

Email Investigation

Scenario: In this exercise, you have been given a compromised device. During your investigation, you have isolated an email address as the source of the compromise.

Goal: You are tasked with investigating the email address to gain more information about the threat actor.

Objective 1: What have you determined about this email address?

Objective 2: Is there any threat actor associated with the email address?

Objective 3: What have to you discovered about this threat actor?

STEP 1: Perform a search for <u>macie.dietrich50@mail.com</u>

https://community.riskiq.com/search/whois/email/macie.dietrich50@mail.com

	riskiq.com/search/whois/email/macie.dietrich50@mail.com			💊 ★ O 🌬 🐴 🖲 🕼 E
	e.dietrich50@mail.com			Tours Enterprise 😡 👤
macie.dietrich50@m	ail.com			
Whois Search Whois History				
* DATA				
FILTERS O	WHOIS HISTORY ()			
DOMAIN (2/2)	v Show:25 < 1-2 of 2 ► Sort:First Seen Ascending *			Download Copy
✓ × tas-cass.org 1	Demain	first seen	last seen	
✓ X wada-arna.org 1	. wada-arma.org	2016-08-18	2018-09-24	
FIST SEEN (2/2)	tas-case.org	2016-10-02	2018-09-23	
✓ ※ 2016-08-18 17 1	1-2 of 2			
✓ × 2016-10-02 00 1				
LAST SEEN (2/2)				
✓ × 2018-09-24 17 1				
				•
				9
v4.0.0-38b7064 0 2018, RiskiQ Inc. All Ry	this Reserved. Proprietary and confidential; do not distribute without prior approval. Privacy Polic	r Terms and Conditions		💍 RISKIQ

From the WHOIS history, we see that two domains were registered using macie.dietrich50@mail.com.

Step 2: wada-arna[.]org and tas-cass[.]org in a new tab.

▼ Show:25 ◄ 1-2 of 2 ► So	t - First Coop According	[□ ▼] Show : 25	1-2 of 2 ▶	Sort : First Seen Ascending 🔻
Domain	t : First seen Ascending *		Domain	
wada-arna.org	Open Link in New Tab		wada-arna.	
tas-cass.org	Open Link in New Window Open Link in Incognito Window		tas-cass.org	Open Link in New Tab Open Link in New Window
2 of 2	Save Link As Copy Link Address	1-2 of 2		Open Link in Incognito Window
	Copy Go to wada-arna.org Print ⊕ Blockade ► ⊸ FatBeagle ► ► Coogle Translate			Copy Link Address Copy Go to tas-cass.org Print Blockade Categole Fanslate
	Inspect			Inspect
	Speech Services			Speech Services

Step 3: Go to the tab for wada-arna[.]org

🗄 💭 RISKIQ 🔍 🔍	wada-arna.org O							Tours Enterprise	0
	Registrar Gabaddy.com, LLC Registrant Domains By Prony, Law	nd 📃 Hashes 🛛 Espio	nage O Fancybear O Russia	• Categorize					
	shift-click the heatmap to filter the results below						_	LEGEND 📕 📕 🕅	in u
	Su					2 2 2	2 2 2 2 2 2 2 2		
	74					2 2 2	2 2 2 2 2 2 2		
	102					2 2 2	2 2 2 2 2 2 2		
	Th Pr				2		$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		
	Sa				2		2 2 2 2 2 2		
		p.d	Aug	Sep	00		Nov Dec		
						2018-06-10 to 2018-12-1	2		
DATA									
DATA		6 6	0 6	0 5	2	10 5	15 5 0		
	Res	olutions WHOIS	Certificate Subdomains	Trackers Compor	ents Host Pairs	OSINT Hashes	DNS Projects Cookies		
		olutions WHOIS	Certificate Subdomains	Trackers Compor	ents Host Pairs	OSINT Hashes	DNS Projects Cookies		
	RESOLUTIONS 0			Trackers Compor	ents Host Pairs	OSINT Hashes	DNS Projects Cookies	Deploy	-
IP (6./ 6)	RESOLUTIONS (0)	Sort : Last Seen Desce	ndirg *					Download (Сору
IF (6/6) ✓ X 0.0.0.0 1	RESOLUTIONS 0			Trackers Compor	First 2018-10-04	OSINT Hashes	DNS Projects Cookies	Download (Tags	Сору
IP (6/6) ✓ × 0.0.0.0 1 ✓ × 149.154.157.171 1	RESOLUTIONS () Show: 25 < 1.6 of 6 + Netable 	Sort : Last Seen Desce Location	nding * Network		First	Last	Source		Сору
IP (6/6) ✓ × 0.0.0.0 1 ✓ × 149.154.157.171 1 ✓ × 209.99.40.223 1 ✓ × 55.265.77.128 1	RESOLUTIONS (0) • Show: 25 • 1.6 of 6 • Resolve - 35.231.151.7 - 25.205.77.128	Sort : Last Seen Desce Location US	nding v Network Unknown	ASN	First 2018-10-04	Last 2018-12-12	Source kaspersky: pingly, riskiq		Сору
IP ⊗//0 ✓ × 0.0.0.0 1 ✓ × 149.154.157.171 1 ✓ × 209.99.40.223 1 ✓ × 35.205.77.128 1 ✓ × 35.205.77.128 1	RESOLUTIONS Ø • Show:25 • 16 ef 6 Becolve 35 231.151.7 25 205.77.128 201.99.40.223	Sort : Last Seen Desce Location US US	nding v Network Urknown 35.204.0.0/15	ASN 15169	First 2018-10-04 2018-10-04	Last 2018-12-12 2018-12-12	Source kaspersky, pingly, rokką kaspersky, pingly, rokką		Сору
IP (b) (b) IP (b) (b) (b) IP (b) (b) (b) (b) IP (b) (b) (b) (b) (b) IP (b) (b) (b) (b) (b) (b) IP (b) (b	RESOLUTIONS 0 - \$500x125 < 16.06 + 50000 - \$5231.151.7 - \$5205.77.128 - \$20.97.40.223 - \$6.6.0	Sort : Last Seen Desce Location US US US N/A	nding • Network Urknown 25.204.0.0/15 209.59.40.0/24	ASN 15169	First 2018-10-04 2018-10-04 2017-08-09	Lass 2018-12-12 2018-12-12 2017-09-19	Source Jaspersky, anky, roka Jaspersky, pryky, roka Raspersky, pryky, roka, unatorał Jaspersky, pryky, roka,		Сору
IP (cr.0) 1 v X 1.09.154,157.171 1 v X 209.99.40.223 1 v X 55.205.77.128 1 v X 35.205.77.128 1 v X 35.235.11.51.7 1	RESOLUTIONS Ø Image: Second Sec	Sort : Last Seen Desce Location US US US NVA US US	nding • Network Urkinown 205.204.02/15 209.99.40.0724 Urkinown 45.32.54.0719	ASN 15169 40094	First 2018-10-04 2018-10-04 2017-08-09 2016-09-22	Last 2018-12-12 2018-12-12 2017-09-19 2017-08-08 2016-09-16	dource kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig projly, vrvatstal	Tags	Сору
IP 6(x + 6) ✓ X 0.0 0.0 1 ✓ X 149,154,157,171 1 ✓ X 209,899,40 223 1 ✓ X 55,265,77,128 1 ✓ X 36,2231,151,77 1 H More X X NETWORK (s/x)4 X	RESOLUTIONS 0 - \$500x125 < 16.06 + 50000 - \$5231.151.7 - \$5205.77.128 - \$20.97.40.223 - \$6.6.0	Sort : Last Seen Desce Location US US US N/A	nding * Network Urknown 35.204.0.0/15 209.59.40.0/24 Urknown	ASN 15169 40034 63949	First 2018-10-04 2018-10-04 2017-08-09 2016-09-22 2016-09-14	Lass 2018-12-12 2018-12-12 2017-09-19 2017-08-08	Source Jaspersky, anky, roka Jaspersky, pryky, roka Raspersky, pryky, roka, unatorał Jaspersky, pryky, roka,		Copy
IP (6/4) ✓ X 0.0.0 1 ✓ X 0.0.9.9.4.0.23 1 ✓ X 0.0.9.9.4.0.23 1 ✓ X 0.0.9.9.4.0.23 1 ✓ X 0.0.9.9.4.0.15.1 1 DOD MORE IV IV IV NETWORK (#/4) IV X 20.0.99.40.024 1 ✓ X 0.0.94.00.024 1 I ✓ X 20.0.99.40.024 1 I	RESOLUTIONS Ø Image: Second Sec	Sort : Last Seen Desce Location US US US NVA US US	nding • Network Urkinown 205.204.02/15 209.99.40.0724 Urkinown 45.32.54.0719	ASN 15169 40034 63949	First 2018-10-04 2018-10-04 2017-08-09 2016-09-22 2016-09-14	Last 2018-12-12 2018-12-12 2017-09-19 2017-08-08 2016-09-16	dource kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig projly, vrvatstal	Tags	Copy
IP (6/4) ✓ X 0.0.0 1 ✓ X 0.0.9.9.4.0.23 1 ✓ X 0.0.9.9.4.0.23 1 ✓ X 0.0.9.9.4.0.23 1 ✓ X 0.0.9.9.4.0.15.1 1 DOD MORE IV IV IV NETWORK (#/4) IV X 20.0.99.40.024 1 ✓ X 0.0.94.00.024 1 I ✓ X 20.0.99.40.024 1 I	RESOLUTIONS 0 • \$909/23 • 1.626 • NOXON 5221151.7 52359.7128 0.00.0 • 423385.774 • 140.554.157.77	Sort : Last Seen Desce Location US US US NVA US US	nding • Network Urkinown 205.204.02/15 209.99.40.0724 Urkinown 45.32.54.0719	ASN 15169 40034 63949	First 2018-10-04 2018-10-04 2017-08-09 2016-09-22 2016-09-14	Last 2018-12-12 2018-12-12 2017-09-19 2017-08-08 2016-09-16	dource kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig projly, vrvatstal	Tags	Copy
IP (6/6) 1 V X 0.0.0 1 V X 10.0.0 1 V X 10.0.154 1 V X 20.0.99.40.223 1 V X 30.205.77.128 1 V X 30.203.151.7 1	RESOLUTIONS 0 • \$909/23 • 1.626 • NOXON 5221151.7 52359.7128 0.00.0 • 423385.774 • 140.554.157.77	Sort : Last Seen Desce Location US US US NVA US US	nding • Network Urkinown 205.204.02/15 209.99.40.0724 Urkinown 45.32.54.0719	ASN 15169 40034 63949	First 2018-10-04 2018-10-04 2017-08-09 2016-09-22 2016-09-14	Last 2018-12-12 2018-12-12 2017-09-19 2017-08-08 2016-09-16	dource kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig kespersky, projly, riskig projly, vrvatstal	Tags	Copy

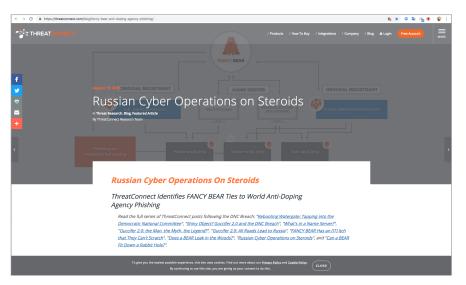
We can see the domain has be flagged as "Malicious," "Espionage," "Fancy Bear," and "Russia."

Review the open source intelligence tab (OSINT).

	da-arna.org			🗞 ★ 🗢 💐 🐾 🛞 😨 Tours Enterprise 😧
	jatur Galladdy.com, LLC	Espinnage O Fanghear O fussia 🔿 Categorize		
Last Seen 2018-12-12 Reg	periorit Dismans by Proxy, La			
	Sa M	Aug Sep Oct	2 2 2 2 2 2 2 2 Nov Dec	
		397 2014 2019-1	56-10 to 2010-12-12	
DATA	6 6 Resolutions WHC	0 6 0 5 2 10 E Certificate Subdomains Trackers Components Hest Pairs OSINT	5 15 5 0 Mashes DNS Projects Cookies	
	OSINT (9) Show: 25 + 1-10 of 10 + Sort: Last Seen Descr			Download Cos
✓ X blogsrendmic 1	Source	Link	Tags	cominate cop
✓ × cointelegraph 1	threatconnect.com	https://threatconnect.com/blog/fancy-bear-anti-dop	search-angine threatconnect	
✓ X documents.tre 1 ✓ X gdpr.report 1	www.weda-ama.org	http://www.wada-ama.org/en/media/news/2016-08/wad	🔦 search-engine 🛛 🔌 wada-arra	
✓ × info/arsightse 1 ow More	blog.trendmicro.com	https://blog.trendmicro.com/pawn-storm-power-socia	Searchiengine Strendmicro	
LINK (10/10)	info.farsightsecurity.com	https://info.farsightsecurity.com/hubfs/FSI%20-%20	• search-angles • famightancurit	7
✓ × https://blog.tr 1	www.theregister.co.uk	https://www.theregister.co.uk/2018/16/05/fancy_bea	search-engine Sco	
 × https://cointel 1 × https://docum 1 	gdpr.report	https://gdpr.report/news/2018/04/20/please-do-not	🗣 search-engine 🖉 gdpr	
✓ × https://gdpt.re 1	documents trendmicro.com	https://documents.trendmicro.com/assets/wp/wp-two	Search-angles Strandmicro	
✓ ※ https://info.far., 1 ow More	www.nytimes.com	https://www.nytimes.com/2018/10/04/sports/russia-c	• search-engine • nytimes	
TAG (10/20)	cointelegraph.com	https://cointelegraph.com/news/us-doj-charges-7-ru	search-engine Scointelegraph	1
✓ × search-engine 10 ✓ × trendmicro 2	www.dnevnik.bg	https://www.drievnik.bg/file/3322000.pdf	Search-engine Schervik	
v × co 1 v × cointelegraph 1 v × dnevnik 1	1-10 of 10			
5W More 0.0-38b7064 b 2018, RiskiQ Inc. All	Rights Reserved. Proprietary and confidential; do not distribut	e without prior approval. Privacy Policy Terms and Canditions		



Step 4: Click on the link from threatconnect.



https://threatconnect.com/blog/fancy-bear-anti-dop...

Objective 1: What have you determined about this email address?

Objective 2: Is there any threat actor associated with the email address?

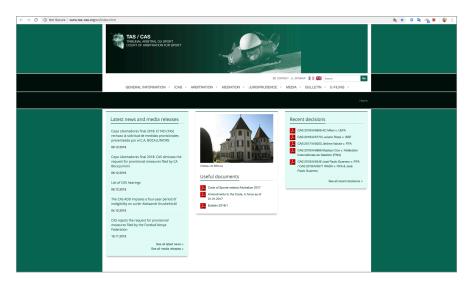
We have determined that macie.dietrich50@mail.com is associated with two seperate domains: wada-arna[.]org and tas-cass[.]org. Through your investigation of a single email address, macie.dietrich50@mail. com, you identified that it was related to wada-arna.org, a confirmed malicious domain. By examining the open source intelligence (OSINT) on this domain, you learned that the wada-arna.org domain was associated with Fancy Bear, a Russian threat actor who targeting the World Anti-Doping Agency Phishing Attack.

Wada-arna[.]org is a typosquatted domain for wada-ama.org, the world Anti-Doping Agency.

 C https://www.add-ama.org/w/weds/www.2016-00/wide-conferm-illegit-add/ AbMS Abit. Events 	WORLD ANTI-DOPING
WHO WE ARE	WHAT WE DO WHAT IS PROHIBITED RESOURCES SEARCH P
Horse / Newsroom / News / WADA o	erfinns likepi achity on Yuliya Sieganowi's ADMIS account
Nires Frequently Asked Questions Uxetful Links O	VAugust 2016 WADDA confirms illegal activity on Yuliya Stepanova's ADAMS account Anov her determined but a table account account
	The World And Daping Agency (MMAD) confirms that Twiley Brogenous's password for WADA's Andi Daping Administration and Management System (DASMM) confirms that Twiley Brogenous's password for WADA's Andi Dapamora well free involutional transformation for WADA's Internet and the account of the WADA's Andi Researce and the transformation for WADA's Internet Amora and the account of the WADA's Andi Researce and the transformation for WADA's Internet Amora and the account of the WADA's Andi Researce and the transformation for WADA's Internet Amora and the account of the transformation of the WADA's Andi Througe WADA's regular security monitoring of AdAMS, the Agency related that sametice.
	accessed for account, WAA immediately locked Ms. Stepanour's account to prevent further access and notified her of the situation. A subsequent investigation by WADA allowed the Agency to determine that no other athlete accounts on ADMAS have been accessed.
	Evire the served, WEAA was mode served on an Balged hack of the weak the works ben dup binding cancer. Regarding the bitter, the Agency confirmed that areas that an extended integrational e-main hand bala as the balan balan of the server to calcula as a list and enter the dire provide contentiation. WEAA (as LoSA) were baland as a list and enter the dire provide contentiation. WEAA (as LoSA) were baland as a list and enter the dire provide contentiation. WEAA (as LoSA) were baland as a list and enter the dire provide contentiation. WEAA (as LoSA) were baland as a list and enter the dire provide as a list and enter the dire provide contentiation. WEAA (as LoSA) were baland as a list and enter the dire provide the table have ABAC (as loss the dire provide the dire and LoSA). WEAA (as LoSA) were baland as a list and enter the dire provide the table have ABAC (as loss the tabl
	We continue monitoring the situation to determine whether or not users have actual call on these a-mails to ensure that data remains secure. Uninfulnetably, like many organizations, MRZA is not immune to attempted option attacks. Stakinitisters can ned assumed that the Agency Salar of Excurbly and data privacy way windows), accordingly, as a matter of course, we remains and and splans on

3

Tas-cass[.]org is a typosquatted domain for tas-cas.org, the Trubunal Arbitral Du Sport also called the Court of Arbitration for sports.



Objective 3: What have you discovered about this threat actor?

The United States District Court Western District of Pennsylvania issued an indictment for the Russian Federation Intelligence Directorate of General Staff (GRU) for this particular attack. You can read the indictment at the following URL: <u>https://www.justice.gov/opa/page/file/1098481/download</u>

Case 2.18-cr-00263-MRH Docume	nt 4 Filed 10/03/18 Page 1 of 41
UNITED STATES I WESTERN DISTRICT	
UNITED STATES OF AMERICA	
v.	Criminal No. 18-263
ALEKSEI SERGEYEVICH MORENETS EVGENII MIKHAYLOVICH SEREBRIAKOV IVAN SERGEYEVICH YERMAKOV ARTEM ANDREYEVICH MALYSHEV DMITRIY SERGEYEVICH BADIN OLEG MIKHAYLOVICH SOTNIKOV ALEXEY VALEREVICH MININ Defendants.	18 U.S.C. §§ 371, 1030(a)(2)(C), 1030(a)(5)(A) (Conspiracy) 18 U.S.C. § 1349 and § 3559(g)(1) (Conspiracy to Commit Wire Fraud) 18 U.S.C. § 1343 (Wire fraud) 18 U.S.C. § 1028A (Aggravated Identity Theft) 18 U.S.C. § 1956(h) (Conspiracy to Launder Money)
	[UNDER SEAL]
INDICT	MENT
COUNT (Conspi	
The grand jury charges:	
1. At all times relevant to the indictm	ent, from at least 2014 up to and including May
2018, the Russian Federation (Russia) operated	a military intelligence agency called the Main
Intelligence Directorate of the General Staff (GR	U). The GRU was headquartered in Moscow,
Russia, and was comprised of multiple units, inc	luding Units 26165 and 74455. Military Unit
26165, also known as the "GRU 85 Main S	Special Service Center," was located at 20
Komsomolskiy Prospekt, Moscow, Russia. Milita	ary Unit 74455 was located at 22 Kirova Street,
Khimki, Moscow, Russia.	
	FILED
	OCT 0 3 2018
1	CLERK U.S. DISTRICT COURT WEST. DIST. OF PENNSYLVANIA

Further information about the FancyBear threat actor group links them to the GRU at Bellingcat. You can read the report at the following url: https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skripal-suspectsconfirmed-gru-operatives-prior-european-operations-disclosed/

C A https://www.belingcat.com/news/uk-and-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior-europeratives-prior	ropean-operations-disclosed/ 🗞 🖈 🔍 🗣 🍖 🖲 🕼 🗄
Home Africa Americas MENA Podcasts Rest of World UK & Europe Article	s Case Studies Events Guides EN 🕶 💓 抗 Enter sourch term >
bellingcat	the home of online investigations
Skripal Suspects Confirmed as o Operatives: Prior European Operations Disclosed	<u>aru</u>
September 20. 2018 By Bellingest Investigation Translations: Process	
In the <u>precision war</u> of a joint investigation, Bellingcat and The Ins established that: • <i>Neurander Petror</i> - a fake cover persona for a yet unidentifie individual - to civiliar but linkeds to one of Rossia's and This assessment was based on an exhaustive analysis of Pe- pasagord robust - a obtained from the Rossian contral pasagord	IRossian thy services. rov' IROssian thy services. Row' IROssian IROssian thy services. Row' IROssian IROSSian IROSSian IROSSian IROSSIAN IRO
 Petrov and Boshirov made last-minute travel plans to fly to th Kingdom, which - coupled with the double-booking of return two consecutive dates - makes the "toursin" explanation im 	lights an and an and an
 Petrov and Boshirov travelled on international passports that 3 consecutive digits, making it implassible that they were ci- obtained their passports through the regular entropic passpo- application process available to Russian citizens. 	ilians who Enter your email address to receive a weekly digest of Bellingcat
	Support Bellingcat The can support the work of Bellingcat by denoting through the latent mice

Conclusion:

You might need to use open source intelligence to help in your investigations. In this particular case finding this email address on a compromised host means that you might be dealing with a nation state threat actor. It is important to fully investigate all avenues to fully understand the scope and nature of the attack.



RiskIQ, Inc.

22 Battery Street, 10th Floor San Francisco, CA. 94111

- Learn more at riskiq.com

Copyright © 2020 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies.01_20

- Sales@riskiq.net
- **L** 1888.415.4447