Webcast: Group Policies That Kill Kill Chains - Q&A

Question Asked	Answer Given
Does smb message signing "break" anything. How dangerous are these changes?	This is purported to be a performance issue. I assume there is validity to this response based on the expectation that traffic will be checked against the agreed upon SigningKey or SessionKey. https://support.microsoft.com/en-us/help/4458042/reduced-performance-after-smb-encryption-or-smb-signing-is-enabled
What do you recommend as a reference for what Win Audit logs need to be enabled?	RTA, amiright??? (Read the article) -- ha. that is a joke. It took no less than the combination of five or six unique combinations of configuration recommendations that we eventually figured out that Microsoft doesn't know how to catch misbevaior either. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations Best config for us (noisy, but functional, and ingests are parseable): https://github.com/SwiftOnSecurity/sysmon-config - filter out your AV, and EDM. For whatever reason they all seem inclined to touch LSASS. Also terrifying...we've migrated in to EDM product executables before... ¯_(ツ)_/¯
So how do you deploy new local admin accounts to use with LAPS if not the builtin admin account?	The LAPS gpo templates allow you to define the account which will be managed
General thoughts about osquery?	There isn't much experience with that solution around here, but we will investigate to be certain. Thank you for the blog idea!
are there any restrictions to running sysmon on more legacy environments(win7, WS 2003, ..)?	last version of sysmon with support for even server 2008 was v3.21 release: 2015. crazy thing? those versions will probably provide pretty darn good optics for those vendor unsupported boxes.
i have an issue on an inherited instance, someone enforced the default domain policy which has a ton of settings in it including forcing encryption types (all selected except future encyryption types) and if we unenforce the policy - people can't login to domain on a number of workstations and servers - need to come up with a plan to get out of this enforced default domain policy nightmare	tagging kent here. I would straight up build a new mirror domain and build a domain migration script with PS. Pilot that to distinct systems in the various departments. domain trusts absolutely suck, but this is probably a good reason. you need a project manager, **strict deadlines**, 4-hour microsoft support, and the finish line is domain trust removal.
Would enabling smb signing on servers only be pointless? Does it need to be enabled on both endpoints AND servers to be effective?	I will still target workstations, especially if BloodHound pointed me to some workstaitons with admin logged on
GPOs to kill 90% of the threats for an average business. Use MDR to ctach the remaining 10%	Yes. Cultural support for security is top down. This has be supported, messaged well, and politically viable in the "let's still do business" context. some GPOs - strong passwords almost inevitably cause fallout. BUT - YOUR POINT IS OURS TOO! You can make your domain so much more secure putting these GPOs in the right places.
do you recommend seperate Admin users for servers vs workstations? Use Microsoft Tiering! DA only for DCs, Member Servers have separate login. Use LAPS for workstations	Yes, and this answer is very concise to describing the system access privilege problem. (There are paid solutions that do very cool things too, but for the cost of your existing domain licensing, can't beat this config recommendation.)
Aren't there vulnerabilities to having WMI enabled?	Yes, Chris Truncer's Offensive WMI stuff is amazing. https://pentestlab.blog/2017/11/20/command-and-control-wmi/
Any thoughts on canary tokens?	Canary Tokens are a very effective way to phish for misbehavior from the Blue Team side. want to know when one of your sites gets cloned? canarytoken. file phishing for adversaries? canarytoken.
What about signing PS scripts ? is this a common practices so harden the environment ?	Best Practice: Enforce PS Scripts be "AllSigned" - https://blogs.technet.microsoft.com/poshchap/2015/01/02/execution-policy-and-group-policy/
Work at an MSSP. We have a lot of customers whose envs are trainwrecks. Usually the IT for these customers are combative when it comes to implementing best practices, so being to set and forget policies to improve posture is a huge win for us in these scenarios.	Been there - 100% - so difficult. we have a slide on this,50 + unique domains, cultures, networks -- terrifying and super difficult
MBSA deprecated in Win10? Kind of works?	MBSA just hasn't been maintained. https://docs.microsoft.com/en-us/windows/security/threat-protection/mbsa-removal-and-guidance -- pretty hard to miss patches these days. someone has to actively disable the update functions...even then MS seems to find a way.
Thoughts on attempting to "take over" responsibility for GPO from Systems team in an organization?	Work at influence not ownership I would think.
Did you guys already discuss PAWS? (Priv Access Workstations)?	Nope. Same as jump host? highly recommended
SYSMON QUESTION: How can you protect your Sysmon config from an attacker? (If they are able to read the config - then they know the blind spots in the "exclude" rules)	You are already owned?
Cant disable WPAD. However you can create the following entry for WPAD in the host file: wpad 255.255.255.255	good tip
YOu may have answerd it, how to disable DNS over HTTPS - FireFox, and others are also starting to do it - how to do disable across all browsers?	I have not personally had to deal with this yet, but this was a super interesting read. https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https -- appears to be a function simply carried out in the background by the web browser.

Question Asked	Answer Given
So what DNS A record would you suggest? WPAD.contoso.com pointing to 0.0.0.0?	wpad 255.255.255.255 - this tip goes to another registrant. link to the initial elevation of privilege finding. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-077 - the article only discusses a hosts file entry. I've heard the DNS entry works the same, as NBT-NS is a fallback only if DNS doesn't work first.
Will you guys be talking about smart card auth/login?	Don't thinks so but recommended. And depends on the culture -- do you run say a fish hatchery? or a police department because the security here makes a difference on the recommendation.
it seems win10 relies on the winhttpautoproxysvc, how is this addressed?	answered - this is wpad.
can you guys talk about the windows 10 winhttpautoproxysvc reliance	
SO would a host file be best then? say for laptop when its not on domain to pull DNS	Recommended by MS, but IMO - no. DNS entry for wpad should mitigate risk.
Do you guys use BloodHound to hunt for weak policies or is that more of a lateral movement exercise?	Weak policies become evident. the first cmd is usually something like cmd# > net accounts /domain then cmd# > gpresult -h report.html --- weak password policy can be the fastest way to the domain's heart :D
I'm getting error 521 when I enable directory access. That is the log that says "critical logging failure". Basically that is what we are using to detect access to our HoneyUser. Any ideas how to resolve this?	Ummmm Google it?
How to send the sysmon logs to a centralized monitoring system/siem?	Collect it from the Event Viewer, most SIEM should be able to do this. WEF is another one
Patching process: Small lab in the cloud that runs a sample set of servers in the environment. Test patches to see if anything breaks, if no: Patch all and save the instance for the next round	
Oh! Speaking of responder, what about BH detection?	osquery
Doesn't Delivery Optimization in W10 affect overall bandwidth?	I thought this was a wild read! https://support.microsoft.com/en-us/help/4468254/windows-update-delivery-optimization-faq - basically allowing devices to connect to each other for update content. seems like this process might be worthy of investigation...crazy thing -- its just another svchost.exe thread. also some interesting discussions about this on technet.
Have you run into Microsoft ATA (Advanced Threat Analytics) on a pentest before?	yeah. one of the most difficult solutions to evade. no joke, seems to see "(almost) all the things"
Have you looked at PolicyPak Least Privileged Manager?	looks good from a marketing context for sure. https://www.policypak.com/products/least-privilege-manager.html. but neither of us have direct experience.
Regarding logs, SIEMs, and storage, yes storage is cheap but certain SIEM products have licensing based upon quantity of ingested data. :(	oh, yeah...they do. uggh.
Another thought, administrative accounts should be flag and not allow to be delegated	yes. there's a GPO for that.
Is there anything other than Quest - Change auditor to monitor for GPO changes and what those where?	Kent used to (iirc) manage a product that did this (monitor changes to GPO) at $previous_gig. this looks like a possible configuration solution via microsoft configuration https://www.lepide.com/how-to/audit-chnages-made-to-group-policy-objects.html
WPAD - DNS record Problem - Previous successful attacks domain names were hijacked and WPAD redirected	yes - not necessarily rare, but the DNS poisoning / injection attack has been demonstrated a few times here (BHIS tests)
You don't have to name names, but do you ever come across endpoint protection that does a good job of securing most of the vectors you listed in the first slide?	we will get there.
Should you always be running the latest functional level for AD?	Yes, it is best to keep up. You may have special reason to now and you probably want to test., Depends on the systems on your network. Windows 7 systems around? windows server 2003/2008 ? you may end up with problems escalating your functional level to "threshold" or 2016/2019
how about utilizing some sort of PAS/PAM (LAPS at least) for local administrator accounts?	We recommend LAPS, be careful tho, without ADSIEdit, the admPwd attribute is readable in your AD schema by anyone.
So something like Thycotic, CyberArk, etc. is better than LAPS...	THIS,But, we are discussing tools that don't cost anything.
Recommended WEC hardware specs per endpoint count?	Our test domain is generally 30 boxes, and we've never had more than one. but, scale is everything in computing life. scale out or scale up? this debate should go to the masses where people manage massive domains. out here in the sticks, most domains are like 30-50 users and 30-40 systems.
Sysmon to SIEM or Sysmon to WEC then SIEM?	great question. we use sysmon to WEC then on to SIEM. but, I guarantee you at least 50% of the time (response population standard deviation taken in to account) I'd be wrong :D
IPsec on workstations REALLY isnt that hard	right!?
The sysmon config file can be tweaked and break sysmon.	true
What was the powershell tool for grabbing logs remotely?	we've got a custom in-house thingy we use. It will be shared via someone's github and announced on some as yet undetermined media platform !
Cyber Ark is a PAM solution to manage local admin passowords with out using clear text passowrd storage	this, and can integrate with every kind of login you can imagine. as400 swapabbleCredential? yeah that one too (or so I've been told).
Are you going to dive further into WMI Filters and Loopback?	this is an interesting topic, the course at WWHF San Dieog will discuss these in depth.

Question Asked	Answer Given
Is there a risk since LAPS pw stored in comp AD acct and most admins only use local admin accts when servers have problems w their domain account..potentially deleting account and creds?	yeah, this is a risk. but, IMO a lesser risk than this finding: "*Widespread Local Administrator Account.*" I have experienced the scripted mimikatzing of an entire domain's server infrastructure because of a recovered local admin account.
In a small env you could configure a proxy for all and exclude only the sites you want them to access from using the proxy	I like this option. Outbound proxies offer so many great things. Start testing. Squid is free, can be ran in HA, and is highly configurable.
LLMNR removal is well documented. Any recommendations for how to disable/remove mDNS?	Discussion now.
Chrome on Windows can use mDNS	Good to know.
Have you attacked Windows Hello for business? I think it requires kereberos armoring on the server and credential guard on the clients?	I have not interacted with this service.
Doesn't windows 10 use port 7680 for sourcing windows updates to other local assets?	Windows 10 features a delivery optimization which enables machines to share downloaded updates with other machines on their local network and even out on the Internet. ... to the Internet even if only local network sharing is enabled). DO then leverages port 7680 to listen for incoming connections from peers.
add admins to Protected Users group and set their account to not be allowed for delgation	yes
using local firewall policy via GPO can get messy and delay troubleshooting. GPO is cleaner (opinion)	
What is the prefered method for deploying a host based firewall for endpoints, where products like lync use P2P connections for phonecalls etc	do not just turn them on. Configure rules for things that are allowed on ports you know are needed from only host netranges that are trusted. The term "baseline" is abused, but necessary. You do really need to understand your network's stack. We recommend services to ports to systems to NATs and back again as part of inventory management. nightmare? dang right. critical systems should be understood intimately :D - yeah I meant it.
Do you have a reccomended SIEM, also do you reccomend logging workstations to it as well as servers?	We use ELK / HELK / SecurityOnion because they're free. As far as ingests, we've never tipped one over logging everything. If you treat your workstations as your network perimeter (I think you should), logging is a requirement.
Im surprised you guys didnt talk about Net Session Enum blocking. can you make some reccomendations on that?	this is really cool. https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b - I need to investigate.
FYI in a gpo any thing you config under Secuirty Settings | Local Polices | User Rights Assigments and Local Polices | Security Options are Tattos. They don't revert back if the gpo goes away.	Hat tip,
SMB Relay checkign that reqirment AD Cert Servise to have a cert issue to every client pc?	Not required. This article gets deep in the weeds of SMB implementations over the years, but includes discussion about derivation of the SigningKey or SessionKey, which are agreed upon by the source and destination. The MiTM (relay attack) would be unable to derive this key properly. (My understanding) https://blogs.msdn.microsoft.com/openspecification/2017/05/26/smb-2-and-smb-3-security-in-windows-10-the-anatomy-of-signing-and-cryptographic-keys/
If you Block users running Power shell Blocks the best way to set users default printers in a Citirx VDI enviorment.	PowerShell scripts that execute printer settings at user logon, thus the scripts are executed as the authenticating user? I swear that I quit a good job because of Citrix Print Drivers.
Do you still recommend changing passwords every 90 days? NIST recommendations have changed.	Not if you are using long passwords. Web cast Dec 4
What about having 2 accounts for users who need to elevate privileges - admin account is prevented from login, and UAC is set to prompt for password every time	definitely a best practice.
Ever used RunAsTool from Sordum? Any comments on that tool?	I have not
If sysmon is enabled, do you still need all that other stuff?	Yes, for reasons undisclosed. I guess in the end sysmon doesn't give me event ID 4724 (password reset attempt) or 4776 (bad password attempted). It gives me event IDs 1 through 20 (or whatever) and that's fine, *too.*
Any recommendations to remove noise when blocking intra-workstation communication?	Block anything you don't need. What do you need interworkstation??
Recommended open-source ingester for sysmon info across workstations & servers? Graylog? ELK? etc.?	Its HELK right now. It's doing all the things I want it to.
Are there any known attacks or concerns with running windows delivery optimzation? As long as they don't go out to the internet for updates.	haven't had a chance to interact. it is an svchost process, but I have not checked things like dep, process migration...
what about the account setting "Account is sensitive and cannot be delegated". link that in a GPO to administrative accounts.	fantastic read here: https://www.cyberark.com/threat-research-blog/weakness-within-kerberos-delegation/
Have any of you guys used open source SOAR platforms?	no
If you are using WPAD, would disabling automatically detect settings and expliciting putting the wpad address in (via https) be an appropriate mitigation?	create the WPAD record in DNS
WIll any of this change for organizations moving to Azure AD for on-prem? *AD newbie*	Don't think so.
Would you recommend using: https://github.com/amarkulo/OpenPasswordFilter for filters based on dictionaries to NOT use with your AD Password? Or is this a freakin no-go?	Good practice. Test it first

Question Asked	Answer Given
I thought, smb signing is enabled by default for member servers in server 2019, but can cause issues with OSX.	SMB signing is available in all currently supported versions of Windows, but it's only enabled by default on Domain Controllers. This is recommended for Domain Controllers
best practices from microsoft for smb signing for member servers is for sure applied to member servers in 2019	thx
Deny logon as batch job > Deny "Company General Users" excluding Admins	nice
99% of the results are pages that go to MS support forums with the last reply consisting of sfc /scannow	
Is it better to consistenly update the desktop JRE with the quarterlies from Oracle and risk breakage of legacy third party sites/apps/interfaces, or lock down the JRE with a signed Deployment Ruleset with a whitelist approach...or both?	patch everything where applicable until you break it. we broke it, the customer just happened to have an app critical to their customer-facing services that relied on like java6-26. upward pressure. I hear oracle isn't the biggest fan of security testing (at least third parties). trust what you can, hope for the best.
Aren't these scripts to view users inside all of these groups alreday written and available somewhere? Why wouldn't I download and customize them for my environment?	I can't confirm or deny. Anyone?
Any suggestions for shipping off the PowerShell Transcripts to somewhere besides local storage?	this is an elegant solution to a pita problem imo: https://4sysops.com/archives/how-to-centralize-powershell-transcript-logs/
if we have sysmon but we are unablw to reach the attacker who is copying the script	
Are Macs/Samba also a mdns risk in AD environments?	they can be. especially because these systems are often integrated with domain functionality, including domain credentials for accessing things like file shares.
We're not using WPAD, does it make sense to create a WPAD dns record even when MDNS/NBNS is disabled? Learned about the Global Query Block list when testing this.... http://www.mpking.com/2010/02/wpad-does-not-resolve-in-dns.html	Yes - and this helps.
(re: question above - Pointing the WPAD record to 127.0.0.1 or such)	wpad 255.255.255.255 - this tip goes to another registrant. link to the initial elevation of privilege finding. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-077 - the article only discusses a hosts file entry. I've heard the DNS entry works the same, as NBT-NS is a fallback only if DNS doesn't work first.
We have devs that say they need to use WPAD for browser proxies -> Fiddler, Charles, etc. True/False?	To my knowledge, this is not a requirement. IE: WPAD can be resolved in DNS, which solves this problem generally. however, your devs may be doing their own thing on their subnet, whathaveyou, and are relying on the fallback mechanism to request the name via NBNS so they can delegate that IP as they see fit.
Please do a blog/webinar on AdminSDHolder - Trying to figure out how to enable/persist auditing on privileged group enumeration. net group "domain admins" /domain, for example	this will be a great blog post for us. in the mean time, this was informative: https://blog.stealthbits.com/persistence-using-adminsdholder-and-sdprop/
So in my environment I inherited the great setting of allow LM and NTLMv1 authentication. I want to shut this down but wondering if there is a easy way to find this type of authentication if it still exist?	This dude seems to have had the same problem you are up against: https://itconnect.uw.edu/wares/msinf/other-help/lmcompatibilitylevel/using-get-ntlmv1logonevents-ps1/ I cannot vouch for the integrity of the script, and without reviewing it closely, please be super cautious!
Any experience with OSSEC on Windows systems? Is it suitable in real production environments?	It has been a while, and we used OSSec for our Linux boxes. It is probably suitable -- but here's the real problem with open source solutions: support when you need it. If you break something critical and can't sort it out...who do you have to call?
couldn't we just deploy a windows firewall rule to block ports 137 - 139 inbound/outbound, and that would be far easier to deploy?	Do both....layers,it could be, but, are you fixing the problem? or just bandaiding it?
any comments about loopback policies?	
Hey guys do you know if Sysmon provides value over and above Defender ATP? Big fan of sysmon but deploying Defender ATP at the moment and wondering if it still warrants the additional log volume. Cheers!	ATP is amazing. Seriously amazing, was always a bit costly for us budget minded ($zero.zero) folks. But, this is a solution that can see through the user behavioral space time continuum.
Is that the DFL and FFL on 2016 or just having 2016 DC's in the environment that you have the 15 character password length available?	functional level upgrade required. We've just been wondering when PCI and microsoft will stop recommending the 7 character passwords.
I keep reading Microsoft is planning to do away with Maximum password age? Saying "They drive users to choose weaker passwords, re-use passwords, or update old passwords in ways that are easily guessed by hackers. So they're basically saying, the same, more complex password is more secure than changing them frequently with a weaker password. "	Correct
If WMI filters are not recommended, would you recommend splitting 32bit/64 bit workstations in separate OUs to apply policies by bit level? (Hopefully this is a non-issue soon enough with Win 7 EoL)	yes. but, I am also not super worried about the chip architecture when I'm deploying the base set of GPOs we are discussing.
Is it assumed everyone has migrated from FRS to DFSR replication these days? Experienced so many replication issues with FRS.	look at the big data on this guy! seriously though, keeping up with all the things is tough. there are literally sprawling functionality upgrades and changes across the Microsoft spectrum. It takes a lot of effort to keep up.

Question Asked	Answer Given
MBSA has been replaced by SCT: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10	thank you
With LAPS, that attribute is limited to Domain Admin by default. You have to delegate further.	nice
For moving to Azure AD, Firewall defaults to public profile and blocks far more than domain profile. Depending on setup, NTLM/Kerb attacks don't work the same either.	great tip.
For WPAD/LLMNR/NBNS disabling via DNS, see this article: https://blog.netspi.com/exploiting-adidns/	Great Tip
If you are using Event Viewer to view this stuff, you are doing it the hard way ;) Ship this stuff to a SIEM	RIGHT
Sysmon now has about 90% of what you are looking for. If you are configuring Sysmon for the first time, I'd start with something more easily digestible like Olaf's amazing work here: https://github.com/olafhartong/sysmon-modular	I was reviewing this recently. and agree - allows better configuration for a custom environmnet
For the question about protecting Sysmon, take a look at how to log and alert on this: https://posts.specterops.io/shhmon-silencing-sysmon-via-driver-unload-682b5be57650	this
For securing privileged identities, follow MS guidance: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material	good tip
With Protected Groups, be very careful with things like SQL AG's where you need kerb delegation. Your DBA accounts may stop working ;)	
RockNSM has handled our 2x 10G links better than Security Onion on the same box. Worth a look ;)	thanks!
You may be able to do all of this via ConfigMgr or whatever MDM you are using, and then you get reporting. GPO is great and free, but use other tools if you can get better reporting or less impact for sign in experience.	
Word of warning on SoS, it is not tuned well. It's supposed to be a starting point.	
If you are doing CIS controls, take a look at CSAT - it's incredibly helpful: https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/	good tip
You could also put a wildcard record in DNS and effectively break LLMNR, NBNS, and WPAD.	
osquery is amazing. Kolide Fleet on top of it is super cool: https://kolide.com/fleet	
Browsers have the ability to disable DoH built in: https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https	this is correct. great read too.
Kushtaka for honeypots! :)	
with LAPS will it create an account if you define one that doesn't exist?	LAPS does not create the account. a GPO can though.
Sysmon on endpoints only or servers as well?	servers too - 100%
What logs are most important to send to a siem?	OMG....just send stuff. Storage is cheap. Numerous recommmendations on logging out on the net. Validate on your own.
mDNS doesn't matter if you have turned on your host firewalls to block intrasubnet traffic incoming and outgoing.	good control!
Hostbased firewalls are the greatest things evar.	In the top 10
So simple. block workstation to workstation traffic. It shouldn't be necessary to begin with. No impact.	correct.
We just completed CIS 1.0, headed to next version soon. Any "gotachas" that you folks are aware of or any guidance on this topic?	No, you have to test everything
would you advocate completely removing other windows logging in favor of sysmon if configured well?	Answered by Kent and Jordan.,Answered by Kent and Jordan.
not all GPOs are tattoos, if they're in the policy keys, they usually unconfigure properly. (usually)	thx
Hello for business uses public/private keys (either cert-based or just locally generated in the domain) to authenticate instead of a password. The private key is stored in the TPM on an individual system.	
Also, WMI filters are not all created equally. A simple 32/64-bit check is not terribly taxing.	k
how do we deal with sccm still relying on port 135? if we are to block that on local endpoints	
how do you keep workstations from talking to each other?	Host based firewalls

Question Asked	Answer Given
Dont the default domain policies have a specific guid and are referenced and used specifically for password policies. i normally remane them and only use them for specific reasons like password policies.	I can't speak to the GUID. but yes otherwise, password policy (unless you are defining fine grained ones) should be applied at the domain level.
How about pingcastle?	I cannot endorse it specifically, because I haven't used it.
I heard mention of a script for deploying AD users/groups in a lab environment. Is that publicly available?	we will make our scripts on github along with the videos. ova's too.
github.com/clong/detectionlab is a great resource for labbing up logging and detection, includes WEC/WEF, Sysmon, OSQuery, and much more	This is worthy of a share
Account partitioning is a best practice according to Microsoft	
do the windows 10 IOT builds support GPO ?	I deployed iot on a pi, and we broke that thing extensively -- treated it as a marketing monitor -- but did not test gpo
@Kent and Jordan, did you ever had to argue with blue team people about SMB Signing, that enabling it will cause performance issues? If yes, how did you convince them to still enable SMB Signing?	Yes, this is definitely a thing. Kent addressing this now. ,Well, its almost 2020 and people don't authenticate over 56kbps anymore, so... :)
RSOP is also deprecated - the current recommendation is GPRESULT.EXE /H filename.htm	
yes	whoa, thank you !!! again, I have relied on the guy to my right for this for a long time
how do you go about getting the transcripts into centralized logging (SIEM)?	Ah pipe it.
We use a product called Secret Server for local account password rotation/storage. Much easier than LAPS, but $$	Hat Tip
We've been testing firewall enabled with the "Apply local firewall rules" and "local connection security rules" to try to soften the pain of enabling firewall. Will these settings cause pain if we leave them enabled?	Let's hive mind this one.
Laps is readable by account operators too, not just DA.	beautiful. will investigate.
How to send the sysmon logs to a centralized monitoring system/siem?	Easy
Isn't there a GPO to prevent the storage of LM Hash even if your password is under 15 chars? I thought it was done by default in WS2008+ (I think)	yes, mentioned soon.
PAM = Privileged Access Management, PAS = Privileged Access Solution (at least, if you follow CyberArk PAS naming)	Hat Tip. Also CyberArk is awesome.
Should you disable the NBT ONLY on the actual network interfaces (wired, wireless), or all of them (like loopback, connected devices, etc.)?	I have never touched the loopback adapter, but the script in that screenshot might.
What about tech support accessing the client computer via \\$COMPUTER-NAME\c$ the drive? They should work from a Jump Server (an actual Windows Server) instead?	Jump server is an excellent practice
Regarding Windows 10 and port 7680, this is true when WU is configured to work in a "P2P" mode, however, can be easily disabled via GPO (Computer Configuration\Administrative Templates\Windows Components\Delivery Optimization\\Download Mode)	thx
We all like logs and want all the logs too. Might be too much in some environment (for whatever reason there is). Relying on the recommendations from the Microsoft Security Baselines for Advanced Audit Policy still works? Or should we enable all of them (with Success/Failure)?	all of them, imo. sadly can get to be a disaster at the ingestor or log storage device. Security Baselines are awesome too.
When you talk about "service accounts", do you mean normal User accounts (in AD) with a special naming convention (ex: svcLDAPPaloAlto) OR do you talk about ACTUAL Managed Service Account?	Latter
Doesn't Sysmon logging have some overlap with Advanced Audit Policies? If so, would you still enable them both, or just use Sysmon to monitor what the Advanced Audit Policies can't monitor?	Yeah, back to our research... all of that work only to realize sysmon did most of what we want. so, we still recommend both
All these are great recommendations and all of us agree that they should be implemented however, we'll most likely all hit the same wall... Selling these to the management, and the user and also convincing them that these "low hanging fruits" can really change everything during a pentest/red team/actual hack. What would be the best way to go about it?	Cost benefits. Find things with big impacts for low costs. Present it as such to Mgmt. Speak their language
It's like SSID cloaking, "security through obscurity" doesn't always works. With the automation available today, it won't slow down the attackers by much (about renaming the local Admin account).	

Question Asked	Answer Given
No need to test patches in DEV, QA and Pre-Prod. Roll it straight to Prod. #LivingOnTheEdge	nice environment
do you recommend seperate Admin users for servers vs workstations?	Interesting idea. Cost benefit for effort vs segmentation / least priv. DB Admins should be separate right?,yes. and we generally drop sec_wksadmins on WKS and sec_serveradmins on Servers. The desktop management group is handled by help desk, server team deals with servers.
Do you recommend disabling SMB 1 now that SMB 2 and 3 are more available?	upcoming
What is the workstation is being used for a printer that is only USB?	fine grain your firewall policies
How about blocking USB without it being encrypted by BitLocker?	removable media is a risk
Would you have a set of GPOs you would recommend as your best practices that is presetup that we could import into the GPO Manager?	this is something we will work on releasing as part of our github project for the explicit purpose of sharing our windows dowmain scripts, powershell tools, etc.
Would you have a set of GPOs you would recommend as your best practices that is presetup that we could import into the GPO Manager?	that is a great idea.
What is your opinion on placing servers in the DMZ? Would you include workstations also?	I consider workstations a network perimeter and consider them hostile by nature. This addresses the front end of the user dilemma -- you cannot trust the users on your network.
What is your opinion on placing servers in the DMZ? Would you include workstations also?	Segment everything logically
Any BIOS tips you would have for security?	BIOS passwords are cool. I have used KonBoot on an engagement. BIOS password would have stopped me from gaining local admin access
Why would you guys set the Guest account status as Not Defined instead of Disabled?	from a high level perspecitive, we have only at best rarely escalated this way.
Have you used Net Cease to deter the use of Bloodhound by red teamers?	we don't but we are attackers.
It is possible to change the service and exe name of sysmon when deployed to hide it a bit more. We also put our sysmon config on a share that is only accessible to domain computers (not domain users) to further protect it.	I have never considered this and do not know. We asked the hive mind for a few other items. Can anyone help us with this? I assume that you can...I mean I was on a test where Kelsey just copied and renamed PowerShell.exe and it worked (service name is another story)
We recently restricted the SeDebugPrivilege from our domain users for workstations. Are there other privileges like that to stop Mimikatz from running/being successful?	limit escalation opportunities up front. Mimikatz requires elevated context. this article discusses this question in depth. https://medium.com/blue-team/preventing-mimikatz-attacks-ed283e7ebdd5
is it a good idea to creat honey pots in the network ? if yes plz suggest some open source	yes. canarytokens. sensitive file names and triggers. this tool will email you if something is opened that shouldn't be.
any thing about honeypots ?? is it good to have ??	check out canary tokens.
I wish there was a tool or set of simple guidelines that we could drop to a client 2-3 weeks before testing to take care of the low-hanging fruit/Barney-style screw ups when a client has a total mess of an AD implementation or they're trying to glue together several different domains after a merger or acquisition. Just basic stuff you know? So that the beginner/intermediate sys admin doesn't get destroyed on a test they had no chance of doing well on in the first place.	Very well said...this is interesting -- and we had an old webcast / blog about preparing for a pentest
Has you guys seen the windows logging cheatsheets from malwarearchaeology.com? Love to see something like that for AD Security	We'll check it out!,Hey that's a pretty cool idea. :-)
Look at Windows Loggin Cheatsheets from malwarearchaeology.com	Good Tip
Windows 7 and older Server OSes will still be around. Microsoft is offering extended security updates on a Pay-to-play model through 2023.	wow.
Does sysmon capture login events?	yup. check out swiftonsecurity's config file.
Default Domain policy is special for password policy if you do try to move it	accurate.
For the love of all that is holy don't disable the Web Proxy Auto Discovery service either. Every single application that loads WinHTTP will do the lookups individually.	good tip
With 15 characters passwords, brute force is not gonna happen at any rate	correct,no, but dictionary attacks still work. recent test, still got DA, dump ntds.dit and executed a dict attack -- rockyou + rockyou & rockyou + crackstation was about 30% of passwords
What if we're following NIST 800-63-3? Thoughts on doing 16 char minimums w/ No complexity, etc?	https://xkcd.com/936/
If you have appropriate Microsoft 365 licensing, Azure ATP can provide most of the capability that bloodhound does from a blue team standpoint.	good tip

Question Asked	Answer Given
Turning off Automatically detect settings causes Office Click to run installations to not update automatically. (obviously Microsoft should fix this, but they haven't yet).	thank you
Do you feel that if an org has all the pre-reqs in place and implements these things that the org may be ready for assumed breach testing?	Yes - one sec, we're on it
Will the configs detailed within this webcast assist in limiting the impact of bloodhound?	potentially, bloodhound isnt a dastardly tool, necessarily. BH is denied to enumerate active directory control paths and can be an amazing blue team tool. Detecting unexpected BH execution will be detailed,*not denied, *DESIGNED
So when event logs are forwarded, will this severely impact data ingestion? I keep hearing that the amount of data ingested by forwarders/siem is a big pain point for management due to cost/performance impact. Is it environment dependant or can you expect it to generate a bit of logs/data.	expect to create a lot of logs. over time, refine your process.
bit off topic, as someone who is still new to security (coming up on 2 yrs in the soc) are there any resources I should ENSURE I'm ingesting? I'm trying to read as much as I can but trying to make sure I'm finding GOOD resources rather than whatever I find through google.	sysmon, ossec, osquery. use helk. start capturing network flows via pcaps. ingest those with bro. these are the basics.
re LDAP and nested groups, if your LDAP application lets you set your search string, you can check nested groups with something like this	Answer 1 of 2
Any input on flavors of sysmon config? SwiftOnSecurity/TaySwift seems popular.	we have relied on the default SOS config with a modification to not report on AV touching lsass...
Does anyone recommend an inexpensive and EASY SIEM?	HELK!
If using a DNS wildcard, use a very low TTL so you aren't contributing to a potential resource exhaustion attack	this.
IF you disable LLMMR and Netbois, Does it stop your machine from asking for WPAD	no. browser configuration also necessary.
Do you feel that WEF, sysmon, osquery and an ELK stack are comparable to commercial tools, like splunk?	Yes. definitely
If you re-create local admins w/GPO, what password do you set for them? Passwords change periodically - who maintains the passwords set by GPO?	Create/Overwrite local admins with GPO. Manage their passwords with LAPS, limit access to AdmPwd attribute in schema. Or use a third party service.