Securing the Windows 10 GIAC Enterprise Endpoint ISE/M 6100 - Security Project Practicum - Technical Paper

Securing the Windows 10 GIAC Enterprise Endpoint

ISE/M 6100 – Security Project Practicum – Technical Paper

Author: Balaji Balakrishnan, dfir.aaa@gmail.com
Matthew Hosburgh, matt.hosburgh@gmail.com
Patrick Neise, patrick.neise@gmail.com
Advisor: Stephen Northcutt
Due: January 5th 2016

Abstract

2015 has proven to be a battleground for the endpoint. According to a report released by the Ponemon Institute, the endpoint is becoming an increasing target for attacks. Because GIAC utilizes some of the latest enterprise technology, it is no surprise that GIAC is also facing the risks outlined by the Ponemon Institute. Keeping with the organization's upgrade cycle, Windows 10 is being considered as the next upgrade from the current Windows 7 environment. A recent pilot of Windows 10 has raised a significant number of privacy concerns for the entire organization. After conducting an assessment of the network traffic originating from Windows 10, it is evident that the default configuration will not provide an adequate level of security and privacy for GIAC Enterprises. By conducting a basic risk assessment, the Security Team has been able to analyze the risks the organization faces from an endpoint perspective, to effectively recommend a plan to secure the GIAC Enterprise system.

1. Introduction

2015 has proven to be a battleground for the endpoint. According to a report released by the Ponemon Institute, the endpoint is becoming an increasing target for attacks. Furthermore, the report highlights that the "primary reason for the difficulty in managing endpoint risk is negligent or careless employees who do not comply with security policies"(2015 State of the Endpoint Report, 2015). Because GIAC utilizes some of the latest enterprise technology, it is no surprise that GIAC is also facing the risks outlined by the Ponemon institute. Keeping with the organization's upgrade cycle, Windows 10 is being considered as the next upgrade from the current Windows 7 environment. A recent pilot of Windows 10 has raised a significant concern for the entire organization. After conducting an assessment of the network traffic originating from Windows 10, it is evident that the default configuration will not provide an adequate level of security and privacy for GIAC Enterprises. Direct traffic analysis has proven that the amount of outbound connections should be limited to only what is required to minimize the impacts to employee private data and system usage. By conducting a basic risk assessment, the Security Team has been able to analyze the risks the organization faces from an endpoint perspective, to effectively recommend a plan to secure the GIAC Enterprise system.

2. Threat and Risk Models

2.1 Overall Method

In order to effectively identify potential solutions to mitigate the vulnerabilities presented by potential information leakage, the GIAC Security Team conducted an evaluation of the possible threats to the enterprise and then completed a risk assessment based on the identified threats and vulnerabilities. The results of the risk assessment were used to identify and prioritize potential solutions for the project tasking.

2.2 Summary of Threats

This section describes the threats and attack techniques that could be leverage against the new Windows 10 operating system.

- Information disclosure
- Unauthorized access due to stolen credentials
- Unauthorized Access from unmanaged endpoint
- Malware attack not prevented by GIAC perimeter
- Endpoint compromise may go undetected
- Information Disclosure due to data exfiltration
- Lack of user awareness decreases the ability for users to operate their systems in a secure manner.

The threats identified (also see Appendix A) were used in risk assessment to prioritize the risks and create mitigation plan accordingly.

2.3 Summary of Risks

The Security Team at GIAC Enterprises conducted a Risk Assessment, centered around the new Windows 10 deployment. It is important to note that due to time constraints, the assessment focuses on the top six risks faced by the organization. As a framework, the Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber defense (CIS Controls, 2015) were used in conjunction with the aforementioned threat model. The top six risks faced by GIAC Enterprises are as follows (in greatest to least):

- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 8: Malware Defenses
- CSC 7: Email and Web Browser Protections

The risk register as completed by the Security Team was leveraged to assist in selecting viable administrative and technical solutions to address the security and privacy

issues. The impact and likelihood of each particular item was based off of an internal review and interviews with key GIAC Enterprises personnel. The complete risk assessment with definitions can be found in Appendix B.

3. Lab Methodology

3.1 Setup

In order to support consistent, repeatable results throughout the project, virtual machines were used for the Windows 10 host and the platform for packet capture of network traffic destined for the Internet. The Windows 10 virtual machine was downloaded from the Microsoft Development website, allowing each of the testers to begin from an identical base image (Virtual Machine(VM), Windows, Virtual PC & BrowserStack: Microsoft Edge Dev, 2015). The use of virtual machines also enabled the testers to create snapshots of the Windows 10 virtual machine as they progressed through the testing and analysis in order to return to a previous state to repeat the tests as necessary.

In order to collect the traffic leaving the Windows 10 host that is destined for the Internet a second virtual machine running VyOS was used as both a router and packet capture device. VyOS is a Linux-based network operating system that provides routing and other networking support features (VyOS, 2015). The VyOS image was configured with two network interface cards in order to provide connectivity to the Windows 10 host and the Internet. The first interface was configured as the internal interface for the Windows 10 host on a custom virtual network to ensure that the Windows 10 host is the only computer communicating the VyOS machine. The external interface of the VyOS machine was configured as a Network Address Translation (NAT) interface in order to provide Internet connectivity for the Windows 10 machine through the VyOS machine.

Traffic passing through the VyOS machine was captured via tcpdump, filtered to only capture traffic to and from the Windows 10 host. Packet captures for each of the

configurations described below were conducted using the same test script in order to provide a base of results to compare the individual traffic captures against.

3.2 Testing

To provide a base image from which to compare the different configurations and firewall software, the following is the install that served as the base Windows 10 install.

- The default install options were utilized, leaving all of the privacy concerns of Windows 10 enabled.
- Adobe PDF reader was installed to provide a third party application that may attempt to unknowingly communicate with servers on the Internet.
- Chrome browser was installed in order to provide an additional web browser to compare against the included Microsoft Edge browser.
- The default Microsoft Windows Firewall rules for a private network were used to simulate a workstation within the corporate environment.
- A separate User account was added to simulate a regular corporate user vice the default Administrator account included with the virtual machine.

In addition to the base install, the testing procedure was conducted against the following additional configurations in order to determine the recommended Windows 10 configuration and software installation to reduce the undesired outbound Internet traffic.

- Modifications to Windows Group Policy to eliminate privacy concerns
- Windows Secure Configuration Management templates
- Installation of Windows Firewall Notifier (https://wfn.codeplex.com)
- Installation of Windows Firewall Control (http://www.binisoft.org/wfc.php)
- Installation of Traps from Palo Alto.

The testing procedure was conducted on each of the above configurations individually in order to determine the impact of each installation and/or configuration change on the amount of undesired outbound Internet traffic from the Windows 10 host. The testing procedure described below was used to determine both the amount of outbound traffic from an idle Windows host and the amount out additional outbound traffic generated from opening a PDF document and browsing to a few chosen websites.

Testing Procedure

- Begin tcpdump packet capture on VyOS VM
- Boot Windows 10 VM
- Wait for 30 minutes
- Open a PDF document with Adobe PDF Reader
- Use the Edge browser for the following sites:
    - cnn.com
    - torproject.org
    - google.com
- Use Chrome browser for the sites above
- Shut down the Windows 10 VM
- Stop the packet capture on the VyoS VM
- Just boot VM and collect pcap for 30min

3.3 Analysis

After completing packet captures for each of the above configurations the captures were parsed with a Python script (full script in Appendix D) in order to quickly parse through the traffic and collect statistics of concern for comparison and solution recommendation. The script essentially parsed each packet capture file and provided a comma separated file that contains information about all outbound connections from the Windows 10 host including destination IP address, domain name, amount of traffic, and whether the traffic was TCP or UDP.

Through collection and analysis of the individual packet captures, the following results were obtained for comparison.

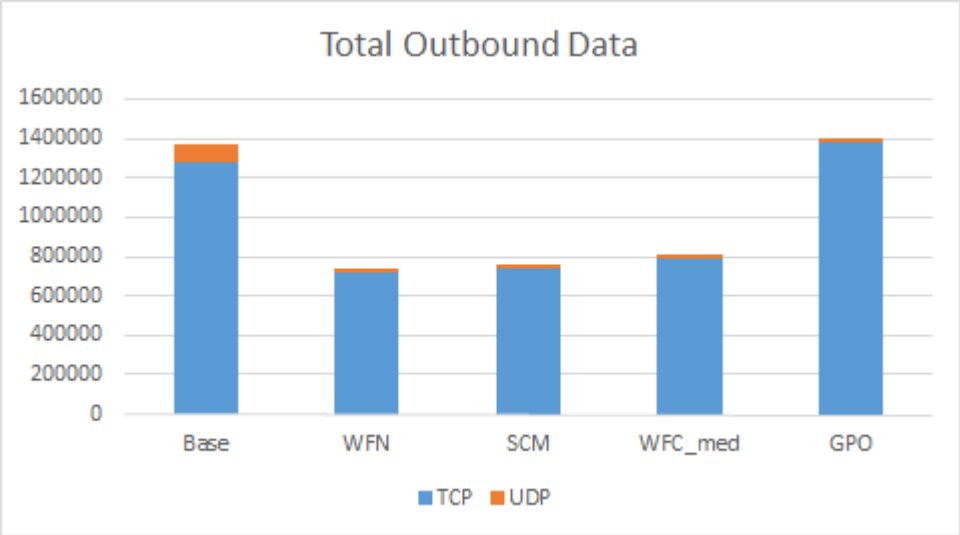


Figure 1. Total outbound data summary

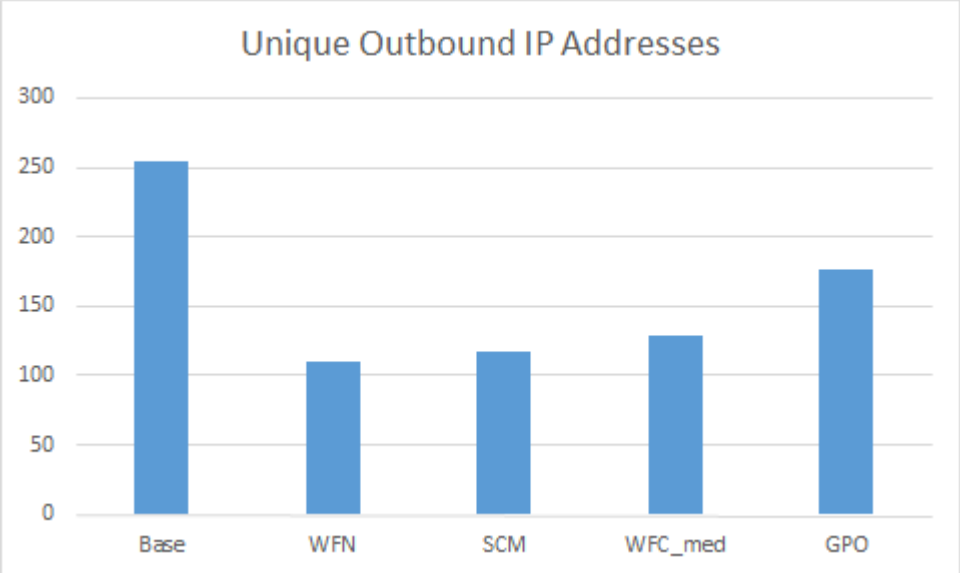


Figure 2. Unique outbound IP address

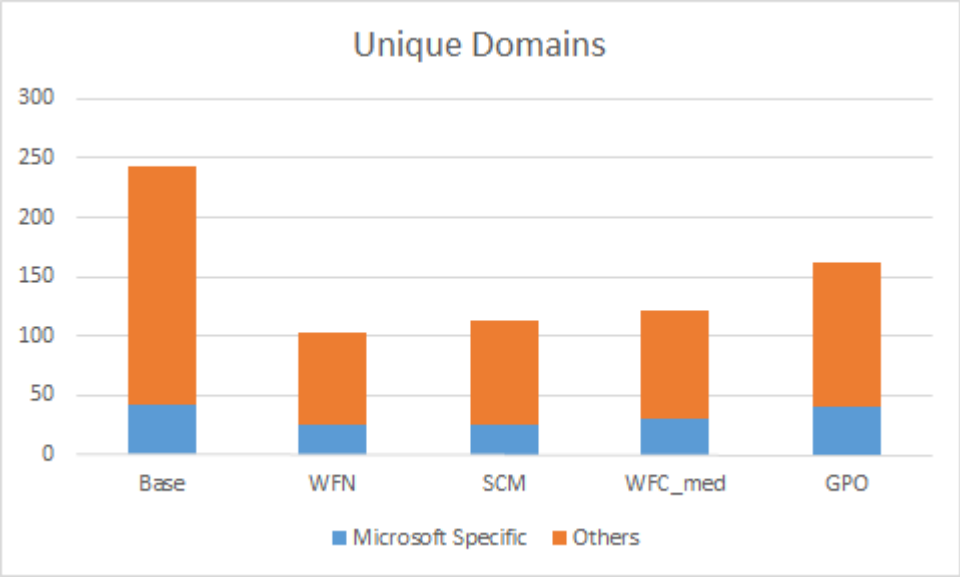


Figure 3. Unique domains contacted.

Of note, no individual configuration or software changes resulted in a dramatic decrease in the amount of outbound traffic from the Windows 10 host. The SCM and GPO changes only impact the Microsoft specific traffic while the WFN and WFC firewall changes impact third party software. For example, when using WFN with its default installation, Google Chrome browser would not connect to the Internet as it was not specifically added to the firewall rules.

4. Recommendations

4.1 Windows Privacy

By default, Windows 10 sends an abundance of personal data to Microsoft's servers, uses a great deal of bandwidth for Microsoft's own purposes, and profiles your Windows usage. There are a lot of articles explaining the privacy concerns and data exposure related to Windows 10, some of them are highlighted in the references section.

Two key recommendations to protect GIAC enterprises from privacy concerns from Windows 10 are to apply group policy templates highlighted in this paper, do not create Microsoft account and use local system accounts instead.

Not using a Microsoft account will protect GIAC enterprises from many of Microsoft's attempts to collapse the local-remote distinction in its privacy policies. Some problematic policies like WiFi-Sense and if a Microsoft account is used to login Windows 10 automatically uploads a copy of recovery key – which can be used to unlock your encrypted disk – to Microsoft's servers, probably without your knowledge and without an option to opt-out (Intercept, 2015).

By applying the group policy templates for privacy settings regular users will not have option to change them by mistake. Microsoft will be unable to revert to the default settings with patch updates, since group policies will be reapplied every 90 minutes. Even though there are many third party privacy configuration tools like DoNotSpy, GIAC Security Team does not recommend installing those third-party solutions since some of them have adware and malware bundled with some of those third party solutions.

4.2 Third Party

Although WFN and WFC produce similar results, the increased customization options provided by WFC make it a more attractive option for protecting against potential outbound traffic from third party applications. While there are similar types of software available for purchase, the open source WFC provides sufficient initial coverage to minimize the potential exposure impact of GIAC proprietary information.

4.3 Awareness Training

Based on the risk assessment, it is clear that awareness training is needed for GIAC Enterprises. This finding aligns also with the Ponemon study that suggests "The primary reason for the difficulty in managing endpoint risk is negligent or careless employees who do not comply with security policies" (2015 State of the Endpoint Report, 2015). The lack of a formal program is the primary reason that CSC CIS 17, Security Skills Assessment and Appropriate Training to Fill Gaps is the highest risk to the organization. When surveyed, users did not understand the implications of clicking a malicious link or browsing to an untrusted site. Furthermore, the users surveyed did not

understand how to report or respond if they suspect a security incident. Awareness is the first step in securing GIAC Enterprises because it affords and equips the end-user with the ability to detect and report potential security issues.

4.4 Results

The previously described testing procedure was repeated with the recommended Group Policy, WFC installed and running with a Medium setting, with and without using Chrome with uBlock for web browsing.

As shown in the figures below, the recommended configuration results in a *significant* decrease in the overall outbound traffic and hosts contacted.

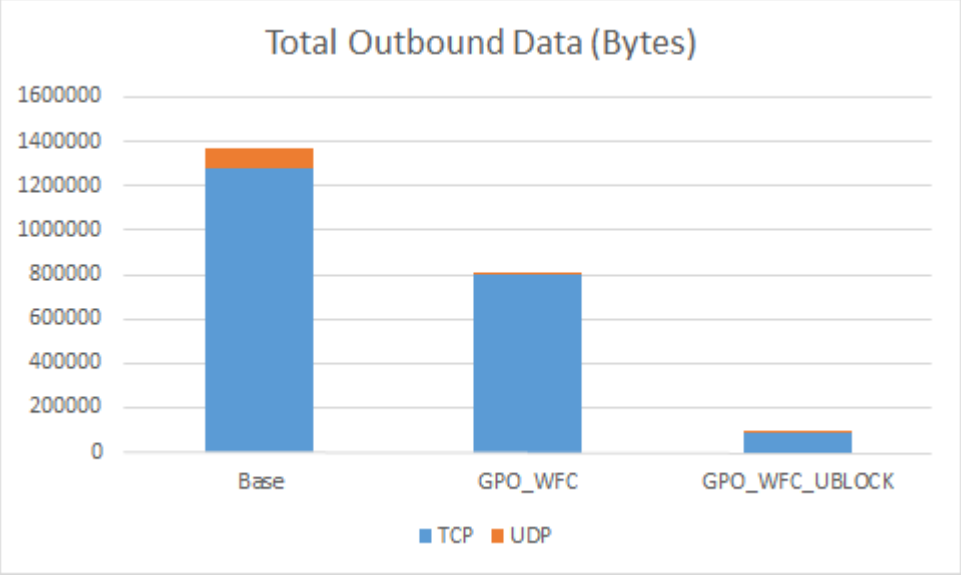


Figure 4. Total outbound data in bytes with mitigation in place.

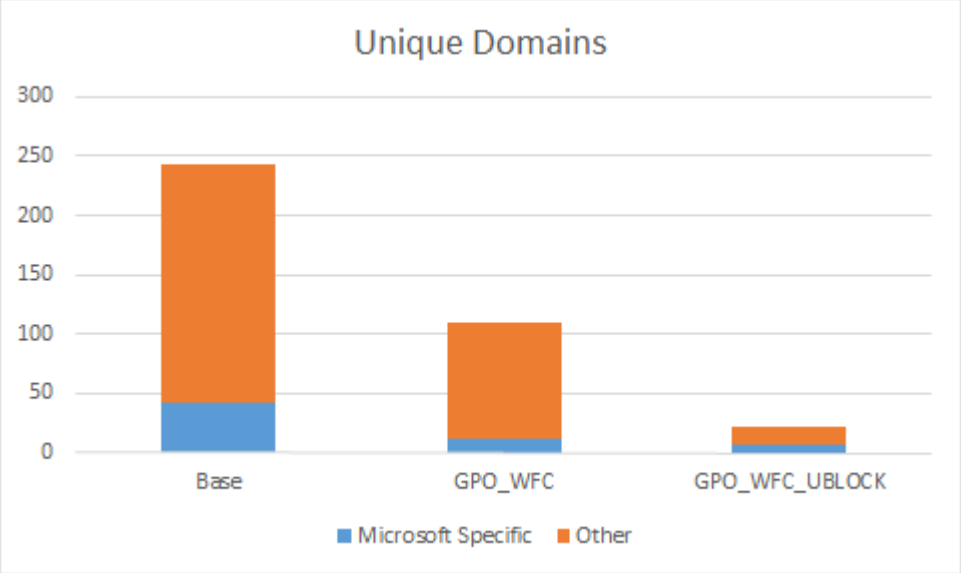


Figure 5. Unique domains contacted with mitigation in place.

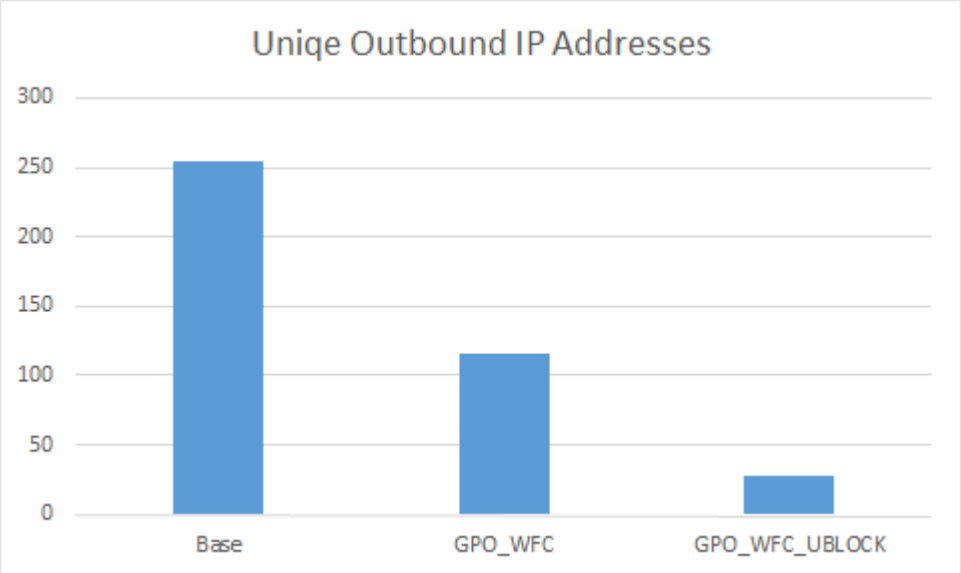


Figure 6. Unique outbound IP address with mitigation in place.

Outbound traffic was reduced by about 75% when using mitigating controls. This reduction was without having to purchase additional software. By leveraging GPO changes, installing open-source WFC, and utilizing an ad blocker for web browsing, GIAC Enterprises is able to achieve the desired outbound traffic results, without having to spend additional money on software.

Although the recommendations can be implemented with relative ease across the GIAC enterprise, additional capabilities such as log aggregation and other features may be desired for further protection and analysis of the effectiveness may be desired. Implementation of tools such as Splunk, Traps, or a commercial firewall application may be worth investigating via a future project.

5. Conclusion

The recent deployment of Windows 10 laptops across the GIAC enterprise has presented the team with opportunities and challenges. While the Windows operating system continues to become more secure and increasingly difficult for attackers to exploit, the operating system itself is sending more and more information out of the network than ever before. Most importantly, this data is being sent out of the network based on default installation settings within the operating system. Additionally, third party applications such as Adobe Reader and others communicate information out of the network, many times without the knowledge of the user. Finally, the amount of advertising based information, including malware delivered by ads, continues to increase and is not only a privacy concern but also a security concern.

After conducting analysis of Windows Group Policy settings, free and commercial endpoint firewall solutions, an adblocker for browsing, and log aggregation software, the project team has recommended modifications to the deployed Group Policy, the installation of Windows Firewall Control, and the use of ad blockers for web browsing activities. While the cost of the recommendations only consists of the time necessary to implement and maintain, it is estimated that the changes will result in an order of magnitude reduction in unwanted traffic leaving the network with little to no impact on user experience or functionality.

Finally, the project team sees the above recommendations as the first step to securing the Windows 10 endpoints in order to prevent sensitive company information

from leaving the enterprise. Further research into products such as Splunk, Palo Alto Traps, and commercial endpoint firewall solutions is warranted and prudent based on the ever growing threat to company information.

References

2015 State of the Endpoint Report: User-Centric Risk. (2015). Retrieved December 22, 2015, from https://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf

CIS Controls. (2015). Retrieved January 3, 2016, from https://www.cisecurity.org/critical-controls/download.cfm?token=NIpEm4h+GLQ0/ChfACTo19Z6voYvhiWxUy0KKWwS38g=&ts=1449354774428

Configure telemetry and other settings in your organization. (2015, December 17). Retrieved January 3, 2016, from https://technet.microsoft.com/en-us/library/mt577208(v=vs.85).aspx

Keep Windows 10 secure. (2015). Retrieved January 3, 2016, from https://technet.microsoft.com/en-us/library/mt158215(v=vs.85).aspx

Microsoft Keeps Backup of Your Encryption Key on its Server - Here's How to Delete it. (2015, December 28). Retrieved January 2, 2016, from http://thehackernews.com/2015/12/windows-encryption-key-backup.html

Microsoft Security Guidance. (2015). Retrieved January 3, 2016, from http://blogs.technet.com/b/secguide/archive/2015/10/08/security-baseline-for-windows-10-draft.aspx

Next-Generation Endpoint Protection. (2015). Retrieved January 3, 2016, from https://www.paloaltonetworks.com/products/endpoint-security.html

Recently Bought a Windows Computer? Microsoft Probably Has Your Encryption Key.

(2015, December 28). Retrieved January 2, 2016, from https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/

Virtual Machine (VM), Windows Virtual PC & BrowserStack : Microsoft Edge Dev. (2015). Retrieved from Microsoft: https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/

VyOS. (2015, 12 10). Retrieved from VyOS: http://vyos.net/wiki/Main_Page

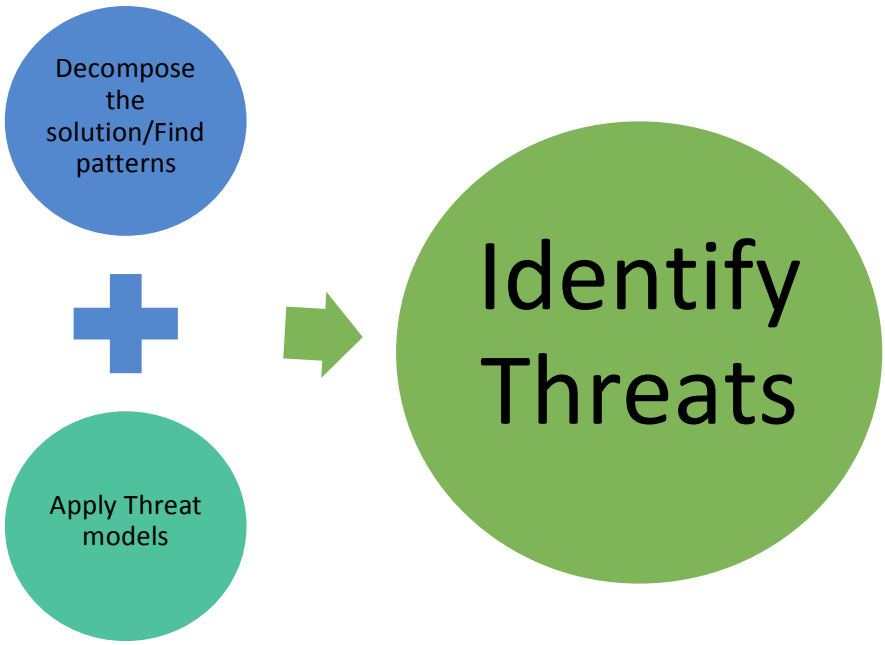
Windows 10 security overview. (2015). Retrieved January 3, 2016, from https://technet.microsoft.com/en-us/library/mt601297(v=vs.85).aspx

Windows 10 update didn't remove spying tool, Microsoft just renamed it. (2015, December 1). Retrieved January 2, 2016, from http://www.networkworld.com/article/3010268/microsoft-subnet/microsoft-windows-10-update-privacy-spying.html#tk.rss_all

Appendix

A. Threat Model

GIAC Security team leverages the most applicable threat models depending upon the business solution and/or the vulnerability that is being reviewed, threat models used for Windows 10 risk assessment was STRIDE and Cyber Kill chain.



STRIDE

STRIDE is a system developed by Microsoft for thinking about computer security threats. It provides a mnemonic for security threats in six categories.

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service (D.o.S)
- Elevation of privilege

Cyber Kill Chain

The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

Identify threats

This phase identifies applicable threats to the proposed Windows 10 solution. This activity takes into consideration the GIAC business context and possible threat actors who might be interested in the business solution. The diamond model of intrusion analysis is applied when applicable different threat actors.

Based on applying above threat models, the threats and attack techniques that could be leverage against the new Windows 10 operating system.

Information disclosure

- Unauthorized access due to stolen credentials
- Unauthorized Access from unmanaged endpoint
- Malware attack not prevented by GIAC perimeter
- Endpoint compromise may go undetected
- Information Disclosure due to data exfiltration
- Lack of user awareness decreases the ability for users to operate their systems in a secure manner.

B. Risk Model

The overall impact and likelihood matrix shows the level of risk when each variable is combined. These definitions were considered when conducting the interviews with GIAC Employees and through a basic security assessment of the organization.

Likelihood

		Remote	Low Probability	Possible	Strong Probability	Probable
Impact	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Insignificant	1	2	3	4	5

The definitions used for impact are as follows:

Numeric Value	**Impact Rating**	**Description**
5	Catastrophic Impact / Zero Tolerance	Risk Tolerance for this risk occurring is zero. Loss of life Extreme financial exposure (e.g fines, penalties, remediation costs, increased capital expenditures) Financial ramifications requiring 10K disclosure or financial liquidity triggers, loss of market cap, or loss of market share Consider >$20MM Income Statement impact or >$75MM Balance Sheet impact and/or direct significant negative impact to 12 month and long-term strategy. Dramatic negative reputational impact and public exposure - customers, suppliers, regulators,

		employees.
4	Major Impact / Low Tolerance	Risk Tolerance for this risk occurring is low. Financial exposure resulting in potential for expenditures that may negatively impact earnings and DCF projections. Immediate senior management attention with ultimate board disclosure required. Required SOX disclosures or short term liquidity issues. Consider >$7MM - <=$20MM Income Statement impact or >$25MM - <= $75MM Balance Sheet impact and/or negative impact to 12 month and long-term strategy. Strong negative reputational impact and public exposure - customers, suppliers, regulators, employees.
3	Moderate Impact or Tolerance	Risk Tolerance for this risk is moderate with some level of occurrence or residual risk acceptable. Potential to financial exposure that would not be recoverable in the current budget Middle management remediation with reporting to board and executive management Consider >$7MM Income Statement impact or >$25MM Balance Sheet impact and/or direct significant negative impact to 12 month and

		long-term strategy. Some negative reputational impact and public exposure - customers, suppliers, regulators, and employees.
2	Minor Impact / High Tolerance	Risk Tolerance for this risk is high with limited constraints on occurrence or levels of residual risk. Financial exposure that is unexpected, but recoverable in the current budget Remediation with middle management attention Consider <=$1MM or no negative impact to 12 month and long-term strategy. General employee dissatisfaction could require heightened management involvement and communication.
1	Insignificant Impact / Unlimited Tolerance	Risk Tolerance for this risk is high with no constraints on occurrence or residual risk. Minimal strategic, financial, operational and reputational exposure or management attention.

The overall likelihood was based off of these descriptions:

Numeric Value	**Likelihood Rating**	**Description**
5	Probable > 90%	The event is already occurring or will almost certainly occur.

4	Strong Possibility 65-90%	The event has occurred recently or is expected to occur soon.
3	Possible 35-65%	The event has occurred in the past and/or is likely to occur in the future.
2	Low Possibility 5-35%	The event has occurred in the past but is unlikely to occur in the future.
1	Remote < 5%	The event has not occurred and is not expected to occur or will occur only in exceptional circumstances.

Risk Assessment for the GIAC Enterprise, based on the above definitions is as follows:

CIS CSC Top 6 for GIAC Enterprises	**Threat**	**Impact**	**Likelihood**	**Overall Risk Rating (I*L)**
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	Lack of user awareness decreases the ability for users to operate their systems in a secure manner.	4.50	5.00	22.5
CSC 9: Limitation and Control of Network Ports, Protocols, and Services	Unrestricted outbound communication could be used by command and control malware; competitors could also use outbound communications and glean details on what systems and browsers are leveraged by GIAC enterprises. A competitor could migrate to faster or better systems, or even launch a targeted attack to exploit these systems.	4.00	5.00	20.0
CSC 6: Maintenance,	A lack of a centralized view into the	4.00	5.00	20.0

Monitoring, and Analysis of Audit Logs	network traffic leaving GIAC Enterprises restricts the ability for the Security Team to respond to incidents.			
CSC 8: Malware Defenses	Although GIAC Enterprises uses Microsoft SCEP for basic Antivirus, the endpoints are still susceptible to more advanced malware and exploits.	4.00	4.00	16.0
CSC 7: Email and Web Browser Protections	The information that a browser sends when connecting to external websites can provide more information that GIAC Enterprises wishes to share. Additionally, browser history can be used by an adversary to track and target sites used by the organization for follow-on attacks e.g. watering hole attacks.	4.00	3.50	14.0
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	A lack of endpoint hardening is also contributing to unnecessary running services.	3.00	4.00	12.0

C. Tool Technical Reference

Most of the Windows 10 security recommendations are part of Windows operating system enhancements and the documentation and reference are available in Technet. Some reference articles are highlighted below:

https://technet.microsoft.com/en-us/library/mt601297(v=vs.85).aspx

https://technet.microsoft.com/en-us/library/mt158215(v=vs.85).aspx

Splunk is one of the leading SIEM solution and there are many references available on developing Splunk queries and dashboards for detecting suspicious and anomalous activities. Below webpage has some reference papers:

http://www.splunk.com/view/resources/SP-CAAAGWZ

Palo Alto Traps is advanced endpoint protection from Palo Alto networks. Below webpage has some reference papers:

https://www.paloaltonetworks.com/products/endpoint-security.html

D. Python Script for Data Analysis

The Security Team utilized a custom written Python script to rapidly and consistently analyze the packet captures. The script is as follows:

```
#! /usr/bin/env python
import pyshark
import csv
import sys


def get_ipv4_info(cap_file, display_filter):
    cap = pyshark.FileCapture(cap_file, display_filter=display_filter,
                              keep_packets=False)
    accum = []


    def ipv4_info(pkt):
        try:
            protocol = pkt.transport_layer
            src_addr = pkt.ip.src
            src_port = pkt[protocol].srcport
```

```
            dst_addr = pkt.ip.dst
            dst_port = pkt[protocol].dstport
            if protocol == "TCP":
                len_payload = int(pkt[protocol].len)
            elif protocol == 'UDP':
                len_payload = int(pkt[protocol].length)
            entry = dict(src_ip=src_addr, src_port=src_port,
                         dst_ip=dst_addr, dst_port=dst_port,
                         payload=len_payload, protocol=protocol)
            accum.append(entry)
        except AttributeError as e:
            pass

    cap.apply_on_packets(ipv4_info, timeout=10000)

    return accum

def get_ipv6_info(cap_file):
    cap = pyshark.FileCapture(cap_file, keep_packets=False)
    accum = []

    def ipv6_info(pkt):
        try:
            protocol = pkt.transport_layer
            src_addr = pkt.ipv6.src
            src_port = pkt[protocol].srcport
            dst_addr = pkt.ipv6.dst
            dst_port = pkt[protocol].dstport
            entry = dict(src_ip=src_addr, src_port=src_port, dst_ip=dst_addr,
                         dst_port=dst_port)
            accum.append(entry)

        except AttributeError as e:
            pass
```

```
    cap.apply_on_packets(ipv6_info, timeout=100)

    return accum

def get_icmp_info(cap_file, display_filter):
    cap = pyshark.FileCapture(cap_file, display_filter=display_filter,
                              keep_packets=False)
    accum = []

    def icmp_info(pkt):
        try:
            src_addr = pkt.ip.src
            dst_addr = pkt.ip.dst
            icmp_type = pkt.icmp.type
            icmp_code = pkt.icmp.code
            entry = dict(src_ip=src_addr, dst_ip=dst_addr,
                         icmp_type=icmp_type, icmp_code=icmp_code)
            accum.append(entry)
        except AttributeError as e:
            pass

    cap.apply_on_packets(icmp_info, timeout=100)

    return accum

def get_dns_info(cap_file):
    cap = pyshark.FileCapture(cap_file, keep_packets=False)
    accum = {}

    def dns_info(pkt):
        try:
            dns_name = pkt.dns.resp_name
            ip_addr = pkt.dns.resp_addr
            accum[ip_addr] = dns_name
        except AttributeError as e:
```

```
            pass

    cap.apply_on_packets(dns_info, timeout=10000)

    return accum

def main(pcap_file, source_ip):
    display_filter = 'ip.src==' + source_ip
    csv_file = pcap_file + ".csv"
    outbound_ipv4 = {}
    dns_list = get_dns_info(pcap_file)
    #icmp_list = get_icmp_info(pcap_file, display_filter)
    #ipv6_list = get_ipv6_info(pcap_file)
    ipv4_list = get_ipv4_info(pcap_file, display_filter)

    for item in ipv4_list:
        dest = item['dst_ip']

        if dest not in outbound_ipv4:
            outbound_ipv4[dest] = dict(tcp_data=0, udp_data=0, name='None')

        if item['protocol'] == 'TCP':
            outbound_ipv4[dest]['tcp_data'] += item['payload']
        elif item['protocol'] == 'UDP':
            outbound_ipv4[dest]['udp_data'] += item['payload']

        try:
            outbound_ipv4[dest]['name'] = dns_list[dest]
        except:
            pass

    with open(csv_file, 'w') as csvfile:
        csvfile.write('IP,TCP,UDP,Name\n')
        for key in outbound_ipv4:
            line = ('{},{},{},{}\n').format(key,
```

```
                                        outbound_ipv4[key]['tcp_data'],
                                        outbound_ipv4[key]['udp_data'],
                                        outbound_ipv4[key]['name'])
            csvfile.write(line)


if __name__ == "__main__":
    main(sys.argv[1], sys.argv[2])
```

E. Microsoft SCM Security Baseline for Windows 10

The following are the steps to get the Windows 10 security baseline installed on a test workstation. To note, if deploying to an enterprise, it is most effective to import the Group Policy Objects (GPOs) into Active Directory for deployment.

Windows 10 Security Baseline Install Steps

1. Download baseline settings to your desktop: http://blogs.technet.com/cfs-filesystemfile.ashx/__key/telligent-evolution-components-attachments/01-4062-00-00-03-65-56-14/Win10_2D00_IE11_2D00_Baselines_2D00_DRAFT.zip
2. Unzip to desktop
3. Download EMET 5.2: https://www.microsoft.com/en-us/download/confirmation.aspx?id=46366
4. Copy the setup.msi file to the extracted folder Win10-IE11-Baselines-DRAFT\Local_Script\EMET and rename the setup file to EXACTLY this: **EMET Setup.msi**
5. Right click on the 10_Client_Install.cmd and run as an admin to install the baseline settings into the local group policy.
6. Next, create a local user account. Now that the baseline is applied, you need to come up with a long and complex password (or change the setting).
7. Run → mmc
    a. add the Group Policy Object editor
    b. Set for the local machine
    c. Once added, save the .msc to your desktop as policy.msc and then close it.
    d. Right click on the policy.msc file and run as an admin
8. Now change the following two security settings:

   a. in the Group Policy Object editor, expand Local Computer Policy -> Windows Settings -> Security Settings -> Local Policies -> Security Options
   b. Enable Interactive logon: Do not display last user name
   c. Disable Interactive logon: Do not require CTRL+ALT+ DEL
9. Finally, run -> netplwiz
   a. make sure the "Users must enter a username and password to use this computer" has a check mark. If not put a checkmark in the box and hit apply
10. Shutdown and take a snap shot.
11. When you power back on, you will have the new settings applied. Make sure you logon with your normal user account to perform tests/captures.
12. Additionally, you can apply more restrictive privacy policies. An explanation of these privacy settings can be found in Appendix E.

F. Group Policy and Privacy Settings Map

This table shows the group policy setting, its privacy implication (if known) and the loss of functionality (if known) if it is disabled.

Setting	UI	GPO	Setting Location	Description & Privacy Implication	Loss of Feature
Cortana		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Search** > **Allow Cortana** > **Disabled**	Microsoft collects and uses information including your device location information and location history, contacts (People), voice input, searching history, calendar details, content and communication history from messages and apps, and other information on your device. In Microsoft Edge, Cortana collects and uses your browsing history. This information is saved on your device, in your Cortana	No voice activated commands or assistance.

				Notebook, and in the cloud on the Bing.com dashboard.	
Device metadata retrieval		x	**Computer Configuration** > **Administrative Templates** > **System** > **Device Installation** > **Prevent device metadata retrieval from the Internet** > **Enabled**	Device metadata is downloaded/pulled from the Internet	More detailed information might be lacking for installed devices.
Insider preview builds		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Data Collection and Preview Builds** >**Toggle user control over Insider builds**> **Disable**		Prevents the downloading of bleeding edge OS from Microsoft
Internet Explorer (IE)		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > Turn on Suggested Sites > **Disabled**		Limits the amount of sites that may be suggested by a user's search behavior.
IE		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > Allow Microsoft services to provide enhanced suggestions as the user types in the Address Bar > **Disabled**		Limits targeted search suggestions.
IE		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > Turn off the auto-complete feature for web addresses > **Enabled**		Autocompleting can help save time when searching. This feature would be disabled.
IE		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Disable Periodic Check for Internet Explorer software updates** > **Disabled**	This setting should remain **enabled** if the system is managed with SCCM or other centralized patch	Can leave the browser exposed to attacks if not centrally managed.

				management solution.	
IE		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer > Turn off browser geolocation > Enabled**		Limits apps and settings that might use geolocation.
Mail synchronization	x		**Settings** > **Accounts** > **Your email and accounts**, remove any connected Microsoft Accounts		
Microsoft Edge		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Microsoft Edge > Allow employees to send Do Not Track headers> Enabled** **Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge> Turn off address bar search suggestions> Disabled**	Browsing data and information about malicious websites is sent back to Microsoft to assist with page prediction and SmartScreen.	Auto search help functions are disabled.
NCSI		x	**Computer Configuration** > **Administrative Templates** > **System** > **Internet Communication Management** > **Internet Communication Settings** > **Turn off Windows Network Connectivity Status Indicator active tests > Enable**		Limits the client from checking to see if the Internet is accessible.
Offline maps		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Maps** > **Turn off Automatic Download and Update of Map Data > Enable**	No setting found in our Windows 10 image.	
OneDrive		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **OneDrive** > **Prevent the usage of OneDrive for file storage > Enable**		Users cannot use OneDrive to centrally store their files in the cloud.

Preinstalled apps	x		To remove the News app: ● Right-click the app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.BingNews"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingNews \| Remove-AppxPackage** To remove the Weather app: ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online \| Where-Object {$_.PackageName -Like "Microsoft.BingWeather**		Limits app specific functionality such as news feeds, weather, etc.

			"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingWeather \| Remove-AppxPackage** To remove the Money app: ● Right-click the app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online \| Where-Object {$_.PackageName -Like "Microsoft.BingFinance" } | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName} ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command:		

			Get-AppxPackage Microsoft.BingFinance | Remove-AppxPackage To remove the Sports app: ● Right-click the app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.BingSports"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingSports | Remove-AppxPackage** To remove the Twitter app: ● Right-click the app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows		

			PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "*.Twitter"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage *.Twitter \| Remove-AppxPackage** To remove the XBOX app: ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online \| Where-Object {$_.PackageName -Like "Microsoft.XboxApp"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt,		

			run the following Windows PowerShell command: **Get-AppxPackage Microsoft.XboxApp | Remove-AppxPackage** To remove the Sway app: ● Right-click the app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.Office.Sway"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.Office.Sway | Remove-AppxPackage** To remove the OneNote app: ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command:		

			Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.Office.OneNote"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.Office.OneNote \| Remove-AppxPackage** To remove the Get Office app: ● Right-click the app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online \| Where-Object {$_.PackageName -Like "Microsoft.MicrosoftOfficeHub"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName} ● -and-		

			● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.MicrosoftOfficeHub | Remove-AppxPackage** To remove the Get Skype app: ● Right-click the Sports app in Start, and then click **Uninstall**. ● -or- ● Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.SkypeApp"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}** ● -and- ● Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.SkypeApp | Remove-AppxPackage**		

Settings > privacy					
General		x	**Computer Configuration > Administrative Templates > System > User Profiles > Turn off the advertising ID > Enabled**		
Location		x	**Computer Configuration > Administrative Templates > Windows Components > Location and Sensors > Turn off location > Enabled**		
Camera		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access the camera > Disabled**	This setting was not found in our image; however, it might be a good idea to disable in a secure environment.	App functionality might be reduced if it relies on a camera.
Microphone		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access the microphone > Disabled**	This setting was not found in our image; however, it might be a good idea to disable in a secure environment.	App functionality might be reduced if it relies on a camera.
Speech, inking, & typing		x	**Computer Configuration > Administrative Templates > Control Panel > Regional and Language Options > Handwriting personalization > Turn off automatic learning > Enabled**		Limits app customization because it cannot learn behavior.
Account info		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access account information > Set the Select a setting box to Force Deny**		

Contacts		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access contacts > Disabled**		
Calendar		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access the calendar > Set the Select a setting box to Force Deny**		
Messaging		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access messaging > Set the Select a setting box to Force Deny**		
Radios		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps control radios > Set the Select a setting box to Force Deny**		
Other devices		x	**Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access trusted devices > Set the Select a setting box to Force Deny**		
Feedback & diagnostics		x	**Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Do not show feedback notifications > Enabled**		
Background apps	x		Turn off the feature in the UI for each app		
Software Protection Platform		x	**Computer Configuration > Administrative Templates > Windows Components > Software**	This setting sends Key Management	Limits the client's ability to activate.

			Protection Platform > **Turn off KMS Client Online AVS Activation** > **Enabled**	Service (KMS) client activation data to Microsoft automatically. Enabling this setting prevents this computer from sending data to Microsoft regarding its activation state.	
Sync your settings		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Sync your settings** > **Do not sync** > **Enabled**		Settings are not synced with any other devices.
Teredo			**netsh interface teredo set state disabled**		Limits the system's ability to communicate with IPv6 devices.
Wi-Fi Sense		x	**Computer Configuration** > **Administrative Templates** > **SCM: Wi-Fi Sense** > **Disable Wi-Fi Sense** > **Enabled**		Removes the ability to enumerate and connect to WiFi discovered to be used by the user's contacts.
Windows Defender		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Defender** > **MAPS** > **Join Microsoft MAPS** > **Disabled**	Depending on the organization's privacy policy, it might be worth considering enabling this to share threat/virus detection info with Microsoft.	Limits the system's ability to share virus information with Microsoft.
Windows Media Player	x		From the **Programs and Features** control panel, click **Turn Windows**		Limits the ability for users to leverage

			features on or off, under **Media Features**, clear the **Windows Media Player** check box, and then click **OK**		the built-in media player.
Windows spotlight		x	**Computer Configuration** > **Administrative Templates** > **Control Panel** > **Personalization** > **Force a specific default lock screen image** > **Enabled** • Add a location in the **Path to local lock screen image** box.		Limits the user's ability to customize a lock screen image.
Windows Store		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Store** > **Disable all apps from Windows Store** > **Enabled**	This setting was not found on the image we were working with. If the endpoint is in an enterprise or managed by SCCM, the store should be disabled to help keep tabs on what applications are installed. For individual deployments, this could be left enabled.	Limits the ability for the apps to contact the Windows Store for updates.
WU Delivery Optimization		x	**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Delivery Optimization** > **None**	Setting was not found in the modern.ie image. This depends on the environment, but if at an enterprise, it might make more sense to	The ability rapidly download and install updates is impacted.

				centrally manage-- however, this setting could cut down on bandwidth requirements.	
Windows Update			**Computer Configuration** > **Administrative Templates** > **Windows Components > Do not connect to any Windows Update Internet locations** > **Enabled**	This setting depends on the environment and whether or not the systems are centrally managed.	

G. Windows 10 Security Features

Windows 10 is designed to protect against known and emerging security threats across the spectrum of attack vectors.

Domain	Windows 10 Security Feature	Description of risk mitigation	Recommendation
Identity	Microsoft Passport	Microsoft Passport replaces	Biometric

Protection		passwords with strong two-factor authentication that consists of an enrolled device and a Windows Hello (biometric) or PIN.	authentication and enterprise grade two-factor authentication in Windows 10 will help protect GIAC business data and online experiences without the need for regularly changing passwords.
	Microsoft Hello	Hello replaces the need for a password to log in, which is both more secure and harder to forget. A PIN is generated which is backed by your biometric information; this is more secure as these are valid only on registered device.	
	Microsoft Azure Active Directory		
	User Access Control(UAC)	User Account Control (UAC) helps prevent malware from damaging a computer and helps organizations deploy a better-managed desktop environment.	
Data Protection	Bitlocker	BitLocker has provided encryption for full drives and portable drives; in Windows 10, BitLocker will even protect individual files, with data loss prevention capabilities.	BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately

			decommissioned computers.
	Enterprise data protection - (EDP)	Enterprise Data Protection makes it easier to perform data separation and containment of corporate data – wherever it might be. Windows acts as an access control broker that gates user and app access to protected data based on the policies that you define.	With the increase of employee-owned devices in the GIAC enterprise, there's also an increasing risk of accidental data disclosure through apps and services that are outside of the enterprise's control like email, social media, and the public cloud. EDP helps to mitigate that threat.
Malware Resistance	Device Guard	Device Guard is a combination of enterprise-related hardware and software security features that, when configured together, will lock a device down so that it can only run trusted applications. If the app isn't trusted it can't run, period. It also means that even if an attacker manages to get control of the Windows kernel, he or she will be much less likely to be able to run malicious executable code after the computer restarts because of how decisions are made about what can run and when.	Device Guard protects against APT and advanced threats.
	Credential Guard	Credential Guard uses hardware to isolate	This isolation helps prevent Pass the

		Windows authentication services (LSA) and user's derived credentials (e.g., NTLM hashes and Kerberos tickets) using virtualization based security and Hyper-V.	Hash attacks, which enable attackers to steal identities and impersonate network users.
	Windows Defender	Anti-malware solution	
	Microsoft Edge	Microsoft Edge is a Universal App that does not run older binary extensions, including Microsoft Active X and Browser Helper Objects (BHO) frequently used for toolbars, thus eliminating risks related to browser add-ons. Edge uses AppContainer-based sandboxing to protect the system from vulnerabilities that may be discovered in the extensions running in the browser (for example, Adobe Flash, Java) or the browser itself.	Microsoft Edge has features like Smartscreen, sandboxing which protects GIAC assets from drive-by web based infections.
	Applocker	AppLocker helps you control which apps and files users can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers.	Applocker prevents successful installation of malware and protects GIAC assets.
	Windows Firewall	Windows Firewall blocks traffic which is not explicitly allowed	Windows Firewall will protect GIAC assets from unwanted network communications.
	Enhanced Mitigation Experience Toolkit (EMET)	Enhanced Mitigation Experience Toolkit (EMET)	EMET will protect GIAC from

		protects against cyberattacks, by helping detect and block exploitation techniques that are commonly used to exploit memory corruption vulnerabilities. EMET anticipates the most common actions and techniques adversaries might use in compromising a computer, and helps protect by diverting, terminating, blocking, and invalidating those actions and techniques.	unknown malware and exploitation techniques.
	Windows Update for Business	Streamlining patch management process	
	Local Administrator Password Solution (LAPS)	Compromised identical local account credentials could allow elevation of privilege if an attacker uses them to elevate from a local user/administrator to a domain/enterprise administrator. Local administrator credentials are needed for occasions when logon is required without domain access. In large environments, password management can become complex, leading to poor security practices, and such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack.	LAPS simplifies password management while helping GIAC implement recommended defenses against cyberattacks. In particular, the solution mitigates the risk of lateral escalation that results when customers use the same administrative local account and password combination on their computers.
	Conditional access	The Windows Device Health Attestation cloud service used in concert with management system such as Microsoft Intune can provide Conditional access services that help prevent	Conditional access help prevent untrustworthy devices from gaining access to corporate resources.

		untrustworthy devices from gaining access to corporate resources.	
Device Security	Trusted Boot	Windows 10 closes off the pathways that allow malware to hide from the OS by starting first. Using hardware-based virtualization, key processes are also isolated from the system so they cannot be tampered with.	

Last Updated: September 18th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Bahrain September 2019	OnlineBH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced