



CUSTOMIZABLE AND FLEXIBLE RISK SCORING

Tech Brief

Most enterprises are faced with the challenge of deciding how to take action on thousands, if not millions, of vulnerabilities in their environment. Often, they'll utilize scoring systems that assign severity ratings to help them decide which vulnerabilities to fix first.

However, many of these systems — and the vulnerability management tools that rely on them — are taking a one-size-fits all approach. The ratings only consider a limited number of factors and do not take into account the unique factors within the organization, such as a vulnerable asset's importance or its exposure within the infrastructure.

Skybox® Security provides a flexible and comprehensive risk scoring method in Skybox® Vulnerability Control that takes into consideration a broad range of risk factors, both from within and outside the organization. This method enables users to identify and prioritize the riskiest assets and vulnerabilities in their organization, and quickly make the best remediation decisions.

Skybox calculates risk for the following entities:

- Vulnerability Occurrences
- Vulnerability Definitions
- Assets
- Asset Groups
- Business Asset Groups
- Business Units
- Networks
- Locations
- Virtual Domains



How it Works

To address the unique needs of each organization, the Skybox risk scoring methodology supports formula flexibility. Each organization can determine which factors such as exposure, exploitability, CVSS and asset importance — along with their respective weight — will be included in the risk formula.

Determining a risk for an entity (i.e., a vulnerability occurrence or asset) depends on two core elements:

1. **Vulnerability rating or asset vulnerability rating:** the technical severity index of the entity that reflects the likelihood of damage to the organization
2. **Asset importance:** the asset's value to the organization

Exposed vulnerabilities will be highlighted and receive a higher risk score. The exposure indication is also available for assets, so that users will be able to identify the assets most likely to be compromised in an attack.

Users will also be able to use risk scores to identify the riskiest asset groups in the organization. This will enable them to examine the riskiest groups first and remediate the assets in those groups.

BENEFITS OF SKYBOX'S RISK SCORING METHOD

- Easy-to-understand scoring method to support risk-based vulnerability management
- Risk analysis from multiple perspectives of vulnerabilities, assets and groups
- Focused attention exposed and exploitable vulnerabilities

Definitions in Skybox Risk Scoring

- **Vulnerability definition:** a unique vulnerability type, including a CVE number, CVSS score, and additional information
- **Vulnerability occurrence:** a specific instance of a vulnerability definition on an asset in your organization
- **Asset importance:** a score from 1-5 that reflects how important an asset is to the organization; the organization can change the asset importance range and the default asset importance value (this is one factor of the risk score for the vulnerability occurrence or asset)
- **Vulnerability rating:** a technical severity score from 0-10 for vulnerability occurrences that takes into consideration (by default) the exposure, exploitability level and the CVSS score; the user has four options for how this will be calculated (see formula flexibility below; the vulnerability rating is one argument of the vulnerability occurrence risk score equation)
- **Asset vulnerability rating:** a technical severity score from 0-10 for assets that takes into consideration the sum of weighted vulnerability ratings for all the vulnerability occurrences on the asset, or the maximum vulnerability rating of all the vulnerability occurrences on the asset
- **Vulnerability occurrence risk score:** The risk score from 0-100 for a vulnerability occurrence; basically, this score is calculated by the vulnerability rating times the asset importance

- **Vulnerability definition risk score:** the sum of the risk scores of all vulnerability occurrences of a vulnerability definition
- **Asset risk score:** the risk score from 0-100 for an asset which takes into consideration both the number of vulnerability occurrences on the asset and their severity

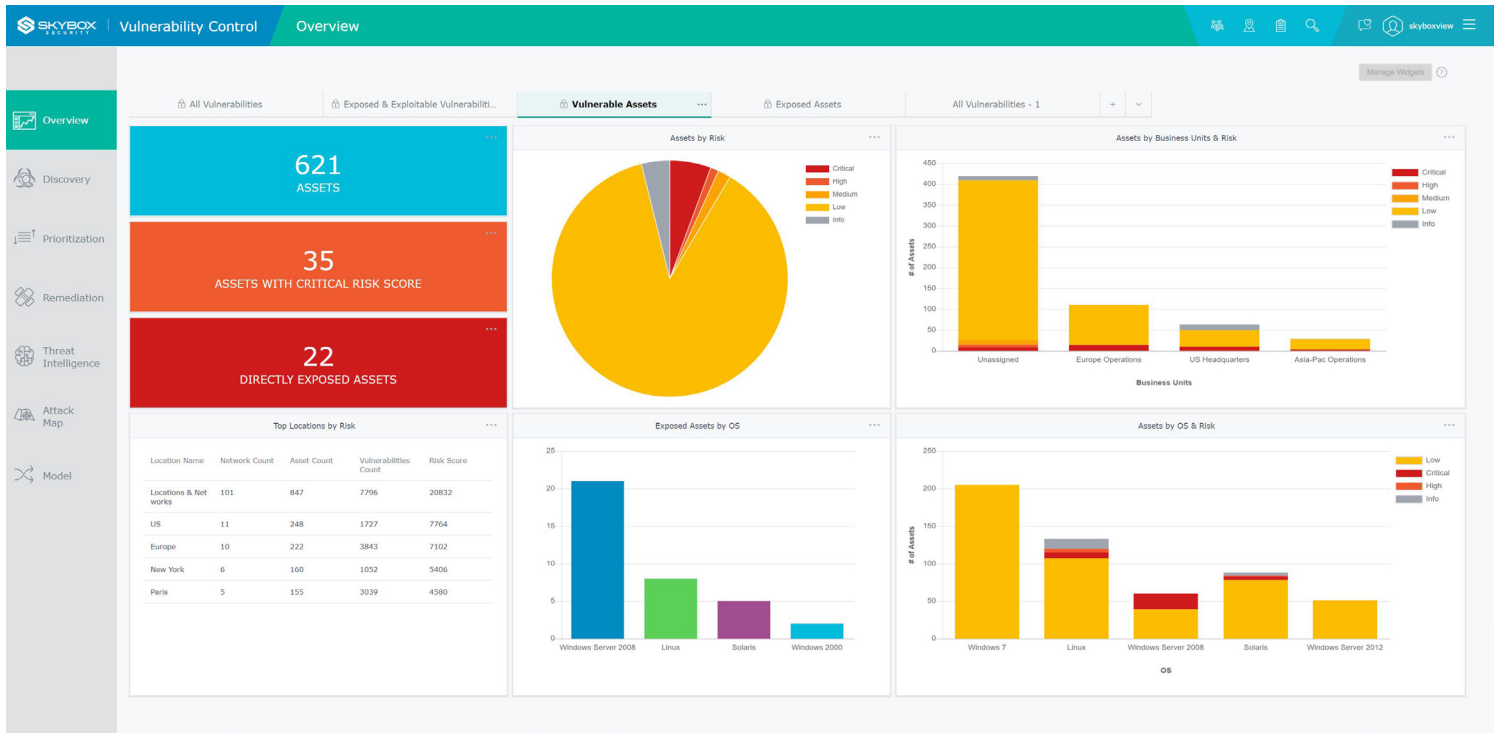


FIG 1: An overview dashboard of Vulnerability Control highlighting assets with a critical risk score and directly exposed. Users can quickly go from high-level overviews to detailed insight to understand what's driving risk.

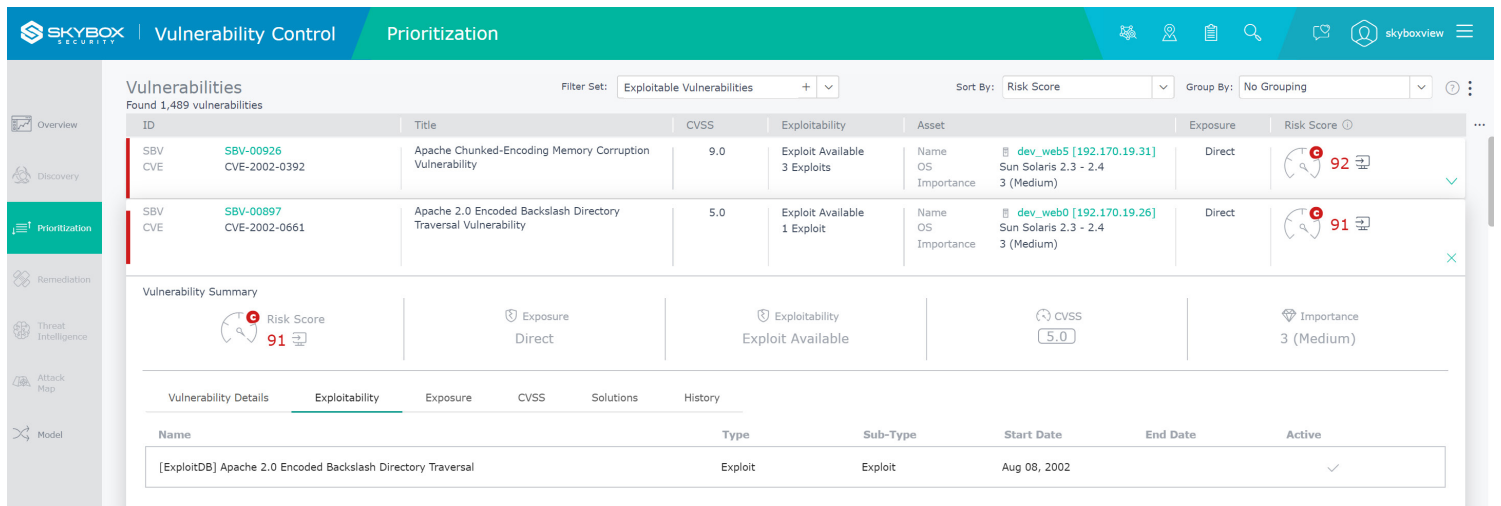


FIG 2: In Vulnerability Control's Prioritization module, users can dive deep into details on vulnerabilities, assets and groups. This view is displaying vulnerabilities with an available exploit ranked by risk score and the summary of CVE-2002-0661.



With Skybox, all entities can have a straightforward and trackable risk score: vulnerability occurrences, vulnerability definitions, assets, asset groups, business asset groups, business units, networks, locations and more.

To learn more about Skybox risk scores in Vulnerability Control and how you can take a simplified, risk-based approach to vulnerability management, [visit our website](#) or [schedule a demo](#) today.



About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with over 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060

Copyright © 2019 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners. 08272019