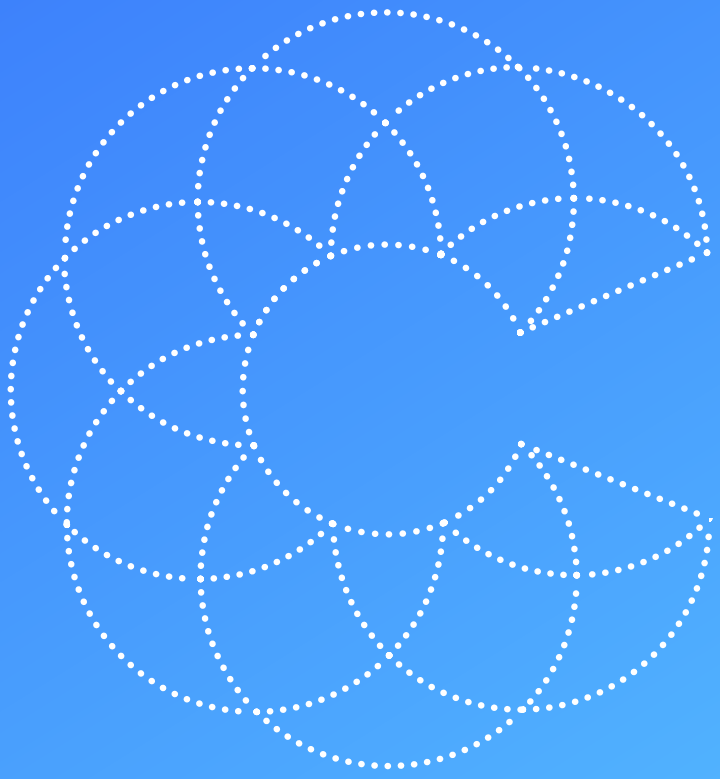
Coalition®

CYBER RISK, SOLVED®



EXAMPLE MEDICAL GROUP

Cyber Risk Assessment

Coalition's insurance products are offered with the financial security of Swiss Re Corporate Solutions and Argo Pro US (A+/A ratings by A.M. Best).

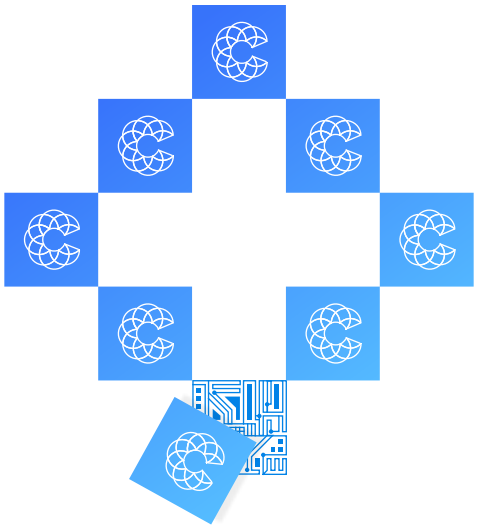
Swiss Re

ARGO GROUP

Coalition®

OVERVIEW

WE'RE A NEW KIND OF INSURANCE



Coalition was purpose-built at the intersection of technology and insurance to help companies manage cyber risk. This risk assessment is the first step in this continuous process. Using externally observable data, this report provides an objective, evidence-based assessment of your cyber risk and overall security preparedness. As your dedicated risk management partner, our security team is available to provide additional context and to help you to implement security and loss controls, all at no additional cost.

HELP@THECOALITION.COM
1-833-866-1337

Example Medical Group

Provided by Example Risks a division of XX, LLC

Current risk level: HIGH

Coalition's signals intelligence platform provides a snapshot of a company's current risk level by using public, external methods (no penetration or intrusive tactics) to:

- Scan infrastructure for publicly accessible servers, services, & technology
- Discover exploitable vulnerabilities & misconfigurations in the scanned infrastructure
- Find exposed available user/employee information
- Uncover other existing threats hidden on the dark web
- Discover proactive measures already taken by the company

This data, combined with Coalition's proprietary claims and loss data provides

- A relative measure of the company's defensive security posture compared to organizations scanned by Coalition
- A clear, fact-based assessment of potentially weak security areas, and steps to fix them
- Recommendations on how the company can further secure their infrastructure informed by actual losses experienced by Coalition policyholders

Vulnerabilities

CRITICAL	HIGH	MODERATE	LOW
1	36	0	1

Exposed Employee Information

USERNAMES & PASSWORDS	PERSONALLY IDENTIFYING INFORMATION (PII)
2	15

Proactive Measures

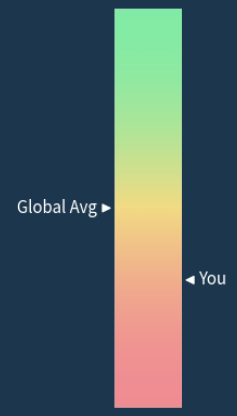
DISCOVERED	RECOMMENDATIONS
3	8

Technology Discovered

DOMAINS	DEVICES	APPLICATIONS	SERVICES
2	3	10	5

Current Ranking

You rank in the 32nd percentile of all Coalition policyholders.



Discovered vulnerabilities will not impact your coverage. However, resolving them may reduce your premium.

SECURITY PUNCH LIST

What is a CVE?
Common Vulnerabilities and Exposures (CVEs) are publicly published descriptions of known software vulnerabilities. They detail the software type and version, and information about the vulnerability.

As new vulnerabilities are discovered, new CVEs are published. Coalition continuously scans a company's infrastructure and will detect these new vulnerabilities as they are discovered.

You can find more about CVEs on our knowledge base.

Vulnerable Service (Database)

A publicly visible database was detected at the following addresses:

- exampledomain.com (MySQL)
- exampledomain.com (MySQL)

Recommendation:

- *It is best practice to remove all databases from public Internet accessibility, even when authentication is required for access. Criminals routinely scan the Internet for databases, and use brute force password attempts or compromised credentials (see below) as a means to gain unauthorized access to a company's data.*

2-Factor Authentication

Approximately 80% of email intrusion incidents happen because of weak or stolen passwords. One of the most effective methods to mitigate risk of an email-based cybersecurity incident is to enable 2-Factor (or Multi-Factor) Authentication.

While our external scans cannot discover if 2-Factor Authentication is enabled for your organization, Coalition highly recommends enabling it across your company -- especially for:

- Corporate email accounts
- Critical internal services
- Critical third-party services

Read more about 2-Factor authentication on our Knowledge Base.

High Severity Vulnerability

A high severity vulnerability, CVE-2019-6977, was detected on your systems.

This vulnerability has known, active exploits as reported by the National Vulnerability Database. Continued usage of this technology is likely to expose the company to a greater risk of criminal targeting. We recommend investigating this vulnerability and patching or upgrading all software.

Enable DMARC / E-mail Protection

Configure DMARC in minutes to prevent phishing attempts and spam. Properly configured DMARC/DKIM records can help ensure that only authorized systems can send email on the behalf of a company. There is no cost to implementing DMARC.

Enable SSL/TLS Encryption

The company should consider implementing SSL/TLS encryption on its websites, and forcing all traffic over HTTPS to protect information transmitted through the company's web application. The following domains were flagged by our system:

- exampledomain.com
- exampledomain.com

Free SSL certificates can be acquired from Let's Encrypt, or by using Cloudflare, one of Coalition's included security applications.

Actively Exploitable Vulnerability

An actively-exploitable, but not severe vulnerability, CVE-2017-16642, was detected on your systems.

This vulnerability has known, active exploits as reported by the National Vulnerability Database. These exploits are not severe, but continued usage of this technology is likely to expose the company to a greater risk of criminal targeting. We recommend investigating this vulnerability and patching or upgrading all software.

Premium discounts are offered to companies that use encryption.

EXPOSED EMPLOYEE INFORMATION

OVERVIEW

Coalition's signals intelligence platform collects information from past data breaches, hacker forums, and other dark web sources to determine whether an organization's data, including employee login credentials and other sensitive information, have been compromised in third party data breaches.

Often, spammers & hackers make up emails in an attempt to guess an employee's true information. Often these incorrect email addresses show up in breached lists, even though they are not real, and may show up in the lists below.

You can find more information about exposed information in our knowledge base.

EXPOSED USERNAMES & PASSWORDS

Most computer systems rely on passwords to prevent unauthorized access, and all the cybersecurity in the world won't help you if someone knows or guesses your password. Criminal actors frequently take advantage of the fact that many individuals reuse passwords, and use credentials compromised from prior data breaches in order to target e-mail, banking, and other corporate accounts. So-called "credential stuffing" attacks are a leading cause of data breaches. **The usernames and passwords here were exposed on third party sites, not from a security breach of Example Medical Group, directly.**

USER/ACCOUNT	LAST EXPOSED	PASSWORD EXPOSED	3RD PARTY BREACH
user1@examplemedical.com	2012-07-01	Yes	Dropbox
user2@examplemedical.com	2017-08-28	Yes	OnlinerSpambot

Total Exposed Usernames & Passwords: 2

EXPOSED PERSONALLY IDENTIFYING INFORMATION (PII)

PII is any kind of information that can be used to uniquely identify someone's identity. This sensitive information can be used by would-be hackers to impersonate employees to create more believable messages used in phishing attempts.

USER/ACCOUNT	LAST EXPOSED	DATA COMPROMISED	3RD PARTY BREACH
user3@examplemedical.com	2018-11-05	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles	Adapt
user4@examplemedical.com	2018-11-05	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Physical addresses, Salutations, Social media profiles	Adapt Apollo
user5@examplemedical.com	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles	Apollo

USER/ACCOUNT	LAST EXPOSED	DATA COMPROMISED	3RD PARTY BREACH
user6@examplemedical.com	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles	Apollo
user7@examplemedical.com	2018-11-05	Email addresses, Employers, Geographic locations, Job titles, Names, Passwords, Phone numbers, Physical addresses, Salutations, Social media profiles	Adapt Apollo Dropbox NetProspex
user8@examplemedical.com	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles	Apollo
user9@examplemedical.com	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles	Apollo
user10@examplemedical.com	2018-11-05	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles	Adapt
user11@examplemedical.com	2016-09-01	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses	NetProspex
user12@examplemedical.com	2018-11-05	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles	Adapt
user13@examplemedical.com	2016-09-01	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses	NetProspex
user14@examplemedical.com	2016-09-01	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses	NetProspex
user15@examplemedical.com	2016-09-01	Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses	NetProspex
user16@examplemedical.com	2017-08-28	Email addresses, Passwords	OnlinerSpambot

Total Exposed PII: 15

WHAT YOU CAN DO

Third party breaches of employee information will continue to happen on a regular basis. Be vigilant about the source of inbound emails, as email addresses that were involved in these types of third party breaches are at a greater risk of targeting in email phishing campaigns.

- Enable Two-Factor Authentication.
- Review your passwords for all services, and especially corporate services, bank accounts, and email accounts.
- Consider a password refresh for particularly sensitive corporate accounts, such as email.
- Use a password manager to generate unique passwords for all accounts.

Read more about https://blog.thecoalition.com/practical-security-passwords/.

RECOMMENDATIONS

Enable DDoS Mitigation

Distributed Denial of Service (DDoS) attacks attempt to disrupt a website's availability by overwhelming it with a flood of fake Internet traffic.

Coalition recommends enabling a DDoS mitigation service to reduce the likelihood of a business interruption to your website.

We offer one such service, Cloudflare, to all of our insureds at no additional cost. Cloudflare is a web performance and security tool that can be set up in under 4 minutes. Coalition policyholders that enable this, or a similar, service are eligible for an enhanced business interruption waiting period of only 1 hour.

Coalition offers an Enhanced Business Interruption Waiting Period of 1 hour by endorsement when a qualified DDoS mitigation solution is used.

Enroll in Security Awareness Training

Over 90% of security incidents are caused by human error -- often through social engineering or phishing. Implementing a comprehensive Security Awareness Training program and phishing simulations will help reduce the likelihood of these errors.

If you have not already done so, Coalition recommends starting a regularly recurring training program that includes phishing simulations.

Coalition has built a partnership with leading Security Awareness Training company Curricula.

Companies participating in a security awareness training program may be eligible for an additional premium discount.

Implement a Password Manager

Often, people will reuse the same password on multiple services, leading attackers to try "credential stuffing". Would-be hackers can find compromised credentials for a username and then try to reuse that leaked password on other websites & services -- including your corporate email.

A password manager allows individuals to remember a single password, and creates unique, secure passwords for each of the other sites or services that the person uses.

Implementing the use of a password manager company-wide will reduce the reuse of passwords and make it less likely for an attacker to successfully use an exposed password to gain access to your systems.

Implement Service-Based Anti-Phishing Software

90% of cyber attacks start with phishing emails sent to an employee. These phishing emails often look like legitimate emails from 3rd party companies, asking to "log in" to take one of many varying actions (update contact information, view account updates, etc). However, the intent is always the same -- to steal usernames and passwords.

Implementing service-based anti-phishing software can prevent these malicious emails from ever reaching their target. Coalition recommends implementing a service-based anti-phishing solution (such as Proofpoint, Mimecast, or Area 1 Security) to reduce the likelihood of your employees falling victim to a phishing attack.

Enable Registry Lock

When you purchase a domain name, your registrar passes along your registration information to the global registry, which serves as the authoritative source for domain resolution. If an attacker were to compromise your registrar account, they could point your domain to a nameserver under their control. The registry, believing that the updates came from an authorized source, would accept the changes without question.

The solution is registry lock: a special flag in the registry (not your registrar) that prevents anybody from making changes to your domain without out-of-band communication with the registry. Contact your registry to enable this feature.

Enable DNSSEC

DNSSEC eliminates the threat of DNS cache poisoning by authenticating all DNS queries with cryptographic signatures. Instead of blindly caching DNS records, DNS servers will reject unauthenticated responses. Combined with secure registrar practices, DNSSEC guarantees that those visiting your domain see your website and not the content on somebody else's web server. You can learn more about DNSSEC here.

Create a security vulnerability disclosure program

Discover critical security vulnerabilities before they can be criminally exploited. Coalition has partnered with HackerOne to provide a free security vulnerability disclosure program to all Coalition policyholders.

For more information, reference the HackerOne app available within the Coalition policyholder dashboard.

DISCOVERED PROACTIVE MEASURES

OVERVIEW

In addition to assessing an organization's cyber risk, Coalition also collects and analyzes protective actions and controls implemented by organizations to mitigate such risk. This information is used for the purposes of assessing an organization's ability to detect and mitigate risks, as well as for the purposes of applying insurance premium discounts. Below are several of the positive security measures we detected.

- SPF
- Office 365 Mail
- HTTPS

APPENDIX: TECHNOLOGY DISCOVERED

Domains

The following domains were detected and enumerated during our security scan.

ANALYSIS

No known issues detected.

example1.com

- www.example1.com

example2.com

- remote.example2.com
- www.example2.com

Devices

The following devices were detected and enumerated during our security scan.

ANALYSIS

No known issues detected.

IP ADDRESS	PORTS	TYPE
100.200.30.400	22, 80, 110, 143, 443, 465, 587, 993, 995, 2082, 2083, 2086, 2087, 3306	Database, Webserver
101.201.31.401	21, 22, 80, 110, 143, 443, 465, 587, 993, 995, 2082, 2083, 2086, 2087, 2095, 3306	Database, Fileserver, Webserver
50.60.70.80	443, 500, 1723	Webserver

Applications

The following technologies and applications were detected and enumerated during our security scan.

- PHP 5.4.45
- Apache
- IIS 10.0
- HTTPS
- LinuxSPF
- Exim 4.92
- WordPress 4.9
- WordPress 5.0

Services

The following services were detected and enumerated during our security scan.

ANALYSIS

No known issues detected.

- GoDaddy DNS
- GoDaddy Hosting
- Microsoft Azure DNS
- Microsoft Exchange Online
- Office 365 Mail

APPENDIX: ALL DETECTED VULNERABILITIES

Severity:

CRITICAL	HIGH	MODERATE	LOW
1	36	0	1

Actively exploitable vulnerabilities discovered.

OVERVIEW

Coalition's signals intelligence platform passively enumerates the devices, technologies, and services used by an organization, and cross-references this information with a proprietary database of software vulnerabilities and versioning information, including comparison against the National Vulnerability Database, a U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).

SIGNIFICANCE

The use of outdated, vulnerable software is a leading cause of data breaches and cyber incidents. Criminal actors scan the Internet for such software, as we do on behalf of our policyholders, and use this information to target and breach an organization's computer systems. However, just because software is vulnerable does not mean that it poses a significant risk to an organization. Our data suggests that fewer than 2% of vulnerabilities are actively exploited by criminals. Our tracking of criminal exploits allows us to more accurately assess risk, and to work with our policyholders to most effectively remediate security issues.

WHAT YOU CAN DO

Coalition continuously monitors for software vulnerabilities, with particular attention to vulnerabilities with active exploits, as well as software upgrade availability to in order help our insureds get ahead of potential threats to their organization. Upon receiving an alert, Coalition's dedicated security team is available to assist with remediation efforts.

LIST OF TECHNICAL VULNERABILITIES

TECHNOLOGY	VERSION	SEEN ON	VULNERABILITIES	ACTIVE EXPLOITS?
PHP	5.4.45	www.example1.com	CVE-2016-7478	No
		www.example2.com	CVE-2015-8994	
Various			CVE-2019-6977	Yes
			CVE-2019-9641	
			CVE-2019-9639	
			CVE-2019-9638	
			CVE-2019-9637	
			CVE-2019-9024	
			CVE-2019-9023	

TECHNOLOGY	VERSION	SEEN ON	VULNERABILITIES	ACTIVE EXPLOITS?
			CVE-2019-9021	
			CVE-2019-9020	
			CVE-2018-20783	
			CVE-2018-19520	
			CVE-2018-15132	
			CVE-2018-10549	
			CVE-2016-0777	
			CVE-2014-1692	
			CVE-2010-4478	
			CVE-2017-16642	
			CVE-2018-19935	
			CVE-2018-19396	
			CVE-2018-19395	
			CVE-2018-17082	
			CVE-2018-14883	
			CVE-2018-10548	
			CVE-2018-10547	
			CVE-2018-10546	
			CVE-2018-10545	
			CVE-2017-15906	
			CVE-2016-10708	
			CVE-2014-9767	
			CVE-2012-0814	
			CVE-2011-5000	
			CVE-2011-4327	
			CVE-2010-5107	
			CVE-2010-4755	

FAQ

WHO IS COALITION?

Coalition is a leading provider of Cyber and Technology Errors & Omissions insurance. We provide comprehensive insurance coverage and free cybersecurity tools to help businesses manage and mitigate cyber risk. Backed by A+/A rated insurers Swiss Re Corporate Solutions and Argo Group, Coalition provides companies with up to $10M of cyber and technology insurance coverage in all 50 states and the District of Columbia. Coalition's cyber risk management platform provides automated security alerts, threat intelligence, expert guidance, and tools to help businesses remain resilient in the face of cyber attacks. Coalition is headquartered in San Francisco. For more information about Coalition, visit www.thecoalition.com.

HOW DO YOU DETERMINE THE SECURITY RANKING?

Our security ranking provides a relative measure of an organization's risk and security posture as compared to the universe of Coalition policyholders. In order to determine the ranking of a company, we correlate identified risk conditions with Coalition's proprietary loss and claims data as a provider of insurance to thousands of organizations. Unlike traditional security ratings that make arbitrary assumptions on the relative impact of an identified risk condition to generate a security score, Coalition uses actual loss and claims data to identify the most significant risks to an organization. The result is not only a more accurate assessment of risk, but actionable prescriptions to help an organization invest its resources against the most impactful remediation actions.

WHERE DOES THE UNDERLYING DATA FOR COALITION'S RISK ASSESSMENT COME FROM?

Coalition passively collects external data on an organization's Internet facing IT infrastructure, compromised system events, file sharing events, and configurations from many different sources. Coalition does not perform active collection of information, including penetration testing against an organization's networks, without the explicit permission of that organization.

HOW CAN I LEARN MORE?

To learn more about Coalition, visit www.thecoalition.com, or our knowledge base at help.thecoalition.com. As a dedicated risk management partner to our policyholders, Coalition's team of security and insurance experts are dedicated to helping you implement security and loss controls, all at no additional cost.

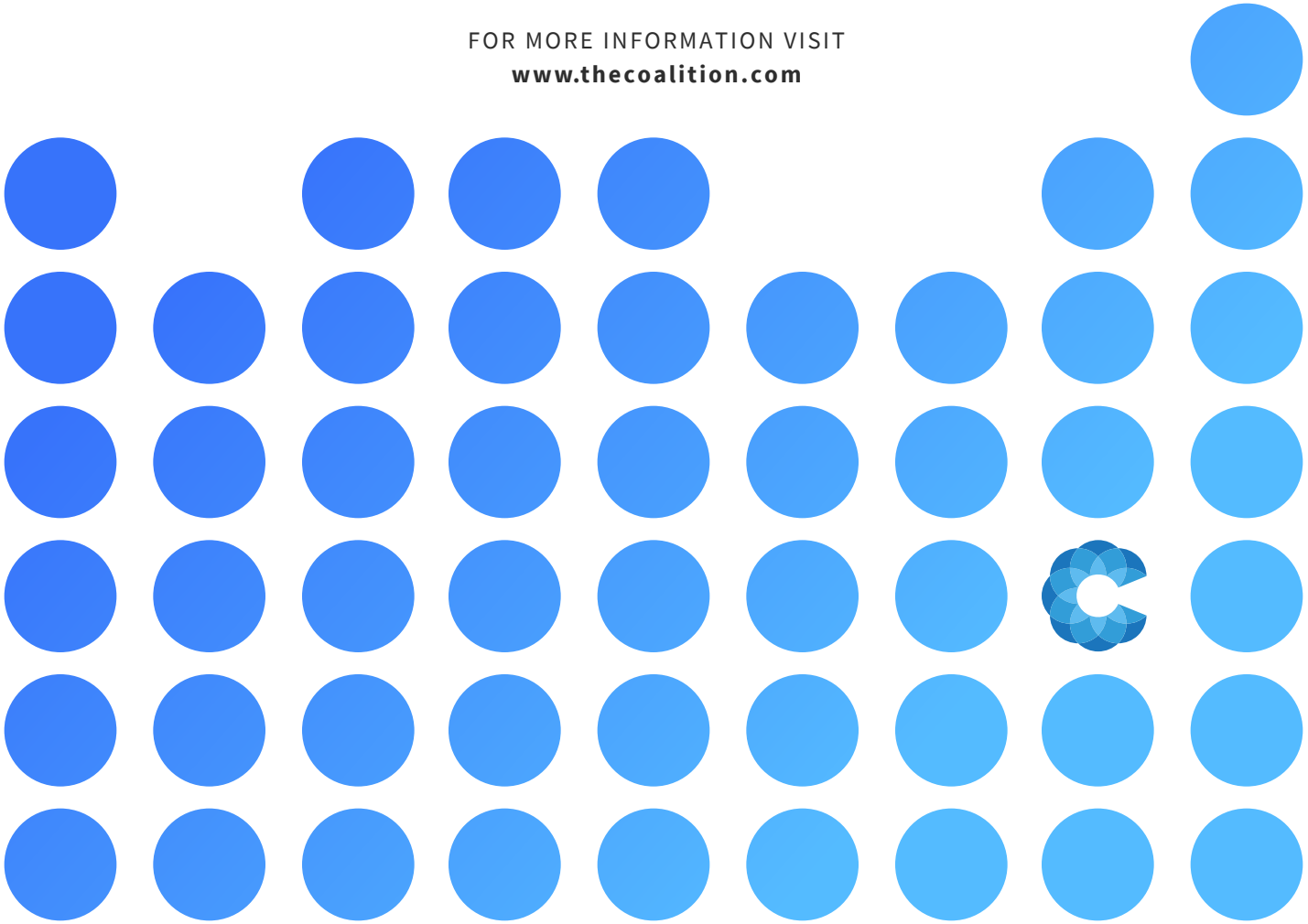
Coalition®

CYBER RISK, SOLVED®

This report was prepared by:

COALITION, INC.
1160 BATTERY STREET, SUITE 350 SAN
FRANCISCO, CA 94111

FOR MORE INFORMATION VISIT
www.thecoalition.com



Coalition's insurance products are offered with the financial security of Swiss Re Corporate Solutions and Argo Pro US (A+/A ratings by A.M. Best).

Swiss Re

ARGO GROUP