cowbell®

Cowbell Insights:

Continuous Risk Awareness

The Leading Cyber Insurance Provider for SMEs | cowbell.insure

V.Mar23

What are Cowbell Insights

Cowbell Insights are recommendations we provide to help you remediate cybersecurity weaknesses and improve your organization's risk profile. They are accessible to policyholders and non-policyholders alike.

The insights are generated from our continuous risk assessment process and add details behind the Cowbell Factors™, our proprietary risk ratings. While Cowbell Factors provide a relative rating against our risk pool, Cowbell Insights are unique to your organization.

Like Cowbell Factors, Cowbell Insights are updated continuously. We recommend that your security and IT staff visit the Cowbell platform frequently to review your company's Cowbell Factors and Cowbell Insights.

How to Use Cowbell Insights

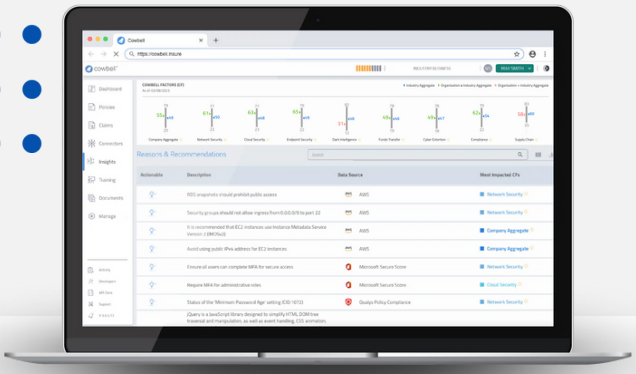
Each insight shows the level of security priority (High, Medium, Low), the impacted Cowbell Factor(s), and what to do to remediate the identified security weakness.

As you are addressing the insights and taking steps to remediate their impact, the insights will be removed from the list of identified cyber risks. Furthermore, Cowbell Factors will be recalculated to reflect the cyber risk improvement.

The Leader in Cyber Insurance for SMEs

Cowbell makes cyber insurance accessible to all and strengthens insureds' cyber resilience. Our policies come bundled with extensive risk management resources so that businesses reduce their exposure and avoid incidents.

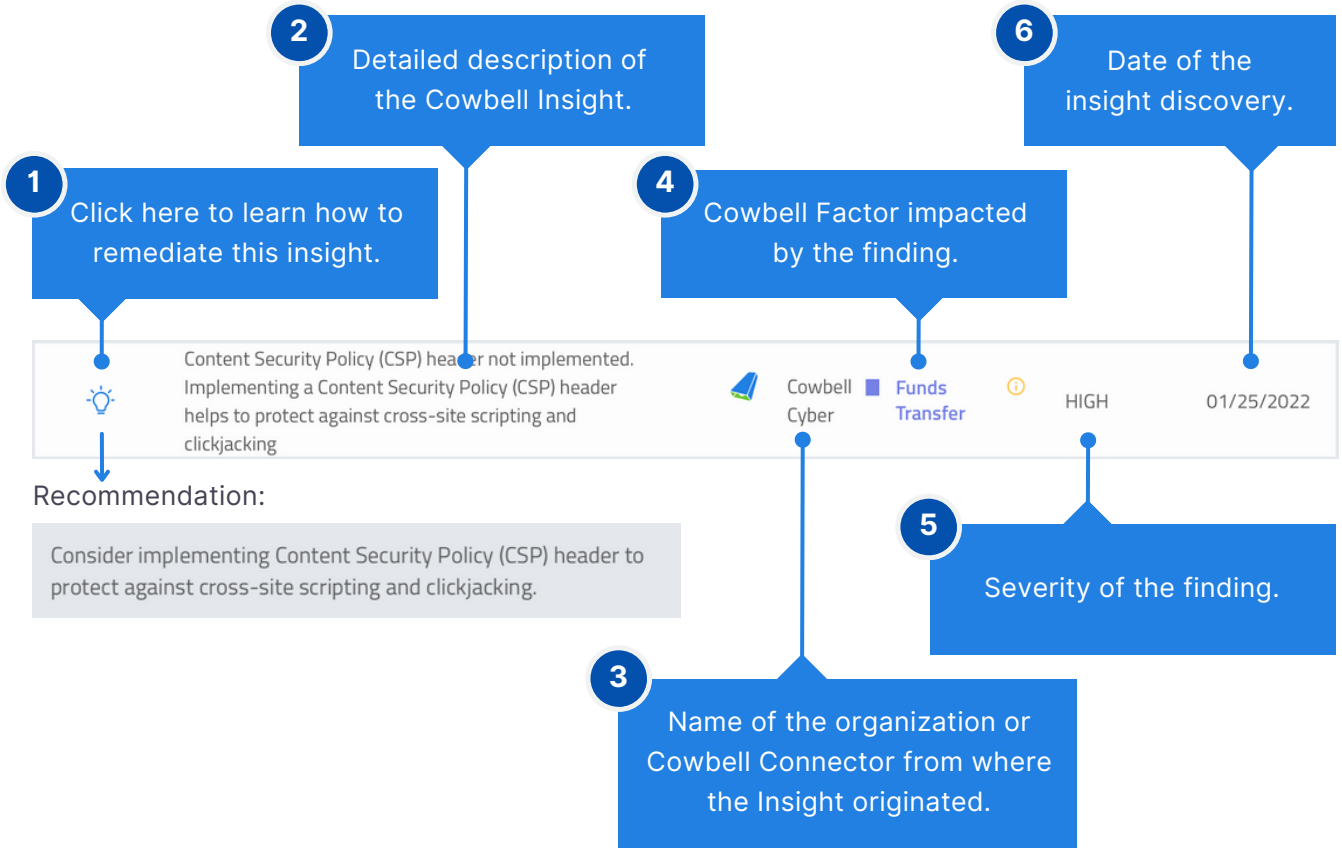
Example of Cowbell Insights



Your Cowbell Insights can be easily found when clicking on the "Insights" tab on the menu.

Breaking down the Cowbell Insights Menu

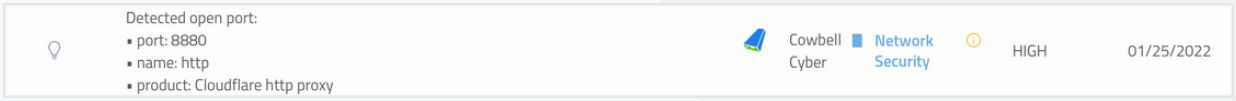
Every insight consists of six elements:



cowbell®

Commonly Reported Cowbell Insights

Example 1: Use of Remote Desktop Protocol (RDP) | Severity: High



Explanation:
RDP is a component of Microsoft Windows that is used for remote maintenance of devices. It is commonly used by IT staff to remotely maintain employee desktops or by third parties to remotely maintain equipment. RDP is a common vector for ransomware attacks, and RDP communications need to have adequate protection.

Most Impacted Cowbell Factor: Network Security

Remediation:

- Disable RDP services if you don't need them.
- Secure port 3389: add a firewall rule to only allow access from known IP addresses.
- Only allow access to port 3389 via a virtual private network (VPN).

Cowbell Insights answer the following questions:

- Which cyber risks are potentially impacting my organization?
- Which Cowbell Factors are impacted by the findings?
- How can I remediate the discovered security weakness?

Derived from up-to-date data

All Cowbell Insights are derived from Cowbell's proprietary risk rating Factors (Cowbell Factors). That means that the data is always current and relevant to your business.

Example 2: Multi-factor Authentication (MFA) | Severity: High

Explanation:
When the Cowbell Connector for Microsoft is activated, Cowbell gains visibility into the security configuration of your Microsoft environment (Office 365 and other Microsoft collaboration tools, Microsoft Azure).

Cowbell Insights, as shown in the above screenshot, indicate that MFA is not yet implemented for Microsoft's Administrator roles.

MFA is an authentication method that requires a user to provide two or more identity authentication factors to gain access to a resource - in this case, your Microsoft Administrator account. This decreases the likelihood of a successful cyber attack.

Most Impacted Cowbell Factor: Cloud Security (via Microsoft Secure Score Connector).

Remediation: Enable MFA on your Microsoft Administrator account.

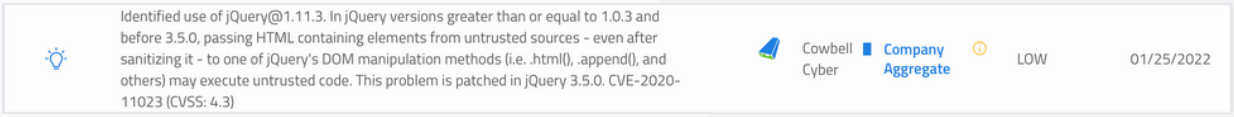
Example 3: Information Only | Severity: None

Explanation:
As we scan and gather Information about your publicly facing Internet presence, we present information that is useful to IT and security personnel but that does not immediately impact your Cowbell Factors.

Most Impacted Cowbell Factor: None (for Information purposes only).

Remediation: No remediation required.

Example 4: End of Life Software / Software Patching | Severity: Low



Explanation:
As vulnerabilities are made public, software vendors issue updates to their products in order to nullify the threats. Unpatched systems (outdated software) can mean easy access for bad actors. You can reduce your organization's cyber risk exposures by ensuring all of your system software is updated to the most current version.

Most Impacted Cowbell Factor: Company Aggregate - your organization's overall risk rating compared to others in your Industry.

Remediation:

- Create an Inventory of your software systems and their current version number.
- Check with your software vendors and compare your current software versions to those currently being published.

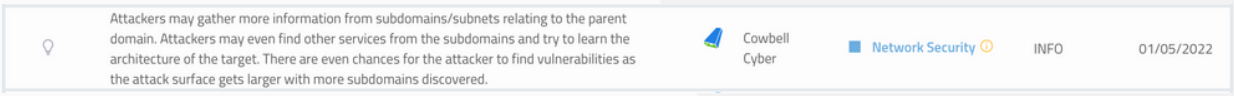
Need more help?

You can contact Cowbell's risk engineering team at https://cowbell.insure/contact-risk-engineering/.

More than Insurance

Every policyholder and non-policyholder can access our platform and benefit from Cowbell Factors and Cowbell Insights.

Example 5: Domain Name System (DNS) Configuration | Severity: None



Explanation:
The (DNS) is the protocol that makes the internet usable by allowing the use of domain names and routing communications to the correct address. There are many known cyberattack vectors based on improperly configured DNS settings. If your DNS is not properly configured, cybercriminals may gain insights into your network topology, presenting opportunities to launch a cyberattack.

Most Impacted Cowbell Factor: Network Security

Remediation: Ensure that your organization's DNS records are properly configured and secured.

Cowbell Insights provide valuable information for you to improve your organization's risk profile. Fixing identified security weaknesses can mean the difference between a successful and unsuccessful cyberattack and will improve your insurability.

For cybersecurity, a simple rule often holds true: You don't need to be perfect, you just need to be better than your neighbor.

By implementing the suggestions from Cowbell Insights, you automatically become a less attractive target for cybercriminals.

Real-time Recommendations

Cowbell Insights are continuously generated recommendations provided by Cowbell to help businesses improve their cyber risk profile.