Network Security Monitoring for Cyber Situational Awareness

A Thesis
Presented in Partial Fulfillment of the Requirements for the
Degree of Master of Science
with a
Major in Computer Science
in the
College of Graduate Studies
University of Idaho
by
Raymon N. Hardy

Major Professor: Michael Haney, Ph.D.
Committee Members: Constantinos Kolias, Ph.D.; Robert Hiromoto, Ph.D.
Department Administrator: Terence Soule, Ph.D.

August 2020

Authorization to Submit Thesis

This thesis of Raymon Hardy, submitted for the degree of Master of Science with a Major in Computer Science and titled "Network Security Monitoring for Cyber Situational Awareness," has been reviewed in final form. Permission, as indicated by the signatures and dates below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____ Date: _____
Michael Haney, Ph.D.

Committee Members: _____ Date: _____
Constantinos Kolias, Ph.D.

_____ Date: _____
Robert Hiromoto, Ph.D.

Department Administrator: _____ Date: _____
Terence Soule, Ph.D.

Abstract

Modern organization networks are diverse and complex, with many different zones and security levels based on systems' functions, missions, or business purposes. This makes maintaining situational awareness of the environment both more critical and more difficult to perform. Cyber situational awareness tools are widely available making it easy to see what is happening in the network and on managed devices. At the University of Idaho, on the Idaho Falls campus, a cybersecurity research lab named the Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) is available for research purposes. The RADICL lab is set up specifically to support cybersecurity research and training for students and the community. To make sure administrators are completely aware of what is happening in this cybersecurity lab, cyber situational awareness tools have been implemented to monitor hardware, software and network packets. When suspicious activity or malware is detected, RADICL administrators will be alerted. The purpose of this thesis is to explain in detail what cyber situational awareness tools are and provide a use case of how cyber situational tools are implemented in the RADICL lab, thus providing a possible solution for small to large businesses and similar research labs.

Acknowledgement

I would like to thank everyone that helped me achieve this academic accomplishment. First, I would like to thank my parents for their love and understanding to help me achieve this degree and thesis. Thank you for all you have done for me. Secondly, like to thank my professors and academic mentors to help me understand computer science information. Specifically, would like to thank my academic professor, Michael Haney, in all the help he did to make this goal happen. As well as my committee members that provided patient advice and guidance throughout the research process. Thirdly, would like to thank all my fellow graduate students to help me understand and write this thesis. The time and devotion that was given to the RADICL lab had helped me achieve my goals. Two graduate students in particular, Jason Allen and Michael Madsen, that were in the RADICL helping to contribute to the RADICL lab and its further development. Lastly, would like to thank the University of Idaho writing center and personal writing advisor for reviewing and revising my paper to correct errors throughout my drafts. Thank you for all your support to achieve this academic goal.

Table of Contents

List of Figures

Chapter 1: Introduction

In today's world, the Internet is a necessity for all organizations. Some businesses have hundreds or even hundreds of thousands of computers connected to the Internet at one time. These hundreds of thousands of computers could be general workstations, servers, network devices, or embedded systems in cyber-physical devices. Administrators in the organization have the responsibility to make sure each of these computers is safe and operating in a correct and secure manner. It is important for businesses to know if any computer on their network has been attacked, and if so, take the appropriate steps needed to remove malicious software. Monitoring and alerting of any suspicious activity are highly valuable to any organization. Being cyber situationally aware of every aspect in an organization's computing environment is extremely important to be resilient to any attacks. In this thesis, a detailed description of cyber situational awareness is given and the different types of cyber situational tools available are explained. Additionally, a use case of cyber situational awareness implemented in a cybersecurity research lab environment at the University of Idaho is provided.

Chapter 2: Cyber Situational Awareness

'Cyber' is a term which refers to all things made possible by the use of computerized devices and interconnected networks. But because of the dynamic and interconnected nature of cyber, computers and networks are not completely secure, opening a whole new aspect of security vulnerabilities to organizations and businesses. There has been an emphasis on security in the Information Technology field for many years, but because of the explosive growth of cyber technology and the growing dependence on the Internet, cybersecurity has become an existential requirement for organizations. Because there are so many vulnerabilities in all types of computing devices, and there are increasing numbers of malicious actors out there, IT administrators need to continuously be assured that none of their networks are exploited or crashed. Cyber situational awareness is the ability to be completely aware of what is operating in one's environment and detecting any suspicious activity. In *Computers & Security* [1], the authors describe cyber situational awareness as "any kind of suspicious/interesting activity taking place in cyberspace, where cyberspace includes any kind of computer network-related activity." In practice, cyber situational awareness is required for cyber management.

An organization needs to know exactly which devices are connected to its network and what they are communicating at all times. IT administrators and security analysts need to be aware of threats and vulnerabilities in their environment and identify, process, and comprehend these vulnerabilities in real time. Organizations can then gauge both their current and future risks and potential mitigations. With so many devices connected to a network and so much data being generated, it is a challenge for cybersecurity experts to see

the whole picture. Cybersecurity professionals need to monitor all data of both network traffic and device activity in real time.

2.1: Complex Modern Networks

For IT managers and security specialists, it is difficult to keep track of what is going on in their organizations. A large enterprise environment can have many devices and software connected and transmitting data at very high rates. Devices such as servers, workstations, switches, routers, wireless access points, firewalls, storage systems are just a few. Now that mobile devices, the Internet of Things, and cloud storage are also being connected to the network, there adds another twist for IT and cybersecurity specialists to worry about. There are a variety of tools to see analysis of enterprise data flows [2] but these solutions still do not offer the capability to fully monitor the state of all devices. For hackers and malicious users, this weakness in monitoring what is on the network can be seen as an opportunity to gain entrance into the enterprise. The wider the range of possible targets, the easier it is to find undetected vulnerabilities. Now with so many devices connected the network, that means more noise and traffic on the network and the less likely they are to be caught. Many organizations are now designing and developing their systems with cyber situational awareness in mind from the beginning [3].

There are many methods to eliminate this risk of potential attacks to an organization. One important step, and a step that is described in this thesis, is for organizations to be cyber situationally aware. This means knowing what devices the organization has, knowing exactly what is happening in real time on the organization's networks, and being ready to respond to

incidents as they occur. For organizations to really be “secure” they need to have the capability of cyber situational awareness.

2.2: Importance of Cyber Situational Awareness

The importance of cyber situational awareness is to have organizations correlate the current vulnerabilities of systems to the inventory of systems they have in order to aid in finding solutions. In order to be resilient to attacks, companies need to find the possible vulnerabilities in their environment. All organizations are vulnerable to malicious attacks that could potentially cost the company money and damage their reputation. When known vulnerabilities are found, there are already known cybersecurity methods to help organizations mitigate them to improve cyber resiliency.

One important method is knowing what IT assets, OSes and software an organization currently has and whether those assets are up to date. These sorts of vulnerabilities apply to both new and old devices. A concern for cybersecurity experts is IT systems that have devices connected to the network that are using legacy software or are not yet hardened enough from the manufacturer. Modern devices include not only computers but IoT and operations technology (OT) devices, which include a risk of vulnerability because of the lack of robustness. Devices running legacy software include a risk of vulnerability because of known exploits of vulnerabilities for which the vendor no longer provides patches. Experts report that companies operating with legacy code and software are exposing themselves by 36 percent increase [4]. Having cyber situational awareness tools in place can aid in finding what devices are not up to date.

Another method of mitigating vulnerabilities of cyber-attacks is by reducing or eliminating human error. Many times, humans are the weakest link for an organization's security. Things like workers looking at malicious websites, workers being scammed to download something they do not need to, and workers being manipulated by social engineering emails are just a few of the many ways malicious attackers may try to get into the organization [5]. IT and security experts know that this is our weakest link, but for an organization to complete its work there needs to be a human factor in the systems. With training and cyber situational software in place, cybersecurity experts can be alerted when suspicious activity occurs.

Cybersecurity experts' role is to make sure nothing malicious gets into the system, and if it does to recognize it quickly enough to stop any damage to the system. Cyber situational awareness has become important to many organizations to establish internal threat intelligence by sharing channels that alert everyone in the organization about cyber risks and attacks. This helps not only IT but also incident response teams when they try to understand what has happened during the cyber-attack.

2.3: Design and Implementation of Cyber Situational Awareness

In the academic sense, situational awareness is defined as knowing what is going on around you [6]. Situational awareness is broken down into three dimensions: perception, comprehension, and projection. Perception means to see the whole picture of the situation. Comprehension entails combining, interpreting, storing and retaining information. Lastly, Projection is to forecast future situation events and dynamics. These dimensions apply to a wide variety of systems and areas of research. Endsley describes this as "the perception of

the elements in the environment within volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [6]. This ideology of situational awareness applies to information technology as well. The idea behind the dimensions mentioned above is to eliminate human error and strengthen first line defense.

Out of the box computers are usually not hacked or looking to do nefarious things. They are usually defined a task to do and could potentially run fairly reliably without any interference. Cybersecurity professionals and IT administrators are trained to secure their devices and networks against cyber-attacks [7]. The Infosec community provides a variety of designs and tools to implement in technology environments. The purpose of these designs and tools are to be aware of what inventory the system currently has and what actions are being performed by humans. If implemented correctly, the operator can see the whole picture of the environment and can also see what is going wrong with individual devices and possible attacks. These tools consist of different aspects including threat detection and management, network management, incident reporting, threat intelligence sharing, risk monitoring, and defense management. It is important for organizations to implement these tools into their environment to make sure the right person sees these events at the right time. These tools and scenarios can be scaled for larger and smaller businesses and can be implemented in a cost-effective manner [8].

Training is also a key aspect in cyber situational awareness. If computers are constantly reporting what status they currently have and whether they are producing any abnormal activity, so too do employees need to report any suspicious or unusual activities that they observe. Situational awareness has to be bi-directional in nature. Where an employee will report unusual activity to a security operator, so too does a security operator

need to report any suspicious activity to employees. Proper training is also important in order for employees to know where to report incidents. This is called incident response and is key to breaking a cyber kill chain. All employees need to be cognizant that their current devices and network can play a vital role in maintaining the overall cyber health of the organization. Research and development have gone into which cyber situational awareness training is most cost effective for organizations to implement [9].

Measuring situational awareness is also a key feature for an organization to become more cyber resilient. Since computer system environments can vary greatly, the situational awareness measurement will need to be specific to each case. The measurement and metrics analysis will need to be in place in order to fulfill the three dimensions of cyber situational awareness. If the operators of that system can piece together the vast array of available information to form a coherent operational picture, the concept of situational awareness measurement can apply to a wide variety of areas, including technology. The measurement of situational awareness can be evaluated in three areas. Those include the design evaluation, evaluation of training techniques, and investing the situational awareness construct. A technology system could be evaluated in the same way to determine if that system is situationally aware.

2.4: Future of Cyber Situational Awareness in an IoT World

More and more devices are becoming connected to the Internet. Many household items such as refrigerators, dishwashers, and lamps now have the capability and functionality to connect to the Internet to make automation and remote connection possible. Not only do we see this with consumer products, but we also see it in the commercial and industrial area

where many of the sensors and controllers are now being connected as well. This interconnection between devices through the Internet is called the Internet of Things (IoT). It is projected that in 2020 there are 25 billion devices connected to the Internet [10]. The IoT is becoming a greater and greater concern for cybersecurity experts because of the devices' lack of intelligence to fend off and alert about an attacker. Of course, IoT devices can be a concern but also a benefit for cyber situational awareness.

One of the functionalities of these devices is to collect data and report data. This could be a concern for cyber situational awareness because of the large amount of storage that will be needed to collect data about each device. An organization's storage will need to increase to take in account of these devices. Each node will also have large amounts of data traffic going through it, so companies will need to make sure their network infrastructure will be able to handle this increase. Cyber situational awareness analytics and real time applications to see what is happening with each device will also need to perform at the same speed as the device. They will need to ensure that the data is being recorded in a trustworthy manner. Analytics will need to be performed on these nodes to make sure that the data is trustworthy. Many changes to current organizations' network-monitoring will need to be upgraded and adapted for these IoT devices.

With all these negative aspects of IoT devices with respect to situational awareness of organizations, there are also positives to IoT devices. After an organization secures and updates their environments for IoT devices and the amount of network traffic, this large amount of data could give us more insight into cyber-attacks that could have happened. Incident response relies on data to make a conclusion concerning what happened and find faults in the system, and this will help improve reliability in the system for future attacks and

business downtime. So, while IoT devices are quite threatening for situational awareness, they can actually be a benefit if set up correctly.

Chapter 3: Security Information and Event Management (SIEM)

In the early days of IT there were very few security tools. When firewall and intrusion detection systems (IDS) came out, they were vendor specific and were only written for that brand or product. As more and more products with vendor specific security tools came out, it became hard for IT or security analysts to see what was happening because each vendor had its own specific GUI and proprietary storage format. Management of these tools became too cumbersome and event management was difficult to perform because analysts had to correlate events in each of these GUIs or logs to see what had happened. This is where SIEM tools come in [11].

Security Information and Event Management (SIEM) is a type of tool that organizations use for IT security and provides a holistic view of the security management [12]. SIEM systems are used to collect data from multiple locations so that when analyzed it can be easier to conclude a legitimate answer. Figure 3.1 shows a layout of what a typical SIEM involves.

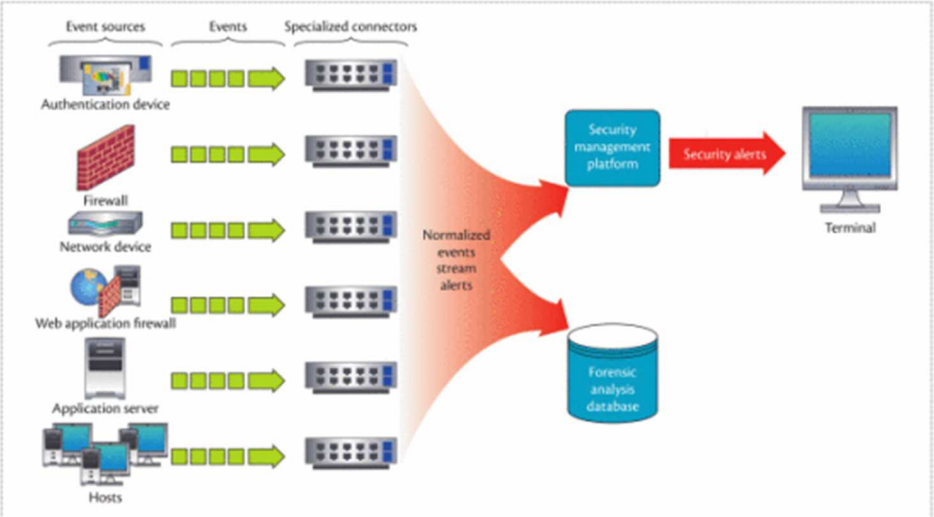

Figure 3. 1 Typical SIEM System Architecture [13]

Some refer to SIEM as security incident and event management but since 2005 Gartner coined SIEM as security information and event management. In an enterprise-like environment, SIEM tools collect information from remote sensors or computers, then SIEM reports to a security operations center (SOC) which is a centralized unit for computer security and incident response teams (CSIRT) which respond to the malicious activity. A recently published IEEE paper describes SIEM by saying, "Security incident and event management (SIEM) systems are an important tool in SaCs-collecting, normalizing, and analyzing security events from diverse sources-but they must evolve to overcome future scalability issues" [13]. The idea is that with more information about an attack, it is easier to make a rational and smarter decision. Typically, SIEM are used in enterprise environments because of the amount devices connected to its network, but SIEM tools can also be applied to small to medium sized businesses and can be an important asset.

The reason why CSIRT would need to investigate is because there might be false alarms. These false alarms are called false positives. False positives look like something suspicious is going on but in actuality there is nothing malicious about it. If there is enough evidence that it truly is an attack, a cyber security expert will want to make sure to eliminate or quarantine that device or those devices. Companies can lose lots of revenue if there is a false attack so security operators will want to make sure that it is the right decision. There are already research and solutions into SIEM tools self-adapting to false positives to reduce the need for intervention of operators [14].

SIEM tools can be broken down into security information management (SIM) and security event management (SEM). SIM is collecting, monitoring, and analyzing data logs of

SIEM tools, and SEM is event management of real-time threat analysis, visualization and incident response. In other words, one looks at log data to create alerts, while the other looks at events in a network to create alerts. Many times, open source and proprietary tools package these two methods of creating alerts and monitoring into one. SIEM tools do a lot of things, but at the core they take data from a lot of sources and provide useful, actionable information to analyze.

3.1: SIEM Tools

There are many SIEM tools available on the market for organizations to use. Most of them can be divided into open source and proprietary. Open source and proprietary SIEM tools each have pros and cons. Open source tools are generally free for use by individuals and enterprises. Sometimes, open source and proprietary tools provide capabilities such as log management, visualization, automation, third-party integrations or cloud environments. The choice between open source and proprietary is dependent on what tasks you wish to do and how large your organization is. Most SIEM tools provide a free trial or free download to try to see if this tool will work for one's organization. For example, cloud services for some SIEM tools can be very expensive, so if one's organization is small, it could be more of a cost benefit to keep all of the organization's event data in house instead of the cloud. SIEM can be uniquely customized to whatever size of organization and across multiple setups. Figure 3.2 is a typical setup of what a SIEM data flow would look like.

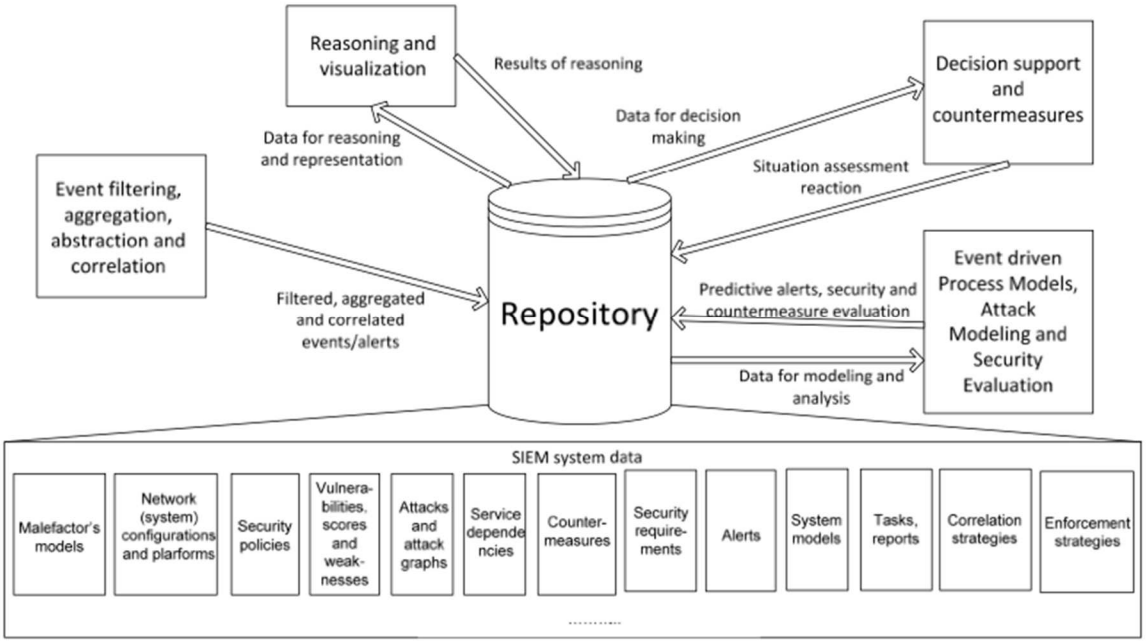

Figure 3. 2 Typical SIEM Data Flow [15]

Some open source and proprietary tools include OSSIM, the ELK Stack, OSSEC, Wazuh, Apache Metron, SIEMonster, Prelude, Security Onion, Mozdef, Snort, Suricata, and Nagios. There are many more out there and they are specific to what sort of environment you have and what sort of security you are looking for. Most of these tools are open source, and some are free to use until one's enterprise has become large enough to require licenses.

3.2: Intrusion Detection Systems

An intrusion detection system (IDS) is software that monitors malicious activity that is either reported by the network or devices. It tries to detect any intrusion into an organization's system, either from observing network packets or by receiving direct logs from remote host devices. The IDS's role is to report suspicious activity to a centralized

location. In larger systems, there could be many IDS tools monitoring devices and the network that all report to an SIEM. IDS tools can also come in open source and commercial solutions for small to large businesses [16]. Figure 3.3 shows a typical IDS architecture. An IDS is commonly broken down into two sub-types: IDS and IPS. In this thesis, mostly the tools and functionalities of IDS software are covered. It is important to explain the difference between IDS and IPS in a little more detail.

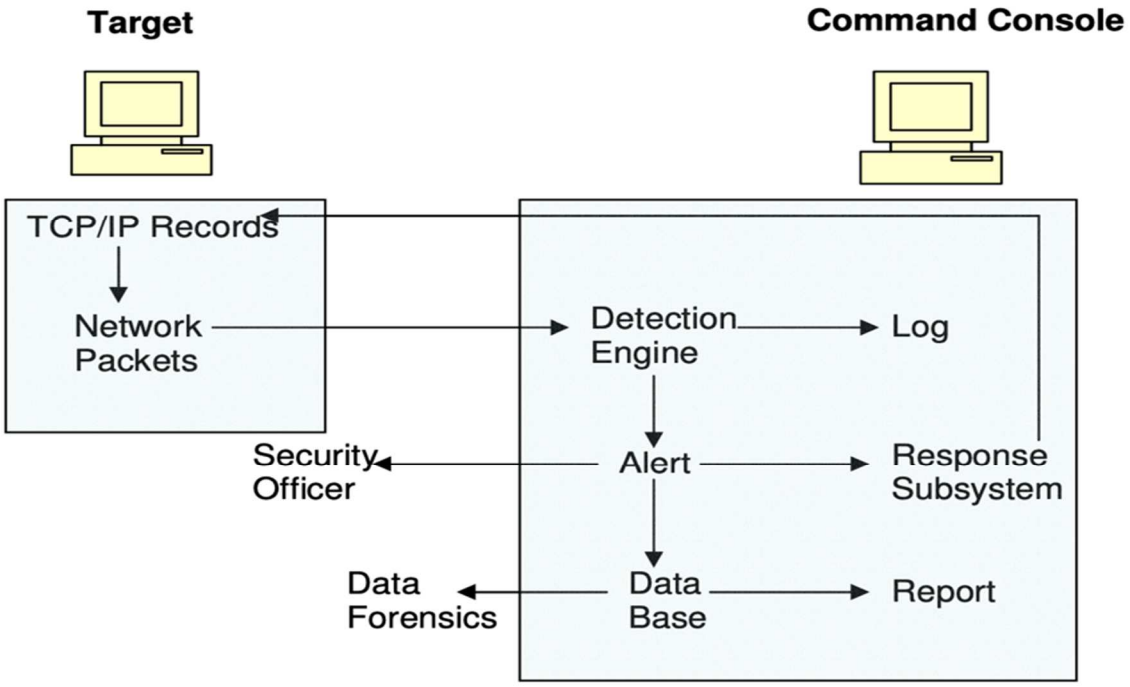

Figure 3. 3 Typical IDS Architecture [16]

3.2.1: Difference Between IDS and IPS

IDS is the application of detecting suspicious activity in a network and host while an intrusion prevention system (IPS), or sometimes called intrusion detection and prevention

system, is the application of prevention of the suspicious activity noticed by the IDS. The prevention includes logging the activity, reporting the activity and attempting to stop or block the malicious activity while it is occurring. IPS are considered add-ons or additions to an IDS system which is why they are also often referred to as IDPS. Sometimes these IPS add-on tools can be bundled with IDS systems as part of a proprietary solution. An IPS creates an actionable response to suspicious activity due to a matched rule or signature. An IPS rule might be to log, report, and cut off a matching connection. There are many options and tools for IPS. Given the scope of this thesis, IDS and incident response will be the main focus.

3.2.2: Two Common Types of IDSs (HIDS and NIDS)

IDS systems can vary from reporting malicious activity on a device to network monitoring. The two most common classifications of IDS systems are network intrusion detection system (NIDS) and host-based intrusion detection systems (HIDS). NIDS are types of IDS systems that analyze network traffic coming into the system while HIDS are systems that monitor important operating system and application files and event logs. NIDS are just for network monitoring while HIDS are for monitoring the hardware and software of the organization's computers and devices.

There are three main types of IDS: signature-based IDS, anomaly-based IDS, and a hybrid of both. Signature-based or rule-driven detection compares the packets, files, and OS software of pre-defined signatures of known malware and filter them out and alert. Anomaly-based or analysis-driven detection compares the current network or computer status to the given baseline for the organization's network including bandwidth and protocols used. Each approach has its downfalls. Signature-based approaches only compare known signatures or

hashes and cannot prepare for newly created malware. Anomaly-based or analysis-driven detection will create more false positives and create false alarms making it hard for security experts to know if there is an actual attack.

NIDS tools are widely used and available to apply on small businesses and enterprise networks. Every webpage and email a user views comes in as a series of packets. These packets can almost be thought of as envelopes and a letter and these packets are sent from one computer to another to exchange data. NIDS "sniffs" or monitors the network to see the details of these packets and filter through them.

A NIDS also differs from the common firewall tool for finding intruders. A NIDS adds more monitoring than a basic firewall. The biggest difference between a firewall and NIDS is a firewall only examines the packet header of network packets while a NIDS will examine the payload and all of its details. NIDS can add extra functionality of monitoring network packets [17]. A firewall only prevents open ports to be exposed to computers and servers. A firewall does not alert when something malicious has happened but only blocks incoming traffic. An IDS alerts when something suspicious has occurred.

HIDS tools have been widely developed and implemented into enterprise networks as well. HIDS tools report any suspicious activity in the local host, which is the actual computer operating system running the HIDS application. This can be computer parts of the host machine such as memory and storage. HIDS can even monitor traffic going specifically to the host to see if there is any suspicious activity. Another important thing that HIDS systems can monitor is what resources programs are accessing. For example, a HIDS system could report that the word processor program has suddenly and unexpectedly started modifying a password database.

Once in a system, attackers try to contaminate files with Trojans, backdoors and other data manipulation. One functionality of HIDS systems is to inspect file integrity [18]. How it checks for file integrity is by keeping and encrypting important information about each monitored file and storing that information about the file and directories in a database. It periodically compares the parameters with the properties of the monitored files and notifies the admin if there is any deviation. Two popular HIDS tools that inspect file integrity are Tripwire and AIDE. Tripwire has pioneered many techniques in intrusion detection and is widely used among corporate and government professionals. AIDE is an open source alternative to Tripwire. It is licensed under GNU and works with many Unix-like systems.

Both HIDS and NIDS have their functionalities and roles in securing a system. One of the key differences between HIDS and NIDS is that HIDS are meant to only monitor the local computer itself and report back to the server while NIDS will monitor all traffic in that environment. An independent study by Kozushko describes HIDS and NIDS as “host-based intrusion detection detects insider misuse while network intrusion detection detects outsider misuse” [19]. One advantage that NIDS has over HIDS is that the NIDS system can track an intruder going to another host computer and can even sound the alarms and prevent the intruder from infecting a computer. On the other hand, HIDS would be able to find out that it has been infected but only after it has been infected. An advantage that HIDS has over NIDS is that it is able to report much more information about the status of the computer itself instead of just packets coming. NIDS and HIDS are thus both useful and should both be implemented to have a secure environment.

3.2.3: Log Collection and Analysis

IDS systems have a place and can be a very high security asset for many organizations. These IDS systems are great at detecting and reporting events, but if there are many IDS systems in an organizations environment and thousands of events are being reported, it can be overwhelming to look at each IDS system and view what is happening. This is why there are specific situational awareness tools available to collect these logs, sift through them, and report in an easy and functional manner. Tools such as Eventlog Analyzer and ElasticSearch have that specific job. They are great tools for collecting, parsing, and filtering the logs that are most important.

Log collection, parsing and filtering can then lead to log analysis. The analysis provides value into the security of the system. It can provide easy to read GUI's and analytical reports for security experts to see weaknesses in the system. With in-depth log analysis and analytics organizations can prepare for and find weaknesses before breaches occur. In a Linux distribution named Security Onion, IDS and log collection and analysis are given right out of the box.

3.2.4: Security Onion

A popular and open source Linux distribution that has both NIDS and HIDS set of tools is Security Onion. Security Onion is a free and open source Linux distribution intrusion detection, enterprise security monitoring, and log management system. Security Onion provides NIDS, HIDS, and NSM. It has a number of tools under its belt to do all of this. Security Onion includes Snort, Bro, Wazuh, Sguil, Logstash and many more security tools.

Security Onion comes as an Ubuntu-based virtual machine (VM) with all these tools pre-installed or can be installed on one or more bare metal computers and customized.

Security Onion's goal is to combine three core functions: full packet capture, NIDS and HIDS, and powerful analysis tools. In a higher-level view of Security Onion, there are functional Security Onion tools configured to capture and filter network packets and computer logs. These logs and packets are then processed, parsed and indexed by certain tools for additional analysis using other tools. Figure 3.4 is a great figure of Security Onion tools at a high-level view. There are several different ways Security Onion can be set up. How Security Onion is set up is related to the environment in which Security Onion will be placed. Security Onion gives certain use cases as examples of what and how to deploy it. The different use cases include evaluation, minimal evaluation, pcap forensics, production server – standalone, production server – distributed deployment, analyst VM, and sensor sending logs to a separate SIEM.

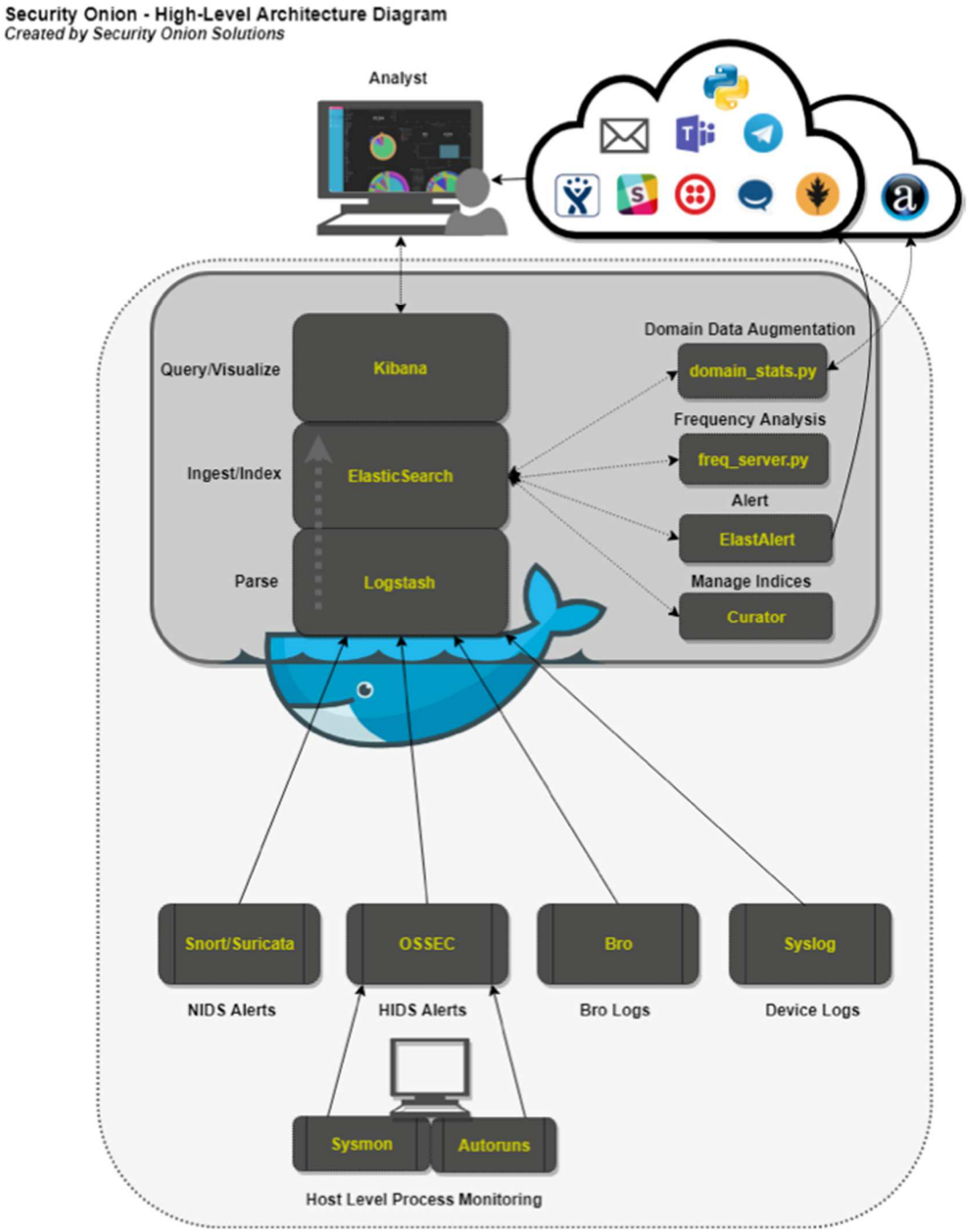

Figure 3. 4 Security Onion Architecture Overview [20]

Within Security Onion there are two types of NIDS tools to use. There are rule-driven and analysis-driven NIDS tools. Rule-driven tools identify malicious traffic by comparing rules defined by the user to filter network packets. If a network packet is similar to a rule defined, then it will alert the user. Snort or Suricata are rule-driven NIDS tools offered in Security Onion [20]. Analysis-driven rules analyze and monitor logs created by other applications. This includes DNS requests, SSL certificates, syslog activity and much more. Analysis-driven tools also have the option to compare files against known malware md5 sums. How this works is, first, when you run a md5 sum on a file, the output is a unique number. If this unique number is the same as other well-known malware md5 sums, then you might have a malicious file. Zeek, or formerly known as Bro, is an analysis-driven tool in the Security Onion suite that provides this capability for files seen in the network traffic [21].

The Security Onion also offers a HIDS tool in its many options. Wazuh uses hosts or remote computers to create logs when events happen. This is described later in the next section, 3.3.3, in more detail.

After all these events and packets are monitored and logged by the NIDS and HIDS tools mentioned above, it is important to have analysis tools to see in an easy and graphical manner. Sguil is a database that has a GUI to see in real time all of the data pulled from Snort, Suricata, and Wazuh. Sguil is a powerful tool for any cybersecurity expert. Squert is an add on for Sguil that offers an easy to use web interface of the logs and additional analytics. Kibana uses ElasticSearch to pull in all of the logs reported into a nice and easy single monitoring pane. Kibana pulls in logs from Snort, Suricata, Wazuh and Zeek. Kibana's intention is to be the "single pane of glass" for all of Security Onion. Lastly, Capme

allows you to view and download full PCAP files. Many of these tools have the option to integrate with other SIEM tools in an enterprise environment.

Other tools that Security Onion offers in the analyst workstation configuration include Wireshark, which is a graphical network packet analyzer. Another tool provided by Security Onion is NetworkMiner. NetworkMiner is used for network forensic analysis to view open ports and parse PCAP files. It helps mitigate and respond to complex malware attacks.

3.2.5: OSSEC/Wazuh

A popular tool used by security experts and managers alike is OSSEC. It stands for Open Source HIDS Security. OSSEC can perform a variety of functions such as log analysis, file integrity monitoring (FIM), centralized policy enforcement, Windows OS registry monitoring, rootkit detection, time-based alerting, and active response. It works with almost all operating systems. OSSEC is a server/agent architecture where a server asks for updated information about the host/computer and the agent reports back the to the server on its current status and logs [22]. Some of the information collected by the agent is collected in real time, others periodically. A fork of OSSEC HIDS and a popular tool currently bundled with Security Onion is called Wazuh.

Wazuh is an open source HIDS tool for monitoring hosts and remote computers. Wazuh is included in the Security Onion Linux distribution. It works with ElasticSearch to offer a SIEM solution tool for Security Onion. It works with major operating systems such as Windows, Mac OS, and many popular Linux distributions. There are a variety of functionalities that Wazuh can manage on a remote host. Functionalities include file integrity

monitoring, root kit detection, and Windows registry monitoring and many more. Wazuh also has the functionality to monitor services on remote servers such as FTP, mail, DNS and many more [23]. Kibana or Grafana is required for Wazuh and used in conjunction with Wazuh to offer a graphical interface for the user.

There are many components to both the Wazuh server and the Wazuh agent. When the Wazuh server receives event data, it forwards them to ElasticSearch, parses them, and interprets them. On both the agent and server side there are Wazuh daemons running processes or tasks to collect information about itself. A daemon is a type of task or process in a computer that runs in the background, and the intention is for the user to not see it. There are lots of daemons running in the background on modern computers. On the agent side it has multiple tasks it has to do for its daemon, and on the server side it has a daemon collecting while also using multiple services.

The client side under its daemon agent has several different tasks that it is running. Some tasks include Rootcheck, Log Collector, Syscheck, and OpenSAC. Each task has a specific purpose, but they are all monitoring and collecting information. The agent daemon can be configured to add or remove other tasks for collecting. The agent daemon uses port 1514 for sending OSSEC protocol events to the analysis server.

In the server analysis daemon, it has services to collect information as they come in from the client agents and triggering alerts if an event matches a rule described by the user. The server side has the Wazuh analysis daemon running with a couple of main services like the registration service and the remote daemon service.

When all of those logs are generated, Wazuh needs something to feed it to report to the user. This is where ElasticSearch comes in. ElasticSearch is a suite of open source

projects for log management [24]. The log management it performs includes taking those logs, indexing them, and putting on a graphical interface for a user to see. Since this is open source, other users in the community contribute to ElasticSearch but need to be within what ElasticSearch calls the Elastic Common Schema. The ELK Stack includes tools such as ElasticSearch, Logstash, Kibana, and Filebeat. Once logs are decoded, ElasticSearch does all of the indexing into different Wazuh types. These types include Wazuh-alerts, Wazuh-events, and Wazuh-monitoring.

3.3: State Monitoring

State monitoring is the process of continuously monitoring all or important devices or software that need to be up and running for everyday use. This means that servers, workstations, switches, routers, etc. all need to report status and error logs to a centralized relational database location. This is not only important for IT departments but also for security professionals. If servers or important services are down or unreachable, this can mean a loss in revenue or disrupted availability. If a cyber-attack happens on an organization's network, security professionals can be alerted in real time what is down and what devices were hit, and this is useful for incident response as well as for security forensics to determine what might have happened.

It is important that after the state monitoring tools are set up to continuously monitor as many devices as possible and the important services those devices might provide. State monitoring gives cybersecurity experts and IT administrators an overview of the current operational state of the environment. State monitoring is also referred to as information security continuous monitoring (ISCM). The National Institute of Standards and Technology

(NIST), has created regulations for government and guidelines for private organizations on the standards for monitoring IT systems. NIST describes ISCM by saying, “Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions” [25]. Many state monitoring tools run off of log collection and analysis.

3.3.1: Common State Monitoring Tools

There is a vast amount and large variety of state monitoring tools. Sometimes they are packaged with other cybersecurity network tools, and other times they are standalone programs that work by themselves. These tools, of course, can be applied to larger or smaller organizations depending on size and demands needed for the tool. Some common state monitoring tools include Nagios, Zabbix, PRTG, and many more. Many of these tools have additional plugins that are installed on the host computers/servers and then report back to the state monitoring server. They almost always have some sort of visual to see all computers reporting, what their status is, and where their location might be. All of this is reported in real time.

For example, Zabbix, a well-known and commonly used state monitoring tool for all sorts of different areas of industries, is used for network monitoring. Just like many other tools, it can be packaged with all sorts of different add-ons to do other things. One of the features that Zabbix includes is a centralized, easy to use web interface. It also includes a server that will run on most Unix operating systems. Agents that are installed on the client computers can run on most Microsoft and Unix-like operating systems. It also has the ability to directly monitor SNMP and IPMI devices. Real-time built-in graphing visualization

capabilities offer ways to customize and configure monitoring tools. A good guide for how to install and configure Zabbix can be found in *Zabbix 1.8 Network Monitoring* [26].

3.3.2: Nagios

A popular and efficient tool to use for state monitoring is called Nagios. Nagios is an open source application for monitoring systems, networks and infrastructure. It alerts IT managers and cybersecurity experts when something goes wrong with that device. There are practically two versions of Nagios: Nagios Core and Nagios XI. Nagios Core is a free open source tool for smaller businesses and smaller environments. There is no limitation on the number of devices for Nagios Core, and there are hundreds of free plugins for Nagios Core. Nagios XI is an extension of Nagios Core and is used for commercial and large enterprise environments. Nagios XI is free for the first 7 devices, but for any greater number of devices it is available by subscription. Nagios XI offers additional benefits such as improved UI and integration with cloud services.

Nagios continuously checks hosts and services of that host. Nagios works by server to client checks. Nagios Core or XI is installed on a Linux system and is the referred to as the Nagios server [27]. Nagios server displays all hosts and services of that host in a well laid out web page. Hosts are added by configuring the Nagios server to look for that host. To look for a host, the Nagios server is given an IP address and set of commands to execute for that host. Nagios comes with some very simple commands or scripts to run on the remote host. Plugins can be added to the Nagios server to expand the number of commands it can run on remote hosts. There are hundreds of free open source plugins to run with Nagios. One popular plugin

framework is the Nagios Remote Plugin Executor (NRPE). NRPE has extra functionality to do checks and monitor a local host [28].

A desired plugin is installed on both the server side and the client side. The plugin is running as a daemon on the host, and when the server wants to know information about it, the plugin on the host side will run that script, grab information, and send it back to the Nagios server through SSL. This makes it easier on the Nagios server to do this, because if it did not have the plugin, the Nagios server would have to create an SSH shell with the remote host and run it. SSH shells can take a lot of computing recourses. Plugins help to keep resourses down. Plugins also help by doing passive checks instead of active polling. Instead of the Nagios server having to actively poll each computer and do checks on each computer, it actually just receives information about the remote host. If the remote host does not send information for a while, the Nagios server will run the check on the computer to see if there is something wrong. Nagios has three states that a computer can be in: Critical, Warning, and OK.

3.4: SOAR

Security Orchestration Automation and Response (SOAR), or SOA, can be thought of as way to automate responses and resolve issues that an SIEM tool might produce. SIEM tools are amazing at generating responses and alerts to suspicious activity, but the sheer number of alerts and responses can overwhelm even to trained cybersecurity specialists. SOAR gives IT managers and cybersecurity experts a way to filter to the responses and incidents that might be more important. They can work in conjunction with SIEM. SOAR can be trained to automatically respond and even resolve certain alarms that are more likely

to be an actual issue or attack. For example, if there are normal alerts that a certain piece of software is insufficient, this might be a normal occurrence, and SOAR could be given the functionality to automatically resolve this issue or ignore it. Because IT managers and security experts have so many things to look at, it makes their job easier to find the important and vital information. A large amount of these alerts can be false positives which can lead to more time wasted for operators. It helps professionals focus on the important things. Thus, SOAR software is used in places for security experts and operators alike in the security operations center (SOC).

There are number of open source and proprietary SOAR tools available on the market. Some SOAR market leaders include IBM, Fireeye, Cisco, Radid7 and many more [29]. Many times, SOAR tools get packed with SIEM tools as addons and are used interchangeably. A lot of the tools mentioned above about SIEM also have SOAR interfaces as well. For example, Splunk, which is a SIEM software, has capabilities of also being a SOAR. Splunk SOAR, which they call Splunk Phantom, has plugins for using in conjunction with their own SIEM tools. Their user interface is well laid out and is easy to exactly see devices and notifications. It is also easy to set up automation for addressing responses to certain incidents and alarms. Thus, it helps by saving time for security experts to see the unexpected alarms and alerts and really focus on those.

3.5: Incident Response

Once an intrusion detection system tool detects an incident, what happens next is a concern for cybersecurity experts. If an organization is able to collect information about something fishy going on, but then do not do anything after that, there is no point in just

detecting. This is where incident response comes in to save the day. Responding to cyber-attacks and incidents needs to be done in an organized and quick process, or else it could make matters worse [30]. An incident response differs from an IPS, which is described earlier, in that an IPS will automatically react to malicious activity if it is a straightforward and efficient action (e.g. terminating a network connection), while incident response is a process of human interaction to investigate in more detail what happened during cyber-attacks. There are often specialized teams just for dealing with cyber-attacks. These teams are usually called computer security incident response team (CSIRT). There are many studies about how incident response teams should be built and the methods and flow of the response. These teams can also include not only cybersecurity experts but business experts as well. One such study explains how to put an incident response team together and who to include [31]. There are also many studies for these incident response teams to handle the incident [32]. Unfortunately, many organizations cannot afford to have specialized teams for handling incident response. Organizations typically can afford incident response tools to make requests and help cybersecurity experts for forensic investigations.

Any incident that is not handled properly and swiftly can lead to more damaging effects such as data breaches or system melt downs. It is important to contain and handle these incidents in a timely and efficient matter. If a system goes down or is not responding, organizations can be out of service, and that often means loss of revenue. If incidents are recorded but not handled there could be potential fines and could cost large amounts of money to trace what happened in a forensic investigation. It is crucial for organizations to have incident response tools in place to maintain cyber situational awareness so that they can quickly and effectively handle suspicious events and contain and recover from cyber-attacks.

There are a number of tools for incident response handling. They can range from open source to expensive proprietary tools. The application of what tools to use varies based on the organization size and the importance of security to the organization. Many times, SIEM tools and IDS tools also come bundled with incident response tools. Some tools can even provide deeper insight into a response such as forensic details, location, and technical support information. Responses to unusual incidents are not only automated from IT assets and scripts but also include human activity. Employee training and awareness is important in an incident response flow.

There is a difference between incident response in the cybersecurity area and the IT area. Cybersecurity incident response has an emphasis on security incidents, containment, and recovery, whereas IT incident response has a focus on getting services for customers and employees up and running again. There are certifications for IT workers to achieve certifications in the ITSM area. One well known framework for delivering IT services is called the IT Infrastructure Library (ITIL). The ITIL is described as "one of IT Governance standards, and it manages and controls IT services effectively" [33]. IT governance is an integral part of an enterprise and defines workflow and planned objectives. When companies provide a product that is reliant upon these IT assets, companies and organizations need to keep these services up and running as much as possible. So, the area of intent is different for IT than it is for cybersecurity. Both are very important to organizations for making sure they are completely operational and cyber resilient.

Incident response tools can be seen in two different ways: responding to incidents in an automated way or responding to incidents manually. There are manual and automated tools for both IT management and cybersecurity. They can be stand alone or be bundled with

other tools like IDS tools. Cybersecurity and IT incident response sometimes have both or just one of the functionalities mentioned above. Typically, SOAR tools and ITSM tools can be both automated and manual. Their functions are to address well known issues in an automated fashion and unknown issues in a ticketing method. Unknown alerts will usually be handed to IT or cybersecurity specialists to address and fix the issue. There are variety of incident handler tools out on the market today. One popular incident handler tool is RTIR.

3.5.1: RTIR

A great incident response tool for alerting and handling incidents for IT managers and cyber security professionals is a tool called Request Tracker for Incident Response (RTIR). RTIR is a add on of RT or Request Tracker. Request Tracker is an open source email-based ticket tracking system used to coordinate tasks and manage requests among an organization or enterprise used for general purpose. RT is commonly used for bug tracking, help desk, invoicing, incidents, sales, network operations, and abuse. RTIR adds the extra functionality for cybersecurity incidents and automation. RTIR automate the alerts from different monitoring software for IT or cyber security managers to receive and resolve. For CERT teams and cyber security experts, RTIR helps immensely [34]. This automation: saves time for cyber security experts and IT admins, helps with large volume of incidents, and increases resiliency within a system. Without RTIR something might happen in the IDS or monitoring tool, and no one would be alerted that something is wrong and that it needs to be resolved. These IDS and monitoring tools have great user interfaces to see what exactly is going wrong once inside of them, but with RTIR it enhances the initial ability to alert the CERT team or cybersecurity manager.

RTIR is written in Perl and runs on an Apache or lighttpd web server that can use MySQL, PostgreSQL, Oracle, and SQLite as the backend database and mod_perl to interpret Perl scripts for the web server [34]. When RTIR is set up, a mail gateway is needed to receive and deliver emails to email accounts which represent ticket queues. RTIR is completely configurable; extra customizations and values can be overridden in Perl configuration files. RTIR's goal is to be completely configurable for every IT system. Customization can be made to tickets, queues, and scrips. Scrips are a condition, an action and a template that allow for the quickest and simplest way to customize RTIR's behavior.

Tickets are used in RTIR to help resolve incidents. These tickets can be created manually by users or automated by scripts from incoming emails or alerts. Tickets are made up of fields which are detailed and configured information about that ticket. Tickets have default fields that are included in RTIR. One field that is critical for RTIR is ticket status. A ticket status field can have various states. These states include "open', 'installed', 'abandoned', etc. Custom fields as well can be created for tickets. RTIR has custom fields that are not included in RT. Tickets also include an aging life cycle where the age of ticket is based on the default or customized "Last Updated" property. Users also lock a ticket to make sure no work is overwritten by other users when editing or changing the ticket. When other people need to be included in a ticket a queue is created.

A Queue, in RTIR, are a group of tickets that are logically related. A queue allows for a group of people inside an organization to resolve an issue. By default, there are four default queues that RTIR comes with: Incident Reports, Incidents, Investigations, and Countermeasures. Queues, like tickets, have fields for configuration and detail. Incidents queue for example can lump 100+ incident reports into one incident. When the queue fields

are set this allows for central point of ownership, communication, collection of data. Custom queues can be created for specific groups within an organization. One field that makes queues highly configurable is the constituency field. Constituency functionality make it possible for queues to be customized to specific group of customers. If for example an organization has two different types of customers and certain groups deal with each type of customer. Constituency can be customized to meet those needs of each type of customer. An admin could possibly set up multiple constituencies for different incident and access rules. Automatic constituency can also be set up for customized queues. IP's can also be used to customize and configure queues for specific use cases.

Let's take for example a process of creating an auto reply for specific queues in RTIR. First the admin would need to create a local autoreply template for a specific queue. The admin would create a new template for your queue. Next the he or she would fill out the create template form and save. Then the admin would tell the specific queue's scrip to use your new template rather than the global one. Finally, he or she would find the On Create Autoreply to Requestors with Global template Autoreply scrip in the list and update it. If that scrip is not found, then the admin would need to create it.

For all RTIR functionality, scrips are used to do every action. Every change that has been made to a ticket; a scrip is ran in the RTIR system. It helps to update RTIR as whole of the status of the ticket. Scrips consists of a condition, an action, and a template. A scrip has a wide range conditions that the RTIR admin can customize. When a condition is true then an action is triggered. An action is what the scrip does. After the action is ran, text is created and sent out typically in form of emails to employees or customers or even stored in other tickets. These are called templates. There are variety of scrips that are installed with RTIR. These

scrips can be customized for each IT system. Email notifications that come in from customers that are reporting have scrips to respond to them.

By default, RTIR never deletes data from the database. Deleting and restoring data can be customized with the TRx::Shredder extension. RTIR includes Perl script or GUI website interaction to delete or customize when to delete data. This extension also provides SQL commands to reverse any data that might have been deleted. Customizations can be added to this shredder extension to maintain database size.

RTIR Admins have the privileges to add new users to access RTIR. The RTIR Admin can create different roles for users of RTIR. The RTIR Admin might give access to RT to create tickets and see tickets for them but not give access to the add portion of RTIR, while the RTIR Admin might give full access to RTIR tickets and incident response management for cybersecurity incident response experts. When an RTIR user logs in, depending on what role they were given by the RTIR Admin, they will either see RT or RT and RTIR in the top display menu. If given access to RT, the user will see just RT ticket queues and if given full access will see both RT and RTIR.

On top of all of this customization and functionality, RTIR also comes with tools that give IT and cyber security admins the ability to search computers and incidents based on IP and network lookups like traceroute and whois. This gives that admins the ability to check DNS records that can link to URLs for log viewing or full packet capture. This functionality also gives users the ability to extract network captures from bulk ticket data.

All of this customization and configuration is completely up to what best fits the use case and what admins find the most appropriate and most suitable their situation. These customizations could be based off of size of organization, types of groups dealing with

incident response and types of incidents. Setting up the incident response system architecture can be challenging and hard to scale. Some issues that CSIRT teams come across with incident response include searchable and reliable metadata, incident categorization, incoming traffic sanitation, lifetime and bulk checks [35]. These short comings can be overcome by correct architecture and correct tools for specific size and organizations.

Chapter 4: IT Asset Management

IT asset management is the organization of IT assets to manage the life cycle of all devices. IAITAM, International Association of IT Asset Managers, describes IT asset management as a "set of business practices that incorporates IT assets across the business units within the organization. It joins the financial, inventory, contractual and risk management responsibilities to manage the overall life cycle of these assets including tactical and strategic decision making" [35]. Many times, IT asset management is referred to as IT inventory. IT managers typically gather detailed information about each computer's hardware and software inventory in their organization. After an inventory is conducted, IT managers make an effective and cost beneficial decision on whether to keep or buy new hardware or software for their organization. Often, IT managers make effective decisions based on metadata and electronic records to track and categorize the organization's assets. IT asset management can be divided into four categories: hardware, software, cloud and End-User Mobile/computer management. Each category adds a new complexity for IT managers and becomes harder to keep track of.

To implement IT asset management, many companies and organizations use an asset management software. Asset management software is a tool to view all controlled software and hardware of each device in a user interface window. Asset management software tools also monitor these devices and make sure everything is in normal and running status. Most IT management software use barcodes or RFID to individually mark each IT device. The ID and location of each device is then placed in an IT asset database to keep track of a record of all devices. Typically, small businesses and labs use a homemade spreadsheet to manage assets; this sort of solution will work but can be hard to update when new hardware or software is

changed or improved. It can also be difficult to keep track of all new hardware and software for growing businesses [36]. Whether an organization space is large or small, an IT asset management system can help significantly. There are many examples of small and large companies implementing these solutions into their work and improving IT management in a lot of ways [37].

4.1 IT Inventory and Cybersecurity

There are a number of ways IT inventory helps increase situational awareness and cybersecurity. The cloud, mobile and IoT devices are adding an extra layer of complexity for IT managers to keep all devices up to date. Cyber attackers can exploit unaccounted and out-of-date hardware and software in an organization. An IT asset management tool helps in monitoring and alerting of possible vulnerabilities in an organization. Two examples of out-of-date software and unaccounted devices leading to problems are the British Airways hack and the NHS WannaCry attack. The British Airways hack was a large data breach where British Airways, at first, did not know exactly how the hackers got in, but later found that baggage claim information pages' scripts were changed by hackers. If better IT inventory was in place for monitoring who is doing what, this could have prevented this serious data breach [38]. The NHS WannaCry attack was a ransomware attack on 600 medical service computers and put five emergency centers out of service. IT inventory of out-of-date computers could have prevented this devastating ransomware attack.

IT inventory should be implemented in the initial design of IT infrastructure for cybersecurity. There are many benefits of IT inventory in the design and management of IT infrastructure. If an IT infrastructure has some sort of IT asset inventory in place, an IT

manger will be able to visibly see all devices and pinpoint risks for each computer. An IT manager will also be able to find threats and detect risks early. An IT manager will also be able to trace data to when an attack happened so further investigation will not leave doubts like the NHS WannaCry attack did. Finally, it will also leave organizations with a cost benefit for cybersecurity. Cybersecurity is not cheap for an organization to implement, so IT inventory by design will leave the organization with added cost benefits by making the cybersecurity tools deployed in a more efficient and effective way.

NIST has released a special publication for national agencies on how to design and implement a cyber secure IT asset management system. They recommend a system with not only a barcode ID of each device but what current software each device is running. The document was proposed with the financial sector in mind since this sector is challenged with the vast diversity of hardware and software in financial IT systems. The first quarter of the document describes approaches and architectures for how to implement IT asset management into an IT system. It describes the IT asset lifecycle and security characteristics and controls mapping for types of systems related to what cybersecurity framework to apply. It also includes different tiers of a typical enterprise and how they are segregated. These tiers are later used for the last third of the publication which describes common and well-known tools for implementing IT inventory management. Tier 3 is composed of enterprise assets themselves like hardware, software, and virtual machines. Tier 2 includes sensors and independent systems that feed data into the enterprise ITAM system. Tier 1 is the enterprise ITAM system that provides the aggregation of data from tier 2. It includes guidelines and configurations of popular tools and how to implement them in an IT enterprise system [39].

Chapter 5: RADICL-IF Use Case

The remainder of this thesis describes a use case of cyber situational awareness tools applied to the RADICL lab, a cybersecurity lab used for research and learning purposes on the University of Idaho – Idaho Falls campus. The purpose of this use case is to help other cybersecurity lab directors and other organizations apply cyber situational practices and tools to their own network. It is intended to help researches and cybersecurity professionals see the importance of these tools, how each tool is applied, and how they help an organization to be cyber situationally aware. The RADICL tries to implement open source instead of proprietary tools. The purpose of open source tools is to help students learn from setting up and configuring these tools, help them be able to completely change and configure the source code, and potentially help support the open source community by finding bugs and adding functionalities to these tools. This cybersecurity lab is meant to be open for students to learn and discover new cybersecurity concepts and ideas.

5.1 What is RADICL

The Reconfigurable Attack-Defend Instructional Computing Lab (RADICL) is an air locked test environment for University of Idaho and Idaho State University undergraduate and graduate students for education and research purposes. It gives students an enterprise and worldwide simulated Internet closed off from the rest of the world and provides an open area for students to try different hacks, introduce malware and monitor devices, and do cyber simulation games. The RADICL lab is built for students to try anything cyber related and not be punished for damage to any real company or services. There are several policies put in

place for students to adhere by to make sure nothing serious or malicious unknowingly leaves or enters the lab environment. The purpose of the air locked environment is the ability to control and mediate any data or software entering or leaving the lab. If damaging malware is introduced or leaves the RADICL lab this could cause serious reputation damages or lawsuits against University of Idaho.

5.2 Purpose of RADICL

Because RADICL is an air locked lab this means that the RADICL's network is physically isolated from school and public networks. There is no direct route to the Internet. So even when hacks get introduced into the lab, they cannot affect the public. University of Idaho and Idaho State University students and faculty are capable of developing samples of self-propagating malicious software. When a new exploit is created U I or ISU does not want to be responsible for the next worldwide hack. The only thing that the lab has access to from the Internet is updates for packages and OS updates. This is the only network traffic coming into the RADICL lab. All other network traffic going to the outside world is completely closed off. Many industries use similar air gapped networks to not allow anything coming in. In the RADICL lab, the goal is to not let anything out.

RADICL lab is also designed for Red vs. Blue skirmishes. Red vs. Blue games are popular and effective for cybersecurity learning and training. Red vs. Blue was originally for military training to prepare in controlled realistic settings for warfare against foreign enemies. This helps train military infantry and special ops to learn what to do in a certain scenario. This is also true with cybersecurity. These training scenarios can be tuned from cybersecurity experts to beginners. Red vs. Blue is not only used for training but can be used

for research purposes. New and unexplored Red vs. Blue scenarios can be played to see new results and research on teams' tactics and responses and provide insight for real world cybersecurity. RADICL is a great place to try such scenarios since students have access to an enterprise-scale environment that might be difficult to simulate on their own.

5.3 RADICL Lab Layout

The RADICL lab has four main segments or zones: Blue, Red, Green, and White; each connected to each other with different purposes. Each area has a specific number and color to differentiate it from the rest. Each network area can be described as one area with one VLAN, one area with separate VLANs, or one area and one VLAN with subnets inside that VLAN. To get access to one of these colored areas, a student or lab administrator will need to add a VLAN and unused IP to their computer. When adding an IP make sure it is not an IP that is already in use. Figure 5.5 shows the VLAN's and the layout of the RADICL lab.

The Green zone is for downloading packages and OS updates from the Internet and provides the network airlock. The White zone is for network and host monitoring and RADICL IT administration. Blue is an enterprise-like test environment to act as a real-world company or target for cyber attackers. Red is the unknown Internet emulation that is full of exploits, malicious users and evil hackers waiting to access anything they can get into. Blue and Red zones are where much of student testing and research can be done. White zone is necessary for lab monitoring and cyber situational awareness tools. Additionally, there are other supporting zones to assist in the operation of RADICL. The Purple zone is a network to connect Blue and Red to each other in a controlled way. The Black zone is for computer and network hardware and VM management hypervisors. Black is where servers, workstations,

and network devices reside. Ovirt, a virtual machine management software, resides in the Black zone VLAN.

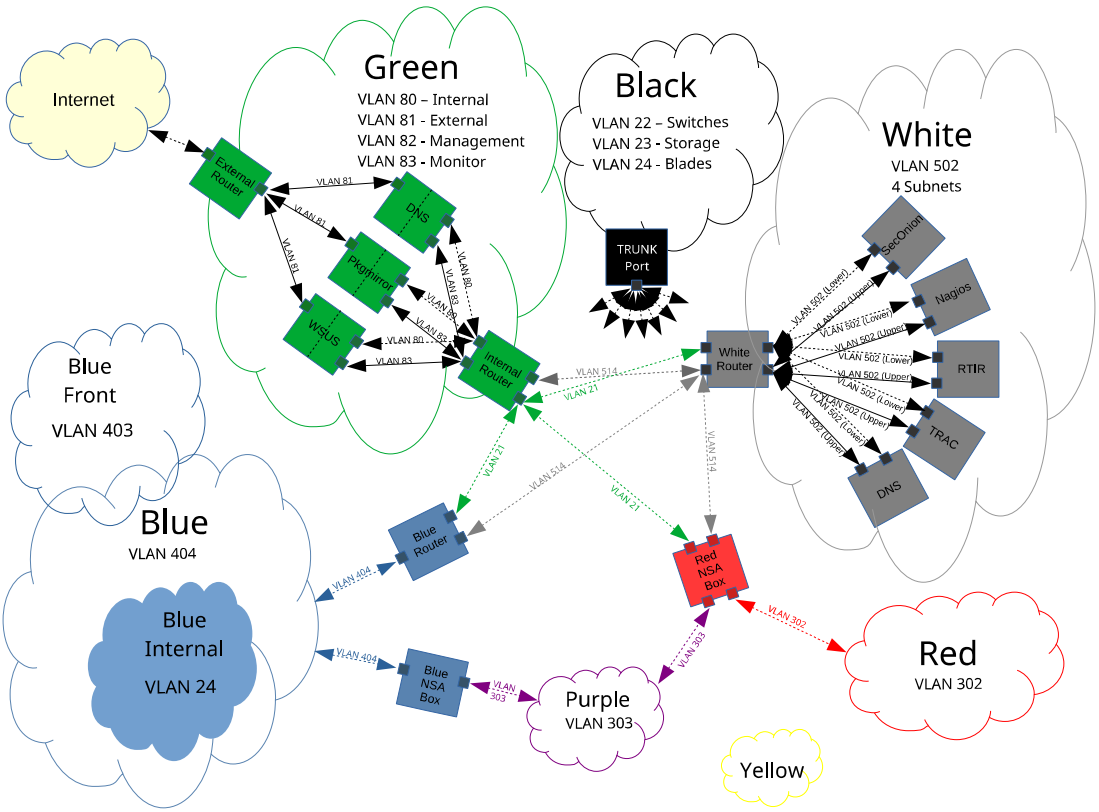

Figure 5. 1 Zones and VLANs Configured in RADICL-IF

The Green zone or VLAN 80, 81, 82, and 83 is for managing a highly firewalled environment used for downloading software packages and OS updates. For security purposes, the RADICL lab requires all computers, servers and VMs to be up to date with the latest OS updates and packages. There are certain times when VMs are left without updating for training and research purposes. An example would be if a certain exploit works on an

older version of an OS (e.g. Windows XP) then RADICL would not update a version of a VM even if it is critical to the simulation enterprise. The Green zone has systems for both Linux package management and Windows Server Updates Services (WSUS) for Windows machines. The Linux boxes used for IT infrastructure in the RADICL lab use the proxy system in the Green zone to get updates rather than connecting directly to Internet servers. There is also a Blue zone WSUS that VMs in the simulated enterprise area use to update to the latest packages. This Blue WSUS uses the Green WSUS to get its updates as an upstream server.

Inside of the Green zone there are a few VLANs each with a certain function in mind. VLAN 80 is for internal routing from all other RADICL zones to the Green zone. VLAN 81 is for external routing to the public Internet. It is the public-facing border network zone. VLAN 82 is for the management of the Green zone proxy servers by RADICL administrators. The last Green zone VLAN is VLAN 83 which is used for monitoring. This monitoring VLAN is used for reporting logs to the White zone.

The White zone or VLAN 514 is for RADICL monitoring, management, and documentation. There are currently two VLANs for the White zone: VLAN 514 is internal to White zone servers, and VLAN 502 is for other RADICL systems to connect and send their logs and network monitoring to the White zone servers. Inside of this zone resides a few VMs for management, monitoring and documentation. There are four VMs currently used for network monitoring and IT management: Nagios, Security Onion, Trac, and RTIR. The White zone does have four subnets to separate certain network traffic. The four subnets were created to separate script traffic from log monitoring traffic. The lowest subnet (0-64) is for

log traffic to the servers. The highest subnet (192-255) of the White VLAN is for these servers to access the Green zone for updates and patches.

The Blue zone or VLAN 404 is a simulated enterprise network used for research and simulation games. This zone and the Red zone are configurable for a student's research. This means that if they wanted to add VMs to try new simulation games or different cyber defense designs, students are more than welcome to do any of that here. If students wish to try different versions of Windows machines or add or remove vulnerable VMs this is network segment for that activity. The Blue network has an outer VLAN and a border gateway which is used for connecting with RADICL infrastructure. The Blue zone has an inner VLAN used for the enterprise for students to configure any way they want. Currently the Blue zone has Windows Active Directory, WSUS, MS Exchange and IIS set up. Currently the Bureau of Land Management (BLM) is the mock organization to attack and a fully operational website and email are open to attack. The Blue zone is also separated into two VLANs. The two areas are separated so that the desks in the front of the room and those in the back can be used for separate training or research scenarios. The front desks have a VLAN of 403. The front desk Blue zone is potentially used for cyber security classes where students can bring their own laptops or other devices so there is no need to go into the back of the room.

The Red zone or VLAN 302 is the malicious "public" like Internet space where attackers are constantly trying to get in and cause havoc. The Red zone, like the Blue zone, is a highly configurable area for students trying things they want. Students are allowed to create and attempt new attack vectors. The Red zone opens a lot of opportunities since its VLAN is set up to allow international IP addresses. Currently each workstation in the back desks have VM's that act as different countries and have IP addresses that are similar to that region.

The Purple area or VLAN 303 is for RADICL infrastructure and is used primarily as a way to route network traffic from Red to Blue in a controlled manner. Purple uses one VLAN and no subnets. The two computers that connect Red to Blue are controlled by RADICL administrators.

The Black zone is used for tracking hardware in the RADICL configuration such as network switches, storage arrays, and servers. The server blades and storage in the server rack use a VM manager called Ovirt. Ovirt is an open source hypervisor created by Red Hat. It is used in RADICL to manage all RADICL infrastructure and virtual machines. To access Ovirt a RADICL administrator needs to be on the Black network with an IP address in that range. Then, to get to the hypervisor GUI, the admin will type in the colors corresponding to area they wish to access followed by the RADICL's domain. For example, to access the hypervisor engine hosting VMs in the Blue network, they will logon to https://blue-engine.hvm.if.radicl.

Two areas that are not in use yet and are still in progress of being implemented are the Gray and Yellow zones. Gray is for all traffic monitoring. Yellow is for remote communication to University of Idaho's Moscow cyber security to Idaho Fall's cyber security lab. When implemented correctly in the future, the Moscow's security lab can play skirmish games and do research in conjunction.

This complexity of the RADICL lab necessitates implementing cyber situational awareness tools. Cyber situational awareness tools bring a possibility to view the whole RADICL network and devices all in one dashboard. This makes it so much easier for researchers and RADICL admins to resolve possible issues and contain cyber-attacks within

an area of the RADICL lab. This sort of value can be applied to small to large enterprises and similar research and training labs in other organizations.

5.4 Benefits of Situational Awareness in RADICL

From movies and media, there are many examples where researchers or scientists grow something evil that they cannot control. The research lab works with new and cutting-edge science but when this science gets out into the public it causes all sorts of harm. This is similar to why cyber situational awareness is needed in the RADICL lab. The importance of having cyber situational awareness is very crucial for the RADICL lab to continue to operate as intended. Even though RADICL is shut off from the public Internet and the rest of the world, it is still very important to be in control of what is going on, so that if something malicious is created, it can be detected first. If the RADICL lab is where cyber experts come to do research, the University of Idaho and Idaho State University want to have a good reputation and maintain their campus networks for other education and research purposes. They want to be known as the place where viruses are discovered and not where a virus got out.

This precaution should be used for undiscovered viruses in the lab and cyber-attack brought into RADICL for cybersecurity testing. There are procedures in place for managing USB drives, network connections, and any data brought into the lab. Even with testing data and testing attacks brought into the lab there might be something that the Cuckoo sandbox, a usb malware analysis tool, might not have found. New cyber-attacks are being created every day and cyber-attacks are getting smarter all the time. There could potentially even be cyber-attacks to hide from USB testing.

For RADICL to run smoothly, services and hardware need to work. Sometimes demonstrations, simulation games and research are conducted in the lab and they need certain services and hardware to be running and available to the researcher. If there is downtime from a service or hardware, less work gets done and time is wasted. For businesses and organizations, this means a loss of revenue. If a router virtual machine goes down, it might cut off all access to RADICL IT infrastructure. If a blade server goes down, that could cut off all access to VMs for a simulation game. Like businesses and organizations, these devices need to work continuously. Being cyber situationally aware helps RADICL administrators know what is down and what might have happened to it and perform quicker troubleshooting, allowing for less time lost.

5.5: Lab Implementation of Cyber Situational Awareness

There are currently four tools that have been implemented into the RADICL lab for intrusion detection and network monitoring. The four tools currently being used are Nagios, SecOnion, Wazuh agents, and RTIR. Each tool has a specific task to monitor and alert RADICL administrators of unexpected events. Each cyber situational awareness tool has a specific purpose and they all work together to make sure everything flows in a smooth and timely manner.

5.5.1: Nagios

At the RADICL lab Nagios was chosen as a way to monitor servers and computers as well as to manage IT asset inventory. Nagios is a great tool because of how widely it is used

and accepted in industry as well as being open source and free. Implementation of Nagios monitoring is on all of the computers used for testing for Red and Blue segments. Nagios is on all routers and internal servers as well as virtual machine management software such as Ovirt. Figure 5.6 shows the first page of the Nagios GUI in RADICL and Figure 5.7 displays the services of each of those hosts. Nagios also has the NRPE plugin installed on both Nagios server and the client side of each of the servers and computers.

Nagios has simple NRPE check commands written for monitoring the remote hosts. The RADICL lab has custom NRPE check commands for servers and computers. Nagios is set to check all Black zone computers, as well as all workstations in the Blue zone and in the Red zone. The RADICL is also set to check infrastructure VMs and computers like the nosuchagency, nationstateactor, and the Blue zone border gateway to monitor their state. Nagios is also set to check Ovirt and servers' hardware connected to the hypervisor engine.

There are custom email alerts for when the state of a VM, computer or server is critical. These custom scripts are in the contacts.cfg file of the Nagios server. When a device or service has become critical it sends an email alert to RTIR. How RTIR handles this is described later. The reason for this alert is for RADICL administrators to see what has happened in the RADICL lab and place this issue as a ticket in RTIR for tracking its resolution. That way administrators will be able to see up front what is wrong and to take care of the issue that is happening on that server or computer.

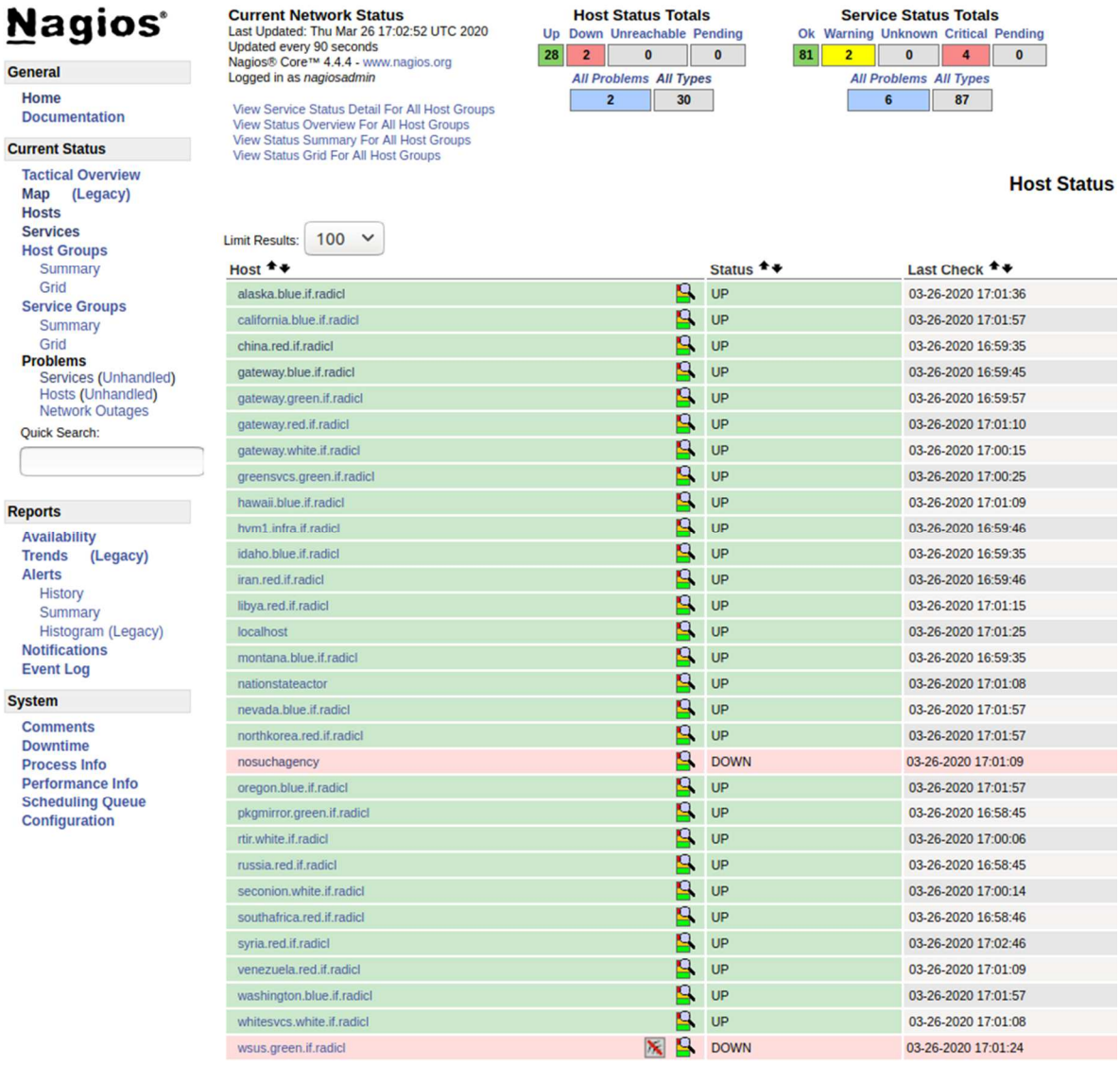

Figure 5. 2 RADICL-IF's Nagios Dashboard

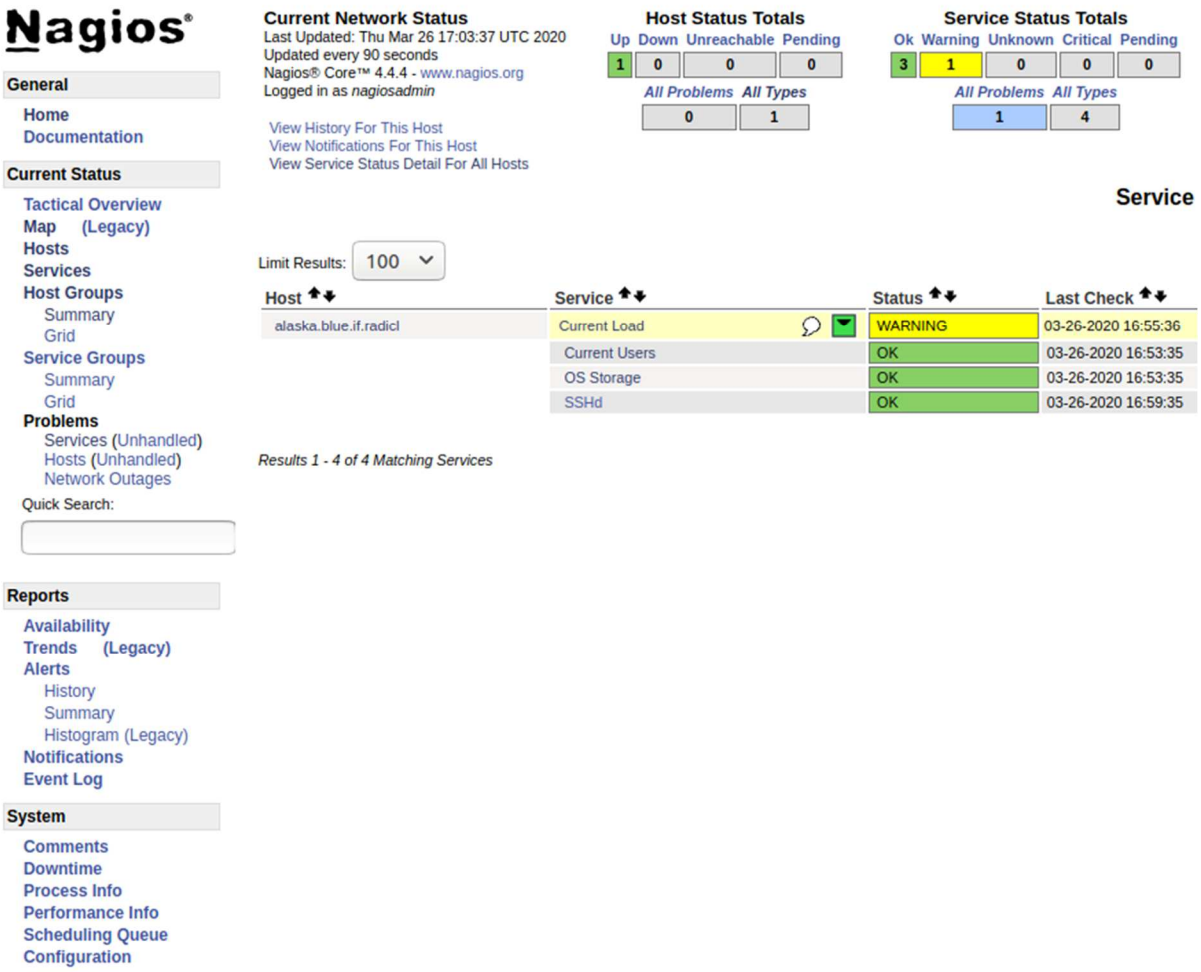

Figure 5. 3 RADICL-IF's Nagios Service Page

5.5.2: Security Onion

Security Onion monitors network traffic in the whole RADICL lab. The main goal of Security Onion in RADICL is to monitor host and network logs. Security Onion in has been set up in evaluation mode for its use case. The evaluation mode is perfect for the environment it is in since this use case is primarily for classrooms and small lab environments. Security Onion monitors network traffic and receives forwarded logs of

activity from other nodes. Other VMs, computers, routers switches and blades report activity and then Security Onion, using Wazuh, collects and processes these logs.

RADICL uses Snort as a means to monitor network traffic. Snort has rules set in the RADICL lab to look for suspicious traffic. There are Snort rules currently in place to look for commonly suspicious activity. Future rules can be set by students that might be doing projects and looking for certain network traffic. If working on a certain malware or attack, students can create specific Snort rules for that malware.

Zeek, formerly known as Bro, is also used in the RADICL lab for analyzing network traffic. As the network is monitored in Zeek it tries to understand everything about network activity in the RADICL lab. Unlike Snort, which is based on rules, Zeek looks for anomalies that are in the RADICL network traffic and tries to sift through packets to see something wrong.

Sguil is the primary source for RADICL administrators to view data from Snort and Wazuh. Sguil can also show session data from SANCP of the RADICL lab network traffic. Sguil is a database that shows alerts coming in real time for the RADICL lab. It is a very powerful asset to see most things and should be a RADICL admin's right-hand tool. Figure 5.8 shows the Sguil user interface and some of the alerts created from Snort, Wazuh, and OSSEC.

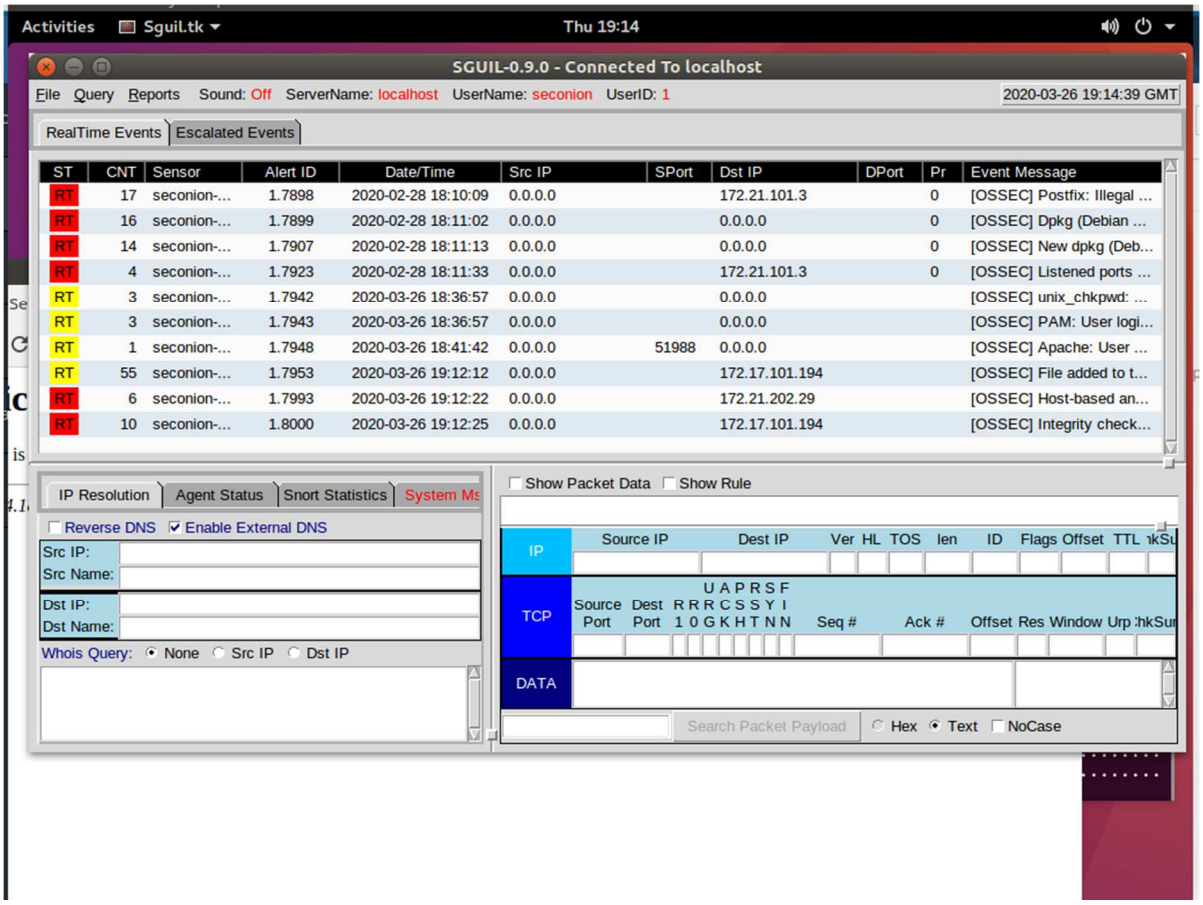

Figure 5. 4 RADICL-IF's Sguil Interface

Squert is used in the RADICL as a way to view and filter the Sguil data in the RADICL lab network traffic. It gives RADICL administrators an easier way to view alerts and data. If RADICL admins or researchers in the RADICL lab wish to see trends and query for certain traffic this is a great spot.

Kibana is used in the RADICL lab to view all alerts and logs from all sources. This tool is to view both HIDS tools and NIDS tools from Security Onion and includes Snort, Zeek and Wazuh alerts and logs. This web application is useful for RADICL admins and

RADICL operators to see more analytics on what packets were sent and what log events were generated when an attack or malware was placed in the RADICL lab.

5.5.3: Wazuh

Wazuh is being used across the RADICL lab for threat detection and integrity monitoring. Wazuh is integrated with all workstations and servers in the room. It gives RADICL administrators log management capabilities and a way to detect suspicious activity. Wazuh is included with Security Onion so its implementations are inside the Security Onion VM running in the White zone.

Signature-based log analysis is set up in the RADICL lab to accelerate threat detection. Wazuh for RADICL administrators will aggregate and analyze log data when the Wazuh agent sends logs messages to the Wazuh server. When Wazuh receives this log data it will parse it and then look for keywords such as match and priority. The priority of how severe the log is, depends on Wazuh config file set. Wazuh also looks for match to see what the message was. Kibana can also be used with the log message to view where the computer or service is located. This can be very useful for RADICL students to see log messages from computers where malware has attempted or even completed a compromise of the device or service.

Knowing if a file has been tweaked is also important for researches and RADICL administrators. Wazuh provides and monitors file integrity. If a file has been tweaked Wazuh will also record this and send this to Wazuh server. RADICL operators and researchers can select which files to monitor. When a file is changed on monitored systems Wazuh agent will send a MD5 and SHA1 checksum, file size, file permissions, file owner, content changes, and the user who changed the file to the server to report for RADICL analysis. This

provides useful insight into what a particular malware or attack might be trying to do. It also can help track down which files and where they are in the Kabana GUI.

Rootkit Detection is also provided by Wazuh for the RADICL lab. Wazuh agents in the RADICL lab periodically scan computers and servers to detect rootkits at both the user level and the kernel level. Malware will replace or manipulate operating system parts to change the behavior of the system. This is very useful for RADICL administrators to see if malware has tried to manipulate anything with an operating system.

Lastly, security policy monitoring specific to RADICL lab is also an added benefit of security in the RADICL lab. Since RADICL lab is an air locked cybersecurity lab there are certain policies in place like USB policies and network policies. The RADICL lab has USB policies in place that only RADICL approved USB devices can be plugged into RADICL lab computers. Wazuh would give users log information about if a USB has been plugged in and if the USB is approved. Another policy of RADICL lab is network packets. The RADICL lab hosts a local package mirror for computer and VM updates. If a computer or VM is getting updates from another source this could IT and cyber security professionals that there might be a hole in the firewall and Wazuh could report this for policy monitoring.

5.5.4: RTIR

RTIR is implemented in the RADICL lab. RTIR is an incident response and alerting tool for RADICL admins to know if something has gone wrong. Inside of the RADICL lab is an email server that is connected to all RADICL admins. This email is used for IT management purposes. When Nagios or Security Onion receives an alert, an email is sent to RTIR. When an email is delivered to RTIR from Security Onion or Nagios, it parses the

email and posts the alert as a ticket in the RTIR queue, visible on the dashboard page. When RADICL administrators see this alert, they can specify who this ticket is for. If, for example, an RADICL admin is in charge of IT infrastructure in the Green zone, then a ticket created by an event in the Green zone systems would be given to that particular admin. If another ticket is for Black boxes like a Blue zone workstation then that ticket would be given to that particular RADICL administrator. Figure 5.10 shows the web interface of RT when a RADICL admin logs in. Figure 5.11 shows what the RADICL admin sees when they have RTIR access and go to the RTIR tab.

RTIR has helped the flow of finding and resolving issues for incidents in the RADICL lab. For example, admins can check the Incidents Reports queue and see if there has been a problem. If there have been multiple reports sent in by monitoring tools, but they are all the same issue, they can be lumped together in one incidents reports queue. If something needs to be changed in RADICL for addressing future similar incidents, it can be placed in the Countermeasures queue. This could help track documentation and configuration changes to make RADICL more secure.

Another asset that RTIR provides is the ability to easily extract network logs and packet captures from a large list of alerts based on IP address and location. Admins can easily relate an IP address to other alerts from different monitoring tools. For example a new user being added to a Black zone workstation, RTIR can parse the alert that comes from Wazuh and provide links to the workstation's full packet capture in Security Onion, or links to the Nagios state for that system to quickly monitor and resolve other things that may be happening by the new user. This lets us organize all the tools and interfaces via one ticket that helps us track our actions to resolve the incident.

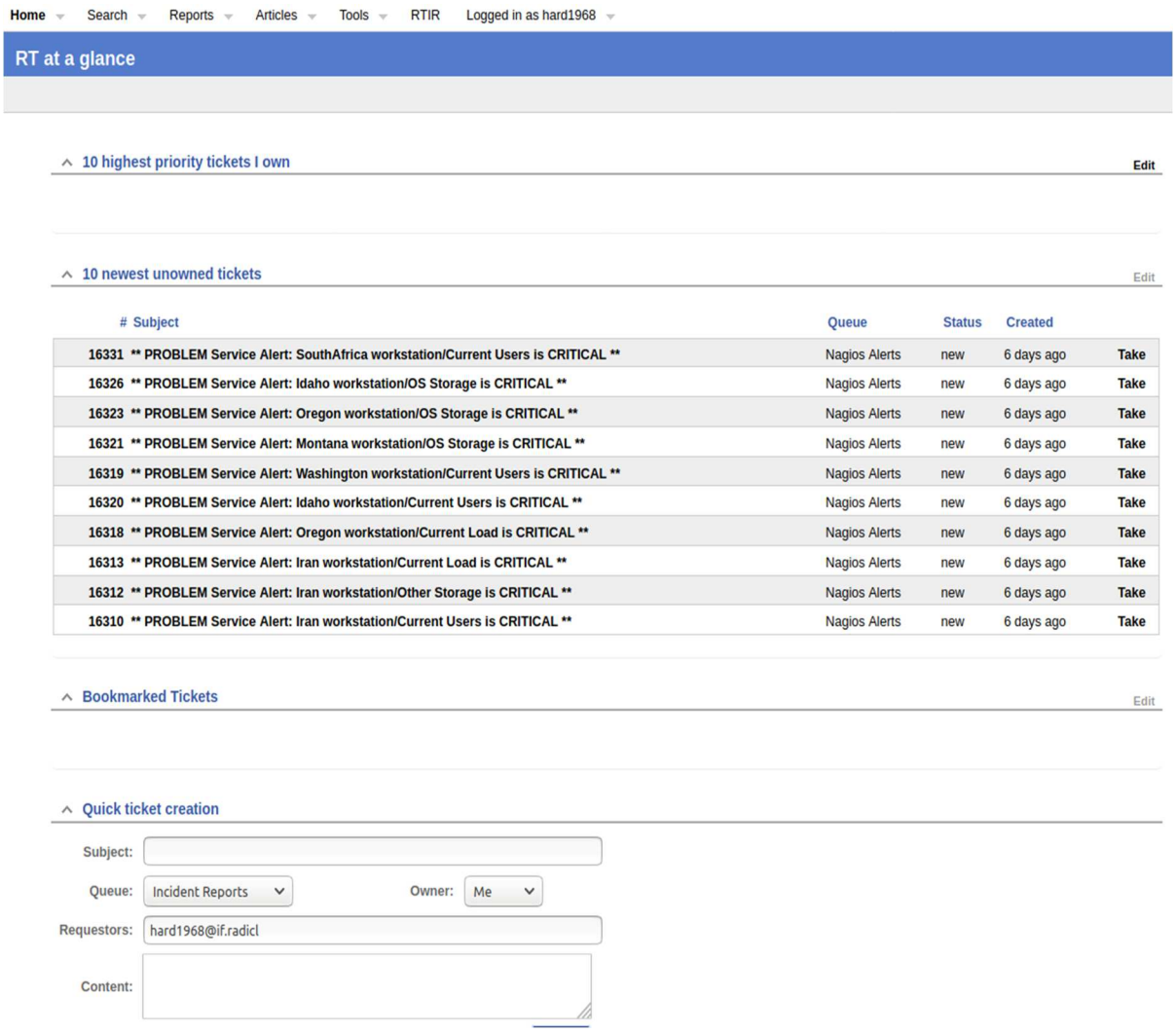

Figure 5. 5 RADICL-IF's RT Dashboard

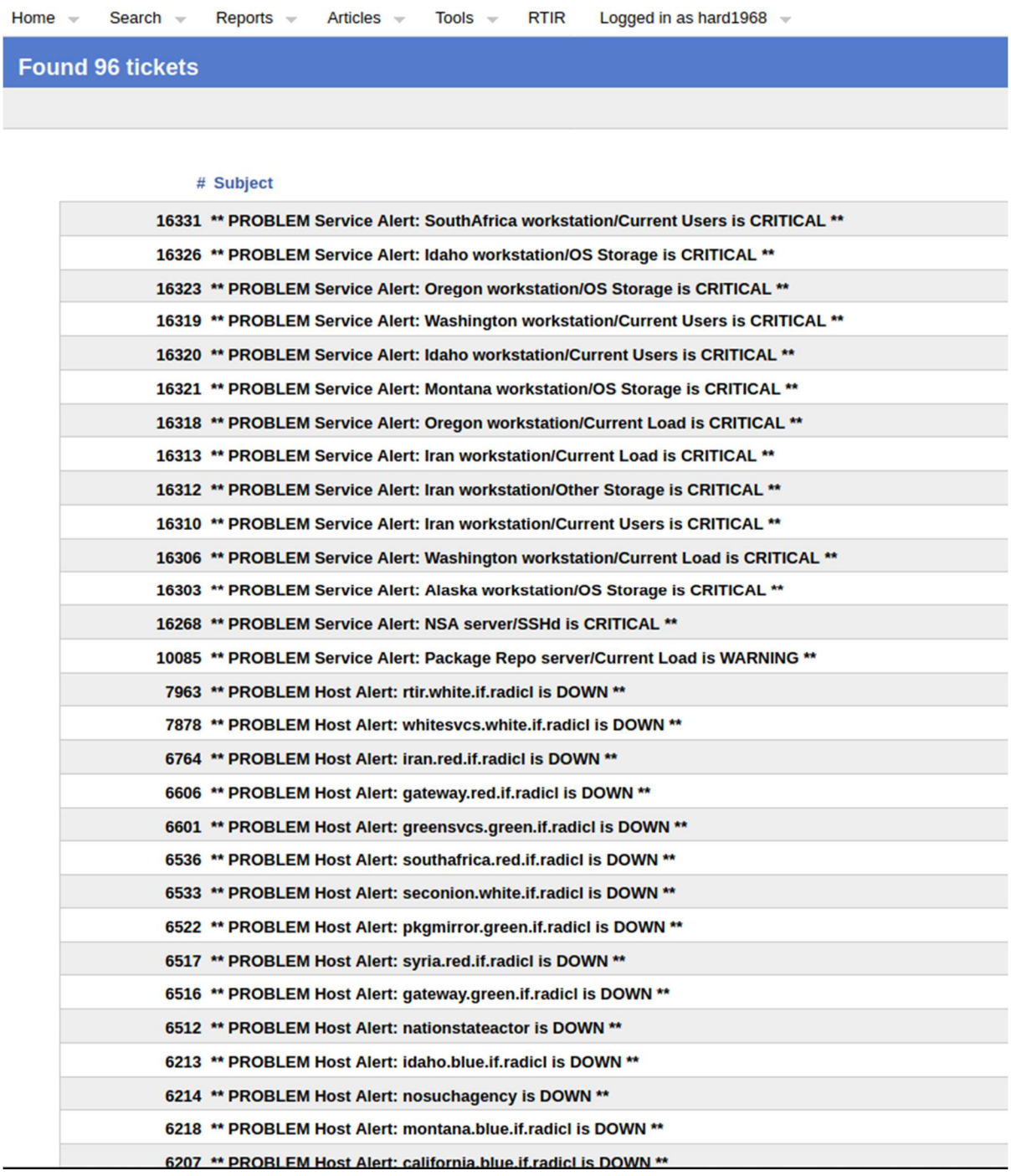

Figure 5. 6 RADICL-IF's RTIR Dashboard

RTIR is the first place that a RADICL administrator or researcher should look in the White zone because this should be the first alert of anything critical. When things have not alerted in the RADICL lab then other tools such as Security Onion and Nagios should be looked at for more detailed view of any issues going on. When checking RTIR for details on an incident RTIR admins might see different things. Since a most RADICL lab admins are cybersecurity incident response users they will see both RT and RTIR. When a RADICL admin logs into RTIR they will be greeted by the front-page dashboard of RT. There they will see tickets that have either been created by another admin or by an auto-generated email from Security Onion or Nagios. Including the ticket, they will also see what the subject is, status of the ticket or alert, the requestor, and the owner of the ticket. If an administrator wishes to create a new ticket for someone else, they can click on the top left "New ticket" and place details into that ticket such as subject, more information, and attachments, and send that ticket to the person who is in charge of it. RTIR will automatically generate detailed information about that ticket. When a RADICL admin goes to the RTIR page they will then see recent incident reports, due incidents, countermeasures, and investigations. RTIR will also include tabs on the top of the web page where RADICL admins can access detailed information about each topic. To resolve a RTIR ticket, an admin will open that ticket, and take actions appropriate to what is needed. When operating the RTIR GUI, the state of the RTIR ticket can be changed by clicking on the actions drop down list. There appropriate actions RADICL admins can take to: resolve it, investigate into it more, assign it to another admin, and add more admins. When a ticket is resolved, the RADICL admin will complete the ticket by resolving the ticket in RTIR. Other admins will be alerted that the ticket has been resolved and no further steps needed.

Chapter 6: Future Work

There are many opportunities to create new VMs to do further analysis and fine tune rules and definitions for all rules defined in the RADICL lab. When new devices are introduced into the RADICL lab, it is important to add those devices to monitor. Better integration between monitoring VMs like Security Onion and Nagios and ticketing software for incident response could also improve the cyber situational awareness in RADICL. There are so many things that can be fine-tuned or even created for future malware research. There could also be the opportunity to have other VM's created for monitoring.

There are many improvements and customizations that can be added to Nagios. There are many plugins for Nagios for specific tasks. If researchers and RADICL admins wish to add more plugins for more functionality, there are vast amount of different free plugins and add on tools for Nagios.

For Security Onion, other improvements can be added onto the current VM in the RADICL lab. Researchers and admins can apply Security Onion configurations to specific rules and policies for malware they bring into the lab. Other extra tools like Suricata and Snort can be added to the Security Onion system as another way of filtering network traffic. Snort and Suricata rules can help researchers and students filter network traffic for specific IP address or keywords.

Future work can also be used for malware detection and malware containment. When future University of Idaho students plan to do research on malware in the RADICL lab, these tools will be in place for monitoring. Say, for example, if a student were to bring in well-

known malware that was designed to hide itself in files of the hosts within the Blue zone, Wazuh would be able to do file integrity checks to look for possible malware in the Blue zone hosts. Another example could be if malware is brought in that uses network packets as its attack and in its network, packets containing malicious payloads that exploit certain versions of Windows computers. Snort could filter out these malicious packets and alert RADICL admins by sending an RTIR email. Researchers and RADICL admins can see what destruction the malware attack has done to the devices through Nagios or Wazuh logs. If researchers are bringing in newly created malware that Security Onion might not recognize, then they can fine tune Wazuh or Snort to look for this sort of activity.

Other future work that would be very interesting to see is when Red vs. Blue battles are occurring in the RADICL lab is the type of alerts and device status logs that would be created. If a Red vs. Blue administrator is watching the battle, they could possibly watch these alerts and know what is happening to the opposing side and find if the Red team has really infiltrated the Blue network.

6.1: Future Network Integration

There are many possibilities for extending RADICL to support future cybersecurity research and training efforts. Potentially, multiple different experiments and training modules may be integrated and run simultaneously. The RADICL lab needs to be dynamic and ready to quickly integrate new research projects, including new network segments and new hardware devices in addition to new virtual machines and software packages. These integrations need to be monitored and RADICL admins need to understand the current and changing landscape with comprehensive cyber situational awareness.

For example, a new network segment may be added to RADICL and included in the Yellow Zone designed for a set of Internet of Things (IoT) and operational technology devices. There are a variety of ways to connect and integrate the Yellow Zone network to the RADICL lab. This zone could be added and connected to the Blue Zone network and could be used with the "enterprise" environment to simulate an engineering or automation operation with OT and IT integration. This represents a realistic scenario as many companies have their automation or engineering VLANs connected to their enterprise network. This details of integrating various research scenarios is ultimately up to the RADICL admins and the researchers' requirements. Regardless, these new devices and software will need to be monitored to maintain control of RADICL as a whole. The White Zone will need to be able to sniff packets and receive logs from devices in the Yellow Zone, and these new data streams will need to be available in the same dashboard tools and ticketing systems used by the RADICL Admins. Devices will also need to be added to state monitoring tools such as Nagios. The situational awareness tools in the White Zone will need to be configured as well as the monitored devices in the Yellow Zone. This is also true as RADICL in Idaho Falls is integrated more tightly with RADICL on the Moscow campus over the long-distance fiber optic network.

Since IoT and OT devices now have the functionality to run over Ethernet and IP protocol and these devices are being added to industry organizations' networks constantly, further research can be done to investigate new ways to integrate the existing cyber situational awareness tools with these devices. Possibly other cyber situational awareness tools could be added to our White Zone specifically for IoT and OT devices. Examples include specialized

monitoring tools for SCADA data historians from industry providers, and specialized protocol decoders that monitor communications such as Modbus and DNP3.

RADICL could also possibly add cloud integration into its existing network. Cloud services such as Amazon Web Services or Microsoft Azure could be used to add VMs and for research and testing. The cloud allows for the ability to quickly add new VMs dynamically. A direct connection to the cloud would be needed for the ability of cyber situational awareness tools to monitor VMs in the cloud. This would need to be deployed in another specialized zone or network segment that connects the White Zone to the cloud based VM infrastructure. As long as these cyber situational awareness tools have the ability to see all devices on the new network segment, sniff packets, and collect logs, RADICL Admins should be able to maintain cyber situational awareness.

A capability that could help RADICL Admins is a pre-defined deployment package and/or checklist for researchers. When new devices and VMs are added to RADICL either via the cloud or in the Yellow Zone network, if there is a tool that could configure them dynamically for our current monitoring tools, this would greatly improve integration for future research projects. A separate tool or added functionality of these cyber situational awareness tools could be created possibly using Ansible or Puppet or another dynamic configuration tool. This could save time and reduce the possibility of errors when configuring new devices and would account for the newly added devices and VMs in the state monitoring and inventory management tools. This effort is left for future work.

Chapter 7: Summary and Conclusions

All tools introduced into the RADICL lab will be highly important assets to have. If RADICL lab is going to be an effective cybersecurity lab, the administrators need to be cyber situationally aware. This use case of RADICL can be used as an example for other research labs and small and large businesses. It can hopefully show an example of why and how important these tools are, and how they work together to create a smooth and productive flow of cybersecurity information. This thesis also provides an easy context how and why each cyber situational awareness tool is important for an organization. Cyber situational awareness is an important concept that should be used across every industry. Cyber-attacks on organizations and businesses can cost thousands to hundreds of thousands of dollars to fix. All organizations should take as much precaution to be cyber situationally aware in their cyberspace environment as possible.

Bibliography

[1] “Cyber Situational Awareness – A Systematic Review of the Literature.” *Computers & Security* 46 (October 1, 2014): 18–31. https://doi.org/10.1016/j.cose.2014.06.008.

[2] Joukov, Nikolai, Stony Brook, Nikolai Joukov, and Stony Brook. “(54) ANALYSIS OF DATA FLOWS IN COMPLEX,” n.d., 11.

[3] Jingmin Lei. “Cyber Situational Awareness and Mission-Centric Resilient Cyber Defense,” 1:1218–1225. IEEE, 2015. https://doi.org/10.1109/ICCSNT.2015.7490952.

[4] “Gale General OneFile - Document - How Legacy Code Is Exposing Business and Government Systems.” Accessed April 7, 2020. https://ida.lib.uidaho.edu:7213/ps/i.do?&id=GALE%7CA364332037&v=2.1&u=mosc00780&it=r&p=ITOF&sw=w.

[5] Conteh, Nabie Y., and Paul J. Schmick. “Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks.” *International Journal of Advanced Computer Research* 6, no. 23 (February 12, 2016): 31–38. https://doi.org/10.19101/IJACR.2016.623006.

[6] Endsley, Mica R., and Daniel J. Garland. *Situation Awareness Analysis and Measurement*. CRC Press, 2000.

[7] Endsley, Mica. “Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64.” *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37 (March 1, 1995): 32–64. https://doi.org/10.1518/001872095779049543.

[8] Sangani, Nilaykumar Kiran, and Balakrishnan Vijayakumar. *Cyber Security Scenarios and Control for Small and Medium Enterprises*, n.d.

[9] Stevens-Adams, Susan, Armida Carbajal, Austin Silva, Kevin Nauer, Benjamin Anderson, Theodore Reed, and Chris Forsythe. “Enhanced Training for Cyber Situational Awareness.” In *Foundations of Augmented Cognition*, edited by Dylan D. Schmorrow and Cali M. Fidopiastis, 8027:90–99. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-39454-6_10.

[10] “The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020 - ProQuest.” Accessed May 1, 2020. https://ida.lib.uidaho.edu:2096/docview/1614633129?accountid=14551&rfr_id=info%3Axri%2Fsid%3Aprimo.

[11] Stephenson, Peter. “SIEM: Security Information and Event Management (SIEM) Tools

Do a Lot of Things, but at the Core They Take Data from Sources and Get Useful, Actionable Information from It, Says Peter Stephenson. (PRODUCT SECTION).” *SC Magazine* 23, no. 4 (2012): 34.

[12] Newmeyer, N. “Changing the Future of Cyber-Situational Awareness.” *Journal of Information Warfare* 14, no. 2 (2015): 31–40.

[13] Bhatt, Sandeep, Pratyusa K Manadhata, and Loai Zomlot. “The Operational Role of Security Information and Event Management Systems.” *IEEE Security & Privacy* 12, no. 5 (2014): 35–41. https://doi.org/10.1109/MSP.2014.103.

[14] Suarez-Tangil, Guillermo, Esther Palomar, Arturo Ribagorda, and Ivan Sanz. “Providing SIEM Systems with Self-Adaptation.” *Information Fusion* 21 (January 1, 2015): 145–58. https://doi.org/10.1016/j.inffus.2013.04.009.

[15] “Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems - ProQuest.” Accessed April 8, 2020. https://ida.lib.uidaho.edu:2096/docview/1524881870?accountid=14551.

[16] Hock, Filip, and Peter Kortis. “Commercial and Open-Source Based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) Design for an IP Networks.” In *2015 13th International Conference on Emerging ELearning Technologies and Applications (ICETA)*, 1–4. Starý Smokovec, High Tatras, Slovakia: IEEE, 2015. https://doi.org/10.1109/ICETA.2015.7558466.

[17] AlYousef, Mutep Y, and Nabih T Abdelmajeed. “Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System’s Database.” *Procedia Computer Science*, Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 23rd International Conference KES2019, 159 (January 1, 2019): 1507–16. https://doi.org/10.1016/j.procs.2019.09.321.

[18] Rowland, Craig H. Intrusion detection system. United States US6405318B1, filed March 12, 1999, and issued June 11, 2002. https://patents.google.com/patent/US6405318B1/en.

[19] Kozushko, Harley. “Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems,” n.d., 23.

[20] *Signature-Based Detection with Snort and Suricata*. Syngress, 2014. https://doi.org/10.1016/B978-0-12-417208-1.00009-X.

[21] “Introduction — Security Onion 16.04.6.5 Documentation.” Accessed April 10, 2020. https://securityonion.readthedocs.io/en/latest/introduction.html.

[22] “Architecture Getting Started · Wazuh 3.12 Documentation.” Accessed April 10,

2020. https://documentation.wazuh.com/3.12/getting-started/architecture.html.

[23] “An in Depth Analysis of Open Source Tools: Host Intrusion Detection System, Intrusion Detection System, and Honeypots, and How They Can Protect a SME’s Network - ProQuest.” Accessed April 10, 2020. https://ida.lib.uidaho.edu:2096/docview/2305853845?pq-origsite=primo.

[24] “Overview | Elastic Common Schema (ECS) Reference [1.5] | Elastic.” Learn/Docs/Elastic Common Schema (ECS)/Reference/1.5. Accessed April 10, 2020. https://www.elastic.co/guide/en/ecs/current/ecs-reference.html.

[25] Dempsey, K L, N S Chawla, L A Johnson, R Johnston, A C Jones, A D Orebaugh, M A Scholl, and K M Stine. “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.” 0 ed. Gaithersburg, MD: National Institute of Standards and Technology, 2011. https://doi.org/10.6028/NIST.SP.800-137.

[26] Olups, Rihards. *Zabbix 1.8 Network Monitoring*. Packt Publishing Ltd, 2010.

[27] “Nagios For Monitoring Servers - ProQuest.” Accessed April 10, 2020. https://ida.lib.uidaho.edu:2096/docview/194170075/7F5108E8EAC64114PQ/2?accountid=14551.

[28] “Official NRPE Documentation - Nagios Exchange.” Accessed April 11, 2020. https://exchange.nagios.org/directory/Documentation/Official-NRPE-Documentation/details.

Olups, Rihards. *Zabbix 1.8 Network Monitoring*. Packt Publishing Ltd, 2010.

[29] “Gale General OneFile - Document - Research and Markets Adds Report: North America Security Orchestration Automation and Response (SOAR) Market.” Accessed April 11, 2020. https://ida.lib.uidaho.edu:7213/ps/i.do?&id=GALE%7CA603991571&v=2.1&u=mosc00780&it=r&p=ITOF&sw=w.

[30] Van Wyk, Kenneth R. *Incident Response*. 1st ed. Sebastopol, CA: O’Reilly, 2001.

[31] “Building a Computer Security Incident Response Team: Required Skills and Characteristics - ProQuest.” Accessed March 11, 2020. https://ida.lib.uidaho.edu:2096/docview/2177380833?pq-origsite=primo.

[32] “Computer Security Incident Response Team Development and Evolution - IEEE Journals & Magazine.” Accessed March 11, 2020. https://ida.lib.uidaho.edu:2274/document/6924672.

[33] Gërvalla, Muhamet, Naim Preniqi, and Peter Kopacek. “IT Infrastructure Library (ITIL) Framework Approach to IT Governance.” *IFAC-PapersOnLine*, 18th IFAC Conference on Technology, Culture and International Stability TECIS 2018, 51, no. 30 (January 1, 2018): 181–85. https://doi.org/10.1016/j.ifacol.2018.11.283.

[34] “RTIR 4.0.1 Documentation - Best Practical.” Accessed April 15, 2020. https://docs.bestpractical.com/rtir/4.0.1/index.html.

[35] IAITAM. “IT Asset Management Key Process Areas.” *IAITAM* (blog). Accessed April 7, 2020. https://iaitam.org/asset-management-key-process-areas/.

[36] Lecklider, Tom. “Keeping Track of What You’ve Got.” *EE-Evaluation Engineering* 56, no. 4 (April 1, 2017): 24–26.

[37] Wheatley, Malcolm. “Managing IT Assets Can Be Tricky, but the Payoff Is Real.” *Manufacturing Business Technology* 23, no. 4 (2005): 54–55.

[38] “Gale OneFile: Business - Document - SECURITY: WannaCry Had Wide Impact; Recent Ransomware Attack Hit Much Harder than Initial Estimates; NHS Facilities, Two U.S. Healthcare Systems Are among Its Victims.” Accessed March 9, 2020. https://ida.lib.uidaho.edu:7213/ps/i.do?&id=GALE%7CA499782077&v=2.1&u=mosc00780&it=r&p=ITBC&sw=w.

[39] Stone, Michael, Chinedum Irrechukwu, Harry Perper, Devin Wynne, and Leah Kauffman. “IT Asset Management: Financial Services.” Gaithersburg, MD: National Institute of Standards and Technology, September 2018. https://doi.org/10.6028/NIST.SP.1800-5.