SEA- Shopigen Security Initiative

Natalie Hoernig

Wilmington University

SEC 410: Web and Data Security

Professor Ed Wiley

April 23, 2023

SEA- Shopigen Security Initiative

When setting up a security program, it is vital that you have an overall strategy to guide you. Having a strategy will ensure that your security program is complete and doesn’t have any gaps (Deo, 2023). For this project we are trying to merge two corporate enterprise environments. It is especially important that we have a plan to guide us and make sure that the merge goes seamlessly. My overall strategy consists of three steps.

The first step will be to evaluate the current security program and IT environments for both companies. I will start by looking at the most recent security risk assessment reports for the companies. This will help me to understand the processes and systems that are already in place. It will also help to figure out if there is anything that needs to be done to fill in gaps or if there are any missing safeguards (Deo, 2023). If either of the companies do not have a recent assessment, then I will conduct my own security risk assessment to get a baseline. Conducting an assessment will help to identify if there are any weaknesses or vulnerabilities that need to be addressed. In this first step, I will also conduct a network audit of the two companies to determine the devices and data.

The next step will be to develop a roadmap for the security program. Once I have the results from evaluating previous reports and conducting my own risk assessment, I can begin to develop recommendations and set up target dates to implement strategies and initiatives for the program. At this step, I will develop recommendations such as whether the company needs to add or modify personnel, procedures, processes, or any upgrades to technologies. I will also recommend due dates for implementing my recommendations.

The last step will be to identify and allocate resources. At this step, I will identify resources that are needed to support my plan. For example, staffing, software to implement, hardware to implement, or any other equipment that might be needed to support the initiative.

One of our first steps is to conduct a network audit. This will help us to identify devices and data. From the recommendation of Owokade (2018), I plan to perform the audit in three stages. The stages are planning, perform audit, and post-audit.

In the planning phase, I will be figuring out what tool to use for the audit, whether I have access to all the devices, and if I have support from all stakeholders (Owokade, 2018). I plan to try and sit down and have a nice talk with the IT team and Network Manager of the acquired company to see if I can get them to cooperate with me and give me more information or access to the network and devices. If that does not work, I will come up with a plan to work around it. For tools, I was looking at Solarwinds Network Configuration Manager and Open-AudIT. Both are great tools for getting an inventory of your network devices. Solarwinds is a popular tool that I have seen mentioned in many articles and Open-AudIT is an open-source option that can be used with both Windows and Linux based systems.

To conduct the audit, I will ultimately be going with the Solarwinds Network Configuration Manager. SNCM is better suited for large enterprises than Open-AudIT is (6 best network inventory tools & software 2022, 2022). It also automatically detects devices and provides other services in addition to the inventory scanner. According to Cooper (2023), when choosing a network inventory software, you want to look for something that automatically discovers assets and software that offers value for the money. I believe that Solarwinds Network Configuration Manager fits those two criteria. “6 best network inventory tools & software 2022” (2022) also highly recommends Solarwinds Network Configuration Manager because it integrates with your broader systems.

Once the audit has been completed, it is important to complete post-audit tasks such as creating a report and making recommendations. Owokade (2018) says, “You need to be able to make sense of all the information that you/your tool pulled up. You will probably need to present management with a special report that addresses the issues from a business angle, not from a technical point of view” (para.22). During the post-audit I can highlight any recommendations I have for next steps as well. This can include things like the need to replace old devices or any quick fixes that can immediately improve the security of the network, etc.

There were a few recommendations that I was looking into as far as ensuring a smooth integration of the corporate enterprise environments. The first recommendation is to either require that the acquired firm provide a security assessment or to immediately conduct a security assessment. If the target company provides you with an assessment, it should have ideally been done within the last nine months (Rosencrance, 2023). If conducting an assessment, it should be done immediately before the paperwork for the merger has even been signed. You want to have all stakeholders from both companies sit down and assess each companies’ network and infrastructure. Plans should be put into place to try and standardize any policies, procedures, or technology. According to Hattar (2023), “A new risk assessment needs to be completed given the changing circumstances, and an agreement put into place to create a new policy or adhere to an existing structure” (para.6).

Another recommendation is to make sure that cybersecurity and/or IT teams are involved early in the process. Rosencrance (2023) mentions that these teams are rarely involved prior to mergers and acquisitions. Having them involved from the start can ensure that weaknesses are identified early. This will ensure that unexpected security issues do not pop up and save you costs for trying to remediate them later.

The last recommendation is to come up with an integration solution that ensures data security consistency. The hardest IT task associated with mergers and acquisitions is integrating data. It’s important to have a plan in place to integrate data so that no data is lost, users can continue to have access to necessary information, and to ensure that both companies remain compliant (Hattar, 2023). There are a couple options for integrating data. The first one is called a forklift solution. This means that you are migrating one dataset to the other. Another option is to just maintain two separate datasets. Which one you choose, will depend on the individual situation. Hattar (2023) says, “Choosing what works for each situation requires an in-depth analysis of the overall cost, capabilities and effectiveness of each choice” (para.8).

For the security initiative, I have been tasked with choosing an intrusion detection or prevention system. There are two kinds of IDS/IPS which are Host-based (HIDS) and Network-based (NIDS). A HIDS examines events on a computer or endpoint on your network. A NIDS monitors traffic on your network as a whole. Cooper (2022) mentions that it would be good to have a combination of HIDS and NIDS. I like the idea of using an IPS since it can respond to threats as well as alerting you to them. I took these two things into consideration and chose a couple of IPS tools that are a combo of HIDS and NIDS.

The first tool is SolarWinds Security Even Manager (SEM). One thing that stood out to me about SEM is that it is designed for enterprise environments. This tool runs on Windows servers, but it can log messages from Unix, Linux, and Mac OS systems in addition to Windows PCs (Cooper, 2022). Generally, SEM is a HIDS, but you can deploy NIDS capabilities by using Snort as a packet sniffer and sending the captured data to SEM for analysis (Cooper, 2022). This tool is very feature dense. For example, it has file integrity monitoring, compliance management and reporting, forensic analysis functions, a firewall log analyzer, and more.

The second tool I looked at was Sagan. Sagan is a free and open-source log analysis tool that acts as a HIDS. It installs on Unix, Linux, and Mac OS, but it can accept log data from Windows systems. Like SolarWinds SEM, this tool can be used as a NIDS by gathering data from Snort. Samson Jr. (2022) mentions that Sagan can integrate with firewalls, and it can block IP addresses from any external attackers that it has detected. A unique feature of Sagan is that it has an IP locator feature that can show you the geographical location or information of an IP address.

Out of the two tools, I would choose SolarWinds Security Event Manager. First, it is designed with enterprise environments in mind. I like the fact that it can be installed on WindowsSolar. If there are devices with another operating system, we can still gather log data from them. SEM has a lot of features built into it which means you most likely will not need any supplementary tools. SEM also comes with a ton of preconfigured detection templates, alerts, and rules. I think SEM will be easier to work with and quicker to set up than Sagan. Cooper (2022) mentions that a pro of SEM is that threat response rules are easy to build. According to Samson Jr. (2022), SolarWinds has a user-friendly interface, but Sagan has a steep learning curve and can be hard to install and configure.

Next, I have been tasked with choosing a security auditing tool for the company to use. Security auditing tools can help you monitor for network threats, can help you work through issues, and expose vulnerabilities before they become a problem (Keary, 2023). Some of the best security auditing tools will have a combination of features such as vulnerability scanning, port scanning, patch management, and more. There are two tools that I considered.

The first option is the Solarwinds Network Configuration Manager. I have already chosen this same tool as the best option for getting an inventory of the network devices. I was thinking that it will save the company on costs if we can use the same tool for more than one thing. The key feature of this tool is its configuration management. With this tool, you can store images that contain recommended configuration settings for each device on your network. According to Keary (2023), “The system repeatedly scans each device and compares its configuration with the stored image. If it finds a difference, the SolarWinds tool applies the stored image, wiping out the unauthorized changes” (para.13). Solarwinds Network Configuration Manager also has a network vulnerability detection feature. This allows you to scan your network devices’ firmware for reported CVEs.

The other tool I was looking at is called Acunetix. This is a web application security scanner, but it can also be used as a network vulnerability scanner by integrating it with OpenVAS. Acunetix is capable of scanning for over 4,500 web application vulnerabilities (What you need to know about acunetix, 2019). When integrated with OpenVas, it can scan for over 50,000 network vulnerabilities (Keary, 2023). Like Solarwinds, Acunetix has a configuration management feature that can auto detect any misconfigurations in your network devices. Acunetix also has a reporting feature that can generate a wide range of reports. For example, you can generate reports related to PCI DSS, HIPAA, or OWASP Top 10 (What you need to know about acunetix, 2019).

After much consideration, I would choose Acunetix as the best option for a security auditing tool. While using Solarwinds Network Configuration Manager might save money, I think that Acunetix offers more features and bang for your buck. I think it’s the better choice since it combines both network vulnerability scanning and web application scanning. I’ve read that it’s a great option if you are looking for a tool that is easy to navigate and one that can integrate with many other tools (Keary, 2023). It’s also known to report very few false positives (What you need to know about acunetix, 2019).

As part of the initiative, I need to also choose a network firewall. There are many good options out there. I was looking at firewalls that were considered NextGen and the best for large enterprises. There were two firewalls that I was trying to decide between. They are Barracuda CloudGen and Palo Alto VM-Series.

The Barracuda CloudGen firewall was designed for hybrid environments that have on-premises, virtual, and cloud infrastructure. It has multiple detection layers including threat signatures and static code analysis (Ingalls, 2023). Some of Barracuda’s key features according to Ingalls (2023) are that it has advanced threat protection, stateful deep packet inspection, and high availability with load balancing/uplink options. Some other features of Barracuda are that it has SSL interception, URL filtering, intrusion detection/prevention capabilities, and DNS sinkholing technology (Lightfoot, 2023). Many users say that it has an intuitive and user-friendly interface, but they find that it can be difficult and time consuming to configure.

Palo Alto VM-Series is another good option for hybrid environments and comes with deployment options for on-premises, hybrid, and cloud. Like Barracuda, this firewall also features deep packet inspection, IPS, URL filtering, and data loss prevention (Lightfoot, 2023). Palo Alto VM-Series is a good option if you need sandboxing capabilities. This firewall also has the capability of blocking lateral threat movements. RobCheney1 (2021) says, “Today’s cyberthreats often compromise an individual user, and then move laterally across your network. Palo Alto’s segmentation and allow listing policies let you control applications communicating across different subnets” (para. 9).

Out of the two firewalls, I think I would go with the Palo Alto VM-Series. It has a lot of good reviews. I’ve read that it is easy to install, and initial configuration can be easy as well. One thing that makes this firewall stand out above Barracuda is that everything can be managed from the same console. This is not the case with Barracuda. Ingalls (2023) says, “Barracuda uses two different management consoles for cloud and for physical and virtual firewalls, which could make extra work for organizations that use Barracuda for both cloud and on-premises environments” (para.34).

When designing a security initiative, there are many factors that need to be considered. These include coming up with a strategy, considering what rules should be in the policies, and deciding on the best options for tools. First you need to make sure that you come up with an overall strategy. This will help you stay on track and ensure that there are not any gaps. The strategy should include an assessment of the current security program/policies and a network audit to determine what devices are on your network and the data that needs to be protected. Once you’ve assessed the current security state, you should sit down and come up with a roadmap that includes recommendations for strengthening the security of the company and due dates for implementing recommendations. You also want to determine what resources will need to be allocated to support the security initiative.

Next, you want to look over the current security policies or create a security policy if the company does not already have one. You want to determine if there is anything in the policy that is not necessary or if there is anything you should add. If you’re creating a policy from scratch, you can use templates such as the AUP from SANS and revise them to meet your needs. A security policy should include overall restrictions such as unauthorized electronic communication, installing malicious software, and disclosing confidential information (Martins, 2023). It should also have password policies, software installation rules, personal device/remote work policies, and guidelines for social media use (Martins, 2023).

There are various tools that might need to be used or implemented. When conducting a network audit, you want to choose a tool that can automatically scan for all devices on your network, and it should offer value for the money. When choosing an IDS/IPS you want to look for one that is user-friendly and offers a lot of features. It’s also recommended to choose one that has both HIDS and NIDS capabilities. It’s recommended to choose security auditing tools that have a combination of features such as network vulnerability scanning, web application scanning, port scanning, patch management, sandboxing, reporting, etc. For firewalls, it’s a good option to choose one that is NextGen. These offer the same options as traditional firewalls, but they can go deeper such as showing where an attack came from or what the attacker is trying to access. It’s also a good idea to purchase a firewall that is designed for hybrid environments as this will allow for expansion.

Below I have a diagram of the general set up I would have for the network. This diagram shows the firewall placed between the servers and the internet. This can help to block out any unwanted incoming traffic. I believe the IPS that I chose, SolarWinds Security Event Manager, can be installed on web servers or domain controllers. I like the idea of the network having a mixture of peer-to-peer and domain model. Peer to peer allows for easy sharing of resources and allows for scalability. This would be good for departments that do not deal with sensitive data. The domain model is good if you need to protect sensitive data. It’s a more secure model since you can have user authentication and access control. The web and network vulnerability scanning tool I chose, Acunetix, can be installed on individual PCs, virtual machines, or you can purchase their Premium Online version.

Diagram

Description automatically generated

# 

**References**

*6 best network inventory tools & software 2022*. DNSstuff. (2022, January 14). Retrieved April 19, 2023, from https://www.dnsstuff.com/network-inventory-tools

Cooper, S. (2022, December 13). *10 top network intrusion detection tools for 2018*. Comparitech. Retrieved April 19, 2023, from https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

Cooper, S. (2023, March 1). *5 best network inventory tools*. Comparitech. Retrieved April 19, 2023, from https://www.comparitech.com/net-admin/network-inventory-tools/

Deo, S. (2023, March 23). *What is guiding your security program?* 24by7security. Retrieved April 19, 2023, from https://blog.24by7security.com/what-is-guiding-your-security-program

Hattar, M. (2023, January 22). *Managing security and network implications of mergers and acquisitions*. SecurityWeek. Retrieved April 19, 2023, from https://www.securityweek.com/managing-security-and-network-implications-mergers-and-acquisitions/

Ingalls, S. (2023, April 13). *9 best next-generation firewall (NGFW) solutions for 2023*. eSecurityPlanet. Retrieved April 21, 2023, from https://www.esecurityplanet.com/products/top-ngfw/

Keary, T. (2023, February 20). *16 Best Network Security Auditing Tools for 2023 (paid & free)*. Comparitech. Retrieved April 20, 2023, from https://www.comparitech.com/net-admin/network-security-auditing-tools/

Lightfoot, L. (2023, January 17). *The Top 11 Network Firewall Solutions*. Expert Insights. Retrieved April 21, 2023, from https://expertinsights.com/insights/the-top-11-network-firewalls/

Martins, A. (2023, February 21). *How to create an acceptable use policy*. business.com. Retrieved April 23, 2023, from https://www.business.com/articles/acceptable-use-policy/

Owokade, A. (2018, January 27). *Network audit: How to perform in a real network (with bonus template)*. RouterFreak. Retrieved April 19, 2023, from https://www.routerfreak.com/how-to-perform-network-audit/

RobCheney1. (2021, June 24). *Palo Alto VM Series Virtual firewall review - corporate armor*. Retrieved April 22, 2023, from https://www.corporatearmor.com/uncategorized/palo-alto-vm-series-virtual-firewall-review/

Rosencrance, L. (2023, April 3). *5 strategies to manage cybersecurity risks in mergers and acquisitions*. CSO Online. Retrieved April 19, 2023, from https://www.csoonline.com/article/3692433/5-strategies-to-manage-cybersecurity-risks-in-mergers-and-acquisitions.html

Samson Jr, R. (2022, August 5). *Top 10 intrusion detection and Prevention Systems*. ClearNetwork, Inc. Retrieved April 19, 2023, from https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/

*What you need to know about acunetix?* C-YBER. (2019, December 3). Retrieved April 20, 2023, from https://www.c-yber.com/what-you-need-to-know-about-acunetix/