com