CHUBB®

# Stay Ahead of Cyber Threats

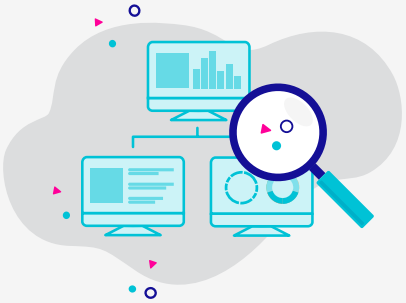
When you choose Chubb for your cyber insurance, you automatically gain access to our essential Vulnerability Management Outreach Program **at no extra cost**.

Think of our Vulnerability Management Outreach Program as a smoke alarm for your network. Just like a smoke alarm alerts you to fire risks before they escalate, our outreach program continuously monitors and scans for known exploited vulnerabilities that are leading to cyber claims.

If we detect a potential threat, we promptly notify you and your broker providing guidance on how to remediate before it spreads through your environment and becomes a serious problem. This support helps you address potential threats early, helping protect your business and giving you peace of mind.

## How It Works

1



**Monitoring**

2

**Alerting**

3

**Remediating**

## Extinguishing the Threat: Our Response to Vulnerabilities

Our policyholders are alerted through two methods.

**Outreach Program:** If a “fire” (an exploited vulnerability) is detected to be on your network, we initially notify you and your broker by email. This email details the exposure and actions required to remediate. Follow-ups are then conducted via email and phone.

**Breaking Alerts:** When new vulnerabilities with a high probability of exploitation are discovered, that may impact your environment, we notify you and your broker via email.

CHUBB®

# FAQs

### What is the purpose of Chubb Vulnerability Outreach program?

The purpose is to notify organizations of their exposure to exploited vulnerabilities and other severe misconfigurations (open ports, malware infections, etc.). Chubb has adopted this approach in order to alert and assist policyholders in identifying and remediating internet-facing issues our threat intelligence team has classified as high-risk exposure due to cyber claims activity. As such, each of the vulnerabilities we identify can and will be identified by threat actors and is identified as highly exploitable in the wild.

### Why is Chubb alerting me to vulnerabilities in my environment?

This is an important part of the symbiotic relationship between Chubb and our policyholders. We have been providing risk engineering services to our policyholders throughout the world for over one hundred years, which makes our policyholders better managers of risk. Cyber is no different. As we identify vulnerabilities that we can see in our policyholders' environment, which may be exploited by threat actors or are on high-risk cyber intelligence lists, we help our clients reduce exposure to those vulnerabilities.

### Do these alerts have any impact on coverage?

No. However, an unwillingness to take action to remediate these prioritized vulnerabilities may have an impact on the underwriting of your policy in the future. For example, if we continuously see these vulnerabilities and no response or action from a policyholder, we may consider not renewing coverage.

### Is this a Penetration Test?

This is not a penetration test. There is no active scanning or attempts at infiltrating your environment. This process utilizes external passive scanning platforms which utilize a combination of open-source intelligence (OSINT) and passive scanning. Passive scanning is non-intrusive and a safe methodology to identify internet-facing assets and any potential vulnerabilities or misconfigurations associated with them.

*This information is pertinent to the US and Canada. For information regarding other regions, please contact your Chubb Underwriter, as other regions may have different regulatory requirements under GDPR and other local regulations.

### Why am I getting this?

You are receiving this alert as a complementary service with your Chubb Cyber Policy. It relates either to a known exploited vulnerability (KEV) or any other severe cybersecurity finding that was detected via non-intrusive external scanning tools such as BitSight and Security Scorecard. The alert includes information that your IT team can use to identify and remediate the exposed asset.

### What if I don't understand these alerts?

The Cyber Threat Intelligence Team at Chubb is happy to discuss this process and the alert details with anyone in your organization. You may also forward it on to your internal information security professional or a third-party MSP who oversees your environment for any clarifications and/or insights.

### I don't know what this is or what to do about it, can you help?

Yes, please **click here** to schedule a complimentary consultation call with Chubb's Cyber Risk Advisory team.

### This isn't my IP address. Is any action needed?

Please forward the alert to **Cyber@Chubb.com** noting the specific misattributed IP addresses and we will update our records indicating they relate to a non-insured asset. If interested, the Chubb Cyber Risk Advisory team can provide instructions for your IT team to submit an inquiry for these findings via Bitsight or Security Scorecard to prevent future automated alerts pertaining to these misattributed IPs.

### This is not my domain.

Please reach out to **Cyber@Chubb.com** with confirmation of the correct domain and Chubb will ensure your policy is updated to reflect it. We will then update our records to show that the vulnerability relates to a non-insured asset and close the related case.

### Does Chubb have any other vulnerability management services available?

Yes, we have a suite of complimentary and discounted vulnerability management solutions available to help prevent emerging threats against your organization. You can learn more on all our cyber loss mitigation services at our **website** or by scheduling a consultation with one of our **Cyber Risk Advisors**.

Chubb. Insured.℠