FREQUENTLY ASKED QUESTIONS

Active Insurance scans & recommendations

SCANNING

What type of scanning does Coalition perform?
Coalition's **Active Risk Platform** enables us to help organisations spot and mitigate cyber risk before it strikes. Our scanning technology is able to create an incredibly accurate picture of an organisation's digital risk. We scan the public web, use signal intelligence from sources including the dark web and combine this with our claims data. Our risk analysis includes but not limited to:

- **Digital risk data:** Public web scanning, tech stack enumeration, and in-depth threat intelligence.
- **Organisational risk data:** Financial health, litigation, M&A, HR compliance, and other firmographic data.
- **Incident and claims data:** Proprietary collection of risk and claims data.

We then apply our own expert analysis combining artificial intelligence and data science to develop insights and identify emerging threats. This enables us to train our models to make faster, better decisions that optimise brokers' quoting and binding processes while actively monitoring policyholders.

Since digital risk is complex, the Active Risk Platform runs three primary types of scans to identify cyber risks:

1. **Coalition Risk Assessment (CRA) —** This is a PDF report of your organisation's cyber risk profile and is typically compiled when you apply or renew your Coalition insurance. It includes internet-facing systems — like website domains and servers. We scan your primary domain and subdomains to gain a better understanding of your externally facing exposures.

2. **Attack Surface Monitor (ASM) —** Your attack surface is anything that's internet-facing that attackers can find and try to exploit. While the resulting data is similar to the CRA, ASM provides access to expanded functions — like richer data, interactive drill-down, and the ability to scan business partners and vendors. Here's how it works:

   - ASM starts by identifying assets including domains and IP addresses, like www.coalitioninc.com and 104.25.148.78.
   - Identified assets are scanned for common web-facing services or applications such as Microsoft RDP, Google Workspace, and web servers (e.g., IIS and nginx). Assets with insecure configurations, outdated software, or other vulnerabilities generate an alert automatically.

3. **Threat and Vulnerability Hunting —** As the most interesting and complex scan type, our threat and vulnerability hunting scans involve a mix of automated and manual technologies designed to find risks that could impact policyholders. These include but not limited to:

   Third-party data breaches. When third parties suffer a data breach, your data may be exposed — especially if users signed up using their work email addresses. We use dark web monitoring tools searching the compromised data to identify email addresses, domain names, and IP addresses belonging to our policyholders.

   Vendor vulnerability notices. When a vendor publishes a security notice, we immediately scan to identify any impacted policyholders and alert them. For example, a security tool provider recently identified an exploit of their product, and we notified all policyholders who used that product within 24 hours.

   Threat hunting. This includes dark web monitoring and advanced security analysis, such as monitoring traffic to known command-and-control hosts where malware receives its instructions. The Coalition data platform identifies policyholder assets communicating with these hosts, which indicates an active malware infection.

Coalition's scans are performed using an outside-in approach — the same perspective a hacker would have. Our data platform doesn't perform invasive testing. (That said, we're happy to recommend trusted partners who can help if you're interested!)

Insurance cover is issued by Coalition Insurance Solutions Pty Ltd ("CIS AU") (ABN 33 657 140 791, AFSL 539846) under a binding authority given by the insurer, Allianz Australia Insurance Limited (ABN 15 000 122 850, AFSL 234708). This information is of a general nature only and does not take into account any person's particular circumstances. All descriptions of coverage are subject to the terms, conditions, and exclusions of the individual policy. Before making a decision (or advising your client), please refer to the relevant policy wording available here or by contacting your broker. CIS AU may receive compensation from an insurer or other intermediary in connection with the sale of insurance cover. See disclaimers. Copyright © 2024. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.

What is Active Insurance?

Active Insurance is an innovative approach to cybersecurity designed to identify and mitigate risks before they strike. Encompassing three pillars — Active Risk Assessment, Active Protection, and Active Response — Coalition's Active Insurance offering is uniquely designed to empower organisations to protect their systems from digital threats and respond to an incident if needed.

The Coalition data platform uses machine learning, artificial intelligence, and in-house tech expertise to accurately analyse your company's risk with speed and precision.

When does Coalition scan and send alerts?

Every alert includes recommendations and instructions to deal with the issue at hand. Different scans are run at different times:

- **Coalition Risk Assessment (CRAs)** are run annually when you initially sign up for Coalition cyber insurance and at renewal. Note: You can download an updated CRA at any time during your policy period from your policyholder dashboard. You will receive the CRA via email when you apply for coverage and renew your policy.
- **ASM scans** run approximately every two weeks, and the data in your ASM dashboard is updated as soon as a new scan result is available. You can subscribe to automated email alerts to receive notifications when new scans become available.
- **Threat and Vulnerability Hunting** is done continuously. You'll receive an alert from Coalition any time our data platform identifies an issue.

FINDINGS

What kind of support is available to understand or implement findings?

- Since many of these alerts are often highly technical, we're always happy to connect you with Coalition cybersecurity expert support via email or Security Office Hours.
- If you have questions about your CRA, you may ask your broker to help since they'll have access to additional information and context!

What happens if Coalition finds an issue that I don't agree is an issue?

There are two main scenarios that could cause a disconnect on a scan result, and different outcomes are possible. These include:

- **False positive**. Mistakes happen, and we're always willing to review and ensure the findings are valid. Automated scans may not capture important context like multifactor authentication being turned on for an otherwise-insecure service.
- **Risk tolerance**. Different organisations have different risk appetites. For example, a healthcare provider dealing with regulated data will be much more risk-averse than a technology startup with less sensitive data.
    - Ultimately, both the policyholder and Coalition have to assess their risk thresholds, which may include a decision around higher insurance premium or retention, declination, or nonrenewal of coverage.

Am I obligated to act on a finding Coalition reports to me?

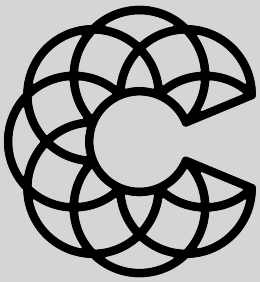
While these alerts will not lead to any changes to coverage or premium during the policy term, an insured's failure to address critical vulnerabilities identified during the policy term may impact their ability to renew their cyber coverage with Coalition. Security notifications are aimed at keeping our policyholder's aware of potential digital threats, and Coalition staff are always available to assist in quickly addressing identified risks.

If I don't act — are there costs and other penalties?

There are no changes to premiums or coverage during the policy term. All security alerts are intended to bring awareness and provide guidance on minimising risk exposures. As your cyber risk management partner, we offer help and guidance to address any findings that show up in our security alerts. Our ultimate goal is to help you reduce the likelihood your business experiences a cyber attack or disruption.

Keep in mind that typically your organisation's cyber insurance premium is a reflection of its cyber risk. Vulnerabilities detected can potentially lead to an insurance claim, and these unaddressed exposures may be reflected in your premium.

Insurance cover is issued by Coalition Insurance Solutions Pty Ltd ("CIS AU") (ABN 33 657 140 791, AFSL 539846) under a binding authority given by the insurer, Allianz Australia Insurance Limited (ABN 15 000 122 850, AFSL 234708). This information is of a general nature only and does not take into account any person's particular circumstances. All descriptions of coverage are subject to the terms, conditions, and exclusions of the individual policy. Before making a decision (or advising your client), please refer to the relevant policy wording available here or by contacting your broker. CIS AU may receive compensation from an insurer or other intermediary in connection with the sale of insurance cover. See disclaimers. Copyright © 2024. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.



Coalition®

COALITIONINC.COM

COALITION INSURANCE SOLUTIONS, INC.

44 MONTGOMERY STREET, SUITE 4210, SAN FRANCISCO, CA 94104

HELP@COALITIONINC.COM

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. (“CIS”), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company (“CIC”) a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.

Incident response services provided through Coalition’s affiliate Coalition Incident Response (CIR) are offered to policyholders via panel selection.

Copyright © 2024. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.