GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

Security Tools for the SMB and SME Segments

GIAC (GCIA) Gold Certification

Author: James Waite, jswaite@zoominternet.net
Advisor: Adam Kliarsky
Accepted: August 23rd, 2017

Abstract

Modern small and medium businesses (SMBs) operate with limited staff and budgets. Today's business environment requires businesses to do more with less. Businesses also have information that they need to protect. This protection is either mandated by law (HIPAA), industry requirements (PCI) or best practices (NIST). What are the recommended policies and tools an SMB should have in place to provide adequate and responsible information security? What tools should an SMB concentrate their time, effort and money towards? Should these tools be network-based tools, monitoring both inline and spanned traffic? Should these tools be end point tools that provide the same functionality and minimize the network tool components? Or should there be a mix of tools? Are certain tools required on end points, in the network or both? What are an SMB's regulatory requirements and how does this affect the choice in tools? These are the difficult questions that require thoughtful, concise and researched guidance.

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

1. Introduction

Information Security organizations and professionals face many challenges in today's business environment. These challenges are financial; Governance, Risk, and Compliance; vendor overload; what assets to protect; the plethora of tools sets and toolset integrations to allow easier intrusion and incident analysis. The concept being addressed in this paper is what tools should an information security group or person concentrate their efforts to maximize their security posture. These issues are driven by other issues that tend to fall into five main areas.

The first area of interest is financial: budgets for staffing, tools, and training. The second area is Governance Risk and Compliance (GRC): applicable laws, government regulations, and industry regulations. Third is vendor overload; sometimes there are too many vendors with differing philosophies and tools. The fourth area of challenge is what assets to protect with what tools. Finally, there are the tools themselves: either too many, not enough, the wrong tools or other issues with tools.

Financial issues in the form of budgets affect several areas. The first area is staffing. Is there proper staffing to run an information security program? Another area affected by budgeting is the ability to purchase the tools that are needed. Finally, budgeting affects training, is there adequate funding to invest in staff development and tools training?

The government has laws and regulations that pertain to various industries such as finance, insurance, and health care. Industry trade groups also have compliance issues that may pertain to these and other industries. These issues affect a business' Governance, Risk and Compliance programs requirements. Some businesses may not have an established GRC program.

Vendor overload is another issue of consideration. Multiple vendors sell the same or similar products. There are also multiple vendors in a product/solution space that can have differing philosophies about how to resolve the problem and are selling products with differing capabilities and functions.

Financial issues, GRC issues and vendor issues; the next big question is what assets to protect. What protections are statutory? What protections are driven by

© 2017 The SANS Institute Author retains full rights.

industry best practices? What protections are required by certain non-governmental agencies? All these issues and others discussed so far lead to tool confusion.

The Information Security community has a plethora of tool sets. Some free and open source while others are commercial. Many tools duplicate others or have more or less functionality compared to others in their category. What tools are absolute necessities? What drives the decision on which tools to use and what to protect?

Finally, multiple tools from multiple vendors and tools from the same vendor, how do they integrate and communicate with each other? Are there integrations that will enable a single or reduced number of tools to correlate and cross-correlate information when trying to analyze if there has been an intrusion or incident.

The goal is to review these areas and their impact on what tools to choose. An additional consideration will be what has been discovered by talking to front line information security practitioners, research of published articles and research of published government resources.

In the end, a "Top Ten" list of the tool type/category will be provided. The appendix will include the raw results of readings and interviews to show what tools were cited the most as required.

2. The Challenges to our selection of Information Security Tools

The decision of which tools to select to secure our businesses and enterprises is challenging in today business environment. We have multiple pressures affecting tool choice. These are financial; governance, risk, and compliance, the tools and tool type themselves, tool set vendors, the decision of what assets to protect and what integrations and types of integrations exist between the tools. An additional point to consider is: What is a tool?

For the purposes of this discussion, a tool will be defined as Any application or hardware (traditional information security tools such as Intrusion Prevention Systems

© 2017 The SANS Institute Author retains full rights.

[IPS], firewalls anti-malware, etc.), compliance programs, processes, research materials or training that affect a business's information security posture.

2.1. Financial Challenges

All businesses, whether a small business with a few hundred employees to a medium size business with fourteen hundred employees, have limited capital and must decide where budget dollars are best allocated. Some businesses may have limited capital to spend outside of core business functions.

This limited funding may lead to improper staffing levels for an information security department. This lack of staffing can impact what tools are purchased. Is a tool worth purchasing and implementing if there is insufficient staff to monitor and manage it?

Another possibility is there is appropriate staffing, but there is not funding for the needed information security tool sets. This can lead to looking at alternatives to commercial software such as free and open source tools. Free and open source tools may not exist as a viable replacement for a commercial tool or may not have the needed functionality.

2.2. Governance, Risk and Compliance Challenges

Different organizations have varying governance, risk and compliance needs. For example, health care organizations have Health Insurance Portability and Accounting Act (HIPAA) compliance issues and requirements. Health care organizations that accept credit cards for payment also have Payment Card Industry (PCI) compliance issues to deal with. Publicly traded companies have compliance requirements under the Sarbanes-Oxley Act of 2002 (SOX). Financial institutions have issues and concerns under the Gramm–Leach–Bliley Act (GLBA) and if publicly traded also under the Sarbanes-Oxley Act.

Businesses that do not have or have minimal regulatory requirements may not consider information security as high a priority as other business needs or functions. This lack of regulatory requirements can cause needed tools to not be funded for purchase. It may also cause staff to look at free and open source tools as replacements for tool sets

© 2017 The SANS Institute Author retains full rights.

when there is lack of funding. For certain types of tools, there may not exist a free and open source tool equivalent or the tool may exist but not be up to the performance and quality desired. Many organizations prohibit the use of free and open source software because of a perceived lack of quality or support options.

Enterprises that do have specific regulatory requirements may dictate and fund only those tools which are required for compliance. Additional funding for tools which are not required but may be industry best practices may not be available. This too may cause staff to look at free and open source tools as replacements for tool sets for which there is lack of funding or no specific regulatory requirements.

2.3. Vendor Overload Challenges

While the crux of this discussion is focusing on tools and tool sets, a driver of these concerns and confusion are the vendors in the information security space. While there is commonality in philosophy among vendors in market verticals, there are also philosophical differences. There are also philosophical differences between vendors selling the current state products and those vendors who believe there is a new way to secure assets and are breaking with old philosophies.

Vendors in the perimeter protection vertical may have a philosophy of best of breed products. This can lead to businesses to purchase an intrusion detection/intrusion prevention appliance, a stateful packet inspection firewall, an application firewall and an internet content filtering appliance. Another vendor may follow a unified protection device philosophy. This philosophy can combine these functions either into fewer appliances or one appliance.

Another major area that can be problematic is shifting philosophies of protection. At the endpoint, is traditional enterprise security suites that include antivirus, anti-malware, phishing protection, application whitelisting, firewalling and IPS appropriate? Will the new Endpoint Detection and Response (EDR) products suffice? Is this behavior-based anomaly detection and protection sufficient? Should there be a combination of these tools in use?

© 2017 The SANS Institute Author retains full rights.

Another potential issue is the sheer number of vendors in the information security tool set space. Some vendors may focus their products on the endpoint, others at the network perimeter, while others on the internal network. Some vendors may espouse a partial or full multi-layer approach. This can be endpoint protection, perimeter protection, or internal network protection or a combination of all three. These vendors may also vary in their protection toolsets.

Figure 1 is a sample of some of the many CyberSecurity firms[12]. This sample is the top twenty-nine by market capitalization per Bessemer Venture Partners.

Absolute Software Technologies Ltd.	Barracuda Networks Inc CyberArk Software, Ltd.	Check Point Software F-Secure
FireEye Inc.	Fortinet Inc.	Gemalto
Guidance Software	Imperva Inc.	Imprivata Inc.
KEW Holding Corp.	LifeLock	Mantech International Corp.
MobileIron	NetQin Mobile Inc.	Palo Alto Networks
Proofpoint	Qualys	Radware Ltd.
Rapid7	SecureWorks Corp.	Sophos
Splunk Inc.	Symantec Corp.	Trend Micro Inc.
VASCO Data Security International Inc.		VeriSign Inc.
Zix Corporation		

Figure 1 A sample of the number of CyberSecurity firms in existence that can cause vendor overload.

Some vendors may be anti-malware only, others may be anti-phishing, others data loss prevention and other intrusion detection/prevention systems. Some vendors may sell perimeter and network tools but their main focus may be enterprise endpoint protection suites that cover anti-malware, intrusion detection/prevention, data loss prevention, endpoint encryption and application control/whitelisting.

All of these vendor issues are also clouded by the vendors claiming best of breed status and superiority to other vendors, products or protection philosophies.

© 2017 The SANS Institute Author retains full rights.

2.4. What Assets to Protect Challenges

Another aspect needing thorough consideration and deliberation before choosing information security tools is determining what assets to protect. There are multiple aspects that will impact tool set selections. Some of these issues are regulatory requirements (HIPAA), industry requirements (PCI), industry best practices (NIST) and vendor philosophies and products.

Various Federal, State, and local regulatory requirements dictate what must be protected or have compensating controls in place. These requirements include endpoint protections such as anti-virus and anti-malware. Also required may be perimeter protections such as firewalls and intrusion detection and prevention. Another requirement may be and frequently is encryption of data at rest or in motion (across internal networks or the internet).

There are also industry requirements that dictate what assets are to be protected and how they are to be protected. An example is the Payment Card Industry requires a firewall at all internet and demilitarized zone (DMZ) connection points. Also, PCI requires a PCI zone on a network that is protected by a firewall and monitored with monitoring tools. These requirements dictate some of the tool types required such as firewalls. Also dictated are monitoring tools which can be either monitoring with real time network monitoring systems, log monitoring with a Security and Incident and Event Management tools or log querying an alerting via a log management system among others.

An additional area of importance but not legally binding are industry best practices. Industry best practices hold a layered approach to security and suggest that all aspects of an enterprise are protected. These traditional protection methods start at protect the perimeter (wide area links and the internet links), proceed to protecting the internal network and then the end points. This can involve firewalls at the perimeter, on internal network segments, and at the endpoints. These best practices can also apply to antivirus/anti-malware, intrusion detection/prevention, data loss prevention and internet traffic filtering at one or more of these layers of the enterprise.

© 2017 The SANS Institute Author retains full rights.

2.5. Tool Set Challenges

Finally, a critical but not necessarily obvious obstacle when choosing which tool sets to use, are the tool sets themselves. There are choices between peer tool sets, choices between old and new philosophies of point protection tool sets, tools based on existing protection philosophies and newer protection philosophies and tools that duplicate some functionality of other tools.

One of the challenges when choosing any tool set is choosing among the tools in the class. It is common for traditional enterprise endpoint protection suites to contain antivirus, data loss prevention, firewall, intrusion detection and prevention, and application whitelisting. Or possibly fewer or additional tools as part of the suite. The trick is to choose the tool that best suits your environments needs, or to only implement the required components. Figures 2 and 3 are sample screens of an enterprise security suite showing in-suite integration of tools.

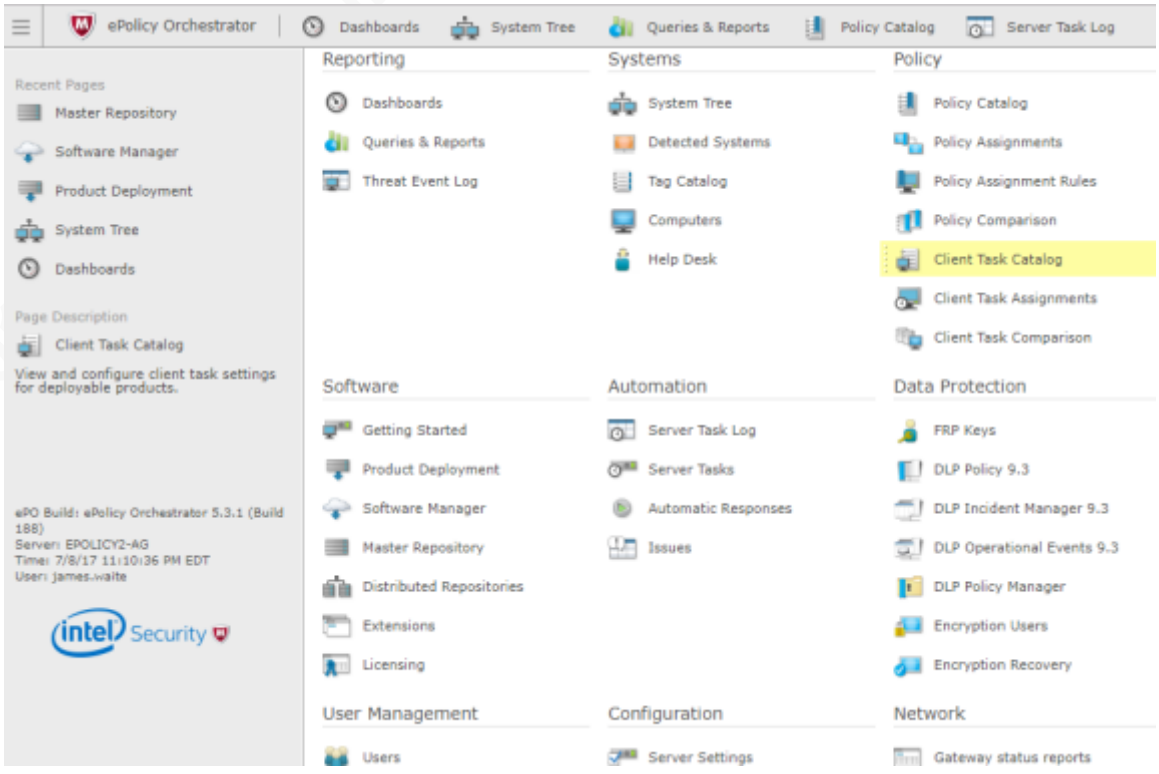
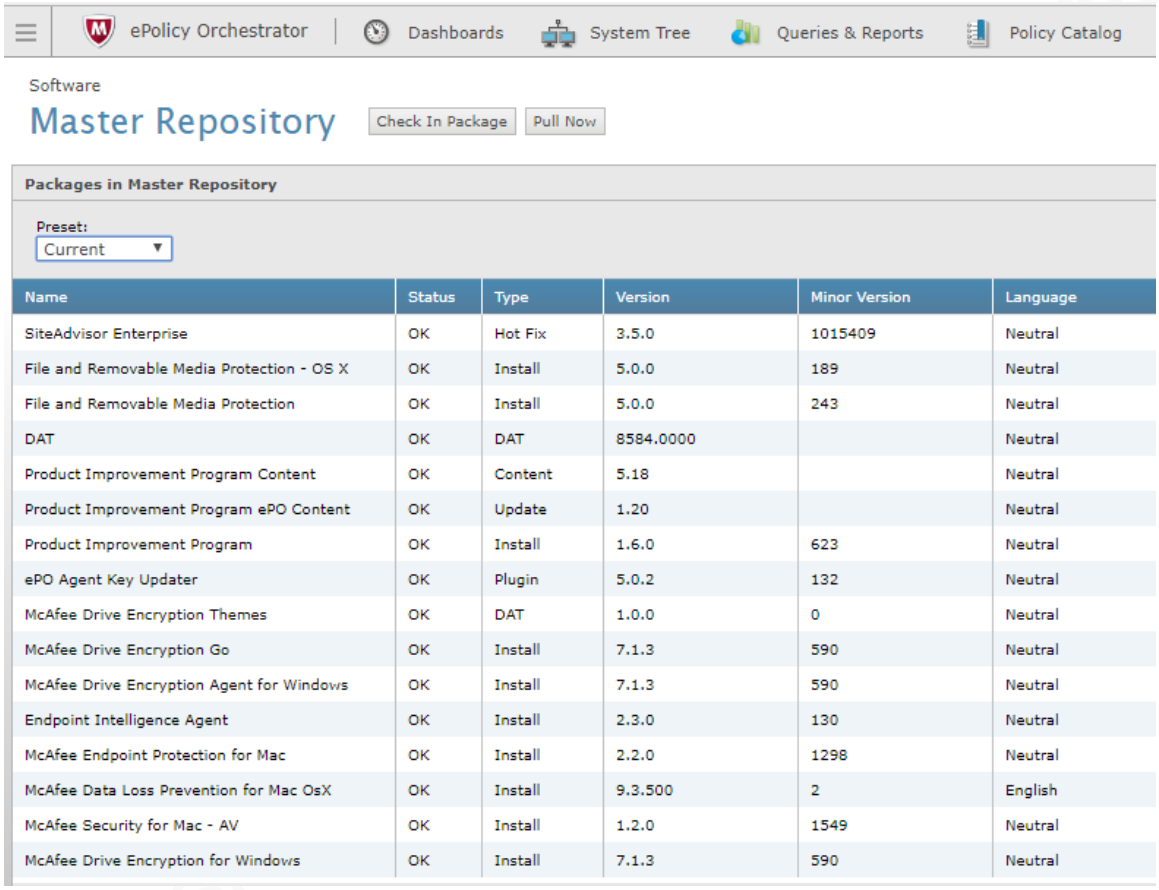


Figure 2 Screen shot of an Enterprise Security Suite with multiple tools integrated into the suite.

© 2017 The SANS Institute Author retains full rights.



Name	Status	Type	Version	Minor Version	Language
SiteAdvisor Enterprise	OK	Hot Fix	3.5.0	1015409	Neutral
File and Removable Media Protection - OS X	OK	Install	5.0.0	189	Neutral
File and Removable Media Protection	OK	Install	5.0.0	243	Neutral
DAT	OK	DAT	8584.0000		Neutral
Product Improvement Program Content	OK	Content	5.18		Neutral
Product Improvement Program ePO Content	OK	Update	1.20		Neutral
Product Improvement Program	OK	Install	1.6.0	623	Neutral
ePO Agent Key Updater	OK	Plugin	5.0.2	132	Neutral
McAfee Drive Encryption Themes	OK	DAT	1.0.0	0	Neutral
McAfee Drive Encryption Go	OK	Install	7.1.3	590	Neutral
McAfee Drive Encryption Agent for Windows	OK	Install	7.1.3	590	Neutral
Endpoint Intelligence Agent	OK	Install	2.3.0	130	Neutral
McAfee Endpoint Protection for Mac	OK	Install	2.2.0	1298	Neutral
McAfee Data Loss Prevention for Mac OsX	OK	Install	9.3.500	2	English
McAfee Security for Mac - AV	OK	Install	1.2.0	1549	Neutral
McAfee Drive Encryption for Windows	OK	Install	7.1.3	590	Neutral

Figure 3 Screen shot of an Enterprise Security Suite with multiple tools integrated into the suite.

Another aspect of one tool set versus another on the same platform is a philosophical difference. Does one implement a traditional enterprise wide endpoint security suite or use the newer endpoint detection and response (EDR) tools instead of traditional anti-malware. Is it best to implement traditional endpoint security suites along with the newer endpoint detection and response tools?

Another challenge of tool set selection is personal and corporate philosophy regarding tools. Is it best to go best of breed or to choose a unified protection product? An example of this philosophical choice is perimeter protection. Is it best to choose the best of breed approach and choose a traditional stateful packet inspection firewall, an intrusion detection and prevention system, an application firewall and internet traffic filter appliance or use a next generation firewall appliance that may contain several or all of these features and possibly include additional features such as appliance based anti-

© 2017 The SANS Institute Author retains full rights.

malware detection and prevention tools? Figure 4 is a sample screen showing a multi-function product performing IDS / IPS and URL filtering.

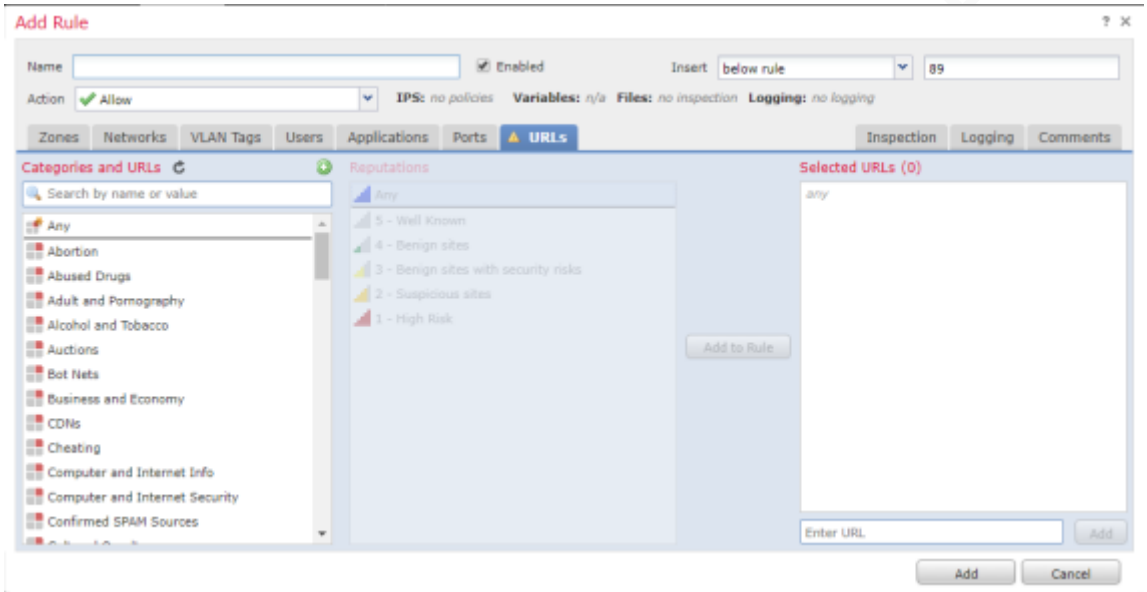


Figure 4 Screen shot of an Enterprise IDS / IPS system with URL filtering tool integrated into the product.

Finally, there may be overlap among the various tools chosen. It's possible an intrusion detection and prevention system may also include internet traffic filtering. This may duplication functionality in a separately chosen internet traffic filtering appliance. Then it must be asked, with these duplicated functions, are they equal in performance where one can be eliminated? Is the combined appliance functionality lesser than the standalone appliance but good enough for use to eliminate the standalone appliance?

2.6. Tool Set Integrations

If the challenges of funding and staffing are met, and progress is advancing to making a decision on the GRC program structure; a tool set or multiple tools can be chosen. A major issue for analysts at this stage for tool choices are the interoperability and integrations of tools and their functions. These integrations and interoperations give security analysts the ability to use fewer tools to perform their job. Some important interoperability features are logging, APIs and direct functional integration.

Logging is an important feature for analysts to have in their security tools. Logging lets various security tools either log directly to a log server or via an intermediate logging agent. This gives analysts a central location to query and search

© 2017 The SANS Institute Author retains full rights.

logs for possible events to research further to determine if there is an incident. Figures 5, 6 and 7 are three samples of a tools integration of receiving and sending logs.

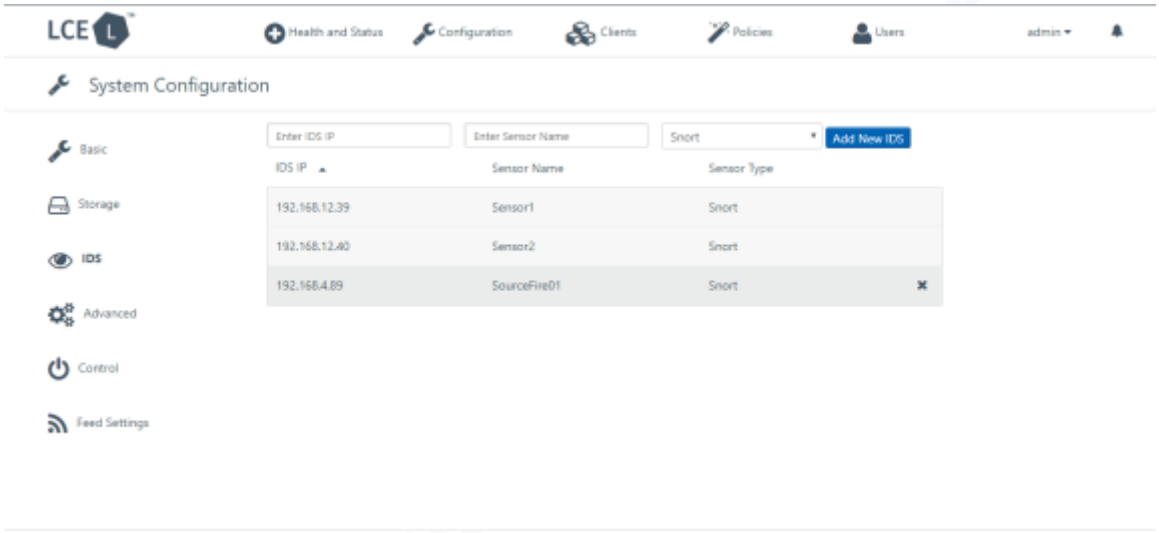


Figure 5 Screen shot of a logging system able to receive and decipher foreign security device logging natively.

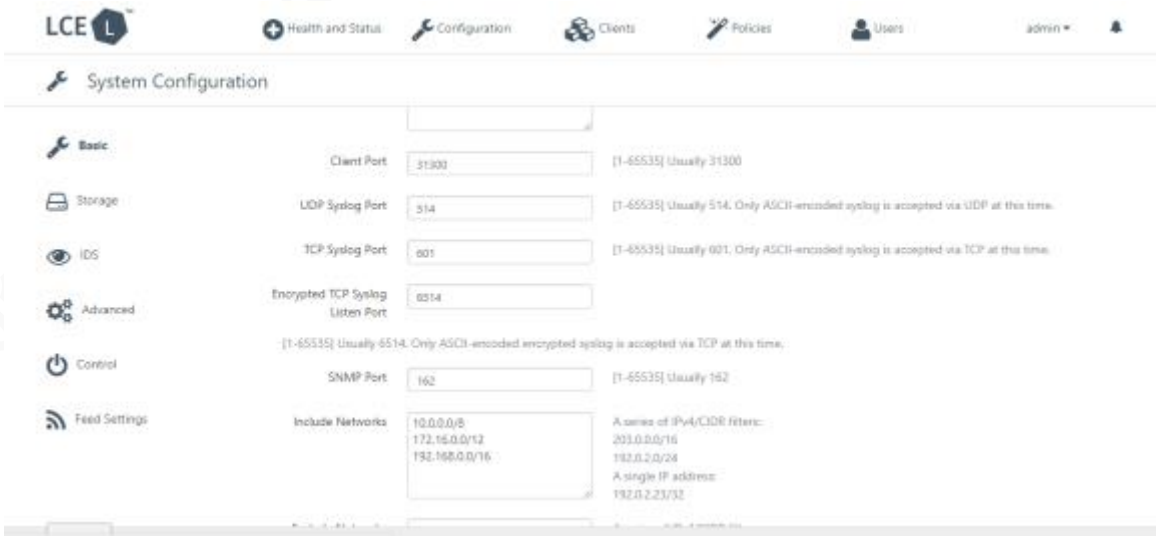


Figure 6 Screen shot of a logging system able to receive and decipher SYSLOG data natively.

© 2017 The SANS Institute Author retains full rights.

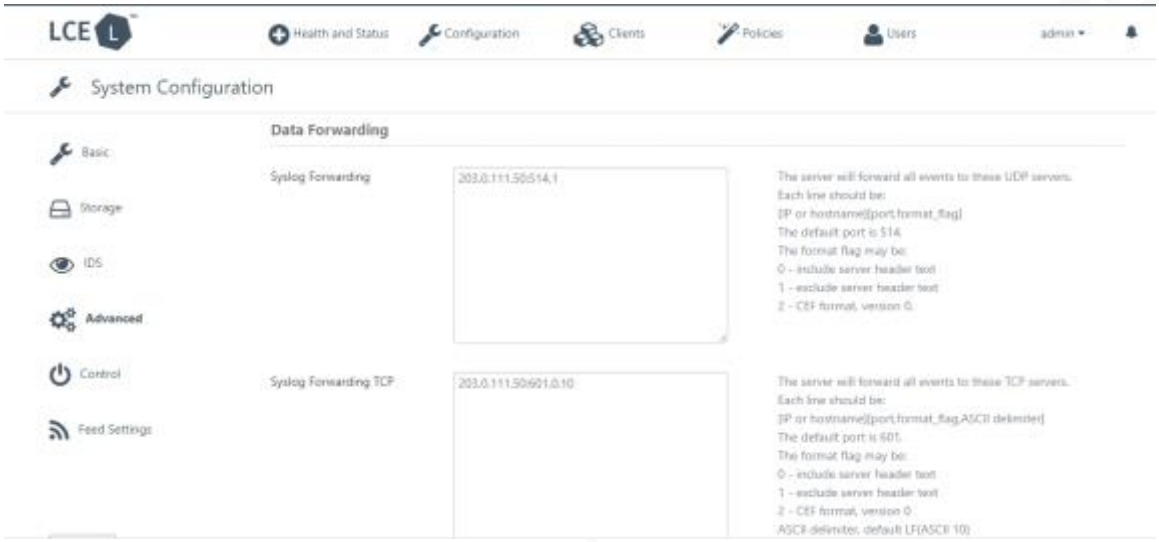


Figure 7 Screen shot of a logging system able to forward system logs to other systems.

Also important is direct function integration in vendor's tools or between vendor tools. This integration allows for such feature as native decoding of log and event messages (such as Snort or Suricata and their ability to directly decode vendor logs) and passing of scan data directly to other tools for automated analysis. Figure 8 illustrates an example of a logging tool aggregating and correlating data from disparate tools.

Figure 8 Screen shot of a logging system able to decipher and correlate native and foreign system logs.

Another important function some products offer is an Application Programming Interface (API). Many vendors publish open APIs for their tools, which lets other vendors directly call features or pass information to other products. This is useful if a

© 2017 The SANS Institute Author retains full rights.

tool has the capability to pull data from another product to either import the data or to use it to perform actions. An example would be a penetration testing tool (or a penetration tester writing a script) using the API of a vulnerability management tool to pull a list of assets to test or choose asset to without having to rescan an entire network. Another example would be using vulnerability management program to do a vulnerability assessment scan and use an API to pull assets to further test those with critical vulnerabilities. Figure 9 is an example of an API published by a vendor for use by other vendors or customers.

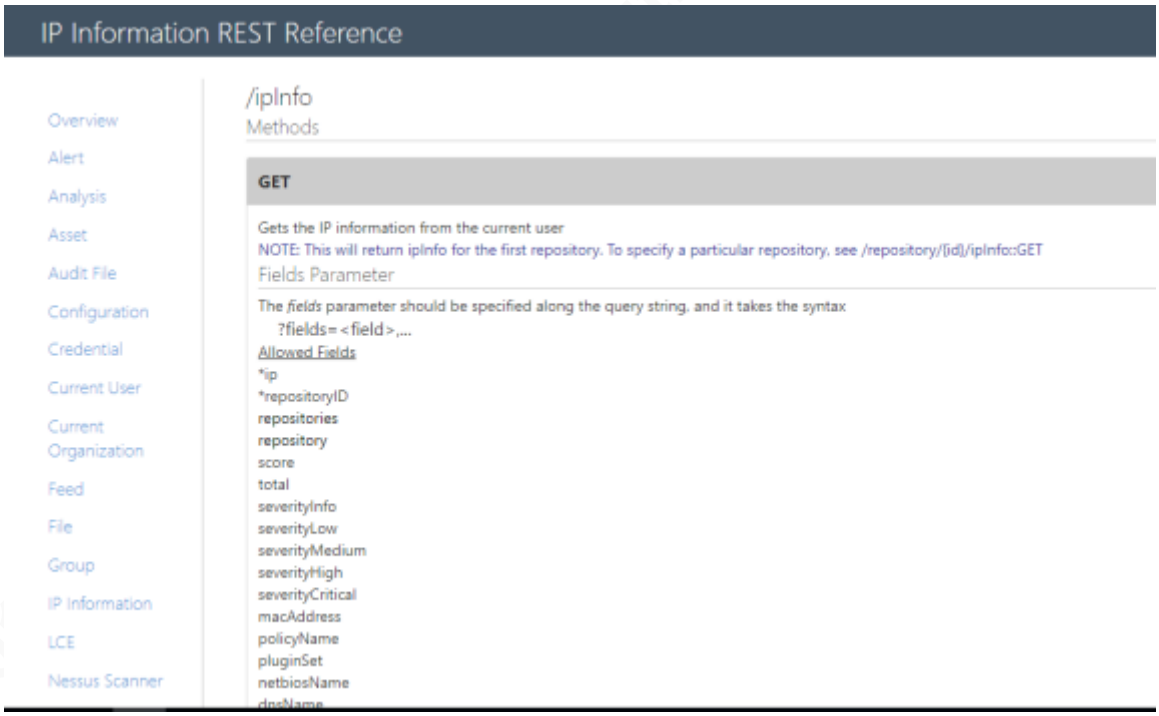


Figure 9 Screen shot of a security tool with published APIs to enable integration with other tools, applications or scripts.

3. Research, methods and the results

The research for this paper uses multiple source materials including training courses, internet sources and personal interviews with information security practitioners and resellers. The sources are overall representative of the general recommendations and trends being presented.

© 2017 The SANS Institute Author retains full rights.

3.1. Research methods and sources

The methodology used falls into two main areas: read and review printed sources, and one on one interviews with information security professional working in the field either as frontline professionals or business partners. In both instances, the results are documented and divided into six major categories.

Several sources of information were used to gather the data to compile these results. The first class of material is various information security training courses. The second class of research material is internet based resources. The internet based resources fall into two main categories: Industry/trade websites and U. S. Government websites. The third class of research materials is information security professionals working in the field or information security business partners.

3.2. Training materials trends results

The training material results are limited in quantity to readily accessible materials that fit the objectives of this paper. While training material resources researched are limited in quantity, they are nearly identical in tools that should be used to secure businesses. The training materials trend towards recommending all security tools at all possible layers should be implemented where feasible. See Appendix 2: Training course survey result for detailed results.

3.3. Internet research trends results

The internet research sources results are generally representative of what is searchable and fit the objectives of this paper. Articles that were specific to one segment of information security practices, such as web application security, we not used. The internet material resources researched are varied in results but there are five noticeable trends for tool recommendations. These tools are endpoint patching, encryption, and malware. Next is network and perimeter firewalls, whether traditional stateful packet inspection or next generation firewalls. The last general trend is authentication services. See Appendix 3: Internet research survey results

© 2017 The SANS Institute Author retains full rights.

3.4. Individual Interview Trends Results

The personal interview sources results are generally representative of presentations and discussions observed over the years. All interviews fit the objectives of this paper as they are the viewpoints of the people being interviewed. The personal interview source results are varied, but there are generally consistent with each other and trend towards matching up with the training materials trends for tool recommendations. See Appendix 4: Personnel interview survey results.

4. Results

Up to this point the discussion has be the about the challenges to information security tool selection, the methods of research and the sources and the presentation of the raw data by research source. Attached as an appendix is the complete research results of all categories. From this research, the responses were totaled for each tool. Below is a top ten list from 1 to 10. Included in this list will be a brief commentary regarding the tool. For tools listed with an equal number of results, there is no particular order of preference for the listing.

4.1. Information Security Tool 1 - Firewall - Network / Perimeter Security - 18 responses

The most common response and number one recommended tool to implement is a perimeter and network based firewalls. The discussion and research leaned towards a next generation firewall, but firewalls of any type are a recommended must-have first line of defense.

Firewalls are the first line of defense in keeping intruders out of your network and permitting into and through your network the traffic desired. Firewalls are a quick line of defense to block traffic (individual IP addresses or whole subnets) inbound to and outbound from your businesses networks. Analysts should ensure their firewall can show adequate logging capability (see figure 10 below) for live analysis as well as long term logging (such as syslog) for more in-depth analysis and forensics.

© 2017 The SANS Institute Author retains full rights.

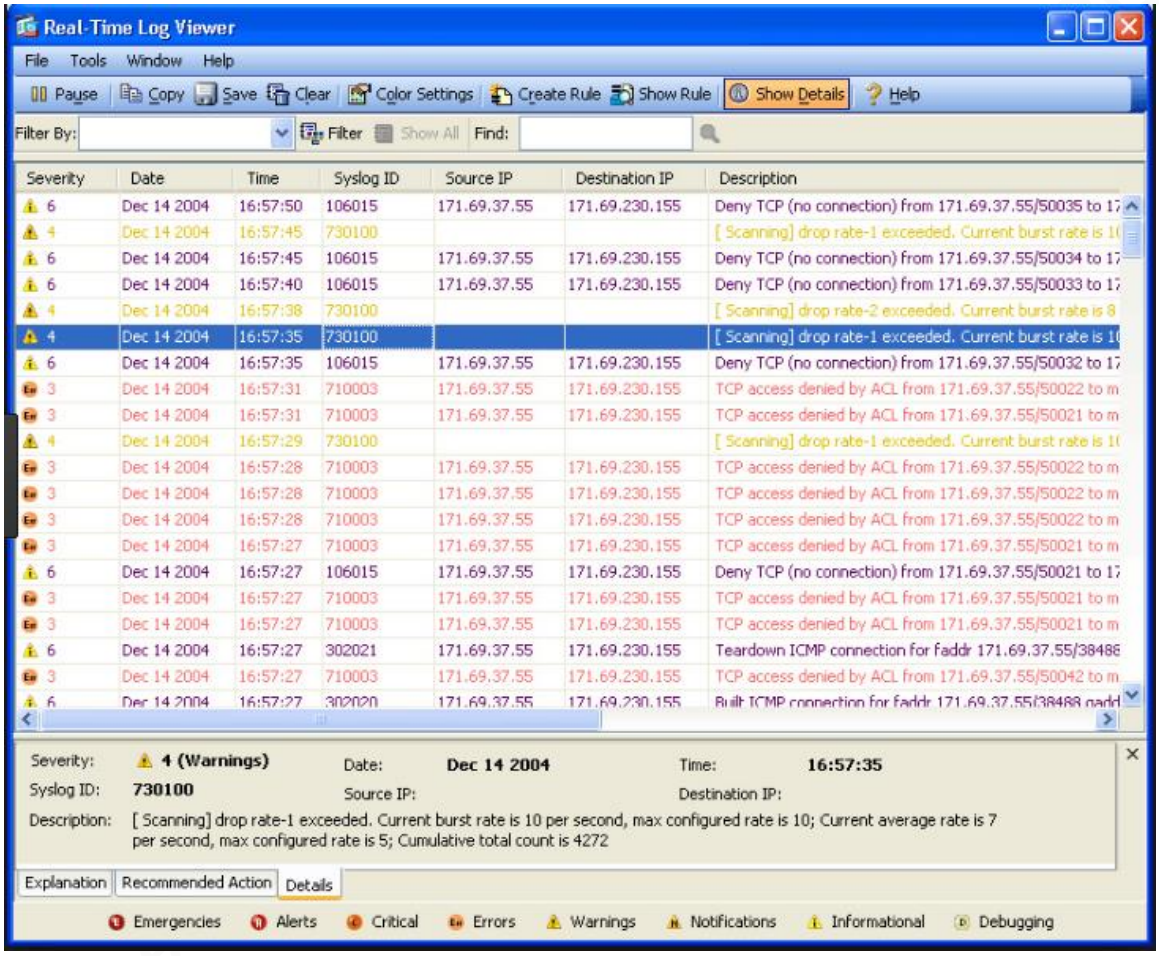


Figure 10 Sample firewall traffic logs for intrusion analysis

4.2. Information Security Tool 2 - Anti-Malware - End Point Security - 17 responses

The second most recommended security tool to implement is endpoint anti-malware software. There will be attacks that a firewall (be it a traditional firewall or a next generation firewall) may and will miss.

End point anti malware software is your second line of defense. There may be 0-day malware or other malware on infected web sites or on phishing emails that firewall rules and software may miss. If you are running a traditional firewall without malware analysis features these will be missed and the end points must have tools to scan and remove these threats.

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

An endpoint anti-malware solution should provide a central management and monitoring system (see figure 11 below) to assist in determining what malware is in the environment and what systems and how many it is affecting.

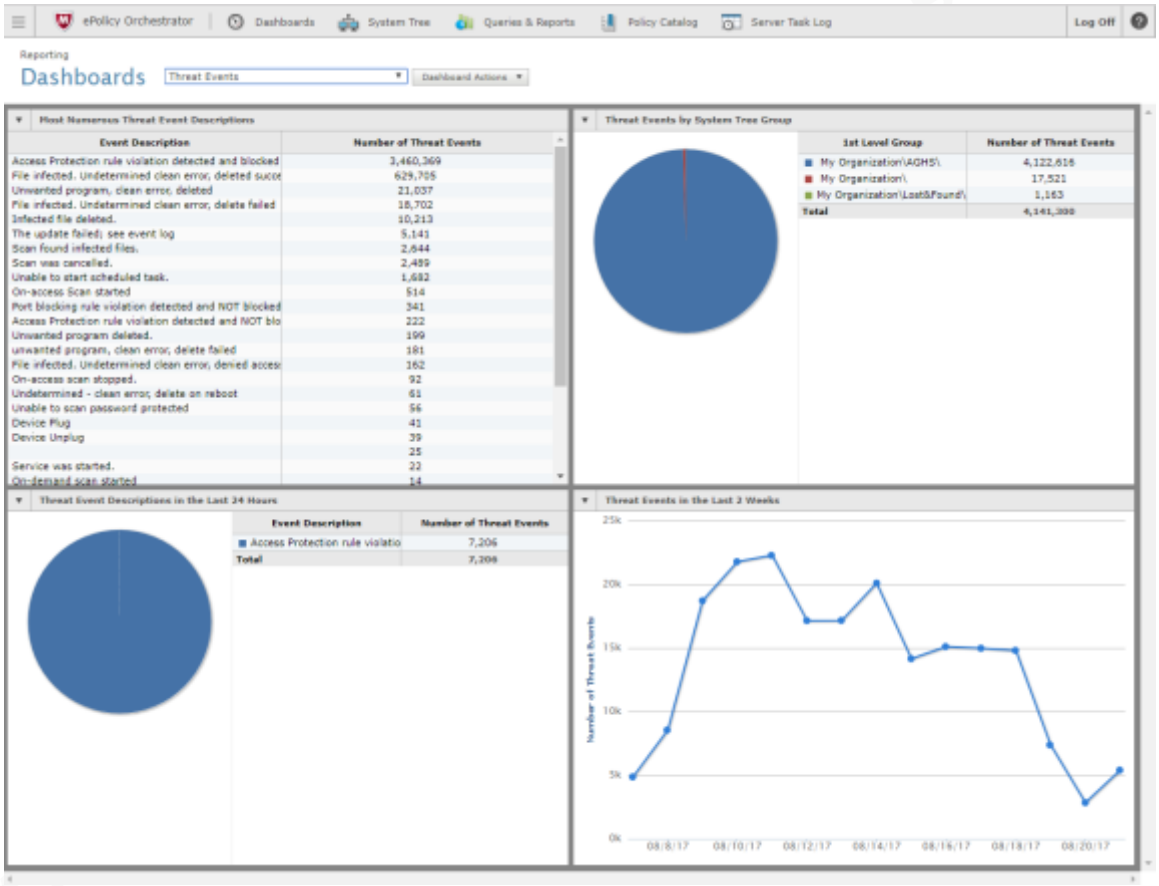


Figure 11 Endpoint malware management interface

4.3. Information Security Tool 3 - Network / Perimeter Security: Intrusion Detection / Prevention Systems - 14 responses

The third tool recommended for use is a perimeter/network based Intrusion Detection/Prevention System. This is a critical tool as it will catch malicious traffic that firewalls are not designed to catch.

Intrusion Detection/Prevention is designed to monitor inbound and outbound traffic, analyze it and detect and block attacks based on short term and long term traffic patterns. Some newer next generation firewalls have this functionality build in but using a different vendor and stand-alone IDS/IPS will provide detections another device may miss.

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Figure 12 shows an example of an IPS connection events. These events will assist an analyst in determining intrusion events that may not be blocked. This will allow firewall and IPS changes to be made as compensating controls.

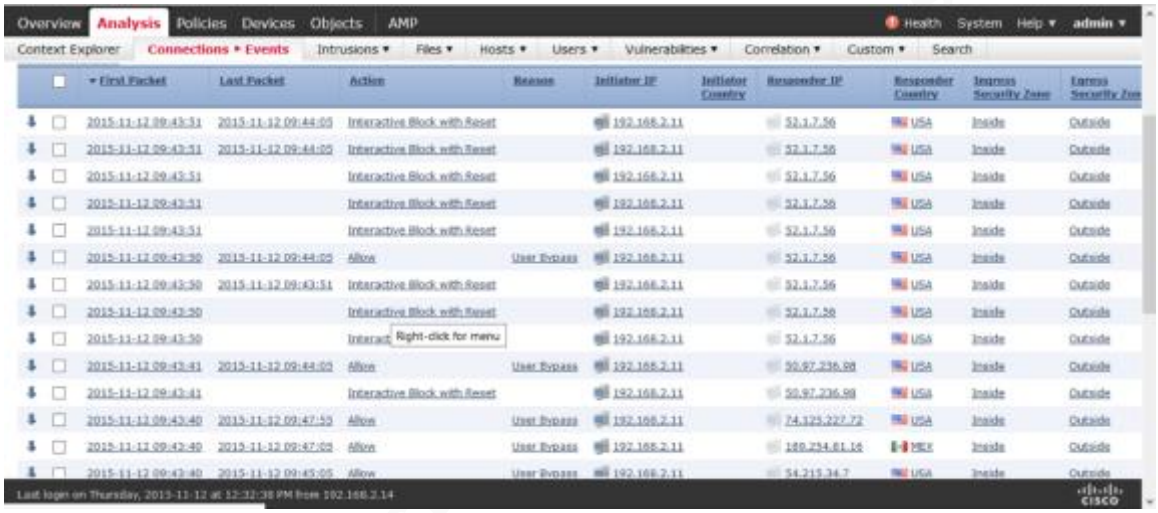


Figure 12 IPS connection events search results

4.4. Information Security Tool 4 - End Point Security: Data/Disk encryption - 14 responses

Data/Disk encryption is an interesting but not surprising result for the fourth most recommended information security tool to implement. The proliferation of laptops, mobile devices, thumb drives and government regulations make encryption a necessity.

With more users having laptops as replacements for desktops and the need for removable media, the opportunity for theft and the possibility of lost devices rise. Also, potential network breaches make it critical to encrypt data. If a laptop or removable media is encrypted and the device is lost or stolen, the contents of the drive or removable media are not accessible. If a corporate network is breached and data files on an endpoint server are encrypted, the criminal breaching the network may be able to retrieve the files, but with the files being encrypted, the data will be unreadable.

A centralized endpoint encryption system (figure 13) is essential for monitoring and management. This will allow an analyst to have centralized control of encrypting and decrypting systems. It will also show encrypted systems and allow an analyst to show a system that may have been lost or stolen is encrypted.

© 2017 The SANS Institute Author retains full rights.

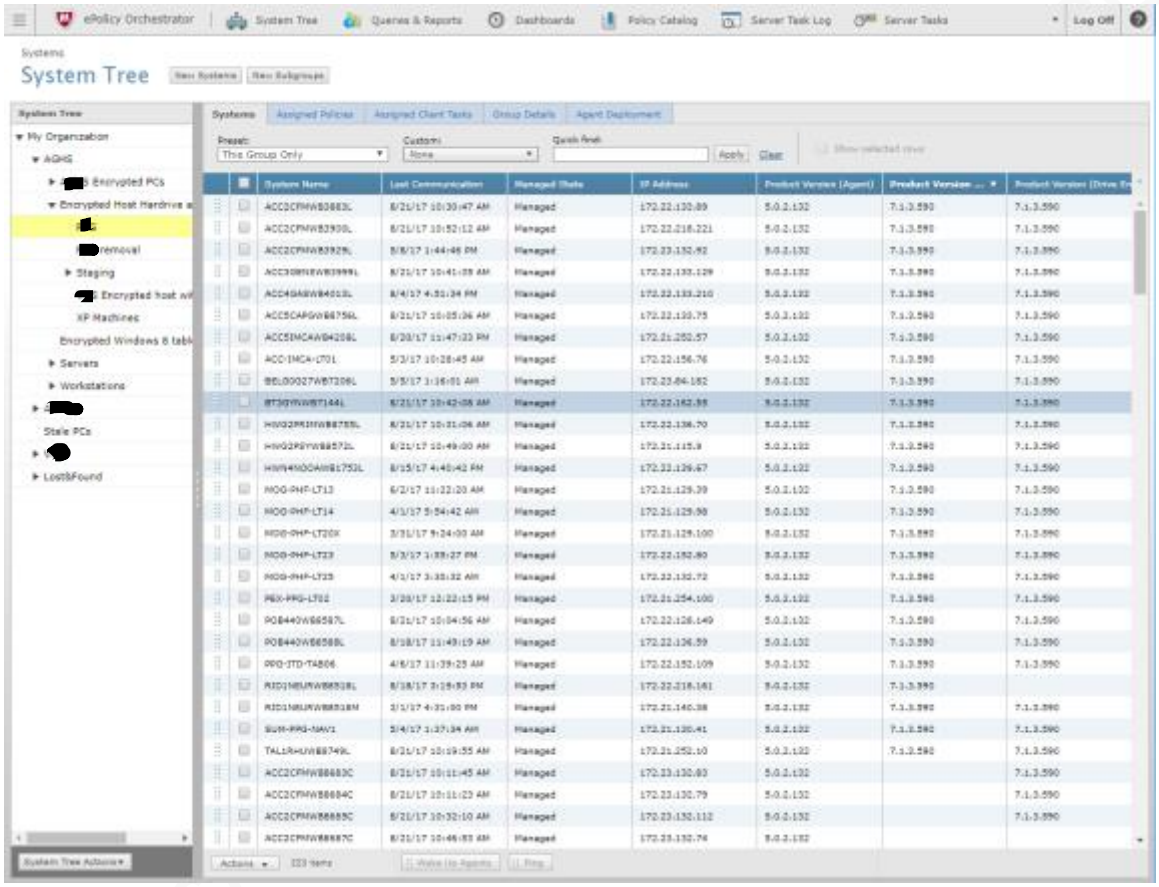


Figure 13 Endpoint encryption management interface

4.5. Information Security Tool 5 - End Point Security: System and application patching - 12 responses

Rounding out the top five of information security tools to implement is patching. A patch management program is a tool as are the patching tools themselves from various vendors including Microsoft Windows built-in patch system. Many, if not most, malware will exploit weaknesses in an operating system or application. These weaknesses, when known, almost always have patches released by the vendor.

There are many examples of malware that would have been rendered ineffective or totally unusable if operating system patches had been applied. The most recent of these is the WannaCrypt (aka WannaCry) ransomware. If IT departments and users had applied Microsoft Patch MS17-010 in a timely manner, this malware would have been ineffective.

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Patching, whether a centralized system or end points with auto updates turned on, will allow an analyst determine which patches are applied to a system. Figure 14 is an example of an endpoint patch status.

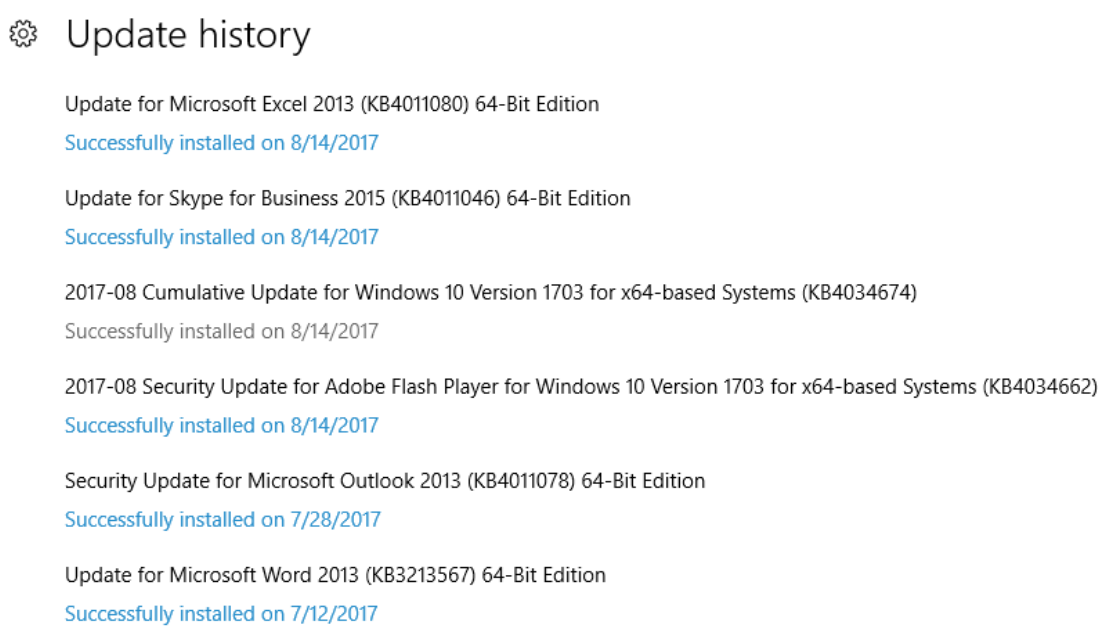


Figure 14 Host system update history

4.6. Information Security Tool 6 - End Point Security: Host Intrusion Detection/Prevention Software - 12 responses

Along with using a network based host intrusion / prevention system, it is highly recommended to implement end point based intrusion detection and prevention systems. Many organizations may not have the financial or staffing ability or desire to implement network based intrusion detection or may have a large remote work force not covered by a corporate network system.

Many businesses implement host based IDS and IPS as an additional layer of infrastructure security. Host based systems are also frequently deployed on traveling and remote worker systems who may not be covered by an enterprise network based system. These host based systems can be standalone software and are often feature of an enterprise end point security suite.

© 2017 The SANS Institute Author retains full rights.

Figure 15 shows the logs from an end point with a host IDS/IPS installed. Whether looking at a centralized host IDS/IPS solution or a stand-alone install, an analyst will be able to use this information to possibly confirm or eliminate an intrusion event.

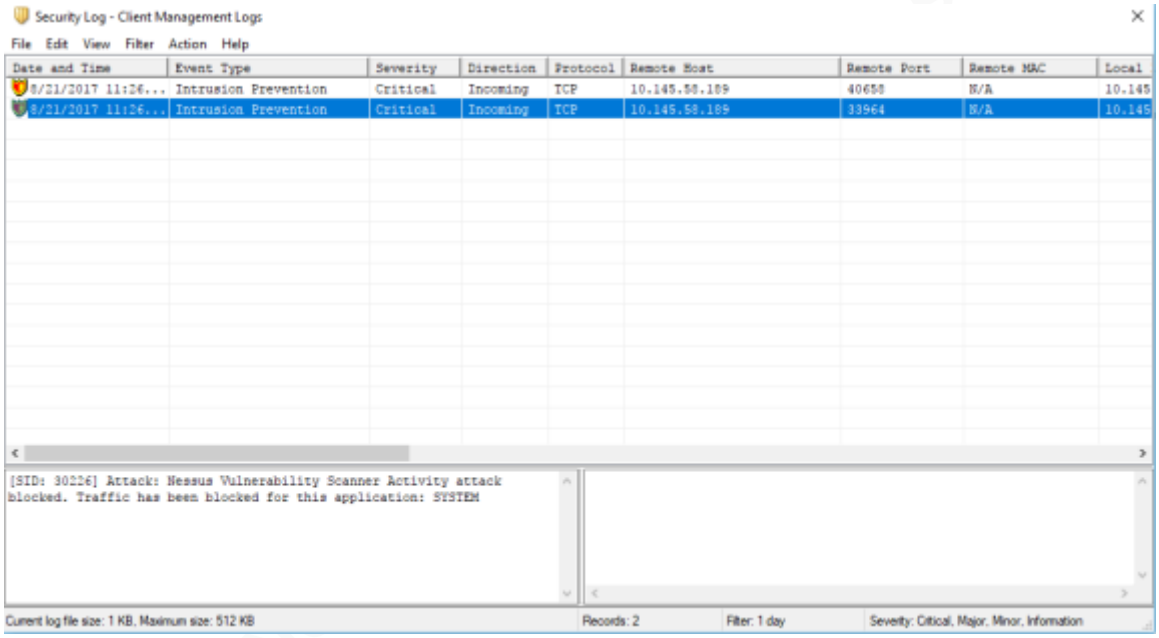


Figure 15 End point IPS logs

4.7. Information Security Tool 7 - Other / non-categorized: Staff security awareness training – 12

End user security awareness training is a consistent theme that drove the definition of an information security tool and is highly recommended by the majority of sources. Today's businesses are internet connected with email, web, business partner connections and other points of contact to end users. End users should be given and may be required by government regulations to have security awareness training.

Many types of attacks by bad actors attack the end user and not the computing infrastructure. For example, proper awareness training to show users how to detect possible bad links in their email can help prevent the outbreak of various malware on corporate and personal systems. Also, proper training can help staff detect possible phishing attacks and not click on links or enter their credentials on bad websites.

© 2017 The SANS Institute Author retains full rights.

4.8. Information Security Tool 8 - Monitoring / Audit: Logging and Log Monitoring – 12 responses

Logging and log monitoring, a highly recommended and often times required activity. Logging will assist with security monitoring and the detection of bad actors or actions. Additionally, logging may be required by industry trade groups or government regulations.

When logging systems are implemented, logs can be sent to specific log analysis tools or to a centralized logging system that performs its own analysis and alerting. Many logging systems are capable and forwards subsets of logs to specialty tools such as security and incident event management (SIEM) systems. These various types of logging tools can detect incorrect or illegal actions such as Health Insurance Portability and Accounting Act violations.

All of the previously mentioned tools will ideally be able to log events or send logs to a centralized log system. This log system will allow analysts to perform event analysis looking for intrusions by various categorization type or by querying the raw syslog events. Examples of this are shown below in Figures 16 and 17.

Figure 16 Logging system showing selections for selectable log view types

© 2017 The SANS Institute Author retains full rights.

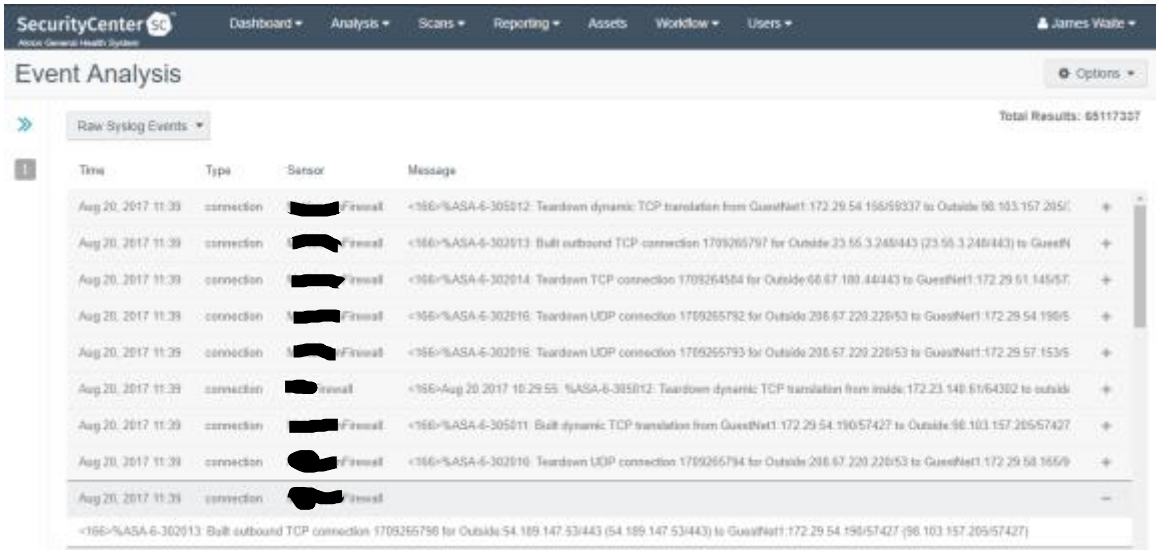


Figure 17 Logging system raw syslog view and search interface

4.9. Information Security Tool 9 - End Point Security: Firewall – 11 responses

Endpoint firewalls are important and highly recommended by over half or the research sources. An end point firewall may be one of the last lines of defense in a defense in depth strategy. This applies equally to end user devices as well as servers in a data center. These firewalls may be a traditional style endpoint firewall or an application aware firewall such as the firewall built into Windows.

While network based firewalls, network and host based IDS and IPS, end point anti-malware and patching may be implemented and end users properly trained, there is always the possibility of a new attack method or human error that can cause a potential compromise. In these cases, it may be the endpoint firewall, especially an application aware one that detects an event and either stops it or displays and alert box that causes a user to stop what they are doing and call to report a possible event.

Whether looking at a centralized management console for host firewall solutions or a standalone install, an analyst will be able to use this information to possibly confirm or eliminate the firewall is preventing intrusion events. Figure 18 shows an example configuration from an end point with a host based firewall installed. Figure 19 shows the host based firewall is centrally managed and configured via Active Directory.

© 2017 The SANS Institute Author retains full rights.

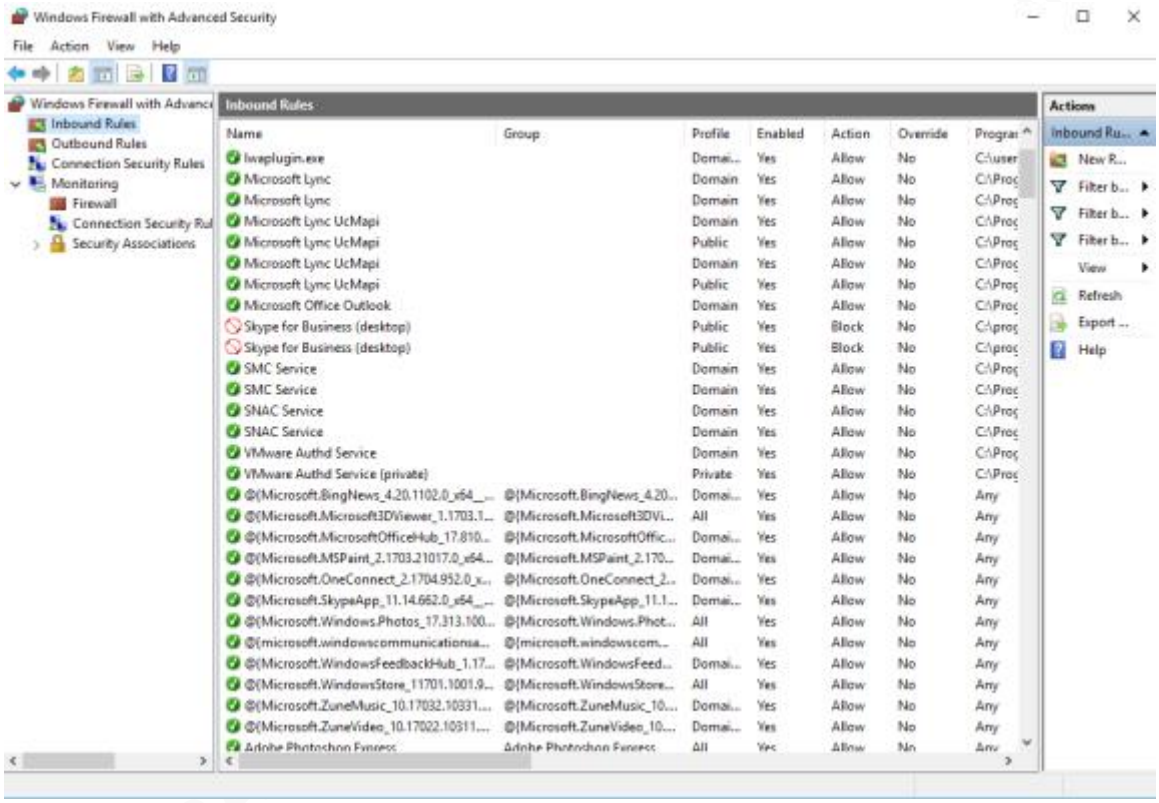


Figure 18 End point firewall configuration and monitoring interface

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

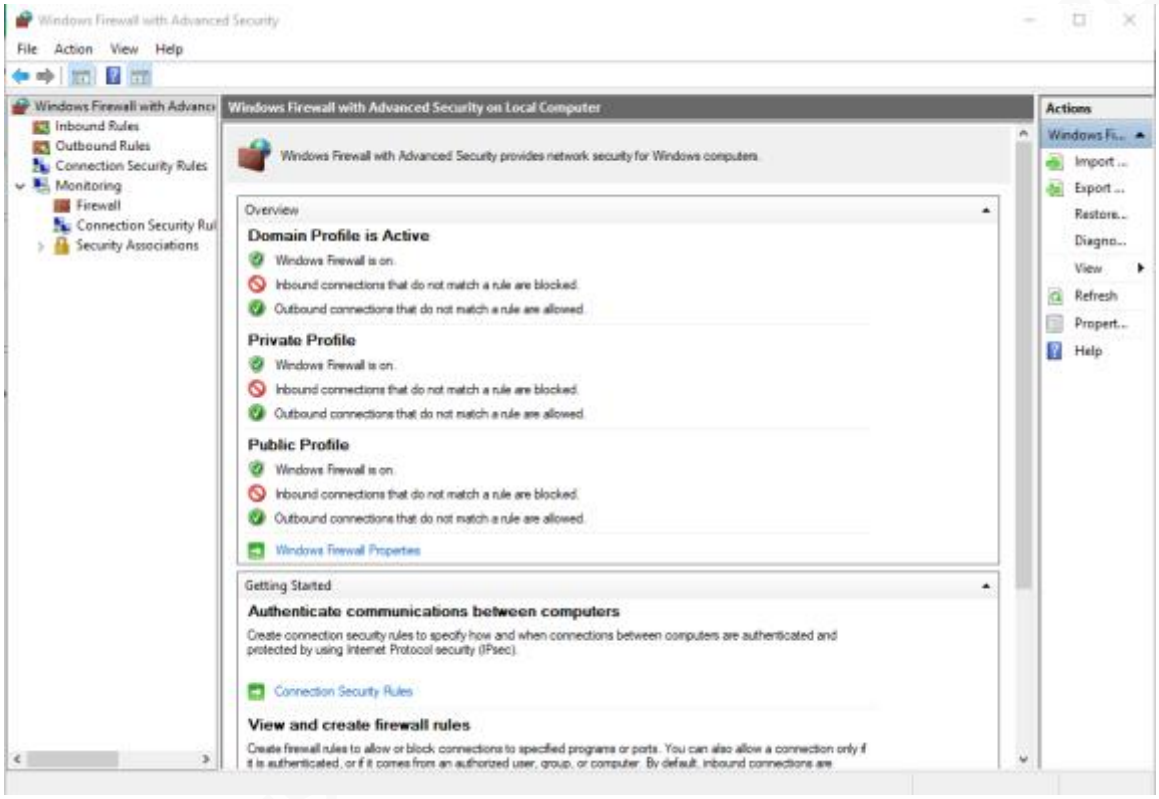


Figure 19 Host based firewall centrally managed

4.10. Information Security Tool 10 - Authentication: Authentication Servers / Services / VPN – 11 responses

While the first nine tools listed are important, an authentication server or services and VPN are just as critical. Authentication services usually provide Authentication, Authorization and Accounting for user accounts and VPNs provide secure access via these services.

Protecting assets with firewalls, IDS/IPS, anti-malware, patching and end user training has little value if user access authentication and authorization is not done. Access to database systems, file transfer servers, patient information applications, corporate accounting and banking data (additionally all business information and network assets) must be controlled. All users must authenticate to gain access to resources and data. All user access to any resource and data should be authorized. Additionally, all user access should be logged for audit purposes.

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

4.11. The quick read of the "Top Ten" recommended Information Security Tools

1. Firewall - Network / Perimeter Security
2. Anti-Malware - End Point Security
3. Network / Perimeter Security: Intrusion Detection / Prevention Systems
4. End Point Security: Data/Disk encryption
5. End Point Security: System and application patching
6. End Point Security: Host Intrusion Detection / Prevention Software
7. Other / non-categorized: Staff security awareness training
8. Monitoring / Audit: Logging and Log Monitoring
9. End Point Security: Firewall
10. Authentication: Authentication Server / Services / VPN

5. Conclusion

This has been an exploration and discussion of the various challenges to the selection of information security tools, and the research that has been done to guide a decision into what tools to select. These are the questions facing small and medium size businesses and enterprises. What tools should be chosen to secure our business data and resources? What are the challenges to the selection of these tools? What do those working in the information security field think? What does the general industry think? These are the questions facing small and medium size businesses and enterprises.

5.1. What have we been discussing?

The first challenge is financial. All businesses, whether a small business with a few hundred employees to a medium size business with fourteen hundred employees, have limited capital and must decide where budget dollars are best allocated. Some businesses may have limited capital to spend outside of core business functions.

Another area of challenge is Governance, Risk, and Compliance. Some businesses will have regulatory requirements such as HIPAA. Others may have PCI

© 2017 The SANS Institute Author retains full rights.

issues if they accept credit cards for payments. Financial institutions have issues and concerns under the Gramm–Leach–Bliley Act (GLBA) and if publicly traded also under the Sarbanes-Oxley Act.

Too many vendors and differing vendor philosophies can be challenging to information security tool selection. While there is a commonality in philosophy among vendors in market verticals, there are philosophical differences. There are also philosophical differences between vendors selling the current state products and those vendors who believe there is a new way to secure assets and are breaking with old philosophies.

What assets need protection and to what level do they need to be protected? This is an aspect needing thorough consideration and deliberation before choosing information security tools. There are multiple aspects that will impact tool set selections. Some of these issues are regulatory requirements (HIPAA), industry requirements (PCI), industry best practices (NIST) and vendor philosophies and products. Various Federal, State, and local regulatory requirements may dictate what must be protected or have compensating controls in place

Finally, a critical but not necessarily obvious obstacle when choosing which tool set to use, are the tool sets themselves. The sheer number and functionality and cross functionality between peer tool sets, between old and new philosophies of point protection, and tools based on existing protection philosophies and newer protection philosophies are a challenge.

5.2. What are the recommendations

The recommendations for the tools to use are presented as a top ten list in section four. This list is the results of the responses done while researching. The spreadsheet in the appendix contains all research sources and result items. The top ten list is a good reference and starting point. The research results are a good source of additional tools referenced and the frequency of recommendation.

References

© 2017 The SANS Institute Author retains full rights.

Hess, Ken (March, 4, 2013). *10 security best practice guidelines for businesses.* Retrieved from: http://www.zdnet.com/article/10-security-best-practice-guidelines-for-businesses

Federal Communications Commission (December, 13, 2016). *Cybersecurity for Small Business.* Retrieved from: https://www.fcc.gov/general/cybersecurity-small-business

Kissel, Richard (October, 2009). *Small Business Information Security: The Fundamentals.* Retrieved from: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Paulsen, Celia and Toth, Patricia (November, 2016). *Small Business Information Security: The fundamentals.* Retrieved from: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Francisco, Max (February, 1, 2017). *Information Security Best Practices for Small Business in 2017.* Retrieved from: http://technoloman.com/information-security-best-practices-small-business-2017/

U.S. Small Business Administration (2017). *Top Ten Cybersecurity Tips.* Retrieved from: https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips

Najjar, Grace (January, 28, 2017). *Must Have Network Security Tools for SMB Owners.* Retrieved from: https://www.engadget.com/2017/01/28/must-have-network-security-tools-for-smb-owners/

My Digital Shield (January, 9, 2015). *14 Cyber Security Tools Every Small Business Needs.* Retrieved from: http://www.mydigitalshield.com/14-cyber-security-tools-every-small-business-needs/

Titova, Elena (February, 2, 2017). *5 Cybersecurity Tools Your Company Should Have.* Retrieve from: https://www.entrepreneur.com/article/286698

Sartain, JD (May, 18, 2015). *Top security tools in the fight against cybercrime.* Retrieved from: http://www.networkworld.com/article/2922730/security0/top-security-tools-in-the-fight-against-cybercrime.html?upd=1493586951052

Liu, Jeff (October, 3, 2016). *Multifaceted cybersecurity.* Retrieved from: https://www.scmagazine.com/multifaceted-cybersecurity/article/530303/

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Bessemer Venture Partners (May, 12, 2017). *BVP Cyber Index.* Retrieved from: https://www.bvp.com/strategy/cyber-security/index

The SANS Institute. (2013). *SANS Security Essentials* (V2013_1006 Revision 1). Bethesda, MD: The SANS Institute

The SANS Institute. (2012). *SANS Intrusion Detection In-Depth* (V2012_0529). Bethesda, MD: The SANS Institute

Prowse, David L (2015). *CompTIA Security+ SY0-401 Cert Guide, Deluxe Edition* (3rd Edition). Indianapolis, IN: Pearson

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Appendix

Appendix 1: Raw Results

	CompTIA Security+	SANS GSEC	SANS GCIA	Internet Source 1	Internet Source 2	Internet Source 3	Internet Source 4	Internet Source 5	Internet Source 6	Internet Source 7	Internet Source 8	Internet Source 9	Internet Source 10	Internet Source 11	Interview Source 1	Interview Source 2	Interview Source 3	Interview Source 4	Interview Source 5	Interview Source 6	Totals
Endpoint																					
Patching	1	1	1	1	1	1	1	1	1				1		1					1	12
Firewall	1	1	1	1		1	1						1			1	1	1	1		11
HIDS / HIPS	1	1	1	1			1			1	1		1			1	1	1	1		12
PopUp Blockers	1														1	1	1	1	1		6
DLP	1			1												1	1	1	1		6
Data / Disk Encryption	1	1	1	1			1		1		1		1	1	1	1	1	1	1		14
OS Hardening	1	1	1												1						4
Patch Mgmt	1	1	1																		3
GPO, Security Templates and configuration baseline	1	1	1																		3
AntiMalware	1	1	1	1	1	1	1	1	1		1		1		1	1	1	1	1	1	17
Comprehensive End Point Sec Suite				1		1									1	1	1	1	1	1	8
																					0
Network / Perimeter																					
NAT	1	1	1												1						4
Network Zones	1	1	1												1	1	1	1	1		8
DMZ	1	1	1												1	1	1	1	1		8
Network Access Control (NAC)	1																				1
VLAN / Subnets	1	1	1												1	1	1	1	1		8
Firewall - Reg or NextGen	1	1	1	1	1	1	1	1	1	1	1		1		1	1	1	1	1	1	18
Proxy Servers	1	1	1																		3
Honey Pots / Nets	1	1	1	1																	4
DLP	1			1						1	1				1	1	1	1	1		9
IPS / IDS	1	1	1	1			1			1	1		1		1	1	1	1	1	1	14
																					0
Authentication																					
Authentication servers / Authentication unique IDs	1	1	1		1	1	1	1	1					1	1						10
802.1x, LDAP, PKI, Kerbeeros, Term Svcs	1	1	1	1											1	1	1	1	1		9
User Authorization - Data, apps and installs	1	1	1			1	1	1						1							7
VPN, RADIUS / TACACS	1	1	1				1			1	1				1	1	1	1	1		11
																					0
Vulnerability / Risk Mgmt																					
Network Mapping Tools	1	1	1							1					1						5
Vulnerability Scanning	1	1	1												1						4
Sniffers	1	1	1							1					1						5
Password Analysis	1	1	1												1						4
Network Scanning - ie nMap		1	1																		2
																					0
Monitoring / Auditing																					
Performance monitors for baselining	1	1	1										1								4
Protocol analyzers	1	1	1												1						4
Network Mon itoring Systems	1												1	1	1						4
Logging servers - Syslog	1	1	1				1				1		1	1	1	1	1	1	1		12
																					0
Other																					
SIEM / Logging		1	1										1		1	1	1	1	1		8
Behaviour Analystics													1			1	1	1	1		5
Cloud Access Security Brokers - CASB																1	1	1	1		4
VM	1	1	1												1						4
eMail Filters				1			1			1		1								1	5
Training				1	1	1	1	1	1			1		1		1	1	1	1		12
MDM					1			1	1				1			1	1	1	1		8
backup / bcp					1	1	1	1					1			1	1	1	1		9
Strategic InfoSec Outsourcing																1	1	1	1		4
salespitch to owner for buy in																					0
GRC Framework							1		1				1			1	1	1	1	1	8
Physical Access Control					1	1		1	1												4
Secure Wireless					1	1	1	1	1		1										6
Web Filter							1			1	1									1	4
Purchase Secure Hardware												1									1
Website SSL									1			1								1	3
Application Control													1								1
Automation, AI and Machine Learning														1							1

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Appendix 2: Training course survey results

	CompTIA Security+	SANS GSEC	SANS GCIA	Totals
Endpoint				
Patching	1	1	1	3
Firewall	1	1	1	3
HIDS / HIPS	1	1	1	3
Pop-up Blockers	1			1
DLP	1			1
Data / Disk Encryption	1	1	1	3
OS Hardening	1	1	1	3
Patch Mgmt.	1	1	1	3
GPO, Security Templates and configuration baseline	1	1	1	3
Antimalware	1	1	1	3
Comprehensive End Point Sec Suite				0
				0
Network / Perimeter				
NAT	1	1	1	3
Network Zones	1	1	1	3
DMZ	1	1	1	3
Network Access Control (NAC)	1			1
VLAN / Subnets	1	1	1	3
Firewall - Reg or NextGen	1	1	1	3
Proxy Servers	1	1	1	3
Honey Pots / Nets	1	1	1	3
DLP	1			1
IPS / IDS	1	1	1	3
				0
Authentication				
Authentication servers / Authentication unique IDs	1	1	1	3
802.1x, LDAP, PKI, Kerberos, Term Svcs	1	1	1	3
User Authorization - Data, apps and installs	1	1	1	3
VPN, RADIUS / TACACS	1	1	1	3
				0
Vulnerability / Risk Mgmt.				
Network Mapping Tools	1	1	1	3
Vulnerability Scanning	1	1	1	3
Sniffers	1	1	1	3
Password Analysis	1	1	1	3
Network Scanning - i.e. nMap		1	1	2
				0
Monitoring / Auditing				
Performance monitors for baselining	1	1	1	3
Protocol analyzers	1	1	1	3
Network Monitoring Systems	1			1
Logging servers - Syslog	1	1	1	3
				0

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Other				
SIEM / Logging		**1**	**1**	**2**
Behavior Analytics				**0**
Cloud Access Security Brokers – CASB				**0**
VM	**1**	**1**	**1**	**3**
eMail Filters				**0**
Training				**0**
MDM				**0**
backup / BCP				**0**
Strategic InfoSec Outsourcing				**0**
sales pitch to owner for buy in				**0**
GRC Framework				**0**
Physical Access Control				**0**
Secure Wireless				**0**
Web Filter				**0**
Purchase Secure Hardware				**0**
Website SSL				**0**
Application Control				**0**
Automation, AI and Machine Learning				**0**

© 2017 The SANS Institute, Author Retains Full Rights

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Appendix 3: Internet research survey results

For this chart, I. S. stands for Internet Source.

	I. S. 1	I. S. 2	I. S. 3	I. S. 4	I. S. 5	I. S. 6	I. S. 7	I. S. 8	I. S. 9	I. S. 10	I. S. 11	Totals
Endpoint												
Patching	1	1	1	1	1	1				1		7
Firewall	1		1	1						1		4
HIDS / HIPS	1			1			1	1		1		5
Pop-up Blockers												0
DLP	1											1
Data / Disk Encryption	1			1		1		1		1	1	6
OS Hardening												0
Patch Mgmt.												0
GPO, Security Templates and configuration baseline												0
Antimalware	1	1	1	1	1	1		1		1		8
Comprehensive End Point Sec Suite	1		1									2
												0
Network / Perimeter												
NAT												0
Network Zones												0
DMZ												0
Network Access Control (NAC)												0
VLAN / Subnets												0
Firewall - Reg or NextGen	1	1	1	1	1	1	1	1		1		9
Proxy Servers												0
Honey Pots / Nets	1											1
DLP	1						1	1				3
IPS / IDS	1			1			1	1		1		5
												0
Authentication												
Authentication servers / Authentication unique IDs		1	1	1	1	1					1	6
802.1x, LDAP, PKI, Kerberos, Term Svcs	1											1
User Authorization - Data, apps and installs			1	1	1						1	4
VPN, RADIUS / TACACS				1			1	1				3
												0
Vulnerability / Risk Mgmt.												
Network Mapping Tools							1					1
Vulnerability Scanning												0

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Sniffers						1					1
Password Analysis											0
Network Scanning - i.e. nMap											0
											0
Monitoring / Auditing											
Performance monitors for baselining									1		1
Protocol analyzers											0
Network Monitoring Systems									1	1	2
Logging servers - Syslog				1			1		1	1	4
											0
Other											
SIEM / Logging									1		1
Behavior Analytics									1		1
Cloud Access Security Brokers - CASB											0
VM											0
eMail Filters	1			1			1				4
Training	1	1	1	1	1	1				1	8
MDM		1			1	1			1		4
backup / BCP		1	1	1	1				1		5
Strategic InfoSec Outsourcing											0
sales pitch to owner for buy in											0
GRC Framework				1		1			1		3
Physical Access Control		1	1		1	1					4
Secure Wireless		1	1	1	1	1		1			6
Web Filter				1			1	1			3
Purchase Secure Hardware									1		1
Website SSL						1			1		2
Application Control									1		1
Automation, AI and Machine Learning										1	1

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

© 2017 The SANS Institute, Author Retains Full Rights

Appendix 4: Personnel interview survey results

For this chart, I. S. stands for Interview Source.

	I. S. 1	I. S. 2	I. S. 3	I. S. 4	I. S. 5	I. S. 6	Totals
Endpoint							
Patching	1					1	2
Firewall		1	1	1	1		4
HIDS / HIPS		1	1	1	1		4
Pop-up Blockers	1	1	1	1	1		5
DLP		1	1	1	1		4
Data / Disk Encryption	1	1	1	1	1		5
OS Hardening	1						1
Patch Mgmt.							0
GPO, Security Templates and configuration baseline							0
Antimalware	1	1	1	1	1	1	6
Comprehensive End Point Sec Suite	1	1	1	1	1	1	6
							0
Network / Perimeter							
NAT	1						1
Network Zones	1	1	1	1	1		5
DMZ	1	1	1	1	1		5
Network Access Control (NAC)							0
VLAN / Subnets	1	1	1	1	1		5
Firewall - Reg or NextGen	1	1	1	1	1	1	6
Proxy Servers							0
Honey Pots / Nets							0
DLP	1	1	1	1	1		5
IPS / IDS	1	1	1	1	1	1	6
							0
Authentication							
Authentication servers / Authentication unique IDs	1						1
802.1x, LDAP, PKI, Kerberos, Term Svcs	1	1	1	1	1		5
User Authorization - Data, apps and installs							0
VPN, RADIUS / TACACS	1	1	1	1	1		5
							0
Vulnerability / Risk Mgmt.							
Network Mapping Tools	1						1
Vulnerability Scanning	1						1
Sniffers	1						1
Password Analysis	1						1
Network Scanning - i.e. nMap							0
							0
Monitoring / Auditing							
Performance monitors for baselining							0
Protocol analyzers	1						1
Network Monitoring Systems	1						1
Logging servers - Syslog	1	1	1	1	1		5
							0

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute Author retains full rights.

Other							
SIEM / Logging	**1**	**1**	**1**	**1**	**1**		**5**
Behavior Analytics		**1**	**1**	**1**	**1**		**4**
Cloud Access Security Brokers - CASB		**1**	**1**	**1**	**1**		**4**
VM	**1**						**1**
eMail Filters						**1**	**1**
Training		**1**	**1**	**1**	**1**		**4**
MDM		**1**	**1**	**1**	**1**		**4**
backup / BCP		**1**	**1**	**1**	**1**		**4**
Strategic InfoSec Outsourcing		**1**	**1**	**1**	**1**		**4**
Sales pitch to owner for buy in							**0**
GRC Framework		**1**	**1**	**1**	**1**	**1**	**5**
Physical Access Control							**0**
Secure Wireless							**0**
Web Filter						**1**	**1**
Purchase Secure Hardware							**0**
Website SSL						**1**	**1**
Application Control							**0**
Automation, AI and Machine Learning							**0**

James Waite, jswaite@zoominternet.net

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.