Slack / Microsoft Teams Notifications

AiVRIC integrates with **Slack** and **Microsoft Teams** using incoming webhooks to deliver real-time security visibility directly into collaboration channels. These integrations are designed for **alerting, triage, and operational awareness**, not bidirectional response or remediation.

Overview

Slack and Microsoft Teams integrations allow you to:

- Receive **real-time security findings**
- Send **scan summary notifications**
- Filter notifications by **severity threshold**
- Route alerts to **specific team channels**
- Reduce mean time to awareness for misconfigurations and risk exposure

These integrations are **one-way (AiVRIC → Slack/Teams)** and are intended for notification and visibility, not command execution or data ingestion back into AiVRIC.

Supported Capabilities

✅ Incoming webhook delivery
✅ Channel-based routing
✅ Configurable severity thresholds
✅ Optional scan summary notifications
✅ Near real-time alert delivery

Slack Integration

Prerequisites

- Slack workspace admin permissions
- Ability to create **Incoming Webhooks**
- Target Slack channel (e.g., #security-alerts)

Configuration Steps

1. Navigate to **Configuration → Integrations → Slack**
2. Click **Add Integration**
3. Create an **Incoming Webhook** in Slack and copy the Webhook URL
4. In AiVRIC, enter:
    - **Webhook URL**
    - **Channel Name** (e.g., #security-alerts)
5. (Optional) Enable **Send Scan Summary**
6. Select a **Severity Threshold**:
    - Only findings at or above this severity will be sent
7. Click **Create Integration**

Notification Behavior

- Individual security findings are posted as messages
- Findings below the configured severity are suppressed
- Scan summaries provide:
    - Total findings by severity
    - Scan completion status
    - Timestamp and account context

Microsoft Teams Integration

Prerequisites

- Microsoft Teams channel owner permissions
- Ability to create **Incoming Webhooks**
- Target Teams channel

Configuration Steps

1. Navigate to **Configuration → Integrations → Microsoft Teams**
2. Click **Add Integration**
3. Create an **Incoming Webhook** in the desired Teams channel
4. Copy the Webhook URL
5. In AiVRIC, paste the **Webhook URL**
6. (Optional) Enable **Send Scan Summary**
7. Select a **Severity Threshold**
8. Click **Create Integration**

Notification Behavior

- Alerts are delivered as channel messages
- Messages include:
    - Finding severity
    - Resource context
    - Scan source
- Scan summaries are posted after scan completion when enabled

---

Severity Thresholds

Severity thresholds act as a **noise-reduction control**.

Threshold	Result
Critical	Only Critical findings sent
High	High + Critical

Threshold	Result
Medium	Medium + High + Critical
Low	All findings

Best practice is to start at **Medium** and tighten over time.

Operational Use Cases

- 🚨 **Security Operations** – Immediate awareness of high-risk misconfigurations
- 📣 **Cloud Teams** – Visibility into scan results without platform login
- 🧭 **Leadership Channels** – High-level scan summaries only
- 🛠️ **DevOps** – Awareness without alert fatigue

Architectural Notes

- Integrations use **stateless HTTPS webhook delivery**
- No data is pulled from Slack or Teams into AiVRIC
- If a webhook is revoked or deleted, delivery will fail silently
- For **bidirectional workflows**, use:
  - ServiceNow SIR
  - Jira
  - REST API + automation

Limitations & Design Intent

AiVRIC's Slack and Teams integrations are intentionally **notification-only** to:

- Preserve least-privilege principles
- Avoid chat-based control paths for security tooling
- Ensure deterministic, auditable remediation via approved workflows

---

Summary

Slack and Microsoft Teams integrations provide **fast, low-friction visibility** into AiVRIC findings and scan outcomes. They are best used as **awareness and coordination channels**, while remediation and lifecycle management remain in AiVRIC or downstream ITSM/SOAR platforms.