

[Help page](#)

[About Us page](#)

About Command Center ASPM

Introducing our Application Security Posture Management Platform built to eliminate the complexity and cost of application security by leveraging AI/ML to identify and eliminate threats, reduce cost, expand security and enforce compliance.

Our story

Command Center Inc. was founded in 2023 by Michael E. Sheppard “Shepp” (CEO) with the goal to transform how organizations approached application security. While working for five organizations he discerned a pain point pervasive across sectors—a bottleneck in application security complexity and cost that could not scale quickly enough to meet burgeoning security demands nor sustain financially.

He set out to solve this problem by building an AI-driven Application Security Posture Management solution that utilizes advanced algorithms to eliminate the complexity and cost of application security.

Command Center ASPM isn't just an Application Security Posture Management platform; it's your application security program. As a pioneer in application security posture management solutions, we offer seamless onboarding and integration to all your critical cybersecurity tools that's easy to integrate in mere minutes. But don't let the simplicity of solution fool you— It is by no means compromising Command Center ASPMs advanced offering— encompassing features from modern application security workflows to the most advanced business problems and capabilities.

Beyond Command Center ASPM

At Command Center Inc., we are not just about application security; we're about revolutionizing the way you identify and eliminate risk to your application assets and the data they handle. From basic application security processes to intricate use cases, Command Center ASPM is your all-in-one solution to cover your business needs from the basic to the utmost advanced.

While application security might start at application security risk management, it certainly doesn't stop there. Modern applications demand more: a solution that effortlessly connects organizations with the protection of their applications assets and data, all while maintaining ironclad security and unwavering compliance standards.

Login Page

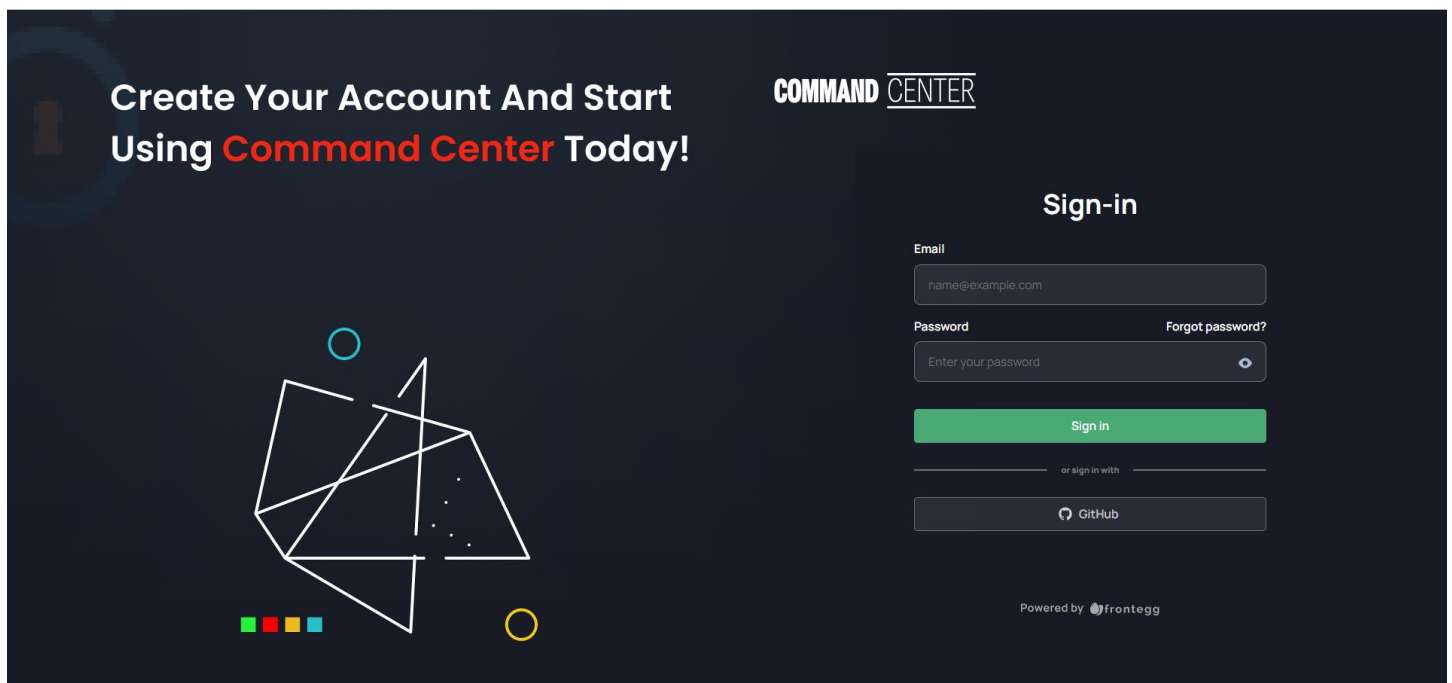
Login

The Login is the visual authentication element your users will see

Login

Getting Started with Your Login

When you go to the [Login](#) of your [Command Center ASPM Portal](#), you will find your Login. The Login is the visual authentication element (box) that your users will see, and you can control its visual elements such as username and password fields, social login options, and a single sign-on button, with a graphic theme to your liking.



Login process

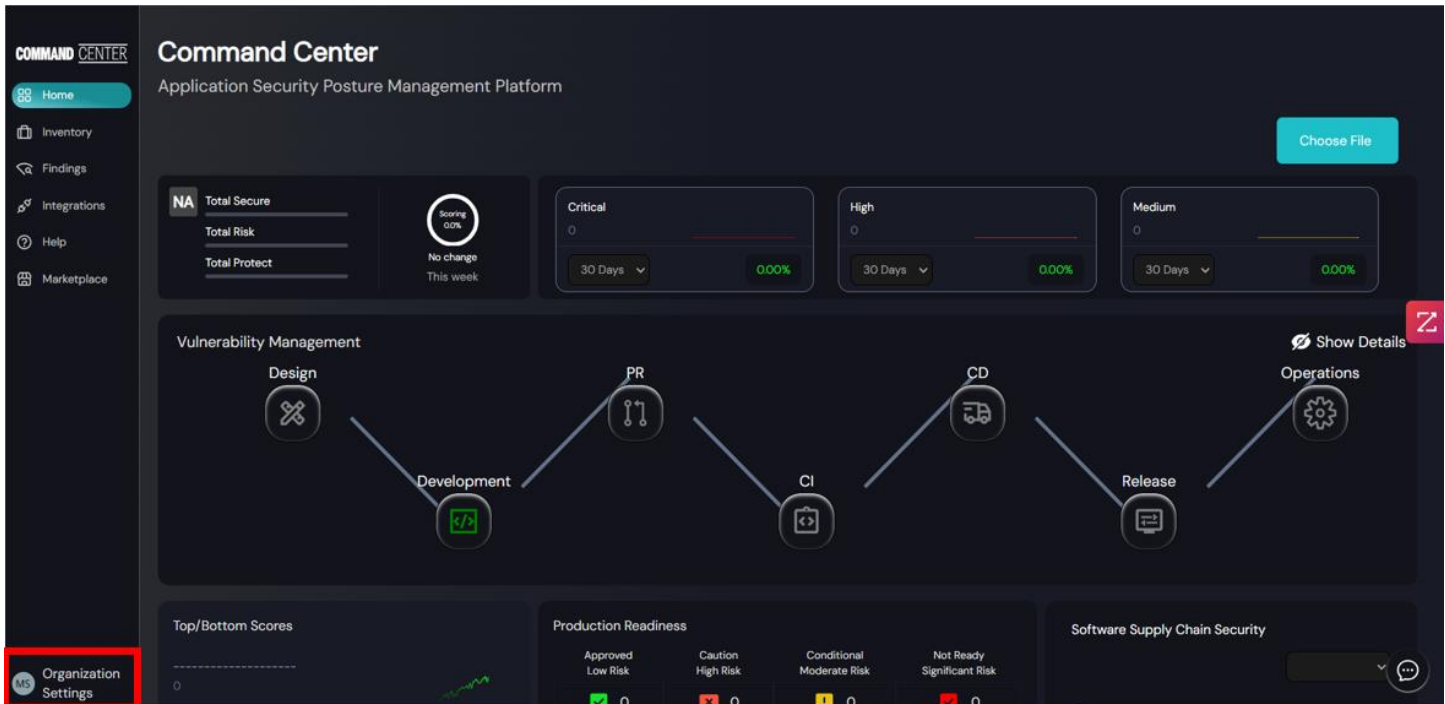
After arriving at the Command Center ASPM login, it's time to sign in. Logging into Command Center ASPM requires only a few easy steps.

- Input your username and password, or select your social login option or select single sign-on
- Select the Sign In button.
- Be redirected to the Command Center new user onboarding page or be redirected to the Command Center ASPM Portal.

Check the complete Login guide [Login](#)

User Management and Administration

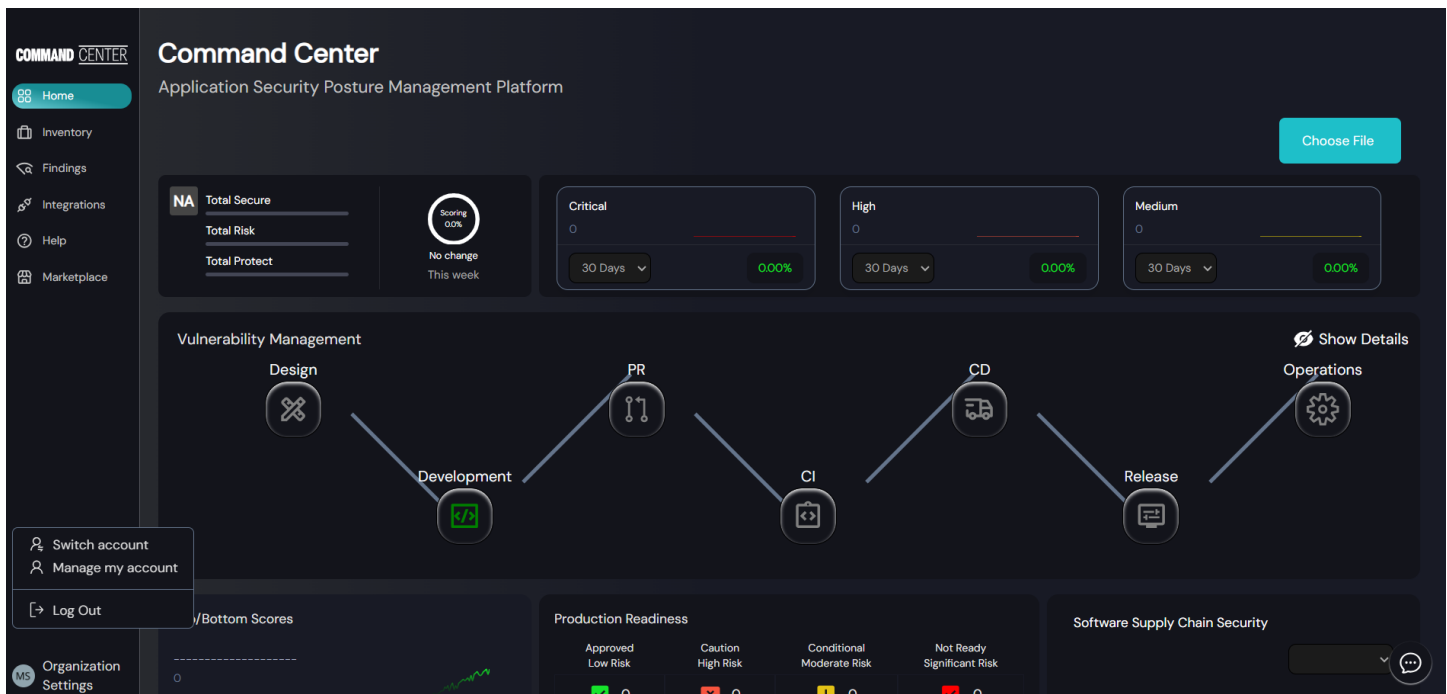
Once you log into Command Center ASPM you can manage and administrate you users accounts using the organizations settings option located on the bottom left hand corner of the Command Center ASPM Portal.



STEP 1: Click on Organization Settings

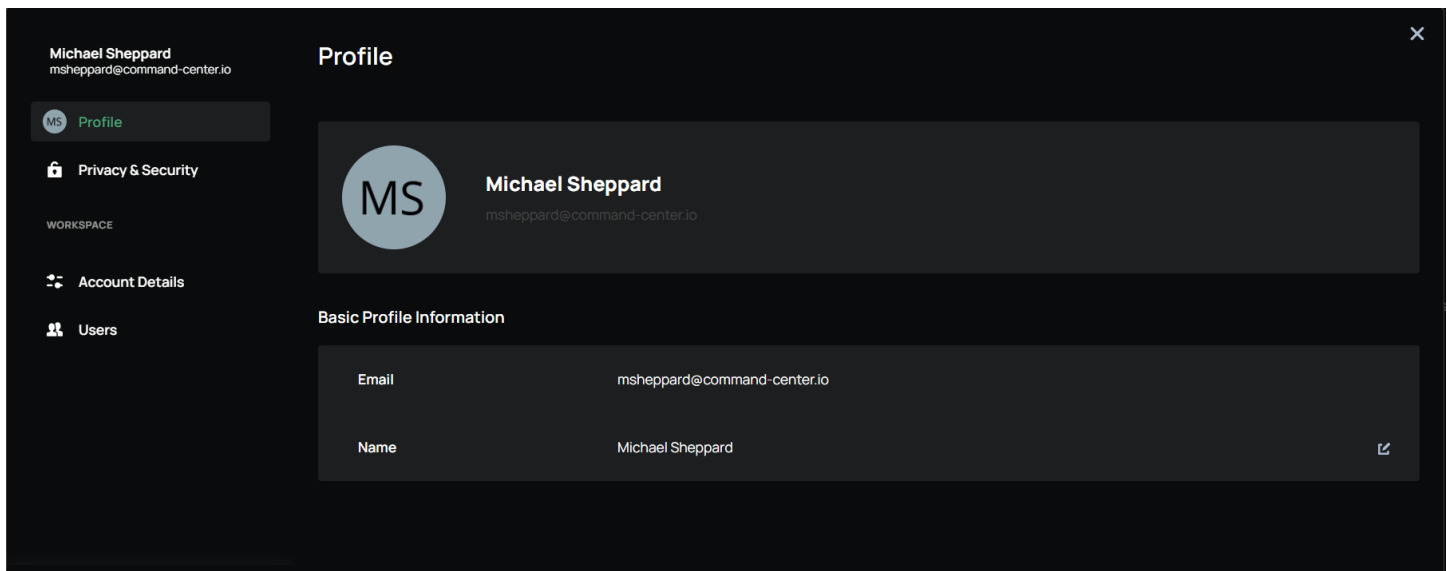
Clicking on Organizational Settings you'll be prompted with the Organizational Settings menu with options to logout, manage my account and switch accounts.

STEP 2: Click on Organization Settings



Select Manage my account

Upon clicking on Manage my account you'll be taken to the Organizational Setting page. Choose manage my account.

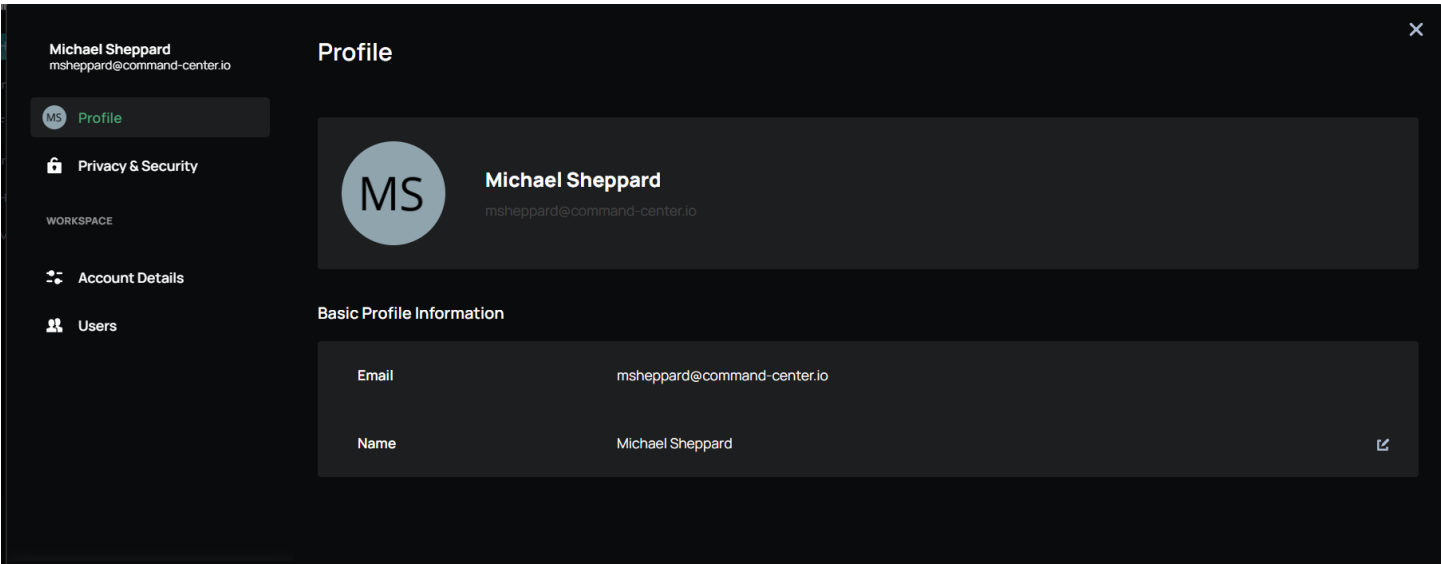


Select Manage my account

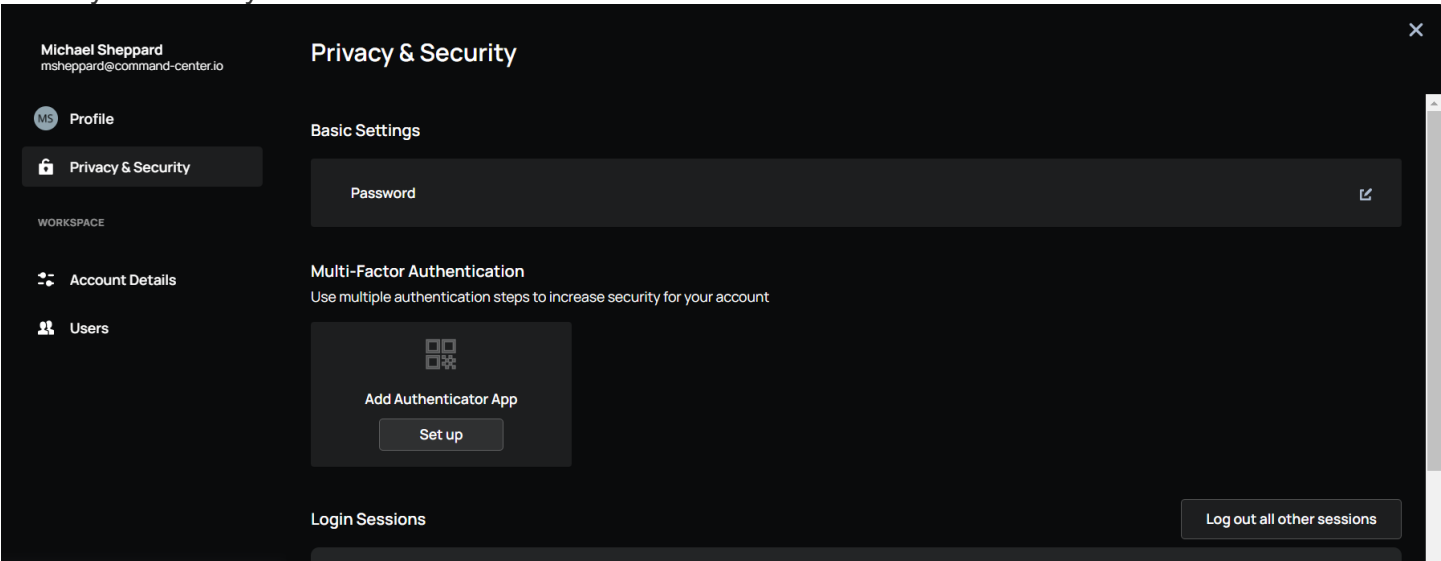
Upon clicking on Manage my account you'll be taken to the Organizational Setting page. Choose manage my account.

Here you'll find options to view;

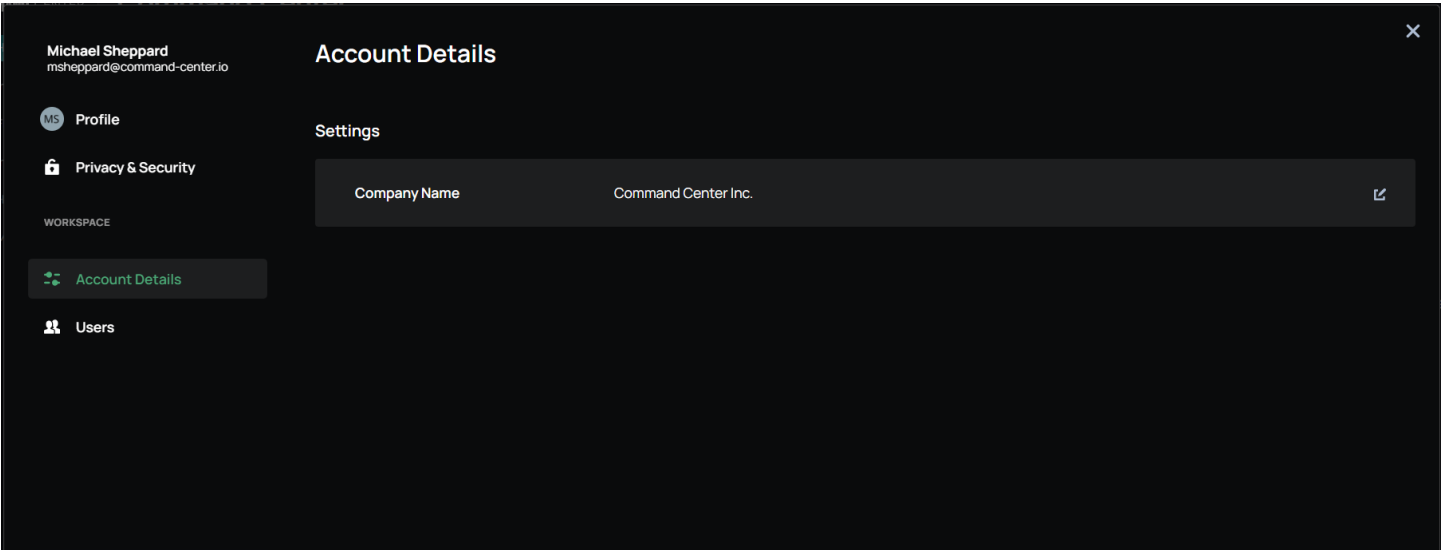
- Profile



- Privacy & Security



- Account Details



- Users

Select Users to invite new users to your organizations Command Center ASPM Platform.

Upon clicking on users you'll have the option to invite new users to the Command Center ASPM Platform.

Invite User

Email & Role *

Select role ▼

Full Name *

Phone Number (optional)

Invite with link

↔ Copy invite link

Cancel

Invite

Enter new user e-mail address, select a role, enter the new users full name and select invite to send the new user an invite to onboard the Command Center ASPM Platform.

You also have the option to enter a phone number as well as copy the invite link and forward it to the new user.

Risk Insights Overview

Explore the wide array of insights available on the Command Center ASPM Portal, including Risk Posture Score Grade, Total Vulnerabilities, Vulnerability Management, Top 5 Activity, Production Readiness, Software Supply Chain Security, Coverage, High Risk Vulnerabilities, Risk Management, Meantime to Resolve and Threat Protection Monitor.

Command Center ASPM Risk Insights

Command Center ASPM offers a range of risk insights with popular metrics such as Risk Posture Score Grade, Total Vulnerabilities, Vulnerability Management, Top 5 Activity, Production Readiness, Software Supply Chain Security, Coverage, High Risk Vulnerabilities, Risk Management, Meantime to Resolve and Threat Protection Monitor. These insights are designed to simplify the process of risk to your organization and its associated application assets including (web applications, source code repositories, APIs and components). The intuitive risk insights provided make it easy to understand your organization's application assets risk posture as well as what immediate actions you should take to eliminate risk to your organization, its application assets and the data they handle.

For cases where a desired risk insight is not available as a preset risk insight, we offer the possibility of developing custom risk insights. This approach enables you to best identify and protect your application assets against threats, ensuring that even unique security needs are met.

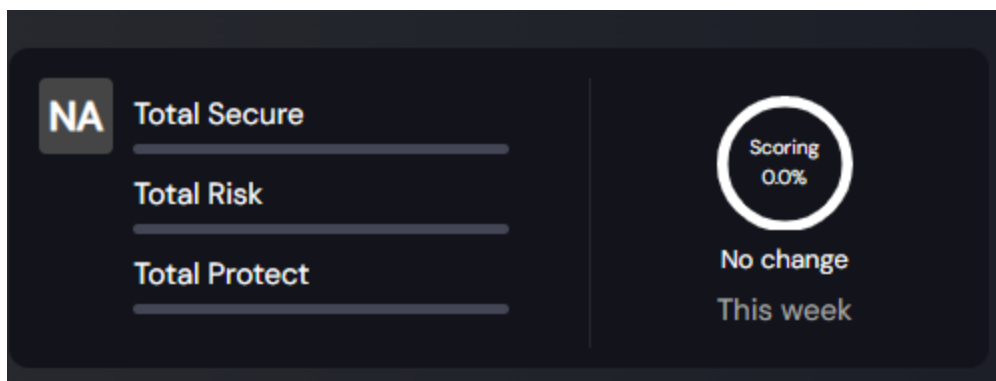
Risk Posture Score Grade Insight

Allows your organization to identify its overall risk posture across all of its application assets including web applications, repositories, components and APIs. The Risk Posture Score grade is determined across three areas of measurement including;

Total Secure indicator: A comprehensive evaluation of all the people, processes, policies, enforcements and capabilities your organization has in place to secure your application assets and the sensitive data / information they handle.

Total Risk indicator: A comprehensive evaluation of all the risk, vulnerabilities, threats and deficiencies your organization's applications assets and data / information has posing risk to your organization.

Total Protect indicator: A comprehensive evaluation of all the controls, protections, notifications and alerts your organizations application assets and the sensitive data / information they handle have in place to protect against malicious threats and activity.



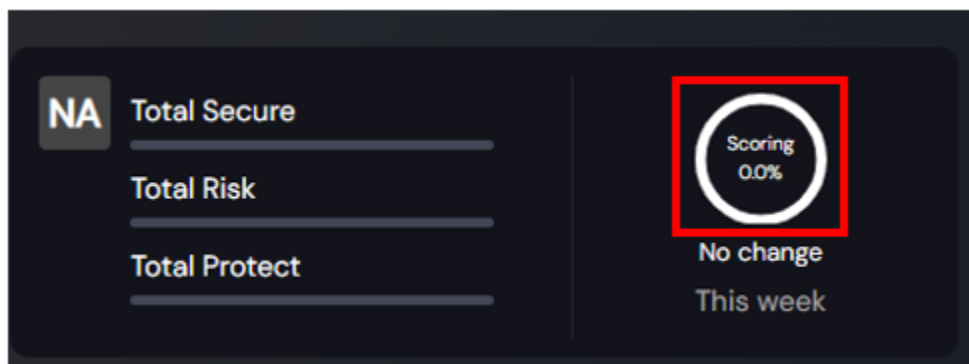
The Risk Posture Score Grade is assigned using a letter grade system A-F illustrated below.

Security Grading System

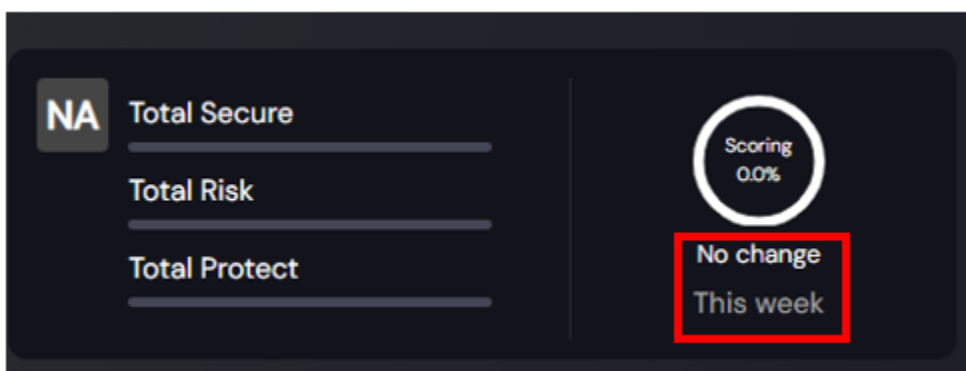
Grade	Description	<u>Production Readiness</u>
A	Your application assets and data have strong security and protection with a minimal amount of risk.	A=Represents Low Risk
B	Your application assets and data have high security and protection with a low amount of risk.	B=Represents Acceptable Risk
C	Your application assets and data have moderate security and protection with a moderate amount of risk.	C=Represents Moderate Risk
D	Your application assets and data have weak security and protection with a high amount of risk.	D=Represents High Risk
F	Your application assets and data have no security and protection with a critical amount of risk.	F=Not Ready for Production

N/A=No Info

The Risk Posture Score Grade is also represented by it's numerical value 0-100% illustrated below.

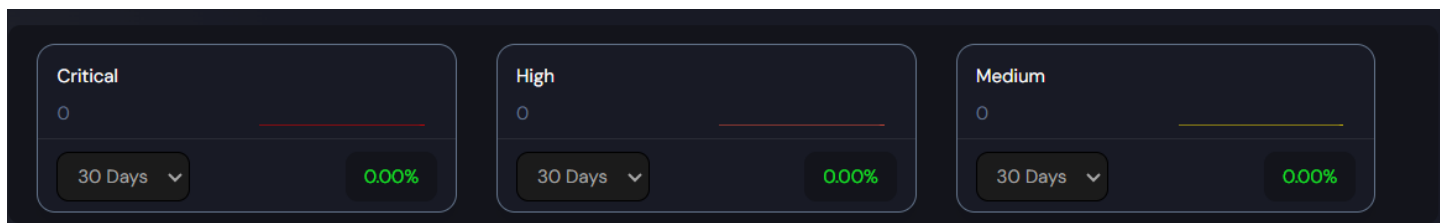


Lastly, your Risk Posture Score Grade has trending providing over a period of time including daily, weekly, monthly and yearly.



Total Vulnerabilities Insight

Allows your organization to obtain a unified view of all your application assets vulnerabilities across all your tools in one place presented by severity with daily, weekly, monthly and yearly trending as well as a percentile up or down over the given trending time.



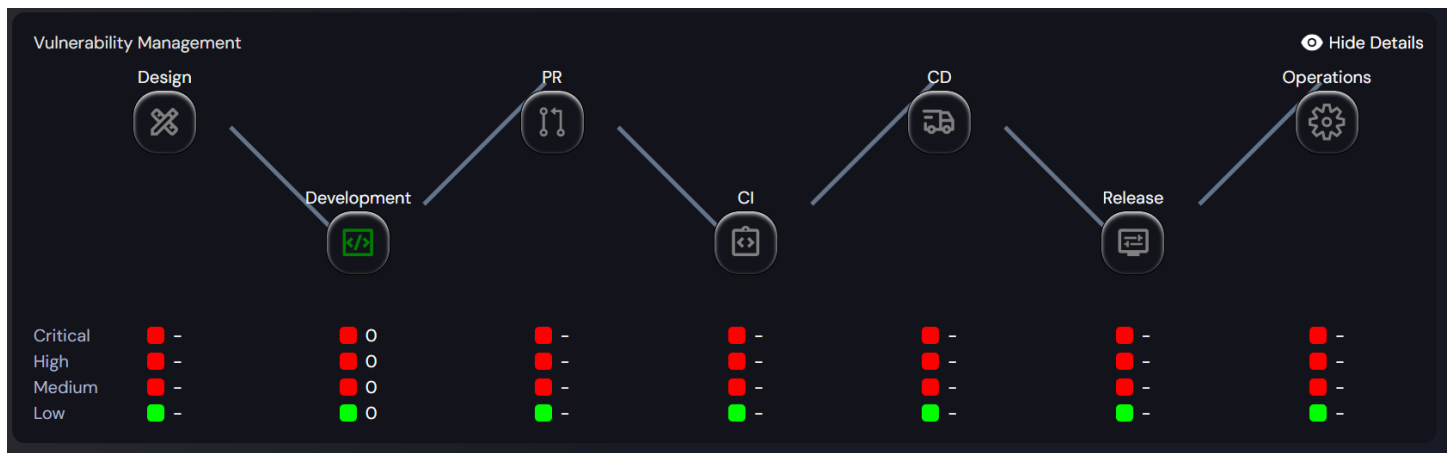
Top 5 Activity Insight

Allows your organization to view it's top 5 and bottom 5 individual application assets risk posture score grades including daily, weekly, monthly and yearly trending as well as a percentile up or down over the given trending time.



Vulnerability Management Insight

Allows your organization to view its unified risk across each phase of the Software Development Lifecycle by severity, critical, high, medium and low. The Vulnerability Management Insight also allows organizations to configure and enable security tollgates at specific stages in the Software Development Lifecycle to prevent risk from being promoted ultimately into production.



Software Supply Chain Security Insight

Allows your organization to assess the risk posture of every application assets at each stage of the software development lifecycle up and into production. The Software Supply Chain Security Insight reviews application assets as they traverse from one phase of the software development lifecycle to another assessing your assets for existing controls that ensure the security of your applications assets and the data they handle. Each stage performs a specific check including;

Design & Develop:

Design & Develop evaluates your application assets for controls and capabilities including (Security Architecture, Threat Model, Security Champion, Security Requirements) and more.

Source code protection:

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Continuous Integration & Delivery:

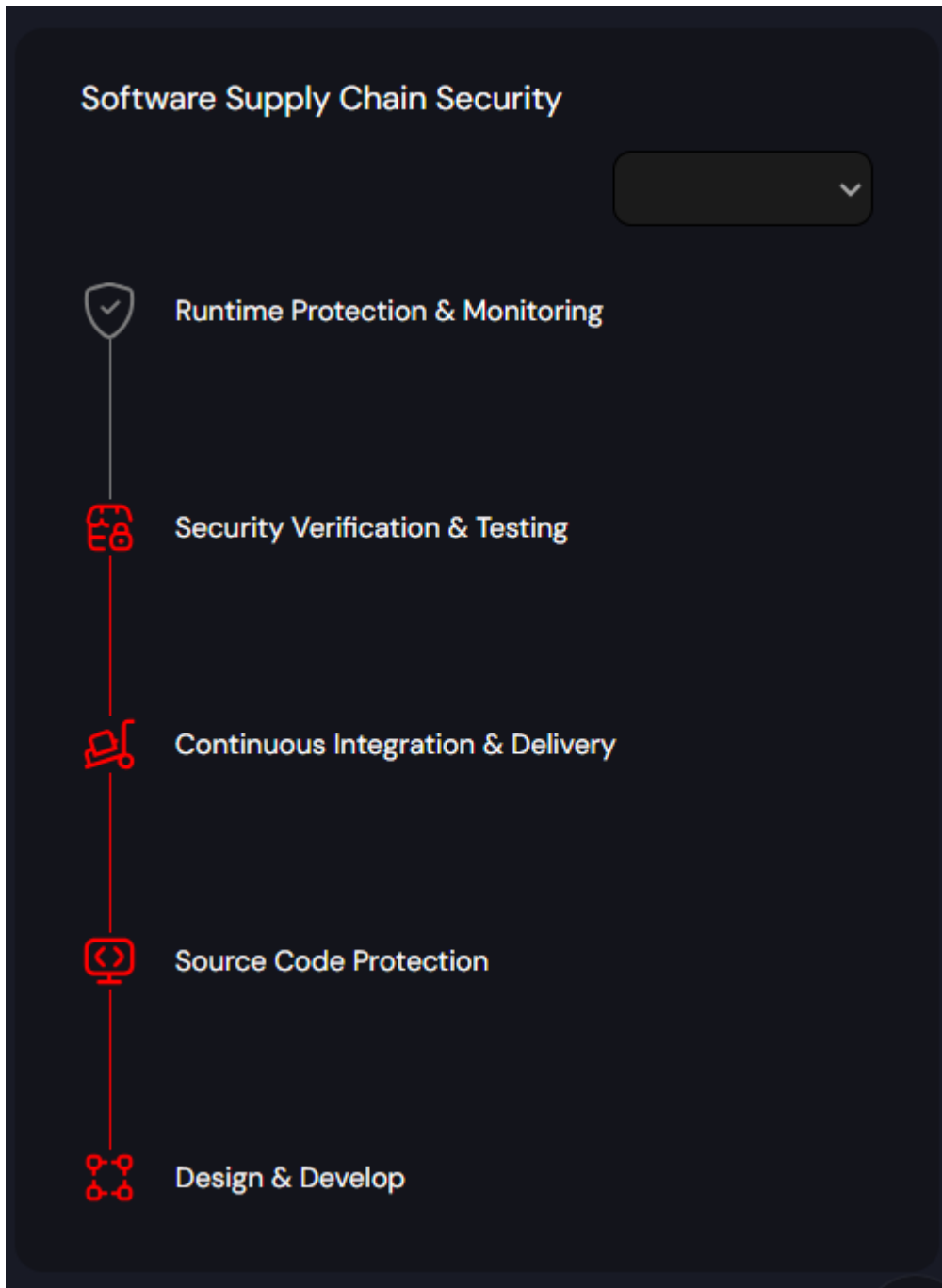
Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Security Verification & Testing:

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

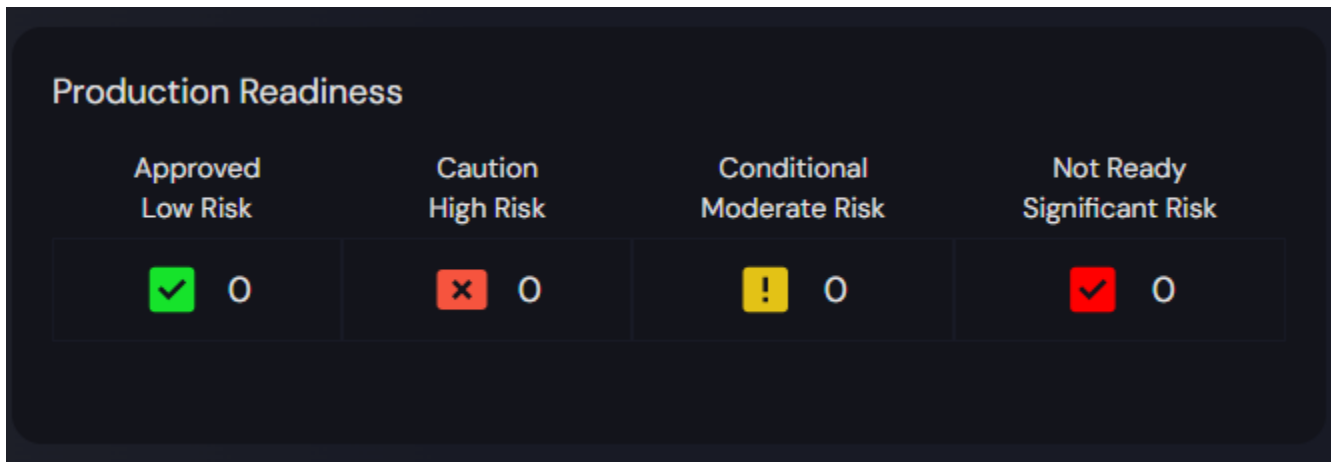
Run-time Protection & Monitoring:

Run-time Protection & Monitoring evaluates your application assets for controls, capabilities and security including (Run-time Application Self Protection, Web Application Firewall, Application Security Posture Management) and more.



Production Readiness Insight

Allows your organization to assess the production readiness of your application assets so that you can release with assurance.



Production Readiness Insight

Your application assets production readiness are determined using 4 risk severity categories including;

Approved Low Risk:

Design & Develop evaluates your application assets for controls and capabilities including (Security Architecture, Threat Model, Security Champion, Security Requirements) and more.

Caution High Risk:

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Conditional Moderate Risk:

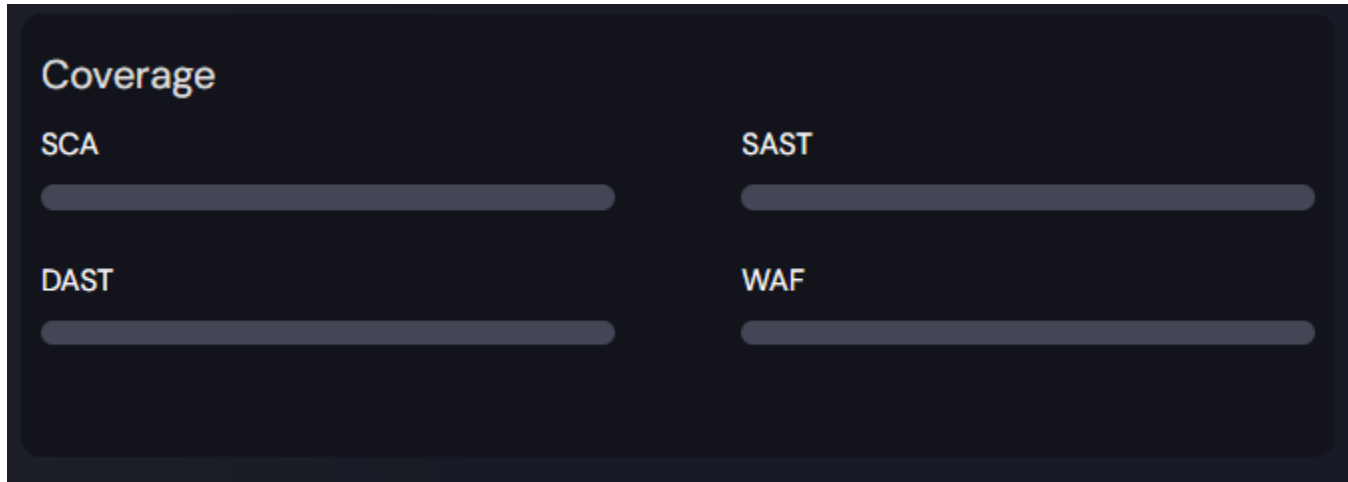
Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Not Ready Significant Risk:

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Coverage Insight

Allows your organization to assess the coverage of your application assets by critical assessment, testing and control capabilities including;



Software Composition Analysis (SCA):

Design & Develop evaluates your application assets for controls and capabilities including (Security Architecture, Threat Model, Security Champion, Security Requirements) and more.

Static Application Security Testing (SAST):

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Dynamic Application Security Testing (DAST):

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Web Application Firewall (WAF):

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Interactive Application Security Testing (IAST):

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Web Application Penetration Testing (WAPT):

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Run-time Application Self Protection (RASP):

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Application Security Posture Management (ASPM):

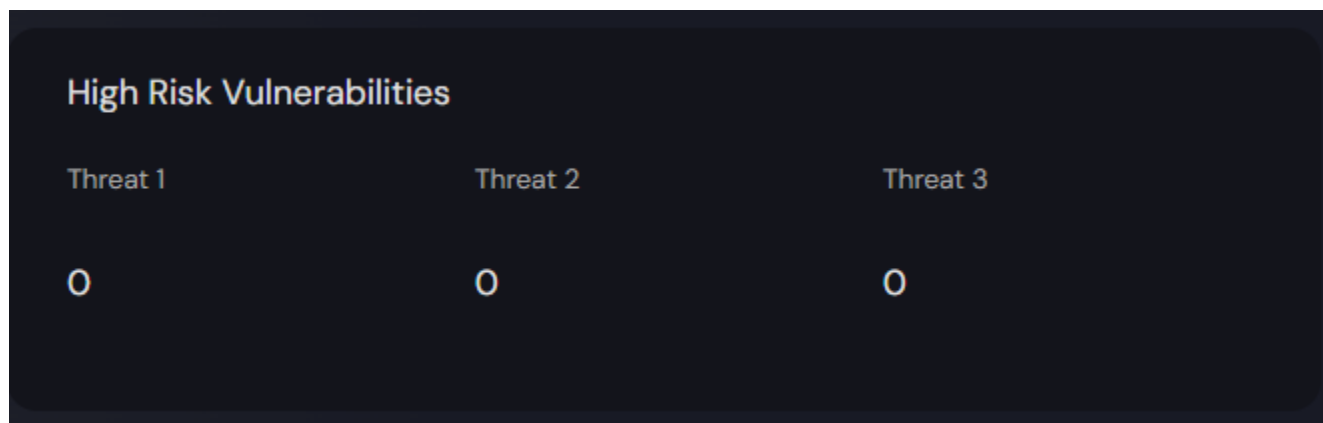
Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Repository Assurance (Repo Sec):

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

High Risk Vulnerabilities Insight

Allows your organization to understand the top 3, most critical by severity and volume, exploitable High-Risk vulnerabilities impacting your application assets and their risk posture;



Threat #1:

The top high severity vulnerability impacting your application assets and their related risk posture.

Threat #2:

The second high severity vulnerability impacting your application assets and their related risk posture.

Threat #3:

The third high severity vulnerability impacting your application assets and their related risk posture.

Risk Management Insight

Allows your organization to understand your unified total risk across your application assets including SLA Violations, Risk Accept, Risk Except, False Positive Audit and Audit Compliance. The Risk Management Insight provides daily, weekly, monthly and yearly trending as well as a percentile up or down over the given trending time. The Risk Management Insight displays risk including;

Risk Management				
SLA Violation	Risk Accept	Risk Except	False Positive Audit	Audit Compliance
1198	750	1053	1191	940
5345.45% ▼	5257.14% ▼	4478.26% ▼	3509.09% ▼	3986.96% ▼

SLA Violation:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Risk Accept:

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Risk Except:

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

False Positive Audit:

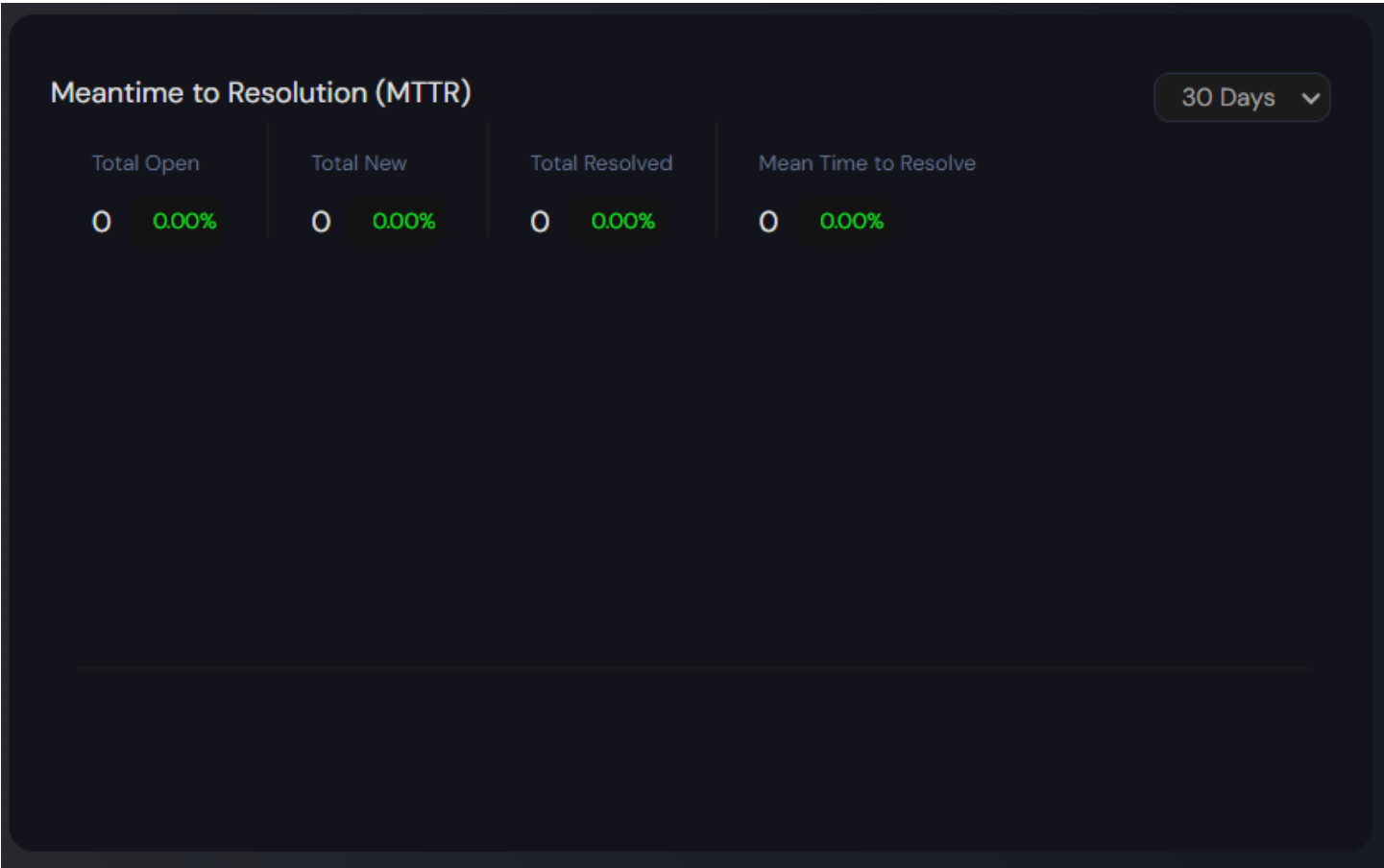
Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Audit Compliance:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Meantime to Resolve Insight

Allows your organization to understand your unified total risk across your application assets including daily, weekly, monthly and yearly trending as well as a percentile up or down over the given trending time with associated line graphs for total open vs total resolved. The Meantime to Resolve Insight displays risk including;



Total Open:

Displays the total number of open vulnerabilities in a given period of time across all your application assets.

Total New:

Displays the total number of new vulnerabilities in a given period of time across all your application assets.

Total Resolved:

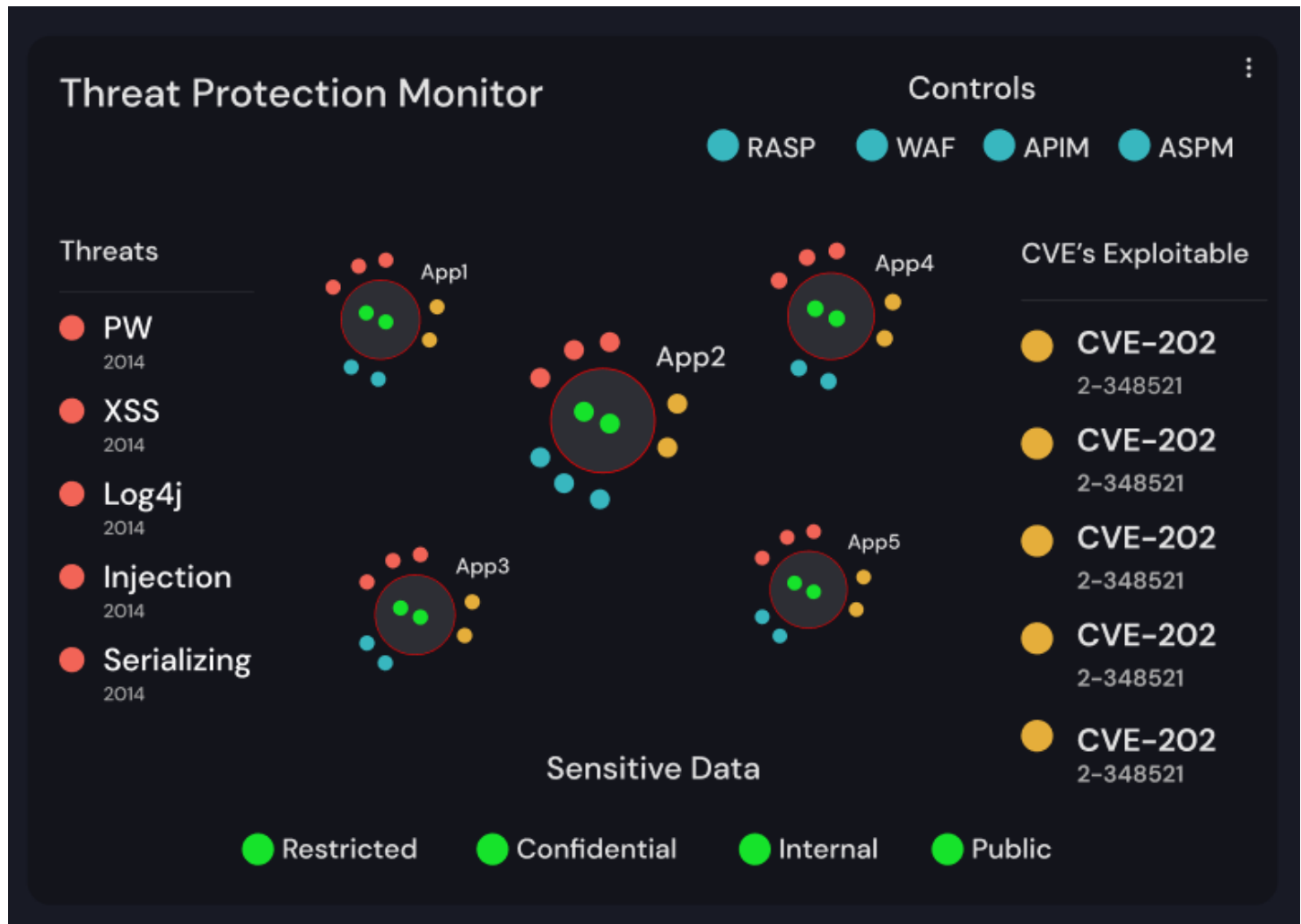
Displays the total number of vulnerabilities remediated in a given period of time across all your application assets.

Meantime to Resolve:

Displays the average amount of time to remediate vulnerabilities in a given period of time across all your application assets.

Threat Protection Monitor Insight

Provides your organization a unified production view of your application assets, the data they handle, the threats actively acting against them, the vulnerabilities impacting them and the controls protecting them all in one place.



Application Assets:

Displays your application assets deployed to production.

Threats:

Displays critical malicious threats actively acting on your application assets and the data they handle.

Data:

Displays the sensitive data your application assets are handling in production.

Exploitable Vulnerabilities:

Displays critical and high severity exploitable vulnerabilities within your application assets in production.

Controls:

Displays the controls actively protecting your application assets and the data they handle in production.

Integrations Overview













Explore the wide array of 3rd party cybersecurity tool integrations available through the Command Center ASPM Platform. These critical 3rd party cybersecurity tools serve as the data foundation for Command Center ASPM along with its AI-driven algorithms that allow it to visualize your organizations risk posture in powerfully intuitive ways.

Command Center ASPM Integrations

Command Center ASPM offers a range of critical 3rd party cybersecurity tool integrations with popular solutions such as Synk, Contrast Security IAST & RASP, Burp Suite Pro & Enterprise, Secure Code Warrior, SonarQube & SonarCloud, Imperva WAF, ServiceNow, Mulesoft, Azure DevOps (ADO) repositories & pipelines, GitHub, Gitlab, Semgrep, Tenable Nessus, Bitbucket and many more. These integrations are designed to simplify the process of incorporating your organizations data as a unified object to visualize your organization's holistic risk posture. The step-by-step instructions provided for each integration make it easy to configure and connect, enabling your organization to protect its critical application assets and the data they handle.

For cases where a desired integration is not available as a preset integration, we offer the possibility of creating custom 3rd party tool integrations for your organization. This approach enables you to ensure your complete risk posture is clear as well is the total protection of your application assets and the data they handle.

Integrations

 API Token URL	 API Token URL	 API Token URL	 Personal Access Token Organisation ID URL	 API Token(Contrast) API Token(Authorization) Service Key Organisation ID URL	 Username Password URL	 Username Password URL
 API Token Secret Key URL	 API Token API Secret URL	 API Token URL	 Authentication Token URL	 Workspace Access Token URL		

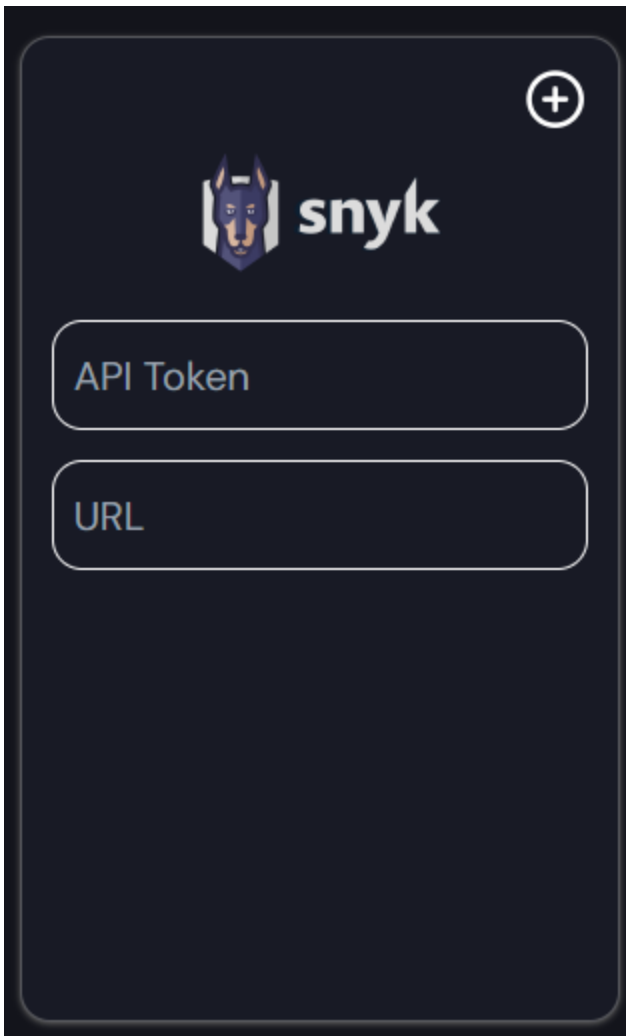
Snyk: Synk provides your application assets open source, 3rd party and code analysis vulnerability data with respect to software composition analysis, static application security testing, infrastructure as code and containers.

Step 1: Enter your API information


Step 2: Enter your Snyk API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.

A dark-themed user interface for Snyk integration. At the top right is a white plus sign in a circle. Below it is the Snyk logo, which consists of a stylized blue and white dog head icon followed by the word "snyk" in white lowercase letters. Below the logo are two rounded rectangular input fields. The first field is labeled "API Token" and the second field is labeled "URL". Both labels are in a light gray font.

+

 snyk

API Token

URL

Contrast Security IAST & RASP: Contrast Security IAST provides your application assets vulnerability data respective to Interactive Application Security Testing. Contrast Security Run-time Application Self Protection (RASP) provides your organizations data with respect to Run-time Application Self Protection.

Step 1: Enter your API information

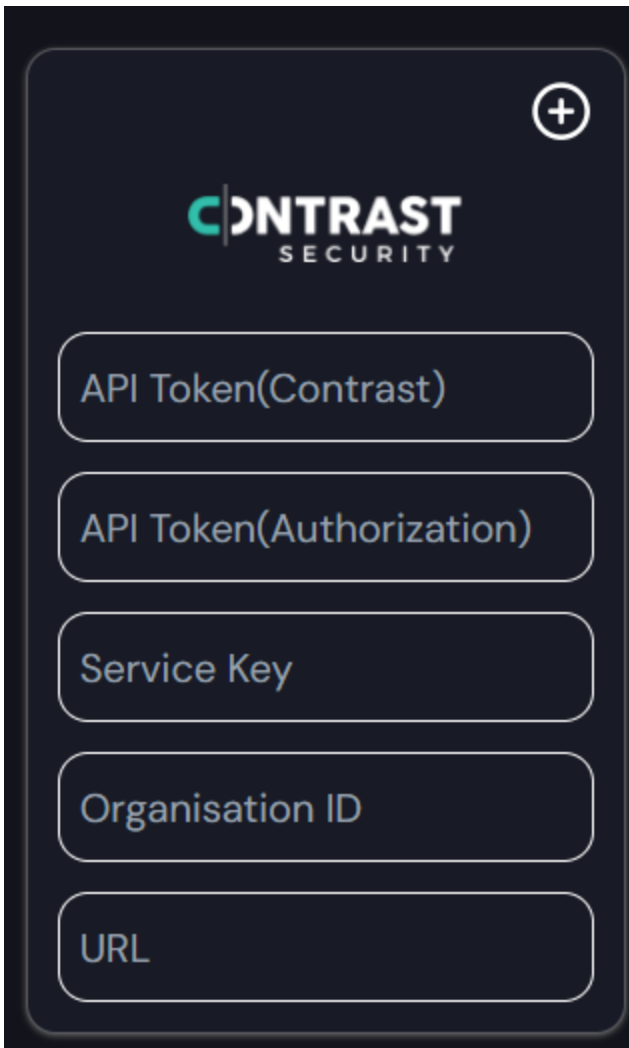
Step 2: Enter your Service Key

Step 3: Enter Organization ID

Step 4: Enter your API url

Step 5: Click the white plus (+) button

Step 6: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.

A dark-themed mobile interface for integrating Contrast Security. At the top right is a white plus sign in a circle. Below it is the Contrast Security logo, with 'CONTRAST' in white and 'SECURITY' in smaller white letters below it. The logo has a green vertical bar to its left. Below the logo are five rounded rectangular input fields, each with a white border and placeholder text: 'API Token(Contrast)', 'API Token(Authorization)', 'Service Key', 'Organisation ID', and 'URL'.

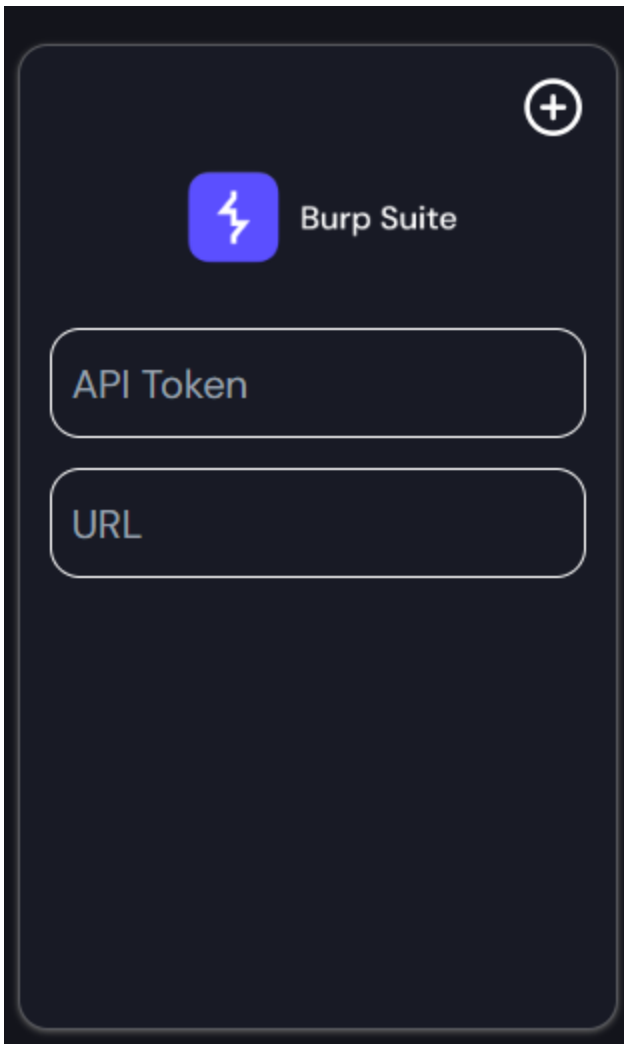
Burp Suite Pro & Enterprise: Burp Suite Pro and Enterprise provide your application assets vulnerability data respective to Dynamic Application Security Testing.

Step 1: Enter your API information

Step 2: Enter your Burp Suite API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.



The image shows a dark-themed user interface for integrating Burp Suite. At the top right is a white plus sign (+) button. Below it, on the left, is a blue square icon with a white lightning bolt. To the right of this icon is the text "Burp Suite". Below the icon and text are two rounded rectangular input fields. The first field is labeled "API Token" and the second field is labeled "URL".

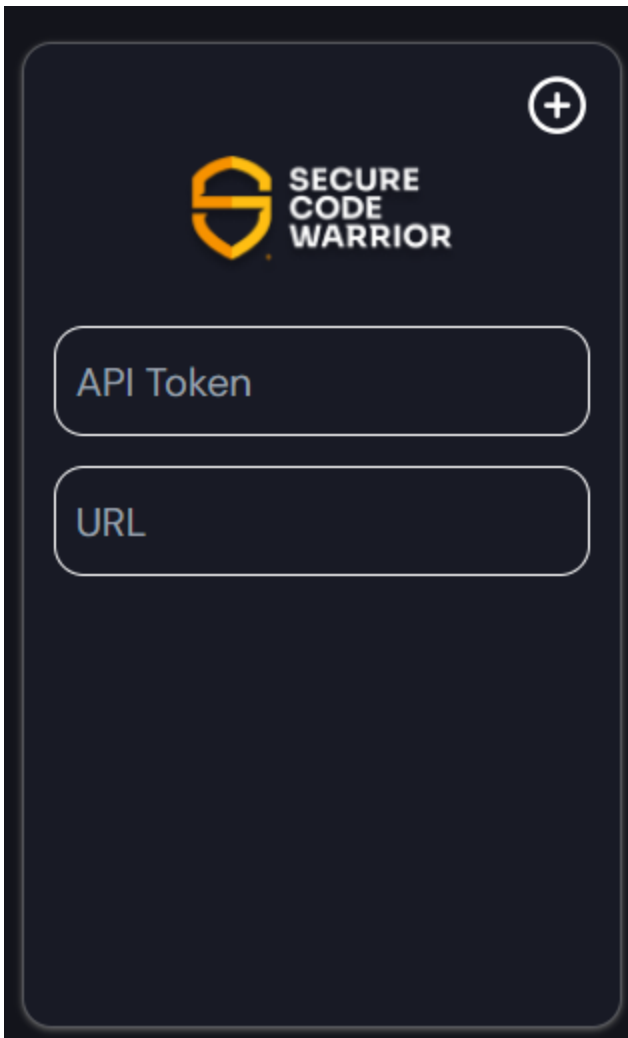
Secure Code Warrior: Secure Code Warrior provides your organizations software developer secure coding knowledge and capability data respective to secure software development.

Step 1: Enter your API information

Step 2: Enter your Secure Code Warrior API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.

A dark-themed mobile application interface for Secure Code Warrior. At the top right is a white plus sign (+) button. Below it is the Secure Code Warrior logo, which consists of a yellow shield icon with a stylized 'S' and the text 'SECURE CODE WARRIOR' in white. Below the logo are two rounded rectangular input fields. The first field is labeled 'API Token' and the second field is labeled 'URL'. Both fields are currently empty.

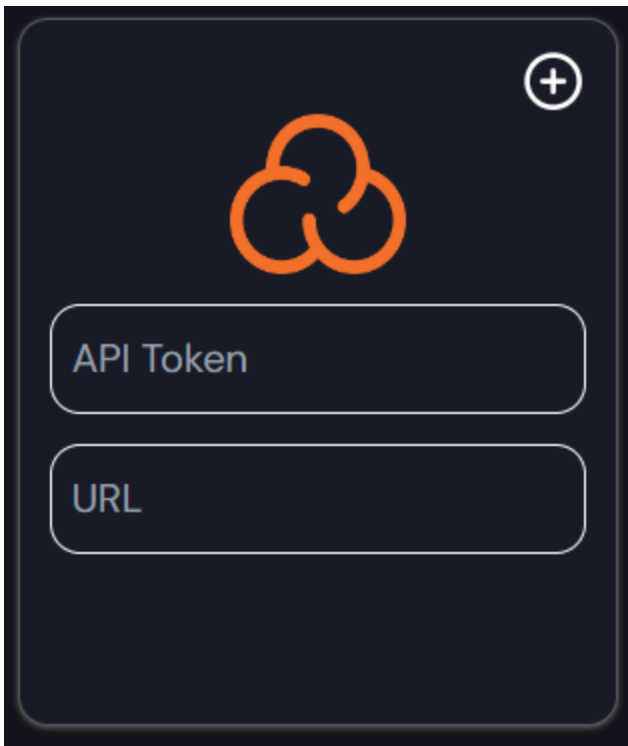
SonarQube & SonarCloud: SonarQube and Cloud provide your organization's application assets data with respect to quality, testing coverage and security.

Step 1: Enter your API information

Step 2: Enter your SonarQube and or SonarCloud API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.



API Token

URL

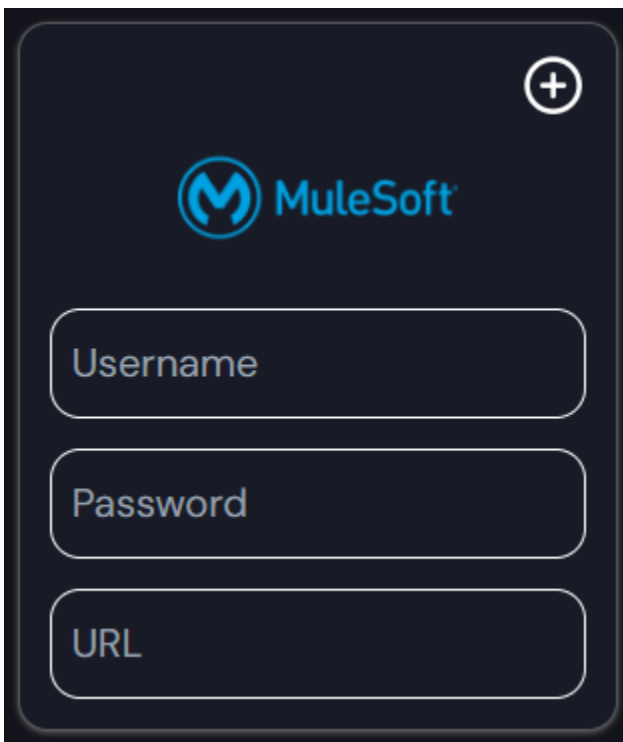
Mulesoft: Mulesoft provides your organization's application asset data specific to API protection.

Step 1: Enter your Mulesoft username & password information

Step 2: Enter your Mulesoft API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.



Username

Password

URL

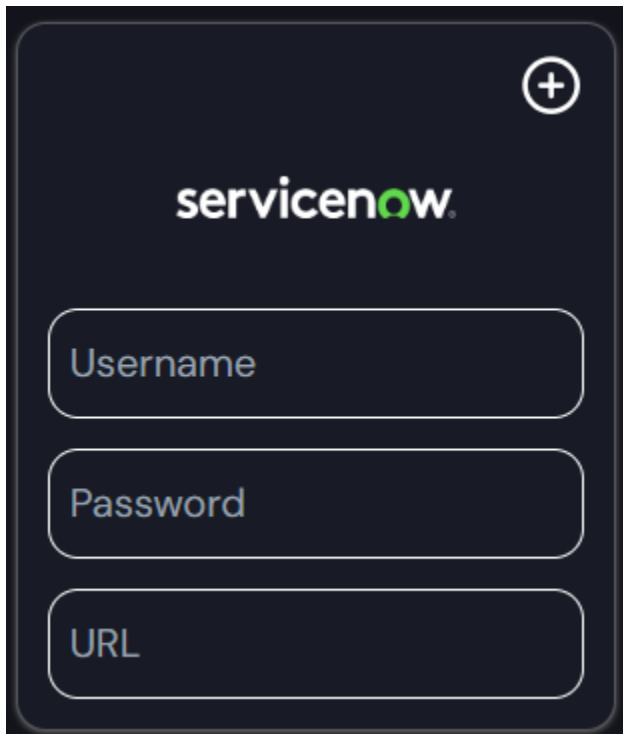
ServiceNow: ServiceNow provides your organization's application asset data specific to issue management and configuration management database (CMDB).

Step 1: Enter your ServiceNow username & password information

Step 2: Enter your ServiceNow API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.

A dark-themed rectangular form for ServiceNow integration. In the top right corner is a white circular button with a plus sign. Below this, the 'servicenow' logo is displayed in white, with the 'o' in 'now' being green. Underneath the logo are three stacked, rounded rectangular input fields. The first field is labeled 'Username', the second 'Password', and the third 'URL'. All labels are in a light gray font.

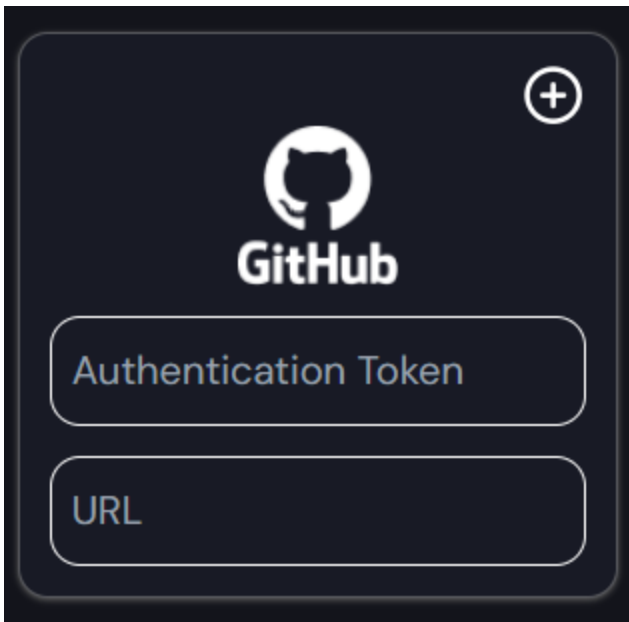
GitHub: GitHub provides your organization's application source code and pipeline data respective to repositories and pipelines.

Step 1: Enter your GitHub API authentication token

Step 2: Enter your GitHub API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.



Gitlab: GitHub provides your organization's application assets source code and pipeline data respective to repositories and pipelines.

Coming Soon

Semgrep: Semgrep provides your application assets open source, 3rd party and code analysis vulnerability data with respect to software composition analysis, static application security testing, infrastructure as code and containers.

Coming Soon

Imperva WAF: Imperva WAF provides your organization's application assets data respective to their protection against threat and attacks in a production environment.

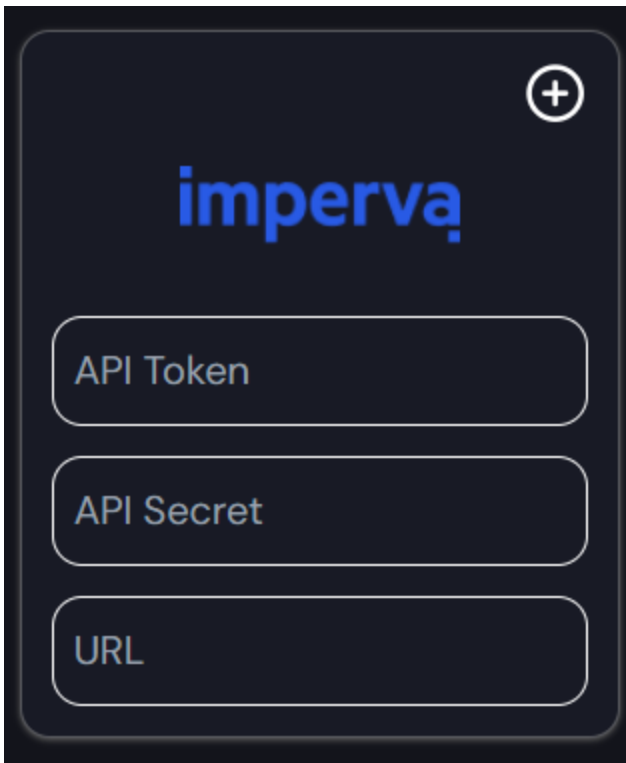
Step 1: Enter your Imperva WAF API Token

Step 2: Enter your Imperva WAF API Secret

Step 3: Enter your Imperva WAF API url

Step 4: Click the white plus (+) button

Step 5: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform.

A dark-themed rectangular form with rounded corners. In the top right corner is a white circle containing a plus sign (+). Below this, the word "imperva" is written in a blue, lowercase, sans-serif font. Further down are three stacked, rounded rectangular input fields with white borders. The first field contains the text "API Token", the second contains "API Secret", and the third contains "URL".

+

imperva

API Token

API Secret

URL

Azure DevOps (ADO) Repositories & Pipelines: Azure DevOps provides your organization's application assets source code and pipeline data respective to repositories and pipelines.

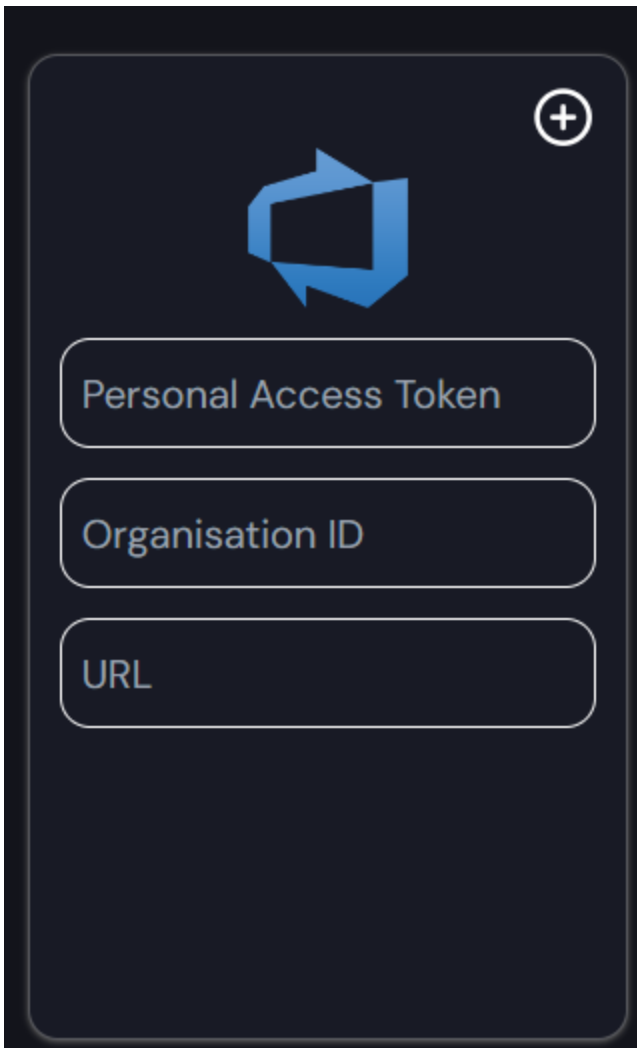
Step 1: Enter your Azure DevOps (ADO) Personal Access Token

Step 2: Enter your Azure DevOps (ADO) Organization ID

Step 3: Enter your Azure DevOps (ADO) API url

Step 4: Click the white plus (+) button

Step 5: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform

The image shows a dark-themed user interface for integrating Tenable Nessus. At the top left is the Tenable logo, a blue shield with a white 'X' inside. In the top right corner is a white plus sign (+) inside a circle. Below the logo are three rounded rectangular input fields stacked vertically. The first field is labeled 'Personal Access Token', the second is labeled 'Organisation ID', and the third is labeled 'URL'. The fields are currently empty.

Tenable Nessus: Tenable Nessus provides your organizations network and infrastructure assets data respective to network and infrastructure vulnerability management.

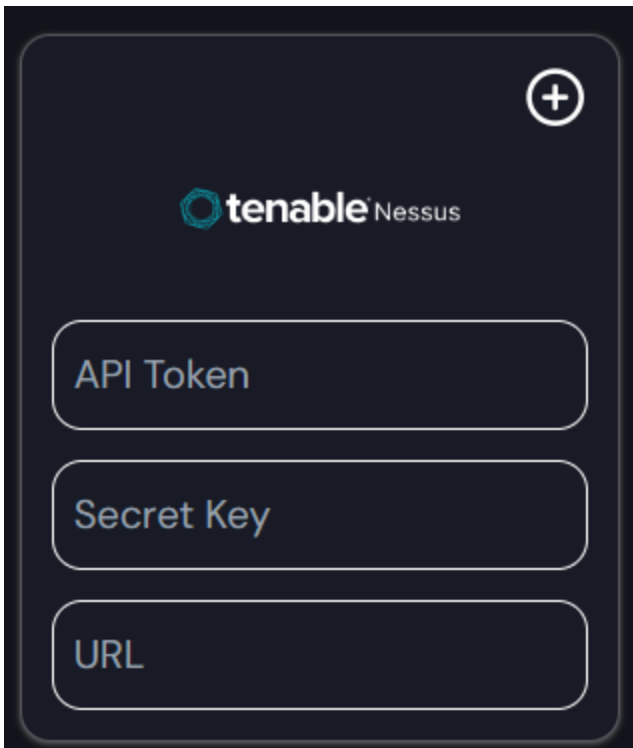
Step 1: Enter your Tenable Nessus API token

Step 2: Enter your Tenable Nessus Secret Key

Step 3: Enter your Tenable Nessus API url

Step 4: Click the white plus (+) button

Step 5: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform



A dark-themed rectangular card with rounded corners. In the top right corner is a white plus sign inside a circle. Below this, the Tenable Nessus logo is displayed. The card contains three stacked, rounded rectangular input fields with white borders. The first field is labeled 'API Token', the second 'Secret Key', and the third 'URL'.

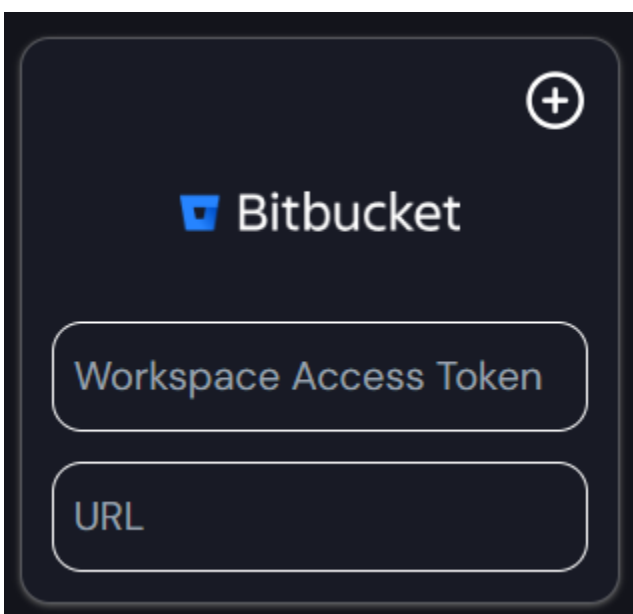
Bitbucket: Bitbucket provides your organization's application assets source code and pipeline data respective to repositories and pipelines.

Step 1: Enter your Bitbucket Workspace token

Step 2: Enter your Bitbucket API url

Step 3: Click the white plus (+) button

Step 4: The white plus (+) button will turn green signaling your integration is now connected to the Command Center ASPM Platform



A dark-themed rectangular card with rounded corners. In the top right corner is a white plus sign inside a circle. Below this, the Bitbucket logo is displayed. The card contains two stacked, rounded rectangular input fields with white borders. The first field is labeled 'Workspace Access Token' and the second 'URL'.

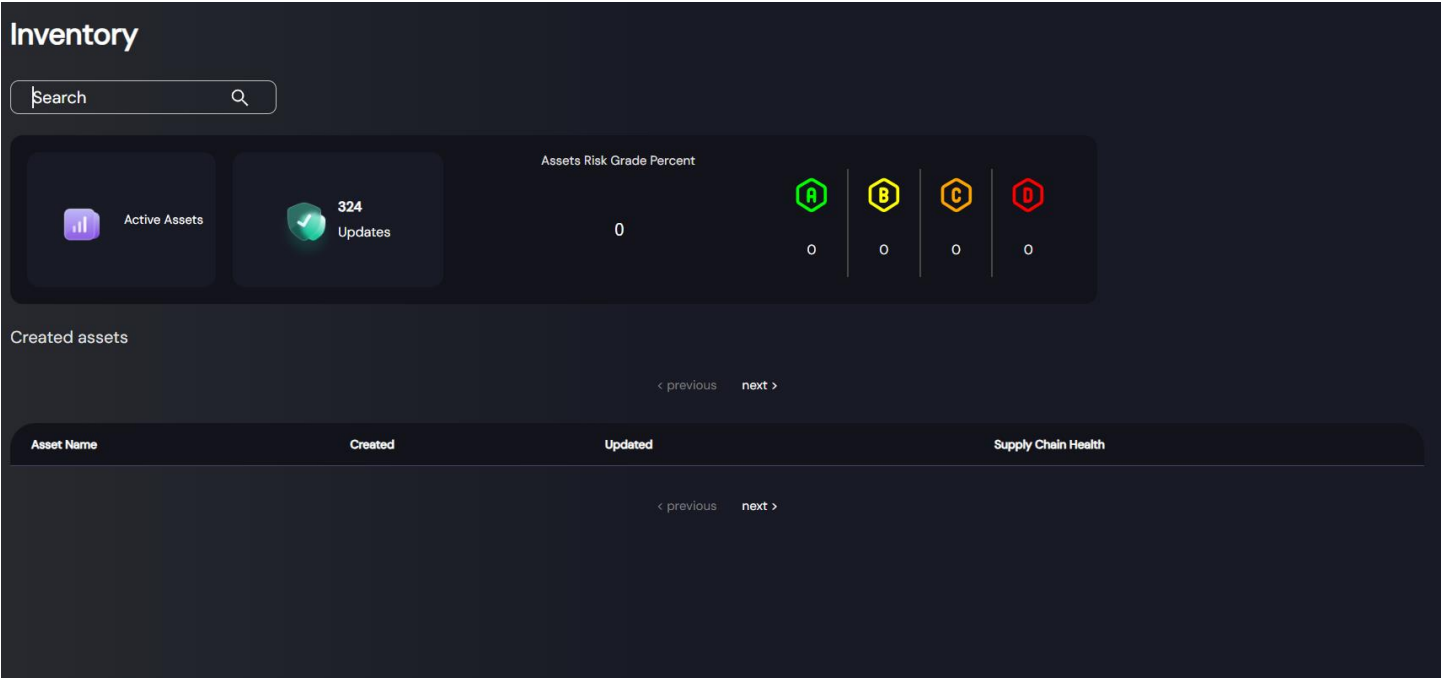
OWASP ZAP: OWASP ZAP provide your application assets vulnerability data respective to Dynamic Application Security Testing.

Coming Soon

We provide this in my morning tomorrow

Inventory Overview

The inventory page list out all your application assets including web applications, components, repositories and APIs. Command Center ASPM discovers your application assets with their assigned risk posture score grade. The inventory page allows your organization to have visibility into your application assets as well as the opportunity to combine and unify each asset with it’s associated repositories, components and APIs. The Inventory page also includes the following features;



Search:

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Active Assets:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Assets Risk Grade Percent:

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Asset Name:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Created:

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Updated:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Supply Chain Health:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Findings Overview

Explore the wide array of 3rd party cybersecurity tool integrations available through the Command Center ASPM Platform. These critical 3rd party cybersecurity tools serve as the data foundation for Command Center ASPM along with it’s AI-driven algorithms that allow it to visualize your organizations risk posture in powerfully intuitive ways.

Findings

Search

Severity

Status

< previous

1

2

3

4

5



...

2573

2574

2575

next >

Severity	URL	Introduced Date	Asset	Finding	Source	FindingID	Status
		Invalid Date					

Search:

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Severity Filter:

Status Filter:

Severity:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

URL:

Security Verification & Testing evaluates your application assets for controls and capabilities including (Dynamic Application Security Testing, Interactive Security Testing, Web Application Security Testing) and more.

Introduced Date:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Asset:

Source code protection evaluates your application assets for controls and capabilities including (Secure Coding Training, Secure Code IDE) and more.

Finding:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Source:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Finding ID:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Status:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Findings



Severity URL Introduced Date Asset Finding Source FindingID Status

Marketplace Overview

Explore the wide array of 3rd party cybersecurity tool integrations available through the Command Center ASPM Platform. These critical 3rd party cybersecurity tools serve as the data foundation for Command Center ASPM along with it's AI-driven algorithms that allow it to visualize your organizations risk posture in powerfully intuitive ways.

Marketplace

Command Center ASPM Premiere Product Vendors

[Show all vendors](#)

Filter By

[Clear](#)

- ☐ Static Application Security Testing
- ☐ Static Composition Analysis
- ☐ Dynamic Application Security Testing
- ☐ Interactive Application Security Testing
- ☐ Run-time Application Self Protection
- ☐ Web Application Firewall
- ☐ Continuous Integration
- ☐ Infrastructure Security Testing
- ☐ Network Security Testing
- ☐ Secure Code Training
- ☐ Bug Bounty
- ☐ Vulnerability Management

Discover Premiere Products

Browse through our product pages to learn about new application security products



Contrast Security

Contrast's patented deep security instrumentation completely disrupts traditional application security approaches with integrated, comprehensive security.

[Link →](#)

[Demo Link →](#)

[Trial Link →](#)



Manicode Security

Jim Manico is the founder of Manicode Security where he trains software developers on secure coding and security engineering. He is also the co-founder of the LocoMoco Security Conference and is an investor/advisor for Nucleus Security, BitDiscovery, Secure Circle and Inspectiv. Jim is a frequent speaker on secure software practices and is a member of the JavaOne rockstar speaker community. He is the author of "Iron-Clad Java: Building Secure Web Applications" from McGraw-Hill.

[Link →](#)

Filter By:

Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Vendors:

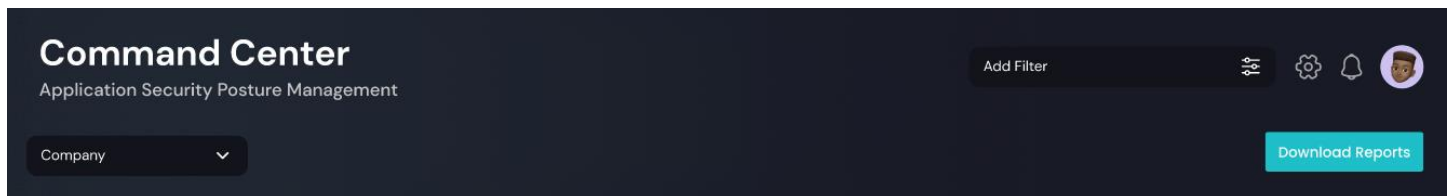
Continuous Integration & Delivery evaluates your application assets for controls and capabilities including (Software Composition Analysis, Static Application Security Testing, Dynamic Application Security Testing, Interactive Security Testing) and more.

Policies Overview

Explore the wide array of 3rd party cybersecurity tool integrations available through the Command Center ASPM Platform. These critical 3rd party cybersecurity tools serve as the data foundation for Command Center ASPM along with it's AI-driven algorithms that allow it to visualize your organizations risk posture in powerfully intuitive ways.

Download Reports

Explore the wide array of 3rd party cybersecurity tool integrations available through the Command Center ASPM Platform. These critical 3rd party cybersecurity tools serve as the data foundation for Command Center ASPM along with it's AI-driven algorithms that allow it to visualize your organizations risk posture in powerfully intuitive ways.



Download Reports: Bitbucket provides your organization's application assets source code and pipeline data respective to repositories and pipelines.

Step 1: Click Download Reports Button

Step 2: Save One-pager report to desired location

Step 3: Open Report

Upload Reports Overview

Explore the wide array of 3rd party cybersecurity tool integrations available through the Command Center ASPM Platform. These critical 3rd party cybersecurity tools serve as the data foundation for Command Center ASPM along with it's AI-driven algorithms that allow it to visualize your organizations risk posture in powerfully intuitive ways.

Command Center

Application Security Posture Management Platform

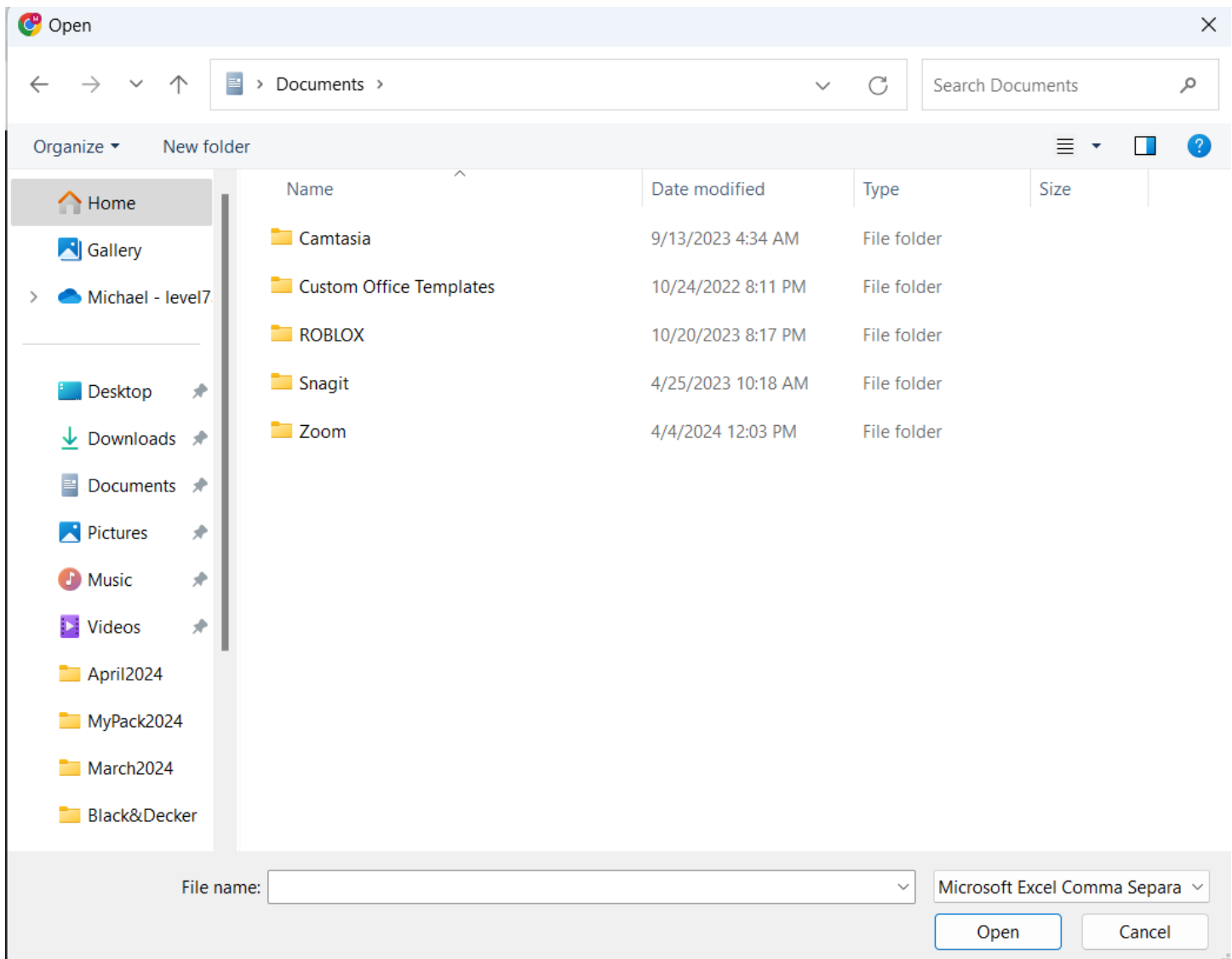
Choose File

Upload CSV: Bitbucket provides your organization's application assets source code and pipeline data respective to repositories and pipelines.

Step 1: Click Choose File Button

Step 2: Select CSV file from desired location

Step 3: Click Open option



Support Page

The Support section of Command Center is dedicated to providing comprehensive assistance to both customers and non-customers. Whether you need help navigating the application, understanding features, or resolving issues, our support options are designed to ensure you receive the help you need in a timely manner..

Search

Submit a Request

General

How to setup SSo group mapping with azure AD? >

How can i split the name field in the signup page to first and last name? >

How to fix {'errors':{'Failed to verify vendor'}}? >

How can i export user data from frotegg? >

Frontegg Token types and structure? >

Errors

How to setup SSo group mapping with azure AD? >

How can i split the name field in the signup page to first and last name? >

How to fix {'errors':{'Failed to verify vendor'}}? >

How can i export user data from frotegg? >

Frontegg Token types and structure? >

Best Practices

How to setup SSo group mapping with azure AD? >

How can i split the name field in the signup page to first and last name? >

How to fix {'errors':{'Failed to verify vendor'}}? >

How can i export user data from frotegg? >

Frontegg Token types and structure? >

General:**How can I find my SME account contact?**

Links to - Your SME account contact information is provided during the initial setup of your service. It can also be found in your welcome package or by contacting support@command-center.io.

What should I include in my support email?

Links - Provide a clear and detailed description of the issue, any steps you have already taken to resolve it, and any relevant screenshots or documentation.

How long does it take to get a response?

Links - We strive to respond to all inquiries in a timely matter. Response times may vary depending on the complexity of the issue and current ticket volume.

Contacting Your SME Account Contact.

Links - If you are a customer, you can reach out directly to your designated SME account contact for specialized assistance. This contact is provided at the start of your service term.

Using Email Support.

Links to - Send an email to support@command-center.io with your query or issue.

Please include as much detail as possible to help us understand and address your concern efficiently.

Phone:** 888.402.2026 option #2 (for urgent issues)

Customer Chat: “**yourcompanyname**”commandcentworkspace.slack.com.

Errors:

Command Center Portal ASPM UI Insights won't load?

Links to – Please refresh your browser when you encounter issues with the Command Center ASPM UI Insights not loading correctly or contact support@command-center.io.

Command Center ASPM Portal UI insight aren't displaying data.

Links - Please refresh your browser when you encounter issues with the Command Center ASPM UI Insights not loading correctly or contact support@command-center.io..

Command Center ASPM Integrations won't connect.

Links – Verify you are connecting to a supported 3rd party tool and version or contact support@command-center.io.

Can't Upload a CSV to Command Center ASPM Portal UI.

Links - Please validate you are uploading the provided Command Center ASPM findings CSV provided in the Command Center Portal or contact support@command-center.io.

Can't Download a Report from Command Center ASPM Portal UI.

Links – Please verify all supported 3rd party tool integrations are connected or contact support@command-center.io.

Best Practices:

Connecting 3rd Party Tool Integrations in Command Center ASPM.

Links to – To realize optimum value with Command Center ASPM it is important that your establish a minimum of one supported 3rd party tool integration or contact. Please contact support@command-center.io for assistance.

Using Auto-fix to Remediate Vulnerabilities in Command Center ASPM.

Links to – The auto-fix capability is only available when using Snyk SCA & SAST and or Mobb AI. Please contact support@command-center.io for assistance.

Configuring Alerts & Notifications Settings in the Command Center ASPM Policies page .

Links to – Enabling all desired policy page settings are necessary in order to deliver alerts and notifications. Please contact support@command-center.io for assistance.

Filtering Vulnerabilities in the Command Center ASPM Findings page.

Links – Multiple filters are available within the Findings page to provide the specific application asset risk posture data you desire. Please contact support@command-center.io for assistance.

Filtering Application Assets in the Command Center ASPM Inventory page.

Links – Multiple filters are available within the Inventory page to provide the specific application asset data you desire. Please contact support@command-center.io for assistance.

Submit a Request:

The Command Center ASPM support form is provided for customers to report issues related to Command Center ASPM. Please complete all required form fields and submit. A Command Center ASPM technical support specialist will respond within the established SLA to ensure resolution of your issue in a timely manner.

Support Ticket Form

×

Get in Touch

Report An Issue▼

Name

Type Name

Company

Type Company Name

Email

Input Email

Phone Number

Type Phone Number

Date

Enter Date

Description

Type Here

Submit Request

Form Fields include:

Get in Touch: Report an Issue – Select the appropriate issue for your request

Name: Provide your full name – First Name, Last Name

Company: Provide your full company name

E-mail: Provide your complete company e-mail address

Phone Number: Provide your preferred phone number should a technical support specialist need to contact you.

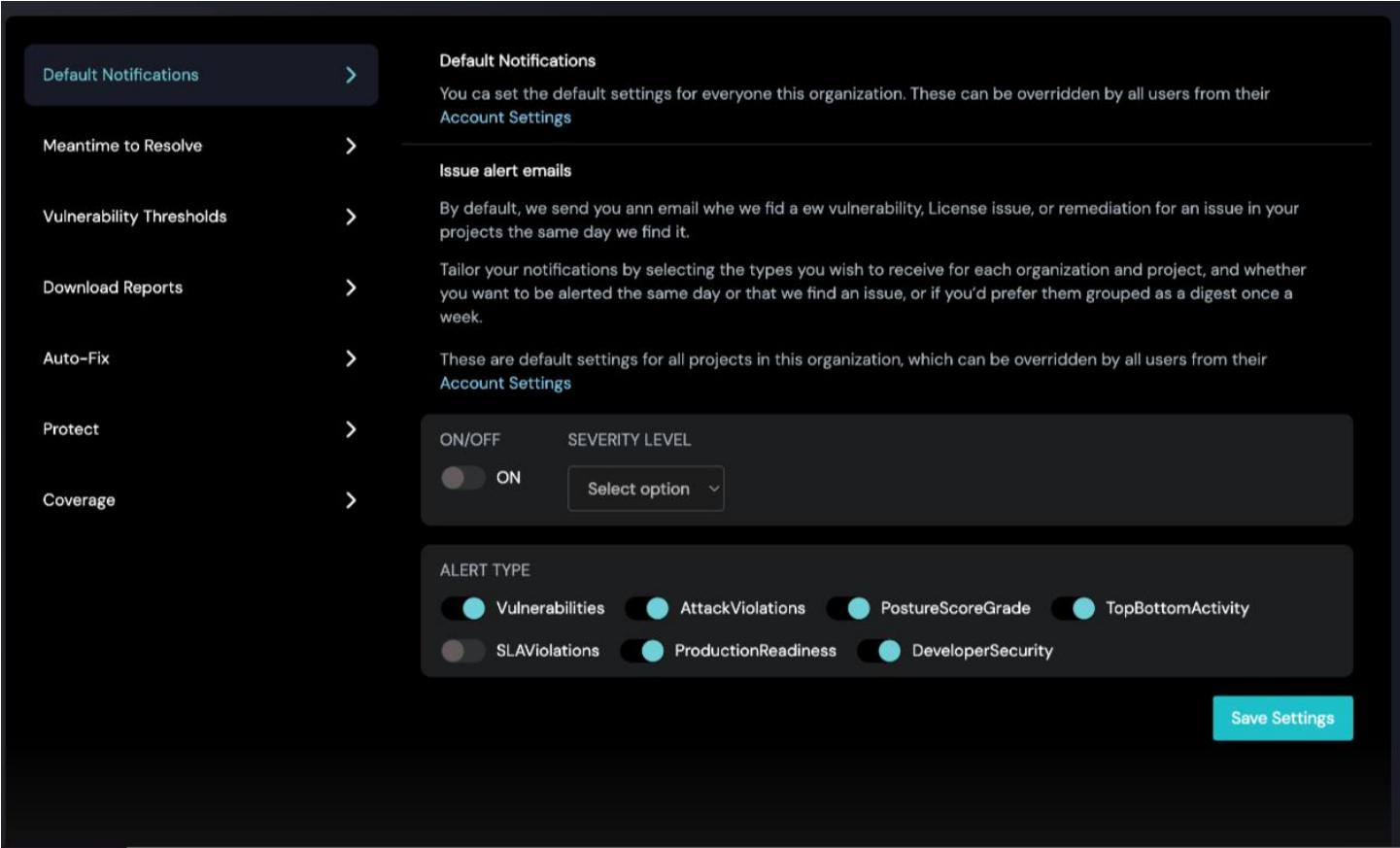
Date: Select the current date for your support request

Description: Provide a detailed description of your issue including;

A clear and detailed description of the issue, any steps you have already taken to resolve it, and any relevant screenshots or documentation.

Policies Overview

The Command Center ASPM Policies page provides a number of settings that when enabled provide critical alerts and notifications that inform you as to the risk posture of your application assets and they data they handle. The Command Center ASPM policies page provides the following settings;



Default Notifications:

Issue alert emails

ON/OFF

SEVERITY LEVEL: Select option

ALERT TYPE:

Vulnerabilities

AttackViolations

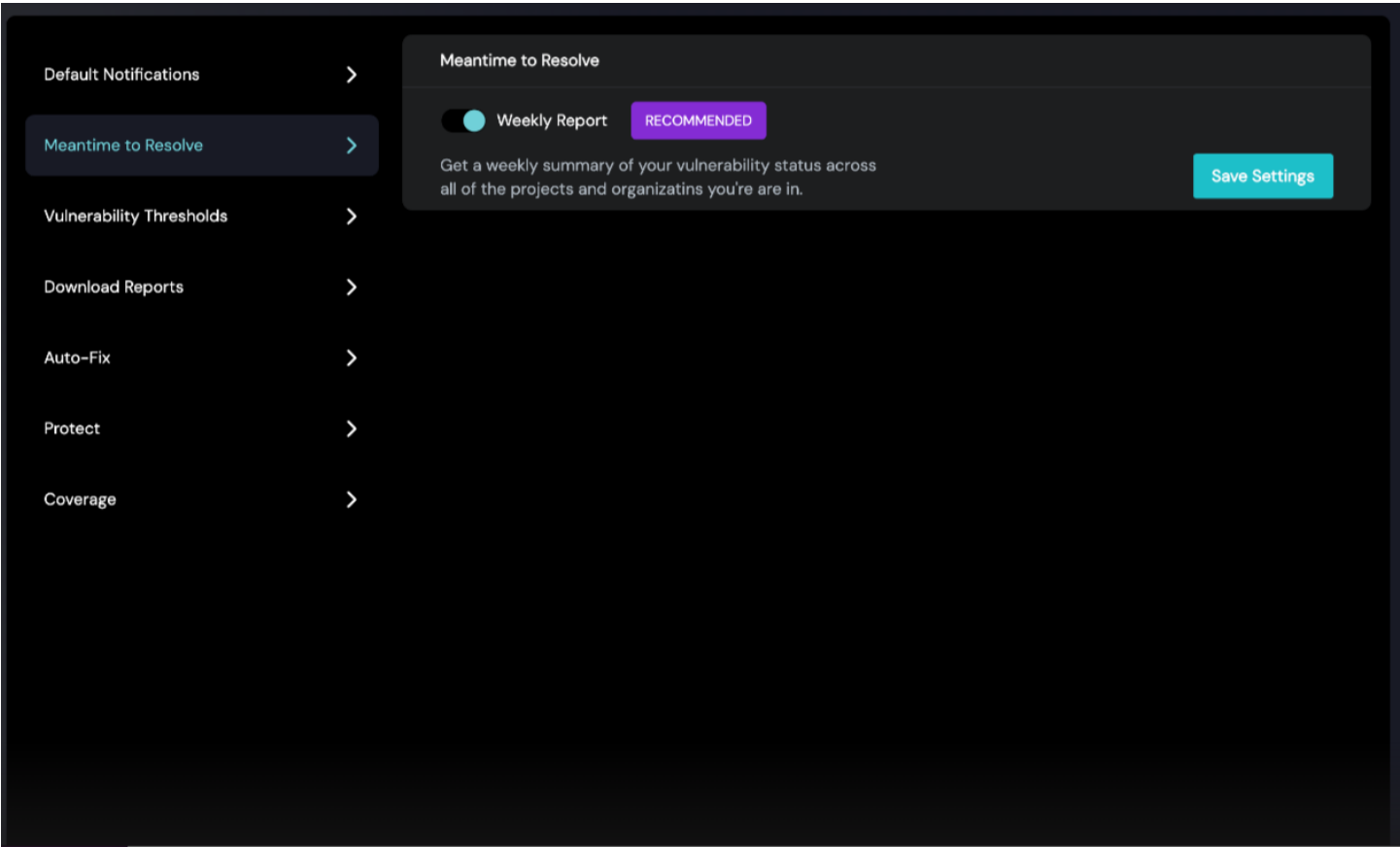
PostureScoreGrade

TopBottomActivity

SLAViolations

ProductionReadiness

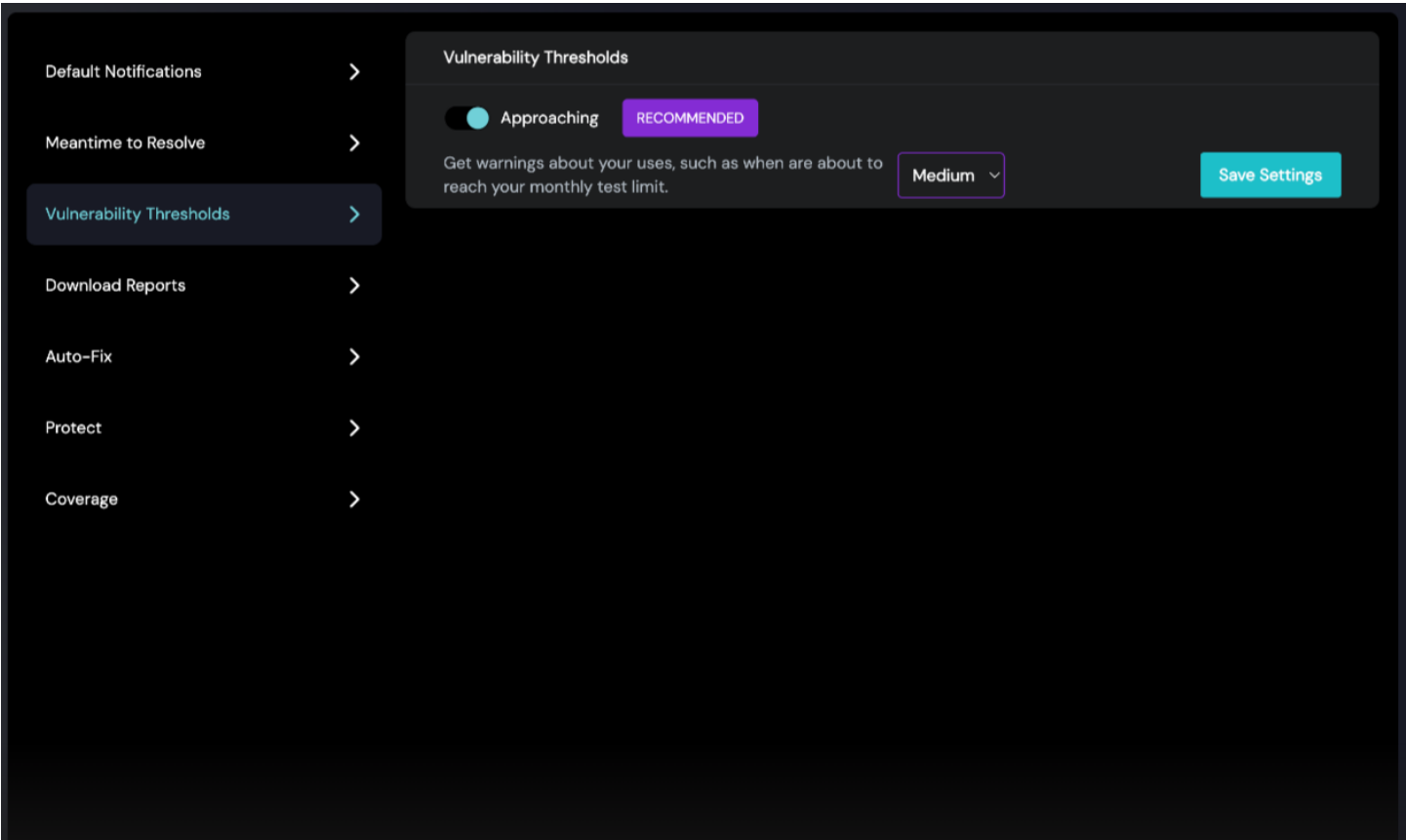
DeveloperSecurity



Meantime to Resolve:

Weekly Report

Save Settings



Vulnerability Thresholds:

Approaching

Severity:

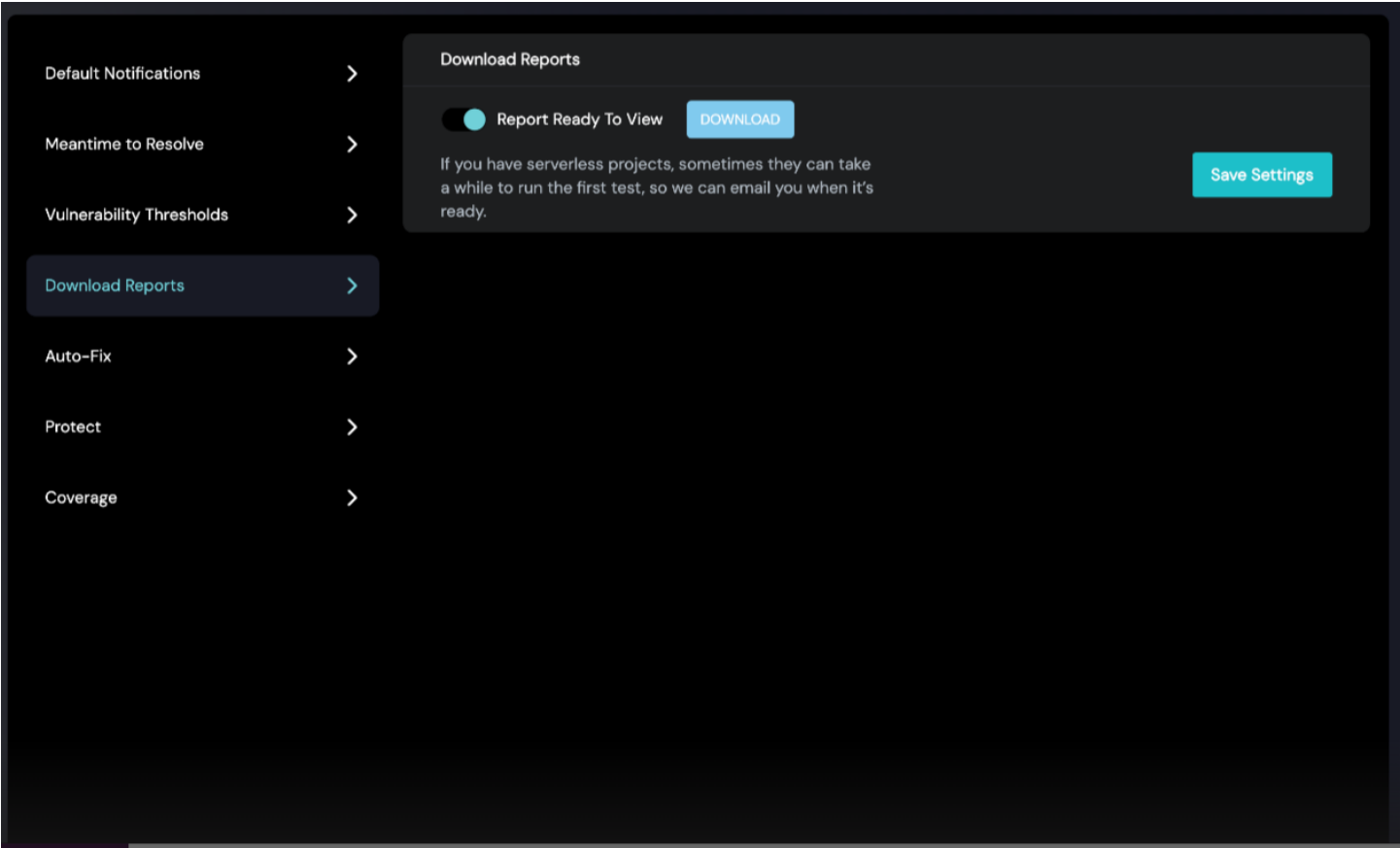
Critical

High

Medium

Low

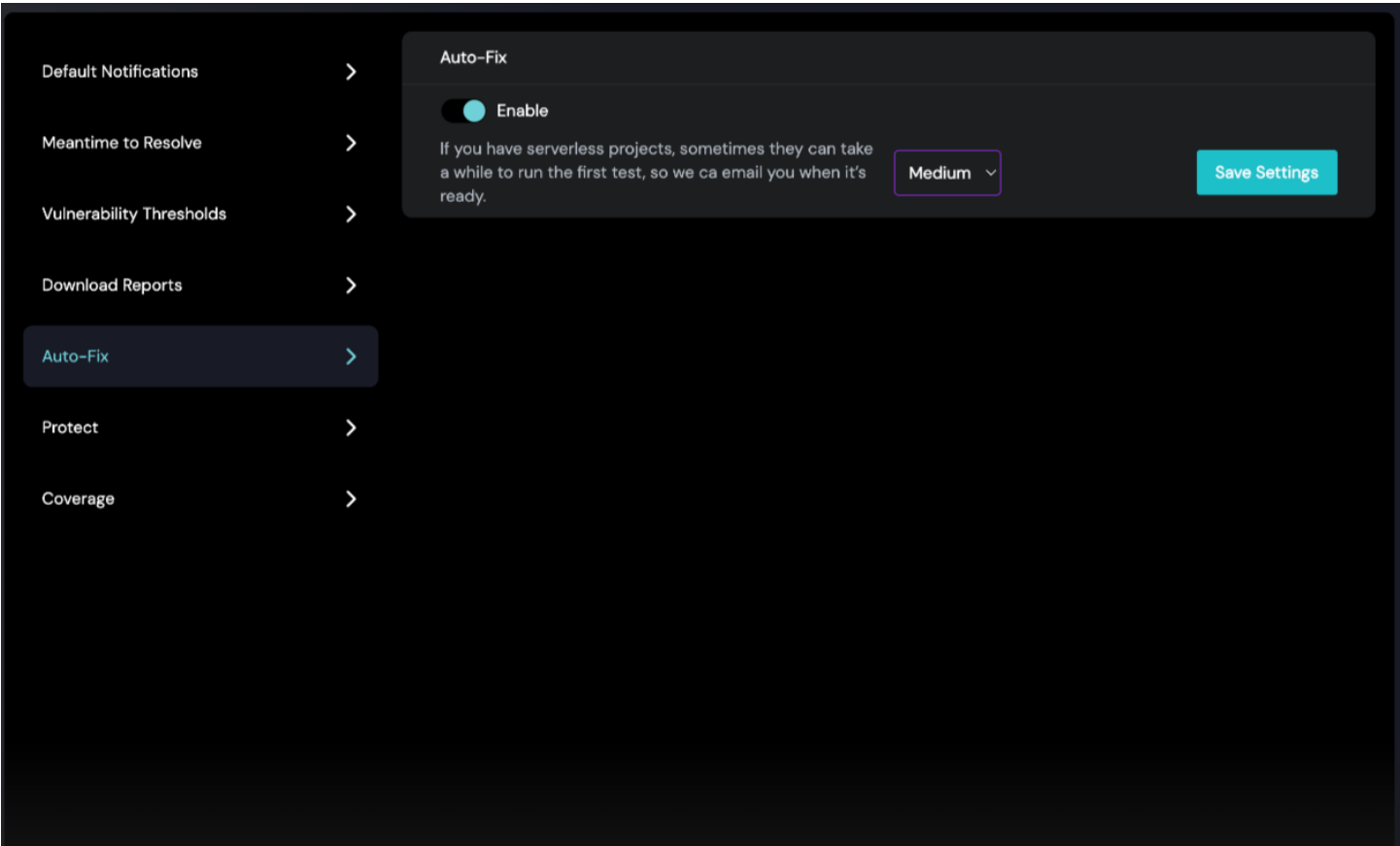
Save Settings



Download Reports:

Report Ready To View

Save Settings



Auto-Fix:

Enable

Severity:

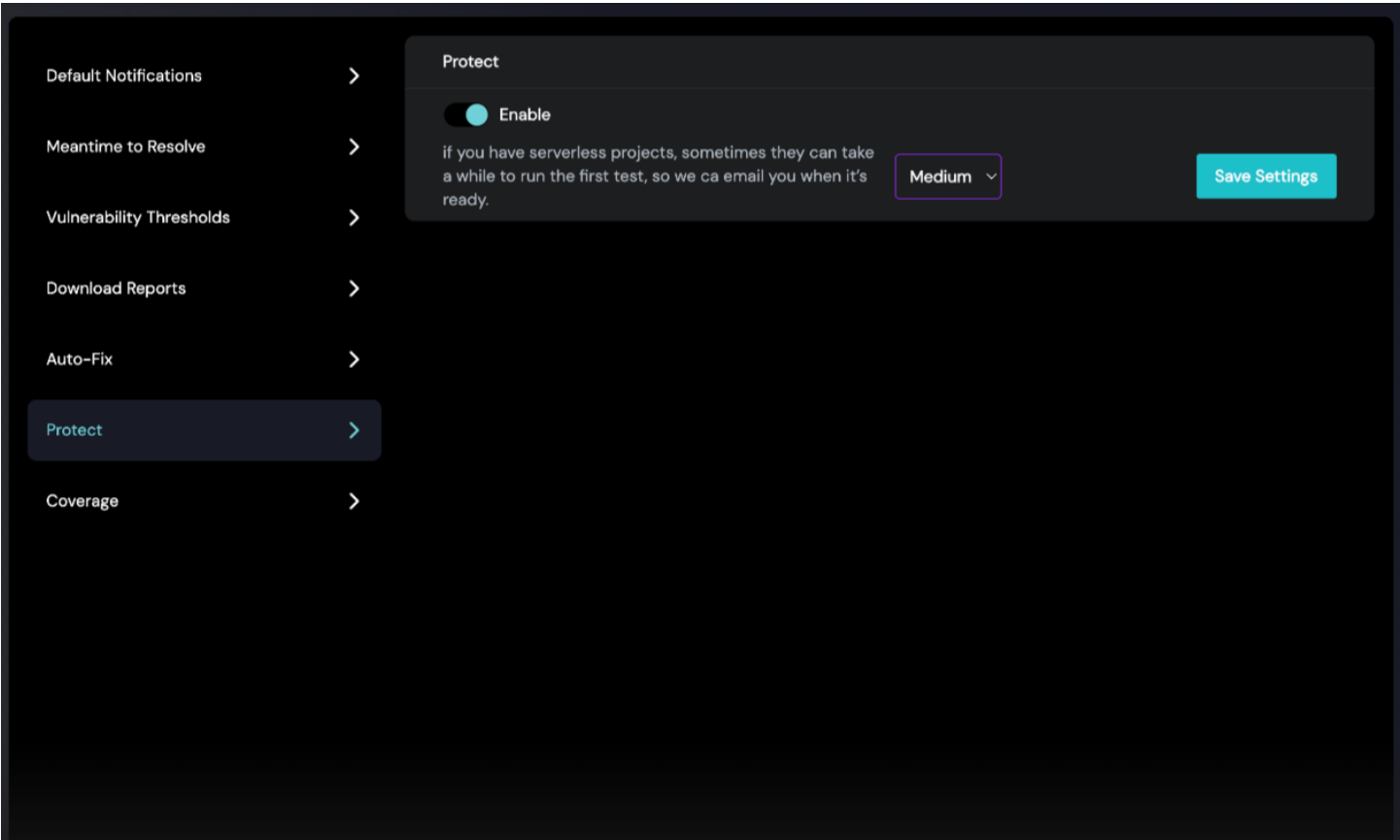
Critical

High

Medium

Low

Save Settings



Protect:

Enable

Severity:

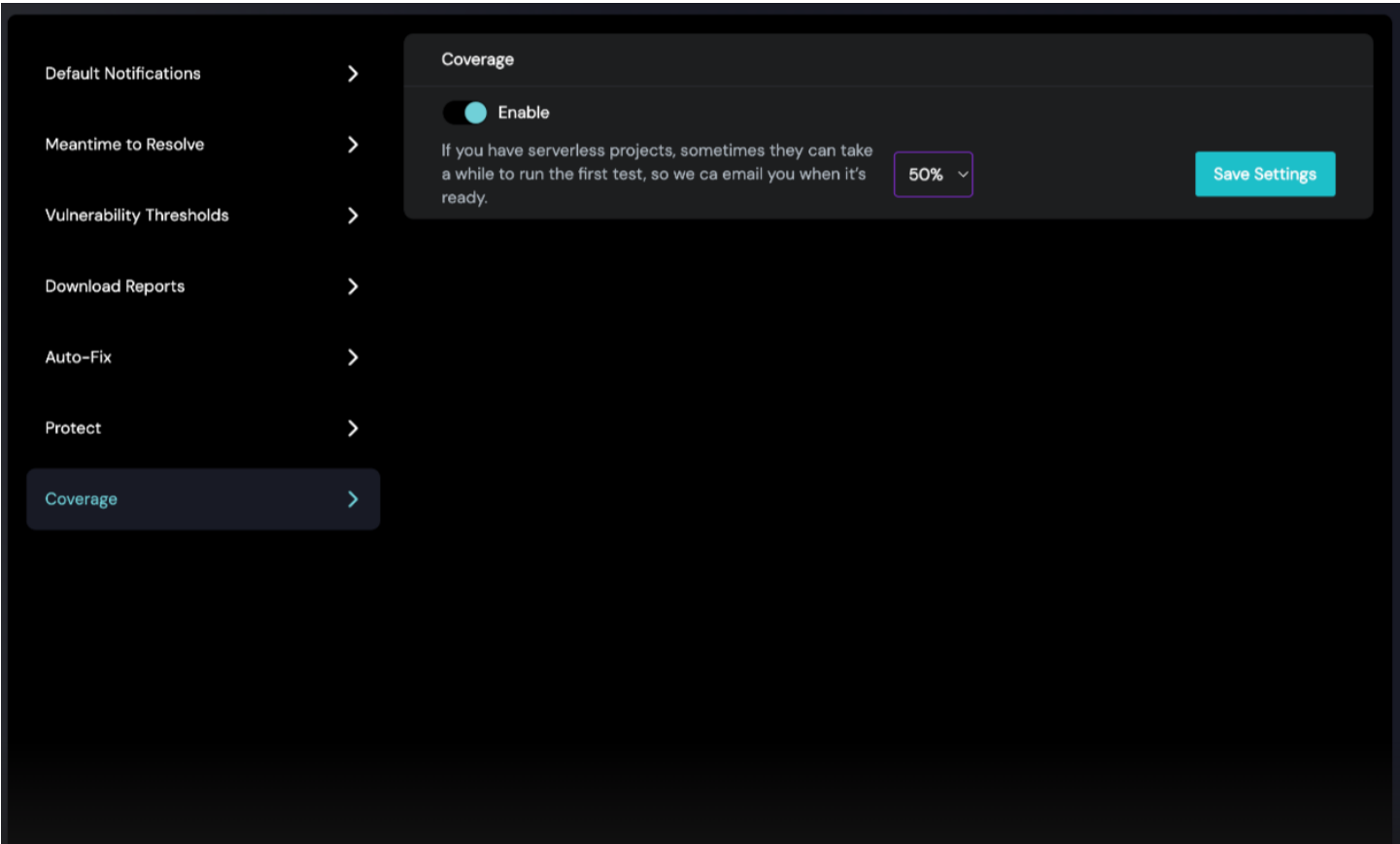
Critical

High

Medium

Low

Save Settings



Coverage:

Enable

Percent:

25%

50%

75%

Save Settings