



Incident Response Card Game

Public Launch in **January 2020**



Type "Backdoors & Breaches" into the Questions Window to find out how, where, and when you can get a deck.

We'll select a few random requests to get a deck before the public launch.





Group Policies that Kill Kill Chains

Jordan Drysdale @rev10d Kent Ickler @krelkci

Black Hills Information Security @BHInfoSecurity @Defensive Origins @DefensiveOrigins





Part One



Warning



This slide deck is dense. There will be videos to follow.

There will (in all likelihood) be a class at WWHF-SD





The Kill Chain — Or, Its much more than just low fruit.





DA in < 2hrs. Sometimes, minutes.



- NTLM, NBNS, LLMNR
- Password (Storage, Reuse, Spray)
- Hash (Storage, Passing)
- Local Weakness
- SMB Signing
- PowerShell and Console
- Network Logons (lateral)
- Exfil & Shellz
- Mimikatz
- Overprivileged Users
- Host based Firewall
- Removable Media
- Security









The next 3 slides might be painful to hear. The goods begin in 4 slides.

You need to know these.

You need to practice these.

Clean what you inherit.



Pre-Reqs



Principal of Least Privilege

Network Segregation

OSI Model – Know your stack!

Centralized Logging

Internet Filtering

Workstation Internet Proxy

Honeypots

Av/AntiMalware

Baseline Analyzer – includes MS's RSOP

Passwords, Passwords!

VPNs... MFA

Password Age/Complexity exemptions!?

You need to know these.

You need to practice these.

Clean what you inherit.



AD Groups



Well Defined Groups

Mail Enabled Security Groups? COOL. More groups than users? Could be OK.

Nested Groups in Nested Groups in Nested Groups? YEP #Winning.

One user in a group? St

Group = Region Campus Department Job Title? **SWEET!**

JUGULAR or AGUDLP – Know them. (Live and Die defending them) J-User-Global-Universal-DomainLocal-Resource

ccount-Global-Universal-DomainLocal-Permission

Job Functional Mail Enabled Security Groups...

All East Region Georgia Atlanta South Marketing Social Media Analysts Sr... @ DefensiveOrigins.com One group (email) is actually many many groups... but the world is a better place.

Who is the Senior Social Media Analyst at the Atlanta South campus?
Will you email all the East Region Sr. Social Media Analysts?
Can you add all of Georgia Campuses to this Fileshare?
Let Atlanta South Office know the firealarm is going to go off at 10AM for a test.
Hi all Marketing Departments, this is our new Corp Marketing Director...

Email all staff.

You need to know these.

You need to practice these.

Clean what you inherit.



Organizational Units M Policies



LSDOU
Local – Site – Domain – Organizational Unit



Baseline Domain-Wide GPO
Policy for User or Computer, not both!
Small GPOs are GOOD

Avoid Policy Inheritance and Policy Enforcement

WMI Filters = Slow. Avoid them. Avoid Loopback At all possible.

RSoP, USE IT.

GPO Removal? Careful.



You need to know these.

You need to practice these.

Clean what you inherit.



Top 10...13...16... Too Many Defencering GPOs

Local admin Rename / LAPS Event Logs / Sysmon / WEF Defender Power (Sleep, Screenlock, etc) Swap file data detstruction Interactive Logon Information Logon Restrictions Disable Guest Account SMB Signing Disable LanMan Hash, NTLMv1, SMBv1 Minimum Password Length Password Age Event Logs Anonymous SID enumeration Anonymous account not in everyone group Enable User account control (UAC) Defender / Host-Based Firewall
Application Whitelist / PowerShell (!?)
Limit Access to Control Panel Do not allow media drives Honey Accounts Restricted CMD and PowerShell PowerShell Transcription Software Restriction Policy
Interactive Logon Restrictions for Service Accounts
Credential Guard UEFI Gizmos - Secure Boot, etc Deploy Certificates Configure Wireless Networks/w 802.1x

Anti-Starbucks GPO (suggest open wifi) etc





0:03 4.5K views



FIPS/Encryption

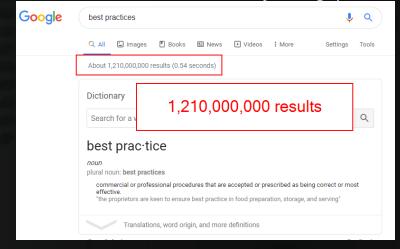
Network Defenses Section to Follow

The next few slides discuss some standards for implementing what we consider to be

"BEST PRACTICES"

for network defensery.

*This is not a term (anyone everyone Google) can define clearly, so we're not sure it means anything (...everything).







Slide #12. We aren't talking about these...





But since we're on the topic...

If you aren't managing these already, Goto slide #12.

Policy Setting

5 passwords remembered

90 days 7 days

15 characters Minimum password length

Store passwords using reversible encryption

Enabled Disabled

Policy Setting

Account lockout duration 60 minutes Account lockout threshold 5 invalid logon attempts

Reset account lockout counter after 30 minutes

Interactive logon: Display user information when the session is locked

Interactive logon: Do not require CTRL+ALT+DEL

Interactive logon: Don't display last signed-in

Password must meet complexity requirements

Interactive logon: Don't display username at sign-in

Interactive logon: Machine account lockout threshold

Interactive logon: Machine inactivity limit

Interactive logon: Message text for users attempting to log on

Interactive logon: Message title for users attempting to log on

Interactive logon: Number of previous logons to cache (in case domain controller ... 2 logons

Do not display user information

Not Defined

Enabled

Enabled

10 invalid logon attempts

600 seconds

You're not welcome, hacker,

Legalese here.

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Lockout Policy

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Security Options

Do they even deserve to be in the "Top".





Enforce password history

Maximum password age

Minimum password age

Dealing with Local Admins





Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Security Options -> Accounts*

Rename local administrator account? Make it a honey account?

Policy	Policy Setting
🗓 Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to cons	Not Defined
🚇 Accounts: Rename administrator account	Wally.Smith



Dealing with Local Admins



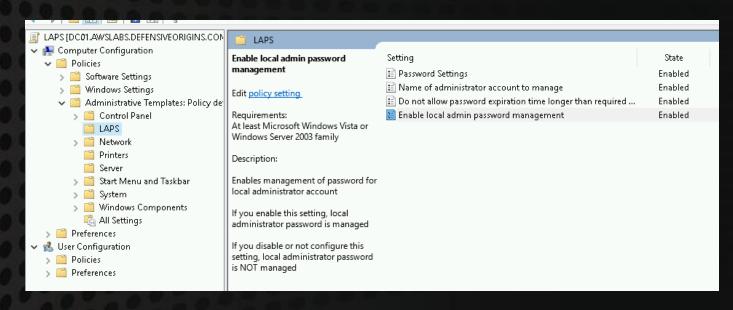


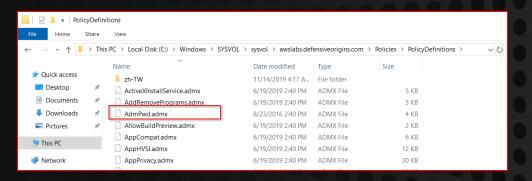
Computer Configuration -> Policies -> Admin Templates -> LAPS

LAPS!

schema.

Restrict access with ADSIEdit







Dealing with Local Admins





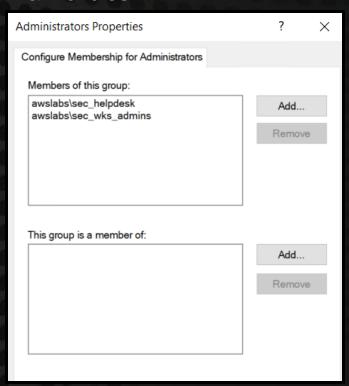
Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups

Members of this group: Add...

Computer Configuration -> Preferences -> Control Panel Settings -> Local Users and Groups Update Administrators, Delete all members users/groups, Add specifics.

Group Policy for managing membership. Two ways. One gives more control.

Via Policies:



Via Preferences:

New Local Group Properties			
Local Group Commo	n		
Action:	Update		~
Group name:	Administrators		·
Rename to:			
Description:			
		☑ Delete all	member users
		☑ Delete all	member groups
Members:			
Name		Action	SID
awslabs\Domain A		ADD	S-1-5-21-3515:
awslabs\sec_wks_	_admins	ADD	S-1-5-21-3515:
	Add	Remove	Change
Ok	Cancel	Apply	Help



Addressing LLMNR (NBNS and WPAD too)





Computer Configuration -> Policies -> Admin Templates -> Network -> DNS Client Turn off multicast name resolution: ENABLED

	DNS Client			20			
MacComputer Configuration A Dolicies	Turn off multicast name	c i comuniti	Setting Allow DNS suff	ix appending to unqualified multi-la	bel nam Not o	State configured	
Software Settings Windows Settings	8		Turn off mu	ulticast name resolution		- 0	x
Administrative Templates: Policy definitions (AD Control Panel Network Background Intelligent Transfer Service (E BranchCache DirectAccess Client Experience Settings DNS Client Hotspot Authentication Lanman Server Link-Layer Topology Discovery	Turn off multicast Not Configured Enabled Disabled	name resolution Comment: Supported on:		Previous Setting ws Vista	Next Setting		() ()
Microsoft Peer-to-Peer Networking Service Metwork Connections Network Connectivity Status Indicator Network Isolation Network Provider Offline Files OSS Packet Scheduler SNMP SSL Configuration Settings	Options:			Specifies that link local multicast redisabled on client computers. LLMNR is a secondary name resolution of the same sent using multicast or single subnet from a client computer on the same subnet that also has I not require a DNS server or DNS cl	ution protocol. Wi ver a local network uter to another clie LLMNR enabled. L	ith LLMNR, k link on a ent compute LMNR does	
Windows Connect Now Windows Connection Manager WLAN Service WWAN Service Printers Server Start Menu and Taskbar				provides name resolution in scena DNS name resolution is not possib If you enable this policy setting, LI available network adapters on the If you disable this policy setting, o policy setting, LLMNR will be enab	rios in which com ble. LMNR will be disal client computer. Ir you do not conf	ventional bled on all	



Addressing LLMNR (NBNS and WPAD too)

Credit due:

http://blog.dbsnet.fr/disable-netbios-with-powershell

(Deploy that with a GPO ©)

```
Write-Host("---- Disable NetBIOS by updating Registry ----")

$key = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"

Get-ChildItem $key !

foreach {
  Write-Host("Modify $key\$($_.pschildname)")

$NetbiosOptions_Value = (Get-ItemProperty "$key\$($_.pschildname)").NetbiosOptions

Write-Host("NetbiosOptions updated value is $NetbiosOptions_Value")

Write-Host("---- NetBIOS is now disabled ----")
```



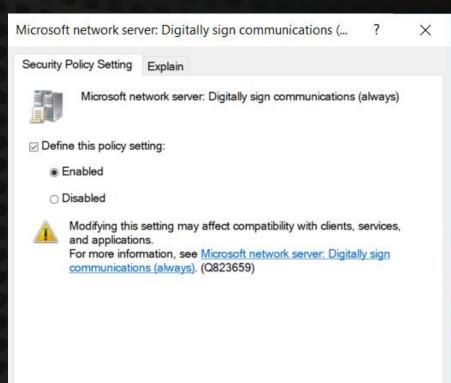
SMB Message Signing

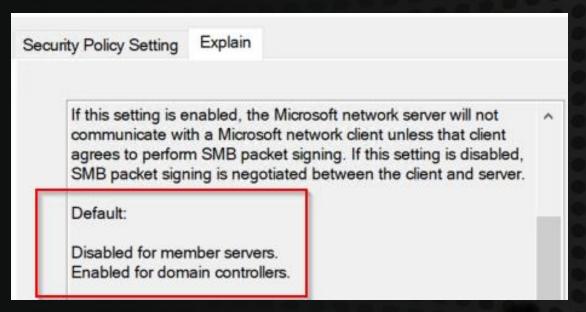




Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options
Microsoft network server: Digitally sign communications (always): ENABLED

Stop most NTLM / SMB relay attacks (yeah, MIC strip is a thing and there are some other attacks)







Configuring Host Based Firewalls





Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Defender Firewall with Advanced Security

Turn them on. All of them. Workstations: Yes. Servers: Yes, but....

Start by turning them on. Really.

Your workstations don't need to talk to each other.

But, like Fine-Grained Password Policies, you might need something a bit more... fine-grained...







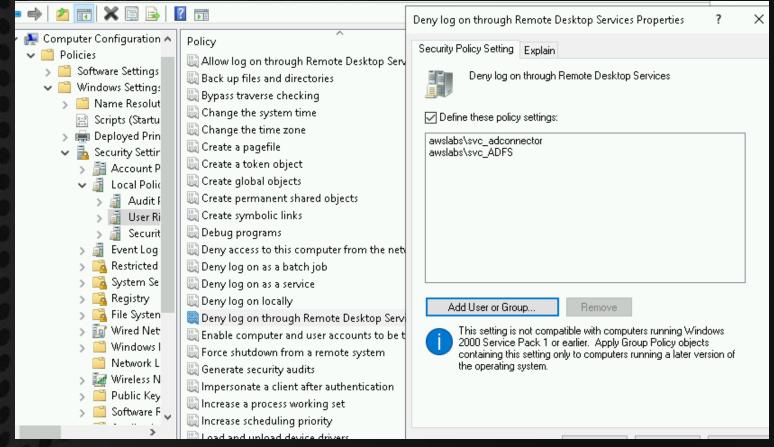
Limiting/Restricting Network Logons ()





Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment

Why would a service account I cracked via kerberoasted hashes easily because the password was set to never expire by an admin in the late 90s need RDP to a DC?





Configuring System Web Proxy





User Configuration -> Preferences -> Control Panel Settings -> Internet Settings -> Connections -> Local Area Network (LAN) Settings

Uncheck "Automatically detect settings"

Check "Use a proxy server for your LAN..."

Proxy = Webfiltering.
But disabling WPAD = GOOD.

Local Area Network (LAN) Settings	X
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.	
☐ Automatically detect settings ☐ Use automatic configuration script	
Address:	
Proxy server	
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).	
Address: squid.defensiveorigins Port: 8080 Advanced	
☐ Bypass proxy server for local addresses	
OK Cancel	

Squid is free and highly configurable.



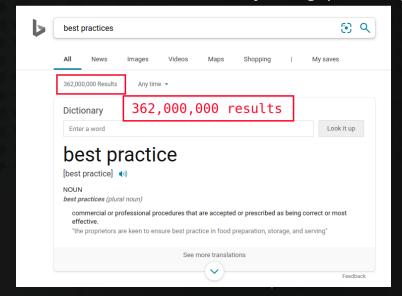
Network Logging and Alerting Section to Follow

The next few slides discuss some standards for implementing what we consider to be

"BEST PRACTICES"

for network alertery.

*This is not a term (anyone everyone Google Bing) can define clearly, so we're not sure it means anything (...everything).







Configuring Windows Auditing and Logging





Wasn't this supposed to be about GPOs...

Information Security

auditpol.exe /set /Category:*
/success:enable
auditpol.exe /set /Category:*
/failure:enable
auditpol.exe /get /Category:*

This here is probably a bit verbose. But, in the wild world of Windows logging...

The IoC's might be in there somewhere...right? wrong

PS C:\Users\Administrator> auditpol.exe /get /Category:* System audit policy Category/Subcategory Setting Security System Extension Success and Failure System Integrity Success and Failure IPsec Driver Success and Failure Other System Events Security State Change Success and Failure Success and Failure ogon/Logoff Logon Success and Failure Success and Failure Logoff Account Lockout Success and Failure IPsec Main Mode Success and Failure IPsec Quick Mode Success and Failure IPsec Extended Mode Success and Failure Special Logon Success and Failure Other Logon/Logoff Events Network Policy Server Success and Failure Success and Failure User / Device Claims Success and Failure Object Access File System Success and Failure Registry Kernel Object Success and Failure Success and Failure Success and Failure Certification Services Success and Failure Application Generated Success and Failure Handle Manipulation Success and Failure File Share Success and Failure Filtering Platform Packet Drop Filtering Platform Connection Success and Failure Success and Failure Other Object Access Events Detailed File Share Success and Failure Success and Failure Removable Storage Success and Failure Central Policy Staging Success and Failure



Windows Auditing and Logging Continued

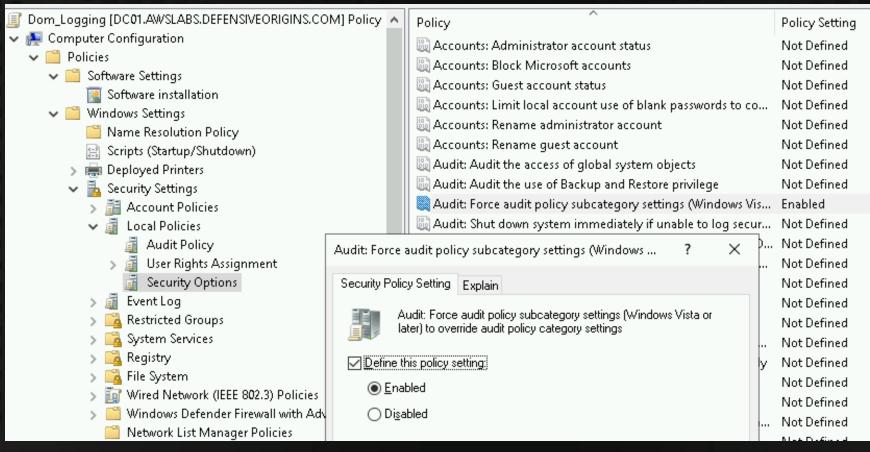




Computer Configuration -> Policies -> Windows Settings-> Security Settings-> Local Policies -> Security Options

Audit: Force audit subcategory settings...: Enabled

Enable the force of audit policy to override "basic" and enforce "advanced" auditing





Kerberos Ticket Operations





Computer Configuration -> Policies -> Windows Settings-> Security Settings-> Advanced Audit Policy Configuration -> Audit Policies -> Account Logon

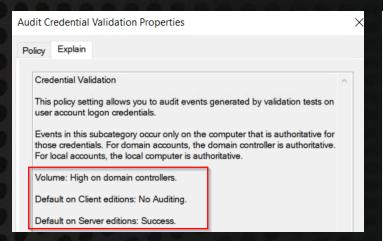
Audit Credential Validation: Success and Failure Audit Kerberos Authentication Service: Success and Failure

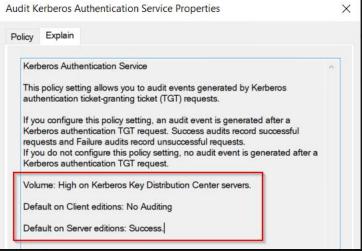
Information Security

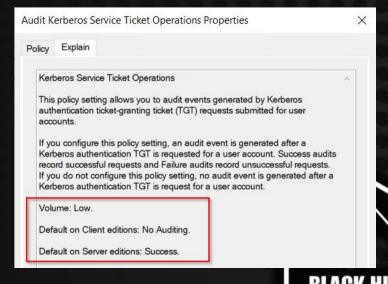
Audit Kerberos Service Ticket Operations: Success and Failure

All those enabled audit functions still miss Kerberoasting.

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Not Configured







PowerShell and CMD Transcription





Windows PowerShell			
Select an item to view its description.	Setting	State	
	Turn on Module Logging	Enabled	
	Turn on PowerShell Script Block Logging	Enabled	
	Turn on Script Execution	Enabled	
	Turn on PowerShell Transcription	Enabled	
	Set the default source path for Update-Help	Not configured	

Computer Configuration -> Administrative Templates -> Windows Components -> Windows Powershell
Turn on Powershell Transcription: Enabled
Turn on Script Execution: Enabled, Allow only signed scripts
Turn on PowerShell Script Block Logging: Enabled, Log script block invocation start / stop events
Turn on Module Logging: Enabled, Select Suggested Modules

Powershell Transcription.

Turn on PowerShell Transcription Turn on PowerShell Transcription Previous Setting **Next Setting** O Not Configured Enabled O Disabled At least Microsoft Windows 7 or Windows Server 2008 family Options: Help: Transcript output directory This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. ☐ Include invocation headers: If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents directory, with a file name that includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session. If you disable this policy setting, transcripting of PowerShell-based applications is disabled by default, although transcripting can still be enabled through the Start-Transcript cmdlet. Cancel Apply

Powershell Script Block Logging.

Furn on PowerShe	I Script Block Log	ging						×
Turn on PowerShe	ell Script Block Log	gging		Previous Setting	Next Setti	ng		
Not Configured Enabled Disabled	Comment: Supported on:	At least Microsc	oft Windows 7	or Windows Server 2	2008 family			^ ~
Options:			Help:					
☑ Log script block inv	ocation start / sto	op events:	input to the log. If you e Windo script block interactive! If you input is dis If you additionally block, functions	enable the Script Bloo y logs events when ir tion, or script or stops. Enabling Inv	s-PowerShell/C ting, g the processin pts - whether i ation. tting, logging ck Invocation I procession of a	Operation of convoked of Power Logging comma	mmands erShell sci , PowerSi nd, script	t ript hell



PowerShell and CMD Transcription





Information Security

Windows PowerShell		
Select an item to view its description.	Setting	State
	Turn on Module Logging	Enabled
	Turn on PowerShell Script Block Logging	Enabled
	Turn on Script Execution	Enabled
	Turn on PowerShell Transcription	Enabled
	Set the default source path for Update-Help	Not configured

Computer Configuration -> Administrative Templates -> Windows Components -> Windows Powershell

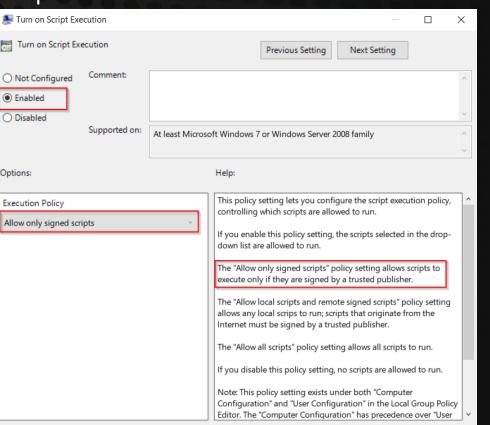
Turn on Powershell Transcription: Enabled

Turn on Script Execution: Enabled, Allow only signed scripts

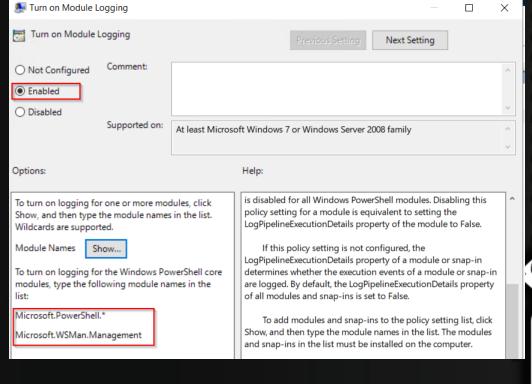
Turn on PowerShell Script Block Logging: Enabled, Log script block invocation start / stop events

Turn on Module Logging: Enabled, Select Suggested Modules

Script Execution.



Module Logging

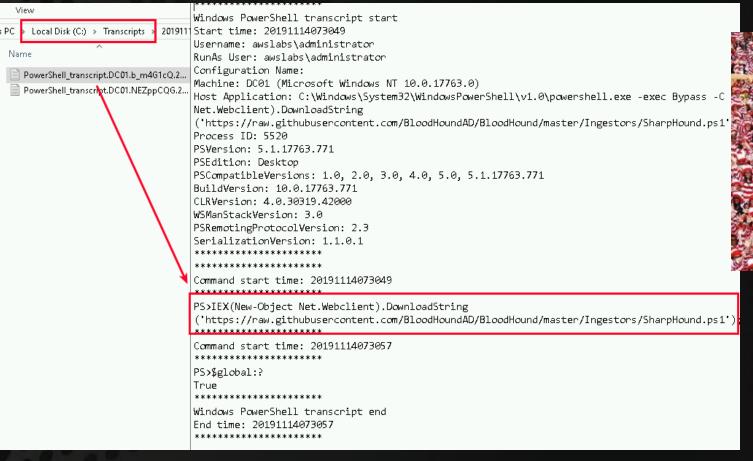


Transcription Results





Found you!







Installing SysMon



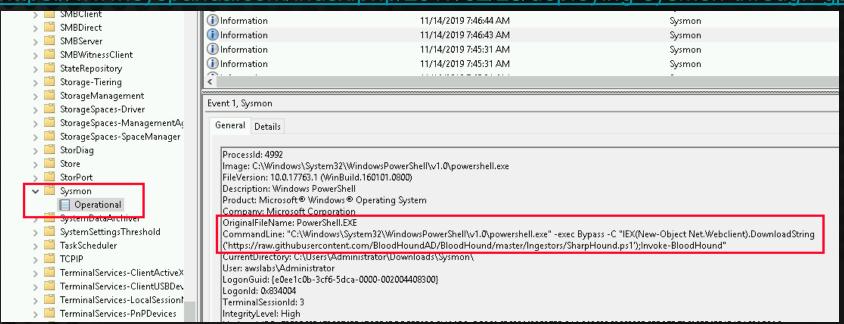


Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup

If we haven't beat this drum loud enough, SysMon is the fastest, easiest way to quickly generate meaningful (security) logging on Windows systems.

The GPO deployment is documented here:

https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/





Important Things





Slides will be available here:

https://www.activecountermeasures.com/presentations/

BHIS blog:

https://www.blackhillsinfosec.com/blog/

The YouTubes:

https://www.youtube.com/channel/UCJ2U9Dq9NckqHMbcUupgF0A

Videos of implementing the GPOs and the ramifications will be available in the next couple of months. We are working on it.

Some questions have likely been addressed.

Seriously, thank you for taking the time to journey with us.



ATTN "Jim"





