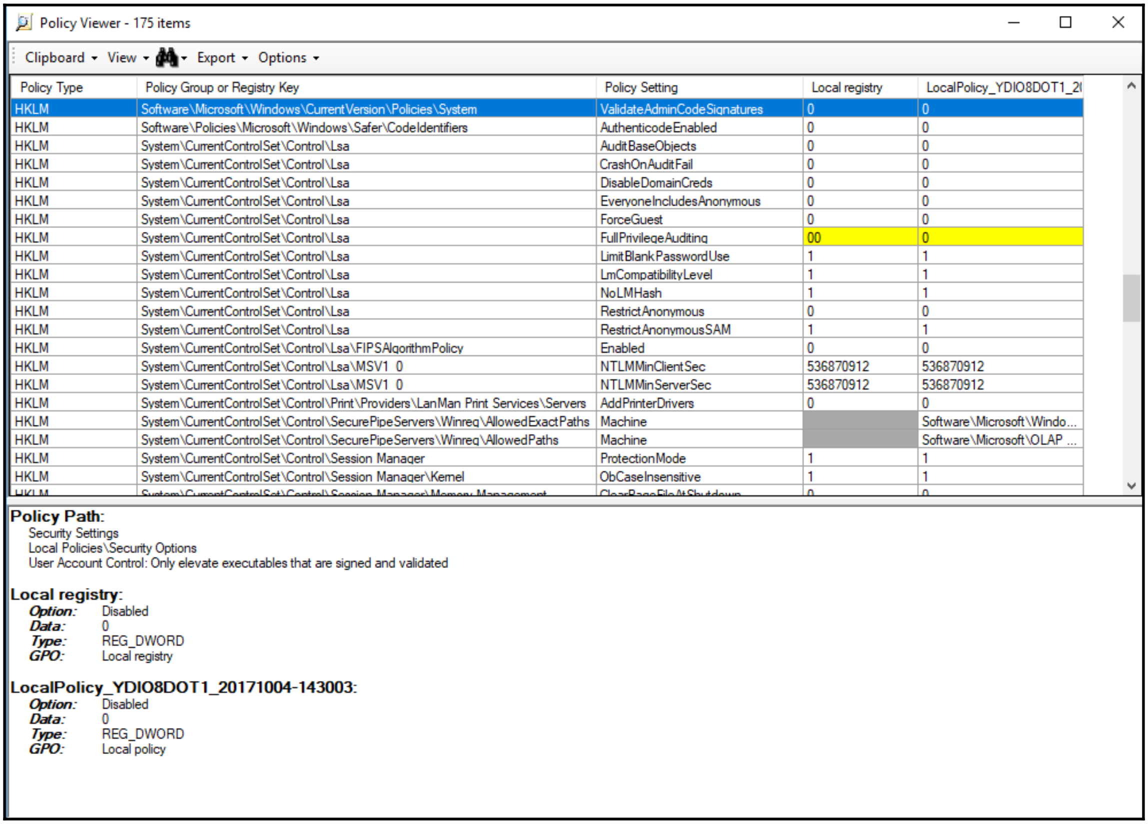
It is also recommended that you perform a backup of the current configuration and make a copy of this report before making any change to the current group policies. Another tool that you can also use to perform this assessment is the policy viewer, part of the Microsoft Security Compliance Toolkit, available at `https://www.microsoft.com/en-us/download/details.aspx?id=55319`:



Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	LocalPolicy_YDIO8DOT1_2(
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ValidateAdminCodeSignatures	0	0
HKLM	Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	0
HKLM	System\CurrentControlSet\Control\Lsa	AuditBaseObjects	0	0
HKLM	System\CurrentControlSet\Control\Lsa	CrashOnAuditFail	0	0
HKLM	System\CurrentControlSet\Control\Lsa	DisableDomainCreds	0	0
HKLM	System\CurrentControlSet\Control\Lsa	EveryoneIncludesAnonymous	0	0
HKLM	System\CurrentControlSet\Control\Lsa	ForceGuest	0	0
HKLM	System\CurrentControlSet\Control\Lsa	FullPrivilegeAuditing	00	0
HKLM	System\CurrentControlSet\Control\Lsa	LimitBlankPasswordUse	1	1
HKLM	System\CurrentControlSet\Control\Lsa	LmCompatibilityLevel	1	1
HKLM	System\CurrentControlSet\Control\Lsa	NoLMHash	1	1
HKLM	System\CurrentControlSet\Control\Lsa	RestrictAnonymous	0	0
HKLM	System\CurrentControlSet\Control\Lsa	RestrictAnonymousSAM	1	1
HKLM	System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy	Enabled	0	0
HKLM	System\CurrentControlSet\Control\Lsa\MSV1 0	NTLMMinClientSec	536870912	536870912
HKLM	System\CurrentControlSet\Control\Lsa\MSV1 0	NTLMMinServerSec	536870912	536870912
HKLM	System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers	AddPrinterDrivers	0	0
HKLM	System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths	Machine		Software\Microsoft\Windo...
HKLM	System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths	Machine		Software\Microsoft\OLAP ...
HKLM	System\CurrentControlSet\Control\Session Manager	ProtectionMode	1	1
HKLM	System\CurrentControlSet\Control\Session Manager\Kernel	ObCaseInsensitive	1	1
HKLM	System\CurrentControlSet\Control\Session Manager\Memory Management	ClearPageFileAtShutdown	0	0

Policy Path:
Security Settings
Local Policies\Security Options
User Account Control: Only elevate executables that are signed and validated

Local registry:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local registry

LocalPolicy_YDIO8DOT1_20171004-143003:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local policy

The advantage of this tool is that it doesn't look only into the GPOs, but also in the correlation that a policy has with a registry's key values.

Application whitelisting

If your organization's security policy dictates that only licensed software is allowed to run in the user's computer, you need to prevent users from running unlicensed software, and also restrict the use of licensed software that is not authorized by IT. Policy enforcement ensures that only authorized applications will run on the system.

We recommend that you read NIST publication *800-167* for further guidance on application whitelisting. Download this guide from `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf`.

When planning policy enforcement for applications, you should create a list of all apps that are authorized to be used in the company. Based on this list, you should investigate the details about these apps by asking the following questions:

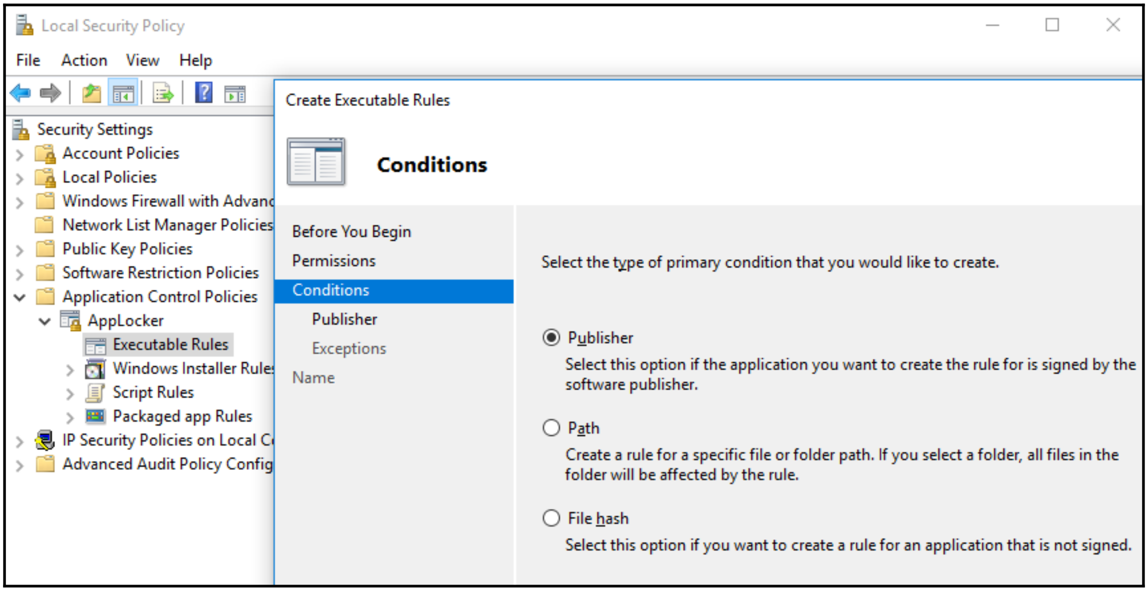
- What's the installation path for each app?
- What's the vendor's update policy for these apps?
- What executable files are used by these apps?

The more information you can get about the app itself, the more tangible data you will have to determine whether or not an app has been tampered with. For Windows systems, you should plan to use AppLocker and specify which applications are allowed to run on the local computer.

In AppLocker, there are three types of conditions to evaluate an app, which are:

- **Publisher**: This should be used if you want to create a rule that will evaluate an app that was signed by the software vendor
- **Path**: This should be used if you want to create a rule that will evaluate the application path
- **File hash**: This should be used if you want to create a rule that will evaluate an app that is not signed by the software vendor

These options will appear in the **Conditions** page when you run the create **Executable Rules** wizard:



Create Executable Rules

Conditions

Select the type of primary condition that you would like to create.

● Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

○ Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

○ File hash
Select this option if you want to create a rule for an application that is not signed.

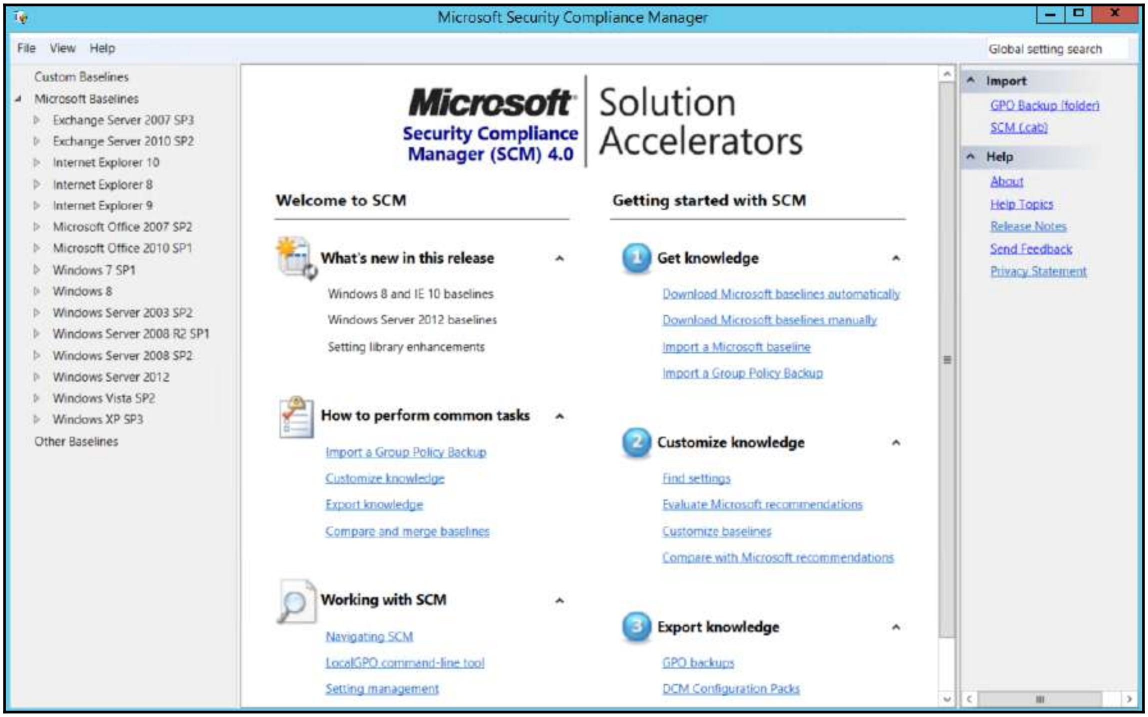
Which option you choose will depend on your needs, but these three choices should cover the majority of the deployment scenarios. Keep in mind that, depending on which option you choose, a new set of questions will appear on the page that follows. Make sure that you read the AppLocker documentation at `https://docs.microsoft.com/en-us/windows/device-security/applocker/applocker-overview`.

To whitelist apps in an Apple OS, you can use Gatekeeper (`https://support.apple.com/en-us/HT202491`), and in a Linux OS you can use SELinux.

Hardening

As you start planning your policy deployment and addressing which setting should be changed to better protect the computers, you are basically hardening these to reduce the attack vector. You can apply **Common Configuration Enumeration** (**CCE**) guidelines to your computers.

To optimize your deployment, you should also consider using security baselines. This can assist you in better managing not only the security aspect of the computer, but also its compliance with company policy. For the Windows platform, you can use the Microsoft Security Compliance Manager:



Custom Baselines
Microsoft Baselines
Exchange Server 2007 SP3
Exchange Server 2010 SP2
Internet Explorer 10
Internet Explorer 8
Internet Explorer 9
Microsoft Office 2007 SP2
Microsoft Office 2010 SP1
Windows 7 SP1
Windows 8
Windows Server 2003 SP2
Windows Server 2008 R2 SP1
Windows Server 2008 SP2
Windows Server 2012
Windows Vista SP2
Windows XP SP3
Other Baselines

Microsoft Security Compliance Manager (SCM) 4.0 | Solution Accelerators

Welcome to SCM

What's new in this release
Windows 8 and IE 10 baselines
Windows Server 2012 baselines
Setting library enhancements

How to perform common tasks
Import a Group Policy Backup
Customize knowledge
Export knowledge
Compare and merge baselines

Working with SCM
Navigating SCM
LocalGPO command-line tool
Setting management

Getting started with SCM

1 Get knowledge
Download Microsoft baselines automatically
Download Microsoft baselines manually
Import a Microsoft baseline
Import a Group Policy Backup

2 Customize knowledge
Find settings
Evaluate Microsoft recommendations
Customize baselines
Compare with Microsoft recommendations

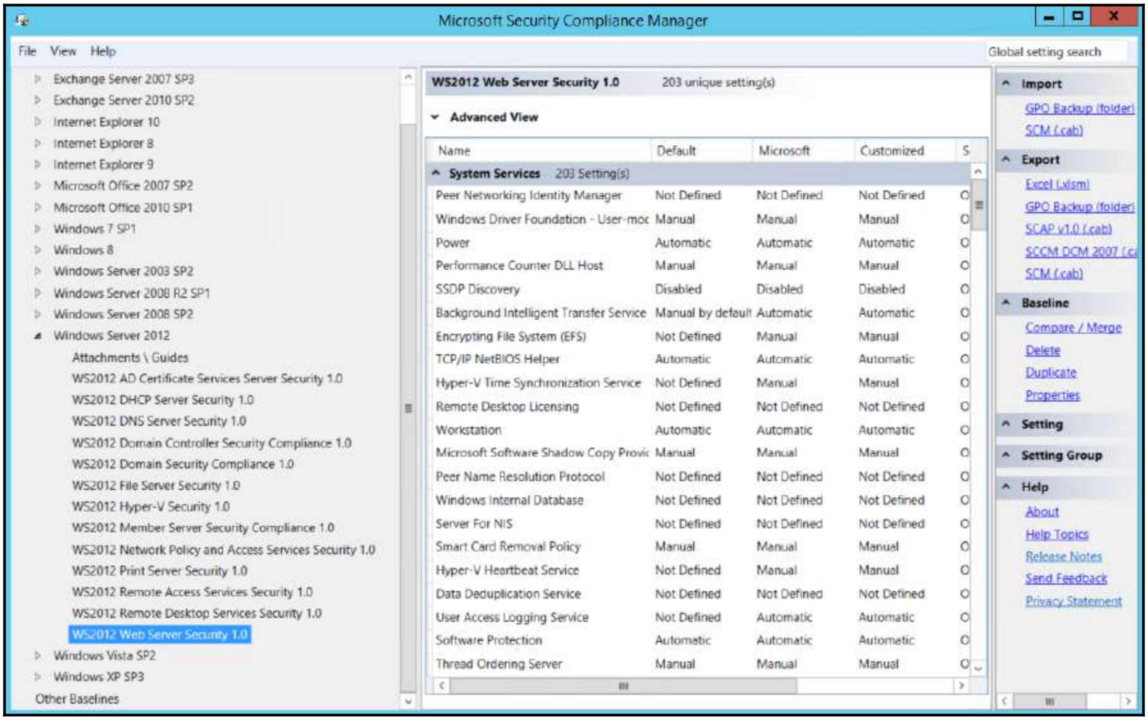
3 Export knowledge
GPO backups
DCM Configuration Packs

Import
GPO Backup (folder)
SCM (cab)

Help
About
Help Topics
Release Notes
Send Feedback
Privacy Statement

On the left-hand pane, you have all supported versions of the operating system and some applications.

Let's use **Windows Server 2012** as an example. Once you click on this operating system, you will bring up the different roles for this server. Using the **WS2012 Web Server Security 1.0** template as an example, we have a set of 203 unique settings that are going to enhance the overall security of the server:


Microsoft Security Compliance Manager
File View Help
Global setting search
Exchange Server 2007 SP3
Exchange Server 2010 SP2
Internet Explorer 10
Internet Explorer 8
Internet Explorer 9
Microsoft Office 2007 SP2
Microsoft Office 2010 SP1
Windows 7 SP1
Windows 8
Windows Server 2003 SP2
Windows Server 2008 R2 SP1
Windows Server 2008 SP2
Windows Server 2012
Attachments \ Guides
WS2012 AD Certificate Services Server Security 1.0
WS2012 DHCP Server Security 1.0
WS2012 DNS Server Security 1.0
WS2012 Domain Controller Security Compliance 1.0
WS2012 Domain Security Compliance 1.0
WS2012 File Server Security 1.0
WS2012 Hyper-V Security 1.0
WS2012 Member Server Security Compliance 1.0
WS2012 Network Policy and Access Services Security 1.0
WS2012 Print Server Security 1.0
WS2012 Remote Access Services Security 1.0
WS2012 Remote Desktop Services Security 1.0
WS2012 Web Server Security 1.0
Windows Vista SP2
Windows XP SP3
Other Baselines
Import
GPO Backup (folder)
SCM (cab)
Export
Excel (.xlsm)
GPO Backup (folder)
SCAP v1.0 (cab)
SCCM DCM 2007 (ca
SCM (cab)
Baseline
Compare / Merge
Delete
Duplicate
Properties
Setting
Setting Group
Help
About
Help Topics
Release Notes
Send Feedback
Privacy Statement

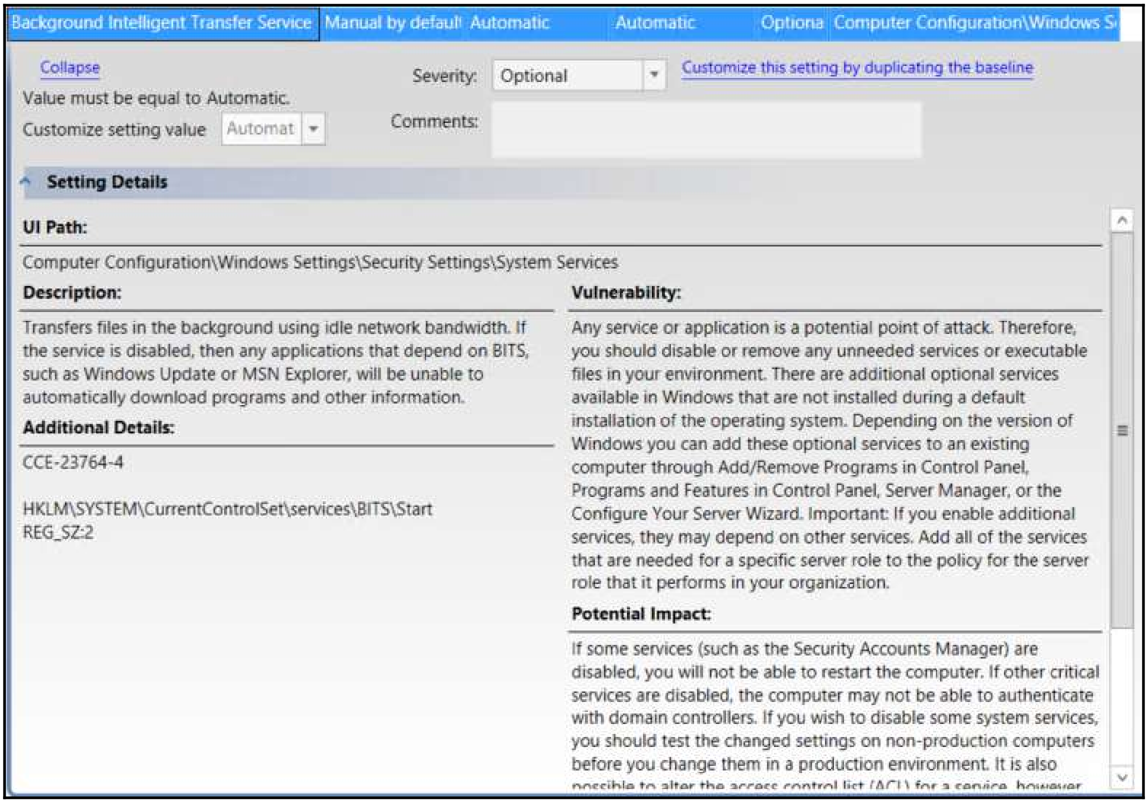
WS2012 Web Server Security 1.0 203 unique setting(s)

Advanced View

System Services 203 Setting(s)

Name	Default	Microsoft	Customized	S
Peer Networking Identity Manager	Not Defined	Not Defined	Not Defined	O
Windows Driver Foundation - User-moc	Manual	Manual	Manual	O
Power	Automatic	Automatic	Automatic	O
Performance Counter DLL Host	Manual	Manual	Manual	O
SSDP Discovery	Disabled	Disabled	Disabled	O
Background Intelligent Transfer Service	Manual by default	Automatic	Automatic	O
Encrypting File System (EFS)	Not Defined	Manual	Manual	O
TCP/IP NetBIOS Helper	Automatic	Automatic	Automatic	O
Hyper-V Time Synchronization Service	Not Defined	Manual	Manual	O
Remote Desktop Licensing	Not Defined	Not Defined	Not Defined	O
Workstation	Automatic	Automatic	Automatic	O
Microsoft Software Shadow Copy Provic	Manual	Manual	Manual	O
Peer Name Resolution Protocol	Not Defined	Not Defined	Not Defined	O
Windows Internal Database	Not Defined	Not Defined	Not Defined	O
Server For NIS	Not Defined	Not Defined	Not Defined	O
Smart Card Removal Policy	Manual	Manual	Manual	O
Hyper-V Heartbeat Service	Not Defined	Manual	Manual	O
Data Deduplication Service	Not Defined	Not Defined	Not Defined	O
User Access Logging Service	Not Defined	Automatic	Automatic	O
Software Protection	Automatic	Automatic	Automatic	O
Thread Ordering Server	Manual	Manual	Manual	O

To see more details about each setting, you should click on the configuration name in the right-hand pane:



Background Intelligent Transfer Service | Manual by default | Automatic | Automatic | Optiona | Computer Configuration\Windows S

Value must be equal to Automatic.

Customize setting value: Automat

Severity: Optional

Comments:

Setting Details

UI Path:

Computer Configuration\Windows Settings\Security Settings\System Services

Description:

Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information.

Additional Details:

CCE-23764-4

HKLM\SYSTEM\CurrentControlSet\services\BITS\Start
REG_SZ:2

Vulnerability:

Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows that are not installed during a default installation of the operating system. Depending on the version of Windows you can add these optional services to an existing computer through Add/Remove Programs in Control Panel, Programs and Features in Control Panel, Server Manager, or the Configure Your Server Wizard. Important: If you enable additional services, they may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.

Potential Impact:

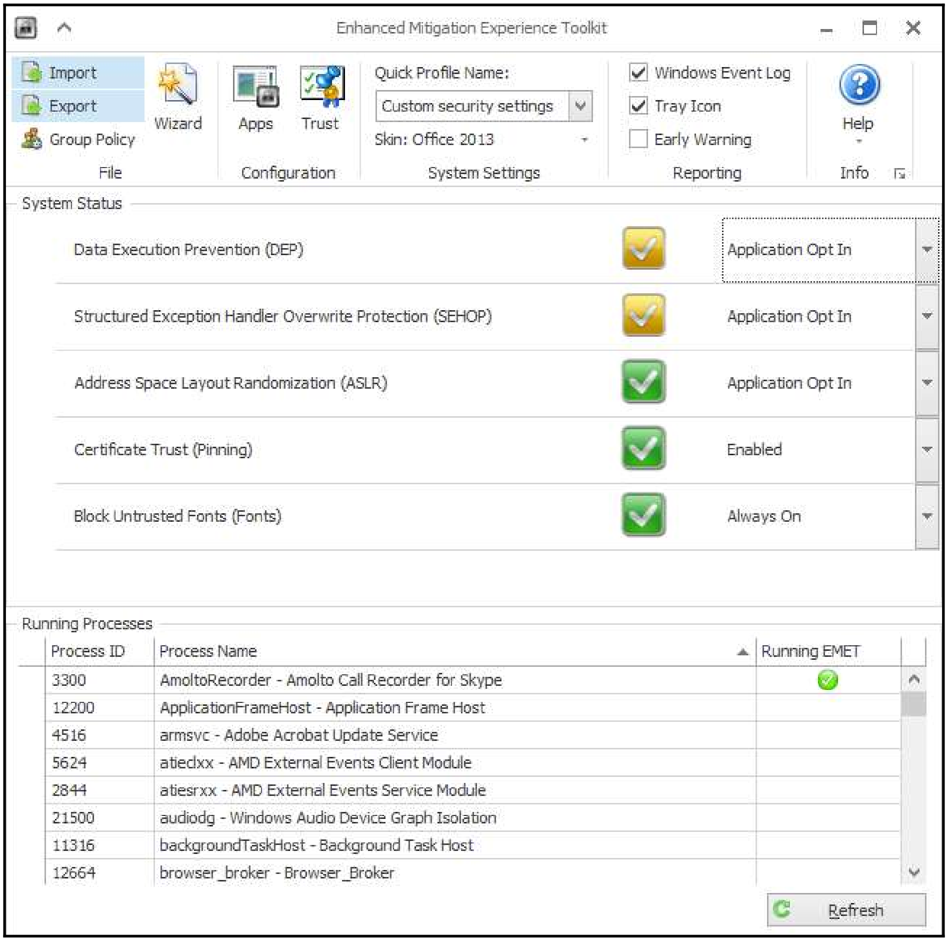
If some services (such as the Security Accounts Manager) are disabled, you will not be able to restart the computer. If other critical services are disabled, the computer may not be able to authenticate with domain controllers. If you wish to disable some system services, you should test the changed settings on non-production computers before you change them in a production environment. It is also possible to alter the access control list (ACL) for a service, however

All these settings will have the same structure—**Description**, **Additional Details**, **Vulnerability**, **Potential Impact**, and **Countermeasure**. These suggestions are based on the CCE, which is an industry standard for baseline security configuration. After you identify the template that is most appropriate for your server/workstation, you can deploy it via GPO.

For hardening a Linux computer, look for the security guidance available on each distribution. For example, for Red Hat, use the security guide, available at `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf`.

When the subject is hardening, you want to make sure you leverage all operating system capabilities to heavily the security state of the computer heavily. For Windows systems, you should consider using the **Enhanced Mitigation Experience Toolkit** (**EMET**).

EMET helps to prevent attackers from gaining access to your computers by anticipating and preventing the most common techniques that attackers are using to exploit vulnerabilities in Windows-based systems. This is not only a detection tool, it actually protects by diverting, terminating, blocking, and invalidating the attacker's actions. One of the advantages of using EMET to protect computers is the ability to block new and undiscovered threats:



Quick Profile Name: Custom security settings

Skin: Office 2013

☑ Windows Event Log
☑ Tray Icon
☐ Early Warning

System Status

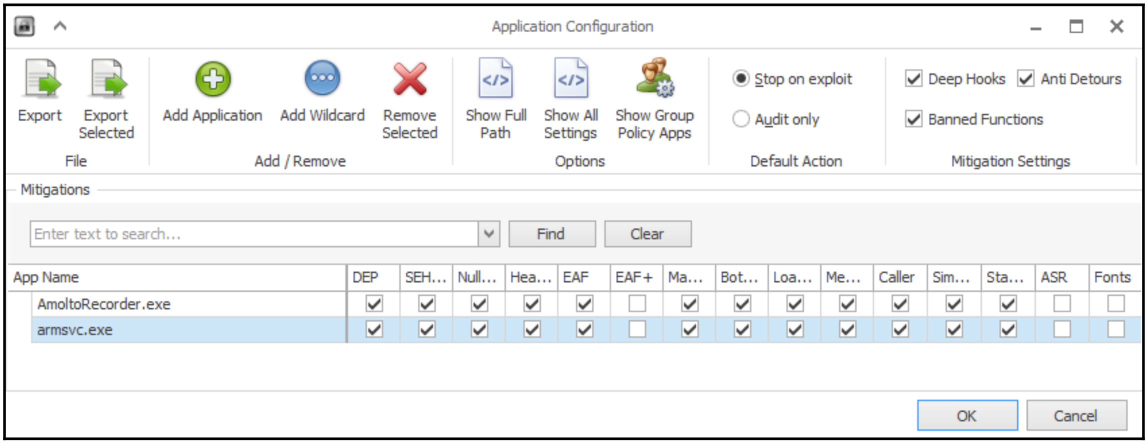
Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled
Block Untrusted Fonts (Fonts)	✓	Always On

Running Processes

Process ID	Process Name	Running EMET
3300	AmoltoRecorder - Amolto Call Recorder for Skype	✓
12200	ApplicationFrameHost - Application Frame Host	
4516	armsvc - Adobe Acrobat Update Service	
5624	atiedxx - AMD External Events Client Module	
2844	atiesrxx - AMD External Events Service Module	
21500	audiodg - Windows Audio Device Graph Isolation	
11316	backgroundTaskHost - Background Task Host	
12664	browser_broker - Browser_Broker	

The **System Status** section shows the security mitigations that are configured. Although the ideal scenario is to have all of them enabled, this configuration can vary according to each computer's needs. The lower part of the screen shows which processes have been EMET-enabled. In the preceding example, only one application was EMET-enabled. EMET works by injecting a DLL into the executable file's memory space, so when you configure a new process to be protected by EMET, you will need to close the application and open it again—the same applies to services.

To protect another application from the list, right-click on the application and click **Configure Process**:



● Stop on exploit
○ Audit only

☑ Deep Hooks ☑ Anti Detours
☑ Banned Functions

App Name	DEP	SEH...	Null...	Hea...	EAF	EAF+	Ma...	Bot...	Loa...	Me...	Caller	Sim...	Sta...	ASR	Fonts
AmoltoRecorder.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
armsvc.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□

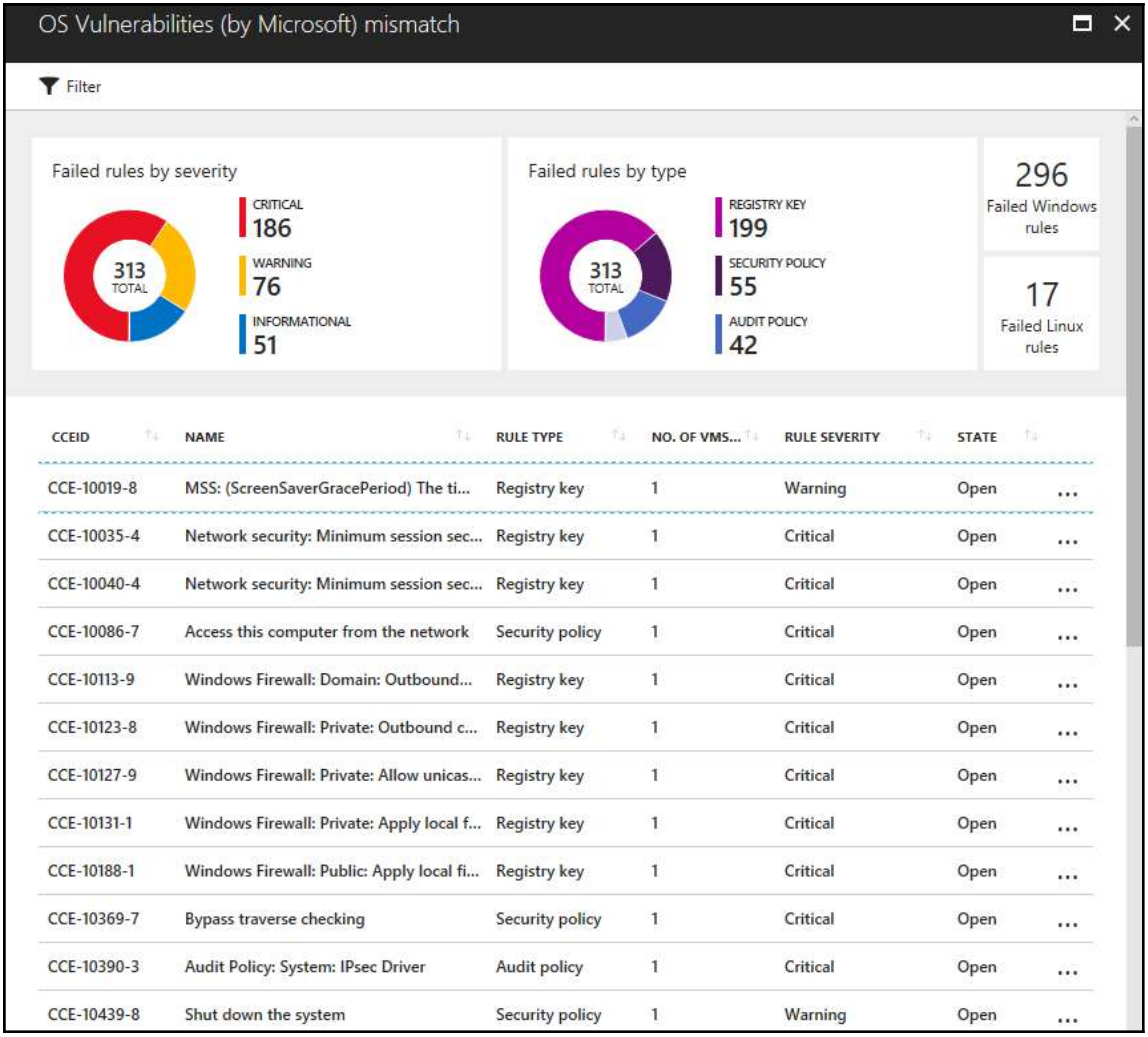
In the **Application Configuration** window, you select the mitigations that you want to enable for this application.

For more information about EMET and the options available, download the EMET user guide at `https://www.microsoft.com/en-us/download/details.aspx?id=53355`.

Monitoring for compliance

While enforcing policies is important to ensure that the upper management's decisions are translated into real actions towards optimizing the security state of your company, monitoring these policies for compliance is also indispensable.

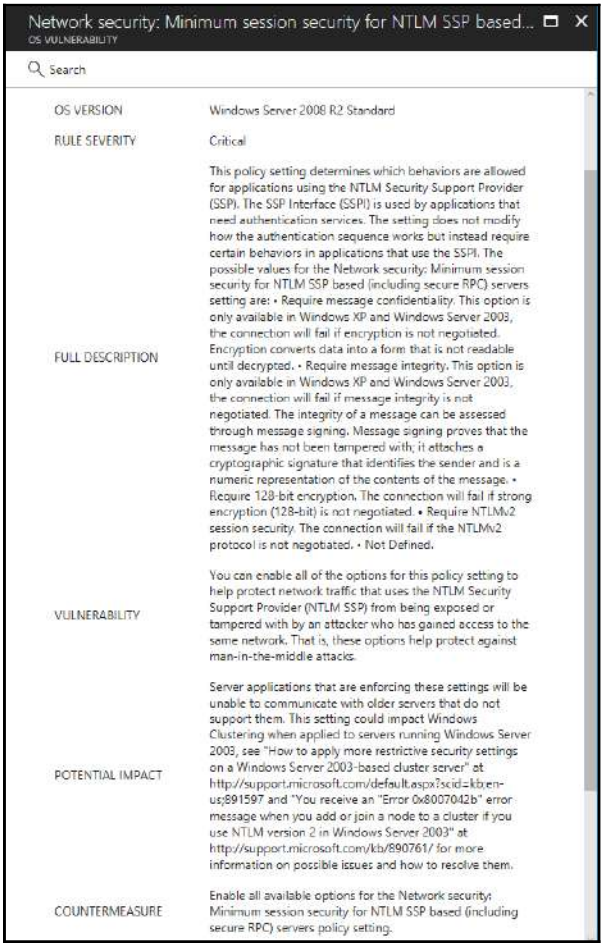
Policies that were defined based on CCE guidelines can be easily monitored using tools, such as Azure Security Center, which not only monitor Windows VMs and computers, but also those operating with Linux software:



CCEID	NAME	RULE TYPE	NO. OF VMS...	RULE SEVERITY	STATE	
CCE-10019-8	MSS: (ScreenSaverGracePeriod) The ti...	Registry key	1	Warning	Open	...
CCE-10035-4	Network security: Minimum session sec...	Registry key	1	Critical	Open	...
CCE-10040-4	Network security: Minimum session sec...	Registry key	1	Critical	Open	...
CCE-10086-7	Access this computer from the network	Security policy	1	Critical	Open	...
CCE-10113-9	Windows Firewall: Domain: Outbound...	Registry key	1	Critical	Open	...
CCE-10123-8	Windows Firewall: Private: Outbound c...	Registry key	1	Critical	Open	...
CCE-10127-9	Windows Firewall: Private: Allow unicas...	Registry key	1	Critical	Open	...
CCE-10131-1	Windows Firewall: Private: Apply local f...	Registry key	1	Critical	Open	...
CCE-10188-1	Windows Firewall: Public: Apply local fi...	Registry key	1	Critical	Open	...
CCE-10369-7	Bypass traverse checking	Security policy	1	Critical	Open	...
CCE-10390-3	Audit Policy: System: IPsec Driver	Audit policy	1	Critical	Open	...
CCE-10439-8	Shut down the system	Security policy	1	Warning	Open	...

The **OS Vulnerabilities** dashboard shows a comprehensive view of all security policies that are currently open in Windows and Linux systems. If you click on one specific policy, you will see more details about this policy, including the reason why it is important to mitigate this vulnerability. Note that towards the end of the page, you will have the suggested countermeasure to mitigate this particular vulnerability. Since this is based on CCE, the countermeasure is always a change in configuration in the operating system or application.

Do not confuse CCE with **Common Vulnerability and Exposure** (**CVE**), which usually requires a patch to be deployed in order to mitigate a certain vulnerability that was exposed. For more information about CVE, visit `https://cve.mitre.org/`.



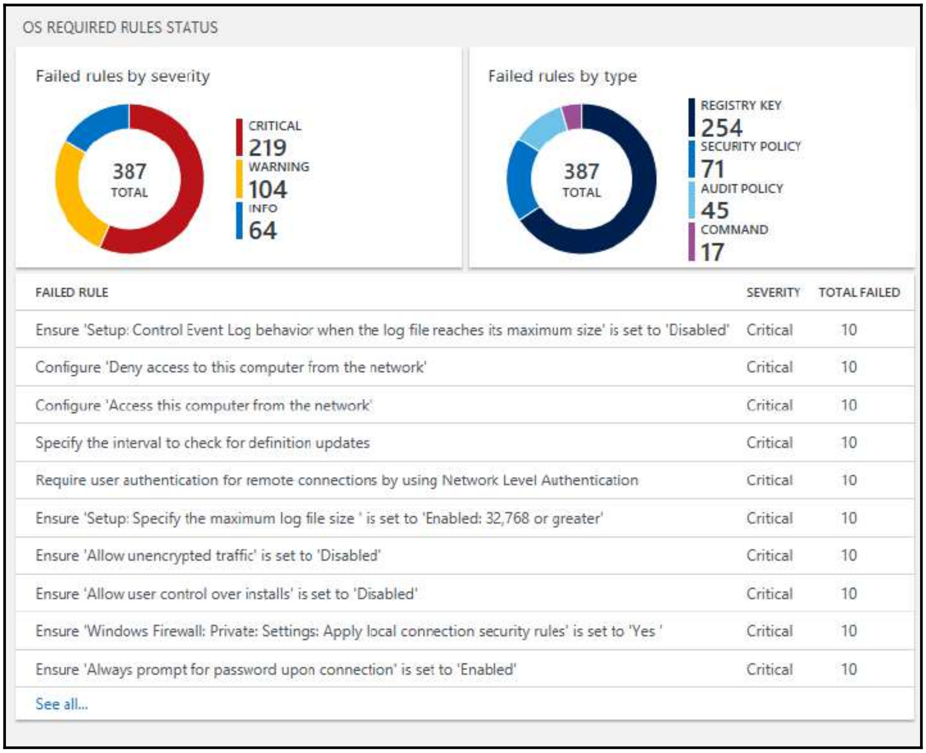
Network security: Minimum session security for NTLM SSP based...

OS VULNERABILITY

OS VERSION	Windows Server 2008 R2 Standard
RULE SEVERITY	Critical
FULL DESCRIPTION	This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are: • Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. • Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. • Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. • Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. • Not Defined.
VULNERABILITY	You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.
POTENTIAL IMPACT	Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.
COUNTERMEASURE	Enable all available options for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers policy setting.

It is important to emphasize that Azure Security Center will not deploy the configuration for you. This is a monitoring tool, not a deployment tool, which means that you need to get the countermeasure suggestion and deploy it using other methods, such as GPO.

Another tool that can also be used to obtain a complete view of the security state of the computers, and identify potential noncompliance cases, is the **Microsoft Operations Management Suite's** (**OMS's**) Security and Audit Solution, in particular the **Security Baseline Assessment** option, as shown in the following screenshot:



FAILED RULE	SEVERITY	TOTAL FAILED
Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Critical	10
Configure 'Deny access to this computer from the network'	Critical	10
Configure 'Access this computer from the network'	Critical	10
Specify the interval to check for definition updates	Critical	10
Require user authentication for remote connections by using Network Level Authentication	Critical	10
Ensure 'Setup: Specify the maximum log file size ' is set to 'Enabled: 32,768 or greater'	Critical	10
Ensure 'Allow unencrypted traffic' is set to 'Disabled'	Critical	10
Ensure 'Allow user control over installs' is set to 'Disabled'	Critical	10
Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes '	Critical	10
Ensure 'Always prompt for password upon connection' is set to 'Enabled'	Critical	10

See all...

This dashboard will give you statistics based on their priority (critical, warning, and informational), as well as the type of rules that are failing (registry, security, audit, or command-based). Both tools (Azure Security Center and OMS Security) are available for Windows and Linux, for VMs in Azure or Amazon AWS, and for on-premises computers.

References

1. *Security and Privacy Controls for Federal Information Systems and Organizations* `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf`
2. *NIST 800-53 Written Information Security Program (WISP)* security policy example `http://examples.complianceforge.com/example-nist-800-53-written-information-security-program-it-security-policy-example.pdf`
3. *Internet Security Threat Report Volume 22* `https://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf`
4. *Uncovering a persistent diet spam operation on Twitter* `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/uncovering-a-persistent-diet-spam-operation-on-twitter.pdf`
5. *Social Media Security* `https://blogs.technet.microsoft.com/yuridiogenes/2016/07/08/social-media-security/`
6. *CBS fires vice president who said Vegas victims didn't deserve sympathy because country music fans 'often are Republican'* `http://www.foxnews.com/entertainment/2017/10/02/top-cbs-lawyer-no-sympathy-for-vegas-vics-probably-republicans.html`
7. *Florida professor fired for suggesting Texas deserved Harvey after voting for Trump* `http://www.independent.co.uk/news/world/americas/us-politics/florida-professor-fired-trump-harvey-comments-texas-deserved-hurricane-storm-a7919286.html`
8. *Microsoft Security Compliance Manager* `https://www.microsoft.com/en-us/download/details.aspx?id=53353`
9. *Red Hat Enterprise Linux 6 Security Guide* `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf`
10. *AppLocker - Another Layer in the Defense in Depth Against Malware* `https://blogs.technet.microsoft.com/askpfeplat/2016/06/27/applocker-another-layer-in-the-defense-in-depth-against-malware/`
11. 11.
    Enhanced Mitigation Experience Toolkit (EMET) 5.52
    `https://www.microsoft.com/en-us/download/details.aspx?id=54264`
    `751be11f-ede8-5a0c-058c-2ee190a24fa6=True`
12. *Social Media Security* `https://blogs.technet.microsoft.com/yuridiogenes/2016/07/08/social-media-security/`

Summary

In this chapter, you learned about the importance of having a security policy and driving this policy through a security program. You understood the importance of having a clear and well-established set of social media guidelines, that give the employee an accurate view of the company's view regarding public posts, and the consequences of violating these guidelines.

Part of the security program includes the security awareness training, which educates the end user on security-related topics. This is a critical step to take, since the end user is always the weakest link in the security chain.

Later on in this chapter, you learned how companies should enforce security policies using different sets of tools. Part of this policy enforcement includes application whitelisting and hardening systems. Lastly, you learned the importance of monitoring these policies for compliance, and learned how to use tools to do this.

In the next chapter, we will continue talking about defense strategies, and this time you will learn more about network segmentation and how to use this technique to enhance your protection.

10
Network Segmentation

We started the defense strategy in the previous chapter by reinforcing the importance of having a strong and effective security policy. Now it's time to continue with this vision by ensuring that the network infrastructure is secure, and the first step to doing that is to make sure the network is segmented, isolated and that it provides mechanisms to mitigate intrusion. The Blue Team must be fully aware of the different aspects of network segmentation, from the physical to the virtual, and remote access. Even if companies are not fully cloud-based, they still need to think about connectivity with the cloud in a hybrid scenario, which means that security controls must also be in place to enhance the overall security of the environment, and network infrastructure security is the foundation for that.

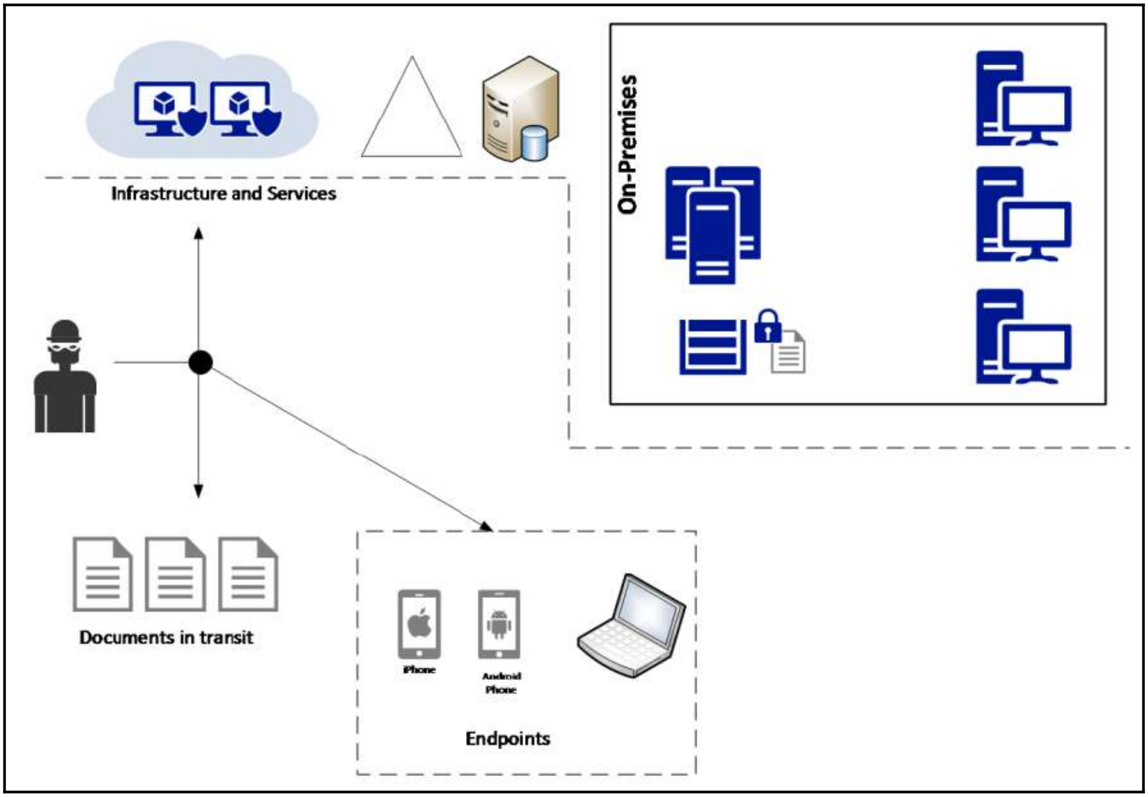
In this chapter, we are going to cover the following topics:

- Defense in depth approach
- Physical network segmentation
- Securing remote access to the network
- Virtual network segmentation
- Hybrid cloud network security

Defense in depth approach

Although you might think that this is an old method and it doesn't apply to today's demands, the reality is that it still does, although you won't be using the same technologies that you used in the past. The whole idea behind the defense in depth approach is to ensure that you have multiple layers of protection, and that each layer will have its own set of security controls, which will end up delaying the attack, and that the sensors available in each layer will alert you to whether or not something is happening. In other words, breaking the attack kill chain before the mission is fully executed.

But to implement a defense in depth approach for today's needs, you need to abstract yourself from the physical layer, and think purely about layers of protection according to the entry point. Let's use the following diagram as an example of how defense in depth is implemented today:



The attacker has broad access to different resources. They can attack the infrastructure and services, the documents in transit, and the endpoints, which means that you need to increase the attacker's cost in each possible scenario. Let's dissect this diagram in the sections that follow.

Infrastructure and services

Attackers can disrupt your company's productivity by attacking its infrastructure and its services. It is important to realize that even in an on-premises-only scenario, you still have services, but they are controlled by the local IT team. Your database server is a service: it stores critical data consumed by users, and if it becomes unavailable, it will directly affect the user's productivity, which will have a negative financial impact on your organization. In this case, you need to enumerate all services that are offered by your organization to its end users and partners, and identify the possible attack vectors.

Once you identify the attack vectors, you need to add security controls that will mitigate these vulnerabilities—for example, enforce compliance via patch management, server protection via security policies, network isolation, backups, and so on. All these security controls are layers of protection, and they are layers of protection within the infrastructure and services realm. Other layers of protection will need to be added for different areas of the infrastructure.

In the same diagram, you also have cloud computing, which in this case is **Infrastructure as a Service** (**IaaS**), since this company is leveraging VMs located in the cloud. If you've already created your threat modeling and implemented the security controls on-premises, now you need to re-evaluate the inclusion of cloud connectivity on-premises. By creating a hybrid environment, you will need to revalidate the threats, the potential entry points, and how these entry points could be exploited. The result of this exercise is usually the conclusion that other security controls must be put in place.

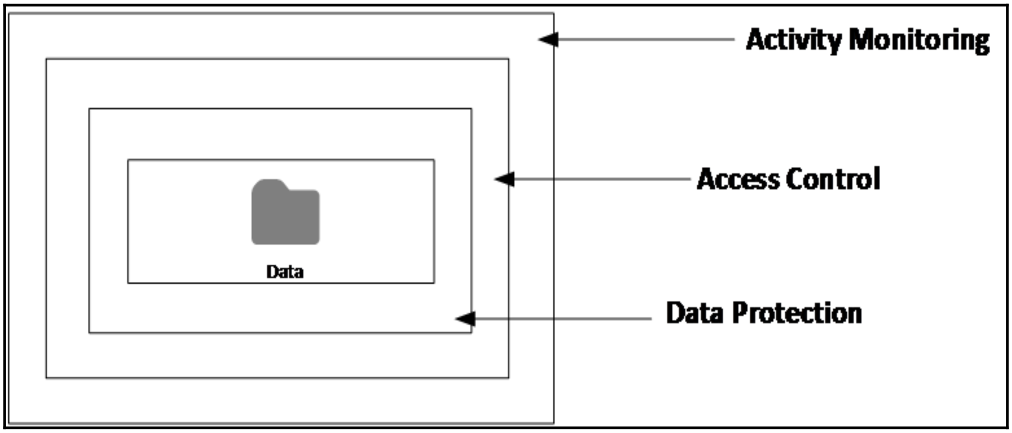
In summary, the infrastructure security must reduce the vulnerability count and severity, reduce the time of exposure, and increase the difficulty and cost of exploitation. By using a layered approach, you can accomplish that.

Documents in transit

While the diagram refers to *documents*, this could be any type of data, and this data is usually vulnerable when it is in transit (from one location to another). Make sure that you leverage encryption to protect data in transit. Also, don't think that encryption in transit is something that should only be done in public networks—it should also be implemented in internal networks.

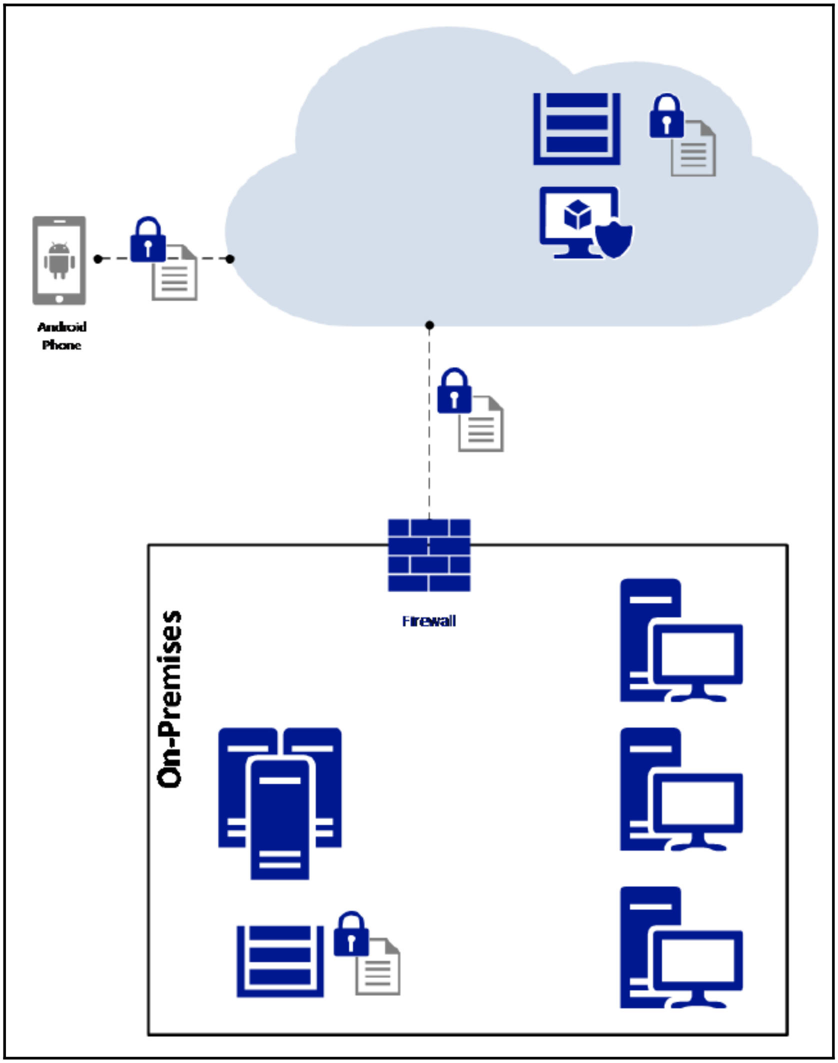
For example, all segments available in the on-premises infrastructure shown in the previous diagram should use network-level encryption, such as IPSec. If you need to transmit documents across networks, make sure that you encrypt the entire path, and when the data finally reaches the destination, encrypt the data also at rest in storage.

Besides encryption, you must also add other security controls for monitoring and access control, as shown in the following diagram:



Note that you are basically adding different layers of protection and detection, which is the entire essence of the defense in depth approach. That's how you need to think through the assets that you want to protect.

Let's go to another example, shown in the following diagram. This is an example of a document that was encrypted at rest in a server located on-premises; it traveled via the internet, the user was authenticated in the cloud, and the encryption was preserved all the way to the mobile device that also encrypted it at rest in the local storage:



This diagram shows that in a hybrid scenario, the attack vector will change, and you should consider the entire end-to-end communication path in order to identify potential threats and ways to mitigate them.

Endpoints

When planning defense in depth for endpoints, you need to think beyond computers. Nowadays, an endpoint is basically any device that can consume data. The application dictates which devices will be supported, and as long as you are working in sync with your development team, you should know what devices are supported. In general, most applications will be available for mobile devices, as well as computers. Some other apps will go beyond this, and allow accessibility via wearable devices, such as Fitbit. Regardless of the form factor, you must perform threat modeling to uncover all attack vectors and plan mitigation efforts accordingly. Some of the countermeasures for endpoints include:

- Separation of corporate and personal data/apps (isolation)
- Use of TPM hardware protection
- OS hardening
- Storage encryption

Endpoint protection should take into consideration corporate-owned devices and BYODs. To read more about a vendor-agnostic approach to BYOD, read this article `https://blogs.technet.microsoft.com/yuridiogenes/2014/03/11/byod-article-published-at-issa-journal/`.

Physical network segmentation

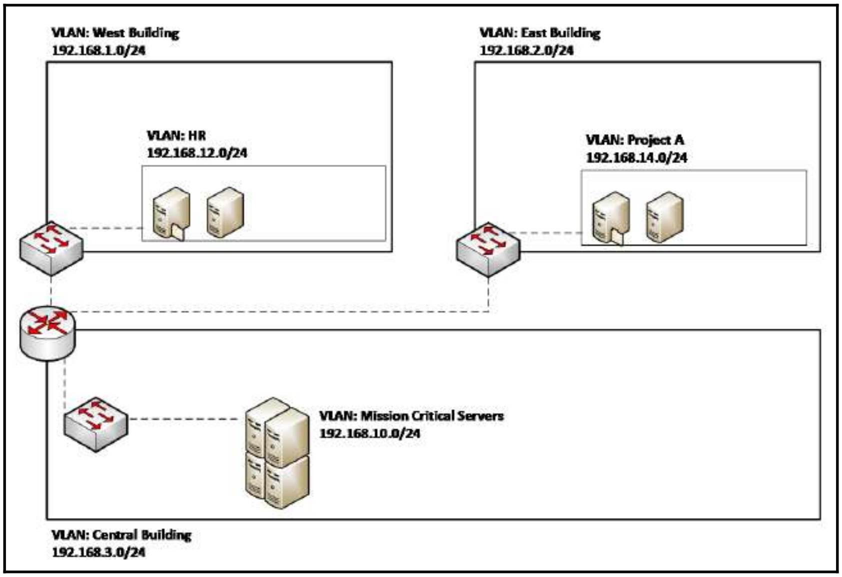
One of the biggest challenges that the Blue Team may face when dealing with network segmentation is getting an accurate view of what is currently implemented in the network. This happens because, most of the time, the network will grow according to the demand, and its security features are not revisited as the network expands. For large corporations, this means rethinking the entire network, and possibly rearchitecting the network from the ground up.

The first step to establishing an appropriate physical network segmentation is to understand the logical distribution of resources according to your company's needs. This debunks the myth that one size fits all, which in reality, it doesn't. You must analyze each network case by case, and plan your network segmentation according to the resource demand and logical access. For small-and medium-sized organizations, it might be easier to aggregate resources according to their departments—for example, resources that belong to the financial department, human resources, operations, and so on. If that's the case, you could create a **virtual local area network** (**VLAN**) per department and isolate the resources per department. This isolation would improve performance and overall security.

The problem with this design is the relationship between users/groups and resources. Let's use the file server as an example. Most departments will need access to the file server at some point, which means they will have to cross VLANs to gain access to the resource. Cross-VLAN access will require multiple rules, different access conditions, and more maintenance. For this reason, large networks usually avoid this approach, but if it fits with your organization's needs, you can use it. Some other ways to aggregate resources can be based on the following aspects:

- **Business objectives**: Using this approach, you can create VLANs that have resources based on common business objectives
- **Level of sensitivity**: Assuming that you have an up-to-date risk assessment of your resources, you can create VLANs based on the risk level (high, low, medium)
- **Location**: For large organizations, sometimes it is better to organize the resources based on location
- **Security zones**: Usually, this type of segmentation is combined with others for specific purposes, for example, one security zone for all servers that are accessed by partners

While these are common methods of aggregating resources, which could lead to network segmentation based on VLANs, you can have a mix of all these. The following diagram shows an example of this mixed approach:



In this case, we have workgroup switches (for example, Cisco Catalyst 4500) that have VLAN capability, connected to a central router that will perform the routing control over these VLANs. Ideally, this switch will have security features available that restrict IP traffic from untrusted layer 2 ports, which is a feature known as port security. This router includes a control access list to make sure that only authorized traffic is able to cross these VLANs. If your organization requires deeper inspection across VLANS, you could also use a firewall to perform this routing and inspection. Note that segmentation across VLANs is done using different approaches, which is completely fine, as long as you plan the current state and how this will expand in the future.

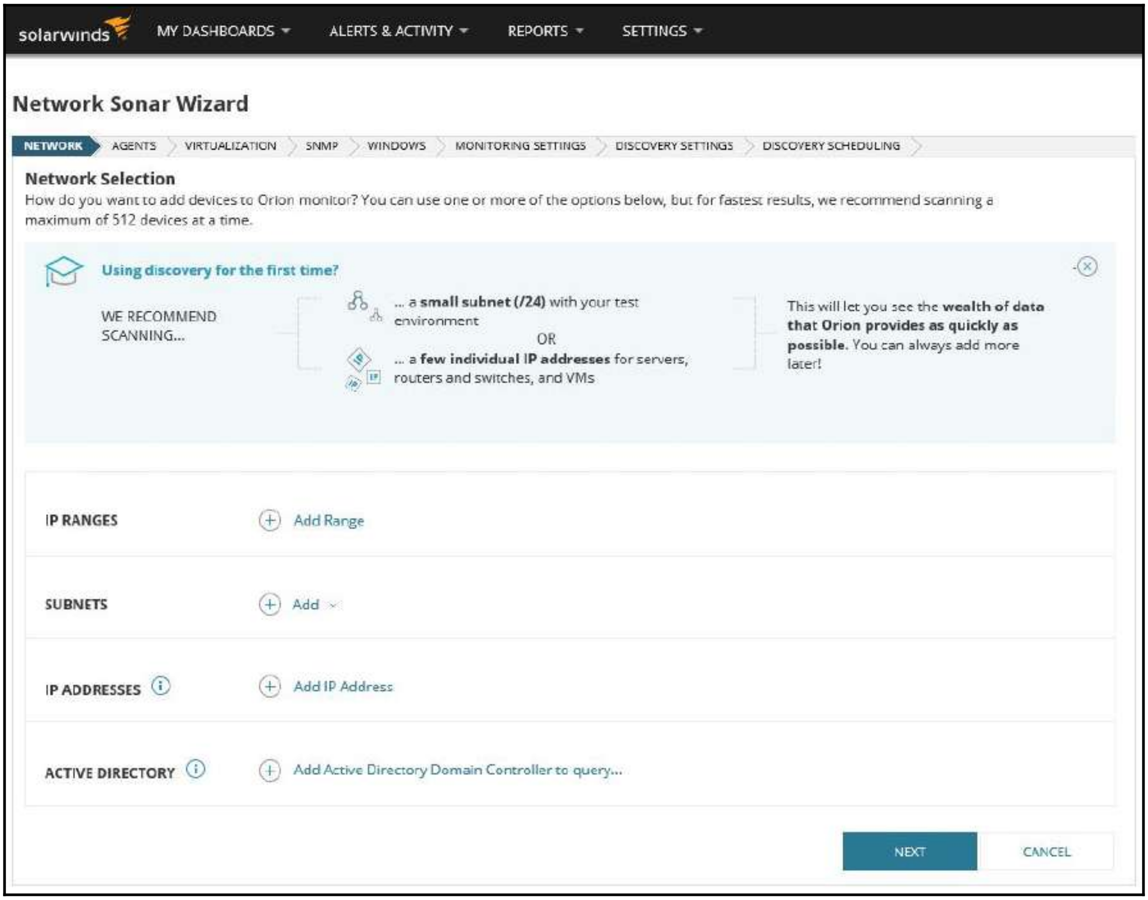
If you are using Catalyst 4500, make sure that you enable dynamic ARP inspection. This feature protects the network from certain "man-in-the-middle" attacks. For more information about this feature, go to `https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html`.

Consult your router and switch documentation to explore more security capabilities that may vary according to the vendor, and in addition to that, make sure that you use the following best practices:

- Use SSH to manage your switches and routers
- Restrict access to the management interface
- Disable ports that are not used
- Leverage security capabilities to prevent MAC flooding attacks
- Leverage port-level security to prevent attacks, such as DHCP snooping
- Make sure that you update the switch's and router's firmware and operating systems

Discovering your network

One challenge that the Blue Team might face when dealing with networks that are already in production is understanding the topology and critical paths, and how the network is organized. One way to address this issue is to use a networking map tool that can present the current network state. One tool that can help you with that is the **Network Performance Monitor Suite** from Solarwinds. After installing it, you need to launch the network discovery process from the **Network Sonar Wizard**, as shown here:



Network Sonar Wizard

Network Selection

How do you want to add devices to Orion monitor? You can use one or more of the options below, but for fastest results, we recommend scanning a maximum of 512 devices at a time.

Using discovery for the first time?

WE RECOMMEND SCANNING...

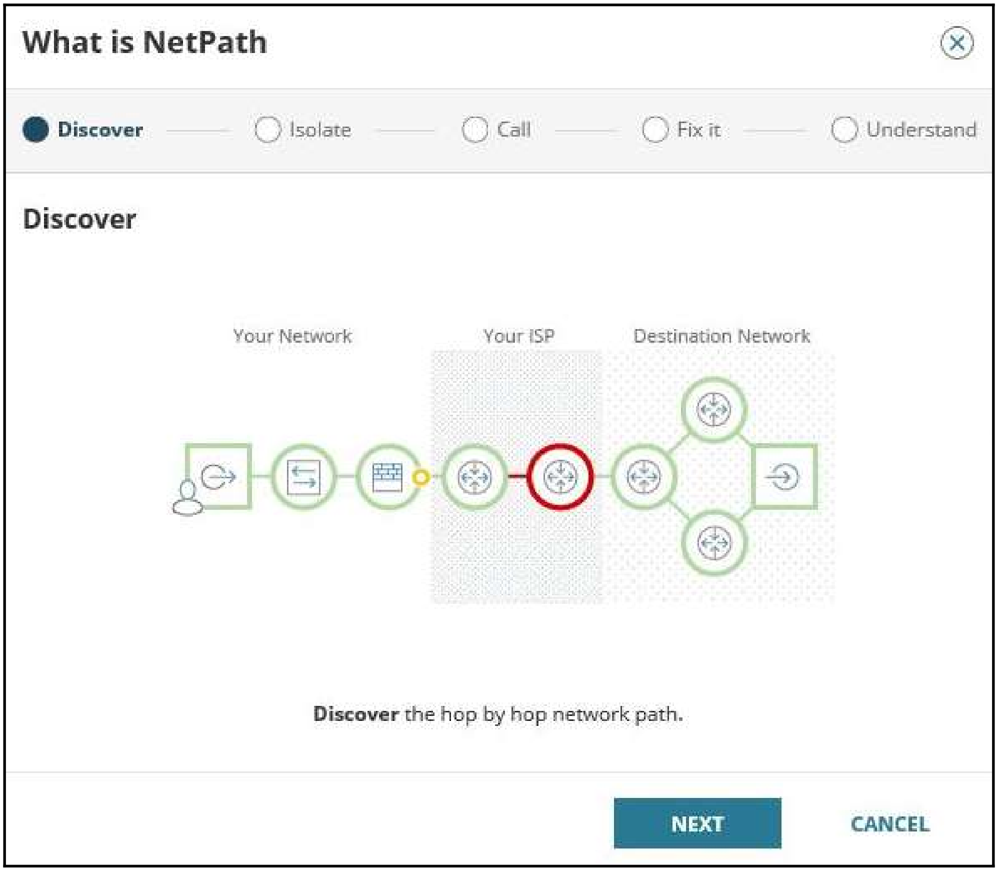
... a **small subnet (/24)** with your test environment

OR

... a **few individual IP addresses** for servers, routers and switches, and VMs

This will let you see the **wealth of data that Orion provides as quickly as possible.** You can always add more later!

You need to fill in all these fields before you click **NEXT**, and once you finish, it will start the discovery process. At the end, you can verify your NetPath, which shows the entire path between your host and the internet:



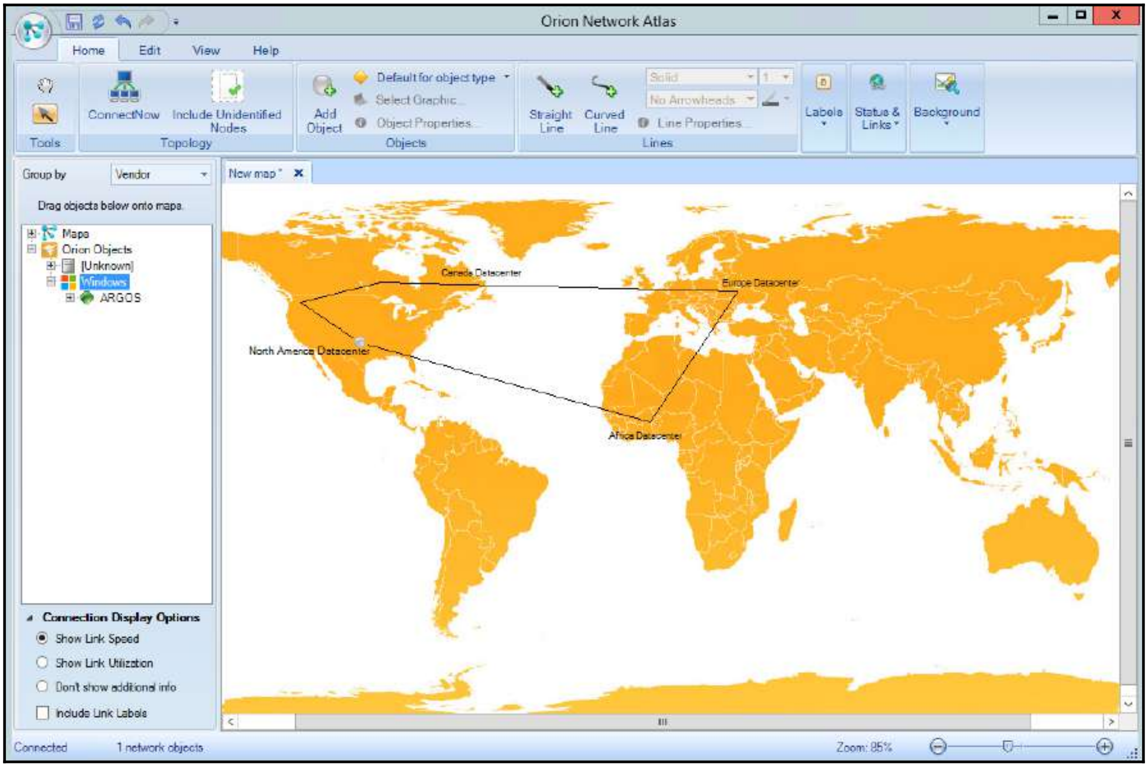
What is NetPath

● Discover ○ Isolate ○ Call ○ Fix it ○ Understand

Discover

Discover the hop by hop network path.

Another option available in this suite is to use the network atlas to create a geolocation map of your resources, as shown here:



When discovering your network, make sure that you document all aspects of it because you will need this documentation later on to properly perform the segmentation.

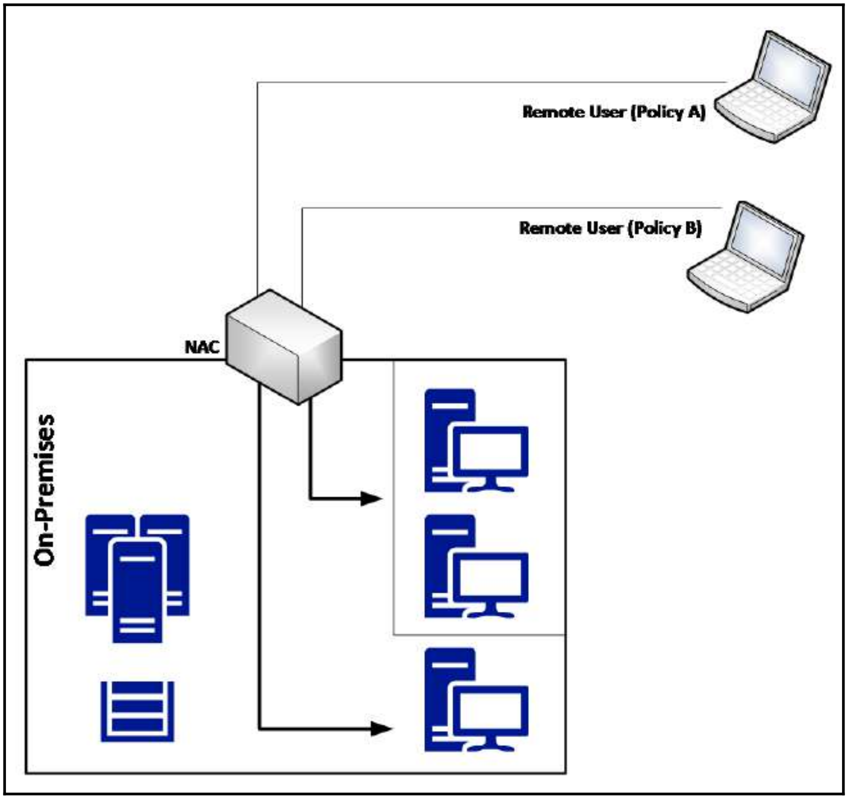
Securing remote access to the network

No networking segmentation planning would be complete without considering the security aspects of remote access to your corporate network. Even if your company does not have employees that work from home, chances are that at some point, an employee will be traveling and will need remote access to the company's resources. If this is the case, you need to consider not only your segmentation plan, but also a network access control system that can evaluate the remote system prior to allowing access to the company's network; this evaluation includes verifying the following details:

- That the remote system has the latest patches
- That the remote system has antivirus enabled

- That the remote system has a personal firewall enabled
- That the remote system is compliant with mandate security policies

The following diagram shows an example of a **network access control** (**NAC**) system:



In this scenario, the NAC is responsible not only for validating the current health state of the remote device, but also performing software-level segmentation by allowing the source device to only communicate with predefined resources located on premises. This adds an extra layer of segmentation and security. Although the diagram does not include a firewall, some companies may opt to isolate all remote access users in one specific VLAN and have a firewall in between this segment and the corporate network to control the traffic coming from remote users. This is usually used when you want to restrict the type of access users will have when they are accessing the system remotely.

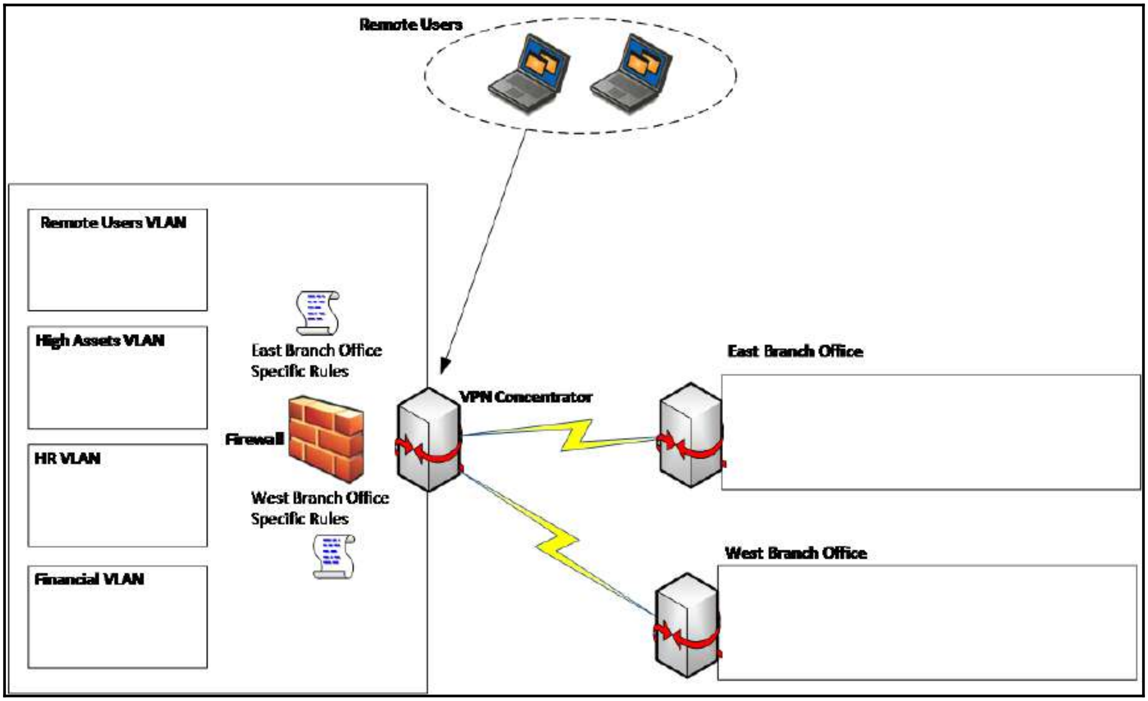
We are assuming that the authentication part of this communication was already performed, and that, for remote access users, one of the preferred methods is to use 802.1X or compatible.

It is also important to have an isolated network to quarantine computers that do not meet the minimum requirements to access network resources. This quarantine network should have remediation services that will scan the computer and apply the appropriate remediation to enable the computer to gain access to the corporate network.

Site-to-site VPN

One common scenario for organizations that have remote locations is to have a secure private channel of communication between the main corporation network and the remote network, and usually this is done via site-to-site VPN. When planning your network segmentation, you must think about this scenario, and how this connectivity will affect your network.

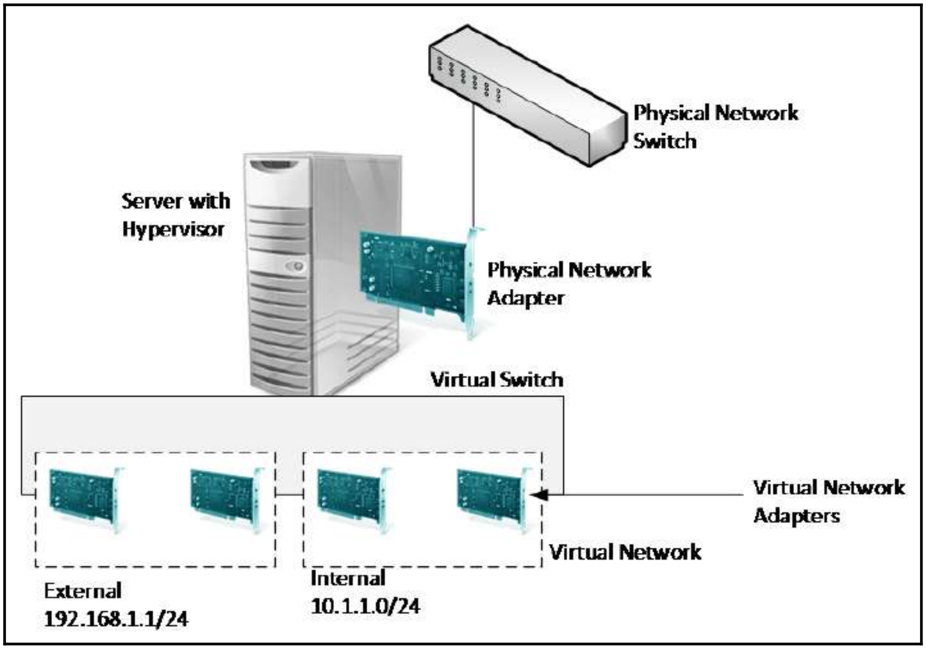
The following diagram shows an example of this connectivity:



In the network design shown in the previous diagram, each branch office has a set of rules in the firewall, which means that when the site-to-site VPN connection is established, the remote branch office will not have access to the entire headquarters' main network, but just some segments. When planning your site-to-site VPN, make sure that you use the "need to know" principle, and only allow access to what is really necessary. If the **East Branch Office** has no need to access the HR VLAN, then access to this VLAN should be blocked.

Virtual network segmentation

Security must be embedded in the network design, regardless of whether this is a physical network or a virtual network. In this case, we are not talking about VLAN, which is originally implemented in a physical network, but virtualization. Let's use the following diagram as our starting point:



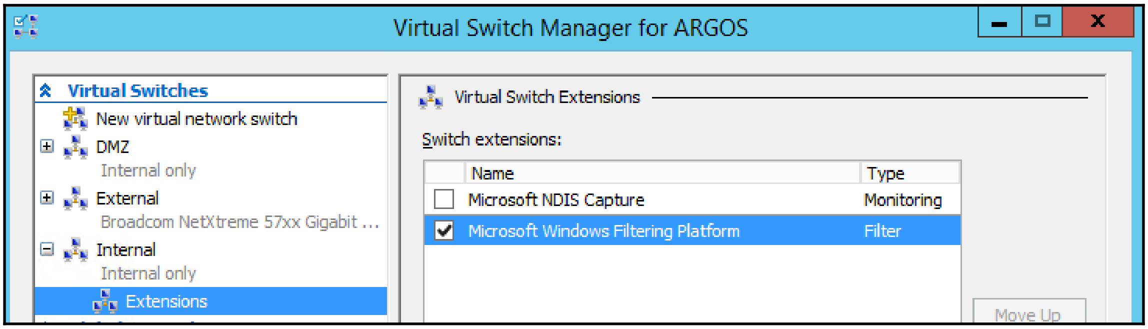
When planning your virtual network segmentation, you must first access the virtualization platform to see which capabilities are available. However, you can start planning the core segmentation using a vendor-agnostic approach, since the core principles are the same regardless of the platform, which is basically what the previous diagram is conveying. Note that there is isolation within the virtual switch; in other words, the traffic from one virtual network is not seen by the other virtual network. Each virtual network can have its own subnet, and all virtual machines within the virtual network will be able to communicate among themselves, but it won't traverse to the other virtual network. What if you want to have communication between two or more virtual networks? In this case, you need a router (it could be a VM with a routing service enabled) that has multiple virtual network adapters, one for each virtual network.

As you can see, the core concepts are very similar to the physical environment, and the only difference is the implementation, which may vary according to the vendor. Using Microsoft Hyper-V (Windows Server 2012 and beyond) as an example, it is possible to implement, at the virtual switch level, some security inspections using virtual extensions. Here are some examples that can be used to enhance your network security:

- Network packet inspection
- Intrusion detection or firewall
- Network packet filter

The advantage of using these types of extensions is that you are inspecting the packet before transferring it to other networks, which can be very beneficial for your overall network security strategy.

The following image shows an example of where these extensions are located. You can access this window by using Hyper-V Manager and selecting the properties of the **Virtual Switch Manager for ARGOS**:


Virtual Switch Manager for ARGOS
Virtual Switches
New virtual network switch
DMZ
Internal only
External
Broadcom NetXtreme 57xx Gigabit ...
Internal
Internal only
Extensions
Virtual Switch Extensions
Move Up

Switch extensions:

	Name	Type
□	Microsoft NDIS Capture	Monitoring
☑	Microsoft Windows Filtering Platform	Filter

Oftentimes, the traffic that originated in one VM can traverse to the physical network and reach another host connected to the corporate network. For this reason, it is important to always think that, although the traffic is isolated within the virtual network, if the network routes to other networks are defined, the packet will still be delivered to the destination. Make sure that you also enable the following capabilities in your virtual switch:

- **MAC address spoofing**: This prevents malicious traffic from being sent from a spoof address
- **DHCP guard**: This prevents virtual machines from acting or responding as a DHCP server
- **Router guard**: This prevents virtual machines from issuing router advertisement and redirection messages
- **Port ACL (access control list)**: This allows you to configure specific access control lists based on MAC or IP addresses

These are just some examples of what you can implement in the virtual switch. Keep in mind that you can usually extend these functionalities if you use a third-party virtual switch.

For example, the Cisco Nexus 1000V Switch for Microsoft Hyper-V offers more granular control and security. For more information, read `https://www.cisco.com/c/en/us/products/switches/nexus-1000v-switch-microsoft-hyper-v/index.html`.

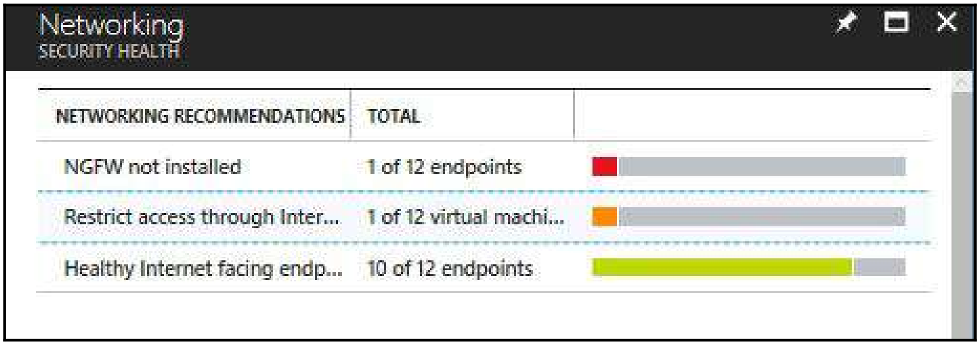
Hybrid cloud network security

According to McAfee's report, *Building Trust in a Cloudy Sky*, released in April 2017, hybrid cloud adoption grew three times in the previous year, which represents an increase from 19% to 57% of the organizations that were surveyed. In a nutshell, it is realistic to say that your organization will have some sort of connectivity to the cloud sooner or later, and according to the normal migration trend, the first step is to implement a hybrid cloud.

This section only covers one subset of security considerations for hybrid clouds. For broader coverage, read *A Practical Guide to Hybrid Cloud Computing*. Download it from `http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Hybrid-Cloud-Computing.pdf`.

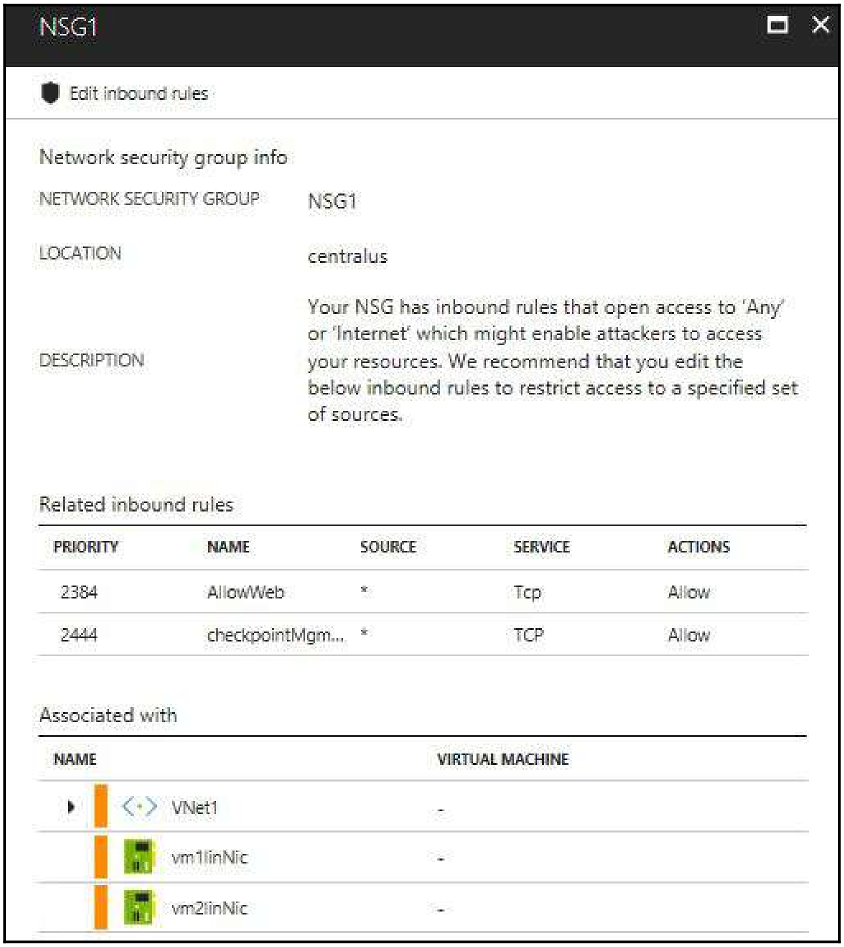
When designing your hybrid cloud network, you need to take everything that was previously explained into consideration and plan how this new entity will integrate with your environment. Many companies will adopt the site-to-site VPN approach to directly connect to the cloud and isolate the segment that has cloud connectivity. While this is a good approach, usually site-to-site VPN has an additional cost and requires extra maintenance. Another option is to use a direct route to the cloud, such as the Azure ExpressRoute.

While you have full control over the on-premises network and configuration, the cloud virtual network is going to be something new for you to manage. For this reason, it is important to familiarize yourself with the networking capabilities available in the cloud provider's IaaS, and how you can secure this network. Using Azure as an example, one way to quickly perform an assessment of how this virtual network is configured is to use Azure Security Center. Azure Security Center will scan the Azure virtual network that belongs to your subscription and suggest mitigations for potential security issues, as shown in the following screenshot:


Networking
SECURITY HEALTH

NETWORKING RECOMMENDATIONS	TOTAL	
NGFW not installed	1 of 12 endpoints	🟥
Restrict access through Inter...	1 of 12 virtual machi...	🟧
Healthy Internet facing endp...	10 of 12 endpoints	🟩

The list of recommendations may vary according to your **Azure Virtual Network** (**VNET**) and how the resources are configured to use this VNET. Let's use the second alert as an example, which is a medium-level alert that says *Restrict access through internet-facing endpoint*. When you click on it, you will see a detailed explanation about this configuration and what needs to be done to make it more secure:



NSG1

Edit inbound rules

Network security group info

NETWORK SECURITY GROUP NSG1

LOCATION centralus

DESCRIPTION Your NSG has inbound rules that open access to 'Any' or 'Internet' which might enable attackers to access your resources. We recommend that you edit the below inbound rules to restrict access to a specified set of sources.

Related inbound rules

PRIORITY	NAME	SOURCE	SERVICE	ACTIONS
2384	AllowWeb	*	Tcp	Allow
2444	checkpointMgm...	*	TCP	Allow

Associated with

NAME	VIRTUAL MACHINE
VNet1	-
vm1linNic	-
vm2linNic	-

This network security assessment is very important for hybrid scenarios where you have to integrate your on-premises network with a cloud infrastructure.

References

1. *Network Performance Monitor* `http://www.solarwinds.com/network-performance-monitor`
2. *User-to-Data-Center Access Control Using TrustSec Deployment Guide* `https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf`
3. *Security guide for Hyper-V in Windows Server 2012* `https://technet.microsoft.com/en-us/library/dn741280(v=ws.11).aspx`
4. *McAfee's Building Trust in a Cloudy Sky report* `https://www.mcafee.com/us/resources/reports/rp-building-trust-cloudy-sky-summary.pdf`
5. *Practical Guide to Hybrid Cloud Computing* `http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Hybrid-Cloud-Computing.pdf`

Summary

In this chapter, you learned about the current needs of using a defense in depth approach, and how this old method should be used to protect against current threats. You learned about the different layers of protection and how to increase the security of each layer. Physical network segmentation was the next topic covered, and here you learned about the importance of having a segmented network and how to correctly plan to implement that. You learned that network segmentation is not exclusively for on-premises resources, but also for remote users and remote offices. You also learned how it can be challenging for the Blue Team to plan and design this solution without accurately knowing the current network topology, and to address this problem, you learned about some tools that can be used during this discovery process. Lastly, you learned the importance of segmenting virtual networks and monitoring hybrid cloud connectivity.

In the next chapter, we will continue talking about defense strategies. This time, you will learn more about the sensors that should be implemented to actively monitor your resources and quickly identify potential threats.

11
Active Sensors

Now that your network is segmented, you need to actively monitor to detect suspicious activities and threats, and take actions based on that. Your security posture won't be fully completed if you don't have a good detection system, which means having the right sensors distributed across the network, monitoring the activities. The Blue Team should take advantages of modern detection technologies that create a profile of the user and computer to better understand anomalies and deviations in normal operations, and take preventative actions.

In this chapter, we are going to cover the following topics:

- Detection capabilities
- Intrusion detection systems
- Intrusion prevention systems
- Behavior analytics on-premises
- Behavior analytics in a hybrid cloud

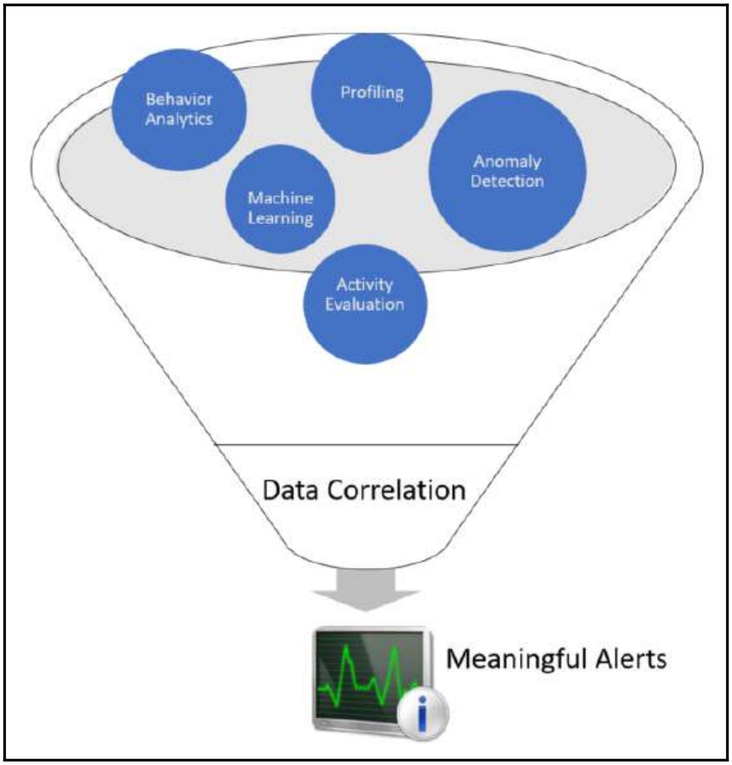
Detection capabilities

The current threat landscape demands a new approach to detection systems, relying on the traditional complexity to fine-tuning initial rules, thresholds, baselines and still deal with lots of false positives is becoming unacceptable for many organizations. When preparing to defend against attackers, the Blue Team must leverage a series of techniques that include:

- Data correlation from multiple data sources
- Profiling
- Behavior analytics
- Anomaly detection
- Activity evaluation
- Machine learning

It is important to emphasize that some of the traditional security controls, such as protocol analysis and signature-based antimalware, still have their space in the line of defense, but to combat legacy threats. You shouldn't uninstall your anti-malware software just because it doesn't have machine learning capability, it is still one level of protection to your host. Remember the defense in depth approach that we discussed in the last chapter? Think of this protection as one layer of defense, and now you need to aggregate the other layers to enhance your security posture.

On the other hand, the traditional defender mindset that focuses on monitoring only high profile users is over and you can't have this approach anymore. Current threat detections must look across all user accounts, profile them, and understand their normal behavior. Current threat actors will be looking to compromise the regular user, stay dormant in the network, continue the invasion by moving laterally, and escalate privileges. For this reason, the Blue Team must have detection mechanisms in place that can identify these behaviors across all devices, locations, and raise alerts based on the **Data Correlation**, as shown in the following diagram:



When you contextualize the data, you naturally reduce the amount of false positives, and give a more meaningful result to the investigator.

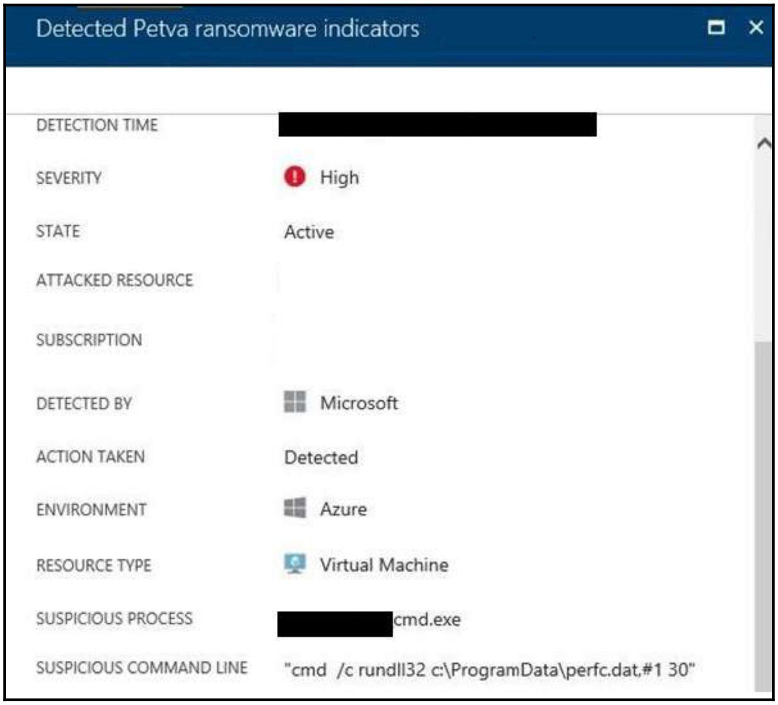
Indicators of compromise

When talking about detection, it is important to talk about **Indicators of Compromise** (**IoC**). When new threats are found in the wild, they usually have a pattern of behavior and they leave their footprint in the target system.

For example, Petya ransomware ran the following commands in the target system to reschedule a restart:

```
    schtasks /Create /SC once /TN "" /TR "<system folder>shutdown.exe /r
/f" /ST <time>
    cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR
"C:Windowssystem32shutdown.exe /r /f" /ST <time>
```

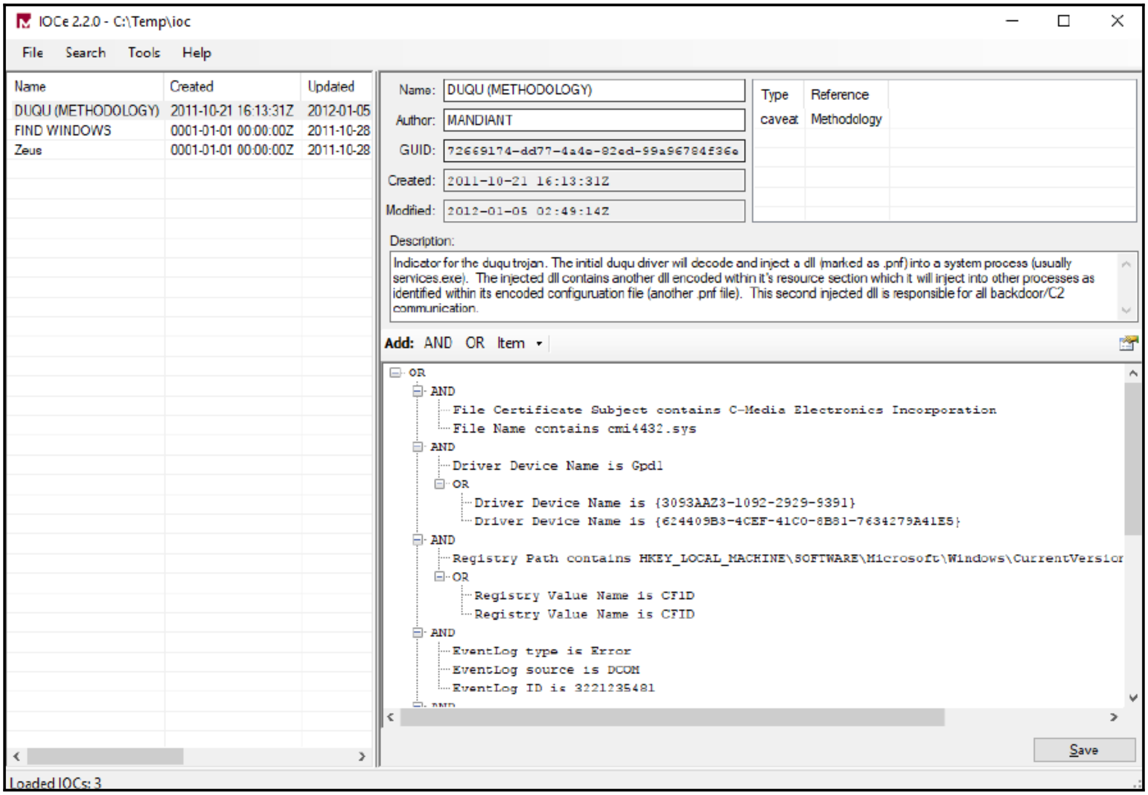
Another Petya IoC is the local network scan on ports TCP `139` and TCP `445`. These are important indications that there is an attack taking place on the target system and, based on this footprint, Petya is the one to blame. Detection systems will be able to gather these indicators of compromise and raise alerts when an attack happens. Using Azure Security Center as an example, some hours after the Petya outbreak, Security Center automatically updates its detection engine and was able to warn users that their machine was compromised, as shown in the following screenshot:



Detected Petva ransomware indicators

DETECTION TIME	[redacted]
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	
SUBSCRIPTION	
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
SUSPICIOUS PROCESS	[redacted]cmd.exe
SUSPICIOUS COMMAND LINE	"cmd /c rundll32 c:\ProgramData\perfc.dat,#1 30"

You can sign up with OpenIOC (`http://openioc.org`) to retrieve information regarding new IoC and also contribute to the community. By using their IoC Editor (consult the reference section for the URL to download this tool), you can create your own IoC or you can review an existing IoC. The example that follows shows the IoC Editor showing the **DUQU** Trojan IoC:



Name	Created	Updated
DUQU (METHODOLOGY)	2011-10-21 16:13:31Z	2012-01-05
FIND WINDOWS	0001-01-01 00:00:00Z	2011-10-28
Zeus	0001-01-01 00:00:00Z	2011-10-28

Name: DUQU (METHODOLOGY)
Author: MANDIANT
GUID: 72669174-dd77-4a4e-82ed-99a96784f36e
Created: 2011-10-21 16:13:31Z
Modified: 2012-01-05 02:49:14Z

Type	Reference
caveat	Methodology

Description:
Indicator for the duqu trojan. The initial duqu driver will decode and inject a dll (marked as .pnf) into a system process (usually services.exe). The injected dll contains another dll encoded within it's resource section which it will inject into other processes as identified within its encoded configuruation file (another .pnf file). This second injected dll is responsible for all backdoor/C2 communication.

```
OR
    AND
        File Certificate Subject contains C-Media Electronics Incorporation
        File Name contains cmi4432.sys
    AND
        Driver Device Name is Gpd1
        OR
            Driver Device Name is {3093AAZ3-1092-2929-9391}
            Driver Device Name is {624409B3-4CEF-41C0-8B81-7634279A41E5}
    AND
        Registry Path contains HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersior
        OR
            Registry Value Name is CF1D
            Registry Value Name is CFID
    AND
        EventLog type is Error
        EventLog source is DCOM
        EventLog ID is 3221235481
```

If you look in the right lower pane, you will see all the indications of compromise, and logic operators (in this case most are **AND**) that compare each sequence and only return positive if everything is true. The Blue Team should always be aware of the latest threats, and IoC.

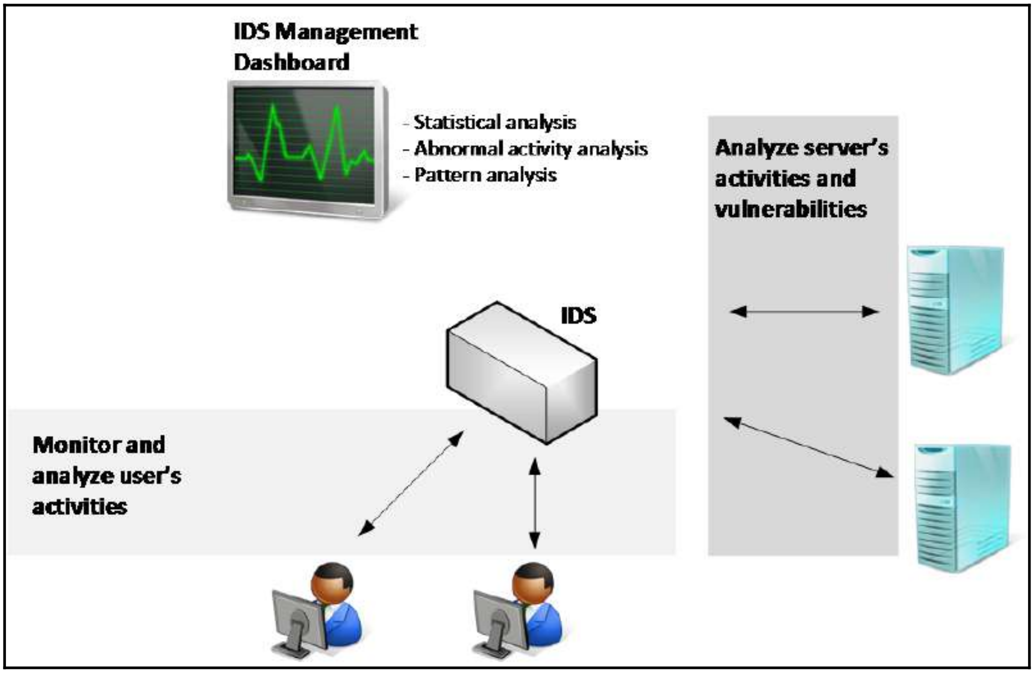
You can use the following PowerShell command to download an IoC from OpenIOC, for the example below you are downloading the IoC for Zeus threat: `wget "http://openioc.org/iocs/72669174-dd77-4a4e-82ed-99a96784f36e.ioc" -outfile "72669174-dd77-4a4e-82ed-99a96784f36e.ioc"`

Intrusion detection systems

As the name implies, an **intrusion detection system** (**IDS**) is responsible for detecting a potential intrusion and trigger an alert. What can be done with this alert depends on the IDS policy. When creating an IDS Policy you need to answer the following questions:

- Who should be monitoring the IDS?
- Who should have administrative access to the IDS?
- How incidents will be handled based on the alerts generated by the IDS?
- What's the IDS update policy?
- Where should we install the IDS?

These are just some examples of initial questions that should help in planning the IDS adoption. When searching for IDS, you can also consult a list of vendors at ICSA Labs Certified Products (`www.icsalabs.com`) for more vendor-specific information. Regardless of the brand, a typical **IDS** has the capabilities shown in the following diagram:


IDS Management Dashboard
- Statistical analysis
- Abnormal activity analysis
- Pattern analysis
Analyze server's activities and vulnerabilities
IDS
Monitor and analyze user's activities

While these are some core capabilities, the amount of features will really vary according to the vendor and the method used by the IDS. The signature-based IDS will query a database of previous attack's signatures (footprints) and known system vulnerabilities to verify what was identified is a threat and if an alert must be triggered. Since this is a database of signatures, it requires constant update in order to have the latest version. The behavior-based IDS works by creating a baseline of patterns based on what it learned from the system. Once it learns the normal behavior, it becomes easier to identify deviations from normal activity.

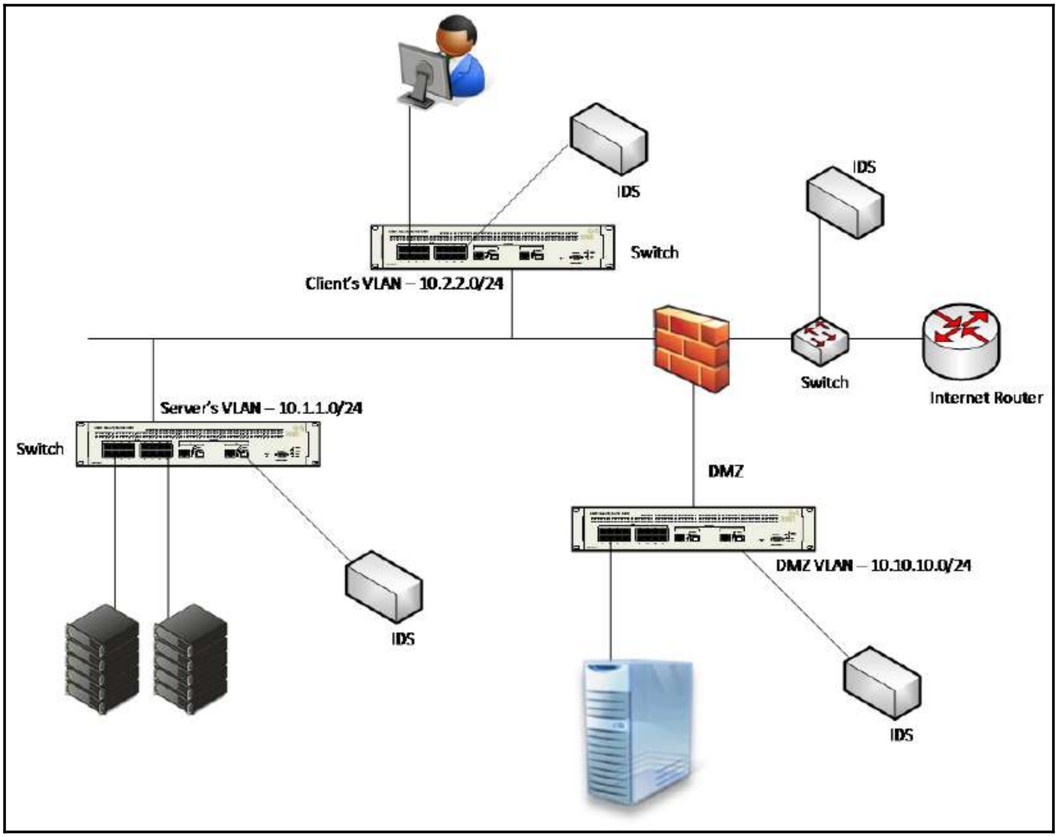
An IDS alert is any type of user notification to bring awareness about a potential intrusion activity.

IDS can be host-based, as known as host-based intrusion detection system (**HIDS**), where the IDS mechanism will only detect an intrusion's attempt against a particular host, or it can be a **network-based intrusion detection system** (**NIDS**), where it detects intrusion for the network segment that the NIDS is installed. This means that in the NIDS case, the placement becomes critical in order to gather valuable traffic. This is where the Blue Team should work closely with the IT Infrastructure team to ensure that the IDS is installed in strategic places across the network. Prioritize the following network segments when planning the NIDS placement:

- DMZ/Perimeter
- Core corporate network
- Wireless network
- Virtualization network
- Other critical network segments

These sensors will be listening to the traffic, which means it won't be consuming too much network bandwidth.

The diagram that follows has an example of where to put the **IDS**:



Notice that, in this case, an **IDS** (which in reality here is a NIDS) was added to each segment (leveraging a SPAN port on the network switch). Is it always like that? Absolutely not! It will vary according to your company's needs. The Blue Team must be aware of the company's constraints and help identify the best location where these devices should be installed.

Intrusion prevention system

An **intrusion prevention system** (**IPS**) uses the same concept of an IDS, but, as the name says, it prevents the intrusion by taking a corrective action. This action will be customized by the IPS administrator in partnership with the Blue Team.

The same way IDS is available for hosts (HIDS) and network (NIDS), IPS is also available for both as HIPS and NIPS. The NIPS placement within your network is critical and the same guidelines that were previously mentioned, are applicable here. You should also consider placing the NIPS inline with traffic in order to be able to take corrective actions. IPS detection can usually operate in one or more of the following modes:

- Rule-based
- Anomaly-based

Rule-based detection

While operating this mode, the IPS will compare the traffic with a set of rules and try to verify if the traffic matches the rule. This is very useful when you need to deploy a new rule to block an attempt to exploit a vulnerability. NIPS systems, such as **Snort**, are able to block threats by leveraging rule-based detection. For example, the Snort rule Sid `1-42329` is able to detect the `Win.Trojan.Doublepulsar` variant.

Snort rules are located under `etc/snort/rules` and you can download other rules from `https://www.snort.org/downloads/#rule-downloads`. When the Blue Team is going through an exercise with the Red Team, chances are that new rules must be created according to the traffic pattern and the attempts that the Red Team is making to infiltrate the system. Sometimes you need multiple rules to mitigate a threat, for example, the rules `42340` (Microsoft Windows SMB anonymous session IPC share access attempt), `41978` (Microsoft Windows SMB remote code execution attempt), and `42329-42332` (`Win.Trojan.Doublepulsar` variant) can be used to detect WannaCry ransomware. The same applies for other IPS, such as Cisco IPS that has signatures `7958/0` and `7958/1`, created to handle WannaCry.

Subscribe to the Snort blog to receive updates regarding new rules at `http://blog.snort.org`.

The advantage of using an open source NIPS, such as Snort, is that when a new threat is available in the wild, the community usually responds pretty fast with with a new rule to detect the threat. For example, when Petya ransomware was detected, the community created a rule, and posted at GitHub (you can see this rule here `https://goo.gl/mLtnFM`). Although vendors and the security community are really fast to publish new rules, the Blue Team should be watching for new IoCs, and create NIPS rules based on these IoCs.

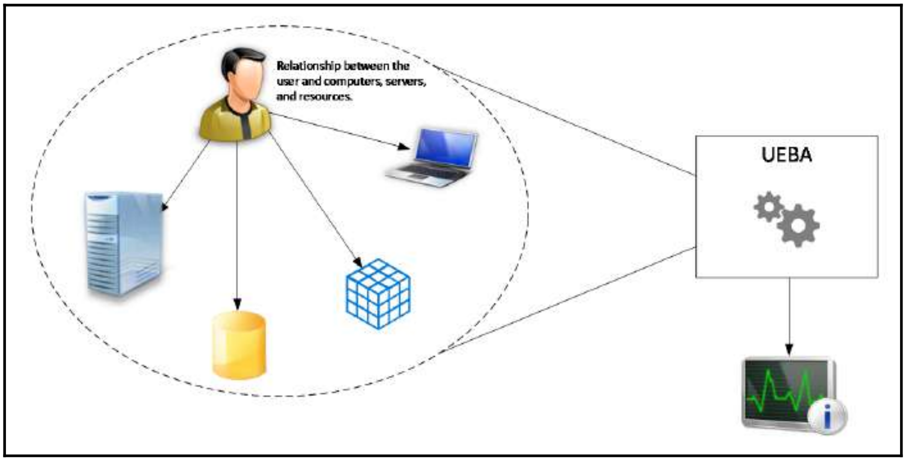
Anomaly-based detection

The anomaly, in this case, is based on what the IPS categorize as anomalous, this classification is usually based on heuristics or a set of rules. One variation of this is called statistical anomaly detection, which takes samples of network traffic at random times, and performs a comparison with a baseline. If this sample fits outside of the baseline, an action is taken (alert followed by action).

Behavior analytics on-premises

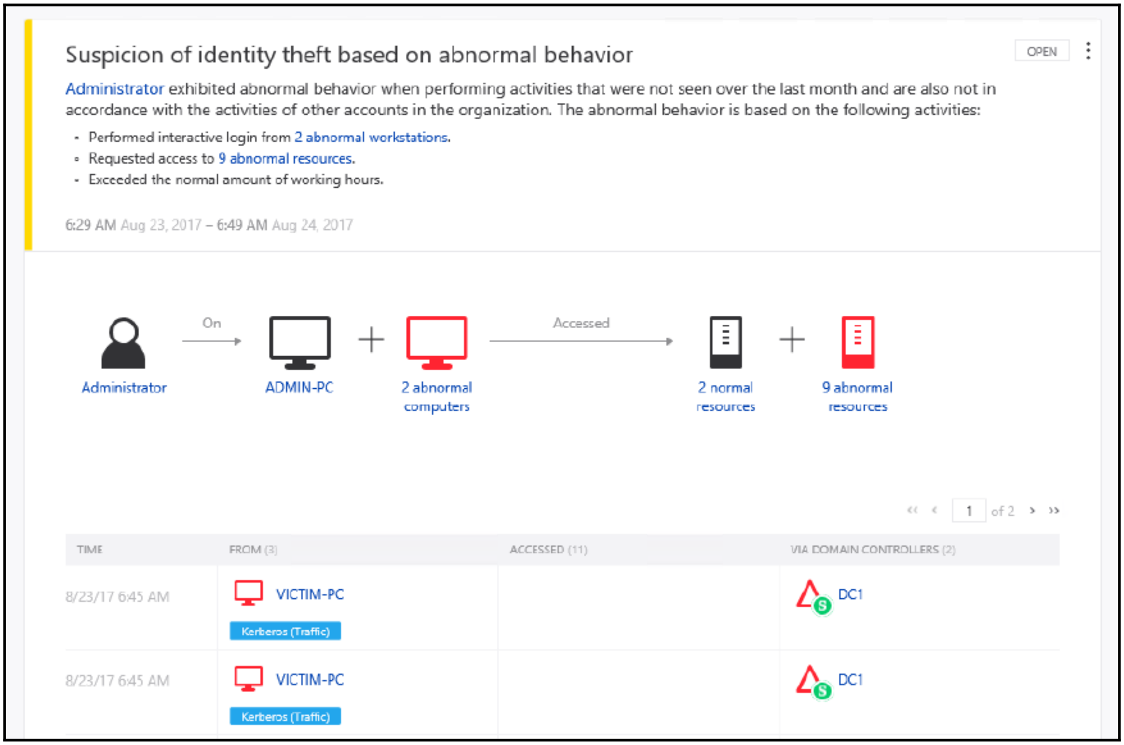
For the vast majority of the companies currently in the market, the core business still happens on-premises. There is where the critical data is located, the majority of the users are working, and the key assets are located. As you know, we covered attack strategies in the first part of this book; the attacker tends to silently infiltrate your on-premises network, move laterally, escalate privilege, and maintain connectivity with command and control until he is able to execute his mission. For this reason, having behavior analytics on-premises is imperative to quickly break the attack kill chain.
According to Gartner, it is primordial to understand how users behave, and by tracking legitimate processes, organizations can enlist **User and Entity Behavior Analytics** (**UEBA**) to spot security breaches. There are many advantages in using an UEBA to detect attacks, but one of the most important ones is the capability to detect attacks in the early stages and take corrective action to contain the attack.

The following diagram shows an example of how **UEBA** looks across different entities in order to take a decision if an alert must be triggered or not:


Relationship between the user and computers, servers, and resources.
UEBA

Without having a system that can look broadly to all data and make correlations not only on the traffic pattern, but also on a user's profile, the chances of having a false positive increase. What happens nowadays is when you use your credit card in a place that you ahve never been before and in a geographic location that you don't constantly go. If your credit card has monitoring protection, someone will call you to validate that transaction; this happens because the system understands your credit card usage pattern, it knows the places that you visited before, the locations that you bought, and even an average of what you usually spend. When you deviate from all these patterns that are interconnected, the system triggers an alert and the action that is taken is to have someone call you to double check if this is really you doing that transaction. Notice that in this scenario, you are acting quickly in the early stage, because the credit card company put that transaction on hold until they get your validation.

The same thing happens when you have an UEBA system on premises. The system knows what servers your users usually access, what shares they usually visit, what operating system they usually use to access these resources, and the user's geo-location. The following figure shows an example of this type of detection coming from Microsoft **Advanced Threat Analytics** (**ATA**), which uses behavior analytics to detect suspicious behavior:



Suspicion of identity theft based on abnormal behavior

Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

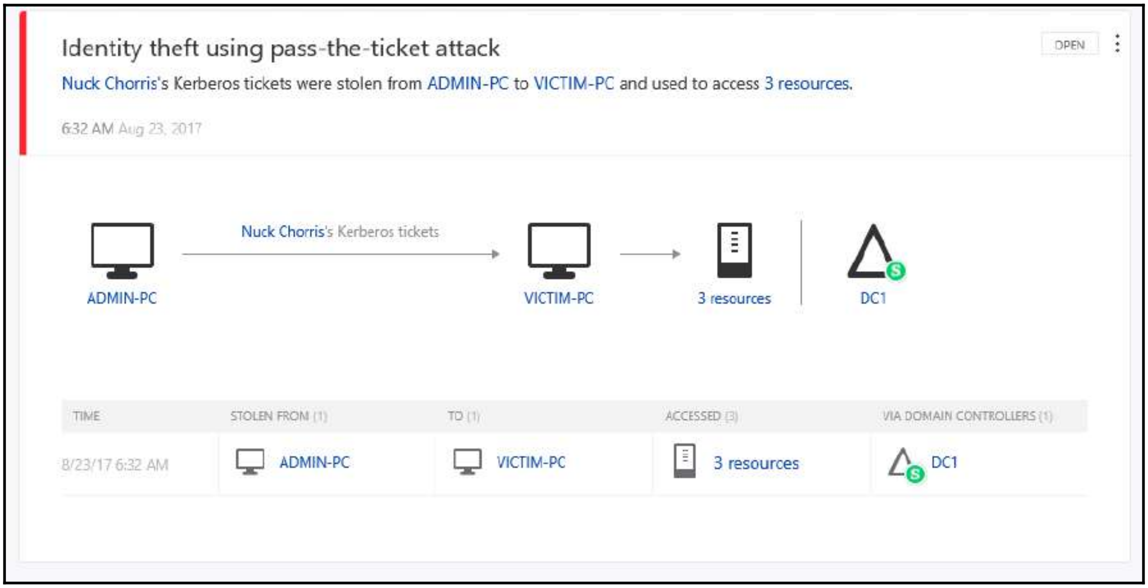
- Performed interactive login from 2 abnormal workstations.
- Requested access to 9 abnormal resources.
- Exceeded the normal amount of working hours.

6:29 AM Aug 23, 2017 – 6:49 AM Aug 24, 2017

TIME	FROM (3)	ACCESSED (11)	VIA DOMAIN CONTROLLERS (2)
8/23/17 6:45 AM	VICTIM-PC Kerberos (Traffic)		DC1
8/23/17 6:45 AM	VICTIM-PC Kerberos (Traffic)		DC1

Notice that, in this case, the message is pretty clear, it says that the **Administrator** didn't perform these activities in the last month and not in correlation with other accounts within the organization. This alert is not something that can be ignored, because it is contextualized, which means it looks to the data that was collected in different angles to create a correlation and make a decision if an alert should be raised or not.

Having a UEBA system on-premises can help the Blue Team to be more proactive, and have more tangible data to accurately react. The UEBA system is composed of multiple modules and another module is the advanced threat detection, which looks for known vulnerabilities and attack patterns. The following figure shows Microsoft ATA detecting a pass-the-ticket attack:



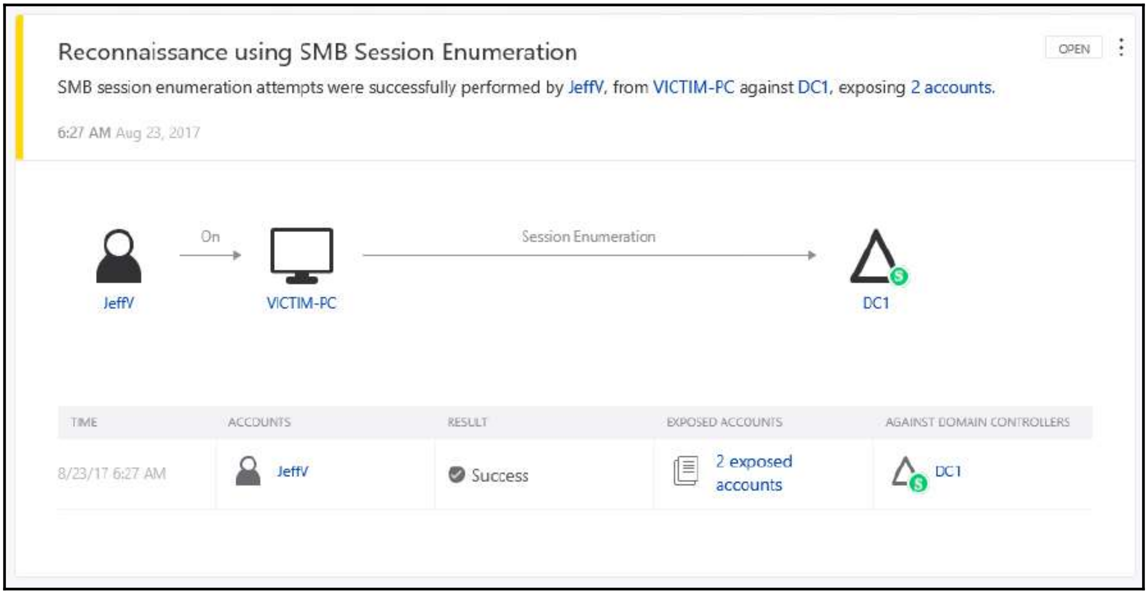
Identity theft using pass-the-ticket attack

Nuck Chorris's Kerberos tickets were stolen from ADMIN-PC to VICTIM-PC and used to access 3 resources.

6:32 AM Aug 23, 2017

TIME	STOLEN FROM (1)	TO (1)	ACCESSED (3)	VIA DOMAIN CONTROLLERS (1)
8/23/17 6:32 AM	ADMIN-PC	VICTIM-PC	3 resources	DC1

Since there are different ways to perform this attack, advanced threat detection can't look just for the signature, it needs to look for the attack pattern and what the attacker is trying to do; this is way more powerful than using a signature-based system. It also looks for suspicious behavior coming from regular users that are not supposed to be doing certain tasks, for example if a regular user tries to run `NetSess.exe` tool against the local domain, Microsoft ATA will consider this a SMB session enumeration, which from the attacker's perspective, is usually done during the reconnaissance phase. For this reason, an alert is raised as shown in the following screenshot:



Reconnaissance using SMB Session Enumeration

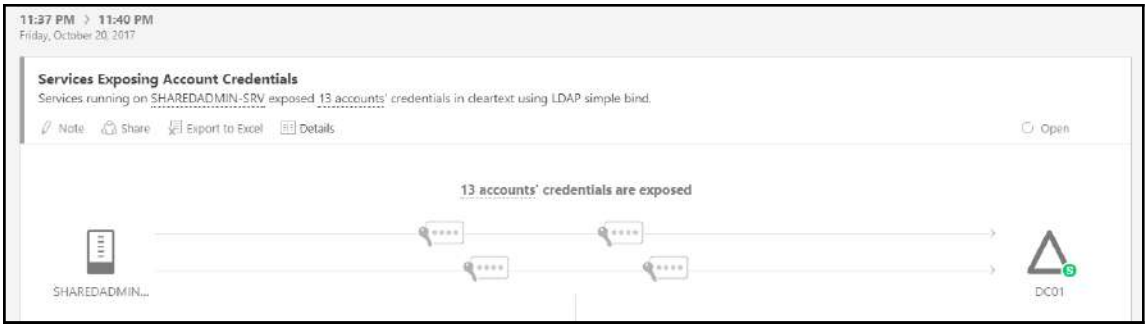
SMB session enumeration attempts were successfully performed by JeffV, from VICTIM-PC against DC1, exposing 2 accounts.

6:27 AM Aug 23, 2017

TIME	ACCOUNTS	RESULT	EXPOSED ACCOUNTS	AGAINST DOMAIN CONTROLLERS
8/23/17 6:27 AM	JeffV	Success	2 exposed accounts	DC1

Attackers will not only exploit vulnerabilities, but also take advantage of misconfigurations in the target system, such as bad protocol implementation and lack of hardening. For this reason, the UEBA system will also detect systems that are lacking a secure configuration.

The following example shows Microsoft Advanced Threat Analytics detecting a service that is exposing account credentials because it is using **LDAP** without encryption:



11:37 PM › 11:40 PM
Friday, October 20, 2017

Services Exposing Account Credentials

Services running on SHAREDADMIN-SRV exposed 13 accounts' credentials in cleartext using LDAP simple bind.

Device placement

Using the same principles that were previously discussed in the IDS section, the location where you will install your UEBA will vary according to the company's needs and the vendor's requirements. The Microsoft ATA that was used in the examples explained in the previous section requires that you use port mirroring with the domain controller (DC). ATA will have no impact in the network bandwidth since it will be only listening to the DC traffic. Other solutions might require a different approach; for this reason, it is important to plan according to the solution that you purchased for your environment.

Behavior analytics in a hybrid cloud

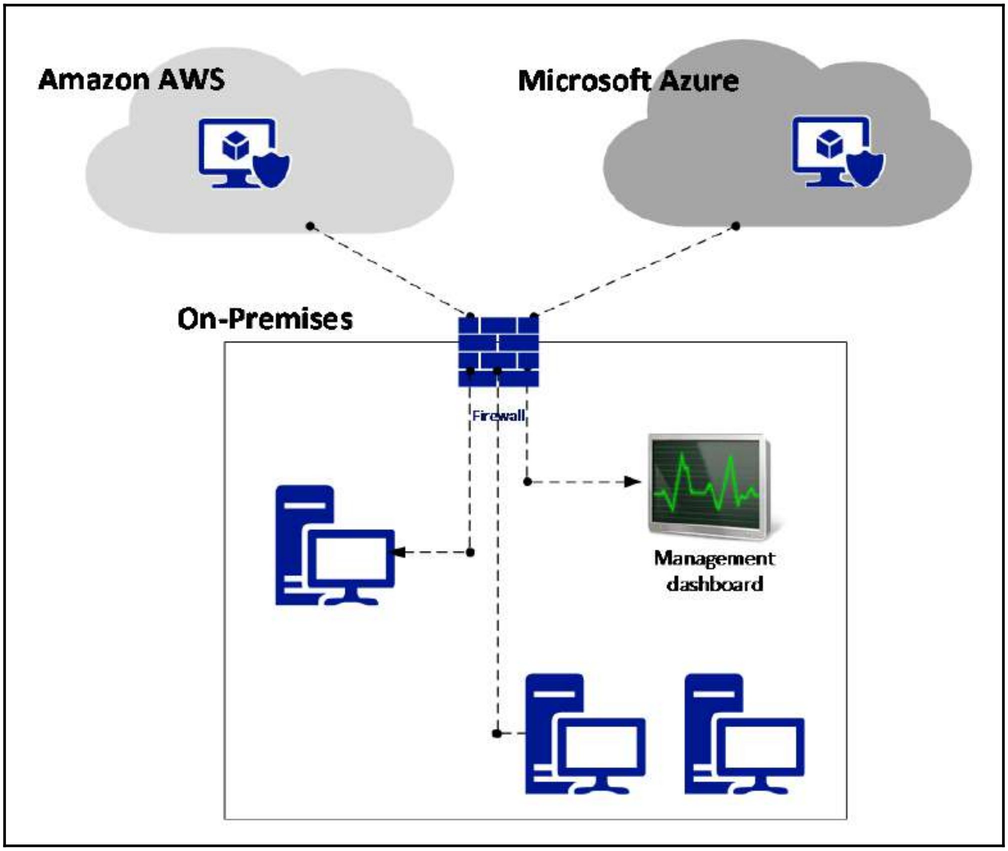
When the Blue Team needs to create countermeasures to secure a hybrid environment, the team needs to expand their view of the current threat landscape, and perform an assessment in order to validate continuous connectivity with the cloud and check the impact on overall security posture. In a hybrid cloud, most companies will opt to use an IaaS model and, although IaaS adoption is growing, the security aspect of it is still the main concern, according to an Oracle survey on IaaS Adoption. According to the same report, *longer term IaaS users suggest the technology ultimately makes a positive impact on security*. In reality, it does have a positive impact and that's where the Blue Team should focus their efforts on improving their overall detection. The intent is to leverage hybrid cloud capabilities to benefit the overall security posture. The first step is to establish a good partnership with your cloud provider and understand what security capabilities they have, and how these security capabilities can be used in a hybrid environment. This is important, because some capabilities are only available in the cloud, and not on-premises.

Read the article *Cloud security can enhance your overall security posture* to better understand some benefits of cloud computing for security.

You can get the article from: `http://go2l.ink/SecPosture`.

Azure Security Center

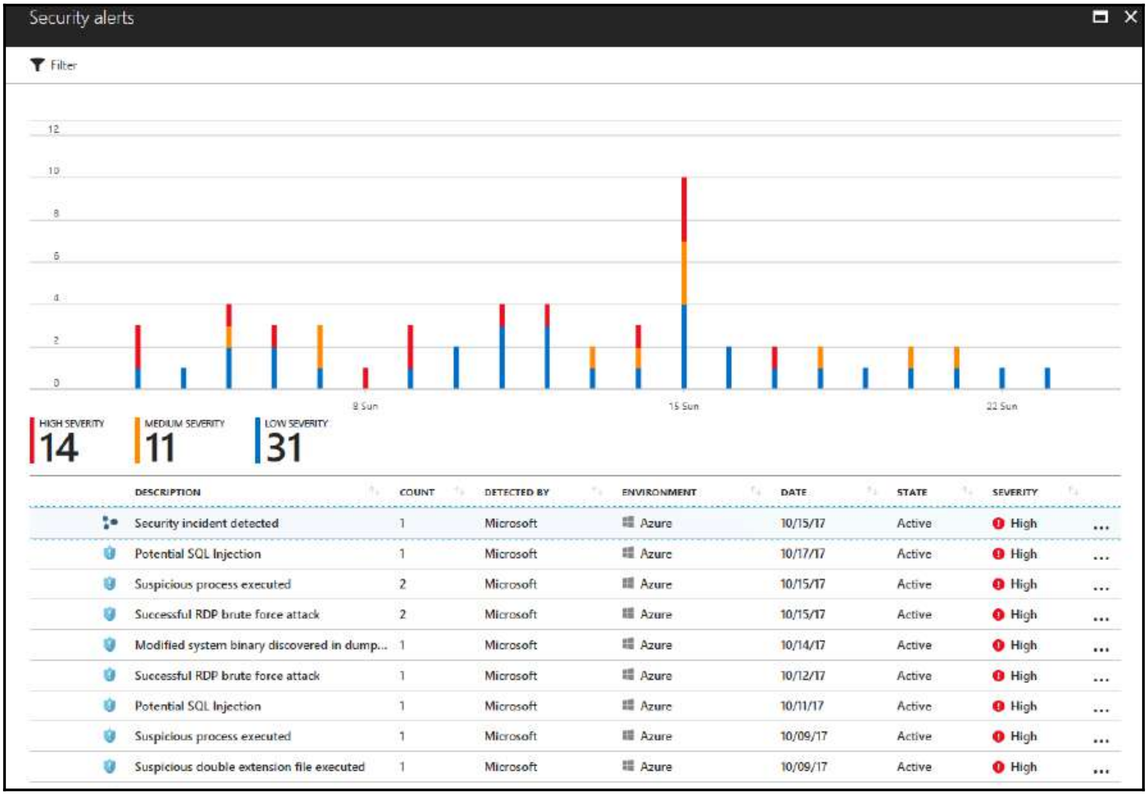
The reason we are using Azure Security Center to monitor hybrid environment is because the Security Center agent can be installed on a computer (Windows or Linux) on-premises, in a VM running in Azure, or in AWS. This flexibility is important and centralized management is important for the Blue Team. Security Center leverages security intelligence and advanced analytics to detect threats more quickly and reduce false positives. In an ideal scenario, the Blue Team will use a single pane of glass to visualize alerts and suspicious activities across all workloads. The core topology looks similar to the one shown in the following figure:



When the Security Center is installed on these computers, it will collect **Event Tracing for Windows** (**ETW**) traces, operating system log events, running processes, machine name, IP addresses, and logged in users. These events are sent to Azure, and stored in your private workspace storage. Security Center will analyze this data using the following methods:

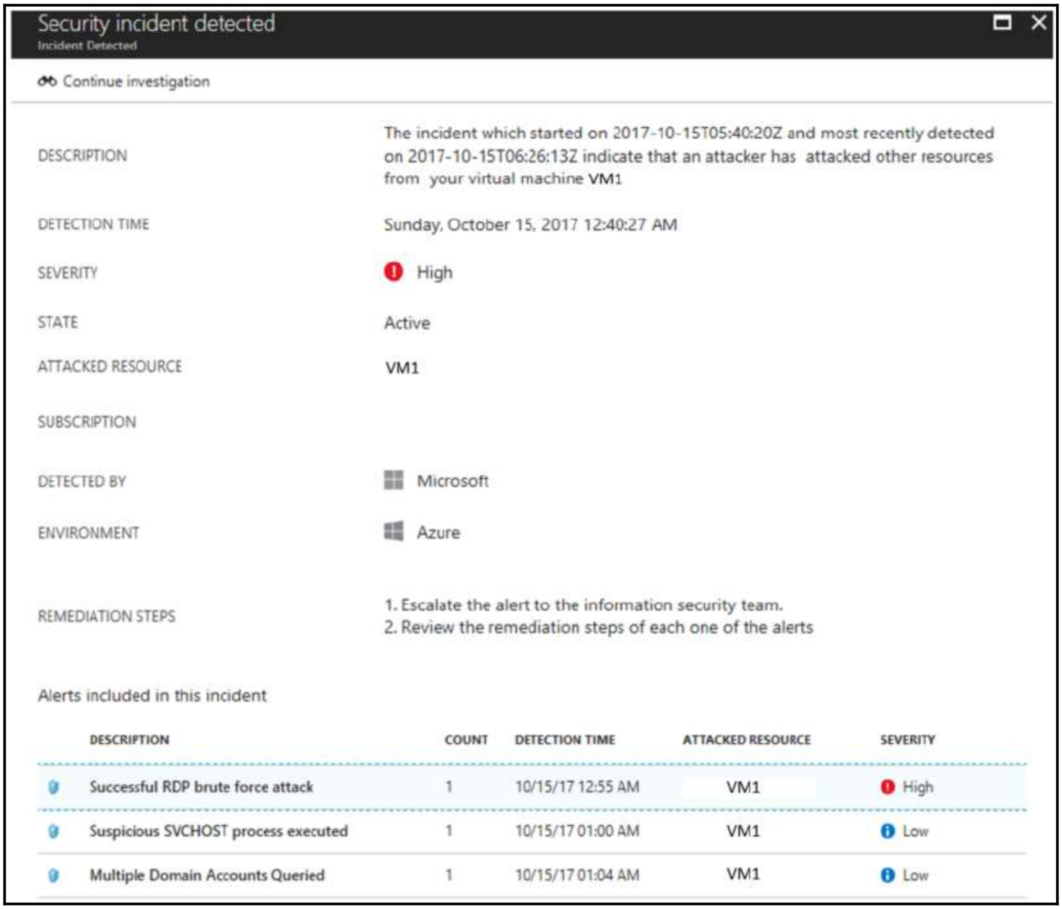
- Threat intelligence
- Behavioral analytics
- Anomaly detection

Once this data is evaluated, Security Center will trigger an alert based on priority and add in the dashboard, as shown in the following screenshot:



DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY	
Security incident detected	1	Microsoft	Azure	10/15/17	Active	High	...
Potential SQL Injection	1	Microsoft	Azure	10/17/17	Active	High	...
Suspicious process executed	2	Microsoft	Azure	10/15/17	Active	High	...
Successful RDP brute force attack	2	Microsoft	Azure	10/15/17	Active	High	...
Modified system binary discovered in dump...	1	Microsoft	Azure	10/14/17	Active	High	...
Successful RDP brute force attack	1	Microsoft	Azure	10/12/17	Active	High	...
Potential SQL Injection	1	Microsoft	Azure	10/11/17	Active	High	...
Suspicious process executed	1	Microsoft	Azure	10/09/17	Active	High	...
Suspicious double extension file executed	1	Microsoft	Azure	10/09/17	Active	High	...

Notice that the first alert has a different icon and it is called **Security incident detected**. This happens because it was identified and two or more attacks are part of the same attack campaign against a specific resource. This means that, instead of having someone from the Blue Team to scavenge the data to find correlation between events, Security Center does that automatically and provides the relevant alerts for you to analyze. When you click on this alert, you will see the following page:



Security incident detected

Incident Detected

DESCRIPTION	The incident which started on 2017-10-15T05:40:20Z and most recently detected on 2017-10-15T06:26:13Z indicate that an attacker has attacked other resources from your virtual machine VM1
DETECTION TIME	Sunday, October 15, 2017 12:40:27 AM
SEVERITY	❗ High
STATE	Active
ATTACKED RESOURCE	VM1
SUBSCRIPTION	
DETECTED BY	Microsoft
ENVIRONMENT	Azure
REMEDIATION STEPS	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts

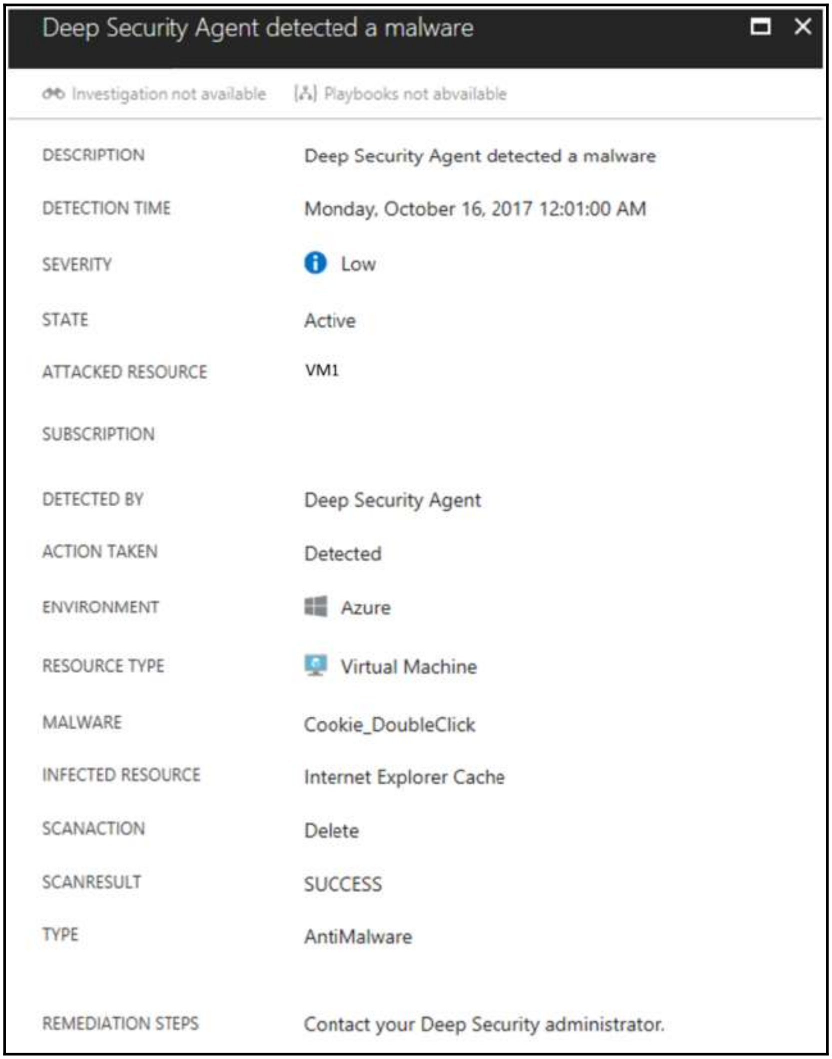
Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Successful RDP brute force attack	1	10/15/17 12:55 AM	VM1	❗ High
Suspicious SVCHOST process executed	1	10/15/17 01:00 AM	VM1	ℹ Low
Multiple Domain Accounts Queried	1	10/15/17 01:04 AM	VM1	ℹ Low

At the bottom of this page, you can see all three attacks (in order of occurrence) that took place against **VM1** and the severity level assigned by Security Center. One important observation about the advantage of using behavior analytics to detect threats, is the third alert (**Multiple Domain Accounts Queried**). The command that was executed to raise this alert was a simple *`net user <username> /domain`*; however, to make the decision that this is a suspicious, it needs to look at the normal behavior for the user that executed this command and cross-reference this information with other data that when analyzed in context, will be categorized as suspicious. As you can see in this example, hackers are leveraging built-in system tools and native command line interface to perform their attack; for this reason, it is paramount to have a command line logging tool.

Security Center will also use statistical profiling to build historical baselines and alert on deviations that conform to a potential attack vector. This is useful in many scenarios; one typical example is deviations from normal activity. For example, let's say a host starts RDP connections three times a day, but in a certain day there are one hundred connections attempted. When such deviation happens, an alert must be triggered to warn you about that.

Another important aspect of working with a cloud based service is the built in integration with other vendors. Security Center can integrate with many other solutions, such as Barracuda, F5, Imperva, and Fortinet for **web application firewall** (**WAF**), among others for endpoint protection, vulnerability assessment, and next-generation firewall. The image below shows an example of this integration. Notice that this alert was generated by **Deep Security Agent** and, since it is integrated with Security Center, it will appear in the same dashboard as the other events that were detected by Security Center:



Deep Security Agent detected a malware

DESCRIPTION	Deep Security Agent detected a malware
DETECTION TIME	Monday, October 16, 2017 12:01:00 AM
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	VM1
SUBSCRIPTION	
DETECTED BY	Deep Security Agent
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
MALWARE	Cookie_DoubleClick
INFECTED RESOURCE	Internet Explorer Cache
SCANACTION	Delete
SCANRESULT	SUCCESS
TYPE	AntiMalware
REMEDIATION STEPS	Contact your Deep Security administrator.

Keep in mind that Security Center is not the only solution that will monitor systems and integrate with other vendors; there are many **Security Information and Event Management** (**SIEM**) solutions, such as **Splunk** and **LogRhythm**, that will perform similar type of monitoring.

References

1. Snort Rules Explanation
   `https://www.snort.org/rules_explanation`
2. Introduction to IoC `http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf`
3. IoC Editor `https://www.fireeye.com/content/dam/fireeye-www/services/freeware/sdl-ioc-editor.zip`
4. DUQU Uses STUXNET-Like Techniques to Conduct Information Theft

   `https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/90/duqu-uses-stuxnetlike-techniques-to-conduct-information-theft`
5. How to Select a Network Intrusion Prevention System (IPS)

   `https://www.icsalabs.com/sites/default/files/HowToSelectANetworkIPS.pdf`
6. Detect Security Breaches Early by Analyzing Behavior

   `https://www.gartner.com/smarterwithgartner/detect-security-breaches-early-by-analyzing-behavior/`
7. Advanced Threat Analytics attack simulation playbook
   `https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/ata-attack-simulation-playbook`
8. You and IaaS - Learning from the success of early adopters
   `https://www.oracle.com/assets/pulse-survey-mini-report-3764078.pdf`

Summary

In this chapter, you learned about the different types of detection mechanisms and the advantages of using them to enhance your defense strategy. You learned about the indications of compromise and how to query current threats. You also learned about IDS, how it works, the different types of IDS, and the best location to install IDS based on your network. Next, you learned about the benefits of using an IPS, how rule-based and how anomaly-based detection works. The defense strategy wouldn't be completed without a good behavior analytics and, in this section, you learned how the Blue Team can benefit from this capability. Microsoft ATA was used as the on-premises example for this implementation and Azure Security Center was used as the hybrid solution for behavior analytics.

In the next chapter, we will continue talking about defense strategies; this time, you will learn more about threat intelligence and how the Blue Team can take advantage of threat intel to enhance the overall security of the defense systems.

12
Threat Intelligence

By now, you've been through different phases in your journey to a better defense model. In the last chapter, you learned about the importance of a good detection system, and now it's time to move to the next level. The use of threat intelligence to better know the adversary, and gain insights about the current threats, is a valuable tool for the Blue Team. Although threat intelligence is a relatively new domain, the use of intelligence to learn how the enemy is operating is an old concept. Bringing intelligence to the field of cybersecurity was a natural transition, mainly because now the threat landscape is so broad and the adversaries vary widely, from state-sponsored actors to cybercriminals extorting money from their victims.

In this chapter, we are going to cover the following topics:

- Introduction to threat intelligence
- Open source tools for threat intelligence
- Microsoft threat intelligence
- Leveraging threat intelligence to investigate suspicious activity

Introduction to threat intelligence

It was clear in the last chapter that having a strong detection system is imperative for your organization's security posture. However, this system can be improved if the number of false positives and noise can be reduced. One of the main challenges that you face when you have many alerts and logs to review is that you end up randomly prioritizing, and in some cases even ignoring, future alerts because you believe it is not worth reviewing them. According to Microsoft's *Lean on the Machine* report, an average large organization has to look through 17,000 malware alerts each week, taking on average 99 days for an organization to discover a security breach.

Alert triage usually happens at the **network operations center** (**NOC**) level, and delays to triage can lead to a domino effect, because if triage fails at this level, the operation will also fail, and in this case, the operation will be handled by the incident response team.

Let's step back and think about threat intelligence outside of cyberspace.

How do you believe the Department of Homeland Security improves the United States, threats to border security?

They have the **Office of Intelligence and Analysis** (**I&A**), which uses intelligence to enhance border security. This is done by driving information sharing across different agencies and providing predictive intelligence to decision makers at all levels. Now, use the same rationale toward cyber threat intelligence, and you will understand how effective and important this is. This insight shows that you can improve your detection by learning more about your adversaries, their motivations, and the techniques that they are using. Using this threat intelligence towards the data that you collect can bring more meaningful results and reveal actions that are not detectable by traditional sensors.

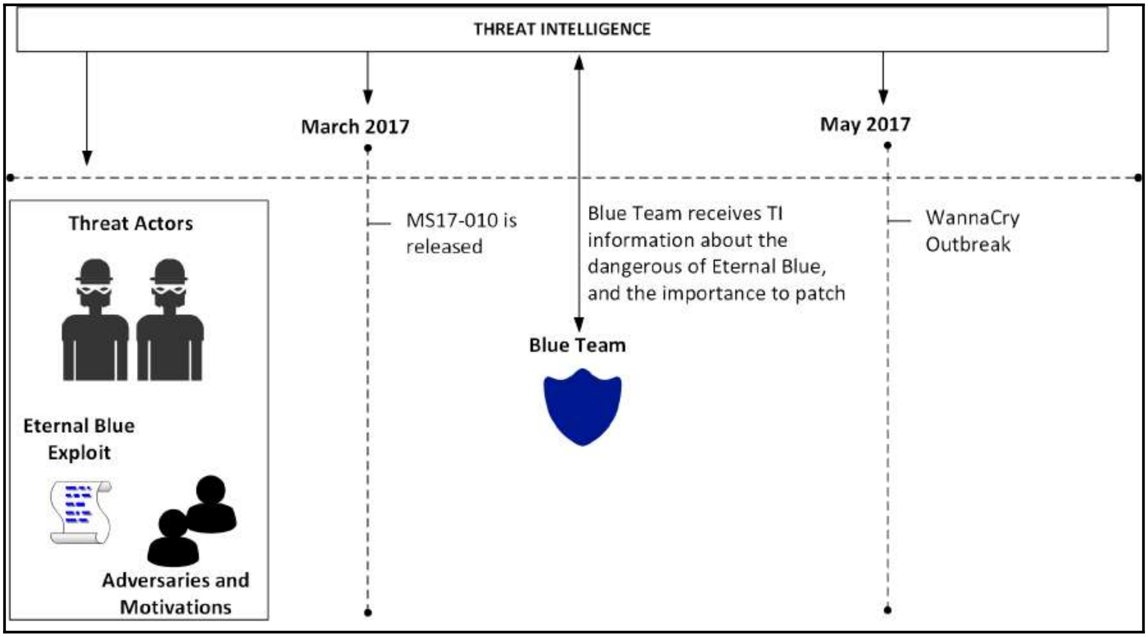
It is important to mention that the attacker's profile will be directly related to their motivation. Here are some examples of an attacker's profile/motivation:

- **Cybercriminal**: The main motivation is to obtain financial results
- **Hacktivist**: This group has a broader scope of motivation—it can range from an expression of political preference to just an expression for a particular cause
- **Cyber espionage/state sponsored**: Although you can have cyber espionage without it being state sponsored (usually in the private sector), a growing number of cyber espionage cases are happening because they are part of bigger state-sponsored campaigns

The question now is: Which attack profile is most likely to target your organization? It depends. If your organization is sponsoring a particular political party, and this political party is doing something that a hacktivist group is totally against, you might be a target. If you identify yourself as the target, the next question is: What assets do I have that are most likely desired by this group? Again, it depends. If you are a financial group, cybercriminals will be your main threat, and they usually want credit card information, financial data, and so on.

Another advantage of using threat intelligence as part of your defense system is the ability to scope data based on the adversary. For example, if you are responsible for the defense of a financial institution, you want to obtain threat intel from adversaries that are actively attacking this industry. It really doesn't help much if you start receiving alerts related to attacks that are happening in education institutions. Knowing the type of assets that you are trying to protect can also help to narrow down the threat actors that you should be more concerned about, and threat intelligence can give you that information.

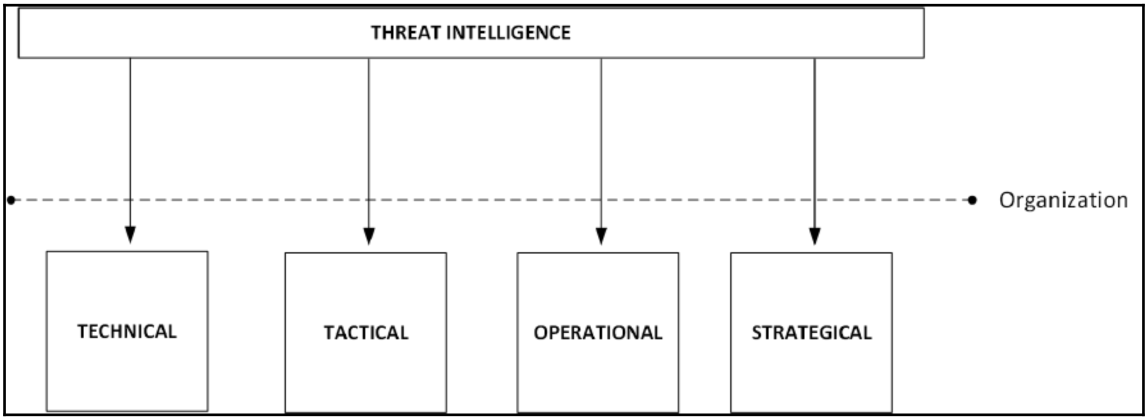
Let's use the WannaCry ransomware as an example. The outbreak happened on Friday, May 12, 2017. At the time, the only **indicator of compromise** (**IoCs**) available were the hashes and filenames of the ransomware sample. However, even before WannaCry existed, the EternalBlue exploit was already available, and as you know, WannaCry used the EternalBlue exploit. EternalBlue exploited Microsoft's implementation of the **Server Message Block** (**SMB**) protocol v1 (CVE-2017-0143). Microsoft released the patch for this vulnerability in March 14, 2017 (almost two months prior to the WannaCry outbreak). Are you following? Well, let's contextualize in the following diagram:


THREAT INTELLIGENCE
March 2017
May 2017
Threat Actors
Eternal Blue Exploit
Adversaries and Motivations
MS17-010 is released
Blue Team receives TI information about the dangerous of Eternal Blue, and the importance to patch
Blue Team
WannaCry Outbreak

Note that threat intelligence is receiving relevant information about this threat in the early stages, even when the EternalBlue exploit (originally discovered by the NSA) was leaked online (April 2017) by a hacker group calling itself **The Shadow Brokers** (**TSB**). The group was not a newbie, which means there was intel related to the work they had done in the past and their previous motivations. Take all this into consideration to predict what your adversary's next movement is going to be. By having this information, and knowing how EternalBlue works, now it is just a matter of waiting for the vendor (Microsoft, in this case) to send out a patch, which happened in March 2017. At this point, the Blue Team has enough information to determine the criticality of this patch to the business that they are trying to protect.

Many organizations didn't fully realize the impact of this issue, and instead of patching, they just disabled SMB access from the internet. While this was an acceptable workaround, it didn't fix the root cause of the issue. As a result, in June 2017 another ransomware outbreak happened—this time it was Petya. This ransomware used EternalBlue for lateral movement. In other words, once it compromised one machine inside the internal network (see, your firewall rule doesn't matter anymore), it was going to exploit other systems that were not patched with MS17-010. As you can see, there is a level of predictability here, since part of the Petya operation was implemented successfully after using an exploit similar to the one used by previous ransomware.

The conclusion to all this is simple: by knowing your adversaries, you can make better decisions to protect your assets. Having said that, it is also fair to say that you can't think of threat intelligence as an IT security tool—it goes beyond that. You have to think of threat intelligence as a tool to help make decisions regarding the organization's defense, help managers to decide how they should invest in security, and help CISOs to rationalize the situation with top executives. The information that you obtain from threat intelligence can be used in different areas, such as:



In summary, the correct use of threat intelligence is going to have a direct impact on the entire organization.

Open source tools for threat intelligence

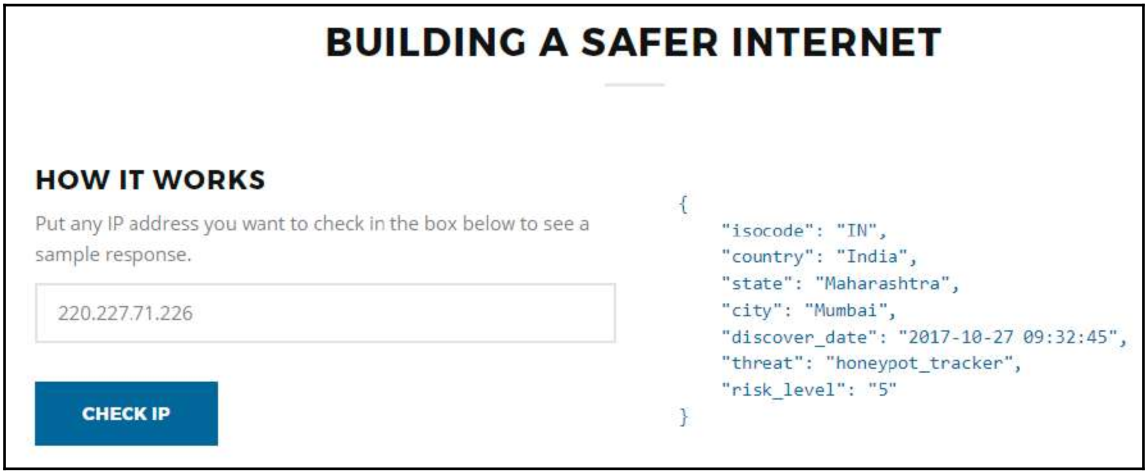
As mentioned earlier, DHS partners with the intelligence community to enhance its own intelligence, and this is pretty much standard in this field. Collaboration and information sharing are the foundations of the intelligence community. There are many open source threat intelligence tools out there that can be used. Some are commercial tools (paid) and some are free. You can start consuming threat intelligence by consuming TI feeds. OPSWAT Metadefender Cloud TI feeds have a variety of options that range from free to paid versions, and they can be delivered in four different formats: JSON, CSV, RSS, and Bro.

For more information about Metadefender Cloud TI feeds, visit: `https://www.metadefender.com/threat-intelligence-feeds`.

Another option for a quick verification is the website `https://fraudguard.io`. You can perform a quick IP validation to obtain threat intel from that location. In the example that follows, the IP 220.227.71.226 was used as a test, (the test result is relative to the day that it was done, which was 10/27/2017), and the result shows the following fields:

```
{
    "isocode": "IN",
    "country": "India",
    "state": "Maharashtra",
    "city": "Mumbai",
    "discover_date": "2017-10-27 09:32:45",
    "threat": "honeypot_tracker",
    "risk_level": "5"
}
```

The complete screenshot of the query is shown here:


BUILDING A SAFER INTERNET
HOW IT WORKS
Put any IP address you want to check in the box below to see a sample response.
220.227.71.226
CHECK IP

```
{
    "isocode": "IN",
    "country": "India",
    "state": "Maharashtra",
    "city": "Mumbai",
    "discover_date": "2017-10-27 09:32:45",
    "threat": "honeypot_tracker",
    "risk_level": "5"
}
```

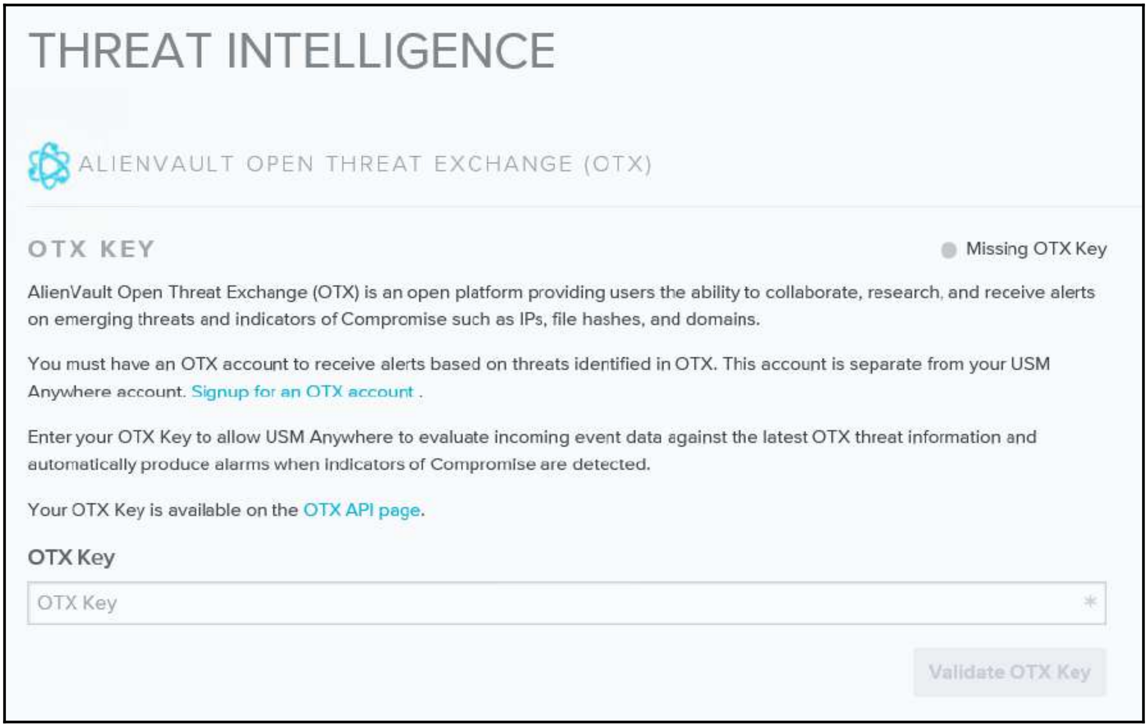
While this is just a simple example, there are more capabilities available that will depend on the level of the service that you are using. It also varies across the free and the paid versions. You also can integrate threat intelligence feeds into your Linux system by using the Critical Stack Intel Feed (`https://intel.criticalstack.com/`), which integrates with The Bro Network Security Monitor (`https://www.bro.org/`). Palo Alto Networks also has a free solution called MineMeld (`https://live.paloaltonetworks.com/t5/MineMeld/ct-p/MineMeld`) that can be used to retrieve threat intelligence.

Visit this GitHub location for a list of free tools, including free threat intel: `https://github.com/hslatman/awesome-threat-intelligence`.

In scenarios where the incident response team is unsure about whether a specific file is malicious or not, you can also submit it for analysis at `https://malwr.com`. They provide a decent amount of detail about IoC and samples that can be used to detect new threats.

As you can see, there are many free resources, but there are also open source initiatives that are paid, such as AlienVault USM Anywhere (`https://www.alienvault.com/products/usm-anywhere`). To be fair, this solution is way more than just a source of threat intelligence. It can perform vulnerability assessment, inspect the network traffic, and look for known threats, policy violations, and suspicious activities.

On the initial configuration of AlienVault USM Anywhere, you can configure the **threat intelligence exchange** (**OTX**). Note that you need an account for this, as well as a valid key, as shown here:



THREAT INTELLIGENCE

ALIENVAULT OPEN THREAT EXCHANGE (OTX)

OTX KEY

● Missing OTX Key

AlienVault Open Threat Exchange (OTX) is an open platform providing users the ability to collaborate, research, and receive alerts on emerging threats and indicators of Compromise such as IPs, file hashes, and domains.

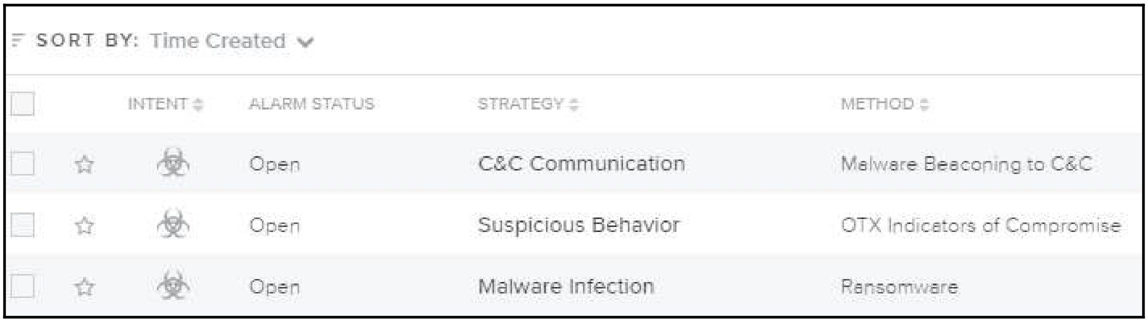
You must have an OTX account to receive alerts based on threats identified in OTX. This account is separate from your USM Anywhere account. Signup for an OTX account .

Enter your OTX Key to allow USM Anywhere to evaluate incoming event data against the latest OTX threat information and automatically produce alarms when indicators of Compromise are detected.

Your OTX Key is available on the OTX API page.

OTX Key

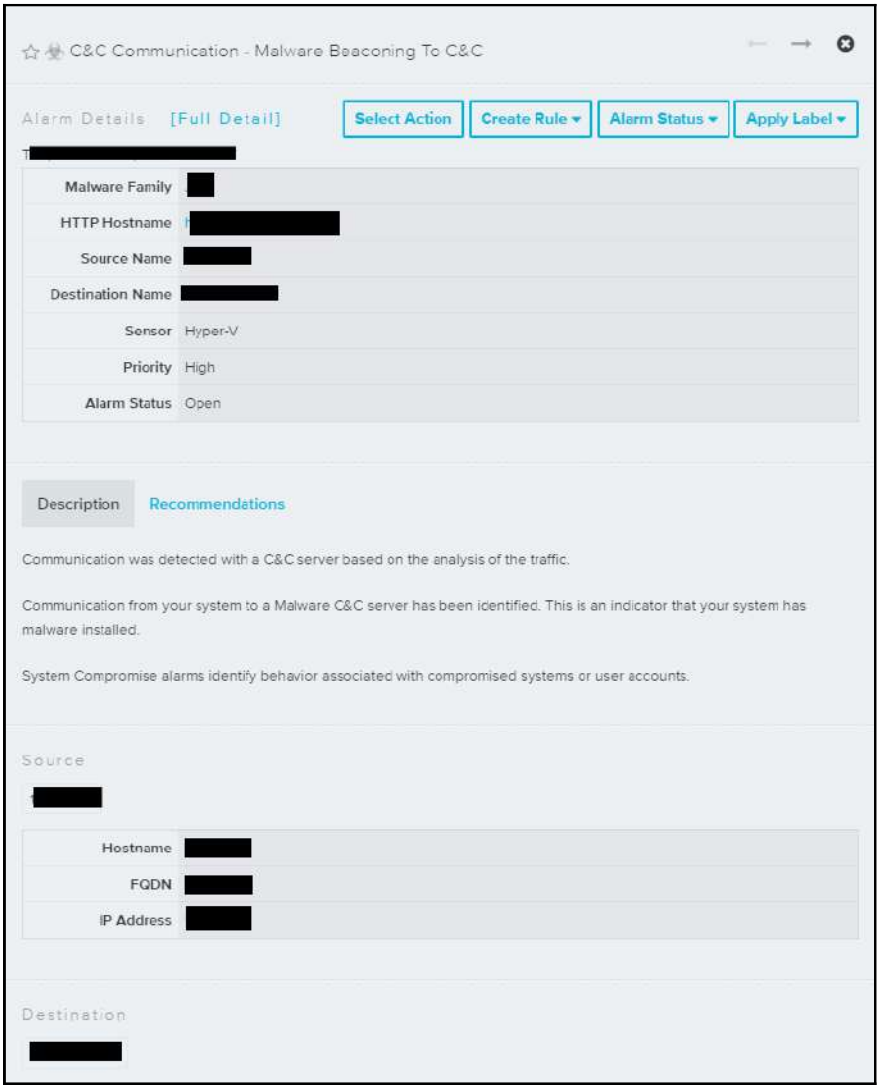
After you finish configuring, USM will continuously monitor your environment, and when something happens, it will trigger an alarm. You can see the alarm status, and most importantly, which strategy and method were used by this attack, as shown here:



SORT BY: Time Created

□		INTENT	ALARM STATUS	STRATEGY	METHOD
□	☆	☣	Open	C&C Communication	Malware Beaconing to C&C
□	☆	☣	Open	Suspicious Behavior	OTX Indicators of Compromise
□	☆	☣	Open	Malware Infection	Ransomware

You can dig into the alert and look for more details about the issue; that's when you will see more details about the threat intelligence that was used to raise this alarm. The image that follows has an example of this alarm; however, for privacy, the IP addresses are hidden:



Alarm Details [Full Detail]

[redacted]

Malware Family	[redacted]
HTTP Hostname	[redacted]
Source Name	[redacted]
Destination Name	[redacted]
Sensor	Hyper-V
Priority	High
Alarm Status	Open

Description Recommendations

Communication was detected with a C&C server based on the analysis of the traffic.

Communication from your system to a Malware C&C server has been identified. This is an indicator that your system has malware installed.

System Compromise alarms identify behavior associated with compromised systems or user accounts.

Source

[redacted]

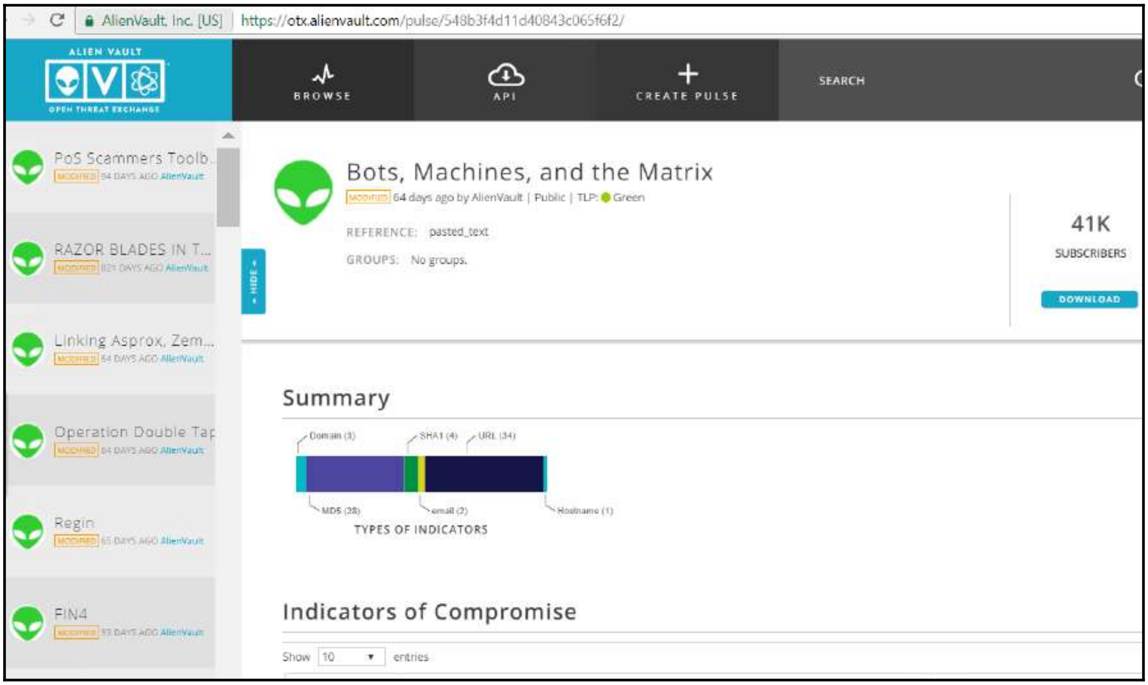
Hostname	[redacted]
FQDN	[redacted]
IP Address	[redacted]

Destination

[redacted]

From this list, you have some very important information—the source of the attack, the destination of the attack, the malware family, and a description, which gives you a lot of details about the attack. If you need to pass this information over to the incident response team to take action, you can also click on the **Recommendations** tab to see what should be done next. While this is a generic recommendation, you can always use it to improve your own response.

At any moment, you can also access OTX Pulse from `https://otx.alienvault.com/pulse`, and there you have TI information from the latest threats, as shown in the following example:



AlienVault, Inc. [US] https://otx.alienvault.com/pulse/548b3f4d11d40843c065f6f2/

PoS Scammers Toolb... MODIFIED 94 DAYS AGO AlienVault

RAZOR BLADES IN T... MODIFIED 821 DAYS AGO AlienVault

Linking Asprox, Zem... MODIFIED 64 DAYS AGO AlienVault

Operation Double Tap MODIFIED 84 DAYS AGO AlienVault

Regin MODIFIED 65 DAYS AGO AlienVault

FIN4 MODIFIED 93 DAYS AGO AlienVault

Bots, Machines, and the Matrix

MODIFIED 64 days ago by AlienVault | Public | TLP: ● Green

REFERENCE: pasted_text

GROUPS: No groups.

41K SUBSCRIBERS

Summary

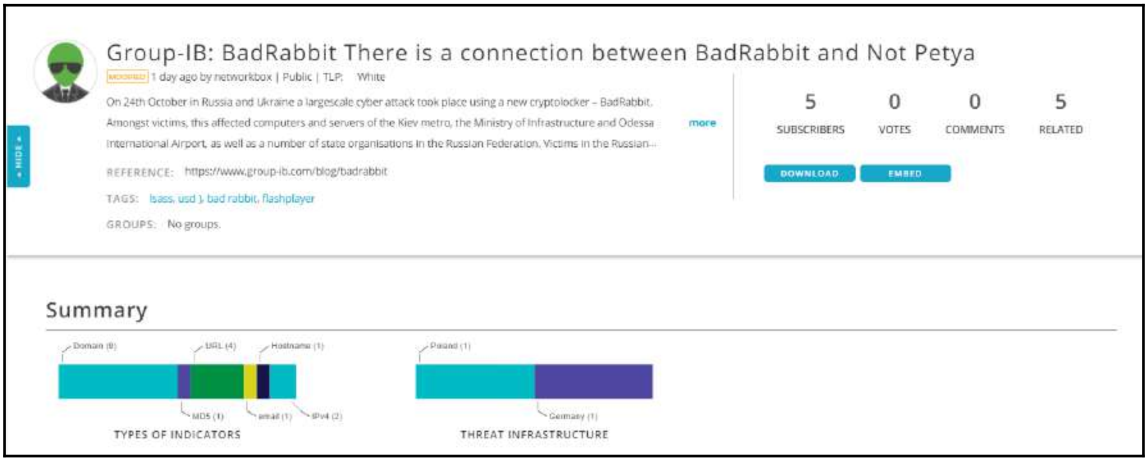
TYPES OF INDICATORS

Indicators of Compromise

Show 10 ▾ entries

This dashboard gives you a good amount of threat intel information, and while the preceding example shows entries from AlienVault, the community also contributes. At the time of writing, we had the BadRabbit outbreak, and I tried to use the search capability on this dashboard to look for more information about BadRabbit, and I got a lot of hits.

Here is one example of some important data that can be useful to enhance your defense system:



Group-IB: BadRabbit There is a connection between BadRabbit and Not Petya

MODIFIED 1 day ago by networkbox | Public | TLP: White

On 24th October in Russia and Ukraine a largescale cyber attack took place using a new cryptolocker – BadRabbit. Amongst victims, this affected computers and servers of the Kiev metro, the Ministry of Infrastructure and Odessa International Airport, as well as a number of state organisations in the Russian Federation. Victims in the Russian... more

REFERENCE: https://www.group-ib.com/blog/badrabbit

TAGS: lsass, usd), bad rabbit, flashplayer

GROUPS: No groups.

5	0	0	5
SUBSCRIBERS	VOTES	COMMENTS	RELATED

DOWNLOAD EMBED

Summary

Microsoft threat intelligence

For organizations that are using Microsoft products, whether on-premises or in the cloud, they threat intelligence as part of the product itself. That's because nowadays many Microsoft products and services take advantage of shared threat intelligence, and with this, they can offer context, relevance, and priority management to help people take action. Microsoft consumes threat intelligence through different channels, such as:

- The Microsoft Threat Intelligence Center, which aggregates data from:
    - Honeypots, malicious IP addresses, botnets, and malware detonation feeds
    - Third-party sources (threat intelligence feeds)
    - Human-based observation and intelligence collection
- Intelligence coming from consumption of their service
- Intelligence feeds generated by Microsoft and third parties

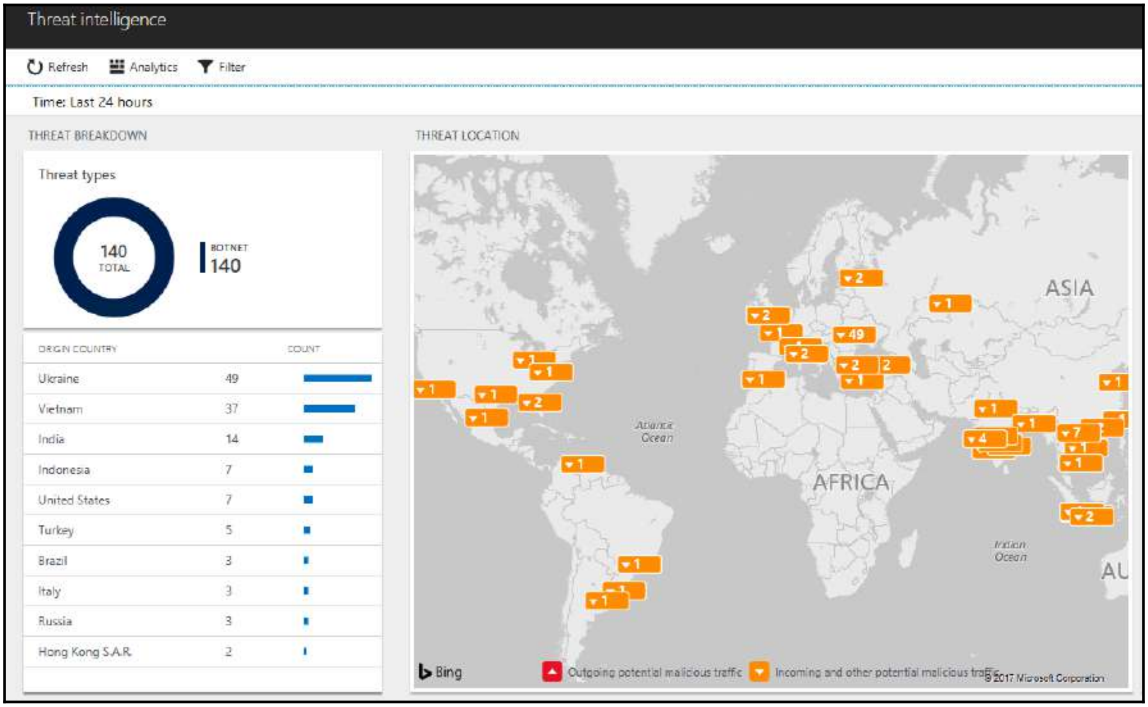
Microsoft integrates the result of this threat intelligence into its products, such as Windows Defender Advanced Threat Protection, Azure Security Center, Office 365 Threat Intelligence, Cloud App Security, and others.

Visit `https://aka.ms/MSTI` for more information about how Microsoft uses threat intelligence to protect, detect, and respond to threat.

Azure Security Center

In the last chapter, we used Security Center to identify suspicious activities based on behavior analytics. While that was a great capability for cloud-based VMs and on-premises servers, you can also leverage threat intelligence to better understand whether your environment was, or still is, compromised. In the Security Center dashboard, there is an option in the left-hand navigation menu called **Threat intelligence**. When you click on it, you have to select the workspace that contains your data, and after making this selection you will be able to see the TI dashboard.

For the purpose of this example, the TI dashboard that you see is a demo environment that is fully compromised, and that's the reason why there are so many alerts:



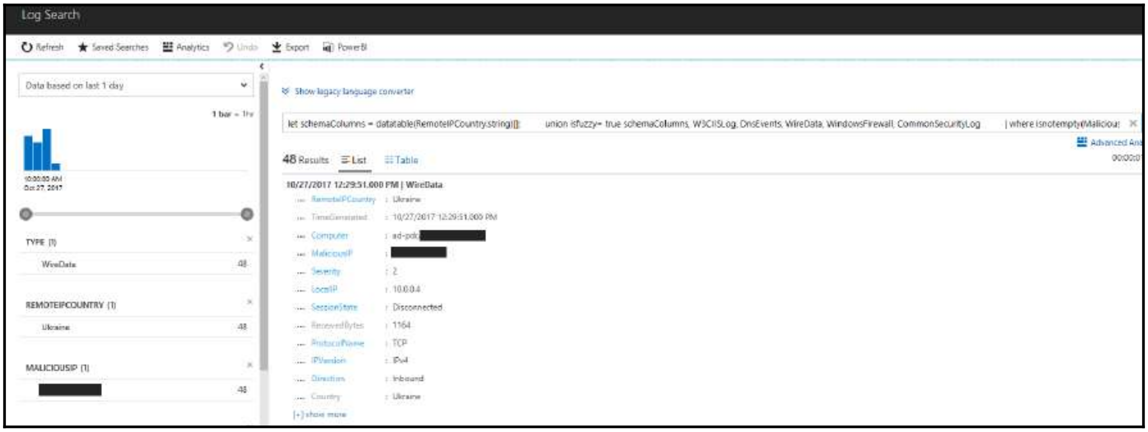
Time: Last 24 hours

ORIGIN COUNTRY	COUNT
Ukraine	49
Vietnam	37
India	14
Indonesia	7
United States	7
Turkey	5
Brazil	3
Italy	3
Russia	3
Hong Kong S.A.R.	2

In this dashboard, you have a summary of the types of threats. In this case, all of them are botnets. You also have the origin country (where the threat is coming from), and a map that shows the geolocation of the threats. The cool thing about this dashboard is that you can keep digging into the data—in other words, if you click on one of the countries, it will open a search result showing all systems that were compromised for this threat coming from this country. In this case, the image that follows is the result of a search for all compromised systems. Where the attacker is coming from Ukraine, the raw search is:

```
let schemaColumns = datatable(RemoteIPCountry:string)[];
union isfuzzy= true schemaColumns, W3CIISLog, DnsEvents, WireData,
WindowsFirewall, CommonSecurityLog          | where
isnotempty(MaliciousIP) and (isnotempty(MaliciousIPCountry) or
isnotempty(RemoteIPCountry))| extend Country =
iff(isnotempty(MaliciousIPCountry), MaliciousIPCountry,
iff(isnotempty(RemoteIPCountry), RemoteIPCountry, ''))
| where Country == "Ukraine"
```

The result is as follows:



TYPE (1)
WireData 48

REMOTEIPCOUNTRY (1)
Ukraine 48

MALICIOUSIP (1)
[redacted] 48

```
let schemaColumns = datatable(RemoteIPCountry:string)[];     union isfuzzy= true schemaColumns, W3CIISLog, DnsEvents, WireData, WindowsFirewall, CommonSecurityLog     | where isnotempty(Maliciou
```

```
10/27/2017 12:29:51.000 PM | WireData
  RemoteIPCountry : Ukraine
  TimeGenerated   : 10/27/2017 12:29:51.000 PM
  Computer        : ad-pdc[redacted]
  MaliciousIP     : [redacted]
  Severity        : 2
  LocalIP         : 10.0.0.4
  SessionState    : Disconnected
  ReceivedBytes   : 1164
  ProtocolName    : TCP
  IPVersion       : IPv4
  Direction       : Inbound
  Country         : Ukraine
[+] show more
```

The initial data that you receive has some interesting information, including the local IP address of the system that was compromised, the protocol that was used, the direction, and the malicious IP. However, the best part appears when you click **show more**.

There, you will see which file was compromised and which application was used:

```
...IndicatorThreatType:Botnet
...Confidence:75
...FirstReportedDateTime:2017-10-27T11:40:44.0000000Z
...LastReportedDateTime:2017-10-27T16:27:01.2410977Z
...IsActive:true
...RemoteIPLongitude:27.82
...RemoteIPLatitude:48.44
...SessionStartTime:10/27/2017 12:29:30.000 PM
...SessionEndTime:10/27/2017 12:29:45.000 PM
...LocalSubnet:10.0.0.0/24
...LocalPortNumber:3389
...RemotePortNumber:0
...SentBytes:1591
...TotalBytes:2755
...ApplicationProtocol:RDP
...ProcessID:3052
...ProcessName:C:WindowsSystem32svchost.exe
```

In this case, the `svchost.exe` process seems to be the process that was compromised by the attacker. What you need to do at this point is go to the target system and start an investigation.

Leveraging threat intelligence to investigate suspicious activity

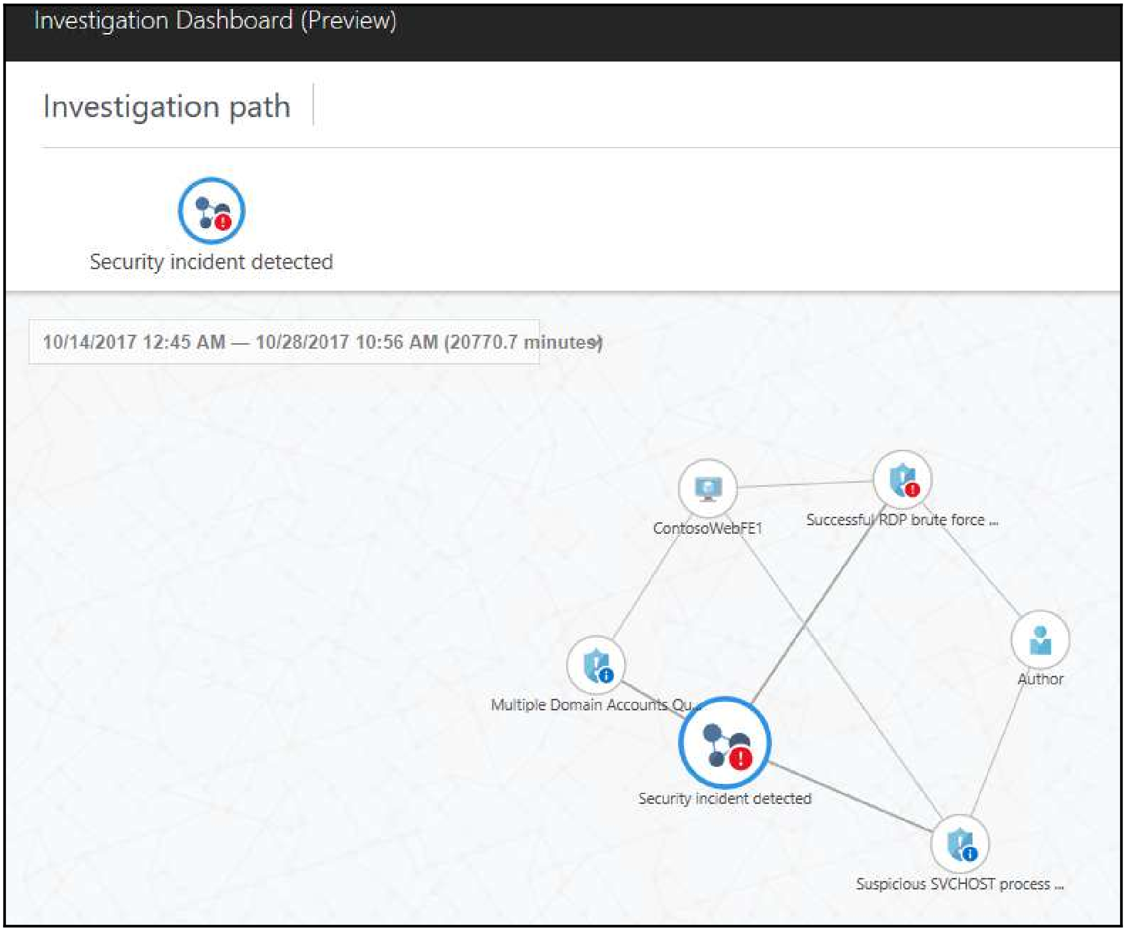
At this point, there is no more doubt that the use of threat intelligence to help your detection system is imperative. Now, how do you take advantage of this information when responding to a security incident? While the Blue Team works primarily on the defense system, they do collaborate with the incident response team by providing the right data that can lead them to find the root cause of the issue. If we use the previous example from Security Center, we could just hand it that search result and it would be good enough. But knowing the system that was compromised is not the only goal of an incident response.

At the end of the investigation, you must answer at least the following questions:

- Which systems were compromised?
- Where did the attack start?
- Which user account was used to start the attack?
- Did it move laterally?
    - If it did, what were the systems involved in this movement?
- Did it escalate privilege?
    - If it did, which privilege account was compromised?
- Did it try to communicate with command and control?
- If it did, was it successful?
    - If it was, did it download anything from there?
    - If it was, did it send anything to there?
- Did it try to clear evidence?
    - If it did, was it successful?

These are some keys questions that you must answer at the end of the investigation, and this can help you to truly bring a close to the case, and be confident that the threat was completely contained and removed from the environment.

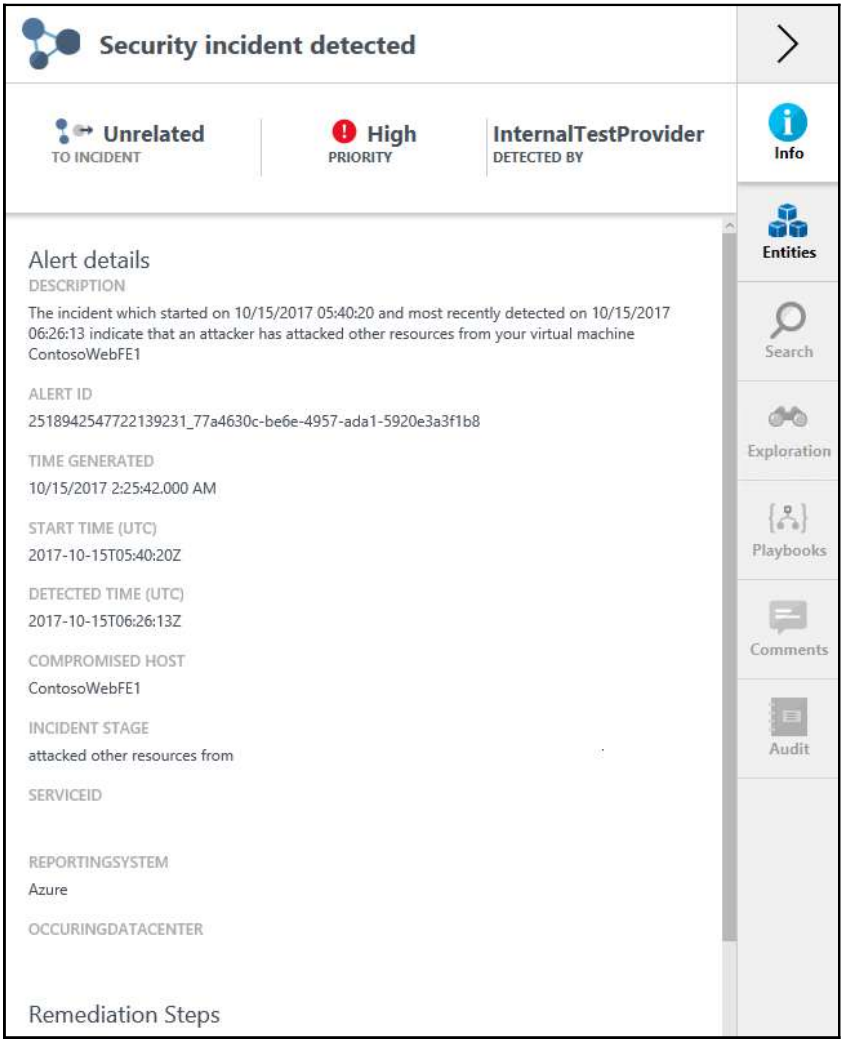
You can use the Security Center investigation feature to answer most of these questions. This feature enables investigators to see the attack path, the user accounts involved, the systems that were compromised, and the malicious activities that were done. In the previous chapter, you learned about the Security Incident feature in Security Center, which aggregates alerts that are part of the same attack campaign. From that interface, you can click **Start Investigation** to access the Investigation dashboard, as shown here:


Investigation Dashboard (Preview)
Investigation path
Security incident detected
10/14/2017 12:45 AM — 10/28/2017 10:56 AM (20770.7 minutes)
ContosoWebFE1
Successful RDP brute force ...
Author
Multiple Domain Accounts Qu...
Security incident detected
Suspicious SVCHOST process ...

The investigation map contains all entities (alerts, computers, and users) that are correlated with this incident. When you first open the dashboard, the focus of the map is the security incident itself; however, you can click on any entity and the map will expand with the information that is correlated with the object that you just selected. The second part of the dashboard has more details about the selected entity, which include:

- Detection timeline
- Compromised host
- Detailed description of the event
- Remediation steps
- Incident stage

In the following example, the security incident was selected on the investigation map, and this is the information available for this entity:



Security incident detected

Unrelated
TO INCIDENT

High
PRIORITY

InternalTestProvider
DETECTED BY

Alert details

DESCRIPTION
The incident which started on 10/15/2017 05:40:20 and most recently detected on 10/15/2017 06:26:13 indicate that an attacker has attacked other resources from your virtual machine ContosoWebFE1

ALERT ID
2518942547722139231_77a4630c-be6e-4957-ada1-5920e3a3f1b8

TIME GENERATED
10/15/2017 2:25:42.000 AM

START TIME (UTC)
2017-10-15T05:40:20Z

DETECTED TIME (UTC)
2017-10-15T06:26:13Z

COMPROMISED HOST
ContosoWebFE1

INCIDENT STAGE
attacked other resources from

SERVICEID

REPORTINGSYSTEM
Azure

OCCURINGDATACENTER

Remediation Steps

The content of this pane will vary according to the entity selection on the left (the investigation map). Note that for the incident itself, there are some options that are grayed out, which means that these options are not available for this particular entity, which is expected.

> Watch one of the authors of this book, Yuri Diogenes, demonstrating how this feature works at Ignite 2017 in Orlando at `https://blogs.technet.microsoft.com/yuridiogenes/2017/09/30/ignite-2017-azure-security-center-domination/`.

References

1. *Microsoft Lean on the Machine Report* `http://download.microsoft.com/download/3/4/0/3409C40C-2E1C-4A55-BD5B-51F5E1164E20/Microsoft_Lean_on_the_Machine_EN_US.pdf`
2. *Wanna Decryptor (WNCRY) Ransomware Explained* `https://blog.rapid7.com/2017/05/12/wanna-decryptor-wncry-ransomware-explained/`
3. *A Technical Analysis of WannaCry Ransomware* `https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/`
4. *New ransomware, old techniques: Petya adds worm capabilities* `https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/`
5. *DUQU Uses STUXNET-Like Techniques to Conduct Information Theft* `https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/90/duqu-uses-stuxnetlike-techniques-to-conduct-information-theft`
6. *Open Source Threat Intelligence* `https://www.sans.org/summit-archives/file/summit-archive-1493741141.pdf`

Summary

In this chapter, you learned about the importance of threat intelligence and how it can be used to gain more information about current threat actors and their techniques, and, in some circumstances, predict their next step. You learned how to leverage threat intelligence from the open source community, based on some free tools, as well as commercial tools. Next, you learned how Microsoft integrates threat intelligence as part of its products and services, and how to use Security Center not only to consume threat intelligence, but also to visualize potentially compromised features of your environment based on the threat intel acquired, compared to your own data. Lastly, you learned about the investigation feature in Security Center and how this feature can be used by the incident response team to find the root cause of a security issue.

In the next chapter, we will continue talking about defense strategies, but this time we will focus on response, which is a continuation of what we started in this chapter. You will learn more about the investigation, both on-premises and in the cloud.

13
Investigating an Incident

In the previous chapter, you learned about the importance of using threat intelligence to help the Blue Team enhance the organization's defense and also to know their adversaries better. In this chapter, you will learn how to put all these tools together to perform an investigation. Beyond the tools, you will also learn how to approach an incident, ask the right questions, and narrow down the scope. To illustrate that, there will be two scenarios, where one is in an on-premises organization and the other one is in a hybrid environment. Each scenario will have its unique characteristics and challenges.

In this chapter, we are going over the following topics:

- Scoping the issue
- On-premises compromised system
- Cloud-based compromised system
- Conclusion and lessons learned

Scoping the issue

Let's face it, not every incident is a security-related incident and, for this reason, it is vital to scope the issue prior to start an investigation. Sometimes, the symptoms may lead you to initially think that you are dealing with a security-related problem, but as you ask more questions and collect more data, you may realize that the problem was not really related to security.

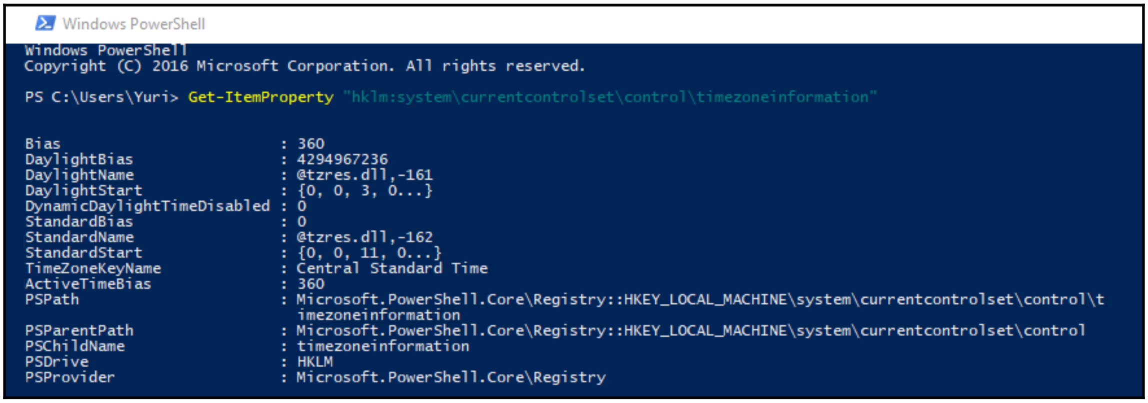
For this reason, the initial triage of the case has an important role on how the investigation will succeed. If you have no real evidence that you are dealing with a security issue other than the end user opening an incident saying that his computer is running slow and he *thinks* it is compromised, than you should start with basic performance troubleshooting, rather than dispatching a security responder to initiate an investigation. For this reason, IT, operations, and security must be fully aligned to avoid false positive dispatches, which results in utilizing a security resource to perform a support-based task.

During this initial triage, it is also important to determine the frequency of the issue. If the issue is not currently happening, you may need to configure the environment to collect data when the user is able to reproduce the problem. Make sure to document all the steps and provide an accurate action plan for the end user. The success of this investigation will depend on the quality of the data that was collected.

Key artifacts

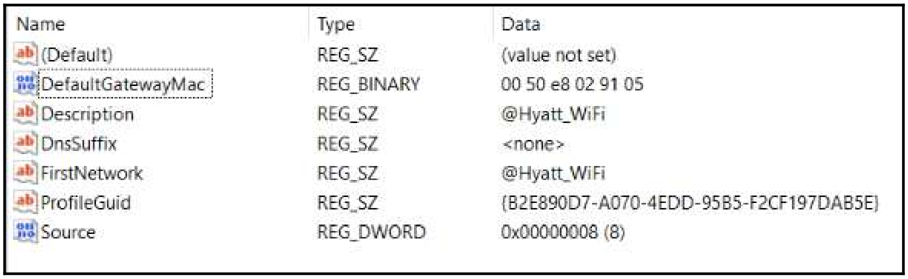
Nowadays, there is so much data available that data collection should focus on obtaining just the vital and relevant artifacts from the target system. More data doesn't necessarily mean better investigation, mainly because you still need to perform data correlation in some cases and too much data can deviate you from the root cause of the problem.

When dealing with an investigation for a global organization that has devices spread out across different regions of the planet, it is important to make sure you know the time zone of the system that you are investigating. In a Windows system, this information is located in the registry key at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`. You could use the PowerShell command `Get-ItemProperty` to retrieve this information from the system, as follows:



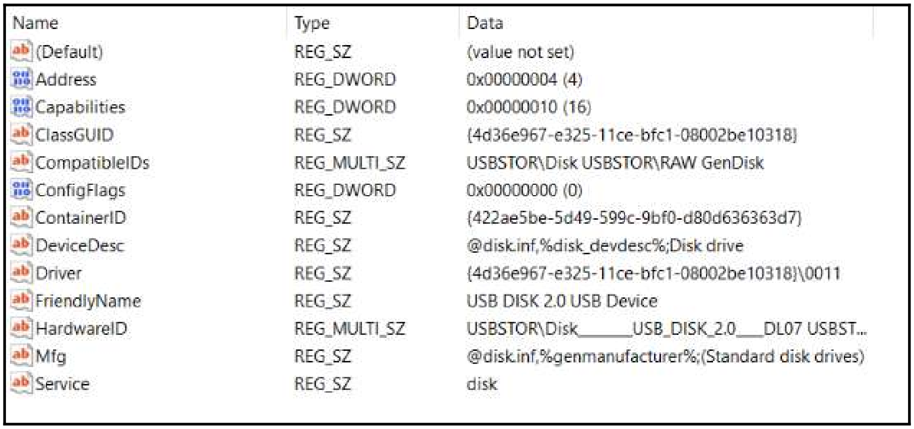
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Yuri> Get-ItemProperty "hklm:system\currentcontrolset\control\timezoneinformation"


Bias                         : 360
DaylightBias                 : 4294967236
DaylightName                 : @tzres.dll,-161
DaylightStart                : {0, 0, 3, 0...}
DynamicDaylightTimeDisabled : 0
StandardBias                 : 0
StandardName                 : @tzres.dll,-162
StandardStart                : {0, 0, 11, 0...}
TimeZoneKeyName              : Central Standard Time
ActiveTimeBias               : 360
PSPath                       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\system\currentcontrolset\control\t
                               imezoneinformation
PSParentPath                 : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\system\currentcontrolset\control
PSChildName                  : timezoneinformation
PSDrive                      : HKLM
PSProvider                   : Microsoft.PowerShell.Core\Registry
```

Notice the value TimeZoneKeyName, which is set to Central Standard Time. This data will be relevant when you start analyzing the logs and performing data correlation. Another important registry key to obtain network information is HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged and Managed. These keys will show the networks that this computer has been connected to. Here is a result of the unmanaged key:



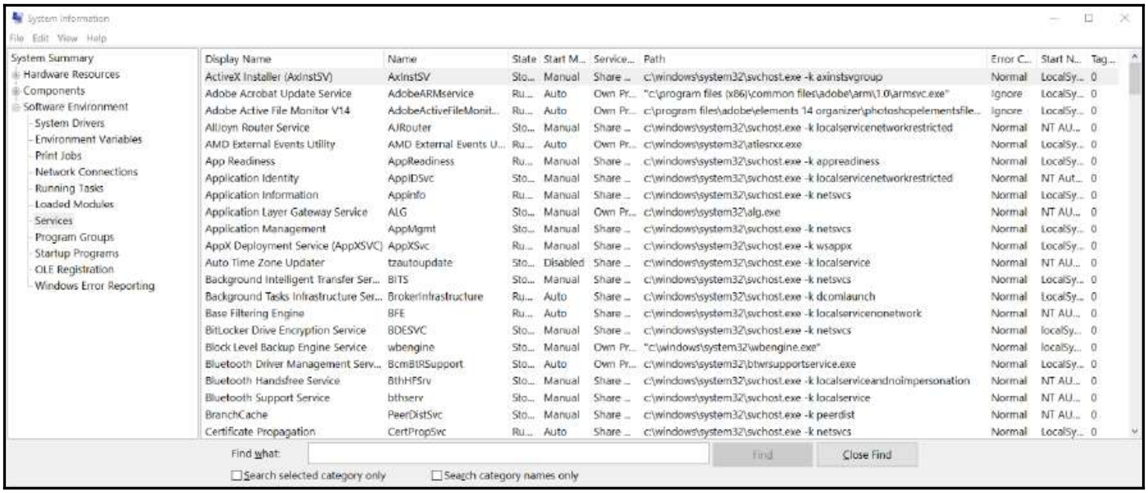
Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	00 50 e8 02 91 05
Description	REG_SZ	@Hyatt_WiFi
DnsSuffix	REG_SZ	<none>
FirstNetwork	REG_SZ	@Hyatt_WiFi
ProfileGuid	REG_SZ	{B2E890D7-A070-4EDD-95B5-F2CF197DAB5E}
Source	REG_DWORD	0x00000008 (8)

These two artifacts are important for determining the location (time zone) of the machine and the networks that this machine visited. This is even more important for devices that are used by employees to work outside the office, such as laptops and tablets. Depending on the issue that you are investigating, it is also important to verify the USB usage on this machine. To do that, export the registry keys HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR and HKLM\SYSTEM\CurrentControlSet\Enum\USB. An example of what this key looks like is shown in the following image:



Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000004 (4)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{422ae5be-5d49-599c-9bf0-d80d636363d7}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0011
FriendlyName	REG_SZ	USB DISK 2.0 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\Disk\_______USB_DISK_2.0___DL07 USBST...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

To determine if there is any malicious software configured to start when Windows starts, review the registry key, `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`. Usually, when the malicious program appears in there, it will also create a service; therefore, it is also important to review the registry key, `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Look for random name services and entries that are not part of the computer's profile pattern. Another way to obtain these services is to run the `msinfo32` utility:



Display Name	Name	State	Start M...	Service...	Path	Error C...	Start N...	Tag...
ActiveX Installer (AxInstSV)	AxInstSV	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k axinstsvgroup	Normal	LocalSy...	0
Adobe Acrobat Update Service	AdobeARMservice	Ru...	Auto	Own Pr...	"c:\program files (x86)\common files\adobe\arm\1.0\armsvc.exe"	Ignore	LocalSy...	0
Adobe Active File Monitor V14	AdobeActiveFileMonit...	Ru...	Auto	Own Pr...	c:\program files\adobe\elements 14 organizer\photoshopelementsfile...	Ignore	LocalSy...	0
AllJoyn Router Service	AJRouter	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k localservicenetworkrestricted	Normal	NT AU...	0
AMD External Events Utility	AMD External Events U...	Ru...	Auto	Own Pr...	c:\windows\system32\atiesrxx.exe	Normal	LocalSy...	0
App Readiness	AppReadiness	Ru...	Manual	Share ...	c:\windows\system32\svchost.exe -k appreadiness	Normal	LocalSy...	0
Application Identity	AppIDSvc	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k localservicenetworkrestricted	Normal	NT Aut...	0
Application Information	Appinfo	Ru...	Manual	Share ...	c:\windows\system32\svchost.exe -k netsvcs	Normal	LocalSy...	0
Application Layer Gateway Service	ALG	Sto...	Manual	Own Pr...	c:\windows\system32\alg.exe	Normal	NT AU...	0
Application Management	AppMgmt	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k netsvcs	Normal	LocalSy...	0
AppX Deployment Service (AppXSVC)	AppXSvc	Ru...	Manual	Share ...	c:\windows\system32\svchost.exe -k wsappx	Normal	LocalSy...	0
Auto Time Zone Updater	tzautoupdate	Sto...	Disabled	Share ...	c:\windows\system32\svchost.exe -k localservice	Normal	NT AU...	0
Background Intelligent Transfer Ser...	BITS	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k netsvcs	Normal	LocalSy...	0
Background Tasks Infrastructure Ser...	BrokerInfrastructure	Ru...	Auto	Share ...	c:\windows\system32\svchost.exe -k dcomlaunch	Normal	LocalSy...	0
Base Filtering Engine	BFE	Ru...	Auto	Share ...	c:\windows\system32\svchost.exe -k localservicenonetwork	Normal	NT AU...	0
BitLocker Drive Encryption Service	BDESVC	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k netsvcs	Normal	localSy...	0
Block Level Backup Engine Service	wbengine	Sto...	Manual	Own Pr...	"c:\windows\system32\wbengine.exe"	Normal	localSy...	0
Bluetooth Driver Management Serv...	BcmBtRSupport	Sto...	Auto	Own Pr...	c:\windows\system32\btwrsupportservice.exe	Normal	LocalSy...	0
Bluetooth Handsfree Service	BthHFSrv	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k localserviceandnoimpersonation	Normal	NT AU...	0
Bluetooth Support Service	bthserv	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k localservice	Normal	NT AU...	0
BranchCache	PeerDistSvc	Sto...	Manual	Share ...	c:\windows\system32\svchost.exe -k peerdist	Normal	NT AU...	0
Certificate Propagation	CertPropSvc	Ru...	Auto	Share ...	c:\windows\system32\svchost.exe -k netsvcs	Normal	LocalSy...	0

In addition to that, make sure to also capture all security events and, when analyzing them focus on the following ones:

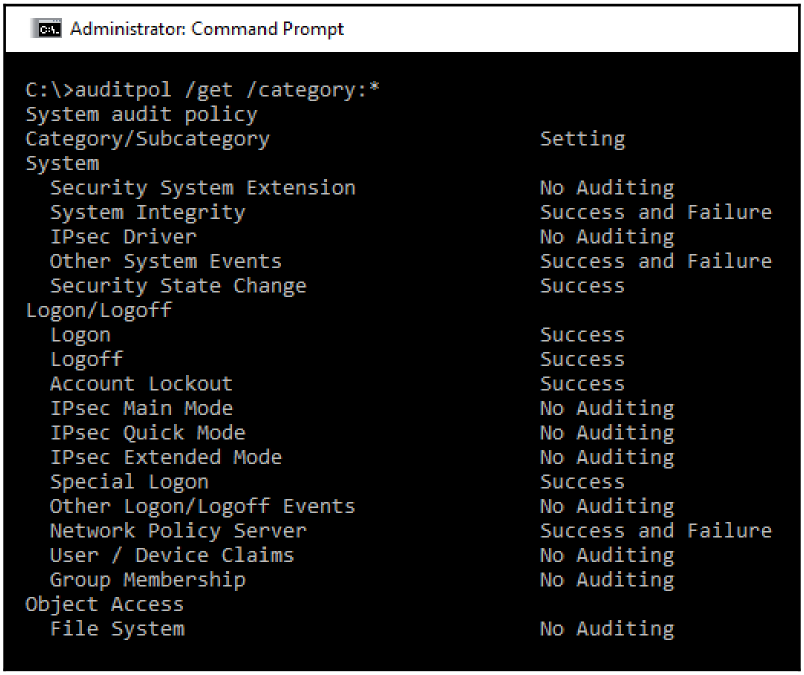
Event ID	**Description**	**Security scenario**
1102	The audit log was cleared	As attackers infiltrate your environment, they might want to clear their evidence and cleaning the event log is an indication of that. Make sure to review who cleaned the log, if this operation was intentional and authorized, or if it was unintentional or unknown (due to a compromised account).
4624	An account was successfully logged on	It is very common to log only the failures, but in many cases knowing who successfully logged in is important for understanding who performed which action.

4625	An account failed to log on	Multiple attempts to access an account can be a sign of a brute force account attack. Reviewing this log can give you some indications of that.
4657	A registry value was modified	Not everyone should be able to change the registry key and, even when you have high privileges to perform this operation, is still an operation that needs further investigation to understand the veracity of this change.
4663	An attempt was made to access an object	While this event might generate a lot of false positives, it is still relevant to collect and look at it on demand. In other words, if you have other evidences that point to unauthorized access to the filesystem, you may use this log to drill down who performed this change.
4688	A new process has been created	When Petya ransomware outbreak happened, one of the indicators of compromise was the `cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "C:Windowssystem32shutdown.exe /r /f" /ST <time>`. When the `cmd.exe` command was executed, a new process was created and an event 4688 was also created. Obtaining the details about this event is extremely important when investigating a security-related issue.
4700	A scheduled task was enabled	The use of scheduled tasks to perform an action has been used over the years by attackers. Using the same example as shown above (Petya), the event 4700 can give you more details about a scheduled task.
4702	A scheduled task was updated	If you see 4700 from a user who doesn't usually perform this type of operation and you keep seeing 4702 to update this task, you should investigate further. Keep in mind that it could be a false positive, but it all depends on who made this change and the user's profile of doing this type of operation.
4719	System audit policy was changed	Just like the first event of this list, in some scenarios, attackers that already compromised an administrative level account may need to perform changes in the system policy to continue their infiltration and lateral movement. Make sure to review this event and follow up on the veracity of the changes that were done.

4720	A user account was created	In an organization, only certain users should have the privilege to create an account. If you see an ordinary user creating an account, the chances are that his credential was compromised and the attacker already escalated privilege to perform this operation.
4722	A user account was enabled	As part of the attack campaign, an attacker may need to enable an account that was previously disabled. Make sure to review the legitimacy of this operation in case you see this event.
4724	An attempt was made to reset an accounts password	Another common action during the system's infiltration, and lateral movement. If you find this event, make sure to review the legitimacy of this operation.
4727	A security-enabled global group was created	Again, only certain users should have the privilege to create a security-enabled group. If you see an ordinary user creating a new group, the chances are that his credential was compromised, and the attacker already escalated privilege to perform this operation. If you find this event, make sure to review the legitimacy of this operation.
4732	A member was added to a security-enabled local group	There are many ways to escalate privilege and, sometimes, one shortcut is to add itself as member of a higher privileged group. Attackers may use this technique to gain privilege access to resources. If you find this event, make sure to review the legitimacy of this operation.
4739	Domain policy was changed	In many cases, the main objective of an attacker's mission is domain dominance and this event could reveal that. If an unauthorized user is making domain policy changes, it means the level of compromise arrived in the domain level hierarchy. If you find this event, make sure to review the legitimacy of this operation.
4740	A user account was locked out	When multiple attempts to log on are performed, one will hit the account lockout threshold, and the account will be locked out. This could be a legitimate log on attempt or it could be an indication of a brute force attack. Make sure to take these facts into consideration when reviewing this event.

4825	A user was denied the access to remote desktop. By default, users are allowed to connect only if they are members of the remote desktop users group or administrators group	This is a very important event, mainly if you have computers with RDP port open to the internet, such as VMs located in the cloud. This could be legitimate, but it could also indicate an unauthorized attempt to gain access to a computer via RDP connection.
4946	A change has been made to Windows Firewall exception list. A rule was added.	When a machine is compromised, and a piece of malware is dropped in the system, it is common that, upon execution, this malware tries to establish access to command and control. Some attackers will try to change the Windows Firewall exception list to allow this communication to take place.
4948	A change has been made to Windows Firewall exception list. A rule was deleted.	This is a similar scenario to the one described above; the difference is that, in this case, the attacker decided to delete a rule, instead of creating a new one. This also could be an attempt to cover his previous action. For example, he could create the rule to allow external communication and, once this operation was finished, delete the rule to clear evidence of compromise.

It is important to mention that some of these events will only appear if the security policy in the local computer is correctly configured. For example, the event 4663 will not appear in the system below because auditing is not enabled for `Object Access`:

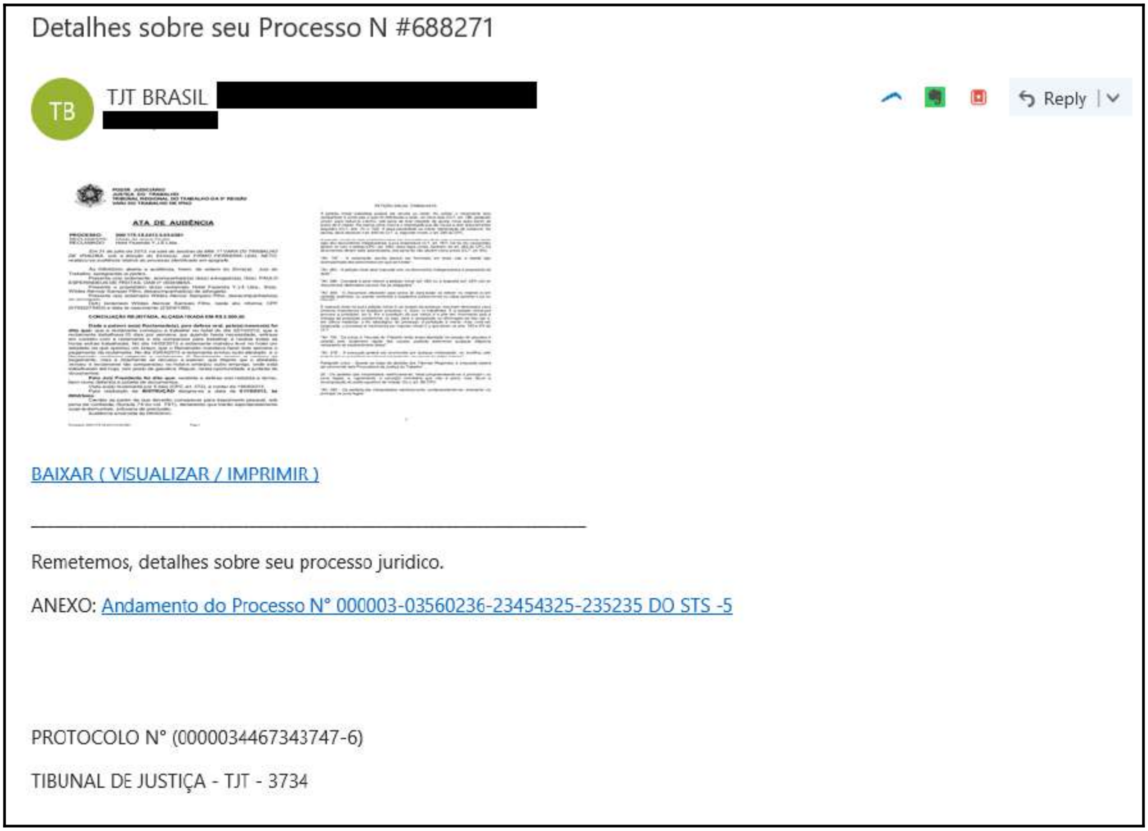


```
C:\>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
```

In addition to that, also make sure to collect network traces using Wireshark when dealing with live investigation and, if necessary, use `procdump` tool from Sysinternals, to create a dump of the compromised process.

Investigating a compromised system on-premises

For the first scenario, we will use a machine that got compromised after the end user opened a phishing email that looks like following:



Detalhes sobre seu Processo N #688271

TJT BRASIL [redacted]
[redacted]

BAIXAR (VISUALIZAR / IMPRIMIR)

Remetemos, detalhes sobre seu processo juridico.

ANEXO: Andamento do Processo N° 000003-03560236-23454325-235235 DO STS -5

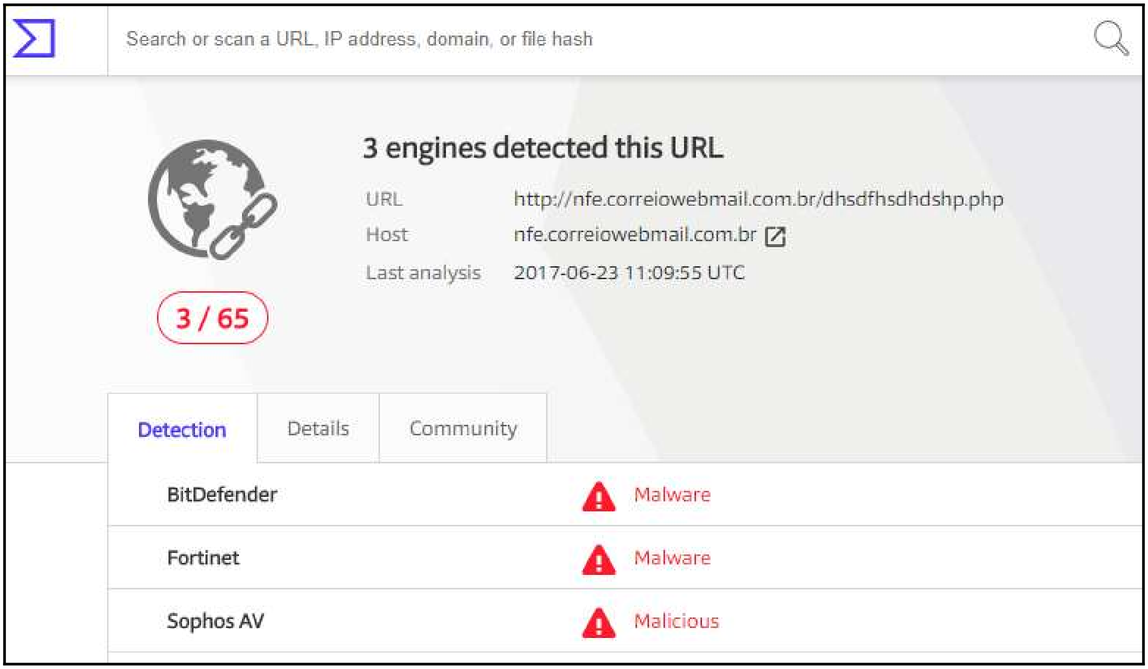
PROTOCOLO N° (0000034467343747-6)

TIBUNAL DE JUSTIÇA - TJT - 3734

This end user was located in the Brazilian branch office, hence the email in Portuguese. The content of this email is a bit concerning, since it talks about an ongoing law process, and the user was curious to see if he really had anything to do with it. After poking around within the email, he noticed that nothing apparently happened. He ignored and continued working. A couple of days later, he receiving an automated report from IT saying that he accessed a suspicious site and he should call support to follow up on this ticket.

He called support and explained that the only suspicious activity that he remembers was to open an odd email, he than presented this email as evidence. When questioned about what he did, he explained that he clicked the image that was apparently attached in the email thinking that he could download it, but nothing came in, only a glimpse of an opening window that quickly disappeared and nothing more.

The first step of the investigation was to validate the URL that was linked to the image in the email. The quickest way to validate is by using VirusTotal, which in this case returned the following value (test performed on November 15, 2017):



3 engines detected this URL

URL http://nfe.correiowebmail.com.br/dhsdfhsdhdshp.php

Host nfe.correiowebmail.com.br

Last analysis 2017-06-23 11:09:55 UTC

3 / 65

BitDefender ⚠ Malware

Fortinet ⚠ Malware

Sophos AV ⚠ Malicious

This was already a strong indication that this site was malicious, the question at that point was: what did it download onto the user's system that the antimalware installed in the local box didn't find? When there is no indication of compromise from the antimalware and there are indications that a malicious file was successfully downloaded in the system, reviewing the event logs is usually the next step.

Using Windows Event Viewer, we filtered the security event for event ID 4688 and started looking into each single event until the following one was found:

```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Event ID:      4688
Task Category: Process Creation
Level:         Information
Keywords:      Audit Success
User:          N/A
Computer:      BRANCHBR
Description:
```

```
A new process has been created.

Creator Subject:
   Security ID:            BRANCHBRJose
   Account Name:           Jose
   Account Domain:         BRANCHBR
   Logon ID:         0x3D3214

Target Subject:
   Security ID:            NULL SID
   Account Name:           -
   Account Domain:         -
   Logon ID:         0x0

Process Information:
   New Process ID:         0x1da8
   New Process Name: C:tempToolsmimix64mimikatz.exe
   Token Elevation Type:   %%1937
   Mandatory Label:        Mandatory LabelHigh Mandatory Level
   Creator Process ID:     0xd88
   Creator Process Name:   C:WindowsSystem32cmd.exe
   Process Command Line:
```

As you can see, this is the infamous `mimikatz`. It is widely used for credential theft attack, such as **Pass-the-Hash**. Further analysis shows that this user shouldn't be able to run this program since he didn't have administrative privileges in the machine. Following this rationale, we started looking to other tools that were potentially executed prior to this one and we found the following ones:

```
Process Information:
   New Process ID:         0x510
   New Process Name: C:tempToolsPSExecPsExec.exe
```

`PsExec` tool is commonly used by attackers to launch a command prompt (`cmd.exe`) with elevated (system) privileges; later on, we also found another 4688 event:

```
Process Information:
   New Process ID:         0xc70
   New Process Name: C:tempToolsProcDumpprocdump.exe
```

`ProcDump` tool is commonly used by attackers to dump the credentials from the `lsass.exe` process. It was still not clear how Jose was able to gain privileged access and one of the reasons is because we found event ID 1102, which shows that, at some point prior to executing these tools, he cleared the log on the local computer:

```
Log Name:      Security
Source:        Microsoft-Windows-Eventlog
Event ID:      1102
Task Category: Log clear
Level:         Information
Keywords:      Audit Success
User:          N/A
Computer:      BRANCHBR
Description:
The audit log was cleared.
Subject:
   Security ID:      BRANCHBRJose
   Account Name:     BRANCHBR
   Domain Name:      BRANCHBR
   Logon ID:   0x3D3214
```

Upon further investigation of the local system, it was possible to conclude:

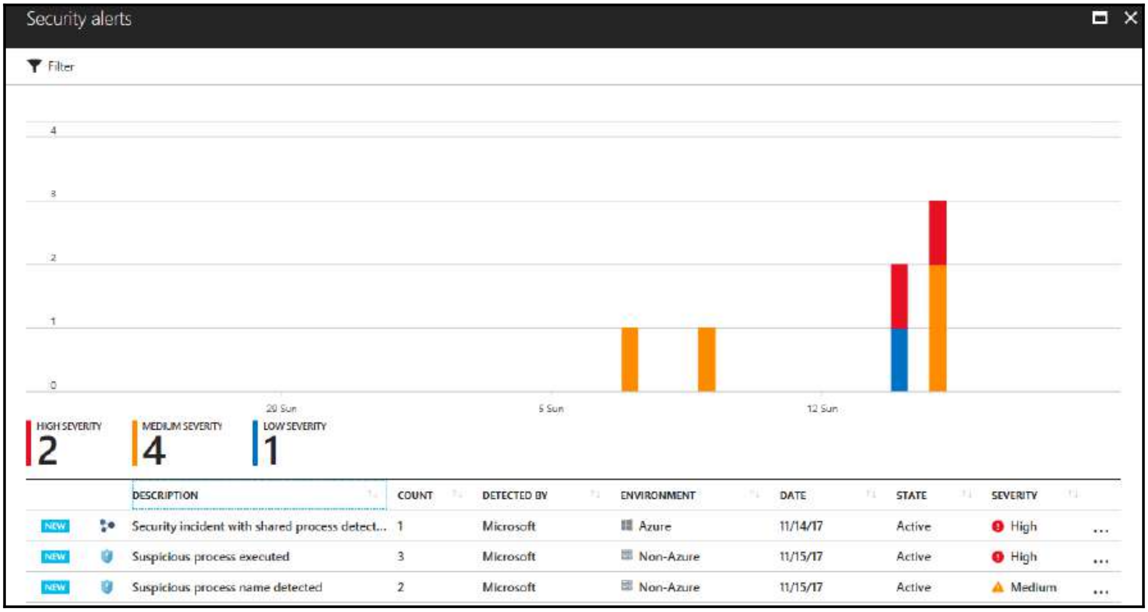
- Everything started with a phishing email
- This email had an embedded image that had a hyperlink to a site that was compromised
- A package was downloaded an extracted in the local system, this package contained many tools, such as *`mimikatz`*, `procdump`, and `psexec`
- This computer was not part of the domain, so only local credentials were compromised

Attacks against Brazilian accounts are growing; by the time we were writing this chapter, Talos Threat Intelligence identified a new attack. The blog *Banking Trojan Attempts To Steal Brazillion$* at `http://blog.talosintelligence.com/2017/09/brazilbanking.html` describes a sophisticated phishing email that used a legitimate VMware digital signature binary.

Investigating a compromised system in a hybrid cloud

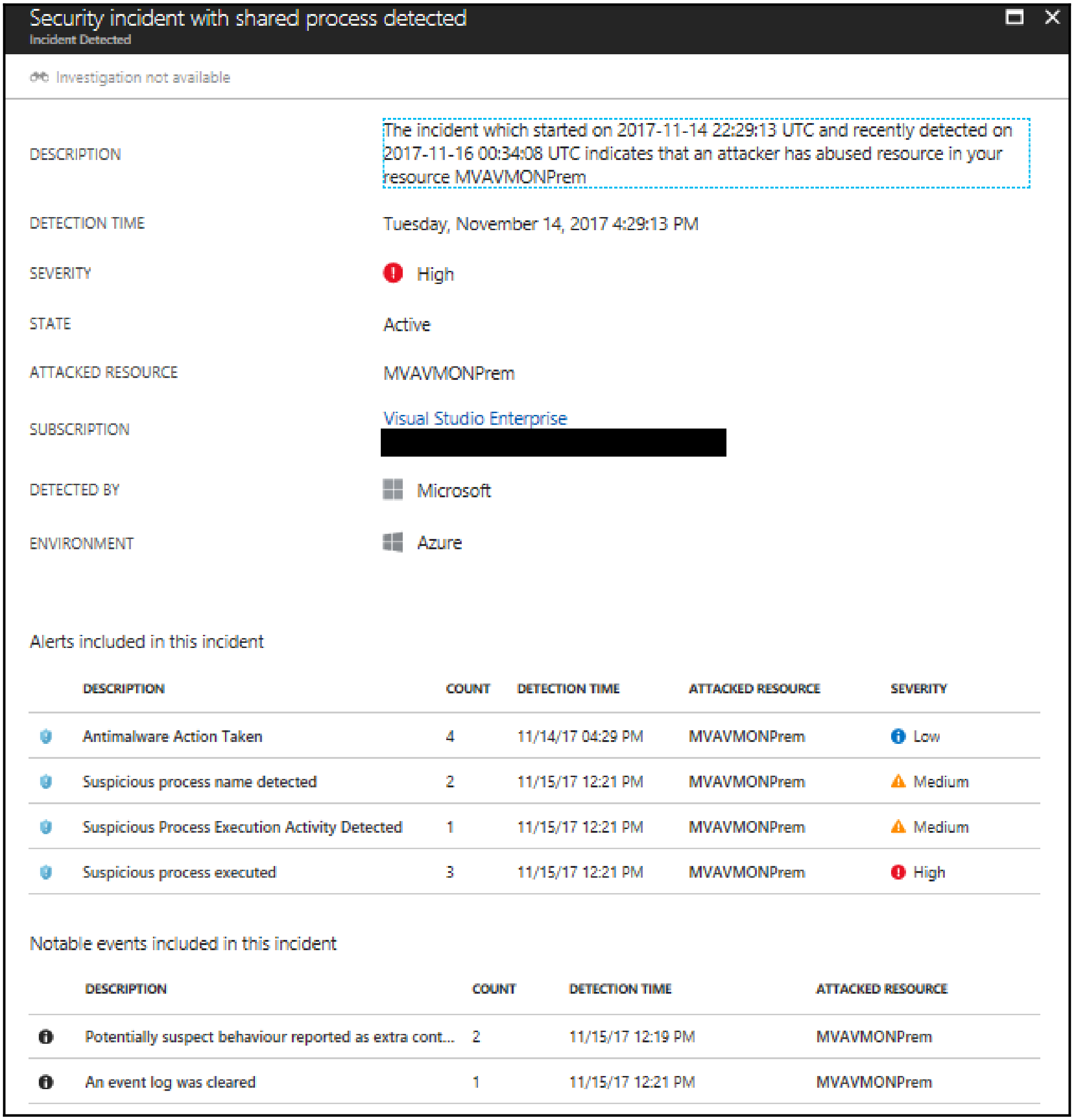
For this hybrid scenario, the compromised system will be located on-premises and the company has a cloud-based monitoring system, which for the purpose of this example will be Azure Security Center. To show how a hybrid cloud scenario can be similar to an on-premises online scenario, we will use the same case that was used before. Again, a user received a phishing email, clicked on the hyperlink, and got compromised. The difference now is that there is an active sensor monitoring the system, which will trigger an alert to SecOps, and the user will be contacted. The users don't need to wait days to realize they were compromised; the response is faster and more accurate.

The SecOps engineer has access to the Security Center dashboard and, when an alert is created, it shows the **NEW** flag besides the alert name. The SecOps engineer also noticed that a new security incident was created, as shown in the following screenshot:



		DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY	
NEW		Security incident with shared process detect...	1	Microsoft	Azure	11/14/17	Active	● High	...
NEW		Suspicious process executed	3	Microsoft	Non-Azure	11/15/17	Active	● High	...
NEW		Suspicious process name detected	2	Microsoft	Non-Azure	11/15/17	Active	▲ Medium	...

As mentioned in `Chapter 11`, *Active Sensors*, a security incident in Azure Security Center represents two or more alerts that are correlated. In other words, they are part of the same attack campaign against a target system. By clicking on this security incident, the SecOps engineer noticed the following alerts:



Security incident with shared process detected
Incident Detected

Investigation not available

DESCRIPTION	The incident which started on 2017-11-14 22:29:13 UTC and recently detected on 2017-11-16 00:34:08 UTC indicates that an attacker has abused resource in your resource MVAVMONPrem
DETECTION TIME	Tuesday, November 14, 2017 4:29:13 PM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	MVAVMONPrem
SUBSCRIPTION	Visual Studio Enterprise [redacted]
DETECTED BY	Microsoft
ENVIRONMENT	Azure

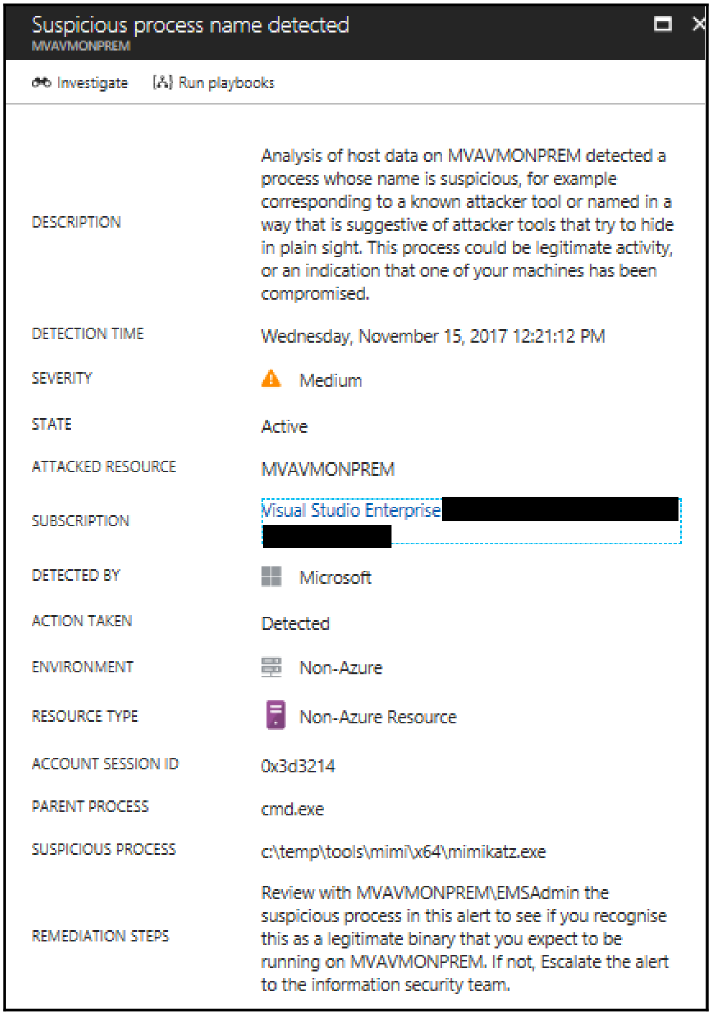
Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Antimalware Action Taken	4	11/14/17 04:29 PM	MVAVMONPrem	Low
Suspicious process name detected	2	11/15/17 12:21 PM	MVAVMONPrem	Medium
Suspicious Process Execution Activity Detected	1	11/15/17 12:21 PM	MVAVMONPrem	Medium
Suspicious process executed	3	11/15/17 12:21 PM	MVAVMONPrem	High

Notable events included in this incident

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE
Potentially suspect behaviour reported as extra cont...	2	11/15/17 12:19 PM	MVAVMONPrem
An event log was cleared	1	11/15/17 12:21 PM	MVAVMONPrem

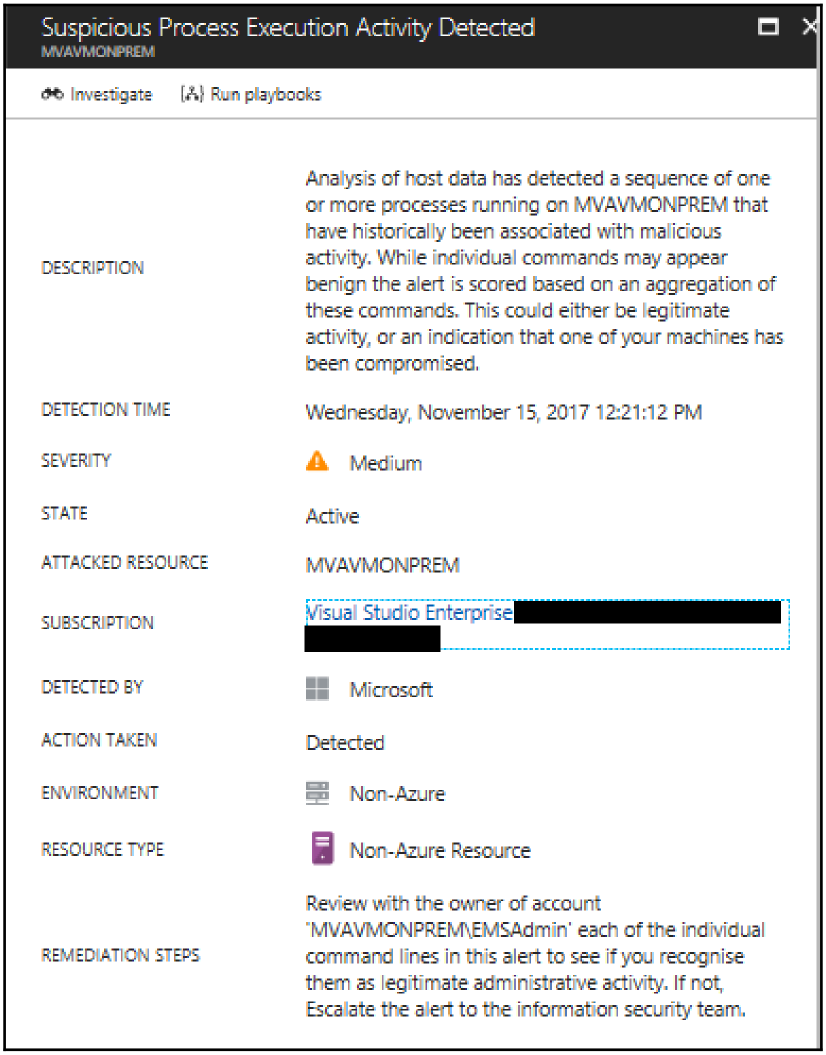
There are four alerts included in this incident and, as you can see, they are organized by time and not by priority. In the bottom part of this pane, there are two notable events included, which are extra information that can be useful during the investigation. The first event only reports that the antimalware installed in the local machine was able to block an attempt to drop a piece of malware in the local system. That's good, but, unfortunately, the attacker was highly motivated to continue his attack and managed to disable antimalware on the local system. It is important to keep in mind that, in order to do that, the attacker had to escalate privilege, and run a command such as `Taskkill` or `killav` to kill the antimalware process. Moving on, we have a medium priority alert showing that a suspicious process name was detected, as show in the following screenshot:



Suspicious process name detected
MVAVMONPREM

DESCRIPTION	Analysis of host data on MVAVMONPREM detected a process whose name is suspicious, for example corresponding to a known attacker tool or named in a way that is suggestive of attacker tools that try to hide in plain sight. This process could be legitimate activity, or an indication that one of your machines has been compromised.
DETECTION TIME	Wednesday, November 15, 2017 12:21:12 PM
SEVERITY	⚠ Medium
STATE	Active
ATTACKED RESOURCE	MVAVMONPREM
SUBSCRIPTION	Visual Studio Enterprise [redacted]
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Non-Azure
RESOURCE TYPE	Non-Azure Resource
ACCOUNT SESSION ID	0x3d3214
PARENT PROCESS	cmd.exe
SUSPICIOUS PROCESS	c:\temp\tools\mimi\x64\mimikatz.exe
REMEDIATION STEPS	Review with MVAVMONPREM\EMSAdmin the suspicious process in this alert to see if you recognise this as a legitimate binary that you expect to be running on MVAVMONPREM. If not, Escalate the alert to the information security team.

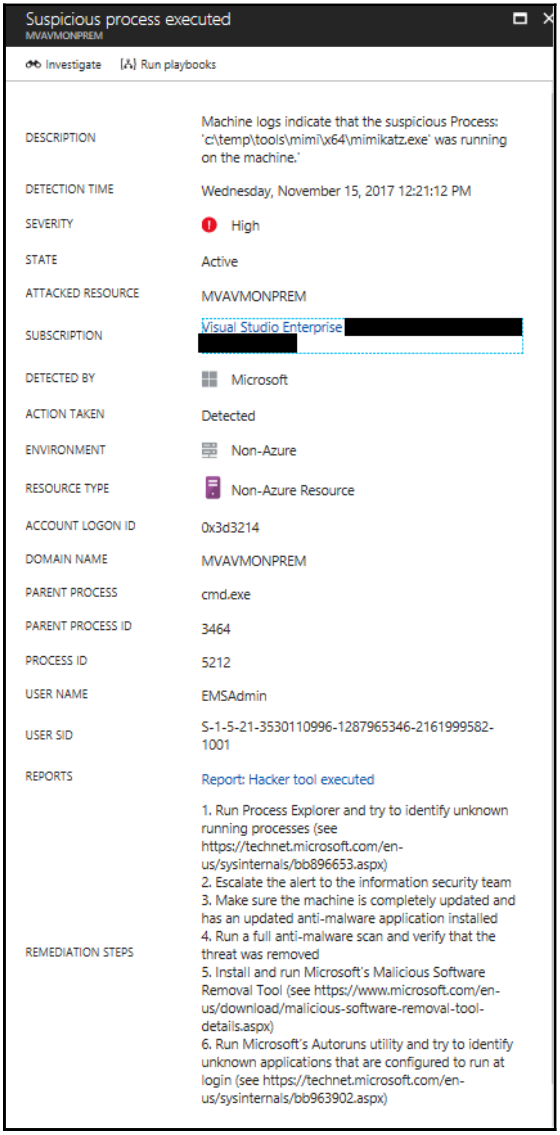
In this case the process is `mimikatz.exe`, which was also used in our previous case. You may ask: why is this medium priority and not high? It is because, at this point, this process was not launched yet. That's why the alert says: **Suspicious process name detected**. Another important fact about this event is that type of attacked resource, which is **Non-Azure Resource**, and this is how you identify that this is on-premises or a VM in another cloud provider (such as Amazon AWS). Moving on to the next alert, we have a **Suspicious Process Execution Activity Detected**:



Suspicious Process Execution Activity Detected
MVAVMONPREM

DESCRIPTION	Analysis of host data has detected a sequence of one or more processes running on MVAVMONPREM that have historically been associated with malicious activity. While individual commands may appear benign the alert is scored based on an aggregation of these commands. This could either be legitimate activity, or an indication that one of your machines has been compromised.
DETECTION TIME	Wednesday, November 15, 2017 12:21:12 PM
SEVERITY	⚠ Medium
STATE	Active
ATTACKED RESOURCE	MVAVMONPREM
SUBSCRIPTION	Visual Studio Enterprise [redacted]
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Non-Azure
RESOURCE TYPE	Non-Azure Resource
REMEDIATION STEPS	Review with the owner of account 'MVAVMONPREM\EMSAdmin' each of the individual command lines in this alert to see if you recognise them as legitimate administrative activity. If not, Escalate the alert to the information security team.

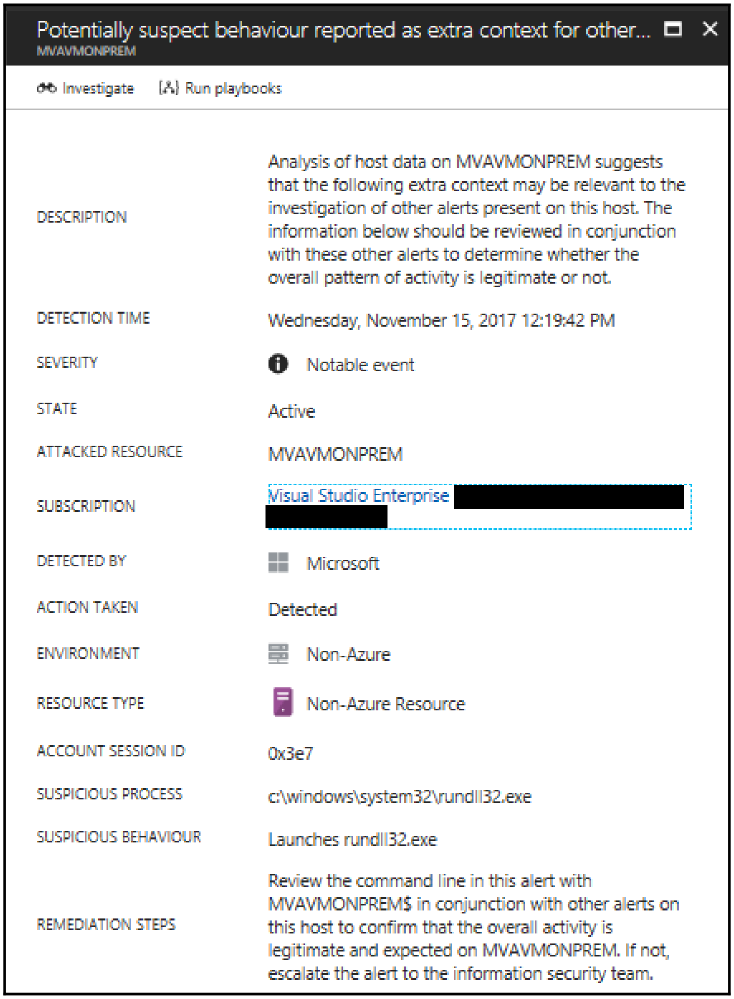
The description of this alert is pretty clear about what is happening at this point and this is one of the biggest advantages of having a monitoring system watching process behavior. It will observe these patterns and correlate this data with its own threat intelligence feed to understand if these activities are suspicious or not. The remediation steps provided can also help to take the next steps. Let's continue looking to the other alerts. The next one is the high priority alert, which is the execution of a suspicious process:



Suspicious process executed
MVAVMONPREM

DESCRIPTION	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe' was running on the machine.'
DETECTION TIME	Wednesday, November 15, 2017 12:21:12 PM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	MVAVMONPREM
SUBSCRIPTION	Visual Studio Enterprise [redacted]
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Non-Azure
RESOURCE TYPE	Non-Azure Resource
ACCOUNT LOGON ID	0x3d3214
DOMAIN NAME	MVAVMONPREM
PARENT PROCESS	cmd.exe
PARENT PROCESS ID	3464
PROCESS ID	5212
USER NAME	EMSAdmin
USER SID	S-1-5-21-3530110996-1287965346-2161999582-1001
REPORTS	Report: Hacker tool executed
REMEDIATION STEPS	1. Run Process Explorer and try to identify unknown running processes (see https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx) 2. Escalate the alert to the information security team 3. Make sure the machine is completely updated and has an updated anti-malware application installed 4. Run a full anti-malware scan and verify that the threat was removed 5. Install and run Microsoft's Malicious Software Removal Tool (see https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx) 6. Run Microsoft's Autoruns utility and try to identify unknown applications that are configured to run at login (see https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx)

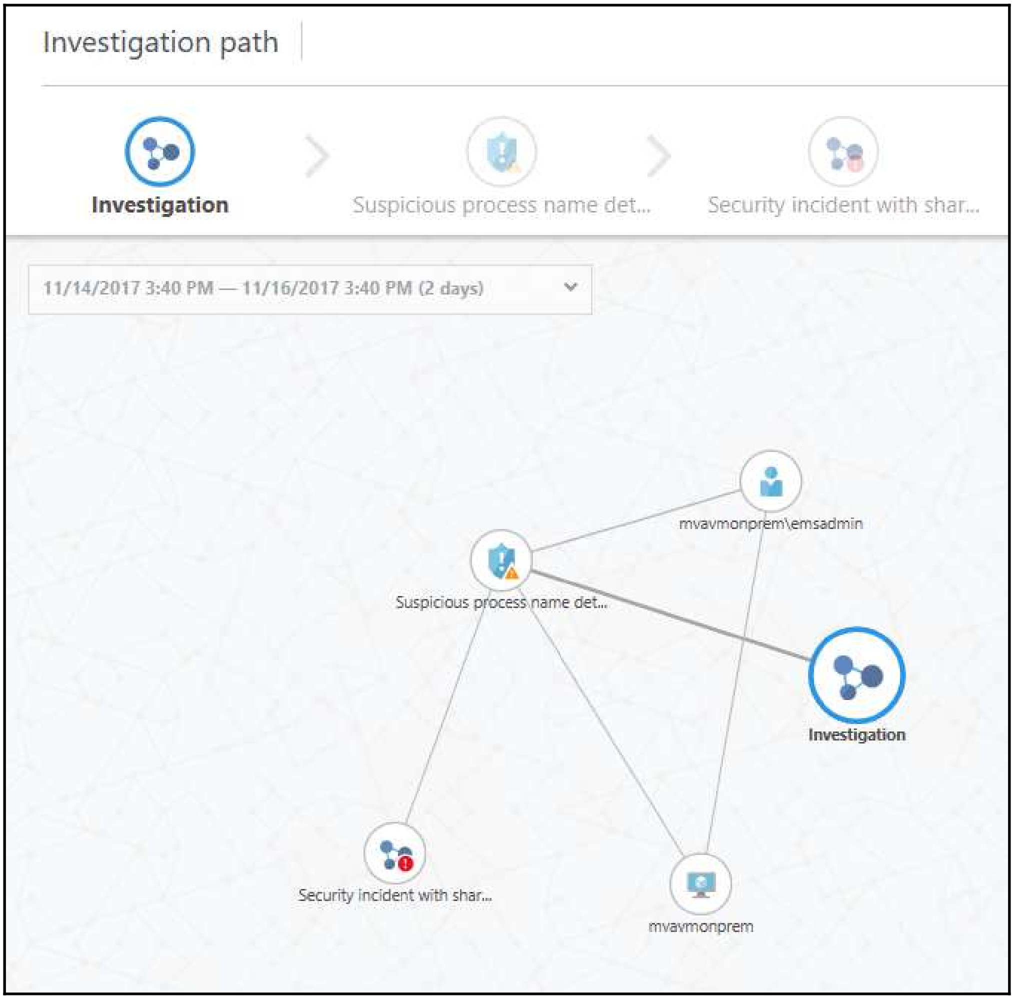
This alert shows that `mimikatz.exe` was executed and that the parent process was `cmd.exe`. Since `mimikatz` requires a privileged account to successfully run, the assumption is that this command prompt is running in the context of a high privilege account, which in this case is **EMSAdmin**. The notable events that you have in the bottle should also be reviewed. We will skip the first one, since we know is about cleaning the evidence (wipe out the logs), but the next one is not so clear, so let's review it:



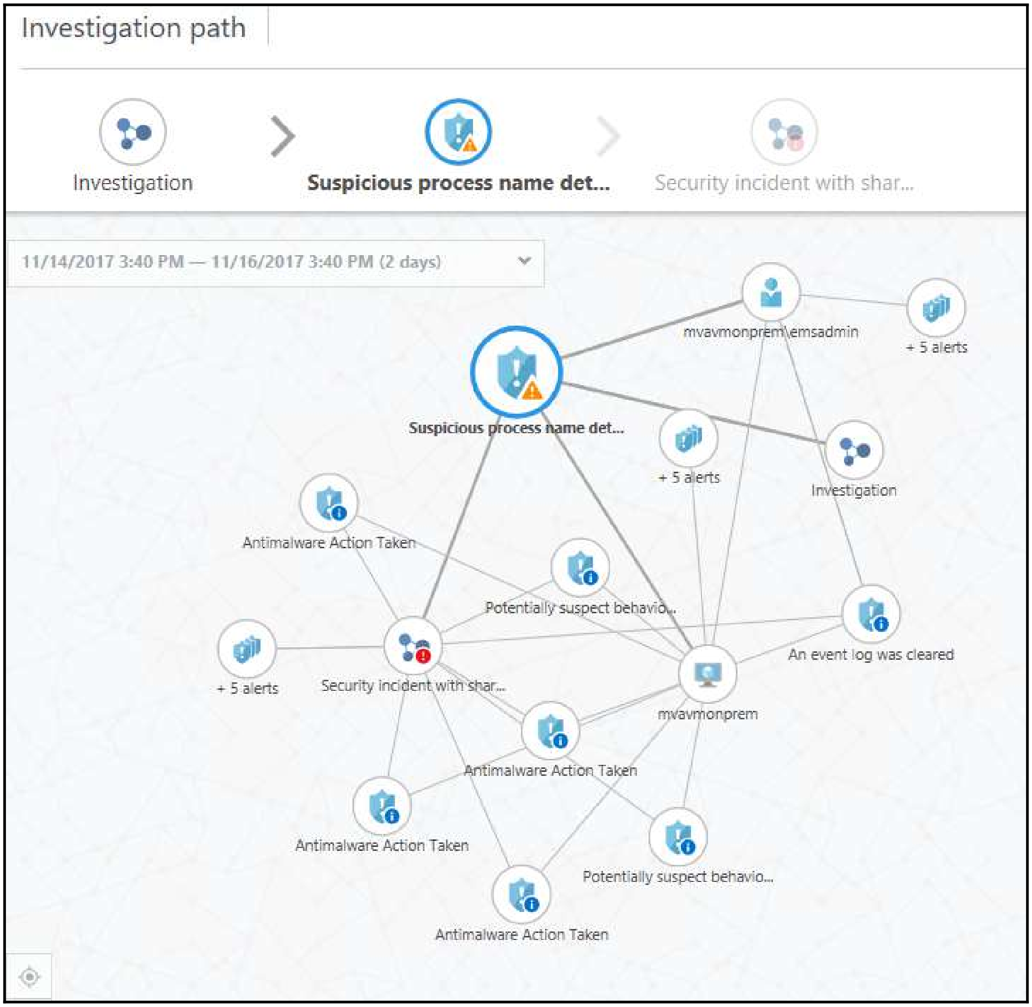
Potentially suspect behaviour reported as extra context for other...
MVAVMONPREM

DESCRIPTION	Analysis of host data on MVAVMONPREM suggests that the following extra context may be relevant to the investigation of other alerts present on this host. The information below should be reviewed in conjunction with these other alerts to determine whether the overall pattern of activity is legitimate or not.
DETECTION TIME	Wednesday, November 15, 2017 12:19:42 PM
SEVERITY	● Notable event
STATE	Active
ATTACKED RESOURCE	MVAVMONPREM
SUBSCRIPTION	Visual Studio Enterprise [redacted]
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Non-Azure
RESOURCE TYPE	Non-Azure Resource
ACCOUNT SESSION ID	0x3e7
SUSPICIOUS PROCESS	c:\windows\system32\rundll32.exe
SUSPICIOUS BEHAVIOUR	Launches rundll32.exe
REMEDIATION STEPS	Review the command line in this alert with MVAVMONPREM$ in conjunction with other alerts on this host to confirm that the overall activity is legitimate and expected on MVAVMONPREM. If not, escalate the alert to the information security team.

This is another indication that the attacker compromised other files, such as the `rundll32.exe`. At this point, you have enough information to continue your investigation process. As described in `Chapter 12`, *Threat Intelligence*, the Azure Security Center has a feature that enables you to go deeply into the details of a security issue, which is the investigation feature. In this case, we will select the second alert of this list and click on the **Investigation** button. The investigation path for this particular case is shown in the following screenshot:


Investigation path
Investigation
Suspicious process name det...
Security incident with shar...
11/14/2017 3:40 PM — 11/16/2017 3:40 PM (2 days)
mvavmonprem\emsadmin
Suspicious process name det...
Investigation
Security incident with shar...
mvavmonprem

Each entity in this diagram provides details about its own object and, if there are other entities related to the one selected, you can pivot it by clicking on the object itself, as shown in the following screenshot:

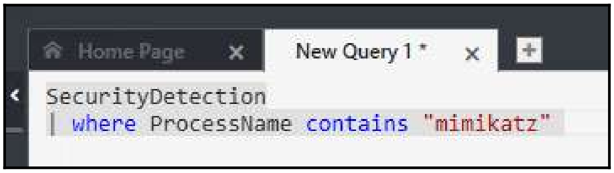

Investigation path
Investigation
Suspicious process name det...
Security incident with shar...
11/14/2017 3:40 PM — 11/16/2017 3:40 PM (2 days)
mvavmonprem\emsadmin
+ 5 alerts
Suspicious process name det...
+ 5 alerts
Investigation
Antimalware Action Taken
Potentially suspect behavio...
An event log was cleared
+ 5 alerts
Security incident with shar...
mvavmonprem
Antimalware Action Taken
Antimalware Action Taken
Potentially suspect behavio...
Antimalware Action Taken

The investigation map helps you to visualize the steps that were taken during this attack and better understand the correlation between all entities that were involved.

Search and you shall find it

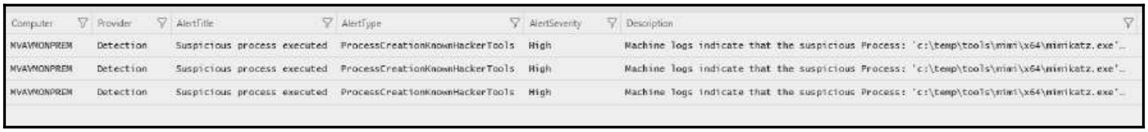
In a real-world scenario, the amount of data that gets collected by sensors and monitoring systems can be overwhelming. Manual investigation of these logs can take days, and that's why you need a security monitoring system that can aggregate all these logs, digest them, and rationalize the result for you. Having said that, you also need searching capabilities to be able to keep digging up more important information as you continue your investigation.

Security Center search capabilities are powered by Azure Log Analytics, which has its own query language. By using Log Analytics, you can search across different workspaces and customize the details about your search. Let's say that you needed to know if there were other machines in this environment that had the process named `mimikatz` present on it. The search query would be similar to the following:



```
SecurityDetection
| where ProcessName contains "mimikatz"
```

Notice that in this case the operator says `contains` but it could be `equals`. The reason to use `contains` is that it could bring more results and, for the purpose of this investigation, we want to know all processes that contain these strings in the name. The result for this query shows the following entries:



Computer	Provider	AlertTitle	AlertType	AlertSeverity	Description
MVAVMONPREM	Detection	Suspicious process executed	ProcessCreationKnownHackerTools	High	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'...
MVAVMONPREM	Detection	Suspicious process executed	ProcessCreationKnownHackerTools	High	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'...
MVAVMONPREM	Detection	Suspicious process executed	ProcessCreationKnownHackerTools	High	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'...

The output always comes in this table format and allows you to visualize all the details about the matches for this query.

> Access the following link for another example of using search capabilities to find important information about an attack: `https://blogs.technet.microsoft.com/yuridiogenes/2017/10/20/searching-for-a-malicious-process-in-azure-security-center/`.

Lessons learned

Every time an incident comes to its closure, you should not only document each step that was done during the investigation but also make sure that you identify key aspects of the investigation that need to be either reviewed to improve or fix since it didn't work so well. The lessons learned are crucial for the continuous improvement of the process and to avoid making the same mistakes again.

In both cases, a credential theft tool was used to gain access to a user's credential and escalate privileges. Attacks against a user's credential are a growing threat and the solution is not based on a silver bullet product, instead, it is an aggregation of tasks, such as:

- Reducing the number of administrative level accounts and eliminating administrative accounts in local computers. Regular users shouldn't be administrators on their own workstation.
- Using multifactor authentication as much as you can.
- Adjusting your security policies to restrict login rights.
- Having a plan to periodically reset the **Kerberos TGT** (**KRBTGT**) account. This account is used to perform a golden ticket attack.

These are only some basic improvements for this environment; the Blue Team should create an extensive report to document the lessons learned and how this will be used to improve the defense controls.

References

1. *Banking Trojan Attempts To Steal Brazillion$*: `http://blog.talosintelligence.com/2017/09/brazilbanking.html`
2. *Security Playbook in Azure Security Center (Preview)*: `https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks`
3. *Handling Security Incidents in Azure Security Center*: `https://docs.microsoft.com/en-us/azure/security-center/security-center-incident`
4. *Threat intelligence in Azure Security Center*: `https://docs.microsoft.com/en-us/azure/security-center/security-center-threat-intel`

Summary

In this chapter, you learned how important it is to correctly scope an issue before investigating it from the security perspective. You learned the key artifacts in a Windows system and how to improve your data analysis by reviewing only the relevant logs for the case. Next, you followed an on-premises investigation case, the relevant data that was analyzed, and how to interpret that data. You also follow a hybrid cloud investigation case, but this time using Azure Security Center as the main monitoring tool.

In the next chapter, you will learn how to perform a recovery process in a system that was previously compromised. You will also learn about backup and disaster recovery plans.

14
Recovery Process

The previous chapter looked at how an attack can be investigated to understand the cause and prevent a similar attack in the future. However, an organization cannot fully depend on protecting itself from attacks and all the risks that it faces. The organization is exposed to a wide range of disasters such that it is impossible to have protective measures against them. The causes of a disaster to the IT infrastructure can either be natural or man-made. Natural disasters are ones that result from environmental hazards or acts of nature. These include blizzards, wildfires, hurricanes, volcanic eruptions, earthquakes, floods, lightning strikes, and even asteroids falling from the sky and impacting the ground. Man-made disasters are ones that arise from the actions of human users or external human actors. They include fires, cyber warfare, nuclear explosions, hacking, power surges, and accidents, among others.

When these strike an organization, its level of preparedness to respond to a disaster will determine its survivability and speed of recovery. This chapter will look at the ways an organization can prepare for a disaster, survive it when it happens, and easily recover from the impact.

We will talk about the following topics:

- Disaster recovery plan
- Live recovery
- Contingency plan
- Best practices for recovery

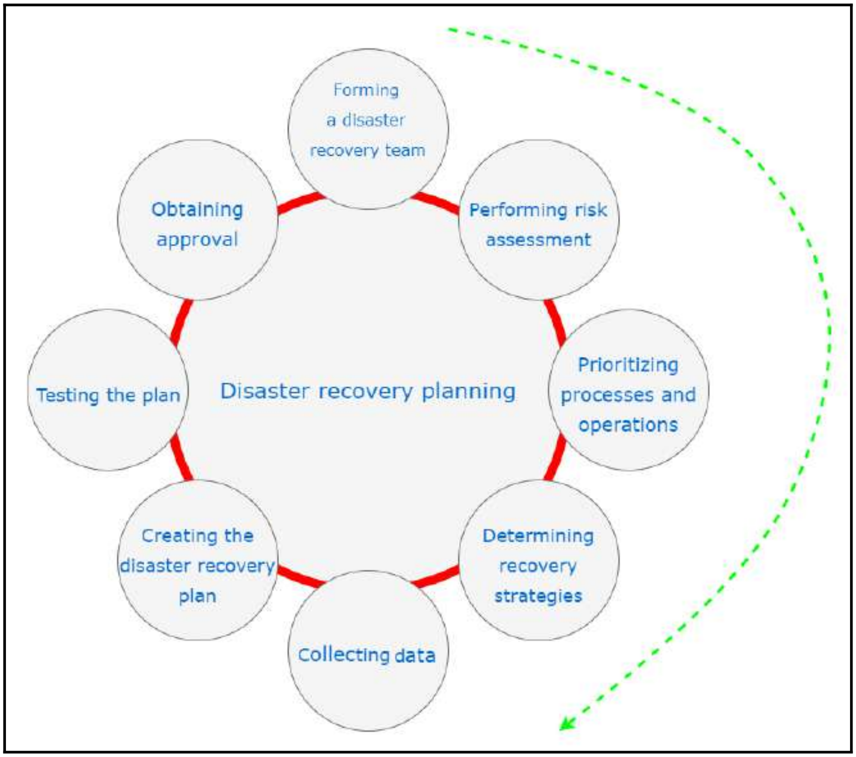
Disaster recovery plan

The disaster recovery plan is a documented set of processes and procedures that are carried out in the effort to recover the IT infrastructure in the event of a disaster. Because of many organizations' dependency on IT, it has become mandatory for organizations to have a comprehensive and well-formulated disaster recovery plan. Organizations are not able to avoid all disasters; the best they can do is plan ahead how they will recover when disasters happen. The objective of the plan is to protect the continuity of business operations when IT operations have been partially or fully stopped. There are several benefits of having a sound disaster recovery plan:

- The organization has a sense of security. The recovery plan assures it of its continued ability to function in the face of a disaster.
- The organization reduces delays in the recovery process. Without a sound plan, it is easy for the disaster recovery process to be done in an uncoordinated way, thereby leading to needless delays.
- There is guaranteed reliability of standby systems. A part of the disaster recovery plan is to restore business operations using standby systems. The plan ensures that these systems are always prepped and ready to take over during disasters.
- The provision of a standard test plan for all business operations.
- The minimization of the time taken to make decisions during disasters.
- The mitigation of legal liabilities that the organization could develop during a disaster.

The disaster recovery planning process

The following are the steps that organizations should take to come up with a comprehensive disaster recovery plan. The diagram gives a summary of the core steps. All the steps are equally important:


Forming a disaster recovery team
Performing risk assessment
Prioritizing processes and operations
Determining recovery strategies
Collecting data
Creating the disaster recovery plan
Testing the plan
Obtaining approval
Disaster recovery planning

Forming a disaster recovery team

A **disaster recovery** (**DR**) team is the team that is mandated with assisting the organization with all the disaster recovery operations. It should be all-inclusive, involving members from all departments and some representatives from top-level management. This team will be key in determining the scope of the recovery plan regarding the operations that they carry out in their individual departments. The team will also oversee the successful development and implementation of the plan.

Performing risk assessment

The disaster recovery team should conduct a risk assessment and identify the natural and man-made risks that could affect organizational operations, especially those tied to the IT infrastructure. The selected departmental staff should analyze their functional areas for all the potential risks and determine the potential consequences associated with such risks. The disaster recovery team should also evaluate the security of sensitive files and servers by listing the threats that they are exposed to and the impacts those threats may have. At the end of the risk assessment exercise, the organization should be fully aware of the impacts and consequences of multiple disaster scenarios. A thorough disaster recovery plan will be made in consideration of the worst-case scenario.

Prioritizing processes and operations

Here, the representatives from each department in the disaster recovery plan identify their critical needs that need to be prioritized in the event of a disaster. Most organizations will not possess sufficient resources to respond to all the needs that arise during disasters (2). This is the reason why some criteria need to be set in order to determine which needs require the organization's resources and attention first. The key areas that need to be prioritized in the making of a disaster recovery plan include functional operations, information flow, accessibility and availability of the computer systems used, sensitive data, and existing policies (2).To come up with the most important priorities, the team needs to determine the maximum possible time that each department can operate without critical systems. Critical systems are defined as systems that are required to support the different operations that take place in an organization. A common approach to establishing priorities is to list the critical needs of each department, identify the key processes that need to take place in order to meet them, and then identify and rank the underlying processes and operations. The operations and processes can be ranked into three levels of priority: essential, important, and nonessential.

Determining recovery strategies

The practical ways to recover from a disaster are identified and evaluated at this step. The recovery strategies need to be formulated to cover all aspects of the organization. These aspects include hardware, software, databases, communication channels, customer services, and end-user systems. At times, there may be written agreements with third parties, such as vendors, to provide recovery alternatives in times of disasters. The organization should review such agreements, the duration of their cover, and their terms and conditions. By the end of this step, the disaster recovery team should have a solution to all that may be affected by a disaster in the organization.

Collecting data

To facilitate the DR team going through a complete disaster recovery process, information about the organization should be collected and documented. The relevant information that should be collected includes inventory forms, policies and procedures, communication links, important contact details, customer care numbers of service providers, and details of the hardware and software resources that the organization has (3). Information about backup storage sites and backup schedules alongside their retention duration should also be collected.

Creating the disaster recovery plan

The preceding steps, if performed correctly, will give the DR team enough information to make a sound disaster recovery plan that is both comprehensive and practical. The plan should be in a standard format that is easily readable and succinctly puts together all the essential information. The response procedures should be fully explained in an easy-to-understand manner. It should have a step-by-step layout and cover all that the response team and other users need to do when disaster strikes. The plan should also specify its own review and updating procedure.

Testing the plan

The applicability and reliability of the plan should never be left to chance since it may determine the continuity of an organization after a major disaster has occurred. It should, therefore, be thoroughly tested to identify any challenges or errors that it may contain. Testing will provide a platform for the DR team and the users to perform the necessary checks and gain a good understanding of the response plan. Some of the tests that can be carried include simulations, checklist tests, full-interruption tests, and parallel tests. It is imperative that the disaster recovery plan that a whole organization will rely on is proven to be practical and effective, for both the end users and the DR team.

Obtaining approval

After the plan has been tested and found to be reliable, practical, and comprehensive, it should be submitted to top management to get approved.

The top management has to approve the recovery plan on two grounds:

- The first one is the assurance that the plan is consistent with the organization's policies, procedures, and other contingency plans (3).

  An organization may have multiple business contingency plans and they should all be streamlined. For instance, a DR plan that can only bring back online services after a few weeks might be incompatible with the goals of an e-commerce company.

- The second grounds for approval of the plan is that the plan can be slotted in for annual reviews.

  The top management will do its own evaluations of the plan to determine its adequacy. It is in the interests of the management that the whole organization is covered with an adequate recovery plan. The top management also has to evaluate the compatibility of the plan with the organization's goals.

Maintaining the plan

The IT threat landscape can change a lot within a very short space of time. In previous chapters, we discussed ransomware called WannaCry, and explained that it hit over 150 countries within a short time span. It caused huge losses in terms of money and even led to deaths when it encrypted computers used for sensitive functions. This is one of the many dynamic changes that affect IT infrastructures and force organizations to quickly adapt. Therefore, a good disaster recovery plan must be updated often (3). Most of the organizations hit by WannaCry were unprepared for it and had no idea what actions they should have taken. The attack only lasted a few days, but caught many organizations unaware. This clearly shows that disaster recovery plans should be updated based on need rather than on a rigid schedule. Therefore, the last step in the disaster recovery process should be the setting up of an updating schedule. This schedule should also make provisions for updates to be done when they are needed, too.

Challenges

There are many challenges that face disaster recovery plans. One of these is the lack of approval by the top management. Disaster recovery planning is taken as a mere drill for a fake event that might never happen (3).

Therefore, the top management may not prioritize the making of such a plan and might also not approve an ambitious plan that seems to be a little bit costly. Another challenge is the incompleteness of the **recovery time objective** (**RTO**) that DR teams come up with. RTOs are the key determiners of the maximum acceptable downtime for an organization. It is at times difficult for the DR team to come up with a cost-effective plan that is within the RTO. Lastly, there is the challenge of outdated plans. The IT infrastructure dynamically changes in its attempts to counter the threats that it faces. Therefore, it is a huge task to keep the disaster recovery plan updated, and some organizations fail to do this. Outdated plans may be ineffective and may be unable to recover the organization when disasters caused by new threat vectors happen.

Live recovery

There are times when a disaster will affect a system that is still in use. Traditional recovery mechanisms mean that the affected system has to be taken offline, some backup files are installed, and then the system is brought back online. There are some organizations that have systems that cannot enjoy the luxury of being taken offline for recovery to be done. There are other systems that are structurally built in a way that they cannot be brought down for recovery. In both instances, a live recovery has to be done. A live recovery can be done in two ways. The first involves a clean system with the right configurations and uncorrupted backup files being installed on top of the faulty system. The end result is that the faulty system is gotten rid of, together with its files, and a new one takes over.

The second type of live recovery is where data recovery tools are used on a system that is still online. The recovery tools may run an update on all the existing configurations to change them to the right ones. It may also replace faulty files with recent backups. This type of recovery is used when there is some valuable data that is to be recovered in the existing system. It allows for the system to be changed without affecting the underlying files. It also allows recovery to be done without doing a complete system restore. A good example is the recovery of Windows using a Linux live CD. The live CD can do many recovery processes, thereby saving the user from having to install a new version of Windows and thus losing all the existing programs (4). The live CD can, for instance, be used to reset or change a Windows PC password. The Linux tool used to reset or change passwords is called `chntpw`. An attacker does not need any root privileges to perform this. The user needs to boot the Windows PC from an Ubuntu live CD and install `chntpw` (4). The live CD will detect the drives on the computer and the user will just have to identify the one containing the Windows installation.

With this information, the user has to input the following commands in the terminal:

```
cd/media
ls
cd <hdd or ssd label>
cd windows/system32/config
```

This is the directory that contains the Windows configurations:

```
sudo chntpw sam
```

In the preceding command, `sam` is the config file that contains the Windows registry (4). Once opened in the terminal, there will be a list showing all the user accounts on the PC and a prompt to edit the users. There are two options: clearing the password or resetting the old password.

The command to reset the password can be issued in the terminal as:

```
sudo chntpw –u <user> SAM
```

As mentioned in the previously discussed example, when users cannot remember their Windows passwords, they can recover their accounts using the live CD without having to disrupt the Windows installation. There are many other live recovery processes for systems, and all share some similarities. The existing system is never wiped off completely.

Contingency planning

Organizations need to protect their networks and IT infrastructure from total failure. Contingency planning is the process of putting in place interim measures to allow for quick recovery from failures and at the same time limit the extent of damage caused by the failures (5). This is the reason why contingency planning is a critical responsibility that all organizations should undertake. The planning process involves the identification of risks that the IT infrastructure is subject to and then coming up with remediation strategies to reduce the impact of the risks significantly. There are many risks that face organizations, ranging from natural disasters to the careless actions of users. The impacts that these risks may cause range from mild, such as disk failures, to severe impacts, such as the physical destruction of a server farm. Even though organizations tend to dedicate resources toward the prevention of the occurrence of such risks, it is impossible to eliminate all of them (5). One of the reasons why they cannot be eliminated is that organizations depend on many critical resources that reside outside their control, such as telecommunications. Other reasons include the advancements of threats and uncontrollable actions of internal users either due to negligence or malice.

Therefore, organizations must come to the realization that they could one day wake to a disaster that has occurred and caused severe damage. They must have sound contingency plans with reliable execution plans and reasonably scheduled updating schedules. For contingency plans to be effective, organizations must ensure that:

- They understand the integration between the contingency plan and other business continuity plans
- They develop the contingency plans carefully and pay attention to the recovery strategies that they choose, as well as their recovery time objectives
- They develop the contingency plans with an emphasis on exercise, training, and updating tasks

A contingency plan must address the following IT platforms and provide adequate strategies and techniques for recovering them:

- Workstations, laptops, and smartphones
- Servers
- Websites
- The intranet
- Wide area networks
- Distributed systems (if any)
- Server rooms or firms (if any)

IT contingency planning process

IT contingency planning helps organizations to prepare for future unfortunate events to ensure that they are in a position to respond to them timely and effectively. Future unfortunate events might be caused by hardware failure, cybercrime, natural disasters, and unprecedented human errors. When they happen, an organization needs to keep going, even after suffering significant damage. This is the reason why IT contingency planning is essential. The IT contingency planning process is made up of the following elaborated five steps.

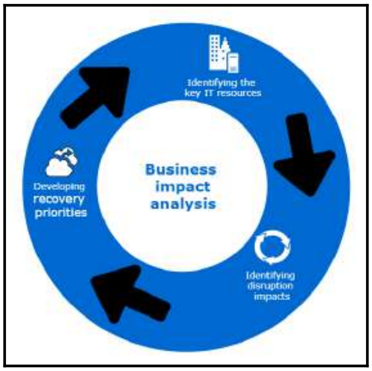
Development of the contingency planning policy

A good contingency plan must be based on a clear policy that defines the organization's contingency objectives and establishes the employees responsible for contingency planning. All the senior employees must support the contingency program. They should, therefore, be included in developing a site-wide, agreed-upon contingency planning policy that outlines the roles and responsibilities of contingency planning. The policy they come up with must contain the following key elements:

- The scope that the contingency plan will cover
- The resources required
- The training needs of the organizational users
- Testing, exercising, and maintenance schedules
- Backup schedules and their storage locations
- The definitions of the roles and responsibilities of the people that are part of the contingency plan

Conducting business impact analysis

Doing **business impact analysis** (**BIA**) will help the contingency planning coordinators to easily characterize an organization's system requirements and their interdependencies. This information will assist them in determining the organization's contingency requirements and priorities when coming up with the contingency plan. The main purpose of conducting a BIA, however, is to correlate different systems with the critical services that they offer (6). From this information, the organization can identify the individual consequences of a disruption to each system. Business impact analysis should be done in three steps, as illustrated in the following diagram:


Identifying the key IT resources
Identifying disruption impacts
Developing recovery priorities
Business impact analysis

Identifying the critical IT resources

Although the IT infrastructure can at times be complex and have numerous components, only a few are critical. These are the resources that support the core business processes, such as payroll processing, transaction processing, or an e-commerce shop checkout. The critical resources are the servers, the network, and the communication channels. Different businesses may, however, have their own distinct critical resources.

Identifying disruption impacts

For each of the identified critical resources, the business should identify their allowable outage times. The maximum allowable outage time is the period of unavailability of a resource within which the business will not feel major impacts (6). Again, different organizations will have different maximum allowable outage times depending on their core business processes. An e-commerce shop, for instance, has less maximum allowable outage time for its network compared to a manufacturing industry. The organization needs to keenly observe its key processes and come up with estimates of the maximum allowable time that they can remain unavailable without having adverse consequences. The best outage time estimates should be obtained by balancing the cost of a disruption and the cost of recovering an IT resource.

Developing recovery priorities

From the information that the organization will have collected from the preceding step, it should prioritize the resources that should be restored first. The most critical resources, such as communication channels and the network, are almost always the first priority. However, this is still subject to the nature of the organization. Some organizations may even prioritize the restoration of production lines higher than the restoration of the network.

Identifying the preventive controls

After conducting the BIA, the organization will have vital information concerning its systems and their recovery requirements. Some of the impacts that are uncovered in the BIA could be mitigated through preventative measures. These are measures that can be put in place to detect, deter, or reduce the impact of disruptions to the system. If preventative measures are feasible and at the same time not very costly, they should be put in place to assist in the recovery of the system. However, at times, it may become too costly to put in place preventative measures for all types of disruptions that may occur. There is a very wide range of preventative controls available, from those that prevent power interruptions to those that prevent fires.

Developing recovery strategies

These are the strategies that will be used to restore the IT infrastructure in a quick and effective manner after a disruption has occurred. Recovery strategies must be developed with a focus on the information obtained from the BIA. There are several considerations that have to be made while choosing between alternative strategies, such as costs, security, site-wide compatibility, and the organization's recovery time objectives (7).

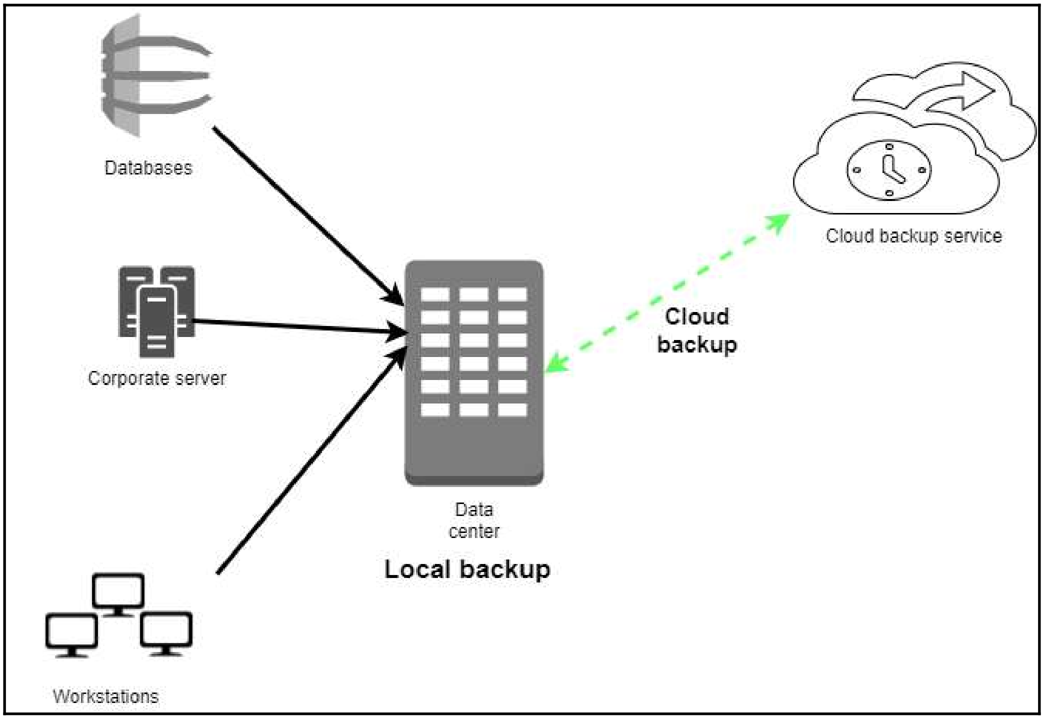
Recovery strategies should also consist of combinations of methods that are complementary and cover the entire threat landscape facing an organization.

The following are the most commonly used recovery methods.

Backups

Occasionally, the data contained in systems should be backed up. The backup intervals should, however, be short enough to capture reasonably recent data (7). In the instance of a disaster that leads to the loss of the systems and the data therein, the organization can easily recover. It can reinstall the system and then load the most recent backup and get back on its feet. Data backup policies should be created and implemented. The policies at the very least should cover the backup storage sites, naming conventions for the backups, the rotation frequency, and the methods for the transmission of the data to backup sites (7).

The following diagram illustrates the complete backup process:



Cloud backups have the advantage of cost, reliability, availability, and size. Since the organization does not buy the hardware or meet the maintenance costs of the cloud servers, it is cheaper. Since cloud backups are always online, they are more reliable and available than backups on external storage devices. Lastly, the flexibility to rent as much space as one wants gives the advantage of storage capacity that grows with demand. The two leading disadvantages of cloud computing are privacy and security.

Alternative sites

There are some disruptions that have long-term effects. These cause an organization to close operations at a given site for a long period. The contingency plan should provide options to continue business operations in an alternative facility.

There are three types of alternative sites: sites owned by the organization, sites acquired through agreements with internal or external entities, and sites commercially acquired through leases (7). Alternative sites are categorized based on their readiness to continue business operations. Cold sites are those that have all the adequate supportive resources for the carrying out of IT operations. The organization, however, has to install the necessary IT equipment and telecommunication services to reestablish the IT infrastructure. Warm sites are partially equipped and maintained in a state where they are ready to continue offering the moved IT systems. However, they require some preparation in order to be fully operational. Hot sites are adequately equipped and staffed to continue with IT operations when the main site is hit with a disaster. Mobile sites are transportable office spaces that come with all the necessary IT equipment to host IT systems. Lastly, mirrored sites are redundant facilities that have the same IT systems and data as the main site and can continue operations seamlessly when the main site is facing a disaster.

The following is a summary of the alternative sites in ascending order of their readiness to continue with operations:

- Cold sites
    - Have the supportive resources ready
    - Require the installation of IT equipment and telecommunication services
- Warm sites
    - Partially equipped and kept in a ready state
    - Require preparation through staffing to be operational
- Hot sites
    - Adequately equipped and staffed to continue with IT operations
- Mirrored sites
    - Exact replicas of the main sites

Equipment replacement

Once a destructive disaster occurs, thus damaging critical hardware and software, the organization will have to make arrangements to have these replaced. There are three options that the contingency plan may go for. One of these is vendor agreements, where the vendors are notified to respond to a disaster with the necessary replacements. The other option is an equipment inventory, where the organization purchases replacements for critical IT equipment in advance and safely stores them. Once a disaster strikes, the replacement equipment may be used for replacements in the main site or installed in the alternative sites to reestablish the IT services. Lastly, the organization might opt to use any existing compatible equipment as the replacement for damaged equipment. This option includes borrowing equipment from alternative sites.

Plan testing, training, and exercising

Once the contingency plan has been developed, it needs to be tested so as to identify the deficiencies that it may have. Testing also needs to be done to evaluate the readiness of employees to implement the plan when a disaster happens. Tests of contingency plans must focus on the speed of recovery from backups and alternative sites, the collaboration between recovery personnel, the performance of recovered systems on alternative sites, and the ease of restoring normal operations. Testing should be done in a worst-case scenario and should be conducted through classroom exercises or functional exercises.

Classroom exercises are the least costly, as the employees are mostly walked through the recovery operations in class before doing a practical exercise.

Functional exercises, on the other hand, are more demanding and require a disaster to be mimicked and the staff to be taught practically how they can respond.

Theoretical training is used to supplement practical training and reinforce what the employees learned during the exercises. Training should be conducted annually at the very least.

Plan maintenance

The contingency plan needs to be maintained in an adequate state so that it can respond to an organization's current risks, requirements, organization structure, and policies. Therefore, it should keep on being updated to reflect the changes made by an organization or changes in the threat landscape. The plan needs to be reviewed regularly and updated if necessary, and the updates should be documented. The review should be done at least annually and all the changes noted should be effected within a short period of time. This is to prevent the occurrence of a disaster that the organization is not yet prepared for.

Best practices for recovery

The aforementioned processes that form part of the disaster recovery plan can achieve better results if certain best practices are followed. One of these is having an offsite location to store archived backups. The cloud is a ready solution for safe off-site storage.

Another practice is to keep recording any changes made to the IT infrastructure to ease the process of reviewing the suitability of the contingency plan against the new systems. It is also good to have proactive monitoring of IT systems so as to determine when a disaster is occurring early enough and to start the recovery process. Organizations should also implement fault-tolerant systems that can withstand a certain degree of exposure to a disaster. Implementing a **redundant array of independent disks** (**RAID**) for servers is one way of achieving redundancy. It is also good to test the integrity of the backups that are made to ensure that they have no errors. It would be disappointing for an organization to realize after a disaster that its backups have errors and are useless. Lastly, the organization should regularly test its process of restoring a system from backups. All the IT staff need to be fully knowledgeable about this.

References

1. C. Bradbury, *DISASTER! Creating and testing an effective Recovery Plan*, Manager, pp. 14-16, 2008. Available: `https://search.proquest.com/docview/224614625?accountid=45049`.
2. B. Krousliss, *Disaster recovery planning, Catalog Age,* vol. 10, *(12),* pp. 98, 2007. Available: `https://search.proquest.com/docview/200632307?accountid=45049`.

2. S. Drill, *Assume the Worst In IT Disaster Recovery Plan, National Underwriter.P & C,* vol. 109, *(8),* pp. 14-15, 2005. Available: `https://search.proquest.com/docview/228593444?accountid=45049`.
3. M. Newton, *LINUX TIPS, PC World,* pp. 150, 2005. Available: `https://search.proquest.com/docview/231369196?accountid=45049`.
4. Y. Mitome and K. D. Speer, "Embracing disaster with contingency planning," *Risk Management,* vol. 48, *(5),* pp. 18-20, 2008. Available: `https://search.proquest.com/docview/227019730?accountid=45049`.
5. J. Dow, "Planning for Backup and Recovery," *Computer Technology Review,* vol. 24, *(3),* pp. 20-21, 2004. Available: `https://search.proquest.com/docview/220621943?accountid=45049`.
6. E. Jordan, *IT contingency planning: management roles, Information Management & Computer Security,* vol. 7, *(5),* pp. 232-238, 1999. Available: `https://search.proquest.com/docview/212366086?accountid=45049`.

Summary

In this chapter, we have discussed ways in which organizations prepare to ensure business continuity during disasters. We have talked about the disaster recovery planning process. We have highlighted what needs to be done to identify the risks faced, prioritize the critical resources to be recovered, and determine the most appropriate recovery strategies. In this chapter, we have also discussed the live recovery of systems while they remain online. We have focused a lot on contingency planning, and discussed the entire contingency planning process, touching on how a reliable contingency plan needs to be developed, tested, and maintained.

Lastly, in this chapter, we have provided some best practices that can be used in the recovery process to achieve optimal results.

This chapter brings to a conclusion the discussion about the attack strategies used by cybercriminals and the vulnerability management and disaster recovery measures that targets can employ.

15
Vulnerability Management

In the previous chapters, you learned about the recovery process and how important it is to have a good recovery strategy and the appropriate tools in place. Oftentimes, an exploitation of a vulnerability might lead to a disaster recovery scenario. Therefore, it is imperative to have a system in place that can prevent the vulnerabilities from being exploited in the first place. But how can you prevent a vulnerability from being exploited if you don't know whether your system is vulnerable? The answer is to have a vulnerability management process in place that can be used to identify vulnerabilities and help you mitigate them. This chapter focuses on the mechanisms that organizations and individuals need to put in place to make it hard to be hacked. It might be impossible for a system to be 100% safe and secure; however, there are some measures that can be employed to make it difficult for hackers to complete their missions.

This chapter will cover the following topics:

- Creating a vulnerability management strategy
- Vulnerability management tools
- Implementing vulnerability management
- Best practices for vulnerability management

Creating a vulnerability management strategy

The optimal approach to creating an effective vulnerability management strategy is to make it a vulnerability management life cycle. Just like the attack life cycle, the vulnerability management life cycle schedules all vulnerability mitigation processes in an orderly way. This enables targets and victims of cybersecurity incidents to mitigate the damage that they have incurred or might incur. The right counteractions are scheduled to be performed at the right time to find and address vulnerabilities before attackers can abuse them.

The vulnerability management strategy is composed of six distinct phases. This section will discuss each of them and what they are meant to protect against. It will also discuss the challenges that are expected to be met at each of those stages.

Asset inventory

The first stage in the vulnerability management strategy should be the making of an inventory. However, many organizations lack an effective asset register and, therefore, have a hard time when securing their devices. An asset inventory is a tool that security administrators can use to go through the devices an organization has and highlight the ones that need to be covered by security software. In the vulnerability management strategy, an organization should start by giving one employee the responsibility of managing an asset inventory to ensure that all devices are recorded and that the inventory remains up to date (1). The asset inventory is also a great tool that network and system admins can use to quickly find and patch devices and systems.

Without the inventory, some devices could be left behind when new security software is being patched or installed. These are the devices and systems that attackers will target. There are hacking tools, as was seen in `Chapter 5`, *Compromising the System*, that can scan the network and find out which systems are unpatched. The lack of an asset inventory may also lead to the organization underspending or overspending on security. This is because it cannot correctly determine the devices and systems that it needs to purchase protection for. The challenges that are expected at this stage are many. IT departments in today's organizations are often faced with poor change management, rogue servers, and a lack of clear network boundaries. Organizations also lack effective tools for maintaining the inventory in a consistent manner.

Information management

The second stage in the vulnerability management strategy is controlling how information flows into an organization. The most critical information flow is internet traffic coming from an organization's network. There has been an increase in the number of worms, viruses and other malware threats that organizations need to guard against. There has also been an increase in the traffic flow both inside and outside of local networks. The increased traffic flow threatens to bring more malware into an organization. Therefore, attention should be paid to this information flow to prevent threats from getting in or out of a network. Other than the threat of malware, information management is also concerned with the organization's data. Organizations store different types of data, and some of it must never get into the hands of the wrong people. Information, such as trade secrets and the personal information of customers, could cause irreparable damage if it is accessed by hackers. An organization may lose its reputation, and could also be fined huge sums of money for failing to protect user data. Competing organizations could get secret formulas, prototypes, and business secrets, allowing them to outshine the victim organization. Therefore, information management is vital in the vulnerability management strategy.

In order to achieve this, an organization could deploy a **computer security incident response team** (**CSIRT**) to handle any threats to its information storage and transmission (2). Said team will not just respond to hacking incidents but will inform management when there are intrusion attempts to access sensitive information and the best course of action to take. Apart from this team, an organization could adopt the policy of least privilege when it comes to accessing information. This policy ensures that users are denied access to all information apart from that which is necessary for them to perform their duties. Reducing the number of people accessing sensitive information is a good measure towards reducing the avenues of attack (2). Lastly, in the information management strategy, organizations could put in place mechanisms to detect and stop malicious people from gaining access to files. These mechanisms can be put in place in the network to ensure that malicious traffic is denied entry and suspicious activities such as snooping are reported. They could also be put in place on end user devices to prevent the illegal copying or reading of data.

There are a few challenges in this step of the vulnerability management strategy. To begin with, over the years information has grown in breadth and depth, making it hard to handle and also to control who can access it. Valuable information about potential hackings, such as alerts, has also exceeded the processing capabilities of most IT departments. It is not a surprise for legitimate alerts to be brushed off as false positives because of the number of similar alerts that the IT department receives daily.

There have been incidents where organizations have been exploited shortly after ignoring alerts from network monitoring tools. The IT department is not entirely to blame as there is a huge amount of new information that such tools are generating per hour, most of which turn out to be false positives. Traffic flowing in and out of organizational networks has also become complex. Malware is being transmitted in nonconventional ways. There is also a challenge when it comes to conveying information about new vulnerabilities to normal users who do not understand technical IT jargon. All these challenges together affect the response times and actions that an organization can take in the case of potential or verified hacking attempts.

Risk assessment

This is the third step in the vulnerability management strategy. Before risks can be mitigated, the security team should do an in-depth analysis of the vulnerabilities that it faces. In an ideal IT environment, the security team would be able to respond to all vulnerabilities since it would have sufficient resources and time. However, in reality, there are a great many limiting factors when it comes to the resources available to mitigate risks. That is why risk assessment is crucial. In this step, an organization has to prioritize some vulnerabilities over others and allocate resources to mitigate against them. Risk assessment is comprised of five stages.

Scope

Risk assessment starts with scope identification. An organization's security team only has a limited budget. It, therefore, has to identify areas that it will cover and those that it will not. It determines what will be protected, its sensitivity, and to what level it needs to be protected. The scope needs to be defined carefully since it will determine from where internal and external vulnerability analysis will occur.

Collecting data

After the scope has been defined, data needs to be collected about the existing policies and procedures that are in place to safeguard the organization from cyber threats. This can be done through interviews, questionnaires, and surveys administered to personnel, such as users and network administrators. All the networks, applications, and systems that are covered in the scope should have their relevant data collected. This data could include the following: service pack, OS version, applications running, location, access control permissions, intrusion-detection tests, firewall tests, network surveys, and port scans. This information will shed more light on the type of threats that the networks, systems, and applications are facing.

Analysis of policies and procedures

Organizations set up policies and procedures to govern the usage of their resources. They ensure that they are put to rightful and safe use. It is therefore important to review and analyze the existing policies and procedures. There could be inadequacies in the policies. There could also be impracticalities in some policies. While analyzing the policies and procedures, one should also determine their level of compliance on the part of the users and administrators. Simply because the policies and procedures are formulated and disseminated do not mean that they are complied with. The punishments set for noncompliance should also be analyzed. In the end, it will be known whether an organization has sufficient policies and procedures to address vulnerabilities.

Vulnerability analysis

After the analysis of the policies and procedures, vulnerability analysis has to be done in order to determine the exposure of the organization and to find out whether there are enough safeguards to protect itself. Vulnerability analysis is done using the tools that were discussed in `Chapter 4`, *Reconnaissance*. The tools used here are the same tools that hackers use to determine an organization's vulnerabilities so that they can decide which exploits to use. Commonly, organizations will call in penetration testers to conduct this process. The biggest setback in vulnerability analysis is the number of false positives that are identified that need to be filtered out. Therefore, various tools have to be used together in order to come up with a reliable list of the existing vulnerabilities in an organization.

The penetration testers need to simulate real attacks and find out the systems and devices that suffer stress and get compromised in the process. At the end of this, the vulnerabilities identified are graded according to the risks that they pose to the organization. Vulnerabilities that have less severity and exposure usually have low ratings. There are three classes in a vulnerability grading system. The minor class is for vulnerabilities that require lots of resources to exploit, yet have a very little impact on the organization. The moderate class is for those vulnerabilities that have moderate potential for damage, exploitability, and exposure. The high-severity class is for vulnerabilities that require fewer resources to exploit but can do lots of damage to an organization if they are.

Threat analysis

Threats to an organization are actions, code, or software that could lead to the tampering, destruction, or interruption of data and services in an organization. Threat analysis is done to look at the risks that could happen in an organization. The threats identified must be analyzed in order to determine their effects on an organization. Threats are graded in a similar manner to vulnerabilities but are measured in terms of motivation and capability. For instance, an insider may have low motivation to maliciously attack an organization but could have lots of capabilities because of the inside knowledge of the workings of the organization. Therefore, the grading system may have some differences to the one used in the vulnerability analysis. In the end, the threats identified are quantified and graded.

Analysis of acceptable risks

The analysis of the acceptable risks is the last thing done in risk assessment. Here, the existing policies, procedures, and security mechanisms are first assessed to determine whether they are adequate. If they are inadequate, it is assumed that there are vulnerabilities in the organization. The corrective actions are taken to ensure that they are updated and upgraded until they are sufficient. Therefore, the IT department will determine the recommended standards that the safeguards should meet. Whatever is not covered is categorized as an acceptable risk. These risks might, however, become more harmful with time, and therefore they have to be analyzed. It is only after it is determined that they will pose no threat that the risk assessment will end. If they might pose a threat, safeguard standards are updated to address them.

The biggest challenge in this vulnerability management stage is the lack of availability of information. Some organizations do not document their policies, procedures, strategies, processes, and security assets. It might, therefore, be difficult to obtain the information needed in order to complete this stage. It might be easier for small and medium-sized companies to keep documentation of everything, but it is a complex task for big companies. Big companies have multiple lines of business, departments, a lack of enough resources, a lack of disciplined documentation, and overlapping duties. The only solution to ready them for this process is by conducting regular housekeeping activities to ensure that everything important is documented and that staff clearly understand their duties.

Vulnerability assessment

Vulnerability assessment closely follows risk assessment in the vulnerability management strategy. This is because the two steps are closely related. Vulnerability assessment involves the identification of vulnerable assets. This phase is conducted through a number of ethical hacking attempts and penetration tests. The servers, printers, workstations, firewalls, routers, and switches on the organizational network are all targeted with these attacks. The aim is to simulate a real hacking scenario with the same tools and techniques that a potential attacker might use. The majority of these tools were discussed in the reconnaissance and compromising the system chapters. The goal in this step is not only to identify the vulnerabilities but also to do so in a fast and accurate manner. The step should yield a comprehensive report of all the vulnerabilities that an organization is exposed to.

The challenges faced in this step are many. The first one to consider should concern what the organization should assess. Without an appropriate asset inventory, an organization will not be able to identify which devices they should focus on. It will also become easy to forget to assess certain hosts, and yet they may be key targets for potential attack. Another challenge has to do with the vulnerability scanners used. Some scanners provide false assessment reports and guide the organization down the wrong path. Of course, false positives will always exist, but some scanning tools exceed the acceptable percentage and keep on coming up with nonexistent vulnerabilities. These may lead to the wasting of the organization's resources when it comes to mitigations. Disruptions are another set of challenges that are experienced at this stage. With all the ethical hacking and penetration-testing activities going on, the network, servers, and workstations suffer. Networking equipment such as firewalls also get sluggish, especially when denial of service attacks are being carried out.

Sometimes, strong attacks will actually bring down servers, disrupting core functions of the organization. This can be addressed by conducting these tests when there are no users using them, or coming up with replacements when core tools are being assessed. There is also the challenge of using the tools themselves. Tools such as Metasploit require you to have a solid understanding of Linux and be experienced with using command-line interfaces. The same is true for many other scanning tools. It is difficult to find scanning tools that offer a good interface and at the same time offer the flexibility of writing custom scripts. Lastly, sometimes scanning tools do not come with a decent reporting feature, and this forces the penetration testers to manually write these reports. Their reports may not be as thorough as those that would have been generated directly by the scanning tools.

Reporting and remediation tracking

After the vulnerability assessment comes to the reporting and remediation stage. This phase has two equally important tasks: reporting and remediation. The task of reporting helps the system admins to understand the organization's current state of security and the areas in which it is still insecure, and it points these out to the person responsible. Reporting also gives something tangible to the management so that they can associate it with the future direction of the organization. Reporting normally comes before remediation so that all the information compiled in the vulnerability management phase can seamlessly flow to this phase.

Remediation starts the actual process of ending the cycle of vulnerability management. The vulnerability management phase, as was discussed, comes to a premature ending after analyzing the threats and vulnerabilities as well as outlining the acceptable risks. Remediation compliments this by coming up with solutions to the threats and vulnerabilities identified. All the vulnerable hosts, servers, and networking equipment are tracked down and the necessary steps are established to remove the vulnerabilities as well as protect them from future exploits. It is the most important task in the vulnerability management strategy, and if it is well executed, the vulnerability management is deemed to be a success. Activities in this task include identifying missing patches and checking for available upgrades to all systems in an organization. Solutions are also identified for the bugs that were picked up by scanning tools. Multiple layers of security, such as antivirus programs and firewalls, are also identified at this stage. If this phase is unsuccessful, it makes the whole vulnerability management process pointless.

As expected, this phase sees a coming together of a great many challenges since it is the phase where all vulnerabilities have their solutions identified. The first challenge arises when reporting is partial and does not contain all the required information about the risks that the organization faces. A poorly written report may lead to poor remediation measures and thus leave the organization still exposed to threats. The lack of software documentation may also bring about challenges in this phase. The vendors or manufacturers of software often leave documentation that includes an explanation of how updating is to be done. Without it, it may prove hard to update bespoke software. Poor communication between software vendors and the organization may also bring about challenges when the patching of a system needs to be done. Lastly, remediation can be compromised by the lack of cooperation of the end users. Remediation may introduce downtimes to end users, something that they never want to experience.

Response planning

Response planning can be thought of as the easiest, but nevertheless a very important, step in the vulnerability management strategy. It is easy because all the hard work will have been done in the previous five steps. It is important because, without its execution, the organization will still be exposed to threats. All that matters in this phase is the speed of execution. Large organizations face major hurdles when it comes to executing it because of a large number of devices that require patches and upgrades.

An incident happened when Microsoft announced the existence of the MS03-023 and released a patch for it. Smaller organizations that have short response plans were able to patch their operating systems with an update shortly after the announcement. However, larger organizations that either lacked or have long response plans for their computers were heavily attacked by hackers. Hackers released the MS Blaster worm to attack the unpatched operating systems barely 26 days after Microsoft gave a working patch to its users. That was enough time for even big companies to patch their systems in totality. However, the lack of response plans or the use of long response plans caused some to fall victim to the worm. The worm caused network sluggishness or outage on the computers it infected. Another famous incident that happened quite recently was that of the WannaCry ransomware. It is the largest ever ransomware attack in history caused by a vulnerability allegedly stolen from the NSA called **Eternal Blue** (3). The attack started in May, but Microsoft had released a patch for the Eternal Blue vulnerability in March. However, it did not release a patch for older versions of Windows, such as XP (3). From March until the day the first attack was recognized, there was enough time for companies to patch their systems. However, most companies had not done so by the time the attack started because of poor response planning. If the attack had not been stopped, even more computers would have fallen victim.

This shows just how important speed is when it comes to response planning. Patches are to be installed the moment that they are made available.

The challenges faced in this phase are many since it involves the actual engagement of end users and their machines. The first of these challenges is getting the appropriate communications out to the right people in time. When a patch is released, hackers are never slow in trying to find ways to compromise the organizations that do not install it. That is why a well-established communication chain is important. Another challenge is accountability. The organization needs to know who to hold accountable for not installing patches. At times, users may be responsible for canceling installations. In other instances, it may be the IT team that did not initiate the patching process in time. There should always be an individual that can be held accountable for not installing patches. The last challenge is the duplication of efforts. This normally occurs in large organizations where there are many IT security personnel. They may use the same response plan, but because of poor communication, they may end up duplicating each other's efforts while making very little progress.

Vulnerability management tools

The available vulnerability management tools are many, and for the sake of simplicity, this section will discuss the tools according to the phase that they are used in. Therefore, each phase will have its relevant tools discussed and their pros and cons given. It is worth noting that not all the tools discussed may deal with the vulnerabilities themselves. Their contributions are, however, very important to the whole process.

Asset inventory tools

The asset inventory phase is aimed at recording the computing assets that an organization has so as to ease their tracking when it comes to performing updates. The following are some of the tools that can be used in this phase.

Peregrine tools

Peregrine is a software development company that was acquired by HP in 2005. It has released three of the most commonly used asset inventory tools. One of these is the asset center. It is an asset management tool that is specifically fine-tuned to meet the needs of software assets. The tool allows organizations to store licensing information about their software. This is an important piece of information that many other asset inventory systems leave out. This tool can only record information about the devices and software in the organization. However, sometimes there is a need for something that can record details about the network. Peregrine created other inventory tools specifically designed for recording assets on a network. These are the network discovery and desktop inventory tools that are commonly used together. They keep an updated database of all computers and devices connected to an organization's network. They can also provide extensive details about a network, its physical topology, the configurations of the connected computers, and their licensing information. All these tools are provided to the organization under one interface. Peregrine tools are scalable, they easily integrate, and are flexible enough to cater for changes in a network. Their disadvantage shows itself when there are rogue desktop clients in a network since the tools will normally ignore them.

LANDesk Management Suite

The LANDesk Management Suite is a vigorous asset inventory tool that is commonly used for network management (4). The tool can provide asset management, software distribution, license monitoring, and remote-based control functionalities over devices connected to the organizational network (4). The tool has an automated network discovery system that identifies new devices connected to the network. It then checks against the devices that it has in its database and adds the new devices if they have never been added. The tool also uses inventory scans running in the background on clients, and this enables it to know information specific to the client, such as license information (4). The tool is highly scalable and gives users a portable backend database. The cons of this tool are that it cannot be integrated with other tools used in command centers and that it also faces the challenge of locating rogue desktops.

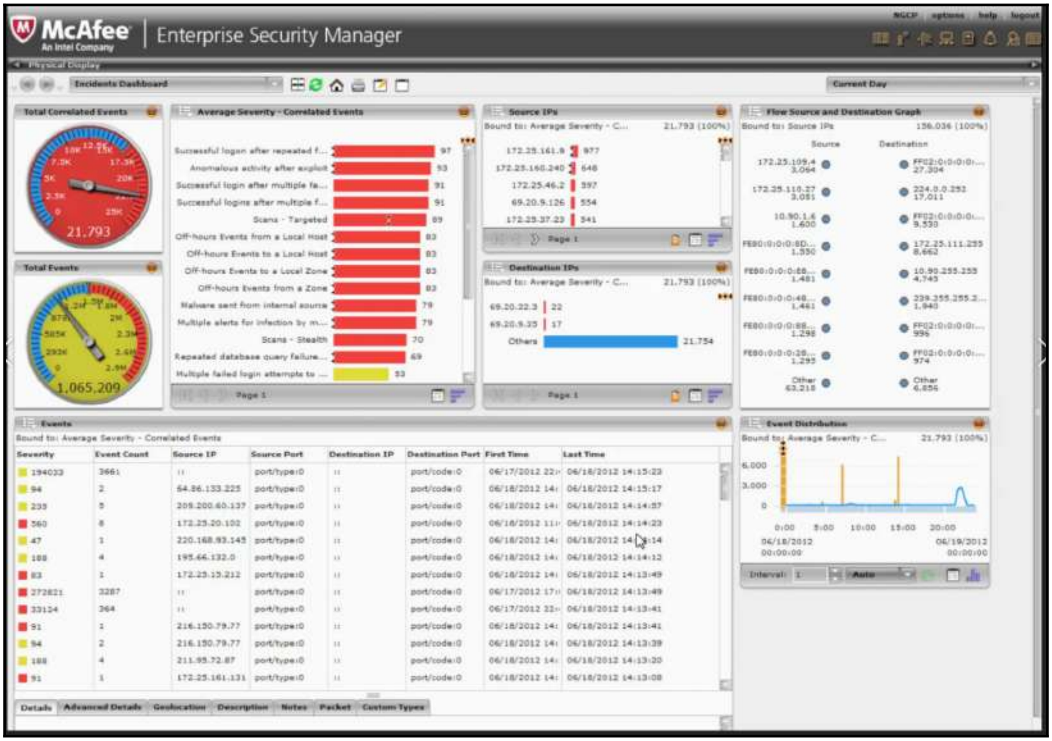
StillSecure

This is a suite of tools created by Latis Networks that provide network discovery functionalities to users (5). The suite comes with three tools tailored for vulnerability management—namely desktop VAM, server VAM, and remote VAM. These three products run in an automated way where they scan and provide a holistic report about a network. The scanning times can also be manually set according to the user's schedule to avoid any network sluggishness that may arise because of the scanning processes. The tools will document all the hosts in a network and list their configurations. The tools will also show the relevant vulnerability scans to be run on each host. This is because the suite is specifically created for vulnerability assessment and management.

The main advantage of this tool is that it scans and records hosts on a network without requiring the installation of a client version on them, like the previously discussed tools. The suite's remote VAM can be used to discover devices running on the perimeter of an internal network from the outside. This is a major advantage when compared to the other inventory tools that have been previously discussed. The suite gives users an option to group the inventory by different business units or through the normal system administrator's sorting methods. The main con of this suite is that, since it does not install a client on the hosts it limits, it is unable to collect in-depth information about them. The main aim of an asset inventory tool is to capture all the relevant information about the devices in an organization, and this suite may at times fail to provide this quality of data.

Foundstone's Enterprise

Foundstone's Enterprise is a tool by Foundscan Engine that performs network discovery using IP addresses. The tool is normally set up by the network administrator to scan for hosts assigned a certain range of IP addresses. The tool can be set to run at scheduled times that the organization deems to be most appropriate. The tool has an enterprise web interface where it lists the hosts and services it has found running on the network. The tool is also said to scan intelligently for vulnerabilities that the hosts may have and give periodic reports to the network admin. However, the tool is seen as falling short of being the ideal asset inventory tool since it only collects data related to vulnerability scanning:


McAfee
An Intel Company
Enterprise Security Manager
Incidents Dashboard
Current Day
Total Correlated Events
21,793
Total Events
1,065,209
Average Severity - Correlated Events
Successful logon after repeated f... 97
Anomalous activity after exploit 93
Successful login after multiple fa... 91
Successful logins after multiple f... 91
Scans - Targeted 89
Off-hours Events from a Local Host 83
Off-hours Events to a Local Host 83
Off-hours Events to a Local Zone 83
Off-hours Events from a Zone 83
Malware sent from internal source 79
Multiple alerts for infection by m... 79
Scans - Stealth 70
Repeated database query failure... 69
Multiple failed login attempts to ... 53
Page 1
Source IPs
Destination IPs
Others 21,754
Flow Source and Destination Graph
Source
Destination
Event Distribution
Interval
Auto

Events

Bound to: Average Severity - Correlated Events

Severity	Event Count	Source IP	Source Port	Destination IP	Destination Port	First Time	Last Time
🟨 194033	3661	::	port/type:0	::	port/code:0	06/17/2012 22:	06/18/2012 14:15:23
🟨 94	2	64.86.133.225	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:15:17
🟨 233	5	209.200.60.137	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:14:57
🟥 360	8	172.25.20.102	port/type:0	::	port/code:0	06/18/2012 11:	06/18/2012 14:14:23
🟨 47	1	220.168.93.145	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:14:14
🟨 188	4	195.66.132.0	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:14:12
🟥 83	1	172.25.15.212	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:13:49
🟥 272821	3287	::	port/type:0	::	port/code:0	06/17/2012 17:	06/18/2012 14:13:49
🟥 33124	364	::	port/type:0	::	port/code:0	06/17/2012 22:	06/18/2012 14:13:41
🟥 91	1	216.150.79.77	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:13:41
🟨 94	2	216.150.79.77	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:13:39
🟨 188	4	211.95.72.87	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:13:20
🟥 91	1	172.25.161.131	port/type:0	::	port/code:0	06/18/2012 14:	06/18/2012 14:13:08

Information management tools

The information management phase concerns the control of the information flow in the organization. This includes the dissemination of information about intrusions and intruders to the right people who can take the recommended actions. There are a number of tools that offer solutions to help with the dissemination of information in organizations. They use simple communication methods such as emails, websites, and distribution lists. Of course, all of these are customized to fit an organization's security incident policies. During security incidents, the first people that have to be informed are those in the incident response team. This is because their speed of action may determine the impacts that security vulnerabilities have in an organization. Most of the tools that can be used to reach them are web-based. One of these tools is the CERT Coordination Center. It facilitates the creation of an online command center that alerts and periodically informs a select number of people via email (6). Another tool is Security Focus, which uses a similar strategy as the CERT tool (7). It creates mailing lists to inform the incident response team when a security incident has been reported.

Symantec Security Response is also another information-management tool (8). There are many advantages of this tool, one of which is that it keeps the incident response team informed. Symantec is renowned globally for its in-depth internet security threat reports. These annual publications are great for learning how cybercriminals are evolving each year. The report also gives meaningful attack statistics. This allows the incident response teams to adequately prepare for certain types of attacks based on the observable trends. As well as this publication, the tool also provides you with the Shadow Data Report, Symantec Intelligence Report, and security white papers (8). The tool also provides threat spotlights for some types of attacks that organizations must prevent. It also has an intelligent system called **DeepSight** that provides 24-7 reporting (8). IT has an A-to-Z listing of risks and threats together with their countermeasures. Finally, the tool provides users with links to Symantec AntiVirus, which can be used to remove malware and treat infected systems. This tool is well-rounded in information management and is, therefore, highly recommendable.

These tools are the most commonly used out of the many available on the internet. The most obvious similarity in all these tools is the use of email alerts through mailing lists. The mailing lists can be set up so that incident responders get the alerts first, and once they have verified a security incident, the rest of the users in an organization can be informed. Organizational security policies are at times good tools that complement these online tools. During an attack, the local security policies can guide users as to what they can do and who they should contact.

Risk assessment tools

Most risk assessment tools are developed in-house since all organizations do not face the same risks at the same time. There are many variations in risk management, and that is why it might be tricky to use only one choice of software as the universal tool to identify and assess the risks that an organization users. The in-house tools that organizations use are checklists developed by the system and network administrators. The checklist should be made up of questions about potential vulnerabilities and threats that the organization is exposed to. These questions will be used by the organization to define the risk levels of the vulnerabilities identified within its network. The following is a set of questions that can be put on the checklist:

- How can the identified vulnerabilities impact the organization?
- Which business resources are at risk of being compromised?
- Is there a risk for remote exploitations?

- What are the consequences of an attack?
- Is the attack reliant on tools or scripts?
- How can the attack be mitigated?

To complement the checklist, organizations can acquire commercial tools that perform automated risk analysis. One of these tools is **ArcSight Enterprise Security Manager** (**ESM**). It is a threat-detection and compliance-management tool used to detect vulnerabilities and mitigate cybersecurity threats. The tool gathers a lot of security-related data from a network and the hosts connected to it. From the event data that it records, it can make real-time correlations with its database to tell when there are attacks or suspicious actions on the network. It can correlate a maximum of 75,000 events per second. This correlation can also be used to ensure that all events follow the internal rules of the organization. It also recommends methods of mitigating and resolving vulnerabilities.

Vulnerability assessment tools

Because of the increase in the number of cybersecurity threats that face organizations, there has been a corresponding growth in the number of vulnerability-scanning tools. There are many freeware and premium tools for organizations to choose from. Most of these tools were discussed in `Chapter 4`, *Reconnaissance* and `Chapter 5`, *Compromising the System*. The two most commonly used vulnerability scanners are Nessus and NMap (the latter of which can be used as a basic vulnerability tool via its scripting function). NMap is highly flexible and can be configured to address the specific scanning needs of the user. It quickly maps a new network and provides information about the assets connected to it and their vulnerabilities.

Nessus can be thought of as an advancement of the Nmap scanner. This is because Nessus can perform an in-depth vulnerability assessment of the hosts connected to a network (9). The scanner will be able to determine their operating systems versions, missing patches, and the relevant exploits that can be used against the system. The tool also sorts the vulnerabilities according to their threat levels. Nessus is also highly flexible such that its users can write their own attack scripts and use them against a wide range of hosts on the network (9). The tool has its own scripting language to facilitate this. It is a great feature since, as was stated when we discussed the challenges faced in this step, many scanners do not find the perfect balance between a good interface and a high level of flexibility. There are other related tools that can also be used for scannings, such as Harris STAT, Foundstone's Foundscan, and Zenmap. Their functionalities are, however, similar to those of both Nessus and Nmap.

Reporting and remediation tracking tools

This step of the vulnerability management strategy allows incident responders to come up with the appropriate ways to mitigate the risks and vulnerabilities faced by an organization. They need tools that can tell them the current security state of the organization and to track all the remediation efforts. There are many reporting tools, and organizations tend to prefer the ones that have in-depth reporting and can be customized for several audiences. There are many stakeholders in an organization and not all of them can understand technical jargon. At the same time, the IT department wants tools that can give them the technical details without any alterations. Therefore, the separation of audiences is important.

Two tools with such capabilities are Foundstone's Enterprise Manager and the Latis Reporting tool. They have similar functionalities: They both provide reporting features that can be customized to the different needs of users and other stakeholders. Foundstone's Enterprise Manager comes with a customizable dashboard. This dashboard enables its users to retrieve long-term reports and reports that are custom-made for specific people, operating systems, services, and regions. Different regions will affect the language of the report, and this is particularly useful for global companies. The reports generated by these tools will show vulnerability details and their frequency of occurrence.

The two tools also provide remediation-tracking functionalities. The Foundstone tool has an option to assign vulnerabilities to a specific system administrator or IT staff member (10). It can then track the remediation process using tickets. The Latis tool also has the option where it can assign certain vulnerabilities to certain people that are responsible for remedying them. It will also track the progress that the assigned parties make. Upon completion, the Latis tool will perform a validation scan to ascertain that the vulnerability was solved. Remediation tracking is normally aimed at ensuring that someone takes responsibility for addressing a certain vulnerability until it is resolved.

Response planning tools

Response planning is the step where most of the resolution, eradication, cleansing, and repair activities take place. Patches and system upgrades also occur at this stage. There are not many commercial tools made to facilitate this step. Mostly, response planning is done through documentation. Documentation helps system and network administrators with the patching and updating process for systems that they are not familiar with. It also helps during changeovers where new staff may be put in charge of systems that they have never used before. Lastly, documentation helps in emergency situations to avoid skipping some steps or making mistakes.

Implementation of vulnerability management

The implementation of vulnerability management follows the stipulated strategy. The implementation starts with the creation of an asset inventory. This serves as a register of all the hosts in a network and also of the software contained in them. At this stage, an organization has to give a certain IT staff member the task of keeping this inventory updated. The asset inventory at the very least should show the hardware and software assets owned by an organization and their relevant license details. As an optional addition, the inventory should also show the vulnerabilities present in any of these assets. An up-to-date register will come in handy when the organization has to respond to vulnerabilities with fixes to all its assets. The aforementioned tools can properly handle the tasks that are to be carried out at this stage.

After the implementation of the asset inventory, the organization should pay attention to information management. The goal should be the setting up of an effective way to get information about vulnerabilities and cybersecurity incidents to the relevant people within the shortest time possible. The right people to whom to send firsthand information about security incidents are the computer security incident response teams. The tools that were described as being capable of facilitating this stage require the creation of mailing lists. The incident response team members should be on the mailing list that receives the alerts from an organization's security monitoring tools.

There should be separate mailing lists created to allow other stakeholders of the organization to access this information once it has been confirmed. The appropriate actions that other stakeholders ought to take should also be communicated via the mailing lists. The most recommendable tool for this step, which is from Symantec, provides periodic publications to the users in an organization to keep them updated about global cybersecurity incidents. All in all, at the end of this stage, there should be an elaborate communication channel to incident responders and other users when there has been a breach of systems.

Following the implementation of mailing lists for information management, there should be a risk assessment. Risk assessment should be implemented in the manner described in the vulnerability management strategy. It should begin with the identification of the scope. It should be followed by the collection of data about the existing policies and procedures that the organization has been using. Data concerning their compliance should also be collected. After it is collected, the existing policies and procedures should be analyzed so as to determine whether they have been adequate in safeguarding the security of the organization. After this, vulnerability and threat analysis should be done. The threats and vulnerabilities that the organization faces should be categorized according to their severity. Lastly, the organization should define the acceptable risks that it can face without experiencing profound consequences.

The risk assessment should closely be followed by a vulnerability assessment. The vulnerability assessment step, not to be confused with vulnerability analysis of the risk management step, is aimed at identifying the vulnerable assets. Therefore, all the hosts in a network should be ethically hacked or have penetration testing done to determine whether or not they are vulnerable. The process should be thorough and accurate. Any vulnerable assets that are not identified in this step might be the weak link that hackers exploit. Therefore, tools that the supposed hackers would use to attack should be used and to the full extent of their capabilities.

The vulnerability assessment step should be followed by reporting and remediation tracking. All the risks and vulnerabilities identified must be reported back to the stakeholders of the organization. The reports should be comprehensive and touch on all hardware and software assets belonging to the organization. The reports should also be fine-tuned to meet the needs of various audiences. There are audiences that might not understand the technical side of vulnerabilities, and it is, therefore, only fair that they get a simplified version of the reports. Remediation tracking should follow the reports. After the risks and vulnerabilities that the organization faces are identified, the appropriate people to remedy them should be stated. They should be assigned the responsibility for ensuring that all the risks and vulnerabilities are resolved in totality. There should be an elaborate way of tracking the progress of the resolution of the identified threats. The tools that we looked at previously have these features and can ensure that this step is implemented successfully.

The final implementation should be response planning. This is where the organization outlines the actions to take against vulnerabilities and proceeds to take them. This step will confirm whether the preceding five steps were done right. In response planning, the organization should come up with a means of patching, updating, or upgrading the systems that were identified as possessing some risks or vulnerabilities. The hierarchy of severity identified in the risk and vulnerability assessment steps should be followed. This step should be implemented with the aid of the asset inventory so that the organization can confirm that all their assets both hardware and software, have been attended to. The step should not take long as hackers are never too far from attacking using the most recently discovered vulnerabilities. The response planning stage must be completed bearing in mind from when monitoring systems send alerts to incident responders.

Best practices for vulnerability management

Even with the best tools, execution is all that matters in vulnerability management. Therefore, all the actions that have been identified in the implementation section must be carried out flawlessly. There is a set of best practices for each step of the implementation of the vulnerability management strategy. Starting off with the asset inventory, the organization should establish a single point of authority. There should be one person that can be held responsible if the inventory is not up to date or has inconsistencies. Another best practice is to encourage the use of consistent abbreviations during data entry. It may become confusing to another person trying to go through the inventory if the abbreviations keep on changing. The inventory should also be validated at least once a year. Lastly, it is advisable to treat changes of inventory management systems with the same degree of care as any other change in a management process.

In the information management stage, the biggest achievement that the organization can get is a fast and effective dissemination of information to the relevant audience. One of the best methods for doing this is allowing employees to make the conscious effort of subscribing to mailing lists. Another one is to allow the incident response team to post its own reports, statistics, and advice on a website for the organization's users. The organization should also hold periodic conferences to discuss new vulnerabilities, virus strains, malicious activities, and social engineering techniques with users. It is best if all the users are informed about the threats that they may face and how to deal with them effectively. This has more impact than the mailing lists telling them to do technical things that they are not knowledgeable of. Lastly, the organization should come up with a standardized template of how all the security-related emails will look. It should be a consistent look that is different from the normal email format that users are used to.

The risk assessment step is one of the most manually demanding stages of the vulnerability management life cycle. This is because there are not many commercial tools that can be used here. One of the best practices is to document the ways to review new vulnerabilities as soon as they appear. This will save a lot of time when it comes to mitigating them since the appropriate countermeasures will already be known. Another best practice is to publish the risk ratings to the public or at least to the organizational users. That information may spread and ultimately reach a person that will find it more useful. It is also recommended that you ensure that asset inventories are both available and updated at this stage so that all hosts in a network can be combed through during risk analysis. The incident response team in every organization should also publish a matrix for each tool that the organization has deployed to secure itself. Lastly, the organization should ensure that it has a strict change management process that ensures that incoming staff are made aware of the security posture of the organization and the mechanisms in place to protect it.

The vulnerability assessment step is not so different from the risk assessment step, and therefore the two might borrow from each other's best practices (which we discussed previously). In addition to what has been discussed in risk assessment, it is good practice to seek permission before extensively testing the network. This is because we saw that this step might introduce serious disruptions to an organization and might do actual damage to the hosts. Therefore, a lot of planning ahead needs to happen. Another best practice is to create custom policies to specific environments—that is the different operating systems of the organization's hosts. Lastly, the organization should identify the scanning tools that are best for its hosts. Some methods may be overkill where they do too much scanning and to an unnecessary depth. Other tools are too shallow and do not discover the vulnerabilities in a network.

There are a few tips that may be used in the reporting and remediation tracking stage. One of these is to ensure that there is a reliable tool for sending reports to asset owners concerning the vulnerabilities they had and whether they have been fixed completely. This reduces the number of unnecessary emails received from users whose machines were found to contain vulnerabilities. The IT staff should also meet with management and other stakeholders to find out the type of reports that they want to see. The level of technicality should also be agreed upon. The incident response team should also agree with the management of the remediation time frames and the required resources, and make known the consequences of nonremediation. Lastly, remediation should be performed following the hierarchy of severity. Therefore, the vulnerabilities that pose the most risk should be sorted first.

The response planning step is the conclusion of the whole vulnerability management process. It is where the responses to different vulnerabilities are implemented. There are several best practices that can be used in this step. One of them is to ensure that the response plans are documented and well-known by the incident response team and the normal users. There should also be fast and accurate information flow to the normal users concerning the progress of fixing the vulnerabilities identified. Since there is a chance of failure after machines are updated or patches installed, contact information should be provided to the end users so that they can reach out to the IT team when such cases arise. Lastly, the incident response team should be given easy access to the network so that they can implement their fixes faster.

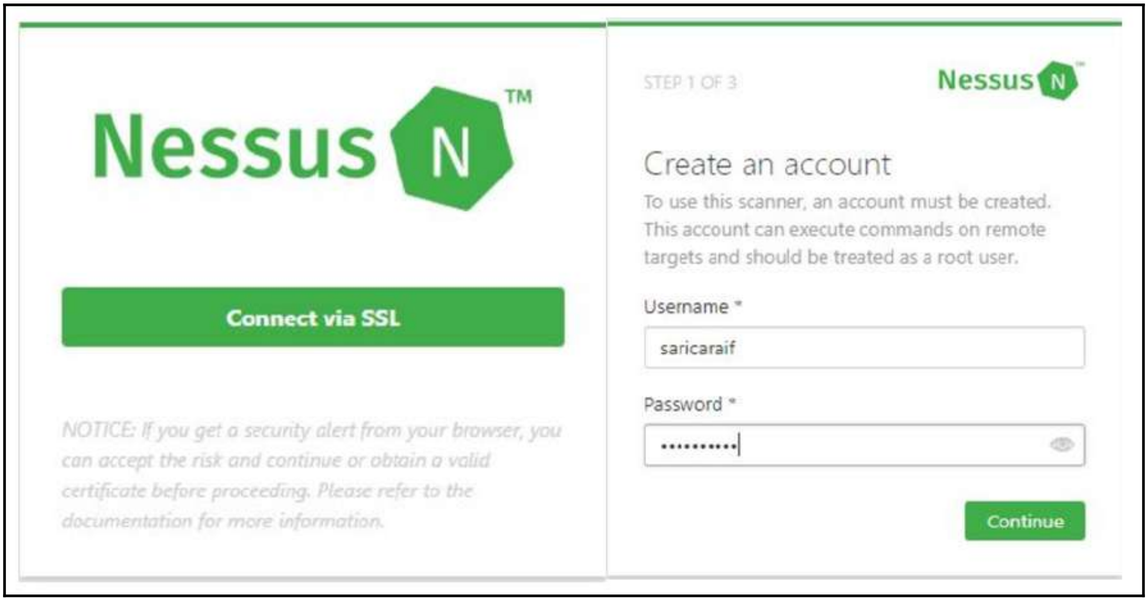
Implementing vulnerability management with Nessus

Nessus is one of the most popular commercial network vulnerability scanners developed by Tenable Network Security. It is designed to automate the testing and discovery of known vulnerabilities before a hacker takes advantage of them. It also suggests solutions for the vulnerabilities identified during the scan. The Nessus vulnerability scanner products are annual subscription-based products. Luckily, the home version is free of charge, and it also offers plenty of tools to help explore your home network.

Nessus has countless capabilities and is fairly complex. We will download the free home version, and cover only the basics of its setup and configuration, as well as creating a scan and reading the report. You can get the detailed installation and user manual from the Tenable website.

Download the latest version of Nessus (appropriate to your operating system) from its download page (`https://www.tenable.com/products/nessus/select-your-operating-system`). In our example, I downloaded 64-bit Microsoft Windows version `Nessus-7.0.0-x64.msi`. Just double-click on the downloaded executable installation file and follow the instructions along the way.

Nessus uses a web interface to set up, scan, and view reports. After the installation, Nessus will load a page in your web browser to establish the initial settings, as shown in *Figure 2*. Click on **Connect via SSL** icon. Your browser will display an error indicating that the connection is not trusted or is unsecured. For the first connection, accept the certificate to continue configuration. The next screen (*Figure 3*) will be about creating your user account for the Nessus server. Create your Nessus System Administrator account with a **Username *** and **Password *** that you will define, and will use in the future every time you log in and then click on the **Continue** button. On the third screen (*Figure 4*), choose Home, Professional or Manager from the drop-down menu:



NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

STEP 1 OF 3

Create an account

To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.

Username *

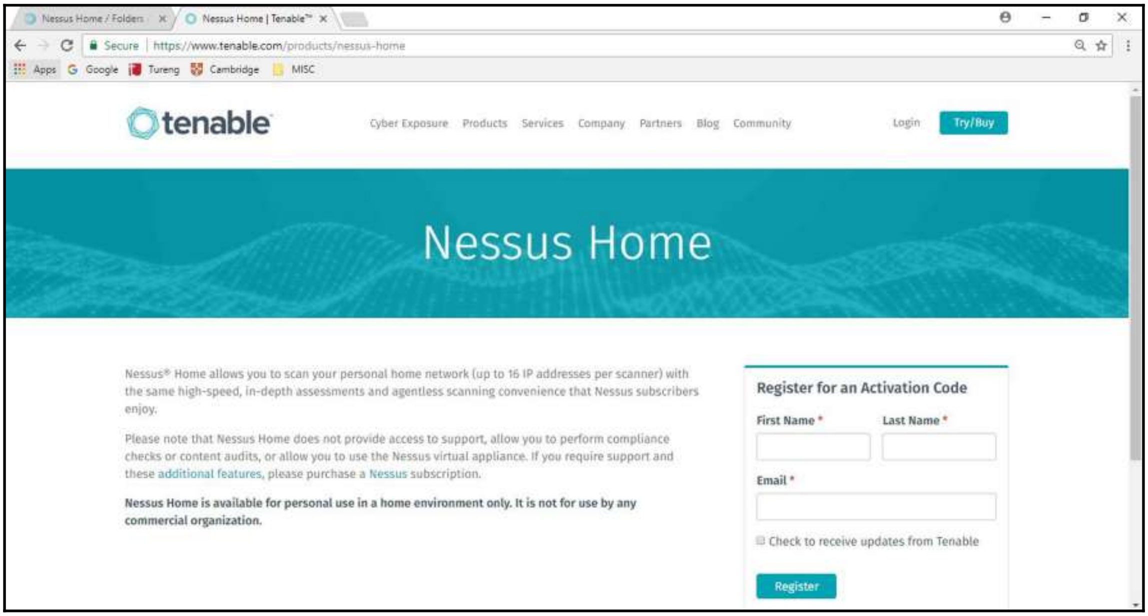
saricaraif

Password *

••••••••••

Figure 2 - Account creation

After that, go to `https://www.tenable.com/products/nessus-home` in a different tab and register for the activation code, as shown in *Figure 2*:



Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these additional features, please purchase a Nessus subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

Register for an Activation Code

First Name *

Last Name *

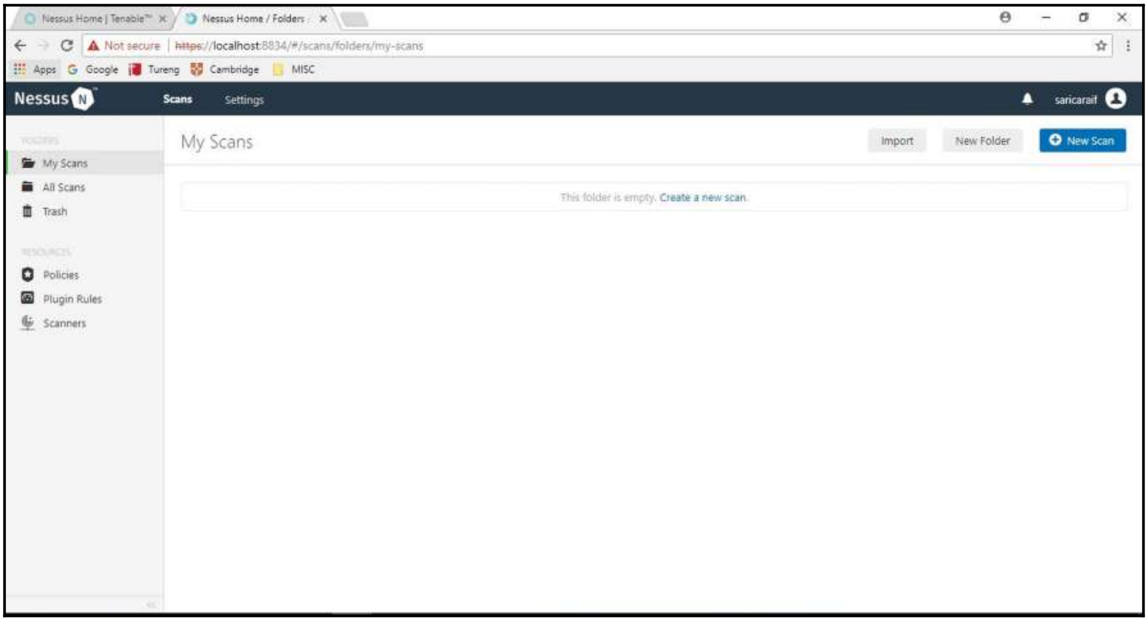
Email *

□ Check to receive updates from Tenable

Figure 3 - Registration and plugin installation

Your activation code will be sent to your email address. Type your activation code in the **Activation Code** box. After registration, Nessus will start downloading plugins from Tenable (*Figure* 2-2). This may take several minutes depending on your connection speed.

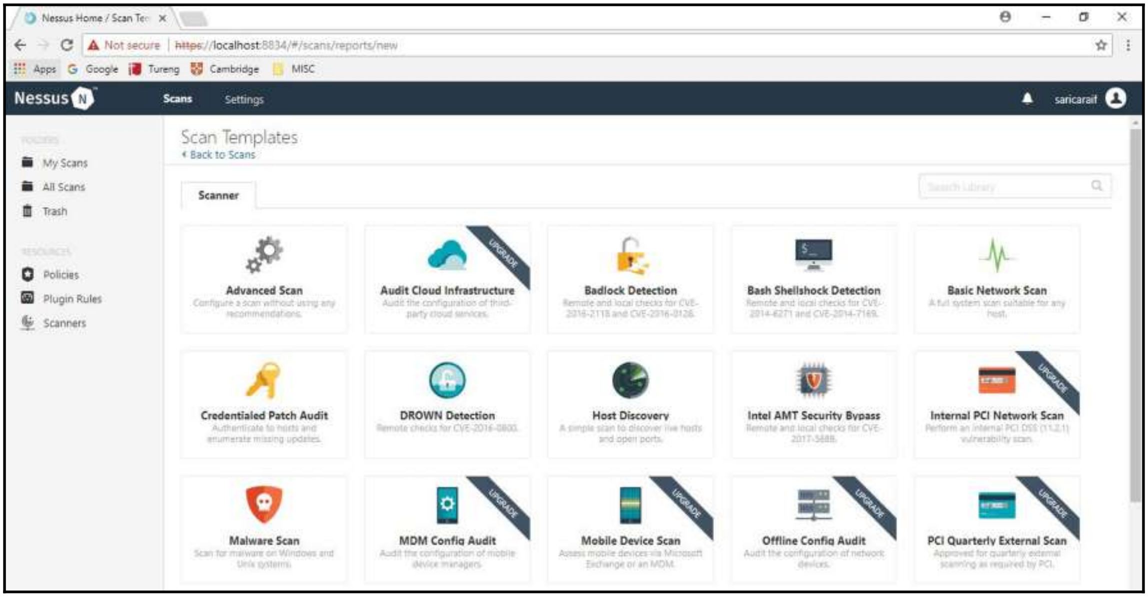
Once the plugins have been downloaded and compiled, the Nessus web UI will initialize and the Nessus server will start, as shown in F*igure 3*:



This folder is empty. Create a new scan.

Figure 4 - Nessus web UI

To create a scan, click on the **New Scan** icon in the upper-right corner. The **Scan Templates** page will appear, as shown in *Figure 5*:



Advanced Scan – Configure a scan without using any recommendations.

Audit Cloud Infrastructure – Audit the configuration of third-party cloud services.

Badlock Detection – Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection – Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan – A full system scan suitable for any host.

Credentialed Patch Audit – Authenticate to hosts and enumerate missing updates.

DROWN Detection – Remote checks for CVE-2016-0800.

Host Discovery – A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass – Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan – Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan – Scan for malware on Windows and Unix systems.

MDM Config Audit – Audit the configuration of mobile device managers.

Mobile Device Scan – Assess mobile devices via Microsoft Exchange or an MDM.

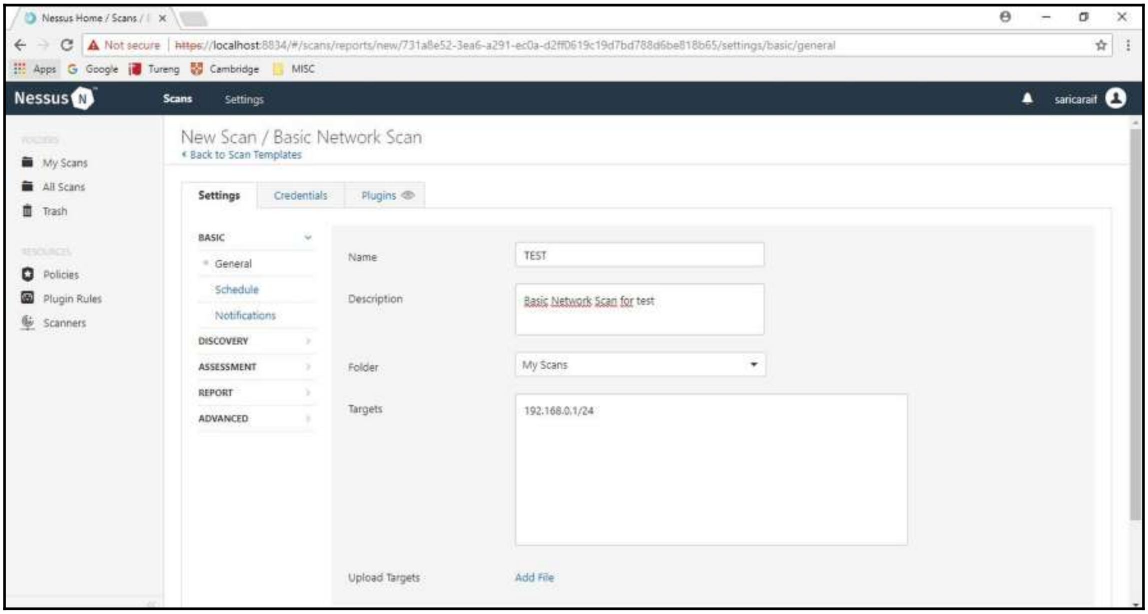
Offline Config Audit – Audit the configuration of network devices.

PCI Quarterly External Scan – Approved for quarterly external scanning as required by PCI.

Figure 5 - Scan Templates

You can choose any template listed on the **Scan Templates** page. We will choose **Basic Network Scan** for our test. The **Basic Network Scan** performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems. As you choose **Basic Network Scan**, the **Settings** page will be launched, as shown in *Figure 6*.

Name your scan "TEST" and add a description. Enter IP scanning details on your home network. Keep in mind that Nessus Home allows you to scan up to 16 IP addresses per scanner. Save the configuration and on the next screen, click the **Play** button to launch the scan. Depending on how many devices you have on your network, the scan will take a while.



New Scan / Basic Network Scan
‹ Back to Scan Templates

Name: TEST

Description: Basic Network Scan for test

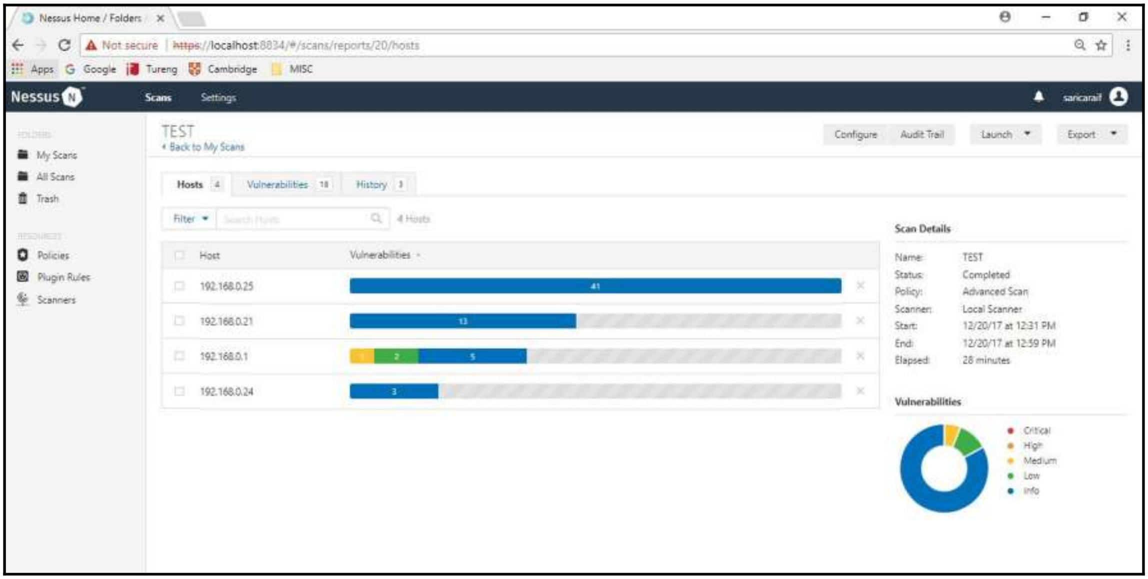
Folder: My Scans

Targets: 192.168.0.1/24

Upload Targets: Add File

Figure 6 - Scan Configuration

Once Nessus finishes scanning, click on the related scan; you'll see a bunch of color-coded graphs for each device on your network. Each color on the graph refers to different results, from information to the danger of a vulnerability, starting from the low level and ranging to critical. In *Figure 7*, we have three hosts (**192.168.0.25**, **192.168.0.1**, and **192.168.0.11**):



TEST

‹ Back to My Scans

Host	Vulnerabilities
192.168.0.25	41
192.168.0.21	13
192.168.0.1	1 2 5
192.168.0.24	3

Scan Details

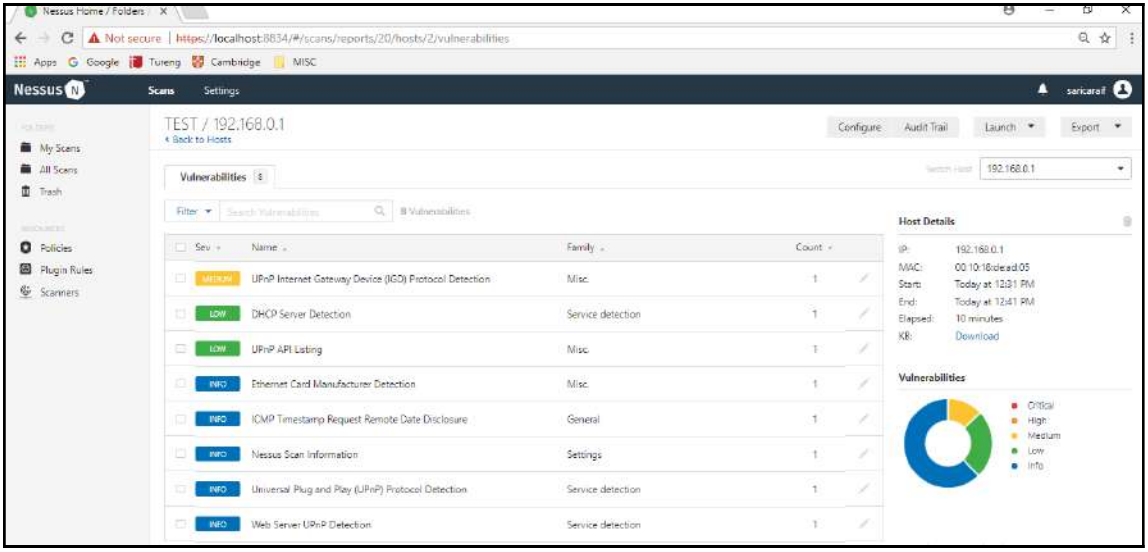
Name:	TEST
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	12/20/17 at 12:31 PM
End:	12/20/17 at 12:59 PM
Elapsed:	28 minutes

Vulnerabilities

Figure 7 - Test results

After the Nessus vulnerability scan, the results will be shown as displayed in *Figure 8*.

Click on any IP address to display the vulnerabilities found on the selected device, as shown in *Figure 9*. I chose **192.168.0.1** to see the details of the vulnerability scan:



TEST / 192.168.0.1

‹ Back to Hosts

Sev	Name	Family	Count
MEDIUM	UPnP Internet Gateway Device (IGD) Protocol Detection	Misc.	1
LOW	DHCP Server Detection	Service detection	1
LOW	UPnP API Listing	Misc.	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Universal Plug and Play (UPnP) Protocol Detection	Service detection	1
INFO	Web Server UPnP Detection	Service detection	1

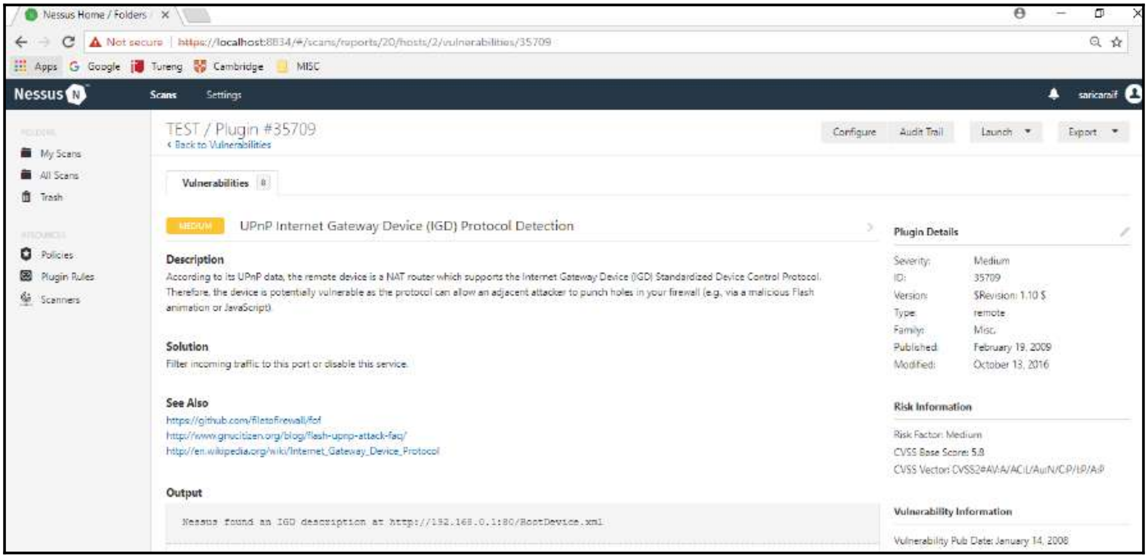
Host Details

IP:	192.168.0.1
MAC:	00:10:18:de:ad:05
Start:	Today at 12:31 PM
End:	Today at 12:41 PM
Elapsed:	10 minutes
KB:	Download

Vulnerabilities

Figure 8 - Vulnerabilities

When an individual vulnerability is selected, it displays more details of that particular vulnerability. My **UPnP Internet Gateway Device (IGD) Protocol Detection** vulnerability is shown in *Figure 9*. It gives lots of information about related details, such as the **Description**, **Solution**, **Plugin Details**, **Risk Information**, and **Vulnerability Information**:



TEST / Plugin #35709

‹ Back to Vulnerabilities

UPnP Internet Gateway Device (IGD) Protocol Detection

Description

According to its UPnP data, the remote device is a NAT router which supports the Internet Gateway Device (IGD) Standardized Device Control Protocol. Therefore, the device is potentially vulnerable as the protocol can allow an adjacent attacker to punch holes in your firewall (e.g. via a malicious Flash animation or JavaScript).

Solution

Filter incoming traffic to this port or disable this service.

See Also

https://github.com/filetofirewall/fof
http://www.gnucitizen.org/blog/flash-upnp-attack-faq/
http://en.wikipedia.org/wiki/Internet_Gateway_Device_Protocol

Output

```
Nessus found an IGD description at http://192.168.0.1:80/RootDevice.xml
```

Plugin Details

Severity:	Medium
ID:	35709
Version:	$Revision: 1.10 $
Type:	remote
Family:	Misc.
Published:	February 19, 2009
Modified:	October 13, 2016

Risk Information

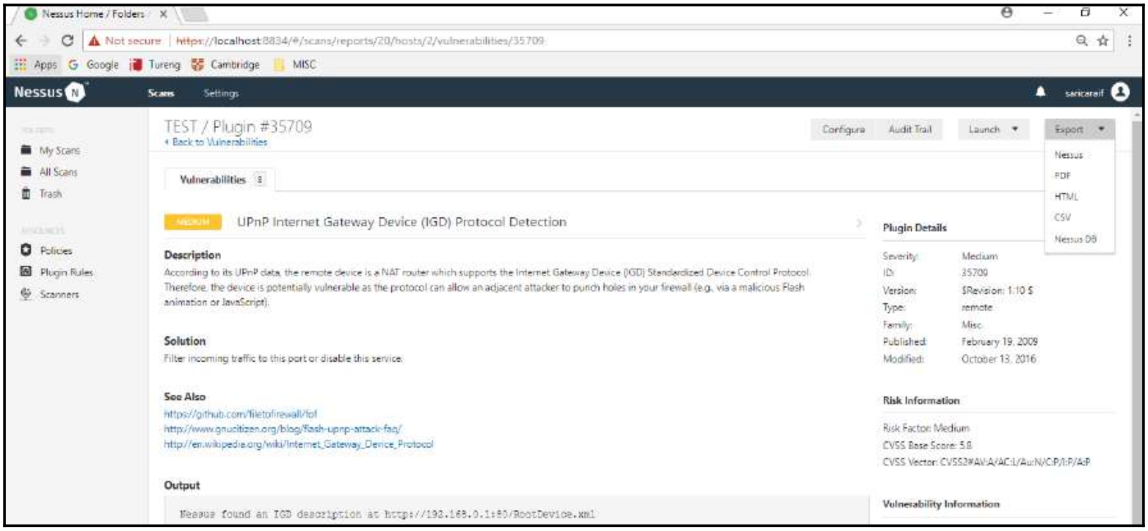
Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Vulnerability Pub Date: January 14, 2008

Figure 9 - Details of vulnerability

Lastly, scan results can be saved in several different formats for reporting purposes. Click on the **Export** tab in the upper-right corner to pull down a menu with the formats **Nessus**, **PDF**, **HTML**, **CSV**, and **Nessus D**B:



TEST / Plugin #35709

‹ Back to Vulnerabilities

UPnP Internet Gateway Device (IGD) Protocol Detection

Description

According to its UPnP data, the remote device is a NAT router which supports the Internet Gateway Device (IGD) Standardized Device Control Protocol. Therefore, the device is potentially vulnerable as the protocol can allow an adjacent attacker to punch holes in your firewall (e.g. via a malicious Flash animation or JavaScript).

Solution

Filter incoming traffic to this port or disable this service.

See Also

https://github.com/filetofirewall/fof
http://www.gnucitizen.org/blog/flash-upnp-attack-faq/
http://en.wikipedia.org/wiki/Internet_Gateway_Device_Protocol

Output

Nessus found an IGD description at http://192.168.0.1:80/RootDevice.xml

Plugin Details

Severity: Medium
ID: 35709
Version: $Revision: 1.10 $
Type: remote
Family: Misc.
Published: February 19, 2009
Modified: October 13, 2016

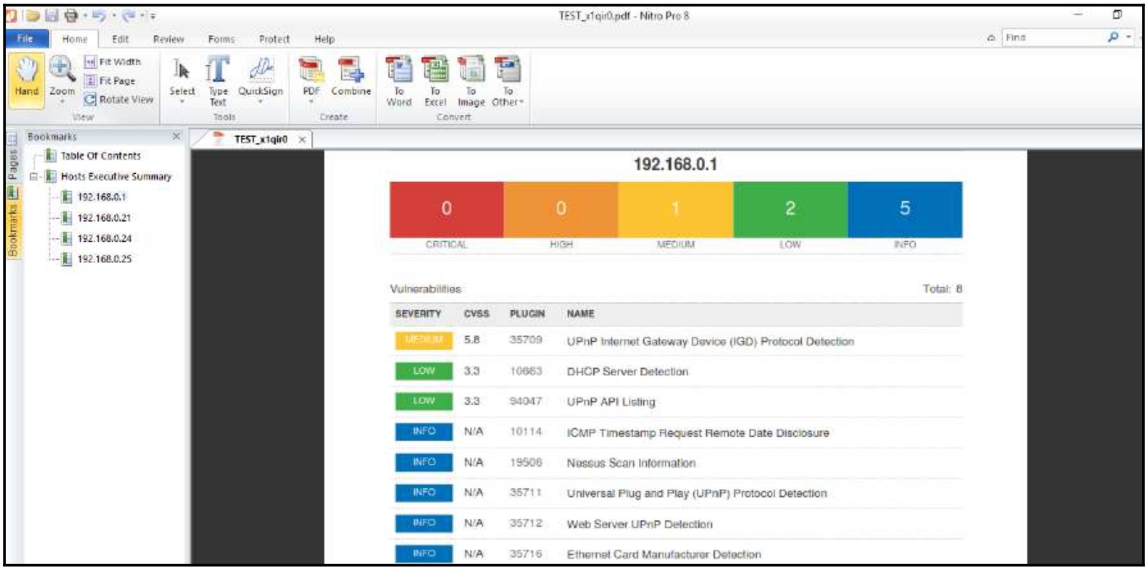
Risk Information

Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Figure 10 - Exporting results

In my case, I chose a PDF format and saved the vulnerability scan results. As shown in *Figure 11*, the report gives detailed information based on the IP addresses scanned. The Nessus scan report presents extensive data about the vulnerabilities detected on the networks. The report can be especially useful to security teams. They can use this report to identify vulnerabilities and the affected hosts in their network, and take the required action to mitigate vulnerabilities:



192.168.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	2	5

Vulnerabilities Total: 8

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.8	35709	UPnP Internet Gateway Device (IGD) Protocol Detection
LOW	3.3	10663	DHCP Server Detection
LOW	3.3	94047	UPnP API Listing
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection

Figure 11 - Results in PDF format

Nessus provides a lot of functionality and ability in one tool. Compared to other network scanning tools, it is fairly user-friendly, had easy-to-update plug-ins, and has nice reporting tools for upper management. Using this tool and seeing the vulnerabilities will help you gain knowledge of your systems, and also teach you how to protect them. New vulnerabilities are released almost daily, and in order to keep your systems consistently secure, you have to scan them regularly.

Keep in mind that finding the vulnerabilities before hackers take advantage of them is a great first step in keeping your systems safe.

Flexera (Secunia) Personal Software Inspector

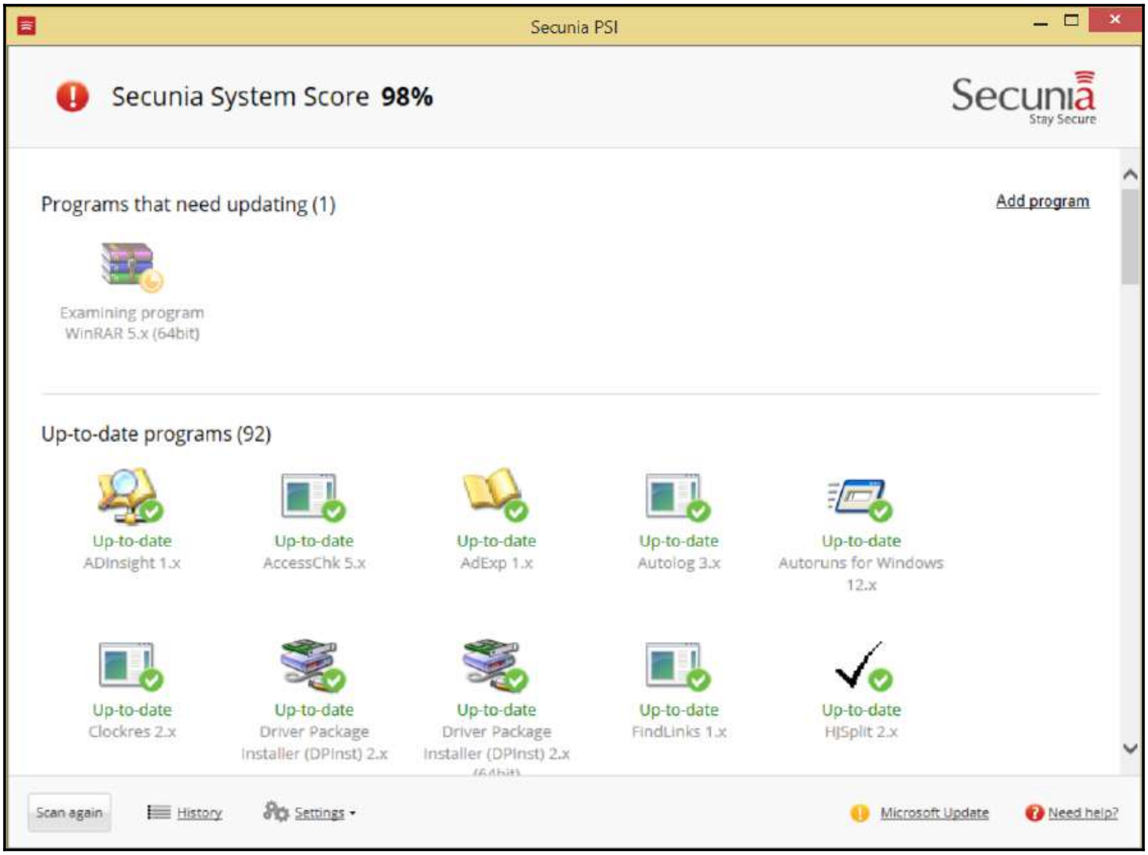
The Secunia **Personal Software Inspector** (**PSI**) is a free security tool that identifies vulnerabilities in non-Microsoft (third-party) systems.

PSI scans installed software on your PC and identifies programs in need of security updates to safeguard your PC against cybercriminals. It then helps you to get the necessary software security updates to keep it safe. To make it easier, PSI even automates the updates for your unsecured programs

This is a free vulnerability assessment tool that is complementary to any antivirus software. It constantly monitors your system for unsecured software installations, notifies you when an unsecured application is installed, and even provides you with detailed instructions for updating the application when updates are available.

To download Secunia PSI, simply visit their website at `https://www.flexera.com/enterprise/products/software-vulnerability-management/personal-software-inspector/`.

Once you install the software, it will examine your computer and give you a percentage score:



Secunia PSI

Secunia System Score **98%**

Programs that need updating (1)

Examining program
WinRAR 5.x (64bit)

Up-to-date programs (92)

Up-to-date
ADInsight 1.x

Up-to-date
AccessChk 5.x

Up-to-date
AdExp 1.x

Up-to-date
Autolog 3.x

Up-to-date
Autoruns for Windows 12.x

Up-to-date
Clockres 2.x

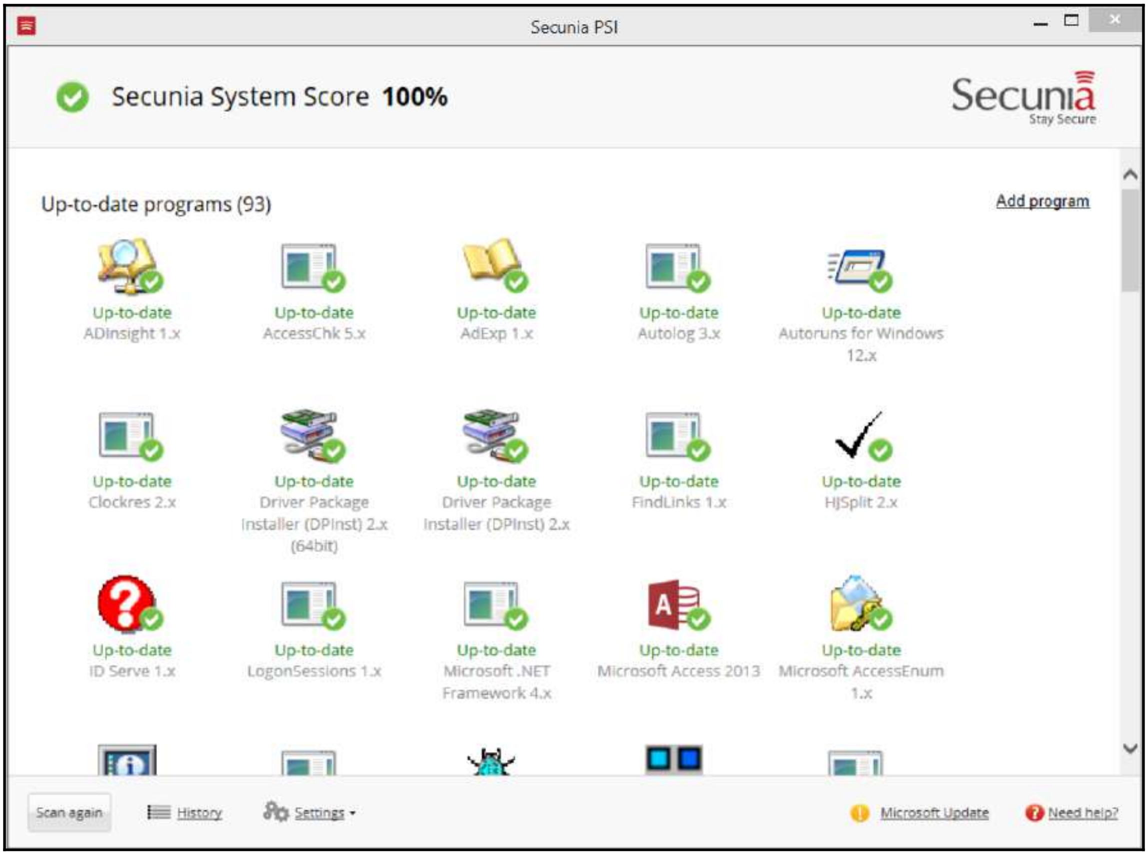
Up-to-date
Driver Package Installer (DPInst) 2.x

Up-to-date
Driver Package Installer (DPInst) 2.x (64bit)

Up-to-date
FindLinks 1.x

Up-to-date
HJSplit 2.x

If you are not at 100%, you need to patch your other missing updates until you have updated all of your software:



But what if you have more computers? The same scanning capabilities of the PSI are available in the commercial edition: Secunia **Corporate Software Inspector** (**CSI**), found at `https://www.flexera.com/enterprise/products/software-vulnerability-management/corporate-software-inspector/`.

The CSI also provides full integration with existing Microsoft deployment tools SCCM and WSUS, so you can now manage the deployment of critical patches for non-Microsoft updates in the same manner in which you deploy Microsoft updates.

Secunia CSI provides the vulnerability intelligence, vulnerability scanning, patch creation, and patch deployment tools to effectively address the challenge of third-party application patch management.

Conclusion

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting and remediation, and finally the planning of the appropriate responses. It has explained the importance of each step in the vulnerability management phase and how each should be carried out. The asset inventory has been described as crucial to the strategy because it is the point where all the details about the hosts are listed to assist in a thorough sanitization of all machines that may have vulnerabilities. The critical function of the information management step in disseminating information in a fast and reliable way has also been highlighted, as well as the tools commonly used to achieve it. The risk identification and classification functions of the risk assessment step have also been discussed. The chapter has also discussed the identification of vulnerabilities in hosts in the vulnerability assessment phase. The roles played by reporting and remediation tracking to inform all stakeholders and follow up on remediation have also been touched upon. The chapter has also discussed the final execution of all responses in the response planning step. The best practices for completing each of the steps successfully have also been discussed.

References

1. K. Rawat, *Today's Inventory Management Systems: A Tool in Achieving Best Practices in Indian Business*, Anusandhanika, vol. 7, *(1),* pp. 128-135, 2015. Available: `https://search.proquest.com/docview/1914575232?accountid=45049`.
2. P. Doucek, *The Impact of Information Management*, FAIMA Business & Management Journal, vol. 3, *(3),* pp. 5-11, 2015. Available: `https://search.proquest.com/docview/1761642437?accountid=45049`.
3. C. F. Mascone, *Keeping Industrial Control Systems Secure*, Chem. Eng. Prog., vol. 113, *(6),* pp. 3, 2017. Available: https://search.proquest.com/docview/1914869249?accountid=45049
4. T. Lindsay, "*LANDesk Management Suite / Security Suite 9.5 L... | Ivanti User Community*", Community.ivanti.com, 2012. [Online]. Available: `https://community.ivanti.com/docs/DOC-26984`. [Accessed: 27- Aug- 2017].

5. I. Latis Networks, "*atis Networks*, Bloomberg.com, 2017. [Online]. Available: `https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=934296`. [Accessed: 27- Aug- 2017].
6. *The CERT Division*, Cert.org, 2017. [Online]. Available: `http://www.cert.org`. [Accessed: 27- Aug- 2017].
7. *SecurityFocus*, Securityfocus.com, 2017. [Online]. Available: `http://www.securityfocus.com`. [Accessed: 27- Aug- 2017].
8. *IT Security Threats*, Securityresponse.symantec.com, 2017. [Online]. Available: `http://securityresponse.symantec.com`. [Accessed: 27- Aug- 2017].
9. G. W. Manes et al, *NetGlean: A Methodology for Distributed Network Security Scanning*, Journal of Network and Systems Management, vol. 13, *(3)*, pp. 329-344, 2005. Available: `https://search.proquest.com/docview/201295573?accountid=45049`. DOI: `http://dx.doi.org/10.1007/s10922-005-6263-2`.
10. *Foundstone Services*, Mcafee.com, 2017. [Online]. Available: `https://www.mcafee.com/us/services/foundstone-services/index.aspx`. [Accessed: 27- Aug- 2017].

Summary

This chapter has outlined the types of response that organizations are expected to provide against attackers. The previous chapters have discussed the attack life cycle and outlined the tools and techniques that attackers normally come packed with. From these tools and techniques, a life cycle capable of mitigating them was designed. This chapter has discussed an effective vulnerability management life cycle composed of six steps. Each of the steps is aimed at making the life cycle effective and thorough in mitigating the vulnerabilities that may be in an organization that attackers may exploit. The well-planned life cycle ensures that not a single host of an organizational network is left exposed to attackers. The life cycle also ensures that the organization ends up with a fully secured IT environment and that it is hard for attackers to find any vulnerabilities to exploit. This chapter has given a set of best practices for each step of the life cycle. These best practices are aimed at ensuring that the incident response teams and the IT staff members make an exhaustive use of each step to secure the organization. In the next chapter, you will learn about the importance of logs and how you can analyze them.

16
Log Analysis

In `Chapter 13`, *Investigating an Incident*, you learned about the investigation process, and some techniques for finding the right information while investigating an issue. However, to investigate a security issue, it is often necessary to review multiple logs from different vendors and different devices. Although each vendor might have some custom fields in the log, the reality is that, once you learn how to read logs, it becomes easier to switch vendors and just focus on deltas for that vendor. While there are many tools that will automate log aggregation, such as a SIEM solution, there will be scenarios in which you need to manually analyze a log in order to figure out the root cause.

In this chapter, we are going cover the following topics:

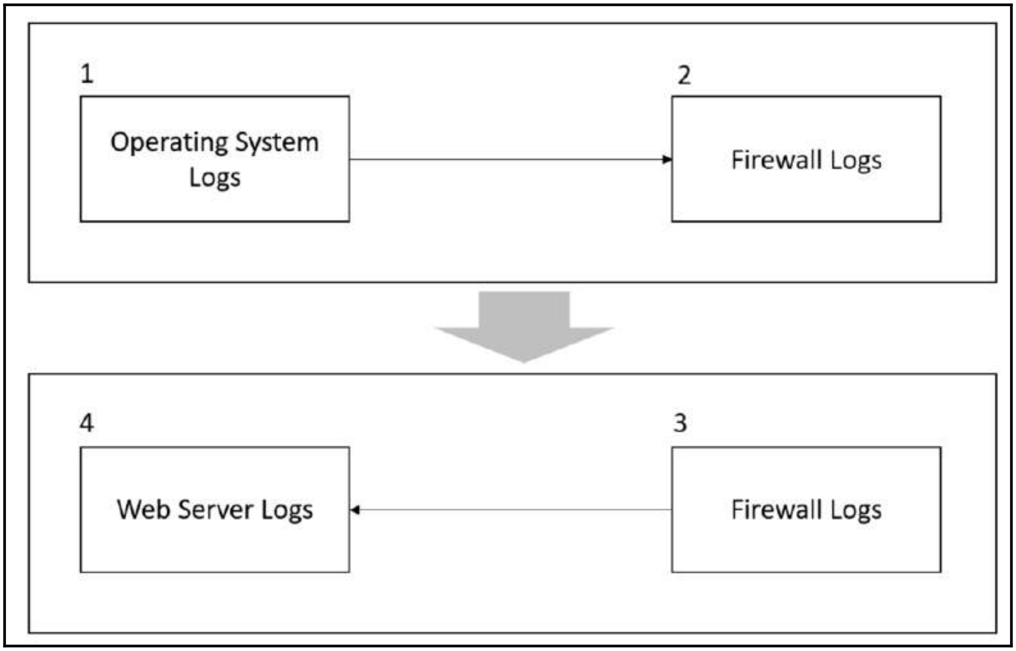
- Data correlation
- Operating system logs
- Firewall log
- Web server logs

Data correlation

There is no doubt that the majority of organizations will be using some sort of SIEM solution to concentrate all of their logs in one single location, and using a custom query language to search throughout the logs. While this is the current reality, as a security professional, you still need to know how to navigate throughout different events, logs, and artifacts to perform deeper investigations. Many times, the data obtained from the SIEM will be useful in identifying the threat, the threat actors, and narrowing down the compromised systems but, in some circumstances, this is not enough; you need to find the root cause and eradicate the threat.

For this reason, every time that you perform data analysis, it is important to think about how the pieces of the puzzle will be working together.

The following diagram shows an example of this data correlation approach to review logs:



Let's see how this flowchart works:

1. The investigator starts reviewing indications of compromise in the operating system's logs. Many suspicious activities were found in the OS and, after reviewing a Windows prefetch file, it is possible to conclude that a suspicious process started a communication with an external entity. It is now time to review the firewall logs in order to verify more information about this connection.
2. The firewall logs reveal that the connection between the workstation and the external website was established using TCP on port `443` and that it was encrypted.
3. During this communication, a callback was initiated from the external website to the internal web server. It's time to review the web server log files.
4. The investigator continues the data correlation process by reviewing the IIS logs located in this web server. He finds out that the adversary tried a SQL injection attack against this web server.

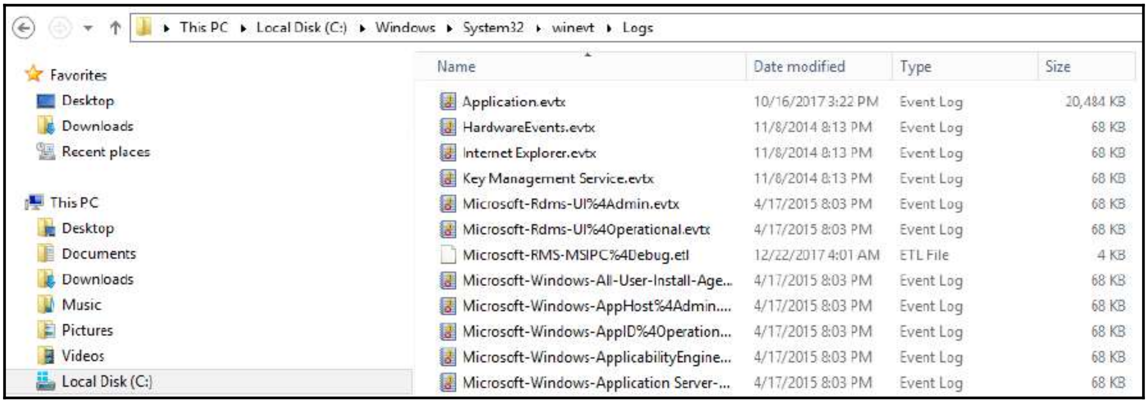
As you can see from this flowchart, there is a logic behind which logs to access, what information you are looking for, and most importantly, how to look at all this data in a contextualized manner.

Operating system logs

The types of logs available in an operating system may vary; in this book, we will focus on core logs that are relevant from a security perspective. We will use Windows and Linux operating systems to demonstrate that.

Windows logs

In a Windows operating system, the most relevant security-related logs are accessible via Event Viewer. In `Chapter 13`, *Investigating an Incident*, we spoke about the most common events that should be reviewed during an investigation. While the events can be easily located in Event Viewer, you can also obtain the individual files at `Windows\System32\winevt\Logs`, as shown in the following screenshot:



Name	Date modified	Type	Size
Application.evtx	10/16/2017 3:22 PM	Event Log	20,484 KB
HardwareEvents.evtx	11/8/2014 8:13 PM	Event Log	68 KB
Internet Explorer.evtx	11/8/2014 8:13 PM	Event Log	68 KB
Key Management Service.evtx	11/8/2014 8:13 PM	Event Log	68 KB
Microsoft-Rdms-UI%4Admin.evtx	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Rdms-UI%4Operational.evtx	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-RMS-MSIPC%4Debug.etl	12/22/2017 4:01 AM	ETL File	4 KB
Microsoft-Windows-All-User-Install-Age...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-AppHost%4Admin....	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-AppID%4Operation...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-ApplicabilityEngine...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-Application Server-...	4/17/2015 8:03 PM	Event Log	68 KB

However, log analysis in an operating system is not necessarily limited to the logging information provided by the OS, especially in Windows. There are other sources of information that you could use, including prefetch files (Windows Prefetch). These files contain relevant information regarding process execution. They can be useful when trying to understand if a malicious process was executed and which actions were done by that first execution.

In Windows 10, you also have OneDrive logs (C:\Users\<USERNAME>\AppData\Local\Microsoft\OneDrive\logs), which can be useful. If you are investigating data extraction, this could be a good place to look to verify if any wrongdoing was carried out. Review the SyncDiagnostics.log for more information.

To parse Windows Prefetch files, use this Python script at //github.com/PoorBillionaire/Windows-Prefetch-Parser.

Another important file location is where Windows stores the user mode crash dump files, which is C:\Users\<username>\AppData\Local\CrashDumps. These crash dump files are important artifacts that can be used to identify potential malware in the system.

One common type of attack that can be exposed in a dump file is the code injection attack. This happens when there is an insertion of executable modules into running processes or threads. This technique is mostly used by malware to access data and to hide or prevent its removal (for example, persistence). It is important to emphasize that legitimate software developers may occasionally use code injection techniques for non-malicious reasons, such as modifying an existing application.

To open these dump files you need a debugger, such as *WinDbg* (http://www.windbg.org) and you need the proper skills to navigate through the dump file to identify the root cause of the crash. If you don't have those skills, you can also use *Instant Online Crash Analysis* (http://www.osronline.com).

The results that follow are a brief summary of the automated analyses from using this online tool (the main areas to follow up are in bold):

```
TRIAGER: Could not open triage file :
e:dump_analysisprogramtriageguids.ini, error 2
TRIAGER: Could not open triage file :
e:dump_analysisprogramtriagemodclass.ini, error 2
GetUrlPageData2 (WinHttp) failed: 12029.
*** The OS name list needs to be updated! Unknown Windows version: 10.0 ***

FAULTING_IP:
eModel!wil::details::ReportFailure+120
00007ffe`be134810 cd29           int     29h

EXCEPTION_RECORD:  ffffffffffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 00007ffebe134810
(eModel!wil::details::ReportFailure+0x0000000000000120)
```

```
    ExceptionCode: c0000409 (Stack buffer overflow)
    ExceptionFlags: 00000001
    NumberParameters: 1
    Parameter[0]: 0000000000000007

    PROCESS_NAME: MicrosoftEdge.exe

EXCEPTION_CODE: (NTSTATUS) 0xc0000409:
```

The system detected an overrun of a stack-based buffer in this application. This overrun could potentially allow a malicious user to gain control of this application.

```
    EXCEPTION_PARAMETER1:  0000000000000007

    NTGLOBALFLAG:  0

    APPLICATION_VERIFIER_FLAGS:  0

    FAULTING_THREAD:  0000000000003208

    BUGCHECK_STR:  APPLICATION_FAULT_STACK_BUFFER_OVERRUN_MISSING_GSFRAME_SEHOP

    PRIMARY_PROBLEM_CLASS: STACK_BUFFER_OVERRUN_SEHOP


    DEFAULT_BUCKET_ID:  STACK_BUFFER_OVERRUN_SEHOP

    LAST_CONTROL_TRANSFER:  from 00007ffebe1349b0 to 00007ffebe134810

    STACK_TEXT:
    000000d4`dc4fa910 00007ffe`be1349b0 : ffffffff`ffffffec 00007ffe`df5e0814
    000000d4`dc4fc158 000002bb`a1d20820 :
    eModel!wil::details::ReportFailure+0x120
    000000d4`dc4fbe50 00007ffe`be0fa485 : 00000000`00000000 00007ffe`df5ee52e
    000002bb`ac0f5101 00007ffe`be197771 :
    eModel!wil::details::ReportFailure_Hr+0x44
    000000d4`dc4fbeb0 00007ffe`be0fd837 : 000002bb`ab816b01 00000000`00000000
    00000000`00010bd8 000002bb`00000000 :
    eModel!wil::details::in1diag3::FailFast_Hr+0x29
    000000d4`dc4fbf00 00007ffe`be12d7dd : 00000000`00010bd8 00000000`00000000
    00000000`80070001 000000d4`dc4ffa60 : eModel!FailFastOnReparenting+0xf3
    000000d4`dc4ffc00 00007ffe`be19e5b8 : 000002bb`ab816b20 00000000`00000000
    00000000`00000000 000002bb`a16b7bb8 :
    eModel!SetParentInBrokerInternal+0x40b5d
    000000d4`dc4ffc40 00007ffe`be19965c : 00000000`00000000 000002bb`ac0f51f0
    000002bb`ac0f51f4 000002bb`ac0f50c0 :
    eModel!CTabWindowManager::_AttemptFrameFastShutdown+0x118
```

```
000000d4`dc4ffc90 00007ffe`be19634e : 000002bb`c0061b00 000000d4`dc4ffd00
00007ffe`be0a9e00 00000000`00000001 :
eModel!CTabWindowManager::CloseAllTabs+0x6c
000000d4`dc4ffcd0 00007ffe`be114a0b : 00000000`00000000 00007ffe`be0a9ed0
000002bb`c0061b00 000002bb`c0061b00 : eModel!CBrowserFrame::_OnClose+0x106
000000d4`dc4ffd50 00007ffe`be07676e : 00000000`00000000 00000000`00000000
00000000`00000000 000002bb`c00711f0 :
eModel!CBrowserFrame::FrameMessagePump+0x6e63b
000000d4`dc4ffe30 00007ffe`be076606 : 000002bb`00032401 000002bb`c0061b00
000000d4`dc4fff50 000002bb`c00711f0 : eModel!_BrowserThreadProc+0xda
000000d4`dc4ffeb0 00007ffe`be0764a9 : 00000000`00000001 000002bb`c0071218
000000d4`dc4fff50 00000000`00000000 : eModel!_BrowserNewThreadProc+0x56
000000d4`dc4ffef0 00007ffe`dea68364 : 000002bb`aae03cd0 00000000`00000000
00000000`00000000 00000000`00000000 : eModel!SHOpenFolderWindow+0xb9
000000d4`dc4fff60 00007ffe`e13470d1 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : kernel32!BaseThreadInitThunk+0x14
000000d4`dc4fff90 00000000`00000000 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
```

In this crash analysis done by Instant Online Crash Analysis, we have an overrun of a stack-based buffer in Microsoft Edge. Now, you can correlate this log (the day that the crash occurred) with other information available in Event Viewer (security and application logs) to verify if there was any suspicious process running that could have potentially gained access to this application. Remember that, in the end, you need to perform data correlation to have more tangible information regarding a specific event and its culprit.

Linux logs

In Linux, there are many logs that you can use to look for security-related information. One of the main ones is the `auth.log`, located under `/var/log`, which contains all authentication related events.

Here is an example of this log:

```
Nov  5 11:17:01 kronos CRON[3359]: pam_unix(cron:session): session opened
for user root by (uid=0)
Nov  5 11:17:01 kronos CRON[3359]: pam_unix(cron:session): session closed
for user root
Nov  5 11:18:55 kronos gdm-password]: pam_unix(gdm-password:auth):
conversation failed
Nov  5 11:18:55 kronos gdm-password]: pam_unix(gdm-password:auth): auth
could not identify password for [root]
Nov  5 11:19:03 kronos gdm-password]: gkr-pam: unlocked login keyring
Nov  5 11:39:01 kronos CRON[3449]: pam_unix(cron:session): session opened
for user root by (uid=0)
```

```
Nov  5 11:39:01 kronos CRON[3449]: pam_unix(cron:session): session closed
for user root
Nov  5 11:39:44 kronos gdm-password]: pam_unix(gdm-password:auth):
conversation failed
Nov  5 11:39:44 kronos gdm-password]: pam_unix(gdm-password:auth): auth
could not identify password for [root]
Nov  5 11:39:55 kronos gdm-password]: gkr-pam: unlocked login keyring
Nov  5 11:44:32 kronos sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/usr/bin/apt-get install smbfs
Nov  5 11:44:32 kronos sudo: pam_unix(sudo:session): session opened for
user root by root(uid=0)
Nov  5 11:44:32 kronos sudo: pam_unix(sudo:session): session closed for
user root
Nov  5 11:44:45 kronos sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/usr/bin/apt-get install cifs-utils
Nov  5 11:46:03 kronos sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/bin/mount -t cifs //192.168.1.46/volume_1/temp
Nov  5 11:46:03 kronos sudo: pam_unix(sudo:session): session opened for
user root by root(uid=0)
Nov  5 11:46:03 kronos sudo: pam_unix(sudo:session): session closed for
user root
```

The preceding logs were collected from a Kali distribution; RedHat and CentOS will store similar information at `/var/log/secure`. If you want to review only failed login attempts, use the logs from `var/log/faillog`.

Firewall logs

The firewall log format varies according to the vendor; however, there are some core fields that will be there regardless of the platform. When reviewing the firewall logs, you must a focus on primarily answering the following questions:

- Who started the communication (source IP)?
- Where is the destination of that communication (destination IP)?
- What type of application is trying to reach the destination (transport protocol and port)?
- Was the connection allowed or denied by the firewall?

The following code is an example of the Check Point firewall log; in this case, we are hiding the destination IP for privacy purposes:

```
"Date","Time","Action","FW.Name","Direction","Source","Destination","Bytes"
,"Rules","Protocol"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.235","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/
http"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.200","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/
http"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.2","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/ht
tp"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.8","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/ht
tp"
```

In this example, rule number 9 was the one that processed all these requests and dropped all connection attempts from 10.10.10.8 to a specific destination. Now, using the same reading skills, let's review a NetScreen firewall log:

```
Nov  2 13:55:46 fire01 fire00: NetScreen device_id=fire01  [Root]system-
notification-00257(traffic): start_time="2016-00-02 13:55:45" duration=0
policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst
zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.10 dst=8.8.8.8
src_port=3036 dst_port=7001
```

One important difference between the Check Point and the NetScreen firewall logs is how they log information about the transport protocol. In the Check Point log, you will see that the proto field contains the transport protocol and the application (in the above case, HTTP). The NetScreen log shows similar information in the service and proto fields. As you can see, there are small changes, but the reality is that, once you are comfortable reading a firewall log from one vendor, others will be easier to understand.

You can also use a Linux machine as a firewall by leveraging iptables. Here is an example of what the iptables.log looks like:

```
# cat /var/log/iptables.log
Nov  6 10:22:36 cnd kernel: PING YuriDio IN=eth3 OUT= MAC=d8:9d:67:cd:b2:14
SRC=192.168.1.10 DST=192.168.1.88 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF
PROTO=ICMP TYPE=8 CODE=0 ID=1007 SEQ=2
```

If you need to review Windows Firewall, look for the `pfirewall.log` log file at `C:\Windows\System32\LogFiles\Firewall`. This log has the following format:

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size
tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2017-12-22 07:38:54 ALLOW TCP 169.254.211.124 169.254.211.124 63863 4369 0
- 0 0 0 - - - SEND
2017-12-22 07:38:54 ALLOW TCP 169.254.211.124 169.254.211.124 63863 4369 0
- 0 0 0 - - - RECEIVE
2017-12-22 07:38:55 ALLOW UDP 169.254.125.142 169.254.255.255 138 138 0 - -
- - - - - SEND
2017-12-22 07:38:55 ALLOW UDP 169.254.211.124 169.254.255.255 138 138 0 - -
- - - - - SEND
2017-12-22 07:38:55 ALLOW UDP 192.168.1.47 192.168.1.255 138 138 0 - - - -
- - - SEND
```

Web server logs

When reviewing web server logs, pay particular attention to the web servers that have web applications interacting with SQL databases. The IIS Web Server log files are located at `\WINDOWS\system32\LogFiles\W3SVC1` and they are `.log` files that can be opened using Notepad. You can also use Excel or Microsoft Log Parser to open this file and perform basic queries.

You can download Log Parser from `https://www.microsoft.com/en-us/download/details.aspx?id=24659`.

When reviewing the IIS log, pay close attention to the `cs-uri-query` and `sc-status` fields. These fields will show details about the HTTP requests that were performed. If you use Log Parser, you can perform a query against the log file to quickly identify if the system experienced a SQL injection attack. Here is an example:

```
logparser.exe -i:iisw3c -o:Datagrid -rtp:100 "select date, time, c-ip, cs-
uri-stem, cs-uri-query, time-taken, sc-status from
C:wwwlogsW3SVCXXXexTEST*.log where cs-uri-query like '%CAST%'".
```

Here is an example of a potential output with the keyword CAST located in the `cs-uri-query` field:

```
80 POST  /pages/Users/index.asp  ID=UT-47-TP-
M17';DECLARE%20@S%20NVARCHAR(4000);SET%30@S=CAST(0x4400);EXEC(@S);--
|31|80040e32|Timeout_expired     500
```

Notice that, in this case, the error code was `500` (internal server error); in other words, the server was not able to fulfil the request. When you see this type of activity in your IIS log, you should take action to enhance your protection on this web server; one alternative is to add a WAF.

If you are reviewing an Apache log file, the access log file is located at `/var/log/apache2/access.log` and the format is also very simple to read, as you can see in the following example:

```
192.168.1.10 - - [07/Dec/2017:15:35:19 -0800] "GET /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22 -0800] "GET /docs/bin/main.php 200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27 -0800] "GET /docs HTTP/1.1" 200 4140
```

If you are looking for a particular record, you can also use the `cat` command in Linux, as follows:

```
#cat /var/log/apache2/access.log | grep -E "CAST"
```

Another alternative is to use apache-scalp tool, which you can download from `https://code.google.com/archive/p/apache-scalp`.

References

1. iptables: `https://help.ubuntu.com/community/IptablesHowTo`
2. Log Parser: `https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/`
3. SQL Injection Finder: `http://wsus.codeplex.com/releases/view/13436`
4. SQL Injection Cheat Sheet: `https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/`

Summary

In this chapter, you learned about the importance of data correlation while reviewing logs in different locations. You also read about relevant security-related logs in Windows and Linux.

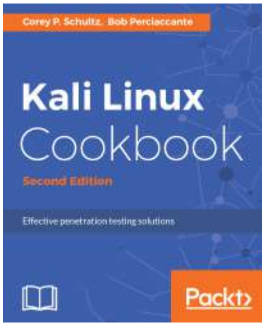
Next, you learned how to read firewall logs using Check Point, NetScreen, iptables, and Windows Firewall as examples.

At the end of this chapter, you learned about web server logs, using IIS and Apache as examples.

As you finish reading this chapter, and this book, it's time to step back and reflect on this cybersecurity journey. It is very important to take the theory that you learned here, aligned with the practical examples that were used throughout this book, and apply it to your environment or to your customer's environment. While there is no such thing as one size fits all in cybersecurity, the lessons learned here can be used as a foundation for your future work. The threat landscape is changing constantly and, by the time we finished writing this book, a new vulnerability was discovered. Probably, by the time you have finished reading this book, another one has been discovered. It's for this reason that the foundation of knowledge is so important, because it will assist you in rapidly absorbing new challenges and applying security principles to remediate threats. Stay safe!

Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:


Corey P. Schultz, Bob Perciaccante
Kali Linux
Cookbook
Second Edition
Effective penetration testing solutions
Packt

Kali Linux Cookbook - Second Edition
Corey P. Schultz, Bob Perciaccante

ISBN: 978-1-78439-030-3

- Acquire the key skills of ethical hacking to perform penetration testing
- Learn how to perform network reconnaissance
- Discover vulnerabilities in hosts
- Attack vulnerabilities to take control of workstations and servers
- Understand password cracking to bypass security
- Learn how to hack into wireless networks
- Attack web and database servers to exfiltrate data
- Obfuscate your command and control connections to avoid firewall and IPS detection

Information Security Handbook
Darren Death

ISBN: 978-1-78847-883-0

- Develop your own information security framework
- Build your incident response mechanism
- Discover cloud security considerations
- Get to know the system development life cycle
- Get your security operation center up and running
- Know the various security testing types
- Balance security as per your business needs
- Implement information security best practices

Leave a review - let other readers know what you think

Please share your thoughts on this book with others by leaving a review on the site that you bought it from. If you purchased the book from Amazon, please leave us an honest review on this book's Amazon page. This is vital so that other potential readers can see and use your unbiased opinion to make purchasing decisions, we can understand what our customers think about our products, and our authors can see your feedback on the title that they have worked with Packt to create. It will only take a few minutes of your time, but is valuable to other potential customers, our authors, and Packt. Thank you!

Index