# **SKYWATCH BEGINSExternal Continuous Threat Exposure Management (CTEM) Solution**

**March 2025**

## ****Executive Summary****

Organizations today face **continuous exposure to external cyber threats**, but many lack the **visibility, intelligence, and structured processes** necessary to **proactively assess, prioritize, and mitigate these risks**. Traditional security solutions primarily focus on **protection and incident response**, leaving a critical gap in **managing risk exposure before it escalates into a security breach**.

**SKYWATCH BEGINS** is designed to **bridge this gap** by providing a **proactive External Continuous Threat Exposure Management (CTEM) solution**. It offers **continuous visibility, security validation, operational efficiency tracking, and risk reduction**, ensuring that organizations can **identify, assess, and manage external cyber risks before they become incidents**.

## ****The Need for SKYWATCH BEGINS****

### ****Key Cybersecurity Challenges:****

1. **Lack of Continuous Visibility into External Threats**
	* Organizations struggle to maintain a **real-time view** of their **Internet-facing assets, vulnerabilities, and risks**.
	* Without proper **asset discovery and inventory management**, security teams are unaware of what is **exposed** and how it might be exploited.
2. **Inefficient or Nonexistent Continuous Testing & Validation**
	* Most organizations rely on **point-in-time penetration testing**, leaving **gaps in security** between assessments.
	* **False positives and unvalidated vulnerabilities** create unnecessary noise, slowing down response times.
	* There is **no structured prioritization**, leaving organizations exposed to critical vulnerabilities.
3. **Security Controls Are in Place but Often Ineffective**
	* Investments in security tools do not guarantee **effective protection**.
	* Without **ongoing security validation**, organizations cannot confirm if their controls are working.
4. **Slow and Unstructured Remediation Processes**
	* **Vulnerability remediation lacks prioritization**, leading to inefficiencies.
	* **Siloed IT and security teams** cause delays and miscommunication.
	* **Lack of remediation tracking and verification** results in unresolved vulnerabilities.
5. **Cyber Risk Exposure Management Is Not an Operationalized Process**
	* Organizations often lack a **structured, continuous approach** to managing external exposure.
	* Security teams operate **reactively**, responding to threats instead of **proactively managing risk exposure**.
	* Without **operational efficiency tracking**, security resources are wasted, and team performance is not optimized.

## ****How SKYWATCH BEGINS Solves These Challenges****

### ****Comprehensive Threat Exposure Management****

SKYWATCH BEGINS provides an integrated **visibility, action, and operational efficiency** approach to external threat exposure management.

1. **Visibility**
	* A **suite of executive and technical dashboards** offering real-time insights.
	* **On-demand and curated reporting** for security and compliance needs.
	* **Device-Centric Model** integrating:
		+ **Inventory tracking** of all Internet-facing assets.
		+ **Asset fingerprinting** for in-depth understanding.
		+ **Visibility into applications, vulnerabilities, threats, and risks**.
		+ **Hardening recommendations** to enhance security posture.
2. **Action**
	* **External vulnerability assessments, penetration testing, and security control validation**.
	* **False positive elimination, prioritization, and remediation planning**.
	* **Support for remediation** while the client executes fixes, followed by verification.
3. **Operational Efficiency**
	* **Continuous monitoring of security team performance and workload distribution**.
	* **Kanban-based remediation tracking**, identifying bottlenecks and optimizing workflows.
	* **Structured vulnerability lifecycle management** from detection to verification.

## ****Services Included in SKYWATCH BEGINS****

1. **MSS-CSO (SKYWATCH Platform Service)**
	* Centralized platform for **cybersecurity oversight and operational efficiency tracking**.
	* Implements the **Device-Centric Model** for comprehensive asset risk management.
	* **NIST-based security and risk management frameworks** for structured compliance.
2. **MSS-VME-ADV** (Vulnerability Management & Exploitation - Advanced)
	* **External: asset discovery, vulnerability scanning, port monitoring, and penetration testing**.
	* **Continuous assessment** of Internet-facing risks and structured remediation support.
3. **MSS-CSME** (Network Monitoring for Availability & Performance)
	* **Non-security service** that ensures uptime and performance of **Internet-facing perimeter and cloud systems**.
4. **MSS-TAS** (Multifactor Authentication Service)
	* Adds **additional authentication layers** to enhance security and can be used for numerous other applications, provides self-service capability and can scale-up to a full zero-tolerance solution for all organizational applications and systems.
5. **MSS-BAS** (Basic Security Control Assessment & Remediation Support)
	* Evaluates **effectiveness of security controls** and provides structured **remediation handling** for web-gateway, endpoint and email attack vectors. Can scale-up to many other attack vector validations.
6. **MSS-INT** (Actionable Threat Intelligence Service)
	* Real-time **threat intelligence** for proactive mitigation of risks.
	* Attack surface analysis to **identify and address external risks** before exploitation.
	* Actionable, provide actual penetration using Breach & Attack Simulation techniques.

## ****Key Value Proposition****

✔ **Continuous visibility** through real-time dashboards, reporting, and asset tracking.
✔ **Device-Centric Model** providing deep asset-level insights, including applications, vulnerabilities, threats, and risks.
✔ **Operational efficiency tracking**, ensuring remediation workflows are streamlined.
✔ **NIST-based security and risk management**, ensuring compliance and risk mitigation.
✔ **Actionable threat intelligence**, helping organizations anticipate cyber risks.
✔ **End-to-end vulnerability lifecycle management**, from discovery to resolution.
✔ **Performance monitoring** for external-facing systems.

## ****Why Choose SKYWATCH BEGINS?****

**Security isn’t just about protection—it’s about managing exposure before threats cause damage.**

* **Without visibility, you can’t protect what you don’t see.**
* **Without validation, you don’t know if your defenses work.**
* **Without prioritization, remediation efforts become inefficient.**

**SKYWATCH BEGINS helps organizations transition from reactive security to proactive exposure management.** It provides the necessary **visibility, structured processes, and intelligence-driven insights** to **reduce risk before exploitation occurs**.