Securing Microsoft Integrated DNS in response to

DHS Emergency Directive 19-01

By

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:

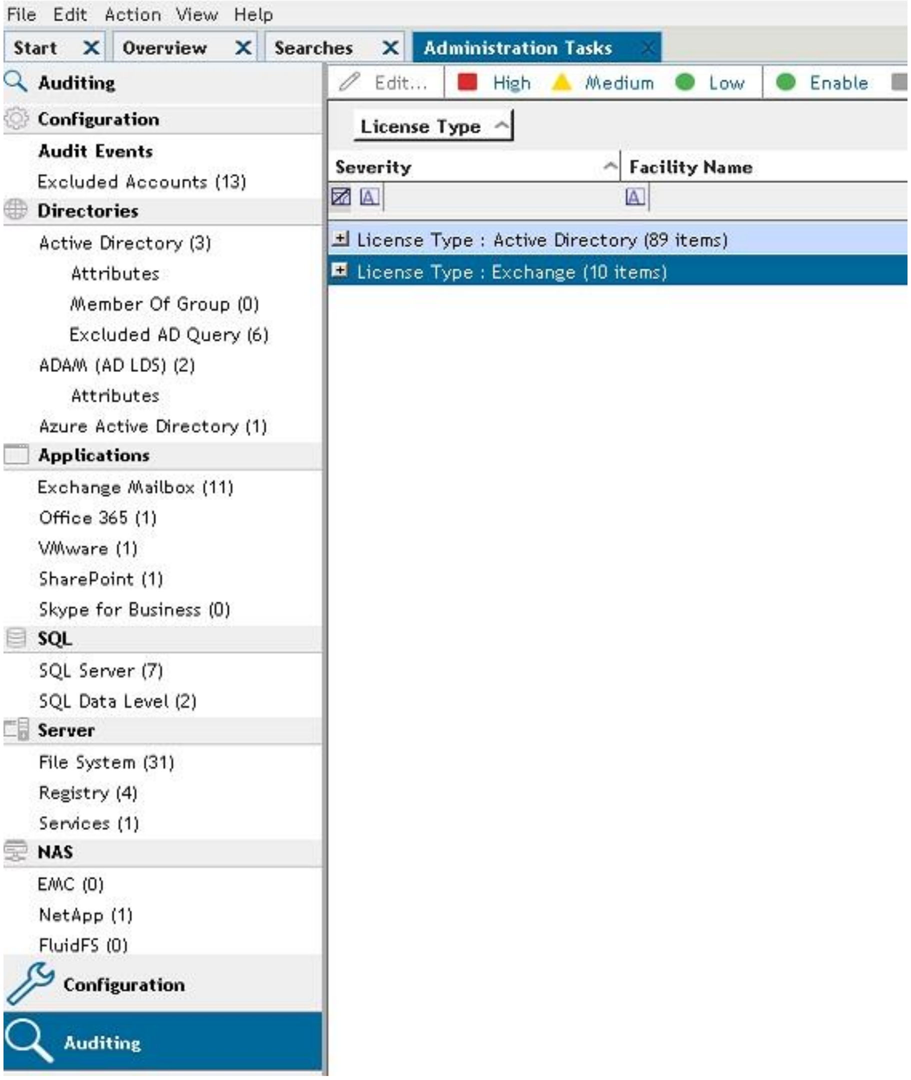
- Proactive threat detection with Change Auditor Threat Detection
- Hybrid environment auditing with a correlated view
- Change prevention
- Auditor-ready reporting

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

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.

Illustration 1: Change Auditor auditing of DNS events

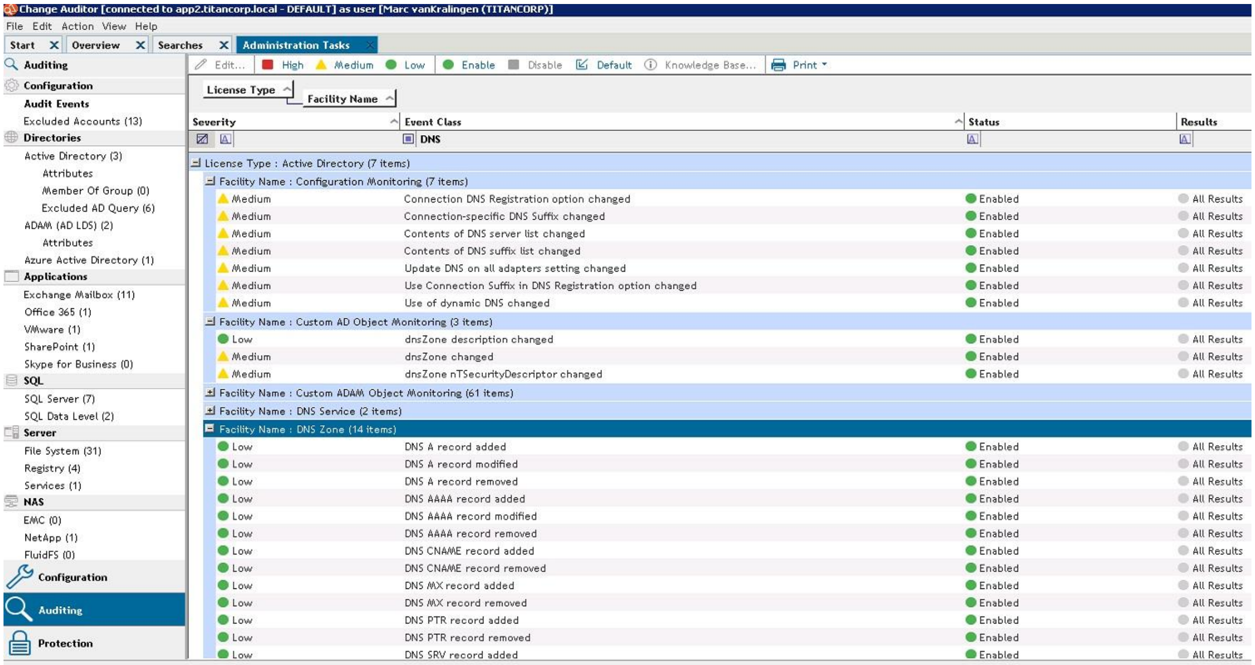


License Type : Active Directory (89 items)

License Type : Exchange (10 items)

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.

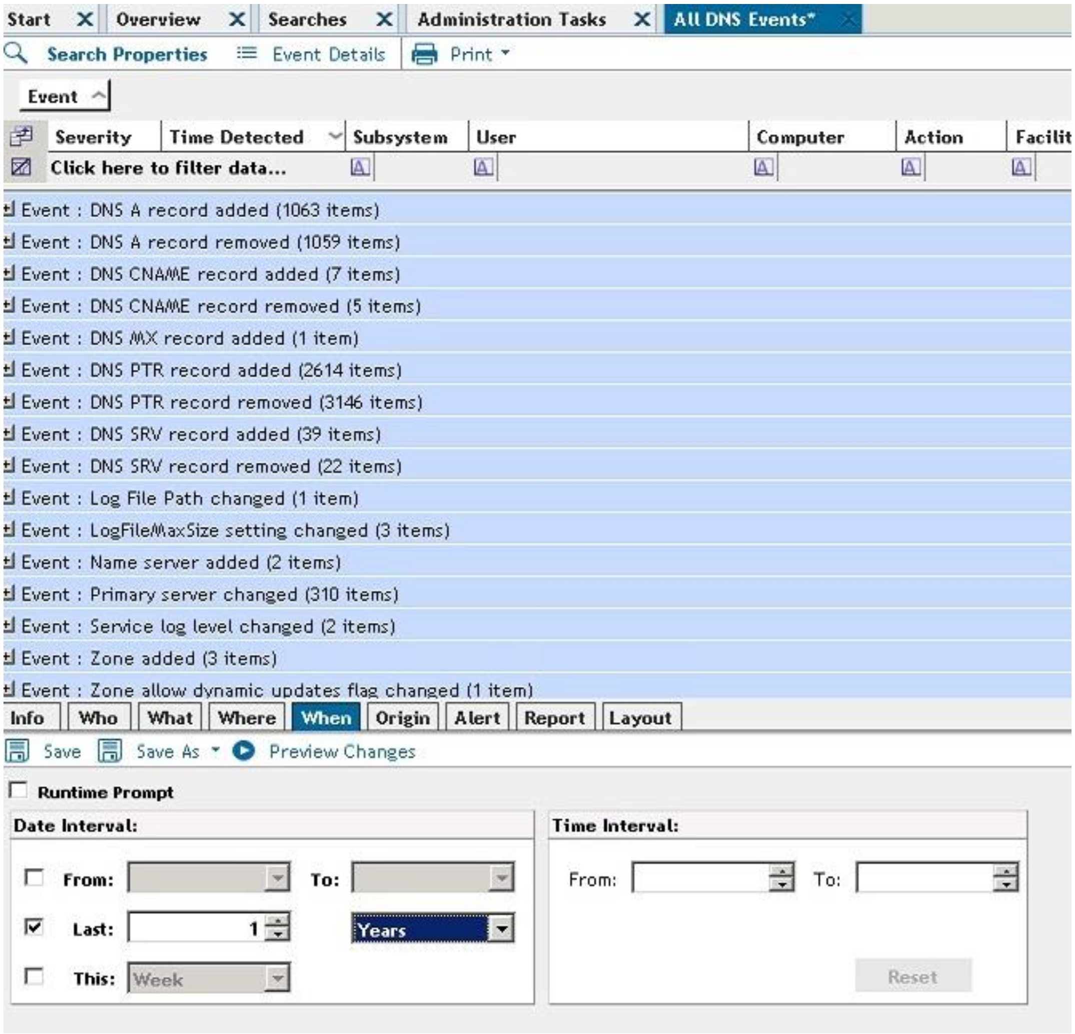
Illustration 2: Categorized and prioritized Change Auditor DNS events



Severity	Event Class	Status	Results
	DNS		
License Type : Active Directory (7 items)			
Facility Name : Configuration Monitoring (7 items)			
Medium	Connection DNS Registration option changed	Enabled	All Results
Medium	Connection-specific DNS Suffix changed	Enabled	All Results
Medium	Contents of DNS server list changed	Enabled	All Results
Medium	Contents of DNS suffix list changed	Enabled	All Results
Medium	Update DNS on all adapters setting changed	Enabled	All Results
Medium	Use Connection Suffix in DNS Registration option changed	Enabled	All Results
Medium	Use of dynamic DNS changed	Enabled	All Results
Facility Name : Custom AD Object Monitoring (3 items)			
Low	dnsZone description changed	Enabled	All Results
Medium	dnsZone changed	Enabled	All Results
Medium	dnsZone nTSecurityDescriptor changed	Enabled	All Results
Facility Name : Custom ADAM Object Monitoring (61 items)			
Facility Name : DNS Service (2 items)			
Facility Name : DNS Zone (14 items)			
Low	DNS A record added	Enabled	All Results
Low	DNS A record modified	Enabled	All Results
Low	DNS A record removed	Enabled	All Results
Low	DNS AAAA record added	Enabled	All Results
Low	DNS AAAA record modified	Enabled	All Results
Low	DNS AAAA record removed	Enabled	All Results
Low	DNS CNAME record added	Enabled	All Results
Low	DNS CNAME record removed	Enabled	All Results
Low	DNS MX record added	Enabled	All Results
Low	DNS MX record removed	Enabled	All Results
Low	DNS PTR record added	Enabled	All Results
Low	DNS PTR record removed	Enabled	All Results
Low	DNS SRV record added	Enabled	All Results

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.

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



Event : DNS A record added (1063 items)
Event : DNS A record removed (1059 items)
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 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 allow dynamic updates flag changed (1 item)

□ Runtime Prompt

Date Interval:

□ From: To:

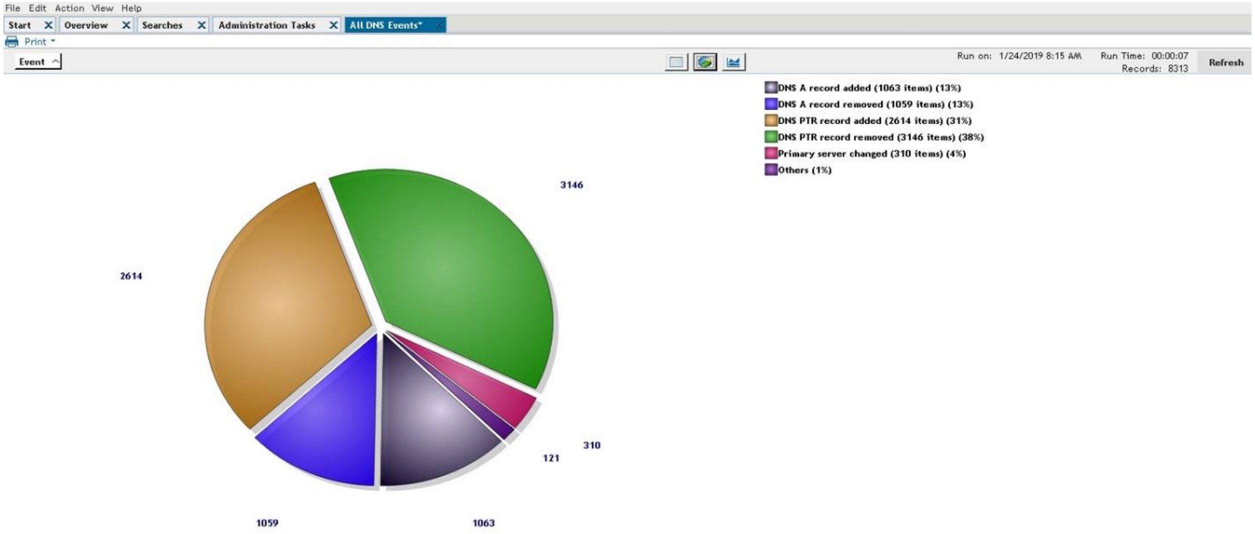
☑ Last: 1 Years

□ This: Week

Time Interval:

From: To:

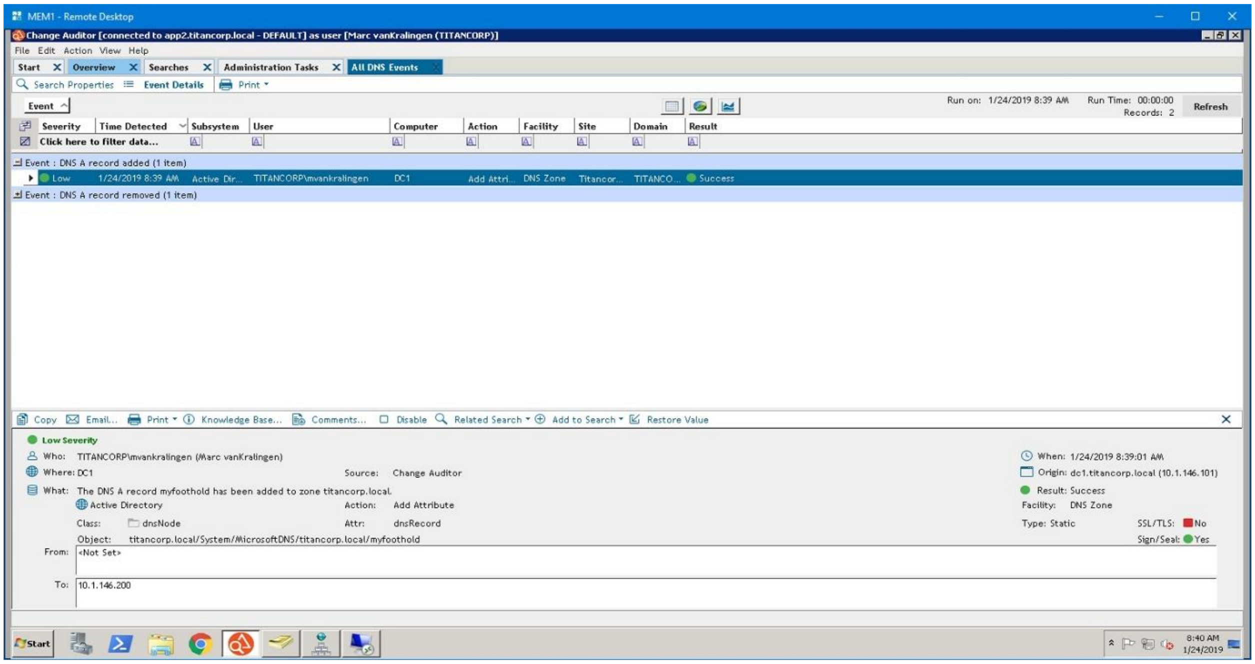
Illustration 4: Change Auditor graphical representation of DNS event auditing



Run on: 1/24/2019 8:15 AM Run Time: 00:00:07
Records: 8313

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

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



Change Auditor [connected to app2.titancorp.local - DEFAULT] as user [Marc vanKralingen (TITANCORP)]

Run on: 1/24/2019 8:39 AM Run Time: 00:00:00
Records: 2

Severity	Time Detected	Subsystem	User	Computer	Action	Facility	Site	Domain	Result
Click here to filter data...									
Event : DNS A record added (1 item)									
● Low	1/24/2019 8:39 AM	Active Dir...	TITANCORP\mvankralingen	DC1	Add Attri...	DNS Zone	Titancor...	TITANCO...	● Success
Event : DNS A record removed (1 item)									

● Low Severity

Who: TITANCORP\mvankralingen (Marc vanKralingen)

Where: DC1 Source: Change Auditor

What: The DNS A record myfoothold has been added to zone titancorp.local.

Active Directory Action: Add Attribute

Class: dnsNode Attr: dnsRecord

Object: titancorp.local/System/MicrosoftDNS/titancorp.local/myfoothold

From: <Not Set>

To: 10.1.146.200

When: 1/24/2019 8:39:01 AM

Origin: dc1.titancorp.local (10.1.146.101)

● Result: Success

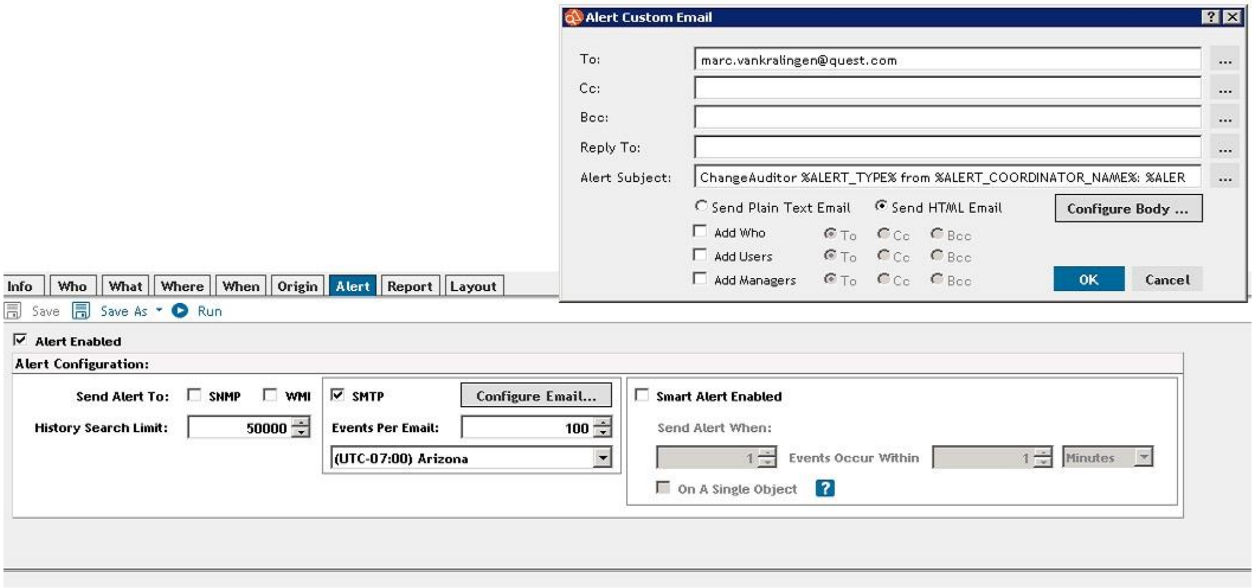
Facility: DNS Zone

Type: Static SSL/TLS: 🟥 No

Sign/Seal: ● Yes

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.

Illustration 6: Configuring near real-time alerting over DNS events



Alert Custom Email

To: marc.vankralingen@quest.com

Cc:

Bcc:

Reply To:

Alert Subject: ChangeAuditor %ALERT_TYPE% from %ALERT_COORDINATOR_NAME%: %ALER

○ Send Plain Text Email ● Send HTML Email Configure Body ...

□ Add Who ● To ○ Cc ○ Bcc

□ Add Users ● To ○ Cc ○ Bcc

□ Add Managers ● To ○ Cc ○ Bcc

OK Cancel

Info | Who | What | Where | When | Origin | Alert | Report | Layout

Save | Save As | Run

☑ Alert Enabled

Alert Configuration:

Send Alert To: □ SNMP □ WMI ☑ SMTP Configure Email...

History Search Limit: 50000

Events Per Email: 100

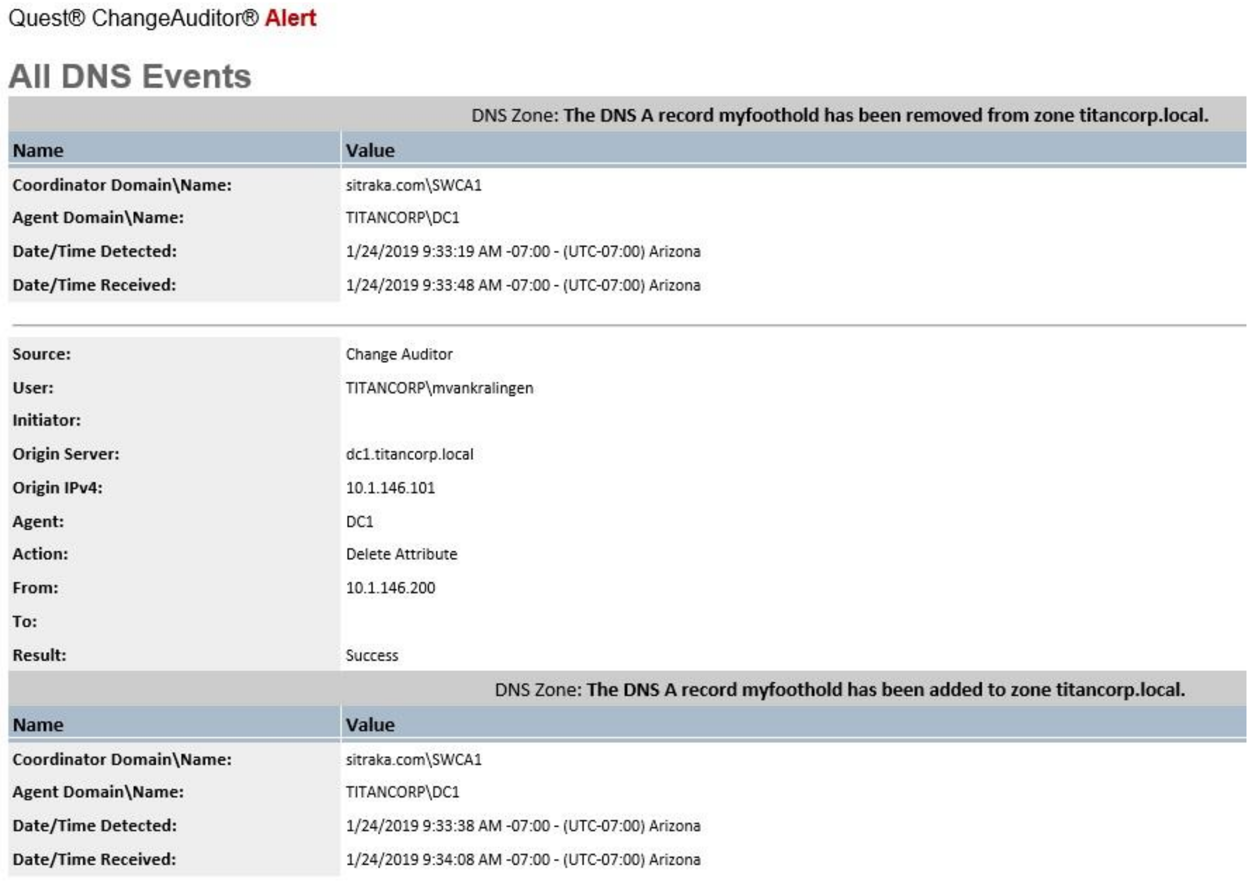
(UTC-07:00) Arizona

□ Smart Alert Enabled

Send Alert When: 1 Events Occur Within 1 Minutes

□ On A Single Object

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

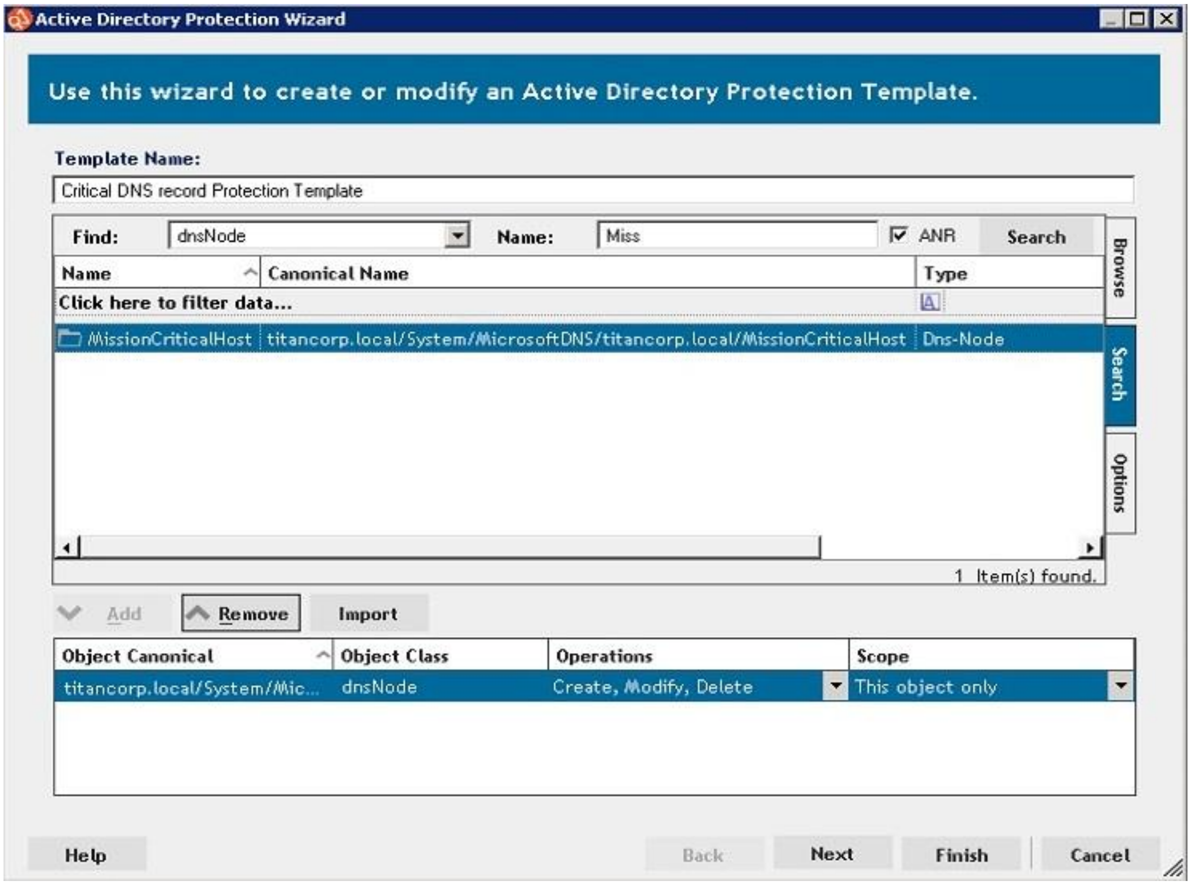
Source:	Change Auditor
User:	TITANCORP\mvankralingen
Initiator:	
Origin Server:	dc1.titancorp.local
Origin IPv4:	10.1.146.101
Agent:	DC1
Action:	Delete Attribute
From:	10.1.146.200
To:	
Result:	Success

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.

Illustration 8: Creating a DNS record protection template



Use this wizard to create or modify an Active Directory Protection Template.

Template Name: Critical DNS record Protection Template

Find: dnsNode

Name: Miss

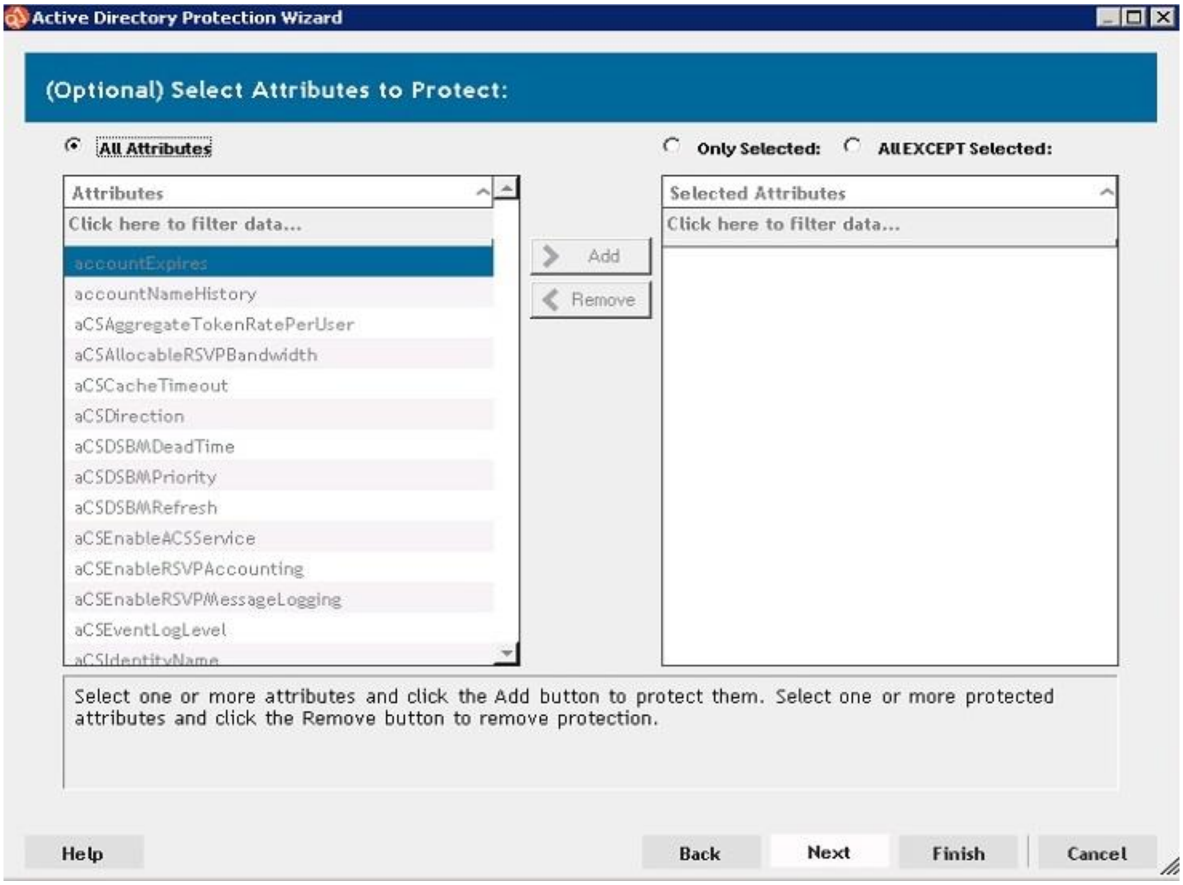
☑ ANR

Name	Canonical Name	Type
Click here to filter data...		
MissionCriticalHost	titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost	Dns-Node

1 Item(s) found.

Object Canonical	Object Class	Operations	Scope
titancorp.local/System/Mic...	dnsNode	Create, Modify, Delete	This object only

Illustration 9: Setting DNS record protection levels

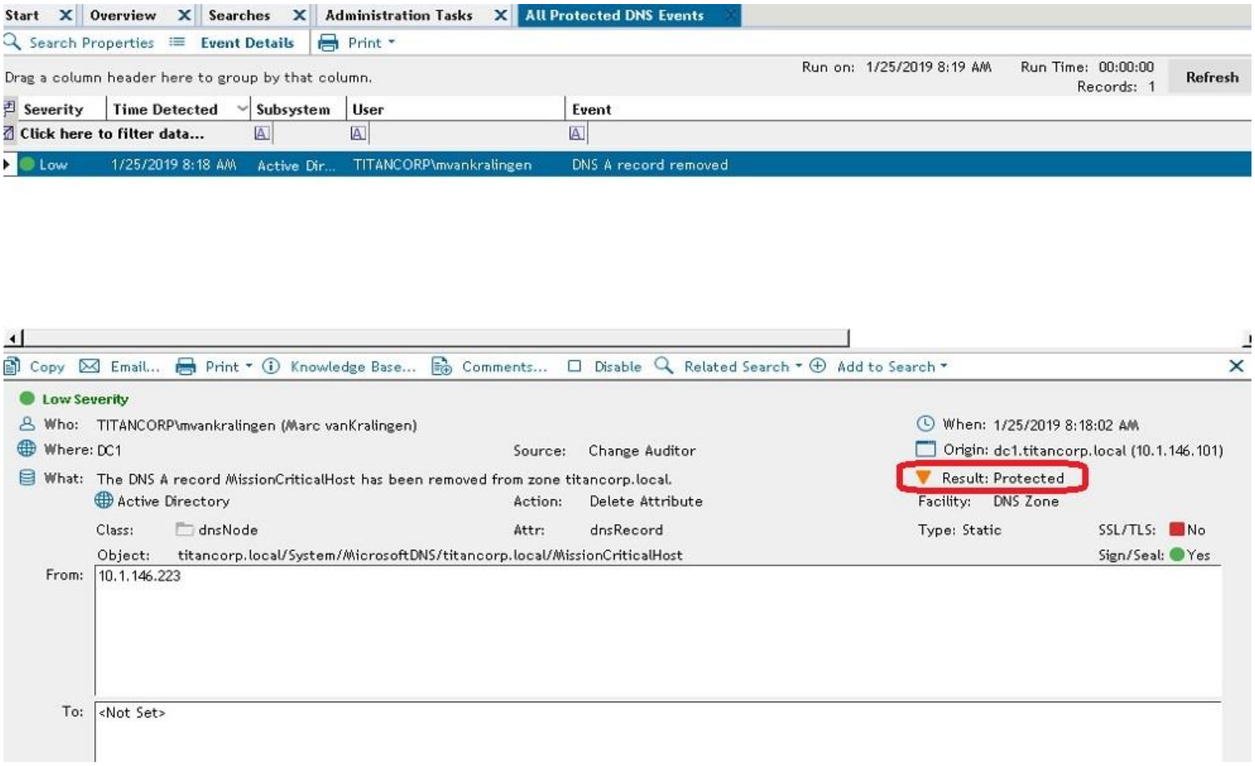

Active Directory Protection Wizard
(Optional) Select Attributes to Protect:
Attributes
Click here to filter data...
Add
Remove
Selected Attributes
Click here to filter data...
Help
Back
Next
Finish
Cancel

● All Attributes ○ Only Selected: ○ All EXCEPT Selected:

accountExpires
accountNameHistory
aCSAggregateTokenRatePerUser
aCSAllocableRSVPBandwidth
aCSCacheTimeout
aCSDirection
aCSDSBMDeadTime
aCSDSBMPriority
aCSDSBMRefresh
aCSEnableACSService
aCSEnableRSVPAccounting
aCSEnableRSVPMessageLogging
aCSEventLogLevel
aCSIdentityName

Select one or more attributes and click the Add button to protect them. Select one or more protected attributes and click the Remove button to remove protection.

Illustration 10: Reporting on protected/prevented DNS activities



Drag a column header here to group by that column.

Run on: 1/25/2019 8:19 AM Run Time: 00:00:00
Records: 1

Severity	Time Detected	Subsystem	User	Event
● Low	1/25/2019 8:18 AM	Active Dir...	TITANCORP\mvankralingen	DNS A record removed

● Low Severity

Who: TITANCORP\mvankralingen (Marc vanKralingen)

When: 1/25/2019 8:18:02 AM

Where: DC1

Source: Change Auditor

Origin: dc1.titancorp.local (10.1.146.101)

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

SSL/TLS: 🟥 No

Object: titancorp.local/System/MicrosoftDNS/titancorp.local/MissionCriticalHost

Sign/Seal: ● Yes

From: 10.1.146.223

To: <Not Set>

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: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757136%28v%3dws.10%29