# Vulnerability Management

## Agent-Based Vulnerability Detection

The platform provides **comprehensive vulnerability analysis** based on operating system and package information collected from deployed agents.

### Data Collection

- Agents gather detailed information about the host's operating system, installed packages, and configurations.
- This data is continuously collected and sent to the central platform for analysis.

### Vulnerability Analysis

- The collected information is correlated with up-to-date vulnerability databases.
- The platform identifies potential vulnerabilities by comparing installed software versions against known vulnerabilities.

### Real-Time Detection

- Agents continuously monitor and report changes, enabling real-time detection of new vulnerabilities.
- This allows for rapid identification of security risks introduced by system updates or new software installations.

### Comprehensive Coverage

- The agent-based approach enables deep scanning of endpoints, including those that may be difficult to assess with network-based scans.
- It provides visibility into vulnerabilities across a diverse range of operating systems and software packages.

### Efficient Processing

- By leveraging agent-collected data, the platform performs vulnerability assessments more efficiently than traditional network-based scans.
- This approach reduces network overhead and allows for more frequent vulnerability checks.

By utilizing this agent-based vulnerability detection method, the platform offers organizations a powerful tool for maintaining a robust security posture and quickly identifying potential threats.

---

# SBOM (Software Bill of Materials) Analysis

The platform provides **advanced SBOM analysis capabilities**, leveraging agent-based systems to generate and analyze comprehensive software component inventories.

## SBOM Generation

- **File System Scanning**: Agents perform thorough scans of file systems to identify and catalog software components.
- **Container Image Analysis**: The system examines container images to extract detailed component information.
- **CycloneDX Format**: SBOMs are generated in the **industry-standard CycloneDX format**, ensuring compatibility and ease of integration.

## Vulnerability Identification

- **Component Analysis**: Each identified software component is scrutinized for known vulnerabilities.
- **Continuous Monitoring**: The system regularly updates its vulnerability database to provide current security insights.
- **Risk Assessment**: Vulnerabilities are prioritized based on severity and potential impact.

## Comprehensive Reporting

- **Detailed Inventories**: Customers receive **comprehensive lists of all software components** in their systems.
- **Vulnerability Reports**: The platform provides **detailed reports** on identified vulnerabilities associated with SBOM components.
- **Actionable Insights**: Reports include recommendations for **remediation and risk mitigation**.

## Integration and Automation

- **CI/CD Pipeline Integration**: SBOM generation and analysis can be integrated into **continuous integration and deployment (CI/CD) processes**.
- **Automated Alerts**: The system can be configured to **send alerts** when critical vulnerabilities are detected in SBOM components.

By utilizing **SBOM analysis**, customers gain **deep visibility into their software supply chain**, proactively identify security risks, and maintain a **robust security posture** across their IT infrastructure.

---

# Remote Vulnerability Analysis

The platform offers **comprehensive remote vulnerability analysis**, focusing on two key areas:

## Public IP Asset Discovery

The system performs thorough scans of **customer public IP ranges** to identify exposed assets.

- Utilizes **advanced IP range detection techniques** to accurately determine the customer's public IP address blocks.
- Employs **network scanning tools** to discover active hosts and services within these IP ranges.
- Identifies and catalogs **internet-facing assets** such as web servers, databases, and other network services.
- Provides a **detailed inventory** of exposed assets, including IP addresses, hostnames, and open ports.

## Automated HTTPS URL Vulnerability Assessment

The platform conducts **automated security scans** on HTTPS URLs to detect vulnerabilities.

- **Comprehensive web application vulnerability scans** on discovered HTTPS endpoints.
- Utilizes a combination of **passive and active scanning techniques** to minimize impact on target systems.
- **Assess SSL/TLS configurations** for potential weaknesses.
- Checks for **common misconfigurations** in web servers and application frameworks.
- Generates **detailed reports** highlighting discovered vulnerabilities, severity levels, and recommended remediation steps.

This approach enables organizations to **proactively identify and address security weaknesses** in their internet-facing infrastructure, significantly enhancing their **overall security posture**.

---

Revision #1
Created 30 March 2025 06:09:31 by Bryan
Updated 30 March 2025 06:15:05 by Bryan