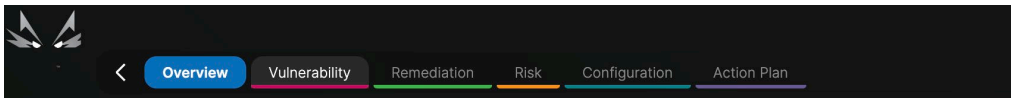
How To Guide – Interpreting Scan Results

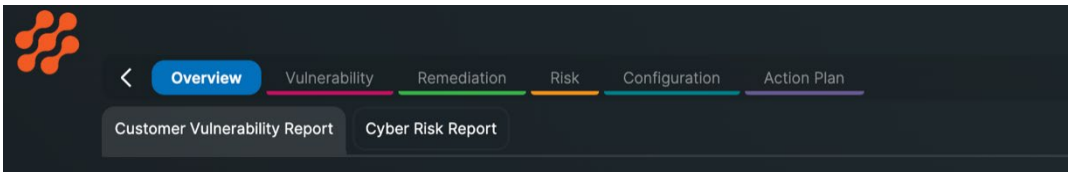
This guide aims to assist you in interpreting the Insight scan results. This tutorial assumes that you already managed to successfully run your first Insight scans.

1. Access the *reports* menu. The menu is accessible from the options displayed on the left side of the screen.

2. Display the scan results using any of the *Overview, Vulnerability*, or *Risk* color-coded tabs from the reports menu. Read below to understand what each tab contains related to interpreting the scan results.



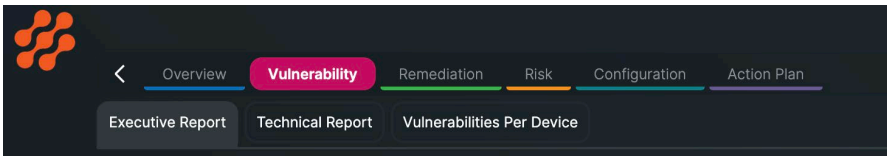
a. *Overview.* This will be displayed first when accessing the *reports* menu. It contains the *Customer Vulnerability Report* and *Cyber Risk Report* sub-tabs.



   i. *Customer Vulnerability Report.* This report is generated a few times a day and contains the combined results of the Agent-Base and Agentless scans. It is suited for keeping an overview of the whole vulnerability management process.

   ii. *Cyber Risk Report.* This report can be generated as a summary or as a full report. It is suited for presenting the scan results to stakeholders.

b. *Vulnerability*. It contains the *Executive Report*, the *Technical Report*, and *Vulnerabilities Per Device* sub-tabs.



i. *Executive Report.* This report presents a real-time overview of the active vulnerabilities. It is suited for keeping an eye on current cybernetic threats.

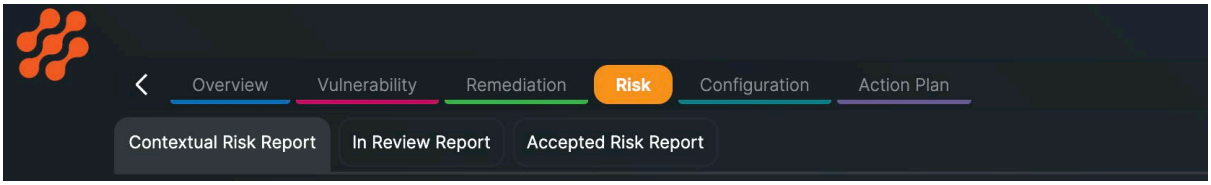
ii. *Technical Report.* This report contains a list of each vulnerability identified through the scan. It is suited for analyzing specific vulnerabilities from a technical point of view.

iii. *Vulnerabilities Per Device.* This report contains a list of vulnerabilities by scanned element (or device). It is also suited for analyzing vulnerabilities from a technical point of view.

You can see past reports and filter out vulnerabilities with rather low criticality in the Technical Report and Vulnerability Per Device.

c. *Risk.* It contains *Contextual Risk Report* sub-tabs.

The Risk tab also contains other sub-tabs that will be used during the vulnerability remediation process.



i. *Contextual Risk Report.* This report contains a list of the riskiest vulnerabilities identified through the scan. It is suited for analyzing vulnerabilities from a prioritization point of view.

The Contextual Risk Report uses the Contextual Risk Scoring System (CRSS) score to identify the riskiest vulnerabilities.

3. Interpret the results from the chosen report using statistics, visualizations, and written explanations. Some key terms to remember:

a. CVE – Common Vulnerabilities and Exposures. This is the name of the list containing known software weaknesses/mistakes. Followed by a number, it identifies a specific vulnerability or exposure.
b. CVSS – Common Vulnerability Scoring System. This is an internationally acknowledged risk score given to a vulnerability or exposure. It ranges from 0.0 to 10.0 and illustrates the severity of a CVE.
c. CRSS – Contextual Risk Scoring System. This is a proprietary risk score that includes both the CVSS and other context-specific information. It illustrates the contextual severity of a CVE.