Using Windows 10 and Windows Server 2016 to create an Endpoint Detection and Response solution

Sebastian Godin

Using Windows 10 and Windows Server 2016 to create an Endpoint Detection and Response solution

GIAC (GCIH) Gold Certification

Author: Sebastien Godin, sebastien.godin@gmail.com
Advisor: Christopher Walker, CISSP, CCISO, GCED, GWEB

Accepted: December 31, 2017

Abstract

It has been established best practice to supplement Microsoft Windows with third-party endpoint security solutions that defend against viruses, malware, internet-based, and other threats. With each iteration of Windows, Microsoft has added security measures that are native to the OS like Windows Defender, Security policy editor, and more. Microsoft has made many noticeable advances in Windows 10 and Windows Server 2016 that improves the overall security posture of endpoints. This new modern Windows enterprise ecosystem, when utilized properly, can be leveraged like an Endpoint Detection and Response capability. This capability can be achieved without third party software and can reduce costs to the enterprise that can be reinvested into other projects.

1. Introduction

A market that is rapidly expanding is protecting client machines and endpoints. This shift in focus is happening because the IT Security domain is finding that protecting perimeters is no longer sufficient and that there needs to be an expansion of the capabilities that an enterprise uses to defend itself. There has been a growing number of companies offering Endpoint Detection and Response (EDR) products. A Gartner study listed over thirty different EDR products (Firstbrook and MacDonald, 2016) and this list was not exhaustive. The average enterprise spends between $5 and $25 per seat per year for licensing of commercial EDR solutions (Firstbrook and MacDonald, 2016). If the costs of possible infrastructure and training are added, the bill can go up quickly. The reverse side of that is that according to the Ponemon Institute, the cost of unsecured endpoints in 2016 is $612.45 on average per endpoint ("The Cost of Insecure Endpoints," 2017). Also, as stated by security professionals, endpoints are often used as entry points by threat actors, and they agree that protecting them is essential to the overall security of the network ("Endpoint Detection and Response (EDR)." 2015). It is more advantageous to have protection than not, but if money and time can be saved with built-in tools, then more resources can be poured into other security mechanisms or diverted to other projects. There are many options to choose from, and they all offer varying levels of capability, so choosing one can be a daunting task. Most solutions focus on protecting Windows machines and networks since they are the majority of the market. Microsoft has expended a lot of effort throughout the years in improving Windows' security, and in Windows 10 they have implemented more effective native endpoint tools, especially in conjunction with Windows Server 2016. If these native tools are capable of protecting the system without third-party software, it could be very advantageous for enterprises. By using tools that are already part of the system the cost of licensing, installation, maintenance, and training would be reduced. This paper will explore if these new security tools offered with Windows 10 and Windows Server 2016 can be considered an EDR.

Sebastien Godin.
Sebastien.godin@gmail.com

2. Endpoint Detection and Response (EDR)

2.1. The Problem Space

In defining an EDR solution, it is important to understand what problem it is trying to solve. The Incident Handling Cycle is a good guide. We will define the EDR capability based on where it is used in the incident handling cycle. Using the Security Architecture model presented by Gartner in figure 1, the overarching steps of the incident handling process can be seen.

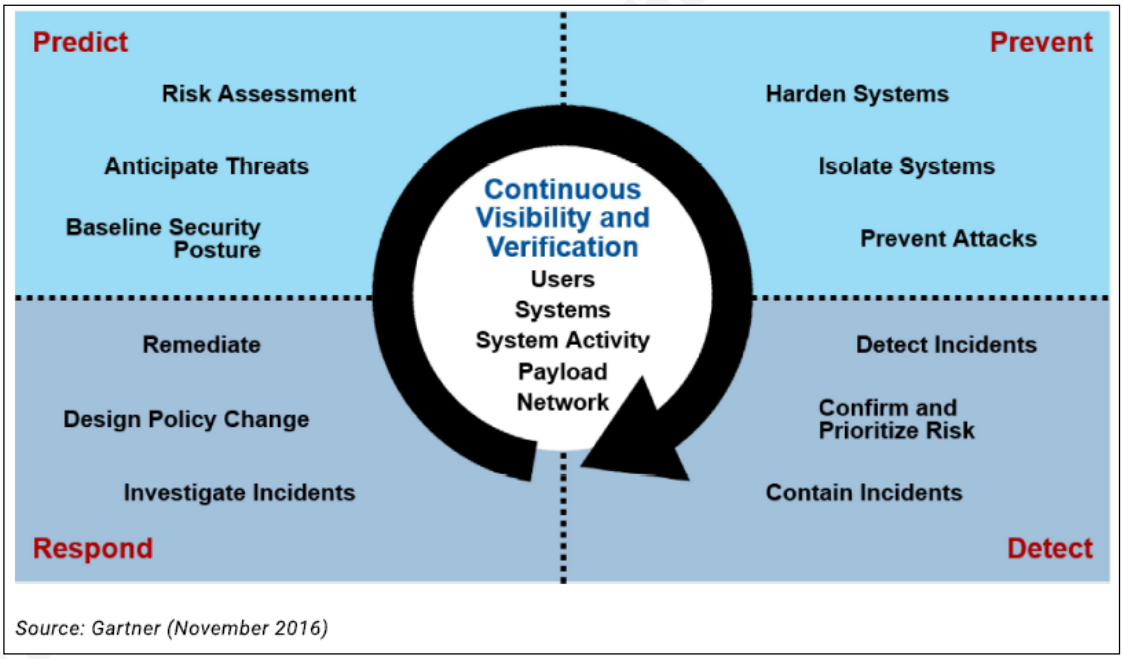

Figure 1. **Adaptive Security Architecture (Firstbrook and MacDonald, 2016).**

By looking at the model and using the name of the solution as a reference, it can be seen that the focus is on the bottom half of figure 1, the Detection and Response stages or the Identification, Containment, Eradication, and Recovery steps. As Lord (2017) states: "all endpoint detection and response tools perform the same essential functions with the same purpose: to provide a means for continuous monitoring and analysis to more readily identify, detect, and prevent advanced threats." Therefore, an EDR solution helps the incident handler post-breach in the swift resolution of the incident and the quick return to a pre-incident operational state preventing further breaches of that nature.

Sebastien Godin.
Sebastien.godin@gmail.com

2.2. EDR defined

By looking at the solution proposed above, it can be seen that to be considered an EDR there are minimum requirements that can be established. According to Gartner, there are four primary capabilities required for EDR solutions: Detection, Containment at the endpoint, a capability to investigate the incident and to help with remediation (Firstbrook and MacDonald, 2016). To provide these capabilities, there are several key functions that an EDR must offer. The security tool resides on the endpoint and stores information either locally (for remote query) or in a centralized database. The EDR solution is capable of detecting signs of illicit activity by monitoring the endpoint directly. It uses indicators of compromise or other forms of detection rules identifying attacks. Following detection, there must be a way for the investigator to query the endpoint and other sources to confirm the history of the incident and the extent of the damage, so logging all critical activities of the endpoint is essential. The tool should also be capable of sending data to another security tool like a Security Information and Event Management (SIEM) capability. The EDR then helps with the containment of the illicit activity. Multiple actions can be taken to achieve containment like putting the machine in quarantine, reimage it, isolation from the network, or interactions with the affected processes (Firstbrook and MacDonald, 2016). Another important function is that once detection of an intrusion happens, the capability stops the spread of intrusion to other endpoint components as well as other parts of the network by putting the system offline or in a quarantine state to enable safe investigation. The tool has to be capable of helping with the investigation of detected incidents. It should also be capable of enabling system auditing to confirm the patch and configuration status, and changes as directed by the security staff. Finally, the tool helps with remediation and cleaning of the compromised endpoint, either directly or by facilitating other methods. Other useful features that could give an extra layer of protection include configuration enforcement, inventory tracking, and pushing configuration changes as required.

Sebastien Godin.
Sebastien.godin@gmail.com

3. Windows 10 and Windows Server 2016 Tools

3.1. Introduction

As discussed there are tools within Windows 10 Enterprise Creators update version 1703 that when utilized in conjunction with Windows Server 2016 datacenter version 1711 work like an EDR. As there is ample literature that describes each tool in technical detail, the paper will go through the principal ones that are relevant to this discussion and only focus on how these tools can be used as an EDR (Figure 2). At the endpoint, the focus will be on the capabilities of Windows Defender and other ingrained protection features. For Windows Server 2016 there are three tools that will be discussed: Group Policy Object (GPO), Windows Event Forwarder (WEF), and PowerShell. Of note, Microsoft is pulling support for the Enhanced Mitigation Experience Toolkit (EMET) stating that Windows 10 has other features that do the same thing or better (Hall, Brower, D'Souza-Wiltshire, Lich, & Méndez, 2017), so EMET will not be evaluated.

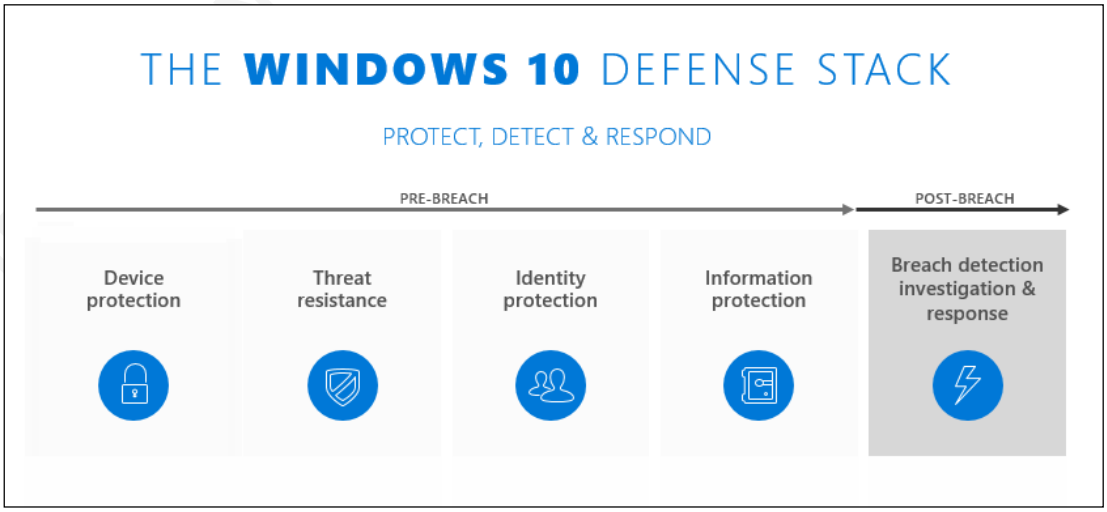

Figure 1. **Windows 10 defense stack. (Hall et al., 2017)**

3.1.1. Windows Defender

Starting with the primary means of defending the endpoint, Windows Defender is the first line. Windows defender contains five sub-functions: Firewall, Antivirus, Exploit Guard, Application Guard, and SmartScreen (Lich, Brower, Ross, & Poggemeyer, 2017). These can be controlled locally through Windows Defender Security Center console.

Sebastien Godin.
Sebastien.godin@gmail.com

These five functions specialize and focus on preventative defense by applying known security measures and known indicators of compromise. Windows Defender Antivirus does well against other commercial options when evaluated in independent testing like the ones conducted by AV-TEST, see Figure 3.

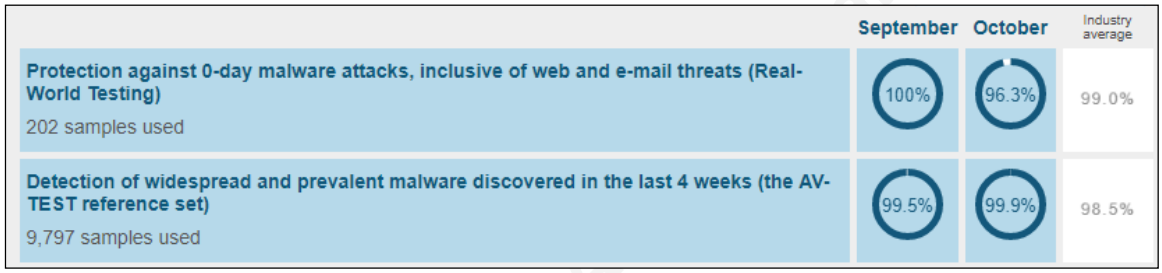

***Figure 2*. AV-TEST for Windows Defender. (AV-TEST, 2017)**

Regarding antivirus and antimalware protection, it is equivalent to commercial solutions. Also, concerning a Firewall capability, Windows Defender Firewall is a complete solution, enough so that there are commercial antivirus solutions that rely on it and only give Windows Defender Firewall a different management GUI. Other features are more on the prevention side like the Unified Extensible Firmware Interface (UEFI) and Device Health Attestation (DHA) that protect the device pre- and post-boot-up by verifying against known good images and signatures to prevent boot-loaders and rootkits. There are also programs like Device Guard and AppLocker that can create whitelists of approved software that can run on the endpoint. Each of these can be used both for proactive protection and to help with incident analysis post-breach (D'Souza-Wiltshire, Brower, and Lich, 2017). These protection measures utilize many system components within the Windows infrastructure to protect the endpoint making it challenging for an attacker to hide their traces with all of these measures.

3.1.2. Group Policy Object (GPO)

GPO is essential for system administrators in the management of a Windows network and is also key in helping with the enterprise's security posture by ensuring that known bad situations are either blocked or can be monitored helping provide the detection and containment functions of an EDR. GPO can set the values and settings of every component on the Windows 10 machine including Registry Keys and all of

Sebastien Godin.
Sebastien.godin@gmail.com

Windows Defender's capabilities. Whenever an endpoint fails a GPO integrity check, through auditing, figure 4, that failure can be logged. Windows Management Instrumentation (WMI) filters can then be used to take action including overwriting the changes with the proper policies to putting the machine in quarantine and everything in between (Pyle, 2008).

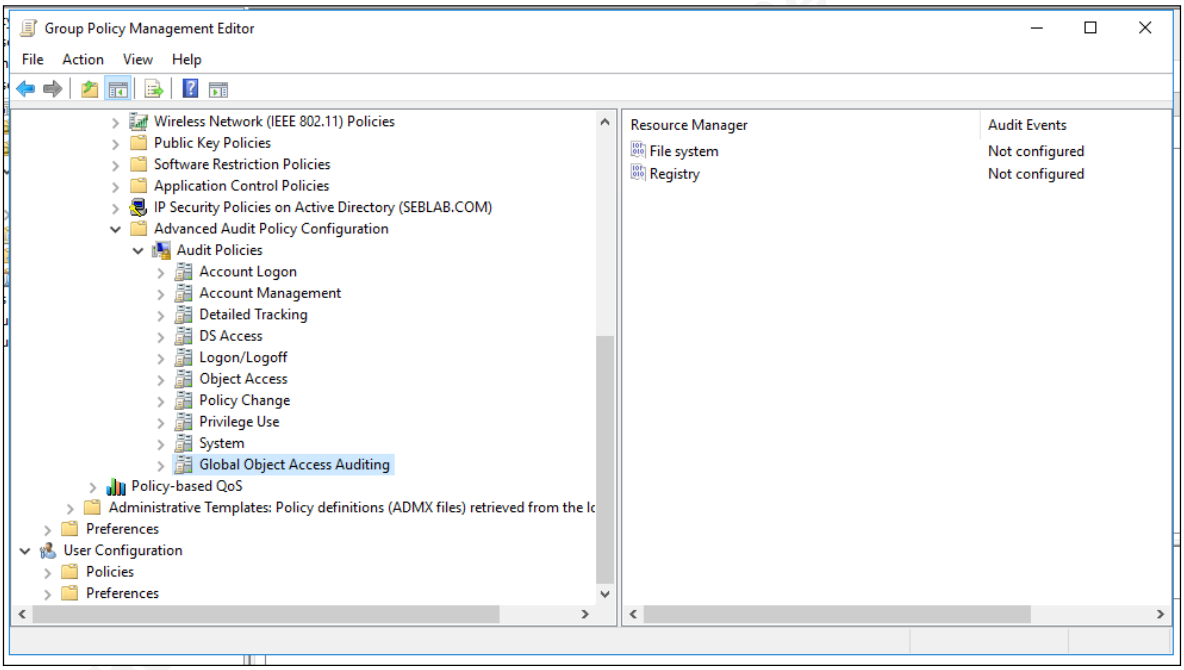

***Figure 3*. GPO Audit policy options.**

Another strength of GPOs is that they can be readjusted on the fly by pushing new GPOs to a specific device or groups of devices once a compromise is detected to stop further proliferation. There are many sites like the National Institute of Standards and Technology (NIST) as well as Microsoft TechNet that have many templates and recommendations on how to create proper GPOs. Windows Server 2016 has made the management of GPOs and audit policies simpler by integrating both into the same Group Policy Management Editor.

3.1.3. Windows Event Forwarder (WEF)

WEF permits a server designated as an event collector to receive all the events from endpoints that are selected by IT and security staff. Windows can generate events in a very granular fashion for everything that can happen on an endpoint. This event

Sebastien Godin.
Sebastien.godin@gmail.com

logging capability is the keystone that turns everything that has been talked about so far into an EDR solution. These logs can be fed into a SIEM that can analyze them in real time and can react or give advice accordingly. The logs can be used to find a post-breach compromise in conjunction with GPO rules and also help in the forensic investigation since they capture all the event history from endpoints (Hardy, Brower, Borg, Hall, and Lich, 2017). Multiple logs can be created depending on the needs of the staff; there can be logs for system administrators and logs for security personnel, permitting a focus on monitoring relevant data to prevent information overload. Also, a key point for WEF is that all traffic can be encrypted via Kerberos to prevent tampering or data capture. Additionally, endpoints can send events to multiple event collectors to ensure high availability and redundancy.[1]

3.1.4. PowerShell

PowerShell is a powerful tool for system administrators by helping them do management functions through scripting. PowerShell can also be utilized for protecting a network's endpoints, discovering incidents, forensic analysis, and resolution. There is a considerable amount of automation that PowerShell provides and scripts that can help in the security posture of a cyber defender. PowerShell can be used to conduct live response to incidents by being able to capture volatile memory and other artifacts on a live system both remotely or locally (Nair, 2013). However, PowerShell is a double-edged sword. Because it is native and essential to Windows, it cannot be turned off completely. Tools like PowerSploit, Invoke-Mimikatz, and many others provide PowerShell functions that conduct reconnaissance, lateral movement and help with further exploitation (Metcalf, 2016b). That is why Microsoft introduced additional security features in version 5. Script Block Logging logs the actual code that is executed on the endpoint and sends it to WEF, even if the original code is obfuscated prior to execution. The System-wide Transcripts feature creates a transcript of all commands executed on a machine by the user. Constrained PowerShell does not allow access to the Windows Application Programming Interface (API) or .NET scripting commands if the script is not approved in Applocker whitelists or has a valid signature. Without being whitelisted, the script will

[1] This reference offers an in-depth breakdown and how-to in using WEF for intrusion detection (Hardy, Brower, Borg, Hall, and Lich, 2017).

only have limited execution capabilities. Lastly, Antimalware Scan Interface (AMSI), in conjunction with Windows Defender, scans all scripting languages for dynamic content before allowing a script to run (Metcalf, 2016a).

3.1.5. Windows Defender Advanced Threat Protection (ATP) and System Center 2016

For additional Windows 10 endpoint protection, Windows ATP and System Center 2016 bring potent capabilities to help protect an enterprise network. These tools help in the prevention, detection, and response to breaches. ATP adds machine learning, behavioral analysis, and automation. Threat Intelligence from Microsoft and sources determined by the system administrator are integrated in real time into the detection and analysis of anomalous activity. By only sending alerts that have already passed through additional analysis ending up sending less but more relevant information to the SIEM, permits the SIEM to be more efficient and smarter about what is being analyzed. Windows Defender ATP also brings a single graphical user interface for the configuration and usage of the security features, making it easier for the security analyst by reducing the number of interfaces that need to be interacted with (Barnett, Tillman, Agiewich, and Bigman, 2017). Windows System Center 2016 has a module called Endpoint Protection within the Configuration Manager. This module permits unified management and monitoring of all Windows Defender's and ATP's capabilities. As a bonus there are Endpoint Protection Clients for both Mac and Linux systems, permitting a view and management of non-Windows endpoints (Tillman et al., 2017).

4. Scenarios

In evaluating how the Windows ecosystem acts like an EDR, a few scenarios will be looked at and evaluated to see how the system can be used to react. The focus will be on post-breach incidents that are of a more sophisticated nature and how the ecosystem can help in detection and response. For most of the following scenarios, the assumption that a successful exploit has occurred on the endpoint and has not been discovered using the Windows 10 defense mechanisms within Windows Defender and other security protocols.

Sebastien Godin.
Sebastien.godin@gmail.com

4.1. Creating covert tunnels

The first case will be when an attacker succeeds in building a covert tunnel to be able to communicate and exfiltrate information. If the attacker creates a tunnel over an uncommon port and has to create an exception within the Windows Defender Firewall, rule changes can be caught using two methods. Firstly, when a rule changes within an endpoint in the Firewall and WEF is turned on, Figure 5, event ID 2004/2006 is sent when there are modifications to the Firewall, Figure 6, a task, Figure 7, that will launch a program or PowerShell script, figure 8, to respond to the event can easily be created (Melber, 2010).

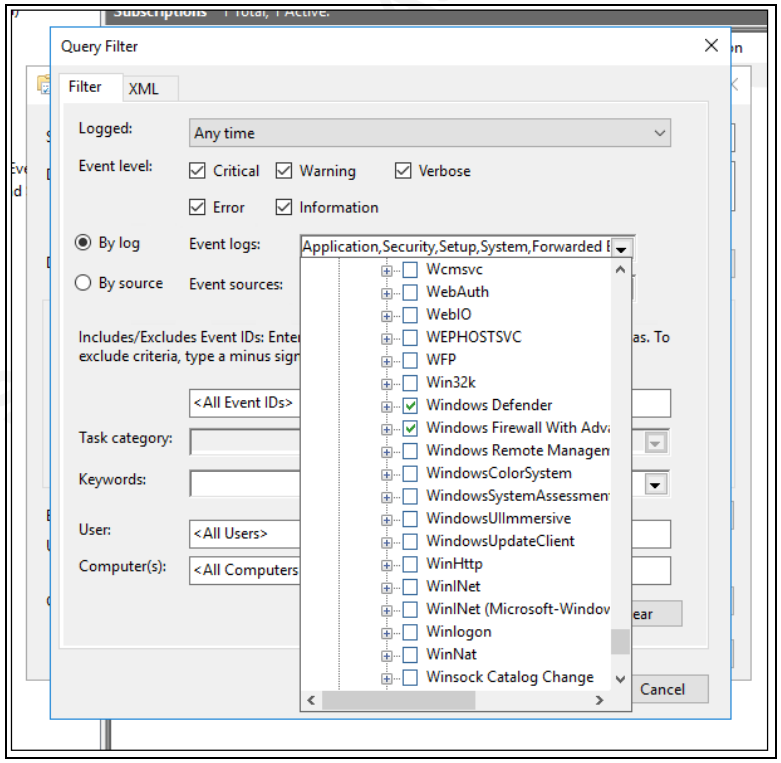

***Figure 4*. Selection of security logs related to Windows Defender and Windows Defender Firewall.**

Sebastien Godin.
Sebastien.godin@gmail.com

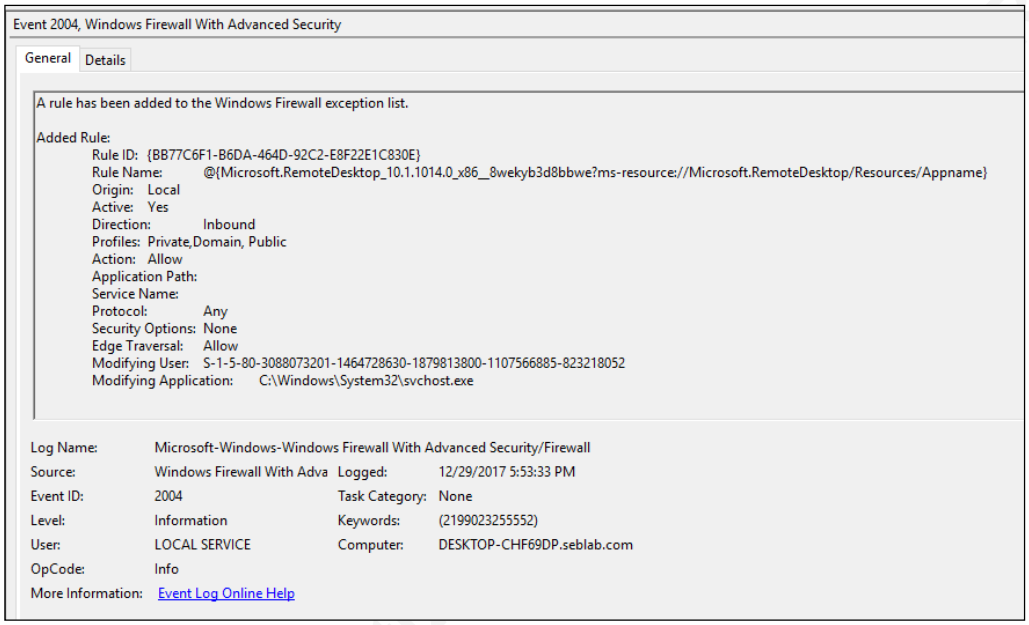

Figure 5 - Example of event viewer message in logs, ID 2004: "A rule has been added to the Windows Firewall exception list."

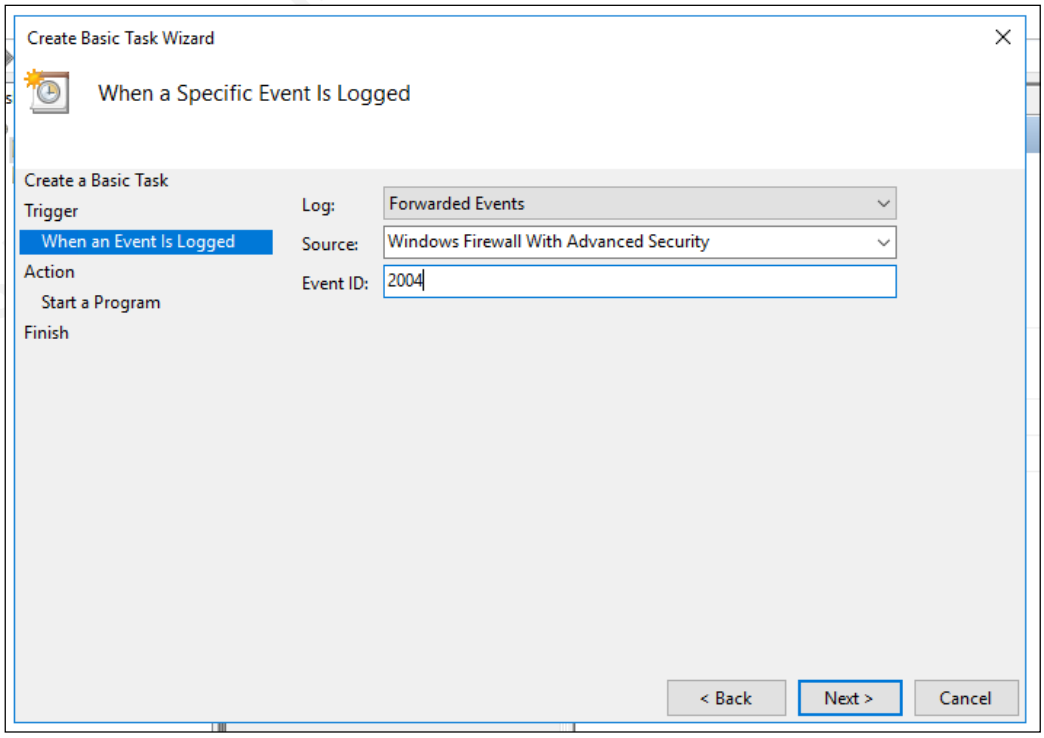

***Figure 6*. Creating a task that will respond to ID 2004.**

Sebastien Godin.
Sebastien.godin@gmail.com

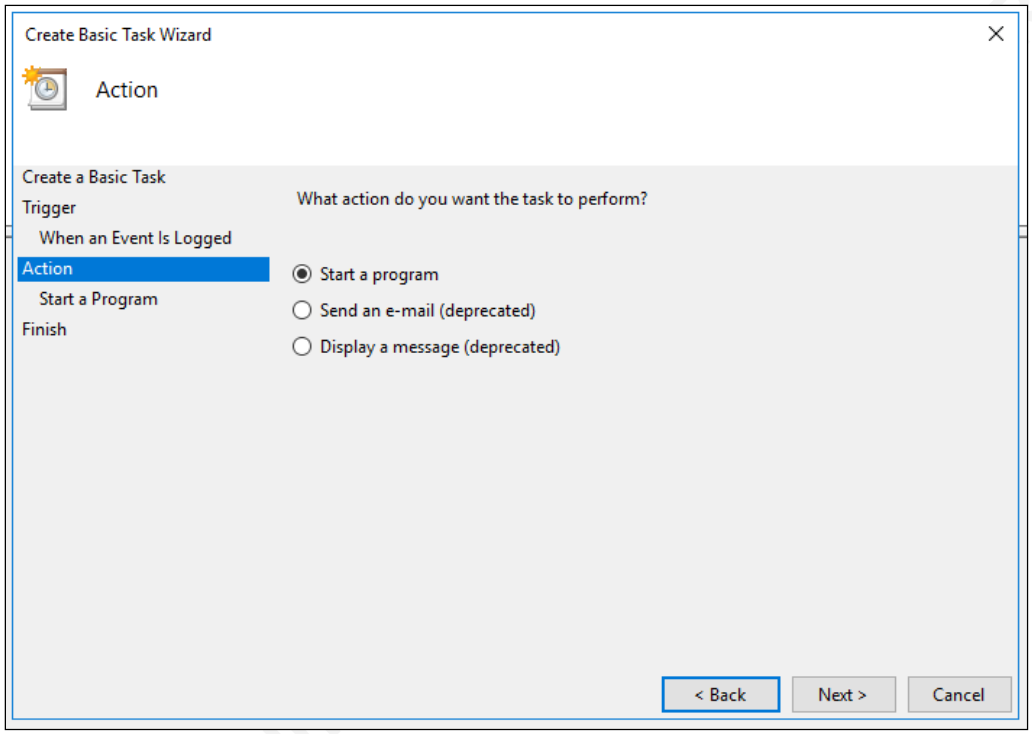

***Figure 7*. Possible response actions.**

If Windows Event Forwarder does not catch the event, GPO audits can be used to detect the change. A GPO audit would compare the firewall rules on the endpoint to the enterprise GPO, and flag any discrepancies. However, this will not work if the port was already open. For example, if port 80 or 443 are used to exfiltrate the data. Then it is a matter of having a whitelist of programs that are allowed to create communications outbound and disallowing anything else. This will block the attacker's script when it attempts to establish an outbound connection. If the enterprise's policy for outbound connection is to allow all that do not fall within the Firewall rules, then a log of all programs that do not fall within an approved rule can be created and if something is written in this log, it triggers an investigation. For containment and remediation, as discussed earlier with Tasks and WMI filters, a special GPO can be applied to the compromised endpoint with whatever actions the security personnel wants. Staff can then use PowerShell and WEF to do forensic and timeline analysis of the incident.

4.2. Lateral movement

Once an attacker has gained a foothold within a network, they want to be able to move through the system to find information to be able to extend their access and to find

the most valuable information. To avoid redundancy, only the steps that are unique in this situation will be discussed. First of all, through GPO and Firewall settings, there can be restrictions on the methods of communication that are allowed within the network.

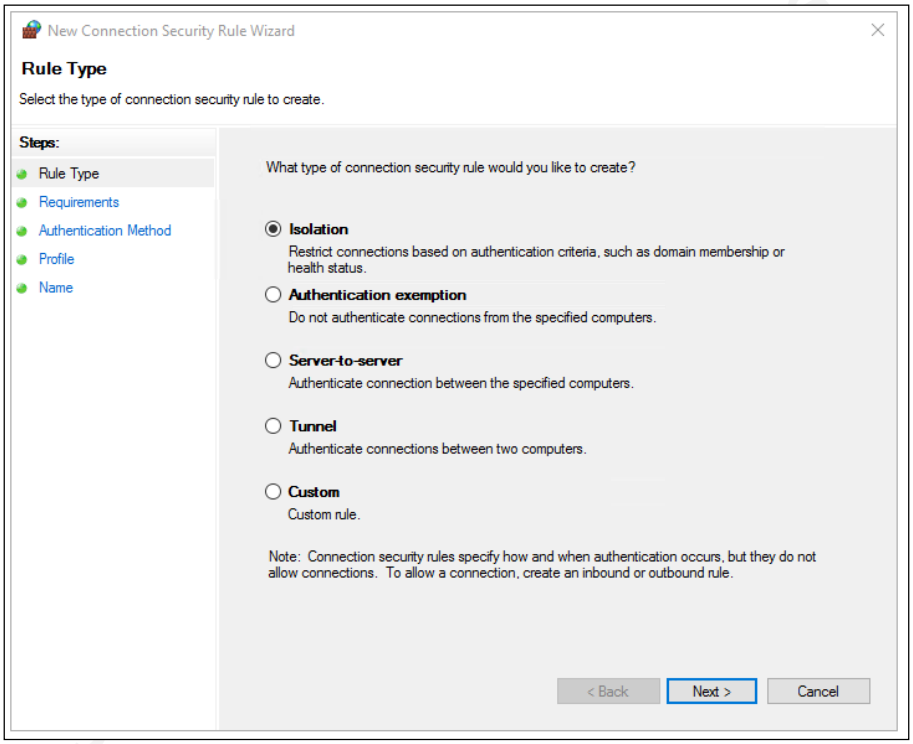

Figure 8. **Types of connections that rules can be created for Connection Security Rules and GPO.**

These rules can then be specific to the type of connections allowed on the network by the enterprise. Unless necessary, all communication between endpoints should be blocked, and if two endpoints need to communicate, then a special tunnel rule should be put in place and logged in WEF. If this is not possible either, then WEF in combination with Windows Defender Firewall and IPSec rules can log when computers communicate with ranges of IP addresses that represent endpoints, and this can initiate an investigation ("Configure NAP Enforcement Clients in Group Policy," 2012).

4.3. Covering Tracks

When an attacker is on a system and wants to stay there, they will want to hide their presence and also how they got into the system. To achieve this, an attacker must manipulate logs, hide in existing Registries and applications, and try to disable protective measures and logging. This is where some of the new capabilities that were introduced

shine and help in incident response and forensic analysis. First, if the attacker tries to hide anywhere in the boot sequence, the Device Health Attestation (DHA) module will identify that there is something wrong and report on it. The endpoint will not be allowed to join the domain. To use DHA, a Trusted Platform Module (TPM) module is needed. If the endpoints do not have TPM, then WEF and GPOs will be able to very if there are changes in the start-up settings. Then the hacker would have a hard time modifying logs, as they are not kept on the endpoint and are sent to a server, and the attacker cannot edit them in transit as they are encrypted at the endpoint. If the WEF service or any other Windows Defender services are turned off, then two actions will take place. As discussed before the act of turning off a service sends an event to the event collector server and can be monitored to trigger an action. If sending the event from the endpoint is blocked or is not caught, then the periodic GPO refresh and audit will detect an anomaly in the system. If the attacker tries to hide in an application's **.dll**, then on the next application execution, Device Guard or AppLocker will verify its signature and will halt its execution as being a modified program and send an alert. The attacker cannot turn off logging or Windows Defender modules, can't modify the actual logging server, and can't hide in system or applications, without being detected rather quickly. The worst-case scenario is that the attacker has access to the logging server and tries to modify the logs. Firstly, having a second logging server is useful, especially in large networks, and have the endpoints send the logs to both simultaneously and then regularly compare both logs. Also, the act of being on the server and modifying logs creates other logs that are sent to the second server, which the attacker then needs to modify. These actions augment the noise and the likelihood of being caught by the other security and detection mechanisms that have been discussed so far.

4.4. Miscellaneous

Other scenarios would only be a repeat of variations of the previous three examples. What is important is to know what the known good in the system is supposed to be and set the GPOs to enforce that and turn on WEF on anything that would indicate behavior outside of that policy. It is also important to have the logs of known good

Sebastien Godin.
Sebastien.godin@gmail.com

activities; this enables incident analysis when an intruder does get in and is not caught by the outlier principle (Payne, 2015).[2]

5. Conclusion

Looking back at figure 1 and the characteristics of an EDR established in paragraph 2, it can be seen that Windows 10 and Windows Server 2016 correctly used together creates a self-contained EDR solution. It achieves both detection and response: detection by detecting incidents, evaluating risk, and containment; and of response by enabling investigation of incidents, helping with policy changes through GPO management, and help with remediation activities. Although being a powerful capability, there are a few drawbacks to this option. This solution does not include a SIEM. A SIEM with machine learning capability integrated with the EDR solution would be a powerful tool in both prevention and response. By contrast, although everything can be managed from the Server Manager console, it is not necessarily as intuitive as a 3rd party solution and has fewer bells and whistles. Using the built-in tools requires an in-depth knowledge of how Windows operates to be able to create proper GPOs and WEF subscriptions, but a good system administrator in cooperation with the security personnel should strive to have that knowledge. Even if the system administrators and security personnel have the appropriate knowledge and experience, it can be very time consuming to create rules and tasks for all possible situations. Note that one of the strengths of using a native toolset is that it avoids introducing vulnerabilities that third-party security software can have. This capability once mastered can be very versatile and in-depth. There is no extra cost for having these tools as it is already captured in the cost to acquire of Windows 10 and Windows Server 2016. Also, there are no extra funds required for training because to become a system administrator or security personnel the education and qualifications include how to do these actions and procedures in an enterprise environment. Using built-in capabilities eliminate the need to have contractors come in and help install a third party system and impact the production environment. As discussed earlier these savings can be reinvested in other endeavors. Therefore this

[2] See reference to find a recommended list of event IDs to monitor and the translation from the Legacy to the current event ID (Mathers et al., 2017). Also, Microsoft published a reference on auditing and monitoring that is very helpful (Miroshnikov, 2016).

option is viable for small and medium enterprises that have limited budgets for IT Security and have a relatively flat and homogeneous network.

Sebastien Godin.
Sebastien.godin@gmail.com

6. References

AV-TEST. (2017). Retrieved December 15, 2017, retrieved from https://www.av-test.org/en/antivirus/home-windows/windows-10/october-2017/microsoft-windows-defender-4.11-174047/.)

Bisson, D. (2016, June 1). *The 4 Commandments of Endpoint Detection and Response (EDR)*. Retrieved August 20, 2017, from https://www.tripwire.com/state-of-security/security-data-protection/the-4-commandments-of-endpoint-detection-and-response/

Barnett, N., Tillman, M., Agiewich, R., & Bigman, N. (2017, March 7). *Windows Defender Advanced Threat Protection*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/sccm/protect/deploy-use/windows-defender-advanced-threat-protection

Configure NAP Enforcement Clients in Group Policy. (2012, February 29). Retrieved December 31, 2017, from https://msdn.microsoft.com/en-us/library/dd314162(v=ws.10).aspx

D'Souza-Wiltshire, I., Brower, N., & Lich, B. (2017, August 26). *Configure Windows Defender AV with Group Policy*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-antivirus/use-group-policy-windows-defender-antivirus

Dauti, B. (2017). *Windows Server 2016 Administration Fundamentals*. S.l.: Packt Publishing Limited.

Endpoint Detection and Response (EDR). (2015, January 14). Retrieved August 20, 2017, from https://digitalguardian.com/resources/data-security-knowledge-base/endpoint-detection-and-response-edr

Echeverri, A, and Sadequl H. (2017, July 11). *Centralizing Windows Logs. The Ultimate Guide to Logging*. https://www.loggly.com/ultimate-guide/centralizing-windows-logs/, accessed December 28, 2017.

Endpoint Protection. (2015, April 1). Retrieved December 31, 2017, from https://technet.microsoft.com/en-us/library/hh508836.aspx

Firstbrook, P., & MacDonald, N. (2016, November 30). *Market Guide for Endpoint Detection and Response Solutions*. Retrieved March 9, 2017, from https://www.gartner.com/doc/reprints?id=1-3N2LROG&ct=161202&st=sb

Hall, J., Brower, N., D'Souza-Wiltshire, I., Lich, B., & Méndez, R. C. (2017, October 13). *Mitigate threats by using Windows 10 security features*. Retrieved December

Sebastien Godin.
Sebastien.godin@gmail.com

30, 2017, from https://docs.microsoft.com/en-us/windows/threat-protection/overview-of-threat-mitigations-in-windows-10

Hardy, T., Brower, N., Borg, M., Hall, J., & Lich, B. (2017, October 27). *Use Windows Event Forwarding to help with intrusion detection*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/windows/threat-protection/use-windows-event-forwarding-to-assist-in-instrusion-detection

Lich, B., & Brower, N. (2017, July 19). *Configure security policy settings (Windows 10)*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/how-to-configure-security-policy-settings

Lich, B., Brower, N., & Hall, J. (2017, October 27). *BitLocker Countermeasures (Windows 10)*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-countermeasures

Lich, B., Brower, N., Ross, E., & Poggemeyer, L. (2017, November 8). *Threat Protection (Windows 10)*. Retrieved December 20, 2017, from https://docs.microsoft.com/en-us/windows/threat-protection/

Lord, N. (2017, July 27). *What is Endpoint Detection and Response? A Definition of Endpoint Detection & Response*. Retrieved August 20, 2017, from https://digitalguardian.com/blog/what-endpoint-detection-and-response-definition-endpoint-detection-response

Lord, N. (2017, July 27). *What is Endpoint Protection? Data Protection 101*. Retrieved August 20, 2017, from https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101

Mathers, B., Poggemeyer, L., Wheeler, S., Kumar, S., Shengjin, Y., & Kumar, S. (2017, May 31). *Appendix L - Events to Monitor*. Retrieved December 24, 2017, from https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Melber, D. (2010, July 14). *Attaching Tasks to Event Viewer Logs and Events*. Retrieved December 31, 2017, from http://techgenix.com/attaching-tasks-event-viewer-logs-events/

Metcalf, S. (2016a, February 11). *PowerShell Version 5 Security*. https://adsecurity.org/?p=2277, accessed December 30, 2017.

Metcalf, S. (2016b, August 13). *PowerShell Security: PowerShell Attack Tools, Mitigation, & Detection*. https://adsecurity.org/?p=2921, accessed December 28, 2017.

Sebastien Godin.
Sebastien.godin@gmail.com

Miroshnikov, A. (2016, June 16). *Windows 10 and Windows Server 2016 Security Auditing and Monitoring Reference*. Microsoft. https://www.microsoft.com/en-us/download/details.aspx?id=52630, accessed December 30, 2017.

Modi, R. (2017). *DevOps with windows server 2016*. S.l.: Packt Publishing Limited.

Morimoto, R., Shapiro, J. R., Yardeni, G., Droubi, O., Noel, M., Abbate, A., & Amaris, C. (2017). *Windows server 2016 unleashed*. Lebanon, IN: Pearson Education, Inc.

Nair, S. (2013, August 7). *Live Response Using PowerShell*. SANS. Retrieved December 30, 2017, from https://www.sans.org/reading-room/whitepapers/forensics/live-response-powershell-34302

Payne, J. (2015, November 23). *Monitoring What Matters – Windows Event Forwarding for Everyone (Even If You Already Have a SIEM.)*. Microsoft TechNet. https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/, accessed December 24, 2017.

Pyle, N. (2008, September 11). *Fun with WMI Filters in Group Policy*. Retrieved December 31, 2017, from https://blogs.technet.microsoft.com/askds/2008/09/11/fun-with-wmi-filters-in-group-policy/

Robb, D. (2017, June 22). *Top 10 Endpoint Detection and Response (EDR) Solutions*. Retrieved August 20, 2017, from http://www.esecurityplanet.com/products/top-endpoint-detection-response-solutions.html

Stark, J. R. (2015, May 8). *EDR: The Future of Cybersecurity and Incident Response*. Retrieved August 20, 2017, from http://www.cybersecuritydocket.com/2015/05/08/edr-the-future-of-cybersecurity-and-incident-response/

Tillman, M., Barnett, N., Cai, S., Agiewich, R., Bigman, N., & Dunsire, B. (2017, July 3). *Plan for Endpoint Protection - Configuration Manager*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/sccm/protect/plan-design/planning-for-endpoint-protection

Tillman, M., Barnett, N., Agiewich, R., Dunsire, B., Bigman, N., Czechowski, A., Cai, S., & Robertson, A. (2017, February 6). *Endpoint Protection*. Retrieved December 31, 2017, from https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-protection

The Cost of Insecure Endpoints. (2017). Ponemon Institute.

Sebastien Godin.
Sebastien.godin@gmail.com

Tomkins, R. (2016, May 18). *Creating Custom Windows Event Forwarding Logs*. Retrieved December 31, 2017, from https://blogs.technet.microsoft.com/russellt/2016/05/18/creating-custom-windows-event-forwarding-logs/

Warner, M. (2016, April 8). *What is Endpoint Detection and Response (EDR)?* Retrieved August 20, 2017, from https://blog.watchpointdata.com/what-is-endpoint-detection-and-response-edr

Windows Firewall with Advanced Security Administration with Windows PowerShell. (2012, August 8). Retrieved December 31, 2017, from https://technet.microsoft.com/en-us/library/hh831755(v=ws.11).aspx

Wheeler, S., Jofre, J., Nikolic, A., & Ka, S. (2017, September 28). *PowerShell Scripting*. Retrieved December 27, 2017, from https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting

Yan, J. (2017, January 1). *Windows Server 2016 Security Auditing for Enhanced Threat Detection*. Retrieved December 31, 2017, from https://blogs.technet.microsoft.com/datacentersecurity/2017/01/30/windows-server-2016-security-auditing/

Sebastien Godin.
Sebastien.godin@gmail.com

Last Updated: February 21st, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 29, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
SANS Riyadh February 2019	OnlineSA	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced