Splunk & Microsoft Sentinel Integration Guide

Overview

AiVRIC integrates with **Splunk Enterprise / Splunk Enterprise Security** and **Microsoft Sentinel** to stream security findings in near real time to your centralized SIEM. This enables correlation, alerting, and response workflows using tools already operational within security and SOC teams.

This guide covers:

- Supported integrations
- Required prerequisites
- Step-by-step configuration in AiVRIC
- Where to locate required values in Splunk and Azure
- Validation and operational considerations

Supported Integrations

SIEM Platform	Integration Method	Delivery Type
Microsoft Sentinel	Azure Log Analytics Data Collector API	Custom Log Table
Splunk	HTTP Event Collector (HEC)	JSON Event Ingestion

General Prerequisites

Before configuring any SIEM integration, ensure:

- You have **Admin** or equivalent permissions in AiVRIC
- At least one cloud scan has completed successfully
- Network egress from AiVRIC to your SIEM endpoint is allowed
- TLS/SSL certificates are valid for the destination endpoint

Microsoft Sentinel Integration

What Gets Sent

AiVRIC forwards findings and metadata into **Log Analytics** as a custom table, enabling:

- Sentinel analytics rules
- Incidents and automation playbooks
- Cross-platform correlation

Required Information

You will need the following from Azure:

Field	Description
Workspace ID	Log Analytics workspace identifier
Shared Key	Primary or secondary workspace key
Log Type	Custom table name (default: AiVRIC_Findings)

Locate Workspace ID & Shared Key

1. Sign in to the **Azure Portal**
2. Navigate to **Log Analytics Workspaces**
3. Select your target workspace
4. Go to **Agents**
5. Copy:
    - **Workspace ID**
    - **Primary or Secondary Key**

Configure Sentinel Integration in AiVRIC

1. Navigate to **Configuration → Integrations**
2. Select **Azure Sentinel**
3. Click **Add Integration**

4. Enter:
    - Workspace ID
    - Shared Key
    - Log Type (default recommended)
5. Click **Create Integration**

✅ Upon successful creation, AiVRIC will begin streaming findings automatically.

Validation

- Open **Azure Sentinel → Logs**
- Query:
- AiVRIC_Findings
- Confirm records appear after the next scan or finding update

---

Splunk Integration

What Gets Sent

AiVRIC streams findings using **HTTP Event Collector (HEC)**, supporting:

- Splunk Enterprise
- Splunk Enterprise Security
- Custom dashboards and correlation searches

Required Information

Field	Description
HEC URL	HTTP Event Collector endpoint
HEC Token	Authentication token
Index	Destination index (default: main)
Source Type	Log categorization field (recommended: aivric:findings)

Configure HTTP Event Collector in Splunk

1. Log into **Splunk Web**
2. Navigate to **Settings → Data Inputs**
3. Select **HTTP Event Collector**
4. Click **New Token**
5. Configure:
    - Enable token
    - Allowed indexes
    - SSL enabled (recommended)
6. Save and copy the generated **HEC Token**

Configure Splunk Integration in AiVRIC

1. Navigate to **Configuration → Integrations**
2. Select **Splunk**
3. Click **Add Integration**
4. Enter:
    - HEC URL
      (example: https://splunk.example.com:8088/services/collector)
    - HEC Token
    - Index
    - Source Type
5. (Optional) Leave **Verify SSL Certificate** enabled
6. Click **Create Integration**

✅ Findings will begin appearing in Splunk shortly after creation.

Validation

In Splunk Search:

```
index=main sourcetype="aivric:findings"
```

Confirm events appear after scan completion or finding state changes.

Operational Notes & Best Practices

- **Near Real Time**: Events are sent as findings are created or updated—not only on scan completion
- **Deduplication**: Use `finding_id` or equivalent UUID for correlation
- **Index Management**: Consider a dedicated index for security posture data
- **Retention**: Align SIEM retention with compliance evidence needs
- **Automation**: Sentinel playbooks and Splunk SOAR are both supported downstream

---

Troubleshooting

Issue	Resolution
No data appearing	Verify credentials and network connectivity
Authentication errors	Revalidate tokens and keys
Parsing issues	Check sourcetype and JSON parsing rules
Duplicate records	Confirm correlation logic in SIEM

Summary

The AiVRIC SIEM integrations are designed to **extend—not replace—existing detection and response workflows**. By streaming normalized cloud security findings into Sentinel or Splunk, teams gain centralized visibility, historical context, and automation capabilities without manual exports or custom scripts.