MSS-EASM Dashboard Manual Page

SKYWATCH OS Operational Dashboard Guide

June 14, 2026

Purpose: This manual page provides operational guidance for the MSS-EASM dashboards inside SKYWATCH OS. The objective is to help users understand the purpose of each dashboard, interpret key indicators, and use the information operationally to reduce the externally exposed attack surface of the organization.

Overview Dashboard – External Exposure Command View

Widget	What It Shows	How to Use It	Operational Value
New Exposures Since Last Scan	New externally visible exposures detected.	Investigate immediately when greater than zero.	Detects newly introduced external risk.
High-Risk Exposures	Critical or high-risk externally visible findings.	Prioritize investigations and remediation activities.	Focuses attention on highest-risk exposure.
Business-Critical Assets Exposed	Critical systems with externally visible exposure.	Escalate quickly due to business impact.	Aligns exposure with operational importance.
Exposure Trend	Whether exposure posture is improving or degrading.	Review weekly and monthly.	Measures exposure reduction effectiveness.
Top Immediate Actions	Prioritized operational recommendations.	Use as operational starting point.	Converts telemetry into action.
External Exposure Index (EEI)	Weighted exposure posture score.	Use as executive exposure indicator.	Simplifies posture understanding.

LATAM HQ +507 836-5355
US HQ +1 (321) 430-0500

History Dashboard – Delta and Trend Intelligence

Widget / View	What It Shows	Operational Use
Vulnerable Host History	Trend of externally vulnerable hosts.	Validate remediation effectiveness over time.
Vulnerability Severity History	Trend of critical, high, medium, and low findings.	Identify severity spikes and exposure growth.
Discovered Host History	Trend of externally discovered systems.	Detect scope expansion and unmanaged growth.
Exposure Comparison	Current vs previous period exposure.	Identify regression or improvement.

Externally Accessible Services Dashboard

Field	Meaning	Operational Use
IP / Hostname	Externally visible system.	Identify affected asset and owner.
Port / Service	Service exposed to the Internet.	Determine if exposure is necessary.
Risk Level	Risk classification of exposed service.	Prioritize risky administrative or database services.
Expected	Whether the service is approved in DCM.	Unexpected exposure should be reviewed immediately.
Owner	Mapped system owner or service owner.	Assign remediation responsibility.
Internet Reachable	External reachability classification.	Validate real exposure context.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

External Risk Register

Column / Concept	Meaning	Operational Use
Severity	Technical vulnerability severity.	Use as part of prioritization.
Priority / Criticality	Business importance of affected asset.	Escalate critical business systems.
Unexpected Service?	Unauthorized exposed service detected.	Investigate immediately.
Available Exploit	Known exploit availability.	Prioritize exploitable vulnerabilities.
Exposure Age	How long exposure has remained visible.	Track unresolved risk and remediation delays.
Remediation	Recommended corrective action.	Guide operational remediation.

DNS Intelligence Dashboard

Widget / View	What It Shows	Operational Use
Apex Domains	Observed domains in monitored scope.	Validate domain inventory.
New Subdomains	Recently discovered subdomains.	Review for authorized deployment or shadow IT.
Hosting Providers	Hosting / ASN visibility.	Detect hosting sprawl and third-party exposure.
DNS Discovery Timeline	Timeline of discovered subdomains.	Identify unexpected DNS growth.
DNS Inventory	Detailed DNS inventory table.	Investigate shadow or third-party assets.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Operational Conditions Monitored by MSS-EASM

Condition	What It Detects	Client Value
External Baseline Changes	Approved external assets or services change unexpectedly	Detects drift from approved architecture
New External Assets	Previously unknown Internet-visible assets	Identifies shadow IT and unmanaged exposure
DNS Exposure Conditions	DNS issues that may increase risk or create operational concerns	Reduces DNS-driven exposure
Unauthorized Service Exposure	Unexpected externally accessible services or ports	Supports hardening validation and attack surface reduction
Certificate & TLS Issues	SSL/TLS weaknesses, mismatches, or expiration conditions	Maintains secure external access
Application Exposure Conditions	Externally visible applications or application-layer findings	Improves application governance and visibility
Shadow Assets	Assets outside the approved inventory	Improves accountability and exposure governance

Operational Objective

The objective of MSS-EASM is not simply to monitor exposure. The objective is to continuously reduce the externally exposed attack surface of the organization through visibility, governance, hardening validation, remediation tracking and governance workflows, and operational accountability.

LATAM HQ +507 836-5355
US HQ +1 (321) 430-0500