

7 ways to frustrate attackers

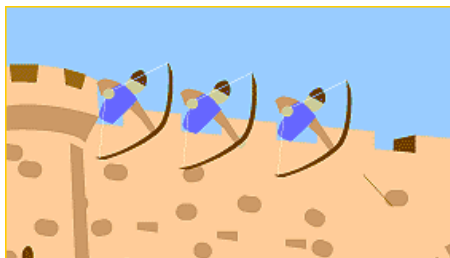
Sean D. Goodwin, GSE | 0xSeanG



<https://web.cvent.com/event/76d46ccb-fe00-4fe5-ba46-e4a77c807f21/summary>

AGENDA

- ▀ Setting the Stage (hint: we're winning)
- ▀ Where to Start (what are the attackers doing??)
- ▀ Attack Techniques and Defensive Measures



WHOAMI

- 10+ years in cybersecurity consulting
- Accounting > IT Audit > Pentesting & beyond
- Collector of alphabet soup



**SEAN D.
GOODWIN, GSE**

Senior Manager, DenSecure

SDGoodwin@wolfandco.com

617.261.8139

<https://www.linkedin.com/in/0xseang/>

<https://twitter.com/0xSeanG>

<https://www.wolfandco.com/services/densecure/>



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

3

- SDGoodwin@wolfandco.com
- <https://www.linkedin.com/in/0xseang/>
- <https://twitter.com/0xSeanG>
- <https://www.wolfandco.com/services/densecure/>

SETTING THE STAGE



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

US news
Cyberattack disrupts hospital computer systems across US, hindering services

**Oakland ransomware attack:
Here's a look at how other cities
solved their cyberattacks**

**K-12 schools in Tucson,
Nantucket respond to
cyberattacks**

**Electoral Commission apologises for
security breach involving UK voters'
data**

LOHRMANN ON CYBERSECURITY

**CL0P Ransomware Gang Attacks Top June Cyber
Headlines**

The CL0P ransomware gang, reportedly based in Russia, has breached at least 122 organizations using MOVEit zero day exploits. Here's what you need to know.



**Ransomware attacks have room
to grow, Verizon data breach
report shows**



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

5

- <https://www.theguardian.com/us-news/2023/aug/04/cyberattack-us-hospitals-California>
- <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cl0p-ransomware-gang-attacks-top-june-cyber-headlines>
- <https://www.infosecurity-magazine.com/news-features/cyber-attacks-media-industry/>
- <https://www.theguardian.com/technology/2023/aug/08/uk-electoral-commission-registers-targeted-by-hostile-hackers>
- <https://abc7news.com/oakland-ransomware-attack-cyberattack-system-down-cybersecurity/12851277/>
- <https://www.scmagazine.com/analysis/ransomware-attacks-have-room-to-grow-verizon-data-breach-report-shows>
- <https://therecord.media/k-12-schools-ransomware-tucson-nantucket>

DEFENDERS ARE WINNING

“In almost one-quarter of all incidents remediated in 2022, the deployment of backdoors at 21% was the top action on objective.”[1]



[1] IBM Security X-Force Threat Intelligence Index 2023: <https://www.ibm.com/reports/threat-intelligence>

© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

6

Andy is the Global Head of Threat Intelligence @ IBM X-Force

- <https://www.ibm.com/downloads/cas/DB4GL8YM>

WHERE TO START



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

CISA ADVISORY AA23-059A

- Red Team Assessment against a large critical infrastructure organization
- Mapped to MITRE ATT&CK®
- 13 distinct measurable events, only 3 were actioned
- No NDAs being violated

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

REPORT A CYBER ISSUE

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Cybersecurity Advisory](#)

SHARE: [f](#) [t](#) [in](#) [e](#)

CYBERSECURITY ADVISORY

CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks

Release Date: February 28, 2023

Alert Code: AA23-059A



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>

8

For all the references of the CISA red team report, it is worth highlighting that these aren't secret techniques (many penetration testers use them so people should ensure their testers are performing it, and they aren't tied to a CVE). For the sake of this talk, we focus on the tactics but not always the exact procedures here, as this is meant to focus on higher-level actions you can take. I **would** however recommend that you look at the detailed appendices in the report to TTX against your environment.

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://attack.mitre.org/>
- <https://d3fend.mitre.org/>

ATTACK TECHNIQUES AND DEFENSIVE MEASURES



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

INITIAL ACCESS

■ The CISA red team gained initial access [[TA0001](#)] to two workstations at geographically separated sites (Site 1 and Site 2) via spearphishing emails. The team first conducted open-source research [[TA0043](#)] to identify potential targets for spearphishing.



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

10

This is arguably the highest effort item discussed today

The answer is not more security awareness training videos

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://web.archive.org/web/20180407204216/https://isc.sans.edu/diary/Deco+Personas+for+Safeguarding+Online+Identity+Using+Deception/16159>
- <https://attack.mitre.org/versions/v12/tactics/TA0001/>
- <https://attack.mitre.org/versions/v12/tactics/TA0043/>

INITIAL ACCESS

▀ Decoy Persona

▀ *"A false online identity is created for the purposes of interacting with adversaries in a direct or indirect manner. This includes the associated email addresses, social media accounts, and other online communication profiles."*

▀ Create Target email address(s)

▀ Create a forwarding rule to ticketing system

▀ Lay the bait where attackers are likely to look

- Web pages (about us, blog post, etc) are lower effort
- Full Decoy Persona (e.g., create a sock account on LinkedIn and include the email)



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

11

Never use a real email address

Try to use a format that slightly differs from normal, but is believable (e.g., normal is fname.lname@example.com, use lname.fname@example.com)

I think it's worth talking about passwords and the fact that MFA is usually not properly applied. Red teams are bypassing it due to MFA fatigue (no number matching) and token tactics (i.e. device code phishing)

- <https://d3fend.mitre.org/technique/d3f:DecoyPersona/>
- <https://canarytokens.org/generate>
- <https://www.wolfandco.com/resources/blog/defending-secure-authentication-processes-against-attacks/>
- <https://www.blackhillsinfosec.com/dynamic-device-code-phishing/>

DOMAIN ENUMERATION

- On Workstation 1, the team leveraged a modified SharpHound collector, ldapsearch, and command-line tool, dsquery, to query and scrape AD information, including AD users [T1087.002], computers [T1018], groups [T1069.002], access control lists (ACLs), organizational units (OU), and group policy objects (GPOs) [T1615].



© 2023 Wolf & Company, P.C. Member Of ALLINIA GLOBAL, An Association Of Legally Independent Firms

12

Bloodhound is an incredibly useful tool for both attackers and defenders. The value of the tool, and the graph theory concept, increases as more data is brought in for analysis.

The more LDAP queries used, the larger the data set for an attacker to find “the best” path forward, but this also increases your ability to detect!

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://bloodhoundenterprise.io/bloodhound-feature-comparison/>
- <https://attack.mitre.org/versions/v12/techniques/T1087/002/>
- <https://attack.mitre.org/versions/v12/techniques/T1018/>
- <https://attack.mitre.org/versions/v12/techniques/T1069/002/>
- <https://attack.mitre.org/versions/v12/techniques/T1615/>

DOMAIN ENUMERATION

- ▀ Enable Directory Service Access Audit Policy
- ▀ Create a Decoy Users, Computer, and Group Objects
 - Referenced blog post includes step-by-step guides
- ▀ Create alerts for the GUID value for all decoy objects created for Windows Event ID 4662

Detecting LDAP enumeration and Bloodhound's Sharphound collector using AD Decoys



Madhukar Raina · Follow

Published in Securonix Tech Blog · 9 min read · Jul 28, 2021



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

13

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://medium.com/securonix-tech-blog/detecting-ldap-enumeration-and-bloodhound-s-sharphound-collector-using-active-directory-decoys-dfc840f2f644>

UNCONSTRAINED DELEGATION

- The team then exploited the Unconstrained Delegation misconfiguration to steal the DC's TGT. They ran the [DFSCoerce](#) python script (DFSCoerce.py), which prompted DC authentication to the SharePoint server using the server's NTLM hash. The team then deployed [Rubeus](#) to capture the incoming DC TGT [T1550.002], [T1557.001]. (DFSCoerce abuses Microsoft's Distributed File System [MS-DFSNM] protocol to relay authentication against an arbitrary server.[1])
- The team then used the TGT to harvest advanced encryption standard (AES)-256 hashes via DCSync [T1003.006] for the krbtgt account and several privileged accounts—including domain admins, workstation admins, and a system center configuration management (SCCM) service account (SCCM Account 1). The team used the krbtgt account hash throughout the rest of their assessment to perform golden ticket attacks [T1558.001] in which they forged legitimate TGTs. The team also used the asktgt command to impersonate accounts they had credentials for by requesting account TGTs [T1550.003].



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

14

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://github.com/Wh04m1001/DFSCoerce>
- <https://github.com/GhostPack/Rubeus>
- <https://attack.mitre.org/techniques/T1550/002/>
- <https://attack.mitre.org/versions/v12/techniques/T1557/001/>
- <https://attack.mitre.org/versions/v12/techniques/T1003/006/>
- <https://attack.mitre.org/versions/v12/techniques/T1558/001/>
- <https://attack.mitre.org/versions/v12/techniques/T1550/003/>
- [1] <https://www.bleepingcomputer.com/news/microsoft/new-dfsc coerce-ntlm-relay-attack-allows-windows-domain-takeover/>

UNCONSTRAINED DELEGATION

Prevention is best here

- MS: [Mitigating Pass-the-Hash \(PtH\) Attacks and Other Credential Theft, Version 1 and 2](#)
- Reset the KRBTGT password **TWICE**

Detection

- Ensure all DCs are logging Event ID 4769
 - Filter out the noise
 - Audit Success
 - Ticket Options: 0x40810000
 - Ticket Encryption: 0x17
- PowerShell v5 & script block logging enabled
 - Event IDs 4100, 4103, 4104 to capture PS Kerberos ticket requests



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

15

At this point your DC is compromised, but all hope is not lost – you are still in the fight

- <https://www.extrahop.com/company/blog/2021/detect-kerberos-golden-ticket-attacks/>
- https://web.archive.org/web/20230225062900/https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
- <https://www.microsoft.com/en-US/download/details.aspx?id=36036>
- <https://adsecurity.org/?p=3458>
- https://github.com/bryant-treacle/Kerberos_Golden_Ticket_Finder
- <https://redsiege.com/tools-techniques/2020/10/detecting-kerberoasting/#detection>

LATERAL MOVEMENT

- While traversing the network, the team varied their lateral movement techniques to evade detection and because the organization had non-uniform firewalls between the sites and within the sites (within the sites, firewalls were configured by subnet). The team's primary methods to move between sites were AppDomainManager hijacking and dynamic-link library (DLL) hijacking [T1574.001]. In some instances, they used Windows Management Instrumentation (WMI) Event Subscriptions [T1546.003].
- The team impersonated several accounts to evade detection while moving. When possible, the team remotely enumerated the local administrators group on target hosts to find a valid user account. This technique relies on anonymous SMB pipe binds [T1071], which are disabled by default starting with Windows Server 2016.



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

16

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://attack.mitre.org/versions/v12/techniques/T1574/001/>
- <https://attack.mitre.org/versions/v12/techniques/T1546/003/>
- <https://attack.mitre.org/versions/v12/techniques/T1071/>

LATERAL MOVEMENT

▀ Tiered Administrative Strategy

- Instead of admins with a daily driver & an admin, break out admin accounts by asset tier (workstations, servers, DCs, etc.)

▀ Local Administrator Password Solution (LAPS)

- Preventive & Detective

▀ Network Intrusion Detection System

- Security Onion includes Suricata

▀ Harden Admin Network

- Admins should be coming from dedicated hosts
- Local client firewalls can be configured to block other inbound traffic (e.g. wkstn-wkstn)
- WinRM can be configured to allow traffic from specified hosts



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

17

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan>
- <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-guide-how-to-configure-microsoft-local/ba-p/2806185>
- <https://redcanary.com/blog/lateral-movement-winrm-wmi/>
- <https://docs.securityonion.net/en/2.3/suricata.html>

UNSECURED CREDENTIALS

- ▀ The team moved laterally to an MDM server (MDM 1) at Site 3, searched files on the server, and found plaintext credentials [T1552.001] to an application programming interface (API) user account stored in PowerShell scripts.
- ▀ The Workstation 5 user had bash history files with what appeared to be SSH passwords mistyped into the bash prompt and saved in bash history [T1552.003].
- ▀ On Workstation 6, the team found a .txt file containing plaintext credentials for the user. Using the pattern discovered in these credentials, the team was able to crack the user's workstation account password [T1110.002]



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

18

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://attack.mitre.org/versions/v12/techniques/T1552/001/>
- <https://attack.mitre.org/versions/v12/techniques/T1552/003/>
- <https://attack.mitre.org/versions/v12/techniques/T1110/002/>

UNSECURED CREDENTIALS

▀ Back to Deception – plant credentials in the network

- Utilize valid user accounts, but plant a bad password
- PowerShell scripts, TXT files, XLSX files, etc.
- Event ID 4624 for the target accounts
 - Filter status code 0xC000006A (user name is correct but the password is wrong)

▀ Hunt your network for users storing credential this way

- I know the AUP says not to.... Someone is



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

19

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://www.trustedsec.com/blog/creating-honey-credentials-with-lsa-secrets/>

COMMAND AND CONTROL

■ The team used third-party owned and operated infrastructure and services [T1583] throughout their assessment, including in certain cases for command and control (C2) [TA0011]. These included:

- [Cobalt Strike](#) and [Merlin](#) payloads for C2 throughout the assessment. Note: Merlin is a post-exploit tool that leverages HTTP protocols for C2 traffic.
 - The team maintained multiple Cobalt Strike servers hosted by a cloud vendor. They configured each server with a different domain and used the servers for communication with compromised hosts. These servers retained all assessment data



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

20

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://attack.mitre.org/versions/v12/techniques/T1583/>
- <https://attack.mitre.org/versions/v12/tactics/TA0011/>
- <https://attack.mitre.org/versions/v12/software/S0154/>
- <https://github.com/Ne0nd0g/merlin>

COMMAND AND CONTROL

Network Intrusion Detection System

- RITA is designed specifically for C2 detection
- Security Onion includes Suricata

Onion-Zeek-RITA: Improving Network Visibility and Detecting C2 Activity

Dallas Haselhorst



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

21

Install

Please see our recommended [System Requirements](#) document if you wish to use RITA in a production environment.

Automated Install

RITA provides an install script that works on Ubuntu 20.04 LTS, Debian 11, Security Onion, and CentOS 7.

Download the latest `install.sh` file [here](#) and make it executable: `chmod +x ./install.sh`

Then choose one of the following install methods:

- `sudo ./install.sh` will install RITA as well as supported versions of Zeek and MongoDB. This is suitable if you want to get started as quickly as possible or you don't already have Zeek or MongoDB.
- `sudo ./install.sh --disable-zeek --disable-mongo` will install RITA only, without Zeek or MongoDB. You may also use these flags individually.
 - If you choose not to install Zeek you will need to [provide your own logs](#).
 - If you choose not to install MongoDB you will need to configure RITA to [use your existing MongoDB server](#).

Docker Install

See [here](#).

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://github.com/activecm/rita>
- <https://www.activecountermeasures.com/free-tools/rita/>
- <https://docs.securityonion.net/en/2.3/suricata.html>
- <https://www.giac.org/research-papers/38755/>

AUDIT LOGGING

- ▀ You can't detect what you can't see
- ▀ 13 observable events
- ▀ 4 events were detected or acted upon



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

22

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>

AUDIT LOGGING



Cheat Sheets to help you in configuring your systems:

- The Windows Logging Cheat Sheet
- The Windows Advanced Logging Cheat Sheet
- The Windows HUMIO Logging Cheat Sheet
- The Windows Splunk Logging Cheat Sheet
- The Windows File Auditing Logging Cheat Sheet
- The Windows Registry Auditing Logging Cheat Sheet
- The Windows PowerShell Logging Cheat Sheet
- The Windows Sysmon Logging Cheat Sheet

MITRE ATT&CK Cheat Sheets

- The Windows ATT&CK Logging Cheat Sheet
- The Windows LOG-MD ATT&CK Cheat Sheet





© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

23

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
- <https://www.malwarearchaeology.com/cheat-sheets>

Measurable Event	ATT&CK Techniques	Audit Log(s)
Internal Port Scan	T1046	Network traffic analysis, Event ID: 5156
Comprehensive Active Directory and Host Enumeration	T1482, T1087.002, T1033, T1018	Event ID: 4688, 4663, 5156
Data Exfiltration – 1 GB of Data	T1048	Network traffic analysis, Event ID: 5156
Malicious Traffic Generation – Workstation to External Host	T1071	Network traffic analysis, Event ID: 5156
Active Directory Account Lockout	T1531	Event ID: 4740
Local Admin User Account Creation (workstation)	T1136.001, T1093	Event ID: 4688, 4624
Local Admin User Account Creation (server)	T1136.001, T1098	Event ID: 4688, 4624
Active Directory Account Creation	T1136.002, T1098	Event ID: 4688, 4624
Workstation Admin Lateral Movement – Workstation to Workstation	T1078.002, T1021.002, T1543.003	Event ID: 4688, 4624, 4625
Domain Admin Lateral Movement – Workstation to Domain Controller	T1078.002, T1021.002, T1543.003	Network Traffic Analysis, Event ID: 5156, 4624, 4625
Malicious Traffic Generation – Domain Controller to External Host	T1071	Network Traffic Analysis, Event ID: 5156
Trigger Host-Based Protection – Domain Controller	T1105	AV/EDR logs
Ransomware Simulation	N/A	**Simulation didn't actually encrypt files

Example Audit Log detections from Malware Archaeology

© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

24

This case study only had 4 actions detected:

- AD and Host enum
 - Collection process was stopped before completion, host was isolated
 - Trigger host based detection DC
 - File removed by malware
 - Ransomware
 - 4 users reported
-
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a>
 - <https://www.malwarearchaeology.com/cheat-sheets>



QUESTIONS



**SEAN D.
GOODWIN, GSE**

Senior Manager, DenSecure

SDGoodwin@wolfandco.com

617.261.8139

<https://www.linkedin.com/in/0xseang/>

<https://twitter.com/0xSeanG>

<https://www.wolfandco.com/services/densecure/>



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

25

- SDGoodwin@wolfandco.com
- <https://www.linkedin.com/in/0xseang/>
- <https://twitter.com/0xSeanG>
- <https://www.wolfandco.com/services/densecure/>

<https://www.wolfandco.com/>

PANY, P.C.

O.
HED

ABOUT WOLF & COMPANY, P.C.

111

YEARS IN BUSINESS

- ⊙ Established in 1911
- ⊙ Built on quality and integrity
- ⊙ Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+

EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- ⊙ Lower-than-industry-average staff turnover means a consistent team structure year after year
- ⊙ Niche team dedicated to your industry



RESOURCES TO LEARN MORE

- ⊙ [Cultures & Values](#)
- ⊙ [Social Responsibility](#)
- ⊙ [Inclusion & Diversity](#)
- ⊙ [Thought Leadership](#)
- ⊙ [Our History](#)
- ⊙ [Wolf Global](#)



Wolf & Company ranked
**#2 BEST LARGE FIRM
TO WORK FOR**
nationwide

accountingTODAY



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

ABOUT WOLF & COMPANY, P.C.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.



ADVISORY

- Business Continuity Planning
- Cybersecurity
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Penetration Testing
- Regulatory Compliance
- Strategic Planning



ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting



TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group



VSUITE

- Virtual Consulting Services
 - Business Continuity Planning (BCP)
 - Virtual Chief Information Security Officer (vCISO)
 - Virtual Chief Privacy Officer (vCPO)
 - Virtual Chief Risk Officer (vCRO)
 - Virtual Vendor Management



WOLFPAC

- Integrated risk management SaaS suite



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

WOLF ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

INSIDE Public
Accounting

TOP 100
Accounting Firms

accountingTODAY

TOP 100
Accounting Firms

#2 BEST LARGE FIRM to
Work For Nationwide

TOP FIRMS:
New England

BOSTON
BUSINESS JOURNAL

- ⊙ Area's Best Places to Work
- ⊙ Area's Most Admired Companies
- ⊙ Area's Fastest Growing Private Companies
- ⊙ Area's Largest I.T. Consulting Firms

Forbes

America's Best
Tax and Accounting
Firms of 2023, 2021



© 2023 Wolf & Company, P.C. Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Advanced Security Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation



© 2023 Wolf & Company, P.C.
Member Of ALLINIAL GLOBAL, An Association Of Legally Independent Firms



<https://www.wolfandco.com/services/densecure/>

