Securing Microsoft Integrated DNS in response to

DHS Emergency Directive 19-01

Ву

Marc van Kralingen

Marc.vankralingen@Quest.com

Summary

On January 22, 2019 the U.S. Department of Homeland Security released Emergency Directive 19-01 entitled "Mitigate DNS Tampering" (DHS, 2019-1). Within this directive, the DHS describes how, in coordination with other partners, it has been tracking a series of incidents involving Domain Name System (DNS) infrastructure tampering. The directive goes on to describe the techniques used to perfect this attack, the net result of which is that attackers can redirect and intercept web, mail, and other network traffic. The directive recommends the following four actions:

- 1. Audit DNS records
- 2. Change DNS account passwords
- 3. Add Multi-factor authentication to DNS accounts
- 4. Monitor Certificate Transparency logs.

This discussion demonstrates the use Quest Software to perform action (1) above: audit DNS records for Microsoft Active Directory-Integrated DNS.

Background

Microsoft Active Directory Integrated DNS

DNS is foundational to a properly functioning Active Directory deployment (Microsoft, 2014). In fact, DNS is the primary name resolution service for Windows Server 2003 and later. As such, Active Directory requires:

- A name resolution service that enables network hosts and services to locate Active Directory domain controllers
- A naming structure that enables an enterprise to reflect its organizational structure in the names of its directory service domains.

This service is referred to as Microsoft Active Directory-Integrated DNS.

Quest Change Auditor

Change Auditor is a real-time security and IT auditing solution for your Microsoft environment. Some of the key features of Change Auditor include:

- Proactive threat detection with Change Auditor Threat Detection
- Hybrid environment auditing with a correlated view
- Change prevention
- Auditor-ready reporting

More information on Quest Change Auditor can be accessed here: <u>https://www.quest.com/change-auditor/</u>

Change Auditor Auditing of DNS

Quest Change Auditor supports the auditing of 99 distinct DNS-related events such as addition and removal of DNS A, MX and PTR records. See illustration 1 below.

		dministrati			1	
Auditing	0 Edit	High	🔺 Medium	Low	🔵 En	able
Configuration	License	Type ^				
Audit Events	Severity			ility Name		
Excluded Accounts (13)	Z A		A	ritty Name		
Directories			الطا			
Active Directory (3)	± License	Type : Activ	e Directory (8	9 items)		
Attributes	💻 License	Type : Exch	ange (10 items)		
Member Of Group (0)						
Excluded AD Query (6)						
ADAM (AD LDS) (2)						
Attributes						
Azure Active Directory (1)						
Applications						
Exchange Mailbox (11)						
Office 365 (1)						
VMware (1)						
SharePoint (1)						
Skype for Business (0)						
SQL						
SQL Server (7)						
SQL Data Level (2)						
Server	-					
File System (31)						
Registry (4)						
Services (1)						
P NAS						
EMC (0)						
NetApp (1)						
FluidFS (0)						
Configuration						
`						

Illustration 1: Change Auditor auditing of DNS events

What is helpful is that Change Auditor organizes and prioritizes (out-of-the-box) all DNS events by Severity type (the severities are configurable). See illustration 2 below.

Start X Overview X Sea	rches X Administration Ta					
Auditing	🖉 Edit 📕 High 🔺	Medium 🜒 Low 🕚 Enable 🔳 Disable 🔟 Default 🛈 Knowledge Base 🚔 Print	×.			
Configuration	License Type	1				
Audit Events	Facil	lity Name 🗠				
Excluded Accounts (13)	Severity	∧ Event Class	∽ Status	Results		
Directories		I DNS		A		
Active Directory (3)	License Type : Active Dire	antony (7 itama)	2,243			
Attributes	Martin Control of Cont					
Member Of Group (0)	A Medium	uration Monitoring (7 items) Connection DNS Registration option changed	Enabled	All Result		
Excluded AD Query (6)	A Medium		Enabled	All Result		
ADAM (AD LDS) (2)		Connection-specific DNS Suffix changed	Enabled	All Result		
Attributes	A Medium	Contents of DNS server list changed				
Azure Active Directory (1)	A Medium	Contents of DNS suffix list changed	Enabled	All Result		
Azure Active Directory (1) Applications Exchange Mailbox (11) Office 365 (1)	A Medium	Update DNS on all adapters setting changed	Enabled	All Result		
	A Medium	Use Connection Suffix in DNS Registration option changed	Enabled	All Result		
	A Medium Use of dynamic DNS changed Enabled					
VMware (1)	a constructive sector and a sector of the se	AD Object Monitoring (3 items)				
SharePoint (1)	Low	dnsZone description changed	Enabled	All Result		
Skype for Business (0)	📥 Medium	dnsZone changed	Enabled	All Result		
SQL	📥 Medium	dnsZone nTSecurityDescriptor changed	Enabled	All Result		
SOL Server (7)	🛨 Facility Name : Custom	ADAM Object Monitoring (61 items)				
SQL Data Level (2)	H Facility Name : DNS Ser	nvice (2 items)				
Server	Facility Name : DNS Zo	ne (14 items)				
File System (31)	Low	DNS A record added	Enabled	All Result:		
Registry (4)	Low	DNS A record modified	Enabled	All Result:		
Services (1)	Low	DNS A record removed	Enabled	 All Result: 		
NAS	Low	DNS AAAA record added	Enabled	All Result		
EMIC (0)	Low	DNS AAAA record modified	Enabled	All Result		
20 C	Low	DNS AAAA record removed	Enabled	All Result		
NetApp (1) FluidFS (0)	Low	DNS CNAME record added	Enabled	All Result		
<i>a</i> .	Low	DNS CNAME record removed	Enabled	All Result		
Configuration	Low	DNS MX record added	Enabled	All Result		
2	Low	DNS MX record removed	Enabled	All Result		
Auditing	Low	DNS PTR record added	Enabled	All Result:		
0	Low	DNS PTR record removed	Enabled	All Results		
Protection	Low	DNS SRV record added	Enabled	All Results		

Illustration 2: Categorized and prioritized Change Auditor DNS events

Change Auditor provides out-of-the-box reporting against DNS events with easily configured filters such as who, what, when, where, and origin computer. See illustration 3 and 4 below.

Click here to filter data Image: Save Right Structure Image: Click here to filter data Image: Click here to filter data <th>Start X Overview X Searches X Administr</th> <th>ation Tasks 🗙 All DN</th> <th>S Events* 🛛 🕹</th> <th></th> <th></th>	Start X Overview X Searches X Administr	ation Tasks 🗙 All DN	S Events* 🛛 🕹		
Severity Time Detected Subsystem User Computer Action Faci Click here to filter data Image: Computer interval: interval: Image: Computer interval: From: Image: Computer interval: Faci	🔍 Search Properties 😑 Event Details 🖶 Print 🔊				
Click here to filter data Image: Save Right Structure Image: Click here to filter data Image: Click here to filter data <th>Event ^</th> <th></th> <th></th> <th></th> <th></th>	Event ^				
Citick here to filter data Image: Structure of the struct	🚰 Severity Time Detected 💛 Subsystem Use	ſ	Computer	Action	Facili
d Event : DNS A record removed (1059 items) d Event : DNS CNAME record added (7 items) d Event : DNS CNAME record removed (5 items) d Event : DNS MX record added (1 item) d Event : DNS PTR record added (2614 items) d Event : DNS PTR record removed (3146 items) d Event : DNS PTR record removed (3146 items) d Event : DNS SRV record added (39 items) d Event : DNS SRV record removed (22 items) d Event : Log File Path changed (1 item) d Event : Log File Path changed (3 items) d Event : Log File Path changed (3 items) d Event : Name server added (2 items) d Event : Name server added (2 items) d Event : Service log level changed (310 items) d Event : Zone added (3 items) d Event : Zone adlow dynamic updates flag changed (1 item) Info Mho What Where When Origin Atert Report Layout Save Save As * Pate Interval: From: To:			A	A	A
± Event : DNS CNAME record added (7 items) ± Event : DNS CNAME record removed (5 items) ± Event : DNS MX record added (1 item) ± Event : DNS PTR record added (2614 items) ± Event : DNS PTR record removed (3146 items) ± Event : DNS SRV record added (39 items) ± Event : DNS SRV record added (39 items) ± Event : DNS SRV record added (39 items) ± Event : Log File Path changed (1 item) ± Event : LogFileMaxSize setting changed (3 items) ± Event : Name server added (2 items) ± Event : Service log level changed (310 items) ± Event : Zone added (3 items) ± Event : Zone added (3 items) ± Event : Zone added (3 items) ± Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Atert Report Layout To:	⊈ Event : DNS A record added (1063 items)				
± Event : DNS CNAWE record removed (5 items) ± Event : DNS MX record added (1 item) ± Event : DNS PTR record added (2614 items) ± Event : DNS PTR record removed (2146 items) ± Event : DNS SRV record added (39 items) ± Event : DNS SRV record removed (22 items) ± Event : Log File Path changed (1 item) ± Event : LogFileMaxSize setting changed (3 items) ± Event : Name server added (2 items) ± Event : Primary server changed (310 items) ± Event : Zone adlew dynamic updates flag changed (1 item) Info Mno What Where When Origin Alert Runtime Prompt Date Interval: From: To: Time Interval: From:	L Event : DNS A record removed (1059 items)				
d Event : DNS MX record added (1 item) d Event : DNS PTR record added (2614 items) d Event : DNS PTR record removed (3146 items) d Event : DNS SRV record added (39 items) d Event : DNS SRV record removed (22 items) d Event : Log File Path changed (1 item) d Event : Log File Path changed (1 item) d Event : LogFileMaxSize setting changed (3 items) d Event : LogFileMaxSize setting changed (3 items) d Event : Primary server added (2 items) d Event : Primary server changed (310 items) d Event : Zone added (3 items) d Event : Zone added (3 items) d Event : Zone added (3 items) d Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout To:	L Event : DNS CNAME record added (7 items)				
El Event : DNS PTR record added (2614 items) El Event : DNS PTR record removed (3146 items) El Event : DNS SRV record added (39 items) El Event : DNS SRV record removed (22 items) El Event : Log File Path changed (1 item) El Event : Log File MaxSize setting changed (3 items) El Event : Name server added (2 items) El Event : Primary server changed (310 items) El Event : Service log level changed (2 items) El Event : Zone added (3 items) El Event : Zone added (3 items) El Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As ▼ ● Preview Changes From: To: ▼ To: ♥ To: ▼ To: ♥ T	L Event : DNS CNAME record removed (5 items)				
± Event : DNS PTR record removed (3146 items) ± Event : DNS SRV record added (39 items) ± Event : DNS SRV record removed (22 items) ± Event : Log File Path changed (1 item) ± Event : LogFileMaxSize setting changed (3 items) ± Event : Name server added (2 items) ± Event : Primary server changed (310 items) ± Event : Service log level changed (2 items) ± Event : Zone added (3 items) ± Event : Zone added (3 items) ± Event : Zone aldow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout To:	t Event : DNS MX record added (1 item)				
Event : DNS SRV record added (39 items) Event : DNS SRV record removed (22 items) Event : Log File Path changed (1 item) Event : Log File MaxSize setting changed (3 items) Event : Name server added (2 items) Event : Primary server changed (310 items) Event : Service log level changed (2 items) Event : Zone added (3 items) Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As * ● Preview Changes Runtime Prompt Date Interval: From: To: To: From: To: To: To: To: To: To: To: To: To: To	t Event : DNS PTR record added (2614 items)				
ti Event : DNS SRV record removed (22 items) ti Event : Log File Path changed (1 item) ti Event : LogFileMaxSize setting changed (3 items) ti Event : Name server added (2 items) ti Event : Primary server changed (310 items) ti Event : Service log level changed (2 items) ti Event : Zone added (3 items) ti Event : Zone added (3 items) ti Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As * • Preview Changes Runtime Prompt Date Interval: From: To: To: To: To: To: To: To: To: To: To	t Event : DNS PTR record removed (3146 items)				
d Event : Log File Path changed (1 item) d Event : LogFileMaxSize setting changed (3 items) d Event : Name server added (2 items) d Event : Primary server changed (310 items) d Event : Service log level changed (2 items) d Event : Zone added (3 items) d Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As * ● Preview Changes Runtime Prompt Date Interval: From: To: From: To: To: To: To: To: To: To: To: To: To	tl Event : DNS SRV record added (39 items)				
ti Event : LogFile/MaxSize setting changed (3 items) ti Event : Name server added (2 items) ti Event : Primary server changed (310 items) ti Event : Service log level changed (2 items) ti Event : Zone added (3 items) ti Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As ▼ ● Preview Changes Runtime Prompt Date Interval: From: To: From: To: To: To: To: To: To: To: To: To: To	tl Event : DNS SRV record removed (22 items)				
Event : Name server added (2 items) Event : Primary server changed (310 items) Event : Service log level changed (2 items) Event : Zone added (3 items) Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As ▼ Preview Changes Runtime Prompt Date Interval: To: ▼ To: ♥ T	≝ Event : Log File Path changed (1 item)				
t Event : Primary server changed (310 items) t Event : Service log level changed (2 items) t Event : Zone added (3 items) t Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As * ● Preview Changes Runtime Prompt Date Interval: From: To: From: To: To: To: To: To: To: To: To: To: To	≝ Event : LogFileMaxSize setting changed (3 items)				
Event : Service log level changed (2 items) Event : Zone added (3 items) Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As ▼ ● Preview Changes Runtime Prompt Date Interval: To: ▼ To: ♥ To:	🖞 Event : Name server added (2 items)				
tl Event : Zone added (3 items) tl Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As * • Preview Changes Runtime Prompt Date Interval: From: To: From: To: To: To: To: To: To: To: To: To: To	법 Event : Primary server changed (310 items)				
tl Event : Zone allow dynamic updates flag changed (1 item) Info Who What Where When Origin Alert Report Layout Save Save As * Preview Changes Runtime Prompt Date Interval: From: To: From: To: To: To: To: To: To: To: To: To: To	t Event : Service log level changed (2 items)				
Info Who When Origin Alert Report Layout Save Save As * • Preview Changes Runtime Prompt Date Interval: Time Interval: • From: • To: • From: • To: •	tl Event : Zone added (3 items)				
B Save B ▼ ● Preview Changes □ Runtime Prompt □ From: To: □ From: To:	d Event : Zone allow dynamic updates flag changed (1 it)	em)			
Runtime Prompt Date Interval: From: To: From: To:	Info Who What Where When Origin Alert	Report Layout			
Date Interval: Time Interval: From: To:	🗐 Save 🔚 Save As 🔻 오 Preview Changes				
From: To: To: To:	Runtime Prompt				
	Date Interval:	Time Interval:			
		1			1000
Vers	From: To:	From:	🛨 To:		Ī
	🗹 Last: 1 🗮 Years	1			
				4.0000	
This: Week Reset	This: Week			Reset	

Illustration 3: Change Auditor out-of-the-box configurable reporting on DNS event

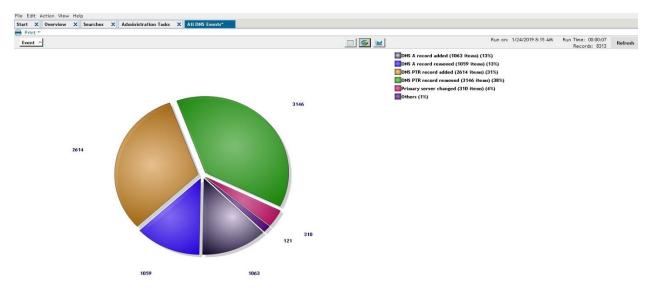


Illustration 4: Change Auditor graphical representation of DNS event auditing

The actual data is normalized and is easy to interpret. See illustration 5 below.

MEM1 - Remote Desktop		
🚳 Change Auditor [connected to app2.titancorp.local - DEFAULT] as user [Marc vanKralingen (TITANCORP)]		8 ×
File Edit Action View Help		
Start X Overview X Searches X Administration Tasks X All DNS Events		
🔍 Search Properties 🗏 Event Details 🚍 Print *		
Event ^	Run on: 1/24/2019 8:39 AM Run Time: 00:00:00 Records: 2 Refr	esh
2 Severity Time Detected V Subsystem User Computer Action Facility Site Domain Result	Kederus, z	_
Click here to filter data		
브 Event : DNS A record added (1 item)		_
Del low 1/24/2019 8:39 AM Active Dir., TITANCORPInvankralingen DC1 Add Attri., DNS Zone Titancor., TITANCO., Success		
Event : DNS A record removed (1 item)		
📓 Copy 🗵 Email 🚍 Print 🖲 Knowledge Base 🛼 Comments 🗈 Disable 🔍 Related Search * 🟵 Add to Search * 🕼 Restore Value		×
Low Severity		
A Who: TITANCORPInwankralingen (Marc vanKralingen)	() When: 1/24/2019 8:39:01 AM	
I Source: Change Auditor	Origin: dc1.titancorp.local (10.1.146.10))
What: The DNS A record myfoothold has been added to zone titancorp.local.	Result: Success	
Active Directory Action: Add Attribute	Facility: DNS Zone	
Class: Class: dnsNode Attr: dnsRecord	Type: Static SSL/TLS: No	
Object: titancorp.locaUSystem/MicrosoftDNS/titancorp.locaU/myfoothold	Sign/Seal: Yes	
From: +Not Set		
To: 10.1.146.200		
Terretaria de la construcción de la		
	0.40.4	_
🖉 Start 💑 🔼 🚞 💽 🚳 🛩 👗 🛼	* 🕞 🐑 🚯 8:40 A	19

Illustration 5: Normalized and easy-to-interpret DNS events

Change Auditor also provides near real-time alerting of the DNS events that you want to be alerted on. See illustrations 6 and 7 below.

<u>Illustration 6</u>: Configuring near real-time alerting over DNS events

Add Who G To C Co Boo Add Users G To C Co Boo Add Users G To C Co G Boo Add Managers G To C Co G Boo OK Can Save Save As * O Run Alert Enabled ert Configuration: Send Alert To: SNMP WHI I SMTP Configure Email History Search Limit: 50000 S Events Per Email: 100 S Sand Alert When:			To: Cc: Boo:	marc.vankralingen@que	st.com	
Add Who G To C Co G Boo Add Users G To C Co G Boo Add Users G To C Co G Boo Add Users G To C Co G Boo OK Can Save S Save As * • Run Alert Enabled ert Configure Email Send Alert To: SNMP WHI M SMTP Configure Email History Search Limit: 50000 S Events Per Email: 100 S				ChangeAuditor %ALERT_	TYPE% from %ALERT_COORI	DINATOR_NAME%: %ALER
History Search Limit: 50000 😴 Events Per Email: 100 😴 Send Alert When:	o Who What Where When Origin Save 扁 Save As * ● Run	Alert Report Layout		□ Add Who © To □ Add Users © To	CC CBCC	Configure Body OK Cancel
Send Alert To: SNMP WHI Image: SMTP Configure Email History Search Limit: 50000 mm Events Per Email: 100 mm						1
(UTC-07:00) Arizona 1 Events Occur Within 1 Hinutes T	Send Alert To: SNMP 🗆 WMI		100 ÷ sen	d Alert When:	cur Within 1	

Illustration 7: Near real-time alerts over DNS change events

Quest® ChangeAuditor® Alert

All DNS Events

	DNS Zone: The DNS A record myfoothold has been removed from zone titancorp.local
Name	Value
Coordinator Domain\Name:	sitraka.com\SWCA1
Agent Domain\Name:	TITANCORP\DC1
Date/Time Detected:	1/24/2019 9:33:19 AM -07:00 - (UTC-07:00) Arizona
Date/Time Received:	1/24/2019 9:33:48 AM -07:00 - (UTC-07:00) Arizona
Source:	Change Auditor
User:	TITANCORP\mvankralingen
Initiator:	
Origin Server:	dc1.titancorp.local
Origin IPv4:	10.1.146.101
Agent:	DC1
Action:	Delete Attribute
From:	10.1.146.200
To:	
Result:	Success
	DNS Zone: The DNS A record myfoothold has been added to zone titancorp.local.
Name	Value
Coordinator Domain\Name:	sitraka.com\SWCA1
Agent Domain\Name:	TITANCORP\DC1
Date/Time Detected:	1/24/2019 9:33:38 AM -07:00 - (UTC-07:00) Arizona
Date/Time Received:	1/24/2019 9:34:08 AM -07:00 - (UTC-07:00) Arizona

Lastly, in addition to the detective security controls described above, Change Auditor also supports preventative security controls through its object protection capabilities. Change Auditor object protection allows you to select critical objects in your environment and protect them from changes. This protection can be enforced at the object level (ex: don't delete the object) or at the attribute-level (ex: prevent modifications to the password attribute). This protection uses a whitelist/blacklist to specify who is or is not allowed to bypass the protection. Furthermore, protection can be enforced using a schedule and/or the origin IP address of the account attempting the change. The events pertaining to protected events are audited, can be reported on, and alerted on. See illustrations 8 to 10 below.

	S record Protection Template							
Find:	dnsNode	-	Name:	Miss	<u>হ</u>	ANR	Search	5
Name	^ Canonical Name					Туре		Browse
Click here	e to filter data					A		e
								options
4								-
 ▲ <u>A</u>dd 	<u>∧ R</u> emove Import	1			_]	1 lt	em(s) found	-
		ass	Ор	erations	Scope		لے em(s) found	-

Illustration 8: Creating a DNS record protection template

<u>Illustration 9</u>: Setting DNS record protection levels

Attributes	<u>^</u> _	Selected A			^
Click here to filter data	- 10 million		to filter data		
accountExpires	> Ac	bb			
accountNameHistory	K Rem	iove			
aCSAggregateTokenRatePerUser					
aCSAllocableRSVPBandwidth					
aCSCacheTimeout					
aCSDirection					
aCSDSBMDeadTime					
aCSDSBMPriority					
aCSDSBARefresh					
aCSEnableACSService					
aCSEnableRSVPAccounting					
aCSEnableRSVPMessageLogging					
aCSEventLogLevel					
aCSIdentityName					
Select one or more attributes and cli	ick the Add button on to remove prote		Select one or	more protec	ted

Illustration 10: Reporting on protected/prevented DNS activities

Severity Time Detected Subsystem User Event Click here to filter data Image: Subsystem Image: Subsystem Image: Subsystem Image: Subsystem I Low 1/25/2019 8:18 AM Active Dir TITANCORPUmvankralingen DNS A record removed I Low 1/25/2019 8:18 AM Active Dir TITANCORPUmvankralingen DNS A record removed I Low 1/25/2019 8:18 AM Active Dir TITANCORPUmvankralingen DNS A record removed I Low Severity Image: Subsystem Image: Subsystem Image: Subsystem Image: Subsystem Who: TITANCORPUmvankralingen (Marc vanKralingen) Image: Subsystem Image: Subsystem Image: Subsystem I No NS A record MissionCriticalHost has been removed from zone titancorp.local. Image: Subsystem Image: Subsystem Image: Subsystem I What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Image: Subsystem Image: Subsystem Image: Subsystem I What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Image: Subsystem Image: Subsystem Image: Subsystem Image: Subsystem Image: Subsystem I Matchive Directory Class	art X (Overview 🗙 Se	arches 🗙 A	dministration Tasks 🗙 🗚	ll Protected DNS Events 🛛 😤			
g a column header here to group by that column. Records: 1 Severity Time Detected ✓ Subsystem User Event Class: □ Active Dir TITANCORP\mvankralingen DVS A record removed Class: □ Arnovledge Base ⓑ Comments □ Disable ♀ Related Search +	Search Pr	roperties 💷 Eve	nt Details 🛛 🔚	Print *				
New 1/25/2019 8:18 AAA Active Dir TITANCORP\mvankralingen DNS A record removed Low 1/25/2019 8:18 AAA Active Dir TITANCORP\mvankralingen DNS A record removed Copy Semail Print * ③ Knowledge Base Ego Comments Disable ④ Related Search * ④ Add to Search * Low Severity Swho: TITANCORP\mvankralingen (Marc vanKralingen) ⑤ When: 1/25/2019 8:18:02 AM Who: TITANCORP\mvankralingen (Marc vanKralingen) ⑤ When: 1/25/2019 8:18:02 AM 〇 Origin: dcl.titancorp.local (10.1.146) What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. ● Origin: dcl.titancorp.local (10.1.146) What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. ● Result: Protected ● Active Directory Action: Delete Attribute Facility: DNS Zone Class: □ dnsNode Attr: dnsRecord Type: Static StL/TLS: Prom: 10.1.146.223 10.1.146.223 Sign/Seal: ● Sign/Seal: ●	g a columi	n header here to g	roup by that co	lumn.		Run on: 1/25/2019 8:1		Refre
Low 1/25/2019 8:18 AM Active Dir TITANCORPImvankralingen DNS A record removed Copy Email Print * ① Knowledge Base Disable Related Search * ① Low Where: DC1 Source: Change Auditor ① Origin: dc1.titancorp.local (10.1.146) Where: DC1 Source: Change Auditor ② Origin: dc1.titancorp.local (10.1.146) What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. ● Result: Protected What: InsRecord Type: Static SSL/TLS: Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal: From: 10.1.146.223 10.1.146.223	Severity	Time Detected	~ Subsystem	User	Event			
Copy Email Print * ③ Knowledge Base Bo Comments Disable Related Search * ④ Add to Search * Low Severity Who: TITANCORP\mvankratingen (Marc vanKratingen) When: 1/25/2019 8:18:02 AM Who: TITANCORP\mvankratingen (Marc vanKratingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Result: Protected What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Result: Protected What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Result: Protected Class: dnsNode Attr: dnsRecord Type: Static From: 10.1.146.223 Sign/Seal: Sign/Seal:	lick here	to filter data	A	A	A			
Low Severity Who: TITANCORPUmvankralingen (Marc vanKralingen) Where: DC1 What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: IndixNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost From: 10.1.146.223	Low	1/25/2019 8:18 A	M Active Dir	TITANCORP\mvankralingen	DNS A record removed			
Low Severity Who: TITANCORP\mvankralingen (Marc vanKralingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System//MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal:								
Low Severity Who: TITANCORP\mvankratingen (Marc vanKratingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal:								
Low Severity Who: TITANCORP\mvankralingen (Marc vanKralingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal:								
Low Severity Who: TITANCORP\mvankralingen (Marc vanKralingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal:								
Low Severity Who: TITANCORP\mvankralingen (Marc vanKralingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal:								
Low Severity Who: TITANCORP\wankralingen (Marc vanKralingen) Where: DC1 What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost From: 10.1.146.223								
Low Severity Who: TITANCORP\mvankralingen (Marc vanKralingen) Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: dnsNode Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal:								
Who: TITANCORP\mwankralingen (Marc vanKralingen) Image: Change Auditor Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Image: Class: Image: Origin: dc1.titancorp.local (10.1.146 What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Image: Result: Protected Facility: DNS Zone Class: Image: Image: Image: Autor Type: Static SSL/TLS: Image: Sign/Seal: From: Int1.146.223 Image: Im	Copy 🖂	🛛 Email 🔚 Pri	nt 🔹 🛈 Knowl	adge Base 🚯 Comments.	🗆 Disable 🔍 Related Se	earch 🔹 🕀 🛛 Add to Search 🔻		
Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local.	Low Sev	verity						
 Where: DC1 Source: Change Auditor What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Class: IndnsNode Attr: dnsRecord Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost From: 10.1.146.223 	S Who:	TITANCORP\mvanki	alingen (Marc v	inKralingen)		(w	/hen: 1/25/2019 8:18:02 AM	
 What: The DNS A record MissionCriticalHost has been removed from zone titancorp.local. Active Directory Class: Indestriction Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost From: 10.1.146.223 					rce: Change Auditor	— 0	rigin: dc1.titancorp.local (10.1.14	46.101
Active Directory Action: Delete Attribute Facility: DNS Zone Class: dnsNode Attr: dnsRecord Type: Static SSL/TLS: Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal: 10.1.146.223	What:	The DNS & record	MissionCriticalH	ost has been removed from 70	one titancorn local	and the second se		
Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal: From: 10.1.146.223							and the second	
Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost Sign/Seal: From: 10.1.146.223				۵+++				No
From: 10,1,146.223						.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
To: <not set=""></not>			i proces system	inter of or of the state of product			51811 5044	103
To: <not set=""></not>								
To: KNot Set>								
To: <not set=""></not>								
To: <not set=""></not>								
To: <not set=""></not>								
	To:	<not set=""></not>						-

Conclusion

This discussion illustrated how Quest Change Auditor can help organizations audit their Microsoft Active Directory-integrated DNS, which is the first action recommendation of the Department of Homeland Security's Emergency Directive 19-01 entitled "Mitigate DNS Tampering" (DHS, 2019-1). Specifically, this discussion illustrated how Change Auditor provides detective and protective security controls to:

- Audit changes to Microsoft Active Directory-Integrated DNS
- Collect this audit information into a centralized repository
- Flexibly report on DNS changes
- Alert key stakeholders of critical DNS changes in near real time
- Protect critical DNS objects from unwanted changes

For more information please visit https://www.quest.com/change-auditor/ or email sales@Quest.com

References

DHS. 2019-1. "Mitigate DNS Infrastructure Tampering". Retrieved from: https://cyber.dhs.gov/ed/19-01/

Microsoft. 2014. "What Is DNS Support for Active Directory?". Retrieved from: <u>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-</u> 2003/cc757136%28v%3dws.10%29