SIEM CAPSTONE

SIEM Architecture in a Healthcare Environment

Abstract

Today more than ever, hospitals need to have a robust security system in place. A vital part of that system should be a well configured Security Information and Event Monitor (SIEM).

Max Kramer

Max.kramer0324@gmail.com

CONTENTS

HARDWARE

-5 user machines running Windows 10

- 5 Linux Servers mail, web, SIEM, compliance data, and proxy

- Router

- Switch

SOFTWARE

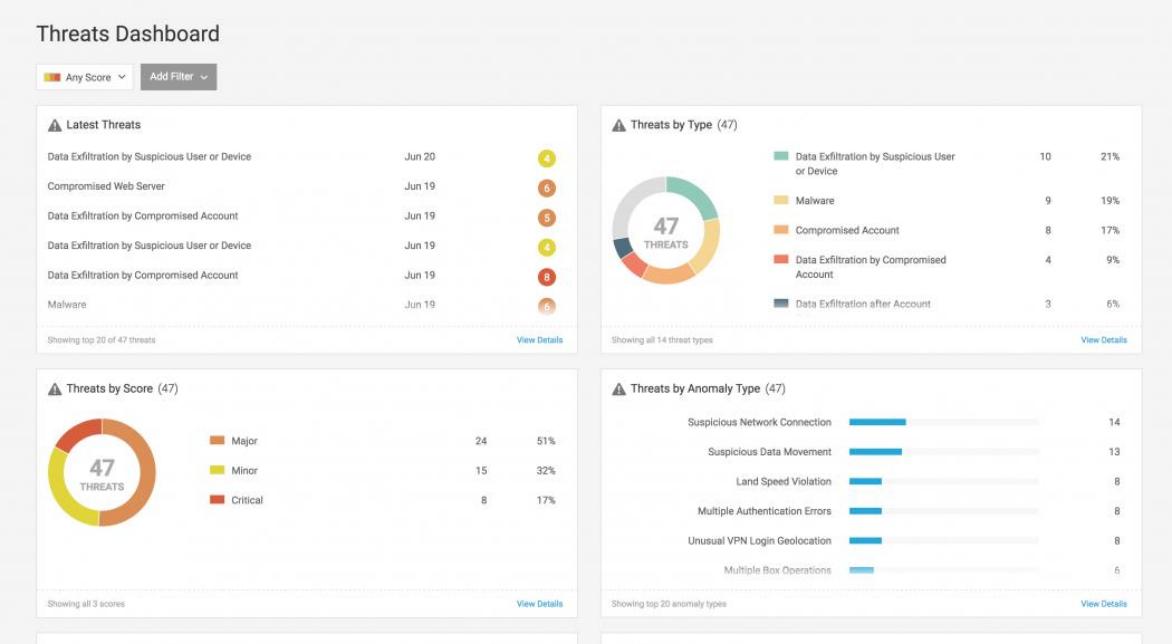
For the SIEM software, I would recommend using Splunk Enterprise. Although it can be costly, Splunk is a reliable SIEM that performs well on an enterprise level. Although it is obviously more expensive than an open-source SIEM, it is much more powerful and does not have the scalability issues that can often be encountered in open-source programs available offline. Another benefit to Splunk is that they have certifications available to ensure that administrators using Splunk are knowledgeable.

DASHBOARDS AND ALERTS

For Splunk, or any SIEM to work properly, data must be forwarded to the SIEM. This data is mostly made up of logs sent to it from other computers on the network that it is monitoring. The forwarders used by this organization are:

- Microsoft Azure for Splunk
- Office 365 Reporting for Splunk
- Splunk App for PCI Compliance- Splunk Enterprise Security
- Splunk Add-on for Unix and Linux
- Splunk App for Unix and Linux

With these in place, I would recommend configuring dashboards and alerts to better utilize Splunk and all of its capabilities. An example of a dashboard that is pictured below is the Splunk Threats Dashboard, an example configured by Splunk. While this isn't a comprehensive list, it provides an example to build off of.



Source

Another vital tool that a Splunk user should configure is the alerts system. This allows the administrator on a Splunk instance to customize the types of events that trigger an alert. A very important aspect of this is to consider that too many alerts can lead to alarm fatigue. This is well documented in both the healthcare community as well as the cyber security community. Alarm fatigue happens when an analyst (or nurse), hears so many alarms, all the time, and it leads to important alarms being tuned out with all of the nonessential white noise in the background. Since a SIEM acts as essentially the same thing as a vitals' monitor for a computer, it's important to configure it with the same goals in mind.

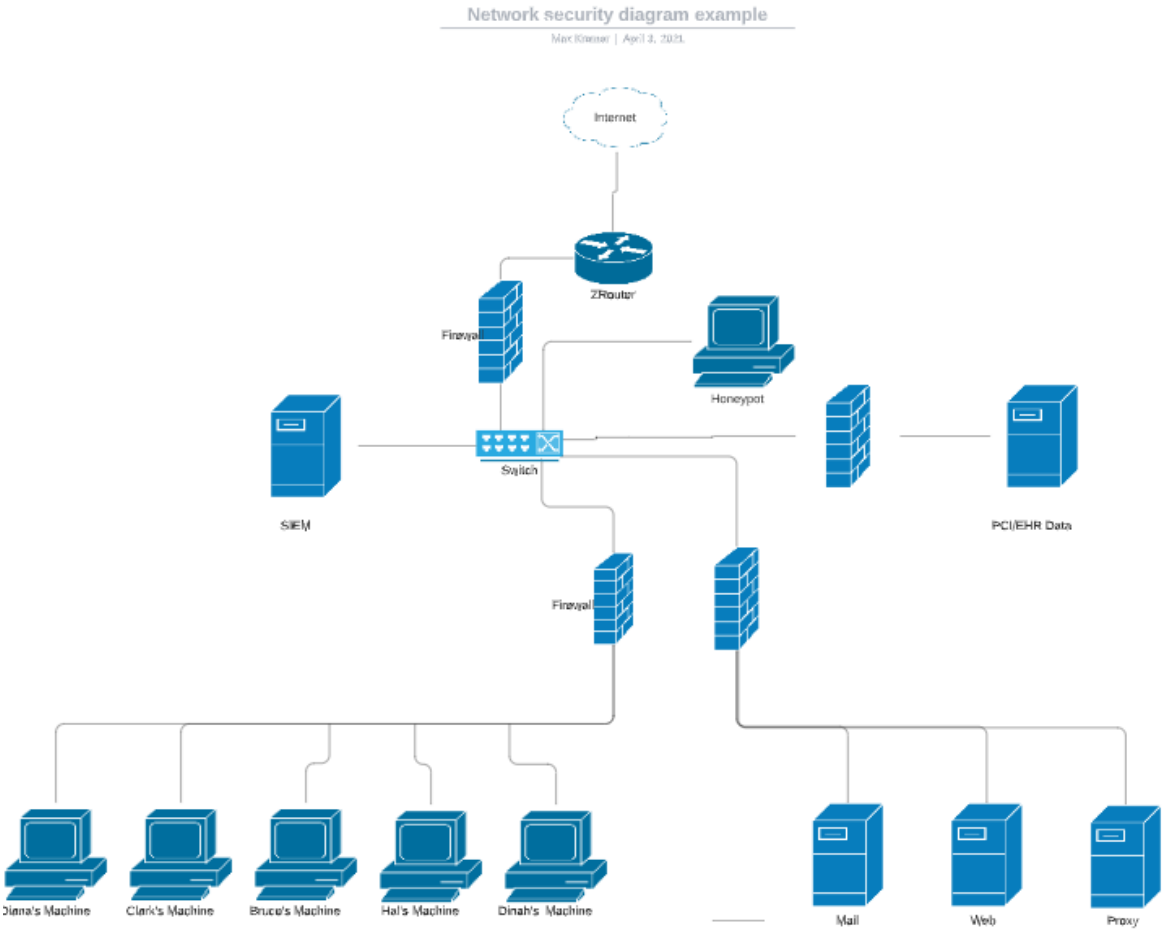
Keeping that in mind, the alerts that need to be configured are any unusual events, for example, an analyst needs to be aware that someone is pinging the network looking for vulnerabilities, which is something a SIEM can help with. Configuring an alert to send an email to an analyst if multiple machines on your network are pinged within a short amount of time would be an example of one important alert to configure.

THREAT ASSESSMENT

The threats faced by the healthcare system grow daily. With news of ransomware on the rise, even during a global pandemic, that targets hospitals, we must be ready to face threats of any kind to our network. With threat actors endangering the lives and privacy of your patients, security must be treated as a priority to keeping patients safe and their information protected. There are standards that must be adhered to with HIPAA compliance in healthcare systems of course, but the fear of an audit should not be the driving force behind a robust security posture of

an organization so long as there are people out there that would endanger the lives of your patients for money.

With that in mind, the network map below addresses security concerns while staying on a limited budget. The SIEM itself does a bulk of the heavy lifting for analyzing the crucial data for your security team to review. By properly configuring it, it can be the most powerful tool on your network. The logs that the SIEM is being told to monitor will be crucial to preventing any unauthorized changes, devices, or users from being on your network without your analysts knowing about it.



LOG DATA

The following log data will be forwarded to the SIEM by the application installed on machines in the network. If a SIEM has no data to draw from, the server is about as useful as a several thousand dollar paperweight. The following logs will be forwarded to the SIEM:

WINDOWS LOGS

Windows logs will be collected by the SIEM and forwarded using the applications mentioned above. Since we have instances of Windows present on our system, collecting them is vital to the health of our network.

- System
- Security
- Application
- Setup

PCI LOGS

PCI compliance covers the security of credit card transactions and ensures that any enterprise using credit cards properly handles, logs, and stores the data obtained from said transactions. The compliance regulations essentially boil down to "who, what, where, when," for the data that needs to be collected. The types of logs that this could include are the following:

- Database transaction logs
- Access logs
- Network activity logs

LINUX LOGS

The following Linux logs should be collected since our servers run on Linux and we need to know what is happening on them as much as we need to know what is happening on our users' desktops.

- /var/log/messages
- /var/log/auth.log
- /var/log/secure
- /var/log/boot.log
- /var/log/dmesg
- /var/log/kern.log
- /var/log/faillog
- /var/log/cron
- /var/log/yum.log
- /var/log/mailllog
- /var/log/httpd/
- /var/log/mysql.log

COMPLIANCE

This SIEM architecture and network security have been configured to be compliant with HIPAA, PCI, and GDPR regulations, saving your enterprise from an

expensive fine from any of the agencies in charge of these regulations. More importantly, however, by collecting and storing data in compliance with these regulations, your enterprise will have a much more robust security posture.

REFERENCES

Adding a Deployment Server / Forwarder Management to a new or existing Splunk Cloud (or Splunk Enterprise) Deployment. (2016, August 31). Retrieved from https://www.splunk.com/en_us/blog/platform/adding-a-deployment-server-forwarder-management-to-a-new-or-existing-splunk-cloud-or-splunk-enterprise-deployment.html

Dasgupta, S., & 22, M. (2020, May 23). Integrating a SIEM solution in a large enterprise with disparate global centers. Retrieved from https://www.helpnetsecurity.com/2020/05/22/siem-solution/

Integrated Data Analytics & IT Security Solutions for Healthcare. (n.d.). Retrieved from https://www.splunk.com/en_us/solutions/industries/healthcare.html

ManageEngine. (n.d.). Payment Card Industry – Data Security Standards (PCI-DSS) Compliance Reports. Retrieved from https://www.manageengine.com/products/eventlog/help/compliance-reports/eventlog-analyzer-pci-dss-compliance-reports.html

Official 2021 HIPAA Compliance Checklist. (2021, March 05). Retrieved from https://www.hipaajournal.com/hipaa-compliance-checklist/

What Are HIPAA Compliant System Logs? (n.d.). Retrieved from https://www.securitymetrics.com/blog/what-are-hipaa-compliant-system-logs

White, J. (2019, January 29). Security Logging and Monitoring (PCI DSS Requirement 10): Why all the Fuss? Retrieved from https://www.pcicomplianceguide.org/security-logging-and-monitoring-pci-dss-requirement-10-why-all-the-fuss/