SIEM for Wayne Enterprises

Western Governors University

Table of Contents

Summary 3

Review of Other Work 6

Changes to the Project Environment 7

Methodology 8

Project Goals and Objectives 10

Project Timeline 12

Unanticipated Requirements 14

Conclusions 14

Project Deliverables 15

References 17

Appendix A 18

Original Wayne Enterprises Network Diagram 18

Appendix B 19

New Wayne Enterprises Network Diagram 19

Appendix C 20

Splunk Environment Overview 20

Appendix D 21

Splunk SIEM Dashboards 21

Appendix E 22

Splunk SIEM Alerts and Reports 22

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 undesirably changed display names of important people, including the CEO. It was days before anyone noticed; many emails and instant messages with the upsetting display names had already gone out.

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

Gutz Sec had 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 log inquiries all over the web via a quick Google search, and there is free training readily available on its use.

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

servers, domain controllers, and network devices go to Splunk via forwarding agents. There is also room for growth. Any future additions to the infrastructure can be easily added.

Splunk acts as a data aggregator, search, alert, and reporting system for the Wayne Enterprises technical environment. The data is categorized and efficiently laid out via a central Splunk console for Wayne Enterprises IT to easily access. Gutz Sec created 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 has helped IT be more proactive in detecting security concerns via Splunk's alert and reporting features. Splunk took the chore and inefficiency out of chasing logs at every device.

The first phase to implement the plan was to determine which logs are available in the Wayne Enterprises infrastructure. The IT Manager provided a brief description of the current inventory. Gutz Sec checked for and confirmed this inventory via a network scan. Out of the complete technical stock, Gutz Sec analyzed which logs were helpful for security monitoring and alerting.

The next phase was to install the Splunk infrastructure. Gutz Sec utilized the Wayne Enterprises provided PowerEdge MX840c Windows 2016 Hyper-V server to build the Splunk indexers, search head, and master server. These were four new Windows 2016 virtual servers that were built into the existing Wayne Enterprises environment.

Once the Splunk environment was installed and configured, Gutz Sec fed all the security logs from the technical environment in Wayne Enterprises into the Splunk SIEM. Feeding the logs into Splunk consisted of installing forwarding agents on the following servers: file server, domain controller, print server, and anti-virus server. The SonicWall logs also went into Splunk.

The domain controller logs were especially beneficial to Wayne Enterprises IT. They 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 was to configure alerts, reports, and dashboards that were useful for the Wayne Enterprises IT team. Some of the many notifications consisted 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. Gutz Sec utilized these codes to provide near real-time alerts for Wayne Enterprises IT. Reports are generated by Splunk monthly with all the Active Directory and Group Policy changes from the month. Gutz Sec installed Splunk application add-ons to provide quick dashboards that IT staff could view upon login. The two dashboards that were installed are the Splunk Add-on for Active Directory and SonicWall Analytics to view graphical visualizations of firewall traffic.

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

Gutz Sec utilized the ADDIE model for the project. The project was split into five phases. All the steps and tasks fit neatly into the phases, and no problematic issues came up. The project was a success and finished within schedule.

Review of Other Work

While selecting a SIEM for this project, Splunk was chosen because it is well recognized in the security community. After Gutz Sec went over several case studies, it was clear why Splunk is an ideal choice. Gutz Sec was able to find the perfect reference from a case study from Enterprisemanagement.com website ("Splunk Enables Security and Improves Business Performance for the Interac organization: An EMA ROI Study - Preview," 2021), which states the following:

> Prior to its deployment of Splunk, the Interac organization had no way to centralize and correlate monitoring data across its diverse IT landscape. This posed a particularly burdensome problem when security issues within the organization's environment warranted investigation, requiring the organization to manually collect and correlate security-relevant data across multiple applications and infrastructure points. This severely hampered the organization's ability to respond in a timely manner, let alone maintain situational awareness on an ongoing basis.

The case study also addresses how beneficial Splunk was to deploy at Interac, a company that had a similar problem that Wayne Enterprises had.

Reports and alerts were developed using automated flags for certain instances, such as users adding themselves to a domain admin group. This method of SIEM development and use case was mirrored from an existing anonymous manufacturing company utilizing Splunk in the same manner. As stated in a case study on the Splunk website, "Today, with Splunk ES alerts,

visualizations and dashboards, the company has a clear understanding of how secure it is and how many vulnerabilities exist" (CASE STUDY Splunk Use Cases • Security • IT operations, n.d.). Wayne Enterprises now utilizes Splunk in the same way, which improves how they used to monitor security logs.

The Splunk dashboards were inspired by how banks use Splunk dashboards for security concerns. As stated in a case study on the convergindata.com website, "Splunk dashboards look at the history of incidents over time and use machine learning algorithms to forecast future incidents. These algorithms can predict when incidents are most likely to occur, by location and also by type" (30 WAYS TO USE SPLUNK IN FINANCIAL SERVICES, n.d.). Gutz Sec created dashboards for Wayne Enterprises for the same purpose, to help their IT department contain security incidents and improve their security posture over time.

Changes to the Project Environment

The original environment at Wayne Enterprises consisted 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 resided on a Dell PowerEdge MX840; this server runs Windows Server 2016 with a Hyper-V role.

The IT Manager had authorized Gutz Sec to utilize the unused hosting server for the Splunk environment. Wayne Enterprises had also permitted Gutz Sec to run a network scan of

the Wayne Enterprises network to look for any devices which were not provided. Wayne Enterprises' network only consisted of two subnets. One subnet for the resources and one for all the employee workstations. Gutz Sec ran a Nmap scan on both Wayne Enterprises network subnets, took the total inventory, and fed all relevant security logs into the Splunk SIEM. There were no unanticipated devices that showed up in the network scan.

For the new environment, Gutz Sec built four new Windows Server 2016 Datacenter virtual machines in the provided host consisting of two Splunk indexers, a search head, and a master server. A new forwarding agent was installed on the existing Wayne Enterprises' file server, domain controller, print server, and anti-virus server. Their SonicWall was configured to forward its logs to the Splunk SIEM. This new environment improved how security logs are utilized at Wayne Enterprises by bringing everything to a centrally managed setting. Wayne Enterprises now has an alerting, reporting, and searching system in place for any notable security concerns mentioned in the logs. They have an ability to stop a breach before it creates too much of an impact, something they did not have before the project.

Methodology

Gutz Sec utilized 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 met with the Wayne Enterprises IT team to review how IT employees looked at logs. This review was needed for Gutz Sec to analyze their needs and evaluate how their current way can be improved. Gutz Sec also performed the evaluation to map out training that would benefit the team. The meeting included 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 was performed. This phase was successful. Gutz Sec was able to see how the Splunk SIEM will improve the current log methods at Wayne Enterprises.

Design – Gutz Sec took the information gathered during the analysis phase and create a rough blueprint of the Splunk environment. Since a complete inventory is significant to know what to protect, a simulation of the network scan actions was written. During this phase, Gutz Sec also designed alerts, reports, and dashboards for Wayne Enterprises IT. This phase was successful. All documentation was designed and provided a clear blueprint for the next phases. Because of this phase, the project finished on schedule with minimal issues.

Development – Gutz Sec developed the steps needed for implementing the SIEM. During this phase, all the software was downloaded, a complete network diagram of the Splunk environment was created. Distribution groups were collected for any email alerts going to the Wayne Enterprises IT team for the Splunk alerts and reports. This phase was successful. No issues came while the software was being downloaded and diagrams were being created.

Implementation – Gutz Sec implemented all the project action items, including 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. This phase was successful. There was a minor hiccup. The change control board needed an extra day to approve the changes. This minor setback did not impact the project timeline too much.

Evaluation – During this phase, Gutz Sec evaluated how Splunk performs. Various tests were generated by Gutz Sec, which included adding users to security groups, locking out test accounts, and changing test usernames. These tests were to make sure the alerts and dashboards

were working and to show the Wayne Enterprises IT Team how the events look. A final meeting with the Wayne Enterprises IT team was conducted to provide documentation and training. Gutz Sec took any feedback to improve the results of the project. This final phase was successful. Splunk alerts are working as intended. The meeting with the Wayne Enterprises IT staff was helpful to them and they were able to improve their whole logging methods with this project.

Project Goals and Objectives

	Goal	Supporting objectives	Deliverables enabling the project objectives	Met/Unmet
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	Met
			1.a.ii. Run a Nmap network scan to look for all technical inventory at Wayne Enterprises	Met
			1.a.iii. Analyze relevant security logs on important systems found during the network scan	Met
		1.b. Build the Splunk SIEM environment	1.b.i. Build four Windows 2016 virtual servers	Met
			1.b.ii. Install the Splunk software for the indexers, search head, and master	Met
			1.b.iii. Download Active Directory and SonicWall dashboard add-ons for Splunk	Met
		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	Met
			1.c.ii. Create custom alerts, reports, and dashboards	Met
			1.c.iii Create documentation	Met
			1.c.iv. Test alerts and dashboards	Met
		1.d. Handoff and training	1.d.i. Provide Splunk documentation to Wayne Enterprises IT team	Met
			1.d.ii. Train Wayne Enterprises IT team on Splunk use and configuration	Met

			1.d.iii. Meet with Wayne Enterprises IT to obtain feedback on any issues or improvement	Met

The SIEM for Wayne Enterprises project's primary goal was to provide a more efficient way for Wayne Enterprises' IT department to access security logs. The Splunk SIEM helped Wayne Enterprises as they did not look at security logs because they were scattered around and time-consuming to look at regularly. If a security incident had happened, it would have been a very long time before anyone at Wayne Enterprises noticed. Having centrally visible logs, alerts, and reports could save Wayne Enterprise from a malicious security event lingering too much or spreading quickly. They can contain or stop it by being more proactive with the logs. The successful completion of this goal relied on these four objectives, which were all completed successfully:

- 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. This objective was completed successfully. Gutz Sec met with Wayne Enterprises IT to evaluate the old way they were looking at logs. Gutz Sec then ran a Nmap scan on the network to take a technical inventory of servers and devices. Finally, all servers and devices found during the scan were analyzed to see which logs should go to the Splunk SIEM.
- Objective 1.b: Build the Splunk SIEM environment. The leading star in this project was the SIEM. The Splunk SIEM is a new system located in Wayne Enterprise to act as a log collection, alerting, reporting, and centrally manageable system. Splunk provides the staff with an efficient means to access and analyze

security logs. This objective was successfully completed. Gutz Sec built the servers needed for the SIEM, installed the software, and downloaded the needed add-ons.

- Objective 1.c: Configure the Splunk SIEM as a central repository for all security logs. Splunk provides an efficient means to view security log information. Splunk helps Wayne Enterprises IT view notable security events more effectively and centrally. This objective was successfully achieved. Gutz Sec fed all relevant security logs into the Splunk SIEM via forwarding agents. Gutz Sec created custom alerts, reports, and dashboards in the SIEM for Wayne Enterprises to utilize for security and event monitoring. Gutz Sec also created documentation and tested alerts and dashboards for this objective to make sure no documentation steps were missed, and all alerts were working.
- Objective 1.d: Handoff and training. Gutz Sec provided a handoff and training for Wayne Enterprises IT on the Splunk SIEM to finalize the project. This training and handoff helped the IT team utilize the SIEM and be informed of all its capabilities. This objective was successful. Gutz Sec provided documentation and training to Wayne Enterprises via a face-to-face meeting. Feedback was also discussed to see how Splunk is helping them and if they had any issues or concerns.

Project Timeline

Milestone or Deliverable	Planned Duration (Hours or Days)	Actual Duration (Hours or Days)	Actual Start Date	Actual End Date

Meet with Wayne Enterprises IT to see which logs they are looking at on a regular basis	4 hours	4 hours	11/8/2021	11/8/2021
Run a Nmap network scan to look for all technical inventory at Wayne Enterprises	2 hours	2 hours	11/8/2021	11/8/2021
Analyze relevant security logs on important systems found during the network scan	2 hours	2 hours	11/9/2021	11/9/2021
Build four Windows 2016 virtual servers	2 Hours	2 Hours	11/9/2021	11/9/2021
Install the Splunk software for the indexers, search head, and master	4 Hours	1 Day	11/9/2021	11/10/2021
Download Active Directory and SonicWall dashboard add-ons for Splunk	1 Hour	1 Hour	11/10/2021	11/102021
Feed relevant security logs into Splunk via forwarding agent on servers	4 Hours	4 Hours	11/10/2021	11/10/2021
Create custom alerts, reports, and dashboards	5 Hours	5 Hours	11/11/2021	11/11/2021
Create documentation	2 Hours	2 Hours	11/11/2021	11/11/2021
Test alerts and dashboards	1 Hour	1 Hour	11/11/2021	11/11/2021
Provide Splunk documentation to Wayne Enterprises IT team	1 Hour	1 Hour	11/12/2021	11/12/2021
Train Wayne Enterprises IT team on Splunk use and configuration	2 Days	2 Days	11/15/2021	11/16/2021

Meet with Wayne Enterprises IT to obtain feedback on any issues or improvement	2 Hours	2 Hours	11/19/2021	11/19/2021

There were no significant setbacks during the project. There was a minor delay of the Wayne Enterprises change board delaying the approval of the new Splunk environment due to an absence of an important member. The install timeframe was estimated to be four hours but ended up being a day due to the postponement. The setback did not impact the overall timeline of the project. Gutz Sec was able to fit in the install side-by-side to the subsequent deliverables. Everything else went smoothly due to utilizing a method like the ADDIE model and keeping to the timelines.

Unanticipated Requirements

During the SIEM for Wayne Enterprises project, not many unanticipated issues or scope creep. There was a minor inconvenience of the Wayne Enterprises change board delaying the approval of the new Splunk environment due to an absence of an important member. The setback was minor. The Wayne Enterprise change board approved the install the next day, and the installation of the Splunk SIEM was successful. The one-day delay did not hinder the project as Gutz Sec was able to work in the install side-by-side with other deliverables. No additional staff or scheduling was needed.

Conclusions

The Splunk SIEM increased the productivity for Wayne Enterprises as it brought visibility to logs by means of a central dashboard, automated alerts, and automated reports. The Wayne Enterprises IT department benefited 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 measured this. The IT Manager claimed that it used to take one person at least two hours to log into every device and examine the logs. The SIEM cut this time by about 85%. It currently takes 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 searching for the data.

For the long-term benefit, this SIEM solution improved the overall security posture for Wayne Enterprises. Before the Splunk SIEM, the IT staff at Wayne Enterprises rarely looked at logs due to the time-consuming process. Security incidents can be unnoticed due to not having someone constantly manning the logs. The SIEM brought 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 goes to the IT staff for them to contain or stop the incident altogether. All security logs now go to the Splunk SIEM, which brought visibility to 100%.

Project Deliverables

Gutz Sec created a couple of network diagrams for the project. These diagrams were handed over to Wayne Enterprises as part of the documentation for the Splunk SIEM. Appendix A shows what the original environment looked like before the Splunk SIEM. The diagram shows their original servers and network structure.

Appendix B shows a diagram of the new Wayne Enterprises environment along with an overview of how their Splunk SIEM is set up. This diagram shows the four new virtual servers built for the Splunk system. There is also a description of what each server does and how the existing server incorporates into Splunk.

Appendix C shows an overview of the new Splunk SIEM environment. There are descriptions of what each exists and its functions.

Appendix D shows a screenshot of the Splunk Dashboards. The first dashboard is from the Active Directory add-on. It provides a brief overview of notable Active Directory concerns, such as users getting locked out by inputting the incorrect password too many times. The second screenshot is of the SonicWall dashboard add-on. This dashboard can show the top destinations, sources, and any notable concerns.

Appendix E shows a screenshot of the alert setup. There can be alerts that generate on a schedule or in real-time. The alerts can be customized to alert on many different types of logs, such as Windows Security Events 4735, 4732, and 4733, which means someone has changed a security group, added a member, or removed a member. The second screenshot is for automated reports. The reports can be scheduled to send a summary via email of notable change or security concern for a specific timeframe, such as monthly domain admin changes for November.

References

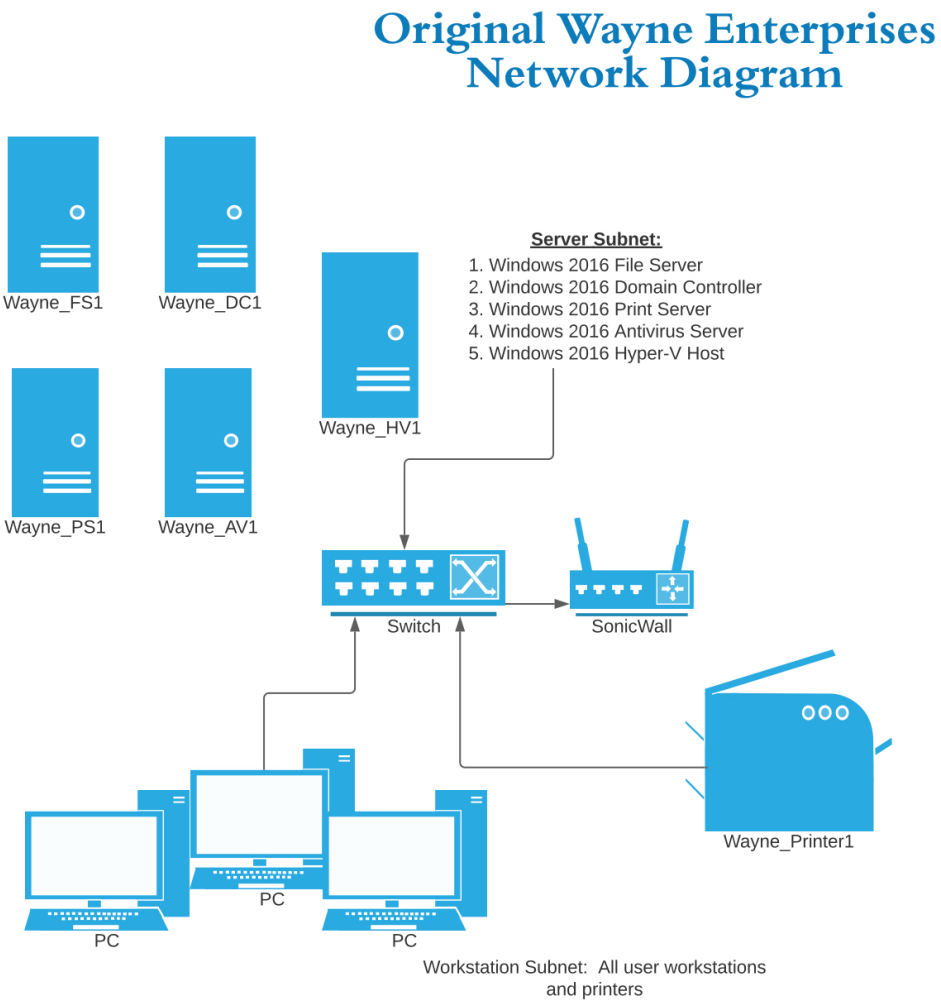
30 WAYS TO USE SPLUNK IN FINANCIAL SERVICES. (n.d.). Retrieved from https://convergingdata.com/wp-content/uploads/2019/08/30-ways-to-use-splunk-in-financial-services.pdf

CASE STUDY Splunk Use Cases • Security • IT operations. (n.d.). Retrieved from https://www.splunk.com/pdfs/customer-success-stories/splunk-at-a-manufactoring-company-2.pdf

Splunk Enables Security and Improves Business Performance for the Interac organization: An EMA ROI Study - Preview. (2021). Retrieved from Enterprisemanagement.com website: https://www.enterprisemanagement.com/research/asset-free.php/2266/pre/Splunk-Enables-Security-and-Improves-Business-Performance-for-the-Interac-organization:-An-EMA-ROI-Study-pre

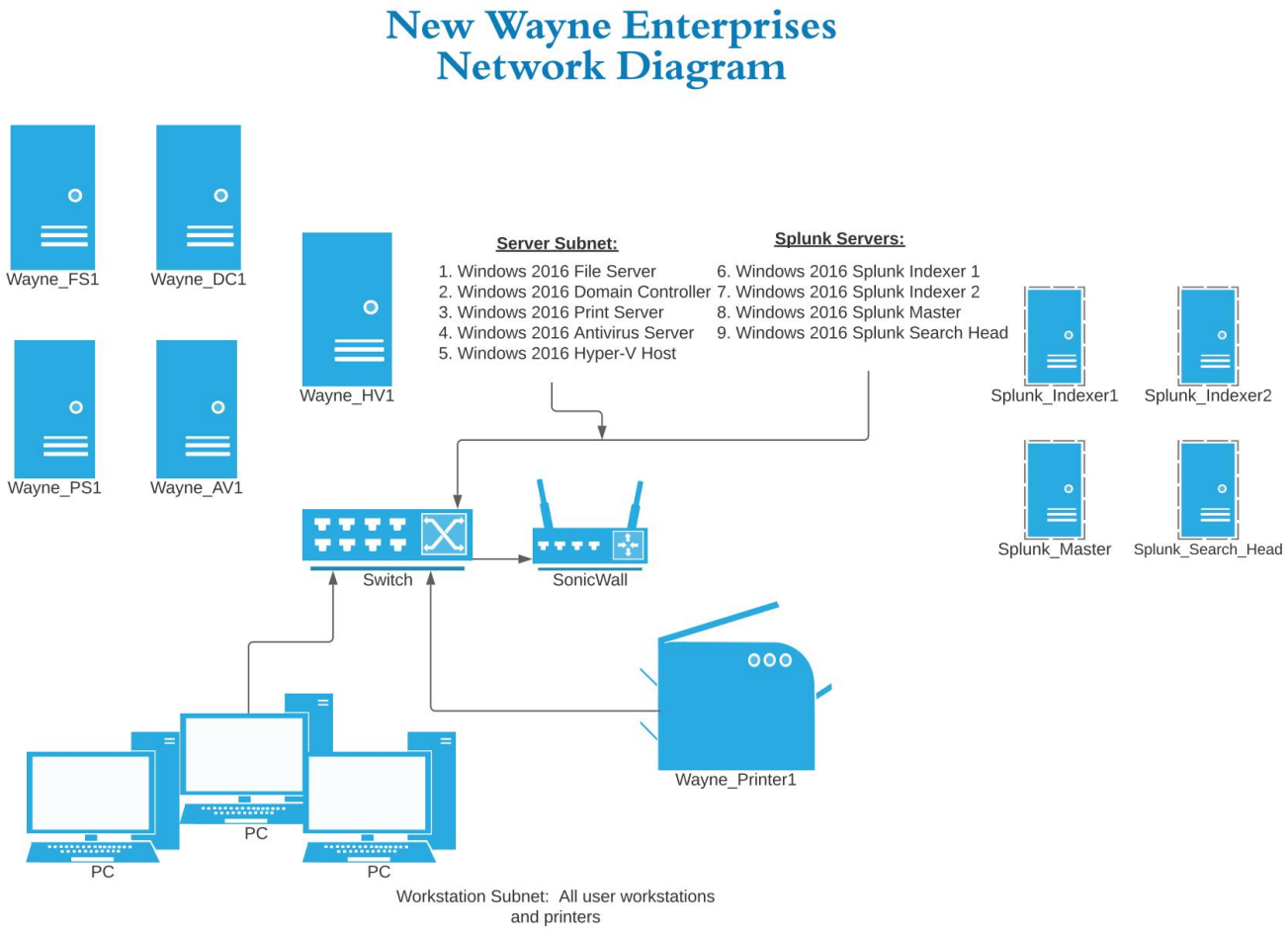
Appendix A

Original Wayne Enterprises Network Diagram



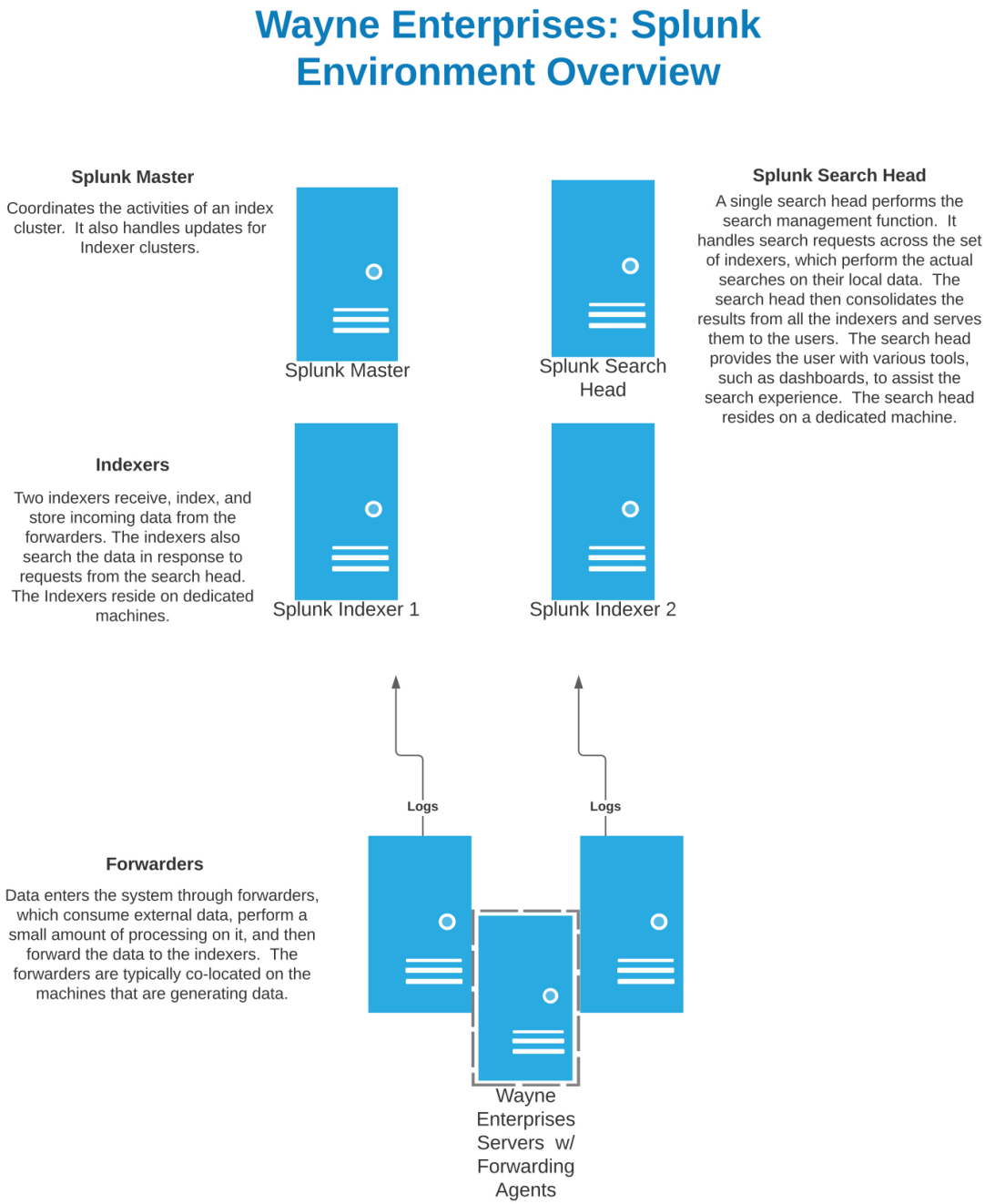
Appendix B

New Wayne Enterprises Network Diagram



Appendix C

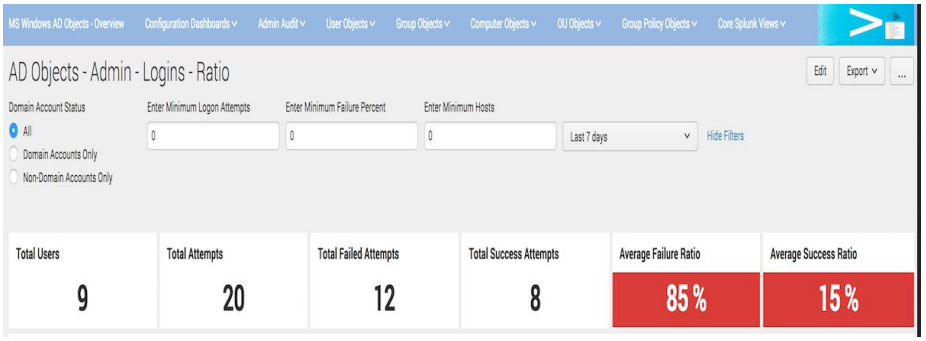
Splunk Environment Overview



Appendix D

Splunk SIEM Dashboards

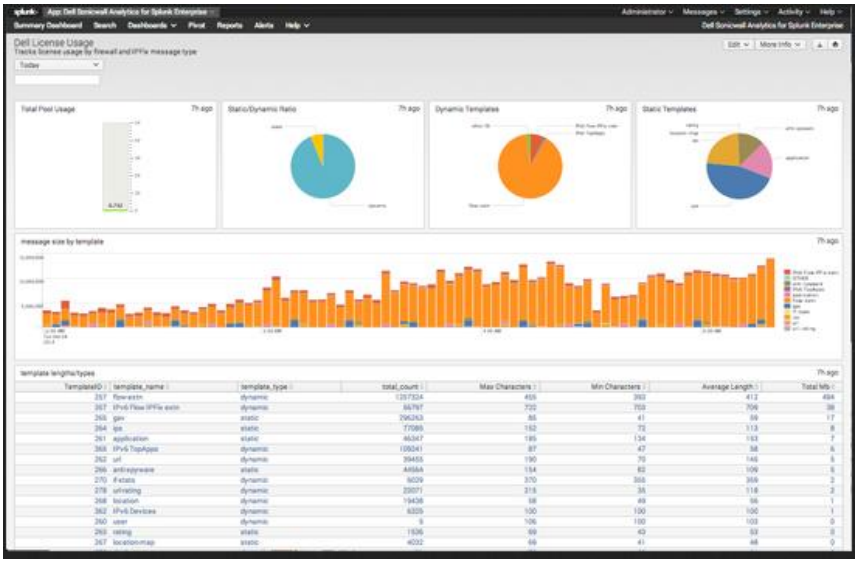
Active Directory Dashboard:



Logon - Sucess - Fail - Ratio Results

Logon_User	Domain_Account	Session_Host_Count	Total_Attempts	Fail_Percent	Success_Percent
bob	False	1	2	100.00% (2)	0.00% (0)
bob-joe	False	1	1	100.00% (1)	0.00% (0)
joe	False	1	1	100.00% (1)	0.00% (0)
joe-bob	False	1	1	100.00% (1)	0.00% (0)
just_guessing	False	1	1	100.00% (1)	0.00% (0)
just_guessing_a	False	1	1	100.00% (1)	0.00% (0)
just_guessing_b	False	1	1	100.00% (1)	0.00% (0)
zzz_win_lab	True	1	9	33.33% (3)	66.67% (6)
administrator	True	1	3	33.33% (1)	66.67% (2)

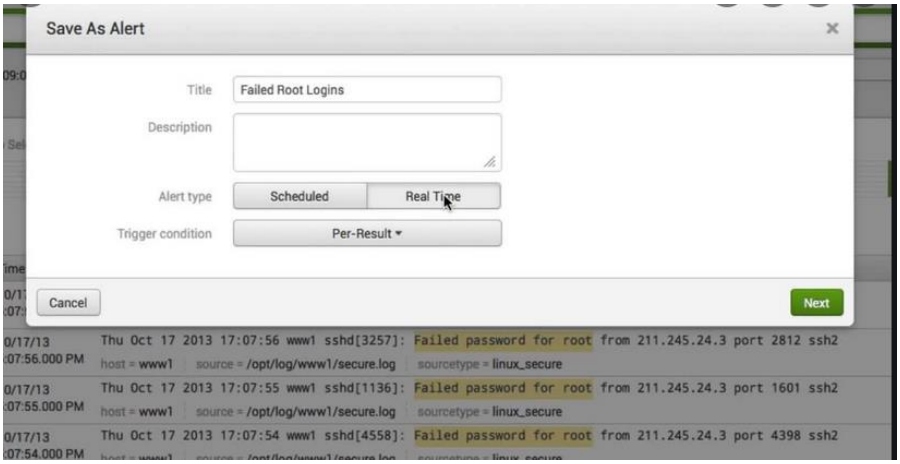
SonicWall Dashboard:



Appendix E

Splunk SIEM Alerts and Reports

Splunk alert for failed logins:



Splunk automated reports: