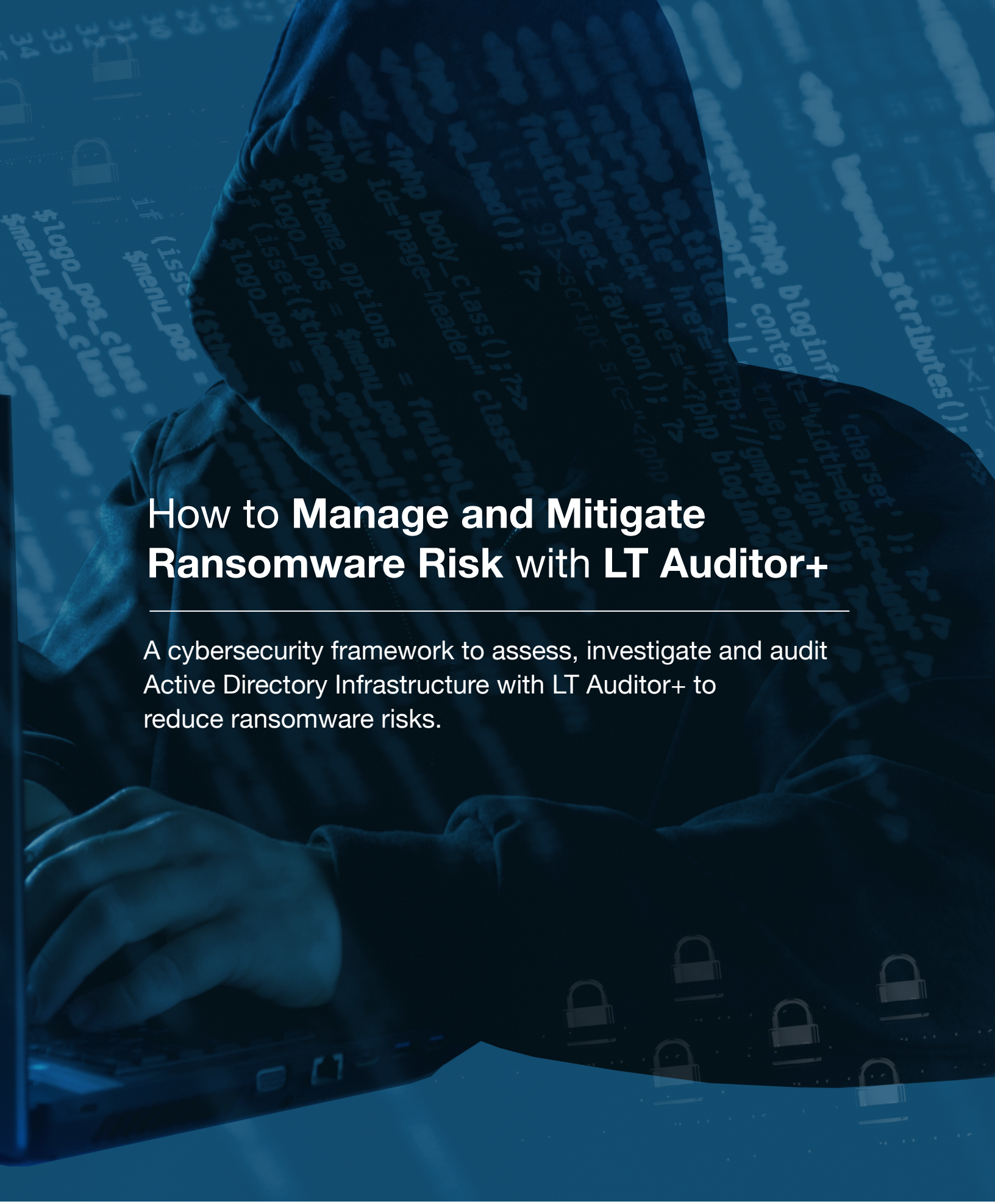


How to **Manage and Mitigate Ransomware Risk** with **LT Auditor+**

A cybersecurity framework to assess, investigate and audit Active Directory Infrastructure with LT Auditor+ to reduce ransomware risks.

BLUE LANCE

ABSTRACT

According to the U.S. Government's Cybersecurity and Infrastructure Security Agency (*CISA*): "Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

In terms of cyberattacks, despite wide-spread media attention to data breaches targeting well known organizations and enterprises such as Equifax, Target, Home Depot, JP Morgan, Capital One, and more, the rise of ransomware has become one of the most pervasive threats to organizations.

Recent high profile ransomware attacks that made the press include *ACER, City of Atlanta, CNA Insurance, Colonial Pipeline, JBS Foods, Kaseya, NBA, Steamship Authority of Massachusetts, the Washington DC Metropolitan Police Department*, and many more.

According to *Harvard Business Review,* the amount companies paid to hackers grew by 300% in 2021. The majority of ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website. More advanced versions gain access using zero-day vulnerabilities on unpatched systems. After attackers gain access, they leverage PowerShell, Command line, WMI and other commands to conduct reconnaissance and identify accounts to take over. Privileges are gained by either taking over a privileged account or using tools to elevate privileges. This allows attackers to move within the network and gain access to valuable data.

This document provides a framework for using LT Auditor+ to continually assess, investigate, and audit an organization's Active Directory infrastructure, reduce the IT network attack surface and mitigate ransomware risks.

KEYWORDS

LT Auditor+; detect; identify; protect; ransomware; malware, cyber-attacks, recover; respond; risk; cybersecurity; assess; investigate; audit, NIST Cybersecurity Framework, CISA, attack surface, remedial action

---

RESOURCES

NISTIR 8374 Ransomware Risk Management: A Cybersecurity Frame work Profile

NIST Special Publication (SP) 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events - addresses how an organization can handle an attack when it occurs and what capabilities it needs to have in place to detect and respond to destructive events.

NIST SP 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events addresses how an organization can work before an attack to identify its assets and potential vulnerabilities and remedy the discovered vulnerabilities to protect these assets.

https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php - TOURO COLLEGE ILLINOIS The 10 Biggest Ransomware Attacks of 2021

https://www.cisa.gov/stopransomware - CISA: STOP RANSOMWARE

https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared

https://advisory.kpmg.us/articles/2021/ransomware-attack-risks.html - KPMG advisory on ransomware risks

TABLE OF CONTENTS

LT AUDITOR+ CYBERSECURITY FRAMEWORK

The LT Auditor+ Cybersecurity Framework consists of three main components or Functions: *Assess, Investigate, and Audit.*

These Functions are defined as:

ASSESS	Identify vulnerable settings or configurations
INVESTIGATE	Detect suspicious activity
AUDIT	Verify, validate and document activity and actions

Each of these Functions provides for a set of actions with LT Auditor+ to reduce the organizational risk of a ransomware attack. These actions are detailed below.

The LT Auditor+ Cybersecurity Framework functions of Assess, Investigate and Audit aligns with the NIST Cybersecurity Framework functions in the following fashion:

Assess -> Identify and Protect
Investigate -> Detect
Audit -> Repond and Recover

HOW TO REDUCE RANSOMWARE RISK WITH LT AUDITOR+

ASSESS	INVESTIGATE	AUDIT
Dormant privileged accounts	Privilege escalation - members added to powerful groups	Privileged User activity
Password age configuration vulnerability	Privileges granted to Active Directory objects	Password changes to privileged and service accounts
Password privilege alterations	Excessive account lockouts	Group Policy changes
Granting group membership privileges	Excessive logon failures	Access to Domain Controllers
Excessive privileges for users, groups, OUs, and containers	Suspicious patterns of logon failures	After-Hour activity
Dormant accounts	Suspicious patterns of logon activity	MSP/Contractor activity
Accounts that have never been used	User rights assignments	Installation of Applications and services
Privileged group membership	Group policy delegations	Create instances of persistence via updates to Task Scheduler
	Unconstrained delegations	Ensure latest updates and patches have been applied to domain controllers, servers and workstations

ASSESS

The Assess Function limits and contains the impact of ransomware attacks. This function hardens the Active Directory infrastructure by reducing the attack surface area, thus mitigating ransomware risk.

A discussion of the pertinent actions follows:

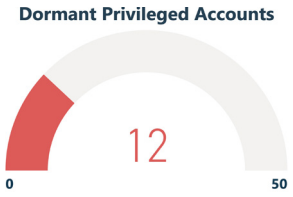
Dormant Privileged Accounts

Dormant Privileged Accounts can be exploited because:

> Attackers use these forgotten accounts to perform unnoticed activities.
>
> Threat actors often use past employee credentials to illegally access the network.
>
> Past employees can sell their credentials to bad actors or use them to snoop, remove or destroy sensitive and/or competitive information.

Privileged dormant accounts are coveted by ransomware attackers as these accounts have total access to the IT infrastructure of an organization and inflict maximum damage. These accounts must be disabled.

LT Auditor+ *Best Practice panels* immediately identify privileged dormant accounts for remedial action.



Dormant Privileged Accounts (Past 90 Days)

Account	Admin	Enabled	Group	Last Logon	Days Since Last Login
ABolton	Yes	Yes	Enterprise Admins	8/12/2020 8:15:10 PM	182
BAndersen	Yes	Yes	Enterprise Admins	10/27/2020 8:15:11 PM	106
CAustin	Yes	Yes	Domain Admins	9/24/2020 8:15:10 PM	139
CRichmond	Yes	Yes	Enterprise Admins	9/21/2020 8:15:10 PM	142
EHancock	Yes	Yes	Enterprise Admins	10/22/2020 8:15:11 PM	111
ESingleton	Yes	Yes	Enterprise Admins	10/26/2020 8:15:11 PM	107
JPark	Yes	Yes	Enterprise Admins	10/21/2020 8:15:10 PM	112
JSmall	Yes	Yes	Enterprise Admins	8/31/2020 8:15:11 PM	163
KClark	Yes	Yes	Domain Admins	8/6/2020 8:15:11 PM	188
KTrevino	Yes	Yes	Domain Admins	9/6/2020 8:15:11 PM	157
OBooker	Yes	Yes	Domain Admins	8/3/2020 8:15:10 PM	191
TLamb	Yes	Yes	Domain Admins	11/5/2020 8:15:11 PM	97

ASSESS

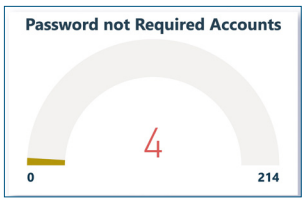
Password age configuration vulnerability

Enforcing periodic password change is an extremely effective mechanism to reduce account take-over exploits. Windows allows for configuring special or service accounts with passwords that never expire to meet critical operational functions. This feature must only be used, when necessary since it creates increased vulnerability to brute force or password spraying attacks.

LT Auditor+ Best Practice panels detect the use of these vulnerable settings on accounts other than the exempted accounts by using exclusion filters and presents them for remediation.

Passwords Never Expire

Account	Domain	Password Never Expires	Never Logged On	Last Logon	Days Since Last Login
Alvarez	reddragon.com	Yes	No	4/14/2022 3:05:06 PM	0
andrewmyles	reddragon.com	Yes	No	4/7/2022 3:43:11 PM	7
bobhopes	reddragon.com	Yes	Yes	1/1/1970 12:00:00 AM	
DavidCoffey	reddragon.com	Yes	No	4/7/2022 4:02:35 PM	7
eartuc	reddragon.com	Yes	No	4/14/2022 3:05:05 PM	0
gramsey	reddragon.com	Yes	Yes	1/1/1970 12:00:00 AM	
Guest	reddragon.com	Yes	No	3/31/2022 10:09:03 PM	13
ldac	reddragon.com	Yes	Yes	1/1/1970 12:00:00 AM	
jhonking	reddragon.com	Yes	Yes	1/1/1970 12:00:00 AM	



Passwords Not Required

Account	Password Required	Never Logged On	Last Logon	Days Since Last Logon
ARice	No	No	2/2/2021 8:15:11 PM	8
HBradford	No	No	1/20/2021 8:15:11 PM	21
JHodges	No	No	1/23/2021 8:15:11 PM	18
LMontoya	No	No	1/25/2021 8:15:11 PM	16

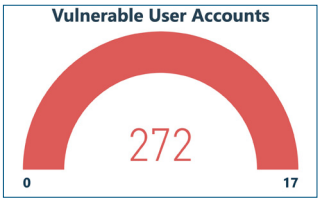
Passwords Change Not Allowed

Account	Password Change Allowed	Never Logged On	Last Logon	Days Since Last Logon
CDavies	No	No	1/18/2021 8:15:11 PM	23
CDennis	No	No	1/27/2021 8:15:11 PM	14
CFinley	No	No	2/3/2021 8:15:11 PM	7
DSchneider	No	No	2/9/2021 8:15:11 PM	1
EHuff	No	No	1/13/2021 8:15:11 PM	28
ELloyd	No	No	1/28/2021 8:15:11 PM	13
JGood	No	No	1/16/2021 8:15:11 PM	25
KGreene	No	No	1/18/2021 8:15:11 PM	23
KLarsen	No	No	1/17/2021 8:15:11 PM	24
KWyatt	No	No	2/3/2021 8:15:11 PM	7
LCaldwell	No	No	1/24/2021 8:15:11 PM	17
LCook	No	No	1/21/2021 8:15:11 PM	20
MAllen	No	No	1/18/2021 8:15:11 PM	23
MCosta	No	No	1/21/2021 8:15:11 PM	20
RZavala	No	No	1/21/2021 8:15:11 PM	20
SBoyle	No	No	1/30/2021 8:15:11 PM	11
SHerring	No	No	1/17/2021 8:15:11 PM	24
TBray	No	No	1/31/2021 8:15:11 PM	10

ASSESS

Password reset privileges

Ensuring that only authorized users have privileges to reset passwords is important and vital in reducing the attack surface area. Unauthorized resets of account passwords often lead to account takeovers. LT Auditor+ identifies users with password reset privileges and makes it easy to validate their authorization.



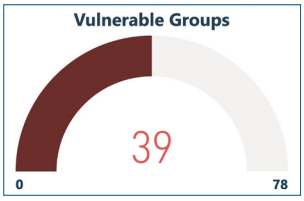
Vulnerable User Accounts

ObjectName	Class	Principal	ActiveDirectoryRights	ObjectTypeName
Ann Bolton	user	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All
Ann Bolton	user	BLDRAGON\KZuniga	GenericAll	All
Areli Henderson	user	BLDRAGON\ASerrano	GenericAll	All
Areli Henderson	user	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All
Areli Henderson	user	BLDRAGON\KZuniga	GenericAll	All
Aryana Riddle	user	BLDRAGON\ASerrano	GenericAll	All
Aryana Riddle	user	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All
Aryana Riddle	user	BLDRAGON\KZuniga	GenericAll	All
Barrett Andersen	user	BLDRAGON\ASerrano	GenericAll	All
Barrett Andersen	user	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All
Barrett Andersen	user	BLDRAGON\KZuniga	GenericAll	All
Braeden Leblanc	user	BLDRAGON\ASerrano	GenericAll	All
Braeden Leblanc	user	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All
Braeden Leblanc	user	BLDRAGON\KZuniga	GenericAll	All
Brianna White	user	BLDRAGON\ASerrano	GenericAll	All
Brianna White	user	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All
Brianna White	user	BLDRAGON\KZuniga	GenericAll	All
Brogan Tyler	user	BLDRAGON\ASerrano	GenericAll	All

ASSESS

Grant group membership privileges

The ability to grant group membership poses significant risks if these rights have been granted to unauthorized individuals, particularly if the group has powerful privileges or has access to sensitive information. Checks to ensure that only authorized accounts are granted this privilege reduces ransomware risk within the environment. LT Auditor+ Best Practice Panels display all users with these privileges and make it easy to validate authorization.

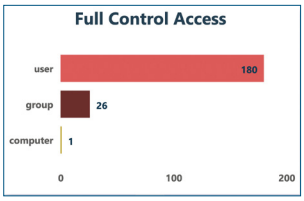


Vulnerable Groups

ObjectName	Class	Principal	ActiveDirectoryRights	ObjectTypeName	AccessControlType
Account Operators	group	BLDRAGON\ASerrano	GenericAll	All	Allow
Account Operators	group	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All	Allow
Account Operators	group	BLDRAGON\KZuniga	GenericAll	All	Allow
Administrators	group	BLDRAGON\ASerrano	GenericAll	All	Allow
Administrators	group	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All	Allow
Administrators	group	BLDRAGON\KZuniga	GenericAll	All	Allow
Backup Operators	group	BLDRAGON\ASerrano	GenericAll	All	Allow
Backup Operators	group	BLDRAGON\JWise	DeleteChild, ListChildren, ReadProperty, GenericWrite	All	Allow
Backup Operators	group	BLDRAGON\KZuniga	GenericAll	All	Allow
Domain Admins	group	BLDRAGON\ASerra	GenericAll	All	Allow

Excessive privileges for users, groups, OUs, and containers

A core tenet for hardening the Active Directory infrastructure is to follow the principle of least privileges. LT Auditor+ automatically lists, in plain English, all Active Directory objects that have been granted full rights or all access to specific Active Directory resources to quickly validate correct authorization.



Full Control Access

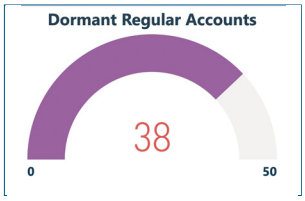
ObjectName	Class	Principal	ActiveDirectoryRights	ObjectTypeName	AccessControl
Abbigail Callahan	user	BLDRAGON\ASerrano	GenericAll	All	Allow
Abbigail Callahan	user	BLDRAGON\KZuniga	GenericAll	All	Allow
Account Operators	group	BLDRAGON\ASerrano	GenericAll	All	Allow
Account Operators	group	BLDRAGON\KZuniga	GenericAll	All	Allow
Addyson Rice	user	BLDRAGON\ASerrano	GenericAll	All	Allow
Addyson Rice	user	BLDRAGON\KZuniga	GenericAll	All	Allow
Administrator	user	BLDRAGON\ASerrano	GenericAll	All	Allow
Administrator	user	BLDRAGON\KZuniga	GenericAll	All	Allow
Administrators	group	BLDRAGON\ASerrano	GenericAll	All	Allow
Administrators	group	BLDRAGON\KZuniga	GenericAll	All	Allow
Ann Bolton	user	BLDRAGON\ASerrano	GenericAll	All	Allow
Ann Bolton	user	BLDRAGON\KZuniga	GenericAll	All	Allow
Areli Henderson	user	BLDRAGON\ASerrano	GenericAll	All	Allow
Areli Henderson	user	BLDRAGON\KZuniga	GenericAll	All	Allow
Aryana Riddle	user	BLDRAGON\ASerrano	GenericAll	All	Allow
Aryana Riddle	user	BLDRAGON\KZuniga	GenericAll	All	Allow
Backup Operators	group	BLDRAGON\ASerrano	GenericAll	All	Allow
Backup Operators	group	BLDRAGON\KZuniga	GenericAll	All	Allow

ASSESS

Dormant accounts

Dormant or Stale user accounts are active accounts that have not logged onto the network for a relatively long period.

Dormant user accounts in Active Directory are a significant security risk since they are available to be used by an attacker or a former employee. These accounts also consume NTDS database space, clutter up the Directory and make investigation inefficient. Additionally, they degrade Active Directory health and performance. In a clear and concise manner, *LT Auditor+ quickly identifies Dormant accounts to be disabled or deleted*. The period of dormancy is configurable.



Dormant Regular Accounts (Past 90 Days)

Account	Enabled	Admin	Never Logged On	Last Logon	Days Since Login
ABrewer	Yes	No	No	10/24/2020 8:15:10 PM	109
ALarson	Yes	No	No	10/28/2020 8:15:11 PM	105
ARobertson	Yes	No	No	9/17/2020 8:15:10 PM	146
BGreer	Yes	No	No	11/3/2020 8:15:10 PM	99
BMann	Yes	No	No	10/1/2020 8:15:10 PM	132
CFrench	Yes	No	No	8/14/2020 8:15:11 PM	180
CGraves	Yes	No	No	10/2/2020 8:15:10 PM	131
CMullins	Yes	No	No	10/12/2020 8:15:11 PM	121
CRich	Yes	No	No	9/26/2020 8:15:11 PM	137
CSimpson	Yes	No	No	8/7/2020 8:15:11 PM	187
DFranklin	Yes	No	No	8/14/2020 8:15:10 PM	180
DWashington	Yes	No	No	9/20/2020 8:15:10 PM	143
FGay	Yes	No	No	7/31/2020 8:15:10 PM	194
HHolloway	Yes	No	No	8/15/2020 8:15:11 PM	179
JAshley	Yes	No	No	9/18/2020 8:15:11 PM	145
JHood	Yes	No	No	8/20/2020 8:15:10 PM	174
JWallace	Yes	No	No	8/22/2020 8:15:10 PM	172
JWilkins	Yes	No	No	9/20/2020 8:15:10 PM	143

Accounts that have never been used

Just like Dormant accounts, Active user accounts that have never been used constitute a security risk since they are easy targets for an attacker or former employee. Such accounts should be disabled or deleted.

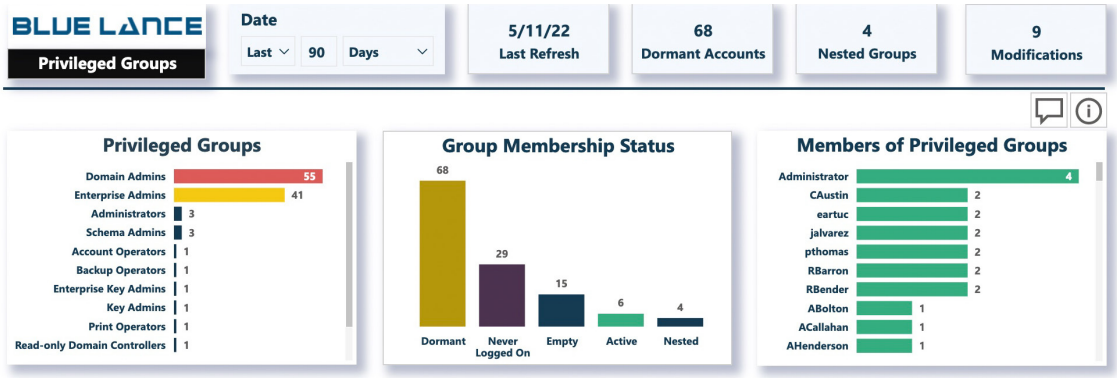
Never Logged On

Account	Never Logged On	Enabled	Account Created Date
ABenson	Yes	Yes	12/03/2020 22:32:51
ABright	Yes	Yes	12/03/2020 22:32:20
ACallahan	Yes	Yes	12/05/2020 00:33:13
ACamacho	Yes	Yes	12/03/2020 22:33:58
ACarr	Yes	Yes	12/03/2020 22:31:43
AChapman	Yes	Yes	12/03/2020 22:32:24
AHayes	Yes	Yes	12/03/2020 22:33:59
AHaynes	Yes	Yes	12/03/2020 22:32:55
ALara	Yes	Yes	12/03/2020 22:28:16
ALuna	Yes	Yes	12/03/2020 22:33:42
AMacias	Yes	Yes	12/03/2020 22:32:35
AMcintyre	Yes	Yes	12/05/2020 00:33:04
AMckinney	Yes	Yes	12/03/2020 22:30:43
ANash	Yes	Yes	12/03/2020 22:34:02
APotter	Yes	Yes	12/03/2020 22:32:45
ARiddle	Yes	Yes	12/03/2020 22:31:45
ASerrano	Yes	Yes	12/03/2020 22:33:19
BBaldwin	Yes	Yes	12/05/2020 00:31:07

ASSESS

Privileged group membership

All memberships to powerful Active Directory groups must be authorized and validated as these privileges literally come with the 'Keys to the Kingdom'. LT Auditor+ comes with a built-in, drill-down panel that lists all privileged group memberships for immediate detection, verification and validation.

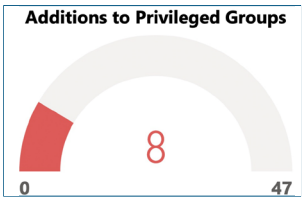


INVESTIGATE

The Investigate function provides evidence of suspicious activities, enabling timely discovery of a ransomware attack.

Privilege escalation - members added to powerful groups

Members of protected groups like '*Domain Admins', 'Enterprise Admins' and 'Schema Admins'* have complete control of Active Directory resources in an organization. Memberships to these powerful groups must be closely monitored to ensure that privileges granted were properly authorized and are not malicious or accidental. LT Auditor+ detects changes to these powerful groups in real-time and quantifies this complex information in an easy-to-understand format.

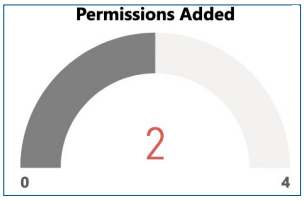


Additions to Privileged Groups

Group	Member Added	Date	Added By	Node
Domain Admins	cn=Andrew Myles,CN=Users,DC=reddragon,DC=com	Monday, May 02, 2022	REDDRAGON\Alvarez	73.155.178.28
Domain Admins	cn=David Coffey,CN=Users,DC=reddragon,DC=com	Monday, May 02, 2022	REDDRAGON\eartuc	73.155.178.28
Domain Admins	cn=Jhon King,CN=Users,DC=reddragon,DC=com	Monday, April 25, 2022	REDDRAGON\eartuc	73.155.178.28
Domain Admins	cn=John Glenn,CN=Users,DC=reddragon,DC=com	Monday, May 09, 2022	BLDRAGON\pthomas	172.31.8.88
Domain Admins	cn=neww user,CN=Users,DC=reddragon,DC=com	Monday, April 25, 2022	REDDRAGON\eartuc	73.155.178.28
Domain Admins	CN=Paul PC. Contractor,CN=Users,DC=reddragon,DC=com	Monday, April 25, 2022	REDDRAGON\eartuc	73.155.178.28
Domain Admins	cn=Steve Jones,CN=Users,DC=reddragon,DC=com	Monday, May 02, 2022	REDDRAGON\Alvarez	73.155.178.28
Domain Admins	cn=Steve Jones,CN=Users,DC=reddragon,DC=com	Monday, May 09, 2022	BLDRAGON\pthomas	

Privileges granted to Active Directory objects

Privileges (DACL's) granted to Active Directory objects are closely monitored to ensure that malicious actors are not escalating privileges to gain access and control.



Object Permissions Added

Object Modified	Class	Date	Set By	Node	Details
cn={460094F8-3D3A-4450-A865-3CA84DDB9D5E},cn=policies,cn=system,DC=reddragon,DC=com	groupPolicyContainer	Monday, May 02, 2022	REDDRAGON\Alvarez	73.155.178.28	Modified Security DACL of groupPolicyCor
cn=Paul PC. Contractor,CN=Users,DC=reddragon,DC=com	user	Monday, April 25, 2022	REDDRAGON\Alvarez	73.155.178.28	Modified Security DACL of user cn=Paul P(

INVESTIGATE

Excessive logon failures

Large numbers of repeated failed logon attempts occurring within a configurable period many times is an indicator of compromise. A LT Auditor+ panel specifically analyzes all logon failures and provides critical information to:

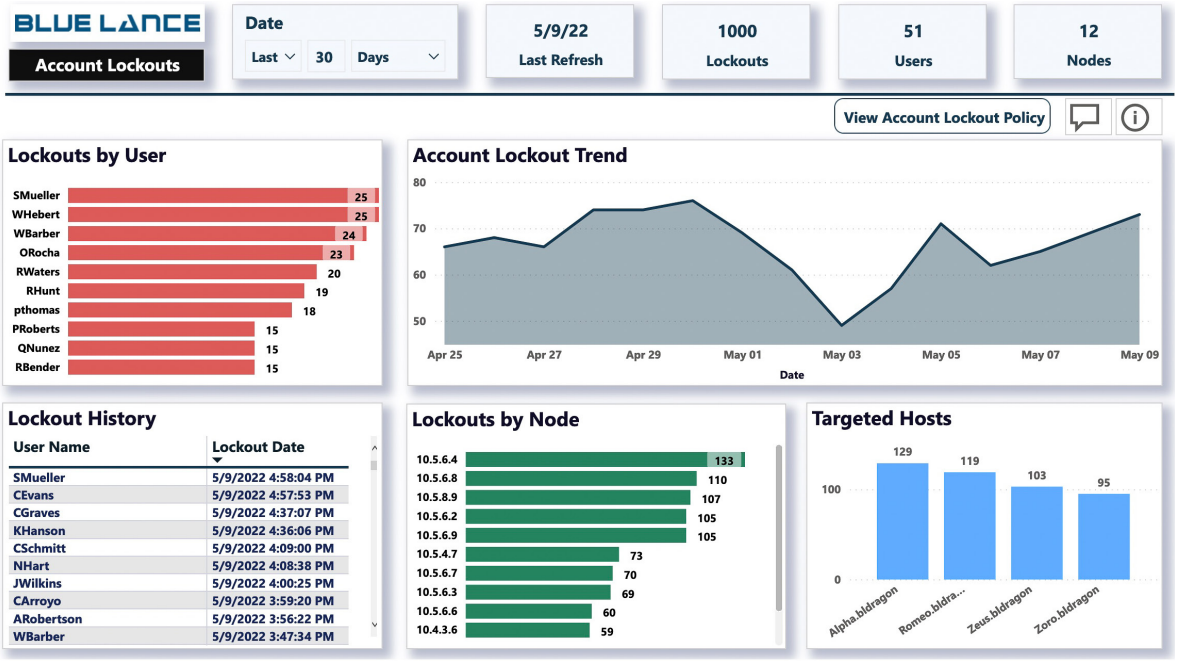
- Identify users and nodes where large numbers of failures are occurring.
- Display trend lines over time to identify periods of time for deeper inspection.
- Investigate security incidents and identify a pattern of attack.
- Clearly explain and document reasons for logon failures.

Multiple logon failures across several user accounts within a given period should be immediately investigated for a password spraying attack. This form of attack tries a password across multiple user accounts so as not to trigger lockouts. By using the LT Auditor+ Failed Logons panel to investigate whether the failures are originating from a single node and determining if this node is the culprit of a password spraying attack allows the organization to take immediate and decisive measures to stop it.

INVESTIGATE

Excessive account lockouts

Excessive account lockouts can be a sign of compromised credentials. LT Auditor+ aggregates all lockouts occurring over a selectable period of time. This data is presented in a series of drill-down visuals to facilitate urgent investigation of suspicious activity and identification of bad actors.

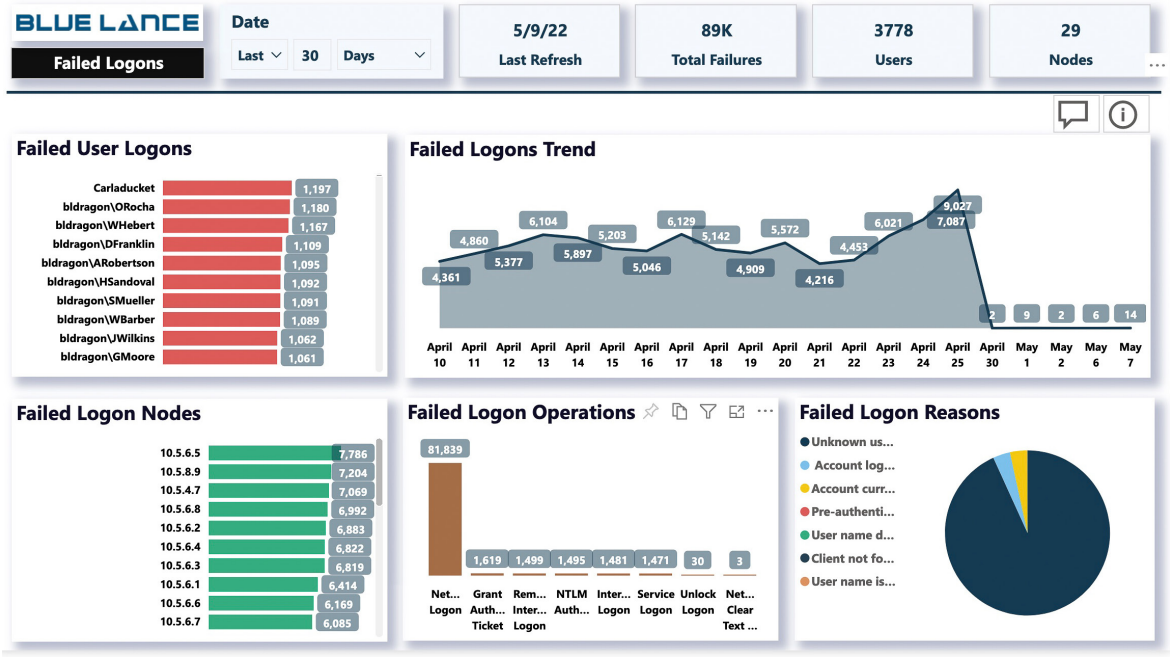


INVESTIGATE

Suspicious patterns of logon failures

Multiple failed logins from a single user on different nodes or machines is an extremely suspicious pattern of activity that should be immediately investigated for a malware infection. This is the kind of situation where malware on an infected host machine is attempting to move laterally within an organization.

The *Suspicious Failed Logons* LT Auditor+ panel quantifies all failed logons of valid users that have attempted access to multiple nodes in the organization. Investigators regularly use this panel to quickly pinpoint machines to scan for malware.

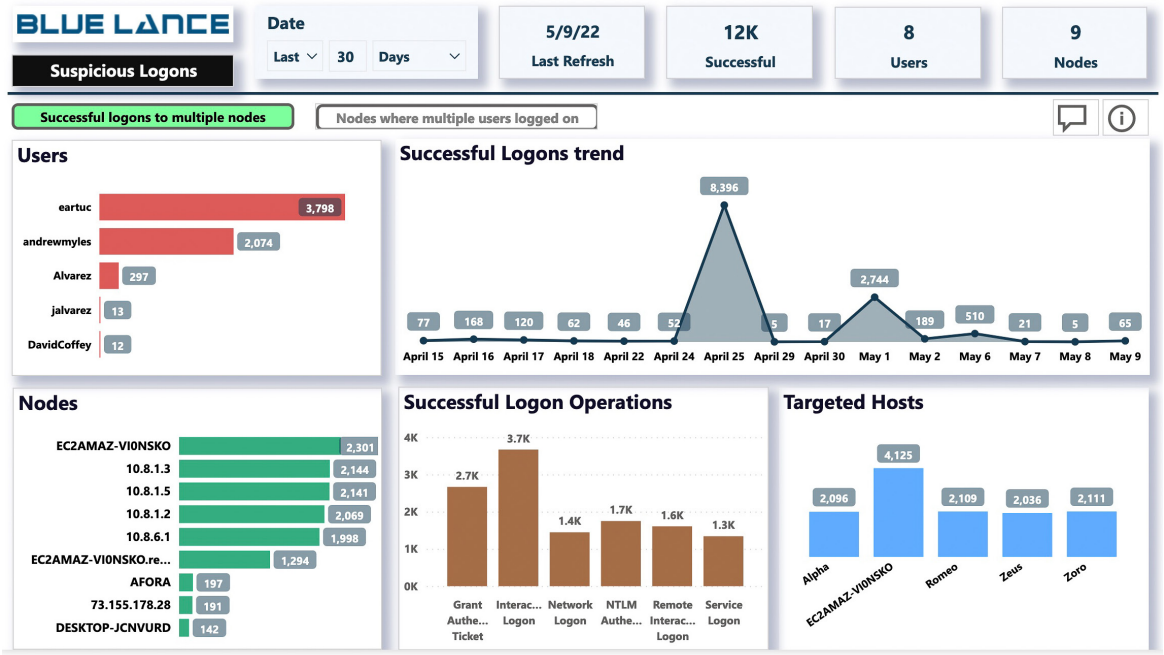


INVESTIGATE

Suspicious patterns of logon activity

Multiple successful logons from a single user on different nodes or machines is another extremely suspicious pattern of activity that warrants an immediate investigation for a malware infection. This is the kind of situation where malware on an infected host machine successfully gains a user's credentials and is moving laterally within an organization.

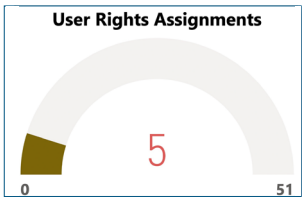
The Suspicious Logons LT Auditor+ panel consolidates all successful logons to multiple nodes in the organization allowing investigators to quickly pinpoint machines that warrant immediate scanning for malware.



INVESTIGATE

User rights assignments

User rights assignments are settings applied to the local devices on the network. They allow users to perform various system tasks, such as local logon, remote logon, backup, debug programs, impersonate a client etc. these rights are used to elevate privileges and need to be monitored by admins and security personnel to verify that there is no malicious activity.

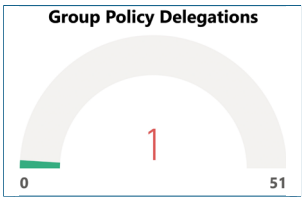


User Assignments

Rights Assigned To	Rights	Group Policy	Date	User	Node	Details
REDDRAGON\Alvarez	Create a token object	Policy Updates	5/9/2022 3:11:08 PM	REDDRAGON\\Alvarez	73.155.178.28	Added member [REDDRAGON\Alvarez] to the us VI0NSKO.reddragon.com]
REDDRAGON\andrewmyles	Generate security audits	Policy Updates	5/9/2022 3:54:11 PM	REDDRAGON\\Alvarez	73.155.178.28	Added member [REDDRAGON\andrewmyles] to t VI0NSKO.reddragon.com]
REDDRAGON\andrewmyles	Manage auditing and security log	Policy Updates	5/9/2022 3:53:41 PM	REDDRAGON\\Alvarez	73.155.178.28	Added member [REDDRAGON\andrewmyles] to t [EC2AMAZ-VI0NSKO.reddragon.com]
REDDRAGON\eartuc	Load and unload device drivers	Policy Updates	5/9/2022 3:11:38 PM	REDDRAGON\\Alvarez	73.155.178.28	Added member [REDDRAGON\eartuc] to the use VI0NSKO.reddragon.com]
REDDRAGON\paultractor	Debug programs	Policy Updates	5/9/2022 3:08:38 PM	REDDRAGON\\Alvarez	73.155.178.28	Added member [REDDRAGON\paultractor] to the VI0NSKO.reddragon.com]

Group policy delegations

Group Policy Delegations delegate rights. This is an important feature used by admins in their day-to-day operations. However, this feature is used by attackers to escalate their rights. Therefore, it is critical that these delegations be monitored continuously and verified to ensure that these assignments are not malicious or mistakenly assigned.



Passwords Reset

Date	User	Node	Target Object	Operation	Details	Member of Group
Monday, April 25, 2022	REDDRAGON\ pthomas		CN=Gordon Ramsey,CN=Users,DC= reddragon,DC=com	Set Password	Set Password for user CN=Gordon Ramsey,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Gordon Ramsey,CN=Users,DC= reddragon,DC=com	Set Password	Set Password for user CN=Gordon Ramsey,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Jhon King,CN=Users,DC=red dragon,DC=com	Set Password	Set Password for user CN=Jhon King,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Jhon King,CN=Users,DC=red dragon,DC=com	Set Password	Set Password for user CN=Jhon King,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, May 02, 2022	REDDRAGON\ eartuc		CN=Carla Ducket,CN=Users,DC=r eddragon,DC=com	Set Password	Set Password for user CN=Carla Ducket,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, May 02, 2022	REDDRAGON\ eartuc		CN=Carla Ducket,CN=Users,DC=r eddragon,DC=com	Set Password	Set Password for user CN=Carla Ducket,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, May 02, 2022	REDDRAGON\ Alvarez		CN=Andrew Myles,CN=Users,DC=re	Set Password	Set Password for user CN=Andrew Myles,CN=Users,DC=reddragon,DC=com	ServiceAccounts

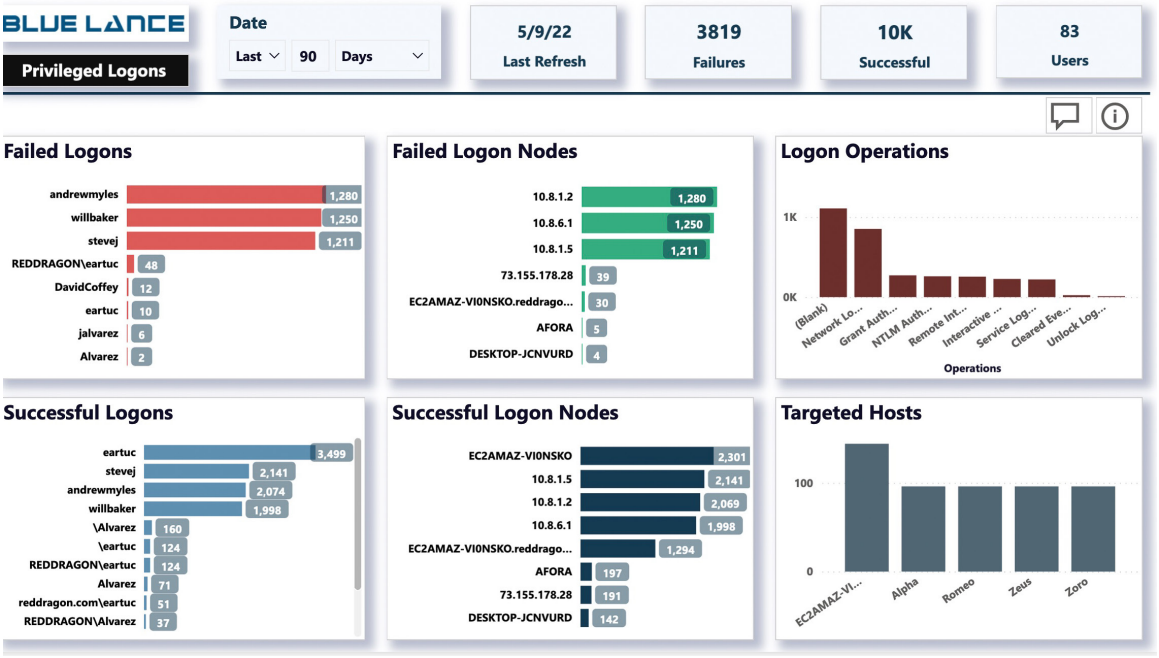
AUDIT

The Audit Function provides a set of activities that document the process of verification, proof and documentation of user, network and application monitoring activity. This data is required to ensure activities do not compromise configurations and settings creating vulnerabilities that are exploitable by a ransomware attack.

Privileged User activity

Privileged accounts consist of privileged and administrative accounts and these accounts have become the primary target for enterprise attacks. Privileged accounts have served as the root cause of some of the most significant cyber security breaches. Threat actors continue to breach the corporate perimeter through means such as phishing attacks, malware infected attachments, social media viruses, and other methods. Once inside, their primary goal is to infiltrate privileged accounts to gain access to additional servers, databases, and other high value systems. Auditing and monitoring privileged user activity is therefore critical to ensure that this activity is not malicious.

LT Auditor+ *Privileged Logons Panel* provides the intelligence on privileged user activity to quickly determine whether the activity is malicious.



AUDIT

Password changes to privileged and service accounts

Changes to passwords for privileged and service accounts must be audited to ensure this activity is not malicious and has been authorized. These accounts are used for administrative purposes as well, running various applications required within organizations making them a ripe target for attackers.

LT Auditor+ monitors all changes to privileged and service user account passwords and presents them in a comprehensive, easy to understand manner.

9

Service Account Password Resets

Passwords Reset

Date	User	Node	Target Object	Operation	Details	Member of Group
Monday, April 25, 2022	REDDRAGON\ pthomas		CN=Gordon Ramsey,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Gordon Ramsey,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Gordon Ramsey,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Gordon Ramsey,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Jhon King,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Jhon King,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Jhon King,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Jhon King,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, May 02, 2022	REDDRAGON\ eartuc		CN=Carla Ducket,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Carla Ducket,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, May 02, 2022	REDDRAGON\ eartuc		CN=Carla Ducket,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Carla Ducket,CN=Users,DC=reddragon,DC=com	ServiceAccounts
Monday, May 02, 2022	REDDRAGON\ Alvarez		CN=Andrew Myles,CN=Users,DC=re	Set Password	Set Password for user CN=Andrew Myles,CN=Users,DC=reddragon,DC=com	ServiceAccounts

16

Privileged User Password Resets

Passwords Reset

Date	User	Node	Target Object	Operation	Details	Member of Group
Friday, April 22, 2022	REDDRAGON\ Alvarez		CN=erayyy,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=erayyy,CN=Users,DC=reddragon,DC=com	Domain Admins
Friday, April 22, 2022	REDDRAGON\ Alvarez		CN=erayyy,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=erayyy,CN=Users,DC=reddragon,DC=com	Domain Admins
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=erayyy,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=erayyy,CN=Users,DC=reddragon,DC=com	Domain Admins
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=erayyy,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=erayyy,CN=Users,DC=reddragon,DC=com	Domain Admins
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=erayyy,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=erayyy,CN=Users,DC=reddragon,DC=com	Domain Admins
Monday, April 25, 2022	REDDRAGON\ eartuc		CN=Jhon King,CN=Users,DC=reddragon,DC=com	Set Password	Set Password for user CN=Jhon King,CN=Users,DC=reddragon,DC=com	Domain Admins
Monday,	REDDRAGON\		CN=Jhon	Set Password	Set Password for user CN=Jhon	Domain Admins

AUDIT

Group Policy changes

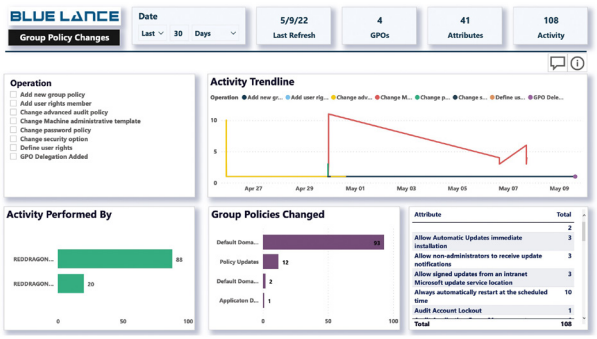
Active Directory Group Policies control the working environment of all Active Directory (AD) objects including users and computers. Group Policies define how different systems, users, and other AD objects interact with each other. Auditing changes to group policies is therefore vital for the following reasons:

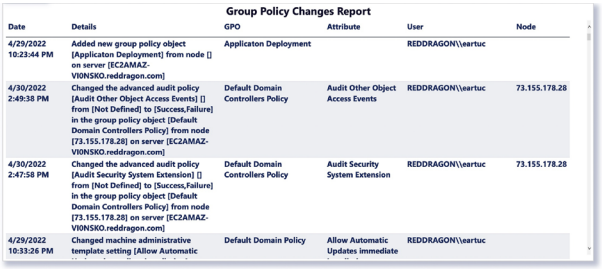
Ensure minimal organization impact from hostile access or denial of resources.

Policies applied comply with organizational security policies

Ensure that accounts are not mistakenly granted enhanced permissions making them susceptible to threat actors.

The LT Auditor+ Group Policy Changes Panel is an intuitive, easy to understand, panel with drill-down capabilities making what is normally a laborious and time-consuming task of auditing all changes made to Group Policies into a sophisticated, time-saving, critical auditing activity.





AUDIT

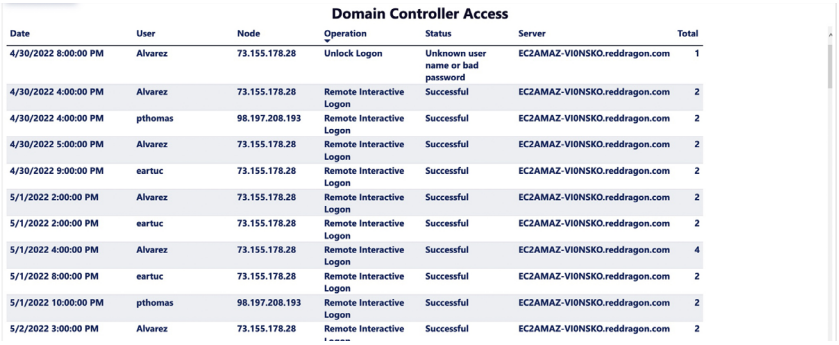
Domain Controller Access

Domain controllers provide the physical storage for the Active Directory database, in addition to providing the services and data that allow enterprises to effectively manage their servers, workstations, users, and applications. Malicious users relish the prospect of gaining privileged access to a domain controller so that they can modify, corrupt, or destroy the Active Directory database and by extension, all the systems and accounts that are managed by Active Directory.

Because domain controllers can read from and write to anything in the Active Directory database, once a malicious user has gained access and compromised a domain controller your Active Directory Forest can never be considered trustworthy again unless you are able to recover using a verifiable good backup and rectify the gaps that allowed the compromise.

For these reasons, it is critical to audit all direct access such as remote desktop access (RDP) and interactive logons on the Domain Controller and validate authorized activity. LT Auditor+ provides detailed auditing of all activity on Domain Controllers.

2433
Domain Controller Access



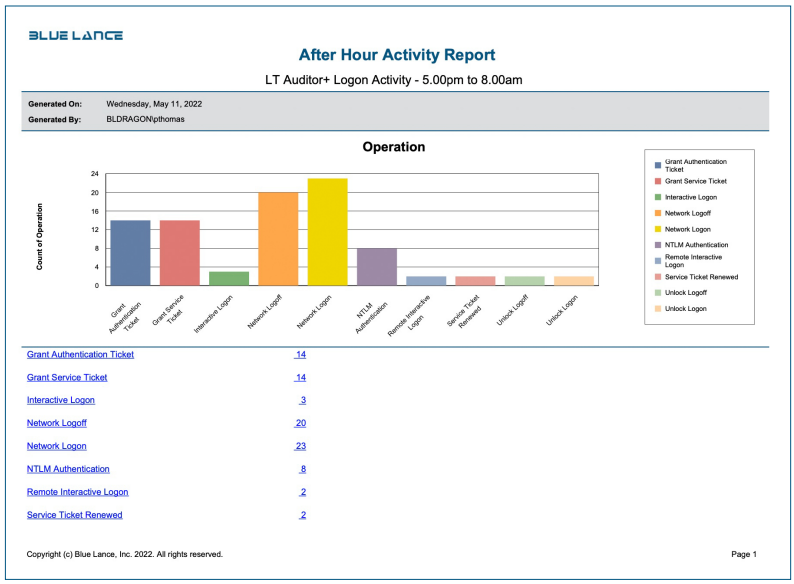
Domain Controller Access

Date	User	Node	Operation	Status	Server	Total
4/30/2022 8:00:00 PM	Alvarez	73.155.178.28	Unlock Logon	Unknown user name or bad password	EC2AMAZ-VI0NSKO.reddragon.com	1
4/30/2022 4:00:00 PM	Alvarez	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
4/30/2022 4:00:00 PM	pthomas	98.197.208.193	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
4/30/2022 5:00:00 PM	Alvarez	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
4/30/2022 9:00:00 PM	eartuc	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
5/1/2022 2:00:00 PM	Alvarez	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
5/1/2022 2:00:00 PM	eartuc	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
5/1/2022 4:00:00 PM	Alvarez	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	4
5/1/2022 8:00:00 PM	eartuc	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
5/1/2022 10:00:00 PM	pthomas	98.197.208.193	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2
5/2/2022 3:00:00 PM	Alvarez	73.155.178.28	Remote Interactive Logon	Successful	EC2AMAZ-VI0NSKO.reddragon.com	2

AUDIT

After-Hours activity

Reviewing authentications on the network outside of business hours is important to ensure this activity was authorized. Unauthorized activity is an indication of malware activity and must be investigated. LT Auditor+ has a specific report on after-hours activity designed to thoroughly research, investigate and validate evidence of authorized or malicious activity.



BLUE LANCE

After Hour Activity Report

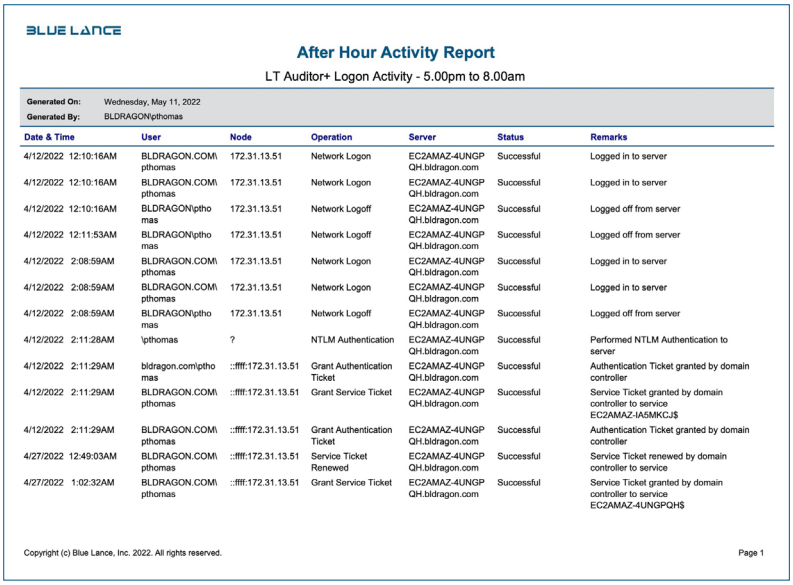
LT Auditor+ Logon Activity - 5.00pm to 8.00am

Generated On: Wednesday, May 11, 2022
Generated By: BLDRAGON\pthomas

Operation

Grant Authentication Ticket	14
Grant Service Ticket	14
Interactive Logon	3
Network Logoff	20
Network Logon	23
NTLM Authentication	8
Remote Interactive Logon	2
Service Ticket Renewed	2

Page 1



BLUE LANCE

After Hour Activity Report

LT Auditor+ Logon Activity - 5.00pm to 8.00am

Generated On: Wednesday, May 11, 2022
Generated By: BLDRAGON\pthomas

Date & Time	User	Node	Operation	Server	Status	Remarks
4/12/2022 12:10:16AM	BLDRAGON.COM\pthomas	172.31.13.51	Network Logon	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged in to server
4/12/2022 12:10:16AM	BLDRAGON.COM\pthomas	172.31.13.51	Network Logon	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged in to server
4/12/2022 12:10:16AM	BLDRAGON\pthomas	172.31.13.51	Network Logoff	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged off from server
4/12/2022 12:11:53AM	BLDRAGON\pthomas	172.31.13.51	Network Logoff	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged off from server
4/12/2022 2:08:59AM	BLDRAGON.COM\pthomas	172.31.13.51	Network Logon	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged in to server
4/12/2022 2:08:59AM	BLDRAGON.COM\pthomas	172.31.13.51	Network Logon	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged in to server
4/12/2022 2:08:59AM	BLDRAGON\pthomas	172.31.13.51	Network Logoff	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Logged off from server
4/12/2022 2:11:28AM	\pthomas	?	NTLM Authentication	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Performed NTLM Authentication to server
4/12/2022 2:11:29AM	bldragon.com\pthomas	::ffff:172.31.13.51	Grant Authentication Ticket	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Authentication Ticket granted by domain controller
4/12/2022 2:11:29AM	BLDRAGON.COM\pthomas	::ffff:172.31.13.51	Grant Service Ticket	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Service Ticket granted by domain controller to service EC2AMAZ-IA5MKCJ$
4/12/2022 2:11:29AM	BLDRAGON.COM\pthomas	::ffff:172.31.13.51	Grant Authentication Ticket	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Authentication Ticket granted by domain controller
4/27/2022 12:49:03AM	BLDRAGON.COM\pthomas	::ffff:172.31.13.51	Service Ticket Renewed	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Service Ticket renewed by domain controller to service
4/27/2022 1:02:32AM	BLDRAGON.COM\pthomas	::ffff:172.31.13.51	Grant Service Ticket	EC2AMAZ-4UNGPQH.bldragon.com	Successful	Service Ticket granted by domain controller to service EC2AMAZ-4UNGPQH$

Page 1

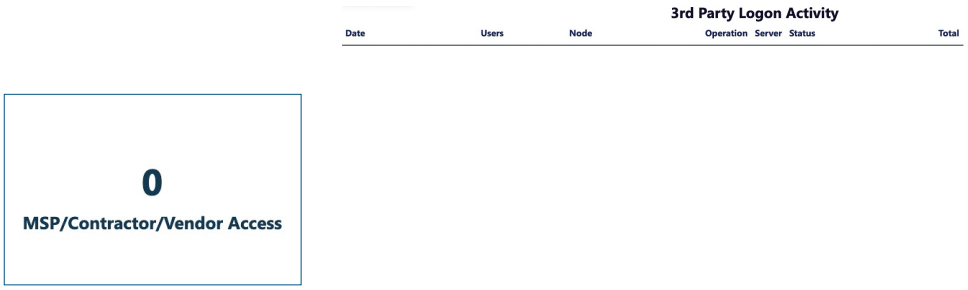
AUDIT

MSP/Contractor activity

Contractors, managed service providers (MSP), consultants, suppliers, IT services providers are among the list of third parties who are provided access to an organization's network. These entities typically connect remotely to service the organization. Several high-profile breaches over the past decade have demonstrated that vendor networks can be leveraged to gain access into customer environments. Increased risks include:

- Introducing malware
- Leaving credentials inadequately protected so that they may be intercepted and/or reused
- Poorly restricted access, allowing for lateral movement

Rigorous auditing of all third-party access across the network, with LT Auditor+, is vital to ensure early detection of unauthorized access.



AUDIT

Installation of Applications and Services

A primary vector used by attackers for embedding malware on the network is malware infected attachments in phishing emails. Upon the attachment being opened, a malicious application or service is installed that seeks out dormant privileged accounts, takes over existing accounts, moves laterally, elevates privileges, encrypts and destroys files and so on. Therefore, installation of all applications and services on the network must be audited to ensure they are authorized. When an organization is in the throes of a ransomware attack, time is of the essence. LT Auditor+ provides real-time alerting and detailed audit reports on all such activities for immediate investigation, validation, and verification.

17
Applications Installed

Applications Installed

Date	Description	Host	User	Node
3/30/2022 5:02:12 PM	Product: Adobe Acrobat DC (64-bit) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/31/2022 4:56:15 PM	Product: Adobe Acrobat DC (64-bit) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:05:00 PM	Product: CorelDRAW Graphics Suite 2022 - Common (x64) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:06:12 PM	Product: CorelDRAW Graphics Suite 2022 - Common (x64) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:05:09 PM	Product: CorelDRAW Graphics Suite 2022 - Draw (x64) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:05:13 PM	Product: CorelDRAW Graphics Suite 2022 - Font Manager (x64) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:04:29 PM	Product: CorelDRAW Graphics Suite 2022 -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:04:36 PM	Product: CorelDRAW Graphics Suite 2022 -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022 5:05:12 PM	Product: CorelDRAW Graphics Suite 2022 - PHOTO-PAINT (x64) -- Installation operation completed successfully.	EC2AMAZ-VI0NSKO.reddragon.com	REDDRAGON\eartuc	EC2AMAZ-VI0NSKO.reddrag
3/30/2022	Product: Dropbox Update Helper -- Installation completed successfully.	EC2AMAZ-	REDDRAGON\eartuc	EC2AMAZ-

31
Windows Services Installed

Services Installed

Date	Description	Host	User	Node	EventID
3/30/2022 4:22:33 PM	A service was installed in the system. Service Name: LT Auditor+ Syslog Server Service File Name: "D:\Program Files\Blue Lance, Inc\LT Auditor+\Syslog Server\Bin \LTASyslogServer.exe" Service Type: user mode service Service Start Type: auto start Service Account: LocalSystem	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon .com	7045
3/30/2022 5:01:48 PM	A service was installed in the system. Service Name: Adobe Acrobat Update Service Service File Name: "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe" Service Type: user mode service Service Start Type: auto start Service Account: LocalSystem	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon .com	7045
3/30/2022 5:07:48 PM	A service was installed in the system. Service Name: McAfee Safe Connect Service	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon .com	7045

AUDIT

Creating instances of persistence via updates to Task Scheduler

Once adversaries have gained access to the network, they configure system settings to automatically execute a ransomware program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. This is achieved by scheduling the execution of malware in the Windows Task Scheduler. The Windows Task Scheduler comes with all Windows operating systems. Attackers leverage this quick and easy way to activate ransomware at system boot or during logon.

LT Auditor+ audits all changes to the task scheduler and provides detailed audit reports for verification and validation.

671
Scheduled Tasks Created

Scheduled Tasks

Date	Description	Host	User	Node	EventID
3/29/2022 3:15:04 PM	A scheduled task was created. Subject: Security ID: S-1-5-21-2646044752-2863034650-815753254-1115 Account Name: eartuc Account Domain: REDDRAGON Logon ID: 0xf43f4 Task Information: Task Name: \eray Task Content: <?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows /2004/02/mit/task"> <RegistrationInfo> <Date>2022-03-29T15:15:04.1417528</Date> <Author>REDDRAGON\eartuc</Author> <Description>aaaaa</Description> <URI>\eray</URI> </RegistrationInfo> <Triggers> <CalendarTrigger>	EC2AMAZ-VI0NSKO.reddragon.com	\	EC2AMAZ-VI0NSKO.reddragon.com	4698

Ensure latest Windows patches are applied to domain controllers, servers and workstations

Unpatched systems are the most vulnerable systems to a ransomware attack. Patch management is a complex and tedious process to implement across the entire organization. Often, there is no validation that patches were successfully applied and vulnerabilities resolved. The LT Auditor+ Windows Updates Applied audit report provides auditors, admins and investigators proof and validation of which patches were successfully applied, when and by whom.

36
Windows Updates Applied

Windows Updates Applied

Date	Description	Host	User	Node	EventID
3/28/2022 11:14:20 PM	Installation Successful: Windows successfully installed the following update: Windows Malicious Software Removal Tool x64 - v5.98 (KB890830)	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon.com	19
3/28/2022 11:18:31 PM	Installation Successful: Windows successfully installed the following update: Windows Malicious Software Removal Tool x64 - v5.99 (KB890830)	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon.com	19
3/29/2022 2:27:43 PM	Installation Successful: Windows successfully installed the following update: 2021-01 Update for Windows Server 2019 for x64-based Systems (KB4589208)	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon.com	19
3/29/2022 2:27:43 PM	Installation Successful: Windows successfully installed the following update: 2022-02 Cumulative Update Preview for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5011267)	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon.com	19
3/29/2022 2:27:43 PM	Installation Successful: Windows successfully installed the following update: 2022-03 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB5011503)	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon.com	19
3/29/2022 2:27:43 PM	Installation Successful: Windows successfully installed the following update: Security Update for Windows Server 2019 for x64-based Systems (KB4535680)	EC2AMAZ-VI0NSKO.reddragon.com	NT AUTHORITY\SYSTEM	EC2AMAZ-VI0NSKO.reddragon.com	19

SUMMARY

In summary, IT Security auditing is key to reducing the attack surface area and network dwell time. Reducing the attack surface area and network dwell time is critical in managing and mitigating the risk of ransomware attacks. The *Assess, Investigate* and *Audit* Functions are imperative in hardening the IT Infrastructure and improving an organization's cyber posture.

Manage and Mitigate Risk of Ransomware Attacks with LT Auditor+ by continuously:

applying principles of least privilege;

performing cyber hygiene tasks such as remediating dormant accounts, passwords settings and excessive privileges;

revewing suspicious logon activity, privilege escalations and security patch updates.

To schedule a demo, or for more information:

Email: reduceransomwareattacks@bluelance.com
Tel: 713-255-4800

ABOUT BLUE LANCE

Blue Lance is a global provider of IT Security Audit and Compliance Automation Software. Headquartered in Houston, Texas, Blue Lance has been committed to corporate vitality and helping companies with the safekeeping of their digitally managed assets.

Blue Lance's IT Security Audit software enables confident oversight and validation of audit readiness for internal policies, industry or government regulations; and the safe keeping of confidential information, trade secrets, intellectual property, critical infrastructure, and other digitally-managed assets.

BLUE LANCE

bluelance.com
410 Pierce Street, Suite 300
Houston, TX 77062
info@bluelance.com
800. 856. 2583.