Cyber Observer and Tenable.sc™ Integration
Unified access control management and awareness

Challenge
Today’s challenging cybersecurity landscape offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so have the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, despite enterprises and organizations worldwide spending more money than ever on new technologies and solutions.

Designed for CISOs and senior InfoSec managers (such as CIOs, C-level managers, risk officers, SOC managers and IT Infrastructure personnel), Cyber Observer empowers leadership with a unified dashboard of their entire cybersecurity ecosystem. Cyber Observer can be fully deployed within an enterprise in a few hours, enabling easy identification of weaknesses, reduction of mean-time-to-detect (MTTD), prevention of breaches, and advancement of your organization’s cybersecurity posture and maturity.

Solution
Cyber Observer’s partnership with Tenable enables CISOs to better manage their cybersecurity ecosystem. They receive alerts from Cyber Observer on the key aspects and issues in Tenable.sc™ such as configuration, incident and investigation management, access control, password policies, user and role administration and more. This joint effort helps enterprises manage their cybersecurity environment and continuously monitor their cybersecurity ecosystem posture.

KEY FEATURES
- Identifies cybersecurity tools that are misconfigured, malfunctioning, or missing
- Finds security gaps and provides recommendations for fixing
- Builds an ongoing security program to ensure alignment with new threats
- Uses continuous analytics to send alerts when there are deviations from normal behavior
- Automatic reporting
The integration between Cyber Observer and Tenable offers CxOs powerful and effective resilience visibility along with compliance validation and controls, to secure and monitor Tenable.sc™ in an unprecedented manner.

Cyber Observer deploys to the corporate network automatically, in a matter of a few hours, predefined with security domains and CSC measurements to deliver three unique cybersecurity ecosystem views:

- First, it provides organizations with the best indicators of the cybersecurity tools that may be misconfigured, malfunctioning, or missing and should be added to provide complete cybersecurity protection.
- It then reveals the security gaps that exist in each security domain and delivers continuous proactive recommendations to close these gaps.
- Finally, Cyber Observer’s machine learning analytics engine continuously calculates online measurements that represent normal behavior, and then alerts when a deviation from normal behavior is detected.

Fast and Secure Deployment

The Cyber Observer connector for Tenable receives security and configuration data from the Tenable server via a secure REST API.
Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting for Managers:**
  Alerts and reporting regarding current configuration implementation status based on vendors’ and security standards best-practices, including security configuration issues, incidents and investigations management, admins and roles administration, and more.

- **Reduced Incident Analysis Time:**
  Cyber Observer provides continuous alerts on deviation from normal behavior in terms of Tenable implementation and effectiveness as well as continuous monitoring of relevant security issues in near real-time.

- **Continuous Incident Response:**
  Provides the CISO and other relevant managers in the organization, as well as the Tenable.sc™ technical owners with continuous mitigation recommendations and steps to improve, for securing and monitoring Tenable implementation, effectiveness, maturity and resilience from a management perspective in an unprecedented manner.

- **Customizable Views and Reports**
  Cyber Observer is highly customizable – all views and reports could be modified to the organization’s needs and structure. The integration between Cyber Observer and Tenable offers CxOs powerful effectiveness and resilience visibility, as well as compliance validation and controls.

### Key Use Cases

1. **Immediate alerts and detailed information regarding critical and high severity vulnerabilities**
   - Number of exploitable vulnerabilities found
   - Number of mitigated vulnerabilities found
   - Number of critical-risk vulnerabilities found on more than X hosts
   - Number of high-risk vulnerabilities found on more than X hosts

2. **Immediate alerts and detailed information regarding vulnerable hosts**
   - Number of hosts with critical severity found in vulnerability overview with more than X vulnerabilities
   - Number of hosts with high severity found in vulnerability overview with more than X vulnerabilities
   - Number of hosts with exploitable vulnerabilities
   - Number of hosts with mitigated vulnerabilities

3. **Detailed information regarding scans issues and users and roles management**
   - Number of hosts not scanned in the last X days
   - Tenable.sc™ last scan is older than X days
   - Number of Users Roles defined
   - Number of Users with more than X Roles defined
   - Number of Groups defined

### About Tenable

**Tenable®, Inc.** (NASDAQ: TENB) is a Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world’s first platform to see and secure any digital asset on any computing platform. Learn more at [tenable.com](http://tenable.com).

### About Cyber Observer

**Cyber Observer** is the premier critical controls monitoring (CCM) solution that simplifies the way cybersecurity tools are monitored and managed. Cyber Observer integrates hundreds of popular cybersecurity tools into a single intuitive interface that enables security and risk management executives to continuously monitor their security tools and improve their cybersecurity posture in alignment with cybersecurity, business, and regulatory frameworks. Learn more at [cyber-observer.com](http://cyber-observer.com).