SIEM for Wayne Enterprises

Western Governors University

Table of Contents

Proposal Overview

Problem Summary

Wayne Enterprises is a small corporate office that specializes in research and development for industrial purposes. They have a small technical infrastructure consisting of one firewall, one domain controller, and several assorted Windows servers. They recently had a security scare when an angry employee was able to add himself to the domain admins security group and negatively changed display names of important people, including the CEO. It was days before anyone noticed; many emails and instant messages with the embarrassing display names had already gone out.

The management team at Wayne Enterprises realize they have a problem. No one is actively looking at security logs due to the inefficiency of going to every device to look for logs and searching through them. Events like the recent security scare may happen at any time and can go undetected for days or weeks. They would like to take a more proactive approach to their security, so they hired Gutz Sec to provide a solution for them.

IT Solution

Gutz Sec has decided to implement a security information and event management (SIEM) system for Wayne Enterprises. A SIEM is an ideal solution for Wayne Enterprises as it will accumulate security log activity from all resources in Wayne Enterprises' technical infrastructure. Gutz Sec selected Splunk as the SIEM solution. The security industry knows Splunk well. There are documentation and example searches all over the web via a quick Google search, and there is free training readily available on its use.

Splunk will get installed on an existing Windows 2016 Hyper-V server that Wayne Enterprises will provide to Gutz Sec for the Splunk environment. This host will inhabit four virtual machines consisting of two Splunk indexers, a search head, and a master server. The logs

from servers, domain controllers, network devices, and anything else Wayne Enterprises decides to implement in the future will go to Splunk via forwarding agents.

Splunk will act as a data aggregator, search, alert, and reporting system for the Wayne Enterprises technical environment. The data will be categorized and efficiently laid out via a central Splunk console for Wayne Enterprises IT to easily access. They will have the ability to create almost real-time alerts for security events, such as users adding themselves to any security groups. The Splunk dashboard is customizable; it is possible to view notable events as soon as anyone from IT logs into it. Splunk will help IT be more proactive in detecting security concerns via Splunk's alert and reporting features. Splunk takes the chore and inefficiency out of chasing logs at every device.

Implementation Plan

The first phase to implement the plan is to determine what logs are available in the Wayne Enterprises infrastructure. The IT Manager provided a brief description of the current inventory. Please see Appendix A for the diagram. Gutz Sec will check for and confirm this inventory via a network scan. Out of the complete technical stock, Gutz Sec will analyze which logs are helpful for security monitoring and alerting.

The next phase is to install the Splunk infrastructure. Gutz Sec will utilize the Wayne Enterprises provided PowerEdge MX840c Windows 2016 Hyper-V server to build the Splunk indexers, search head, and master server. These will be four new Windows 2016 virtual servers. Please see Appendix B for the diagram.

Once the Splunk environment is installed and configured, Gutz Sec will feed security logs from the technical environment of Wayne Enterprises into the Splunk SIEM. Feeding the logs into Splunk will consist of installing forwarding agents on servers such as file servers,

domain controllers, print servers, anti-virus servers, and whatever else turns up in the inventory scan. The domain controller logs will be beneficial to Wayne Enterprises IT. They will receive almost real-time alerts for Windows Security Events 4735, 4732, and 4733, which means someone has changed a security group, added a member, or removed a member.

The next step is to configure alerts, reports, and dashboards that will be useful for the Wayne Enterprises IT team. Some of the many notifications will consist of Windows Security events from the domain controllers that match the addition of users into certain security groups such as domain admin and account lockouts to prevent the brute force of accounts. Many Windows Event codes can assist in detecting security issues at Wayne Enterprises. Please see Appendix C for a small portion of the available Windows Security Log numbers. Gutz Sec will utilize these codes to provide near real-time alerts for Wayne Enterprises IT. Reports will be generated by Splunk monthly with all the Active Directory and Group Policy changes from the month. Gutz Sec will install Splunk application add-ons to provide quick dashboards that IT staff will view upon login. The two dashboards that will get installed are the Splunk Add-on for Active Directory and SonicWall Analytics to view graphical visualizations of firewall traffic.

The final phase is for Gutz Sec to hand off the documentation and management of Splunk to the Wayne Enterprises IT team. Gutz Sec will meet with the IT team face-to-face to provide an overview and training on using Splunk. A tutorial on adding logs from future devices, creating alerts, reports, and searching will be provided by the Gutz Sec team, along with information on how all this helps become proactive in preventing and stopping security breaches.

Review of Other Work

The Splunk SIEM can be very beneficial to any company that cares about its security posture. Logs that typically go unseen can be brought to attention by a SIEM. Shaun Butler, a

Sr. Technology Specialist at Corporate Express, stated that "The IT operations team uses Splunk to provide a single search repository for systems logs, management logs and application logs. This provides advanced visibility across the entire infrastructure for all the different IT teams, including systems, networking, security, applications and development" (Butler, n.d.). Gutz Sec chose to go with the Splunk SIEM for this very reason. Wayne Enterprises suffers from logs scattered everywhere and has the issue of no one taking the time to look at them. Their current method is inefficient. Splunk will help productivity with its automation capabilities. Butler also states that "Further efficiencies have been gained by automating common investigation processes with saved searches and creating dashboards to find issues, understand dependencies and spot trends and patterns far faster and much easier" (Butler, n.d.).

The Splunk SIEM solution will help contain a security incident and bring light to any malicious activity that can usually go unnoticed. As stated in an online article by BusinessWire, "With Splunk technology, the security and network teams have drastically reduced the mean-time-to-investigate (MTTI) and the mean-time-to-resolve (MTTR) issues, allowing intervention before any impact is felt" ("Forschungszentrum Jülich Standardizes on Splunk Enterprise," 2014). Wayne Enterprises recently had a security incident where some important account display names were changed to awful words by an angry employee; this event was embarrassing because emails containing the bad names went out to external parties. Splunk could have prevented the embarrassment by alerting the IT team to resolve the issue before emails went out.

Splunk has helped the Nevada Department of Transportation (NDOT) with efficiency. As listed in a case study, their reason for choosing Splunk was to help with how inefficient their log reviewing method was. "NDOT's manual processes for system log reviews were tedious, unreliable, and often too late to mitigate time-critical issues. To gain visibility into network

traffic, the ISO needed to systematically collect the logs from various hosts" ("Case Study: Nevada Department of Transportation Bolsters Security and Operational Efficiencies," 2016). Wayne Enterprises has the same issue. Their logs are not centrally managed, so the IT staff must manually log in to each device to comb through logs. The case study then states: "Once NDOT began sending log event data from across its infrastructure into Splunk Enterprise, it immediately gained operational visibility into security and IT operations issues that had previously taken numerous man-hours to resolve" ("Case Study: Nevada Department of Transportation Bolsters Security and Operational Efficiencies," 2016). Splunk will provide the same benefit to Wayne Enterprises as they are currently suffering from the same issue. IT staff will have the central visibility they desperately need within Splunk.

Automation is an excellent feature of Splunk. ASICS, a Japanese multinational corporation, utilizes Splunk for its automation. As seen in a success story on the Splunk website, "Splunk software consolidates log data from all systems and analyzes them on a central platform, generating insights and visibility into the entire operation in real time. It then calculates risk scores based on correlation searches and identifies anomalies and threats" ("ASICS Automates Incident Management and Resolution using Splunk," n.d.). The success story also states that "The SOC operators can now access the analysis status anytime and anywhere through an intuitive web console and receive alerts through their smartphones in case of emergency incidents, while the ASICS CSIRT can track post-incident activities easily ("ASICS Automates Incident Management and Resolution using Splunk," n.d.). Splunk can benefit Wayne Enterprises in the same way as it will allow the IT staff to monitor its systems with very little manual intervention. This is a huge step up from what they are doing now, which is rarely looking at logs due to how much time the process consumes.

Project Rationale

Wayne Enterprises would like to be more proactive in security monitoring. These days it is necessary to be proactive in security monitoring due to how common security breaches have been lately. Almost every day, there are news articles of various companies getting breached. Wayne Enterprises had a security scare when a disgruntled employee was able to add themselves to the domain admins security group in Active Directory. The disgruntled employee then made malicious changes to important accounts. It was days before anyone noticed due to IT not checking security logs.

Wayne Enterprises IT claims that it is very inefficient and time-consuming to log into every device and comb through logs to catch an abnormality. They simply do not have time to do this every day and do their day-to-day duties as well. The IT Manager claims that it takes one person two hours a day to log into every device and comb through the logs. The proposed Splunk SIEM will resolve this issue for them.

Splunk will act as a log collecting, investigating, notification, and reporting system for Wayne Enterprises' technical environment. The data will be sorted and efficiently laid out via a central Splunk dashboard for Wayne Enterprises IT to access quickly. They will have the ability to create almost real-time alerts for security events, such as users adding themselves to any security groups. This feature alone would have caught their security scare much sooner.

The Splunk dashboard is customizable; it is possible to view notable events as soon as anyone from IT logs into it. Splunk will help IT be more proactive in detecting security concerns via Splunk's alert and reporting features. Splunk takes the chore and inefficiency out of chasing logs at every device.

Wayne Enterprises IT will automatically receive alerts and effectively view notable security events much faster than logging into individual devices and combing through all the logs. Although Splunk SIEM will not prevent breaches, it will help IT notice security events a lot sooner. IT can then contain or even stop the breach or malicious intent.

Current Project Environment

The IT Manager at Wayne Enterprises has provided Gutz Sec with a brief overview of their technical environment. He stated that the current environment consists of the following: a SonicWall NSa Gen 7 Series Firewall, a physical PowerEdge R750xs rack server running Windows Server 2016 Datacenter acting as a File Server, a physical PowerEdge R750xs rack server running Windows Server 2016 Datacenter acting as a Print Server, a physical PowerEdge R750xs rack server running Windows Server 2016 Datacenter acting as a Sophos Anti-Virus Server, a physical PowerEdge R620 running Windows Server 2016 Datacenter acting as a domain controller. An unused virtual machine host resides on a Dell PowerEdge MX840; this server runs Windows Server 2016 with a Hyper-V role.

The IT Manager has authorized Gutz Sec to utilize the unused hosting server for the Splunk environment. Wayne Enterprises has also permitted Gutz Sec to run a network scan of the Wayne Enterprises network to see if any other devices which were not provided are found. Wayne Enterprises' network only consists of two subnets. One subnet for the resources and one for all the employee workstations. Gutz Sec will run a Nmap scan on both Wayne Enterprises network subnets, take the total inventory, and feed all relevant security logs into the Splunk SIEM. The relevant logs will notify of any network or server breach and any unauthorized changes to their Active Directory environment.

Gutz Sec will build four Windows Server 2016 Datacenter virtual machines consisting of two Splunk indexers, a search head, and a master server in the provided host. The security logs from Wayne Enterprises' servers, domain controller, network devices will go to Splunk via forwarding agents.

Methodology

Gutz Sec will utilize the ADDIE model for this project. There are five phases in the ADDIE Model: Analysis, Design, Development, Implementation, and Evaluation. The phases of the SIEM for Wayne Enterprises project are laid out below:

Analysis – Gutz Sec will meet with the Wayne Enterprises IT team to review how IT employees currently look at logs. This review is needed for Gutz Sec to analyze their needs and evaluate how their current way can be improved. Gutz Sec will additionally see what training will benefit the IT team. This meeting will also include going over the Wayne Enterprises inventory in detail; A system that is not known is not protected. Every important device needs to have its logs investigated by IT. A complete analysis of the environment will be performed.

Design – Gutz Sec will take the information gathered during the analysis phase and create a rough blueprint of the Splunk environment. Since a complete inventory is so important to know what to protect, a model of the network scan steps will be written. During this phase, Gutz Sec will also design alerts, reports, and dashboards to use for Wayne Enterprises IT.

Development – Gutz Sec will develop the steps needed for implementing the SIEM. During this phase, all the software will be downloaded, a complete network diagram of the Splunk environment will be created. Distribution groups will be collected for any email alerts going to the Wayne Enterprises IT team for the Splunk alerts and reports.

Implementation – Gutz Sec will implement all the project action items, which include building the virtual servers, installing all the Splunk software, installing the dashboard add-ons, feeding all the security logs, configuring alerts and reports, and creating documentation and a training schedule.

Evaluation – During this phase, Gutz Sec will evaluate how Splunk performs. Various tests will be generated by Gutz Sec, which includes adding users to security groups, locking out test accounts, and changing test usernames. This is to make sure the alerts and dashboards are working and to show the Wayne Enterprises IT Team how they look. A final meeting with the Wayne Enterprises IT team will be conducted to provide documentation and training. Gutz Sec will take any feedback to see if anything can be done to improve the results.

Project Goals, Objectives, and Deliverables

Goals, Objectives, and Deliverables Table

	Goal	Supporting objectives	Deliverables enabling the project objectives
1	Make accessing security logs more efficient at Wayne Enterprises	1.a. Inventory all assets that offer security logs	1.a.i. Meet with Wayne Enterprises IT to see which logs they are looking at on a regular basis
			1.a.ii. Run an Nmap network scan to look for all technical inventory at Wayne Enterprises
			1.a.iii. Analyze relevant security logs on important systems found during the network scan
		1.b. Build the Splunk SIEM environment	1.b.i. Build four Windows 2016 virtual servers
			1.b.ii. Install the Splunk software for the indexers, search head, and master
			1.b.iii. Download Active Directory and SonicWall dashboard add-ons for Splunk
		1.c. Configure the Splunk SIEM to serve as a central repository for all security logs	1.c.i. Feed relevant security logs into Splunk via forwarding agent on servers
			1.c.ii. Create custom alerts, reports, and dashboards
			1.c.iii Create documentation
			1.c.iv. Test alerts and dashboards

		1.d. Handoff and training	1.d.i. Provide Splunk documentation to Wayne Enterprises IT team
			1.d.ii. Train Wayne Enterprises IT team on Splunk use and configuration
			1.d.iii. Meet with Wayne Enterprises IT to obtain feedback on any issues or improvement

Goals, Objectives, and Deliverables Descriptions

The SIEM for Wayne Enterprises project's primary goal is to provide a more efficient way for Wayne Enterprises' IT department to access security logs. The Splunk SIEM will help Wayne Enterprises as they currently do not look at security logs because they are scattered around and time-consuming to look at on a regular basis. If a security incident happens, it will be a very long time before anyone at Wayne Enterprises notices. Having centrally visible logs, alerts, and reports can save Wayne Enterprise from a malicious security event lingering too much or spreading quickly. They will be able to contain or stop it by being more proactive with the logs. The successful completion of this goal relies on these four objectives and their deliverables:

- Objective 1.a: Inventory all assets that offer security logs. The first step in protecting an environment is knowing what to defend. No one will look at a device or log that is not known to exist.
    - Deliverable 1.a.i: Meet with Wayne Enterprise IT to see which security logs they are looking at regularly. An analysis will be made on what they are looking for and how. Gutz Sec can then improve their process and provide a way to fill in any gaps.
    - Deliverable 1.a.ii: Run a Nmap network scan to look for all technical inventory at Wayne Enterprises. Having a current inventory is vital for knowing which devices exist in the Wayne Enterprises environment.

    - Deliverable 1.a.iii: Analyze relevant security logs on critical systems found during the network scan. Once the inventory is complete, there is a need to know which logs these devices provide.

- Objective 1.b: Build the Splunk SIEM environment. The leading player in this project is the SIEM. The Splunk SIEM will be a new system located in Wayne Enterprise to act as a log collection, alerting, reporting, and centrally manageable system. Splunk will provide the staff with an efficient means to access and analyze security logs.
    - Deliverable 1.b.i: Build four Windows 2016 virtual servers. Splunk will require four servers for the SIEM environment. Two indexers, a search head, and a master server. These are programs that run on Windows.
    - Deliverable 1.b.ii: Install the Splunk software for the indexers, search head, and master. Splunk will need the software downloaded and installed on each server that will be part of the SIEM environment.
    - Deliverable 1.b.iii: Download Active Directory and SonicWall dashboard add-ons for Splunk. To provide dashboards with helpful information, add-ons will need to be installed. The dashboards offer graphical charts and essential alerts that greet the user upon Splunk login.
- Objective 1.c: Configure the Splunk SIEM to be a central repository for all security logs. Splunk will provide an efficient means to view security log information. Splunk will help Wayne Enterprises IT view notable security events more effectively and centrally.

    - Deliverable 1.c.i: Feed relevant security logs into Splunk via forwarding agent on servers. The logs from the Wayne Enterprises domain controller, file server, print server, SonicWall, and Anti-Virus server will get sent into the Splunk SIEM via a small forwarding agent that gets installed locally on the devices.
    - Deliverable 1.c.ii: Create custom alerts, reports, and dashboards. To be an effective way of viewing security logs and notable events, Gutz Sec will create custom alerts, reports, and dashboards. Relevant Windows event codes will generate alerts such as Windows Security Events 4735, 4732, and 4733, which means that someone has changed a security group, added a member, or removed a member.
    - Deliverable 1.c.iii: Create documentation. As the environment is being configured, the documentation will be created as it will be an effective way to capture screenshots and settings. A network diagram of the Splunk environment will also be created.
    - Deliverable 1.c.iv: Test alerts and dashboards. Various tests will be generated by Gutz Sec, which includes adding users to security groups, locking out test accounts, and changing test usernames. These tests are to make sure the alerts and dashboard configurations are working.
- Objective 1.d: Handoff and training. To finalize the project, Gutz Sec will provide a handoff and training for Wayne Enterprises IT on the Splunk SIEM. This training and handoff will help the IT team utilize the SIEM and be informed of all its capabilities.

- Deliverable 1.d.i: Provide Splunk documentation to Wayne Enterprises IT team. All documentation that Gutz Sec will produce will be provided to Wayne Enterprises for their records and future reference. Network diagrams, configurations, step-by-step process on how it was built, and how-to guides will all be included in the documentation packet.
- Deliverable 1.d.ii: Train Wayne Enterprises IT team on Splunk use and configuration. Gutz Sec will provide training to Wayne Enterprises on how to log into the Splunk SIEM, perform searches, customize the dashboard, create, or modify alerts and reports. They will be shown how each alert can help with potential security incidents. How to build onto the SIEM for future growth will also be taught.
- Deliverable 1.d.iii: Meet with Wayne Enterprises IT to obtain feedback on any issues or improvements. A week after the handoff, Gutz Sec will meet with Wayne Enterprises IT to get feedback on how the SIEM is working for them and obtain input on how they utilize and what they think can improve.

Project Timeline with Milestones

Milestone or deliverable	Duration (hours or days)	Projected start date	Anticipated end date
Meet with Wayne Enterprises IT to see which logs they are looking at on a regular basis	4 hours	11/22/2021	11/22/2021
Run an Nmap network scan to look for all technical inventory at Wayne Enterprises	2 hours	11/22/2021	11/22/2021

Analyze relevant security logs on important systems found during the network scan	2 hours	11/23/2021	11/23/2021
Build four Windows 2016 virtual servers	2 Hours	11/23/2021	11/23/2021
Install the Splunk software for the indexers, search head, and master	4 Hours	11/23/2021	11/23/2021
Download Active Directory and SonicWall dashboard add-ons for Splunk	1 Hour	11/24/2021	11/24/2021
Feed relevant security logs into Splunk via forwarding agent on servers	4 Hours	11/24/2021	11/24/2021
Create custom alerts, reports, and dashboards	5 Hours	11/26/2021	11/26/2021
Create documentation	2 Hours	11/26/2021	11/26/2021
Test alerts and dashboards	1 Hour	11/26/2021	11/26/2021
Provide Splunk documentation to Wayne Enterprises IT team	1 Hour	11/29/2021	11/29/2021
Train Wayne Enterprises IT team on Splunk use and configuration	2 Days	01/02/2022	01/03/2022
Meet with Wayne Enterprises IT to obtain feedback on any issues or improvement	2 Hours	01/10/2022	01/10/2022

Outcome

The Splunk SIEM will increase the productivity for Wayne Enterprises as it will bring visibility to logs by means of a central dashboard, automated alerts, and automated reports. The Wayne Enterprises IT department will benefit in the short term by cutting down the time it takes to staff to log into every device and chase down significant security events. An increase in IT

Staff productivity can measure this. The IT Manager claims that it takes one person at least two hours to log into every device and examine the logs. The SIEM will cut this time by about 85%. It can take one person about 20 minutes to log into the SIEM and view all the relevant graphs and numbers in the dashboard. The alerts and reports can be automated, so the data will come to them instead of them going to search for the data.

For the long-term benefit, this SIEM solution will improve the overall security posture for Wayne Enterprises. Currently, the IT staff at Wayne Enterprises rarely looks at logs due to the time-consuming process. Security incidents can be unnoticed due to not having someone constantly manning the logs. The SIEM will bring automated alerts that happen when certain events get flagged. Suppose a malicious user adds themselves to the domain admins security group or tries to brute force a password and locks an account out. In that case, an almost real-time alert can go to the IT staff to contain or stop the incident altogether. All security logs will go to the Splunk SIEM, which brings visibility to 100%.

References

ASICS Automates Incident Management and Resolution using Splunk. (n.d.). Retrieved from Splunk website: https://www.splunk.com/en_us/customers/success-stories/asics.html

Butler, S. (n.d.). *The Business*. Retrieved from https://cdn.featuredcustomers.com/CustomerCaseStudy.document/splunk_corporate-express_20720.pdf

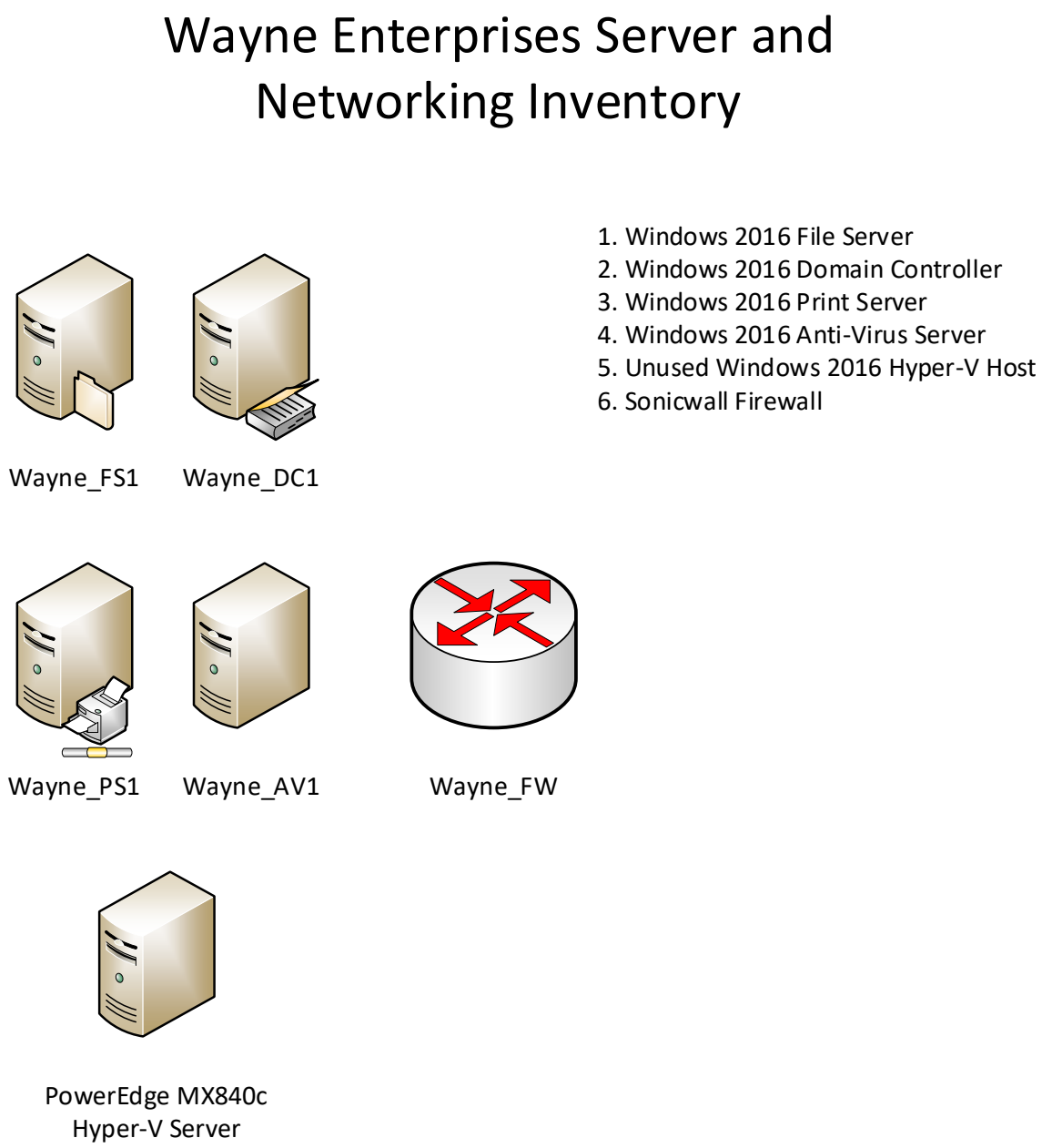
Case Study: Nevada Department of Transportation Bolsters Security and Operational Efficiencies. (2016, July 8). Retrieved from Techwire. Website: https://www.techwire.net/sponsored/case-study-nevada-department-of-transportation-bolsters-security-and-operational-efficiencies.html

Forschungszentrum Jülich Standardizes on Splunk Enterprise. (2014, December 9). Retrieved from www.businesswire.com website: https://www.businesswire.com/news/home/20141209005145/en/Forschungszentrum-J%C3%BClich-Standardizes-on-Splunk-Enterprise

Appendix A

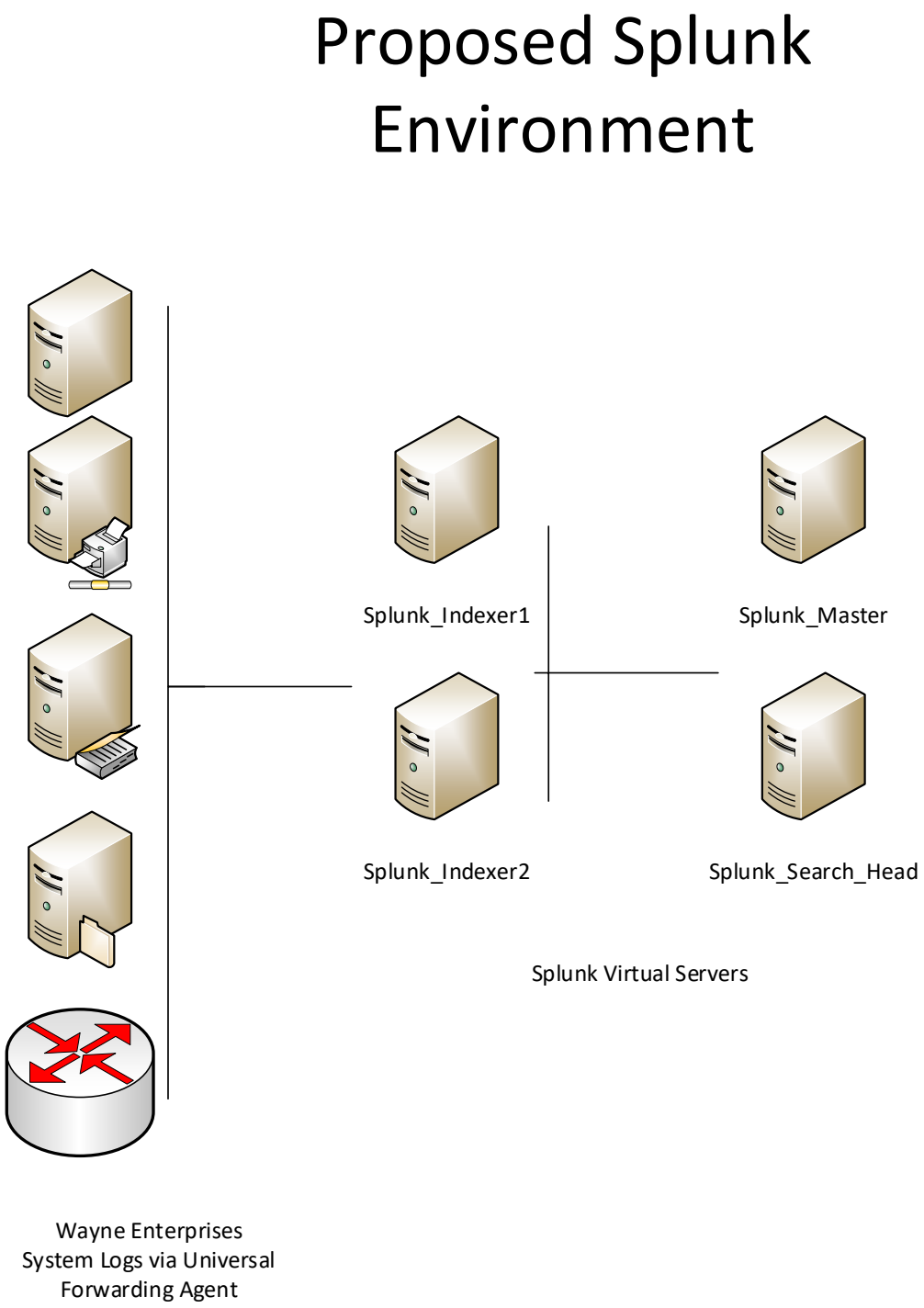
Note: The appendices are not required in this proposal. If you don't use them delete this section and update the Table of Contents.

Wayne Enterprises IT Infrastructure



Appendix B

Proposed Splunk Environment



Appendix C

Example of Available Windows Event Log Numbers

User Account Changes	
4720	Created
4722	Enabled
4723	User changed own password
4724	Privileged User changed this user's password
4725	Disabled
4726	Deleted
4738	Changed
4740	Locked out
4767	Unlocked
4781	Name change

Domain Controller Authentication Events		
4768	A Kerberos authentication ticket (TGT) was requested	
4771	Kerberos pre-authentication failed	See Kerberos Failure Codes
4772	A Kerberos authentication ticket requested failed	

Group Changes		Created	Changed	Deleted	Member	
					Added	Removed
Security	Local	4731	4735	4734	4732	4733
	Global	4727	4737	4730	4728	4729
	Universal	4754	4755	4758	4756	4757
Distribution	Local	4744	4745	4748	4746	4747
	Global	4749	4750	4753	4751	4752
	Universal	4759	4760	4763	4761	4762

Logon Failure Codes	
0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction
0xC00000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC0000224	User is required to change password at next logon
0xC0000225	Evidently a bug in Windows and not a risk
0xC000015b	The user has not been granted the requested logon type (aka logon right) at this machine

Logon Session Events		
4624	Successful logon	Correlate by Logon ID
4647	User initiated logoff	
4625	Logon failure (See Logon Failure Codes)	
4778	Remote desktop session reconnected	
4779	Remote desktop session disconnected	
4800	Workstation locked	
4801	Workstation unlocked	
4802	Screen saver invoked	
4803	Screen saver dismissed	