Cyber Observer Technology Partners

Solution Brief

Cyber Observer and Cisco ISE 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 Cisco enables CISOs to better manage their cybersecurity ecosystem. They receive alerts from Cyber Observer on the key aspects and issues in Cisco ISE 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

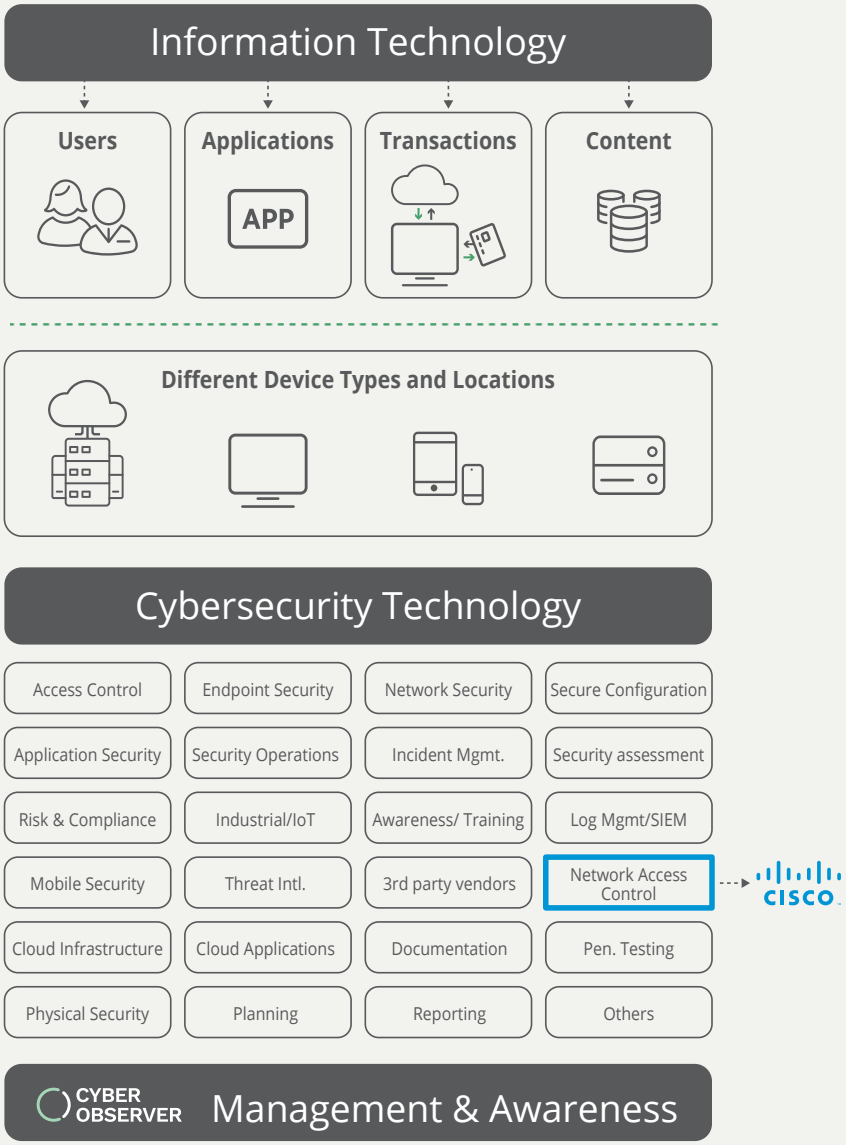
The integration between Cyber Observer and Cisco offers CxOs powerful and effective **resilience visibility** along with **compliance validation** and **controls**, to secure and monitor CISCO ISE in an unprecedented manner.

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 CISCO ISE receives security and configuration data from the Cisco server via a secure REST API.



Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting for Managers:**
  Alerts and reporting regarding Cisco ISE 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 Cisco ISE 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 Cisco ISE technical owners with continuous mitigation recommendations and steps to improve, for securing and monitoring Cisco ISE 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 Cisco ISE offers CxOs powerful effectiveness and resilience visibility, as well as compliance validation and controls.

Key Use Cases

1 Immediate alerts and detailed information regarding endpoints, network devices and high severity alarms

- High-risk severity alarms triggered
- Non-compliant endpoints found
- Endpoints denied access
- Network devices added
- Network devices changed
- Network devices configured with insecure protocols

2 Detailed configuration information regarding policies and insecure protocols and cyphers settings

- Policy changes
- Policies added and removed
- Policy set without denying all authentication last rule
- Legacy TLS renegotiation status
- Insecure TLS version status
- Insecure cypher status
- Repeated failed client policies

3 Detailed information regarding admin users, password policies, licenses and certificates statuses

- Super Admin members
- Network Device Admin members
- Administrator login failure details
- Administrator minimum password length
- License expiry status
- License compliance status
- System certificates expiry status
- Trusted certificates expiry status

About CISCO

Cisco Systems, Inc. (NASDAQ: CSCO) designs, manufactures and sells Internet Protocol (IP)-based networking and other products related to the communications and information technology (IT) industry and provide services associated with these products and their use. The company provides products for transporting data, voice, and video within buildings, across campuses, and globally.

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**.